



La arquitectura segura de computación en nube (SCCA) está activa AWS para el Departamento de Defensa de EE. UU.

# AWS Recomendaciones de



# AWS Recomendaciones de: La arquitectura segura de computación en nube (SCCA) está activa AWS para el Departamento de Defensa de EE. UU.

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

---

# Table of Contents

|   |    |
|---|----|
| Introducción .....  | 1  |
| Destinatarios previstos .....                                   | 1  |
| Descripción general del acelerador de zonas de aterrizaje ..... | 3  |
| Planifique la implementación de la LZA en AWS .....             | 5  |
| Componentes y requisitos del SCCA .....                         | 6  |
| Punto de acceso a la nube .....                                 | 8  |
| Paquete de seguridad para centros de datos virtuales .....      | 9  |
| Virtual Data Center Managed Services .....                      | 18 |
| Integración de servicios complementarios .....                  | 25 |
| Revisiones del sistema operativo .....                          | 26 |
| Administrador de credenciales en la nube de confianza .....     | 26 |
| Conclusión .....  | 33 |
| Recursos .....  | 34 |
| AWS documentación .....   | 34 |
| Otros recursos .....  | 34 |
| Historial de documentos .....                                   | 35 |
| Glosario .....  | 36 |
| # .....   | 36 |
| A .....   | 37 |
| B .....   | 40 |
| C .....   | 42 |
| D .....   | 45 |
| E .....   | 50 |
| F .....   | 52 |
| G .....   | 53 |
| H .....   | 54 |
| I .....   | 55 |
| L .....   | 58 |
| M .....   | 59 |
| O .....   | 63 |
| P .....   | 66 |
| Q .....   | 69 |
| R .....   | 69 |
| S .....   | 72 |

---

|         |       |
|---------|-------|
| T ..... | 76    |
| U ..... | 77    |
| V ..... | 78    |
| W ..... | 78    |
| Z ..... | 80    |
| .....   | lxxxi |

# La arquitectura segura de computación en nube (SCCA) está en marcha AWS para el Departamento de Defensa de EE. UU.

Rob Higareda y Rughved Gadgil, Amazon Web Services (AWS)

Marzo de 2024 ([historial del documento](#))

El Departamento de Defensa (DoD) de EE. UU. segmenta la información de la nube en niveles de impacto (IL). El nivel de impacto está asociado a la sensibilidad de la información y al riesgo de perder su confidencialidad, integridad o disponibilidad. La IL4 aloja la información no clasificada (CUI) controlada por el DoD y la IL5 aloja la información de la CUI del DoD y de los Sistemas de Seguridad Nacional (NSS). Esta guía está diseñada para ayudarte a construir una landing zone que soporte la información de IL4 e IL5.

Para crear una infraestructura de nube compatible con IL4 o IL5, debe crear componentes específicos. La arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA) es una selección de servicios de administración y seguridad en la nube. Proporciona un enfoque estandarizado para crear un límite entre las nubes. La SCCA también incluye componentes de seguridad a nivel de aplicación para la información de IL4 e IL5 alojada en la nube.

Esta guía le ayuda a cumplir los requisitos de la SCCA mediante el uso del acelerador de [zonas de aterrizaje](#) (LZA) activado. AWS La solución LZA implementa un conjunto básico de capacidades diseñadas para adaptarse a las AWS mejores prácticas y a varios marcos de cumplimiento globales. La LZA puede ayudarlo a crear muchos de los componentes necesarios para cumplir con la SCCA del DoD. Esta guía también recomienda cómo añadir componentes adicionales para cumplir con la SCCA y establecer una base segura para sus entornos de nube. AWS Si bien esta guía no incluye todas las situaciones posibles, proporciona orientación sobre cómo empezar y cuáles Servicios de AWS pueden ayudarlo a cumplir los requisitos de la SCCA.

## Destinatarios previstos

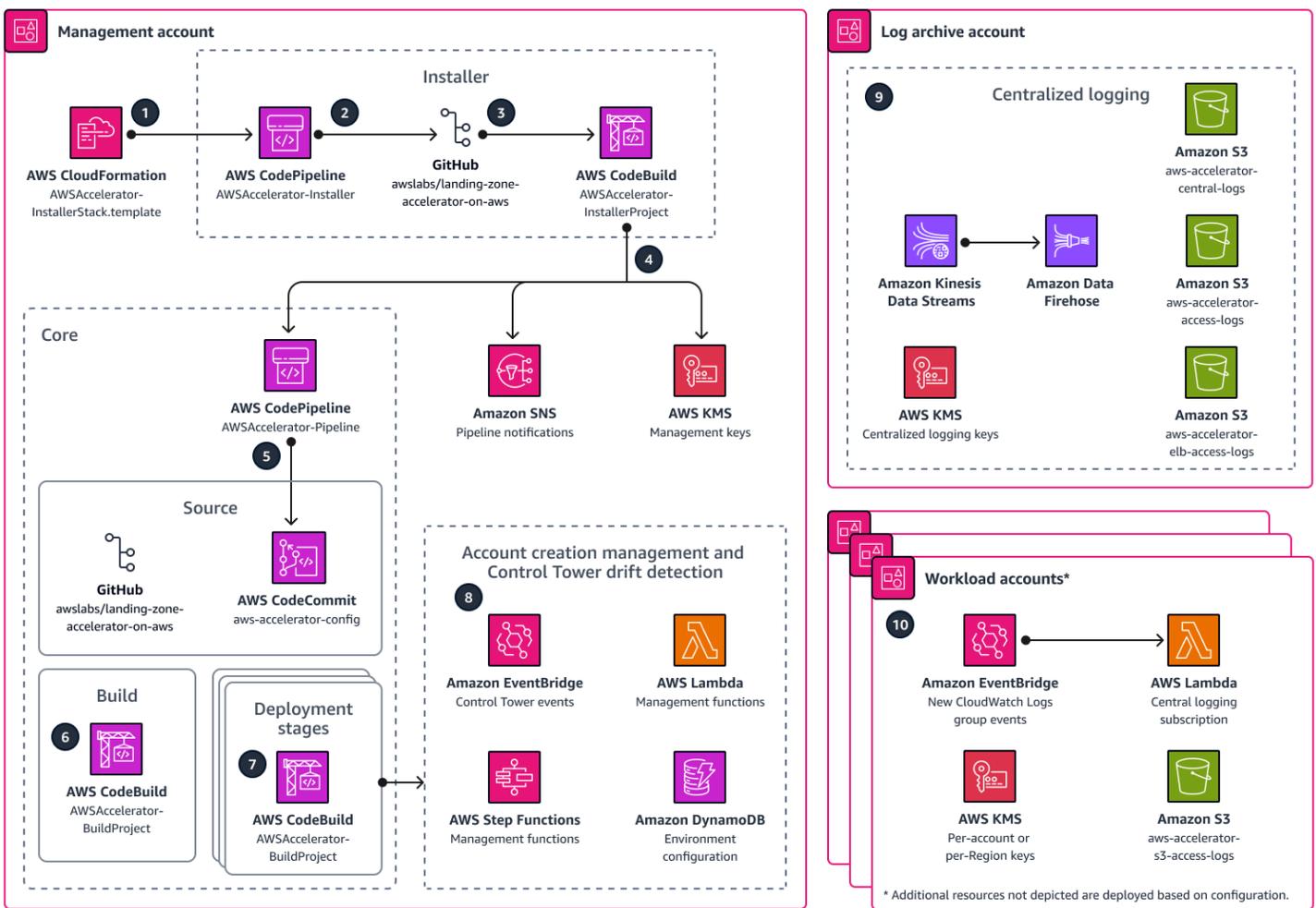
Esta guía está destinada a personas que necesitan cumplir con la arquitectura de computación en la nube segura del DoD para ayudar a proteger la información de IL4 e IL5 en el. Nube de AWS Si

aún no lo ha hecho, consulte la Guía de [requisitos de seguridad de la computación en nube de DISA antes de leer esta guía](#).

# Descripción general del acelerador de zonas de aterrizaje

Para construir una landing zone AWS que se ajuste a la arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA), debes contar con ciertos elementos que te ayuden a cumplir con los requisitos mínimos. AWS ha creado el [Landing Zone Accelerator \(LZA\)](#) para ayudarte a desplegar una zona de aterrizaje que cumpla con los requisitos necesarios. Con la solución LZA, puede implementar el entorno mediante un conjunto de archivos de configuración. Estos archivos de configuración le ayudan a centrarse en la entrega de un entorno en lugar de aprender a cada individuo Servicio de AWS y cómo implementarlo.

La siguiente imagen muestra los servicios involucrados en la implementación de la LZA. Los números indican el flujo de trabajo, desde la modificación de los archivos de configuración hasta la configuración de las cuentas Servicios de AWS de carga de trabajo.



Esta solución está diseñada para alinearse con las AWS mejores prácticas y ajustarse a varios marcos de cumplimiento globales. Cuando se usa en coordinación con servicios como [AWS Control Tower](#), por ejemplo, esta solución proporciona una solución integral Servicios de AWS y de bajo código con más de 35 funciones. En concreto, esta solución le ayuda a gestionar y gestionar un entorno de múltiples cuentas diseñado para soportar cargas de trabajo altamente reguladas y requisitos de conformidad complejos. LZA le ayuda a establecer la idoneidad de la plataforma con capacidades operativas, de seguridad y de conformidad. Esta guía incluye notas específicas sobre el uso de esta solución para respaldar la alineación con [las directrices federales y del Departamento de Defensa \(DoD\) de los Estados Unidos \(EE. UU.\)](#).

AWS proporciona la solución LZA como un proyecto de código abierto que se creó utilizando el [AWS Cloud Development Kit \(AWS CDK\)](#). Puede instalarla directamente en su entorno, lo que le brinda acceso total a la solución de infraestructura como código (IaC).

Mediante un conjunto simplificado de archivos de configuración, puede:

- Configurar funciones, barandas y servicios de seguridad adicionales, como reglas [AWS Config](#) administradas y [AWS Security Hub](#)
- Administre su topología de red fundamental a través de servicios como [Amazon Virtual Private Cloud \(Amazon VPC\)](#) y [AWS Transit Gateway](#) [AWS Network Firewall](#)
- [Genere cuentas de carga de trabajo adicionales mediante Account Factory AWS Control Tower](#) .

