Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación Unidad de Aprendizaje 1

1. ¿Qué se entiende por seguridad informática?

a. El uso exclusivo de antivirus en los sistemas informáticos.
b. El conjunto de medidas destinadas a proteger sistemas, programas y datos frente a accesos no autorizados o daños.
c. La instalación de *software* en un ordenador.
d. El almacenamiento de información en bases de datos.

2. ¿Cuáles son los tres principios fundamentales de la seguridad de la información?

a. Protección, control y monitorización.
b. Seguridad física, seguridad digital y seguridad jurídica.
c. Confidencialidad, integridad y disponibilidad.
d. Acceso, control y supervisión.

3. ¿Qué principio garantiza que la información solo sea accesible por personas autorizadas?

a. Integridad
b. Disponibilidad
c. Confidencialidad
d. Autenticación

4. ¿Qué se entiende por vulnerabilidad en seguridad informática?

a. Una técnica utilizada para atacar un sistema.
b. Una debilidad del sistema que puede ser explotada por una amenaza.
c. Un *software* malicioso.
d. Un sistema de protección.

5. ¿Qué técnica de ataque consiste en manipular a las personas para obtener información o acceso a sistemas?

a. *Malware*
b. Ingeniería social

c. Ataque DDoS
d. *Firewall*

6. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La seguridad informática solo se encarga de proteger los ordenadores y no la información.

- Verdadero
- **Falso**

b. Los errores humanos pueden provocar incidentes de seguridad informática.

- **Verdadero**
- Falso

c. Un ataque de ingeniería social consiste en manipular a las personas para obtener información o acceso a sistemas.

- **Verdadero**
- Falso

d. Las amenazas informáticas siempre son provocadas por atacantes externos.

- Verdadero
- **Falso**

7. Relaciona cada concepto con su definición.

a. Activo
b. Vulnerabilidad
c. Amenaza
d. *Exploit*

b. Debilidad que puede ser explotada por una amenaza
c. Evento que puede causar un daño a un sistema
a. Recurso o información que tiene valor para la organización
d. Técnica utilizada para aprovechar una vulnerabilidad

8. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La seguridad informática forma parte del sistema global de seguridad de una organización.

- **Verdadero**
- Falso

b. El uso de contraseñas seguras y la actualización periódica de los sistemas son medidas básicas para prevenir incidentes de seguridad informática.

- **Verdadero**
- Falso

c. Los ataques informáticos únicamente afectan a grandes empresas y organizaciones con muchos recursos tecnológicos.

- Verdadero
- **Falso**

d. Un sistema informático puede ser utilizado tanto como objetivo de un ataque como para lanzar ataques contra otros sistemas.

- **Verdadero**
- Falso

9. Ordena las siguientes fases que pueden producirse en un incidente de seguridad informática:

3. Explotación de la vulnerabilidad
2. Existencia de una vulnerabilidad en el sistema
1. Aparición de una amenaza
4. Producción de un incidente de seguridad

10. Ordena los siguientes pasos del proceso de gestión de la seguridad informática:

1. Identificación de amenazas y vulnerabilidades
3. Aplicación de medidas de seguridad
2. Evaluación del riesgo
4. Monitorización y revisión de los sistemas

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. ¿Qué se entiende por ingeniería social?

a. Un tipo de *software* de seguridad.
b. Una técnica basada en la manipulación de personas para obtener información o acceso a sistemas.
c. Un sistema de cifrado de datos.
d. Un ataque exclusivamente técnico a servidores.

2. ¿Cuál de las siguientes opciones describe mejor el *phishing?*

a. Un ataque físico a infraestructuras tecnológicas.
b. Un tipo de *malware* que borra archivos.
c. Una técnica que suplanta identidades para obtener información confidencial.
d. Un sistema de protección de redes.

3. ¿Cuál de los siguientes elementos es característico de un correo de *phishing?*

a. Uso de lenguaje formal y personalizado.
b. Solicitud urgente de datos o acciones inmediatas.
c. Envío desde dominios oficiales verificados.
d. Ausencia de enlaces.

4. ¿Qué es una vulnerabilidad en una aplicación web?

a. Un sistema de protección avanzado.
b. Una debilidad que puede ser explotada por un atacante.
c. Un antivirus instalado en el sistema.
d. Un tipo de base de datos.

5. ¿Qué ataque aprovecha la falta de validación de datos en formularios web?

a. *Phishing*
b. Ingeniería social

c. Inyección de código (SQL *Injection*)
d. *Firewall*

6. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La ingeniería social solo afecta a sistemas tecnológicos, no a las personas.

