Documento técnico de AWS

# Información general sobre el cumplimiento del reglamento GDPR en AWS

# Información general sobre el cumplimiento del reglamento GDPR en AWS: Documento técnico de AWS

# Table of Contents

# Información general sobre el cumplimiento del reglamento GDPR en AWS

Fecha de publicación: diciembre de 2020 (Revisiones del documento)

## Resumen

Este documento proporciona información sobre los servicios y los recursos que Amazon Web Services (AWS) ofrece a los clientes para ayudarlos a cumplir con los requisitos del Reglamento general de protección de datos (RGPD) que pueden aplicarse a sus actividades. Entre estos, se encuentran el cumplimiento de los estándares de seguridad de TI, la acreditación del Catálogo de controles de conformidad de computación en la nube (C5) de AWS, el cumplimiento del Código de conducta de los proveedores de servicios de infraestructura en la nube de Europa (CISPE), controles del acceso a los datos, herramientas de supervisión y registro, cifrado y administración de claves.

# Información general sobre el Reglamento general de protección de datos

El Reglamento general de protección de datos es una ley de privacidad europea (Reglamento 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016) que entró en vigor el 25 de mayo de 2018. El RGPD deroga la Directiva de Protección de Datos de la UE (Directiva 95/46/EC) y su objetivo es unificar las leyes de protección de datos de toda la Unión Europea (UE) mediante la aplicación de una única ley de protección de datos que sea obligatoria en todos los estados miembro.

El RGPD se aplica a todo el procesamiento de datos personales, ya sea por parte de organizaciones establecidas en la UE u organizaciones que procesan datos personales de residentes de la UE al ofrecer bienes o servicios a personas de la UE o supervisan el comportamiento de los residentes de la UE en la UE. Los datos personales son toda la información relacionada con una persona natural identificable o identificada.

## Cambios que introduce el RGPD en las organizaciones que operan en la UE

Uno de los aspectos clave del RGPD es que unifica la forma en la que los datos personales pueden procesarse, utilizarse e intercambiarse de manera segura en los estados miembro de la UE. Las organizaciones deben demostrar la protección de los datos que procesan y su cumplimiento del RGPD de manera continua mediante la implementación y la revisión frecuentes de medidas técnicas y organizativas sólidas, así como de políticas de conformidad aplicables al procesamiento de los datos personales. Las autoridades de control de la UE pueden imponer multas de hasta 20 millones de euros o el 4 % de la facturación mundial anual (lo que sea mayor) por incumplimiento del RGPD.

## Preparación de AWS para el RGPD

Los expertos en cumplimiento, protección de datos y seguridad de AWS trabajan con clientes de todo el mundo para responder a sus preguntas y ayudarlos a prepararse para ejecutar cargas de trabajo en la nube de conformidad con el RGPD. Estos equipos también revisan la preparación de AWS en relación con los requisitos del RGPD.

> **Note**
>
> Podemos afirmar que se pueden utilizar todos los servicios de AWS de conformidad con el RGPD.

## Anexo de procesamiento de datos (DPA) de AWS

AWS cuenta con un Anexo de procesamiento de datos para el cumplimiento del RGPD (DPA para RGPD), que permite a los clientes cumplir con las obligaciones contractuales del RGPD. El DPA para GDPR de AWS está integrado en los términos de servicio de AWS y se aplica automáticamente a los clientes de todo el mundo que tengan que cumplir con el RGPD.

El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea (TJUE) emitió una sentencia sobre el escudo de privacidad UE-EE. UU. y las cláusulas contractuales tipo (SCC, por sus siglas en inglés), también conocidas como “cláusulas modelo”. El TJUE dictaminó que el escudo de privacidad UE-EE. UU. ya no es válido para la transferencia de datos personales de la Unión Europea (UE) a los Estados Unidos (EE. UU.). Sin embargo, en la misma sentencia, el TJUE validó que las empresas puedan seguir utilizando las SCC como mecanismo para transferir datos fuera de la UE.

De conformidad con esta norma, los clientes y socios de AWS pueden seguir utilizando AWS para transferir su contenido de Europa a EE. UU. y a otros países, de conformidad con las leyes de protección de datos de la UE, incluido el Reglamento general de protección de datos (RGPD). Los clientes de AWS pueden confiar en las SCC incluidas en el Anexo de procesamiento de datos (DPA) de AWS si eligen transferir sus datos fuera de la Unión Europea de conformidad con el RGPD.
A medida que evolucione el panorama normativo y legislativo, trabajaremos para garantizar que nuestros clientes no dejen de disfrutar de las ventajas de AWS dondequiera que operen. Para obtener información adicional, consulte las preguntas frecuentes sobre el escudo de privacidad UE-EE.

## El papel de AWS en virtud del RGPD

AWS desempeña los roles de procesador y controlador de datos según el RGPD.

De conformidad con el artículo 32, los controladores y procesadores están obligados a “implementar medidas técnicas y organizativas adecuadas”, teniendo en cuenta “la tecnología y los costes de implementación, y la naturaleza, el alcance, el contexto y la finalidad del procesamiento, así como el riesgo de las distintas posibilidades y gravedades a las que están expuestos los derechos y las

libertades de las personas naturales". El RGPD ofrece sugerencias específicas para todos los tipos de acción de seguridad que puedan requerirse, incluidas:

- La seudonimización y el cifrado de datos personales.
- La capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los servicios y sistemas de procesamiento.
- La capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de que ocurra un incidente técnico o físico.
- Un proceso para probar, valorar y evaluar regularmente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento.

## AWS como procesador de datos

Cuando los clientes y los socios de la Red de socios de AWS (APN, por sus siglas en inglés) usan los servicios de AWS para procesar datos personales en su contenido, AWS actúa como procesador de datos. Los clientes y los socios de APN pueden utilizar los controles disponibles en los servicios de AWS, entre los que se incluyen los controles de configuración de seguridad, para procesar los datos personales. En estas circunstancias, el cliente o socio de APN puede actuar como controlador o procesador de datos, y AWS actúa como procesador o subprocesador de datos. El Anexo de procesamiento de datos (DPA) que cumple con el RGPD de AWS incorpora los compromisos de AWS como procesador de datos.

## AWS como controlador de datos

Cuando AWS recopila datos personales y determina los fines y los medios de procesamiento de dichos datos personales, actúa como controlador de datos. Por ejemplo, cuando AWS procesa la información de la cuenta para el registro de la cuenta, la administración, el acceso a los servicios o la información de contacto de la cuenta de AWS para proporcionar asistencia a través de las actividades de soporte al cliente, actúa como controlador de datos.

# Modelo de seguridad de responsabilidad compartida

La seguridad y la conformidad es una responsabilidad compartida entre AWS y el cliente. Cuando los clientes trasladan sus sistemas informáticos y los datos a la nube, las responsabilidades de seguridad se comparten entre el cliente y el proveedor de servicios en la nube. Cuando los clientes se trasladan a la nube de AWS, AWS es responsable de proteger la infraestructura

global que ejecuta todos los servicios ofrecidos en la nube de AWS. Para los servicios abstractos, como Amazon S3 y Amazon DynamoDB, AWS también es responsable de la seguridad del sistema operativo y de la plataforma. Los clientes de AWS y los socios de APN, que actúan como controladores o procesadores de datos, son responsables de todos los datos personales que suban a la nube de AWS. Las diferentes responsabilidades se diferencian normalmente como seguridad de la nube y seguridad en la nube. Este modelo compartido puede ayudar a reducir la carga operativa de los clientes y proporcionarles la flexibilidad y el control necesarios para implementar su infraestructura en la nube de AWS. Para obtener más información, consulte el modelo de responsabilidad compartida de AWS.

El RGPD no cambia el modelo de responsabilidad compartida de AWS, que continúa aplicándose a los clientes y socios de APN centrados en el uso de los servicios de computación en la nube. El modelo de responsabilidad compartida es un método útil para ilustrar las diferentes responsabilidades de AWS (como subprocesador o procesador de datos) y de los clientes o socios de APN (como controladores o procesadores de datos) según el RGPD.

# Estándares de seguridad y marco de conformidad sólidos

De conformidad con el RGPD, es posible que las medidas técnicas y organizativas adecuadas deban incluir “la capacidad para garantizar la confidencialidad, integridad, disponibilidad y adaptación continuas de los servicios y sistemas de procesamiento”, así como procesos fiables de gestión del riesgo general, de restauración y de prueba.

## Programa de conformidad de AWS

AWS conserva de manera permanente un alto estándar de seguridad y conformidad en todas sus operaciones globales. La seguridad siempre ha sido nuestra prioridad. AWS se somete regularmente a auditorías de certificación independientes de terceros para garantizar que las actividades de control funcionen según lo previsto. Más específicamente, AWS se audita en función de una variedad de marcos de seguridad globales y regionales que dependen de la región y el sector. En la actualidad, AWS participa en más de 50 programas de auditoría diferentes.

