Jose Juan Herrera Reyes

ISO 27017

La norma ISO 27017 introduce un conjunto de controles complementarios a la ISO 27002, orientados directamente a los servicios desplegados en la nube y a los proveedores que los proporcionan, proponiendo controles específicos vinculados con la gestión y provisión de servicios seguros en la nube.

Además, la implantación de la ISO 27017 proporciona a los proveedores de servicios en la nube una imagen de coherencia e implicación en la gestión de la seguridad de cara a sus clientes, y requiere disponer previamente de la norma ISO 27001. El objetivo principal es una gestión segura de los datos almacenados por parte de los clientes, aumentando la confianza en la gestión y tratamiento de la información.

ISO/IEC 27017 proporciona orientación sobre los aspectos de seguridad de la información de la informática en la nube y recomienda la implementación de controles de seguridad de la información específicos de la nube que complementan las directrices de las normas ISO/IEC 27002 e ISO/IEC 27001. Este código de conducta proporciona orientación sobre implementación de controles de seguridad de la información adicionales específica para proveedores de servicios de nube.

¿Qué implica la norma ISO 27017 como cliente?

La ratificación de la norma ISO/IEC 27017 por parte de AWS no solo demuestra nuestro compromiso constante de alinearnos con prácticas recomendadas globalmente reconocidas, sino que también verifica que AWS cuenta con un sistema con controles altamente precisos específicos para los servicios de nube.

La norma ISO/IEC 27017, junto con muchas otras normas económicas, medioambientales y sociales, está disponible en el sitio web de ISO.

ISO/IEC ha tomado la decisión de proteger estas normas con derechos de autor para ayudar a financiar los procesos dirigidos al desarrollo.

¿En qué se centra la norma ISO 27017 principalmente?

Esta norma se centra en la protección de los entornos de virtualización y la configuración de las máquinas virtuales alojadas en los mismos para la prestación de los servicios, así como del proceso de entrega y eliminación de información en el momento que un cliente rescinde su contrato con un proveedor de servicios en la nube. Del mismo modo, establece el marco de relación entre el cliente y prestador del servicio en la nube, en referencia a la gestión y administración de los servicios que el proveedor ofrece, con el objetivo de garantizar la protección de las dimensiones clave de la seguridad de la información como son, la confidencialidad, la integridad y la disponibilidad de la información.

Desde el punto de vista de las empresas que desean implantar o trasladar parte de sus sistemas y servicios a la nube, la ISO 27017 proporciona referencia clara en cuanto a controles y riesgos que deben ser evaluados y tratados adecuadamente, así como una visibilidad de los proveedores de servicios en la nube que mantienen una correcta alineación entre tecnología, gestión de riesgos y seguridad.

Para las empresas proveedoras de servicios en la nube proporciona una clara oportunidad de transmitir confianza y responsabilidad en los productos y servicios que ofrecen.

La norma ISO 27017 proporciona controles para proveedores y clientes de servicios en la nube. A diferencia de muchas otras normas relacionadas con la tecnología, la norma ISO 27017 aclara las funciones y las responsabilidades para ayudar a que los servicios en la nube sean tan seguros como el resto de los datos incluidos en un Sistema de Gestión de la Información certificado. La norma ISO 27017 proporciona una guía con 37 controles en la nube basados en ISO 27002. Además, ofrece siete nuevos controles en la nube que tratan los siguientes puntos:

- Quién es el responsable de lo que sucede entre el proveedor del servicio y cliente
- La eliminación de activos cuando un contrato se resuelve.
- Protección y separación del entorno virtual del cliente.

ISO 27018

La norma ISO 27018 es un código de prácticas diseñado para proteger datos personales en la nube. Se basa en la norma ISO/IEC de seguridad de la información 27002 y proporciona pautas de implementación sobre los controles IEC/IEC 27002 aplicables a la información personalmente identificable (PII) en la nube pública. Además, proporciona un conjunto de controles adicionales y asesoramiento relacionado a fin de satisfacer los requisitos de protección de la información personalmente identificable en la nube no cubiertos por el conjunto de controles existentes de la norma ISO/IEC 27002.

¿Qué nos propone específicamente ISO 27018?

La ISO 27018 pretende, a grandes rasgos, identificar de manera precisa como el proveedor gestiona los datos personales de los interesados, establece los procedimientos necesarios para cualquier solicitud o acceso a los mismos ofreciendo de este modo a los clientes una total transparencia en este sentido

La ISO 27018, aporta una base de buenas prácticas para la protección de información de identificación personal (PII) en la nube para organizaciones que actúan como procesadores de esta información".

