Preguntas frecuentes

Revisión ISO/IEC 27002:2022

Aprende de los expertos

Acerca de ISO/IEC 27002:2022

1. ¿Qué es ISO/IEC 27002?

ISO/IEC 27002:2022 seguridad de la información, ciberseguridad y protección de la privacidad: los controles de seguridad de la información brindan orientación para los estándares de seguridad de la información organizacional y ofrecen las mejores prácticas para la gestión de la seguridad de la información. Tiene en cuenta un entorno de seguridad de la información único en la empresa, centrándose en la selección, implementación y gestión de controles de seguridad de las organizaciones.

2. ¿ISO/IEC 27002:2022 es una revisión completa?

Sí, ISO/IEC 27002:2022 es una revisión completa del estándar y actualiza la versión 2013. Tras su publicación, la versión de 2013 será retirada

3. ¿Qué ha cambiado en la ISO/IEC 27002:2022?

Dentro de la ISO/IEC 27001:2022, los usuarios encontrarán que ha habido una reestructuración de los controles existentes y el número de controles de seguridad enumerados ha disminuido de 114 a 93, con algunos controles eliminados porque ya no reflejan las mejores prácticas.

Se han introducido once nuevos controles en la última edición de la norma ISO/IEC 27002. Los nuevos controles incluyen aspectos como inteligencia de amenazas, seguridad de la información para el uso de servicios en la nube y prevención de fuga de datos. Esto garantizará que las empresas puedan mantener un control continuo sobre la seguridad de su información, a pesar de que cambie la naturaleza de los ataques cibernéticos.

4. ¿Qué hay de nuevo en ISO/IEC 27002:2022?

ISO/IEC 27002 ha sido revisado para facilitar la adopción por parte de las empresas y continuar con su objetivo de garantizar que no se hayan pasado por alto los controles necesarios. Utiliza cuatro categorías temáticas de controles: Tecnológico, Organizacional, Personas y Físico. Dentro de este arsenal existen otras ayudas como, utilizar marcos de ciberseguridad; identificar, Proteger, Detectar, responder, Recuperar y la tríada habitual de Confidencialidad, Integridad y Disponibilidad. Los atributos también se pueden usar para filtrar, ordenar y presentar controles desde diferentes perspectivas para diferentes audiencias.

5. ISO/IEC 27002 es una guía complementaria - ¿Qué acciones debe tomar mi organización?

BSI recomienda que mantenga sus mejores prácticas para la seguridad de la información, la seguridad de la nube y la seguridad de los datos revisando su evaluación de riesgos y los controles necesarios y asegúrese de que se alineen con la nueva guía. De esta forma, su organización estará en una mejor posición para superar futuros riesgos. Además, dado que este cambio desencadena una actualización a ISO 27001, estará preparando a su organización para una actualización de su certificado.

Los beneficios a su organización

6. ¿Cómo ayudará ISO/IEC 27002 a su empresa?

- Identificar controles de seguridad adecuados dentro del proceso de creación de un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Lograr las mejores prácticas en la gestión de la seguridad de la información
- Cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales en relación con la seguridad de la información.
- Fortalecer la gestión de riesgos y reducir la probabilidad de violaciones de la seguridad de la información
- Aumentar la confianza en el SGSI de las organizaciones
- Aumentar la solidez general y la resiliencia del SGSI y fortalecer la gestión de riesgos
- Contribuir al Objetivo de Desarrollo Sostenible 9 de la ONU sobre industria, innovación e infraestructura

El impacto en ISO/IEC 27001:2013

7. ¿Se cambiará ISO/IEC 27001 en 2022 debido a la revisión de ISO/IEC 27002?

Se realizará una enmienda que es una revisión parcial de la norma ISO/IEC 27001 para actualizar los controles del anexo A de la norma ISO/IEC 27002:2022 revisada e incluir las 2 correcciones menores que se publicaron en 2014 y 2015. ISO/IEC 27001:2022 se prevé que se publique en la segunda mitad de 2022. Lo guiaremos a través del proceso a su debido tiempo.

8. ¿Cuál será el impacto de la norma ISO/IEC 27001 una vez modificada?

Se requerirá una evaluación de transición y se definirá un plan para cada cliente en función de su alcance, número de sitios, sistemas y complejidad de cada organización para garantizar que sus controles y SGSI cumplan con el estándar actualizado.

9. ¿Qué significa la revisión de ISO/IEC 27002 para una organización que está implementando su SGSI o está a punto de obtener la certificación ISO/IEC 27001?

Ya sea que su organización recién esté implementando ISO 27001 o esté lista para obtener la certificación, es importante asegurarse de maximizar los beneficios de su SGSI aprovechando la guía proporcionada en la nueva edición. La ISO 27002:2022 le servirá de referencia para identificar e implementar los controles adecuados para su organización.