Lista de verificación de controles y cumplimiento

Lista de verificación de evaluación de controles

Sí	No	Control
☐	☑	Mínimo privilegio
☐	☑	Planes de recuperación de desastres
☐	☑	Políticas de contraseña
☐	☑	Separación de funciones
☑	☐	Cortafuegos
☐	☑	Sistema de detección de intrusos (IDS)
☐	☑	Copias de seguridad
☑	☐	software antivirus
☑	☑	Monitoreo, mantenimiento e intervención manuales para sistemas heredados
☐	☑	Cifrado
☑	☑	Sistema de gestión de contraseñas
☑	☐	Cerraduras (oficinas, escaparate, almacén)
☑	☐	Vigilancia por circuito cerrado de televisión (CCTV)
☑	☐	Detección/prevención de incendios (alarma de incendios, sistema de rociadores, etc.)

* Atención: al indicar sí y no significa que el tipo de control existe pero no es efectivo o está obsoleto

Lista de verificación de cumplimiento

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

Sí	No	Mejores prácticas
☐	☑	Sólo los usuarios autorizados tienen acceso a la información de la tarjeta de crédito de los clientes.
☐	☑	La información de la tarjeta de crédito se almacena, acepta, procesa y transmite internamente, en un entorno seguro.
☐	☑	Implemente procedimientos de cifrado de datos para proteger mejor los datos y los puntos de contacto de las transacciones con tarjetas de crédito.
☐	☑	Adopte políticas seguras de gestión de contraseñas.

Reglamento General de Protección de Datos (GDPR)

Sí	No	Mejores prácticas
☐	☑	UE. Los datos de los clientes se mantienen privados/seguros.
☑	☐	Existe un plan para notificar a la UE. clientes dentro de las 72 horas si sus datos se ven comprometidos/hay una violación.
☐	☑	Asegúrese de que los datos estén clasificados e inventariados adecuadamente.
☑	☐	Hacer cumplir políticas, procedimientos y procesos de privacidad para documentar y mantener adecuadamente los datos.

Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)

Sí	No	Mejores prácticas
☐	☑	Se establecen políticas de acceso de usuarios.
☐	☑	Los datos confidenciales (PII/SPII) son confidenciales/privados.

☑ ☐ La integridad de los datos garantiza que los datos sean coherentes, completos, precisos y hayan sido validados.

☑ ☐ Los datos están disponibles para las personas autorizadas a acceder a ellos.

Recomendaciones para mejorar la postura de seguridad de Botium Toys

1. Implementar el principio de privilegio mínimo:
    - Recomendación: Asegúrese de que solo los usuarios autorizados tengan acceso a datos y sistemas críticos, incluida la información de la tarjeta de crédito del cliente. Revise y actualice periódicamente los permisos de acceso para garantizar que solo el personal necesario tenga acceso a la información confidencial.
2. Desarrollar e implementar políticas de gestión segura de contraseñas:
    - Recomendación: Adopte políticas de contraseña sólidas que incluyan requisitos de complejidad, longitud y cambios periódicos de contraseña. Considere implementar un sistema centralizado de administración de contraseñas para facilitar el cumplimiento y reducir la fatiga de las contraseñas.
3. Implementar procedimientos de cifrado de datos:
    - Recomendación: Cifre la información de la tarjeta de crédito durante el almacenamiento, el procesamiento y la transmisión para protegerla del acceso no autorizado. Asegúrese de que los datos confidenciales estén cifrados tanto en reposo como en tránsito.
4. Establecer un plan de recuperación ante desastres:
    - Recomendación: Desarrollar e implementar un plan de recuperación ante desastres para garantizar la continuidad del negocio en caso de una violación de seguridad o un desastre. Pruebe y actualice periódicamente el plan según sea necesario.
5. Adopte una estrategia de respaldo integral:
    - Recomendación: Realice copias de seguridad periódicas de todos los datos críticos y guárdalas en una ubicación segura. Verifique la integridad de las copias de seguridad y realice pruebas de recuperación periódicas para garantizar una restauración efectiva de los datos.
6. Implementar un Sistema de Detección y Prevención de Intrusos (IDS/IPS):
    - Recomendación: Instale y configure un IDS/IPS para detectar y prevenir tráfico sospechoso o malicioso en la red. Asegúrese de que el sistema esté actualizado con las últimas firmas y reglas de detección.
7. Garantizar el Cumplimiento de las Políticas de Privacidad y Protección de Datos:

    - Recomendación: Revisar y fortalecer las políticas y procedimientos de privacidad para garantizar el cumplimiento de las normas de protección de datos, como el GDPR. Implementar procesos para clasificar, documentar y mantener adecuadamente los datos.
8. Fortalecer los controles físicos y operativos:
    - Recomendación: Asegurar que las áreas físicas de alto riesgo (oficinas, almacenes) estén protegidas con cerraduras adecuadas, sistemas de CCTV y medidas de detección y prevención de incendios. Implementar controles para limitar el acceso físico a activos críticos.
9. Realizar monitoreo y mantenimiento continuo:
    - Recomendación: Establezca procesos continuos de monitoreo y mantenimiento para identificar y gestionar vulnerabilidades en sistemas heredados y otras infraestructuras críticas. Considere implementar una herramienta de gestión de vulnerabilidades para automatizar este proceso.

Estas recomendaciones pueden ayudar a mitigar los riesgos para los activos de Botium Toys y mejorar su postura general de seguridad.