

Más allá del cumplimiento

ISO 27001:2022, un escudo contra las amenazas emergentes y la transición hacia un futuro más seguro

MATEOS CONSULTORES / ARTÍCULO / Edrei Oliveros

Introducción

La norma ISO 27001:2022 marca un hito en la evolución de la seguridad de la información, ofreciendo un marco de referencia más robusto y adaptable para enfrentar los desafíos cibernéticos actuales. Esta nueva versión introduce cambios significativos en su estructura y controles, lo que plantea la necesidad de una transición planificada y eficiente para aquellas organizaciones que desean mantenerse a la vanguardia en materia de seguridad de la información.

La necesidad de la transición y las amenazas emergentes

La rápida evolución del panorama de las amenazas cibernéticas, junto con la creciente complejidad de los sistemas de información y la inclusión de la variable del uso de la Inteligencia Artificial (para bien o para mal), hacen que la versión 2013 de ISO 27001 quede obsoleta muy independientemente del proceso de revisión y actualización por la organización internacional de estandarización (ISO) que tiene como fecha límite el último día de Octubre del 2025. Las organizaciones que cuentan con un Sistema de Gestión de Seguridad de la Información basado en esta versión o aquellas que desean proteger sus activos de información de manera efectiva deberían considerar seriamente los siguientes factores:

- **Nuevas tecnologías:** La adopción de tecnologías como la nube, el internet de las cosas (IoT) y la inteligencia artificial introduce nuevos vectores de ataque y aumenta la superficie de ataque.
- **Regulaciones más exigentes:** Las leyes de protección de datos, como la Ley Federal de Protección de datos Personales en posesión de Particulares (LFPDPP para México) o el Reglamento General de Protección de Datos (RGPD para la Unión Europea), imponen requisitos cada vez más estrictos en materia de seguridad de la información.
- **Ciberataques más sofisticados:** Los ataques cibernéticos se vuelven más dirigidos y personalizados, aprovechando las vulnerabilidades específicas de las organizaciones, es decir los ataques son dirigidos hacia ciertas industrias o a la cadena de valor de las organizaciones.
- **Cambios en el entorno de negocio:** La transformación digital, el trabajo remoto y la globalización modifican la forma en que las organizaciones operan y gestionan sus datos.

El futuro de la seguridad de la información y el papel de ISO 27001:2022.

Las tendencias clave que están moldeando el presente (¿Futuro?) de la Seguridad de la Información deben tomarse en consideración para bien o para mal. Para mantener un ritmo similar al de la evolución del ecosistema debemos conocer y usar las mismas herramientas que los ciberdelincuentes para protección de las organizaciones, utilizar el conocimiento generado por comunidades y especialistas y explotarlo a nuestro favor, mantener capacitado al personal involucrado en la seguridad de la información y al mismo tiempo sensibilizar a la totalidad del personal de la organización.

Por lo anterior, es sumamente importante conocer el lado negativo para estar preparado así como el positivo y aprovechar estas tendencias.

Por un lado, usando la **Inteligencia Artificial** se puede programar código malicioso a partir de un prompt bastante simple o, en conjunto con el **Machine Learning**, dirigir un ataque de phishing mucho mas enfocado a la organización o industria seleccionada. Esto mantiene ocupadas a las corporaciones que comercializan productos

ISO 27001:2022**Amenazas emergentes y un futuro más seguro**

Antivirus o protecciones para endpoint, al mismo tiempo que requiere que las empresas enfoquen capacitaciones y recursos tecnológicos para poder identificar el phishing y prevenir la fuga de datos accidental. En el otro extremo la **IA** y el **ML** están revolucionando la forma en que se detectan y previenen las amenazas cibernéticas. Estas tecnologías permiten el análisis de grandes volúmenes de datos para identificar patrones y anomalías, lo que mejora la capacidad de respuesta ante incidentes.

