Entendiendo los estándares de cumplimiento y auditoría del centro de datos

Entendiendo los estándares de cumplimiento y auditoría del centro de datos.Una de las características más importantes de cualquier centro de datos es su seguridad .

Después de todo, las empresas confían en que sus datos de misión crítica estén contenidos dentro de las instalaciones.

En los últimos años, la seguridad se ha vuelto aún más crítica para las empresas. Ya sea que almacene sus datos en un centro de datos interno o con un proveedor externo, los ciberataques son una amenaza real y creciente para sus operaciones. ¿Tienen un plan para prevenir los ataques DDoS ?

Cada año, la cantidad de incidentes de seguridad aumenta y el volumen de datos comprometidos se amplifica proporcionalmente.

En los primeros 6 meses de 2018, se comprometieron 3,353,172,708 registros. Un aumento del 72% en comparación con el mismo período de 2017. Según el Índice de nivel de incumplimiento ,

En consecuencia, la protección de datos en todos los niveles importa más que nunca. Asegurar su centro de datos o elegir un proveedor compatible debe ser el núcleo de su estrategia de seguridad.

La realidad es que los incidentes y ataques de seguridad cibernética son cada vez más frecuentes y agresivos.

¿Cuáles son los niveles de seguridad del centro de datos?

Los estándares de seguridad del centro de datos ayudan a hacer cumplir las mejores prácticas de protección de datos. Comprender su alcance y valor es esencial para elegir un proveedor de servicios. También desempeña un papel en el desarrollo de una estrategia de TI a largo plazo que puede implicar una amplia subcontratación.

Este artículo cubre los estándares críticos de los centros de datos y sus historias de cambio. Además de aprender lo que significan estos estándares, las empresas también deben mantenerse al día con cualquier actualización operativa que pueda afectarlos.

El verdadero desafío es que muchos fuera del ámbito de la auditoría pueden no entender completamente las diferentes clasificaciones. Es posible que ni siquiera sepan qué buscar en el diseño y la certificación de un centro de datos.

Para ayudarlo a tomar una decisión más informada sobre los servicios de su centro de datos, aquí hay una descripción

general de los conceptos que debe comprender.

Cumplimiento del Centro de Datos

Estándar de Auditoría y Certificación SSAE 18

Un estándar de larga data en la industria de los centros de datos, SAS 70 se retiró oficialmente a fines de 2010. Poco después de su suspensión, muchas instalaciones cambiaron a SSAE 16.

Sin embargo, es importante comprender que no existe una certificación para SSAE 16. Es un estándar desarrollado por la Junta de Normas de Auditoría (ASB) del Instituto Americano de Contadores Públicos Certificados (AICPA).

Además de las siglas, la SSAE 16 no es algo que una empresa pueda lograr. Es un estándar de certificación utilizado para dar credibilidad a los procesos organizativos. A diferencia de SAS 70, SSAE 16 requería que los proveedores de servicios “proporcionaran una declaración escrita con respecto a la efectividad de los controles”. De esa manera, SSAE 18 introdujo un control más efectivo de los procesos y sistemas de una compañía, mientras que SAS 70 era principalmente una práctica de auditoría.

Es importante mencionar que SSAE 16 solía dar como resultado un informe 1 de Control de Organización de Servicios (SOC o centro de operaciones de seguridad). Este informe todavía está en uso y proporciona información sobre las políticas y los procesos de informes de la compañía.

Después de años de existencia, SSAE 16 fue reemplazado recientemente con una versión revisada. A partir del 1 de mayo de 2017, ya no se puede emitir, y en su lugar se utiliza un SSAE 18 mejorado.

SSAE 18 se basa en la versión anterior con varias adiciones importantes. Ambos se refieren a los procesos de evaluación de riesgos, que anteriormente solo formaban parte de la certificación SOC 2 .

Las actualizaciones de SSAE 18 incluyen:

La orientación en evaluación de riesgos. Esta parte ayuda a hacer que las organizaciones evalúen y revisen los riesgos potenciales de la tecnología con regularidad.
Controles complementarios de la organización de servicios. Una nueva sección en el estándar apunta a dar más claridad a las actividades de un proveedor externo específico.
Con estos cambios, el estándar actualizado apunta a mejorar aún más el monitoreo del centro de datos. Una de las medidas de precaución más importantes contra las infracciones y las acciones fraudulentas, el monitoreo de los sistemas y actividades críticas es la base de las organizaciones seguras. Es posible que haya creado un poco más de trabajo para un proveedor de servicios, pero también lleva su seguridad al siguiente nivel.

De los informes relevantes para los centros de datos, SOC 1 es el más cercano al antiguo SAS 70. La organización de servicios (centro de datos) define los controles internos contra los cuales se realizan las auditorías.

