# Botium Toys: Scope, goals, and risk assessment report



## Scope and goals of the audit

**Scope:** The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

**Goals:** Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that need to be implemented to improve Botium Toys’ security posture.

## 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.
* Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human monitoring

## Risk assessment

### Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully 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 will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

### Risk score

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.

### 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 at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system that enforces the password policy’s minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* The store’s physical location, which includes Botium Toys’ main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

**Botium Toys: Alcance, objetivos e informe de evaluación de riesgos**

**Alcance y objetivos de la auditoría**

**Alcance:** El alcance de esta auditoría se define como todo el programa de seguridad de Botium Toys. Esto incluye sus activos, como el equipo y dispositivos de los empleados, su red interna y sus sistemas. Será necesario revisar los activos que posee Botium Toys, así como los controles y prácticas de cumplimiento que tiene implementados.

**Objetivos:** Evaluar los activos existentes y completar la lista de verificación de controles y cumplimiento para determinar qué controles y mejores prácticas de cumplimiento deben implementarse con el fin de mejorar la postura de seguridad de Botium Toys.

**Activos actuales**

Los activos gestionados por el Departamento de TI incluyen:

* Equipos locales para las necesidades de negocio en la oficina.
* Equipos de los empleados: dispositivos de usuario final (sobremesas/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etc.
* Productos de tienda disponibles para la venta minorista en el local y en línea; almacenados en el almacén contiguo de la empresa.
* Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventario.
* Acceso a Internet.
* Red interna.
* Retención y almacenamiento de datos.
* Mantenimiento de sistemas heredados: sistemas en fin de vida que requieren supervisión humana.

**Evaluación de riesgos**

**Descripción del riesgo:**  
Actualmente, existe una gestión inadecuada de los activos. Además, Botium Toys no cuenta con todos los controles adecuados y puede que no cumpla plenamente con las normativas y estándares estadounidenses e internacionales.

**Mejores prácticas de control:**  
La primera de las cinco funciones del NIST CSF es *Identificar*. Botium Toys deberá dedicar recursos para identificar los activos y poder gestionarlos adecuadamente. Además, deberá clasificar los activos existentes y determinar el impacto de la pérdida de dichos activos, incluidos los sistemas, sobre la continuidad del negocio.

**Puntuación de riesgo:**  
En una escala del 1 al 10, la puntuación de riesgo es **8**, lo que se considera bastante alto. Esto se debe a la falta de controles y de adhesión a las mejores prácticas de cumplimiento.

**Comentarios adicionales:**  
El impacto potencial de la pérdida de un activo se valora como **medio**, porque el departamento de TI no sabe qué activos estarían en riesgo. El riesgo para los activos o las sanciones de los organismos reguladores es **alto**, ya que Botium Toys no cuenta con todos los controles necesarios y no sigue plenamente las mejores prácticas de cumplimiento para mantener los datos críticos privados y seguros.

Detalles específicos:

* Actualmente, todos los empleados de Botium Toys tienen acceso a los datos almacenados internamente y podrían acceder a datos de titulares de tarjetas y a la PII/SPII de los clientes.
* No se utiliza cifrado para garantizar la confidencialidad de la información de tarjetas de crédito de clientes que se acepta, procesa, transmite y almacena localmente en la base de datos interna de la empresa.
* No se han implementado controles de acceso basados en el principio de privilegio mínimo ni separación de funciones.
* El departamento de TI ha asegurado la disponibilidad y ha integrado controles para garantizar la integridad de los datos.
* El departamento de TI cuenta con un cortafuegos que bloquea el tráfico según un conjunto de reglas de seguridad adecuadamente definido.
* El software antivirus está instalado y es supervisado regularmente por el departamento de TI.
* El departamento de TI no ha instalado un sistema de detección de intrusiones (IDS).
* No existen planes de recuperación ante desastres, y la empresa no dispone de copias de seguridad de datos críticos.
* El departamento de TI ha establecido un plan para notificar a los clientes de la UE en un plazo de 72 horas en caso de violación de seguridad. Además, se han desarrollado políticas, procedimientos y procesos de privacidad, que se aplican entre los miembros del departamento de TI y otros empleados, para documentar y mantener adecuadamente los datos.
* Aunque existe una política de contraseñas, sus requisitos son mínimos y no cumplen con los requisitos actuales de complejidad mínima (por ejemplo, al menos ocho caracteres, una combinación de letras y al menos un número, y caracteres especiales).
* No existe un sistema centralizado de gestión de contraseñas que haga cumplir los requisitos mínimos de la política de contraseñas, lo que a veces afecta a la productividad cuando empleados/proveedores envían un ticket al departamento de TI para recuperar o restablecer una contraseña.
* Aunque los sistemas heredados son supervisados y mantenidos, no existe un calendario regular para estas tareas y los métodos de intervención no están claros.
* La ubicación física de la tienda, que incluye las oficinas principales de Botium Toys, el local comercial y el almacén de productos, dispone de cerraduras suficientes, sistemas de videovigilancia (CCTV) actualizados, así como sistemas de detección y prevención de incendios en funcionamiento.

**RESUMEN DEL INFORME**

**1. Alcance:**  
Revisión de todo el programa de seguridad, incluyendo:

* Equipos y dispositivos de empleados.
* Red interna y sistemas.
* Activos físicos y digitales.
* Controles y cumplimiento normativo.

**2. Objetivos:**

* Evaluar los activos existentes.
* Completar la lista de verificación de controles y cumplimiento.
* Proponer mejoras para reforzar la seguridad.

**3. Activos clave:**

* Equipos de oficina y dispositivos de empleados (PCs, portátiles, móviles, etc.).
* Productos de tienda (venta física y online).
* Sistemas y software (contabilidad, seguridad, e-commerce, inventario).
* Acceso a Internet y red interna.
* Datos y almacenamiento.
* Sistemas heredados que requieren supervisión manual.

**4. Riesgos detectados:**

* Gestión insuficiente de activos.
* Controles de seguridad incompletos.
* Posible incumplimiento de normativas de EE. UU. e internacionales.
* Falta de identificación y clasificación de activos.
* Puntuación de riesgo: **8/10 (alta)**.

**5. Principales deficiencias:**

* Acceso excesivo a datos internos y PII/SPII de clientes.
* Sin cifrado para datos de tarjetas de crédito.
* Ausencia de controles de privilegio mínimo y separación de funciones.
* Sin IDS ni plan de recuperación ante desastres.
* Política de contraseñas poco estricta y sin gestión centralizada.
* Mantenimiento irregular de sistemas heredados.

**6. Aspectos positivos:**

* Cortafuegos configurado correctamente.
* Antivirus instalado y monitorizado.
* Controles para integridad y disponibilidad de datos.
* Seguridad física adecuada (cerraduras, CCTV, detección y prevención de incendios).

**7. Impacto estimado:**

* **Medio**: pérdida de activos por falta de inventario claro.
* **Alto**: multas y sanciones por incumplimiento de normativas de protección de datos.