No se requieren cargos adicionales ni compromisos por adelantado para utilizar Landing Zone Accelerator en. AWS Solo pagas por lo Servicios de AWS que enciendas para configurar tu plataforma y operar tus barandillas. Esta solución también admite AWS particiones no estándar, incluidas las AWS GovCloud (US) regiones AWS Secret y AWS Top Secret.

#### Important

La solución LZA, por sí sola, no hace que cumpla con las normas. Proporciona la infraestructura básica desde la que puede integrar soluciones complementarias adicionales. La información incluida en la [guía de implementación de la LZA](#) no es exhaustiva. Debe revisar, evaluar y aprobar la solución de conformidad con las características, herramientas y configuraciones de seguridad específicas de su organización. Es responsabilidad exclusiva de usted y de su organización determinar qué requisitos reglamentarios son aplicables y asegurarse de que cumplen con todos los requisitos. Si bien esta solución analiza los

requisitos técnicos y administrativos, no le ayuda a cumplir con los requisitos administrativos no técnicos.

## Planifique la implementación de la LZA en AWS

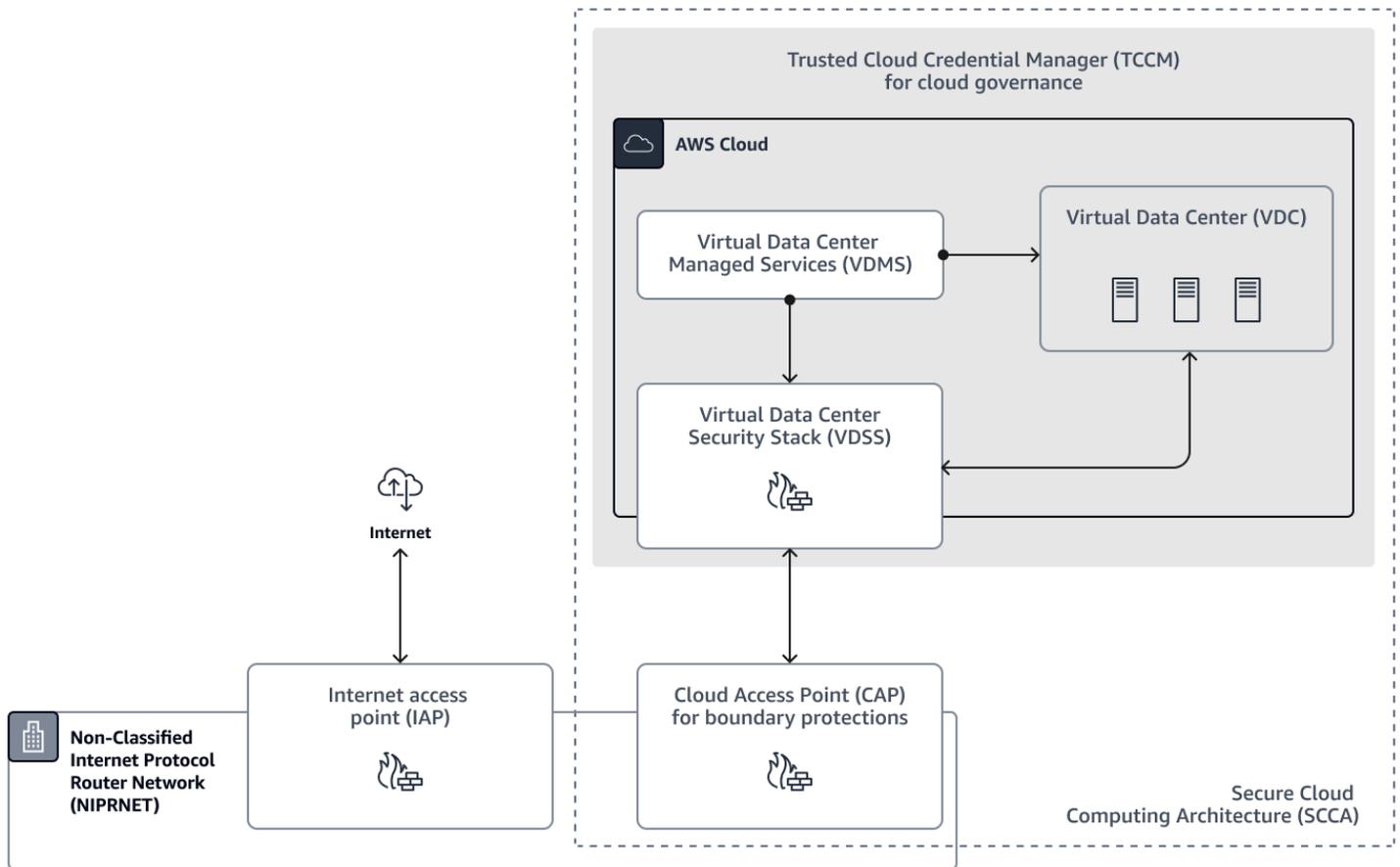
AWS ha creado una [guía de implementación](#) detallada para implementar la solución Landing Zone Accelerator (LZA) en AWS. Para ver un diagrama de arquitectura y una descripción general de los pasos de implementación, consulte el [diagrama de arquitectura](#) en la guía de implementación de Landing Zone Accelerator. AWS Su entorno debe cumplir los [requisitos previos](#) antes de implementar la solución. Con los requisitos del capítulo sobre los componentes y requisitos de la SCCA de esta guía, puede elegir entre las opciones de implementación que se describen en la guía de implementación de la [LZA](#).

## Componentes y requisitos del SCCA

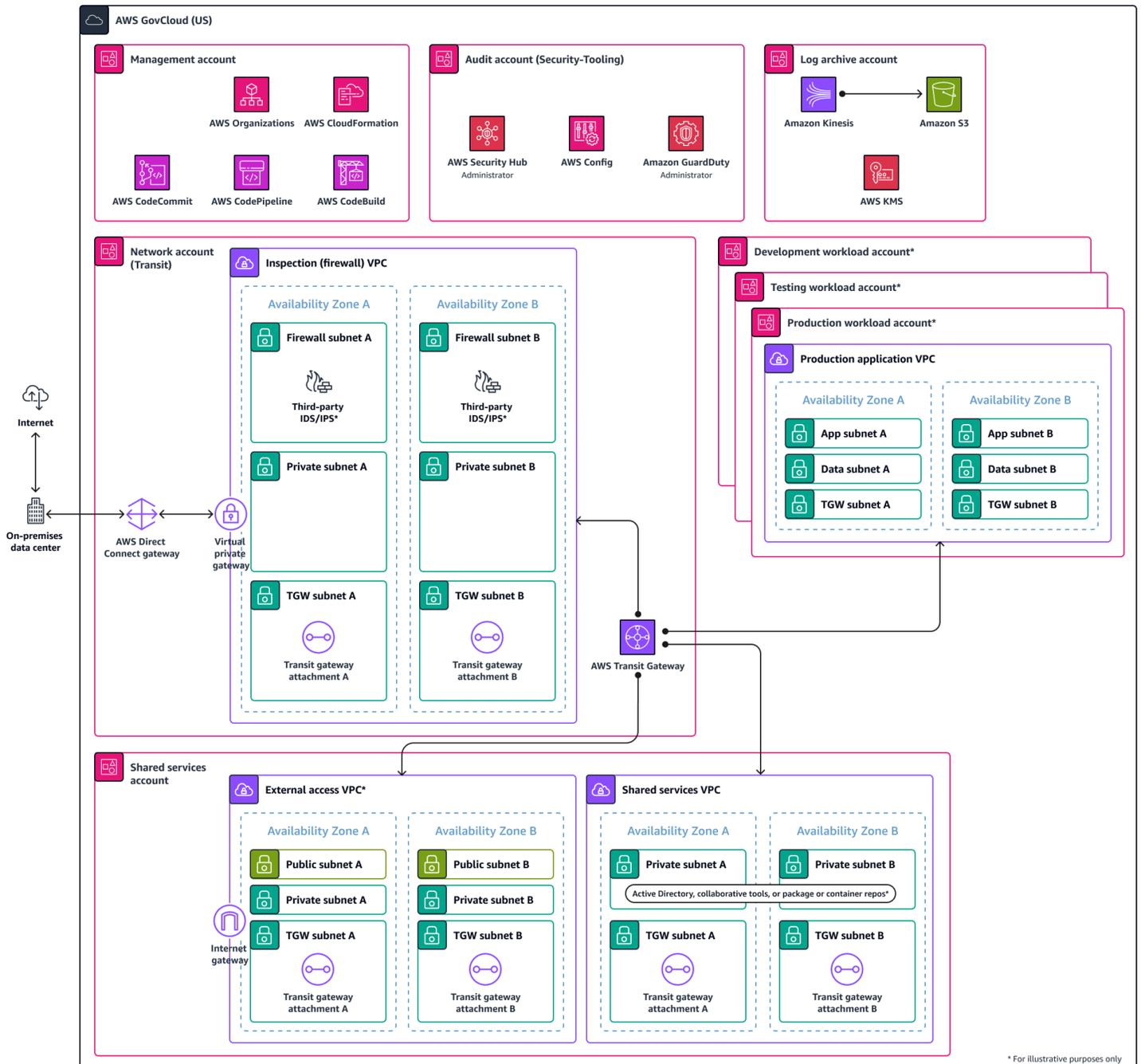
La arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA), adoptada por el Departamento de Defensa de los Estados Unidos (DoD), pretende ser un enfoque escalable y rentable para proteger las aplicaciones basadas en la nube bajo una arquitectura de seguridad común. Proporciona un enfoque estándar para proteger los datos de IL4 e IL5 en entornos de nube. Como se describe en la [hoja informativa sobre la SCCA de la DISA](#), los componentes principales de la SCCA incluyen:

- Punto de acceso a la nube (CAP): proporciona acceso a la nube y protege las redes del DoD desde la nube. Protecciones simplificadas centradas en proteger los límites de la red.
- Paquete de seguridad para centros de datos virtuales (VDSS): seguridad de enclave de red virtual para proteger las aplicaciones y los datos en las ofertas de nube comercial.
- Virtual Data Center Managed Services (VDMS): seguridad de host de aplicaciones para el acceso de usuarios privilegiados en entornos comerciales.
- Trusted Cloud Credential Manager (TCCM): administrador de credenciales en la nube para aplicar el control de acceso basado en roles (RBAC) y el acceso con menos privilegios.