El organismo evaluador documenta los resultados de estas auditorías y los pone a disposición de todos los clientes de AWS a través de AWS Artifact. AWS Artifact es un portal de autoservicio gratuito para acceder a los informes de conformidad de AWS bajo demanda. Cuando se publican nuevos informes, estos están disponibles en AWS Artifact, lo que permite a los clientes supervisar continuamente la seguridad y la conformidad de AWS con acceso inmediato a los nuevos informes.

Los clientes pueden aprovechar las certificaciones y acreditaciones reconocidas internacionalmente, lo que demuestra conformidad con estándares internacionales estrictos, como la ISO 27017 para seguridad en la nube, la ISO 27018 para privacidad en la nube, la SOC 1, la SOC 2 y la SOC 3, PCI DSS Nivel 1 y otros. AWS también ayuda a los clientes a cumplir estándares de seguridad locales, como el catálogo de controles comunes de computación en la nube (C5) de BSI, una acreditación respaldada por el gobierno de Alemania.

Para obtener información más detallada sobre los programas de certificación de AWS, los informes y las certificaciones de terceros, consulte el tema Programas de conformidad de AWS. Para obtener información específica de los servicios, consulte el tema Servicios de AWS en el ámbito del programa de conformidad.

## Catálogo de controles de conformidad de computación en la nube

El Catálogo de controles de conformidad de computación en la nube (C5) es un esquema de certificación respaldado por el gobierno alemán introducido en Alemania por la Oficina Federal

de Seguridad de la Información (BSI, por sus siglas en alemán). Se creó para ayudar a las organizaciones a demostrar la seguridad operativa contra los ciberataques comunes en el contexto de las Recomendaciones de seguridad para los proveedores de servicios en la nube del gobierno alemán.

Las medidas técnicas y organizativas de protección de datos y las medidas de seguridad de la información apuntan a la seguridad de los datos para garantizar la confidencialidad, la integridad y la disponibilidad. El C5 define los requisitos de seguridad que también pueden ser relevantes para la protección de datos. Los clientes de AWS y sus asesores de cumplimiento pueden utilizar la certificación C5 como recurso para comprender la gama de servicios de control de seguridad de TI que AWS ofrece a medida que migran sus cargas de trabajo a la nube. El C5 agrega el nivel de seguridad de TI definido por la normativa equivalente al “IT-Grundschutz” con la incorporación de controles específicos de la nube.

El C5 agrega más controles adicionales que proporcionan información relativa a la ubicación de datos, aprovisionamiento de servicios, fuero jurisdiccional, certificación existente, obligaciones de divulgación de la información y una descripción del servicio completo. Con esta información, los clientes pueden evaluar cómo las normativas legales (es decir, la privacidad de los datos), sus propias políticas o el entorno de amenazas se relaciona con su uso de servicios de computación en la nube.

# Controles de acceso a datos

El artículo 25 del RGPD establece que el controlador “deberá implementar las medidas técnicas y organizativas adecuadas para garantizar que, de forma predeterminada, solo se procesen los datos personales necesarios para cada finalidad específica del procesamiento”. Al permitir que solo obtengan acceso a los datos de clientes y recursos de AWS los administradores, usuarios y aplicaciones autorizados, los siguientes mecanismos de control de acceso de AWS ayudan a los clientes a cumplir este requisito:

## AWS Identity and Access Management

Al crear una cuenta de AWS, se crea automáticamente una cuenta de usuario raíz para la cuenta de AWS. Esta cuenta tiene acceso completo a todos los servicios y recursos de AWS de su cuenta de AWS. En lugar de usar esta cuenta para tareas diarias, solo debe usarla para crear inicialmente roles y cuentas de usuario adicionales, y para actividades administrativas que lo requieran. AWS recomienda aplicar el principio de privilegios mínimos desde los inicios: defina diferentes cuentas de usuario y roles para diferentes tareas y especifique el conjunto mínimo de permisos necesarios para completar cada tarea. Este enfoque es un mecanismo para adaptar un concepto clave introducido en el RGPD: la protección de datos desde el proceso de diseño. AWS Identity and Access Management (IAM) es un servicio web que puede utilizar para controlar de forma segura el acceso a sus recursos de AWS.

Los usuarios y los roles definen identidades de IAM con permisos específicos. Un usuario autorizado puede asumir un rol de IAM para realizar tareas específicas. Las credenciales temporales se crean cuando se asume el rol. Por ejemplo, puede utilizar roles de IAM para proporcionar de forma segura aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2) con las credenciales temporales necesarias para acceder a otros recursos de AWS, como buckets de Amazon S3 y Amazon Relational Database Service (Amazon RDS) o bases de datos de Amazon DynamoDB. Del mismo modo, los roles de ejecución proporcionan a las funciones de AWS Lambda los permisos necesarios para acceder a otros servicios y recursos de AWS, como Amazon CloudWatch Logs para la transmisión de registros o la lectura de un mensaje desde una cola de Amazon Simple Queue Service (Amazon SQS). Al crear un rol, se añaden políticas para definir las autorizaciones.

Para ayudar a los clientes a supervisar las políticas de recursos e identificar recursos con acceso público o multicuenta que quizá no pretendían, se puede habilitar el IAM Access Analyzer para generar resultados exhaustivos que identifiquen los recursos a los que se puede acceder desde

fuera de una cuenta de AWS. El IAM Access Analyzer evalúa las políticas de recursos con la lógica matemática y la inferencia para determinar las posibles rutas de acceso permitidas por las políticas. El IAM Access Analyzer supervisa continuamente las políticas nuevas o actualizadas, y analiza los permisos otorgados mediante políticas para los roles de IAM, aunque también para los recursos de los servicios como los buckets de Amazon S3, las claves de AWS Key Management Service (AWS KMS), las colas de Amazon SQS y las funciones de AWS Lambda.

Access Analyzer para S3 le avisa de los buckets que están configurados para permitir el acceso a cualquier usuario de Internet u otras cuentas de AWS, incluidas las cuentas de AWS ajenas a su organización. Al revisar un bucket en riesgo en Access Analyzer para Amazon S3, puede bloquear todo el acceso público al bucket con un solo clic. AWS recomienda que bloquee todo el acceso a sus buckets a menos que necesite acceso público para admitir un caso de uso específico. Antes de bloquear todo el acceso público, asegúrese de que las aplicaciones sigan funcionando correctamente sin ese acceso público. Para obtener más información, consulte el tema sobre el uso de Amazon S3 para bloquear el acceso público.

IAM también proporciona la información a la que se accedió por última vez para poder identificar los permisos no utilizados y que pueda eliminarlos de las entidades principales asociadas. Con la última información a la que se accedió, puede afinar sus políticas y permitir el acceso solo a los servicios y acciones necesarios. De este modo, podrá aplicar mejor las prácticas recomendadas del principio de privilegios mínimos. Puede ver la información a la que se accedió por última vez para las entidades o políticas que existen en IAM o en todo un entorno de AWS Organizations.

## Tokens de acceso temporal a través de AWS STS

Puede utilizar el AWS Security Token Service (AWS STS) para crear y proporcionar a los usuarios de confianza credenciales de seguridad temporales que puedan otorgar acceso a sus recursos de AWS. Las credenciales de seguridad temporales funcionan prácticamente igual que las credenciales de clave de acceso a largo plazo que proporciona a sus usuarios de IAM, con las siguientes diferencias:

- Las credenciales de seguridad temporales son a corto plazo. Puede configurar el período de validez desde 15 minutos hasta un máximo de 12 horas. Cuando las credenciales temporales caducan, AWS no las reconoce ni permite ningún tipo de acceso desde las solicitudes de API que se realice con ellas.
- Las credenciales de seguridad temporales no se almacenan en la cuenta de usuario. En cambio, se generan dinámicamente y se proporcionan al usuario cuando se solicitan. Cuando (o antes de que) las credenciales de seguridad temporales caduquen, un usuario podrá solicitar credenciales nuevas, si ese usuario tiene permisos para hacerlo.

Estas diferencias proporcionan las siguientes ventajas cuando se usan credenciales temporales:

- No es necesario que distribuya ni incluya credenciales de seguridad de AWS a largo plazo en una aplicación.
- Las credenciales temporales son la base de los roles y las identidades federadas. Para proporcionar acceso a los usuarios a sus recursos de AWS, debe definir una identidad de AWS temporal para ellos.
- Las credenciales de seguridad temporales tienen una vida útil limitada y personalizable. Por ello, no tiene que rotarlas ni revocarlas explícitamente cuando ya no sean necesarias. Cuando las credenciales de seguridad temporales caducan, ya no se pueden volver a utilizar. Puede especificar el período máximo de validez de las credenciales.

## Autenticación multifactor

Para mayor seguridad, puede agregar la autenticación de dos factores a la cuenta de AWS y a los usuarios de IAM. Con la autenticación multifactor (MFA, por sus siglas en inglés) habilitada, al iniciar sesión en la consola de administración de AWS, se le solicitará su nombre de usuario y contraseña (el primer factor), así como una respuesta de autenticación del dispositivo MFA de AWS (el segundo factor). Puede habilitar la MFA para la cuenta de AWS y para usuarios concretos de IAM que haya creado en dicha cuenta. También puede utilizar la MFA para controlar el acceso a las API de servicios de AWS.

