Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

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

a. La triada CIA establece los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

- **Verdadero**
- Falso

b. La confidencialidad garantiza que los sistemas estén siempre operativos y accesibles.

- Verdadero
- **Falso**

c. Los ataques de ingeniería social explotan principalmente vulnerabilidades técnicas en el *software.*

- Verdadero
- **Falso**

2. ¿Qué representa la triada CIA en ciberseguridad?

a. Un sistema de cifrado de datos
b. Un modelo de clasificación de *malware*
c. Los principios de confidencialidad, integridad y disponibilidad de la información
d. Un protocolo de seguridad de redes

3. ¿Qué se entiende por ataque informático?

a. Una actualización automática del sistema
b. Un intento deliberado de acceder, alterar, destruir o bloquear información sin autorización
c. Un error técnico en el servidor
d. Un proceso de mantenimiento informático

4. ¿Cuál de los siguientes ejemplos representa una vulneración de la confidencialidad?

a. Un servidor que deja de funcionar temporalmente
b. Un empleado sin permisos accede a una base de datos de clientes
c. Una copia de seguridad realizada correctamente
d. Una actualización de *software*

5. ¿Qué tipo de ataque busca saturar un sistema para impedir su funcionamiento normal?

a. Ataque de fuerza bruta
b. *Phishing*
c. Ataque de denegación de servicio (DoS/DDoS)
d. Ingeniería social

6. ¿Qué caracteriza principalmente a los ataques de ingeniería social?

a. Aprovechan fallos en el *software*
b. Manipulan a las personas para obtener información o acceso
c. Saturan servidores mediante tráfico masivo
d. Se basan únicamente en *malware*

7. ¿Qué es un vector de entrada en un incidente de seguridad?

a. Un programa de protección de datos
b. El método utilizado por un atacante para acceder a un sistema
c. Una herramienta de análisis de redes
d. Un sistema de recuperación de datos

8. ¿Qué se entiende por superficie de ataque?

a. El número de ataques recibidos por una empresa
b. El conjunto de puntos potenciales por los que un atacante puede intentar acceder a una organización
c. El *software* de seguridad instalado en la empresa
d. El número de empleados con acceso al sistema

9. ¿Cuál de las siguientes situaciones puede considerarse un indicador de compromiso (IoC)?

a. Una copia de seguridad programada
b. Accesos al sistema fuera del horario habitual
c. Un reinicio del servidor
d. Una actualización del sistema operativo

10. ¿Qué técnica de ingeniería social consiste en el envío masivo de correos electrónicos fraudulentos que simulan proceder de entidades legítimas?

a. *Vishing*
b. *Smishing*
c. *Spear phishing*
d. *Phishing*

Ejercicios de autoevaluación
Unidad de Aprendizaje 2

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

a. La autenticación multifactor refuerza la seguridad de acceso al exigir más de un factor para verificar la identidad del usuario.

- **Verdadero**
- Falso

b. La revocación de un certificado digital consiste en renovarlo automáticamente cuando está próximo a caducar.

- Verdadero
- **Falso**

c. La continuidad de negocio hace referencia a la capacidad de una organización para seguir operando tras un incidente que afecte a sus sistemas o servicios.

- **Verdadero**
- Falso

2. ¿Qué se entiende por seguridad perimetral en una organización?

a. La protección exclusiva de los equipos informáticos de una empresa.
b. El conjunto de medidas destinadas a proteger los puntos de acceso a los sistemas de información.
c. El uso obligatorio de certificados digitales en todas las comunicaciones.
d. La gestión de contraseñas en aplicaciones internas.

3. ¿Qué elemento forma parte del perímetro de seguridad de una organización?

a. Los accesos remotos del personal o colaboradores.
b. Las impresoras domésticas de los trabajadores.
c. Los sistemas operativos personales de los usuarios.
d. Las aplicaciones instaladas en dispositivos privados.

4. ¿Qué función cumple una infraestructura de clave pública (PKI)?

a. Controlar el tráfico de red entre servidores.
b. Administrar las redes internas de una organización.
c. Emitir, gestionar y validar certificados digitales.
d. Supervisar el rendimiento de los sistemas.

5. ¿Qué entidad es responsable de emitir certificados digitales?

a. Autoridad de registro
b. Autoridad de certificación
c. Proveedor de servicios en la nube
d. Administrador de red

6. ¿Qué elemento de un certificado digital indica quién es su propietario?

a. La firma digital
b. El periodo de validez
c. La identidad del titular
d. La clave pública

7. ¿Qué mecanismo permite comprobar en tiempo real si un certificado sigue siendo válido?

a. CRL
b. DNS
c. HTTPS
d. OCSP

8. ¿Qué característica define la autenticación multifactor (MFA)?

a. Utilizar únicamente contraseñas complejas.
b. Verificar la identidad mediante más de un factor de autenticación.
c. Utilizar certificados digitales sin contraseña.
d. Conectarse a la red mediante VPN.

9. ¿Cuál es uno de los objetivos del marco regulatorio en ciberseguridad?

a. Sustituir las políticas de seguridad internas.
b. Eliminar los riesgos tecnológicos.
c. Establecer obligaciones para proteger los sistemas y los datos.
d. Controlar el acceso a internet de los empleados.

10. ¿Qué objetivo tiene la gestión de riesgos en seguridad de la información?

a. Eliminar completamente las amenazas.
b. Identificar y evaluar los riesgos para aplicar medidas de protección adecuadas.
c. Sustituir las políticas de seguridad.
d. Aumentar la velocidad de los sistemas.