UNIVERSIDAD DE COLIMA
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA
Ingeniería en Computación Inteligente

Normas ISO

Profesor: Carrillo Zepeda Oswaldo.
Alumno: Guerrero Gómez Brandon Yair.

6° B

Fecha de entrega: Domingo, 29 de mayo de 2022

ISO 27017

ISO / IEC 27017:2015 / UIT-T X.1631 — Tecnología de la información — Técnicas de seguridad — Repertorio de recomendaciones prácticas para los controles de seguridad de la información basado en ISO / IEC 27002 para servicios en la nube.

Abstracto

ISO / IEC 27017:2015 proporciona directrices para los controles de seguridad de la información aplicables a la prestación y el uso de servicios en la nube al proporcionar: orientación de implementación adicional para los controles relevantes especificados en ISO / IEC 27002; controles adicionales con orientación de implementación que se relacionan específicamente con los servicios en la nube. Esta Recomendación International Standard proporciona controles y orientación de implementación tanto para los proveedores de servicios en la nube como para los clientes de servicios en la nube.
[Fuente: ISO / IEC 27017:2015 / ITU-T X.1631]

Introducción

Esta norma proporciona orientación sobre los aspectos de seguridad de la información de la computación en la nube, recomendando y ayudando con la implementación de controles de seguridad de la información específicos de la nube que complementan la orientación de ISO / IEC 27002:2013 y otras normas ISO27k.

Alcance y finalidad

El código de prácticas proporciona consejos adicionales de implementación de controles de seguridad de la información más allá de los proporcionados en ISO / IEC 27002:2013, en el contexto de la computación en la nube.

El estándar asesora tanto a los clientes de servicios en la nube como a los proveedores de servicios en la nube, con la guía principal presentada una al lado de la otra en cada sección. Por ejemplo, la sección 6.1.1 sobre funciones y responsabilidades de seguridad de la información dice, además de la sección 6.1.1 de ISO / IEC 27002:2013:

- **Cliente de servicio en la nube**: El cliente del servicio en la nube debe acordar con el proveedor de servicios en la nube una asignación adecuada de las funciones y responsabilidades de seguridad de la información, y confirmar que puede cumplir con las funciones y responsabilidades asignadas. Las funciones y responsabilidades de seguridad de la información de ambas partes deben indicarse en un acuerdo. El cliente del servicio en la nube debe identificar y gestionar su relación con la función de atención y atención al cliente del proveedor de servicios en la nube.
- **Proveedor de servicios en la nube**: El proveedor de servicios en la nube debe acordar y documentar una asignación adecuada de las funciones y responsabilidades de seguridad de la información con sus clientes de

servicios en la nube, sus proveedores de servicios en la nube y sus proveedores.

Normas normativas

La norma cita ISO / IEC 27000 y 27002:2013, por supuesto, además de ISO / IEC 17788 (Computación en la nube - Descripción general y vocabulario) e ISO / IEC 17789 (Computación en la nube - Arquitectura de referencia). Curiosamente, aunque ISO / IEC 27001 se anota en la bibliografía, no se considera 'normativa', es decir, lectura esencial: aunque inusual, es posible hacer uso de los controles recomendados por ISO / IEC 27002 sin tener también un SGSI.

Situación de la norma

La norma fue desarrollada conjuntamente por ISO / IEC y la UIT y, por lo tanto, tiene un doble numerado como ISO / IEC 27017 y UIT-T X.1631 con contenido idéntico. La primera edición se publicó a finales de 2015.

Se está redactando una segunda edición. Se actualizará para "capturar un conjunto completo de orientación para los controles de seguridad de la información aplicables a los servicios en la nube, tanto de la 3ª edición de ISO / IEC 27002 como de cualquier control adicional específico relacionado específicamente con los servicios en la nube". El SC 27 y el UIT-T colaboran una vez más en este sentido.

