ISOTools EXCELLENCE

Norma ISO 27001

¿Qué es la Norma **ISO 27001?**

Sistemas de Gestión la Seguridad de la Información ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar **ISO 27001:2022** para los **Sistemas Gestión de la Seguridad de la Información** permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de **ISO-27001** significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La **Gestión de la Seguridad de la Información** se complementa con las buenas prácticas o controles establecidos en la norma **ISO 27002**.

1. **Norma ISO 27001Estructura de la norma ISO 27001**Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de **ISO27001**.

2. Términos y Definiciones: Describe la terminología aplicable a este estándar.Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del **SGSI**.

3. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un **Sistema de Gestión de Seguridad de la Información**, así como de establecer objetivos de **Seguridad de la Información** y el modo de lograrlos.

4. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del **SGSI** la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

5. Operación: Para cumplir con los requisitos de **Seguridad de la Información**, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la **Seguridad de la Información** y un tratamiento de ellos.

6. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del **Sistema de Gestión de Seguridad de la Información**, para asegurar que funciona según lo planificado.

7. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del **SGSI**.

Novedades de la ISO 27001:2022

Esta norma fue publicada a finales de 2022, aportó una serie de cambios con respecto a su antecesora, la **ISO 27001:2013** que los usuarios de los **SGSI** tienen que asimilar para continuar gestionando de forma eficaz la **Seguridad de la Información**. Las novedades que manifiesta son:

- No aparece la sección "Enfoque a procesos" con su respectiva metodología basada en el ciclo **PHVA**, ahora ofrece mayor flexibilidad.

- Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad.

- Se han revisado los requisitos y controles.

- Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación.

- **Cambios en los controles de la nueva versión de ISO 27001** Nueva agrupación de los controles de Seguridad de la Información: En esta nueva versión, en lugar de contar con 14 dominios, se agrupan en 4 temas para conformar el total de los controles, incluyendo aquellos nuevos que son novedad en la **ISO 27001:2022**. En esta nueva versión encontramos:

1. **Controles organizacionales,** con 37 controles enfocados en la seguridad administrativa y las políticas de seguridad de la información.

2. **Controles de personas**, que agrupa a 8 controles orientados a la protección de la Seguridad de la Información en lo que respecta capital humano de la organización.

3. **Controles físicos,** con 14 controles orientados a la instalación e infraestructura IT de la empresa.

4. **Controles tecnológicos,** con 34 controles enfocados en aspectos como autentificación, cifrado y otras materias tecnológicas no relacionadas con las instalaciones físicas o la infraestructura.

Además de la agrupación de los controles, la nueva versión implica la eliminación de uno de ellos, la fusión, algunos existentes en la versión 2013 y la creación de 11 nuevos controles de seguridad de la información para adaptar la norma a los tiempos actuales.

Cambios en los atributos de la nueva versión 2022

Para los controles también se han implementado atributos, siendo los que aplican a la nueva norma: Tipo de control, Propiedad del SI, Concepto de Ciberseguridad, Capacidad Operacional y Dominio de Seguridad, cada uno de ellos orientado, de nuevo, a adaptar los controles a los nuevos tiempos.

Software para Sistemas de Gestión de Seguridad de la Información

La Plataforma ISOTools facilita la automatización de la ISO 27001

La **ISO27001** para los **SGSI** es sencilla de implantar, automatizar y mantener con la **Plataforma Tecnológica ISOTools**. Con **ISOTools** se da cumplimiento a los requisitos basados en el **ciclo PHVA (Planear – Hacer – Verificar – Actuar)** para establecer, implementar, mantener y mejorar el **Sistema Gestión de la Seguridad en la Información**, así como se da cumplimiento de manera complementaria a las buenas prácticas o controles establecidos en **ISO 27002**.

ISOTools también permite aplicar los requisitos de otras normas de **Seguridad de la Información** como PMG SSI de los Servicios Públicos de Chile, entre otros.

Este software, permite integrar la **ISO 27001** con otras normas, como ISO 9001, ISO 14001 e ISO 45001 de una forma sencilla gracias a su estructura modular.

CONOCE EL SOFTWARE

ISOTools
EXCELLENCE

isotools.us
+34 957 102 000