CHECKLIST
ISO 27001:2022

Esta lista de verificación se puede utilizar para evaluar la preparación de la organización para la certificación ISO 27001. Ayude a descubrir brechas en los procesos y revise el SGSI de su organización según la norma ISO 27001:2022.

HACKNOID

Desde las primeras etapas de planificación hasta las auditorías de certificación, esta lista de comprobación de la norma ISO 27001 proporciona un recurso completo para implementar eficazmente un Sistema de Gestión de Seguridad de la Información (SGSI).

En nuestro compromiso por promover la mejora continua en las organizaciones, hemos creado esta lista de comprobación ISO 27001.

Esta lista de comprobación tiene por objeto proporcionar orientación y las mejores prácticas para lograr el cumplimiento de las normas internacionales y garantizar el más alto nivel de seguridad de la información.

Adicionalmente desde el equipo de Hacknoid estaremos incorporando las recomendaciones que atañen a nuestro ámbito de alcance para poder ayudar a las organizaciones en el cumplimiento y mejor implementación de cada control.

Esa columna no necesariamente debe ser tomada en cuenta por el lector, sino que es una información adicional que puede servirles a la hora de considerar una mejor solución y automatización del control.

¿Qué objetivo tienen los controles y cuál es la re-estructura propuesta desde la ISO 27001: 2013 a la ISO 27001:2022?

Los controles buscan ordenar y estructurar aquellos elementos que deben considerarse en una gestión de seguridad de la información para que sea completa y esté debidamente cubierta en su faceta preventiva, es decir, antes de que las "cosas sucedan", y por tanto evitar al máximo posible que, al tener un incidente, éstos impacten fuertemente a la organización.

Sin embargo, la lista de controles es simplemente una enumeración de descriptiva, y no específica de su implementación final, dejando esto a criterio y recursos de la organización cómo se realizará dicha implementación y los elementos que utilizará como herramientas para cada caso.

De la versión anterior de la ISO, se redujo la cantidad de controles de 114 a 93 y se reorganizaron en **cuatro categorías**, incorporando nuevos conceptos dentro del mundo de la seguridad de la información como el de **inteligencia de amenazas, seguridad en la nube, y fugas de datos.** De esta forma tenemos:

- Controles organizativos: 37
- Controles de personas: 8
- Controles físicos: 14
- Controles tecnológicos: 34

NOTA

Es importante destacar que las empresas certificadas en la versión anterior ISO 27001:2013 tienen hasta octubre de 2025 para regularizar su situación, adaptándose a los nuevos requisitos de la versión 2022.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

A continuación para ser una guía para aquellos que ya tengan implementada la versión anterior de la ISO (27001:2013), incorporaremos un mapeo entre los controles de las dos versiones para facilitar la actualización.

Se destaca del cuadro anterior los **11 nuevos controles** que se han incorporado. Estos son:

1. Inteligencia de amenazas (A.5.7)

Implementación de procesos para recopilar, analizar y utilizar **inteligencia de amenazas** para mejorar la seguridad de la información.

Ejemplo en una entidad de Educación (Universidades, Institutos, Colegios)

📌 **Ejemplo:**
Una universidad monitorea fuentes de inteligencia de amenazas como **CISA KEV (Known Exploited Vulnerabilities)** y detecta que hay una vulnerabilidad crítica en **Apache Tomcat**, que es explotada activamente en ataques contra portales de estudiantes.
✅ **Acción:** El equipo de TI prioriza la actualización inmediata de **Apache Tomcat** en sus servidores web y bloquea temporalmente accesos externos hasta aplicar el parche.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

2. Seguridad en el uso de servicios en la nube (A.5.23)

Aplicación de controles de seguridad específicos para proteger los datos y la infraestructura en entornos de **computación en la nube.**

Ejemplo Retail

Una cadena de supermercados protege su plataforma e-commerce en la nube con autenticación multifactor (MFA) para los administradores.

3. Prevención de fuga de datos (A.5.30)

Implementación de medidas para prevenir la pérdida, filtración o

Ejemplo en Industria de construcción

Un proveedor de infraestructura usa herramientas para evitar que sus empleados copien planos de proyectos estratégicos en dispositivos USB no autorizados.

4. Monitoreo de seguridad física (A.5.24)

Uso de sistemas de vigilancia y monitoreo para detectar accesos no autorizados o incidentes en las instalaciones físicas.