ISO 27018

ISO / IEC 27018:2019 — Tecnología de la información — Técnicas de seguridad — Código de buenas prácticas para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII

Abstracto

Este documento establece objetivos de control, controles y pautas comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) en línea con los principios de privacidad en ISO / IEC 29100 para el entorno de computación en la nube pública. En particular, este documento especifica directrices basadas en ISO / IEC 27002, teniendo en cuenta los requisitos reglamentarios para la protección de la PII que pueden ser aplicables en el contexto de los entornos de riesgo para la seguridad de la información de un proveedor de servicios de nube pública. Este documento es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que brindan servicios de procesamiento de información como procesadores de PII a través de la computación en la nube bajo contrato con otras organizaciones. Las directrices de este documento también pueden ser relevantes para las organizaciones que actúan como controladores de PII. Sin embargo, los controladores de PII pueden estar sujetos a legislación, regulaciones y obligaciones adicionales de protección de PII, que no se aplican a los procesadores de PII. Este documento no pretende cubrir tales obligaciones adicionales.
[Fuente: ISO / IEC 27018:2019]

Introducción

Esta norma proporciona orientaciones destinadas a garantizar que los proveedores de servicios en la nube (como Amazon y Google) ofrezcan controles de seguridad de la información adecuados para proteger la privacidad de los clientes de sus clientes mediante la seguridad de la formación de los clientes que seles confía.

Consulte también ISO / IEC 27017 que cubre los ángulos más amplios de seguridad de la información de la computación en la nube, aparte de la privacidad.

El proyecto de elaboración de normas contó con un amplio apoyo de los organismos nacionales de normalización, además de la seguridad de Cloud S.

Alcance y finalidad

La norma pretende ser "una referencia para seleccionar controles de protección de PII dentro del proceso de implementación de un sistema de gestión de seguridad de la información de computación en la nube basado en ISO / IEC 27001, o como

un documento de orientación para organizaciones para implementar controles de protección de PII comúnmente aceptados" [citado de la versión DIS].

El estándar se refiere principalmente a los proveedores de servicios de computación en la nube pública que actúan como procesadores de PII. "Un proveedor de servicios de nube pública es un 'procesador de PII' cuando procesa PII para y de acuerdo con las instrucciones de un cliente de servicio en la nube" [de la versión DIS]. No cubre oficialmente los principales de PII (es decir, las personas que procesan su propia PII en la nube, por ejemplo, utilizando Google Drive) o los controladores de PII (es decir, los clientes de servicios en la nube que procesan la PII de sus clientes / clientes / empleados y otros en la nube), aunque claramente comparten muchas preocupaciones y tienen interés en los controles de privacidad del proveedor de servicios en la nube.

La norma interpreta en lugar de duplicar ISO / IEC 27002 en el contexto de la protección de los datos personales procesados en la nube. Un anexo amplía 27002, por ejemplo, aconsejando a los proveedores de servicios en la nube que asesoren a sus clientes si utilizan subcontratistas.

ISO / IEC 27000, 27001 y 27002 se citan como estándares "normativos" (es decir, esenciales), junto con ISO / IEC 17788 "Computación en la nube - descripción general y vocabulario" e ISO / IEC 29100 "Marco de privacidad".

Situación de la norma

La primera edición se publicó en 2014.
La segunda edición (una revisión menor) se publicó en 2019.

Comentarios personales

El estándar se basa en ISO / IEC 27002, ampliando el asesoramiento genérico de 27002 en algunas áreas y refiriéndose a los principios de privacidad de la OCDE que están consagrados en varias leyes y regulaciones de privacidad.

ISO 27036

ISO / IEC 27036:2013 — Tecnología de la información — Técnicas de seguridad — Seguridad de la información para las relaciones con los proveedores (cuatro partes)

Introducción

ISO / IEC 27036 es un estándar de múltiples partes que ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios de proveedores. El contexto implícito son las relaciones de empresa a empresa, en lugar de la venta al por menor, y los productos relacionados con la información.

Los términos adquisición y adquirente se utilizan en lugar de compra y compra, ya que el proceso, los riesgos de información y los controles son muy similares, ya sea que las transacciones sean comerciales o no (por ejemplo, una parte de una organización o grupo que adquiere productos de otra).

Alcance y finalidad

Al ser un estándar de seguridad de la información, los productos más obviamente cubiertos por los estándares incluyen:

- Servicios de externalización de TI y computación en la nube;
- Otros servicios profesionales, por ejemplo, servicios legales, contables/fiscales y de recursos humanos, guardias de seguridad, limpiadores, servicios de entrega (mensajeros), mantenimiento / servicio de equipos, servicios de consultoría y asesoramiento especializado, gestión del conocimiento, investigación y desarrollo, fabricación, logística, custodia del código fuente y atención médica;
- Suministro de equipo, programas informáticos y servicios de TIC, incluidos los servicios de telecomunicaciones e Internet;
- Productos y servicios a medida en los que el adquirente especifica los requisitos y, a menudo, desempeña un papel activo en el diseño del producto (a diferencia de los productos básicos y los productos estándar disponibles);
- Servicios públicos como la energía eléctrica y el agua.