Por ejemplo, puede definir una política que permita acceso completo a todas las operaciones de la API de AWS en Amazon EC2, pero denegar explícitamente el acceso a operaciones de la API específicas, como `StopInstances` y `TerminateInstances`, si el usuario no está autenticado mediante la MFA.

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Sid”: “AllowAllActionsForEC2”,
        “Effect”: “Allow”,
        “Action”: “ec2:*”,
        “Resource”: “*”
     },
    {
```

```
                "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
                "Effect": "Deny",
                "Action": [
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Resource": "*",
                "Conditions": {
                    "BoolIfExists": {"aws:MultiFactorAuthPresent":false}
                }
            }
        }
}
```

Para añadir una capa adicional de seguridad a los buckets de Amazon S3, puede configurar la eliminación con MFA, que requiere autenticación adicional para cambiar el estado de versiones de un bucket y eliminar permanentemente una versión de objeto. Por lo tanto, la eliminación con MFA refuerza la seguridad en caso de que sus credenciales de seguridad estén en riesgo.

Para usar la eliminación con MFA, puede utilizar hardware o un dispositivo MFA virtual para generar un código de autenticación. Consulte la página Autenticación multifactor para obtener una lista de los dispositivos MFA virtuales o de hardware compatibles.

## Acceso a recursos de AWS

Para implementar el acceso pormenorizado a sus recursos de AWS, puede otorgar diferentes niveles de permisos a diferentes personas en función de los recursos. Por ejemplo, puede permitir que solo algunos usuarios tengan acceso total a Amazon EC2, Amazon S3, DynamoDB, Amazon Redshift y a otros servicios de AWS.

Para otros usuarios, puede permitir el acceso de solo lectura a algunos buckets de Amazon S3; permitir la administración de únicamente algunas instancias de Amazon EC2 o el acceso solo a la información de facturación.

La siguiente política es un ejemplo de un método que puede utilizar para permitir todas las acciones en un bucket de Amazon S3 específico y denegar explícitamente el acceso a todos los servicios de AWS que no sean Amazon S3.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

Puede adjuntar una política a una cuenta de usuario o a un rol. Para ver otros ejemplos de políticas de IAM, consulte el tema sobre ejemplos de políticas basadas en identidad de IAM.

## Definición de límites para acceder a servicios regionales

Como cliente, sigue siendo propietario del contenido y puede seleccionar qué servicios de AWS pueden procesar el contenido, almacenarlo y alojarlo. AWS no puede accede al contenido ni usarlo para ningún otro fin sin su consentimiento. Según el modelo de responsabilidad compartida, usted elige las regiones de AWS en las que se almacena el contenido, lo que le permite implementar los servicios de AWS en las ubicaciones que elija, de acuerdo con los requisitos geográficos que especifique. Por ejemplo, si desea asegurarse de que el contenido se encuentre solo en Europa, puede optar por implementar los servicios de AWS exclusivamente en una de las regiones europeas de AWS.

Las políticas de IAM proporcionan un mecanismo simple para limitar el acceso a los servicios en regiones específicas. Puede añadir una condición global (`aws:RequestedRegion`) a las políticas de IAM adjuntas a las entidades principales de IAM para aplicarla a todos los servicios de AWS. Por ejemplo, la siguiente política utiliza el elemento `NotAction` con el efecto `Deny`, que niega

explícitamente el acceso a todas las acciones que no figuran en la declaración si la región solicitada no es europea. No se deben negar las acciones en los servicios de CloudFront, IAM, Amazon Route 53 y AWS Support porque se trata de servicios globales populares de AWS.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “DenyAllOutsideRequestedRegions”,
                “Effect”: “Deny”,
                “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     ”route53:*”,
                     “support:*”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “StringNotLike”: {
                        “aws:RequestedRegion”: [
                              “eu-*”
                        ]
                     }
                  }
           }
          ]
}
```

Esta política de IAM de ejemplo también se puede implementar como política de control de servicios (SCP, por sus siglas en inglés) en AWS Organizations, que define los límites de los permisos que se aplican a cuentas o unidades organizativas (OU) de AWS específicas dentro de una organización. Esto le permite controlar el acceso de los usuarios a los servicios regionales en entornos complejos de varias cuentas.

Existen capacidades de limitación geográfica para las regiones que se acaben de lanzar. Las regiones introducidas después del 20 de marzo de 2019 están desactivadas de forma predeterminada. Debe habilitar estas regiones para poder usarlas. Si una región de AWS está deshabilitada de forma predeterminada, puede utilizar la consola de administración de AWS para habilitarla y deshabilitarla. La habilitación y deshabilitación de regiones de AWS permite controlar si

los usuarios de su cuenta de AWS pueden acceder a los recursos de esa región. Para obtener más información, consulte el tema sobre la administración de regiones de AWS.

## Control del acceso a aplicaciones web y móviles

AWS proporciona servicios para administrar el control de acceso a los datos en las aplicaciones del cliente. Si necesita añadir funciones de inicio de sesión y control de acceso de usuarios a sus aplicaciones web y móviles, puede utilizar Amazon Cognito. Los grupos de usuarios de Amazon Cognito le ofrecen un directorio de usuarios seguro con capacidad de escalado para gestionar cientos de millones de usuarios. Puede añadir la autenticación multifactor a su grupo de usuarios para proteger la identidad de los usuarios. También puede utilizar la autenticación flexible, que usa un modelo basado en riesgos, para predecir cuándo es posible que sea necesario utilizar otro factor de autenticación.

Con los grupos de identidades de Amazon Cognito (identidades federadas), puede ver quién ha accedido a sus recursos y desde dónde (aplicación móvil o web). Puede usar esta información para crear roles y políticas de IAM que permitan o denieguen el acceso a un recurso en función del tipo de origen de acceso (aplicación móvil o web) y del proveedor de identidades.

# Monitorización y registro

El artículo 30 del RGPD requiere que “cada controlador y, cuando proceda, el representante del controlador mantengan un registro de las actividades de procesamiento bajo su responsabilidad”. Este artículo también incluye detalles sobre la información que debe registrarse al supervisar el procesamiento de todos los datos personales. Los controladores y procesadores también deben enviar notificaciones de vulneración de los datos de manera oportuna, por lo que es importante detectar los incidentes rápidamente. Para ayudar a los clientes a cumplir con estas obligaciones, AWS ofrece los siguientes servicios de supervisión y registro.

## Administración y configuración de los recursos con AWS Config

AWS Config brinda una visión detallada de la configuración de los tipos de recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.

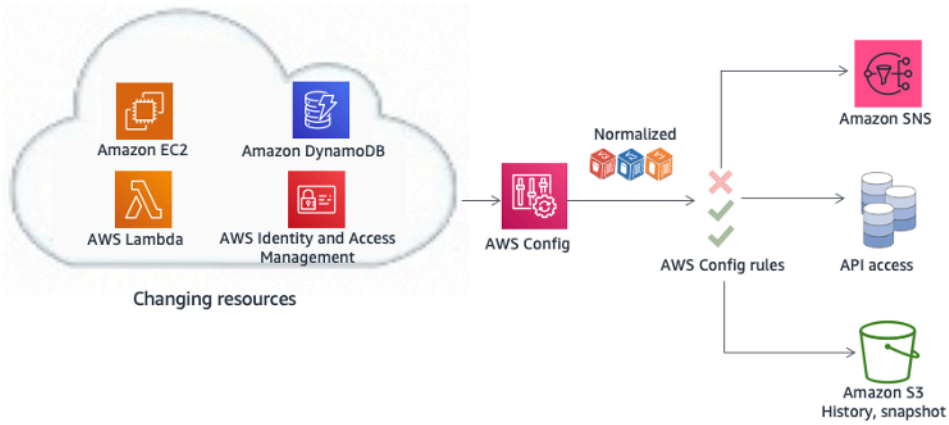


Ilustración 1 - Supervisión de los cambios de configuración a lo largo del tiempo con AWS Config

Un recurso de AWS es una entidad que puede funcionar en AWS, como una instancia de EC2, un volumen de Amazon Elastic Block Store (Amazon EBS), un grupo de seguridad o una Amazon Virtual Private Cloud (Amazon VPC). Para obtener una lista completa de los recursos de AWS compatibles con AWS Config, consulte el tema sobre tipos de recursos de AWS admitidos.

Con AWS Config puede hacer lo siguiente:

- Evaluar las configuraciones de recursos de AWS para verificar que la configuración sea correcta.

- Obtener una instantánea de las configuraciones actuales de los recursos admitidos asociados a su cuenta de AWS.
- Recuperar las configuraciones de uno o más recursos existentes en la cuenta.
- Recuperar las configuraciones históricas de uno o más recursos.
- Recibir una notificación cuando se cree, modifique o elimine un recurso.
- Ver las relaciones entre los recursos. Por ejemplo, puede buscar todos los recursos que usen un grupo de seguridad en particular.

