ISOTools

ISO 28000

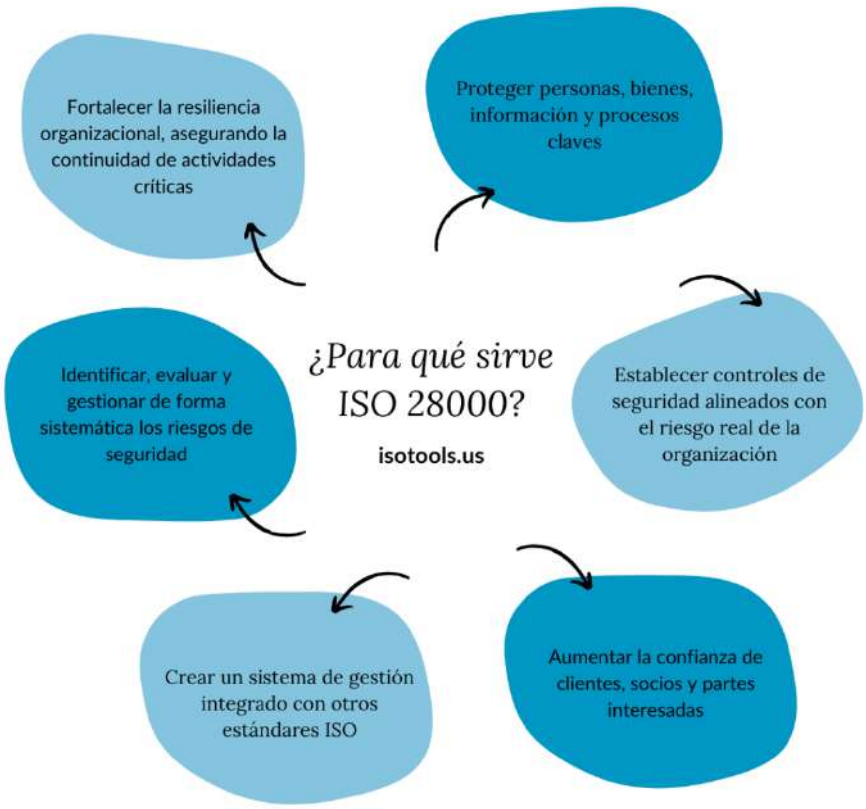
¿Qué es la ISO 28000?

Sistemas de Gestión de la Seguridad para la Cadena de Suministro

La **ISO 28000:2022** es la norma internacional que establece los requisitos para implementar un **Sistema de Gestión de la Seguridad y la Resiliencia**, aplicable a cualquier tipo de organización, independientemente de su tamaño, sector o nivel de complejidad operativa.

Si bien su origen estuvo fuertemente vinculado a la **seguridad en la cadena de suministro**, la versión 2022 amplía su alcance para abarcar la protección de **personas, activos, información, instalaciones, procesos críticos y continuidad operativa** frente a amenazas internas y externas.

Esta nueva edición adopta la **Estructura de Alto Nivel (HLS)**, lo que facilita la integración con otros sistemas de gestión como **ISO 9001, ISO 22301, ISO 27001, ISO 14001** y normas de gestión del riesgo. Gracias a ello, la organización puede gestionar la seguridad y la resiliencia desde un enfoque homogéneo, basado en riesgos y orientado a la mejora continua.



¿Para qué sirve la ISO 28000?

La ISO 28000:2022 ayuda a las organizaciones a:

- Identificar, evaluar y gestionar de forma sistemática los **riesgos de seguridad**.
- Fortalecer la **resiliencia organizacional**, asegurando la continuidad de actividades críticas.
- Proteger personas, bienes, información y procesos claves.
- Establecer controles de seguridad alineados con el riesgo real de la organización.
- Crear un sistema de gestión integrado con otros estándares ISO.

- Aumentar la confianza de clientes, socios y partes interesadas.

La norma es especialmente útil en entornos complejos, dinámicos o expuestos a amenazas físicas, logísticas, tecnológicas o sociales.

¿Qué organizaciones pueden aplicar la ISO 28000?

La versión 2022 aclara que la norma puede aplicarse a **cualquier organización**, ya sea pública o privada, grande o pequeña, y en todo tipo de sectores:

- Logístico y transporte
- Servicios públicos
- Industria
- Distribución y comercio
- Infraestructuras críticas
- Seguridad y vigilancia
- Servicios tecnológicos
- Empresas multinacionales y pymes

La norma ya no limita su aplicación a cadenas de suministro: ahora es un **marco global para la gestión de la seguridad y la resiliencia**.

Estructura de la norma ISO 28000

A diferencia de la edición 2007, la norma ahora se organiza siguiendo la **Estructura Armonizada de 10 capítulos**, común a la mayoría de normas ISO modernas.

A continuación te presento el copy actualizado para cada sección.

