aws

Unable to locate subtitle

Amazon Web Services: Risk and Compliance

Amazon Web Services: Risk and Compliance: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: Risk and Compliance

Fecha de publicación: 11 de marzo de 2021 (Revisiones del documento)

Resumen

AWS atiende a una variedad de clientes, incluidos los de sectores regulados. A través de nuestro modelo de responsabilidad compartida, permitimos a los clientes administrar el riesgo de manera efectiva y eficiente en el entorno de TI, y garantizamos una gestión de riesgos efectiva a través de nuestra conformidad de marcos y programas establecidos y ampliamente reconocidos. Este documento pone de relieve los mecanismos que AWS ha implementado para administrar riesgos del lado de AWS con el modelo de responsabilidad compartida de AWS, y las herramientas que los clientes pueden utilizar para garantizar que esos mecanismos se aplican de manera eficaz.

Introducción

AWS y sus clientes ejercen el control compartido del entorno de TI. Por tanto, la seguridad es una responsabilidad compartida. Cuando se trata de administrar la seguridad y la conformidad en la nube de AWS, cada parte tiene responsabilidades distintas. La responsabilidad del cliente depende de los servicios que utilice. Sin embargo, en general, los clientes son responsables de construir su entorno de TI de una manera que esté en consonancia con sus requisitos específicos de seguridad y conformidad.

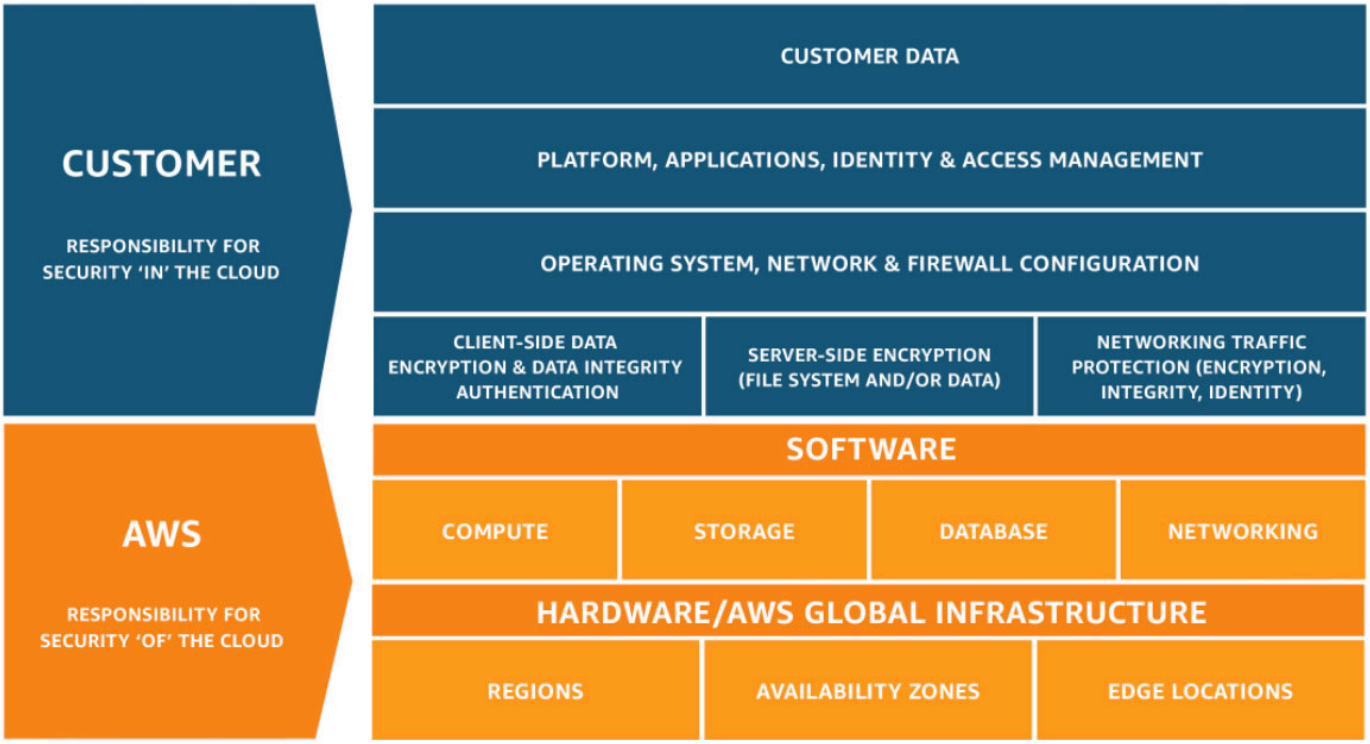
Este documento proporciona más detalles sobre las responsabilidades de seguridad de cada parte y las formas en que los clientes pueden beneficiarse del programa de conformidad y riesgos de AWS.

