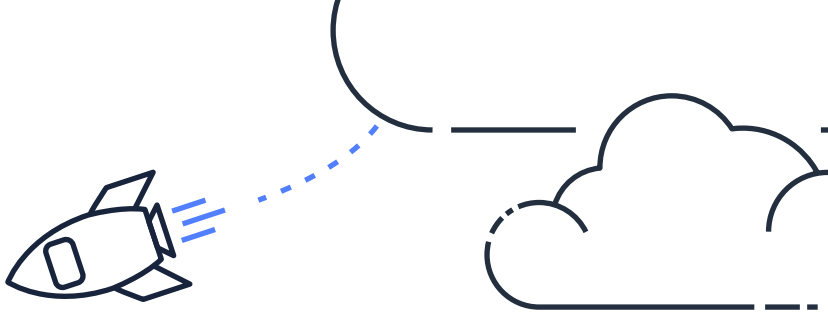
Seguridad y conformidad

Guía de referencia rápida

2021

Aviso

Los clientes son responsables de realizar su propia evaluación independiente de la información contenida en este documento. Este documento: (a) está previsto únicamente para fines informativos, (b) representa las prácticas y las ofertas de productos de AWS vigentes, sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía de AWS, sus empresas afiliadas, proveedores o concesionarios de licencias. Los productos o servicios de AWS se proporcionan "tal cual", sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS en relación con sus clientes se rigen por los acuerdos de AWS, y este documento no modifica ni forma parte de ningún acuerdo entre AWS y sus clientes.



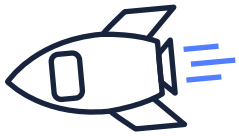
Contenido

Información general

En AWS, la seguridad es nuestra máxima prioridad.

Eso significa que la seguridad está profundamente arraigada en nuestra cultura y nuestros procesos, y que impregna todo lo que hacemos. ¿Qué implica esto para usted? Como cliente de AWS, se beneficia de una arquitectura de red y de centros de datos concebida para satisfacer los requisitos de seguridad de las organizaciones más exigentes del mundo. También obtiene servicios de seguridad avanzados diseñados por ingenieros con información sólida sobre las tendencias mundiales de seguridad, creados para trabajar integrados con productos que ya conoce y en los que confía de nuestra red de socios de AWS. Eso significa que puede elegir la seguridad que mejor se adapte a sus necesidades a medida que crezca, con una visibilidad profunda y un monitoreo continuo de su infraestructura en la nube, así como la capacidad de automatizar tareas para reducir el riesgo.

Esta Guía de referencia rápida (QRG) sobre seguridad y conformidad se ha creado para brindarle una amplia información general sobre cómo mantenemos la seguridad y la conformidad de la infraestructura de AWS, así como sobre los servicios de seguridad y conformidad que tiene a su disposición.



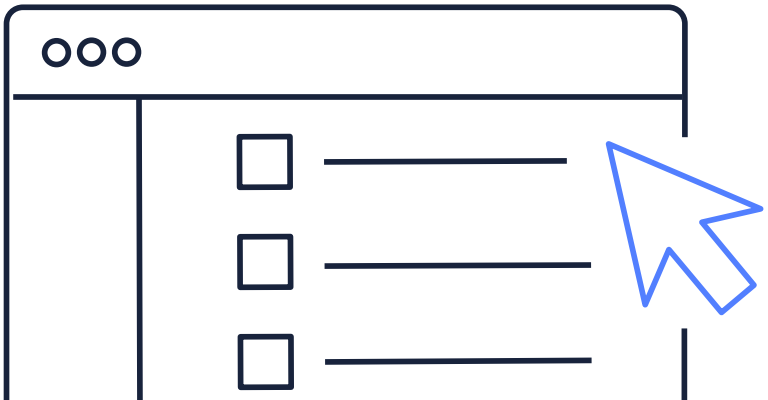
Beneficios de la seguridad con AWS

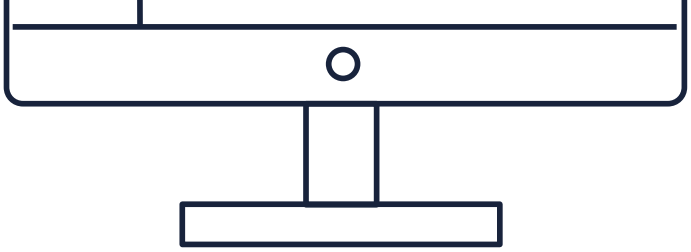
Desde que esta guía se publicó por primera vez hace varios años, la percepción sobre los proveedores de la nube pública ha cambiado.

La seguridad ya no se ve como algo que bloquee o frene la migración; por el contrario, es un factor diferenciador clave que puede utilizar para guiar las decisiones comerciales digitales de su organización, las selecciones de proveedores y tecnología y las estrategias de inversión. Muchos clientes ya han migrado con total confianza, porque saben que AWS se ha diseñado para que sea el entorno de informática en la nube más flexible y seguro disponible en la actualidad. Estos clientes han transformado el modo en que operan para centrarse en su negocio principal y, al mismo tiempo, proteger mejor su organización. Como cliente de AWS, puede obtener cinco beneficios principales de la seguridad con AWS.

Escale de forma segura con una visibilidad y un control superiores

Con AWS, puede controlar dónde se almacenan los datos, quién puede acceder a ellos y qué recursos está consumiendo su organización en cualquier momento. Los controles detallados de identidad y acceso, combinados con el monitoreo continuo de información de seguridad obtenida casi en tiempo real, le ayudan a garantizar que los recursos correctos cuentan con el acceso adecuado en todo momento, independientemente de dónde se encuentre almacenada la información. Reduzca el riesgo a medida que crece utilizando nuestros servicios de automatización de seguridad y monitoreo de la actividad para detectar eventos de seguridad sospechosos, tales como cambios de configuración, en todo su ecosistema. Puede incluso integrar nuestros servicios con sus propias soluciones para respaldar los flujos de trabajo existentes, optimizar las operaciones y simplificar la generación de informes de conformidad.





Automatice y reduzca el riesgo con servicios profundamente integrados

La automatización de las tareas de seguridad en AWS le permite lograr un mayor nivel de seguridad, ya que reduce los errores de configuración manuales y le da a su equipo más tiempo para centrarse en otras tareas esenciales para su organización. Seleccione entre una gran variedad de soluciones profundamente integradas que se pueden combinar para automatizar tareas de formas novedosas, lo que facilita a su equipo de seguridad trabajar mano a mano con los equipos de desarrollo y operaciones para crear e implementar código de forma más rápida y segura. Por ejemplo, al emplear tecnologías como el aprendizaje automático, AWS le permite descubrir, clasificar y proteger de forma automática y continua datos confidenciales en AWS con tan solo unos clics en la consola de AWS. También puede automatizar las verificaciones de seguridad de las aplicaciones y la infraestructura para aplicar constantemente sus comprobaciones de seguridad y conformidad, y contribuir a garantizar la confidencialidad, la integridad y la disponibilidad en todo momento. Automatice en un entorno híbrido con nuestras herramientas de seguridad y administración de la información para integrar AWS fácilmente como una extensión continua y segura de sus entornos locales y tradicionales.

Construya con los estándares más elevados de privacidad y seguridad de los datos

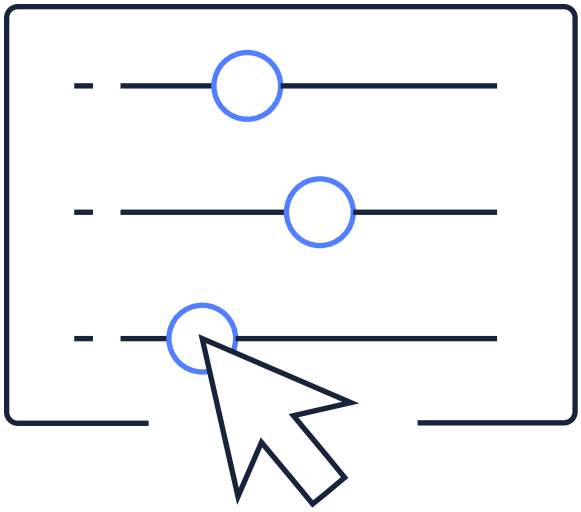
Sabemos que nuestros clientes se preocupan profundamente por la privacidad y la seguridad de los datos. Puesto que la seguridad de los datos es primordial para nuestros clientes, contamos con un equipo de expertos en seguridad de primer nivel que monitorean nuestros sistemas las 24 horas del día y los 7 días de la semana para proteger su contenido. Con AWS, puede crecer sobre la infraestructura global más segura, con la garantía de que siempre tendrá el control de sus datos, incluida la posibilidad de cifrarlos, trasladarlos y administrar su retención. Todos los datos que fluyen a través de la red global de AWS que interconecta nuestros centros de datos y regiones se cifran automáticamente en la capa física antes de salir de nuestras instalaciones protegidas. También existen capas de cifrado adicionales; por ejemplo, en todo el tráfico de interconexión entre VPC de diferentes regiones y en las conexiones TLS de cliente o de servicio a servicio. Le facilitamos herramientas para ayudarle a cifrar los datos fácilmente, en tránsito y en reposo, y garantizar que únicamente los usuarios autorizados puedan acceder a ellos. Puede utilizar claves administradas por AWS Key Management Service (KMS), con módulos de seguridad de hardware (HSM) con validación FIPS 140-2 Nivel 2, o administrar sus propias claves de cifrado con AWS CloudHSM mediante HSM con validación según FIPS 140-2 Nivel 3. También le ofrecemos el control y la visibilidad que necesita para demostrar que cumple con las leyes y normativas de privacidad de datos regionales y locales. El diseño de nuestra infraestructura global le permite conservar un control total sobre las regiones en las que se encuentran físicamente sus datos, lo que puede facilitarle el cumplimiento de los requisitos de residencia.

