AWS Guía de decisiones

# Elegir servicios AWS de seguridad, identidad y gobierno

# Elegir servicios AWS de seguridad, identidad y gobierno: AWS Guía de decisiones

# Table of Contents

# Elegir servicios AWS de seguridad, identidad y gobierno

Dando el primer paso

| | | |
|---|---|---|
| Es hora de leer | 27 minutos | |
| Finalidad | Le ayudan a determinar qué servicios de AWS seguridad, identidad y gobierno son los más adecuados para su organización. | |
| Última actualización | 30 de diciembre de 2024 | |
| Servicios cubiertos | • AWS Artifact<br>• AWS Audit Manager<br>• AWS Certificate Manager<br>• AWS CloudHSM<br>• AWS CloudTrail<br>• Amazon Cognito<br>• AWS Config<br>• AWS Control Tower<br>• Amazon Detective<br>• AWS Firewall Manager<br>• Amazon GuardDuty<br>• AWS IAM<br>• AWS IAM Identity Center<br>• Amazon Inspector | • AWS KMS<br>• Amazon Macie<br>• AWS Network Firewall<br>• AWS Organizations<br>• AWS Payment Cryptography<br>• AWS Private CA<br>• AWS RAM<br>• AWS Secrets Manager<br>• AWS Security Hub CSPM<br>• Amazon Security Lake<br>• AWS Respuesta a incidentes de seguridad<br>• AWS Shield<br>• AWS WAF |

## Introducción

La seguridad, la identidad y la gobernanza en la nube son componentes importantes para lograr y mantener la integridad y la seguridad de sus datos y servicios. Esto es especialmente relevante a medida que más empresas migran a proveedores de nube como Amazon Web Services (AWS).

Esta guía le ayuda a seleccionar los servicios y herramientas de AWS seguridad, identidad y gobierno que mejor se adapten a sus necesidades y a las de su organización.

En primer lugar, analicemos qué entendemos por seguridad, identidad y gobierno:

- La seguridad en la nube se refiere al uso de medidas y prácticas para proteger los activos digitales de las amenazas. Esto incluye tanto la seguridad física de los centros de datos como las medidas de ciberseguridad para protegerse contra las amenazas en línea. AWS prioriza la seguridad mediante el almacenamiento de datos cifrados, la seguridad de la red y la supervisión continua de las posibles amenazas.
- Los servicios de identidad le ayudan a gestionar de forma segura las identidades, los recursos y los permisos de forma escalable. AWS proporciona servicios de identidad diseñados para aplicaciones orientadas al personal y al cliente, y para administrar el acceso a sus cargas de trabajo y aplicaciones.
- La gobernanza de la nube es un conjunto de reglas, procesos e informes que guían a su organización a seguir las mejores prácticas. Puede establecer la gobernanza de la nube en todos sus AWS recursos, utilizar las mejores prácticas y estándares integrados y automatizar los procesos de conformidad y auditoría. El cumplimiento en la nube se refiere al cumplimiento de las leyes y reglamentos que rigen la protección y la privacidad de los datos. AWS Los programas de conformidad proporcionan información sobre las certificaciones, los reglamentos y los marcos a los que AWS se ajustan.

Este video de one-and-a-half un minuto resume cómo crear una AWS seguridad sólida en nuestro núcleo.

# Comprenda los servicios de AWS seguridad, identidad y gobierno

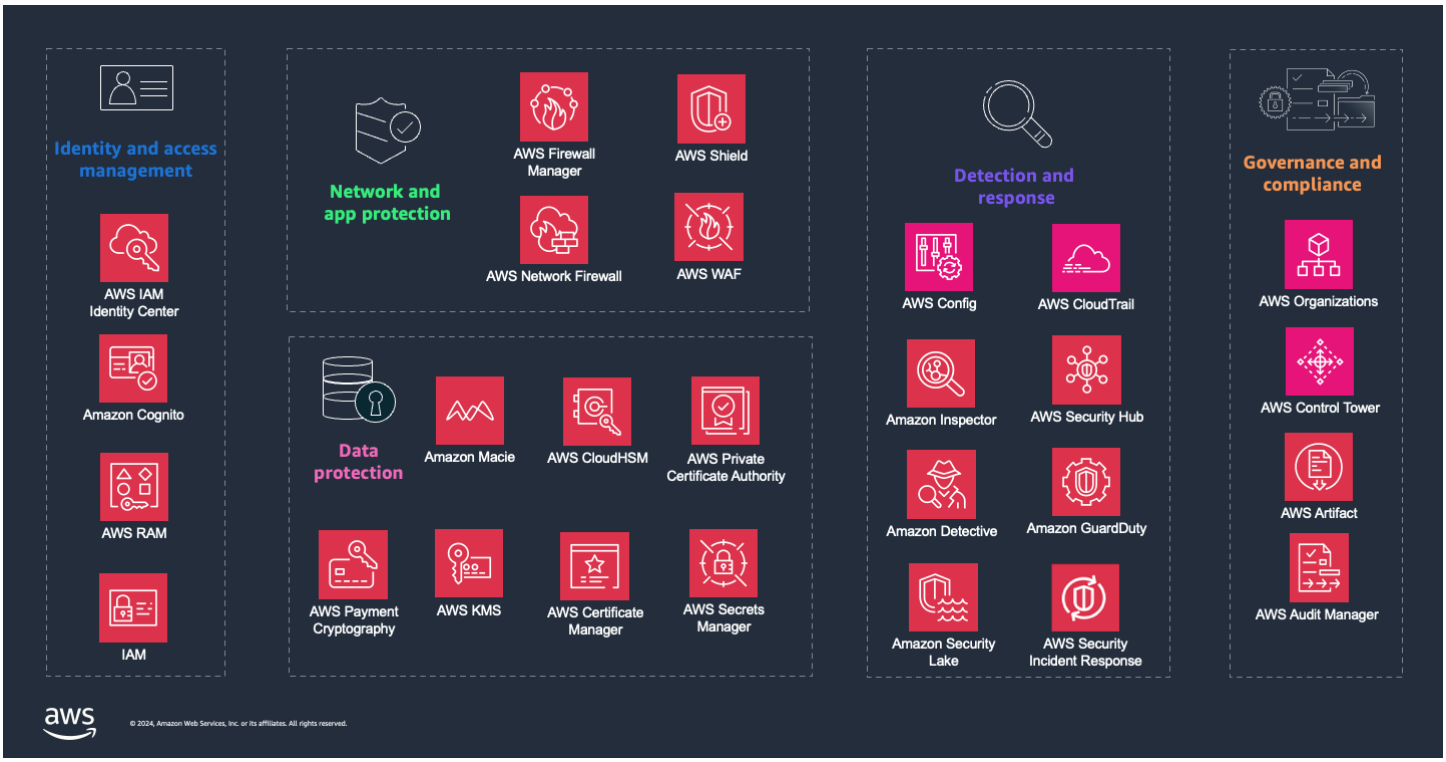
## La seguridad y el cumplimiento son responsabilidades compartidas

Antes de elegir sus servicios de AWS seguridad, identidad y gobierno, es importante que comprenda que la seguridad y el cumplimiento son responsabilidades compartidas entre usted y él AWS.