La siguiente imagen muestra estos componentes de la SCCA.



En esta sección se analiza cada componente en detalle y los componentes correspondientes de la LZA que pueden ayudarle a cumplir con el estándar de la Agencia de Sistemas de Información de Defensa (DISA). La siguiente imagen muestra la estructura de cuentas múltiples de la LZA que construye los componentes de la SCCA dentro de la Nube de AWS. Esta estructura de cuentas múltiples de la LZA es la base que le ayuda a lograr una arquitectura que cumpla totalmente con los requisitos de la SCCA de la DISA. Para ver un ejemplo de una arquitectura que le ayude a cumplir plenamente los requisitos de conformidad, consulte el diagrama [SCCA](#) sobre arquitectura. AWS GovCloud



## Punto de acceso a la nube

Su organización predetermina el punto de acceso a la nube (BCAP) o el punto de acceso a la nube (CAP). Por lo tanto, no está incluido en el ámbito de esta guía. El CAP proporciona acceso a entornos de nube comerciales desde la Red de Sistemas de Información de Defensa (DISN). El CAP también protege los límites de la DISN desde la nube. En el límite de la DISN, incluye capacidades de ciberdefensa, como el firewall, los sistemas de detección de intrusos (IDS) y los sistemas de

prevención de intrusiones (IPS). Es habitual que las organizaciones utilicen el [diseño de referencia del punto de acceso nativo de la nube](#) del DoD para acceder. AWS

## Paquete de seguridad para centros de datos virtuales

El objetivo del paquete de seguridad para centros de datos virtuales (VDSS) es proteger las aplicaciones alojadas en las misiones del Departamento de Defensa. AWS El VDSS proporciona un enclave para los servicios de seguridad. El VDSS realiza la mayor parte de las operaciones de seguridad en la SCCA. Este componente contiene servicios de seguridad y red, como la conectividad entrante, los controles de acceso y los servicios de protección perimetral, incluidos los firewalls de aplicaciones web, la protección contra DDOS, los equilibradores de carga y los recursos de enrutamiento de redes. El VDSS puede residir en la infraestructura de la nube o de forma local, en su centro de datos. AWS o los proveedores externos pueden proporcionar capacidades de VDSS a través de infraestructura como servicio (IaaS) o AWS pueden ofrecer estas capacidades a través de soluciones de software como servicio (SaaS). Para obtener más información sobre el VDSS, consulte la Guía de requisitos de seguridad de la [computación en la nube del DoD](#).

La siguiente tabla contiene los requisitos mínimos del VDSS. En ella se explica si la LZA aborda cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

| ID      | Requisito de seguridad del VDSS  | AWS tecnologías   | Recursos adicionales de                | Cubierto por LZA |
|---------|--|---|--|------------------|
| 2.1.2.1 | El VDSS mantendrá una separación virtual de todo el tráfico de administración, usuarios y datos. | <a href="#">AWS Network Firewall</a><br><br><a href="#">Lista de control de acceso a la red (ACL)</a><br><br><a href="#">Grupos de seguridad para interfaces de red elásticas</a> | <a href="#">Aíse las VPC</a>           | Cubierto         |
| 2.1.2.2 | El VDSS permitirá el uso   | <a href="#">Amazon VPC</a> (cifrado del   | <a href="#">Prácticas recomendadas</a> | Cubierto         |

| ID      | Requisito de seguridad del VDSS   | AWS tecnologías   | Recursos adicionales de   | Cubierto por LZA      |
|---------|---|---|---|-----------------------|
|         | del cifrado para la segmentación del tráfico de gestión.  | tráfico entre instancias)                                   | <a href="#">de cifrado para Amazon VPC</a>  |                       |
| 2.1.2.3 | El VDSS proporcionará una capacidad de proxy inverso para gestionar las solicitudes de acceso de los sistemas cliente.  | N/A   | <a href="#">Servir contenido mediante un proxy inverso totalmente gestionado</a>  | No está cubierto      |
| 2.1.2.4 | El VDSS proporcionará la capacidad de inspeccionar y filtrar las conversaciones de la capa de aplicación en función de un conjunto predefinido de reglas (incluida la HTTP) para identificar y bloquear el contenido malicioso. | <a href="#">AWS WAF</a><br><a href="#">Network Firewall</a> | <a href="#">Inspección del organismo de solicitud web</a><br><a href="#">Inspección de tráfico TLS con Network Firewall</a> | Cubierto parcialmente |

| ID      | Requisito de seguridad del VDSS   | AWS tecnologías  | Recursos adicionales de   | Cubierto por LZA      |
|---------|---|--|---|-----------------------|
| 2.1.2.5 | El VDSS proporcionará una capacidad que pueda distinguir y bloquear el tráfico no autorizado de la capa de aplicación.  | <a href="#">AWS WAF</a>  | <a href="#">Cómo usar Amazon GuardDuty y AWS WAF bloquear automáticamente los anfitriones sospechosos</a> | ¿No está cubierto     |
| 2.1.2.6 | El VDSS proporcionará una capacidad que supervise las actividades de la red y el sistema a fin de detectar y denunciar las actividades maliciosas del tráfico que entra y sale de las redes o enclaves privados virtuales del propietario de la misión. | <a href="#">Logs de flujo de VPC</a><br><a href="#">Amazon GuardDuty</a><br><a href="#">AWS Nitro Enclaves</a> | <a href="#">AWS Taller sobre Nitro Enclaves</a>   | Cubierto parcialmente |

| ID      | Requisito de seguridad del VDSS   | AWS tecnologías   | Recursos adicionales de  | Cubierto por LZA      |
|---------|---|---|--|-----------------------|
| 2.1.2.7 | El VDSS proporcionará una capacidad que supervise las actividades de la red y el sistema para detener o bloquear las actividades maliciosas detectadas. | <a href="#">Network Firewall</a><br><br><a href="#">AWS WAF</a> | N/A  | Cubierto parcialmente |
| 2.1.2.8 | El VDSS inspeccionará y filtrará el tráfico que circule entre las redes o enclaves privados virtuales del propietario de la misión.                     | <a href="#">Network Firewall</a>                                | <a href="#">Implemente un filtrado de tráfico centralizado</a> | Cubierto              |

| ID       | Requisito de seguridad del VDSS   | AWS tecnologías                  | Recursos adicionales de   | Cubierto por LZA |
|----------|---|----------------------------------|---|------------------|
| 2.1.2.9  | El VDSS detectará e inspeccionará el tráfico de comunicación SSL/TLS para permitir la autenticación simple y doble del tráfico destinado a los sistemas alojados en el CSE.               | <a href="#">Network Firewall</a> | <a href="#">Modelos de implementación para Network Firewall</a> | Cubierto         |
| 2.1.2.10 | El VDSS proporcionará una interfaz para llevar a cabo las actividades de administración de puertos, protocolos y servicios (PPSM) a fin de proporcionar control a los operadores del MCD. | <a href="#">Network Firewall</a> | <a href="#">Modelos de implementación para Network Firewall</a> | Cubierto         |

| ID       | Requisito de seguridad del VDSS  | AWS tecnologías   | Recursos adicionales de  | Cubierto por LZA |
|----------|--|---|--|------------------|
| 2.1.2.11 | El VDSS proporcionará una capacidad de monitoreo que capture archivos de registro y datos de eventos para el análisis de ciberseguridad.   | <a href="#">Amazon CloudWatch</a><br><a href="#">AWS CloudTrail</a> | <a href="#">Registro de la respuesta a incidentes de seguridad</a> | Cubierto         |
| 2.1.2.12 | El VDSS proporcionará o alimentará la información de seguridad y los datos de los eventos a un sistema de archivo asignado para que los usuarios privilegiados que realicen actividades de la CND de Boundary y Mission recopilen, almacenen y accedan a ellos de forma común. | <a href="#">Amazon CloudWatch Logs</a>                              | <a href="#">Seguridad en CloudWatch los registros</a>              | Cubierto         |

| ID       | Requisito de seguridad del VDSS   | AWS tecnologías  | Recursos adicionales de  | Cubierto por LZA |
|----------|---|--|--|------------------|
| 2.1.2.13 | El VDSS proporcionará un sistema de gestión de claves de cifrado compatible con la FIPS-140-2 para almacenar las credenciales de las claves de cifrado privadas del servidor generadas y asignadas por el DoD para su acceso y uso por parte del Web Application Firewall (WAF) en la ejecución de la interrupción de SSL/TLS y la inspección de las sesiones de comunicación cifradas. | <a href="#">AWS Secrets Manager</a><br><br><a href="#">AWS Key Management Service(AWS KMS)</a> | <a href="#">Mejora la seguridad de Amazon CloudFront Origin con AWS WAF Secrets Manager</a><br><br><a href="#">AWS KMS administración de claves con FIPS 140-2</a> | No está cubierto |

| ID       | Requisito de seguridad del VDSS  | AWS tecnologías | Recursos adicionales de | Cubierto por LZA |
|----------|--|-----------------|-------------------------|------------------|
| 2.1.2.14 | El VDSS proporcionará la capacidad de detectar e identificar el secuestro de sesiones de la aplicación.      | N/A             | N/A                     | No está cubierto |
| 2.1.2.15 | El VDSS proporcionará una extensión DMZ del DoD para respaldar las aplicaciones orientadas a Internet (IFA). | N/A             | N/A                     | No está cubierto |

| ID       | Requisito de seguridad del VDSS   | AWS tecnologías  | Recursos adicionales de  | Cubierto por LZA |
|----------|---|--|--|------------------|
| 2.1.2.16 | El VDSS proporcionará una capacidad de captura completa de paquetes (FPC) o una capacidad de FPC equivalente a un servicio en la nube para grabar e interpretar las comunicaciones transversales. | <a href="#">Network Firewall</a><br><br><a href="#">Logs de flujo de VPC</a> | N/A  | Cubierto         |
| 2.1.2.17 | El VDSS proporcionará métricas y estadísticas del flujo de paquetes de la red para todas las comunicaciones transversales.  | <a href="#">CloudWatch</a>   | <a href="#">Supervise el rendimiento de la red de los puntos finales de la interfaz de VPC mediante CloudWatch</a> | Cubierto         |

| ID       | Requisito de seguridad del VDSS  | AWS tecnologías                  | Recursos adicionales de  | Cubierto por LZA |
|----------|--|----------------------------------|--|------------------|
| 2.1.2.18 | El VDSS se encargará de inspeccionar el tráfico que entra y sale de la red privada virtual del propietario de cada misión. | <a href="#">Network Firewall</a> | <a href="#">Implemente un filtrado de tráfico centralizado</a> | Cubierto         |

Hay componentes del CAP que usted define y que no se tratan en esta guía porque cada agencia tiene su propia conexión con el CAP AWS. Puede complementar los componentes del VDSS con el LZA para poder inspeccionar el tráfico entrante. AWS Los servicios que se utilizan en la LZA permiten analizar los límites y el tráfico interno para ayudar a proteger su entorno. Para seguir creando un VDSS, hay algunos componentes de infraestructura adicionales que no están incluidos en el LZA.

