Legalidad y Protección de la Información
ISO/CEI 27001:2022

Contenido

Introducción

La norma ISO/IEC 27001:2022 es una actualización clave en el ámbito de la seguridad de la información, diseñada para proporcionar un marco sistemático que permita gestionar, proteger y mejorar continuamente los sistemas de seguridad de la información dentro de una organización. Esta norma internacional establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), ofreciendo a las organizaciones una estructura integral para identificar y mitigar los riesgos asociados al manejo de datos sensibles.

La versión 2022 actualiza y refina los lineamientos previos, adaptándose a la evolución tecnológica y a las crecientes amenazas cibernéticas, integrando medidas más avanzadas de control de riesgos. Enfocado en la confidencialidad, integridad y disponibilidad de la información, ISO/IEC 27001:2022 se convierte en una herramienta crítica para proteger los activos de información, cumpliendo con las regulaciones y normativas vigentes a nivel global y fomentando la confianza de clientes y socios comerciales.

Diferencias entre ISO/IEC 27001:2013 & ISO/IEC 27001:2022

La norma ISO/IEC 27001 es un estándar internacional para la gestión de la seguridad de la información. En 2022, se publicó una nueva versión que actualiza la edición anterior de 2013. Aquí te detallo las principales diferencias entre ambas versiones:

Actualización de los controles en el Anexo A

- ISO/IEC 27001:2013: El Anexo A contiene 114 controles organizados en 14 cláusulas.
- ISO/IEC 27001:2022: Se redujeron a 93 controles agrupados en 4 categorías:
  - Controles organizacionales.
  - Controles tecnológicos.
  - Controles físicos.
  - Controles de personas.

Razón de cambio: Simplificar y agrupar de forma más clara los controles para facilitar la implementación y alinearlos con los riesgos emergentes.

2. Nuevos controles

En la versión 2022 se incluyen 11 nuevos controles para abordar riesgos tecnológicos actuales, como:

- Seguridad en el uso de la nube.
- Filtrado web.
- Prevención de fuga de datos (DLP).
- Seguridad de la información para entornos de trabajo remoto.
- Gestión de la configuración.

3. Controles fusionados o eliminados

ISO/IEC 27001:2022: Se consolidaron varios controles, eliminando redundancias. Por ejemplo, algunos controles relacionados con la criptografía se fusionaron, y otros menos utilizados se eliminaron o modificaron para mejorar su claridad.

4. Estructura del Anexo A

La nueva estructura de controles es más flexible y fácil de adaptar a diferentes organizaciones. Se busca que la norma sea más ágil, respondiendo a las tecnologías y prácticas actuales.

5. Mejor alineación con otros estándares

La versión 2022 se alinea mejor con otros marcos de ciberseguridad y gestión de riesgos, como el NIST Cybersecurity Framework y la norma ISO 31000 (Gestión de Riesgos), facilitando la integración de diferentes sistemas de gestión.

Terminología

Se han ajustado algunas definiciones y términos para alinearse con el lenguaje y prácticas modernas en ciberseguridad.

Énfasis en la mejora continua

La versión 2022 pone un mayor énfasis en la necesidad de que las organizaciones no solo implementen los controles, sino que también busquen continuamente mejorar sus prácticas de seguridad de la información.

Cláusulas 5 Controles organizacionales

5.1 Políticas de seguridad de la información

Control
La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.

5.2 Roles y responsabilidades de seguridad de la información

Control
Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.

5.3 Segregación de deberes

Control
Deben separarse los deberes y las áreas conflictivos de responsabilidad.

5.4 Responsabilidades de gestión

Control
La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.

5.5 Contacto con autoridades

Control
La organización deberá establecer y mantener contacto con las autoridades pertinentes.

5.6 Contacto con grupos de interés especial

Control
La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

5.7 Inteligencia de amenazas

Control
La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas.

5.8 Seguridad de la información en la gestión de proyectos.

Control
La seguridad de la información se integrará en la gestión de proyectos.

5.9 Inventario de información y otros activos asociados

Control

Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.

5.10 Uso aceptable de la información y otros activos asociados

Control
Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

5.11 Devolución de activos

Control
El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

5.12 Clasificación de la información

Control
La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

5.13 Etiquetado de información

Control
Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.

5.14 Transferencia de información

Control
Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

5.15 Control de acceso

Control

Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio.

5.16 Gestión de identidad

Control
Se gestionará el ciclo de vida completo de las identidades.

5.17 Información de autenticación

Control
La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

5.18 Derechos de acceso

Control
Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.

5.19 Seguridad de la información en las relaciones con los proveedores

Control
Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

5.20 Abordar la seguridad de la información en los acuerdos con los proveedores

Control
Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.

5.21 Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)

Control

Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores

Control
La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.

5.23 Seguridad de la información para el uso de servicios en la nube

Control
Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Control
La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Control
La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.