La naturaleza de esta responsabilidad compartida ayuda a aliviar su carga operativa y le proporciona flexibilidad y control sobre su implementación. Esta diferenciación de responsabilidades suele denominarse seguridad «de» la nube y seguridad «en» la nube.

Una vez que conozca este modelo, podrá comprender la gama de opciones disponibles y la Servicios de AWS forma en que se combinan las opciones aplicables.

# Puede combinar AWS herramientas y servicios para ayudar a proteger sus cargas de trabajo




Como se muestra en el diagrama anterior, AWS ofrece herramientas y servicios en cinco dominios para ayudarle a lograr y mantener una seguridad, una gestión de identidades y un gobierno sólidos en la nube. Puede utilizarlos Servicios de AWS en estos cinco dominios como ayuda para hacer lo siguiente:

- Adopte un enfoque de varios niveles para proteger sus datos y entornos
- Fortalezca su infraestructura de nube contra las amenazas en constante evolución
- Cumpla con los estrictos estándares regulatorios

Para obtener más información sobre AWS la seguridad, incluida la documentación de seguridad Servicios de AWS, consulte AWS la documentación de seguridad.

En las siguientes secciones, examinamos cada dominio con más detalle.

## Comprenda los servicios de administración de AWS identidad y acceso

En el centro de la AWS seguridad está el principio del mínimo privilegio: las personas y los servicios solo tienen el acceso que necesitan. AWS IAM Identity Centeres el recomendado Servicio de AWS

para administrar el acceso de los usuarios a AWS los recursos. Puede usar este servicio para administrar el acceso a sus cuentas y los permisos dentro de esas cuentas, incluidas las identidades de proveedores de identidad externos.

En la siguiente tabla se resumen las ofertas de administración de identidades y accesos que se describen en esta guía:

AWS IAM Identity Center

AWS IAM Identity Centerle ayuda a conectar su fuente de identidades o a crear usuarios. Puede gestionar de forma centralizada el acceso de los empleados Cuentas de AWS a múltiples aplicaciones.

Amazon Cognito

Amazon Cognito proporciona una herramienta de identidad para que las aplicaciones web y móviles autentiquen y autoricen a los usuarios desde el directorio de usuarios integrado, el directorio empresarial y los proveedores de identidad de los consumidores.

AWS RAM

AWS RAMle ayuda a compartir de forma segura sus recursos entre toda la organización Cuentas de AWS, dentro de ella y con las funciones y los usuarios de IAM.

IAM

La IAM permite un control seguro y detallado del acceso a los recursos de la carga de trabajo. AWS

## Comprenda los servicios de protección de datos AWS

La protección de datos es vital en la nube y AWS proporciona servicios que le ayudan a proteger sus datos, cuentas y cargas de trabajo. Por ejemplo, cifrar los datos tanto en tránsito como en reposo ayuda a protegerlos de la exposición. Con AWS Key Management Service(AWS KMS), AWS CloudHSMpuede crear y controlar las claves criptográficas que utiliza para proteger sus datos.

En la siguiente tabla se resumen las ofertas de protección de datos que se analizan en esta guía:

Amazon Macie

Amazon Macie descubre datos confidenciales mediante el aprendizaje automático y la coincidencia de patrones, y permite la protección automatizada contra los riesgos asociados.

AWS KMS

AWS KMScrea y controla las claves criptográficas que utiliza para proteger sus datos.

AWS CloudHSM

AWS CloudHSMproporciona módulos de seguridad de hardware basados en la nube y de alta disponibilidad (HSMs).

AWS Certificate Manager

AWS Certificate Managergestiona la complejidad de crear, almacenar y renovar certificados y claves SSL/TLS X.509 públicos y privados.

AWS Private CA

AWS Private CAle ayuda a crear jerarquías de autoridades de certificación privadas, incluidas las autoridades de certificación raíz y subordinadas (). CAs

AWS Secrets Manager

AWS Secrets Managerle ayuda a administrar, recuperar y rotar las credenciales de las bases de datos, las credenciales de las aplicaciones, OAuth los tokens, las claves de API y otros secretos.

AWS Payment Cryptography

AWS Payment Cryptographyproporciona acceso a las funciones criptográficas y a la gestión de claves que se utilizan en el procesamiento de pagos de acuerdo con los estándares del sector de las tarjetas de pago (PCI).

## Comprenda los AWS servicios de protección de redes y aplicaciones

AWS ofrece varios servicios para proteger sus redes y aplicaciones. AWS Shieldle proporciona protección contra los ataques de denegación de servicio (DDoS) distribuida y le AWS WAFayuda a proteger las aplicaciones web de los ataques de explotación web más comunes.

En la siguiente tabla se resumen las ofertas de protección de redes y aplicaciones que se analizan en esta guía:

AWS Firewall Manager

AWS Firewall Managersimplifica las tareas de administración y mantenimiento en múltiples cuentas y recursos de protección.

AWS Network Firewall

AWS Network Firewallproporciona un firewall de red gestionado y con estado y un servicio de detección y prevención de intrusiones con su VPC.

AWS Shield

AWS Shieldproporciona protección contra los ataques DDo S a los AWS recursos en las capas de red, transporte y aplicación.

AWS WAF

AWS WAFproporciona un firewall de aplicaciones web para que pueda supervisar las solicitudes HTTP (S) que se reenvían a los recursos de aplicaciones web protegidas.

## Comprenda los servicios de AWS detección y respuesta

AWS proporciona herramientas que le ayudan a optimizar las operaciones de seguridad en todo su AWS entorno, incluidos los entornos con varias cuentas. Por ejemplo, puede usar Amazon GuardDuty para la detección inteligente de amenazas y puede usar Amazon Detective para identificar y analizar los hallazgos de seguridad mediante la recopilación de datos de registro. AWS Security Hub CSPMes compatible con varios estándares de seguridad y proporciona una visión general de las alertas de seguridad y del estado de conformidad de todos ellos Cuentas de AWS. AWS CloudTrailrastrea la actividad de los usuarios y el uso de la interfaz de programación de aplicaciones (API), lo cual es crucial para comprender los eventos de seguridad y responder a ellos.

