¡Felicitaciones! ¡Aprobaste!

Calificación recibida 86 % **Calificación del último envío** 86 % **Para Aprobar** 80 % o más

Volver a realizar la tarea en **7 h 29 m**

Ir al siguiente elemento

1. Considera el siguiente escenario: **0 / 1 punto**

Un proveedor de servicios en la nube configuró mal una unidad en la nube. Se olvidó de cambiar los permisos de uso compartido predeterminados. Esto permite a todos sus clientes acceder a los datos que se almacenan en la unidad.

Esta unidad en la nube mal configurada es un ejemplo de:

- [ ] Una amenaza
- [ ] Un exploit
- [ ] Un control de seguridad
- [x] Una vulnerabilidad

Correcto

No seleccionaste todas las respuestas correctas

2. Completa el espacio en blanco: Las cinco capas de la estrategia de defensa en profundidad son: perimetral, de red, de punto de conexión, de aplicación y _____. **1 / 1 punto**

- ( ) de transporte
- ( ) física
- ( ) de sesiones
- (•) de datos

Correcto

3. ¿Cuál es la diferencia entre las capas de aplicación y de datos, de la estrategia de defensa en profundidad? **1 / 1 punto**

- ( ) La capa de datos autentica a los usuarios para permitir solo el acceso a partes confiables. La capa de aplicación asegura la información con controles que están programados en la propia aplicación.
- ( ) La capa de datos incluye controles como el cifrado y el hashing para proteger los datos en reposo. La capa de aplicación autoriza a los usuarios que tienen acceso para realizar una tarea.
- ( ) La capa de aplicación autoriza a los usuarios que tienen acceso para realizar una tarea. La capa de datos mantiene la integridad de la información con controles como el cifrado y el hashing.
- (•) La capa de aplicación asegura la información con controles que están programados en la propia aplicación. La capa de datos mantiene la integridad de la información con controles como el cifrado y el hashing.

Correcto

4. ¿Cuáles de los siguientes criterios debe cumplir una vulnerabilidad para calificar para una identificación CVE®? Selecciona todas las opciones que correspondan. **0.6 / 1 punto**

- [x] Debe ser reconocida como un riesgo potencial de seguridad.

Correcto

- [ ] Debe ser independiente de otras cuestiones.
- [ ] Debe representar un riesgo financiero.
- [ ] Solo puede afectar una base de código.
- [x] Se debe presentar con evidencia que la respalde.

Correcto

No seleccionaste todas las respuestas correctas

5. ¿Cuáles de las siguientes son características del proceso de gestión de vulnerabilidades? Selecciona dos respuestas. 1 / 1 punto

- [ ] La gestión de vulnerabilidades es una manera de descubrir activos nuevos.
- [x] La gestión de vulnerabilidades debe considerar varias perspectivas.

Correcto

- [x] La gestión de vulnerabilidades es una manera de limitar los riesgos de seguridad.

Correcto

- [ ] La gestión de vulnerabilidades debe ser un proceso único.

6. ¿Cuáles son algunos de los objetivos de realizar evaluaciones de vulnerabilidad? Selecciona dos respuestas. 1 / 1 punto

- [x] Realizar una auditoría que mida el cumplimiento normativo.

Correcto

- [x] Identificar debilidades y prevenir ataques.

Correcto

- [ ] Transferir las responsabilidades de remediación al departamento de TI.
- [ ] Catalogar los activos que deben protegerse.

7. Completa el espacio en blanco: Todas las vulnerabilidades potenciales que un agente de amenaza podría explotar se llaman _____ de ataque. 1 / 1 punto

- ( ) vector
- ( ) red
- ( ) base de datos
- (•) superficie

Correcto

8. Un gerente de proyectos de una empresa de servicios públicos recibe un correo electrónico sospechoso que contiene un archivo adjunto. Abre el archivo e instala software malicioso en su computadora portátil. 1 / 1 punto

¿Cuáles son los vectores de ataque utilizados en esta situación? Selecciona dos respuestas.

- [x] El archivo adjunto.

Correcto

- [ ] La estación de trabajo infectada.
- [x] El correo electrónico sospechoso.

Correcto

- [ ] El software malicioso.

9. ¿Cuáles de las siguientes son las razones por las que los equipos de seguridad practican una mentalidad de atacante? Selecciona tres respuestas. 1 / 1 punto

- [x] Identificar vectores de ataque.

Correcto

- [x] Descubrir vulnerabilidades que deben monitorearse.

Correcto

- [x] Encontrar información sobre los mejores controles de seguridad para usar.

Correcto

- [ ] Explotar fallas en la base de código de una aplicación.

10. Considera el siguiente escenario: **1 / 1 punto**

Trabajas como profesional de seguridad para un distrito escolar. Un desarrollador de aplicaciones en el distrito escolar creó una aplicación que conecta a los estudiantes con los recursos educativos. Se te asignó evaluar la seguridad de la aplicación.

Pensando como un atacante, ¿cuál de los siguientes pasos tomarías para evaluar la aplicación? Selecciona dos respuestas.

- [ ] Integrar la aplicación con los recursos educativos existentes.
- [x] Identificar los tipos de usuarios que interactuarán con la aplicación.

Correcto

- [ ] Asegurar que el formulario de inicio de sesión de la aplicación funcione.
- [x] Evaluar cómo la aplicación maneja los datos de usuario.

Correcto