4.1. Alcance (Scope)

Define los objetivos del sistema de gestión y establece cómo la organización aplicará los requisitos para proteger sus activos, personas, procesos e información. Incluye la identificación de actividades clave y del entorno operativo en el que se desempeña la organización.

4.2. Referencias normativas

Indica los documentos esenciales para interpretar el estándar, destacando las conexiones con la terminología de gestión de seguridad y resiliencia, como **ISO 22300**.

4.3. Términos y definiciones

Reúne vocabulario fundamental relacionado con seguridad, gestión del riesgo, resiliencia y protección de la cadena de actividades. Su objetivo es asegurar que todos los actores del sistema utilicen un lenguaje común y coherente.

4.4. Contexto de la organización

La organización debe analizar factores internos y externos que influyen en su seguridad y resiliencia. Esto incluye:

- Necesidades y expectativas de partes interesadas.
- Amenazas relevantes.
- Actividades críticas.

- Requisitos legales y regulatorios.
- Delimitación del alcance del Sistema de Gestión de la Seguridad y la Resiliencia.

Este análisis inicial es clave para definir controles adecuados y estrategias de protección reales.

4.5. Liderazgo

La alta dirección debe demostrar compromiso activo con la seguridad y la resiliencia. Entre sus responsabilidades se encuentran:

- Establecer una **política de seguridad y resiliencia**.
- Asignar roles y responsabilidades.
- Proporcionar recursos.
- Fomentar una cultura preventiva.

Su liderazgo garantiza coherencia entre la estrategia corporativa y los controles de seguridad implementados.

4.6. Planificación

En esta nueva versión, la planificación se enfoca en:

- La **identificación de riesgos y oportunidades**.
- La definición de **objetivos de seguridad**.

- El establecimiento de planes para gestionar amenazas, vulnerabilidades y eventos potenciales.
- La integración del pensamiento basado en riesgos en toda la organización.

La planificación adecuada permite anticipar incidentes y minimizar impactos.

4.7. Soporte

La gestión de la seguridad requiere recursos adecuados, incluyendo:

- Competencia y formación del personal.
- Conciencia organizacional.
- Comunicación interna y externa.
- Información documentada actualizada.

Esta sección asegura que el sistema esté debidamente respaldado y pueda operar eficazmente.

4.8. Operación

Uno de los apartados más robustos de la versión 2022. Incluye:

- Implementación de controles operativos de seguridad física, tecnológica y organizacional.
- Gestión de accesos, transporte, almacenamiento y protección de activos.

- Respuesta ante incidentes de seguridad.
- Mantenimiento de procesos esenciales.
- Coordinación de actores internos y externos.

Es el corazón práctico del sistema de gestión.

4.9. Evaluación del desempeño

La organización debe realizar:

- Monitoreo continuo.
- Medición de resultados.
- Auditorías internas.
- Revisión por la dirección.
- Evaluación de eficacia de procesos y controles.

Este apartado asegura que el sistema funcione y se mantenga actualizado frente a cambios del contexto.

4.10. Mejora continua

Finalmente, la norma exige:

- Detectar no conformidades.
- Implementar acciones correctivas.

- Ajustar el sistema según resultados obtenidos.
- Avanzar hacia un nivel de resiliencia cada vez mayor.

La mejora continua garantiza que la organización incremente su capacidad para anticipar, resistir y recuperarse de incidentes.

Certificación ISO-28000. Requerimientos y pasos para conseguirla

La **certificación ISO 28000 es un reconocimiento internacional que afirma que una empresa ha implementado de manera efectiva un sistema de gestión de seguridad para su cadena de suministro**. Obtener esta certificación implica cumplir con unos requisitos y seguir ciertos pasos que garantizan la seguridad y la integridad en todas las fases de la cadena logística.

Requisitos para la Certificación ISO 28000

- **Compromiso de la Alta Dirección:** la alta dirección debe comprometerse con el establecimiento, implementación y mejora continua del sistema de gestión de seguridad de la cadena de suministro.
- **Análisis de Riesgos y Amenazas:** identificación y evaluación de los riesgos y amenazas potenciales que podrían afectar la seguridad en la cadena de suministro.
- **Desarrollo de Políticas de Seguridad:** creación de políticas y objetivos de seguridad alineados con los requisitos de la ISO 28000.
- **Diseño e Implementación de Controles:** establecimiento de controles y medidas para reducir los riesgos, abarcando la seguridad física y la gestión de la información.

- **Formación**: formación del personal en aspectos de seguridad y sobre la importancia de cumplir con los protocolos.

- **Comunicación Interna y Externa**: establecimiento de canales de comunicación dentro de la empresa y con socios comerciales para compartir información de seguridad.

Pasos para Obtener la Certificación ISO 28000

- **Preparación Inicial:** acercamiento a los requisitos de la ISO 28000 y evaluación de la conformidad de la empresa.

- **Diseño del Sistema de Gestión:** desarrollo de un sistema de gestión de seguridad adaptado a las necesidades de la cadena de suministro de la empresa.

