Facultad de Ingeniería Mecánica y Eléctrica

Ingeniería en Computación Inteligente

Materia: Computo en la nube

Profesor: Oswaldo Carrillo Zepeda
Alumno: Jazmín Azucena González Peredia

6to semestre.
Grupo B.

Investigación sobre las normas ISO que existen para computo en la nube.

26 de mayo de 2022.

Normas ISO.

Norma 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

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.

La norma ISO 27001 expone la importancia de la comunicación entre una empresa y sus clientes a la hora de definir ciertos procesos de gestión de seguridad adaptados. La norma ISO 27001 es generalista, pues se aplica a cualquier tipo de entidad. Sin embargo, la norma ISO 27017 enmarca con precisión las relaciones entre el cliente y el proveedor de servicios en la nube. La norma establece que es lo que el cliente debe exigirle a un proveedor y qué información debe proporcionar este último. Una relación entre cliente y proveedor conforme con la ISO 27017 garantiza que se tengan en cuenta todos los aspectos clave de la seguridad durante la gestión del servicio.

El proveedor de servicios en la nube debe proporcionar información a los clientes sobre la arquitectura, la tecnología utilizada, las medidas de seguridad adoptadas y las funcionalidades disponibles. El proveedor también debe establecer el lugar que ocupa para el cliente en estos procedimientos operativos y en la gestión de modificaciones, actualizaciones o incidentes. De forma general, la norma incide en la importancia de definir de forma clara el papel y las responsabilidades del cliente y el proveedor en materia de seguridad.

La norma ISO 27001 permite estandarizar las relaciones entre los clientes y los proveedores de servicios en la nube mediante un modelo de análisis e intercambio común, facilitando la gestión.

Norma 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:

- 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

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.

Ámbito de aplicación y objetivo.

La norma pretende ser “una referencia para la selección de los controles de protección información de carácter personal en el proceso de implementación de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001 para un sistema cloud, o como un documento de orientación para las organizaciones para la implementación de los controles de protección de PII comúnmente aceptados”.

Aportaciones de la nueva norma.

El estándar ISO 27018 se alinea de modo muy directo con el modelo europeo de protección de datos personales y ofrece confianza al mercado para los proveedores que lo implanten.

En esta norma podemos apreciar con claridad la identidad de objetivos de los controles del estándar ISO con las normativas vigentes y con los objetivos que incorpora la Propuesta de Reglamento General de Protección de Datos actualmente en tramitación.

Por otra parte, en el desarrollo del estándar ISO 27018 se incluye no sólo una revisión de buenas prácticas en materia de tratamiento de información en Cloud a nivel internacional sino que adicionalmente se recogieron los contenidos del “Dictamen sobre Cloud Computing” publicado por el Grupo de Trabajo del artículo 29 de la Directiva.

Norma ISO 27036.

La norma ISO 27036, esta 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.

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

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.

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.).

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).

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.

El **ciclo de vida de la ISO 27036** se compone de varias fases:

- Análisis de coste-beneficio, comparación de opciones de desarrollo interno o externalización, o mezcla de ambos.

- Definición de requisitos.
- Selección, evaluación y contratación con los proveedores.
- Aplicación de los acuerdos de suministro.
- Operación: gestión y supervisión de relaciones, cumplimiento, incidentes y cambios, etc.
- Actualización en la posible renovación del contrato, con la revisión de términos y condiciones, rendimiento, problemas, procesos de trabajo, etc.
- Fin de la relación comercial.

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. ISO/IEC 17788:2014 especifica la “Arquitectura de Referencia de la Computación en Nube” (CCRA – Cloud Computing Reference Architecture”). Dicha arquitectura de referencia incluye las funciones, las actividades, y los componentes funcionales de cloud computing y sus relaciones. Algo que es de resaltar es que en estos estándares se muestra una nueva definición y unos modelos de implementación no necesariamente iguales a los comúnmente aceptados bajo la descripción de NIST.

