


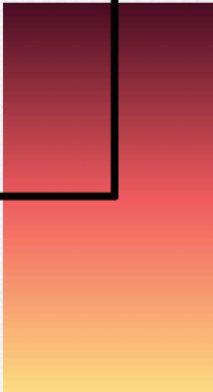
Auditoría de Seguridad Interna
2025



PORT FOLIO

CAMILE
CARRASCO SOTO

camile.dcs@gmail.com



Auditoría de Seguridad – Botium Toys

1. Alcance y Objetivos

Alcance:

- Activos físicos y digitales de empleados
- Productos en venta física y en línea
- Sistemas de gestión y software
- Red interna y acceso a Internet
- Retención y almacenamiento de datos
- Sistemas heredados con supervisión manual

Objetivos:

1. Evaluar activos y su impacto en el negocio.
 2. Completar lista de controles y cumplimiento.
 3. Fortalecer la postura de seguridad.
 4. Cumplir con regulaciones (PCI DSS, GDPR, SOC 1/2).
-

2. Evaluación de Riesgos

- **Riesgo principal:** Gestión de activos inadecuada y falta de controles.
- **Puntuación de Riesgo:** **8/10 (Alto)**

Hallazgos clave:

- Acceso abierto a PII/SPII de clientes.
- Datos de tarjetas sin cifrar.
- Sin planes de recuperación ni copias de seguridad.
- Políticas de contraseñas débiles.
- Sistemas heredados sin mantenimiento.
- Seguridad física robusta (CCTV, cerraduras, alarmas).

3. Controles Administrativos

Control	Tipo	Estado	Observaciones
Menor privilegio	Preventivo	No	Acceso abierto a datos sensibles.
Planes de recuperación	Correctivo	No	No existen backups ni DRP.
Políticas de contraseñas	Preventivo	No	Requisitos básicos.
Gestión de cuentas	Preventivo	No	No se controla ciclo de vida.
Separación de funciones	Preventivo	No	Riesgo de abuso interno.

4. Controles Técnicos

Control	Tipo	Estado	Observaciones
Firewall	Preventivo	Sí	Filtra tráfico malicioso.
IDS/IPS	Detectivo	No	No implementado.
Cifrado	Disuasivo	No	Sin cifrado en datos críticos.
Copias de seguridad	Correctivo	No	Riesgo alto de pérdida.
Antivirus	Preventivo	Sí	Activo y monitoreado.
Monitoreo sistemas heredados	Preventivo	Parcial	Sin cronograma formal.

5. Controles Físicos

Control	Tipo	Estado	Observaciones
Caja fuerte	Disuasivo	Sí	Acceso restringido.
CCTV	Preventivo	Sí	Monitoreo constante.
Armarios cerrados	Preventivo	Sí	Protege red interna.
Señalización de alarmas	Disuasivo	Sí	Disuasión activa.
Detección incendios	Preventivo	Sí	Inventario protegido.

6. Cumplimiento Normativo

PCI DSS

- **No cumple** | Acceso restringido a datos
- **No cumple** | Procesamiento seguro
- **No cumple** | Cifrado de datos
- **No cumple** | Políticas de contraseñas

GDPR

- **Parcial** | Control de acceso insuficiente
- **Cumple** | Notificación en 72h
- **No cumple** | Inventario de datos inexistente
- **Parcial** | Políticas de privacidad parciales



SOC 1/2

- **No cumple** | Políticas de acceso no aplicadas
- **No cumple** | Confidencialidad no asegurada
- **Parcial** | Integridad parcial (sin cifrado/backups)
- **Parcial** | Disponibilidad comprometida

7. Recomendaciones

1. Implementar menor privilegio y separación de funciones.
 2. Instalar IDS/IPS para monitoreo de red.
 3. Cifrar datos sensibles y tarjetas de crédito.
 4. Crear planes de recuperación y realizar backups regulares.
 5. Usar gestión centralizada de contraseñas.
 6. Clasificar e inventariar activos críticos.
 7. Reforzar cumplimiento de PCI DSS, GDPR y SOC.
-

Resumen

La auditoría de seguridad interna de Botium Toys identificó una postura de alto riesgo **(8/10)** caracterizada por la ausencia de controles críticos como el principio de mínimo privilegio, cifrado de datos, planes de recuperación ante desastres y sistemas de detección de intrusos, junto con incumplimientos normativos graves en PCI DSS y GDPR que exponen datos sensibles de clientes y amenazan la continuidad del negocio, requiriendo la implementación inmediata de un plan de remediación integral que priorice la protección de activos críticos y el cumplimiento regulatorio para mitigar riesgos financieros y operativos.