# Evaluación de controles

Para revisar las categorías de control, los tipos y los propósitos de cada uno, lea el [categorías de control](https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) documento.

## Activos circulantes

Los activos gestionados por el Departamento de TI incluyen:

* Equipo local para necesidades comerciales en la oficina
* Equipos de los 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.
* Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventarios.
* acceso a Internet
* Red interna
* Gestión de acceso de proveedores
* Servicios de alojamiento de centros de datos
* Retención y almacenamiento de datos
* Lectores de insignias
* 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.** | **Necesita ser implementado (X)** | **Prioridad** |
| Privilegios mínimos | Preventivo; Reduce el riesgo al garantizar que los proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar su trabajo. | X | ALTA |
| Planes de recuperación de desastres | Correctivo; continuidad del negocio para garantizar que los sistemas puedan funcionar en caso de un incidente/que haya un tiempo de inactividad limitado o nulo de productividad/impacto en los componentes del sistema, incluidos: entorno de la sala de computadoras (aire acondicionado, suministro de energía, etc.); hardware (servidores, equipos de empleados); conectividad (red interna, inalámbrica); solicitudes (correo electrónico, datos electrónicos); datos y restauración | X | ALTA |
| Políticas de contraseña | Preventivo; establecer reglas de seguridad de la contraseña para mejorar la seguridad/reducir la probabilidad de que la cuenta se vea comprometida mediante fuerza bruta o técnicas de ataque de diccionario | X | ALTA |
| Políticas de control de acceso | Preventivo; aumentar la confidencialidad y la integridad de los datos | X | ALTA |
| Políticas de gestión de cuentas | Preventivo; reducir la superficie de ataque y limitar el impacto general de los empleados descontentos/ex empleados | X | MEDIA |
| Separación de tareas | Preventivo; Asegúrese de que nadie tenga tanto acceso como para poder abusar del sistema para beneficio personal. | X | ALTA |

| **Controles técnicos** | | | |
| --- | --- | --- | --- |
| **Nombre del control** | **Tipo de control y explicación.** | **Necesita ser implementado**  **(X)** | **Prioridad** |
| Cortafuegos | Preventivo; Ya existen firewalls para filtrar el tráfico no deseado/malicioso que ingresa a la red interna. | N/A | N/A |
| Sistema de detección de intrusiones (IDS) | Detective; permite al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente | X | ALTA |
| Cifrado | Disuasorio; hace que la información/datos confidenciales sean más seguros (por ejemplo, transacciones de pago en sitios web) | X | MEDIA |
| Copias de seguridad | Correctivo; apoya la productividad continua en caso de un evento; se alinea con el plan de recuperación ante desastres | X | ALTA |
| Sistema de gestión de contraseñas | Correctivo; recuperación de contraseña, restablecimiento, bloqueo de notificaciones | X | MEDIO |
| Software antivirus (AV) | Correctivo; detectar y poner en cuarentena amenazas conocidas | X | ALTA |
| Monitoreo, mantenimiento e intervención manual | Preventivo/correctivo; Requerido para que los sistemas heredados identifiquen y mitiguen amenazas, riesgos y vulnerabilidades potenciales. | X | ALTA |

| **Controles físicos** | | | |
| --- | --- | --- | --- |
| **Nombre del control** | **Tipo de control y explicación.** | **Necesita ser implementado**  **(X)** | **Prioridad** |
| Caja fuerte con control de tiempo | Disuasorio; Reducir la superficie de ataque/impacto de las amenazas físicas. | X | MEDIA |
| Iluminación adecuada | Disuasorio; limitar los lugares de “escondite” para disuadir las amenazas | X | MEDIA |
| Vigilancia por circuito cerrado de televisión (CCTV) | Preventivo/detective; puede reducir el riesgo de ciertos eventos; Se puede utilizar después del evento para investigación. | X | MEDIA |
| Gabinetes con cerradura (para equipos de red) | Preventivo; aumentar la integridad evitando que personal/individuos no autorizados accedan físicamente/modifiquen los equipos de la infraestructura de red | X | MEDIA |
| Señalización que indica proveedor de servicios de alarma | Disuasorio; hace que la probabilidad de un ataque exitoso parezca baja | X | BAJA |
| Cerraduras | Preventivo; Los activos físicos y digitales son más seguros. | X | ALTA |
| 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 | MEDIA |