El mayor ecosistema de socios y soluciones de seguridad

Amplíe los beneficios de AWS mediante la tecnología de seguridad y los servicios de consultoría de proveedores de soluciones que ya conoce y en los que confía. Hemos seleccionado cuidadosamente a proveedores con una amplia experiencia y un éxito demostrado en la protección de todas las etapas de la adopción de la nube, desde la migración inicial hasta la administración diaria continua. Elija en nuestra Red de Socios de AWS (APN), un programa global de socios tecnológicos y consultores, muchos de los cuales se especializan en ofrecer soluciones y servicios centrados en la seguridad para sus cargas de trabajo y casos de uso específicos. Las soluciones de los socios de AWS permiten la automatización, la agilidad y el escalado de sus cargas de trabajo. Localice, compre, implemente y administre fácilmente estas soluciones de software listas para la nube, incluidos productos de software como servicio (SaaS), en cuestión de minutos en el AWS Marketplace. Estas soluciones trabajan de forma conjunta para ayudar a proteger sus datos de formas que no son viables en entornos locales, con soluciones disponibles para una amplia gama de cargas de trabajo y casos de uso.

Herede los controles de seguridad y conformidad más completos

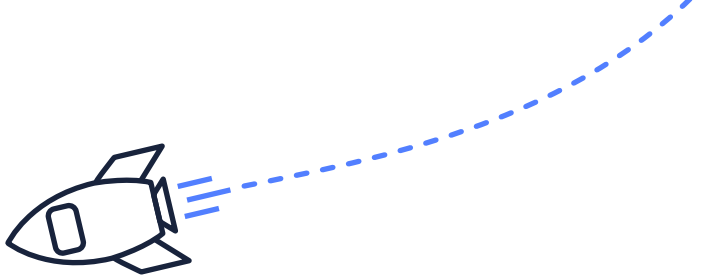
Para ayudarle en sus iniciativas de conformidad, AWS obtiene periódicamente certificaciones validadas por un tercero para miles de requisitos globales de conformidad que monitoreamos continuamente con el fin de ayudarle a cumplir las normas de seguridad y conformidad de los sectores financiero, venta minorista, salud, gubernamental, etc. Heredará los controles de seguridad más recientes operados por AWS, lo que reforzará sus propios programas de conformidad y certificación, a la vez que obtendrá acceso a herramientas que puede utilizar para reducir el costo y el tiempo necesarios para ejecutar sus propios requisitos específicos de garantía de la seguridad. AWS es compatible con más normas de seguridad informática y certificaciones de conformidad que cualquier otro proveedor, tales como SOC 2, PCI-DSS, HIPAA/HITECH, FedRAMP, el RGPD, FIPS 140-2 y NIST 800-171, lo que ayuda a que los clientes a cumplir con los requisitos de conformidad de prácticamente todas las agencias reguladoras del mundo.



Cómo compartimos la responsabilidad

Cuando migra su infraestructura a AWS, adopta el modelo de responsabilidad compartida. Este modelo reduce su carga operativa, porque nosotros operamos, administramos y controlamos las capas de los componentes de tecnología, desde el sistema operativo host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios. Así como comparte la responsabilidad de operar el entorno de tecnología con nosotros, también comparte la administración, operación y verificación de los controles de tecnología.

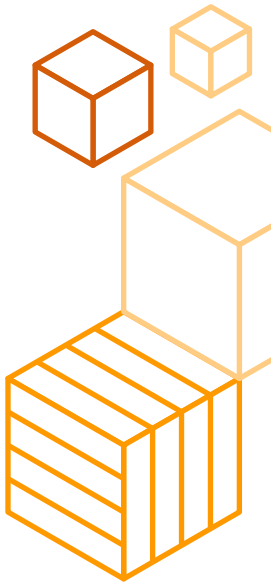
En resumen, AWS es responsable de la **seguridad "de" la nube**, y como cliente usted es responsable de la **seguridad "en" la nube** que describimos con más detalle a continuación.



Seguridad “de” la nube

AWS es responsable de la seguridad “de” la nube. Usted se beneficia de los centros de datos de AWS y de una red diseñada para proteger su información, sus identidades, sus aplicaciones y sus dispositivos. Y, además, hereda los controles de conformidad más completos creados para ayudar a cumplir los requisitos de conformidad de las agencias reguladoras de todo el mundo.

Garantía de seguridad de AWS



Gracias a nuestro modelo de responsabilidad compartida, los clientes pueden gestionar el riesgo de forma eficaz y eficiente en el entorno de tecnología, y brindamos la garantía de una administración de riesgos eficaz a través de nuestra conformidad con marcos y programas establecidos y ampliamente reconocidos.

Para demostrar que mantenemos un entorno de control integral que funciona de forma efectiva en nuestros servicios e instalaciones de todo el mundo, recurrimos a evaluaciones independientes de terceros.

Nuestro entorno de control incluye políticas, procesos y actividades de control que aprovechan diversos aspectos del entorno de control general de Amazon.

Certificaciones, programas, informes y acreditaciones independientes de AWS

AWS colabora con organismos de certificación externos y auditores independientes para ofrecer a los clientes información considerable acerca de las políticas, los procesos y los controles que establece y opera AWS.

Para ver una lista completa de los programas, visite *aws.amazon.com/compliance/programs*

El entorno de control colectivo incluye el personal, los procesos y la tecnología que se necesitan para establecer y mantener un entorno que respalde la eficacia operativa de nuestro marco de control. Hemos integrado en nuestro entorno controles aplicables específicos para la nube que fueron identificados por organismos de la industria de la informática en la nube. Monitoreamos estos grupos del sector para identificar prácticas recomendadas que usted pueda implementar y para ayudarle a administrar su propio entorno de control.

Demostramos nuestra conformidad para ayudarle a verificar su propia conformidad con los requisitos gubernamentales y del sector. Trabajamos con organismos de certificación externos y auditores independientes para ofrecerle información detallada acerca de las políticas, los procesos y los controles que definimos y aplicamos. Le proporcionamos certificados de conformidad, informes y otra documentación directamente a través del portal de autoservicio conocido como AWS Artifact. Puede utilizar esta información para realizar sus procedimientos de evaluación y verificación de control según sea necesario conforme al estándar de conformidad aplicable.

"De ninguna forma hubiéramos podido alcanzar los niveles de seguridad que tiene AWS. Tenemos una gran confianza en la separación lógica de los clientes en la nube de AWS, especialmente a través de Amazon VPC, lo que nos permite personalizar nuestro entorno de red virtual para cumplir con nuestros requerimientos específicos".

- Michael Lockhart
Administrador de infraestructura de tecnología

The GPT Group

Puede incorporar la información que suministramos sobre nuestro programa de riesgo y conformidad en su propio marco de conformidad. Utilizamos miles de controles de seguridad para monitorear que mantenemos la conformidad con los estándares y las prácticas recomendadas globalmente.

Privacidad

AWS vela por su privacidad. Usted siempre será dueño de su contenido, incluida la capacidad para cifrarlo, trasladarlo y administrar su retención. Le facilitamos herramientas para ayudarle a cifrar los datos fácilmente, en tránsito y en reposo, y a garantizar que únicamente los usuarios autorizados puedan acceder a ellos.