En la siguiente tabla se resumen las ofertas de detección y respuesta que se describen en esta guía:

AWS Config

AWS Configproporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS.

AWS CloudTrail

AWS CloudTrailregistra las acciones realizadas por un usuario, rol o Servicio de AWS.

AWS Security Hub CSPM

AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS.

Amazon GuardDuty

Amazon monitorea GuardDuty continuamente tus cargas de trabajo Cuentas de AWS, actividad en tiempo de ejecución y datos para detectar actividades maliciosas.

Amazon Inspector

Amazon Inspector analiza sus AWS cargas de trabajo en busca de vulnerabilidades de software y exposición no intencionada a la red.

Amazon Security Lake

Amazon Security Lake centraliza automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS, los entornos locales, las fuentes en la nube y las fuentes de terceros en un lago de datos.

Amazon Detective

Amazon Detective ayuda a analizar, investigar e identificar rápidamente la causa raíz de resultados de seguridad o actividades sospechosas.

AWS Security Incident Response

AWS Respuesta a incidentes de seguridad

Le ayuda a prepararse, responder y recibir orientación rápidamente para recuperarse de los incidentes de seguridad.

## Comprenda AWS los servicios de gobierno y cumplimiento

AWS proporciona herramientas que le ayudan a cumplir sus estándares de seguridad, operativos, de cumplimiento y de costos. Por ejemplo, puede utilizarlas AWS Control Towerpara configurar y gobernar un entorno de varias cuentas con controles prescriptivos. Con AWS Organizationsél, puede configurar la administración basada en políticas para varias cuentas de su organización.

AWS también le ofrece una visión completa de su estado de conformidad y supervisa continuamente su entorno mediante comprobaciones de conformidad automatizadas basadas en las AWS mejores prácticas y los estándares del sector que sigue su organización. Por ejemplo, AWS Artifactproporciona acceso bajo demanda a los informes de conformidad y AWS Audit Managerautomatiza la recopilación de pruebas para que pueda evaluar más fácilmente si sus controles funcionan de forma eficaz.

En la siguiente tabla se resumen las ofertas de control y cumplimiento que se analizan en esta guía:

AWS Organizations

AWS Organizationsle ayuda a consolidar varias organizaciones Cuentas de AWS en una organización que usted crea y administra de forma centralizada.

AWS Control Tower

AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas que se basa en las mejores prácticas.

AWS Artifact

AWS Artifactproporciona descargas a pedido de documentos de AWS seguridad y conformidad.

AWS Audit Manager

AWS Audit Manager

Le ayuda a auditar continuamente su AWS uso para simplificar la evaluación del riesgo y el cumplimiento.

# Tenga en cuenta los criterios de AWS seguridad, identidad y gobierno

La elección de los servicios de seguridad, identidad y gobierno adecuados AWS depende de sus requisitos y casos de uso específicos. La decisión de adoptar un servicio de AWS seguridad proporciona un árbol de decisiones que le ayuda a decidir si la adopción Servicios de AWS de un servicio de seguridad, identidad y gobierno es adecuada para su organización. Además, estos son algunos criterios que debe tener en cuenta a la hora de decidir qué servicios utilizar.

Security requirements and threat landscape

Realice una evaluación exhaustiva de las vulnerabilidades y amenazas específicas de su organización. Esto implica identificar los tipos de datos que maneja, como la información personal de los clientes, los registros financieros o los datos comerciales patentados. Comprenda los posibles riesgos asociados a cada uno de ellos.

Evalúe la arquitectura de su aplicación e infraestructura. Determine si sus aplicaciones están orientadas al público y qué tipo de tráfico web gestionan. Esto influye en su necesidad de servicios, por ejemplo, de AWS WAF protección contra la explotación web. En el caso de las aplicaciones internas, tenga en cuenta la importancia de la detección interna de amenazas y la supervisión continua con Amazon GuardDuty, que puede identificar patrones de acceso inusuales o despliegues no autorizados.

Por último, tenga en cuenta la sofisticación de su postura de seguridad actual y la experiencia de su equipo de seguridad. Si su equipo tiene recursos limitados, elegir servicios que ofrezcan más

automatización e integración puede proporcionarle mejoras de seguridad eficaces sin abrumar a su equipo. Algunos ejemplos de servicios son AWS Shield la protección DDo S y AWS Security Hub CSPM la supervisión centralizada de la seguridad.

Compliance and regulatory requirements

Identifique las leyes y estándares relevantes para su sector o región geográfica, como el Reglamento General de Protección de Datos (GDPR), la Ley de Portabilidad y Responsabilidad de los Seguros de Salud de los Estados Unidos de 1996 (HIPAA) o el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).

AWS ofrece servicios como AWS Config AWS Artifact para ayudarlo a gestionar el cumplimiento de varios estándares. Con él AWS Config, puede evaluar, auditar y evaluar las configuraciones de sus AWS recursos, lo que le facilita garantizar el cumplimiento de las políticas internas y los requisitos reglamentarios. AWS Artifact proporciona acceso bajo demanda a la documentación de AWS cumplimiento, lo que le ayuda con las auditorías y los informes de cumplimiento.

Elegir servicios que se ajusten a sus necesidades de cumplimiento específicas puede ayudar a su organización a cumplir con los requisitos legales y a crear un entorno seguro y confiable para sus datos. Explore los programas de AWS conformidad para obtener más información.

Scalability and flexibility

Considere cómo crecerá su organización y con qué rapidez. Elija lo Servicios de AWS que ayude a que sus medidas de seguridad crezcan sin problemas con su infraestructura y se adapten a las amenazas en constante evolución.

Para ayudarlo a escalar rápidamente, AWS Control Tower organiza las capacidades de varios otros Servicios de AWS, incluido AWS Organizations el AWS IAM Identity Center, para crear una landing zone en menos de una hora. Control Tower configura y administra los recursos en tu nombre.

AWS también diseña muchos servicios para que se escalen automáticamente con los patrones de tráfico y uso de una aplicación, como Amazon GuardDuty para la detección de amenazas y AWS WAF para la protección de las aplicaciones web. A medida que su empresa crece, estos servicios crecen con ella, sin requerir ajustes manuales ni provocar cuellos de botella.

Además, es fundamental que pueda personalizar sus controles de seguridad para que se adapten a los requisitos de su empresa y al panorama de amenazas. Considere la posibilidad de gestionar sus cuentas con AWS Organizations los recursos de más de 40 servicios de varias cuentas. Esto

proporciona a los equipos de aplicaciones individuales la flexibilidad y la visibilidad necesarias para gestionar las necesidades de seguridad específicas de su carga de trabajo, al tiempo que les proporciona control y visibilidad para los equipos de seguridad centralizados.

