EDUCACIÓN CON RESPONSABILIDAD SOCIAL

UNIVERSIDAD DE COLIMA

Universidad de Colima

Facultad de Ingeniería Mecánica y Eléctrica

Computo en la nube

Profesor: Oswaldo Carrillo Zepeda

Alumno: Oscar Dalí Nattaniel Romero Raygoza

6°B

Normas ISO

ISO 27017

¿Qué es ISO 27017?

ISO/IEC 27017 es un marco de seguridad de la información para organizaciones que usan (o consideran) servicios en la nube. Los proveedores de servicios en la nube deben cumplir con este estándar porque mantiene a sus clientes de servicios en la nube (y otros) más seguros al proporcionar un enfoque coherente e integral de la seguridad de la información.

ISO 27017 es parte de la familia de estándares ISO/IEC 27000, que proporciona pautas de mejores prácticas para la gestión de la seguridad de la información. Este estándar se derivó de ISO/IEC 27002 y sugiere controles de seguridad en la nube adicionales que no se especificaron completamente en ISO/IEC 27002.

Orientación para una mayor implementación de controles adicionales y controles relevantes especificados en ISO/IEC 27002, incluidas específicamente reglas sobre el uso de servicios en la nube. También se aplican controles de seguridad adicionales.

La Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (IEC) lo publicaron bajo el subcomité conjunto ISO/IEC ISO/IEC JTC 1/SC 27.

Esta Norma Internacional ofrece orientación para los clientes de servicios en la nube, que adoptan los controles, y los proveedores de servicios en la nube, que facilitan las implementaciones de los controles.

El marco define la alineación de la gestión de la seguridad para la computación en la nube, las redes virtuales y físicas.

ISO 27017 toma todas las precauciones de seguridad necesarias, el análisis basado en riesgos para la seguridad en línea y los extiende directamente a la seguridad en la nube, donde los controles de seguridad de la información son aplicables al marco.

¿Cuál es el propósito de ISO 27017?

ISO 27017 complementa el marco ISO/IEC 27002 para el entorno de computación en la nube al incluir información complementaria, medidas de seguridad y orientación para la implementación. Este marco proporciona orientación para la implementación de 37 controles que se encuentran en ISO/IEC 27001, así como siete requisitos adicionales.

Los nuevos controles en la nube abordan el siguiente código de mejores prácticas:

- Quién es responsable de qué entre el proveedor de servicios en la nube y el cliente de la nube.
- La retirada/devolución de bienes cuando se rescinde un contrato.
- Protección y separación del entorno virtual del cliente.
- Configuración de máquinas virtuales.
- Operaciones y procedimientos administrativos asociados al entorno de la nube, permitiendo a los clientes monitorear las actividades relevantes.
- Seguimiento de clientes en la nube de la actividad dentro de la nube.
- Alineación del entorno de red virtual y en la nube.

- Controles de seguridad de la información basados en la norma ISO 27001 y el marco ISO 27017.

Al adoptar este código de práctica, los consumidores y proveedores de la nube ahora pueden cumplir con los requisitos básicos de seguridad de la información al seleccionar los controles relevantes y la guía de implementación en función de las evaluaciones de riesgo para los servicios en la nube.

Si trabaja para un proveedor de servicios en la nube o está considerando trasladar su empresa a la nube. Nuestra descripción general de ISO 27017 lo ayudará a comprender los componentes centrales del marco, los nuevos controles y cómo este código de práctica beneficiará a su organización.

¿Por qué implementar ISO 27017?

Es fundamental que los clientes confíen en la seguridad de sus datos en la nube. ISO/IEC 27017 es un marco reconocido a nivel mundial que, cuando se implementa, reducirá de manera efectiva la probabilidad de filtraciones de datos y aumentará la confianza del cliente al demostrar su compromiso con las técnicas de seguridad de la información.

Como se señaló, el marco aborda varios problemas, incluida la propiedad de activos, la eliminación y devolución de activos después de la terminación del contrato de un cliente y la seguridad del entorno virtual de un cliente.

El marco define las operaciones administrativas para manejar un entorno de nube, los requisitos para fortalecer una máquina virtual de acuerdo con las necesidades comerciales.

Como proveedor de servicios en la nube o usuario de servicios en la nube, es vital demostrar que su organización está haciendo todo lo posible para minimizar los riesgos que plantean las filtraciones de datos.

ISO 27017 se basa en el estándar ISO 27001 y el marco ISO 27002, la implementación demuestra que su organización ha implementado las mejores prácticas para proteger contra las amenazas relacionadas con la nube tanto para los proveedores de servicios en la nube como para los clientes de servicios en la nube. Complementa, pero no reemplaza, los requisitos de ISO/IEC 27002.

¿Cuáles son los beneficios del proceso de certificación ISO 27017?