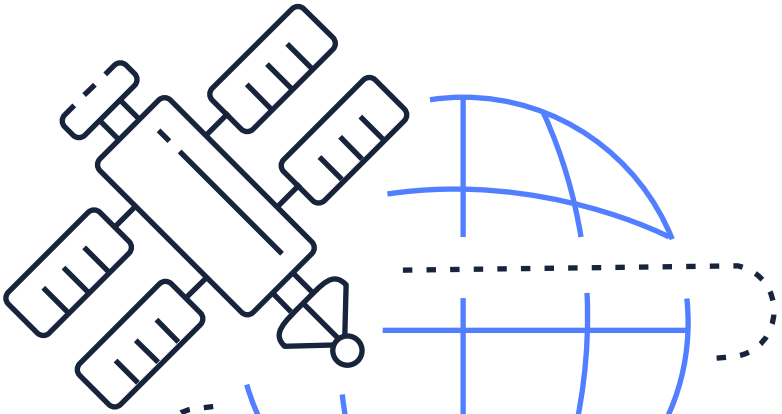
AWS le brinda un control que puede ayudarle a cumplir las leyes y normativas de privacidad de datos regionales y locales aplicables a su organización. El diseño de nuestra infraestructura global le permite conservar un control total sobre las ubicaciones en las que se almacenan físicamente sus datos, lo que puede facilitarle el cumplimiento de los requisitos de residencia.

Con AWS, usted sabe quién está accediendo a su contenido y qué recursos está consumiendo su organización en todo momento.

Asegúrese de que sus recursos cuentan con el nivel de acceso adecuado en todo momento aprovechando los controles detallados de identidad y acceso junto con el monitoreo continuo de información de seguridad obtenida casi en tiempo real, independientemente de dónde se encuentre almacenada la información.

Reduzca el nivel de riesgo y permita el crecimiento utilizando nuestros servicios de monitoreo de la actividad, que detectan cambios de configuración y eventos de seguridad en todo su sistema. Incluso puede integrar nuestros servicios con sus propias soluciones para contribuir a simplificar sus operaciones y la generación de informes de conformidad.

Obtenga más información en: *aws.amazon.com/compliance/data-privacy-faq*



Zonas de disponibilidad

- Regiones
- Disponibles próximamente

Dónde se almacena su contenido

Los centros de datos de AWS se agrupan en clústeres distribuidos por varias ubicaciones en todo el mundo. A cada uno de nuestros clústeres de centros de datos en una determinada ubicación lo denominamos “región de AWS”.

Usted tiene acceso a numerosas regiones de AWS en todo el mundo, y puede optar por utilizar una sola región, todas o cualquier combinación de regiones.

Usted conserva un control total sobre en qué regiones de AWS se almacenan físicamente sus datos, lo que puede facilitarle el cumplimiento de los requisitos de conformidad y residencia. Por ejemplo, si es un cliente europeo, puede optar por implementar sus servicios de AWS exclusivamente en la región EU (Frankfurt). Si elige esta opción, su contenido se almacenará exclusivamente en Alemania, a menos que seleccione una región de AWS diferente.

Información general sobre los centros de datos

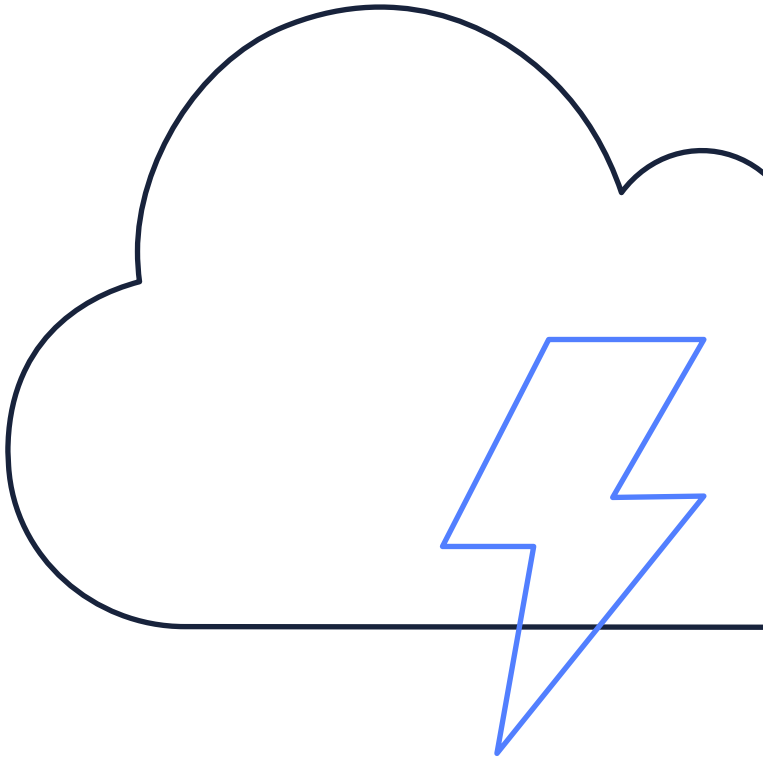
En AWS fuimos pioneros en informática en la nube en 2006, cuando creamos una infraestructura que le permite crear e innovar de forma segura y con más rapidez. Estamos innovando continuamente en lo que se refiere al diseño y los sistemas de nuestros centros de datos, para protegerlos de los riesgos naturales y de los provocados por el ser humano. Después implementamos controles, creamos sistemas automatizados y pasamos auditorías de terceros para confirmar la seguridad y la conformidad. Como resultado, las organizaciones altamente reguladas en todo el mundo confían en AWS todos los días.

Para obtener más información, visite: *aws.amazon.com/compliance/data-center/controls/*

Continuidad del negocio

Nuestra infraestructura presenta un alto nivel de disponibilidad y le ofrecemos las características que necesita para implementar una arquitectura de tecnología resiliente. Nuestros sistemas están diseñados para tolerar errores del sistema o del hardware con un impacto mínimo en los clientes.

El plan de continuidad del negocio de AWS expone medidas para evitar y reducir las interrupciones del entorno. Incluye detalles operativos sobre los pasos que se deben seguir antes, durante y después de un evento. El plan de continuidad del negocio está respaldado por pruebas que incluyen simulaciones de diferentes escenarios. Durante las pruebas y después de ellas, AWS documenta el rendimiento de las personas y los procesos, las acciones correctivas y las experiencias aprendidas con el propósito de mejorar continuamente.



"AWS nos permitió almacenar la información de una forma rentable y al mismo tiempo alivió la carga de prestar soporte a la infraestructura necesaria, ya que AWS se encarga de eso. Ciertamente es una opción con la que ganamos nosotros y nuestros clientes".

- Michael Lockhart
Administrador de infraestructura de tecnología

Nasdaq

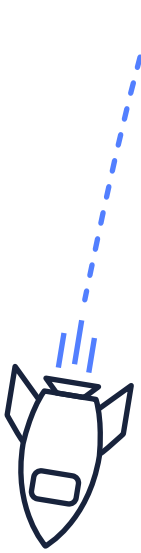
Recuperación de desastres

La nube de AWS admite muchas arquitecturas de recuperación de desastres, que van desde entornos de tipo "luz piloto", que están preparados para escalar verticalmente con poca antelación, hasta entornos de "espera activa", que permiten realizar una rápida conmutación por error.

Con nosotros, tiene la posibilidad de distribuir las aplicaciones entre varias zonas de disponibilidad de AWS, de modo que puede mantener la resiliencia ante la mayoría de los modos de error, incluidos desastres naturales o errores del sistema. Es importante señalar que todos los centros de datos se encuentran en línea y a disposición de los clientes, ninguno de ellos permanece "quieto". En caso de error, los procesos automatizados retiran el tráfico de datos de la zona afectada. Puede utilizar la infraestructura de AWS para lograr una recuperación de desastres más rápida de sus sistemas de tecnología esenciales y así evitar los gastos en infraestructura que supondría una segunda instalación física. Recuerde que usted es responsable de administrar y probar las copias de seguridad y la recuperación del sistema de información que se cree en la infraestructura de AWS. AWS ofrece **CloudEndure Disaster Recovery**, que minimiza el tiempo de inactividad y la pérdida de datos, ya que proporciona una recuperación rápida y fiable para servidores físicos, virtuales y basados en la nube en AWS.

Para obtener más información, visite
aws.amazon.com/cloudendure-disaster-recovery/

Seguridad “en” la nube



Aunque AWS se encarga de todo el trabajo pesado de la seguridad “de” la nube, usted, como cliente de AWS, sigue siendo responsable de la seguridad “en” la nube. Usted es responsable de administrar el sistema operativo invitado, lo que incluye la instalación de actualizaciones y parches de seguridad. También es responsable de administrar el software de aplicaciones asociado, así como de la configuración del firewall que haya elegido. Sus responsabilidades varían en función de los servicios de AWS que elija, de cómo los integre en su entorno de tecnología y de las leyes y normativas correspondientes.

Para administrar sus recursos de AWS de forma segura, debe hacer estas cuatro cosas:

1. Automatice la administración del inventario y los recursos para saber lo que tiene; después, aplique la protección adecuada según convenga.