Modelo de responsabilidad compartida

Los asuntos relacionados con la seguridad y la conformidad son responsabilidades compartidas entre AWS y el cliente. En función de los servicios implementados, este modelo compartido puede ayudar a aliviar la carga operativa del cliente. Esto es porque AWS dirige, administra, y controla los componentes del sistema operativo host y la capa de virtualización con el fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad) y de cualquier otro software de aplicaciones asociado, además de la configuración del firewall del grupo de seguridad que ofrece AWS.

Recomendamos que los clientes piensen detenidamente en los servicios que eligen, ya que sus responsabilidades varían en función de los servicios que utilizan, la integración de estos en su entorno de TI y la legislación y los reglamentos aplicables. Los clientes pueden mejorar la seguridad o cumplir requisitos de conformidad más estrictos mediante la utilización de aplicaciones tecnológicas como firewalls basados en host, prevención y detección de intrusiones basadas en host, cifrado y administración de claves.

La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y el control que permite a los clientes implementar soluciones que satisfagan los requisitos de certificación específicos del sector.



Este modelo de responsabilidad compartida también abarca los controles de TI. De la misma forma que AWS y sus clientes comparten la responsabilidad operativa del entorno de TI, compartir la administración, la operación y la verificación de los controles de TI es también una responsabilidad compartida. AWS puede ayudar a los clientes administrando los controles asociados a la infraestructura física implementada en el entorno de AWS. Los clientes pueden usar la documentación de conformidad y control de AWS disponible para ejecutar sus procedimientos de verificación y evaluación de controles según sea necesario. Para ver ejemplos de cómo se comparte la responsabilidad de ciertos controles entre AWS y sus clientes, consulte el Modelo de responsabilidad compartida de AWS.

Evaluación e integración de los controles de AWS

AWS ofrece a los clientes una gran variedad de información sobre el entorno de control informático a través de documentos técnicos, informes, certificaciones y otras acreditaciones de terceros. Esta documentación ayuda a los clientes a conocer los controles existentes relevantes para los servicios de AWS que utilizan y cómo se han validado estos controles. Esta información también ayuda a los clientes a tener en cuenta y validar que los controles de su entorno de TI ampliado funcionen de manera efectiva.

Tradicionalmente, los auditores internos y/o externos validan el diseño y la efectividad operativa de los controles mediante revisiones de procesos y evaluación de evidencias. Este tipo de observación y verificación directas, por parte del cliente o el auditor externo del cliente, generalmente se realiza para validar los controles en las implementaciones locales tradicionales.

En el caso de que se utilicen proveedores de servicios (como AWS), los clientes pueden solicitar y evaluar acreditaciones y certificaciones de terceros. Estas acreditaciones y certificaciones pueden ayudar a garantizar al cliente el diseño y la efectividad operativa del objetivo de control y los controles validados por un tercero calificado e independiente. Como resultado, aunque es posible que AWS administre algunos controles, el entorno de control puede seguir siendo un marco unificado en el que los clientes puedan dar cuenta y verificar que los controles funcionan de manera efectiva y aceleran el proceso de revisión de conformidad.

