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

**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.

**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 cumplir con las metas y objetivos organizacionales.

**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. Ellos disuaden

Estos controles trabajan juntos para proporcionar defensa en profundidad y proteger los activos.**Controles preventivos:**Están diseñados para evitar que ocurra un incidente en primer lugar.**Controles correctivos:**Se utilizan para restaurar un activo después de un incidente.**Controles de detectives:**Se implementan para determinar si ha ocurrido un incidente o si está en progreso.**Controles disuasorios:**Están diseñados para desalentar los ataques.

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

| **Administrativo/GerencialControles** | | |
| --- | --- | --- |
| **Nombre del control** | **Tipo de control** | **Control Objetivo** |
| El menos Privilegio | Preventivo | Reducir el riesgo e impacto general de información privilegiada maliciosa o cuentas comprometidas |
| Planes de recuperación ante desastres | Correctivo | Proporcionar continuidad de negocio |
| Políticas de contraseñas | Preventivo | Reducir la probabilidad de comprometer la cuenta 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 impacto general de ex empleados descontentos y uso de cuentas predeterminadas |
| Separación de funciones | Preventivo | Reducir el riesgo e impacto general de información privilegiada maliciosa o cuentas comprometidas |

|  |  |  |
| --- | --- | --- |
| **Controles técnicos** | | |
| **Nombre del control** | **Tipo de control** | **Propósito del control** |
| Cortafuegos | Preventivo | Para filtrar el tráfico no deseado o malicioso que ingresa a la red |
| IDS/IPS | Detective | Para detectar y prevenir tráfico anómalo que coincida con una firma o regla |
| Cifrado | Ellos disuaden | Proporcionar confidencialidad a la información sensible |
| Copias de seguridad | Correctivo | Restaurar/recuperarse de un evento |
| Gestión de contraseñas | Preventivo | Reducir la fatiga de las contraseñas |
| Software antivirus (AV) | Preventivo | Escaneos para detectar y poner en cuarentena amenazas conocidas |
| Monitoreo, mantenimiento e intervención manual | Preventivo | Necesario para identificar y gestionar amenazas, riesgos o vulnerabilidades de sistemas obsoletos |

|  |  |  |
| --- | --- | --- |
| **Controles físicos/operacionales** | | |
| **Nombre del control** | **Tipo de control** | **Propósito del control** |
| Caja fuerte controlada por tiempo | Ellos disuaden | Reducir la superficie de ataque e impacto general de amenazas físicas |
| Iluminación adecuada | Ellos disuaden | 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 cerradura (para equipos de red) | Preventivo | Reforzar la integridad al evitar que personal no autorizado y otras personas accedan físicamente o modifiquen los equipos de infraestructura de red. |
| Señalización que indica el proveedor del servicio de alarma | Ellos disuaden | Disuadir ciertos tipos de amenazas haciendo que la probabilidad de un ataque exitoso parezca baja |
| Cabellos | Disuasorio/Preventivo | Reforzar la integridad disuadiendo y evitando que personal y personas no autorizadas accedan físicamente a los activos. |
| Detección y prevención de incendios (alarma contra incendios, sistema de rociadores, etc.) | Detective/Preventivo | Detectar incendios en ubicaciones físicas y prevenir daños a activos físicos como inventario, servidores, etc. |