A: Gerente/a de TI, partes interesadas
DE: Ginely De Vita
FECHA: Jueves, 13/11/2025
ASUNTO: Hallazgos y recomendaciones de la auditoría interna de TI

Estimados/as colegas,

Por favor, revisen la siguiente información con relación al alcance, objetivos, hallazgos críticos, resumen y recomendaciones de la auditoría interna de Botium Toys.

Alcance de la auditoría:

El alcance de la auditoría evaluó todos los sistemas críticos: contabilidad, detección de terminal, cortafuegos, IDS y SIEM fueron tomados en consideración para asegurar que estén alineados con los requisitos de cumplimientos de PCI DSS y GDPR. y que también se tome en consideración para el mejor manejo de estos mismos:

- Permisos de usuario
- Controles existentes
- Procedimientos y protocolos
- Incluye una revisión del inventario de activos tecnológicos, tanto hardware como software, y del acceso de proveedores.
- Y se analizó la gestión de datos, la red interna, los sistemas legacy y el almacenamiento de información.

Objetivos de la auditoría:

- Alinear la postura de seguridad de Botium Toys con CSF del NIST
- Identificar los riesgos y brechas en controles, políticas y procedimientos, incluyendo sus manuales de estrategias
- Establecer el principio de privilegios mínimos
- Determinar las obligaciones regulatorias que aplican a la empresa
- Proporcionar recomendaciones que fortalezcan la seguridad, mejoren la continuidad del negocio y aseguren el cumplimiento

Hallazgos críticos (que deben abordarse de inmediato):

Es necesario implementar los siguientes controles para cumplir con los objetivos de la auditoría

- Falta un plan de recuperación de desastres
- Existen permisos inadecuados de los usuarios, se debe aplicar el privilegio mínimo
- Se necesitan implementar mejores políticas de contraseña, control de acceso y gestión de cuentas.
- No existe una gestión eficiente de los activos tecnológicos
- IDS y SIEM no están optimizadas
- Cifrado de datos para transacciones de web seguras
- Copias de seguridad que apoyen la continuidad de negocio
- Software Antivirus
- Monitoreo y mantenimiento adecuados de los sistemas Legacy y/o su estrategia de reemplazo
- La empresa no cumple con los requisitos de PCI DSS y GDPR y aumenta la probabilidad de brechas y multas
- Es de urgencia implementar el desarrollo de políticas que se ajusten a las directrices de SOC1 y SOC2
- CCTV
- Cerraduras

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

- Caja fuerte con control de tiempo
- Iluminación adecuada
- Armarios con cerradura
- Señalización que indica el proveedor del servicio de alarmas
- Deteccion y prevencion de incendios
- Capacitación de personal en prácticas de seguridad.

Resumen/Recomendaciones:

Botium Toys presenta riesgos de alto riesgo debido a una débil gestión de activos, permisos excesivos y controles de seguridad incompletos. Es esencial comenzar fortaleciendo el inventario de activos, corrigiendo accesos de usuario e implementando controles básicos en cortafuegos, IDS y SIEM. Asimismo, se debe priorizar el cumplimiento de PCI DSS y las obligaciones de GDPR para evitar sanciones regulatorias. Se les recomienda urgentemente desarrollar planes formales de respuesta a incidentes y continuidad del negocio, e implementar un mejor control de monitoreo de sus sistemas legacy o una sustitución de los mismos. También se aconseja optimizar el SIEM para una mejor detección y capacitar al personal en prácticas esenciales de seguridad. Estas acciones combinadas permitirán a la empresa reducir riesgos, mejorar su postura de seguridad y sostener su crecimiento internacional con mayor resiliencia.