**Botium Toys: Alcance y objetivos de la auditoría**

**Resumen:** Realizar una auditoría del programa de ciberseguridad de Botium Toys. La auditoría debe alinear las prácticas comerciales actuales con los estándares y las mejores prácticas de la industria. La auditoría tiene como objetivo proporcionar recomendaciones de mitigación para las vulnerabilidades encontradas que se clasifican como de "alto riesgo" y presentar una estrategia general para mejorar la postura de seguridad de la organización. El equipo de auditoría debe documentar sus hallazgos, proporcionar planes y esfuerzos de remediación y comunicarse con las partes interesadas.

**Alcance:** (*Para comprender el alcance de la auditoría, revise la lectura de la auditoría de seguridad. Tenga en cuenta que el alcance no es constante de una auditoría a otra. Sin embargo, una vez que el alcance de la auditoría está claramente definido, solo se deben auditar los elementos dentro del alcance. En este escenario, el alcance se define como todo el programa de seguridad de Botium Toys. Esto significa que todos los activos deben evaluarse junto con los procesos y procedimientos internos*).

La auditoría interna de TI de Botium Toys evaluará lo siguiente:

1. Permisos de usuario actuales establecidos en los siguientes sistemas: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusos, herramienta de gestión de eventos e información de seguridad (SIEM).
2. Controles actualmente implementados en los siguientes sistemas: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusos, herramienta de gestión de eventos e información de seguridad (SIEM).
3. Procedimientos y protocolos actuales establecidos para los siguientes sistemas: contabilidad, detección de puntos finales, firewall, sistema de detección de intrusos, herramienta de gestión de eventos e información de seguridad (SIEM).
4. Asegúrese de que los permisos, controles, procedimientos y protocolos de usuario actuales se alineen con los requisitos de cumplimiento necesarios.
5. Asegúrese de que se tenga en cuenta la tecnología actual. Tanto el hardware como el acceso al sistema.

**Objetivos:** (*El objetivo de una auditoría son los entregables o resultados deseados. El objetivo de una auditoría puede ser lograr el cumplimiento, identificar debilidades o vulnerabilidades dentro de una organización y/o comprender las fallas en los procesos y procedimientos y corregirlas. En este escenario, el gerente de TI establece los objetivos. Espera un informe de la postura de seguridad actual de la organización y recomendaciones para mejorar la postura de seguridad de la organización, así como una justificación para contratar personal adicional de ciberseguridad).*

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

1. Cumplir con el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF)
2. Establecer un mejor proceso para que sus sistemas garanticen que cumplen con la normativa.
3. Fortalezca los controles del sistema
4. Implemente el concepto de permisos mínimos cuando se trata de la administración de credenciales de usuario
5. Establecer sus políticas y procedimientos, lo que incluye sus libros de jugadas
6. Asegúrese de que cumplen con los requisitos de cumplimiento