CONTROLES
ISO 27001:2022

93 Controles ISO/IEC 27001:2022

- **37** Controles Organizacionales
- **8** Controles de Personas
- **14** Controles Físicos
- **34** Controles Tecnológicos

La norma menciona que se añadieron **11 controles completamente nuevos** respecto a la versión anterior (2013). El resto de los controles provienen de una consolidación, fusión o reestructuración de los antiguos 114 controles.

Recurso Gratuito Hacker Mentor
2025 Controles ISO/IEC 27001:2022

HACKER MENTOR

Controles Organizacionales

5.1 Políticas de seguridad de la información
5.2 Roles y responsabilidades de seguridad de la información
5.3 Segregación de funciones
5.4 Gestión de contactos con las autoridades
5.5 Gestión de contactos con grupos de interés
5.6 Seguridad en la gestión de proyectos
5.7 Inventario de activos
5.8 Aceptación del uso de activos
5.9 Devolución de activos
5.10 Clasificación de la información
5.11 Etiquetado de la información
5.12 Manipulación de la información
5.13 Política de control de acceso
5.14 Gestión de acceso de usuario
5.15 Gestión de credenciales de autenticación
5.16 Revisión de los derechos de acceso
5.17 Responsabilidades del usuario
5.18 Acceso a código fuente
5.19 Política de uso de criptografía
5.20 Gestión de claves criptográficas
5.21 Gestión de configuraciones
5.22 Eliminación de información
5.23 Gestión de amenazas
5.24 Seguridad de la información en relaciones con proveedores
5.25 Gestión de la cadena de suministro de TIC
5.26 Supervisión, revisión y evaluación de proveedores
5.27 Seguridad de la información para uso de servicios en la nube
5.28 Gestión de eventos de seguridad de la información
5.29 Gestión de incidentes de seguridad de la información
5.30 Aprendizaje de incidentes de seguridad de la información
5.31 Recopilación de evidencias
5.32 Continuidad de la seguridad de la información
5.33 Redundancia
5.34 Cumplimiento de requisitos legales
5.35 Propiedad intelectual
5.36 Protección de registros
5.37 Privacidad y protección de información personal

34

Controles Tecnológicos

8.1 Gestión de identidades
8.2 Gestión de autenticación
8.3 Gestión de acceso
8.4 Control de acceso a información
8.5 Restricción de acceso a código
8.6 Seguridad de aplicaciones en redes públicas
8.7 Protección de transacciones
8.8 Control de software instalado
8.9 Protección contra malware
8.10 Copias de seguridad
8.11 Registro y monitoreo
8.12 Sincronización de reloj
8.13 Instalación de software
8.14 Gestión de vulnerabilidades
8.15 Uso de tecnologías de monitoreo
8.16 Filtrado web
8.17 Prevención de pérdida de datos
8.18 Seguridad de correo electrónico
8.19 Seguridad de redes
8.20 Segregación en redes
8.21 Seguridad en servicios de red
8.22 Intercambio de información
8.23 Mensajería electrónica
8.24 Acuerdos de confidencialidad
8.25 Protección de datos de prueba
8.26 Revisión técnica tras cambios en sistemas
8.27 Gestión de cambios
8.28 Política de desarrollo seguro
8.29 Entorno de desarrollo seguro
8.30 Externalización del desarrollo
8.31 Pruebas de seguridad funcional
8.32 Pruebas de aceptación de seguridad
8.33 Ingeniería de seguridad
8.34 Control de cambios en paquetes de software

8

Controles de Personas

6.1 Cribado
6.2 Términos y condiciones del empleo
6.3 Responsabilidades de seguridad de la información
6.4 Concienciación, educación y formación
6.5 Disciplinas
6.6 Terminación o cambio de empleo
6.7 Responsabilidades de seguridad después del empleo
6.8 Acuerdos de confidencialidad o no divulgación

14

Controles Físicos

7.1 Perímetro de seguridad física
7.2 Controles de acceso físico
7.3 Seguridad en oficinas, locales y facilidades
7.4 Protección contra amenazas físicas y ambientales
7.5 Trabajo en áreas seguras
7.6 Áreas de carga y descarga
7.7 Seguridad del equipo
7.8 Seguridad del cableado
7.9 Mantenimiento del equipo
7.10 Eliminación segura o reutilización de equipos
7.11 Retiro de activos
7.12 Equipos fuera del sitio
7.13 Equipos desatendidos
7.14 Puesto de trabajo limpio y pantalla despejada

93 Controles ISO/IEC 27001:2022

Recurso Gratuito Hacker Mentor
2025 Controles ISO/IEC 27001:2022

HM HACKER MENTOR

CURSO GRATUITO

SGSI

AUDITOR ISO 27001:2022 FUNDAMENTALS

Clases Virtuales
En Vivo

5 Horas Académicas

abril **30** / mayo **01**

7pm GMT-5
Hora de:

34

Controles Tecnológicos

8.1 Gestión de identidades
8.2 Gestión de autenticación
8.3 Gestión de acceso
8.4 Control de acceso a información
8.5 Restricción de acceso a código
8.6 Seguridad de aplicaciones en redes públicas
8.7 Protección de transacciones
8.8 Control de software instalado
8.9 Protección contra malware
8.10 Copias de seguridad
8.11 Registro y monitoreo
8.12 Sincronización de reloj
8.13 Instalación de software
8.14 Gestión de vulnerabilidades
8.15 Uso de tecnologías de monitoreo
8.16 Filtrado web
8.17 Prevención de pérdida de datos
8.18 Seguridad de correo electrónico
8.19 Seguridad de redes
8.20 Segregación en redes
8.21 Seguridad en servicios de red
8.22 Intercambio de información
8.23 Mensajería electrónica
8.24 Acuerdos de confidencialidad
8.25 Protección de datos de prueba
8.26 Revisión técnica tras cambios en sistemas
8.27 Gestión de cambios
8.28 Política de desarrollo seguro
8.29 Entorno de desarrollo seguro
8.30 Externalización del desarrollo
8.31 Pruebas de seguridad funcional
8.32 Pruebas de aceptación de seguridad
8.33 Ingeniería de seguridad
8.34 Control de cambios en paquetes de software

Controles Organizacionales 37

14 Controles Físicos

Controles de Personas 8

34 Controles Tecnológicos

93 Controles ISO/IEC 27001:2022

Recurso Gratuito Hacker Mentor
2025 Controles ISO/IEC 27001:2022

IT Services Workflow From Request to Resolution

01 Service Request Intake

Receive service requests from users/customers via various channels (e.g., email, ticketing system, phone).

02 Ticket Creation

Create a ticket in the IT service management (ITSM) system for each service request.

03 Initial Triage

Review the ticket to determine its priority and assign it to the appropriate support team or individual

04 Investigation

The assigned support team or individual investigates the reported issue or fulfills the requested service.

05 Communication

Keep the requester informed about the progress of their ticket, including any findings, troubleshooting steps, or estimated time for resolution.

06 Resolution

Document the steps taken, changes made, and any additional information relevant to the ticket.

07 Testing and Verification

Validate the resolution or service delivery to ensure it meets the requester's requirements and resolves the reported issue.

08 Ticket Closure

Update the ticket status to reflect the resolution or service completion

09 Knowledge Base Update

Document the troubleshooting steps, solutions, and any new knowledge gained during the process

10 Continuous Improvement

Analyze trends and patterns in service requests and resolutions to identify recurring issues or areas for process improvement.