# 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, incluyendo el tipo y la finalidad, consulte el documento de categorías de control.

A continuación, seleccione "sí" o "no" para responder a la pregunta: ¿Botium Toys cuenta actualmente con este control?

## Lista de verificación para la evaluación de controles

**SI NO CONTROL**

Mínimo Privilegio

Plan de recuperación ante Desastres

Políticas de Contraseña

Separación de Funciones

Cortafuegos (Firewalls)

Sistema de Detección de Intrusos (IDS)

Respaldos (Backups)

Software Antivirus

Monitoreo manual, mantenimiento e intervención para sistemas heredados

Encriptación

sistema de gestión de contraseñas

Candados (oficinas, escaparates, almacenes)

Vigilancia por Circuito cerrado de televisión (CCTV)

Detección / prevención de incendios (alarma contra incendios, sistemas de

rociadores etc)

Para completar la lista de verificación de cumplimiento, consulte la información proporcionada en el alcance, los objetivos y el informe de evaluación de riesgos. Para obtener más detalles sobre cada normativa de cumplimiento, revise los controles, los marcos y la información de cumplimiento.

A continuación, seleccione "sí" o "no" para responder a la pregunta: ¿Botium Toys cumple actualmente con esta práctica recomendada de cumplimiento?

## Lista de verificación de cumplimiento

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

SI NO BUENAS PRACTICAS

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.

Adoptar políticas de gestión de contraseñas seguras.

Reglamento General de Protección de Datos (GDPR)

SI NO BUENAS PRACTICAS

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)

SI NO BUENAS PRACTICAS

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.

Recomendaciones:

Es necesario implementar múltiples controles para mejorar la seguridad de Botium Toys y garantizar la confidencialidad de la información sensible. Estos controles incluyen: mínimos privilegios, planes de recuperación ante desastres, políticas de contraseñas, separación de funciones, un sistema de detección de intrusos (IDS), gestión continua de sistemas heredados, cifrado y un sistema de gestión de contraseñas.

Para abordar las deficiencias en el cumplimiento normativo, Botium Toys debe implementar controles como mínimos privilegios, separación de funciones y cifrado. La empresa también debe clasificar adecuadamente los activos para identificar controles adicionales que puedan ser necesarios para mejorar su seguridad y proteger mejor la información sensible.