# Ejemplo de evaluación de controles

Para revisar las categorías de control, los tipos y los propósitos de cada uno, lea el documento [de categorías de control](https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?usp=sharing&resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA) .

## Activos corrientes

Los activos administrados por el Departamento de TI incluyen:

* Equipos locales 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 supervisión humana

| **Controles administrativos** | | | |
| --- | --- | --- | --- |
| **Nombre del control** | **Tipo de control y explicación** | **Necesita ser implementado (X)** | **Prioridad** |
| Mínimo privilegio | Preventivo; reduce el riesgo al garantizar que los proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para hacer su trabajo. | incógnita | Alto |
| Planes de recuperación ante desastres | Correctivo; continuidad del negocio para garantizar que los sistemas puedan funcionar en caso de un incidente/hay un tiempo de inactividad/impacto limitado o nulo en la pérdida de productividad en los componentes del sistema, incluidos: entorno de la sala de computadoras (aire acondicionado, fuente de alimentación, etc.); hardware (servidores, equipos de empleados); conectividad (red interna, inalámbrica); aplicaciones (correo electrónico, datos electrónicos); datos y restauración | incógnita | Alto |
| Políticas de contraseñas | Preventivo; establecer reglas de fortaleza de contraseñas para mejorar la seguridad/reducir la probabilidad de que la cuenta se vea comprometida mediante técnicas de fuerza bruta o ataques de diccionario | incógnita | Alto |
| Políticas de control de acceso | Preventivo; aumentar la confidencialidad e integridad de los datos | incógnita | Alto |
| Políticas de gestión de cuentas | Preventivo: reduce la superficie de ataque y limita el impacto general de los empleados descontentos o ex empleados | incógnita | Alto/  Medio |
| Separación de funciones | Preventivo; garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales. | incógnita | Alto |

| **Controles técnicos** | | | |
| --- | --- | --- | --- |
| **Nombre del control** | **Tipo de control y explicación** | **Necesita ser implementado**  **(INCÓGNITA)** | **Prioridad** |
| Cortafuegos | Preventivo: ya existen firewalls para filtrar el tráfico no deseado o 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 | incógnita | Alto |
| Encriptación | Disuasorio; hace que la información/datos confidenciales sean más seguros (por ejemplo, transacciones de pago en sitios web) | incógnita | Alto/  Medio |
| Copias de seguridad | Correctivo; apoya la productividad continua en caso de un evento; se alinea con el plan de recuperación ante desastres | incógnita | Alto |
| Sistema de gestión de contraseñas | Correctivo; recuperación de contraseña, restablecimiento, bloqueo de notificaciones | incógnita | Alto/  Medio |
| Software antivirus (AV) | Correctivo; detectar y poner en cuarentena amenazas conocidas | incógnita | Alto |
| Monitoreo, mantenimiento e intervención manual | Preventivo/correctivo; necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades. | incógnita | Alto |

| **Controles físicos** | | | |
| --- | --- | --- | --- |
| **Nombre del control** | **Tipo de control y explicación** | **Necesita ser implementado**  **(INCÓGNITA)** | **Prioridad** |
| Caja fuerte controlada por tiempo | Disuasión; reduce la superficie de ataque/impacto de las amenazas físicas | incógnita | Medio/  Bajo |
| Iluminación adecuada | Disuasión; limitar los lugares donde se pueden “esconder” para disuadir amenazas | incógnita | 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 | incógnita | Alto/  Medio |
| Armarios con cerradura (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. | incógnita | Medio |
| Señalización que indica el proveedor del servicio de alarma | Disuasorio; hace que la probabilidad de un ataque exitoso parezca baja | incógnita | Bajo |
| Cabellos | Preventivo; los activos físicos y digitales son más seguros | incógnita | Alto |
| Detección y prevención de incendios (alarma contra incendios, sistema de rociadores, etc.) | Detective/Preventivo; detectar incendios en la ubicación física de la juguetería para evitar daños al inventario, servidores, etc. | incógnita | Medio/  Bajo |