INTERNAL AUDIT
WEBINAR SERIES

Auditoría Interna de Seguridad del Departamento de Tecnologías de la Informática - Botium Toys

Fecha: Jueves 13/11/2025
Autor: Ginely De Vita
Curso: Fundamentos de Ciberseguridad -- Simulación de Auditoría Interna de Seguridad
Organización: Botium Toys

Resumen Ejecutivo

Esta auditoría interna del departamento de TI evalúa la postura de ciberseguridad de Botium Toys, una pequeña empresa de juguetes con sede en EE. UU., una única oficina física y una presencia global en el comercio electrónico en rápida expansión. La auditoría se inició debido al aumento de las exigencias operativas del departamento de TI y a la creciente exposición a clientes internacionales y requisitos normativos.

La evaluación reveló varias deficiencias de alto riesgo: gestión incompleta de activos, controles insuficientes en sistemas críticos, falta de procedimientos documentados y posible incumplimiento de marcos normativos como PCI DSS, RGPD y las mejores prácticas del sector alineadas con el Marco de Ciberseguridad (CSF) del NIST. La puntuación de riesgo general actual es de 8/10, debido principalmente a la falta de controles y a la escasa visibilidad de los activos y los permisos de acceso de los usuarios.

Es necesario tomar medidas correctivas inmediatas para fortalecer las defensas del sistema, cumplir con las obligaciones de cumplimiento relacionadas con los pagos en línea y los clientes de la UE, y respaldar el crecimiento de la empresa. Los hallazgos justifican la solicitud del gerente de TI de ampliar el equipo de ciberseguridad para satisfacer las necesidades operativas y de cumplimiento.

---

1. Introducción

Este informe documenta los resultados de una auditoría interna simulada de seguridad informática realizada a Botium Toys como parte de un programa de capacitación en ciberseguridad. El ejercicio se basa íntegramente en documentación de auditoría ficticia, pero realista, que incluye:

- Instrucciones del escenario
- Alcance y objetivos definidos por la dirección de TI
- Una evaluación formal de riesgos
- Una evaluación de la aplicabilidad de los controles
- Una referencia de las categorías de control
- Una lista de verificación de los requisitos de cumplimiento
- Un memorándum para las partes interesadas

Botium Toys mantiene infraestructura local para sus operaciones comerciales y, al mismo tiempo, gestiona un mercado global en línea. Estas condiciones aumentan la exposición de la organización a amenazas de seguridad y obligaciones regulatorias, lo que exige una revisión integral de su postura de seguridad.

---

2. Alcance y objetivos

2.1 Alcance de la Auditoría

El alcance, definido por el responsable de TI, abarca todo el programa de seguridad informática, incluyendo:

- Permisos de usuario en:
    - Sistemas de contabilidad
    - Detección de endpoints
    - Firewalls
    - Sistema de detección de intrusiones (IDS)
    - Gestión de información y eventos de seguridad (SIEM)
    - Controles actuales implementados en los sistemas mencionados
    - Procedimientos y protocolos de TI relacionados con el uso del sistema
    - Cumplimiento con las normativas estadounidenses e internacionales aplicables
    - Inventario de hardware, sistemas y accesos
    - Activos heredados y obsoletos que requieren monitorización

2.2 Objetivos de la Auditoría

El gerente de TI estableció los siguientes objetivos:

- Alinear el programa con el Marco de Ciberseguridad (CSF) del NIST
- Fortalecer los controles y procesos del sistema
- Aplicar el principio de privilegio mínimo
- Mejorar la preparación para el cumplimiento de las normativas estadounidenses y europeas
- Desarrollar políticas, procedimientos y manuales de procedimientos fundamentales
- Proporcionar evidencia que justifique la ampliación del equipo de seguridad informática

---

3. Metodología

3.1 Revisión de documentos

Se analizaron los documentos proporcionados por el escenario:

- Instrucciones del escenario
- Evaluación de riesgos
- Categorías de control
- Lista de verificación de aplicabilidad de controles
- Lista de verificación de cumplimiento
- Memorándum para las partes interesadas

3.2 Evaluación de riesgos

- Se evaluaron el impacto y la probabilidad con base en la puntuación de riesgo proporcionada.
- Las deficiencias se asignaron a las categorías del Marco de Factores de Conformidad (CSF) del NIST.