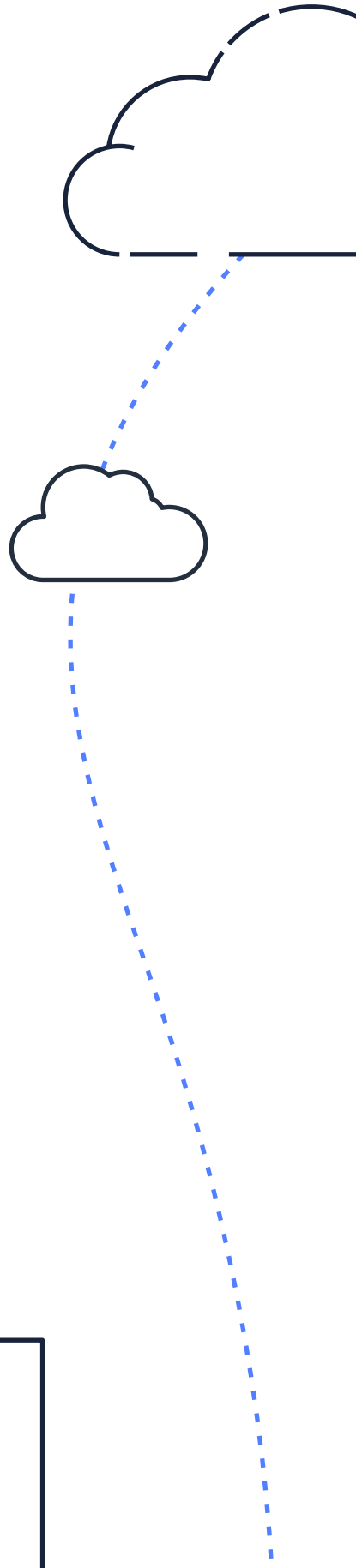
2. Configure de forma segura el SO invitado y las aplicaciones en sus recursos (ajustes de configuración seguros, implementación de parches y antimalware).

3. Controle los cambios que se realizan en los recursos (administración de cambios).

4. Cree y automatice sus planes de respuesta ante incidentes y recuperación de desastres.

Identity and Access Management

Los servicios de identidad de AWS le permiten administrar identidades, recursos y permisos de forma segura y a escala. Con AWS, dispone de servicios de identidad para las aplicaciones orientadas al personal y los clientes, de modo que puede comenzar a trabajar rápidamente y administrar el acceso a las cargas de trabajo y las aplicaciones. Además, con servicios como **IAM Access Analyzer**, AWS también le da libertad para elegir dónde administrar las identidades y las credenciales de los empleados, así como los permisos detallados para otorgar el acceso correcto a las personas adecuadas en el momento apropiado. Servicios como **AWS Identity & Access Management (IAM)** le permiten administrar de forma segura el acceso a los servicios y recursos de AWS, mientras que **AWS Organizations** le brinda la capacidad de centralizar la gobernanza y la administración en todas las cuentas de AWS, y con **AWS Single Sign-On (SSO)** puede habilitar el servicio de inicio de sesión único en la nube.



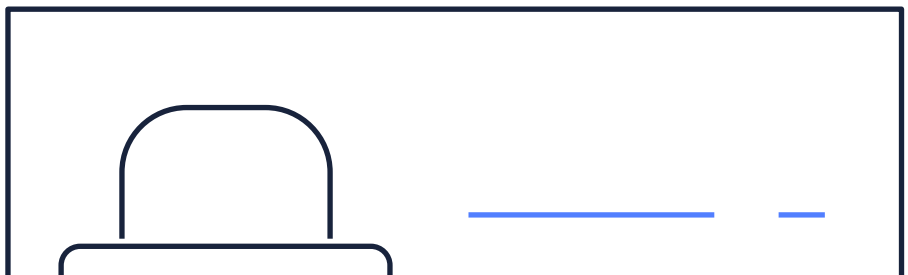
"Creemos que la gestión de la seguridad, la identidad y el acceso, realizada correctamente, puede permitir a nuestros ingenieros centrarse en los productos sintiéndose protegidos por unas paredes sólidas y fiables, y por eso utilizamos AWS IAM a modo de cimientos de una seguridad autoservicio y auditable".

- Rob Witoff
Director

coinbase

Servicios de seguridad e identidad de AWS

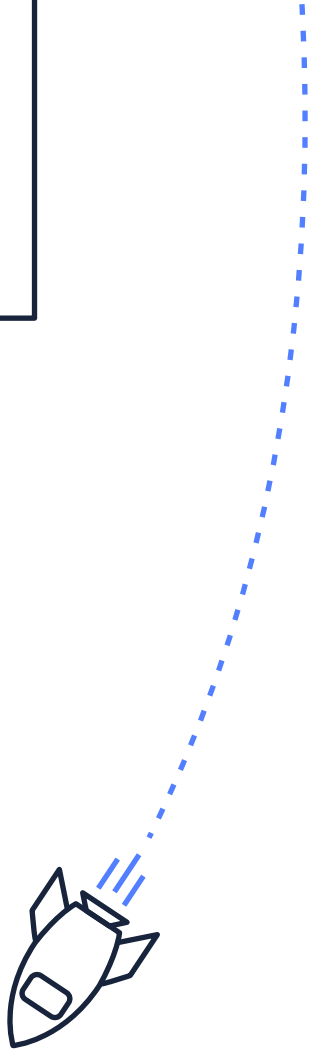
Para ayudarle a establecer la seguridad "en" la nube, AWS ofrece una amplia selección de servicios de seguridad innovadores que pueden ayudarle a simplificar el cumplimiento de sus propios requisitos normativos y de seguridad. Nuestros servicios y soluciones de seguridad se centran en ofrecer beneficios estratégicos clave en las siguientes áreas críticas con objeto de ayudarle a implementar la posición de seguridad óptima para su organización.



Protección de los datos

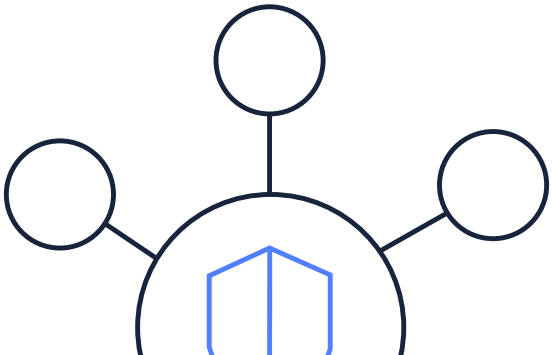
AWS proporciona servicios que le ayudan a proteger sus datos, cuentas y cargas de trabajo contra acceso no autorizado.

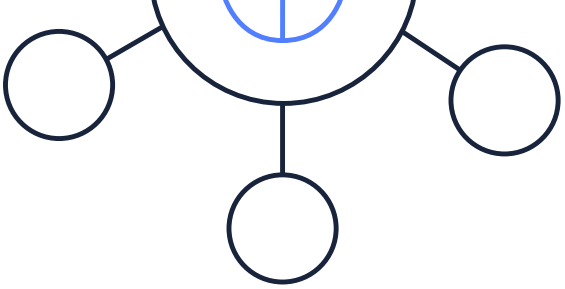
Los servicios de protección de datos de AWS ofrecen cifrado y administración de claves, así como un sistema de detección de amenazas que ayuda a monitorear y proteger continuamente sus cuentas y cargas de trabajo. Con nuestros servicios de protección de datos, puede descubrir y proteger su información confidencial a escala con **Amazon Macie**; crear y controlar fácilmente las claves utilizadas para cifrar o firmar digitalmente sus datos mediante **AWS Key Management Service (KMS)**; rotar, administrar y recuperar secretos con **AWS Secrets Manager**; generar y utilizar fácilmente sus propias claves de cifrado con **AWS CloudHSM**, y aprovisionar, administrar e implementar fácilmente certificados públicos y privados mediante **AWS Certificate Manager**.



Protección de bordes y redes

Los clientes pueden proteger sus aplicaciones web mediante servicios de AWS que filtran el tráfico en función de las reglas que creen. Por ejemplo, se pueden filtrar las solicitudes web por direcciones IP, encabezados HTTP, cuerpo HTTP o cadenas URI, lo que permite bloquear patrones de ataque habituales, como la inyección SQL o el filtro de scripts de sitios. Proteja sus aplicaciones web de vulnerabilidades más comunes mediante **AWS Web Application Firewall (WAF)**; administre la protección contra DDoS con **AWS Shield**; configure y administre de forma centralizada las reglas de firewall en sus cuentas y aplicaciones de AWS Organizations con **AWS Firewall Manager,** e implemente la seguridad de la red en sus VPC de Amazon con solo unos pocos clics mediante **AWS Network Firewall**.





