¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Calificación del último envío** 100 % **Para Aprobar** 80 % o más

Ir al siguiente elemento

1. ¿Qué utiliza un/a profesional de seguridad informática para crear pautas y planes que instruyan al personal sobre cómo puede ayudar a proteger la organización? **1 / 1 punto**

- ○ Auditoría de seguridad
- ○ Fortalecimiento de la seguridad
- ○ Postura de seguridad
- ◉ Marco de seguridad

Correcto

2. Completa el espacio en blanco: Un/a profesional de seguridad informática utiliza _____ para verificar que un/a empleado/a tiene permiso para acceder a un recurso específico del sistema. **1 / 1 punto**

- ○ la admisión
- ○ el cifrado
- ◉ la autorización
- ○ la integridad

Correcto

3. ¿Qué tipo de ataque de ingeniería social intenta aprovechar los datos biométricos? **1 / 1 punto**

- ○ Ataque de “caza de ballenas” (whaling)
- ◉ Vishing
- ○ Ataque criptográfico
- ○ Spear phishing

Correcto

4. Imagina que trabajas como analista de seguridad informática para una organización de una cadena de suministro y necesitas confirmar que todos los datos de inventario son correctos, auténticos y confiables. ¿Qué principio básico de la tríada CID usarías? **1 / 1 punto**

- ○ Credibilidad
- ◉ Integridad
- ○ Disponibilidad
- ○ Confidencialidad

Correcto

5. ¿Cuáles de las siguientes afirmaciones describe con precisión el CSF del NIST? Selecciona todas las opciones que correspondan. **1 / 1 punto**

- ☑ El CSF del NIST es un marco de adhesión voluntaria que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de ciberseguridad.

Correcto

- ☑ Investigar un incidente para determinar cómo ocurrió, qué afectó y dónde se originó el ataque es parte de la función de responder del CSF del NIST.

Correcto

- ☐ La función de detectar del CSF del NIST implica asegurarse de que se utilicen los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad.

- [x] La función de proteger el CSF implica implementar políticas, procedimientos, capacitaciones y herramientas para mitigar las amenazas.

Correcto

6. Un equipo de seguridad está analizando cómo evitar soluciones innecesariamente complejas al implementar controles de seguridad. ¿Qué principio de OWASP describe este escenario? **1 / 1 punto**

- (•) Simplificar la seguridad
- ( ) Principio del mínimo privilegio
- ( ) Defensa en profundidad
- ( ) Solucionar los problemas de seguridad correctamente

Correcto

7. ¿Cuáles son algunos de los objetivos principales de una auditoría de seguridad interna? Selecciona todas las opciones que correspondan. **1 / 1 punto**

- [x] Ayudar a los equipos de seguridad a corregir problemas de cumplimiento normativo.

Correcto

- [ ] Limitar el tráfico en el cortafuegos (firewall) de una organización.
- [x] Permitir que los equipos de seguridad evalúen los controles.

Correcto

- [x] Identificar las fallas de seguridad o debilidades dentro de una organización.

Correcto

8. Completa el espacio en blanco: En una auditoría de seguridad interna, _____ implica identificar posibles amenazas, riesgos y vulnerabilidades para decidir qué medidas de seguridad deben implementarse. **1 / 1 punto**

- (•) realizar una evaluación de riesgos
- ( ) determinar el alcance y los objetivos
- ( ) comunicar a las partes interesadas
- ( ) evaluar el cumplimiento

Correcto

9. Un/a analista de seguridad informática lleva a cabo una auditoría de seguridad interna. Se centra en el componente humano de la ciberseguridad, como las políticas y los procedimientos que definen de qué manera la empresa gestiona los datos. ¿Qué es lo que quiere implementar? **1 / 1 punto**

- ( ) Controles de cumplimiento
- ( ) Controles físicos
- ( ) Controles técnicos
- (•) Controles administrativos

Correcto

10. ¿Qué información se suele comunicar a las partes interesadas después de realizar una auditoría de seguridad interna? Selecciona tres respuestas. **1 / 1 punto**

- [x] Los riesgos que deben abordarse de inmediato o a futuro

Correcto

- [x] Las estrategias para mejorar la postura de seguridad

Correcto

- [x] Un resumen de los objetivos

Correcto

- [ ] Una descripción detallada sobre incidentes de ciberseguridad pasados