Tener en cuenta la escalabilidad y la flexibilidad le ayuda a garantizar que su postura de seguridad sea sólida, receptiva y capaz de adaptarse a entornos empresariales dinámicos.

Integration with existing systems

Considere medidas de seguridad que mejoren sus operaciones actuales, en lugar de interrumpirlas. Por ejemplo, considere lo siguiente:

- Optimice sus flujos de trabajo agregando datos y alertas de seguridad Servicios de AWS y analizándolos junto con los sistemas de gestión de eventos e información de seguridad (SIEM) existentes.
- Cree una visión unificada de las amenazas y vulnerabilidades de seguridad tanto en los entornos locales como en los AWS entornos locales.
- Intégrelo AWS CloudTrail con las soluciones de administración de registros existentes para una supervisión integral de las actividades de los usuarios y el uso de las API en toda su AWS infraestructura y aplicaciones existentes.
- Examine las formas de optimizar la utilización de los recursos y aplicar políticas de seguridad de forma coherente en todos los entornos. Esto le ayuda a reducir el riesgo de brechas en la cobertura de seguridad.

Cost and budget considerations

Revisa los modelos de precios de cada servicio que estés considerando. AWS a menudo, los cargos se basan en el uso, por ejemplo, en función del número de llamadas a la API, el volumen de datos procesados o la cantidad de datos almacenados. Por ejemplo, Amazon GuardDuty cobra en función de la cantidad de datos de registro analizados para la detección de amenazas, mientras que las AWS WAF facturas se basan en la cantidad de reglas implementadas y en la cantidad de solicitudes web recibidas.

Calcule el uso previsto para pronosticar los costes con precisión. Tenga en cuenta tanto las necesidades actuales como el crecimiento potencial o los picos de demanda. Por ejemplo, la escalabilidad es una característica clave Servicios de AWS, pero también puede provocar un aumento de los costes si no se gestiona con cuidado. Úselo Calculadora de precios de AWSpara modelar diferentes escenarios y evaluar su impacto financiero.

Evalúe el costo total de propiedad (TCO), que incluye los costos directos e indirectos, como el tiempo y los recursos necesarios para la administración y el mantenimiento. Optar por los servicios gestionados puede reducir los gastos operativos, pero podría tener un precio más elevado.

Por último, priorice sus inversiones en seguridad en función de la evaluación de riesgos. No todos los servicios de seguridad serán igual de importantes para su infraestructura, por lo que debe concentrar su presupuesto en las áreas que tendrán un impacto más significativo a la hora de reducir el riesgo y garantizar el cumplimiento. Equilibrar la rentabilidad con el nivel de seguridad que necesita es clave para una estrategia de AWS seguridad exitosa.

Organizational structure and access needs

Evalúe cómo está estructurada y funciona su organización, y cómo sus necesidades de acceso pueden variar según el equipo, el proyecto o la ubicación. Esto influye en la forma en que administra y autentica las identidades de los usuarios, asigna funciones y aplica los controles de acceso en todo el AWS entorno. Implemente las mejores prácticas, como la aplicación de permisos con privilegios mínimos y la exigencia de la autenticación multifactor (MFA).

La mayoría de las organizaciones necesitan un entorno de cuentas múltiples. Revise las prácticas recomendadas para este tipo de entorno y considere utilizarlas AWS Organizations y ayudarle AWS Control Tower a implementarlas.

Otro aspecto que debe tener en cuenta es la administración de las credenciales y las claves de acceso. Considere la posibilidad de utilizar el IAM Identity Center para centralizar la gestión del acceso en múltiples aplicaciones Cuentas de AWS y aplicaciones empresariales, lo que mejora tanto la seguridad como la comodidad del usuario. Para ayudarle a gestionar sin problemas el acceso a todas las cuentas de su organización, IAM Identity Center se integra con. AWS Organizations

Además, evalúe cómo estos servicios de administración de identidad y acceso se integran con sus servicios de directorio existentes. Si ya tiene un proveedor de identidad, puede integrarlo con el Centro de identidades de IAM mediante SAML 2.0 u OpenID Connect (OIDC). El Centro de Identidad de IAM también es compatible con el aprovisionamiento del Sistema de Gestión de Identidad entre Dominios (SCIM) para ayudar a mantener sus directorios sincronizados. Esto le ayuda a garantizar una experiencia de usuario segura y fluida al acceder a los recursos. AWS

# Elija un servicio AWS de seguridad, identidad y gobierno

Ahora que conoce los criterios para evaluar sus opciones de seguridad, está listo para elegir qué servicios de AWS seguridad podrían ser adecuados para los requisitos de su organización.

En la siguiente tabla, se muestran los servicios que están optimizados para determinadas circunstancias. Utilice la tabla para determinar el servicio que mejor se adapta a su organización y caso de uso.

> **Note**
>
> [1] Se integra con AWS Security Hub CSPM (lista completa)
> [2] Se integra con Amazon GuardDuty (lista completa)
> [3] se integra con Amazon Security Lake (lista completa)

## Elija los servicios de administración de AWS identidad y acceso

Otorgue a las personas adecuadas el nivel de acceso adecuado a los sistemas, las aplicaciones y los datos.

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de seguridad, identidad y gobierno |
|---|---|---|
| Utilice estos servicios para gestionar y controlar de forma segura el acceso de sus clientes, personal y cargas de trabajo. | Le ayuda a conectar su fuente de identidades o a crear usuarios. Puede gestionar de forma centralizada el acceso de los empleados a varias AWS cuentas y aplicaciones. | AWS IAM Identity Center |
| | Optimizado para autenticar y autorizar a los usuarios de aplicaciones web y móviles. | Amazon Cognito |
| | Optimizado para compartir recursos internos de forma segura. AWS | AWS RAM |

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de seguridad, identidad y gobierno |
|---|---|---|
| | Permite un control seguro y detallado del acceso a los recursos de la carga de trabajo. AWS | IAM 1 |

## Elija AWS los servicios de protección de datos

Automatice y simplifique las tareas de protección y seguridad de datos, que van desde la administración de claves y el descubrimiento de datos confidenciales hasta la administración de credenciales.