Ejemplo Industria de alimentos: Una planta de producción usa lectores biométricos para restringir el acceso al área donde se manipulan recetas secretas.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

5. Gestión de la configuración (A.5.25)

Establecimiento de un proceso formal para la gestión de configuraciones de hardware, software y sistemas.

Ejemplo Retail

Un supermercado documenta todas las configuraciones de su sistema de punto de venta (POS) para evitar errores en futuras actualizaciones.

6. Eliminación de información (A.5.26)

Definición de procesos seguros para la eliminación de datos cuando ya no sean necesarios.

Ejemplo Estudios profesionales

Un despacho contable elimina registros de clientes antiguos después de cumplir con los plazos legales de retención.

7. Enmascaramiento de datos (A.5.27)

Uso de técnicas de enmascaramiento para proteger datos sensibles en ambientes de prueba o desarrollo.

Ejemplo Salud

Un hospital reemplaza nombres reales por datos ficticios al probar un nuevo sistema de historias clínicas electrónicas.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

8. Prevención de código malicioso (A.5.28)

Aplicación de medidas de protección contra malware, virus y otras amenazas basadas en software malicioso.

Ejemplo Educación

Una universidad implementa restricciones para evitar que los estudiantes descarguen software malicioso en laboratorios de computación.

9. Seguridad en tecnologías y servicios de seguridad de la información (A.5.29)

Protección específica de tecnologías y servicios diseñados para gestionar la seguridad de la información.

Ejemplo Gobierno

Un ministerio cifra y restringe el acceso a su sistema de monitoreo de seguridad para evitar alteraciones en los registros.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

10. Monitoreo de actividades de seguridad (A.5.31)

Implementación de mecanismos para supervisar y registrar eventos de seguridad en tiempo real.

Ejemplo Industria de alimentos

Un fabricante de bebidas configura alertas para identificar intentos de acceso fuera del horario laboral a sus servidores ERP.

11. Resiliencia de las TIC (A.5.32)

Establecimiento de estrategias para asegurar la disponibilidad y recuperación de los sistemas TIC en caso de incidentes.

Ejemplo Gobierno

Un ayuntamiento implementa servidores de contingencia para mantener en funcionamiento su sistema de atención ciudadana ante una caída de infraestructura.

Mapeo de cambios entre la versión ISO 27001:2013 y la ISO 27001:2022

Categoría ISO 27001:2013	Cantidad de Controles (2013)	Categoría ISO 27001:2022	Cantidad de Controles (2022)	Notas/Revisión
A.5 - Políticas de seguridad de la información	2	**A.5 - Controles organizativos**	37	Integrado con otros controles organizativos
A.6 - Organización de la seguridad de la información	7			Reestructurado dentro de los controles organizativos
A.7 - Seguridad de los recursos humanos	6	**A.6 - Controles de personas**	8	Se fusionaron controles de seguridad de RRHH
A.8 - Gestión de activos	10	**A.7 - Controles físicos**	14	Incluye aspectos físicos de la seguridad
A.9 - Control de acceso	14	**A.8 - Controles tecnológicos**	34	Integrado en la nueva estructura tecnológica
A.10 - Criptografía	2			Incluido en controles tecnológicos
A.11 - Seguridad física y del entorno	15			Integrado en los controles físicos
A.12 - Seguridad en las operaciones	14			Redistribuido entre controles tecnológicos y organizativos
A.13 - Seguridad en las comunicaciones	7			Parte de controles tecnológicos
A.14 - Adquisición, desarrollo y mantenimiento de sistemas	13			Integrado en controles tecnológicos
A.15 - Relaciones con proveedores	5			Fusionado en controles organizativos
A.16 - Gestión de incidentes de seguridad	7			Se mantiene en organizativos
A.17 - Continuidad del negocio en seguridad de la información	4			Incorporado en controles organizativos
A.18 - Cumplimiento normativo	8			Integrado en controles organizativos

* En naranjo donde opera Hacknoid

¿Cómo apoya esta gestión Hacknoid?

Categoría ISO 27001:2013	Cantidad de Controles (2013)	Categoría ISO 27001:2022	Cantidad de Controles (2022)	Notas/Revisión
A.5 - Políticas de seguridad de la información	2	**A.5 - Controles organizativos**	37	Integrado con otros controles organizativos

En este punto la reportería que proporciona Hacknoid se puede personalizar y alinear a normas, marcos, y demás necesidades sobre los controles organizativos, como aquellas vulnerabilidades que puedan comprometer el proceso de continuidad de negocio.
Un destacado nuevo control referido a la inteligencia de amenazas, es una GRAN incorporación de la plataforma Hacknoid, en donde se vincula la inteligencia de amenazas en su algoritmo de priorización de vulnerabilidades HARVEX para lograr una óptima priorización de las vulnerabilidades que se deben resolver de forma urgente.