Al utilizar la nube privada virtual (VPC), puede establecer límites en cada uno de ellos Cuenta de AWS para cumplir con los estándares de la SCCA. Esto no está configurado como parte de la LZA porque las VPC, el direccionamiento IP y el enrutamiento son componentes que debe configurar según sea necesario para su infraestructura. Puede implementar componentes como las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) en [Amazon Route 53](#). También puede añadir WAF comerciales AWS WAF o de terceros para ayudarle a alcanzar los estándares necesarios.

Además, para cumplir con el requisito 2.1.2.7 de la DISA SCCA, puede utilizar un [Network GuardDutyFirewall](#) para proteger y monitorear el entorno en busca de tráfico malicioso.

## Virtual Data Center Managed Services

El propósito de Virtual Data Center Managed Services (VDMS) es proporcionar seguridad para el host y servicios de centro de datos compartidos. Las funciones del VDMS pueden ejecutarse en el centro de su SCCA o el propietario de la misión puede implementar partes de él por su cuenta.

Cuentas de AWS Este componente se puede proporcionar en su entorno. AWS Para obtener más información sobre el VDMS, consulte la Guía de requisitos de seguridad de la [computación en la nube del DoD](#).

La siguiente tabla contiene los requisitos mínimos del VDMS. En ella se explica si la LZA cumple con cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

| ID      | Requisito de seguridad de VDMS  | AWS tecnologías   | Recursos adicionales de  | Cubierto por LZA      |
|---------|---|---|--|-----------------------|
| 2.1.3.1 | El VDMS proporcionará una solución de evaluación asegurada del cumplimiento (ACAS), o un equivalente aprobado, para llevar a cabo una supervisión continua de todos los enclaves del CSE. | <a href="#">AWS Config</a><br><a href="#">AWS Security Hub</a><br><a href="#">AWS Audit Manager</a><br><a href="#">Amazon Inspector</a> | <a href="#">Escaneo de vulnerabilidades con Amazon Inspector</a> | Cubierto parcialmente |
| 2.1.3.2 | El VDMS proporcionará un sistema de seguridad basado en el host (HBSS), o un equivalente aprobado, para gestionar la seguridad  | N/A   | N/A  | No está cubierto      |

| ID      | Requisito de seguridad de VDMS   | AWS tecnologías   | Recursos adicionales de   | Cubierto por LZA      |
|---------|--|---|---|-----------------------|
|         | de los puntos finales en todos los enclaves del CSE.   |   |   |                       |
| 2.1.3.3 | El VDMS proporciona servicios de identidad para incluir un respondedor del Protocolo de estado de certificados en línea (oCloud Workload Security) para la autenticación de dos factores mediante la tarjeta de acceso común (CAC) del DoD remota de los usuarios con privilegios del DoD en los sistemas instanciados dentro del CSE. | La autenticación multifactor (MFA) está disponible a través de:<br><br><a href="#">AWS Identity and Access Management (IAM)</a><br><br><a href="#">AWS IAM Identity Center</a><br><br><a href="#">AWS Directory Service for Microsoft Active Directory</a><br><br><a href="#">AWS Private Certificate Authority</a> | <a href="#">Configurar una tarjeta CAC para Amazon WorkSpaces</a> | Cubierto parcialmente |

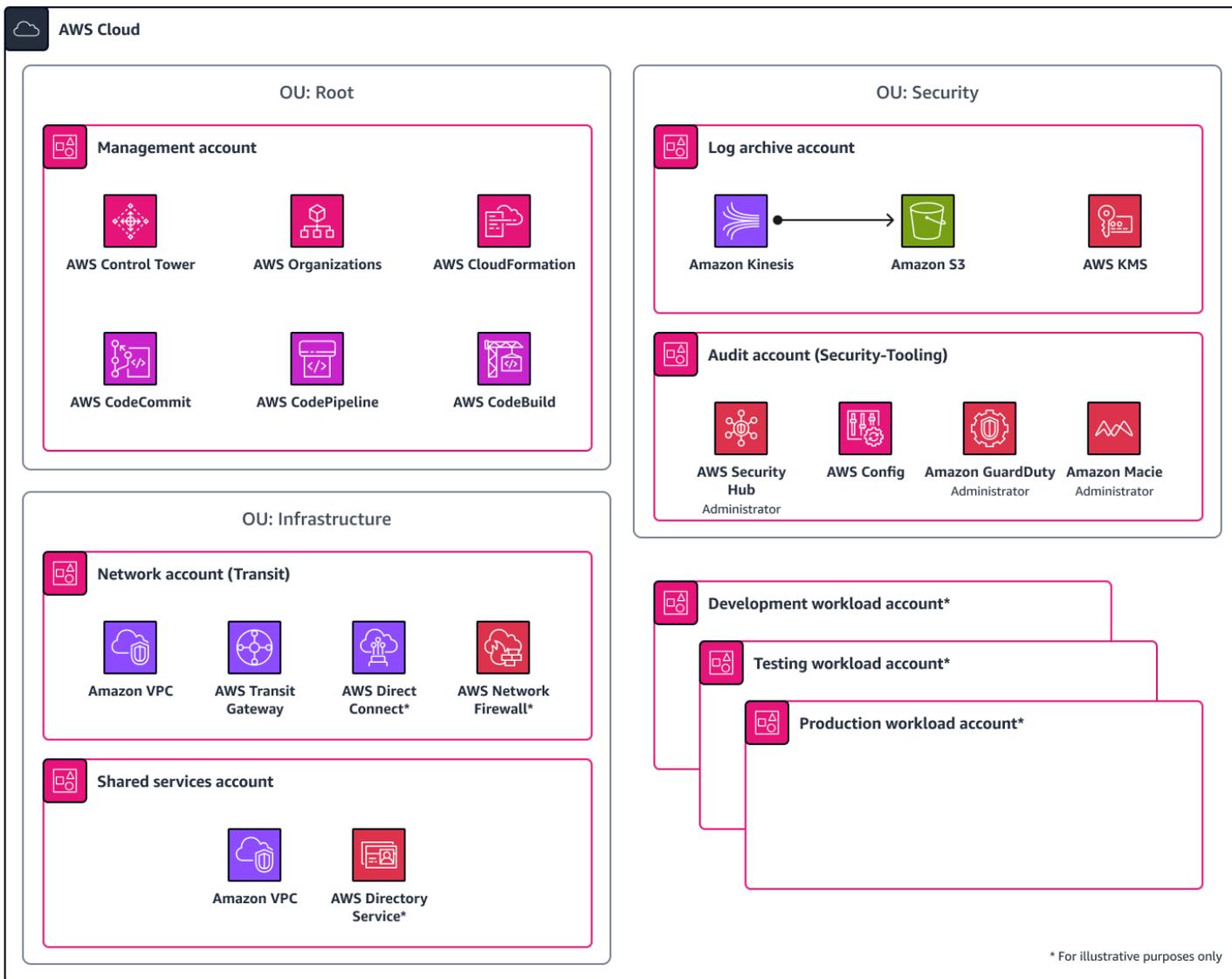
| ID      | Requisito de seguridad de VDMS  | AWS tecnologías  | Recursos adicionales de  | Cubierto por LZA      |
|---------|---|--|--|-----------------------|
| 2.1.3.4 | El VDMS proporcionará un sistema de gestión de configuraciones y actualizaciones que sirva a los sistemas y aplicaciones de todos los enclaves del CSE.   | <a href="#">AWS Systems Manager Patch Manager</a><br><a href="#">AWS Config</a>  | <a href="#">Automatizar la administración de parches</a> con (vídeo)<br>AWS Systems Manager<br>YouTube | Cubierto parcialmente |
| 2.1.3.5 | El VDMS proporcionará servicios de dominio lógico que incluyan el acceso a los directorios, la federación de directorios, el protocolo de configuración dinámica de host (DHCP) y el sistema de nombres de dominio (DNS) para todos los enclaves del CSE. | <a href="#">AWS Managed Microsoft AD</a><br><a href="#">Amazon Virtual Private Cloud (Amazon VPC)</a><br><a href="#">Amazon Route 53</a> | <a href="#">Configure los atributos de DNS para su VPC</a>   | Cubierto parcialmente |

| ID      | Requisito de seguridad de VDMS  | AWS tecnologías  | Recursos adicionales de | Cubierto por LZA |
|---------|---|--|-------------------------|------------------|
| 2.1.3.6 | El VDMS proporcionará una red para gestionar los sistemas y las aplicaciones dentro del CSE que esté separada lógicamente de las redes de usuarios y datos. | <a href="#">Amazon VPC</a><br><a href="#">Subredes de Amazon VPC</a> | N/A                     | Cubierto         |