Las normas podrían referirse a:

- Metas estratégicas, objetivos, necesidades empresariales y obligaciones de cumplimiento en relación con la seguridad y el aseguramiento de la información al adquirir productos relacionados con las TIC o la información;
- Riesgos de información tales como:
  - La dependencia del adquirente de los proveedores, lo que complica los acuerdos de continuidad del negocio del adquirente (tanto la resiliencia como la recuperación);
  - Acceso físico y lógico y protección de activos de información de segunda y tercera parte;

- Crear un entorno de "confianza extendida" con responsabilidades compartidas para la seguridad de la información;
- Crear una responsabilidad compartida para el cumplimiento de las políticas, normas, leyes, reglamentos, contratos y otros compromisos/obligaciones de seguridad de la información;
- Coordinación entre el proveedor y el adquirente para adaptar o responder a los requisitos de seguridad de la información nuevos/modificados;
- ... y más.

- Controles de seguridad de la información como:
  - Gestión de relaciones que cubre todo el ciclo de vida de la relación comercial;
  - Análisis preliminar, preparación de un caso de negocio sólido, invitación a licitar, etc., teniendo en cuenta los riesgos, controles, costos y beneficios asociados con el mantenimiento de una seguridad de la información adecuada;
  - Creación de objetivos estratégicos compartidos explícitos para alinear al adquirente y al proveedor en la seguridad de la información y otros aspectos (por ejemplo, una "estrategia de relación" de propiedad conjunta);
  - Especificación de requisitos importantes de seguridad de la información (como exigir que los proveedores estén certificados conformes con ISO / IEC 27001 y/o utilicen normas como ISO27k) en contratos, acuerdos de nivel de servicio, etc.;
  - Procedimientos de gestión de la seguridad, incluidos los que pueden desarrollarse y gestionarse conjuntamente, como el análisis de riesgos, el diseño de la seguridad, la gestión de identidades y accesos, la gestión de incidentes y la continuidad de las actividades;
  - Controles especiales para atender a riesgos únicos (como pruebas y acuerdos de reserva asociados con la etapa de transición / implementación cuando un proveedor de subcontratación proporciona servicios por primera vez);
  - Propiedad clara, rendición de cuentas y responsabilidad por la protección de activos de información valiosos, incluidos registros de seguridad, registros de auditoría y pruebas forenses;
  - Un "derecho de auditoría" y otros controles de cumplimiento/ aseguramiento, con sanciones o responsabilidades en caso de incumplimiento identificado, o bonificaciones por el pleno cumplimiento;
  - ... y más.

- Todo el ciclo de vida de la relación:
  - Iniciación: alcance, análisis de casos de negocio/costo-beneficio, comparación de opciones insource versus outsource, así como enfoques variantes o híbridos como el co-sourcing;
  - Definición de requisitos, incluidos los requisitos de seguridad de la información, por supuesto;
  - Adquisiciones que incluyen la selección, evaluación y contratación con proveedores;

- Transición o aplicación de los acuerdos de suministro, con mayores riesgos durante el período de aplicación;
- Operación que incluye aspectos como la gestión rutinaria de relaciones, cumplimiento, gestión de incidentes y cambios, monitoreo, etc.;
- Actualización: una etapa opcional para renovar el contrato, tal vez revisando los términos y condiciones, el rendimiento, los problemas, los procesos de trabajo, etc.;
- Terminación y salida, es decir, poner fin a una relación comercial que ha seguido su curso de manera controlada, lo que tal vez conduzca de nuevo al paso 1.

ISO / IEC 27036-1:2014 — Seguridad de la información para las relaciones con los proveedores — Parte 1: Descripción general y conceptos.

