### Auditoría de seguridad - Parte 1: Botium Toys

#### 1. Alcance y objetivos de la auditoría

**Resumen**

Realizar una auditoría del programa de ciberseguridad de Botium Toys con el propósito de alinear las políticas comerciales actuales con las prácticas recomendadas y los estándares de la industria. El objetivo de la auditoría es proporcionar recomendaciones de mitigación para las vulnerabilidades de alto riesgo y presentar una estrategia general para mejorar la postura de seguridad de la organización.

**Alcance**

La auditoría interna de TI de Botium Toys analizará la totalidad del programa de seguridad de la empresa. Esto incluye la evaluación de todos los activos, así como los procesos y procedimientos internos.

La auditoría se centrará en los permisos de usuario, los controles y los protocolos para sistemas como contabilidad, detección de puntos de conexión, *firewalls*, sistema de detección de intrusiones y SIEM. Además, verificará que los permisos, controles, procedimientos y protocolos de los usuarios estén alineados con los requisitos de cumplimiento normativo y que la tecnología esté debidamente registrada.

**Objetivos**

Los objetivos de la auditoría interna de TI de Botium Toys son los siguientes:

* Cumplir con el Marco de Ciberseguridad (CSF) del NIST.
* Establecer un proceso más efectivo para garantizar el cumplimiento de los sistemas.
* Fortalecer los controles del sistema.
* Implementar el principio de mínimo privilegio en la gestión de credenciales o tarjetas de identificación de usuarios.
* Establecer políticas y procedimientos claros, que incluyan manuales de estrategia.
* Asegurar el acatamiento de los requisitos de cumplimiento normativo.

#### 2. Evaluación de riesgos

**Descripción del riesgo**

Actualmente, existe una gestión insuficiente de los activos. Botium Toys no ha implementado los controles adecuados y es posible que no cumpla con las regulaciones y los estándares estadounidenses e internacionales. La probabilidad de pérdida de un activo o de multas por parte de órganos reguladores es alta, ya que la empresa no tiene los controles necesarios implementados y no cumple con las normativas y estándares requeridos para mantener la privacidad de los datos de los clientes.

**Puntuación de riesgo** En una escala de 1 a 10, la puntuación de riesgo es de 8, lo cual es bastante alto. Esto se debe a la falta de controles y al incumplimiento de las regulaciones y los estándares necesarios.

#### 3. Evaluación de controles

**Controles administrativos**

| **Nombre de control** | **Tipo de control y explicación** | **Se tiene que implementar (X)** | **Prioridad** |
| --- | --- | --- | --- |
| Principio de mínimo privilegio | Preventivo. Reduce el riesgo al asegurar que proveedores y personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar su trabajo. | X | Alta |
| Planes de recuperación ante incidentes | Correctivo. Garantiza la continuidad del negocio y la productividad en caso de incidentes. | X | Alta |
| Políticas de contraseñas | Preventivo. Establece requisitos de seguridad de contraseñas para reducir la probabilidad de comprometer la cuenta. | X | Alta |
| Políticas de control de acceso | Preventivo. Aumenta la confidencialidad e integridad de los datos. | X | Alta |
| Políticas de gestión de cuentas | Preventivo. Reduce la superficie expuesta a ataques y limita el impacto de ex empleados/as. | X | Media |
| Separación de funciones | Preventivo. Garantiza que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales. | X | Media |

**Controles técnicos**

| **Nombre de control** | **Tipo de control y explicación** | **Se tiene que implementar (X)** | **Prioridad** |
| --- | --- | --- | --- |
| Cortafuegos (firewall) | Preventivo. Ya hay instalados firewalls para filtrar el tráfico no deseado/malicioso. |  |  |
| Sistema de detección de intrusiones (IDS) | De detección. Permite al equipo de TI identificar posibles intrusiones (tráfico anómalo) rápidamente. | X | Alta |
| Cifrado | Disuasivo. Garantiza que la información y los datos confidenciales sean más seguros (por ejemplo, transacciones de pago). | X | Alta |
| Copias de seguridad | Correctivo. Permite la continuidad del negocio y mantiene la productividad en caso de incidentes. | X | Alta |
| Gestión de contraseñas | Correctivo. Recupera y restablece contraseñas, bloqueo de notificaciones. | X | Media |
| Software de antivirus (AV) | Correctivo. Detecta amenazas conocidas y las aísla. | X | Alta |
| Monitoreo manual, mantenimiento e intervención | Preventivo/correctivo. Necesario para los sistemas heredados para identificar y mitigar amenazas. | X | Alta |

