EDUCACIÓN CON RESPONSABILIDAD SOCIAL

UNIVERSIDAD DE COLIMA

INGENIERÍA EN COMPUTACIÓN INTELIGENTE

Facultad de Ingeniería Mecánica y Eléctrica

Materia: Computo en la nube

Profesor: Oswaldo Carillo Zepeda

Alumno: Dante Villanueva López

Semestre: 6

Grupo: B

Actividad. Normas ISO

ISO 27017

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 el cliente
- La eliminación de activos cuando un contrato se resuelve
- Protección y separación del entorno virtual del cliente
- Configurar una máquina virtual
- Operaciones y procedimientos administrativos relacionados con el entorno en la nube
- Seguimiento de la actividad de clientes en la nube
- Alineación del entorno de la red virtual y en la nube

Si trabaja para un proveedor de servicios en la nube o está buscando trasladar su negocio en la nube, es importante que conozca cómo funciona la norma ISO 27017. Para ayudarle a entender las áreas principales de la norma, es necesario conocer más sobre los siete nuevos controles, y como las empresas se pueden beneficiar.

¿Cómo se beneficiará un proveedor de servicios en la nube de la certificación ISO 27017?

- Inspira confianza en su negocio: proporciona una mayor seguridad a clientes y partes interesadas de que los datos y la información sean protegidos.
- Ventaja competitiva: demuestra que existen sistemas de control sólidos para proteger sus datos puestos en marcha.
- Protege su reputación de marca: reduce el riesgo de publicidad negativa debido a las violaciones de datos.
- Protege contra las multas: garantiza que las normas locales se cumplan, lo cual implica una reducción del riesgo de multas por violaciones de datos.
- Ayuda a crecer a su negocio: proporciona pautas comunes en diferentes países, que facilita el hacer negocios a nivel mundial y acceder como "proveedor preferente".

¿Cómo se benefician los clientes de servicios en la nube de la formación en ISO 27017?

La norma ISO 27017 es una norma de tecnología única, ya que proporciona tanto los requisitos para el cliente como para el proveedor del servicio en la nube. Los gerentes de TI del departamento técnico responsables de mover a las empresas a la nube o de la ampliación de un contrato de servicio en la nube, puede reducir los riesgos de su negocio asegurándose de que entienden sus responsabilidades y toman las mejores decisiones en torno a su elección de proveedor.

La norma ISO 27017, relativa a la seguridad de los servicios en la nube, es un código de conducta coherente con la norma ISO 27002. Sirve de complemento a esta última norma y establece buenas prácticas de seguridad en el marco de los servicios en la nube. Se especifican las posibles consideraciones relativas a estos servicios en la nube. Aunque los expertos en seguridad y calidad pueden adoptar la norma rápidamente.

La norma ISO 27017 no solo se centra en los proveedores de servicios en la nube, sino también en la seguridad del conjunto de estos servicios. También se tiene en cuenta el punto de vista del cliente. Dichas exigencias adicionales permiten estandarizar todas las relaciones entre el cliente y el proveedor de servicios en la nube.

ISO 27018

La nube ofrece a las empresas y a los consumidores múltiples beneficios: el ahorro de costes, la flexibilidad y el acceso móvil a la información encabezan la lista. Sin embargo, por otro lado, plantea preocupaciones sobre la protección de datos y la privacidad; especialmente en torno a la información de identificación personal (PII). PII incluye cualquier tipo de información que pueda identificar a un usuario específico. Los ejemplos más obvios son los nombres y datos de contacto. Pero también se puede pensar fácilmente en registros médicos, las direcciones IP y los estados bancarios.

Utilizada conjuntamente con ISO/IEC 27001, ISO/IEC 27018 ha sido publicada para permitir que proveedores de servicios cloud cuya infraestructura está certificada con esta norma, le puedan decir a sus clientes actuales y potenciales que sus datos están garantizados y que no serán usados para ningún propósito para el cual no se dé expresamente su consentimiento.

¿Cuáles son los beneficios de la norma ISO/IEC 27018?

- Inspira confianza en su negocio: da una mayor seguridad a clientes y partes interesadas de que los datos y la información está protegida
- Ventaja competitiva - permite diferenciarse de sus competidores mediante la protección de la información personal al más alto nivel
- Protege su reputación de marca - reduce el riesgo de publicidad negativa debido a las violaciones de datos
- Reduce los riesgos - garantiza la identificación de los riesgos y la aplicación de controles para su gestión o posible reducción
- Protege contra las multas - garantiza que las normas locales se cumplan, lo cual implica una reducción del riesgo de multas por violaciones de datos
- Ayuda a crecer a su negocio - proporciona una guía común en diferentes países por lo que es más fácil hacer negocios a nivel mundial y obtener acceso como un proveedor preferido

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

ISO 27036

La ISO 27000 es una serie de normas de seguridad de la información desarrolladas y publicadas por la Organización Internacional de Normalización (ISO), que proporciona un marco reconocido mundialmente para las mejores prácticas en el desarrollo del Sistema de Gestión de Seguridad de la información (SGSI).

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.

¿Cómo está divida la norma?

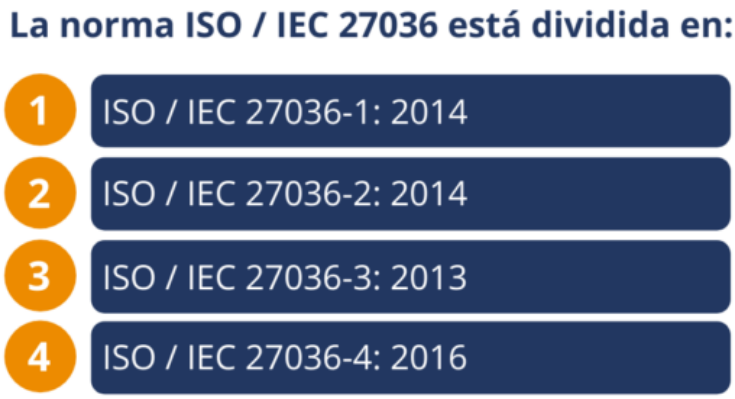
La norma ISO/IEC 27036 está dividida en las siguientes cuatro partes:

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.

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.