Categoría ISO 27001:2013	Cantidad de Controles (2013)	Categoría ISO 27001:2022	Cantidad de Controles (2022)	Notas/Revisión
A.9 - Control de acceso	14	**A.8 - Controles tecnológicos**	34	Integrado en la nueva estructura tecnológica

Todos los controles tecnológicos comparten en cierta medida o en su totalidad, las funcionalidades de gestión de vulnerabilidades que hacknoid provee. Siendo de las primeras líneas de defensa, ser una defensa proactiva, preventiva y que una efectiva gestión permitiría cerrar las puertas de entrada de los atacantes..

Si bien para los controles propuestos en A.6 y A.7 de la versión 2022, Hacknoid no aplica por tratarse de controles fuera el ámbito tecnológico IT, pueden integrarse en un sistema de compliance que maneje la organización, que además se nutra automáticamente de los resultados en tiempo real que provea Hacknoid sobre el ámbito de ciberseguridad.

Controles Organizativos

Principalmente en reportes e informes, y en términos de Inteligencia de Amenazas como se explicó anteriormente, el monitoreo, y siendo parte de la gestión para la resiliencia de TI por ser una plataforma que tiene una perspectiva preventiva.

Se centran en las políticas, procesos y gestión de la seguridad de la información.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.5.1 Políticas para la seguridad de la información			
A.5.2 Funciones y responsabilidades de la seguridad de la información			
A.5.3 Segregación de funciones			
A.5.4 Contacto con autoridades			
A.5.5 Contacto con grupos de interés			
A.5.6 Seguridad de la información en la gestión de proyectos			
A.5.7 Inteligencia de amenazas (Nuevo)			
A.5.8 Seguridad de la información en el uso de servicios en la nube			
A.5.9 Gestión de activos			
A.5.10 Uso aceptable de activos			
A.5.11 Retorno de activos			
A.5.12 Clasificación de la información			
A.5.13 Etiquetado de la información			
A.5.14 Transferencia de información			
A.5.15 Seguridad en el desarrollo de relaciones con proveedores			
A.5.16 Gestión de la seguridad en la cadena de suministro			
A.5.17 Monitoreo, revisión y cambios en los servicios proporcionados por terceros			

Controles Organizativos

Principalmente en reportes e informes, y en términos de Inteligencia de Amenazas como se explicó anteriormente, el monitoreo, y siendo parte de la gestión para la resiliencia de TI por ser una plataforma que tiene una perspectiva preventiva.

Se centran en las políticas, procesos y gestión de la seguridad de la información.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.5.18 Seguridad de la información para el uso de dispositivos móviles			
A.5.19 Seguridad en el teletrabajo			
A.5.20 Gestión de accesos y privilegios			
A.5.21 Gestión de identidades			
A.5.22 Uso de autenticación segura			
A.5.23 Seguridad en el uso de servicios en la nube (Nuevo)			
A.5.24 Monitoreo de seguridad física (Nuevo)			
A.5.25 Gestión de la configuración (Nuevo)			
A.5.26 Eliminación de información (Nuevo)			
A.5.27 Enmascaramiento de datos (Nuevo)			
A.5.28 Prevención de código malicioso (Nuevo)			
A.5.29 Seguridad de la información en tecnologías y servicios de seguridad de la información (Nuevo)			
A.5.30 Prevención de fuga de datos (Nuevo)			
A.5.31 Monitoreo de actividades de seguridad (Nuevo)			
A.5.32 Resiliencia de las TIC (Nuevo)			
A.5.33 Planificación de la continuidad del negocio			
A.5.34 Implementación de la continuidad del negocio			
A.5.35 Validación de la continuidad del negocio			
A.5.36 Redundancias en la tecnología de la información y comunicaciones			

Controles de Personas

Establecen medidas de seguridad relacionadas con el personal y su concienciación.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.6.1 Screening del personal			
A.6.2 Términos y condiciones de empleo			
A.6.3 Responsabilidades posteriores al empleo			
A.6.4 Concienciación, educación y formación en seguridad de la información			
A.6.5 Procesos disciplinarios en seguridad de la información			
A.6.6 Obligaciones de confidencialidad y no divulgación			
A.6.7 Gestión de la seguridad en las relaciones laborales			
A.6.8 Denuncia de incidentes de seguridad de la información			

