**MEMORÁNDUM**

**A:** Gerente/a de TI, partes interesadas

**DE:** ODYMAR AUGUSTO PARDO ECHEVERRIA

**FECHA:** 16 DE AGOSTO DE 2025

**ASUNTO:** Hallazgos y recomendaciones de la auditoría interna de TI

Estimados/as compañeros/as:

La siguiente información incluye el ámbito, los objetivos, los hallazgos críticos, un resumen y las recomendaciones de la auditoría interna de Botium Toys.

**Alcance:**

La auditoría interna de TI de Botium Toys analizó la totalidad del programa de seguridad de la empresa. El alcance incluyó la evaluación de todos los activos, procesos y procedimientos internos, así como la revisión de los permisos de usuario, los controles y los protocolos en sistemas clave como la contabilidad, detección de puntos de conexión, *firewalls*, sistema de detección de intrusiones y SIEM. También se verificó que estos elementos estuvieran alineados con los requisitos de cumplimiento normativo y que la tecnología estuviera debidamente registrada.

**Objetivos:**

Los objetivos principales de la auditoría fueron:

* 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.
* Establecer políticas y procedimientos claros.
* Asegurar el acatamiento de los requisitos de cumplimiento normativo.

**Hallazgos críticos (que deben abordarse de inmediato):**

* **Alto riesgo general:** La postura de seguridad de la organización es débil, con una puntuación de riesgo de **8 sobre 10** debido a la falta de controles de seguridad adecuados y a un cumplimiento normativo inexistente.
* **Incumplimiento normativo:** Botium Toys no cumple con los estándares esenciales de la industria. En particular, no se están siguiendo las regulaciones del **PCI DSS** para proteger los datos de las tarjetas de pago de los clientes, ni el **Reglamento General de Protección de Datos (RGPD)**, a pesar de realizar negocios en la Unión Europea. El incumplimiento de estas normativas expone a la empresa a graves multas y a la pérdida de confianza del cliente.
* **Falta de controles técnicos clave:** No se han implementado controles técnicos vitales como el **cifrado** de datos y un **Sistema de Detección de Intrusiones (IDS)**. Esta deficiencia deja a la empresa vulnerable a filtraciones de datos, ataques de intrusión y robo de información.
* **Ausencia de un plan de recuperación:** La falta de un **plan de recuperación ante incidentes** pone en riesgo la continuidad del negocio y la productividad en caso de una interrupción o un desastre.

**Hallazgos (que deben abordarse, aunque no de inmediato):**

* **Sistemas heredados sin monitoreo:** Los sistemas heredados de la empresa carecen de monitoreo automatizado y requieren una supervisión manual constante, lo que aumenta la probabilidad de fallas y vulnerabilidades.
* **Controles de acceso y políticas incompletos:** Las políticas de control de acceso y contraseñas no están bien definidas ni documentadas, lo que podría conducir a un acceso indebido a la información.
* **Debilidades en la seguridad física:** La seguridad física en la oficina no es suficiente. Hay una falta de **vigilancia por CCTV**, **cerraduras** en gabinetes de equipos de red y otros controles físicos importantes que podrían evitar el acceso no autorizado a los activos.

**Resumen/recomendaciones:**

La auditoría ha revelado que la falta de un plan de seguridad cohesivo y de controles robustos ha llevado a un alto nivel de riesgo en Botium Toys. Para mitigar estos riesgos y mejorar nuestra postura de seguridad, se recomienda una acción inmediata y priorizada.

**Recomendaciones:**

1. **Prioridad alta:** Desarrollar e implementar políticas de **cumplimiento normativo** para **PCI DSS** y **RGPD**.
2. **Prioridad alta:** Invertir en **controles técnicos** esenciales, como un **IDS**, soluciones de **cifrado** y **copias de seguridad** automatizadas.
3. **Prioridad alta:** Desarrollar un **plan de respuesta y recuperación ante incidentes** para proteger la continuidad del negocio.
4. **Prioridad alta:** Formalizar políticas de **control de acceso** y de **contraseñas**, e implementar el **principio de mínimo privilegio**.
5. **Recomendación estratégica:** Utilizar estos hallazgos para justificar la contratación de **personal adicional de ciberseguridad**, lo cual es crucial para gestionar la creciente carga de trabajo y asegurar la empresa contra futuras amenazas.