- RESUMEN: Proporciona una visión general de la orientación destinada a ayudar a las organizaciones a asegurar su información y sistemas de información dentro del contexto de las relaciones con los proveedores. Aborda las perspectivas tanto de los adquirentes como de los proveedores.
- Alcance y propósito: La parte 1 presenta todas las partes de esta norma, proporcionando información general de antecedentes e introduciendo los términos y conceptos clave en relación con la seguridad de la información en las relaciones con los proveedores, incluida "cualquier relación con el proveedor que pueda tener implicaciones de seguridad de la información, por ejemplo, tecnología de la información, servicios de atención médica, servicios de limpieza, servicios de consultoría, asociaciones de I + D, aplicaciones subcontratadas (ASP), o servicios de computación en la nube (como software, plataforma o infraestructura como servicio)".
- Describe una serie de riesgos de información que comúnmente surgen de o están relacionados con las relaciones comerciales entre adquirentes y proveedores, cuando los bienes / servicios adquiridos tienen un contenido de información o relevancia para la seguridad de la información, o cuando el proveedor obtiene acceso a la información interna del adquirente.
- Curiosamente, la situación inversa, es decir, los adquirentes que obtienen acceso a la información interna de los proveedores, no se menciona explícitamente en la parte 1, sino que se señala en la parte 2. La norma está escrita principalmente desde la perspectiva del adquirente, cubriendo las preocupaciones de seguridad de la información del adquirente que deben abordarse al formar relaciones con proveedores.
- Estado: Publicado en 2014 y descargable gratuitamente desde el sitio de la ITTF.
- La próxima versión de esta norma será "Ciberseguridad — Relaciones con proveedores — Parte 1: Visión general y conceptos". Se encuentra en la etapa de bronceado de la balsa Final puede publicarse hacia finales de 2021 o en 2022.

ISO / IEC 27036-2:2014 — Seguridad de la información para las relaciones con los proveedores — Parte 2: Requisitos

- RESUMEN: Especifica los requisitos fundamentales de seguridad de la información para definir, implementar, operar, monitorear, revisar, mantener y mejorar las relaciones con proveedores y adquirentes.
- Alcance y propósito: La parte 2 especifica los requisitos fundamentales de seguridad de la información relacionados con las relaciones comerciales entre proveedores y adquirentes de diversos productos (bienes y servicios). Les ayuda a alcanzar una comprensión común de los riesgos de información asociados y a tratarlos en consecuencia para su satisfacción mutua.
- La introducción establece explícitamente que ISO / IEC 27036 Parte 2 no está destinada a fines de certificación, a pesar de tener "Requisitos" en el título y "deberá" en el contenido [estas son normalmente palabras reservadas en ISO-land].
- Las medidas de control recomendadas en la parte 2 cubren diversos aspectos de la gobernanza y la gestión empresarial (por ejemplo, operaciones, gestión de recursos humanos, gestión de TI, gestión de relaciones, métricas), así como la gestión de la seguridad de la información (por ejemplo, análisis y tratamiento de riesgos de la información, especificación de controles, arquitectura / diseño, estrategia).
- Dadas las presunciones, el estilo, la estructura, la profundidad, la amplitud, el rigor y los requisitos de documentación establecidos en la parte 2, seguir la norma en detalle impondría una carga significativa de burocracia en el caso de los suministros de productos básicos, pero puede ser totalmente apropiado para aquellos con fuertes implicaciones para la seguridad de la información (por ejemplo, la contratación militar y gubernamental de sistemas y servicios de TIC clasificados, o la adquisición comercial de sistemas y servicios de TIC críticos para la seguridad o el negocio, incluido el soporte de computación en la nube para los procesos comerciales principales, además de servicios de información como servicios de consultoría, legales o de recursos humanos). Sin embargo, el estándar es una lista de verificación útil o un recordatorio de los aspectos de seguridad de la información que deben considerarse en la mayoría, si no en todas, las relaciones comerciales.
- Estado: Publicado en 2014.
  - La Parte 2 se está revisando tras los cambios en ISO / IEC 15288.
  - Aunque la norma revisada ya ha pasado una votación en la etapa de bronceado de la balsa internacional D, no se publicará en septiembre de 2023.
  - El título será: “Ciberseguridad — Relaciones con proveedores — Parte 2: Requisitos”.

