Jonathan A nderson

AWS

Certified Solutions Architect

Associate

The ultimate guide for the

SAA-C03

Imagen que contiene lego, juguete

Descripción generada automáticamenteE X A M

# Chapter 5

**AWS Risk and Compliance**

Este capítulo proporciona información para ayudar a los clientes a integrar AWS en su marco de control existente, incluido un enfoque básico para evaluar los controles de AWS.

AWS y sus clientes comparten el control del entorno informático. Parte de esta responsabilidad compartida de AWS incluye proporcionar sus servicios en una plataforma altamente segura y monitoreada y proporcionar una amplia variedad de características de seguridad para clientes a utilizar. La responsabilidad del cliente incluye la configuración de su entornos TI de forma segura y controlada para sus fines. Si bien los clientes no comunican sus usos y configuraciones a AWS, AWS sí comunica el entorno de seguridad y control relevante a los clientes. PARA ello, AWS sigue estos pasos:

* 1. Obtener certificaciones industriales y certificaciones externas independientes como se describe en este documento
  2. Publicar información sobre las prácticas de auditoría y seguridad de AWS en notas del producto y contenido del sitio web
  3. Proporcionar certificados, informes y otros documentos directamente a los clientes de AWS bajo NDA (si es necesario)

**Shared Responsibility Environment**

La transición de la infraestructura de TI a los servicios de AWS crea un modelo de responsabilidad compartida entre el cliente y AWS. A medida que AWS ejecuta, administra y monitorea los componentes desde el sistema operativo host y desde la capa de virtualización hasta la protección física de las instalaciones donde se ejecuta el servicio, este modelo compartido ayudará a reducir la carga operativa para el cliente. El sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), otro software de aplicación relacionado y la configuración del firewall del grupo de seguridad admitido por AWS son responsables para y operado por el cliente.

Como sus funciones difieren según los servicios utilizados, la incorporación de esos servicios en su entorno de TI y las leyes y regulaciones relevantes, los clientes deben considerar cuidadosamente los servicios que eligen. Al aprovechar tecnologías como los firewalls basados en host, la detección/prevención de intrusiones en el host basada en la red, el cifrado y la administración de claves, los clientes pueden mejorar la protección y/o cumplir con requisitos de aplicación más estrictos.

La flexibilidad y el control del consumidor que permiten introducir soluciones que cumplen con los criterios de certificación específicos de la industria, a menudo proporcionan la esencia de esta responsabilidad compartida.

Este modelo de responsabilidad compartida entre el cliente y AWS también se extiende a los controles de TI. Así como la responsabilidad de operar el entorno de TI se comparte entre AWS y sus clientes, la administración, ejecución y validación de los controles de TI se comparten. Al manejar los controles asociados con la infraestructura física instalada en la configuración de AWS que anteriormente habría sido gestionado por el cliente, AWS puede ayudar al cliente a aliviar la carga de los controles operativos.

Debido a que cada cliente se implementa de manera diferente en AWS, los clientes pueden beneficiarse de mover la administración de algunos controles de TI a AWS, lo que resulta en un (nuevo) entorno de control distribuido. A continuación, los clientes pueden utilizar la documentación de conformidad y supervisión de AWS disponible (descrita en certificaciones de AWS y atestaciones de terceros) para llevar a cabo los procedimientos de revisión de supervisión y verificación requeridos.

## Strong Compliance Management

Como siempre, los clientes de AWS deben mantener una gobernanza adecuada en todo el entorno de control de TI, independientemente de cómo se implemente la TI. Las mejores prácticas incluyen comprender los objetivos y los requisitos de cumplimiento requeridos (de fuentes relevantes), establecer un entorno controlado que cumpla con estos objetivos y requisitos, comprender la validación requerida basada en la tolerancia al riesgo de la organización y la verificación de la efectividad operativa de su entorno de control.

La implementación en la nube de AWS ofrece a las empresas varias opciones para aplicar diferentes tipos de controles y diferentes métodos de autenticación.

El cumplimiento y la gobernanza sólidos del cliente pueden incluir los siguientes enfoques básicos:

1. Revise la información disponible en AWS junto con otra información para obtener la mayor información posible sobre todo el entorno de TI y, a continuación, documente todos los requisitos de conformidad.
2. Diseñar e implementar objetivos de auditoría para cumplir con los requisitos de cumplimiento del negocio.
3. Identificar y documentar auditorías de terceros.
4. Verifique que todos los objetivos de control estén en línea y que todos los controles significativos estén diseñados y funcionen de manera efectiva.

Al abordar el gobierno de cumplimiento de esta manera, las empresas comprenderán mejor su entorno de control y podrán definir las actividades de auditoría que se realizarán.