Proporciona seguridad a los clientes y orientación basada en la nube.

El nuevo código de prácticas ISO 27017 para controles de seguridad de la información basados en servicios en la nube es una excelente oportunidad para que los proveedores de servicios brinden una garantía externa a sus clientes de que la información procesada en la nube por el proveedor de servicios en la nube es segura.

Reduzca los riesgos basados en el almacenamiento de clientes en la nube

El código de prácticas ISO 27017 para los controles de seguridad de la información implementados en los servicios en la nube ayudará a la organización a elaborar un plan que se utilizará para proteger y reducir los riesgos de una filtración de datos y, por lo tanto, inculcar la confianza de las partes interesadas en la organización.

Proporciona un marco para los clientes de servicios en la nube

La implementación y certificación ISO 27017 define un sólido sistema de monitoreo de seguridad de la información para usuarios de computación en la nube y mantiene a los proveedores responsables.

Extiende y mejora la certificación ISO 27001

En el mundo de la Seguridad de la Información, la certificación ISO 27001 es el estándar más conocido. Ayuda a las organizaciones a gestionar los riesgos de seguridad de la información. ISO 27017 brinda nuevas herramientas y una cobertura ampliada para la protección de la información de identificación personal (PII) en lo que respecta al almacenamiento en la nube y los controles de seguridad de la información. En resumen, proporciona un marco estratégico para prevenir, detectar y tratar las filtraciones de datos.

Establece un marco adecuado de gestión de la seguridad de la información.

El marco establece un sólido sistema de gestión de la seguridad de la información para los proveedores de servicios virtuales en la nube que buscan brindar una mayor certeza sobre los controles de seguridad de sus servicios, las técnicas de seguridad y los datos de sus clientes.

Pasos para la Certificación ISO 27017

Debido al éxito anticipado de ISO 27017, algunos organismos de certificación quieren comenzar a certificar en su contra. Dado que ISO 27017 no es un estándar de gestión, la certificación de rutina no será posible; en cambio, los organismos de certificación probablemente ofrecerán algún tipo de "declaración de cumplimiento".

Sin embargo, las empresas que buscan la credencial ISO 27017 seguramente tendrán que someterse primero a la certificación ISO 27001. Como parte de la auditoría, recibirán una declaración que certifica que también cumplen con la norma ISO 27017. Tenga en cuenta que debe demostrar que su sistema de gestión de la información ha estado funcionando completamente durante un mínimo de tres meses y ha sido sujeto a una revisión y una serie completa de auditorías internas.

ISO 27018

ISO/IEC 27018 es un estándar de seguridad que forma parte de la familia de estándares ISO/IEC 27000. Fue el primer estándar internacional sobre la privacidad en los servicios de computación en la nube que fue promovido por la industria. Fue creado en 2014 como una adición a ISO/IEC 27001, el primer código internacional de prácticas para la privacidad en la nube. Ayuda a los proveedores de servicios en la nube que procesan información de identificación personal (PII) a evaluar el riesgo e implementar controles para proteger la PII. Fue publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) bajo el subcomité conjunto de ISO e IEC, ISO/IEC JTC 1/SC 27.

Versiones estándar

Ese estándar tiene dos versiones:

- ISO/CEI 27018:2014
- ISO/CEI 27018:2019

Estructura de la norma

El título oficial de la norma es "Tecnología de la información - Técnicas de seguridad - Código de práctica para la protección de información de identificación personal (PII) en nubes públicas que

actúan como procesadores de PII". ISO/IEC 27018:2019 tiene dieciocho secciones, además de un largo anexo, que cubren:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Resumen
5. Políticas de seguridad de la información
6. Organización de la seguridad de la información
7. Seguridad de los recursos humanos
8. Gestión de activos
9. Control de acceso
10. Criptografía
11. Seguridad física y ambiental
12. Seguridad de las operaciones
13. Seguridad de las comunicaciones
14. Adquisición, desarrollo y mantenimiento del sistema
15. Relaciones con proveedores
16. Gestión de incidentes de seguridad de la información
17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio
18. Cumplimiento

Objetivos

El objetivo de este documento, cuando se usa junto con los objetivos y controles de seguridad de la información en ISO/IEC 27002, es crear un conjunto común de categorías y controles de seguridad que puede implementar un proveedor de servicios de computación en la nube pública que actúe como un procesador de PII. Tiene los siguientes objetivos:

- Ayudar al proveedor de servicios de nube pública a cumplir con las obligaciones aplicables cuando actúe como procesador de PII, ya sea que dichas obligaciones recaigan sobre el procesador de PII directamente o por contrato.
- Permitir que el procesador de PII de la nube pública sea transparente en asuntos relevantes para que los clientes de servicios en la nube puedan seleccionar servicios de procesamiento de PII basados en la nube y bien administrados.
- Ayudar al cliente del servicio en la nube y al procesador de PII de la nube pública a celebrar un acuerdo contractual.
- Proporcionar a los clientes de servicios en la nube un mecanismo para ejercer los derechos y responsabilidades de auditoría y cumplimiento en los casos en que las auditorías individuales de los clientes de servicios en la nube de los datos alojados en un entorno de servidor virtualizado (nube) de varias partes pueden ser poco prácticas desde el punto de vista técnico y pueden aumentar los riesgos físicos y lógicos. controles de seguridad de la red en su lugar.