Las acreditaciones y certificaciones de terceros de AWS proporcionan a los clientes visibilidad y validación independiente del entorno de control. Dichas acreditaciones y certificaciones pueden ayudar a liberar a los clientes del requisito de realizar ciertos trabajos de validación por sí mismos para su entorno de TI en la nube de AWS.

Programa de riesgos y conformidad de AWS

AWS ha integrado un programa de riesgos y conformidad en toda la organización. Este programa tiene como objetivo gestionar el riesgo en todas las fases del diseño e implementación de servicios y mejorar y revaluar continuamente las actividades relacionadas con el riesgo de la organización. Los componentes del programa integrado de riesgos y conformidad de AWS se analizan en mayor detalle en las siguientes secciones.

Gestión de riesgos empresariales de AWS

AWS cuenta con un programa de gestión de riesgos empresariales (BRM) que se asocia con las unidades de negocio de AWS para ofrecer a la junta directiva de AWS y a los directivos de AWS una visión integral de los principales riesgos en AWS. El programa BRM demuestra una supervisión independiente de los riesgos de las funciones de AWS. Específicamente, el programa BRM hace lo siguiente:

- Realiza evaluaciones de riesgos y monitoreo de riesgos de áreas funcionales clave de AWS
- Identifica e impulsa la corrección de riesgos
- Mantiene un registro de riesgos conocidos

Para impulsar la corrección de riesgos, el programa BRM informa de los resultados de sus esfuerzos y, cuando es necesario, los remite a los directores y vicepresidentes de toda la empresa para informar de la toma de decisiones de la empresa.

Gestión operativa y empresarial

AWS realiza una combinación de reuniones e informes semanales, mensuales y trimestrales para, entre otras cosas, garantizar la comunicación de los riesgos en todos los componentes del proceso de gestión de riesgos. Además, AWS implementa un proceso de escalado para proporcionar visibilidad a la dirección de los riesgos de alta prioridad en toda la organización. Estos esfuerzos, en conjunto, ayudan a garantizar que el riesgo se administre de manera coherente con la complejidad del modelo de negocio de AWS.

Además, a través de una estructura de responsabilidad en cascada, los vicepresidentes (propietarios de empresas) son responsables de la supervisión de su negocio. Con este fin, AWS realiza

reuniones semanales para revisar las métricas operativas e identificar las tendencias y los principales riesgos antes de que afecten al negocio.

Los altos cargos desempeñan funciones importantes a la hora de definir los valores principales y el tono de AWS. Todos los empleados reciben el Código deontológico y de conducta comercial de la empresa y, además, completan un proceso de capacitación periódica de empleados. Las auditorías de conformidad se realizan a fin de que los empleados puedan conocer y seguir las políticas establecidas.

La estructura organizativa de AWS ofrece una estructura de planificación, ejecución y control de las operaciones empresariales. Esta estructura organizativa incluye funciones y responsabilidades a fin de habilitar al personal adecuado, realizar las operaciones con eficacia y facilitar la segregación de funciones. La dirección también tiene líneas apropiadas definidas para generar informes del personal clave. Los procesos de verificación para la contratación de la empresa comprenden la validación de la formación, la experiencia profesional anterior y, en algunos casos, la comprobación de antecedentes de conformidad con la legislación y los reglamentos a efectos de que los empleados se ajusten al cargo que ocuparán y al nivel de acceso a las instalaciones de AWS. La empresa sigue un proceso de contratación estructurado para familiarizar a los nuevos empleados con las herramientas, los procesos, los sistemas, las políticas y los procedimientos de Amazon.

Entorno de control y automatización

AWS implementa controles de seguridad como un elemento fundamental para administrar el riesgo en toda la organización. El entorno de control de AWS se compone de estándares, procesos y estructuras que proporcionan la base para implementar un conjunto mínimo de requisitos de seguridad en AWS.