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de protección de datos |
|---|---|---|
| Utilice estos servicios para lograr y mantener la confidencialidad, integridad y disponibilidad de los datos confidenciales almacenados y procesados en AWS los entornos. | Optimizado para descubrir datos confidenciales. | Amazon Macie 1 |
| | Optimizado para claves criptográficas. | AWS KMS |
| | Optimizado para. HSMs | AWS CloudHSM |
| | Optimizado para claves y certificados SSL/TLS X.509 privados. | AWS Certificate Manager |
| | Optimizado para crear jerarquías de autoridades de certificación privadas. | AWS Private CA |
| | Optimizado para credenciales de bases de datos, credenciales de aplicaciones, OAuth | AWS Secrets Manager |

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de protección de datos |
| --- | --- | --- |
| | tokens, claves de API y otros secretos. | |
| | Optimizado para proporcionar acceso a las funciones criptográficas y a la gestión de claves utilizadas en el procesamiento de pagos de acuerdo con los estándares PCI. | AWS Payment Cryptography |

## Elija servicios AWS de protección de redes y aplicaciones

Proteja de forma centralizada sus recursos de Internet contra DDo los ataques comunes a aplicaciones y sistemas.

| ¿Cuándo deberías usarlo? | ¿Para qué está optimizado? | Servicios de protección de redes y aplicaciones |
| --- | --- | --- |
| Utilice estos servicios para aplicar políticas de seguridad detalladas en cada punto de control de la red. | Optimizado para configurar y administrar de forma centralizada las reglas de firewall. | AWS Firewall Manager[1.] |
| | Optimizado para proporcionar un firewall de red gestionado y con estado y un servicio de detección y prevención de intrusiones. | AWS Network Firewall |
| | Optimizado para proteger contra los ataques DDo S a AWS los recursos en las capas de red, transporte y aplicaciones. | AWS Shield |

| ¿Cuándo deberías usarlo? | ¿Para qué está optimizado? | Servicios de protección de redes y aplicaciones |
|---|---|---|
| | Optimizado para proporcionar un firewall de aplicaciones web. | AWS WAF |

## Elija los servicios AWS de detección y respuesta

Identifique y priorice continuamente los riesgos de seguridad, al tiempo que integra las mejores prácticas de seguridad desde el principio.

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de detección y respuesta |
|---|---|---|
| Utilice estos servicios para detectar y responder a los riesgos de seguridad en sus cuentas, de modo que pueda proteger sus cargas de trabajo a gran escala. | Optimizado para automatizar los controles de seguridad y centralizar las alertas de seguridad con integraciones de terceros AWS y con terceros. | AWS Security Hub CSPM[2, 3] |
| | Optimizado para evaluar, auditar y evaluar la configuración de sus recursos. | AWS Config[1.] |
| | Optimizado para registrar eventos de otros Servicios de AWS como registro de auditoría. | AWS CloudTrail |
| | Optimizado para la detección inteligente de amenazas y la elaboración de informes detallados. | Amazon GuardDuty [1] |

| ¿Cuándo se debe usar? | ¿Para qué está optimizado? | Servicios de detección y respuesta |
|---|---|---|
| | Optimizado para la gestión de vulnerabilidades. | Amazon Inspector [1] |
| | Optimizado para centralizar los datos de seguridad. | Amazon Security Lake [1] |
| | Optimizado para agregar y resumir posibles problemas de seguridad. | Amazon Detective [1, 2, 3] |
| | Optimizado para ayudarlo a clasificar los hallazgos , escalar los eventos de seguridad y administrar los casos que requieren su atención inmediata. | AWS Respuesta a incidentes de seguridad |

## Elija servicios de AWS gobierno y cumplimiento

Establezca la gobernanza de la nube en todos sus recursos y automatice sus procesos de conformidad y auditoría.

| ¿Cuándo debe usarlo? | ¿Para qué está optimizado? | Servicios de gobierno y cumplimiento |
|---|---|---|
| Utilice estos servicios para ayudarle a implementar las mejores prácticas y cumplir con los estándares del sector cuando los utilice AWS. | Optimizado para gestionar de forma centralizada varias cuentas y la facturación unificada. | AWS Organizations |
| | Optimizado para proporcio nar descargas a pedido de documentos de AWS seguridad y cumplimiento. | AWS Artifact |

| ¿Cuándo debe usarlo? | ¿Para qué está optimizado? | Servicios de gobierno y cumplimiento |
|---|---|---|
| | Optimizado para auditar AWS el uso. | AWS Audit Manager[1] |
| | Optimizado para configurar y administrar un entorno de AWS múltiples cuentas. | AWS Control Tower |

# Utilice los servicios de AWS seguridad, identidad y gobierno

Ahora debería tener una idea clara de lo que hace cada servicio de AWS seguridad, identidad y gobierno (y las AWS herramientas y servicios de apoyo) y cuáles podrían ser adecuados para usted.

Para explorar cómo usar cada uno de los servicios de AWS seguridad, identidad y gobierno disponibles y obtener más información sobre ellos, hemos proporcionado una guía para explorar cómo funciona cada uno de los servicios. En las siguientes secciones se proporcionan enlaces a documentación detallada, tutoriales prácticos y recursos para que pueda empezar.

## Utilice los AWS servicios de administración de identidad y acceso

Las siguientes tablas muestran algunos recursos útiles de administración de identidades y accesos, organizados por servicio, para ayudarle a empezar.

AWS IAM Identity Center

- Habilitación del Centro de Identidad de AWS IAM

  Habilite el Centro de identidad de IAM y comience a usarlo con su. AWS Organizations

  Explore la guía
- Configure el acceso de los usuarios con el directorio predeterminado del IAM Identity Center

  Utilice el directorio predeterminado como fuente de identidad y configure y pruebe el acceso de los usuarios.

  Comience con el tutorial

- Uso de Active Directory como fuente de identidad

  Complete la configuración básica para usar Active Directory como fuente de identidad del Centro de identidades de IAM.

  Comience con el tutorial
- Configure SAML y SCIM con Okta e IAM Identity Center

  Configure una conexión SAML con Okta e IAM Identity Center.

  Comience con el tutorial

Amazon Cognito

- Introducción a Amazon Cognito

  Obtenga información sobre las tareas más comunes de Amazon Cognito.

  Explore la guía
- Tutorial: Crear un grupo de usuarios

  Cree un grupo de usuarios que permita a sus usuarios iniciar sesión en su aplicación web o móvil.

  Comience con el tutorial
- Tutorial: Crear un grupo de identidades

  Cree un grupo de identidades que permita a sus usuarios obtener AWS credenciales temporales para acceder Servicios de AWS.

  Comience con el tutorial
- Taller de Amazon Cognito

  Practique el uso de Amazon Cognito para crear una solución de autenticación para una hipotética tienda de mascotas.

  Comience con el tutorial

### AWS RAM

- Empezando con AWS RAM

  Obtenga información sobre AWS RAM términos y conceptos.

  Explore la guía
- Trabajar con AWS recursos compartidos

  Comparta AWS los recursos que le pertenezcan y acceda a AWS los recursos que comparten con usted.