| ID      | Requisito de seguridad de VDMS  | AWS tecnologías   | Recursos adicionales de                              | Cubierto por LZA |
|---------|---|---|--|------------------|
| 2.1.3.7 | El VDMS proporcionará un sistema de registro y archivado de eventos del sistema, la seguridad, las aplicaciones y la actividad del usuario para que los usuarios privilegiados que realicen actividades de BCP y MCP recopilen, almacenen y accedan a los registros de eventos de manera común. | <a href="#">AWS Security Hub</a><br><a href="#">AWS CloudTrail</a><br><a href="#">Amazon CloudWatch Logs</a><br><a href="#">Amazon Simple Storage Service (Amazon S3)</a> | <a href="#">Registro centralizado con OpenSearch</a> | Cubierto         |

| ID      | Requisito de seguridad de VDMS  | AWS tecnologías   | Recursos adicionales de   | Cubierto por LZA      |
|---------|---|---|---|-----------------------|
| 2.1.3.8 | El VDMS permitirá el intercambio de los atributos de autenticación y autorización de los usuarios con privilegios del DoD con el sistema de administración de identidad y acceso del CSP para permitir el aprovisionamiento, la implementación y la configuración del sistema en la nube. | <a href="#">AWS Managed Microsoft AD</a>  | <a href="#">Mejore su configuración de seguridad AWS Managed Microsoft AD</a> | No está cubierto      |
| 2.1.3.9 | El VDMS implementará las capacidades técnicas necesarias para ejecutar la misión y los objetivos de la función de TCCM.   | <a href="#">AWS Managed Microsoft AD</a><br><br><a href="#">IAM</a><br><br><a href="#">Centro de identidades de IAM</a> | N/A   | Cubierto parcialmente |

Como se muestra en la siguiente imagen, la LZA establece los componentes fundamentales para cumplir con los requisitos básicos del VDMS. Hay algunos componentes adicionales que debe configurar después de implementar la LZA para cumplir con los estándares del VDMS. En la tabla anterior, asegúrese de revisar los enlaces de la columna Recursos adicionales. Estos enlaces le ayudan a configurar estos elementos adicionales o proporcionan más mejoras de seguridad.



## Integración de servicios complementarios

En la columna de recursos adicionales de la tabla anterior se enumeran los recursos que le ayudarán a ampliar la LZA para cumplir con los requisitos del VDMS. Además, ofrece algunos materiales

de taller que le ayudarán a configurar una arquitectura de nube segura. Sin modificaciones, la LZA cumple con los requisitos de la IL4/IL5, pero puede implementar servicios adicionales para mejorar la seguridad de su entorno. AWS

Por ejemplo, Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus AWS cargas de trabajo en busca de vulnerabilidades de software y exposición no intencionada a la red. Puede usarlo para identificar e investigar vulnerabilidades en los sistemas operativos anfitriones, como Windows y Linux. Aunque es posible que Amazon Inspector no incorpore por completo todos los requisitos necesarios para un sistema de seguridad basado en host (HBSS), al menos proporciona una evaluación de vulnerabilidad de nivel básico de las instancias.

## Revisiones del sistema operativo

La aplicación de parches al sistema operativo es un componente fundamental del funcionamiento de un entorno seguro. AWS ofrece y recomienda el uso del [Administrador de parches](#), una capacidad que permite mantener bases de AWS Systems Manager referencia de parches consistentes y automatizar la implementación de parches. Patch Manager automatiza el proceso de parchear los nodos gestionados tanto con actualizaciones relacionadas con la seguridad como con otros tipos de actualizaciones.

Puede utilizar Patch Manager para aplicar parches a los sistemas operativos y a las aplicaciones. (En Windows Server, el soporte de aplicaciones se limita a las actualizaciones de las aplicaciones publicadas por Microsoft). Para obtener más información, consulte [Cómo organizar procesos de parches personalizados y de varios pasos mediante AWS Systems Manager Patch Manager en el blog](#) sobre operaciones y migraciones en la AWS nube.

Para step-by-step obtener instrucciones sobre el uso de Patch Manager, consulte el taller sobre herramientas [AWS de gestión y gobierno](#).

Para obtener más información sobre cómo proteger las cargas de trabajo de Microsoft Windows en AWS, consulte el taller [Cómo proteger las cargas de trabajo de Windows en el AWS taller](#).

## Administrador de credenciales en la nube de confianza

El Trusted Cloud Credential Manager (TCCM) es un componente de la SCCA. Es responsable de la administración de credenciales. Al establecer la TCCM, es importante permitir el acceso de los [menos privilegiados a la SCCA](#). Esto se puede lograr mediante el uso AWS de servicios de administración de identidad y acceso. Un componente adicional del TCCM es una conexión a Virtual

Data Center Managed Services (VDMS). Puede utilizar esta conexión según sea necesario para acceder al TCCM y administrar el TCCM AWS Management Console .

El TCCM es una combinación de tecnologías y estándares que rigen el acceso a. AWS El TCCM se considera fundamental para la mayoría de las implementaciones porque controla los permisos de acceso. La función TCCM no pretende imponer requisitos exclusivos de gestión de identidades al proveedor de servicios en la nube (CSP) comercial. La TCCM tampoco prohíbe el uso de la federación CSP del DoD o de soluciones de agentes de identidad de terceros para proporcionar el control de identidad previsto.

Los componentes de la política de TCCM se basan en el entendimiento general de que los CSP ofrecen un sistema de gestión de identidad y acceso que permite controlar el acceso a los sistemas en la nube. Dichos sistemas pueden incluir los componentes de servicio de la consola de acceso, la API y la interfaz de línea de comandos (CLI) del CSP. En el nivel básico, el TCCM debe bloquear las credenciales que se pueden utilizar para crear redes y otros recursos no autorizados. El TCCM es nombrado por el oficial autorizado (AO) encargado de supervisar los sistemas de TI. Las políticas del TCCM establecen la necesidad de un modelo de acceso con privilegios mínimos. Estas políticas son responsables del suministro y el control de las credenciales de los usuarios privilegiados en la nube comercial. Esto es para mantener la coherencia con la [Guía de requisitos de seguridad de la computación en la nube del DoD](#), que aborda la implementación de políticas, planes y procedimientos para administrar las credenciales de la cuenta del portal. [Antes de conectarse a la Red de Sistemas de Información de Defensa \(DISN\), DISA valida la existencia del Plan de administración de credenciales en la nube \(CCMP\) como parte del proceso de aprobación de la conexión definido en la Guía del proceso de conexión.](#)

La siguiente tabla contiene los requisitos mínimos para el TCCM. Explica si la LZA aborda cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

| ID      | Requisitos de seguridad de TCCM  | AWS tecnologías | Recursos adicionales de | Cubierto por LZA |
|---------|--|-----------------|-------------------------|------------------|
| 2.1.4.1 | La TCCM desarrollará y mantendrá un plan de gestión de credenciales en la nube | N/A             | N/A                     | No está cubierto |

| ID      | Requisitos de seguridad de TCCM   | AWS tecnologías  | Recursos adicionales de | Cubierto por LZA |
|---------|---|--|-------------------------|------------------|
|         | (CCMP) para abordar la implementación de las políticas, los planes y los procedimientos que se aplicarán a la gestión de las credenciales de las cuentas del portal de clientes del propietario de la misión. |  |                         |                  |
| 2.1.4.2 | El TCCM recopilará, auditará y archivará todos los registros de actividad y alertas del Portal del Cliente.   | <a href="#">AWS CloudTrail</a><br><br><a href="#">Amazon CloudWatch Logs</a> | N/A                     | Cubierto         |

| ID      | Requisitos de seguridad de TCCM   | AWS tecnologías   | Recursos adicionales de | Cubierto por LZA |
|---------|---|---|-------------------------|------------------|
| 2.1.4.3 | El TCCM se asegurará de que los usuarios privilegiados del DoD que participan en actividades de MCP y BCP compartan las alertas del registro de actividades, las reenvíen o las puedan recuperar. | <a href="#">AWS CloudTrail</a><br><a href="#">CloudWatch Registros</a><br><a href="#">Amazon Simple Notification Service (Amazon SNS)</a><br><a href="#">CloudWatch Información sobre los registros</a> | N/A                     | Cubierto         |

| ID      | Requisitos de seguridad de TCCM  | AWS tecnologías  | Recursos adicionales de | Cubierto por LZA |
|---------|--|--|-------------------------|------------------|
| 2.1.4.4 | Según sea necesario para el intercambio de información, el TCCM creará cuentas de acceso al repositorio de registros para que los usuarios privilegiados que realicen actividades tanto de MCP como de BCP puedan acceder a los datos del registro de actividades. | <a href="#">AWS CloudTrail</a><br><a href="#">CloudWatch Registros</a><br><a href="#">Amazon SNS</a><br><a href="#">CloudWatch Información sobre los registros</a> | N/A                     | Cubierto         |
| 2.1.4.5 | El TCCM recuperará y controlará de forma segura las credenciales de las cuentas del portal de clientes antes de conectar la aplicación a la DISN.  | <a href="#">AWS IAM</a><br><a href="#">Identity Center</a>   | N/A                     | Cubierto         |

| ID      | Requisitos de seguridad de TCCM   | AWS tecnologías  | Recursos adicionales de | Cubierto por LZA |
|---------|---|--|-------------------------|------------------|
| 2.1.4.6 | El TCCM creará, emitirá y revocará, según sea necesario, las credenciales del portal de clientes menos privilegiados con acceso basado en roles para los administradores de aplicaciones y sistemas propietarios de la misión (es decir, los usuarios con privilegios del DoD). | <a href="#">AWS Identity and Access Management (IAM)</a><br><br><a href="#">AWS Directory Service for Microsoft Active Directory</a> | N/A                     | Cubierto         |

Para permitir que el TCCM cumpla con los requisitos, la LZA utiliza el control programático de los recursos a través del servicio IAM. Además, puede combinar la IAM para implementar el inicio de sesión único AWS Managed Microsoft AD en otro directorio. Esto vincula el AWS entorno a la infraestructura local mediante la confianza de Active Directory. En la LZA, la implementación se implementa con funciones de IAM para un acceso temporal y basado en sesiones. Las funciones de IAM son credenciales efímeras que ayudan a la organización a cumplir los requisitos de TCCM necesarios.

