Lista de verificación de controles y cumplimiento

Para completar la lista de verificación de evaluación de controles, consulte la información proporcionada en el Informe de alcance, objetivos y evaluación de riesgos. Para obtener más detalles sobre cada control, incluido el tipo y el propósito, consulte lacategorías de control documento.

Luego, seleccione “sí” o “no” para responder la pregunta:*¿Botium Toys cuenta actualmente con este control?*

Lista de verificación de evaluación de controles

Sí	No	Control
☐	☑	Mínimo privilegio
☐	☑	Planes de recuperación ante desastres
☑	☐	Políticas de contraseñas
☐	☐	Separación de funciones
☑	☐	Cortafuegos
☐	☑	Sistema de detección de intrusiones (IDS)
☐	☑	Copias de seguridad
☑	☐	software antivirus
☑	☐	Monitoreo manual, mantenimiento e intervención para sistemas heredados
☐	☑	Cifrado
☐	☑	Sistema de gestión de contraseñas
☑	☐	Cerraduras (oficinas, escaparates, almacenes)

☑	☐	Vigilancia por circuito cerrado de televisión (CCTV)
☑	☐	Detección/prevención de incendios (alarma contra incendios, sistema de rociadores, etc.)

Para completar la lista de verificación de cumplimiento, consulte la información proporcionada en laInforme de alcance, objetivos y evaluación de riesgos. Para obtener más detalles sobre cada normativa de cumplimiento, revise lacontroles, marcos y cumplimiento lectura.

Luego, seleccione “sí” o “no” para responder la pregunta:*¿Botium Toys cumple actualmente con estas mejores prácticas de cumplimiento?*

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 las tarjetas de crédito de los clientes.
☐	☑	La información de las tarjetas de crédito se almacena, acepta, procesa y transmite internamente, en un entorno seguro.
☐	☑	Implementar procedimientos de cifrado de datos para proteger mejor los puntos de contacto y los datos de las transacciones con tarjetas de crédito.
☐	☑	Adopte políticas de gestión de contraseñas seguras.

Reglamento General de Protección de Datos (RGPD)

Sí	No	Mejores prácticas
☐	☑	Los datos de los clientes de la UE se mantienen privados y seguros.

☑	☐	Hay un plan establecido para notificar a los clientes de la UE dentro de las 72 horas si sus datos se ven comprometidos o se produce una violación.
☐	☑	Asegúrese de que los datos estén correctamente clasificados e inventariados.
☑	☐	Hacer cumplir las 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 sensibles (PII/SPII) son confidenciales/privados.
☐	☑	La integridad de los datos garantiza que los datos sean consistentes, completos, precisos y hayan sido validados.
☐	☑	Los datos están disponibles para las personas autorizadas a acceder a ellos.

Esta sección es *opcional* puede usarse para brindar un resumen de recomendaciones al gerente de TI con respecto a qué controles y/o mejores prácticas de cumplimiento debe implementar Botium Toys, en función del riesgo que supone si no se implementan de manera oportuna.

Recomendaciones (opcional): En esta sección, proporcione recomendaciones relacionadas con los controles y/o las necesidades de cumplimiento que su gerente de TI podría comunicar a las partes interesadas para reducir los riesgos de los activos y mejorar la postura de seguridad de Botium Toys.

Sugerencias:

Backups fuera de la oficina: No podemos tener la única copia de los datos en el mismo edificio que el servidor. Hay que mandarlos a otro lado para que, si pasa algo físico (fuego/robo), el negocio pueda seguir andando.

Cifrado de PII/SPII: Es crítico proteger los datos de tarjetas y clientes. Hay que cifrar la base de datos para que, si los datos se filtran, sean ilegibles y estemos cubiertos legalmente.