# Categorías de control

## Categorías de control

Dentro de la ciberseguridad, los controles se agrupan en tres categorías principales:

* Controles administrativos/directivos
* Controles técnicos
* Controles físicos

Los **controles administrativos/directivos** se enfocan en el componente humano de la ciberseguridad. Incluyen políticas y procedimientos que definen cómo una organización gestiona los datos y establecen las responsabilidades de los empleados y las empleadas en la protección de la organización. Si bien este tipo de controles se basan principalmente en políticas, su cumplimiento puede requerir el uso de controles técnicos o físicos.

Por su parte, los **controles técnicos** comprenden soluciones como cortafuegos (firewalls), sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), productos audiovisuales (AV), cifrado o encriptación, entre otros. Estos controles se emplean de diversas formas para cumplir con los objetivos de la organización en términos de ciberseguridad.

En tanto, los **controles físicos** abarcan cerraduras de puertas y de gabinetes, cámaras de vigilancia y lectores de tarjetas, entre otros. Su propósito es proteger los activos físicos de la organización y prevenir posibles intrusiones o daños.

## Tipos de controles

Existen cinco tipos de controles:

1. Preventivos
2. Correctivos
3. De detección
4. Disuasivos
5. Compensatorios

Estos controles trabajan en conjunto para asegurar y proteger los activos. Los **controles preventivos** están diseñados para evitar que ocurra un incidente. El fin de los **controles correctivos**, en cambio, es recuperar un activo después de un incidente. Los **controles de detección** se implementan para determinar si ya ha ocurrido un incidente o está en proceso. Por su parte, los **controles disuasivos** están diseñados para desalentar los ataques. Y, por último, los **controles compensatorios** se utilizan para fortalecer la seguridad de un activo cuando los controles existentes no son suficientes para protegerlo adecuadamente.

Te recomendamos revisar las siguientes tablas para obtener detalles específicos sobre cada tipo de control y su propósito.

| **Controles administrativos** | | |
| --- | --- | --- |
| **Nombre de control** | **Tipo de control** | **Objetivo del control** |
| Principio de mínimo privilegio | Preventivo | Reducir el riesgo y el impacto general de las cuentas maliciosas o comprometidas. |
| Planes de recuperación ante incidentes | Correctivo | Evitar la interrupción del negocio. |
| Políticas de contraseñas | Preventivo | Reducir la probabilidad de comprometer la cuenta debido a técnicas de ataque por fuerza bruta o diccionario. |
| Políticas de control de acceso | Preventivo | Reforzar la confidencialidad y la integridad al definir qué grupos pueden acceder o modificar los datos. |
| Políticas de gestión de cuentas | Preventivo | Gestionar el ciclo de vida de la cuenta, reducir la superficie expuesta a ataques y limitar el impacto general de ex empleados/as disconformes y el uso predeterminado de la cuenta. |
| Separación de funciones | Preventivo | Reducir el riesgo y el impacto general de las cuentas maliciosas o comprometidas. |

| **Controles técnicos** | | |
| --- | --- | --- |
| **Nombre de control** | **Tipo de control** | **Objetivo del control** |
| Cortafuegos (firewall) | Preventivo | Filtrar el tráfico no deseado/malicioso que ingresa a la red interna. |
| Sistema de detección de intrusiones (IDS)/Sistema de prevención de intrusiones (IPS) | De detección | Detectar y prevenir el tráfico anómalo que coincide con una firma o regla. |
| Cifrado | Disuasivo | Garantizar la confidencialidad de la información sensible. |
| Copias de seguridad | Correctivo | Restablecimiento/recuperación luego de un incidente. |
| Gestión de contraseñas | Preventivo | Reducir la fatiga de contraseña. |
| Software de antivirus (AV) | Correctivo | Detectar amenazas conocidas y aislarlas. |
| Monitoreo manual, mantenimiento e intervención | Preventivo | Necesario para identificar y administrar amenazas, riesgos o vulnerabilidades a sistemas desactualizados. |

| **Controles físicos** | | |
| --- | --- | --- |
| **Nombre de control** | **Tipo de control** | **Objetivo del control** |
| Caja fuerte con control de tiempo | Disuasivo | Reduce la superficie expuesta a ataques y el impacto general de las amenazas físicas. |
| Iluminación adecuada | Disuasivo | Disuadir las amenazas al limitar los lugares “ocultos”. |
| Vigilancia de circuito cerrado de televisión (CCTV) | Preventivo/De detección | La televisión de circuito cerrado es un control tanto preventivo como de detección, porque su presencia puede reducir el riesgo de que ocurran ciertos tipos de eventos y, a la vez, se puede usar después de un incidente para ver qué ocurrió. |
| Cerradura de gabinetes (para equipos de red) | Preventivo | Aumentar la integridad al evitar que personas no autorizadas accedan físicamente o modifiquen el equipo de infraestructura de la red. |
| Carteles que indican el nombre de la empresa proveedora del servicio de alarmas | Disuasivo | Reducir la probabilidad de éxito de ciertos tipos de amenazas al dar la apariencia de que un ataque exitoso es poco probable. |
| Cerraduras | Disuasivo/Preventivo | Aumentar la integridad al evitar que personas no autorizadas accedan físicamente a los activos. |
| Detección y prevención de incendios (alarma de incendios, sistema de rociadores, entre otros) | De detección/Preventivo | Detectar incendios en la ubicación física y evitar daños a los activos, como inventario y servidores, entre otros. |