La migración a la nube ha transformado la infraestructura de TIC desde hace años, mejorando el rendimiento de los sistemas bajo demanda, pagando lo que se consume, incrementando la disponibilidad de los servicios que, on-premise, sería sumamente prohibitivo de alcanzar a esos costos, pero también ha introducido nuevos desafíos de seguridad. La protección de los datos en entornos de nube requiere un enfoque especializado y una sólida gestión de la seguridad con una perspectiva de responsabilidad compartida entre el cliente/usuario de nube y los proveedores de estos servicios. Un ejemplo entre varios, es el ataque a la cadena de suministro de servicios, en el que se aprovecha alguna vulnerabilidad de los proveedores de nube y el ataque afecta a las organizaciones que consumen ese servicio, impactando directamente en el cliente/usuario final.

La proliferación de dispositivos **IoT** (Internet de las cosas) ha ampliado la superficie de ataque, lo que aumenta la vulnerabilidad a las amenazas cibernéticas. La seguridad de IoT se ha convertido en una preocupación creciente derivado de que estos dispositivos la mayor parte de las veces no cuentan con seguridad integrada o es muy limitada. Estos dispositivos ofrecen bastantes posibilidades de automatización y monitoreo, aunque al mismo tiempo carecen de la seguridad necesaria, pueden ser usados en un honeypot para simular un dispositivo y detectar si hay atacantes tratando de acceder a la infraestructura y tomar medidas correctivas.

La computación cuántica es un avance significativo en estos días, si bien no se ha extendido su uso a todas las organizaciones, existen sin embargo algunas que cuentan con este tipo de cómputo. Esto plantea una amenaza potencial para los sistemas de cifrado actuales ya que en cuestión de segundos podrían descifrar datos/contraseñas por diversos métodos (análisis de frecuencias, fuerza bruta, etc.) que para una computadora con procesadores “comunes” tomaría mayor tiempo. La ciberseguridad cuántica se enfoca en el desarrollo de técnicas de cifrado resistentes a los ataques cuánticos.

La pandemia de la COVID-19 aceleró el trabajo remoto (Home-Office o Teletrabajo). Esto ha generado nuevos retos en la seguridad de la información, ya que muchas empresas tuvieron que adaptar sus sistemas para que sus trabajadores pudieran acceder a ellos de forma remota, si bien esto ha representado reducción de costos asociados a los servicios de mantenimiento de oficinas, servicios, infraestructura on-premise, etc. Inevitablemente ha incrementado las vulnerabilidades de seguridad de la información, esto debido a que, usualmente los servicios de comunicaciones en las residencias distan mucho de contar con los requerimientos de seguridad de las organizaciones, esto implica inevitablemente incrementar la inversión en herramientas que incrementen la seguridad en los endpoints y la transmisión de datos cifrados a la organización.

Entonces ¿Por qué adoptar la Norma ISO27001:2022?

Lejos de todos los beneficios comerciales, reputacionales de cumplimiento normativo o por los que se haya decidido implementarla, la realidad es que esta versión de la Norma provoca que cambiemos el enfoque cuasi pasivo de un sistema de gestión de la seguridad basado en la versión 2013.

Es imperativo para esta versión adoptar un enfoque basado en la gestión de riesgos en todos los procesos identificados apoyándose de la inteligencia de amenazas que resulte en una mejora de procedimientos para la continuidad del negocio y de la seguridad de la información durante un evento catastrófico. Esta gestión de riesgos con esteroides (basada en la ISO 31000 + 27005) propone un mayor énfasis en la identificación y evaluación de riesgos y proporciona un marco para abordar los riesgos de seguridad de la información ofreciendo una hoja de ruta estratégica para evaluar y mitigar los riesgos y ayudar a implementar la seguridad de la información con un enfoque de gestión de riesgos sin dejar de lado la mejora continua.

Esta versión se ha diseñado para ser más adaptable a los cambios en el entorno empresarial y tecnológico, por lo que la integración con otros sistemas de gestión es mucho más simple ya que ha adoptado completamente la estructura del anexo SL.