## Auditoría de cumplimiento y análisis de seguridad

AWS CloudTrail le permite supervisar de forma continua la actividad de la cuenta de AWS. Se genera un historial de las llamadas a la API de AWS de su cuenta, incluidas las llamadas a la API realizadas mediante la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y los servicios de AWS de nivel superior. Puede identificar los usuarios y las cuentas que han llamado a las API de AWS para servicios compatibles con CloudTrail, la dirección IP desde la que se efectuaron y cuándo se realizaron. Puede integrar CloudTrail en las aplicaciones con la API, automatizar la creación de trazos en su organización, comprobar el estado de los trazos y controlar la manera en que los administradores activan y desactivan el registro en CloudTrail.

Los registros de CloudTrail se pueden agregar desde varias regiones y varias cuentas de AWS en un único bucket de Amazon S3. AWS recomienda escribir registros, especialmente los registros de AWS CloudTrail, en un bucket de Amazon S3 con acceso restringido en una cuenta de AWS designada para el registro (Log Archive). Los permisos del bucket deben evitar la eliminación de los registros. Además, deben cifrarse en reposo mediante el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) o claves administradas por AWS KMS (SSE-KMS). Puede usar la validación de la integridad de los archivos de registro de CloudTrail para determinar si un archivo de registro se ha modificado, eliminado o continúa igual después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta difícil desde el punto de vista informático modificar, eliminar o falsificar archivos de registro de CT sin que se sepa. Puede utilizar la AWS Command Line Interface (AWS CLI) para validar los archivos en la ubicación en la que los entregó CloudTrail.

Los registros de CloudTrail añadidos a un bucket de Amazon S3 se pueden analizar con fines de auditoría o para actividades de resolución de problemas. Una vez centralizados los registros, puede integrarlos con soluciones de administración de eventos e información de seguridad (SIEM) o utilizar

los servicios de AWS, como Amazon Athena o CloudTrail Insights, para analizarlos y visualizarlos con los paneles de Amazon QuickSight. Una vez centralizados los registros de CloudTrail, también puede usar la misma cuenta de Log Archive para centralizar los registros de otros orígenes, como CloudWatch Logs y los equilibradores de carga de AWS.

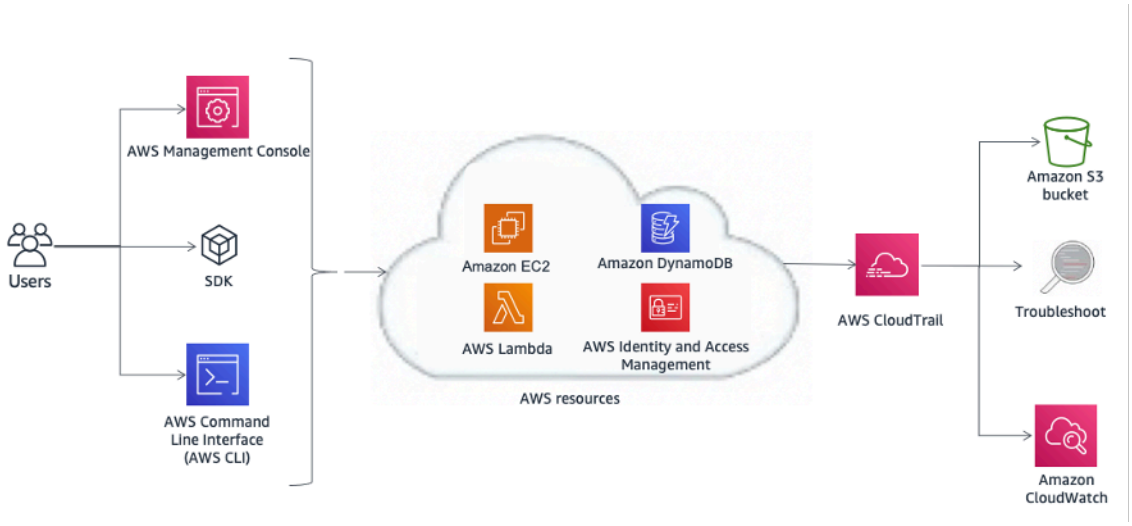


Ilustración 2 - Ejemplo de arquitectura para la auditoría de conformidad y el análisis de seguridad con AWS CloudTrail

Los registros de AWS CloudTrail también pueden desencadenar eventos de Amazon CloudWatch preconfigurados. Puede usar estos eventos para notificar a los usuarios o sistemas que se ha producido un evento o para acciones de corrección. Por ejemplo, si desea supervisar las actividades de las instancias de Amazon EC2, puede crear una regla de eventos de CloudWatch. Cuando se produzca una actividad específica en la instancia de Amazon EC2 y el evento se capture en los registros, la regla desencadenará una función de AWS Lambda, que enviará un correo electrónico de notificación sobre el evento al administrador. (Consulte la ilustración 3). El correo electrónico incluye detalles sobre el momento en que tuvo lugar el evento, el usuario que realizó la acción, detalles de Amazon EC2 y mucho más. En el siguiente diagrama se muestra la arquitectura de la notificación de eventos.

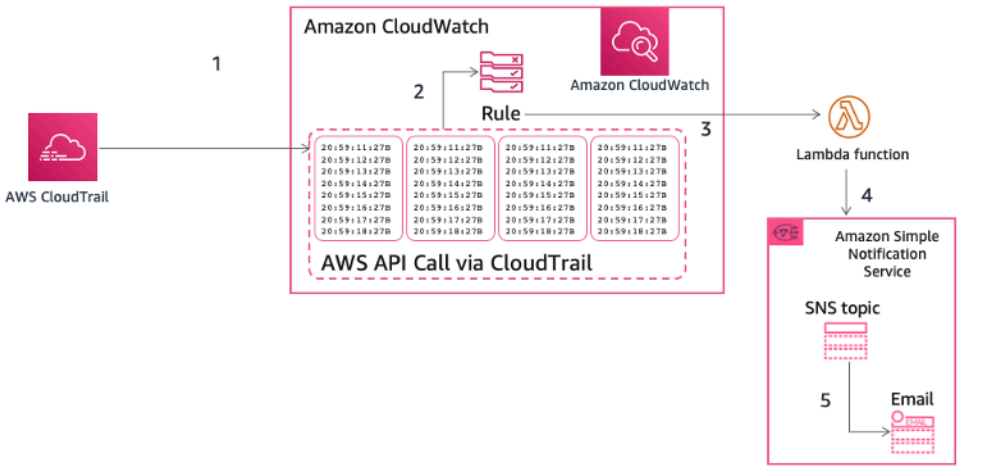


Ilustración 3 — Ejemplo de notificación de eventos de AWS CloudTrail

# Recopilación y procesamiento de registros

CloudWatch Logs se puede utilizar para supervisar, almacenar y acceder a los archivos de registro desde las instancias de Amazon EC2, AWS CloudTrail, Route 53 y otros orígenes. Consulte la página de documentación de los servicios de AWS que publican registros en CloudWatch Logs.

La información de los registros puede incluir:

- Registro pormenorizado de acceso a objetos de Amazon S3
- Información detallada sobre flujos en la red mediante registro de flujos de VPC
- Verificación de configuración basada en reglas y acciones con reglas de AWS Config
- Filtrado y supervisión del acceso HTTP a las aplicaciones con funciones de firewall de aplicaciones web (WAF, por sus siglas en inglés) en CloudFront

Las métricas y los registros de aplicaciones personalizados también se pueden publicar en CloudWatch Logs mediante la instalación de CloudWatch Agent en instancias de Amazon EC2 o en servidores locales.

Los registros se pueden analizar de forma interactiva con CloudWatch Logs Insights, realizando consultas para ayudarlo a responder de manera más eficiente y efectiva a los problemas operativos.

CloudWatch Logs se puede procesar casi en tiempo real mediante la configuración de filtros de suscripción y se puede entregar a otros servicios, como un clúster de Amazon OpenSearch Service

(OpenSearch Service), una transmisión de Amazon Kinesis, una transmisión de Amazon Kinesis Data Firehose o Lambda para el procesamiento, el análisis o la carga en otros sistemas de forma personalizada.

Los filtros de métricas de CloudWatch se pueden usar para definir patrones que se deben buscar en los datos de registro, transformarlos en métricas numéricas de CloudWatch y configurar alarmas en función de los requisitos de su empresa. Por ejemplo, siguiendo la recomendación de AWS de no utilizar el usuario raíz para las tareas cotidianas, se puede configurar un filtro de métricas de CloudWatch específico en un registro de CloudTrail (entregado a CloudWatch Logs) para crear una métrica personalizada y configurar una alarma para notificar a las partes interesadas cuando se utilicen credenciales raíz para acceder a la cuenta de AWS.