3.3 Revisión de controles

- Los controles se marcaron como “**Aplicables**” o “**No aplicable**s” utilizando la lista de verificación de evaluación.
- Los controles faltantes se asignaron a las necesidades de remediación inmediatas o futuras.

3.4 Mapeo de cumplimiento

- Se revisó la exposición a PCI DSS y al RGPD de la UE con base en:
    - Procesamiento de pagos en línea
    - Base de clientes internacionales

3.5 Síntesis para el informe

- Los hallazgos se clasificaron como **Inmediatos** (alto riesgo) o **Futuros** (riesgo medio/bajo).
- Las recomendaciones se alinearon con los estándares de la industria y las limitaciones organizacionales

---

4. Resultados y observaciones

4.1 Hallazgos Inmediatos (de Alto Riesgo)

1. Gestión de Activos Inadecuada

- No existe un inventario completo de hardware, software ni accesos.
- Impacto desconocido en caso de fallo o vulneración de los activos.

2. Falta de Controles Críticos

Los sistemas clave carecen de configuraciones necesarias, tales como:

- Reglas de firewall adecuadas
- Ajuste del IDS
- Políticas de protección de endpoints
- Reglas de correlación del SIEM

3. Permisos de Usuario Inconsistentes

- Varios usuarios poseen privilegios elevados sin justificación.
- No existe un proceso estandarizado de aprovisionamiento/desaprovisionamiento.
- No se aplica el principio de privilegio mínimo.

4. Posible Incumplimiento

- Riesgo de RGPD debido a clientes de la UE y falta de gobernanza de la privacidad.
- Riesgo de PCI DSS debido al procesamiento de pagos en línea sin controles documentados.
- Falta documentación para:
    - Retención de datos
    - Control de acceso
    - Respuesta a incidentes

4.2 Hallazgos de Riesgo Medio/Bajo

1. Falta de políticas y procedimientos formales

- Falta un protocolo de respuesta ante incidentes
- La gestión de cambios no está documentada
- No existe un programa de concientización sobre seguridad

2. Deficiencias tecnológicas

- Algunos sistemas están obsoletos y requieren supervisión humana
- Los sistemas heredados aumentan el riesgo operativo

3. Supervisión del acceso de proveedores

- No se supervisa el acceso de terceros
- No se revisan los requisitos de cumplimiento de los proveedores

---

5. Análisis de riesgos

Basado en la evaluación de riesgos proporcionada en el curso:

Categoría	Descripción
Puntuación de Riesgo General	**8/10 (Alta)**
Impacto	Medio (debido al impacto desconocido en los activos)
Probabilidad	Alta (falta de controles + riesgo de incumplimiento
Factores Clave	Falta de controles, inventario incompleto, ausencia de políticas

El mayor riesgo se debe a:

- Falta de visibilidad de los activos
- Alta probabilidad de exposición de datos
- Alta probabilidad de sanciones regulatorias

---

6. Evaluación del cumplimiento

1. Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS)

Dado que la empresa acepta pagos en línea. El incumplimiento de los controles PCI puede resultar en:

- Multas
- Auditorías obligatorias
- Aumento de las comisiones de los procesadores de pago

2. Reglamento General de Protección de Datos (RGPD)

Botium Toys vende a clientes en la Unión Europea, lo que implica la aplicación del RGPD. Deficiencias actuales:

- Ausencia de un Delegado de Protección de Datos
- Ausencia de una política de privacidad alineada con el RGPD
- Ausencia de procesos documentados de retención de datos o consentimiento

3. Expectativas de Privacidad y Manejo de Datos en EE. UU.

Si bien no son específicas del sector:

- Se requieren controles de seguridad razonables
- Se aplican las leyes de notificación de violaciones de datos

4. Alineación con el Marco de Seguridad de NIST

El gerente espera una alineación completa con:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar
- Gobernar (incluido en NIST CSF 2.0)

5. Controles de Sistemas y Organizaciones (SOC 1 y SOC 2)

Aplica debido al manejo de información financiera (SOC 1) y datos sensibles (SOC 2).
Deficiencias observadas:

- Controles de acceso no estandarizados
- Falta de monitoreo continuo
- Ausencia de evaluaciones formales de terceros

6. Ley de Privacidad del Consumidor de California/Ley de Derechos de Privacidad de California (CCPA/CPRA)

Botium Toys atiende clientes en EE. UU., incluidos residentes de California y:

- No se observa un mecanismo claro para que los usuarios ejerzan sus derechos
- La política de privacidad no sigue formato CCPA
- Existe una falta de registro de solicitudes de privacidad

7. Ley de Protección de la Privacidad Infantil en Internet (COPPA)

La empresa vende juguetes y procesa datos de menores.
Requerimientos:

- Consentimiento verificable de padres
- Limitación estricta de datos procesados
- Mecanismos de eliminación de datos

Deficiencia clave:

- No existe proceso formal de verificación parental

---

7. Evaluación de los controles

Según la lista de verificación de aplicabilidad de controles:

Controles faltantes (Alta prioridad)

- Políticas de control de acceso
- Mecanismos de aplicación del principio de privilegio mínimo
- Configuración base del firewall y del IDS
- Reglas de monitoreo del SIEM
- Estándares de registro y alertas

Controles para implementar posteriormente

- Ampliación de la autenticación multifactor
- Flujos de trabajo de gestión de cambios
- Documentación del ciclo de vida de los activos
- Programa de gestión de riesgos de proveedores

---

8. Recomendaciones

8.1 Recomendaciones inmediatas

1. **Crear un inventario completo de activos** (software, hardware, accesos).
2. **Implementar el principio de mínimo privilegio mediante:**
    - Revisión de roles
    - Eliminación de accesos innecesarios

3. **Reforzar los controles técnicos:**
    - Firewalls
    - IDS
    - Protección de endpoints
    - Correlación SIEM

4. **Implementar controles de cumplimiento fundamentales:**
    - Mapeo de requisitos PCI DSS
    - Avisos y documentación de privacidad del RGPD

5. **Desarrollar políticas obligatorias:**
    - Política de control de acceso
    - Política de retención de datos
    - Plan de respuesta ante incidentes

8.2 Recomendaciones futuras

1. **Ampliar la autenticación multifactor (MFA) a todos los sistemas.**
2. **Desarrollar un proceso de gestión de riesgos de proveedores.**
3. **Crear manuales de procedimientos para:**
    - Respuesta ante incidentes
    - Gestión de cambios
4. **Capacitar al personal en concienciación sobre ciberseguridad.**
5. **Planificar actualizaciones graduales o sustitución de los sistemas heredados.**

---

9. Conclusión

Botium Toys enfrenta importantes riesgos de seguridad y cumplimiento normativo debido al rápido crecimiento de sus operaciones en línea y la ausencia de controles fundamentales. El nivel de riesgo actual de 8/10 pone de manifiesto la necesidad urgente de mejorar la gestión de activos, el control de acceso, la preparación para el cumplimiento normativo y el fortalecimiento de los sistemas.

Los resultados de la auditoría respaldan la solicitud del gerente de TI de ampliar el equipo de seguridad para mantener el control, reducir la exposición al riesgo y cumplir con las crecientes exigencias regulatorias.

La implementación de las recomendaciones descritas en este informe ayudará a la empresa a avanzar hacia la alineación con el Marco de Ciberseguridad (CFS) del NIST, respaldar operaciones comerciales internacionales seguras y fortalecer su postura general de ciberseguridad.

Apéndices

Los documentos de referencia y materiales utilizados como soporte durante la ejecución de esta auditoría interna están disponibles en la carpeta de apéndices del repositorio del proyecto. A continuación, se detallan los anexos incluidos:

- **Apéndice A — Escenario de Auditoría y Lineamientos Operativos**
- **Apéndice B — Alcance y Objetivos de Auditoría Establecidos**
- **Apéndice C — Matriz de Evaluación de Riesgos**
- **Apéndice D — Clasificación y Descripción de Categorías de Control**
- **Apéndice E — Matriz de Evaluación y Resultados de Controles**
- **Apéndice F — Lista de Verificación de Cumplimiento Normativo**
- **Apéndice G — Memorándum de Comunicación a Partes Interesadas**