Introducción a la seguridad de AWS

Enero de 2020

Avisos

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

Contenido

Seguridad de la infraestructura de AWS 1

Características y productos relacionados con la seguridad 2

- Seguridad de la infraestructura 2
- Administración de la configuración y el inventario 2
- Cifrado de datos 3
- Control de accesos e identidades 3
- Supervisión y registro 4
- Productos de seguridad en AWS Marketplace 5

Recomendaciones de seguridad 5

Conformidad 7

Otra documentación 8

Revisiones del documento 8

Resumen

Amazon Web Services (AWS) conforma una plataforma de informática en la nube que, además de ser escalable, ofrece un elevado nivel de disponibilidad y de fiabilidad, así como herramientas que permiten ejecutar una gran variedad de aplicaciones. Para AWS, es de suma importancia ayudar a proteger la confidencialidad, integridad y disponibilidad de los sistemas y los datos de los clientes, además de mantener la seguridad y la confianza. La finalidad de este documento es ofrecer una introducción al enfoque de AWS en relación con la seguridad, incluidos los controles del entorno y algunos de los productos y características que AWS pone a disposición de los clientes para que puedan cumplir sus objetivos de seguridad.

Seguridad de la infraestructura de AWS

La infraestructura de AWS se ha diseñado para hacer de este entorno de informática en la nube uno de los más flexibles y seguros que existen en la actualidad. Está ideada para ofrecer una plataforma con un alto nivel de escalabilidad y confianza que permita a los clientes implementar aplicaciones y datos de forma rápida y segura.

En el diseño y la administración de esta infraestructura, no solo se han seguido las prácticas recomendadas y los estándares de seguridad, sino que se han tenido en cuenta las necesidades únicas de la nube. Para garantizar que la infraestructura subyacente esté supervisada y protegida las 24 horas, AWS utiliza controles redundantes organizados en niveles, validaciones y pruebas continuas, y un alto nivel de automatización. AWS garantiza que estos controles se replican en cada nuevo centro de datos o servicio.

Todos los clientes de AWS se benefician de una arquitectura de red y de centro de datos diseñada para satisfacer los requisitos de seguridad más exigentes. Esto se traduce en que usted obtiene una infraestructura resiliente, diseñada para ofrecer un elevado nivel de seguridad, sin los gastos ni la fuerte carga operativa de un centro de datos tradicional.

AWS se rige por un modelo de seguridad de responsabilidad compartida, en el que AWS es responsable de la seguridad de la infraestructura en la nube subyacente, mientras que usted es responsable de las cargas de trabajo que implementa en AWS (*Figura 1*). Esto le ofrece la flexibilidad y agilidad necesarias para implementar los controles de seguridad más apropiados de acuerdo con las funciones de su organización en el entorno de AWS. Puede imponer estrictos controles para acceder a los entornos donde se procesa información confidencial o aplicar controles menos exigentes en la información que desea hacer pública.

