**Categorías de control**

**Categorías de control**

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

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

**Los 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 definen claramente las responsabilidades de los empleados, incluyendo su rol en la protección de la organización. Si bien los controles administrativos suelen basarse en políticas, su aplicación puede requerir el uso de controles técnicos o físicos.

**Los controles técnicos** consisten en soluciones como firewalls, 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 alcanzar las metas y objetivos organizacionales.

**Los controles físicos/operativos** incluyen cerraduras de puertas, cerraduras de gabinetes, cámaras de vigilancia, lectores de credenciales, etc. Se utilizan para limitar el acceso físico a activos físicos por parte de personal no autorizado.

**Tipos de control**

Los tipos de control incluyen, entre otros:

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

Estos controles trabajan en conjunto para proporcionar una defensa exhaustiva y proteger los activos. Los controles preventivos están diseñados para prevenir 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 ataques.

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

| **Controles administrativos / gerenciales** | | |
| --- | --- | --- |
| **Nombre del Control** | **Tipo de Control** | **Propósito del control** |
| Mínimo privilegio | Preventivo | Reducir el riesgo y el impacto general de cuentas maliciosas internas o comprometidas. |
| Planes de recuperación de desastres | Correctivo | Proporcionar continuidad del negocio |
| Políticas de Contraseña | Preventivo | Reducir la probabilidad de que la cuenta se vea comprometida mediante técnicas de fuerza bruta o ataques de diccionario |
| Políticas de control de acceso | Preventivo | Reforzar la confidencialidad y la integridad definiendo qué grupos pueden acceder o modificar los datos |
| Políticas de gestión de cuentas | Preventivo | Administrar el ciclo de vida de la cuenta, reducir la superficie de ataque y limitar el impacto general de los ex empleados descontentos y el uso predeterminado de la cuenta |
| Separación de funciones | Preventivo | Reducir el riesgo y el impacto general de cuentas maliciosas internas o comprometidas |

|  |  |  |
| --- | --- | --- |
| **Controles Técnicos** | | |
| **Nombre del Control** | **Tipo de Control** | **Propósito del control** |
| Firewall | Preventivo | Para filtrar el tráfico no deseado o malicioso que ingresa a la red |
| IDS/IPS | Detective | Detectar y prevenir el tráfico anómalo que coincida con una firma o regla |
| Encriptación | Disuasorio | Proporcionar confidencialidad a la formación sensible |
| Backups | Correctiva | Restaurar/recuperarse de un evento |
| Gestión de Contraseñas | Preventiva | Reducir la fatiga de las contraseñas |
| Software Antivirus (AV) | Preventiva | Escaneos para detectar y poner en cuarentena amenazas conocidas |
| Monitoreo, mantenimiento e intervención manual | Preventiva | Necesario para identificar y gestionar amenazas, riesgos o vulnerabilidades de sistemas obsoletos |

|  |  |  |
| --- | --- | --- |
| **Control Físico / Operativo** | | |
| **Nombre del Control** | **Tipo de Control** | **Propósito del Control** |
| Caja fuerte con control de tiempo | Disuasoria | Reducir la superficie de ataque y el impacto general de las amenazas físicas |
| Iluminación adecuada | Disuasoria | Disuadir las amenazas limitando los escondites |
| Circuito cerrado de televisión (CCTV) | Preventivo / Detective | El circuito cerrado de televisión es un control tanto preventivo como de detección porque su presencia puede reducir el riesgo de que ocurran ciertos tipos de eventos y puede usarse después de un evento para informar sobre las condiciones del mismo |
| Armarios con cerraduras( para equipos de red) | Preventivo | Reforzar la integridad, evitando que el personal no autorizado y otras personas accedan físicamente o modifiquen los equipos de infraestructura de red |
| Señalización que indica el proveedor de servicios de alarma | Disuasorio | Disuadir ciertos tipos de amenazas haciendo que la probabilidad de ataque exitoso parezca baja |
| Candados | Disuasorio / Preventivo | Reforzar la integridad disuadiendo y evitando que el personal y personas no autorizadas accedan físicamente a los activos |
| Detección y prevención de incendios, sistemas ( alarma, rociadores, etc.) | Detective / Preventivo | Detectar incendios en ubicaciones físicas y prevenir daños de activos físicos como inventario, servidores, etc. |