

Botium Toys: 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 encontradas que sean clasificadas como de “alto riesgo” y presentar una estrategia general para mejorar la postura de seguridad de la organización. El equipo de auditoría se encargará de documentar los hallazgos, crear soluciones y comunicarse con las partes interesadas.

Alcance: (Para comprender cuál es el alcance de la auditoría, revisa la lectura de auditoría de seguridad. Ten en cuenta que el alcance no es el mismo para todas las auditorías. Sin embargo, una vez que está bien definido, solo se deben auditar los elementos que corresponden a dicho alcance. En este escenario, el alcance se define como la totalidad del programa de seguridad en Botium Toys. Esto implica que todos los activos deben ser evaluados, así como los procesos y procedimientos internos).

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

- Permisos de usuario actuales creados en los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewalls), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Controles actuales implementados en los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewalls), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Procedimientos y protocolos actuales establecidos para los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewalls), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Comprueba si los permisos, controles, procedimientos y protocolos actuales de los usuarios/as están alineados con los requisitos de cumplimiento normativo necesarios.

- Verifica si la tecnología actual está debidamente registrada, tanto hardware como acceso al sistema.
-

Objetivos: (*El objetivo de una auditoría es el producto o resultado final deseado. Por ejemplo, lograr el cumplimiento normativo, identificar debilidades o vulnerabilidades dentro de una organización o comprender las fallas en los procesos y procedimientos y luego corregirlos. En este escenario, el/la gerente de TI es quien determinara cuales son los objetivos. Espera un informe sobre la postura actual de seguridad de la organización y recomendaciones para mejorarla, así como una justificación para contratar personal de ciberseguridad.*)

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

- Cumplir con el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (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/as.
- Establecer políticas y procedimientos claros, que incluyan manuales de estrategia.
- Asegurarse de que se acatan los requisitos de cumplimiento normativo.