Auditoría

El objetivo de esta auditoria es analizar si la política en materia de seguridad de la empresa sigue los estándares establecidos por las instituciones internacionales en materia de seguridad. Para ello vamos a identificar las vulnerabilidades, poniendo mucho énfasis en los fallos de alto riesgo y que nos puede causar un gran problema en la empresa.

Alcance de la auditoría.

- Sistemas de contabilidad.
- Detección de puntos de conexión.
- Firewalls.
- Sistemas de detección de intrusiones.
- Herramienta de gestión de eventos e información de seguridad.

Objetivos de la auditoría

- Detectar las vulnerabilidades del sistema.
- Asegurarnos del cumplimiento de lo establecido por CSF y NIST y de la normativa aplicable.
- Revisión de permisos y controles.
- Mitigar los riesgos.
- Establecer unos requisitos mínimos

Gestión de Riesgos.

Activos actuales

- Equipos de los departamentos comerciales y resto de la empresa
- Equipos de todo el personal que trabaja dentro y fuera de la empresa. Desde portátiles, teléfonos inteligentes…
- Sistemas de software y servicios, bases de datos, seguridad
- Acceso a Internet
- Red interne.
- Acceso a proveedores.
- Alojamiento de la base de datos

Descripción del riesgo

En la actualidad Botium Toys carece de la implementación con los estándares internacionales.

Prácticas recomendadas.

Implementas los cinco fundamentos del Marco de Ciberseguridad del NIST.

Determinar el impacto sobre la perdida de activos para continuidad del negocio.

Actualización de equipos y software para la seguridad.

Mejorar la red interna.

Puntuación de riesgo:

La puntuación sobre riesgo es 8 para mejorar necesitamos realizar las prácticas anteriores.

Análisis de controles

Controles administrativos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Principio de mínimo privilegio	Preventivo. Reducir el riesgo asegurándose de que proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar su trabajo.	SÍ	ALTA
Planes de recuperación ante incidentes	Correctivo. Garantizar la continuidad del negocio, asegurando que los sistemas puedan ejecutarse en caso de incidentes, que no haya pérdida de productividad por tiempo de inactividad ni impacto en los componentes del sistema, que incluyen entorno de la sala de computadoras (aire acondicionado, fuentes de alimentación, etc.), hardware (servidores, equipos de empleados), conectividad (red interna, inalámbrica), aplicaciones (correo electrónico, datos electrónicos), así como datos y restauración.	NO	ALTA
Políticas de contraseñas	Preventivo. Establecer requisitos de seguridad de contraseñas para reducir la probabilidad de comprometer la cuenta debido a técnicas de ataque por fuerza bruta o diccionario.	SÍ	ALTA
Políticas de control de acceso	Preventivo. Aumentar la confidencialidad e integridad de los datos.	SÍ	ALTA
Políticas de gestión de cuentas	Preventivo. Reducir la superficie expuesta a ataques y limita el impacto general de ex empleados/as disconformes.	SÍ	ALTA
Separación de funciones	Preventivo. Garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales.	NO	MEDIA

Controles técnicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Cortafuegos (firewall)	Preventivo. Ya hay instalados firewalls para filtrar el tráfico no deseado/malicioso que ingresa a la red interna.	SÍ	NO
Sistema de detección de intrusiones (IDS)	De detección. Permitir al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente.	SÍ	ALTA
Cifrado	Disuasivo. Garantizar que la información y los datos confidenciales sean más seguros (por ejemplo, transacciones de pago en el sitio web).	SÍ	ALTA
Copias de seguridad	Correctivo. Permitir la continuidad del negocio y mantener la productividad en caso de incidentes, al mantener los sistemas funcionando.	NO	ALTA
Gestión de contraseñas	Correctivo. Recuperar y restablecer contraseñas, bloqueo de notificaciones.	SÍ	ALTA
Software de antivirus (AV)	Correctivo. Detectar amenazas conocidas y aislarlas.	SÍ	ALTA
Monitoreo manual, mantenimiento e intervención	Preventivo/correctivo. Necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades.	NO	MEDIA