5.26 Respuesta a incidentes de seguridad de la información

Control
Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

5.27 Aprender de los incidentes de seguridad de la información

Control
El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para

fortalecer y mejorar los controles de seguridad de la información.

5.28 Recolección de evidencia

Control
La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

5.29 Seguridad de la información durante la interrupción

Control
La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

5.30 Preparación de las TIC para la continuidad del negocio

Control
La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

5.31 Requisitos legales, estatutarios, reglamentarios y contractuales

Control
Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.

5.32 Derechos de propiedad intelectual

Control
La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.

5.33 Protección de registros

Control

Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.

5.34 Privacidad y protección de la información de identificación personal (PII)

Control
La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

5.35 Revisión independiente de la seguridad de la información.

Control
El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

Control
El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente.

5.37 Procedimientos operativos documentados

Control
Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

Cláusulas 6 Controles de personas

6.1 Poner en pantalla

Control
Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los

requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.

6.2 Términos y condiciones de empleo

Control
Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.

6.3 Concientización, educación y capacitación en seguridad de la información

Control
El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.

6.4 Proceso Disciplinario

Control
Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

6.5 Responsabilidades después de la terminación o cambio de empleo

Control
Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas.

6.6 Acuerdos de confidencialidad o no divulgación

Control
Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

6.7 Trabajo remoto

Control
Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.

6.8 Informes de eventos de seguridad de la información

Control
La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

Cláusulas 7 Controles físicos

7.1 Perímetros físicos de seguridad

Control
Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.

7.2 Entrada física

Control
Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.

7.3 Asegurar oficinas, salas e instalaciones

Control
Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.

7.4 Monitoreo de seguridad física

Control
Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.

7.5 Protección contra amenazas físicas y ambientales.

Control
Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

7.6 Trabajar en áreas seguras

Control
Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.

7.7 Escritorio y pantalla despejados

Control
Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.

7.8 Emplazamiento y protección de equipos

Control
El equipo se colocará de forma segura y protegida.

7.9 Seguridad de los activos fuera de las instalaciones

Control
Se protegerán los activos fuera del sitio.

7.10 Medios de almacenamiento

Control
Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

7.11 Utilidades de apoyo

Control
Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

7.12 Seguridad del cableado

Control
Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.

7.13 Mantenimiento de equipo

Control
El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

7.14 Eliminación segura o reutilización de equipos

Control
Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Cláusulas 8 Controles tecnológicos

8.1 Dispositivos de punto final de usuario

Control
Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.

8.2 Derechos de acceso privilegiado

Control
La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.

8.3 Restricción de acceso a la información

Control
El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.

8.4 Acceso al código fuente

Control
El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.

8.5 Autenticación segura

Control
Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

8.6 Gestión de capacidad

Control
El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.

8.7 Protección contra malware

Control
La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.

8.8 Gestión de vulnerabilidades técnicas

Control
Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.

8.9 Gestión de la configuración

Control
Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

8.10 Eliminación de información

Control
La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.

8.11 Enmascaramiento de datos

Control
El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.

8.12 Prevención de fuga de datos

Control
Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

8.13 Copia de seguridad de la información

Control
Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.

8.14 Redundancia de las instalaciones de procesamiento de información

Control
Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15 Inicio sesión

Control

Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.

8.16 Actividades de seguimiento

Control
Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.

8.17 Sincronización de reloj

Control
Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.

8.18 Uso de programas de utilidad privilegiados

Control
El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.

8.19 Instalación de software en sistemas operativos

Control
Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

8.20 Seguridad en redes

Control
Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.

8.21 Seguridad de los servicios de red.

Control

Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

8.22 Segregación de redes

Control
Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

8.23 Filtrado web

Control
El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.

8.24 Uso de criptografía

Control
Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.

8.25 Ciclo de vida de desarrollo seguro

Control
Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.

8.26 Requisitos de seguridad de la aplicación

Control
Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

8.27 Principios de arquitectura e ingeniería de sistemas seguros

Control
Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.

8.28 Codificación segura

Control
Los principios de codificación segura se aplicarán al desarrollo de software.

8.29 Pruebas de seguridad en desarrollo y aceptación.

Control
Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.

8.30 Desarrollo subcontratado

Control
La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

8.31 Separación de los entornos de desarrollo, prueba y producción

Control
Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.

8.32 Gestión del cambio

Control
Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.

8.33 Información de prueba

Control
La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Control
Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

Bibliografía

ISO/CEI 27002:2022,Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información

ISO/CEI 27003,Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información sistemas — Orientación

ISO/CEI 27004,Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información — Seguimiento, medición, análisis y evaluación

ISO/CEI 27005,Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información

ISO 31000:2018,Gestión de riesgos — Directrices

Gómez Fernández, L. & Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad: (ed.). AENOR - Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ucags/titulos/53624

https://www.iso.org/es/contents/data/standard/08/28/82875.html?tid=331662889277#:~:text=La%20ISO%2FIEC%2027001%20promueve%20un%20enfoque%20integral%20de,riesgos%2C%20la%20resiliencia%20cibern%C3%A9tica%20y%20la%20excelencia%20operativa.