¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. Completa el espacio en blanco: Una mentalidad de seguridad es la _____. **1 / 1 punto**

- (●) capacidad de evaluar el riesgo e identificar una vulnerabilidad potencial o real de un sistema, aplicación o datos
- ( ) intención de proporcionar servicios de seguridad de calidad al equipo de operaciones de desarrollo de una organización
- ( ) capacidad para ayudar al departamento de Recursos Humanos (RR.HH.) de una organización a cumplir con la normativa en todo momento
- ( ) oportunidad de mostrar tus habilidades con Linux y otras habilidades técnicas relacionadas con la codificación

Correcto

2. Como analista de seguridad, eres responsable de proteger los activos de bajo y alto nivel de una organización. ¿Cuál de los siguientes se considera un activo de alto nivel? **1 / 1 punto**

- ( ) Red de Wi-Fi para invitados
- (●) Propiedad intelectual
- ( ) Descripciones de los puestos de trabajo de la empresa
- ( ) Comunicados de prensa

Correcto

3. ¿Cuál de los siguientes enunciados describe mejor la relación entre una mentalidad de seguridad y la protección de activos? **1 / 1 punto**

- (●) Una mentalidad de seguridad ayuda a los analistas a proteger activos de todos los niveles.
- ( ) Una mentalidad de seguridad no es importante para la protección de activos.
- ( ) Una mentalidad de seguridad ayuda a los analistas a proteger los activos de mayor importancia.
- ( ) Una mentalidad de seguridad ayuda a los analistas a proteger los activos de bajo nivel.

Correcto

4. Un empleado de una empresa de atención médica accede a la historia clínica y a la información de pago de un paciente para proporcionarle tratamiento. ¿Cómo se clasifica a este tipo de datos? **1 / 1 punto**

- (●) Datos sensibles
- ( ) Datos privados
- ( ) Datos confidenciales
- ( ) Datos públicos

Correcto

5. Completa el espacio en blanco: A _____ les interesa proteger los datos financieros sensibles, los nombres de usuario y contraseñas de los clientes y la seguridad de proveedores externos. **1 / 1 punto**

- (●) las partes interesadas
- ( ) los influencers de las redes sociales
- ( ) los funcionarios de cumplimiento normativo de HIPAA
- ( ) los programadores web

Correcto

6. ¿A quiénes afectarán las decisiones que tomes como analista de seguridad? Selecciona dos respuestas. **1 / 1 punto**

- [x] A la organización que te contrató

Correcto

- [ ] A la competencia en la industria
- [x] A los clientes de la organización que te contrató

Correcto

- [ ] A los mercados financieros

7. Un analista de seguridad nota que un empleado instaló una aplicación en su equipo de trabajo sin obtener permiso del servicio de soporte. También se da cuenta de que el software antivirus registró una ejecución potencialmente maliciosa en la misma computadora. ¿Cuál de estos eventos de seguridad debe escalar a su supervisor? **1 / 1 punto**

- (•) Ambos eventos deben escalarse.
- ( ) Ninguno de los eventos debe escalarse.
- ( ) Debe escalarse el código potencialmente malicioso que detectó el software de antivirus.
- ( ) Debe escalarse al empleado que instaló la aplicación sin permiso.

Correcto

8. ¿Cuál de las siguientes opciones define un incidente de seguridad? **1 / 1 punto**

- (•) Un evento de seguridad que resulta en una filtración de datos
- ( ) Una filtración que altera la seguridad física de una organización
- ( ) Una vulnerabilidad que altera la seguridad en la nube de una organización
- ( ) Un evento de seguridad que no da lugar a una filtración de datos

Correcto

9. Completa el espacio en blanco: Hay que proteger _____ en todo momento. De lo contrario, una organización puede llegar a perder la credibilidad ante sus clientes. **1 / 1 punto**

- ( ) la página de redes sociales de una organización
- (•) los datos sensibles de los clientes
- ( ) la política de cese del empleo de una organización
- ( ) los salarios de los empleados

Correcto

10. ¿Cuáles de los siguientes son los mejores ejemplos de las posibles consecuencias de una filtración de datos? Selecciona dos respuestas. **1 / 1 punto**

- [x] Pérdida de credibilidad

Correcto

- [ ] Reducción significativa en la retención de empleados
- [x] Multas regulatorias

Correcto

- [ ] Mejora de la funcionalidad del hardware