RESUMEN DE NORMA · CERT.GT

ISO/IEC 27001 en español

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Gerencia, responsables de seguridad y de cumplimiento.

ISO/IEC 27001 es la norma internacional para gestionar la seguridad de la información. No dice qué tecnología comprar: describe cómo organizarse para identificar riesgos, decidir qué controles aplicar y mejorar con el tiempo. Es la única de la familia 27000 que se puede certificar.

Lo esencial

- La versión vigente es la de 2022. Los certificados de la versión 2013 dejaron de ser válidos el 31 de octubre de 2025.
- Pide implementar un Sistema de Gestión de Seguridad de la Información (SGSI): políticas, responsables, análisis de riesgos, controles y revisión periódica.
- Se basa en el riesgo: cada organización decide qué controles aplica y lo justifica por escrito.
- Aplica a cualquier tamaño y sector; el alcance lo defines tú (toda la empresa, un servicio, una sede).

Qué exige: cláusulas 4 a 10

4. Contexto	Entender la organización, las partes interesadas y definir el alcance del SGSI.
5. Liderazgo	Compromiso de la dirección, política de seguridad y asignación de roles.
6. Planificación	Evaluar y tratar los riesgos, fijar objetivos y planificar los cambios.
7. Apoyo	Recursos, competencia, concientización, comunicación e información documentada.
8. Operación	Ejecutar el tratamiento de riesgos y controlar los procesos.
9. Evaluación	Medir, auditar internamente y revisar con la dirección.
10. Mejora	Corregir las no conformidades y mejorar de forma continua.

Los controles del Anexo A

El Anexo A lista 93 controles de referencia en cuatro temas. No todos son obligatorios: la Declaración de Aplicabilidad indica cuáles aplicas y por qué excluyes los demás.

Organizacionales (37)	Políticas, roles, inventario de activos, proveedores, nube, gestión de incidentes, continuidad, cumplimiento.
Personas (8)	Selección, contratos, concientización, proceso disciplinario, teletrabajo, reporte de eventos.
Físicos (14)	Perímetro, acceso a oficinas, equipo fuera de las instalaciones, medios, cableado, mantenimiento.
Tecnológicos (34)	Accesos, cifrado, respaldos, registros, vulnerabilidades, redes, desarrollo seguro.

Lo nuevo en la versión 2022

- Once controles nuevos: inteligencia de amenazas, seguridad en servicios de nube, preparación de TI para la continuidad, monitoreo de seguridad física, gestión de configuración, borrado de información, enmascaramiento de datos, prevención de fuga de datos, actividades de monitoreo, filtrado web y codificación segura.
- Los 114 controles de 2013 se reorganizaron y fusionaron en 93.
- Cada control tiene atributos (tipo, propiedad que protege, concepto de ciberseguridad) que facilitan relacionarlo con otros marcos.

Cómo empezar

- Consigue el respaldo explícito de la dirección: sin presupuesto ni autoridad, el SGSI no avanza.
- Define un alcance pequeño y útil, por ejemplo el servicio más crítico para tus clientes.
- Haz el inventario de activos de información y sus responsables.
- Evalúa los riesgos con un método simple y repetible, y decide el tratamiento de cada uno.
- Redacta la Declaración de Aplicabilidad y el plan de tratamiento de riesgos.
- Implementa, mide, audita internamente y haz la revisión por la dirección antes de buscar la certificación.

La certificación

- La otorga un organismo de certificación acreditado, no ISO.
- Etapa 1: revisión documental. Etapa 2: auditoría de la implementación.
- El certificado dura tres años, con auditorías de seguimiento anuales.
- No es obligatoria para beneficiarse de la norma: muchas organizaciones la usan como guía sin certificarse.

Errores frecuentes

- Tratarla como un proyecto de TI y no como un sistema de gestión de toda la organización.
- Copiar políticas de otra empresa que nadie lee ni cumple.
- Elegir un alcance tan amplio que el proyecto nunca termina.
- Documentar mucho y operar poco: el auditor pide evidencia de que los controles funcionan.

Texto oficial

ISO/IEC 27001:2022, publicada por ISO e IEC (iso.org). El texto oficial es de pago.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Resumen elaborado por cert.gt con fines educativos; no es el texto oficial de la norma ni sustituye asesoría legal o de cumplimiento. No es un documento de una entidad gubernamental. Puedes copiarlo y adaptarlo citando la fuente (CC BY 4.0).