ISO / IEC 27036-3:2013 — Seguridad de la información para las relaciones con los proveedores — Parte 3:- Directrices para la seguridad de la cadena de suministro de la tecnología de la información y las comunicaciones

- RESUMEN: Proporciona orientación a los adquirentes y proveedores de productos y servicios en la cadena de suministro de TIC.
- Alcance y propósito: Esta parte de la norma guía tanto a los proveedores como a los adquirentes de bienes y servicios de TIC sobre la gestión de riesgos de información relacionada con la cadena de suministro ampliamente dispersa y compleja, incluidos los riesgos como el malware y los productos falsificados, además de los "riesgos organizativos", y la integración de la gestión de riesgos con los procesos del ciclo de vida del sistema y el software, basándose en ISO / IEC 15288, 12207 y 27002.
  - Se refiere explícitamente a las TIC.
  - Esta parte de ISO/IEC 27036 no cubre los aspectos de continuidad del negocio y resiliencia de las cadenas/redes de suministro.

- Contenido: En la parte 3 se señala una amplia gama de controles de seguridad de la información, tales como:
  - Cadena de custodia; acceso con privilegios mínimos; separación de funciones; resistencia a la manipulación y evidencia; protección persistente; gestión del cumplimiento; evaluación y verificación del código; capacitación en seguridad; evaluación y respuesta a la vulnerabilidad; expectativas de seguridad definidas; derechos y responsabilidades de propiedad intelectual; evitar el mercado gris; procesos de adquisición, incluida la adquisición anónima y todo a la vez; pasar los requisitos de seguridad a los proveedores ascendentes; gestión de la calidad; Gestión de RRHH; gestión de proyectos; gestión de proveedores/relaciones; gestión de riesgos y seguridad (por ejemplo, el análisis de requisitos debe incluir requisitos de seguridad de la información que aborden los riesgos potenciales); configuración y gestión de cambios; gestión de la información; arquitectura/diseño de seguridad; aplicación y transición de las TIC; integración de las TIC; Pruebas y verificación de TIC (por ejemplo, pruebas de seguridad/penetración, escaneo de vulnerabilidades, pruebas de estrés, pruebas de cumplimiento); protección contra malware; Gestión, mantenimiento y eliminación de TIC, etc.
  - La mayoría de ellos están cubiertos en términos generales por ISO / IEC 27002: esta norma proporciona orientación adicional en el contexto particular de los suministros de TIC.
  - La mayor parte del estándar proporciona orientación de seguridad de la información para proveedores y adquirentes de TI, como un conjunto de procesos para cada etapa del ciclo de vida típico del sistema de TI.
  - Las orientaciones relativas a la "obtención de visibilidad de las actividades del proveedor" recomiendan varias medidas de garantía.
  - Un anexo incluye un desglose de cláusulas comparables en ISO / IEC 15288 y 12207, y otro identifica cláusulas relevantes de ISO / IEC

27002 (las referencias se actualizarán a la versión 2022 en breve en la segunda edición).

- Estado: Primera edición publicada en 2013. Actualmente en proceso de revisión.
  - La segunda edición no se publicará en 2024, pero ya se encuentra en la etapa de bronceado de la balsa D I, por lo que parece probable que salga a la superficie antes de lo previsto.
  - El título será: “Ciberseguridad — Relaciones con proveedores — Parte 3: Directrices para la seguridad de la cadena de suministro de hardware, software y servicios”.
  - A pesar de eliminar "TIC" del título, la norma sigue centrándose miopemente en esa área (por ejemplo, servicios de TI). Instamos a las organizaciones a considerar los riesgos de información de la cadena de suministro en general (por ejemplo, robo de propiedad intelectual, representación indebida, apropiación indebida, fraude ...) así como los riesgos comerciales y de otro tipo, no solo las TIC o el "ciber", que afectan a los servicios profesionales de todo tipo.

ISO / IEC 27036-4:2016 — Seguridad de la información para las relaciones con los proveedores — Parte 4: Directrices para la seguridad de los servicios en la nube

