¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Para Aprobar** 75 % o más

Ir al siguiente elemento

1. Un analista de seguridad nota que un empleado instaló una aplicación en su equipo de trabajo sin obtener permiso del servicio de soporte. El registro indica que posiblemente se haya ejecutado código malicioso en el host. ¿Cuál de estos eventos de seguridad debe escalar el analista de seguridad a un supervisor? **1 / 1 punto**

- ○ Debe escalarse al empleado que instaló la aplicación sin permiso.
- ○ Debe escalarse el registro que indica que el código malicioso podría haberse ejecutado en el host.
- ○ Ninguno de los eventos debe escalarse.
- ◉ Ambos eventos deben escalarse.

Correcto
Ambos eventos deben escalarse a un supervisor. Ningún problema es demasiado pequeño o demasiado grande. Siempre es mejor pecar de ser precavidos e informar de lo sucedido a las personas adecuadas del equipo.

2. ¿Cuáles son los tipos de datos y activos que a las partes interesadas les importa especialmente proteger? Selecciona dos respuestas. **1 / 1 punto**

- ☑ Datos financieros sensibles

Correcto
Los datos financieros sensibles y los nombres de usuario y contraseñas de los clientes son ejemplos de datos y activos que a las partes interesadas les importa proteger.

- ☐ Políticas de la empresa
- ☑ Nombres de usuario y contraseñas de los clientes

Correcto
Los datos financieros sensibles y los nombres de usuario y contraseñas de los clientes son ejemplos de datos y activos que a las partes interesadas les importa proteger.

- ☐ Presencia en redes sociales

3. Completa el espacio en blanco: Cuando un evento de seguridad resulta en una filtración de datos, se clasifica como _____. **1 / 1 punto**

- ○ una amenaza
- ◉ un incidente de seguridad
- ○ una vulnerabilidad
- ○ un activo

Correcto
Cuando un evento de seguridad resulta en una filtración de datos, se clasifica como un incidente de seguridad. Sin embargo, si el evento se resuelve *sin* dar lugar a una filtración, no se considera un incidente.

4. ¿Cuáles de los siguientes son ejemplos del potencial impacto de un incidente de seguridad relacionado con código malicioso? **1 / 1 punto**

- ☑ Consecuencias financieras

Correcto
El tiempo de inactividad operacional, las consecuencias financieras y la pérdida de activos son ejemplos del potencial impacto de un incidente de seguridad relacionado con código malicioso.

- ☑ Tiempo de inactividad operacional

Correcto
El tiempo de inactividad operacional, las consecuencias financieras y la pérdida de activos son ejemplos del potencial impacto de un incidente de seguridad relacionado con código malicioso.

- ☑ Pérdida de activos

Correcto

El tiempo de inactividad operacional, las consecuencias financieras y la pérdida de activos son ejemplos del potencial impacto de un incidente de seguridad relacionado con código malicioso.

☐ Protección de datos