Si bien los procesos y estándares incluidos como parte del entorno de control de AWS se mantienen por sí solos, AWS también aprovecha aspectos del entorno de control general de Amazon. Las herramientas utilizadas incluyen:

- Herramientas utilizadas en todas las empresas de Amazon, como la herramienta que gestiona la separación de tareas
- Ciertas funciones empresariales en todo Amazon, como las legales, de recursos humanos y financieras

En los casos en que AWS aprovecha el entorno de control general de Amazon, los estándares y procesos que rigen estos mecanismos se adaptan específicamente al negocio de AWS. Esto

significa que las expectativas para su uso y aplicación dentro del entorno de control de AWS pueden diferir de las expectativas de su uso y aplicación en el entorno general de Amazon. El entorno de control de AWS actúa en última instancia como la base para la entrega segura de ofertas de servicios de AWS.

La automatización del control es una forma de que AWS reduzca la intervención humana en ciertos procesos recurrentes que comprenden el entorno de control de AWS. Es clave para la implementación efectiva del control de seguridad de la información y la gestión asociada de los riesgos. La automatización del control busca minimizar de manera proactiva las posibles inconsistencias en la ejecución del proceso que pueden surgir debido a la naturaleza defectuosa de los humanos que realizan un proceso repetitivo. Mediante la automatización del control, se eliminan las posibles desviaciones del proceso. Esto proporciona mayores niveles de seguridad de que se aplicará un control según lo diseñado.

Los equipos de ingeniería de AWS en todas las funciones de seguridad son responsables de diseñar el entorno de control de AWS para admitir mayores niveles de automatización de controles siempre que sea posible. Entre los ejemplos de controles automatizados en AWS se incluyen:

- Gobernanza y supervisión: control de versiones y aprobación de políticas
- Administración de personal: impartición de formación automatizada, despido rápido de empleados
- Administración de desarrollo y configuración: canalizaciones de implementación de código, análisis de código, copia de seguridad de código, pruebas de implementación integradas
- Identity and Access Management: división automatizada de tareas, revisiones de acceso, administración de permisos
- Monitoreo y registro: recopilación y correlación de registros automatizadas, alarmas
- Seguridad física: procesos automatizados relacionados con los centros de datos de AWS, incluida la administración de hardware, la formación en seguridad del centro de datos, alarmas de acceso y administración de acceso físico
- Análisis y administración de parches: análisis de vulnerabilidades, administración de parches e implementación automatizados

Evaluación de controles y monitoreo continuo

AWS implementa diversas actividades antes y después de la implementación del servicio para reducir aún más el riesgo en el entorno de AWS. Estas actividades integran los requisitos de

seguridad y conformidad durante el diseño y el desarrollo de cada servicio de AWS y, a continuación, validan que los servicios funcionen de forma segura una vez que pasan a producción (lanzamiento).

Las actividades de conformidad y gestión de riesgos incluyen dos actividades previas al lanzamiento y dos actividades posteriores al lanzamiento. Las actividades previas al lanzamiento son las siguientes:

- Revisión de la administración de riesgos de seguridad de aplicaciones de AWS para validar que los riesgos de seguridad se han identificado y mitigado
- Revisión de la preparación de la arquitectura para ayudar a los clientes a garantizar que están en consonancia con los regímenes de conformidad

En el momento de su implementación, un servicio habrá pasado por evaluaciones rigurosas en relación con los requisitos de seguridad detallados para cumplir con los altos estándares de seguridad de AWS. Las actividades posteriores al lanzamiento son las siguientes:

- Revisión continua de AWS Application Security para garantizar que se mantenga la posición de seguridad del servicio
- Análisis continuo de la administración de vulnerabilidades

Estas evaluaciones de control y el monitoreo continuo permiten a los clientes regulados la capacidad de crear con confianza soluciones conformes en los servicios de AWS. Para obtener una lista de los servicios incluidos en el ámbito de varios programas de conformidad, consulte la página web Servicios de AWS en el ámbito.