Detección y administración de amenazas

AWS le ayuda a identificar las amenazas monitoreando de forma constante la actividad de la red y el comportamiento de las cuentas dentro de su entorno en la nube.
Con nuestros servicios, puede lograr la visibilidad que necesita para identificar problemas antes de que afecten al negocio, mejorar su posición de seguridad y reducir el perfil de riesgo de su entorno. Utilice **Amazon GuardDuty** como servicio de detección de amenazas administrado; **Amazon Detective** para analizar y visualizar datos de seguridad con el fin de localizar rápidamente la causa raíz de posibles problemas de seguridad; **Amazon Inspector** para automatizar las evaluaciones de seguridad y contribuir a mejorar la seguridad y la conformidad de las aplicaciones implementadas en AWS, y use **AWS Security Hub** como centro de seguridad y conformidad unificado donde ver y administrar de forma centralizada las alertas de seguridad y automatizar las comprobaciones de seguridad.

Para obtener más información sobre los servicios de seguridad e identidad de AWS, visite: *aws.amazon.com/products/security*

Conformidad y privacidad de datos, Amazon Security Hub, Systems Manager y CloudWatch

AWS le proporciona una vista completa de su estado de conformidad y monitorea de forma continua su entorno mediante comprobaciones de conformidad automatizadas que se basan en las prácticas recomendadas de AWS y los estándares del sector que aplique su organización. Puede utilizar **AWS Audit Manager** para auditar de forma continua el uso que hace de AWS y así simplificar la forma en que evalúa el riesgo y la conformidad; **AWS CloudTrail** para hacer un seguimiento de la actividad de los usuarios y del uso de las API; **AWS Config** para registrar y evaluar las configuraciones de los recursos de AWS, y **AWS Artifact** como portal autoservicio para el acceso a los reportes de conformidad de AWS. También puede utilizar el **estándar de prácticas recomendadas de seguridad fundamentales de AWS Security Hub** para detectar si las cuentas y los recursos implementados se desvían de las prácticas recomendadas de seguridad, así como los **paquetes de conformidad de Config** para evaluar la configuración de los recursos de AWS comparada con la configuración ideal.

Servicios de AWS dentro del alcance

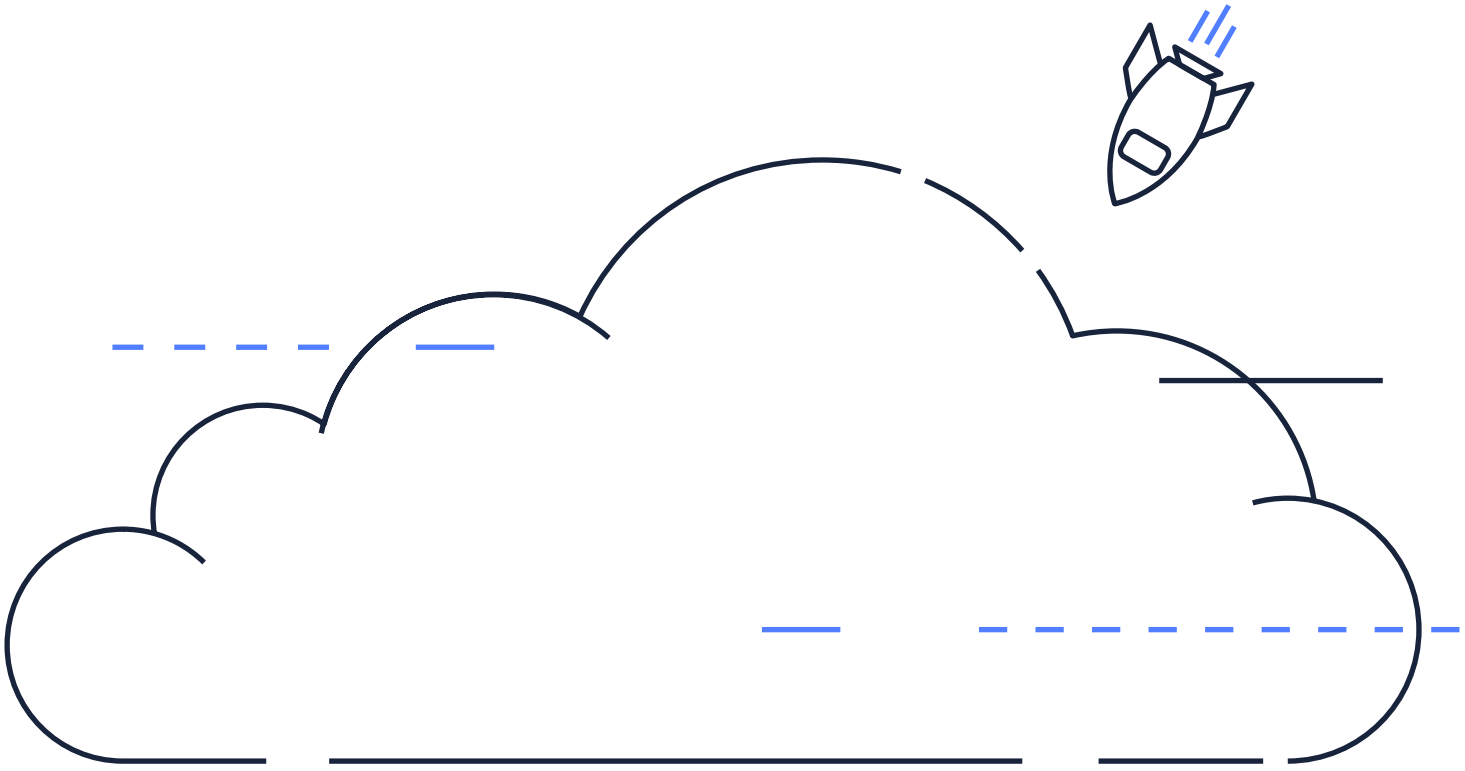
Incluimos servicios en el alcance de nuestros programas de conformidad en función del caso de uso esperado, de la retroalimentación y de la demanda. Según la naturaleza de lo que esté creando en AWS, debe determinar si el servicio procesará o almacenará datos de los clientes y cómo afectará o no a la conformidad de su entorno de datos de los clientes.

Visite nuestra página web Servicios dentro del alcance para obtener más información: *aws.amazon.com/compliance/services-in-scope*

Prácticas recomendadas de AWS para la seguridad “en” la nube

A la hora de crear su estrategia de migración hacia AWS, o si está revisando sus cargas de trabajo existentes en AWS, hay una serie de estándares y marcos aceptados en el sector que pueden ayudarle a construir unos cimientos de seguridad sólidos.

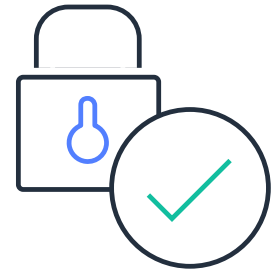
Marcos tales como CIS, ISO 27001 y el Marco de seguridad cibernética (CSF) del NIST ofrecen un enfoque estructurado para crear sus sistemas de gobernanza de tecnología y administración de la seguridad, y AWS Security Hub proporciona comprobaciones de seguridad automatizadas con respecto a estos estándares. AWS también proporciona su propia orientación mediante prácticas recomendadas a través del Marco de adopción de la nube de AWS, AWS Well-Architected y el estándar de prácticas recomendadas de seguridad fundamentales de AWS.



Migración a AWS: el Marco de adopción de la nube de AWS

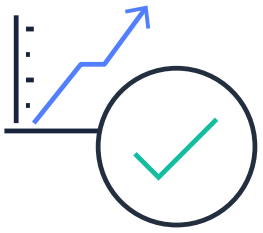
Los Servicios profesionales de AWS crearon el Marco de adopción de la nube (CAF) basándose en miles de migraciones de clientes para ayudar a las organizaciones a planificar una migración a la nube eficaz y segura. Dado que el camino de cada organización será diferente, es importante planificar con antelación y conectar los objetivos empresariales y los resultados deseados con las tecnologías y los procesos correctos. El CAF se centra en seis perspectivas utilizadas para la planificación y en consideraciones estratégicas basadas en principios comunes que se pueden aplicar a la mayoría de las organizaciones. Tres de las perspectivas —Negocio, Personas y Gobernanza— se centran en las capacidades empresariales, mientras que los aspectos técnicos se abordan en las perspectivas Plataforma, Seguridad y Operaciones. En conjunto, las seis perspectivas permiten que el equipo directivo de la organización planifique y dirija su transición a la nube identificando a las partes interesadas adecuadas y descubriendo brechas en las capacidades y los procesos existentes.

La perspectiva de Seguridad del CAF captura la experiencia de AWS trabajando con clientes empresariales en su proceso de adopción de la nube. Detalla cómo estructurar un enfoque basado en el riesgo para la identificación y la selección de controles (por ejemplo, elaborando una cartografía de seguridad), cómo crear un programa de seguridad que permita la maduración a través de la iteración y cómo aconseja AWS a los clientes configurar su modelo de seguridad en la nube de AWS.



