Informe de Auditoría de Seguridad de Botium Toys

INDICE

1. Alcance y Objetivos de la Auditoría

Alcance:
El alcance de esta auditoría abarca la revisión completa del programa de seguridad de Botium Toys, incluyendo:

- Los activos tecnológicos (equipos y dispositivos de empleados).
- La red interna y los sistemas críticos.
- Los sistemas de gestión de datos y su almacenamiento.

Objetivos:
El objetivo es evaluar los activos tecnológicos actuales de la empresa y completar una lista de verificación de cumplimiento y control. Esto permitirá identificar qué controles y mejores prácticas se deben implementar para mejorar la postura de seguridad de Botium Toys y asegurar el cumplimiento con normativas internacionales.

2. Activos Tecnológicos Evaluados

Los principales activos gestionados por el departamento de TI incluyen:

- Equipos locales: Computadoras, servidores y otros dispositivos utilizados en la oficina para actividades comerciales.
- Dispositivos de empleados: Equipos finales como computadoras de escritorio, portátiles, teléfonos inteligentes, estaciones de trabajo remotas, periféricos (auriculares, cables, teclados, ratones, cámaras de vigilancia, entre otros).
- Productos de escaparate: Mercancía disponible para la venta tanto en la tienda física como en la plataforma de comercio electrónico.
- Sistemas de gestión: Software relacionado con contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventarios.
- Red interna: La infraestructura de red interna que soporta todas las operaciones de TI.
- Almacenamiento de datos: Sistemas utilizados para almacenar datos críticos y confidenciales.
- Sistemas heredados: Sistemas que han llegado al final de su ciclo de vida y requieren monitoreo manual para su correcto funcionamiento.

3. Evaluación de Riesgos

Descripción del Riesgo:
Actualmente, se ha identificado una gestión ineficaz de los activos. Botium Toys no tiene implementados todos los controles de seguridad necesarios y no cumple con diversas normativas, tanto nacionales como internacionales.

Controles y Mejores Prácticas:
La primera función del Marco de Ciberseguridad del NIST (NIST CSF) es "Identificar". Botium Toys necesita destinar recursos para identificar y clasificar los activos críticos, determinando el impacto que tendría su pérdida en la continuidad del negocio.

Puntuación de Riesgo:
La puntuación de riesgo asignada es 8/10, lo que representa un nivel alto de vulnerabilidad debido a la falta de controles y el incumplimiento de las mejores prácticas de seguridad.

Impacto Potencial:
El impacto potencial de la pérdida de un activo es considerado "medio", ya que el departamento de TI no tiene claro qué activos específicos estarían en riesgo. Sin embargo, el riesgo de sufrir sanciones regulatorias es alto, debido a que Botium Toys no cumple con las normativas necesarias para proteger la privacidad y seguridad de los datos.

4. Principales Vulnerabilidades Identificadas

- Acceso no controlado: Todos los empleados tienen acceso a los datos internos, incluidos los datos sensibles de los clientes (información de tarjetas de crédito y PII/SPII).
- Falta de cifrado: La información de tarjetas de crédito almacenada, procesada y transmitida no está cifrada.
- Controles de acceso insuficientes: No se han implementado controles relacionados con el principio de privilegio mínimo ni con la separación de funciones.
- Seguridad de red: Aunque la empresa cuenta con un firewall para bloquear tráfico no autorizado, no dispone de un Sistema de Detección de Intrusos (IDS).
- Planes de contingencia ausentes: No existen planes de recuperación ante desastres, ni se realizan copias de seguridad de los datos críticos.
- Contraseñas inseguras: Las políticas de contraseñas son débiles, no exigen requisitos de complejidad mínimos.
- Falta de sistema centralizado de gestión de contraseñas: Esto afecta la productividad cuando los empleados o proveedores necesitan restablecer contraseñas.
- Mantenimiento irregular de sistemas heredados: No hay un cronograma regular ni procedimientos claros para el monitoreo y mantenimiento de sistemas críticos al final de su ciclo de vida.
- Controles físicos: Aunque la infraestructura física está protegida con sistemas de CCTV, cerraduras adecuadas y sistemas de prevención de incendios, se recomienda fortalecer estas medidas.