- Verdadero
- **Falso**

b. El *phishing* puede realizarse mediante correos electrónicos, mensajes o llamadas.

- **Verdadero**
- Falso

c. Verificar la identidad del remitente ayuda a prevenir ataques de ingeniería social.

- **Verdadero**
- Falso

d. Las aplicaciones web no pueden tener vulnerabilidades si están en internet.

- Verdadero
- **Falso**

7. Relaciona cada concepto con su definición.

a. *Phising*
b. Ingeniería social
c. Vulnerabilidad web
d. Autenticación multifactor

b. Técnica que manipula a las personas para obtener información.
c. Debilidad en una aplicación que pueda ser explotada.
d. Método de seguridad que requiere más de una forma de verificación.
a. Suplantación de identidad para obtener datos confidenciales.

8. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Los ataques de ingeniería social suelen aprovechar emociones como la urgencia o el miedo.

- **Verdadero**
- Falso

b. Compartir contraseñas es una práctica segura si se hace dentro de la organización.

- Verdadero
- **Falso**

c. El uso de HTTPS mejora la seguridad de una aplicación web.

- **Verdadero**
- Falso

d. Los ataques de *phishing* solo afectan a grandes empresas.

- Verdadero
- **Falso**

9. Ordena las fases de un ataque de *phishing*.

3. El usuario introduce sus credenciales.
1. El atacante envía el mensaje fraudulento.
4. El atacante utiliza la información obtenida.
2. El usuario recibe y abre el mensaje.

10. Ordena las acciones de prevención frente a ingeniería social

2. Verificar la identidad del solicitante.
1. Detectar una solicitud sospechosa.
4. Aplicar protocolos de seguridad.
3. Evitar compartir información confidencial.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. ¿Qué es una política de seguridad?

a. Un *software* de protección informática.
b. Un conjunto de normas y procedimientos para proteger la información.
c. Un tipo de ataque informático.
d. Un sistema de cifrado de datos.

2. ¿Cuál es el objetivo principal de las políticas de seguridad?

a. Aumentar el uso de dispositivos digitales.
b. Proteger los sistemas y la información frente a riesgos.
c. Facilitar el acceso libre a los datos.
d. Sustituir las herramientas tecnológicas.

3. ¿Cuál de los siguientes es un ejemplo de política de seguridad específica?

a. Compromiso de la empresa con la seguridad.
b. Normas sobre el uso de contraseñas.
c. Objetivos generales de la organización.
d. Declaración de principios de seguridad.

4. ¿Qué herramienta permite controlar el tráfico de red?

a. Antivirus
b. *Firewall*
c. Copia de seguridad
d. Contraseña

5. ¿Cuál de las siguientes opciones mejora la seguridad del acceso a sistemas?

a. Compartir contraseñas
b. Uso de autenticación multifactorial
c. No actualizar el sistema
d. Utilizar redes públicas

6. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Las políticas de seguridad solo afectan al departamento de informática.

- Verdadero
- **Falso**

b. Las copias de seguridad permiten recuperar la información en caso de pérdida.

- **Verdadero**
- Falso

c. El cifrado protege la confidencialidad de los datos.

- **Verdadero**
- Falso

d. Las actualizaciones no influyen en la seguridad.

- Verdadero
- **Falso**

7. Relaciona cada concepto con su definición.

a. *Firewall*
b. Cifrado
c. Autenticación multifactorial
d. Copia de seguridad

a. Sistema que controla el acceso a la red
b. Método que protege la información transformándola
c. Verificación mediante varios factores
d. Copia de datos para recuperación

8. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El RGPD regula el tratamiento de datos personales.

- **Verdadero**
- Falso

b. Los datos pueden utilizarse para cualquier finalidad sin restricciones.

- Verdadero
- **Falso**

c. El usuario tiene derecho a acceder a sus datos.

- **Verdadero**
- Falso

d. La confidencialidad es un principio del RGPD.

- **Verdadero**
- Falso

9. Ordena las acciones en la gestión de una brecha de seguridad.

2. Evaluar el riesgo para los afectados
1. Detectar la brecha
3. Notificar a la autoridad competente
4. Aplicar medidas correctoras

10. ¿Cuál de las siguientes opciones representa una correcta aplicación de buenas prácticas de seguridad?

a. Utilizar la misma contraseña en todos los sistemas para facilitar el acceso.
b. Mantener los sistemas actualizados y aplicar medidas de protección adecuadas.
c. Compartir credenciales con compañeros de confianza para agilizar el trabajo.
d. Ignorar las actualizaciones si el sistema funciona correctamente.