Capacidades de la perspectiva Seguridad:

- Identity and Access Management (IAM) ayuda a los clientes a integrar AWS en su ciclo de vida de administración de identidad y sus fuentes de autenticación y autorización.
- El control de detección ofrece orientación para ayudar a identificar incidentes de seguridad potenciales dentro del entorno de AWS.
- La seguridad de la infraestructura ayuda a los clientes a implementar las metodologías de control que puedan ser necesarias para respetar las prácticas recomendadas y cumplir las obligaciones normativas o exigidas por el sector.
- La protección de los datos ayuda a los clientes a implementar garantías adecuadas que protejan los datos en tránsito y en reposo.
- La respuesta ante incidentes ayuda a los clientes a definir y ejecutar una respuesta a los incidentes de seguridad.



Documentación adicional:
Marco de adopción de la nube de AWS: *aws.amazon.com/professional-services/CAF/*

Prácticas recomendadas para cargas de trabajo seguras y resilientes: AWS Well-Architected

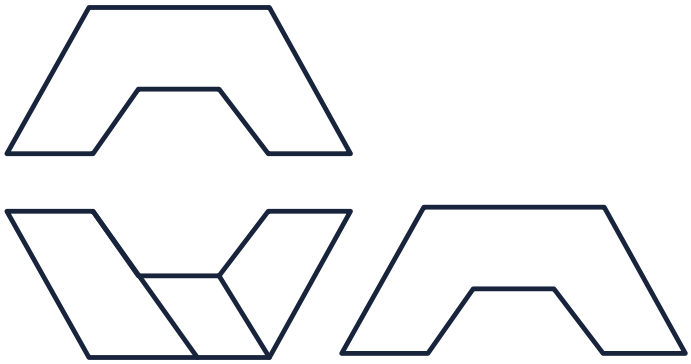
AWS Well-Architected es un conjunto de prácticas recomendadas y una herramienta disponible en la consola de administración de AWS que le ayuda a responder a una pregunta: "¿Está bien diseñada mi arquitectura?" Well-Architected se centra en el nivel de la carga de trabajo —su infraestructura, sistemas, datos y procesos— mediante el examen de cinco pilares principales:

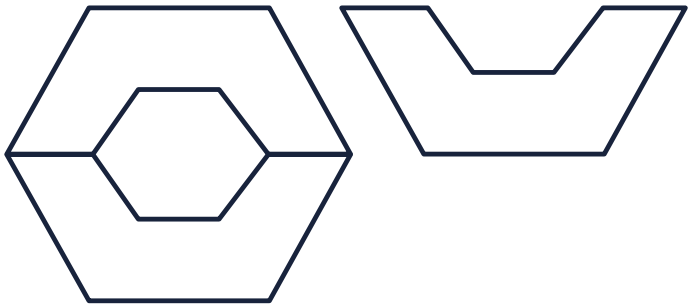
- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficiencia del rendimiento
- Optimización de costos

El pilar Seguridad tiene cinco componentes:

- Identity and Access Management
- Detección
- Protección de la infraestructura
- Protección de los datos
- Respuesta ante incidentes

Well-Architected proporciona orientación para una implementación segura, así como enfoques para seleccionar los servicios de AWS adecuados para garantizar que estas prácticas de seguridad básicas se aplican en las cargas de trabajo. Quizá haya notado que estos componentes son parecidos a los de la perspectiva de Seguridad del CAF. Ello se debe a que las brechas de capacidad que se detecten en el plano estratégico deben abordarse en el plano técnico.
Esa trazabilidad desde el requisito empresarial hasta la arquitectura técnica y las operaciones es un elemento crucial para garantizar que la seguridad se aplica en todos los niveles de la organización y que satisface una necesidad empresarial.





AWS Well-Architected Tool (AWS WA Tool) es un servicio disponible a través de la consola de administración de AWS que proporciona un proceso sistemático para medir la arquitectura aplicando las prácticas recomendadas de AWS. AWS WA Tool le acompaña a lo largo del ciclo de vida del producto, ya que:

- Le ayuda a documentar las decisiones que toma

- Proporciona recomendaciones para mejorar la carga de trabajo basándose en prácticas recomendadas

- Le orienta para que consiga que las cargas de trabajo sean más fiables, seguras, eficientes y rentables

En la actualidad, puede utilizar la AWS WA Tool para documentar y medir su carga de trabajo aplicando las prácticas recomendadas el marco AWS Well-Architected Framework. Estas prácticas recomendadas las desarrollaron arquitectos de soluciones de AWS basándose en sus años de experiencia creando soluciones para una amplia variedad de negocios. Este marco proporciona un enfoque sistemático para medir arquitecturas y ofrece orientación para implementar diseños que se adapten a sus necesidades a lo largo del tiempo.

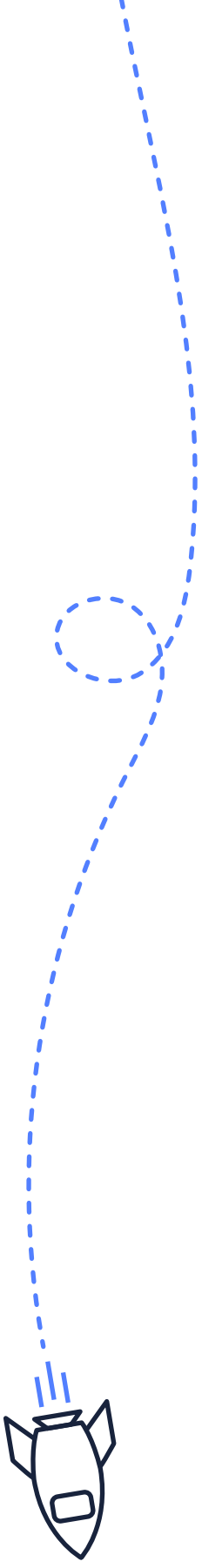
Documentación adicional:

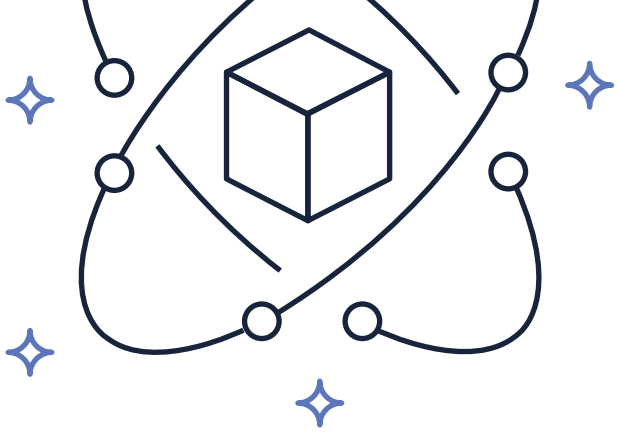
Información general sobre el marco AWS Well-Architected Framework:
aws.amazon.com/architecture/well-architected/

Pilar Seguridad del marco Well-Architected Framework:
d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

AWS Well-Architected Tool:
aws.amazon.com/well-architected-tool/

Introducción a Well-Architected Tool:
docs.aws.amazon.com/wellarchitected/latest/userguide/getting-started.html





Comprobaciones automatizadas de las prácticas recomendadas de seguridad de AWS: estándar de prácticas recomendadas de seguridad fundamentales de AWS Security Hub

El estándar de prácticas recomendadas de seguridad fundamentales de AWS es un conjunto de controles que detectan si las cuentas y los recursos implementados se desvían de las prácticas recomendadas de seguridad. Este estándar le permite evaluar de forma continua todas sus cuentas y cargas de trabajo de AWS para identificar rápidamente las áreas que se desvían de las prácticas recomendadas. Con él conseguirá una orientación práctica y prescriptiva sobre cómo mejorar y mantener la posición de seguridad de su organización.

Documentación adicional:

Estándar de prácticas recomendadas de seguridad fundamentales de AWS:
docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html

"Cuando trabajas en telemedicina y estás en contacto con datos clínicos protegidos, la seguridad es primordial. AWS es absolutamente fundamental para lo que hacemos en la actualidad. La seguridad y la conformidad son cuestiones ineludibles. Si te faltan, lo demás importa poco".