Si bien la LZA implementa el acceso con privilegios mínimos y el acceso programático a corto plazo a AWS los recursos, revise las [mejores prácticas de IAM para asegurarse de seguir las pautas](#) de seguridad recomendadas.

---

Para obtener más información sobre la implementación AWS Managed Microsoft AD, consulte la [AWS Managed Microsoft AD](#) sección del taller del Día de Inmersión de Active Directory en AWS.

El [modelo de responsabilidad AWS compartida](#) se aplica a la TCCM y a la LZA. La LZA desarrolla los aspectos fundamentales del control de acceso, pero cada organización es responsable de la configuración de sus controles de seguridad.

## Conclusión

Para el Departamento de Defensa de los EE. UU. (DoD), esta guía explica cuáles son los requisitos de la Agencia de Sistemas de Información de Defensa (DISA) para implementar una arquitectura de computación en nube segura (SCCA). Al utilizar el acelerador de zonas de aterrizaje (LZA) AWS, puede implementar las AWS ofertas y eliminar el trabajo pesado e indiferenciado. Esto le ayuda a centrarse en su misión de crear una infraestructura de nube compatible con IL4 o IL5.

# Recursos

## AWS documentación

- [AWS Servicios incluidos en el ámbito de aplicación del programa](#) de AWS cumplimiento (conformidad)
- [Guía de requisitos de seguridad de la computación en la nube del Departamento de Defensa \(AWS cumplimiento\)](#)
- [Landing Zone Accelerator está activado AWS](#) (biblioteca de AWS soluciones)
- [Guía de implementación de Landing Zone Accelerator on AWS](#)
- [SCCA en el diagrama de arquitectura AWS GovCloud](#)

## Otros recursos

- [Guía de requisitos de seguridad de la computación en la nube](#) (sitio web de DISA)
- [Diseño de referencia del punto de acceso nativo en la nube \(CNAP\) del Departamento de Defensa \(DoD\)](#) (sitio web del DoD)
- [Hoja de datos sobre la arquitectura de computación en nube segura del DoD](#) (sitio web de DISA)

---

## Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las [notificaciones RSS](#).

| Cambio                              | Descripción | Fecha               |
|-------------------------------------|-------------|---------------------|
| <a href="#">Publicación inicial</a> | —           | 12 de marzo de 2024 |

# AWS Glosario de las Recomendaciones de

Los siguientes son términos de uso común en las estrategias, guías y patrones que se ofrecen en las AWS Recomendaciones de. Para sugerir entradas, utilice el enlace [Enviar comentarios](#) al final del glosario.

## Números

### Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- **Refactorizar/rediseñar:** traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migre la base de datos Oracle en las instalaciones a Amazon Aurora Postgre Compatible Edition. SQL
- **Redefinir la plataforma (transportar y redefinir):** traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: Migre la base de datos Oracle en las instalaciones a Amazon Relational Database Service (RDSAmazon) para Oracle en. Nube de AWS
- **Recomprar (readquirir):** cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: Migre el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- **Volver a alojar (migrar mediante lift-and-shift):** traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: Migre la base de datos de Oracle en las instalaciones a Oracle en una EC2 instancia de Nube de AWS.
- **Reubicar:** (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar un Microsoft Hyper-V aplicación a AWS.
- **Retener (revisitar):** conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

## A

### ABAC

Consulte control de [acceso basado en atributos](#).

servicios abstractos

Consulte [servicios gestionados](#).

### ACID

Consulte [atomicidad, consistencia, aislamiento, durabilidad](#).

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que la migración [activa y pasiva](#).

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la base de datos de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

SQLFunción que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen SUM yMAX.

### IA

Véase [inteligencia artificial](#).

### AIOps

Consulte las [operaciones de inteligencia artificial](#).

## anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

## antipatronos

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

## control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

## cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para [el proceso de detección y análisis de la cartera](#) y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

## inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte [¿Qué es la inteligencia artificial?](#)

## operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración de, consulte la [Guía de integración de operaciones](#).

## cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

## atomicidad, consistencia, aislamiento, durabilidad () ACID

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

## control de acceso basado en atributos () ABAC

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte [ABAC](#) la [AWS](#) documentación de AWS Identity and Access Management (IAM).

## origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

## Zona de disponibilidad

Ubicación diferenciada de una Región de AWS que está aislada de los errores que se producen en otras zonas de disponibilidad y que brinda conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

## AWS Marco de adopción de la nube ()AWS CAF

Marco de directrices y prácticas recomendadas de AWS para ayudar a las empresas a desarrollar un plan eficiente y eficaz a fin de migrar con éxito a la nube de. AWS CAForganiza la orientación en seis áreas de enfoque llamadas perspectivas: empresarial, humana, gobernanza, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF brinda orientación para el desarrollo, la capacitación y la comunicación de las personas, con el fin de ayudar a preparar la organización para una adopción exitosa de la nube. Para obtener más información, consulte el [AWS CAFsitio web](#) y el [AWS CAFdocumento técnico](#).

## AWS Marco de calificación de la carga de trabajo ()AWS WQF

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y brinda estimaciones de trabajo. AWS WQFse incluye con AWS

Schema Conversion Tool (AWS SCT). Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

## B

bot malo

Un [bot](#) destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la [planificación de la continuidad del negocio](#).

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las API llamadas sospechosas y acciones similares. Para obtener más información, consulte [Datos en un gráfico de comportamiento](#) en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también [endianismo](#).

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

## bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

## botnet

Redes de [bots](#) que están infectadas por [malware](#) y que están bajo el control de una sola parte, conocida como pastor u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

## rama

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte [Acerca de las sucursales](#) (GitHub documentación).

## acceso con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador [Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS](#) .

## estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de [implementación desde cero](#).

## caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

## capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección [Organizado en torno a las capacidades empresariales](#) del documento técnico [Ejecutar microservicios en contenedores en AWS](#).

## planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

# C

## CAF

Consulte el [marco AWS de adopción de la nube](#).

## implementación de valores controlados

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando está seguro, despliega la nueva versión y reemplaza la versión actual en su totalidad.

## CCoE

Consulte [Centro de excelencia en la nube](#).

## CDC

Consulte la [captura de datos de cambios](#).

## captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizarse CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

## ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar [AWS Fault Injection Service \(AWS FIS\)](#) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

## CI/CD

Consulte [la integración y la entrega continuas](#).

### clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

### cifrado del cliente

Cifrado de datos de forma local, antes de que el de destino los Servicio de AWS reciba.

### Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las [CCoE Publicaciones](#) del Blog de estrategia Nube de AWS empresarial.

### computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de [computación](#) de punta.

### modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte [Creación de su modelo operativo de nube](#).

### etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a las Nube de AWS siguientes:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una landing zone, definir un CCoE, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales

- Reinención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la publicación del blog [The Journey Toward Cloud-First & the Stages of Adoption \(El camino hacia la nube como prioridad y las etapas de adopción\)](#) en el Blog de estrategia Nube de AWS empresarial. Para obtener información sobre cómo se relacionan con la estrategia de AWS migración, consulte la [Guía de preparación para la migración](#).

## CMDB

Consulte la [base de datos de administración de la configuración](#).

## repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub o AWS CodeCommit. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

## caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

## datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

## visión artificial (CV)

Campo de la [IA](#) que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, AWS Panorama ofrece dispositivos que añaden CV a las redes de cámaras locales, y Amazon SageMaker proporciona algoritmos de procesamiento de imágenes para CV.

## desviación de configuración

En el caso de una carga de trabajo, un cambio de configuración con respecto al estado esperado. Puede provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntario.

## base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos se utilizan CMDB en la etapa de detección y análisis de la cartera de productos durante la migración.

## paquete de conformidad

Una colección de acciones correctivas y AWS Config reglas de que puede reunir para personalizar sus controles de seguridad y conformidad. Puede implementar un paquete de conformidad como una sola entidad en una región Cuenta de AWS y, o en toda una organización, mediante una YAML plantilla. Para obtener más información, consulte [Paquetes de conformidad](#) en la AWS Config documentación de.

## integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte [Beneficios de la entrega continua](#). CD también puede significar implementación continua. Para obtener más información, consulte [Entrega continua frente a implementación continua](#).

## CV

Consulte [visión artificial](#).

## D

### datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

### clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del Marco AWS Well-Architected. Para obtener más información, consulte [Clasificación de datos](#).

## desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

## datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

## mallado de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con administración y gobierno centralizados.

## minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos en Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono derivada de los análisis.

## perímetro de datos

Conjunto de barreras preventivas en su AWS entorno de que ayudan a garantizar que solo las identidades de confianza accedan a los recursos de confianza desde las redes esperadas. Para obtener más información, consulte [Crear un perímetro de datos sobre AWS](#)

## preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

## procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

## titular de los datos

Persona cuyos datos se recopilan y procesan.

## almacenamiento de datos

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y análisis.

## lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

## lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

## DDL

Consulte el [lenguaje de definición de bases](#) de datos.

## conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

## aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

## defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Cuando se adopta esta estrategia en AWS, se suman varios controles en diferentes capas de la AWS Organizations estructura de para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactor, la segmentación de la red y el cifrado.

## administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro de a fin de administrar las cuentas de la organización y los permisos para ese servicio. Esta cuenta

se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte [Servicios que funcionan con AWS Organizations](#) en la documentación de AWS Organizations .

## Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

### entorno de desarrollo

Consulte [entorno](#).

### control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte [Controles de detección](#) en Implementación de controles de seguridad en AWS.

### asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

### gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

### tabla de dimensiones

En un [esquema en estrella](#), tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

## desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

## recuperación de desastres (DR)

La estrategia y el proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos causados por un [desastre](#). Para obtener más información, consulte [Recuperación de desastres de cargas de trabajo en AWS: Recuperación en la nube en AWS Well-Architected Framework](#).

