

Examen Final

Guía para solución y presentación

Caso: Cyber Breach at Target

Entregables:

- Documento con solución detallada: Plan comprensivo de recuperación y continuidad.
- Presentación ejecutiva: Resumen conciso y estratégico de 10 minutos dirigido a la junta directiva.

Planteamiento

Ustedes han sido contratados por la junta directiva de Target para asesorarlos en la gestión de riesgos ante un evento de ciberseguridad similar al ocurrido previamente. Su objetivo es proporcionar recomendaciones prácticas para reducir el impacto, acelerar la recuperación y fortalecer la respuesta organizacional. La junta directiva está consciente de que, a pesar de sus esfuerzos, este tipo de incidentes pueden ocurrir, por lo que buscan estrategias para una respuesta organizada y efectiva.

La junta directiva tiene inquietudes sobre los siguientes temas:

- Mitigación de riesgos: Cómo reducir la probabilidad de un ataque y minimizar el impacto en caso de que ocurra.
- Estructura organizativa para la respuesta: Identificar si deben contratar personal adicional, con qué perfiles, y definir las responsabilidades clave.
- Responsabilidad y comunicación interna: Determinar quién debería asumir responsabilidades en distintos niveles organizacionales.

Actualmente, están trabajando en la identificación de riesgos, vulnerabilidades e impacto con un CISO y un equipo interdisciplinario. No necesitan asesoría técnica en seguridad informática, sino un enfoque en la gestión del riesgo y la respuesta organizada ante incidentes.

Guía de solución

Para estructurar su solución, consideren responder a las siguientes preguntas (sin necesidad de hacerlo de forma directa en el documento final):

- ¿Qué acciones clave deben tomarse en las primeras horas tras la detección de un incidente?
- ¿Qué procedimientos de recuperación implementarían para reanudar operaciones críticas con la menor interrupción posible?
- ¿Qué perfiles serían esenciales en el equipo de respuesta ante incidentes?
- ¿Qué enfoque de comunicación propondrían para diferentes audiencias (clientes, empleados, inversionistas) en caso de un ataque?
- ¿Cómo asegurar la transparencia y mantener la confianza sin comprometer la seguridad de la información?
- ¿Cómo recomendaría realizar evaluaciones periódicas para mejorar la preparación ante incidentes futuros?
- ¿cómo deberían incorporar las lecciones aprendidas en los planes de continuidad del negocio?

Cronograma:

- Fecha de entrega de documento: 10 de noviembre
 - Punteo: 30
- Fecha de presentación: 11 de noviembre
 - Punteo: 70