Institución: Universidad de Colima

Escuela: Facultad de Ingeniería Mecánica y Eléctrica

Carrera: Ingeniería en Computación Inteligente

Materia: Cómputo en la Nube

Profesor: Carrillo Zepeda Oswaldo

Alumno: Herrera Escareño Kevin Alejandro

Grado y grupo: 6°B

Nombre de la actividad: Normas ISO

Fecha: 29 de Mayo de 2022

Lugar: Colima, Col.

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. La ISO 27001 define un conjunto de 114 controles de seguridad estructurados en 14 dominios, que son aplicados dentro del alcance que cada compañía establezca en la implantación de su Sistema de Gestión de la Seguridad de la Información.

En relación con la gestión de riesgos, se establecen referencias para la identificación y mitigación de riesgos específicos vinculados a los entornos en la nube, de forma que puedan ser tratados de la forma adecuada. 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.

¿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.

¿Qué implicaciones tiene?

Integrar las normas en un Sistema de Gestión de Seguridad de la Información según ISO 27001 implica:

- Identificar amenazas específicas para servicios en la nube y definir acciones para su tratamiento.
- Cumplir con el Reglamento General de Protección de Datos y demás normativa aplicable en la materia.
- Implantar controles de seguridad adicionales y específicos para servicios en la nube.
- Ofrecer a los clientes una información clara sobre los niveles de protección de los servicios.

Ventajas de su aplicación

- Mejorar la seguridad de la información en los servicios en la nube.
- Aumento de la transparencia en las relaciones con clientes.
- Garantizar el cumplimiento de la legislación vigente y las normas y regulaciones internacionales.
- Optimizar los recursos asignados a la seguridad de la información.

Servicios que cumplen la norma

Entre los servicios de Cloud Computing que satisfacen la norma ISO/IEC 27017 es posible destacar, entre otros:

- Microsoft Azure y Microsoft Intune
- Office 365
- Google Cloud Platform
- Amazon Web Services

ISO 27018

La norma ISO 27018 fue publicada el 29 de julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube. La norma se complementa con la norma ISO 27001 e ISO 27002 en el ámbito de gestión de la seguridad de la información y que se dirige de forma específica a los proveedores de servicios de nube.

¿Qué 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, establecer 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 cuenta con un gran bloque 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

¿Qué define el Anexo A de la norma ISO 27018?

Los 8 principios o controles específicos de privacidad de la información, aplicables al gestor de datos en la nube y el modo de implantarlos, lo que conforma un conjunto de requisitos para la protección de PII. Los principios en los que se basa son los siguientes:

- Consentimiento y elección
- Propósito de legitimidad y especificación
- Minimización de los datos
- Límite de uso, retención y divulgación
- Apertura, trasparencia y notificación
- Responsabilidad
- Seguridad de la Información
- Cumplimiento de la privacidad

Beneficios de su aplicación

La implantación del estándar conlleva grandes beneficios a los operadores de datos en la nube, más si cabe con la certificación del estándar ISO 27018, el cual solo es certificable de manera conjunta con la ISO 27001. Entre los beneficios podemos destacar:

- Aporta confianza sobre la protección de la información de los clientes y partes interesadas, protegiendo la imagen de la organización frente a accesos o violación de datos.
- Permite identificar los riesgos a los que está expuesta la información (PII) estableciendo controles para su mitigación.
- Diferenciación respecto a los competidores del mismo sector, proveyendo una protección a la información bajo un estándar internacional.
- Protección frente a multan, aportando un sistema de gestión que vela por la protección de la información de los interesados.

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.

Organización y usos de la ISO 27036

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.

Riesgos en la seguridad de la información:

Las situaciones donde se ve comprometida la seguridad de la información se clasifican en:

- Dependencia del adquirente de los proveedores.
- Acceso y protección de activos de información de terceros.
- Coordinación adquirente-proveedor para adaptar o responder a los nuevos requisitos de seguridad de la información.

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.