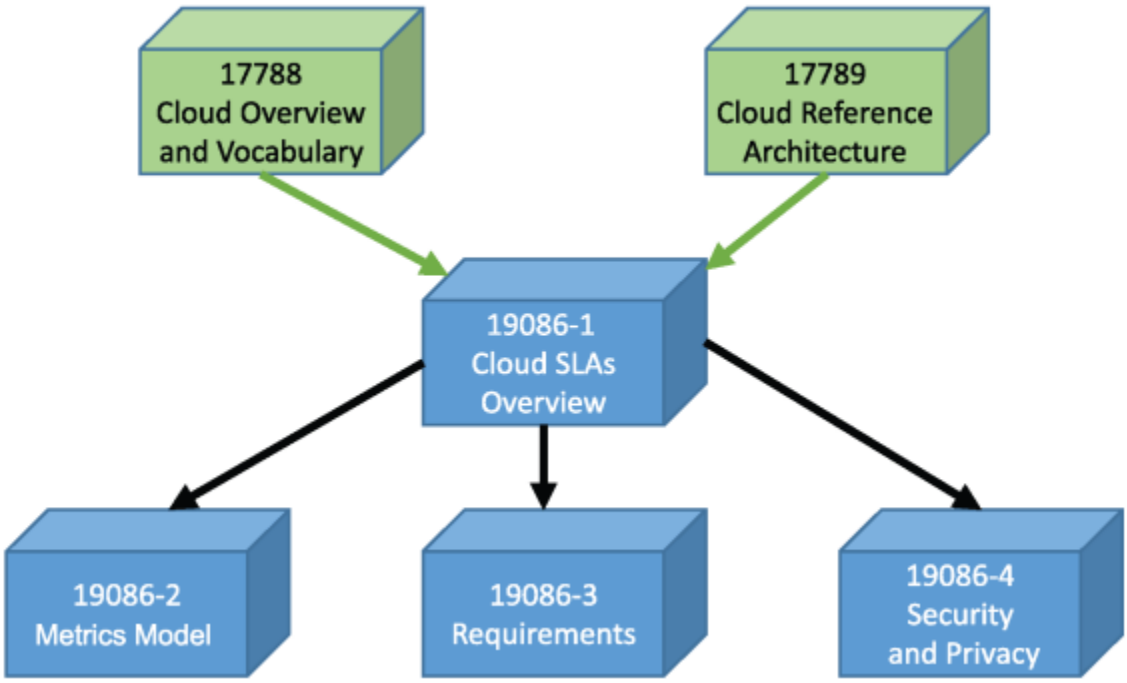
- RESUMEN: Definir directrices que apoyen la implementación de la gestión de la seguridad de la información para el uso del servicio en la nube.
- Alcance y propósito: La parte 4 ofrece orientación sobre seguridad de la información a los proveedores y clientes de servicios en la nube. El alcance es:
  - Proporcionar a los clientes de servicios en la nube y proveedores de servicios en la nube orientación sobre
    a. Obtener visibilidad de los riesgos de seguridad de la información asociados con el uso de servicios en la nube y gestionar esos riesgos de manera efectiva, y
    b. Responder a riesgos específicos de la adquisición o prestación de servicios en la nube que puedan tener un impacto en la seguridad de la información en las organizaciones que utilizan estos servicios.
  - [El estándar] no incluye los problemas de gestión/resiliencia de la continuidad del negocio relacionados con el servicio en la nube. ISO / IEC 27031 aborda la continuidad del negocio. [El estándar] no proporciona orientación sobre cómo un proveedor de servicios en la nube debe implementar, administrar y operar la seguridad de la información. La orientación sobre estos se puede encontrar en ISO / IEC 27002 e ISO / IEC 27017. El alcance de este [estándar] es definir pautas que apoyen la implementación de la gestión de la seguridad de la información para el uso de servicios en la nube".
- Estado: Publicado en 2016.

Revisión de ISO / IEC 27036

La revisión de esta norma de varias partes está en marcha. Se ha propuesto revisar el conjunto para mejorar la coherencia interna y alinearlo con ISO / IEC 15288 (ciclos de vida de los sistemas de TI). Una pista de que: las normas están tan centradas en las TIC que apenas mencionan bienes y servicios que no son TIC, incluso aquellos con un componente de información sustancial y, por lo tanto, riesgos de información significativos (por ejemplo, servicios profesionales como asesoramiento legal, contabilidad, recursos humanos, consultoría de gestión de riesgos de información y seguridad ...).