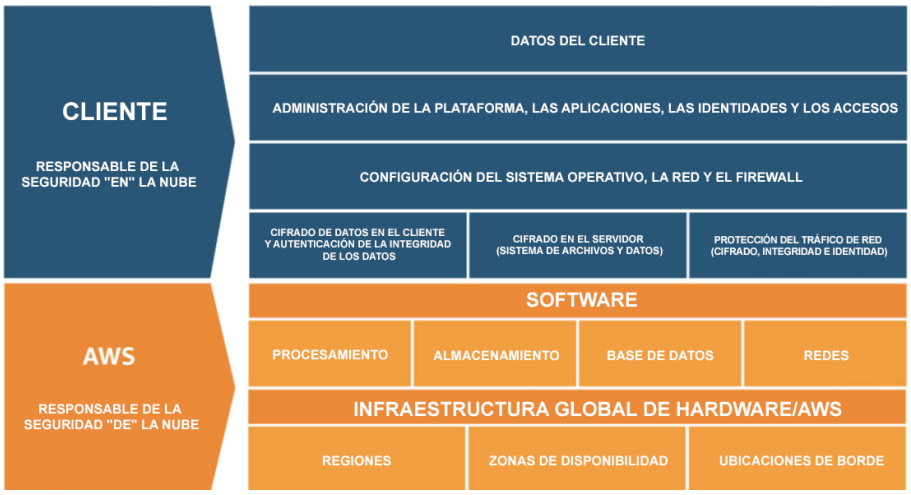

Figura 1: Modelo de seguridad de responsabilidad compartida de AWS

Características y productos relacionados con la seguridad

AWS y sus socios le ofrecen una variada cartera de herramientas y características que le ayudarán a satisfacer sus objetivos de seguridad. Estas herramientas son un reflejo exacto de los controles que ya conoce e implementa en los entornos locales. AWS dispone de herramientas y características específicas para la seguridad de la red, la administración de la configuración, el control del acceso y el cifrado de datos. Asimismo, cuenta con herramientas de supervisión y registro que le proporcionarán toda la información de lo que ocurre en su entorno.

Seguridad de la infraestructura

AWS cuenta con varias funcionalidades y servicios de seguridad que le permitirán mejorar la privacidad y controlar el acceso a la red. Algunos de ellos son:

- Los firewalls de red integrados en la VPC de Amazon, que le permiten crear redes privadas y supervisar el acceso a las instancias o aplicaciones. Los clientes pueden controlar el cifrado en tránsito entre los distintos servicios de AWS con TLS.
- Opciones de conectividad que permiten realizar conexiones privadas (o dedicadas) desde las oficinas o el entorno local.
- Tecnologías de mitigación de ataques DDoS, que se aplican en el nivel 3 o 4, así como en el nivel 7. Estas tecnologías pueden aplicarse como parte de las estrategias de entrega de aplicaciones y contenido.
- Cifrado automático de todo el tráfico que circula por las redes globales y regionales de AWS entre las instalaciones protegidas por AWS.

Administración de la configuración y el inventario

AWS le ofrece una gran variedad de herramientas que le permitirán moverse rápidamente con la garantía de que sus recursos en la nube se ajustan a las prácticas recomendadas y los estándares de la organización. Algunos de ellos son:

- Herramientas de implementación, que le permiten administrar la creación y retirada de los recursos de AWS conforme a los estándares de la organización.

- Herramientas de gestión del inventario y la configuración, que le permiten identificar los recursos de AWS para controlarlos y administrar los cambios que se producen en ellos con el transcurso del tiempo.
- Herramientas de definición y administración de plantillas, con las que puede crear máquinas virtuales estándar, preconfiguradas y reforzadas para las instancias EC2.

Cifrado de datos

AWS le brinda la posibilidad de añadir un nivel de seguridad adicional a los datos en reposo que almacena en la nube y pone a su disposición características de cifrado escalables y eficaces. Algunas de ellas son:

- Funcionalidades de cifrado de datos en reposo, disponibles en la mayoría de los servicios de AWS, como Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda y Amazon SageMaker
- Opciones flexibles para la gestión de claves, como AWS Key Management Service, que le permite elegir si las claves de cifrado las va a administrar AWS o si prefiere mantener todo el control sobre sus propias claves
- Almacenamiento de claves criptográficas basado en hardware dedicado a través de AWS CloudHSM, lo que le permite cumplir los requisitos de seguridad
- Colas de mensajes cifrados para transmitir información confidencial utilizando el cifrado del lado del servidor (SSE) de Amazon SQS

Además, AWS cuenta con varias API que le permiten integrar el cifrado y la protección de datos en cualquiera de los servicios que desarrolle o implemente en un entorno de AWS.