Controles Físicos

Aseguran la protección de las instalaciones y dispositivos físicos.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.7.1 Seguridad en las instalaciones físicas			
A.7.2 Seguridad en áreas seguras			
A.7.3 Protección contra amenazas físicas y ambientales			
A.7.4 Seguridad del equipo			
A.7.5 Eliminación de activos físicos			
A.7.6 Protección contra interrupciones y desastres			
A.7.7 Seguridad del cableado			
A.7.8 Bloqueo y protección de estaciones de trabajo			
A.7.9 Uso seguro de dispositivos móviles			
A.7.10 Restricciones en el uso de dispositivos personales			
A.7.11 Gestión segura del almacenamiento			
A.7.12 Eliminación de datos en medios físicos			
A.7.13 Protección contra accesos no autorizados a la información			
A.7.14 Supervisión de acceso físico			

Controles Tecnológicos

Aseguran la protección de las instalaciones y dispositivos físicos.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.8.1 Gestión de la seguridad en redes			
A.8.2 Segmentación de redes			
A.8.3 Protección contra malware			
A.8.4 Gestión de parches y vulnerabilidades			
A.8.5 Registro de eventos de seguridad de la información			
A.8.6 Monitoreo del tráfico de red y actividades sospechosas			
A.8.7 Protección de datos en tránsito			
A.8.8 Protección de datos en almacenamiento			
A.8.9 Control de accesos a la información y sistemas			
A.8.10 Gestión de claves criptográficas			
A.8.11 Seguridad en el desarrollo de software			
A.8.12 Seguridad en pruebas y validación de software			
A.8.13 Gestión de cambios en sistemas de información			
A.8.14 Seguridad en bases de datos			
A.8.15 Gestión de logs y registros de auditoría			
A.8.16 Gestión de vulnerabilidades en software y hardware			

Controles Tecnológicos

Dentro de las capas de la ciberseguridad y los nichos específicos donde cada herramienta actúa (e idealmente las organizaciones las considerarán todas), para llegar al dato específico, es necesario saltarse varios pasos anteriores, y dentro de ellos, las vulnerabilidades que dejemos expuestas, son las primeras puertas de entrada y barreras que un atacante irá a probar. Por eso Hacknoid, entra a formar parte de las primeras barreras (preventivas) para implementar y compartir o efectivamente realizar, varios de los controles de esta categoría.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.8.17 Protección contra ataques de denegación de servicio (DDoS)			
A.8.18 Configuración segura de sistemas y dispositivos			
A.8.19 Seguridad en interfaces de programación de aplicaciones (APIs)			
A.8.20 Seguridad en la nube y entornos virtuales			
A.8.21 Detección y respuesta ante incidentes de seguridad			
A.8.22 Uso seguro de herramientas administrativas			
A.8.23 Seguridad en aplicaciones web			
A.8.24 Protección contra amenazas internas			
A.8.25 Gestión de accesos remotos			
A.8.26 Monitoreo de comportamientos anómalos			
A.8.27 Gestión segura de backups			
A.8.28 Seguridad en el correo electrónico			

Controles Tecnológicos

Dentro de las capas de la ciberseguridad y los nichos específicos donde cada herramienta actúa (e idealmente las organizaciones las considerarán todas), para llegar al dato específico, es necesario saltarse varios pasos anteriores, y dentro de ellos, las vulnerabilidades que dejemos expuestas, son las primeras puertas de entrada y barreras que un atacante irá a probar. Por eso Hacknoid, entra a formar parte de las primeras barreras (preventivas) para implementar y compartir o efectivamente realizar, varios de los controles de esta categoría.

ISO 27001:2022 Checklist	Completamente implementado	Parcialmente implementado	Aún por empezar
A.8.29 Protección de dispositivos IoT			
A.8.30 Protección contra ataques de ingeniería social			
A.8.31 Seguridad en dispositivos móviles			
A.8.32 Seguridad en la infraestructura de telecomunicaciones			
A.8.33 Seguridad en entornos DevOps y CI/CD			
A.8.34 Protección contra amenazas avanzadas persistentes (APT)			

HACKNOID

Solicita una Demo de Hacknoid

www.hacknoid.com

URUGUAY
Durazno 1504 Oficina 1 esq. Martínez Trueba
Palermo, Montevideo

CHILE
Av. Nueva Tajamar 481 Torre Norte, Of 1403,
Las Condes, Santiago