Ventajas

El uso de este estándar tiene las siguientes ventajas:

- Brinda mayor seguridad a los datos e información de los clientes.
- Hace que la plataforma sea más confiable para el cliente, logrando un nivel superior a la competencia.
- Habilitación más rápida de operaciones globales
- Contratos simplificados
- Brinda protecciones legales para proveedores y usuarios de la nube.

ISO 27036

Introducción

ISO/IEC 27036 es una norma de varias partes que ofrece orientación sobre la evaluación y el tratamiento de los riesgos de la información relacionados con la adquisición de bienes y servicios de los 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 otro).

Alcance y propósito

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

- Outsourcing de TI y servicios de computación en la nube.
- Otros servicios profesionales, p. servicios legales, contables/fiscales y de recursos humanos, guardias de seguridad, limpiadores, servicios de entrega (mensajes), mantenimiento/servicio de equipos, servicios de consultoría y asesoramiento especializado, gestión del conocimiento, investigación y desarrollo, fabricación, logística, custodia de código fuente y atención médica.
- Suministro de hardware, software y servicios de TIC, incluidos servicios de telecomunicaciones e Internet.
- Productos y servicios personalizados en los que el adquirente especifica los requisitos y, a menudo, tiene un papel activo en el diseño del producto (a diferencia de los productos básicos y los productos estándar listos para usar).
- Servicios públicos como energía eléctrica y agua.

Los estándares podrían cubrir:

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

- 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, estándares, leyes, reglamentos, contratos y otros compromisos/obligaciones de seguridad de la información.
- Coordinación entre el proveedor y el adquirente para adaptarse o responder a requisitos de seguridad de la información nuevos o modificados.

Controles de seguridad de la información tales 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 Licitación, etc., teniendo en cuenta los riesgos, controles, costos y beneficios asociados con el mantenimiento de la 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 importantes requisitos de seguridad de la información (como exigir que los proveedores estén certificados en conformidad con ISO/IEC 27001 y/o utilicen estándares como ISO27k) en contratos, acuerdos de nivel de servicio, etc.
- Procedimientos de gestión de la seguridad, incluidos aquellos que pueden desarrollarse y operarse conjuntamente, como el análisis de riesgos, el diseño de la seguridad, la gestión de identidades y accesos, la gestión de incidentes y la continuidad del negocio.
- Controles especiales para atender riesgos únicos (como pruebas y arreglos alternativos asociados con la etapa de transición/implementación cuando un proveedor subcontratado presta servicios por primera vez).
- Propiedad, rendición de cuentas y responsabilidad claras para 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/garantía, con sanciones o responsabilidades en caso de incumplimiento identificado, o bonificaciones por cumplimiento total.

Todo el ciclo de vida de la relación:

- Iniciación: determinación del alcance, caso de negocios/análisis de costo-beneficio, comparación de opciones internas versus externas, así como enfoques variantes o híbridos, como la contratación conjunta.
- Definición de requisitos, incluidos los requisitos de seguridad de la información, por supuesto.
- Adquisiciones incluyendo selección, evaluación y contratación con proveedor/es;
- Transición o implementación de los acuerdos de suministro, con mayores riesgos alrededor del período de implementación.
- Operación, incluidos aspectos como la gestión de relaciones de rutina, el cumplimiento, la gestión de cambios e incidentes, el seguimiento, etc.

- Actualizar: una etapa opcional para renovar el contrato, quizás revisando los términos y condiciones, el desempeño, 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, tal vez volviendo al paso 1.

ISO/IEC 17788:2014

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:** 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 función 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.
- **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. 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 característica 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 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 de abstracción más alto (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. 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 el cliente del servicio en la nube y el proveedor del servicio en la nube con respecto al 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 en 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.
- **Desempeño**: 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 la 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**: Habilidad de un sistema para brindar y mantener un nivel aceptable de servicio frente a fallas (involuntarias, intencionales o causadas naturalmente) que afecten la operación normal.
- **Reversibilidad**: un proceso para que el cliente del servicio en la nube recupere sus datos de cliente del servicio en la nube y artefactos de 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 autenticación, autorización, disponibilidad, confidencialidad, gestión de identidad, integridad, no repudio, auditoría, control de seguridad, respuesta a incidentes y 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. entregado. 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).