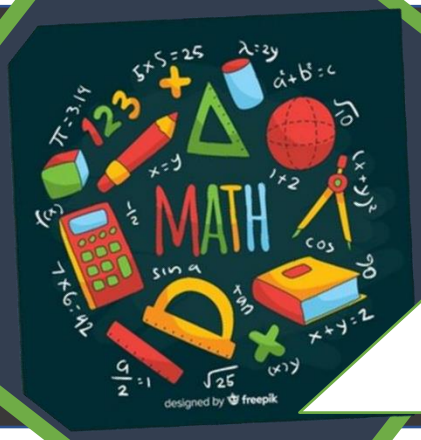
UNIVERSIDAD DE COLIMA



30/05/2022

Computo en la nube

CARLOS ALEJANDRO BALTAZAR PADILLA

6 B

¿Qué controles complementarios introduce la 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.

Recordemos que 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.

¿Cómo abordar ISO 27017 a través de un software?

Desde GlobalSuite Solutions disponemos de GlobalSuite® Security. Un software íntegramente desarrollado por nuestro equipo que permite la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información basados en la norma **ISO 27001** y la **ISO 27017**. Una herramienta que ayuda a las empresas y equipos de trabajo en la gestión integral de la

norma y cumple con el ciclo completo de la misma, desde el inicio y planificación del proyecto hasta el mantenimiento y su mejora continua.

Además, nuestro equipo de consultoría especializada ofrece el asesoramiento y el soporte necesarios para ayudar a las empresas a la consecución de la norma ISO 27001, así como de la ISO 27017.

¿Qué nos 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, 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 dos grandes bloques de actuación:

- **Controles Declaración de Aplicabilidad:** Partiendo de los controles de seguridad establecidos en el Anexo A de la ISO 27001 o el código de buenas prácticas ISO 27002, la norma añade requisitos de seguridad para la **información de identificación personal (PII)** sobre controles específicos**.** En este sentido, de los 114 controles que propone el estándar de Seguridad de la Información, la ISO 27018 establece requisitos adicionales sobre 15 controles, distribuidos entre los siguientes dominios:
    - Dominio 5: Políticas de Seguridad de la Información
    - Dominio 6: Organización de la Seguridad de la Información
    - Dominio 7: Seguridad de los Recursos Humanos
    - Dominio 9: Control de Acceso
    - Dominio 10: Criptografía
    - Dominio 11: Seguridad física y ambiental
    - Dominio 12: Seguridad de las operaciones
    - Dominio 13: Seguridad de las comunicaciones
    - Dominio 16: Gestión de incidentes
    - Dominio 18: Cumplimiento

¿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

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.

Por último, destacar que **GlobalSuite®** permite una implantación eficaz del estándar ISO 27018 al estar plenamente adaptada a los requisitos identificados en el presente artículo, ya no solo para empresas que estén certificadas en la ISO 27001, sino aquellas que deciden abordar la implantación de ambos estándares.

¿Qué es la norma 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, 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.

Organización y usos de la ISO 27036

¿Cómo está divida la norma?

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

1. ISO/IEC 27036-1:2014: Recoge la descripción general y los conceptos principales. Sirve de introducción a las cuatro partes de esta norma, dando información **general de los antecedentes normativos** (ISO 27000, TI – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción general y vocabulario), e **introduciendo los términos y conceptos clave**, incluidos los riesgos, en relación con la seguridad de la información en las relaciones con los proveedores.

2. ISO/IEC 27036-2:2014: Especifica los **requisitos fundamentales de la seguridad de la información** relativa a las relaciones comerciales entre proveedores y adquirientes. Las medidas de control recomendadas abarcan diversos aspectos de la gobernanza, la gestión empresarial y la gestión de la seguridad de la información (habilitación de proyectos organizacionales, planificación de la relación con el proveedor, acuerdos de relación, gestión de relaciones con proveedores, etc.).

3. ISO/IEC 27036-3:2013: Proporciona las **directrices para la seguridad de la cadena de suministro de las TIC**. Recoge las pautas tanto para los proveedores como para los adquirientes sobre gestión de riesgos de seguridad de la información, relacionados con la cadena de suministro (malware, productos falsificados, riesgos organizativos, integración de la gestión de riesgos con los procesos del ciclo de vida del sistema y del software, etc).

4. ISO/IEC 27036-4:2016: Describe las **directrices para la seguridad de los servicios en la nube.** Proporciona a los clientes y proveedores de servicios en la nube orientación acerca de los riesgos de seguridad de la información asociados con el uso de servicios en la nube y la gestión eficaz de esos riesgos mediante la implantación de controles específicos para su mitigación.

¿Dónde se aplica la ISO 27036?

La norma se aplica a las relaciones comerciales entre compradores y proveedores de diversos bienes y servicios, tales como:

- Suministro de hardware, software y servicios TIC, incluidos los servicios de telecomunicaciones e Internet.
- Externalización de servicios de computación en la nube.
- Otros servicios como guardias de seguridad, limpiadores, mensajería, mantenimiento de equipos, servicios de consultoría y asesoramiento especializado, etc.
- Productos y servicios a medida donde el adquirente especifica los requisitos y normalmente tiene un papel activo en el diseño del producto.
- Servicios públicos como energía eléctrica, combustibles y agua.