- Cory Costley
Director de productos

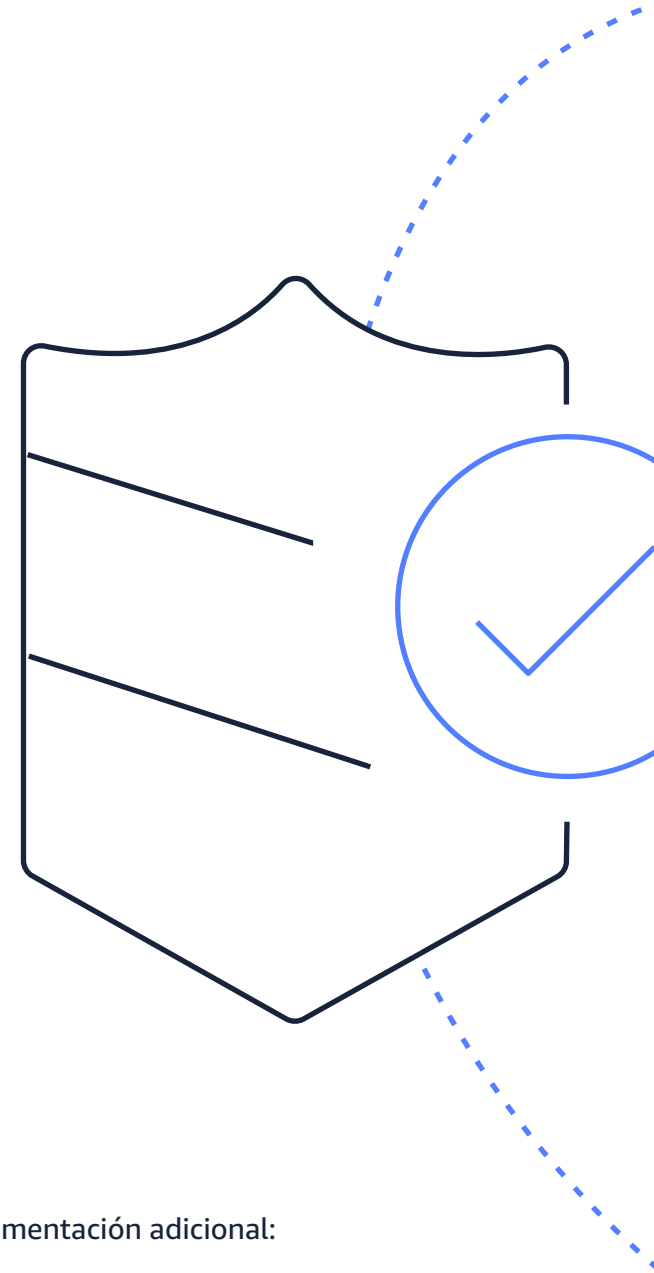
Avizia

Lea más testimonios de clientes en nuestro sitio web:
aws.amazon.com/compliance/testimonials/

Orientación sobre seguridad cibernética independiente del proveedor: Marco de seguridad cibernética del NIST

Según cuáles sean las necesidades de su negocio, las obligaciones de conformidad normativa y los requisitos tecnológicos, es probable que su estrategia de seguridad cambie a medida que realice la transición a un modelo de responsabilidad de seguridad compartida. Es recomendable que adapte su programa de seguridad a un marco del sector, como el Marco para la mejora de la seguridad cibernética (CSF) del NIST, para garantizar que haya tenido en cuenta la seguridad en todos los aspectos de su negocio. Esto también le permitirá evaluar las tecnologías nuevas y emergentes basándose en objetivos de seguridad imparciales y no como una comparación con las soluciones existentes, con las que las personas tienen vínculos emocionales (positivos o negativos). Lo ideal es que su organización ya esté utilizando un marco para su programa de seguridad organizativa; si no es así, puede considerar el CSF.

Pero, ¿por qué el CSF, si hay otros estándares conocidos, como el sistema de gestión de la seguridad de la información ISO 27001:2013 o COBIT? Aunque puede adoptar cualquier marco, el CSF proporciona un método gratuito, sencillo y efectivo para comprender y comunicar el riesgo en lo relevante a seguridad cibernética en toda su organización. Su enfoque tecnológico e independiente del sector permite una taxonomía común que se puede utilizar en toda la organización, desde el nivel del consejo de dirección hasta los equipos de DevSecOps. Incluso si decide no adoptar la metodología CSF en su totalidad, las cinco funciones principales (identificar, proteger, detectar, responder y recuperar) se pueden comprender fácilmente y ponerse en relación con otros estándares o requisitos de control según lo que necesite su negocio. El CSF se ha adoptado internacionalmente y en todos los sectores.



Documentación adicional:

Optimización de la gobernanza de la nube en AWS: integración del Marco de seguridad cibernética del NIST, del Marco de adopción de la nube de AWS y de AWS Well-Architected:
aws.amazon.com/blogs/security/optimizing-cloud-governance-on-aws-integrating-the-nist-cybersecurity-framework-aws-cloud-adoption-framework-and-aws-well-architected/

Adaptación al CSF del NIST en la nube de AWS:
d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

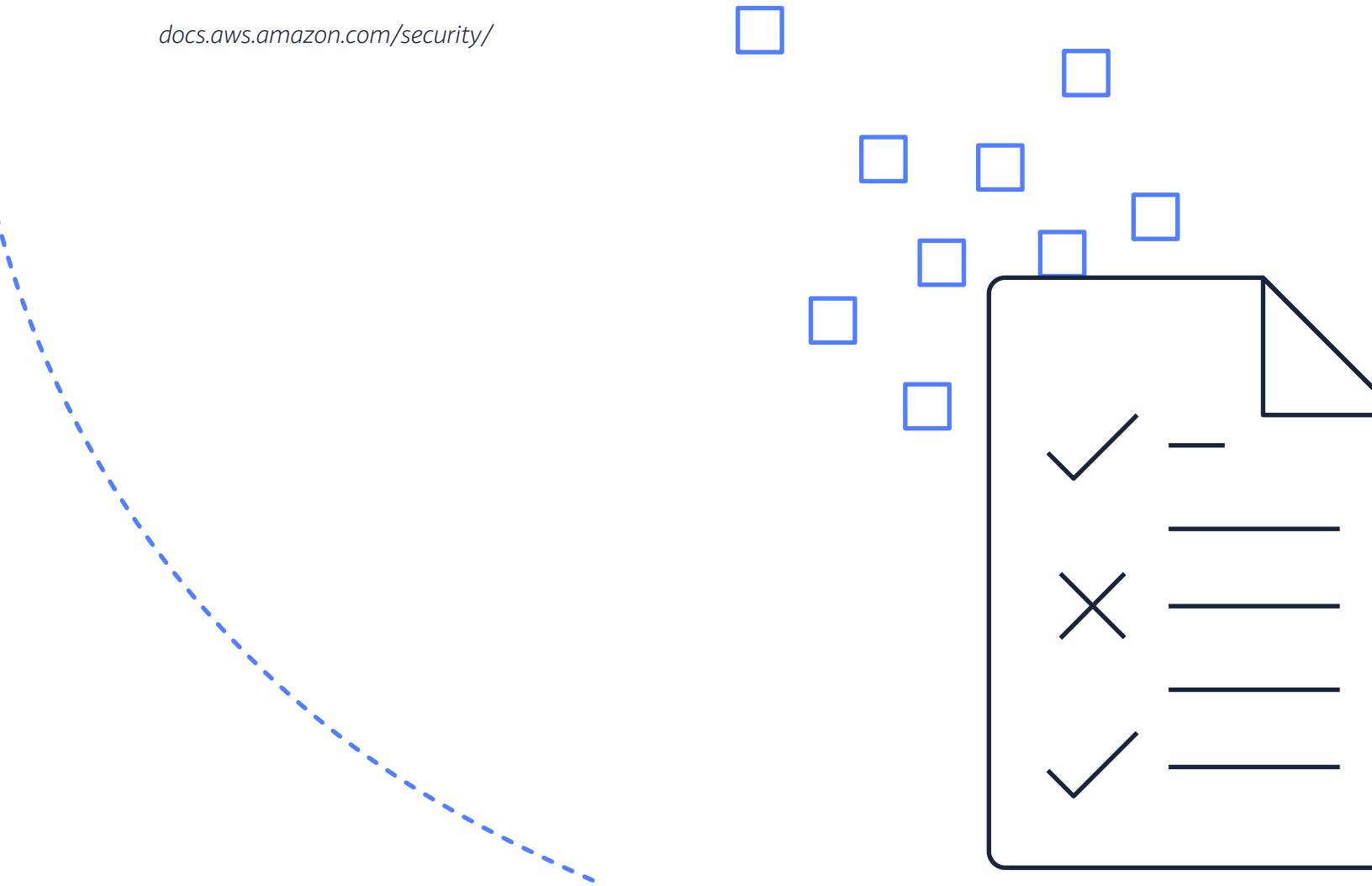
Encajar todas las piezas

No existe un enfoque único para la seguridad de su organización, ni tampoco se limita únicamente a los aspectos técnicos. Evaluando sus requisitos y su contexto empresarial, comprendiendo sus brechas y riesgos en cuanto seguridad cibernética y aplicando prácticas probadas y auténticas para lograr una arquitectura segura, puede tener garantías de que la seguridad está presente en todas sus prácticas organizativas, desde la gobernanza hasta las operaciones.

Orientación de seguridad específica para cada servicio

Todos los servicios de AWS disponen de orientación de seguridad en el sitio web de documentación de AWS. Esta documentación le muestra cómo configurar los servicios de AWS para ayudarle a cumplir sus objetivos de seguridad y conformidad.

docs.aws.amazon.com/security/



Socios y Marketplace

Uno de los beneficios que obtiene como cliente de AWS es el acceso a una amplia red de soluciones y socios de seguridad con la que es posible que ya puede esté familiarizado, y que funcionan a la perfección con los servicios de seguridad y conformidad propios de AWS.