Los registros de acceso al servidor de Amazon S3, los registros de acceso a Elastic Load Balancing, los registros de flujos de VPC y los registros de flujos de AWS Global Accelerator se pueden entregar directamente a un bucket de Amazon S3. Por ejemplo, si habilita los registros de acceso al servidor de Amazon Simple Storage Service, puede obtener información detallada sobre las solicitudes que se realizan al bucket de Amazon S3. Un registro de acceso contiene detalles sobre la solicitud, como el tipo de solicitud, los recursos especificados en la solicitud y la fecha y hora en que se procesó la solicitud. Para obtener más información acerca del contenido de un mensaje de registro, consulte el tema sobre el formato de registro de acceso al servidor del servicio de Amazon Simple Storage en la guía para desarrolladores del servicio de Amazon Simple Storage. Los registros de acceso del servidor resultan útiles para muchas aplicaciones, ya que ofrecen a los propietarios del bucket información clave sobre la naturaleza de las solicitudes realizadas por clientes que no están bajo su control. De manera predeterminada, Amazon S3 no recopila registros de acceso al servicio, pero, si activa el registro, Amazon S3 suele enviar registros de acceso a su bucket en el plazo de unas horas. Si necesita una entrega más rápida o entregar registros a varios destinos, considere usar registros de CloudTrail o una combinación de registros de CloudTrail y Amazon S3. Los registros se pueden cifrar en reposo configurando el cifrado de objetos predeterminado en el bucket de destino. Los objetos se cifran con el cifrado del lado del servidor con las claves administradas de Amazon S3 (SSE-S3) o las claves maestras del cliente (CMK, por sus siglas en inglés) almacenadas en AWS Key Management Service (AWS KMS).

Los registros almacenados en un bucket de Amazon S3 se pueden consultar y analizar con Amazon Athena. Amazon Athena es un servicio de consultas interactivo que le permite analizar datos en S3 con SQL estándar. Se puede usar Athena para ejecutar consultas ad-hoc con ANSI SQL, sin necesidad de combinar ni cargar datos en Athena. Athena puede procesar conjuntos de datos no estructurados, semiestructurados y estructurados, y se integra con Amazon QuickSight para una visualización sencilla.

Los registros también son una fuente de información útil para la detección automatizada de amenazas. Amazon GuardDuty es un servicio de supervisión de seguridad continuo que analiza y procesa eventos de varias fuentes, como registros de flujos de VPC, registros de eventos de administración de CloudTrail, registros de eventos de datos de Amazon S3 de CloudTrail y registros de DNS. Utiliza fuentes de información de amenazas, como listas de direcciones IP y dominios maliciosos, y machine learning para identificar toda actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS. Al habilitar GuardDuty en una región, el servicio comienza a analizar inmediatamente los registros de eventos de CloudTrail. Además, consume la administración de CloudTrail y los eventos de datos de Amazon S3 directamente desde CloudTrail a través de un flujo de eventos independiente y duplicativo.

## Detección y protección de datos a escala con Amazon Macie

El artículo 32 del RGPD establece que “el controlador y el procesador deberán implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, según corresponda: [...]

(b) la capacidad para garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia continuas de los servicios y sistemas de procesamiento.

[…]

(d) un proceso para probar, examinar y evaluar periódicamente la efectividad de las medidas técnicas y organizativas a fin de garantizar la seguridad del procesamiento”.

Tener un proceso de clasificación de datos continuo es fundamental para adaptar el procesamiento de datos de seguridad a la naturaleza de los datos. Si su organización administra datos confidenciales, supervise dónde residen, protéjalos adecuadamente y proporcione pruebas de que aplica la seguridad y la privacidad de los datos según sea necesario para cumplir con los requisitos de cumplimiento normativo. Para ayudar al cliente a identificar y proteger su información confidencial a escala, AWS ofrece Amazon Macie, un servicio de seguridad y privacidad de datos totalmente administrado que utiliza modelos de machine learning y coincidencia de patrones para la detección de información de identificación personal (PII, por sus siglas en inglés) para detectar y proteger la información confidencial almacenada en los buckets de S3. Amazon Macie escanea estos buckets y los categoriza con identificadores de datos administrados diseñados para detectar varias categorías de información confidencial. Macie puede detectar la PII, por ejemplo, el nombre completo, la dirección de correo electrónico, la fecha de nacimiento, el número de identificación nacional, el número de identificación fiscal o el número de referencia. El cliente puede definir identificadores

de datos personalizados que reflejen los escenarios particulares de su organización (por ejemplo, números de cuenta de clientes o clasificación de datos interna).

Amazon Macie evalúa continuamente el objeto dentro de los buckets y proporciona automáticamente un resumen de los resultados (ilustración 4) de cualquier dato no cifrado o de acceso público detectado que coincida con la categoría de datos definida. Estos datos pueden incluir alertas de objetos o buckets no cifrados y de acceso público que se compartan con cuentas de AWS que estén fuera de los límites definidos en AWS Organizations. Amazon Macie se integra con otros servicios de AWS, como AWS Security Hub, para generar resultados de seguridad procesables y proporcionar una acción automática y reactiva a los resultados (ilustración 5).

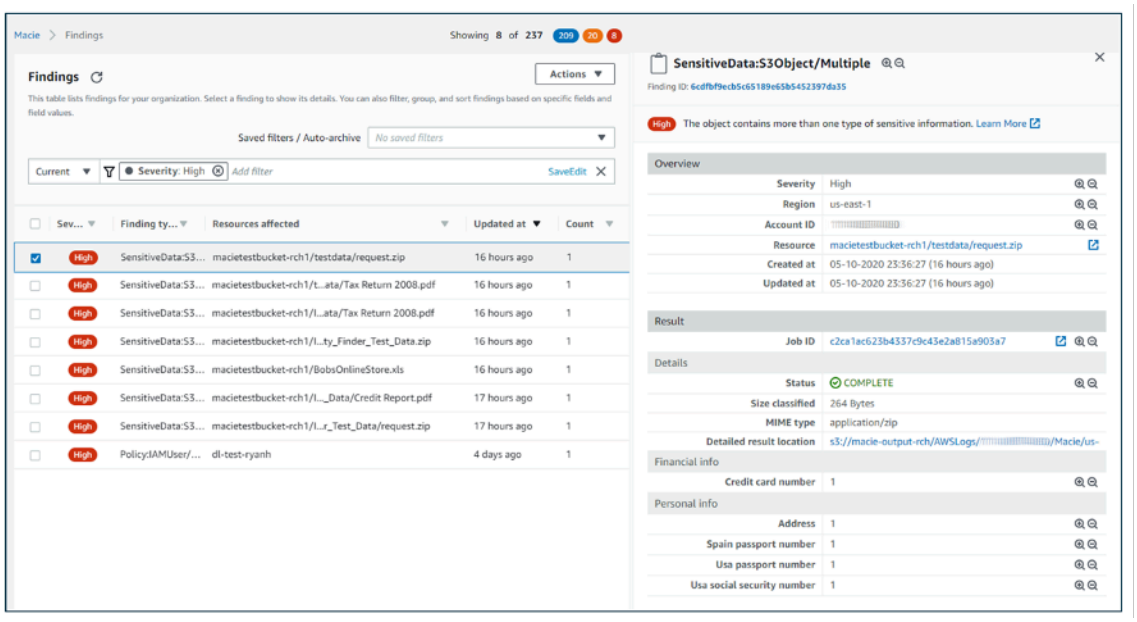


Ilustración 4 — Ejemplo de inspecciones de datos y resultados

## Administración centralizada de la seguridad

Muchas organizaciones se enfrentan a desafíos relacionados con la visibilidad y la administración centralizada de sus entornos. A medida que crece la huella operativa, este desafío puede agravarse a menos que estudie cuidadosamente sus diseños de seguridad. La falta de conocimiento, combinada con una gestión descentralizada y desigual de los procesos de gobernanza y seguridad, puede hacer que su entorno sea vulnerable.

AWS proporciona herramientas que lo ayudan a abordar algunos de los requisitos más desafiantes de la gestión y la gobernanza de TI, además de ofrecer un enfoque de protección de datos por diseño.

AWS Control Tower proporciona un método para configurar y regir un entorno de AWS de varias cuentas nuevo y seguro. Aquí se automatiza la configuración de una zona de aterrizaje, que es un entorno de varias cuentas que se basa en esquemas de prácticas recomendadas y permite la gobernanza mediante barreras de protección que puede elegir de una lista preempaquetada. Las barreras de protección implementan reglas de gobernanza para la seguridad, el cumplimiento y las operaciones. AWS Control Tower proporciona administración de identidades mediante el directorio AWS IAM Identity Center (IAM Identity Center) predeterminado y permite la auditoría multicuenta mediante IAM Identity Center y IAM. También centraliza los registros procedentes de CloudTrail y de AWS Config, que se almacenan en Amazon S3.

AWS Security Hub es otro servicio que apoya la centralización y puede mejorar la visibilidad de una organización. Security Hub centraliza y prioriza los hallazgos de seguridad y cumplimiento de todas las cuentas y servicios de AWS, como Amazon GuardDuty y Amazon Inspector. Además, se puede integrar con el software de seguridad de socios externos para ayudarlo a analizar las tendencias de seguridad e identificar problemas de seguridad de máxima prioridad.