  Explora la guía
- Administrar los permisos en la AWS RAM

  Obtenga información sobre los dos tipos de permisos administrados: permisos AWS administrados y permisos administrados por el cliente.

  Explore la guía
- Configure el acceso detallado a los recursos que se comparten mediante la AWS RAM

  Utilice los permisos gestionados por el cliente para personalizar el acceso a los recursos y aplicar las mejores prácticas en materia de privilegios mínimos.

  Lea el blog

### IAM

- Cómo empezar con IAM

  Cree funciones, usuarios y políticas de IAM mediante. Consola de administración de AWS

  Comience con el tutorial
- Delega el acceso mediante el Cuentas de AWS uso de roles

  Utilice un rol para delegar el acceso a recursos distintos de Cuentas de AWS los suyos, denominado Producción y Desarrollo.

  Comience con el tutorial
- Cree una política gestionada por el cliente

Utilice la Consola de administración de AWS para crear una política gestionada por el cliente y, a continuación, adjunte esa política a un usuario de IAM de la suya Cuenta de AWS.

Comience con el tutorial

- Defina los permisos para acceder a AWS los recursos en función de las etiquetas

  Cree y pruebe una política que permita a los roles de IAM con etiquetas principales acceder a los recursos con etiquetas coincidentes.

  Comience con el tutorial
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)

  Ayude a proteger sus AWS recursos mediante las prácticas recomendadas de IAM.

  Explore la guía

## Utilice AWS los servicios de protección de datos

La siguiente sección le proporciona enlaces a recursos detallados que describen la protección AWS de datos.

Macie

- Cómo empezar a usar Amazon Macie

  Habilite Macie para usted Cuenta de AWS, evalúe su postura de seguridad de Amazon S3 y configure los ajustes y recursos clave para descubrir y reportar datos confidenciales en sus buckets de S3.

  Explore la guía
- Supervisión de la seguridad y la privacidad de los datos con Amazon Macie

  Utilice Amazon Macie para supervisar la seguridad de los datos de Amazon S3 y evaluar su nivel de seguridad.

  Explore la guía
- Análisis de los hallazgos de Amazon Macie

  Revise, analice y gestione los hallazgos de Amazon Macie.

Explore la guía

- Recuperación de muestras de datos confidenciales con los hallazgos de Amazon Macie

  Utilice Amazon Macie para recuperar y revelar muestras de datos confidenciales que se obtienen mediante hallazgos individuales.

  Explore la guía

- Descubrimiento de datos confidenciales con Amazon Macie

  Automatice el descubrimiento, el registro y la generación de informes de datos confidenciales en su patrimonio de datos de Amazon S3.

  Explore la guía

AWS KMS

- Empezando con AWS KMS

  Administre las claves KMS de cifrado simétrico, desde su creación hasta su eliminación.

  Explore la guía

- Teclas de uso especial

  Obtenga información sobre los distintos tipos de claves que AWS KMS admite, además de las claves KMS de cifrado simétrico.

  Explore la guía

- Amplíe sus capacidades de cifrado en reposo con AWS KMS

  Obtenga información sobre las opciones de cifrado en reposo disponibles en AWS.

  Explore el taller

AWS CloudHSM

- ¿Cómo empezar con AWS CloudHSM

  Crear, inicializar y activar un AWS CloudHSM clúster.

Explore la guía

- Administración de AWS CloudHSM clústeres

  Conéctese a su AWS CloudHSM clúster y a las distintas tareas administrativas de la administración de su clúster.

  Explore la guía

- Administrar los usuarios y las claves de HSM AWS CloudHSM

  Cree usuarios y claves HSMs en su clúster.

  Explore la guía

- Automatice la implementación de un servicio web de NGINX mediante Amazon ECS con la descarga de TLS en CloudHSM

  Úselo AWS CloudHSM para almacenar las claves privadas de los sitios web que están alojados en la nube.

  Lee el blog

AWS Certificate Manager

- ¿Solicitar un certificado público

  Utilice la consola AWS Certificate Manager (ACM) o AWS CLI solicite un certificado ACM público.

  Explore la guía

- Mejores prácticas para AWS Certificate Manager

  Conozca las mejores prácticas basadas en la experiencia real de los clientes actuales de ACM.

  Explore la guía

- Cómo utilizar para hacer AWS Certificate Manager cumplir los controles de emisión de certificados

  Utilice las claves de condición de IAM para asegurarse de que sus usuarios emitan o soliciten certificados TLS de acuerdo con las directrices de su organización.

Lea el blog

AWS Private CA

- ¿Planeando su AWS Private CA despliegue

  Prepárese AWS Private CA para su uso antes de crear una entidad de certificación privada.

  Explore la guía
- AWS Private CA administración

  Cree una jerarquía completamente AWS alojada de autoridades de certificación raíz y subordinadas para uso interno de su organización.

  Explore la guía
- Administración de certificados

  Realice tareas básicas de administración de certificados AWS Private CA, como emitir, recuperar y enumerar certificados privados.

  Explore la guía
- AWS Private CA taller

  Desarrolle experiencia práctica con varios casos de uso de autoridades de certificación privadas.

  Explore el taller
- Cómo simplificar el aprovisionamiento de certificados en Active Directory con AWS Private CA

  Úselo AWS Private CA para aprovisionar certificados más fácilmente para usuarios y máquinas dentro de su entorno de Microsoft Active Directory.

  Lea el blog
- Cómo hacer cumplir las restricciones de nombres de DNS en AWS Private CA

  Aplique restricciones de nombres DNS a una CA subordinada mediante el AWS Private CA servicio.

  Lea el blog

AWS Secrets Manager

- AWS Secrets Manager conceptos

  Realice tareas básicas de administración de certificados AWS Private CA, como emitir, recuperar y enumerar certificados privados.

  Explore la guía
- Configure la rotación alterna de usuarios para AWS Secrets Manager

  Configure una rotación alterna de usuarios para un secreto que contenga las credenciales de la base de datos.

  Explore la guía
- Cómo usar AWS Secrets Manager los secretos con Kubernetes

  Muestre los secretos de Secrets Manager como archivos montados en los pods de Amazon EKS mediante el proveedor de AWS secretos y configuración (ASCP).

  Explore la guía

AWS Payment Cryptography

- Empezando con AWS Payment Cryptography

  Cree claves y utilícelas en diversas operaciones criptográficas.

  Explore la guía
- AWS Payment Cryptography FAQs

  Comprenda los conceptos básicos de AWS Payment Cryptography.

  Explore el FAQs

## Utilice los servicios de protección de AWS redes y aplicaciones

Las siguientes tablas proporcionan enlaces a recursos detallados que describen la protección AWS de redes y aplicaciones.

