# Botium Toys: Internal Security Audit Report

## 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 will assess:

* Current user permissions in the accounting system, endpoint detection, firewalls, intrusion detection system, and Security Information and Event Management (SIEM) tool.
* Implemented controls in the aforementioned systems.
* Procedures and protocols for these systems.
* Alignment of user permissions, controls, procedures, and protocols with compliance requirements.
* Inventory of current technology, including both 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 by the IT Department include:

* On-premises equipment for in-office business needs.
* Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce, and inventory management.
* Internet access.
* Internal network.
* Vendor access management.
* Data center hosting services.
* Data retention and storage.
* Badge readers.
* Legacy system maintenance: end-of-life systems requiring human monitoring.

### Risk Description

Currently, asset management is inadequate. Additionally, Botium Toys lacks proper controls and may not be compliant with U.S. and international regulations and standards.

### Control Best Practices

The first of the five functions of the NIST CSF is Identify. Botium Toys needs to dedicate resources to managing assets. Additionally, they must determine the impact of losing existing assets, including systems, on business continuity.

### Risk Score

On a scale of 1 to 10, the risk score is 8, which is quite high due to a lack of controls and adherence to necessary compliance regulations and standards.

### Additional Comments

The potential impact from the loss of an asset is rated as medium because the IT department does not know which assets would be lost. The likelihood of a lost asset or fines from governing bodies is high because Botium Toys lacks necessary controls and does not adhere to required regulations and standards related to customer data privacy.

## Conclusions and Recommendations

### Major Risks to the Organization

1. **Inadequate Asset Management:** The lack of proper inventory and management of technological assets, including end-user devices and critical systems.
2. **Lack of Adequate Controls:** The absence of necessary security controls in critical systems such as accounting, endpoint detection, firewalls, intrusion detection systems, and SIEM tools.
3. **Compliance Issues:** Potential non-compliance with U.S. and international regulations and standards related to data privacy and online payment acceptance.

### Essential Controls to Implement Immediately

1. **User Permission Management:** Implement the concept of least permissions to ensure users only have access to resources necessary for their job.
2. **Strengthening Security Controls:** Establish and reinforce security controls across all critical systems, including implementing multi-factor authentication and continuous security event monitoring.
3. **Security Policies and Procedures:** Develop and formalize security policies and procedures, including operational playbooks and incident response plans.

### Compliance Regulations to Ensure Data Security

1. **General Data Protection Regulation (GDPR):** To comply with conducting business in the European Union, Botium Toys must adhere to GDPR, which regulates the protection of personal data of EU citizens.
2. **Payment Card Industry Data Security Standard (PCI DSS):** Since Botium Toys accepts online payments, compliance with PCI DSS is crucial to protect payment card data and avoid significant fines.
3. **Health Insurance Portability and Accountability Act (HIPAA):** If Botium Toys handles protected health information, it must comply with HIPAA to ensure the privacy and security of customers' health information.

# Informe de Auditoría Interna de Seguridad 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 propósito 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 sus hallazgos, proporcionará planes de remediación y comunicará los resultados a los interesados.

## Alcance de la Auditoría

El alcance de la auditoría interna de TI de Botium Toys abarca el programa de seguridad completo, lo que incluye todos los activos, procesos internos y procedimientos. Específicamente, la auditoría evaluará:

* Permisos de usuario actuales en los sistemas de contabilidad, detección de puntos finales, firewalls, sistemas de detección de intrusos y herramientas de gestión de información y eventos de seguridad (SIEM).
* Controles implementados en los sistemas mencionados.
* Procedimientos y protocolos establecidos para estos sistemas.
* Alineación de permisos de usuario, controles, procedimientos y protocolos con los requisitos de cumplimiento necesarios.
* Inventario de la tecnología actual, tanto hardware como acceso a sistemas.