5. Lista de Verificación de Controles

Control Evaluado	Sí	No
Privilegio mínimo		✔
Plan de recuperación ante desastres		✔
Políticas de contraseñas seguras		✔
Separación de funciones		✔
Cortafuegos	✔	
Sistema de Detección de Intrusos (IDS)		✔
Copias de seguridad		✔
Software antivirus	✔	
Mantenimiento de sistemas heredados		✔
Cifrado de datos		✔
Sistema de gestión de contraseñas		✔
Control de acceso físico (cerraduras, CCTV)	✔	
Sistemas de prevención de incendios	✔	

6. Lista de verificación de cumplimiento

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

Sí	No	Mejores prácticas
	✔	Sólo los usuarios autorizados tienen acceso a la información de la tarjeta de crédito de los clientes.
	✔	La información de la tarjeta de crédito se almacena, acepta, procesa y transmite internamente, en un entorno seguro.
	✔	Implemente procedimientos de cifrado de datos para proteger mejor los datos y los puntos de contacto de las transacciones con tarjetas de crédito.
	✔	Adopte políticas seguras de gestión de contraseñas.

Reglamento General de Protección de Datos (GDPR)

Sí	No	Mejores prácticas
	✔	UE. Los datos de los clientes se mantienen privados/seguros.
✔		Existe un plan para notificar a la UE y sus clientes dentro de las 72 horas si sus datos se ven comprometidos/hay una violación.

✔ Asegúrese de que los datos estén clasificados e inventariados adecuadamente.

✔ Hacer cumplir políticas, procedimientos y procesos de privacidad para documentar y mantener adecuadamente los datos.

Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)

Sí	No	Mejores prácticas
	✔	Se establecen políticas de acceso de usuarios.
	✔	Los datos confidenciales (PII/SPII) son confidenciales/privados.
✔		La integridad de los datos garantiza que los datos sean coherentes, completos, precisos y hayan sido validados.
✔		Los datos están disponibles para las personas autorizadas a acceder a ellos.

7. Recomendaciones para Mejorar la Postura de Seguridad de Botium Toys

- Implementar el Principio de Privilegio Mínimo: Limitar el acceso a los datos y sistemas críticos solo a los empleados autorizados. Revisar y actualizar los permisos de acceso de manera periódica.
- Adoptar Políticas de Gestión de Contraseñas Seguras: Implementar políticas de contraseñas más estrictas, que incluyan requisitos de complejidad (número mínimo de caracteres, inclusión de letras, números y caracteres especiales) y la necesidad de cambios periódicos. Además, se recomienda instalar un sistema de gestión centralizada de contraseñas.
- Cifrar los Datos Sensibles: Implementar procedimientos de cifrado para la información de tarjetas de crédito tanto en reposo como en tránsito. Esto incluye cifrar todos los datos confidenciales almacenados en la base de datos y las transacciones que involucran estos datos.
- Desarrollar un Plan de Recuperación ante Desastres: Establecer un plan formal de recuperación ante desastres para asegurar la continuidad del negocio en caso de incidentes. El plan debe ser probado y revisado regularmente.
- Adoptar una Estrategia de Copias de Seguridad Integral: Realizar copias de seguridad periódicas de todos los datos críticos y almacenarlas en ubicaciones seguras. Se recomienda probar las copias de seguridad periódicamente para asegurar que los datos puedan recuperarse correctamente.
- Implementar un Sistema de Detección y Prevención de Intrusos (IDS/IPS): Instalar y configurar un IDS/IPS para monitorear y detectar actividades sospechosas en la red. Asegurarse de que el sistema esté actualizado y en pleno funcionamiento.
- Fortalecer el Cumplimiento de las Políticas de Privacidad: Revisar y actualizar las políticas de privacidad y protección de datos para cumplir con regulaciones

internacionales como el GDPR. Implementar procesos de clasificación y documentación adecuada de los datos.

- Reforzar los Controles Físicos y Operacionales: Asegurar que las áreas sensibles, como oficinas y almacenes, estén adecuadamente protegidas con cerraduras, CCTV y sistemas de detección de incendios. Limitar el acceso físico a los activos críticos.
- Monitoreo y Mantenimiento Regular de Sistemas Heredados: Establecer un plan de monitoreo continuo y mantenimiento preventivo de los sistemas heredados, implementando herramientas de gestión de vulnerabilidades.

Estas recomendaciones ayudarán a Botium Toys a reducir los riesgos de seguridad, asegurar la integridad de sus datos y mejorar el cumplimiento de normativas internacionales.