### AWS Firewall Manager

- Cómo empezar con AWS Firewall Manager las políticas

  Se utiliza AWS Firewall Manager para activar diferentes tipos de políticas de seguridad.

  Explore la guía
- Cómo auditar y limitar continuamente los grupos de seguridad con AWS Firewall Manager

  Úselo AWS Firewall Manager para limitar los grupos de seguridad, asegurándose de que solo estén abiertos los puertos necesarios.

  Lea el blog
- AWS Firewall Manager Úselo para implementar la protección a gran escala AWS Organizations

  Úselo AWS Firewall Manager para implementar y administrar políticas de seguridad en toda su empresa AWS Organizations.

  Lea el blog

### AWS Network Firewall

- Empezando con AWS Network Firewall

  Configure e implemente un AWS Network Firewall firewall para una VPC con una arquitectura básica de puerta de enlace a Internet.

  Explore la guía
- AWS Network Firewall Taller

  Implemente y utilice la infraestructura como código. AWS Network Firewall

  Explore el taller
- Guía práctica del motor de reglas AWS Network Firewall flexibles: primera parte

  Implemente una demostración AWS Network Firewall de Cuenta de AWS cómo interactuar con su motor de reglas.

  Lea el blog
- Tutorial práctico del motor de reglas AWS Network Firewall flexibles: parte 2

Cree una política de firewall con un orden de reglas estricto y establezca una o más acciones predeterminadas.

Lea el blog

- Modelos de despliegue para AWS Network Firewall

  Conozca los modelos de implementación para casos de uso comunes que puede agregar AWS Network Firewall a la ruta de tráfico.

  Lea el blog

- Modelos de implementación AWS Network Firewall con mejoras de enrutamiento de VPC

  Utilice primitivas de enrutamiento de VPC mejoradas para insertar AWS Network Firewall entre cargas de trabajo en diferentes subredes de la misma VPC.

  Lea el blog

AWS Shield

- ¿Cómo AWS Shield funciona

  Aprenda AWS Shield Standard a proteger los AWS recursos de las capas de red y transporte (capas 3 y 4) y de aplicación (capa 7) y AWS Shield Advanced proporcione protección contra los ataques DDo S.

  Explore la guía

- Empezando con AWS Shield Advanced

  Comience con AWS Shield Advanced la consola Shield Advanced.

  Explore la guía

- AWS Shield Advanced taller

  Proteja los recursos expuestos a Internet contra los ataques DDo S, supervise los ataques DDo S contra su infraestructura y notifique a los equipos correspondientes.

  Explore el taller

AWS WAF

- ¿Cómo empezar con AWS WAF

  Configura AWS WAF, crea una ACL web y protege Amazon CloudFront añadiendo reglas y grupos de reglas para filtrar las solicitudes web.

  Comience con el tutorial

- Análisis AWS WAF de registros en Amazon CloudWatch Logs

  Configure el AWS WAF registro nativo en CloudWatch los registros de Amazon y visualice y analice los datos de los registros.

  Lea el blog

- Visualiza AWS WAF los registros con un CloudWatch panel de Amazon

  Usa Amazon CloudWatch para monitorear y analizar AWS WAF la actividad mediante CloudWatch métricas, Contributor Insights y Logs Insights.

  Lea el blog

## Utilice los servicios AWS de detección y respuesta

Las siguientes tablas proporcionan enlaces a recursos detallados que describen los servicios AWS de detección y respuesta.

AWS Config

- Empezando con AWS Config

  Configurar AWS Config y trabajar con AWS SDKs.

  Explora la guía

- Taller sobre riesgo y cumplimiento

  Automatice los controles mediante AWS Config AWS Managed Config Rules.

  Explore el taller

- AWS Config Biblioteca de kits de desarrollo de reglas: Cree y opere reglas a escala

Utilice el kit de desarrollo de reglas (RDK) para crear una AWS Config regla personalizada e implementarla con. RDKLib

Lea el blog

AWS CloudTrail

- Ver el historial de eventos

  Revisa la actividad AWS de la API en tu Cuenta de AWS página para ver los servicios compatibles CloudTrail.

  Comience con el tutorial
- Cree un registro para registrar los eventos de administración

  Cree un registro para registrar los eventos de administración en todas las regiones.

  Comience con el tutorial

AWS Security Hub CSPM

- Habilitación AWS Security Hub CSPM

  AWS Security Hub CSPM Actívalo con AWS Organizations o en una cuenta independiente.

  Explora la guía
- Agregación entre regiones

  Agregue AWS Security Hub CSPM los hallazgos de varias regiones de agregación Regiones de AWS a una sola región de agregación.

  Explore la guía
- AWS Security Hub CSPM taller

  Aprenda a usar, administrar AWS Security Hub CSPM y mejorar la postura de seguridad de sus AWS entornos.

  Explore el taller
- Tres patrones de uso recurrentes de Security Hub (CSPM) y cómo implementarlos

Obtenga información sobre los tres patrones de AWS Security Hub CSPM uso más comunes y cómo mejorar su estrategia para identificar y gestionar los hallazgos.

Lea el blog

Amazon GuardDuty

- Cómo empezar con Amazon GuardDuty

  Activa Amazon GuardDuty, genera muestras de resultados y configura alertas.

  Explora el tutorial
- Protección EKS en Amazon GuardDuty

  Utilice Amazon GuardDuty para supervisar los registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS).

  Explore la guía
- Protección Lambda en Amazon GuardDuty

  Identifique las posibles amenazas de seguridad al invocar una AWS Lambda función.

  Explore la guía
- GuardDuty Protección Amazon RDS

  Utilice Amazon GuardDuty para analizar y perfilar la actividad de inicio de sesión del Amazon Relational Database Service (Amazon RDS) para detectar posibles amenazas de acceso a sus bases de datos de Amazon Aurora.

  Explore la guía
- Protección de Amazon S3 en Amazon GuardDuty

  Úselo GuardDuty para monitorear CloudTrail los eventos de datos e identificar los posibles riesgos de seguridad en sus depósitos de S3.

  Explore la guía
- Detección y respuesta a amenazas con Amazon GuardDuty y Amazon Detective

  Aprende los conceptos básicos de Amazon GuardDuty y Amazon Detective.

Explore el taller

Amazon Inspector

- Primeros pasos con Amazon Inspector

  Activa los escaneos de Amazon Inspector para entender los resultados de la consola.

  Comience con el tutorial

- Gestión de vulnerabilidades con Amazon Inspector

  Utilice Amazon Inspector para escanear las instancias de Amazon EC2 y las imágenes de contenedores del Amazon Elastic Container Registry (Amazon ECR) en busca de vulnerabilidades de software.