ISO 27001:2022

Amenazas emergentes y un futuro más seguro

La seguridad de la información es un viaje continuo, no un destino. ISO 27001:2022, los riesgos nunca se eliminan, la superficie de ataque tiende a crecer y las tecnologías emergentes no se detendrán, la Inteligencia artificial crece exponencialmente todos los días y no siempre se usa éticamente y es relativamente sencillo burlar los candados de los modelos que se usan libremente para que entreguen resultados “deseados” aunque sean ilegales, al final quien tenga la Inteligencia Artificial más poderosa será la nueva super-potencia transgrediendo el límite de las fronteras físicas. Teniendo en mente esta premisa, la Norma ISO 27001:2022 proporciona las herramientas para mantenernos a la vanguardia de las amenazas cibernéticas e ir mejorando continuamente con la finalidad de construir un futuro digital mucho más seguro para las organizaciones.

Procesos de transición, adopción y modificación

La transición o adopción de la norma ISO 27001:2022 implica una serie de desafíos:

- **Evaluación del SGSI existente:** Es necesario evaluar el Sistema de Gestión de Seguridad de la Información actual para identificar las brechas y las áreas que requieren mejora.
- **Creación del SGSI:** Verificar los requisitos de la Seguridad de la Información de la organización, conocer los requisitos de la normativa ISO 27001:2022 y planificar la implementación de la estructura del Sistema de Gestión de la Seguridad de la información.
- **Adopción de nuevos controles:** El cambio de la estructura del anexo A, con la incorporación de los nuevos controles de la norma implica cambios en los procesos, procedimientos y tecnologías.
- **Modificación de la documentación:** La documentación del SGSI debe actualizarse para reflejar los cambios en la norma.
- **Capacitación del personal:** Es fundamental capacitar al personal sobre los nuevos requisitos y responsabilidades.
- **Gestión del cambio:** La transición debe gestionarse de manera efectiva para minimizar la resistencia al cambio y garantizar la aceptación de los nuevos procesos.

La mejor vía para la implementación de ISO 27001:2022

Para llevar a cabo una transición exitosa a ISO 27001:2022, se recomienda seguir los siguientes pasos:

1. **Busque apoyo:** Considere la posibilidad de trabajar con un consultor o proveedor de servicios con experiencia en la implementación de ISO 27001:2022.
2. **Análisis de la situación actual:** Realizar una evaluación exhaustiva del SGSI existente para identificar las brechas y las áreas de mejora.
3. **Desarrollo de un plan de transición:** Elaborar un plan detallado que incluya un cronograma, asignación de responsabilidades y recursos necesarios.
4. **Capacitación del personal:** Impartir formación a todo el personal involucrado en el SGSI sobre los cambios en la norma y sus implicaciones.
5. **Implementación de los nuevos controles:** Implementar los nuevos controles de manera gradual, priorizando aquellos que tienen un mayor impacto en la seguridad de la información.
6. **Actualización de la documentación:** Revisar y actualizar toda la documentación del SGSI para reflejar los cambios en la norma.
7. **Auditorías internas:** Realizar auditorías internas periódicas para verificar el cumplimiento de los requisitos de la norma.
8. **Certificación:** Solicitar la certificación de un organismo de certificación acreditado para verificar la conformidad del SGSI con la norma ISO 27001:2022.

ISO 27001:2022**Amenazas emergentes y un futuro más seguro****Conclusión**

Lejos de que la transición de la norma ISO 27001:2013 sea un requisito de la Organización Internacional de Estandarización (ISO), representa un desafío y una excelente oportunidad para fortalecer la seguridad de la información. Ahí es donde la ISO 27001:2022 se erige como un faro guía en este panorama complejo, ofreciendo un marco sólido y adaptable para proteger los activos de información de su organización.

Abordar los nuevos requisitos y los cambios estructurales, al tiempo que se gestionan las amenazas emergentes, requiere una planificación cuidadosa y una ejecución eficaz, si se sigue adecuadamente una metodología de implementación, seguimiento, adopción y adaptación adecuada y considerando los riesgos asociados a la transición, requisitos específicos de la norma (Incluyendo los cambios en los controles), las organizaciones pueden garantizar una transición exitosa y beneficiarse de las múltiples ventajas que ofrece ISO 27001:2022.

Del cambio del entorno a la adaptación del SGSI