# Botium Toys: Internal Security Audit Report, part 2

## Summary

The internal audit of Botium Toys aims to align current business practices with industry standards and best practices. The goal is to identify vulnerabilities classified as "high risk," provide mitigation recommendations, and present an overall strategy for improving the organization's security posture. The audit team will document findings, provide remediation plans, and communicate results to stakeholders.

## Audit Scope

The scope of Botium Toys' internal IT audit covers the entire security program, including all assets, internal processes, and procedures. Specifically, the audit assessed:

* Current user permissions in accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tools.
* Implemented controls in critical systems.
* Procedures and protocols for these systems.
* Alignment of user permissions, controls, procedures, and protocols with compliance requirements.
* Inventory of current technology, including hardware and system access.

## Audit Goals

The goals of Botium Toys' internal IT audit are:

* Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
* Establish better processes to ensure system compliance.
* Strengthen system controls.
* Implement the concept of least permissions in user credential management.
* Establish policies and procedures, including playbooks.
* Ensure compliance with regulatory requirements.

## Risk Assessment: Current Assets

Assets managed include on-premises equipment, employee devices, system management, internet access, internal network, vendor access, data center services, data retention, badge readers, and legacy system maintenance.

### Risk Description

Significant risks include inadequate asset management, insufficient controls, and potential non-compliance with regulations.

### Control Best Practices

The audit identified the need to adopt asset management practices and enhance controls to meet compliance and security standards.

### Risk Score

The risk score is 8/10 due to inadequate controls and potential compliance issues.

## **Conclusions and Recommendations:** **Major Risks Identified**

1. **Inadequate Asset Management:** Lack of proper inventory and management of technological assets, including end-user devices and critical systems.
2. **Insufficient Controls:** Critical systems like accounting, endpoint detection, firewalls, intrusion detection systems, and SIEM tools lack necessary security controls.
3. **Compliance Issues:** Potential non-compliance with GDPR, PCI DSS, and possibly HIPAA regulations.

### Immediate Recommendations

* Implement least privilege principles for user permissions.
* Strengthen security controls with multi-factor authentication and continuous monitoring.
* Formalize security policies, procedures, and incident response plans.

### Future Recommendations

* Address asset management gaps and enhance control frameworks.
* Achieve compliance with GDPR, PCI DSS, and potentially HIPAA regulations.

### Summary of Recommendations to Stakeholders

Immediate actions are critical to mitigate current risks, enhance security posture, and ensure compliance with regulatory requirements. By implementing least privilege for user access, enhancing security controls, and formalizing policies and procedures, Botium Toys can significantly improve its security and regulatory compliance posture.

# Informe de Auditoría de Seguridad Interna de Botium Toys (Spanish)

## Resumen

La auditoría interna de Botium Toys tiene como objetivo alinear las prácticas comerciales actuales con los estándares y mejores prácticas de la industria. El objetivo es identificar vulnerabilidades clasificadas como "alto riesgo", proporcionar recomendaciones de mitigación y presentar una estrategia general para mejorar la postura de seguridad de la organización. El equipo de auditoría documentará los hallazgos, proporcionará planes de remedios y comunicará los resultados a las partes interesadas.

## Alcance de la Auditoría

El alcance de la auditoría interna de IT de Botium Toys cubre todo el programa de seguridad, incluidos todos los activos, procesos internos y procedimientos. Específicamente, la auditoría evaluó:

* Permisos de usuario actuales en contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusiones y herramientas de Gestión de Información y Eventos de Seguridad (SIEM).
* Controles implementados en sistemas críticos.
* Procedimientos y protocolos para estos sistemas.
* Alineación de permisos de usuario, controles, procedimientos y protocolos con los requisitos de cumplimiento.
* Inventario de la tecnología actual, incluido el acceso a hardware y sistemas.

## Objetivos de la Auditoría

Los objetivos de la auditoría interna de IT de Botium Toys son:

* Adherirse al Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST CSF).
* Establecer mejores procesos para garantizar el cumplimiento del sistema.
* Fortalecer los controles del sistema.
* Implementar el concepto de permisos mínimos en la gestión de credenciales de usuario.
* Establecer políticas y procedimientos, incluidos los playbooks.
* Asegurar el cumplimiento de los requisitos normativos.

## Evaluación de Riesgos: Activos Actuales:

Los activos gestionados incluyen equipos en las instalaciones, dispositivos de empleados, gestión de sistemas, acceso a internet, red interna, gestión de acceso de proveedores, servicios de hosting de centros de datos, retención y almacenamiento de datos, lectores de tarjetas, y mantenimiento de sistemas heredados.

### Descripción del Riesgo

Los riesgos significativos incluyen una gestión de activos inadecuada, controles insuficientes y posibles incumplimientos normativos.

### Mejores Prácticas de Control

La auditoría identificó la necesidad de adoptar prácticas de gestión de activos y mejorar los controles para cumplir con los estándares de cumplimiento y seguridad.

### Puntuación de Riesgos

La puntuación de riesgo es de 8/10 debido a controles inadecuados y posibles problemas de cumplimiento.

## Conclusiones y Recomendaciones Principales Riesgos Identificados

1. **Gestión de Activos Inadecuada:** Falta de inventario adecuado y gestión de activos tecnológicos, incluidos dispositivos de usuarios finales y sistemas críticos.
2. **Controles Insuficientes:** Sistemas críticos como contabilidad, detección de puntos finales, firewalls, sistemas de detección de intrusiones y herramientas SIEM carecen de controles de seguridad necesarios.
3. **Problemas de Cumplimiento:** Posible falta de cumplimiento con regulaciones como GDPR, PCI DSS y posiblemente HIPAA.

### Recomendaciones Inmediatas

* Implementar principios de permisos mínimos para la gestión de permisos de usuario.
* Fortalecer los controles de seguridad con autenticación multifactor y monitoreo continuo de eventos de seguridad.
* Formalizar políticas de seguridad, procedimientos y planes de respuesta a incidentes.

### Recomendaciones Futuras

* Abordar las brechas en la gestión de activos y mejorar los marcos de control.
* Lograr el cumplimiento con GDPR, PCI DSS y posiblemente HIPAA.

### Resumen de Recomendaciones a las Partes Interesadas

Las acciones inmediatas son críticas para mitigar riesgos actuales, mejorar la postura de seguridad y garantizar el cumplimiento normativo. Al implementar el principio de permisos mínimos, fortalecer los controles de seguridad y formalizar políticas y procedimientos, Botium Toys puede mejorar significativamente su postura de seguridad y cumplimiento normativo.