El propósito clave de SOC 1 es proporcionar información sobre la estructura de control de un proveedor de servicios. Es particularmente crucial para SaaS y las empresas de tecnología que ofrecen algunos servicios vitales para las empresas. En ese sentido, están más integrados en los procesos de sus clientes que un socio comercial general o un colaborador.

SOC 1 también se aplica cuando las aplicaciones financieras de los clientes o la infraestructura subyacente están involucradas. Cloud calificaría para este tipo de informe. Sin embargo, SOC 1 no se aplica a los proveedores de colocación

que no están realizando servicios administrados.

SOC 2 es exclusivo para organizaciones de servicio cuyos controles no son relevantes para las aplicaciones financieras de los clientes o los requisitos de informes. Las instalaciones del centro de datos de colocación que proporcionan controles de energía y ambientales calificarían aquí. Sin embargo, a diferencia de un SOC 1, los controles son proporcionados (o prescritos) por el AICPA (Principios de Servicios de Confianza) y auditados.

Convertirse en una queja SOC 2 es un proceso más riguroso. Se requiere que los proveedores de servicios informen sobre todos los detalles con respecto a sus prácticas de control de autorización y acceso interno, así como los procesos de supervisión y notificación.

SOC 3 requiere una auditoría similar a SOC 2 (controles prescritos). Sin embargo, no incluye tablas de informes o pruebas. Cualquier organización de tipo consumidor puede optar por seguir esta ruta para poder publicar un logotipo de SOC en sus sitios web, etc.

Normasad

i

cionales de cumplimiento

HIPAA y PCI DSS son dos nociones críticas que se deben comprender al evaluar la seguridad del centro de datos.

HIPAA

HIPAA (Ley de responsabilidad y portabilidad de seguros de salud) regula los datos, la seguridad del almacenamiento en la nube y las mejores prácticas de administración en la industria de la salud. Dada la naturaleza sensible de los datos de salud, cualquier institución que los maneje debe seguir prácticas estrictas de seguridad.

El cumplimiento de HIPAA también afecta a los proveedores de centros de datos. De hecho, se aplica a cualquier organización que trabaje con un proveedor de atención médica y tenga acceso a datos médicos. HIPAA considera a todas estas organizaciones como Asociado de negocios de un proveedor de atención médica.

Si usted o sus clientes tienen acceso a datos de atención médica, debe verificar si está utilizando un proveedor de alojamiento compatible con HIPAA . Este cumplimiento garantiza que puede ofrecer los niveles necesarios de seguridad de datos. Además, puede proporcionar la documentación que debe presentar para demostrar el cumplimiento.

Estándar de seguridad de datos de la industria de tarjetas de pago PCI-DSS

En cuanto a PCI DSS (Estándar de seguridad de datos de la industria de tarjetas de pago), es un estándar relacionado con todos los tipos de negocios de comercio electrónico. Cualquier sitio web o compañía que acepte transacciones en línea debe ser verificada por PCI DSS. Hemos creado una lista de verificación de cumplimiento de PCI para ayudar.

PCI DSS fue desarrollado por el PCI SSC (Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago), cuyos miembros incluían compañías de tarjetas de crédito como Visa, Mastercard, American Express, etc. La idea clave detrás de su esfuerzo de colaboración para desarrollar esta norma fue ayudar a mejorar la Seguridad de la información financiera de los clientes.

PCI DSS 3.2 se actualizó recientemente. Se trata de una serie de actualizaciones para hacer frente a los pagos móviles. Al seguir el ritmo del cambio en la industria, PCI sigue siendo un estándar relevante para todas las empresas de comercio electrónico.

Consideraciones finales: Auditoría y cumplimiento del centro de datos

Los estándares de auditoría de seguridad del centro de datos continúan evolucionando.

Las revisiones y actualizaciones continuas les ayudan a seguir siendo relevantes y ofrecen información valiosa sobre el compromiso de la empresa con la seguridad. Es cierto que estas normas generan algunas preguntas de vez en cuando y no pueden proporcionar una garantía del 100% en la seguridad de la información.

Sin embargo, todavía ayudan a evaluar la credibilidad de un proveedor. Un proveedor de servicios de seguridad gestionada que hace un esfuerzo por cumplir con las regulaciones del gobierno es más probable que ofrecen protección de datos de calidad. Esto es particularmente importante para los proveedores de SaaS y IaaS. Sus plataformas y servicios se convierten en partes vitales de las operaciones de sus clientes y deben proporcionar seguridad avanzada.

Al elegir su proveedor de centro de datos, comprender estos

estándares puede ayudarlo a tomar una decisión más inteligente. Si no está seguro de cuál se aplica al centro de datos, siempre puede preguntar.

Compruebe si sus estándares coinciden con lo establecido por AICPA y otras organizaciones. Eso le dará tranquilidad sobre su elección y la seguridad de sus datos.

Leer también: Virtualización de un data center o centro de datos, ¿qué es?; Redes de centros de datos, que son, para que se usan; Data center services, servicios de centro de datos