Evaluación de Controles

Para revisar las categorías de control, los tipos y los propósitos de c/u, lea el documento de categorías de control.

Los activos gestionados por el Departamento de TI incluyen:

- Equipos en las instalaciones para las necesidades operativas de la oficina
- Equipos de empleados: dispositivos de usuario final (PCs, laptops, smartphones), 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 inventario
- Acceso a Internet
- Red Interna
- Gestión de acceso de proveedores
- Servicios de alojamiento de centros de datos
- Retención y almacenamiento de datos
- Lectores de tarjetas
- Mantenimiento de sistemas heredados: sistemas obsoletos que requieren supervisión humana

Controles Administrativos			
Nombre del Control	**Tipo de control y explicación**	**Se debe implementar (X)**	**Prioridad**
Privilegio minimo	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 sus tareas	X	Inmediata /Alta
Planes de recuperación de	Correctivo; continuidad del negocio para garantizar el	X	Inmediata /Alta

Controles Administrativos			
desastres	funcionamiento de los sistemas en caso de incidente, minimizando o eliminando la pérdida de productividad y el impacto en los componentes del sistema, incluyendo: entorno de la sala de servidores (aire acondicionado, suministro eléctrico, etc.); hardware (servidores, equipos de empleados); conectividad (red interna, inalámbrica); aplicaciones (correo electrónico, datos electrónicos); datos y restauración.		
Políticas de contraseña	Preventivas: establecen reglas de seguridad para contraseñas robustas con el fin de mejorar la seguridad y reducir la probabilidad de que las cuentas se vean comprometidas mediante ataques de fuerza bruta o de diccionario.	X	Inmediata /Alta
Políticas de control de acceso	Preventivo; aumenta la confidencialidad e integridad de los datos	X	Inmediata /Alta
Políticas de gestión de cuentas	Preventivas: reducen la superficie de ataque y limitan el impacto general de empleados descontentos o ex empleados.	X	Futuro /Media
Separación de funciones	Medidas preventivas: garantizar que nadie tenga tanto acceso que pueda abusar del sistema para su beneficio personal.	X	Inmediata /Alta

Controles Tecnicos			
Nombre del Control	**Tipo de control y explicación**	**Se debe implementar (X)**	**Prioridad**
Cortafuegos	Preventivo: ya existen cortafuegos para filtrar el tráfico no deseado o malicioso que intenta ingresar a la red interna.	NA	NA
Sistema de detección de intrusiones (IDS)	Detectivo; permite al equipo de TI identificar rápidamente posibles intrusiones (p. ej., tráfico anómalo).	X	Inmediata /Alta
Cifrado	Disuasorio; aumenta la seguridad de la información/datos confidenciales (p. ej., transacciones de pago en sitios web)	X	Inmediata /Alta
Copias de seguridad	Correctivo; apoya la productividad continua en caso de un evento; se alinea con el plan de recuperación ante desastres plan	X	Inmediata /Alta
Sistema de gestión de contraseñas	Correctivo; recuperación de contraseña, restablecimiento, notificaciones de bloqueo	X	Inmediata /Alta
Software antivirus (AV)	Correctivo; detectar y poner en cuarentena las amenazas conocidas	X	Inmediata /Alta
Monitoreo, mantenimiento e intervención manuales	Preventivo/correctivo; necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades.	X	Inmediata /Alta

Controles fisicos			
Nombre del Control	**Tipo de control y explicación**	**Se debe implementar (X)**	**Prioridad**
Caja fuerte con control de tiempo	Disuasorio; reduce la superficie de ataque/el impacto de las amenazas físicas	X	Futuro /Media
Iluminación adecuada	Disuasorio: limitar los escondites para disuadir las amenazas.	X	Futuro /Baja
Vigilancia por circuito cerrado de televisión (CCTV)	Preventivo/detectivo; puede reducir el riesgo de ciertos eventos; puede utilizarse después del evento para la investigación.	X	Inmediata /Alta
Armarios con cerradura (para equipos de red)	Preventivo: aumentan la integridad al impedir que personal o individuos no autorizados accedan físicamente a los equipos de infraestructura de red o los modifiquen.	X	Futuro /Media
Señalización que indica el proveedor del servicio de alarmas	Disuasorio; reduce la probabilidad de éxito del ataque.	x	Futuro /Baja
Cerraduras	Preventivo: los activos físicos y digitales son más seguros.	X	Inmediata /Alta
Detección y prevención de incendios (alarma contra incendios, sistema de rociadores, etc.)	Detectivo/Preventivo; detectar incendios en el local físico de la juguetería para evitar daños al inventario, servidores, etc.	X	Futuro /Baja