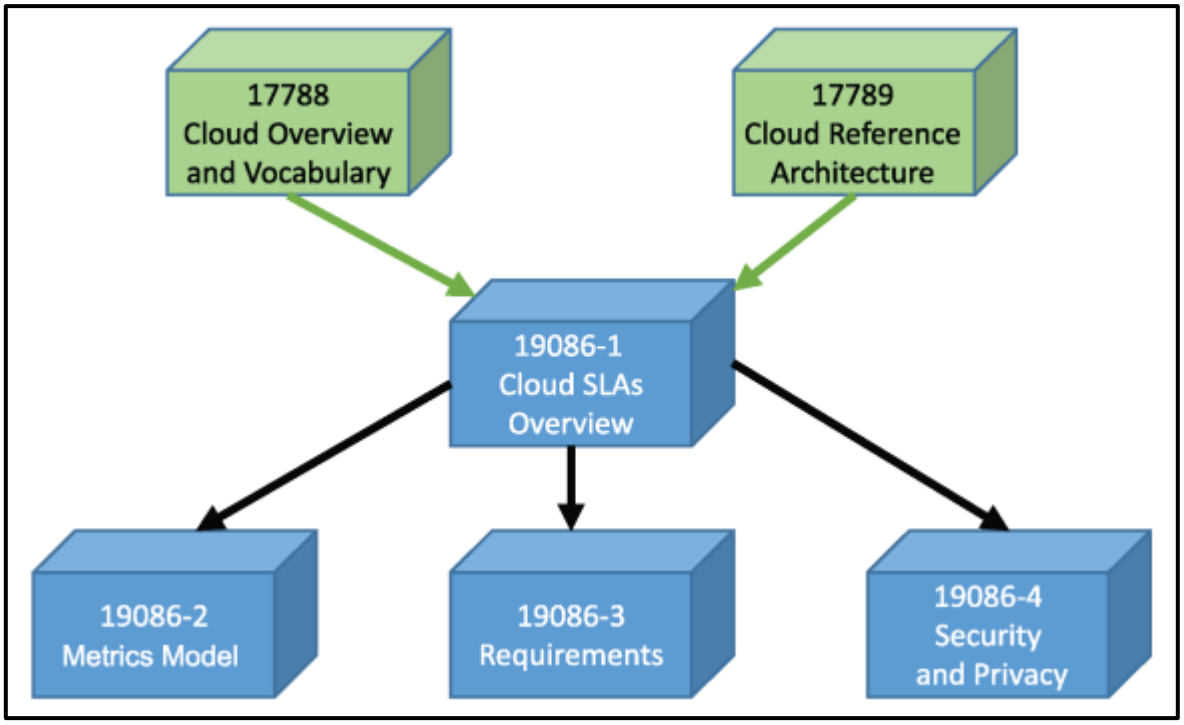

Figura 1. Estándares de computación en la nube.

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.

Bibliografía

Alonso, C. (2021, 3 mayo). ISO 27036 – Seguridad de la información para las relaciones con los proveedores. GlobalSuite Solutions. Recuperado 29 de mayo de 2022, de https://www.globalsuitesolutions.com/es/que-es-iso-27036-relaciones-proveedores/.

Martín, D. (2021, 13 octubre). ISO 27017 e ISO 27018. Cohaerentis. Recuperado 29 de mayo de 2022, de https://cohaerentis.com/servicios/seguridad-de-la-informacion/iso-27017-e-iso-27018/.

Ortega, A. (2020, 6 marzo). ISO 27018. Seguridad y Protección de Información Personal en la nube. GlobalSuite Solutions. Recuperado 29 de mayo de 2022, de https://www.globalsuitesolutions.com/es/que-es-iso-27018/.

Wu, W. (2022, 3 febrero). Cloud Computing by ISO/IEC 17788:2014 by Wentz Wu, CISSP/ISSMP/ISSAP/ISSEP,CCSP,CSSLP,CISM,PMP,CBAP. Wentz Wu. Recuperado 29 de mayo de 2022, de https://wentzwu.com/2022/02/03/cloud-computing-by-iso-iec-177882014/.