Su implantación va ligada a la norma ISO 27001, que actúa como base a la hora de especificar los requisitos propios del estándar. En este sentido, la ISO 27018 se divide en dos grandes bloques de actuación:

Controles Declaración de Aplicabilidad: Partiendo de los controles de seguridad establecidos en el Anexo A de la ISO 27001 o el código de buenas prácticas ISO 27002, la norma añade requisitos de seguridad para la información de identificación personal (PII) sobre controles específicos. En este sentido, de los 114 controles que propone el estándar de Seguridad de la Información, la ISO 27018 establece requisitos adicionales sobre 15 controles, distribuidos entre los siguientes dominios:

- Dominio 5: Políticas de Seguridad de la Información

- Dominio 6: Organización de la Seguridad de la Información
- Dominio 7: Seguridad de los Recursos Humanos
- Dominio 9: Control de Acceso
- Dominio 10: Criptografía
- Dominio 11: Seguridad física y ambiental
- Dominio 12: Seguridad de las operaciones
- Dominio 13: Seguridad de las comunicaciones
- Dominio 16: Gestión de incidentes
- Dominio 18: Cumplimiento

¿Cuáles son los objetivos del sgsi de acuerdo con iso 27018?

- Permite la identificación de los riesgos y la aplicación de controles para su mitigación.
- Dar mayor seguridad a clientes y partes interesadas respecto a los datos y la protección datos
- Proteger la información y garantizar su seguridad

Beneficios

- Fácil integración con la norma ISO/IEC 27001 de Seguridad de la Información
- Minimizar los riesgos inherentes a la seguridad de los datos personales
- Generar confianza en los clientes asegurando la buena gestión de los datos confiados a su organización.
- Desarrollar una ventaja competitiva para la empresa.
- Mejorar la eficiencia de la organización.

¿A quién va dirigida esta norma?

Cualquier empresa, independientemente de su tamaño o de su actividad, que disponga de la Norma ISO 27001:2013 y cuyo ámbito principal de actividad esté relacionado con los servicios Cloud.

ISO 27036

La norma ISO 27036, está dividida en cuatro partes y es una de las normas perteneciente a la familia ISO 27000, referida a la Seguridad de la información para las relaciones con proveedores, ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios de proveedores.

ISO 27000, referida a la Seguridad de la información para las relaciones con proveedores, que ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios de proveedores.

¿Cómo está divida la norma?

La norma ISO/IEC 27036 está dividida en las siguientes cuatro partes:

1. ISO/IEC 27036-1:2014: Recoge la descripción general y los conceptos principales. Sirve de introducción a las cuatro partes de esta norma, dando información general de los antecedentes normativos (ISO 27000, TI – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción general y vocabulario), e introduciendo los términos y conceptos clave, incluidos los riesgos, en relación con la seguridad de la información en las relaciones con los proveedores.
2. ISO/IEC 27036-2:2014: Especifica los requisitos fundamentales de la seguridad de la información relativa a las relaciones comerciales entre proveedores y adquirientes. Las medidas de control recomendadas abarcan diversos aspectos de la gobernanza, la gestión empresarial y la gestión de la seguridad de la información

(habilitación de proyectos organizacionales, planificación de la relación con el proveedor, acuerdos de relación, gestión de relaciones con proveedores, etc.).

3. ISO/IEC 27036-3:2013: Proporciona las directrices para la seguridad de la cadena de suministro de las TIC. Recoge las pautas tanto para los proveedores como para los adquirientes sobre gestión de riesgos de seguridad de la información, relacionados con la cadena de suministro (malware, productos falsificados, riesgos organizativos, integración de la gestión de riesgos con los procesos del ciclo de vida del sistema y del software, etc).

4. ISO/IEC 27036-4:2016: Describe las directrices para la seguridad de los servicios en la nube. Proporciona a los clientes y proveedores de servicios en la nube orientación acerca de los riesgos de seguridad de la información asociados con el uso de servicios en la nube y la gestión eficaz de esos riesgos mediante la implantación de controles específicos para su mitigación.

¿Dónde se aplica la ISO 27036?

La norma se aplica a las relaciones comerciales entre compradores y proveedores de diversos bienes y servicios, tales como:

- Suministro de hardware, software y servicios TIC, incluidos los servicios de telecomunicaciones e Internet.
- Externalización de servicios de computación en la nube.
- Otros servicios como guardias de seguridad, limpiadores, mensajería, mantenimiento de equipos, servicios de consultoría y asesoramiento especializado, etc.
- Productos y servicios a medida donde el adquirente especifica los requisitos y normalmente tiene un papel activo en el diseño del producto.
- Servicios públicos como energía eléctrica, combustibles y agua.

