

Lista de verificación de controles y cumplimiento

Esta lista permite identificar los controles actualmente implementados en Botium Toys, con base en el alcance, los objetivos y la evaluación de riesgos previamente definidos.

Cada control se relaciona con una categoría específica y cumple un propósito dentro del marco de seguridad de la organización.

La evaluación consiste en indicar si el control se encuentra implementado o no en la actualidad.

Marcar con “sí” o “no” según corresponda.

¿Botium Toys tiene actualmente implementado este control?

Lista de verificación de evaluación de controles

Si	No	Control
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mínimo privilegio
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Planes de recuperación ante desastres
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Políticas de contraseñas
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separación de funciones
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sistema de detección de intrusos (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Software Antivirus
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitoreo, mantenimiento e intervención manual para sistemas heredados
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cifrado
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sistema de gestión de contraseñas

- | | | |
|-------------------------------------|--------------------------|--|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Cerraduras (oficinas, tienda, almacén) |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Vigilancia por circuito cerrado de televisión (CCTV) |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Detección/previsión de incendios (alarma, sistema de rociadores, etc.) |

Marcar con “sí” o “no” según corresponda.

¿Botium Toys cumple actualmente con esta mejor práctica de cumplimiento?

Lista de verificación de cumplimiento

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

- | Si | No | Mejor práctica |
|--------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Solo los usuarios autorizados tienen acceso a la información de las tarjetas de crédito de los clientes. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | La información de las tarjetas de crédito se almacena, acepta, procesa y transmite internamente en un entorno seguro. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Se implementan procedimientos de cifrado de datos para proteger mejor los puntos de contacto y los datos de las transacciones con tarjeta de crédito. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Se adoptan políticas seguras de gestión de contraseñas. |

Reglamento General de Protección de Datos (GDPR)

- | Si | No | Mejor práctica |
|-------------------------------------|-------------------------------------|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Los datos de los clientes de la UE se mantienen privados/seguros. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Existe un plan para notificar a los clientes de la UE en un plazo de 72 horas si sus datos se ven comprometidos o hay una violación. |

- | | | |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Se asegura que los datos estén correctamente clasificados e inventariados. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Se aplican políticas, procedimientos y procesos de privacidad para documentar y mantener adecuadamente los datos. |

Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

- | Yes | No | Mejor práctica |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Se han establecido políticas de acceso de usuarios. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Los datos sensibles (PII/SPII) se mantienen confidenciales/privados. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | La integridad de los datos garantiza que estos sean consistentes, completos, precisos y hayan sido validados. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Los datos están disponibles para las personas autorizadas a acceder a ellos. |

Recomendaciones:

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

Para abordar las brechas en cumplimiento, Botium Toys debe implementar controles como mínimo privilegio, separación de funciones y cifrado.

Además, la empresa debe clasificar adecuadamente sus activos para identificar controles adicionales que puedan ser necesarios para mejorar su postura de seguridad y proteger mejor la información sensible.