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 brindar 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, brindar 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 esté 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:

- Permisos de usuario actuales establecidos en los siguientes sistemas: contabilidad, punto final detección, firewalls, sistema de detección de intrusiones, herramienta de gestión de información y eventos de seguridad (SIEM).
- Controles implementados actualmente en los siguientes sistemas: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusos, herramienta de Gestión de Información y Eventos de Seguridad (SIEM).
- Procedimientos y protocolos actuales establecidos para los siguientes sistemas: contabilidad, detección de puntos finales, firewall, sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM). • Asegúrese

de que los permisos, controles, procedimientos y protocolos de usuario actuales estén implementados. alinearse con los requisitos de cumplimiento necesarios.

- 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 resultados o productos deseados. El objetivo de una auditoría puede ser lograr el cumplimiento, identificar debilidades o vulnerabilidades dentro de una organización y/o comprender 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 de ciberseguridad adicional).

Los objetivos de la auditoría interna de TI de Botium

Toys son: • Cumplir con las normas de ciberseguridad del Instituto Nacional de Estándares y Tecnología. Marco (NIST CSF) •

Establecer un mejor proceso para sus sistemas para garantizar que cumplan con las normas • Fortalecer los

controles del sistema • Implementar el concepto de permisos mínimos cuando se trata de credenciales de usuario gestión

• Establecer sus políticas y procedimientos, incluidos sus manuales de estrategias •

Asegurarse de que cumplen con los requisitos de cumplimiento