Certificaciones, programas e informes de AWS y acreditaciones independientes

AWS se somete regularmente a auditorías de certificación independientes de terceros para garantizar que las actividades de control funcionen según lo previsto. Más específicamente, AWS se audita en función de una variedad de marcos de seguridad globales y regionales que dependen de la región y el sector. AWS participa en más de 50 programas de auditoría diferentes.

El organismo evaluador documenta los resultados de estas auditorías y los pone a disposición de todos los clientes de AWS a través de AWS Artifact. AWS Artifact es un portal autoservicio gratuito para obtener acceso a informes de conformidad de AWS bajo demanda. Cuando se publican nuevos

informes, están disponibles en AWS Artifact, lo que permite a los clientes supervisar continuamente la seguridad y la conformidad de AWS con acceso inmediato a los nuevos informes.

En función de los requisitos contractuales o reglamentarios locales de un país o sector, AWS también puede someterse a auditorías directamente con los clientes o los auditores gubernamentales. Estas auditorías proporcionan una supervisión adicional del entorno de control de AWS para garantizar que los clientes tengan las herramientas para ayudarse a sí mismos a operar con confianza, conformidad y de manera basada en el riesgo mediante el uso de los servicios de AWS.

Para obtener información más detallada sobre los programas de certificación de AWS, los informes y las atestaciones de terceros, visite la página web del programa de conformidad de AWS. También puede visitar la página web de Servicios de AWS en el ámbito para obtener información específica del servicio.

Cloud Security Alliance

AWS participa en la autoevaluación voluntaria de Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) de CSA para documentar nuestra conformidad con las prácticas recomendadas publicadas por CSA. La CSA es “la organización líder mundial dedicada a definir y crear conciencia sobre las prácticas recomendadas para ayudar a garantizar un entorno de computación en la nube seguro”. El Cuestionario de la Iniciativa de Evaluación de Consenso de la CSA (CAIQ) proporcionado por la CSA anticipa un conjunto de preguntas que un cliente de la nube. y/o un auditor de la nube preguntaría a un proveedor de la nube. Contiene una serie de preguntas sobre la seguridad, el control y los procesos que pueden utilizarse para una amplia variedad de esfuerzos, entre otros, para evaluar la seguridad y seleccionar al proveedor de la nube.

Hay dos recursos disponibles para los clientes que documentan la alineación de AWS con el CAIQ de CSA. El primero es el documento técnico de CAIQ de CSA y el segundo es una asignación de control más detallada para nuestros controles SOC-2, que está disponible a través de AWS Artifact. Para obtener más información sobre la participación de AWS en el CAIQ de CSA, consulte el sitio de CSA de AWS.

Gobernanza del conformidad de la nube

Los clientes de AWS son responsables de mantener una gobernanza adecuada en todo su entorno de control de TI, independientemente de cómo o dónde se implemente la TI. Las prácticas principales incluyen:

- Conocer los objetivos y los requisitos necesarios en materia de conformidad (a partir de las fuentes pertinentes)
- Crear un entorno de control que satisfaga tales objetivos y requisitos
- Conocer la validación necesaria conforme a la tolerancia de riesgos de la organización
- Verificar la eficacia operativa del entorno de control

La implementación en la nube de AWS ofrece a las compañías diferentes opciones para aplicar varios tipos de controles y diversos métodos de verificación.

A efectos de conseguir un sólido nivel de control y conformidad por parte del cliente se puede realizar lo siguiente:

1. Revisar el Modelo de responsabilidad compartida de AWS, la Documentación de seguridad de AWS los Informes de conformidad de AWS e información adicional disponible en AWS, junto con otra documentación específica del cliente. Intentar comprender la mayor parte posible de todo el entorno de TI y, a continuación, documentar todos los requisitos de conformidad en un marco de control de la nube integral.
2. Diseñar e implementar objetivos de control para cumplir con los requisitos de conformidad empresarial según lo establecido en el modelo de responsabilidad compartida de AWS.
3. Identificar y documentar los controles que sean propiedad de terceros.
4. Comprobar que se cumplen todos los objetivos de control, que se han diseñado todos los controles principales y que estos operan con eficacia.

