Categorías de control

Categorías de control

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

- Controles administrativos/de gestión
- Controles técnicos
- Controles físicos/operativos

Los controles administrativos/de gestión abordan el factor humano en la ciberseguridad. Estos controles incluyen políticas y procedimientos que definen cómo una organización gestiona los datos y definen claramente las responsabilidades de los empleados, incluyendo su papel en la protección de la organización. Si bien los controles administrativos suelen basarse en políticas, la aplicación de estas puede requerir el uso de controles técnicos o físicos.

Los controles técnicos consisten en soluciones como cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), productos antivirus (AV), cifrado, etc. Los controles técnicos se pueden utilizar de diversas maneras para cumplir con las metas y objetivos de la organización.

Los controles físicos/operativos incluyen cerraduras de puertas, cerraduras de armarios, 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 control

Los tipos de control incluyen, entre otros:

1. Preventivo
2. Correctivo
3. Detectivo
4. Disuasorio

Estos controles trabajan en conjunto para brindar una defensa integral y proteger los activos. **Los controles preventivos** están diseñados para evitar que ocurra un incidente. **Los controles correctivos** se utilizan para restaurar un activo después de un incidente. **Los controles de detección** se implementan para determinar si un incidente ha ocurrido o está en curso. **Los controles disuasorios** están diseñados para desalentar los ataques.

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

Controles Administrativos/De Gestión		
Nombre del control	**Tipo de control**	**Propósito del control**
Privilegio minimo	Preventivo	Reducir el riesgo y el impacto general de cuentas internas maliciosas o comprometidas.
Planes de recuperación de desastres	Correctivo	Proporcionar continuidad del negocio
Políticas de contraseña	Preventivo	Reducir la probabilidad de que una cuenta se vea comprometida mediante técnicas de ataque de fuerza bruta o de diccionario.
Políticas de control de acceso	Preventivo	Refuerce la confidencialidad y la integridad definiendo qué grupos pueden acceder a los datos o modificarlos.
Políticas de gestión de cuentas	Preventivo	Gestionar el ciclo de vida de las cuentas, reducir la superficie de ataque y limitar el impacto general de ex empleados descontentos y el uso de cuentas predeterminadas.
Separación de funciones	Preventivo	Reducir el riesgo y el impacto general de cuentas internas maliciosas o comprometidas.

Controles Tecnicos		
Nombre del control	**Tipo de control**	**Propósito del control**
Cortafuegos	Preventivo	Para filtrar el tráfico no deseado o malicioso que pueda entrar en la red
IDS/IPS	Detectivo	Para detectar y prevenir el tráfico anómalo que coincida con una firma o regla
Cifrado	Disuasorio	Garantizar la confidencialidad de la información sensible.
Copias de seguridad	Correctivo	Restaurar/recuperarse de un evento
Sistema de gestión de contraseñas	Preventivo	Reducir la fatiga de las contraseñas
Software antivirus (AV)	Preventivo	Escaneos para detectar y aislar amenazas conocidas
Monitoreo, mantenimiento e intervención manuales	Preventivo	Es necesario identificar y gestionar las amenazas, los riesgos o las vulnerabilidades de los sistemas obsoletos.

Controles Físicos/Operativos		
Nombre del control	**Tipo de control**	**Propósito del control**
Caja fuerte con control de tiempo	Disuasorio	Reducir la superficie de ataque y el impacto general de las amenazas físicas

Iluminación adecuada	Disuasorio	Disuadir amenazas limitando los lugares donde “esconderse”
Vigilancia por circuito cerrado de televisión (CCTV)	Preventivo/Detectivo	Los sistemas de circuito cerrado de televisión constituyen un control tanto preventivo como de detección, su presencia puede reducir el riesgo de que ocurran ciertos tipos de sucesos y, puede utilizarse para informar sobre las circunstancias del mismo.
Armarios con cerradura (para equipos de red)	Preventivo	Refuerza la integridad impidiendo que personal no autorizado y otras personas accedan físicamente a los equipos de infraestructura de red o los modifiquen.
Señalización que indica el proveedor del servicio de alarmas	Disuasorio	Disuadir ciertos tipos de amenazas haciendo que la probabilidad de un ataque exitoso parezca baja
Cerraduras	Disuasorio/Preventivo	Reforzar la integridad disuadiendo y previniendo el acceso físico de personal o individuos no autorizados a los activos
Detección y prevención de incendios (alarma contra incendios, sistema de rociadores, etc.)	Disuasorio/Preventivo	Detectar incendios en una ubicación física y prevenir daños a los activos físicos como inventario, servidores, etc.