Las soluciones de la Red de Socios de AWS (APN) permiten la automatización y la agilidad, y escalan con sus cargas de trabajo. Además, solo pagará por lo que necesite y use. Amplíe los beneficios de AWS utilizando la tecnología y los servicios de consultoría de socios competentes en seguridad que ya conoce y en los que confía. Desde la migración inicial hasta las operaciones diarias, los socios de AWS aprovechan su vasta experiencia para ayudar a los clientes a proteger cada una de las etapas de su proceso de adopción de la nube.

Elija en nuestra lista global de socios de tecnología y consultoría de AWS entre aquellos que son competentes en seguridad de AWS, muchos de los cuales están especializados en ofrecer soluciones y servicios centrados en la seguridad para sus cargas de trabajo y casos de uso específicos. Benefíciese de una mayor agilidad, automatización y escalado de las cargas de trabajo con las soluciones de los socios de AWS, y recurra a AWS Marketplace para localizar, comprar, implementar y administrar soluciones de nube de los socios de forma fácil y rápida, incluidos productos de software como servicio (SaaS).

Para obtener más información, visite: *aws.amazon.com/security/partner-solutions* y *aws.amazon.com/marketplace/solutions/security*

Recursos adicionales

Blog de seguridad y redes sociales de AWS

Manténgase al día con actualizaciones de servicios, lanzamientos y soluciones innovadoras relacionadas con las seguridad de AWS siguiendo el blog de seguridad de AWS, disponible en aws.amazon.com/blogs/security.

Síganos en Twitter:
twitter.com/awssecurityinfo y
twitter.com/awsidentity

Capacitación y certificación de AWS

Independientemente de que esté empezando, desarrollando habilidades de tecnología existentes o perfeccionando su conocimiento de la nube, la formación de AWS puede ayudarles a usted y a su equipo a profundizar en sus conocimientos para hacer un uso más eficiente de la nube. Visite www.aws.training.

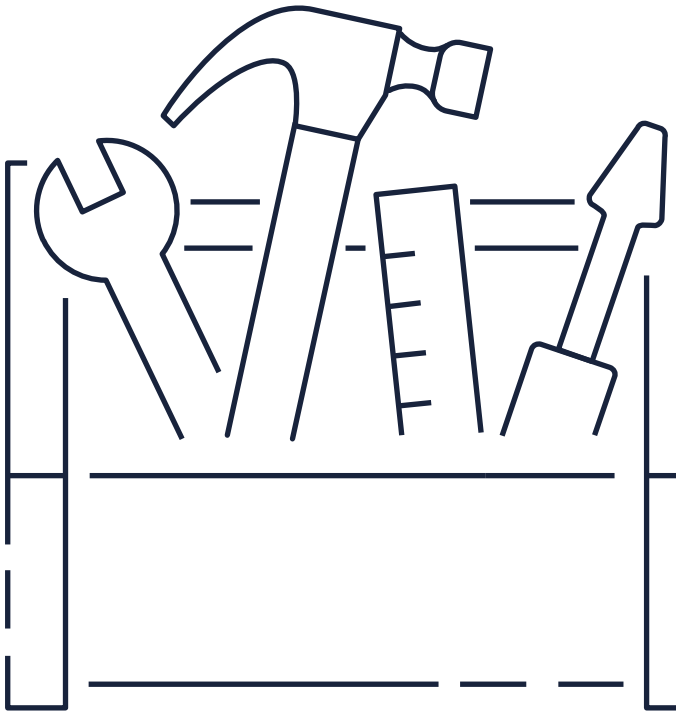
La certificación AWS Certified Security – Specialty está destinada a personas que desempeñan un rol de seguridad con al menos dos años de experiencia práctica en la protección de cargas de trabajo de AWS.

Visite:
aws.amazon.com/certification/certified-security-specialty

Centro de arquitectura de seguridad, identidad y conformidad

Aprenda cómo lograr sus objetivos de seguridad y conformidad mediante la infraestructura y los servicios de AWS con documentación, blogs, vídeos, y otros recursos.

Visite:
aws.amazon.com/architecture/security-identity-compliance



Academia de auditoría de nube de AWS

La academia de auditoría de nube (CAA) está diseñada para quienes desempeñan roles de auditoría, riesgos y conformidad y participan en la evaluación de las cargas de trabajo reguladas en la nube. El plan de estudios de la CAA traza una ruta de aprendizaje escalonada que comienza con un ámbito amplio (independiente de la nube y del sector) y se va estrechando a medida que el alumno avanza para centrarse en AWS y en contenido específico del sector.

Visite: *aws.amazon.com/compliance/auditor-learning-path*

AWS Security Fundamentals

Se trata de un curso gratuito a su ritmo para aprender conceptos básicos de seguridad de la nube de AWS, como el control de acceso de AWS, los métodos de cifrado de datos y cómo se puede proteger el acceso de red a su infraestructura de AWS. Se aborda la responsabilidad del cliente en cuanto a seguridad en la nube de AWS, así como los diferentes servicios disponibles orientados a la seguridad.

Visite:
aws.amazon.com/training/course-descriptions/security-fundamentals

Servicios profesionales de AWS

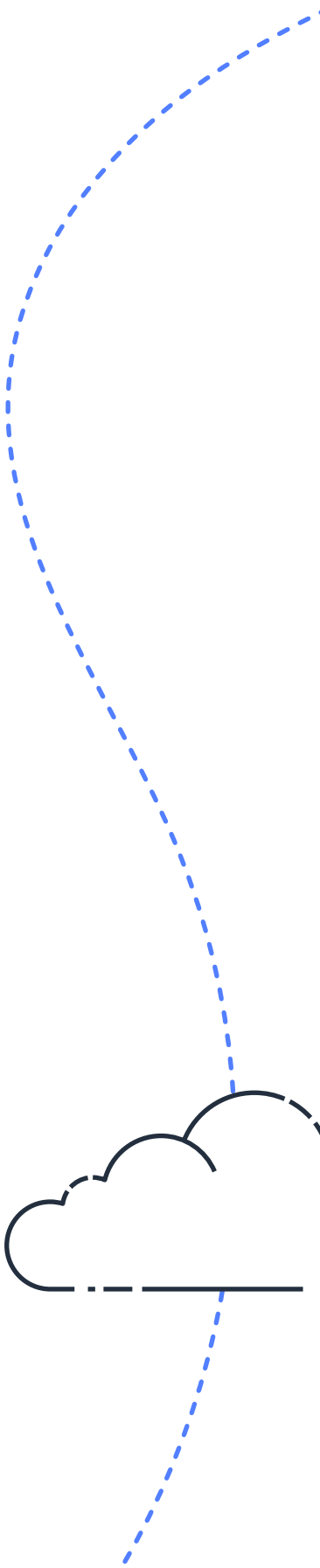
La organización de Servicios profesionales de AWS es un equipo global de expertos que pueden ayudarle a aprovechar la nube de AWS para conseguir los resultados empresariales que desea. Este equipo ofrece orientación focalizada mediante nuestras prácticas de especialidad globales, que cubren diversas soluciones, tecnologías y sectores. Existen diversas ofertas centradas en la seguridad que están disponibles para ayudar a los clientes en sus procesos de migración a la nube, así como a proteger sus cuentas y cargas de trabajo existentes de acuerdo con las prácticas recomendadas de AWS y del sector.

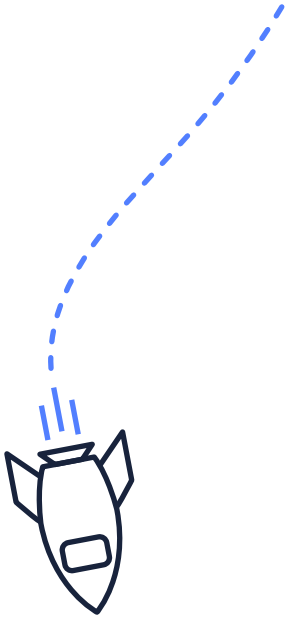
Visite: *aws.amazon.com/professional-services/*

Tutoriales prácticos de seguridad de AWS Well-Architected

Los tutoriales de seguridad son documentación y código en formato práctico para ayudarle a aprender, medir y crear utilizando las prácticas recomendadas para arquitectura. Estos tutoriales están clasificados por niveles: 100 es introductorio, 200/300 es intermedio y 400 es avanzado.

Visite: *wellarchitectedlabs.com/security*





Gracias por tomarse la molestia de revisar la Guía de referencia rápida sobre seguridad y conformidad de AWS.

Dispone de información adicional en el sitio web de seguridad y conformidad de AWS, *aws.amazon.com/security/*

y tiene información sobre nuestros servicios de seguridad en: *aws.amazon.com/products/security/*