Enfocar el control de la conformidad de esta forma ayudará a los clientes a conocer mejor su entorno de control y a definir con claridad las actividades de verificación que cabe ejecutar.

Conclusión

Proporcionar una infraestructura y servicios altamente seguros y resilientes a nuestros clientes es una de las principales prioridades de AWS. Nuestro compromiso con nuestros clientes se centra en trabajar para ganarnos su confianza de forma continua y garantizar que ellos mantengan la confianza en la la realización segura de las operaciones de sus cargas de trabajo en AWS. Para lograrlo, AWS ha integrado mecanismos de riesgo y conformidad que incluyen:

- La implementación de una amplia gama de controles de seguridad y herramientas automatizadas
- Supervisión y evaluación continuas de los controles de seguridad para ayudar a garantizar la eficacia operativa de AWS y la estricta adhesión a los regímenes de conformidad
- Evaluación de riesgos independiente por parte del programa de gestión de riesgos empresariales de AWS
- Mecanismos de administración operativa y empresarial

Además, AWS se somete regularmente a auditorías independientes de terceros para garantizar que las actividades de control funcionen según lo previsto. Estas auditorías, junto con las numerosas certificaciones que AWS ha obtenido, proporcionan un nivel adicional de validación del entorno de control de AWS que beneficia a los clientes.

En conjunto con los controles de seguridad administrados por el cliente, estos esfuerzos permiten a AWS innovar de forma segura en nombre de los clientes y ayudar a los clientes a mejorar su posición de seguridad al crear en AWS.

Colaboradores

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

- Marta Taggart, directora sénior de programas, Seguridad de AWS
- Bradley Roach, administrador de riesgos, Administración de riesgos empresariales de AWS
- Patrick Woods, especialista sénior en seguridad, Seguridad de AWS

Documentación adicional

AWS proporciona a los clientes información sobre su entorno de seguridad y control mediante:

- Obtener y mantener las certificaciones del sector y las acreditaciones de terceros independientes que se enumeran en la página del programa de conformidad de AWS.
- Publicar de forma consistente información de forma coherente sobre las prácticas de seguridad y control de AWS en documentos técnicos y contenido web, como el blog de seguridad de AWS.
- Proporcionamos descripciones detalladas de cómo AWS utiliza la automatización a escala para administrar nuestra infraestructura de servicios en La Amazon Builders' Library.
- Mejora de la transparencia al proporcionar certificados de conformidad, informes y otra documentación directamente a los clientes de AWS a través del portal de autoservicio conocido como AWS Artifact.
- Proporcionar recursos de conformidad de AWS y documentar y publicar respuestas a las consultas en la página web Preguntas frecuentes sobre conformidad de AWS.
- Los clientes pueden seguir los principios de diseño de AWS Well-Architected Framework para obtener orientación sobre cómo abordar la configuración por encima de la línea de sus cargas de trabajo creadas en AWS.

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

update-history-change	update-history-description	update-history-date
Actualizaciones menores	Revisado para garantizar la precisión técnica	10 de marzo de 2021
Documento técnico actualizado	Esta versión incluye cambios sustanciales que incluyen la eliminación de la información de referencia sobre programas y esquemas de conformidad, ya que esta información está disponible en las páginas web de Programas de conformidad de AWS y Servicios de AWS en el ámbito del programa de conformidad. Además, eliminamos la sección que cubre las preguntas comunes de conformidad porque esa información ya está disponible en la página web de preguntas frecuentes sobre conformidad de AWS.	1 de noviembre de 2020
Publicación inicial	Amazon Web Services: documento técnico sobre riesgos y conformidad publicado	1 de mayo de 2011

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 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.