Ejemplo de evaluación de controles

Activos actuales

Entre los activos administrados por el departamento de TI se encuentran los siguientes:

- Equipos en las instalaciones para las necesidades comerciales en la oficina.
- Equipos del personal: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, mouse, 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 a proveedores.
- Servicios de alojamiento del centro de datos.
- Retención y almacenamiento de datos.
- Lectores de tarjetas de identificación.
- Mantenimiento de sistemas heredados: sistemas obsoletos que requieren supervisión humana.

Controles administrativos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Principios de mínimo privilegio	Preventivo. Reducir el riesgo asegurándose de que proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar su trabajo.	X	Alto
Planes de recuperación ante incidentes	Correctivo. Garantizar la continuidad del negocio, asegurando que los sistemas puedan ejecutarse en caso de incidentes, que no haya pérdida de productividad por tiempo de inactividad ni impacto en los	X	Alto

Controles administrativos			
	componentes del sistema, que incluyen, entorno de la sala de computadoras (aire acondicionado, fuentes de alimentación, etc.), hardware (servidores, equipos de empleados), conectividad (red interna, inalámbrica), aplicaciones (correo electrónico, datos electrónicos), así como datos y restauración.		
Políticas de contraseñas	Preventivo. Establecer requisitos de seguridad de contraseñas para reducir la probabilidad de comprometer la cuenta debido a técnicas de ataque por fuerza bruta o diccionario.	X	Alto
Políticas de control de acceso	Preventivo. Aumentar la confidencialidad e integridad de los datos.	X	Alto
Políticas de gestión de cuentas	Preventivo. Reducir la superficie expuesta a ataques y limita el impacto general de ex empleados/as disconformes.	X	Alto/ Medio
Separación de funciones	Preventivo. Garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales.	X	Alto

Controles técnicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**

Cortafuegos (firewall)	Preventivo. Ya hay instalados firewalls para filtrar el tráfico no deseado/malicioso que ingresa a la red interna.	N/D	N/D
Sistema de detección de intrusiones (IDS)	De detección. Permitir al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente.	X	Alto
Cifrado	Disuasivo. Garantizar que la información y los datos confidenciales sean más seguros (por ejemplo, transacciones de pago en el sitio web).	X	Alto/ Medio
Copias de seguridad	Correctivo. Permitir la continuidad del negocio y mantener la productividad en caso de incidentes, al mantener los sistemas funcionando	X	Alto
Gestión de contraseñas	Correctivo. Recuperar y restablecer contraseñas, bloqueo de notificaciones.	X	Alto/ Medio
Software de antivirus (AV)	Correctivo. Detectar amenazas conocidas y aislarlas.	X	Alto
Monitoreo manual, mantenimiento e intervención	Preventivo/correctivo. Necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades.	X	Alto

Controles físicos			
Nombre de control	**Tipo de control y objetivo**	**Se tiene que implementar (X)**	**Prioridad**

Caja fuerte con control de tiempo	Disuasivo. Reducir la superficie expuesta a ataque y el impacto de las amenazas físicas.	X	Medio/ Bajo
Iluminación adecuada	Disuasivo. Limitar los lugares “ocultos” para disuadir las amenazas.	X	Medio/ Bajo
Vigilancia del circuito cerrado de televisión (CCTV)	Preventivo/De detección. Reducir el riesgo de ciertos eventos y ver qué sucedió después del incidente, al llevar a cabo una investigación.	X	Alto/ Medio
Cerradura de gabinetes (para equipos de red)	Preventivo. Aumentar la integridad al evitar que personas no autorizadas accedan físicamente o modifiquen el equipo de infraestructura de la red.	X	Medio
Carteles que indican el nombre de la empresa proveedora del servicio de alarmas	Disuasivo. Reducir la probabilidad de éxito de ciertos tipos de amenazas al dar la apariencia de que un ataque exitoso es poco probable.	X	Bajo
Cerraduras	Preventivo. Lograr que los activos físicos y digitales estén más seguros.	X	Alto
Detección y prevención de incendios (alarma de incendios, sistema de rociadores, entre otros)	De detección/Preventivo. Detectar incendios en la ubicación física de la juguetería para evitar daños en el inventario, servidores, entre otros.	X	Medio/ Bajo