# Botium Toys: Informe de alcance, objetivos y 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 los equipos y dispositivos de los empleados, su red interna y sus sistemas. Deberá revisar los activos de Botium Toys y los controles y prácticas de cumplimiento implementados.

**Objetivos:** Evalúe los activos existentes y complete la lista de verificación de controles y cumplimiento para determinar qué controles y mejores prácticas de cumplimiento deben implementarse para mejorar la postura de seguridad de Botium Toys.

## Activos corrientes

Los activos gestionados por el Departamento de TI incluyen:

- Equipos locales para necesidades comerciales en la oficina
- Equipos de los empleados: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etc.
- Productos de tienda disponibles para venta minorista en el sitio 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 inventarios.
- acceso a Internet
- Red interna
- Retención y almacenamiento de datos
- Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren supervisión humana

# Evaluación de riesgos

## Descripción del riesgo

Actualmente, la gestión de activos es deficiente. Además, Botium Toys no cuenta con todos los controles adecuados y podría no cumplir plenamente con las regulaciones y estándares estadounidenses e internacionales.

## Mejores prácticas de control

La primera de las cinco funciones del CSF del NIST es la de Identificar. Botium Toys deberá dedicar recursos a la identificación de activos para gestionarlos adecuadamente. Además, deberá clasificar los activos existentes y determinar el impacto de su pérdida, incluidos los sistemas, en la continuidad del negocio.

## Puntuación de riesgo

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

## Comentarios adicionales

El impacto potencial de la pérdida de un activo se considera medio, ya que el departamento de TI desconoce qué activos estarían en riesgo. El riesgo de que se produzcan daños a los activos o multas por parte de los organismos reguladores es alto porque Botium Toys no cuenta con todos los controles necesarios ni cumple plenamente con las mejores prácticas de cumplimiento normativo que garantizan la privacidad y seguridad de los datos críticos. Consulte los siguientes puntos para obtener más información:

- Actualmente, todos los empleados de Botium Toys tienen acceso a datos almacenados internamente y pueden acceder a los datos del titular de la tarjeta y a la información personal identificable (PII/SPII) de los clientes.
- Actualmente no se utiliza el cifrado para garantizar la confidencialidad de la información de las tarjetas de crédito de los 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 relacionados con el mínimo privilegio y la separación de funciones.
- El departamento de TI ha garantizado la disponibilidad y controles integrados para garantizar la integridad de los datos.
- El departamento de TI tiene un firewall que bloquea el tráfico según un conjunto

de reglas de seguridad definidas adecuadamente.

- El departamento de TI instala y supervisa periódicamente el software antivirus.
- El departamento de TI no ha instalado un sistema de detección de intrusiones (IDS).
- Actualmente no existen planes de recuperación ante desastres y la empresa no tiene 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 una vulneración 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.
- Si bien existe una política de contraseñas, sus requisitos son nominales y no están en línea con los requisitos mínimos de complejidad de contraseñas actuales (por ejemplo, al menos ocho caracteres, una combinación de letras y al menos un número; caracteres especiales).
- No existe un sistema centralizado de gestión de contraseñas que aplique los requisitos mínimos de la política de contraseñas, lo que a veces afecta la productividad cuando los empleados/proveedores envían un ticket al departamento de TI para recuperar o restablecer una contraseña.
- Si bien los sistemas heredados se monitorean y mantienen, no existe un cronograma 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 frente de la tienda y el almacén de productos, cuenta con cerraduras suficientes, vigilancia por circuito cerrado de televisión (CCTV) actualizada, así como sistemas de detección y prevención de incendios en funcionamiento.