Amazon GuardDuty es un servicio de detección de amenazas inteligente que puede ayudar a los clientes a supervisar y proteger con mayor precisión y facilidad sus cuentas, cargas de trabajo y datos de AWS almacenados en Amazon S3. GuardDuty analiza miles de millones de eventos de sus cuentas de AWS de varios orígenes, incluidos eventos de administración de AWS CloudTrail, eventos de datos de Amazon S3 de CloudTrail, registros de flujo de Amazon Virtual Private Cloud y registros de DNS. Por ejemplo, detecta llamadas a la API inusuales, comunicaciones de salida sospechosas hacia direcciones IP malintencionadas conocidas o posibles robos de datos mediante consultas de DNS como mecanismo de transporte. GuardDuty puede proporcionar resultados más precisos al aprovechar la inteligencia contra amenazas impulsada por el machine learning y los socios de seguridad externos.

Amazon Inspector es un servicio automático de evaluación de la seguridad que ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones implementadas en las instancias de Amazon EC2. Amazon Inspector evalúa automáticamente las aplicaciones en busca de exposiciones, vulnerabilidades y desviaciones de las prácticas recomendadas. Después de la evaluación, Amazon Inspector genera una lista detallada de problemas de seguridad ordenados por nivel de gravedad.

Amazon CloudWatch Events le permite configurar la cuenta de AWS para enviar eventos a otras cuentas de AWS o convertirse en receptor de eventos de otras cuentas u organizaciones. Este mecanismo puede resultar muy útil para implementar escenarios de respuesta a incidentes entre cuentas, pues se pueden tomar las medidas correctivas oportunas (por ejemplo, llamar a una función

de Lambda o ejecutar un comando en una instancia de Amazon EC2) según sea necesario cada vez que se produzca un incidente de seguridad.

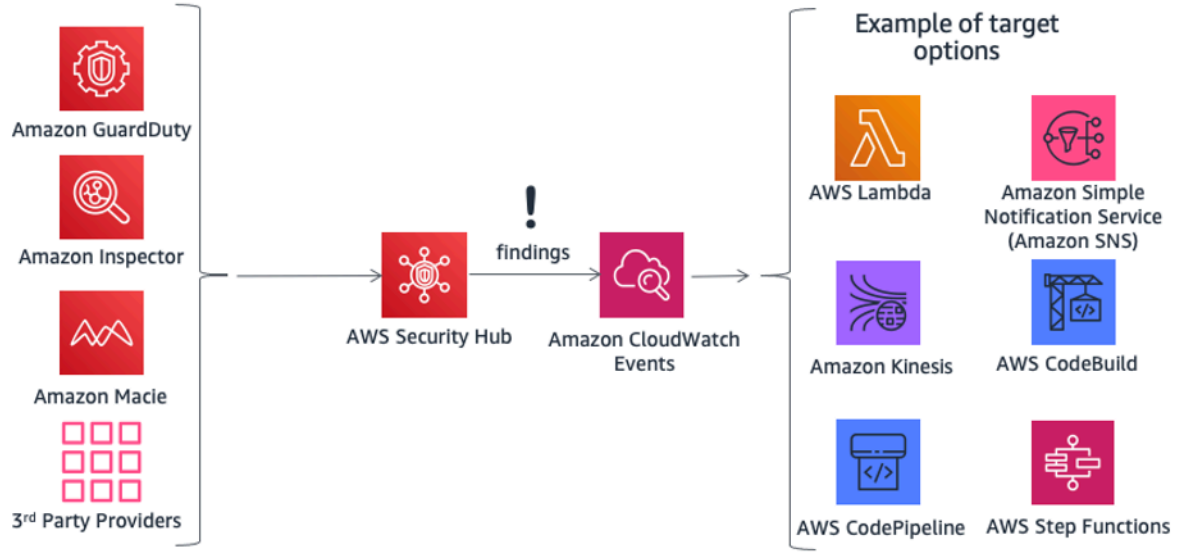


Ilustración 5 - Toma de medidas con AWS Security Hub y Amazon CloudWatch Events

AWS Organizations le ayuda a administrar y gobernar de manera centralizada entornos complejos. Le permite controlar el acceso, el cumplimiento y la seguridad en un entorno de varias cuentas. AWS Organizations admite políticas de control de servicios (SCP, por sus siglas en inglés), que definen las acciones de servicio de AWS que se pueden usar con cuentas o unidades organizativas (OU) específicas dentro de una organización.

AWS Systems Manager le ofrece visibilidad y control de la infraestructura de AWS. Puede ver los datos operativos de varios servicios de AWS desde una consola unificada y automatizar las tareas operativas en todos ellos. Puede obtener información sobre las actividades recientes de la API, los cambios en la configuración de los recursos, las alertas operativas, el inventario de software y el estado de cumplimiento de las revisiones. Al utilizar la integración con otros servicios de AWS, también puede tomar medidas sobre los recursos en función de las necesidades operativas, para ayudar a que su entorno sea conforme.

Por ejemplo, al integrar Amazon Inspector con AWS Systems Manager, las evaluaciones de seguridad se simplifican y automatizan, ya que puede instalar el agente de Amazon Inspector automáticamente con Amazon Elastic Compute Cloud Systems Manager al lanzar una instancia de Amazon EC2. También puede realizar correcciones automáticas de los resultados de Amazon Inspector mediante las funciones de Amazon EC2 System Manager y Lambda.

# Protección de sus datos en AWS

El artículo 32 del RGPD requiere que las organizaciones “implementen medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para el riesgo, entre las que se incluyen (...) la seudonimización y el cifrado de datos personales [...]”. Además, las organizaciones deben protegerse de la divulgación o el acceso no autorizado a datos personales.

El cifrado reduce los riesgos asociados con el almacenamiento de datos personales porque los datos no se pueden leer sin la clave correcta. Una estrategia de cifrado exhaustiva puede ayudar a mitigar el impacto de varios eventos de seguridad, incluidas algunas brechas de seguridad.

## Cifrado de los datos en reposo

El cifrado de los datos en reposo es vital para el cumplimiento normativo y la protección de los datos. El cifrado ayuda a garantizar que ningún usuario o aplicación pueda leer la información confidencial guardada en las unidades sin una clave válida. AWS ofrece varias opciones para el cifrado en reposo y la administración de claves de cifrado. Por ejemplo, puede usar el SDK de cifrado de AWS con una CMK creada y administrada en AWS KMS para cifrar datos arbitrarios.

Los datos cifrados se pueden almacenar de forma segura en reposo y solo los puede descifrar quien tenga acceso autorizado a la CMK. En consecuencia, recibe los datos cifrados en sobres confidenciales, mecanismos de políticas para la autorización y cifrado autenticado, y el registro de auditoría mediante AWS CloudTrail. Algunos de los servicios básicos de AWS tienen funciones integradas de cifrado en reposo, que ofrecen la opción de cifrar los datos antes de que se escriban en un almacenamiento no volátil. Por ejemplo, puede cifrar volúmenes de Amazon EBS y configurar buckets de Amazon S3 para el cifrado del lado del servidor (SSE) mediante el cifrado AES-256. Amazon S3 también admite el cifrado del lado del cliente, lo que le permite cifrar los datos antes de enviarlos a Amazon S3. Los SDK de AWS admiten el cifrado del lado del cliente para facilitar las operaciones de cifrado y descifrado de objetos. Amazon RDS también admite el cifrado de datos transparente (TDE, por sus siglas en inglés).

Se pueden cifrar datos en almacenes de instancias de Amazon EC2 de Linux mediante el uso de bibliotecas de Linux integradas. Mediante este método se cifran los archivos de forma transparente, lo que protege los datos confidenciales. Como resultado, las aplicaciones que procesan los datos ignoran el cifrado a nivel del disco.

Puede usar dos métodos para cifrar archivos en almacenes de instancias:

- Cifrado en el nivel del disco: con este método, se cifra todo el disco (o un bloque dentro del disco) con una o más claves de cifrado. El cifrado del disco funciona por debajo del nivel de sistema de archivos, es independiente del sistema operativo y oculta información sobre el archivo y el directorio, como el nombre y el tamaño. El sistema de cifrado de archivos, por ejemplo, es una extensión de Microsoft para el sistema New Technology File System (NTFS) del sistema operativo Windows NT que proporciona cifrado del disco.
- Cifrado en el nivel del sistema de archivos: con este método, se cifran los archivos y directorios, pero no todo el disco o la partición. El cifrado del sistema de archivos funciona sobre el sistema de archivos y se puede transferir a diversos sistemas operativos.

Para los volúmenes de almacén de instancias SSD de memoria rápida no volátil (NVMe, por sus siglas en inglés), el cifrado en el nivel del disco es la opción predeterminada. Los datos incluidos en el almacenamiento de instancias de NVMe se cifran mediante un cifrado de bloques XTS-AES-256 en un módulo de hardware de la instancia. Las claves de cifrado se generan mediante el módulo de hardware y son únicas para cada dispositivo de almacenamiento de instancias de NVMe. Todas las claves de cifrado se destruyen cuando se detiene o termina la instancia y no se pueden recuperar. No puede usar sus propias claves de cifrado.

