# ***EVALUACIÓN DE CONTROLES***

## Activos actuales

Los activos administrados por el Departamento de TI incluyen:

● Equipos locales para las necesidades comerciales en la oficina

● Equipos de empleados: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes),estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento,cámaras de vigilancia, etc.

● Administración de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y administración de inventario

● Acceso a Internet

● Red interna

● Administración de acceso de proveedores

● Servicios de alojamiento de centros de datos

● Retención y almacenamiento de datos

● Lectores de credenciales

● Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren monitoreo humano

| Controles administrativos | | | |
|---|---|---|---|
| Nombre del control | Tipo de control y explicación | Se debe implementar (X) | Prioridad |
| Privilegio mínimo | Preventivo; reduce el riesgo al garantizar que los proveedores y el personal no autorizado solo tengan acceso a los activos o datos que necesitan para hacer su trabajo | X | Alto |
| Planes de recuperación ante desastres | Corrección; continuidad del negocio para garantizar que los sistemas puedan funcionar en caso de un incidente/hay una pérdida de productividad limitada o nula; el impacto en los componentes del sistema, incluidos: el entorno de la sala de computadoras (aire acondicionado, suministro de energía, etc.); hardware (servidores, equipos de los empleados); conectividad (red interna, inalámbrica); aplicaciones (correo electrónico, datos electrónicos); datos y restauración. | X | Alto |
| Políticas de contraseñas | Preventivas: establecer reglas de seguridad de contraseñas para mejorar la seguridad y reducir la probabilidad de que la cuenta se vea comprometida mediante técnicas de ataque de diccionario o de fuerza bruta | X | Alto |
| Políticas de control de acceso | Preventivas; aumentan la confidencialidad e integridad de los datos | X | Alto / Medio |
| Políticas de gestión de cuentas | Preventivas: reducen la superficie de ataque y limitan el impacto general de los empleados descontentos o ex empleados | X | Alto |
| Separación de funciones | Preventiva: garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales | X | Alto |

| Controles técnicos | | | |
|---|---|---|---|
| Nombre del control | Tipo de control y explicación | Se debe implementar (X) | Prioridad |
| Firewall | Preventivo: ya existen firewalls para filtrar el tráfico no deseado o malicioso que ingresa a la red interna. | NA | NA |
| Intrusion Detection System (IDS) (Sistema de detección de intrusiones) | Detective; permite al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente | X | Alto |
| Encryption | Disuasorio; hace que la información/datos confidenciales sean más seguros (por ejemplo, transacciones de pago en sitios web) | X | Alto / Medio |
| Backups (Copias de seguridad) | Corrección; respalda la productividad continua en caso de un evento; se alinea con el plan de recuperación ante desastres | X | Alto |
| Password management system (Sistema de gestión de contraseñas) | Correctivo; recuperación de contraseña, restablecimiento, aviso de bloqueo | X | Alto / Medio |
| Software antivirus (AV) | Corrección: detecta y pone en cuarentena amenazas conocidas | X | Alto |
| Monitoreo, mantenimiento e intervención manual | Preventivo/correctivo; necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades. | x | Alto |

| Controles físicos | | | |
|---|---|---|---|
| Nombre del control | Tipo de control y explicación | Se debe implementar (X) | Prioridad |
| Time-controlled safe<br>(Caja fuerte controlada por tiempo) | Disuasivo; reduce el impacto de las amenazas físicas en superficies negras | X | Medio /Bajo |
| Iluminación adecuada | Disuasión: limite los lugares donde se pueden “esconder” para disuadir amenazas | X | Medio /Bajo |
| Vigilancia por circuito cerrado de televisión (CCTV) | Preventivo/detective; puede reducir el riesgo de ciertos eventos; puede usarse después del evento para investigación | X | Alto / Medio |
| Armarios con cerradura<br>(para equipos de red) | Preventivo; aumenta la integridad al evitar que personal o individuos no autorizados accedan físicamente o modifiquen los equipos de infraestructura de red. | X | Medio |
| Señalización que indica el proveedor del servicio de alarma | Disuasorio; hace que la probabilidad de un ataque exitoso parezca baja | X | Bajo |
| Locks (Cerraduras) | Preventivas; los activos físicos y digitales son más seguros | X | Alto |
| Detección y prevención de incendios (alarma contra incendios, sistema de rociadores, etc.) | Detective/Preventivo; detectar incendio en la ubicación física de la juguetería para evitar daños al inventario, servidores, etc. | X | Medio /Bajo |