Categorías de controles

Los controles dentro de la ciberseguridad se agrupan en **tres categorías principales**:

- **Controles administrativos/gerenciales**
- **Controles técnicos**
- **Controles físicos/operativos**

Controles administrativos/gerenciales

Abordan el componente humano de la ciberseguridad. Estos controles incluyen políticas y procedimientos que definen cómo una organización gestiona los datos y establecen claramente las responsabilidades de los empleados, incluyendo su rol en la protección de la organización.
Aunque los controles administrativos suelen estar basados en políticas, **su cumplimiento puede requerir el uso de controles técnicos o físicos**.

Controles técnicos

Consisten en soluciones como cortafuegos (firewalls), sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), antivirus (AV), cifrado, etc.
Estos controles pueden utilizarse de múltiples formas para lograr los objetivos y metas de la organización.

Controles físicos/operativos

Incluyen cerraduras de puertas, cerraduras de gabinetes, cámaras de vigilancia, lectores de tarjetas, etc.

Se utilizan para **limitar el acceso físico a los activos físicos** por parte de personal no autorizado.

Tipos de controles

Los tipos de controles incluyen, pero no se limitan a:

- **Preventivos:** Diseñados para evitar que ocurra un incidente.
- **Correctivos:** Se utilizan para restaurar un activo después de un incidente.
- **Detectivos:** Implementados para determinar si ha ocurrido o está ocurriendo un incidente.
- **Disuasivos:** Diseñados para desalentar los ataques.

Estos controles **trabajan en conjunto para proporcionar una defensa en profundidad y proteger los activos**.

Controles administrativos/gerenciales

Nombre del control	Tipo de control	Propósito del control
Mínimo privilegio	Preventivo	Reducir el riesgo y el impacto general de un actor malicioso interno o cuentas comprometidas
Planes de recuperación ante desastres	Correctivo	Proporcionar continuidad del negocio
Políticas de contraseñas	Preventivo	Reducir la probabilidad de compromiso de cuentas mediante ataques de fuerza bruta o diccionario

Políticas de control de acceso	Preventivo	Reforzar la confidencialidad e integridad al definir qué grupos pueden acceder o modificar datos
Políticas de gestión de cuentas	Preventivo	Gestionar el ciclo de vida de las cuentas, reducir la superficie de ataque y limitar el impacto de antiguos empleados descontentos o cuentas por defecto
Separación de funciones	Preventivo	Reducir el riesgo y el impacto general de un actor malicioso interno o cuentas comprometidas

---

Controles técnicos

Nombre del control	Tipo de control	Propósito del control
Cortafuegos (Firewall)	Preventivo	Filtrar tráfico no deseado o malicioso que intenta ingresar a la red
IDS/IPS	Detectivo	Detectar y prevenir tráfico anómalo que coincide con firmas o reglas
Cifrado	Disuasivo	Proporcionar confidencialidad a información sensible
Copias de seguridad (Backups)	Correctivo	Restaurar/recuperar datos después de un evento
Gestión de contraseñas	Preventivo	Reducir la fatiga de contraseñas
Software antivirus (AV)	Preventivo	Analiza para detectar y poner en cuarentena amenazas conocidas
Monitoreo, mantenimiento e intervención manual	Preventivo	Necesario para identificar y gestionar amenazas, riesgos o vulnerabilidades en sistemas desactualizados

---

Controles físicos/operativos

Nombre del control	Tipo de control	Propósito del control
Caja fuerte con temporizador	Disuasivo	Reducir la superficie de ataque y el impacto general de amenazas físicas
Iluminación adecuada	Disuasivo	Disuadir amenazas al limitar lugares donde esconderse
Televisión de circuito cerrado (CCTV)	Preventivo / Detectivo	Su presencia puede reducir el riesgo de ciertos eventos, y también puede usarse después de un incidente para investigar
Gabinetes con cerradura (para equipos de red)	Preventivo	Reforzar la integridad evitando el acceso físico no autorizado al equipo de red
Señalización de empresa de alarmas	Disuasivo	Disuadir ciertos tipos de amenazas al hacer parecer poco probable un ataque exitoso
Cerraduras	Disuasivo / Preventivo	Reforzar la integridad disuadiendo y evitando el acceso físico no autorizado
Detección y prevención de incendios (alarma, rociadores, etc.)	Detectivo / Preventivo	Detectar incendios en la ubicación física y prevenir daños a activos físicos como inventario, servidores, etc.