Control de accesos e identidades

En AWS, encontrará funcionalidades que le permitirán definir, aplicar y gestionar políticas de acceso entre los diferentes servicios de AWS. Algunas de ellas son:

- AWS Identity and Access Management (IAM), que le permite definir cuentas de usuario individuales con permisos para los diferentes recursos de AWS y AWS Multi-Factor Authentication para las cuentas con privilegios, incluidos algunos sistemas de autenticación basados en software y hardware. IAM se puede utilizar para conceder a los empleados y las aplicaciones acceso federado a la consola de administración y a las API de servicio de AWS a través de los sistemas de identidades existentes, como Microsoft Active Directory o servicios de otros socios.

- AWS Directory Service, que permite integrar directorios corporativos y federarse con ellos para reducir la sobrecarga administrativa y mejorar la experiencia del usuario final.
- AWS Single Sign-On (AWS SSO), que le permite administrar de forma centralizada el inicio de sesión único de los usuarios y los permisos de acceso a todas las cuentas de AWS Organizations.

AWS permite integrar la administración de los accesos y las identidades de forma nativa en muchos de sus servicios. También permite integrar las API con cualquiera de sus aplicaciones y servicios propios.

Supervisión y registro

AWS le ofrece herramientas y características con las que puede ver todo lo que ocurre en el entorno de AWS. Algunas de ellas son:

- AWS CloudTrail es un servicio con el que puede supervisar las implementaciones de AWS en la nube a través del historial de las llamadas a las API de AWS registradas en su cuenta, como las llamadas a las API realizadas con la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y los servicios de AWS de mayor nivel. También puede identificar a los usuarios y las cuentas que llamaron a las API de AWS de los servicios compatibles con CloudTrail, la dirección IP desde la que efectuaron las llamadas y cuándo las realizaron.
- Amazon CloudWatch es una solución de supervisión escalable y flexible de total confianza que puede empezar a usar en cuestión de minutos. Ya no necesita configurar, administrar y escalar sus propios sistemas de supervisión ni su propia infraestructura.
- Amazon GuardDuty es un servicio de detección de amenazas que supervisa sin descanso cualquier actividad malintencionada o comportamiento no autorizado para proteger sus cargas de trabajo y sus cuentas de AWS. Amazon GuardDuty envía notificaciones a través de Amazon CloudWatch para que pueda desencadenar una respuesta automatizada o avisar a alguna persona.

Estas herramientas y características le proporcionan información para identificar los problemas antes de que afecten a la actividad y le permiten tanto mejorar su nivel de seguridad como reducir el perfil de riesgo de su entorno.

Productos de seguridad en AWS Marketplace

Al migrar las cargas de trabajo de producción a AWS, las organizaciones pueden mejorar la agilidad, la escalabilidad, la innovación y el ahorro de costes, al tiempo que mantienen la seguridad del entorno. En AWS Marketplace, encontrará destacados productos de seguridad que son equivalentes o idénticos a los controles que ya utiliza en sus entornos en las instalaciones o que pueden integrarse con ellos. Estos productos complementan a los servicios de AWS y le permiten implementar una completa arquitectura de seguridad, así como disfrutar de una experiencia más coherente tanto en la nube como en los entornos locales.

Recomendaciones de seguridad

AWS ofrece orientación y pone su experiencia a disposición de los clientes a través de las herramientas en línea, los recursos, el equipo de soporte técnico y los servicios profesionales que proporciona junto con sus socios.

AWS Trusted Advisor es una herramienta en línea que funciona como un experto en la nube y que puede personalizarse para que le ayude a configurar los recursos conforme a las prácticas recomendadas. Trusted Advisor inspecciona su entorno de AWS para acabar con las deficiencias de seguridad y busca oportunidades para ahorrar dinero, mejorar el rendimiento del sistema y aumentar la fiabilidad.

Los **equipos de cuentas de AWS** constituyen un primer punto de contacto. Además de guiarle por la implementación, le indicarán los recursos de seguridad a los que puede recurrir para solucionar los problemas de seguridad que pudiera encontrar.

