Botium Toys: Informe de alcance, objetivos y evaluación de riesgos

---

Alcance y objetivos de la auditoría

Alcance:
El alcance de esta auditoría abarca 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. Deberás revisar los activos que posee Botium Toys y las prácticas de control y cumplimiento que tienen implementadas.

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 en las instalaciones para necesidades comerciales en la oficina
- Equipos de los empleados: dispositivos de usuario final (computadores de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etc.
- Productos en la tienda disponibles para venta minorista en el sitio y en línea; almacenados en el almacén adyacente 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 obsoletos que requieren supervisión humana

Evaluación de riesgos

Descripción del riesgo:
Actualmente, existe una gestión inadecuada de los activos. Además, Botium Toys no tiene implementados todos los controles necesarios y puede no estar cumpliendo completamente 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 deberá dedicar recursos a la identificación de activos para poder gestionarlos adecuadamente. Además, deberán clasificar los activos existentes y determinar el impacto que tendría la pérdida de dichos activos, 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 que indica un riesgo bastante alto. Esto se debe a la falta de controles y al incumplimiento de las mejores prácticas en materia de cumplimiento.

Comentarios adicionales:
El impacto potencial por la pérdida de un activo se califica como **medio**, debido a que el departamento de TI no sabe con certeza cuáles activos estarían en riesgo. El **riesgo para los activos o sanciones por parte de organismos reguladores es alto**, ya que Botium Toys no cuenta con todos los controles necesarios y no cumple completamente con las regulaciones de cumplimiento que garantizan la privacidad y seguridad de los datos críticos. A continuación, se detallan puntos específicos:

- Actualmente, todos los empleados de Botium Toys tienen acceso a los datos almacenados internamente y podrían acceder a datos de tarjetas de crédito y PII/SPII (información personal identificable o sensible) de los clientes.

- No se utiliza cifrado para garantizar la confidencialidad de la información de 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 principio de **mínimo privilegio** ni con la **separación de funciones**.

- El departamento de TI ha garantizado la disponibilidad y ha integrado controles para asegurar la integridad de los datos.

- El departamento de TI cuenta con un firewall que bloquea el tráfico con base en un conjunto apropiado de reglas de seguridad.

- El software antivirus está instalado y es monitoreado regularmente por el departamento de TI.

- El departamento de TI no ha instalado un sistema de detección de intrusos (IDS).

- No existen planes de recuperación ante desastres y la empresa no tiene copias de seguridad de los datos críticos.

- El departamento de TI tiene un plan para notificar a los clientes de la UE en un plazo de 72 horas en caso de una violación de seguridad. Además, se han desarrollado políticas, procedimientos y procesos de privacidad que se aplican tanto al personal de TI como a otros empleados, para documentar y mantener correctamente los datos.

- Aunque existe una política de contraseñas, sus requisitos son mínimos y no cumplen con los estándares actuales de complejidad mínima (por ejemplo, al menos ocho caracteres, una combinación de letras y al menos un número o carácter especial).

- No existe un sistema centralizado de gestión de contraseñas que imponga los requisitos mínimos de la política de contraseñas, lo cual a veces afecta la productividad cuando los empleados/proveedores deben enviar un ticket al departamento de TI para recuperar o restablecer una contraseña.

- Aunque los sistemas heredados son monitoreados y mantenidos, no existe un cronograma regular para estas tareas ni están claros los métodos de intervención.

- La ubicación física de la tienda, que incluye las oficinas principales de Botium Toys, la tienda y el almacén de productos, cuenta con cerraduras adecuadas, sistemas actualizados de vigilancia por CCTV, así como sistemas de detección y prevención de incendios en funcionamiento.