Controles físicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Caja fuerte con control de tiempo	Disuasivo. Reducir la superficie expuesta a ataque y el impacto de las amenazas físicas.	NO	MEDIA
Iluminación adecuada	Disuasivo. Limitar los lugares “ocultos” para disuadir las amenazas.	NO	BAJA
Vigilancia del circuito cerrado de televisión (CCTV)	Preventivo/De detección. Reducir el riesgo de ciertos eventos y ver qué sucedió, después del incidente al llevar a cabo una investigación.	NO	BAJA
Cerradura de gabinetes (para equipos de red)	Preventivo. Aumentar la integridad al evitar que personas no autorizadas accedan físicamente o modifiquen el equipo de infraestructura de la red.	SÍ	MEDIA
Carteles que indican el nombre de la empresa proveedora del servicio de alarmas	Disuasivo. Reducir la probabilidad de éxito de ciertos tipos de amenazas al dar la apariencia de que un ataque exitoso es poco probable.	SÍ	BAJA
Cerraduras	Preventivo. Lograr que los activos físicos y digitales estén más seguros.	SÍ	MEDIA
Detección y prevención de incendios (alarma de incendios, sistema de rociadores, entre otros)	De detección/Preventivo. Detectar incendios en la ubicación física de la juguetería para evitar daños en el inventario, servidores, entre otros.	SÍ	ALTA

Cumplimiento normativo.

El Real Decreto-ley 12/2018, que transpone la Directiva (UE) 2016/1148, establece medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Este informe evalúa si Botium Toys cumple con los requisitos establecidos por dicho real decreto en el marco de la auditoría de su programa de ciberseguridad.

Seguridad de las redes y sistemas de información:

Medidas técnicas y organizativas adecuadas y proporcionadas: Botium Toys debe adoptar medidas adecuadas para gestionar los riesgos que afectan a la seguridad de las redes y sistemas de información utilizados en la prestación de servicios esenciales.
Cumplimiento: Parcial. Se han identificado varias áreas que requieren mejoras, especialmente en la implementación de copias de seguridad, separación de funciones, y la actualización de equipos y software.
Notificación de incidentes:

Notificación de incidentes que tengan efectos perturbadores significativos: Botium Toys debe notificar a la autoridad competente los incidentes significativos que afecten a la seguridad de sus servicios.
Cumplimiento: Parcial. Se necesita un sistema de notificación más robusto y procesos claros para la gestión y comunicación de incidentes.

Supervisión y auditoría :

Supervisión del cumplimiento y auditorías periódicas: La empresa debe someterse a auditorías y permitir la supervisión de sus medidas de seguridad.
Cumplimiento: Parcial. La auditoría actual proporciona una buena base, pero es necesario un programa continuo de auditoría y supervisión.
Gestión de riesgos (Artículo 16.1):

Evaluación y gestión de riesgos: Implementación de un enfoque basado en riesgos para gestionar la seguridad de la información.
Cumplimiento: Parcial. La gestión de riesgos está en proceso, pero requiere una evaluación y documentación más completa.

Protección del notificante y confidencialidad:
Protección de los empleados que informan sobre incidentes y confidencialidad de la información: Debe garantizarse la confidencialidad y protección de los informantes.
Cumplimiento: Sí. Botium Toys cuenta con políticas que aseguran la confidencialidad de la información y protegen a los empleados que informan sobre incidentes.

Requisitos específicos para operadores de servicios esenciales y proveedores de servicios digitales:

Designación de responsables de seguridad: Botium Toys debe designar responsables para la seguridad de la información y establecer un punto de contacto.
Cumplimiento: Parcial. Se recomienda formalizar la designación de un responsable de seguridad y establecer puntos de contacto claros.

Cooperación y coordinación:
Colaboración con otras autoridades y CSIRT (Computer Security Incident Response Team):
Coordinación efectiva con las autoridades y equipos de respuesta a incidentes.
Cumplimiento: Parcial. Es necesario mejorar la coordinación con autoridades y CSIRT, y formalizar procedimientos de colaboración.
Recomendaciones

Para cumplir completamente con el Real Decreto-ley 12/2018, Botium Toys debe:
Implementar un sistema de notificación de incidentes robusto y procesos claros para la gestión de incidentes.
Formalizar la designación de responsables de seguridad y establecer puntos de contacto claros.
Mejorar la gestión de riesgos mediante evaluaciones más completas y documentación adecuada.
Asegurar la implementación de todas las medidas técnicas y organizativas adecuadas, incluyendo copias de seguridad, separación de funciones, y actualización de equipos y software.
Establecer un programa continuo de auditoría y supervisión.
Mejorar la coordinación con las autoridades y CSIRT, y formalizar procedimientos de colaboración.