## Cifrado de los datos en tránsito

AWS recomienda encarecidamente cifrar los datos en tránsito de un sistema a otro, incluidos los recursos dentro y fuera de AWS.

Al crear una cuenta de AWS, se le aprovisiona una sección lógicamente aislada de la nube de AWS, la nube privada virtual de Amazon (Amazon VPC). Allí, puede lanzar recursos de AWS en una red virtual que haya definido. Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y de puertas de enlace de red. También puede crear una conexión de red privada virtual (VPN) de hardware entre el centro de datos de la empresa y Amazon VPC, y utilizar la nube de AWS como una extensión del centro de datos corporativo.

Para proteger la comunicación entre su Amazon VPC y su centro de datos corporativo, puede seleccionar entre varias opciones de conectividad de VPN y elegir la que mejor se adapte a sus necesidades. Puede utilizar la AWS Client VPN para permitir el acceso seguro a sus recursos de AWS mediante servicios de VPN basados en clientes. También puede utilizar un dispositivo de VPN por software de terceros disponible en AWS Marketplace, que puede instalar en una instancia de Amazon EC2 en su Amazon VPC. Como alternativa, puede crear una conexión de VPN IPsec para

proteger la comunicación entre la VPC y la red remota. Puede utilizar AWS Direct Connect para crear una conexión privada dedicada desde la red remota a su Amazon VPC. Esta conexión se puede combinar con AWS Site-to-Site VPN para crear una conexión privada con cifrado IPsec.

AWS proporciona puntos de conexión HTTPS mediante el protocolo TLS para la comunicación, que proporciona cifrado en tránsito cuando utiliza las API de AWS. Puede usar el servicio AWS Certificate Manager (ACM) para generar, administrar e implementar los certificados públicos y privados que utiliza para establecer el transporte cifrado entre sistemas para sus cargas de trabajo. Elastic Load Balancing se integra con ACM y se usa para admitir protocolos HTTPS. Si su contenido se distribuye a través de Amazon CloudFront, entonces admite puntos de conexión cifrados.

## Herramientas de cifrado

AWS ofrece varios servicios, herramientas y mecanismos de cifrado de datos altamente escalables para ayudar a proteger los datos almacenados y procesados en AWS. Para obtener información sobre la funcionalidad y la privacidad de los servicios de AWS, consulte el tema Características de privacidad de los servicios de AWS.

Los servicios criptográficos de AWS utilizan una amplia gama de tecnologías de cifrado y almacenamiento diseñadas para mantener la integridad de sus datos en reposo o en tránsito. AWS ofrece cuatro herramientas principales para las operaciones criptográficas.

- AWS Key Management Service(AWS KMS) es un servicio administrado de AWS que genera y administra tanto claves maestras como claves de datos. AWS KMS se integra con muchos servicios de AWS para proporcionar cifrado de datos del lado del servidor mediante claves AWS KMS de cuentas de clientes. Los módulos de seguridad de hardware (HSM, por sus siglas en inglés) de AWS KMS están validados por FIPS 140-2 Nivel 2.
- AWS CloudHSM proporciona HSM validados por FIPS 140-2 Nivel 3. Almacenan de forma segura una variedad de claves criptográficas autogestionadas, incluidas las claves maestras y las claves de datos.
- Herramientas y servicios de criptografía de AWS
  - El SDK de cifrado de AWS proporciona una biblioteca de cifrado del lado del cliente para implementar operaciones de cifrado y descifrado en todo tipo de datos.
  - Amazon DynamoDB Encryption Client proporciona una biblioteca de cifrado del lado del cliente para cifrar tablas de datos antes de enviarlas a un servicio de base de datos, como Amazon DynamoDB.

# AWS Key Management Service

AWS Key Management Service es un servicio administrado que facilita la creación y el control de las claves de cifrado que se utilizan para cifrar los datos. Además, utiliza módulos de seguridad de hardware (HSM) para proteger la seguridad de sus claves. AWS KMS se integra con otros servicios de AWS para ayudarlo a proteger los datos que almacene con estos servicios. AWS KMS también se integra con AWS CloudTrail para proporcionarle registros de todo su uso clave en función de los requisitos normativos y de cumplimiento.

Puede crear e importar claves y asignarlas a otros usuarios, así como definir políticas de uso y auditar el uso de forma sencilla desde la AWS Management Console o mediante el SDK o la CLI de AWS.

Las claves maestras de AWS KMS, tanto si las ha importado como si KMS las ha creado por usted, se almacenan cifradas en un almacén de larga duración para garantizar su recuperación cuando sea necesario. Puede optar por que KMS asigne automáticamente las CMK creadas en KMS a otros usuarios una vez al año sin necesidad de tener que volver a cifrar los datos que ya se han cifrado con la clave maestra. No necesita realizar un seguimiento de las versiones anteriores de las CMK porque KMS las mantiene disponibles para descifrar los datos cifrados anteriormente.

Para cualquier CMK de AWS KMS, puede controlar quién tiene acceso a esas claves y con qué servicios se pueden usar mediante una serie de controles de acceso, incluidas las concesiones y las condiciones de políticas clave dentro de las políticas clave o políticas de IAM. También puede importar claves de su infraestructura de administración de claves y utilizarlas en KMS.

Por ejemplo, la siguiente política utiliza la condición `kms:ViaService` para permitir que una CMK administrada por el cliente se use para las acciones especificadas solo cuando la solicitud provenga de Amazon EC2 o Amazon RDS en una región específica (us-west-2) en nombre de un usuario específico (`ExampleUser`).

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Effect”: “Allow”,
        “Principal”: {
            “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
         }
```