Fases de la ISO 27036:

Se dan las **pautas para la detección y evaluación de los riesgos de información** involucrados en la adquisición de bienes y servicios y la implantación de los controles necesarios para su mitigación, a lo largo de todo el ciclo de vida o fases de la relación entre adquirientes y proveedores:

¿Cuál es el ciclo de vida de la relación?

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.

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.
- Responsabilidades compartidas respecto a la seguridad de la información en lo referente al cumplimiento de políticas, normas, leyes, reglamentos, contratos y otros compromisos/obligaciones de seguridad de la información.
- Coordinación adquirente-proveedor para adaptar o responder a los nuevos requisitos de seguridad de la información.

Controles de seguridad de la información:

Los **controles de seguridad** que se refieren a la información, se deben llevar a cabo a cabo en:

- El análisis preliminar de riesgos, controles, costes y beneficios asociados con el mantenimiento de una seguridad de la información adecuada.
- La creación de objetivos estratégicos compartidos para alinear en materia de seguridad de la información a comprador y proveedor.
- La especificación de requisitos de seguridad de la información: exigencia a los proveedores de cumplimiento de la norma ISO / IEC 27001 en contratos, acuerdos de nivel de servicio, etc.
- En los procedimientos de gestión de la seguridad: análisis de riesgos, diseño de seguridad, gestión de incidentes, planes de continuidad de negocio, entre otros.
- Para la responsabilidad por la protección de activos críticos de información (registros de seguridad, registros de auditoría, pruebas, etc).
- El derecho de auditoría y cumplimiento, con sanciones o responsabilidades en caso de incumplimiento o bonificaciones en caso de pleno cumplimiento.

En **GlobalSuite Solutions** ofrecemos la ayuda y el asesoramiento necesarios para la implementación de su Sistema de Gestión de Seguridad de la Información (SGSI) basado en los requisitos de la ISO 27001.

Además, contamos con el **software GlobalSuite®**, íntegramente desarrollado por nuestro equipo, que permite la implantación, gestión y mantenimiento de los requisitos exigidos por la norma ISO 27001 en todo tipo de organizaciones y sectores.

ISO 17788

La computación en nube es muy posiblemente el concepto más caliente, más discutido y, a menudo mal entendido en tecnología de la información (TI) de hoy. Este concepto revolucionario ha llegado a alturas inesperadas en la última década y es reconocido por los gobiernos y las organizaciones del sector privado como la principal tecnología que cambia el juego.

Las organizaciones y los individuos por igual están dispuestos a almacenar y procesar sus datos en la nube, el acceso desde cualquier lugar, las aplicaciones y la información importante se mantiene en la nube, ya que implica hacerlo más rápido ya un costo más bajo que a través de medios convencionales. Las empresas comerciales y organizaciones del sector público están ansiosos por ganar eficiencia y agilidad, mientras que el usuario medio desea la flexibilidad de la nube. Y, por encima de todo, todo el mundo quiere reducir los costos.

¿Realmente la nube, permite algo nuevo? ¿Cómo funciona?

Pocas innovaciones tecnológicas han generado tanto bombo, ofrecido tanta promesa o sido tan amplia y rápidamente adoptado como la computación en nube. El cloud computing es una forma de TI que implica el uso de los recursos que no son propiedad, controlados y mantenidos por el usuario individual. Más bien, se accede a los recursos a través de una red y se comparten entre alguna comunidad de usuarios. Con la computación en nube, los recursos se pueden aprovisionar dinámicamente - si los usuarios necesitan más potencia de cálculo, más capacidad de almacenamiento, o más capacidades de procesamiento

¿Cuáles son las ventajas del uso de la computación en nube?

La computación en nube significa diferentes cosas para diferentes personas. Dependiendo de la concentración, los beneficios de la computación en nube son:

Reducir el gasto en tecnología de la información y la comunicación mediante el despliegue y uso de los recursos de una manera más rentable

Ofrecer una mayor velocidad, la potencia de cálculo y capacidad de usuarios individuales a través de la puesta en común de los recursos

Hacen que la informática sea más accesible a las personas ya las organizaciones de todos los tamaños

Aumentar la seguridad

Las primeras normas internacionales de cloud computing se acaban de publicar: ISO / IEC 17788 e ISO / IEC 17789. ISO / IEC 17788 , La computación en nube - Información general y vocabulario , proporciona definiciones de términos de computación en nube común, incluidos los de las categorías de servicios en la nube, como software como servicio (SaaS), plataforma como servicio (PaaS) e Infraestructura como Servicio (IaaS). También especifica la terminología para los modelos de despliegue de la nube como "público" y "privado" cloud. Más de carácter técnico, ISO / IEC 17789 , La computación en nube - Arquitectura de referencia , contiene diagramas y descripciones de cómo los diversos aspectos de la computación en nube se relacionan entre sí.