**Controles físicos**

| **Nombre de control** | **Tipo de control y explicación** | **Se tiene que implementar (X)** | **Prioridad** |
| --- | --- | --- | --- |
| Caja fuerte con control de tiempo | Disuasivo. Reduce la superficie expuesta a ataque y el impacto de las amenazas físicas. | X | Baja |
| Iluminación adecuada | Disuasivo. Limita los lugares “ocultos” para disuadir las amenazas. | X | Baja |
| Vigilancia del circuito cerrado de televisión (CCTV) | Preventivo/De detección. Reduce el riesgo y permite investigar después de un incidente. | X | Media |
| Cerradura de gabinetes (para equipos de red) | Preventivo. Aumenta la integridad al evitar que personas no autorizadas accedan físicamente. | X | Media |
| Carteles que indican el nombre de la empresa proveedora del servicio de alarmas | Disuasivo. Reduce la probabilidad de éxito de ciertos tipos de amenazas. | X | Baja |
| Cerraduras | Preventivo. Logra que los activos físicos y digitales estén más seguros. | X | Media |
| Detección y prevención de incendios | De detección/Preventivo. Detecta incendios en la ubicación física para evitar daños. | X | Alta |

#### 4. Lista de control de cumplimiento normativo

| **Cumplimiento normativo** | **¿Aplica? (X)** | **Explicación** |
| --- | --- | --- |
| **FERC-NERC** |  | No aplica. Esta normativa se aplica a organizaciones que trabajan con electricidad o la red eléctrica de EE. UU. y América del Norte. Botium Toys no se ajusta a este perfil. |
| **Reglamento General de Protección de Datos (RGPD)** | X | Aplica. El RGPD protege los datos de los residentes de la Unión Europea (UE). Dado que Botium Toys realiza negocios en la UE, está obligada a cumplir con esta normativa. Si se produce una filtración de datos, debe ser informada en un plazo de 72 horas. |
| **Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)** | X | Aplica. El PCI DSS es un estándar de seguridad internacional para organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito. Como Botium Toys acepta pagos en línea, debe cumplir con este estándar para proteger la información financiera de sus clientes. |
| **Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)** |  | No aplica. La HIPAA es una ley federal de EE. UU. establecida para proteger la información médica de las personas. Botium Toys es una empresa de juguetes y no maneja información de salud de sus clientes. |
| **Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)** | X | Aplica. Los SOC 1 y 2 se enfocan en las políticas de acceso de los usuarios y evalúan el cumplimiento financiero, así como los niveles de riesgo. Son importantes para Botium Toys porque la empresa debe garantizar la confidencialidad, privacidad, integridad, disponibilidad, seguridad y protección general de los datos que maneja en sus sistemas. |

#### 5. Conclusiones y sugerencias

**Conclusiones**

La auditoría revela que la postura de seguridad de Botium Toys es débil y presenta un **alto nivel de riesgo**.

La empresa tiene una gestión de activos insuficiente y una falta crítica de controles de seguridad adecuados y cumplimiento normativo.

Los riesgos clave incluyen la pérdida de activos y multas por incumplimiento de normativas como el **RGPD** y el **PCI DSS**, lo que podría afectar gravemente la operación y reputación del negocio.

**Sugerencias y recomendaciones** Para mitigar los riesgos identificados y fortalecer la postura de seguridad, se recomienda lo siguiente:

* **Prioridad alta:**
  + **Implementar políticas de acceso:** Establecer políticas de contraseñas sólidas y el **principio de mínimo privilegio** para limitar el acceso a los activos a lo estrictamente necesario.
  + **Reforzar controles técnicos:** Instalar un **Sistema de Detección de Intrusiones (IDS)**, realizar copias de seguridad de forma regular y utilizar **cifrado** para proteger la información confidencial, especialmente en transacciones de pago.
  + **Plan de respuesta a incidentes:** Desarrollar un **plan de recuperación ante incidentes** para asegurar la continuidad del negocio y mitigar el impacto de cualquier evento adverso.
* **Prioridad media:**
  + **Mejorar la seguridad física:** Asegurar los gabinetes de red con **cerraduras** e instalar un sistema de **vigilancia por CCTV**.
* **Prioridad baja:**
  + **Implementar medidas físicas disuasorias:** Colocar carteles de alarmas y garantizar una iluminación adecuada para disuadir posibles amenazas físicas.

Finalmente, se aconseja que el gerente de TI utilice los hallazgos de esta auditoría como justificación para **contratar personal adicional de ciberseguridad**, ya que el crecimiento del negocio en línea exige un equipo más robusto para gestionar la seguridad de manera efectiva.