  Explore el taller

- Cómo escanear EC2 con Amazon AMIs Inspector

  Cree una solución mediante el uso de varios Servicios de AWS dispositivos AMIs para analizar sus vulnerabilidades conocidas.

  Lea el blog

Amazon Security Lake

- Introducción a Amazon Security Lake

  Habilite Amazon Security Lake y comience a usarlo.

  Explore la guía

- Administrar varias cuentas con AWS Organizations

  Recopile registros de seguridad y eventos de varias Cuentas de AWS.

  Explore la guía

- Incorpore, transforme y entregue eventos publicados por Amazon Security Lake a Amazon Service OpenSearch

Ingiera, transforme y entregue datos de Amazon Security Lake a Amazon OpenSearch Service para que los usen sus SecOps equipos.

Lea el blog

- Cómo visualizar los resultados de Amazon Security Lake con Quick

  Consulte y visualice datos de Amazon Security Lake con Amazon Athena y Quick.

  Lea el blog

Amazon Detective

- Términos y conceptos de Amazon Detective

  Conozca los términos y conceptos clave que son importantes para entender Amazon Detective y su funcionamiento.

  Explore la guía
- Configuración de Amazon Detective

  Active Amazon Detective desde la consola Amazon Detective, la API de Amazon Detective o AWS CLI.

  Explore la guía
- Detección y respuesta a amenazas con Amazon GuardDuty y Amazon Detective

  Aprende los conceptos básicos de Amazon GuardDuty y Amazon Detective.

  Explore el taller

## Utilice los servicios de AWS gobierno y cumplimiento

Las siguientes tablas proporcionan enlaces a recursos detallados que describen la gobernanza y el cumplimiento.

AWS Organizations

- Crear y configurar una organización

Cree su organización y configúrela con dos cuentas de AWS miembros.

Comience con el tutorial

- Servicios que funcionan con AWS Organizations

  Comprenda cuáles Servicios de AWS puede utilizar AWS Organizations y las ventajas de utilizar cada servicio a nivel de toda la organización.

  Explore la guía

- Organice su AWS entorno mediante el uso de varias cuentas

  Implemente las mejores prácticas y las recomendaciones actuales para organizar su AWS entorno general.

  Lea el documento técnico

AWS Artifact

- Empezando con AWS Artifact

  Descargue informes de seguridad y conformidad, gestione los acuerdos legales y gestione las notificaciones.

  Explore la guía

- Gestión de acuerdos en AWS Artifact

  Úselo Consola de administración de AWS para revisar, aceptar y administrar los acuerdos de su cuenta u organización.

  Explore la guía

- Prepárese para una auditoría en la AWS primera parte: AWS Audit Manager y AWS Artifact AWS Config

  Úselo Servicios de AWS para ayudarlo a automatizar la recopilación de evidencia que se utiliza en las auditorías.

  Lea el blog

### AWS Audit Manager

- Activación AWS de Audit Manager

  Habilite Audit Manager mediante Consola de administración de AWS la API de Audit Manager o la AWS CLI.

  Explore la guía
- Tutorial para propietarios de auditorías: Cómo crear una evaluación

  Cree una evaluación mediante el marco de ejemplo de Audit Manager.

  Explore la guía
- Tutorial para delegados: Revisión de un conjunto de controles

  Revise un conjunto de controles que el propietario de una auditoría haya compartido con usted en Audit Manager.

  Explore la guía

### AWS Control Tower

- Empezando con AWS Control Tower

  Configura y lanza un entorno de múltiples cuentas, denominado landing zone, que siga las mejores prácticas prescriptivas.

  Explore la guía
- Modernización de la gestión de cuentas con Amazon Bedrock y AWS Control Tower

  Proporcione una cuenta de herramientas de seguridad y aproveche la IA generativa para agilizar el Cuenta de AWS proceso de configuración y administración.

  Lea el blog
- Construir un entorno bien diseñado AWS GovCloud (EE. UU.) con AWS Control Tower

  Configure su gobierno en las regiones AWS GovCloud (EE. UU.), incluida la gestión de sus AWS cargas de trabajo mediante las unidades organizativas () OUs y. Cuentas de AWS

  Lea el blog

# Explore los servicios de AWS seguridad, identidad y gobierno

Editable architecture diagrams

### Diagramas de arquitectura de referencia

Explore los diagramas de arquitectura de referencia que le ayudarán a desarrollar su estrategia de seguridad, identidad y gobierno.

Explore las arquitecturas de referencia de seguridad, identidad y gobierno

Ready-to-use code

| Solución destacada | AWS Soluciones |
| --- | --- |
| Información sobre seguridad en AWS<br><br>Implemente código AWS creado que le ayude a visualizar los datos en Amazon Security Lake para investigar y responder a los eventos de seguridad con mayor rapidez.<br><br>Explore esta solución | Explore las soluciones preconfiguradas y desplegables y sus guías de implementación, creadas por. AWS<br><br>Explore todas las AWS soluciones de seguridad, identidad y gobierno |

Documentation

| Documentos técnicos sobre seguridad, identidad y gobierno | AWS Blog de seguridad |
| --- | --- |
| Consulte los documentos técnicos para obtener más información y mejores prácticas sobre la elección, la implementación y el uso de los servicios de seguridad, identidad y gobierno que mejor se adapten a su organización.<br><br>Consulte los documentos técnicos sobre seguridad, identidad y gobierno | Explore las publicaciones del blog que abordan casos de uso de seguridad específicos.<br><br>Explore el blog AWS de seguridad |

# Historial de documentos

La siguiente tabla describe los cambios importantes en esta guía de decisiones. Para recibir notificaciones sobre las actualizaciones de esta guía, puede suscribirse a una fuente RSS.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualización de Re:Invent | Se agregó información sobre la respuesta a incidentes AWS de seguridad y. AWS Payment Cryptography Información de servicio actualizada para AWS Identity and Access Management y AWS IAM Identity Center. | 30 de diciembre de 2024 |
| Actualización de vídeo | Vídeo introductorio actualizado con una reciente charla relámpago de Re:inForce 2024. | 25 de junio de 2024 |
| Se agregaron servicios de gobierno | Amplió el alcance del documento para incluir la gobernanza, incluida la adición de AWS CloudTrail AWS Control Tower, y AWS Organizations. Se actualizaron los gráficos para reflejar el nuevo alcance. Se han aclarado las mejores prácticas en materia de identidad. Se hicieron cambios editoriales en todo el documento. | 7 de junio de 2024 |
| Publicación inicial | Guía publicada por primera vez. | 21 de marzo de 2024 |

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