El **servicio de soporte de AWS para empresas** ofrece un tiempo de respuesta de 15 minutos, está disponible las 24 horas del día a través del teléfono, el chat o el correo electrónico, y pone a su disposición un director técnico de cuenta dedicado. Este servicio de asistencia garantiza que los problemas de los clientes se resuelven con la mayor rapidez posible.

La **red de socios de AWS** le ofrece cientos de productos destacados que son equivalentes o idénticos a los controles que ya utiliza en sus entornos locales o que pueden integrarse con ellos. Estos productos complementan a los servicios de AWS y le permiten implementar una completa arquitectura de seguridad, así como disfrutar de una experiencia más coherente tanto en la nube como en los entornos locales. Además, pone a su disposición miles de socios de consultoría de AWS de todo el mundo que darán respuesta a sus necesidades de seguridad y conformidad.

AWS Professional Services está especializado, entre otras cosas, en seguridad, riesgo y conformidad, lo que le ayudará a generar confianza y a desarrollar funcionalidades técnicas cuando migre las cargas de trabajo más sensibles a la nube de AWS. AWS Professional Services ayuda a los clientes a elaborar políticas y prácticas de seguridad basadas en diseños de eficacia probada y a garantizar que el diseño de seguridad de los clientes se ajusta a los requisitos de conformidad internos y externos.

AWS Marketplace es un catálogo digital con miles de productos de software de proveedores independientes en el que resulta muy fácil buscar, probar, comprar e implementar el software que se ejecuta en AWS. Los productos de seguridad de AWS Marketplace complementan a los servicios de AWS que ya tiene y le permiten implementar una completa arquitectura de seguridad, así como disfrutar de una experiencia más coherente tanto en la nube como en los entornos locales.

AWS Security Bulletins envía boletines de seguridad sobre las vulnerabilidades y amenazas actuales, y permite que los clientes colaboren con expertos en seguridad de AWS para abordar los problemas, como la notificación de abusos, vulnerabilidades y pruebas de intrusión. También disponemos de recursos en línea para informar de las vulnerabilidades.

En la **documentación sobre seguridad de AWS**, se explica cómo deben configurarse los servicios de AWS para satisfacer los objetivos de seguridad y conformidad. Los clientes de AWS tienen a su disposición una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

AWS Well-Architected Framework ayuda a los arquitectos de la nube a crear una infraestructura segura, eficiente y de alto rendimiento para sus aplicaciones. AWS Well-Architected Framework incluye un pilar de seguridad que se centra en la protección de la información y los sistemas. Algunos de los temas principales son la confidencialidad e integridad de los datos, la administración de privilegios para identificar y controlar quién puede hacer qué, la protección de los sistemas y el establecimiento de controles para detectar eventos de seguridad. Los clientes pueden utilizar el servicio Well-Architected desde la consola o contratar los servicios de uno de los socios de APN para que les ayude.

AWS Well-Architected Tool le ayuda a revisar el estado de las cargas de trabajo y a compararlas con las últimas prácticas recomendadas para la arquitectura de AWS. Esta herramienta gratuita está disponible en la consola de administración de AWS. En primer lugar, se muestra un conjunto de preguntas relacionadas con la excelencia operativa, la seguridad, la fiabilidad, la eficiencia del rendimiento y la optimización de costes. Luego, AWS Well-Architected Tool le proporcionará un plan para diseñar los recursos de la nube siguiendo las prácticas recomendadas establecidas.