La siguiente informacion es un extracto de ISO/IEC 17788:2014.

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 de la computación en la nube son:

Acceso amplio a la red: una función en la que los recursos físicos y virtuales están disponibles a través de una red y se accede a ellos a través de mecanismos estándar que promueven el uso por parte de plataformas de clientes heterogéneas. 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. Esta es una característica importante necesaria para optimizar y validar el servicio en la nube entregado. El enfoque de esta característica clave es que el cliente solo puede pagar por los recursos que utiliza. Desde la perspectiva de los clientes, la computación en la nube ofrece valor a los usuarios al permitirles pasar de un modelo comercial de baja eficiencia y utilización de activos a uno de alta eficiencia;

Multiusuario : una función en la que los recursos físicos o virtuales se asignan de tal manera que varios usuarios y sus cálculos y datos están aislados y son inaccesibles entre sí. Por lo general, y dentro del contexto de la tenencia múltiple, el grupo de usuarios de servicios en la nube que forman un arrendatario pertenecerá a la misma organización de clientes del servicio en la nube. Puede haber casos en los que el grupo de usuarios del servicio en la nube involucre a usuarios de múltiples clientes de servicios en la nube diferentes, particularmente en el caso de implementaciones de nube pública y nube comunitaria. Sin embargo, una determinada organización de clientes de servicios en la nube puede tener muchos arrendamientos diferentes con un solo proveedor de servicios en la nube que represente a diferentes grupos dentro de la organización;

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 característica en la que los recursos físicos o virtuales se pueden ajustar rápida y elásticamente, en algunos casos automáticamente, para aumentar o disminuir rápidamente los recursos. Para el cliente del servicio en la nube, los recursos físicos o virtuales disponibles para el aprovisionamiento a menudo parecen ser ilimitados y se pueden comprar en cualquier cantidad y en cualquier momento automáticamente, sujeto a las restricciones de los acuerdos de servicio. Por lo tanto, 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. Esto descarga parte de la carga de trabajo original del cliente, como los requisitos de mantenimiento, al proveedor. Incluso con este nivel de abstracción, se debe señalar que los usuarios aún pueden especificar la ubicación en un nivel más alto de abstracción (p. ej., país, estado o centro de datos).

Aspectos transversales de la computación en la nube.

Los aspectos transversales son comportamientos o capacidades que deben coordinarse entre roles e implementarse de manera consistente en un sistema de computación en la nube. Dichos aspectos pueden afectar múltiples roles, actividades y componentes, de tal manera que no es posible asignarlos claramente a roles o componentes individuales y, por lo tanto, convertirse en problemas compartidos entre los roles, actividades y componentes.

Los aspectos transversales clave incluyen:

Auditabilidad : la capacidad de recopilar y poner a disposición la información probatoria necesaria relacionada con la operación y el uso de un servicio en la nube, con el fin de realizar una auditoría;

Disponibilidad : La propiedad de ser accesible y utilizable a pedido de una entidad autorizada. La "entidad autorizada" suele ser un cliente de servicios en la nube;

Gobernanza : el sistema mediante el cual se dirige y controla la provisión y el uso de los servicios en la nube. El gobierno de la nube se cita como un aspecto transversal debido al requisito de transparencia y la necesidad de racionalizar las prácticas de gobierno con SLA y otros elementos contractuales de la relación entre el cliente del servicio de nube y el proveedor del servicio de nube. El término gobernanza interna de la nube se utiliza para la aplicación de políticas de tiempo de diseño y tiempo de ejecución para garantizar que las soluciones basadas en la computación en la nube se diseñen e implementen, y que los servicios basados en la computación en la nube se brinden, de acuerdo con las expectativas especificadas. El término gobernanza de la nube externa se utiliza para algún tipo de acuerdo entre la nube cliente del servicio y el proveedor de servicios en la nube en relación con el uso de los servicios en la nube por parte del cliente del servicio en la nube;

