Actividad: Realiza una auditoría de seguridad

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Este escenario se basa en una empresa ficticia:

Botium Toys es una pequeña empresa estadounidense que desarrolla y vende juguetes. La empresa tiene una sola sede física. Sin embargo, su presencia en línea ha crecido, atrayendo a clientes de Estados Unidos y del extranjero. Su departamento de tecnología de la información (TI) está sometido a una presión cada vez mayor para dar soporte a su mercado en línea en todo el mundo.

La gerente del departamento de TI ha decidido que es necesario realizar una auditoría interna de TI. Expresa su preocupación por no tener un plan de acción consolidado para garantizar la continuidad del negocio y el cumplimiento de la normativa, a medida que la empresa crece. Cree que una auditoría interna puede ayudar a asegurar mejor la infraestructura de la empresa y ayudar a identificar y mitigar los posibles riesgos, amenazas o vulnerabilidades de los activos críticos. La gerente también está interesada en asegurarse de que cumplen con la normativa relacionada con la aceptación de pagos en línea y la realización de negocios en la Unión Europea (UE).

La gerente de TI comienza aplicando el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), estableciendo un alcance y unos objetivos de auditoría y completando una evaluación de riesgos. El objetivo de la auditoría es proporcionar una visión general de los riesgos que la empresa podría experimentar debido al estado actual de su postura de seguridad. La gerente de TI quiere utilizar los resultados de la auditoría como prueba para obtener la aprobación para ampliar su departamento.

Tu tarea consiste en revisar el alcance, los objetivos y la evaluación de riesgos de la gerente de TI. Luego, realiza una auditoría interna para completar una evaluación de los controles y una lista de verificación de cumplimiento.

1. **Analiza el alcance, los objetivos y la evaluación de riesgos de la auditoría**.

Recibes el siguiente correo electrónico de tu gerente de TI:

¡Hola!

Completé el alcance y los objetivos de la auditoría, así como una evaluación de riesgos. A grandes rasgos, los principales objetivos y riesgos son los siguientes:

Objetivos:

- Mejorar la postura de seguridad actual de Botium Toys alineándola con las mejores prácticas de la industria (por ejemplo, adhiriéndose al CSF del NIST, implementando el concepto de permisos mínimos).
- Proporcionar recomendaciones de mitigación (es decir, controles, políticas, documentación), basadas en los riesgos actuales.
- Identificar las normativas de cumplimiento a las que Botium Toys debe adherirse, principalmente en función de *dónde* realizamos negocios y *cómo* aceptamos pagos.
- Para revisar el informe completo, lee el documento **Botium Toys: Alcance y objetivos de la auditoría**.

Riesgos:

- Gestión inadecuada de los activos.
- Inexistencia de controles adecuados.
- Es posible que no se cumplan las normativas y directrices estadounidenses e internacionales.
- La puntuación de riesgo actual es de 8/10 (alta), debido a la falta de controles y la adhesión a las normativas y estándares de cumplimiento normativo.

Gracias, Gerente de TI de Botium Toys

Tras revisar el alcance, los objetivos y la evaluación de riesgos de la auditoría, ten en cuenta las siguientes preguntas:

- ¿Cuáles son los mayores riesgos para la organización?
- ¿Qué controles son más esenciales implementar de inmediato que en el futuro?
- ¿Qué normativas de cumplimiento debe cumplir Botium Toys para garantizar la seguridad de los datos de clientes y proveedores, evitar multas, etc.?

2. Evaluación de los controles

Realiza el siguiente paso de la auditoría de seguridad completando la evaluación de los controles.

Para completar la evaluación de los controles, abre los materiales de apoyo. A continuación:

1. **Revisa** la lista de los activos de Botium Toys.
2. **Revisa** el nombre de cada control.
3. **Revisa** los tipos de controles y su explicación.
4. **Marca con una X** cada control que deba aplicarse.
5. **Anota los niveles de prioridad** (alta, media y/o baja; NA si no corresponde).

3. Lista de verificación de cumplimiento normativo

Para completar la lista de verificación de cumplimiento normativo, abre los materiales de apoyo. A continuación:

1. **Ten en cuenta dónde** desarrolla su actividad la empresa y **cómo** recibe los pagos de los clientes.
2. **Haz clic en las casillas** para seleccionar las normativas y estándares de cumplimiento que Botium Toys debe cumplir.*
3. **Explica** por qué la empresa debe cumplir con las normativas y estándares de cumplimiento seleccionados.

4. ¿Qué debes incluir en tu respuesta?

Asegúrate de incluir los siguientes elementos en la actividad terminada:

a) Evaluación de los controles
   - Todos los **activos** enumerados se tienen en cuenta en los controles seleccionados.
   - Se seleccionan los **controles administrativos, técnicos** y **físicos** apropiados (marcados con una X).
   - Se indica el **nivel de prioridad** para cada control seleccionado, en función de la necesidad de implementación inmediata o futura.

b) Lista de verificación de cumplimiento normativo
   - Se seleccionan **las normativas y estándares de cumplimiento** a los que Botium Toys debe adherirse (por ejemplo, relacionados con el desarrollo de actividades en la UE, la aceptación de pagos en línea, las políticas de permiso de los usuarios).
   - Se **explica** la necesidad de cada normativa y estándar seleccionado.

c) Asegúrate de incluir los siguientes elementos en la actividad terminada:
   - Se proporciona un resumen de alto nivel del **alcance de la auditoría** (4-6 frases o viñetas).
   - Se proporciona un resumen de alto nivel de los **objetivos de la auditoría** (4-6 frases o viñetas).
   - Se enumeran y explican las **conclusiones críticas**.
   - Se enumeran y explican otras **conclusiones**.
   - **El resumen/las recomendaciones** sintetizan de manera clara y concisa la información más importante del alcance, los objetivos, las conclusiones críticas y de otro tipo de la auditoría (5-10 frases).