Conformidad

AWS Compliance proporciona a los clientes los recursos necesarios para conocer los férreos controles que se aplican en AWS para mantener la seguridad y la protección de los datos en la nube de AWS. Cuando se diseñan sistemas en la nube de AWS, las responsabilidades de conformidad recaen conjuntamente en AWS y los clientes. Los entornos informáticos de AWS se auditan constantemente con certificaciones de entidades de acreditación de diferentes zonas geográficas y diferentes segmentos verticales, como SOC 1/SSAE 16/ISAE 3402 (anteriormente, SAS 70), SOC 2, SOC 3, ISO 9001/ISO 27001, FedRAMP, DoD SRG y PCI DSS Level 1.i. Asimismo, AWS dispone de programas de control que ayudan a los clientes a determinar el grado de conformidad de los entornos que se ejecutan en AWS. Para ver una lista completa de estos programas, consulte los programas de conformidad de AWS.

Podemos afirmar que todos los servicios de AWS pueden utilizarse conforme al RGPD. Esto significa que, además de beneficiarse de todas las medidas que AWS ya ha implantado para mantener la seguridad de los servicios, los clientes pueden implementar servicios de AWS en sus planes de conformidad con el RGPD. AWS cuenta con un Anexo de Procesamiento de Datos para el cumplimiento del RGPD (DPA para RGPD), lo que le permite cumplir las obligaciones contractuales de este reglamento. El DPA para RGPD de AWS está integrado en los Términos de servicio de AWS y se aplica automáticamente a los clientes de todo el mundo que necesiten cumplir con el RGPD. Amazon.com, Inc. cuenta con la certificación del Escudo de la privacidad UE-EE. UU., y AWS está cubierto por dicha certificación. Esto ayuda a los clientes que deciden transferir a EE. UU. los datos personales a cumplir sus obligaciones de protección de datos. La certificación de Amazon.com Inc. está disponible en el sitio web del Escudo de la privacidad UE-EE. UU.: https://www.privacyshield.gov/list.

Al trabajar en un entorno acreditado, los clientes reducen el ámbito y el coste de las auditorías que tienen que realizar. La infraestructura subyacente de AWS se evalúa continuamente, incluida la seguridad física y del entorno del hardware y los centros de datos, para que los clientes puedan beneficiarse de estas certificaciones y utilizar estos controles sin preocuparse de nada más.

En un centro de datos tradicional, las actividades que se realizan normalmente en relación con la conformidad suelen ser manuales y periódicas. Estas actividades incluyen la verificación de la configuración de los activos y la generación de informes en relación con las actividades administrativas. Sin embargo, dichos informes se quedan obsoletos antes de que tan siquiera lleguen a publicarse. El entorno de AWS permite a los clientes utilizar herramientas automatizadas e integradas, como AWS Security Hub, AWS Config y AWS CloudTrail, para validar la conformidad. Con estas herramientas, se reduce el esfuerzo de las auditorias, ya que estas tareas se realizan de forma rutinaria, automatizada y continuada. Al dedicar menos tiempo a las actividades manuales, es posible incluso modificar el papel de la conformidad en la organización para que deje de ser una carga administrativa necesaria y se convierta en una tarea que gestione los riesgos y mejore el nivel de seguridad.

Otra documentación

Para obtener más información, consulte los siguientes recursos:

Para obtener información sobre…	Consulte
Temas clave, áreas de investigación y oportunidades de formación sobre la seguridad en la nube de AWS	Aprendizaje sobre seguridad en la nube de AWS
El Marco de adopción de la nube de AWS, que contiene directrices organizadas en seis áreas: Empresa, Personal, Conformidad, Gestión, Plataforma, Seguridad y Operaciones	Marco de adopción de la nube de AWS
Controles específicos aplicados en AWS y cómo integrar AWS en el marco existente	Amazon Web Services: Riesgos y conformidad
Prácticas recomendadas para implementar los controles de seguridad en un entorno de AWS	Prácticas de seguridad recomendadas de AWS
El pilar de seguridad de AWS Well-Architected Framework	Pilar de seguridad de AWS Well-Architected Framework

Revisiones del documento

Fecha	Descripción
Enero de 2020	Se actualizaron los servicios, recursos y tecnologías más recientes.
Julio de 2015	Publicación inicial.