Noma ISO/IEC 17788:2014

La norma ISO/IEC 17788:2014 proporciona una visión general de la computación en la nube en conjunto con una serie de términos y definiciones. Esta norma es una terminología base para los estándares de computación en la nube.

La computación en la nube es un paradigma para permitir el acceso a la red a un conjunto escalable y elástico de recursos físicos o virtuales compartibles con aprovisionamiento de autoservicio y administración bajo demanda. El servicio en la nube se refiere a una o más capacidades ofrecidas a través de la computación en la nube invocadas mediante una interfaz definida.

Las características clave de la computación en la nube son:

Acceso amplio a la red. El enfoque de esta característica clave es que la computación en la nube ofrece un mayor nivel de conveniencia en el sentido de que los usuarios pueden acceder a los recursos físicos y virtuales desde cualquier lugar donde necesiten trabajar, siempre que sea accesible en red, utilizando una amplia variedad de clientes, incluidos dispositivos como teléfonos móviles, tabletas, computadoras portátiles y estaciones de trabajo.

Servicio medido. Una característica en la que la entrega medida de los servicios en la nube es tal que el uso se puede monitorear, controlar, informar y facturar. El enfoque de esta característica clave es que el cliente solo puede pagar por los recursos que utiliza.

Tenencia múltiple. Una función en la que los recursos físicos o virtuales se asignan de tal manera que los múltiples inquilinos y sus cálculos y datos están aislados y son inaccesibles entre sí.

Autoservicio a pedido. Una función en la que un cliente de servicios en la nube puede proporcionar capacidades informáticas, según sea necesario, automáticamente o con una interacción mínima con el proveedor de servicios en la nube. El enfoque de esta característica clave es que la computación en la nube ofrece a los usuarios una

reducción relativa en los costos, el tiempo y el esfuerzo necesarios para realizar una acción, ya que otorga al usuario la capacidad de hacer lo que necesita, cuando lo necesita, sin requerir recursos humanos adicionales, interacciones del usuario o gastos generales.

Elasticidad y escalabilidad rápidas. Una función en la que los recursos físicos o virtuales se pueden ajustar rápida y elásticamente, en algunos casos automáticamente, para aumentar o disminuir los recursos rápidamente. El enfoque de esta característica clave es que la computación en la nube significa que los clientes ya no necesitan preocuparse por los recursos limitados y es posible que no tengan que preocuparse por la planificación de la capacidad.

Agrupación de recursos. Una función en la que los recursos físicos o virtuales de un proveedor de servicios en la nube se pueden agregar para atender a uno o más clientes de servicios en la nube. El enfoque de esta característica clave es que los proveedores de servicios en la nube pueden admitir múltiples inquilinos y, al mismo tiempo, usar la abstracción para enmascarar la complejidad del proceso del cliente. Desde la perspectiva del cliente, todo lo que saben es que el servicio funciona, mientras que generalmente no tienen control ni conocimiento sobre cómo se proporcionan los recursos o dónde se encuentran los recursos.

Beneficios

Brinda una terminología base para comprender la computación en la nube y una visión general del tema, útil tanto para proveedores relacionados a computación en la nube como para los clientes de estos.

Público objetivo

Empresas u organizaciones de cualquier tipo, tamaño, sector o rubro que este proyectando, implementando, adquiriendo, evaluando o relacionada con computación en la nube tanto como proveedor o como cliente.

Valor global

Brinda claridad en los aspectos relacionados a la computación en la nube, en un entorno cambiante y donde hace falta un entendimiento común sobre la diversidad de ofertas y tendencias que se relacionan con esto.

Bibliografia

Alonso, C. (2022). ISO 27036 – Seguridad de la información para las relaciones con los proveedores. Retrieved 30 May 2022, from https://www.globalsuitesolutions.com/es/que-es-iso-27036-relaciones-proveedores

ISO 27018:2020 - Protección de la Información de Identificación Personal (PII) en la nube en calidad de procesadores PII. (2022). Retrieved 30 May 2022, from https://www.appluscertification.com/global/es/what-we-do/service-sheet/iso-27018-2020-proteccion-informacion-personal

Martin, D. (2021). ¿Qué es la ISO 27017 – controles de seguridad para servicios cloud?. Retrieved 30 May 2022, from https://www.globalsuitesolutions.com/es/que-es-iso-27017/

Wu, W. (2022). Cloud Computing by ISO/IEC 17788:2014 by Wentz Wu, CISSP/ISSMP/ISSAP/ISSEP,CCSP,CSSLP,CISM,PMP,CBAP. Retrieved 30 May 2022, from https://wentzwu.com/2022/02/03/cloud-computing-by-iso-iec-177882014/