## AWS Monitors Assessment and Integration

AWS proporciona una amplia gama de información sobre su entorno de control de TI a los clientes a través de white papers, informes, certificaciones y otras declaraciones de terceros. Esta documentación ayuda a los clientes a comprender los controles existentes que son aplicables a los servicios de AWS que utilizan y cómo han comprobado esos controles. Esta información también ayuda a los clientes en sus esfuerzos por informar y validar que los controles funcionan de manera efectiva en su entorno de TI integral.

Tradicionalmente, el diseño y la efectividad operativa de los objetivos y controles de auditoría son validados por auditores internos y / o externos a través de procesos paso a paso y evaluación de evidencia. La observación/verificación directa, por parte del cliente o del auditor externo del cliente, generalmente se realiza para validar los controles. Al utilizar proveedores de servicios como AWS, las empresas solicitan y revisan licencias y certificaciones de terceros para obtener una garantía justa en cuanto al diseño. y la eficacia operacional de los objetivos y controles de la auditoría. Por lo tanto, si bien AWS puede administrar los controles principales del cliente, el entorno de control puede seguir siendo un marco unificado en el que todos los controles se consideran y verifican como si funcionaran de manera efectiva.

Las atestaciones de AWS y las certificaciones de terceros no solo pueden proporcionar un mayor nivel de validación del entorno de control, sino que también pueden eximir a los clientes de la obligación de determinar algún tipo de validación para su entorno de TI. en la nube de AWS.

**AWS IT control information**

AWS entrega información de control de TI a los clientes de las siguientes maneras:

## Definition of specific control.

Los clientes de AWS pueden identificar los controles clave administrados por AWS. Los controles clave son esenciales para el entorno de control del cliente y requieren certificación de la eficacia operativa de estos controles clave para cumplir con los requisitos de cumplimiento, como la auditoría financiera anual. Con este fin, AWS publica una amplia variedad de controles de TI específicos en su organización de servicios.

**Control report 1 (SOC 1) Type II.**

El informe SOC 1, anteriormente la Declaración del Informe de las Organizaciones de Servicios sobre Normas de Auditoría (SAS) No. 70, es un estándar de auditoría comúnmente aceptado establecido por el Instituto Americano de Contadores Públicos Certificados. La auditoría SOC 1 es una auditoría interna del diseño y la eficacia operativa de los objetivos de control y las actividades de control identificados por AWS (incluidos los objetivos de control y actividades de control por parte de la infraestructura controlada por AWS). «Tipo II» se refiere al hecho de que cada uno de los controles mencionados en el informe no solo es verificado por el auditor externo para determinar su adecuación del diseño, sino que también se evalúa. para el rendimiento operativo. Debido a la independencia e integridad del auditor externo de AWS, los controles definidos en el informe deben dar a los clientes un alto grado de confianza en el entorno de control de AWS.

Las auditorías de AWS están diseñadas y creadas para funcionar de manera efectiva para muchos fines de conformidad, incluidas las auditorías de los estados financieros de la Sección 404 de Sarbanes-Oxley (SOX). El uso de informes SOC 1 Tipo II según lo generalmente permitido por otras autoridades de certificación de terceros (por ejemplo, los auditores ISO 27001 pueden solicitar un informe SOC 1 Tipo II para completar sus revisiones de clientes).

Otras actividades de monitoreo específicas están relacionadas con el cumplimiento de AWS por parte de la industria de tarjetas de pago (PCI) y la Ley Federal de Administración de Seguridad de la Información (FISMA). AWS cumple con FISMA Moderate y EL ESTÁNDAR DE SEGURIDAD DE DATOS PCI. Estos estándares PCI y FISMA son altamente prescriptivos y requieren una validación independiente para que AWS cumpla con el estándar publicado.

**Compliance with General Auditing Standards.**

Si un cliente de AWS necesita que se cumpla un amplio conjunto de objetivos de auditoría, se puede realizar una evaluación de las certificaciones del sector de AWS. Con la certificación AWS ISO 27001, AWS se adhiere a un estándar de seguridad amplio e integral y sigue las prácticas recomendadas para mantener un entorno seguro. Junto con el estándar de seguridad de datos PCI (PCI DSS), AWS cumple con una serie de controles clave para las empresas que administran la información de las tarjetas de crédito. Como AWS es compatible con FISMA, AWS cumple con una amplia variedad de controles específicos requeridos por las agencias gubernamentales de EE. UU. La adhesión a estos estándares globales proporciona a los clientes información detallada sobre la naturaleza general de los controles y procesos de seguridad implementados, que se pueden tener en cuenta al administrar el cumplimiento.

**AWS Global Regions**

Los centros de datos se construyen en clústeres en diferentes regiones del mundo, incluidos EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Oregón), EE. UU. Oeste (Norte de California), AWS GovCloud (EE. UU.) (Oregón), UE (Frankfurt), UE (Irlanda)), Asia-Pacífico (Seúl), Asia-Pacífico (Singapur), Asia-Pacífico (Tokio), Asia-Pacífico (Sydney), China (Beijing) y América del Sur (Sao Paulo).