## Objetivos de la Auditoría

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

* Adherirse al Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF).
* Establecer un mejor proceso para asegurar la conformidad de sus sistemas.
* Fortalecer los controles del sistema.
* Implementar el concepto de "mínimos permisos" en la gestión de credenciales de usuario.
* Establecer políticas y procedimientos, incluyendo sus manuales de operaciones.
* Asegurar el cumplimiento de los requisitos normativos.

## Evaluación de Riesgos

### Activos Actuales

Los activos gestionados por el Departamento de TI incluyen:

* Equipos en las instalaciones para necesidades comerciales de oficina.
* Equipos de empleados: dispositivos de usuario final (desktops/laptops, smartphones), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etc.
* Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventarios.
* Acceso a Internet.
* Red interna.
* Gestión de acceso de proveedores.
* Servicios de alojamiento en centros de datos.
* Retención y almacenamiento de datos.
* Lectores de tarjetas.
* Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren monitoreo humano.

### Descripción del Riesgo

Actualmente, la gestión de activos es inadecuada. Además, Botium Toys no tiene los controles adecuados y puede no cumplir con las regulaciones y estándares de EE. UU. e internacionales.

### Mejores Prácticas de Control

La primera de las cinco funciones del NIST CSF es Identificar. Botium Toys necesitará dedicar recursos a la gestión de activos. Además, deberán determinar el impacto de la pérdida de activos existentes, incluidos los sistemas, en la continuidad del negocio.

### Puntuación del Riesgo

En una escala del 1 al 10, la puntuación de riesgo es 8, lo cual es bastante alto debido a la falta de controles y adherencia a las regulaciones y estándares de cumplimiento necesarios.

### Comentarios Adicionales

El impacto potencial de la pérdida de un activo se califica como medio, ya que el departamento de TI no sabe qué activos se perderían. La probabilidad de pérdida de un activo o multas por parte de organismos reguladores es alta porque Botium Toys no tiene todos los controles necesarios en su lugar y no está cumpliendo con las regulaciones y estándares requeridos para mantener la privacidad de los datos de los clientes.

## Conclusiones y Recomendaciones

### Principales Riesgos para la Organización

1. **Gestión Inadecuada de los Activos:** La falta de un inventario y gestión adecuados de los activos tecnológicos, incluidos los dispositivos de usuario final y los sistemas críticos.
2. **Inexistencia de Controles Adecuados:** Falta de controles de seguridad necesarios en sistemas críticos como contabilidad, detección de puntos finales, firewalls, sistemas de detección de intrusos y herramientas SIEM.
3. **Cumplimiento Normativo:** Posible incumplimiento de las regulaciones y estándares de EE. UU. e internacionales relacionados con la privacidad de datos y la aceptación de pagos en línea.

### Controles Esenciales a Implementar Inmediatamente

1. **Gestión de Permisos de Usuario:** Implementar el concepto de "mínimos permisos" para garantizar que los usuarios solo tengan acceso a los recursos necesarios para su trabajo.
2. **Fortalecimiento de Controles de Seguridad:** Establecer y reforzar los controles de seguridad en todos los sistemas críticos mencionados, incluyendo la implementación de autenticación multifactor y monitoreo continuo de eventos de seguridad.
3. **Políticas y Procedimientos de Seguridad:** Desarrollar y formalizar políticas y procedimientos de seguridad, incluidos manuales de operaciones y planes de respuesta a incidentes.

### Normativas de Cumplimiento para Garantizar la Seguridad

1. **Reglamento General de Protección de Datos (GDPR):** Para garantizar el cumplimiento al realizar negocios en la Unión Europea, Botium Toys debe adherirse al GDPR, que regula la protección de datos personales de los ciudadanos de la UE.
2. **Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS):** Dado que Botium Toys acepta pagos en línea, es crucial cumplir con el PCI DSS para proteger los datos de las tarjetas de pago y evitar multas significativas.
3. **Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA):** Si Botium Toys maneja información de salud protegida, debe cumplir con HIPAA para garantizar la privacidad y seguridad de la información de salud de los clientes.