ISO/IEC 17788:2014

Computación en la nube por ISO/IEC 17788:2014



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

Las características clave de la computación en la nube son:

- **Amplio acceso a la red**: Una característica donde los recursos físicos y virtuales están disponibles a través de una red y se accede a través de mecanismos estándar que promueven el uso por parte de plataformas cliente heterogéneas. El enfoque de esta característica clave es que la computación en la nube ofrece un mayor nivel de conveniencia en el que los usuarios pueden acceder a recursos físicos y virtuales desde 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 servicios en la nube es tal que el uso puede ser monitoreado, controlado, reportado y facturado. 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 permitir un cambio de un modelo de negocio de baja eficiencia y utilización de activos a uno de alta eficiencia;

- **Multi-tenancy**: Una característica en la que los recursos físicos o virtuales se asignan de tal manera que varios inquilinos y sus cálculos y datos están aislados e inaccesibles entre sí. Normalmente, y en el contexto de la multitenencia, el grupo de usuarios de servicios en la nube que forman un inquilino pertenecerá a la misma organización de clientes de servicios en la nube. Puede haber casos en los que el grupo de usuarios de servicios 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 organización de clientes de servicios en la nube determinada puede tener muchos arrendamientos diferentes con un único proveedor de servicios en la nube que represente diferentes grupos dentro de la organización;
- **Autoservicio bajo demanda**: Una característica en la que un cliente de servicios en la nube puede aprovisionar capacidades informáticas, según sea necesario, de forma automática 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 tomar una acción, ya que otorga al usuario la capacidad de hacer lo que necesita, cuando lo necesita, sin requerir interacciones adicionales del usuario humano 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 característica en la que los recursos físicos o virtuales de un proveedor de servicios en la nube se pueden agregar para servir 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, utilizar 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 o 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, debe señalarse que los

usuarios aún pueden especificar la ubicación en un nivel más alto de abstracción (por ejemplo, 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. Tales aspectos pueden afectar a 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:

1. **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;
2. **Disponibilidad**: La propiedad de ser accesible y utilizable a petición de una entidad autorizada. La "entidad autorizada" suele ser un cliente de servicio en la nube;
3. **Gobernanza**: El sistema por el cual se dirige y controla la provisión y el uso de los servicios en la nube. La gobernanza de la nube se cita como un aspecto transversal debido al requisito de transparencia y la necesidad de racionalizar las prácticas de gobernanza con los SLA y otros elementos contractuales de la relación entre el cliente del servicio en la nube y el proveedor de servicios en la nube. El término gobernanza interna de la nube se utiliza para la aplicación de políticas en tiempo de diseño y tiempo de ejecución para garantizar que se diseñen e implementen soluciones basadas en computación en la nube, y que se entreguen servicios basados en computación en la nube, de acuerdo con las expectativas especificadas. El término gobernanza externa de la nube se utiliza para alguna forma de acuerdo entre el cliente del servicio en la nube y el proveedor de servicios en la nube con respecto al uso de los servicios en la nube por parte del cliente del servicio en la nube;
4. **Interoperabilidad**: Capacidad de un cliente de servicio en la nube para interactuar con un servicio en la nube e intercambiar información de acuerdo con un método prescrito y obtener resultados predecibles;
5. **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 razones comerciales. El control de versiones implica el etiquetado adecuado de un servicio para que el cliente del servicio en la nube tenga claro que se está utilizando una versión en particular;
6. **Rendimiento**: Un conjunto de comportamientos relacionados con el funcionamiento de un servicio en la nube y tener métricas definidas en un SLA;
7. **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 esté utilizando;

8. **Protección de la PII**: Proteger la recopilación, el procesamiento, la comunicación, el uso y la eliminación seguros, adecuados y consistentes de la Información de Identificación Personal (PII) en relación con los servicios en la nube;
9. **Regulatorio**: Hay una serie de regulaciones diferentes que pueden influir en el uso y la entrega 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 esos requisitos suele estar relacionado con las actividades de gobernanza y gestión de riesgos;
10. **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;
11. **Reversibilidad**: Un proceso para que el cliente del servicio en la nube recupere sus 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;
12. **Seguridad**: Abarca desde la seguridad física hasta la seguridad de las aplicaciones, e incluye requisitos como autenticación, autorización, disponibilidad, confidencialidad, administración de identidades, integridad, no repudio, auditoría, monitoreo de seguridad, respuesta a incidentes y administración de políticas de seguridad;
13. **Niveles de servicio y acuerdo de nivel de servicio**: El acuerdo de nivel de servicio de computación en la nube (SLA en la nube) 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 computación en la nube (cliente de servicio en la nube y proveedor de servicios en la nube y sub-roles relacionados).