Interoperabilidad : capacidad de un cliente de servicios en la nube para interactuar con un servicio en la nube e intercambiar información de acuerdo con un método prescrito y obtener resultados predecibles;

Mantenimiento y control de versiones : el mantenimiento se refiere a los cambios en un servicio en la nube o los recursos que utiliza.

para corregir fallas o para actualizar o ampliar las capacidades por motivos comerciales. El control de versiones implica el etiquetado apropiado de un servicio para que quede claro para el cliente del servicio en la nube que una versión particular está en uso;

Rendimiento : un conjunto de comportamientos relacionados con la operación de un servicio en la nube y que tiene métricas definidas en un SLA;

Portabilidad : capacidad de los clientes de servicios en la nube para mover sus datos o sus aplicaciones entre múltiples proveedores de servicios en la nube a bajo costo y con una interrupción mínima. La cantidad de costo e interrupción que es aceptable puede variar según el tipo de servicio en la nube que se utilice;

Protección de PII : Proteger la recopilación, el procesamiento, la comunicación, el uso y la eliminación seguros, adecuados y coherentes de la información de identificación personal (PII) en relación con los servicios en la nube;

Normativa : existe una serie de normas diferentes que pueden influir en el uso y la prestación de servicios en la nube. Los requisitos legales, reglamentarios y legales varían según el sector del mercado y la jurisdicción, y pueden cambiar las responsabilidades tanto de los clientes de servicios en la nube como de los proveedores de servicios en la nube. El cumplimiento de tales requisitos a menudo está relacionado con las actividades de gobierno y gestión de riesgos;

Resiliencia : Capacidad de un sistema para proporcionar y mantener un nivel aceptable de servicio frente a fallas (involuntarias, intencionales o causadas naturalmente) que afectan el funcionamiento normal;

Reversibilidad : un proceso para que el cliente del servicio en la nube recupere los datos del cliente del servicio en la nube y los artefactos de la aplicación y para que el proveedor del servicio en la nube elimine todos los datos del cliente del servicio en la nube, así como los datos derivados del servicio en la nube especificados contractualmente después de un período acordado;

Seguridad : va desde la seguridad física hasta la seguridad de las aplicaciones e incluye requisitos como la autenticación, la autorización, la disponibilidad, la confidencialidad, la gestión de identidades, la integridad, el no repudio, la auditoría, la supervisión de la seguridad, la respuesta a incidentes y la gestión de políticas de seguridad;

Niveles de servicio y acuerdo de nivel de servicio : El acuerdo de nivel de servicio de computación en la nube (Cloud SLA) es un acuerdo de nivel de servicio entre un proveedor de servicios en la nube y un cliente de servicios en la nube basado en una taxonomía de términos específicos de computación en la nube para establecer la calidad de los servicios en la nube entregados. . Caracteriza la calidad de los servicios en la nube entregados en

términos de: 1) un conjunto de propiedades medibles específicas de la computación en la nube (comerciales y técnicas) y 2) un conjunto determinado de roles de la computación en la nube (cliente del servicio en la nube y proveedor del servicio en la nube y subcontratistas relacionados). papeles).

Bibliografía.

Alonso, C. (2022, 24 mayo). *ISO 27036 – Seguridad de la información para las relaciones con los proveedores*. GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-iso-27036-relaciones-proveedores/

Martín, D. (2022, 24 mayo). *¿Qué es la ISO 27017 – controles de seguridad para servicios cloud?* GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-iso-27017/

Normas ISO. (2017, 24 noviembre). *ISO / IEC 27018 Protección de la información de identificación personal*. https://www.normas-iso.com/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal/

Ortega, A. (2022, 24 mayo). *ISO 27018. Seguridad y Protección de Información Personal en la nube*. GlobalSuite Solutions. 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. https://wentzwu.com/2022/02/03/cloud-computing-by-iso-iec-177882014/