- **Implementación del Sistema**: puesta en práctica de los procesos y controles definidos en el sistema de gestión, asegurándose de que todos los empleados estén informados y formados.

- **Auditoría Interna:** realización de auditorías internas para evaluar la efectividad del sistema y corregir desviaciones.

- **Selección del Organismo:** elección de un organismo de certificación reconocido que llevará a cabo la auditoría final para otorgar la certificación.

- **Auditoría Externa**: auditoría realizada por el organismo para verificar el cumplimiento de la empresa con los requisitos de la norma.

- **Obtención de la Certificación: u**na vez superada la auditoría externa, la empresa recibe la Certificación ISO 28000, demostrando su compromiso con la seguridad en la cadena de suministro.

Obtener la Certificación ISO 28000 afirma el compromiso de la empresa con la seguridad en su cadena logística y fortalece su posición en el mercado, generando confianza entre los clientes y socios comerciales. La mejora continua es fundamental, ya que la **norma exige la revisión constante y la adaptación del sistema de gestión** para enfrentar los desafíos en la seguridad de la cadena de suministro.

Paso	Descripción
1. Preparación Inicial	La organización se familiariza con los requisitos de la ISO 28000:2022 y realiza un diagnóstico inicial para identificar brechas entre el estado actual y los requisitos del sistema de gestión de seguridad y resiliencia. Incluye revisión documental, entrevistas y evaluación preliminar del riesgo.
2. Diseño del Sistema de Gestión	Se desarrolla el Sistema de Gestión de la Seguridad y la Resiliencia, definiendo políticas, alcance, procedimientos, controles y responsabilidades. El diseño debe adaptarse al contexto de la organización y a las necesidades reales de protección de activos, procesos críticos e interacción con la cadena de suministro.
3. Implementación del Sistema	El sistema se pone en funcionamiento: los procesos se activan, los controles se aplican y se asegura la correcta capacitación del personal. Es una fase clave para generar cultura de seguridad, garantizar cumplimiento y verificar la operatividad de los controles definidos.
4. Auditoría Interna	Se realizan auditorías internas para evaluar la eficacia del sistema, identificar desviaciones, validar el cumplimiento y establecer oportunidades de mejora. Es un requisito obligatorio antes de la certificación y permite asegurar que el sistema funciona adecuadamente.
5. Selección del Organismo de Certificación	La organización elige un organismo acreditado y reconocido internacionalmente que ejecutará la auditoría de certificación. Esta selección debe basarse en su experiencia, acreditaciones y compatibilidad con el sector de la empresa.

Paso	Descripción
6. Auditoría Externa de Certificación	El organismo de certificación realiza una auditoría formal para verificar el cumplimiento de los requisitos de ISO 28000:2022. Normalmente se desarrolla en dos etapas: revisión documental y auditoría operativa.
7. Obtención de la Certificación	Si la organización cumple con los requisitos, el organismo emite el certificado ISO 28000. Esta certificación demuestra el compromiso con la seguridad y la resiliencia, fortaleciendo la confianza de clientes, socios y partes interesadas.
8. Mejora Continua	Luego de certificarse, la organización debe mantener y mejorar su sistema de gestión. La norma exige revisiones periódicas, control de riesgos, evaluación del desempeño y ajustes que permitan responder a nuevos desafíos en seguridad y continuidad operativa.

Software para ISO 28000

La Plataforma ISOTools facilita la automatización de la ISO 28000

La **Plataforma Tecnológica ISOTools** facilita la **implementación, automatización y mantenimiento** de **Sistemas de Gestión de Seguridad en la Cadena de Suministro conforme a la norma ISO28000**, sea cual sea el tamaño de la empresa.

ISOTools proporciona a las organizaciones del sector de logística y distribución una herramienta web para minimizar el riesgo de incidencias de seguridad y alcanzar los objetivos de almacenamiento y distribución.

La Plataforma Tecnológica permite seguir la lógica del **ciclo PHVA (Planear – Hacer – Verificar – Actuar)** , planificando la estrategia en toda la cadena de producción y distribución, desarrollo y mantenimiento de los procesos, medición de indicadores, evaluación y control de riesgos para alcanzar la mejora continua.

Este software también permite integrar la **ISO-28000**, con otras normas, como la norma ISO 9001 e ISO 14001, dando cumplimiento a todos los requisitos.

Fuentes bibliográficas:

- International Organization for Standardization. (2022). ISO 28000:2022 – Security and resilience — Security management systems — Requirements. ISO.

- Bureau Veritas. (s. f.). ISO 28000: Seguridad en la cadena de suministro. Recuperado de **https://www.bureauveritas.es/certificacion/seguridad-y-salud/iso-28000-seguridad-en-la-cadena-de-suministro**

- ISO. (s. f.). Gestión de riesgos. Recuperado de **https://www.iso.org/es/sectores/seguridad-proteccion-riesgo/gestion-de-riesgos**

ISOTools

+34 957 102 000
isotools.us