## DML

Consulte el lenguaje de manipulación de [bases de datos](#).

## diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, *Diseño impulsado por el dominio: abordando la complejidad en el corazón del software* (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte [Modernización de la versión antigua de Microsoft. ASP NET\(ASMX\) servicios web de forma incremental mediante contenedores y Amazon API Gateway](#).

## DR

Consulte [recuperación ante desastres](#).

## detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración de referencia. Por ejemplo, puedes usarlo AWS CloudFormation para [detectar desviaciones en los recursos del sistema](#) o puedes usarlo AWS Control Tower para [detectar cambios en tu landing zone](#) que puedan afectar al cumplimiento de los requisitos de gobierno.

## DVSM

Consulte [el mapeo de flujos de valor para el desarrollo](#).

## E

### EDA

Consulte el [análisis exploratorio de datos](#).

### computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con [la computación en la nube](#) de, la computación en la nube de puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

### cifrado

Proceso informático que transforma datos de texto plano, legibles por humanos, en texto cifrado.

### clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

### endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

### punto de conexión

[Consulte el punto final del servicio](#).

### servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final con otros Cuentas de AWS o AWS Identity and Access Management (IAM) principales AWS PrivateLink y conceder permisos a ellos. Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de interfazVPC. Para obtener más información, consulte [Creación de un servicio de punto](#) de conexión en la documentación de Amazon Virtual Private Cloud (AmazonVPC).

### planificación de recursos empresariales (ERP)

Sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad y la gestión de proyectos) de una empresa. [MES](#)

## cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte [Cifrado de sobre](#) en la documentación de AWS Key Management Service (AWS KMS).

## environment

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

## epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas de AWS CAF seguridad incluyen la administración de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS, consulte la [Guía de implementación del programa](#).

## ERP

Consulte la [planificación de recursos empresariales](#).

## análisis de datos de tipo exploratorio () EDA

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para

encontrar patrones, detectar anomalías y comprobar las suposiciones. EDAse realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

## F

### tabla de datos

La tabla central de un [esquema en forma de estrella](#). Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

### fallar rápido

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

### límite de aislamiento de errores

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte [Límites de AWS aislamiento de errores](#).

### rama de característica

Consulte la [sucursal](#).

### características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

### importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley los SHAP gradientes integrados. Para obtener más información, consulte [Interpretabilidad del modelo de machine learning con:AWS](#).

### transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de

datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

## FGAC

Consulte [control de acceso detallado](#).

control de acceso detallado () FGAC

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la [captura de datos de cambios](#) para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

## G

bloqueo geográfico

Consulta [las restricciones geográficas](#).

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulte [Restricción de la distribución geográfica de su contenido](#) en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, y el [flujo de trabajo basado en troncos](#) es el enfoque moderno preferido.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las

tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como [implementación sobre infraestructura existente](#). Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

## barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y la conformidad en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de IAM permisos. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

## H

### JA

Consulte [alta disponibilidad](#).

## migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. [AWS ofrece AWS SCT](#), lo cual ayuda con las conversiones de esquemas.

## alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

## modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

## migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS for SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

## datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

## hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, el hotfix suele realizarse fuera del flujo de trabajo típico de las DevOps versiones.

## periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

## I

## laC

Vea [la infraestructura como código](#).

## políticas basadas en identidad

Una política asociada a una o más entidades IAM principales que define sus permisos en el Nube de AWS entorno de la.

## aplicación inactiva

Aplicación que utiliza un promedio CPU de memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

## IloT

Consulte [Internet de las cosas industrial](#).

### infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar parches o modificar la infraestructura existente. [Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables](#). Para obtener más información, consulte las Mejores prácticas de [implementación mediante una infraestructura inmutable](#) en Well-Architected Framework AWS .

### entrante (de entrada) VPC

En una arquitectura de AWS varias cuentas de, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La [Arquitectura de referencia de AWS seguridad](#) de recomienda configurar su cuenta de red con entrada, saliente e inspección VPCs para proteger la interfaz bidireccional entre su aplicación e Internet en general.

### migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

### Industria 4.0

Un término que [Klaus Schwab](#) introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y la inteligencia artificial/aprendizaje automático.

### infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

### infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

## Internet de las cosas industrial (IIoT)

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte [Creación de una estrategia de transformación digital del Internet de las cosas industrial \(IIoT\)](#).

## inspección VPC

En una arquitectura de AWS varias cuentas de, una centralizada VPC que administra las inspecciones del tráfico de red entre VPCs (en la misma o en diferentes Regiones de AWS), Internet y las redes en las instalaciones. La [Arquitectura de referencia de AWS seguridad](#) de recomienda configurar su cuenta de red con entrada, saliente e inspección VPCs para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte [¿Qué es IoT?](#).

## interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte [Interpretabilidad del modelo de machine learning con AWS](#).

## IoT

Consulte [Internet de las cosas](#).

## Biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. ITIL proporciona la base para ITSM.

## Administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con ITSM las herramientas, consulte la [Guía de integración de operaciones](#).

## ITIL

Consulte la [biblioteca de información de TI](#).

## ITSM

Consulte [Administración de servicios de TI](#).

## L

### control de acceso basado en etiquetas () LBAC

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

### zona de aterrizaje

Una landing zone es un AWS entorno de correctamente diseñado, con varias cuentas, que es escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte [Configuración de un entorno de AWS seguro y escalable con varias cuentas](#).

### migración grande

Migración de 300 servidores o más.

### LBAC

Consulte control de [acceso basado en etiquetas](#).

### privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte [Aplicar permisos de privilegio mínimo](#) en la documentación. IAM

### migrar mediante lift-and-shift

[Consulte 7 Rs](#).

## sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también [endianness](#).

## entornos inferiores

[Véase entorno](#).

# M

## machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte [Machine learning](#).

## rama principal

Ver [sucursal](#).

## malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los keyloggers.

## servicios administrados

Servicios de AWS para los que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios gestionados. También se conocen como servicios abstractos.

## sistema de ejecución de fabricación () MES

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

## MAP

Consulte [Migration Acceleration Program](#).

## mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar ajustes. Un mecanismo es un ciclo que se refuerza y mejora a sí mismo a medida que funciona. Para obtener más información, consulte [Creación de mecanismos en AWS Well-Architected Framework](#).

## cuenta de miembro

Todas las Cuentas de AWS distintas de las cuentas de administración que forman parte de una organización en AWS Organizations. Una cuenta no puede pertenecer a más de una organización a la vez.

## MES

Consulte el [sistema de ejecución de la fabricación](#).

## Message Queuing Telemetry Transport (MQTT)

[Un protocolo de comunicación ligero machine-to-machine \(M2M\), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.](#)

## microservicio

Un servicio pequeño e independiente que se comunica a través de equipos pequeños APIs e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte [Integración de microservicios mediante servicios AWS sin servidor](#) de.

## arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte [Implementación de microservicios en AWS](#).

## Migration Acceleration Program (MAP)

AWS Programa de que brinda soporte de consultoría, capacitación y servicios para ayudar a las empresas a construir una base operativa sólida para migrar a la nube y ayudar a compensar el costo inicial de las migraciones. MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

### migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la [estrategia de migración de AWS](#).

### fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de la fábrica de migración suelen incluir operaciones, analistas y propietarios de negocios, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan en tiempo y forma. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la [discusión sobre las fábricas de migración](#) y la [Guía de fábricas de migración a la nube](#) en este contenido.

### metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son las subredes de destino, los grupos de seguridad y las AWS cuentas de.

### patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: Volver a alojar la migración en Amazon EC2 con AWS Application Migration Service.

## Migration Portfolio Assessment (MPA)

Herramienta en línea que brinda información a fin de validar los argumentos comerciales necesarios para migrar a Nube de AWS. MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, TCO comparaciones, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La [MPA herramienta](#) (requiere inicio de sesión) está disponible de forma gratuita para todos los AWS consultores de y los consultores APN asociados.

## Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de la nube de una organización, identificar los puntos fuertes y débiles, y elaborar un plan de acción para cerrar las brechas identificadas, mediante AWS CAF. Para obtener más información, consulte la [Guía de preparación para la migración](#). MRA es la primera fase de la [estrategia de AWS migración](#).

## estrategia de migración

Enfoque utilizado para migrar una carga de trabajo a Nube de AWS. Para obtener más información, consulte la entrada de las [7 R](#) de este glosario y consulte [Movilice a su organización para acelerar las migraciones a gran escala](#).

## ML

[Consulte aprendizaje automático.](#)

## modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para obtener más información, consulte [Estrategia para modernizar las aplicaciones en la Nube de AWS](#).

## evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para obtener más información, consulte [Evaluación de la preparación para la modernización de las aplicaciones en Nube de AWS](#).

## aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte [Descomposición de monolitos en microservicios](#).

## MPA

Consulte [la evaluación de la cartera de migración](#).

## MQTT

Consulte [Message Queuing Telemetry Transport](#).

## clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar “¿Este producto es un libro, un automóvil o un teléfono?” o “¿Qué categoría de productos es más interesante para este cliente?”.

## infraestructura mutable

Un modelo que actualiza y modifica la infraestructura existente para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso [de una infraestructura inmutable](#) como práctica recomendada.

## O

### OAC

[Consulte el control de acceso de origen](#).

### OAI

Consulte la [identidad de acceso de origen](#).

### OCM

Consulte [gestión del cambio organizacional](#).

## migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

### OI

Consulte [integración de operaciones](#).

### OLA

Ver acuerdo de [nivel operativo](#).

## migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

### OPC-UA

Consulte [Open Process Communications: arquitectura unificada](#).

## Comunicaciones de proceso abierto: arquitectura unificada (OPC-UA)

Un protocolo de comunicación machine-to-machine (M2M) para la automatización industrial. OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

## acuerdo de nivel operativo () OLA

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (). SLA

## revisión de la preparación operativa () ORR

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte [Operational Readiness Reviews \(ORR\) en AWS Well-Architected Framework](#).

## tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la

integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de [la industria 4.0](#).

#### integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la [Guía de integración de las operaciones](#).

#### registro de seguimiento organizativo

Registro de seguimiento creado por AWS CloudTrail que registra todos los eventos para todas las Cuentas de AWS en una organización en AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte [Creación de un registro de seguimiento para una organización](#) en la CloudTrail documentación.

#### administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. OCMayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración de, este marco se denomina aceleración de personas, debido a la velocidad de cambio requerida en los proyectos de adopción de la nube. Para obtener más información, consulte la [OCMguía de](#).

#### control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso a su contenido de Amazon Simple Storage Service (Amazon S3). OACadmite todos los depósitos de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y el cifrado dinámico PUT y DELETE las solicitudes al depósito de S3.

#### identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso al contenido de Amazon S3. Cuando lo utilizaOAI, CloudFront crea una entidad principal con la que Amazon S3 puede autenticarse. Las entidades principales autenticadas solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica CloudFront . Consulte también [OAC](#), que proporciona un control de acceso más detallado y mejorado.

## ORR

Consulte la [revisión de la preparación operativa](#).

## NO

Consulte [tecnología operativa](#).

### saliente (de salida) VPC

En una arquitectura de AWS varias cuentas de, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La [Arquitectura de referencia de AWS seguridad](#) de recomienda configurar su cuenta de red con entrada, saliente e inspección VPCs para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## P

### límite de permisos

Una política IAM de administración que se adjunta a IAM las entidades principales para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte [Límites de permisos](#) en la IAM documentación de.

### Información personalmente identificable (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos PII son los nombres, las direcciones y la información de contacto.

## PII

Consulte la [información de identificación personal](#).

### manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

## PLC

Consulte [controlador lógico programable](#).

## PLM

Consulte la [gestión del ciclo de vida del producto](#).

### política

Un objeto que puede definir los permisos (consulte la [política basada en la identidad](#)), especifique las condiciones de acceso (consulte la [política basada en los recursos](#)) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de [servicios](#)).

### persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte [Habilitación de la persistencia de datos en los microservicios](#).

### evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la [Evaluación de la preparación para la migración](#).

### predicate

Una condición de consulta que devuelve true o false, por lo general, se encuentra en una cláusula. WHERE

### inserción de predicados

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y mejora el rendimiento de las consultas.

### control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte [Controles preventivos](#) en Implementación de controles de seguridad en AWS.

## entidad principal

Entidad de AWS que puede realizar acciones y obtener acceso a los recursos. Esta entidad suele ser un usuario raíz de un Cuenta de AWS, un IAM rol o un usuario. Para obtener más información, consulte los [términos y conceptos de Principal in Roles](#) en la IAM documentación.

## Privacidad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de ingeniería.

## zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a DNS las consultas de un dominio y sus subdominios en uno o varios VPCs. Para obtener más información, consulte [Uso de zonas alojadas privadas](#) en la documentación de Route 53.

## control proactivo

[Control de seguridad](#) diseñado para evitar el despliegue de recursos que no cumplan con las normas. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la [guía de referencia de controles](#) en la AWS Control Tower documentación y consulte [Controles proactivos](#) en Implementación de controles de seguridad en AWS.

## gestión del ciclo de vida del producto (PLM)

La gestión de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta el rechazo y la retirada.

## entorno de producción

Consulte [el entorno](#).

## controlador lógico programable ( ) PLC

En la industria manufacturera, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

## seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

## publicar/suscribirse (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un microservicio basado en microservicios [MES](#), un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

## Q

### plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos SQL relacional.

### regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

## R

### RACIMatriz

Véase [responsable, confiable, consultada e informada \(RACI\)](#).

### ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

### RASCIMatriz

Véase [responsable, confiable, consultada e informada \(RACI\)](#).

### RCAC

Consulte [control de acceso por filas y columnas](#).

## read replica

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

## rediseñar

Ver [7 Rs.](#)

## objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

## objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

## refactorizar

Ver [7 Rs.](#)

## Región

Conjunto de AWS recursos de que se encuentran en un área geográfica. Cada Región de AWS está aislada y es independiente de las demás para ofrecer tolerancia a errores, estabilidad y resistencia. Para obtener más información, consulte [Regiones de AWS Especificar qué cuenta puede usar.](#)

## regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de “¿A qué precio se venderá esta casa?”, un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

## volver a alojar

Consulte [7 Rs.](#)

## versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

## trasladarse

Ver [7 Rs.](#)

## redefinir la plataforma

Ver [7 Rs.](#)

## recompra

Ver [7 Rs.](#)

## resiliencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. [La alta disponibilidad](#) y la [recuperación ante desastres](#) son consideraciones comunes a la hora de planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte [Nube de AWS Resiliencia](#).

## política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

## matriz responsable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina RASCI matriz y, si la excluye, se denomina RACI matriz.

## control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte [Controles receptivos](#) en Implementación de controles de seguridad en AWS.

## retain

Consulte [7 Rs.](#)

## jubilarse

Ver [7 Rs.](#)

## rotación

Proceso en el que periódicamente se cambia el [secreto](#) para que resulte más difícil que un atacante pueda acceder a las credenciales.

## control de acceso por filas y columnas (RCAC)

El uso de SQL expresiones básicas y flexibles que tienen reglas de acceso definidas. RCAC consta de permisos de fila y máscaras de columnas.

## RPO

Consulte el [objetivo del punto de recuperación](#).

## RTO

Consulte el [objetivo de tiempo de recuperación](#).

## manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

# S

## SAML2.0

Un estándar abierto que utilizan muchos proveedores de identidades (IdPs). Esta característica permite el inicio de sesión único (SSO) federado para que los usuarios puedan iniciar sesión en la AWS Management Console o invocar las AWS API operaciones de sin necesidad de crear un inicio de sesión de usuario IAM para cada persona de la organización. Para obtener más información sobre la federación SAML basada en 2.0, consulte [Acerca de la federación SAML basada en 2.0](#) en la IAM documentación.

## SCADA

Consulte el [control de supervisión y la adquisición de datos](#).

## SCP

Consulte la [política de control de servicios](#).

## secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus

metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulte [¿Qué hay en un secreto de Secrets Manager?](#) en la documentación de Secrets Manager.

## control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Hay cuatro tipos principales de controles de seguridad: [preventivos](#), de detección, de [respuesta](#) y [proactivos](#).

## refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

## sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un SIEM sistema recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

## automatización de respuesta de seguridad

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad [detectables](#) o [adaptables](#) que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automática incluyen la modificación de un grupo VPC de seguridad, la aplicación de parches a una EC2 instancia de Amazon o la rotación de credenciales.

## cifrado del servidor

Cifrado de los datos en su destino, por parte del Servicio de AWS que los recibe.

## política de control de servicios (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs define barreras de protección o establezca límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra

permitidos o prohibidos. Para obtener más información, consulte [Políticas de control de servicios](#) en la AWS Organizations documentación de.

#### punto de enlace de servicio

El URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte [Puntos de conexión de Servicio de AWS](#) en Referencia general de AWS.

#### acuerdo de nivel de servicio () SLA

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

#### indicador de nivel de servicio () SLI

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

#### objetivo de nivel de servicio () SLO

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de [servicio](#).

#### modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el [Modelo de responsabilidad compartida](#).

#### SIEM

Consulte [información sobre seguridad y sistema de administración de eventos](#).

#### punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

#### SLA

Consulte el acuerdo [de nivel de servicio](#).

#### SLI

Consulte el indicador de nivel de [servicio](#).

## SLO

Consulte el objetivo de nivel de [servicio](#).

### split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para obtener más información, consulte [Enfoque gradual para modernizar las aplicaciones en Nube de AWS](#).

## SPOF

Consulte el [punto único de fallo](#).

### esquema de estrellas

Estructura organizativa de una base de datos que utiliza una tabla de hechos grande para almacenar datos transaccionales o medidos y utiliza una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un [almacén de datos](#) o con fines de inteligencia empresarial.

### patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda dismantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue [presentado por Martin Fowler](#) como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte [Modernización gradual de MicrosoftASP. NET\(ASMX\) servicios web de forma incremental mediante contenedores y Amazon API Gateway](#).

## subred

Un intervalo de direcciones IP en su VPC Una subred debe residir en una sola zona de disponibilidad.

### control de supervisión y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

## cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

## pruebas de síntesis

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar [Amazon CloudWatch Synthetics](#) para crear estas pruebas.

# T

## etiquetas

Pares de clave y valor que funcionan como metadatos para organizar los recursos de. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte [Etiquetado de los recursos de AWS](#).

## variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

## lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

## entorno de prueba

[Consulte entorno.](#)

## entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

## puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar sus redes con las de VPCs las instalaciones. Para obtener más información, consulte [¿Qué es una puerta de enlace de tránsito?](#) en la AWS Transit Gateway documentación de.

## flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

## acceso de confianza

Concesión de permisos a un servicio que especifique para realizar tareas en su empresa en AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte [AWS Organizations Utilización con otros AWS servicios](#) en la AWS Organizations documentación.

## ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

## equipo de dos pizzas

Un pequeño DevOps equipo al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

# U

## incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía [Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo](#).

## tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

## entornos superiores

Ver [entorno](#).

## V

### succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

### control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

### VPCmirando

Conexión entre dos VPCs que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte [¿Qué es una VPC interconexión?](#) en la VPC documentación de Amazon.

### vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

## W

### caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

## datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

## función de ventana

SQLFunción que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

## carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

## flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

## WORM

Mira, [escribe una vez, lee muchas](#).

## WQF

Consulte el [marco AWS de calificación de la carga](#) de trabajo.

## escribe una vez, lee muchas (WORM)

Un modelo de almacenamiento que escribe los datos una sola vez y evita que los datos se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no pueden cambiarlos. Esta infraestructura de almacenamiento de datos se considera [inmutable](#).

---

## Z

### ataque de día cero

Un ataque, normalmente de malware, que se aprovecha de una [vulnerabilidad de día cero](#).  
vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

### aplicación zombi

Aplicación que utiliza un promedio CPU y un uso de memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.