```
                “Action”: [
                     “kms:Encrypt*”,
                     “kms:Decrypt”,
                     “kms:ReEncrypt*”,
                     “kms:GenerateDataKey*”,
                     “kms:CreateGrant”,
                     “kms:ListGrants”,
                     “kms:DescribeKey”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “ForAnyValue:StringEquals”: {
                        “kms:ViaService”: [
                              “ec2.us-west-2.amazonaws.com”,
                              “rds.us-west-2.amazonaws.com”
                        ]
                     }
               }
}
```

## Integración con servicios de AWS

AWS KMS se ha integrado con varios servicios de AWS. Consulte el sitio web de KMS para obtener una lista completa de los servicios integrados. Estas integraciones le permiten usar las CMK de AWS KMS fácilmente para cifrar los datos que almacena con estos servicios. Además de usar una CMK administrada por el cliente, varios de los servicios integrados le permiten usar una CMK administrada por AWS que se crea y administra automáticamente, pero que solo se puede utilizar en el servicio específico que la creó.

## Funciones de auditoría

AWS CloudTrail registra cada uso de una clave almacenada en AWS KMS en un archivo de registro que se entrega al bucket de Amazon S3 especificado en la configuración de CloudTrail. La información registrada incluye detalles del usuario, la hora, la fecha y la operación ejecutada y la clave utilizada.

## Seguridad

AWS KMS se ha diseñado para garantizar que nadie tenga acceso a las claves maestras. El servicio se basa en sistemas diseñados para proteger las claves maestras con técnicas extensivas de seguridad reforzada, como no almacenar jamás claves maestras no cifradas en el disco, no

mantenerlas en la memoria y limitar los sistemas que puedan conectarse a los hosts que usan claves. Todo el acceso al software de actualización del servicio lo controla un servicio de aprobación de varios niveles de cuya auditoría y revisión se encarga un grupo independiente dentro de AWS.

Para obtener más información sobre AWS KMS, consulte el documento técnico AWS Key Management Service.

## AWS CloudHSM

AWS CloudHSM es un módulo de seguridad de hardware (HSM) basado en la nube que permite cumplir los requisitos de cumplimiento corporativo, contractual y normativo de seguridad de los datos pues le permite generar y usar sus claves de cifrado en un hardware validado por el FIPS 140-2 Nivel 3.

Con AWS CloudHSM controla las claves de cifrado y las operaciones criptográficas que realiza el HSM.

Los socios de AWS y AWS Marketplace ofrecen una gran variedad de soluciones para proteger la información confidencial dentro de la plataforma de AWS, pero puede ser necesaria una protección adicional para las aplicaciones y los datos que estén sujetos a estrictas condiciones contractuales o normativas para la administración de claves de cifrado. Anteriormente, la única opción para almacenar información confidencial (o las claves de cifrado que protegen dicha información) era en los centros de datos locales. Lamentablemente, esto impedía migrar las aplicaciones a la nube o reducía significativamente su rendimiento. Gracias a AWS CloudHSM, puede proteger sus claves de cifrado dentro del HSM diseñado y aprobado de acuerdo con los estándares gubernamentales para la administración segura de claves. Puede generar, almacenar y administrar con seguridad las claves criptográficas que se utilizan para el cifrado de datos, de forma que solo usted pueda tener acceso a ellas. AWS CloudHSM le ayuda a cumplir los estrictos requisitos de administración de claves sin sacrificar el rendimiento de las aplicaciones.

El servicio de AWS CloudHSM funciona con Amazon VPC. Las instancias de AWS CloudHSM se aprovisionan dentro de la Amazon VPC con la dirección IP que especifique, que proporciona conectividad de red simple y privada a sus instancias de Amazon EC2. Al ubicar las instancias de HSM cerca de las instancias de Amazon EC2, reduce la latencia de la red, lo que mejora el rendimiento de las aplicaciones. AWS proporciona acceso exclusivo y específico (inquilino único) a las instancias de HSM, aisladas de otros clientes de AWS. AWS CloudHSM, que está disponible en varias regiones y zonas de disponibilidad, le permite añadir un almacenamiento de claves seguro y duradero a sus aplicaciones.

### Integración con los servicios de AWS y las aplicaciones de terceros

Puede utilizar CloudHSM con Amazon Redshift, Amazon RDS for Oracle o aplicaciones de otros fabricantes (como SafeNet Virtual KeySecure) a modo de raíz de confianza, Apache (terminación SSL) o Microsoft SQL Server (cifrado transparente de datos). También puede usar AWS CloudHSM cuando escriba sus propias aplicaciones y siga usando las bibliotecas criptográficas estándar, incluidas PKCS #11, Java JCA/JCE, Microsoft CAPI y CNG.

### Actividades de auditoría

Si necesita realizar un seguimiento de los cambios en los recursos o auditar las actividades con fines de seguridad y cumplimiento, puede revisar las llamadas a la API de administración a través de AWS CloudHSM realizadas desde su cuenta mediante AWS CloudTrail. Además, puede auditar las operaciones en el dispositivo HSM a través de syslog o enviar mensajes de registro de syslog a su recopilador de datos.

## Herramientas y servicios de criptografía de AWS

AWS ofrece mecanismos que cumplen con una amplia selección de estándares de seguridad criptográfica que puede utilizar para implementar el cifrado recomendado. El SDK de cifrado de AWS es una biblioteca de cifrado del lado del cliente, disponible en Java, Python, C, JavaScript y una interfaz de línea de comandos que admite Linux, macOS y Windows. Ofrece funciones avanzadas de protección de datos que incluyen conjuntos de algoritmos de clave simétrica, autenticados y seguros, como AES-GCM de 256 bits con derivación y firma de claves. Como se diseñó específicamente para aplicaciones que usan Amazon DynamoDB, DynamoDB Encryption Client permite a los usuarios proteger los datos de sus tablas antes de enviarlos a la base de datos. También verifica y descifra los datos cuando se recuperan. El cliente está disponible en Java y Python.

### Infraestructura DM-Crypt de Linux

Dm-crypt es un mecanismo de cifrado en el kernel de Linux que permite a los usuarios montar un sistema de archivos cifrado. El montaje de un sistema de archivos es el proceso por el cual se incluye un sistema de archivos en un directorio (punto de montaje) para ponerlo a disposición del sistema operativo. Después de montarlo, todos los archivos del sistema de archivos estarán disponibles para las aplicaciones sin ninguna interacción adicional. Sin embargo, estos archivos se cifran cuando se almacenan en el disco.

El asignador de dispositivos es una infraestructura del kernel de las versiones 2.6 y 3.x de Linux que proporciona una forma genérica para crear capas virtuales de dispositivos de bloques. El

destino de cifrado del asignador de dispositivos proporciona cifrado transparente de dispositivos de bloques mediante la API de criptografía del kernel. La solución de esta publicación utiliza dm-crypt junto con un sistema de archivos respaldado en disco asociado con un volumen lógico mediante el administrador de volúmenes lógicos (LVM, por sus siglas en inglés). EL LVM proporciona una administración de volúmenes lógicos para el kernel de Linux.

## Protección de datos por diseño y de forma predeterminada

Cada vez que un usuario o una aplicación intentan utilizar la AWS Management Console, la API de AWS o la CLI de AWS, se envía una solicitud a AWS. El servicio de AWS recibe la solicitud y ejecuta un conjunto de pasos para determinar si se permite o deniega la solicitud, de acuerdo con una lógica de evaluación de políticas específica. A excepción de las solicitudes de credenciales raíz, todas las solicitudes a AWS se rechazan de forma predeterminada (se aplica la política de denegación predeterminada). Esto significa que se niega todo lo que la política no permite de forma explícita. En la definición de políticas y como práctica recomendada, AWS sugiere que se aplique el principio de privilegios mínimos, lo que significa que cada componente (como usuarios, módulos o servicios) debe poder acceder solo a los recursos necesarios para completar sus tareas.

Este enfoque es conforme al artículo 25 del RGPD que establece que el controlador “deberá implementar las medidas técnicas y organizativas adecuadas para garantizar que, de forma predeterminada, solo se procesen los datos personales necesarios para cada finalidad específica del procesamiento”.

AWS también proporciona herramientas para implementar la infraestructura como código, que es un mecanismo poderoso para incluir la seguridad desde el principio del diseño de una arquitectura. AWS CloudFormation proporciona un lenguaje común para describir y aprovisionar todos los recursos de infraestructura, incluidas las políticas y los procesos de seguridad. Con estas herramientas y prácticas, la seguridad se convierte en parte del código y se puede versionar, supervisar y modificar (con un sistema de control de versiones) de acuerdo con los requisitos de cada organización. Esto permite la protección de datos por diseño, ya que los procesos y políticas de seguridad se pueden incluir en la definición de la arquitectura y también se pueden supervisar continuamente aplicando medidas de seguridad en la organización.

# Cómo puede ayudar AWS

Tabla 1 - Cómo AWS puede ayudar a cumplir el RGPD

| Área | Descripción | Servicios y herramientas de AWS |
| --- | --- | --- |
| Marco de conformidad sólido | Es posible que las medidas técnicas y organizativas adecuadas deban incluir “la capacidad para garantizar la confidencialidad, integridad, disponibilidad y adaptación continuas de los servicios y sistemas de procesamiento”. | SOC 1 / SSAE 16 / ISAE 3402 (anteriormente SAS 70) / SOC 2 / SOC 3<br>PCI DSS Nivel 1<br>ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018<br>NIST FIPS 140-2<br>Catálogo de controles de conformidad de computación en la nube (C5) |
| Control de acceso a los datos | El controlador “deberá implementar las medidas técnicas y organizativas adecuadas para garantizar que, de forma predeterminada, solo se procesen los datos personales | AWS Identity and Access Management (IAM)<br>Amazon Cognito<br>AWS Shield y AWS WAF<br>AWS Resource Access Manager<br>Amazon CloudFront<br>AWS Organizations<br>AWS CloudTrail |

| Área | Descripción | Servicios y herramientas de AWS |
| --- | --- | --- |
| | necesarios para cada finalidad específica del procesamiento”. | |
| Supervisión y registro | “Cada controlador y, cuando proceda, el representante del controlador deben mantener un registro de las actividades de procesamiento bajo su responsabilidad”.<br><br>“...el controlador y el procesador implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo [...]”. | AWS Config<br><br>Amazon CloudWatch<br><br>AWS Control Tower<br><br>Amazon GuardDuty<br><br>Amazon Inspector<br><br>Amazon Macie<br><br>AWS Systems Manager<br><br>AWS Security Hub<br><br>Herramientas y SDK de AWS |

| Área | Descripción | Servicios y herramientas de AWS |
| --- | --- | --- |
| Protección de sus datos en AWS | Las organizaciones deben “implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adaptado al riesgo, entre las que se incluyen la seudonimización y el cifrado de datos personales”. | AWS Certificate Manager<br>AWS CloudHSM<br>AWS Key Management Service |

# Colaboradores

Entre los colaboradores de este documento, están las siguientes personas:

- Tim Anderson, especialista en la industria técnica, Amazon Web Services
- Carmela Gambardella, arquitecta de soluciones para el sector público, Amazon Web Services
- Giuseppe Russo, responsable de control de seguridad, Amazon Web Services
- Marta Taggart, responsable sénior de programas, Amazon Web Services
- Luca Iannario, arquitecto de soluciones para el sector público, Amazon Web Services

# Revisiones del documento

| Fecha | Descripción |
| --- | --- |
| Noviembre de 2017 | Primera publicación |
| Diciembre de 2020 | Se ha actualizado para incluir los nuevos servicios y funcionalidades de AWS. |

# Avisos

Los clientes son responsables de realizar sus propias evaluaciones de la información contenida en este documento. Este documento: (a) se ha creado solo para fines informativos, (b) representa las prácticas y las ofertas de productos vigentes de AWS, que están sujetas a cambios sin previo aviso, y (c) no establece ningún compromiso ni garantía de AWS y sus empresas afiliadas, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS en relación con sus clientes se rigen por los acuerdos de AWS, y este documento no modifica ni forma parte de ningún acuerdo entre AWS y sus clientes.