Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. ¿Cuál es el objetivo principal de la seguridad informática en la empresa?

a. Aumentar la velocidad de la red.
b. Reducir costos operativos.
c. Proteger la confidencialidad, integridad y disponibilidad de los datos.
d. Mejorar la experiencia del usuario.

2. ¿Qué principio de seguridad asegura que los datos estén disponibles cuando se necesiten?

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

3. ¿Qué ejemplo representa el principio de integridad?

a. Restringir el acceso mediante contraseñas.
b. Verificar que un precio en un sistema de comercio electrónico no sea alterado maliciosamente.
c. Garantizar acceso continuo a los sistemas durante fallos.
d. Cifrar credenciales de un usuario.

4. ¿Qué estrategia ayuda a proteger la confidencialidad de los datos?

a. Realizar respaldos regulares.
b. Implementar controles de acceso y cifrado de información.
c. Utilizar *software* antivirus.
d. Configurar roles de usuario.

5. ¿Qué tipo de amenaza compromete la disponibilidad de un sistema?

a. Ataques de denegación de servicio (DoS).
b. Errores humanos al ingresar contraseñas.

c. Exposición accidental de datos sensibles.
d. Accesos no autorizados mediante contraseñas débiles.

6. ¿Qué describe un árbol de ataque?

a. Una herramienta para encriptar datos sensibles.
b. Una representación visual de posibles rutas de ataque.
c. Un plan de respaldo ante fallos de sistema.
d. Un método para asignar roles de usuario en redes.

7. ¿Qué acción es un ejemplo de *phishing*?

a. Inundar un servidor con solicitudes.
b. Enviar correos fraudulentos para obtener credenciales.
c. Usar contraseñas débiles en sistemas empresariales.
d. Monitorizar el tráfico en busca de anomalías.

8. ¿Qué política de seguridad fomenta el uso responsable de los sistemas?

a. Uso de *software* no actualizado.
b. Definir contraseñas robustas y cambios periódicos.
c. Abrir puertos para un acceso más rápido.
d. Permitir acceso total a todos los usuarios.

9. ¿Qué recomendación básica mejora la seguridad de una red?

a. Configurar contraseñas simples y fáciles de recordar.
b. Realizar auditorías de seguridad periódicas.
c. Usar versiones desactualizadas de *software.*
d. Reducir la segmentación de redes.

10. ¿Qué táctica de ataque utiliza *software* malicioso como virus o *ransomware?*

a. *Phishing*
b. *Malware*
c. Fuerza bruta
d. Segmentación de red

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. **¿Cuál es el objetivo general de las políticas de seguridad informática?**

   a. Proteger exclusivamente los sistemas operativos.
   b. Garantizar la confidencialidad, integridad y disponibilidad de la información.
   c. Establecer restricciones de acceso para todo tipo de usuarios.
   d. Mejorar la velocidad de los sistemas informáticos.

2. **¿Qué elemento no debería contener una política de seguridad?**

   a. Ambigüedad
   b. Roles y responsabilidades
   c. Gestión de accesos
   d. Procedimientos y normas

3. **¿Qué norma internacional se menciona como referencia para políticas de seguridad?**

   a. ISO 9001
   b. ISO 27001
   c. GDPR
   d. NIST 800-53

4. **¿Cuál es una de las razones principales para implementar políticas de seguridad?**

   a. Incrementar la productividad laboral.
   b. Prevenir amenazas internas y externas.
   c. Sustituir sistemas tecnológicos obsoletos.
   d. Eliminar completamente los incidentes de seguridad.

5. **¿Qué estrategia fomenta el cumplimiento de políticas de seguridad?**

   a. Capacitación continua.
   b. Uso de contraseñas compartidas.
   c. Evitar auditorías periódicas.
   d. Redactar las políticas en lenguaje técnico.

6. ¿Qué ventaja ofrece la personalización de políticas de seguridad?

a. Maximiza la interoperabilidad global.
b. Se ajusta a las necesidades específicas de la organización.
c. Reduce costos y tiempo de implementación.
d. Evita la necesidad de realizar auditorías.

7. ¿Cuál de los siguientes es un error común en políticas de seguridad?

a. Claridad de responsabilidades.
b. Inclusión de sanciones.
c. Uso excesivo de tecnicismos.
d. Actualización periódica.

8. ¿Qué permite el análisis de riesgos en una política de seguridad?

a. Identificar y priorizar amenazas relevantes.
b. Garantizar el cumplimiento normativo.
c. Evitar simulacros de seguridad.
d. Reducir la necesidad de controles de acceso.

9. ¿Qué aspecto fortalece una cultura organizacional de ciberseguridad?

a. Capacitar únicamente al personal técnico.
b. Supervisar actividades sin sancionar incumplimientos.
c. Fomentar una concienciación compartida en la seguridad.
d. Excluir normativas locales.

10. ¿Qué directriz ayuda a mantener la seguridad en sistemas y dispositivos?

a. Permitir acceso irrestricto a todos los usuarios.
b. Instalar actualizaciones de *software* periódicamente.
c. Utilizar contraseñas simples para todos los equipos.
d. Desactivar el cifrado en dispositivos móviles.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. **¿Cuál es el objetivo principal de la auditoría de seguridad de la información?**

    a. Incrementar la velocidad de la red.
    b. Identificar vulnerabilidades y garantizar el cumplimiento normativo.
    c. Reducir el costo de implementación de software.
    d. Desarrollar *hardware* nuevo para la organización.

2. **¿Qué norma internacional se utiliza como referencia para un SGSI?**

    a. ISO 14001
    b. ISO 9001
    c. ISO 27001
    d. ISO 31000

3. **¿Cuál es el enfoque utilizado en el ciclo del sistema de gestión de seguridad de la información?**

    a. Modelo de cascada
    b. PDCA (Planificar, Hacer, Verificar, Actuar)
    c. Ciclo en espiral
    d. Método ágil

4. **¿Qué acción se realiza en la fase "Planificar" del modelo PDCA?**

    a. Realizar pruebas de penetración.
    b. Identificar activos y evaluar riesgos.
    c. Implementar tecnologías de seguridad.
    d. Ajustar políticas de seguridad.

5. **¿Qué aspecto aborda la seguridad humana en la gestión de la seguridad de la información?**

    a. Control de accesos físicos.
    b. Capacitación en riesgos y políticas de seguridad.

c. Protección contra incendios.
d. Gestión de sistemas biométricos.

6. ¿Qué principio del modelo CIA garantiza que la información esté accesible cuando se necesita?

a. Confidencialidad
b. Integridad
c. Disponibilidad.
d. No repudio

7. ¿Qué herramienta facilita la centralización de la gestión de activos en una organización?

a. VPN
b. CMDB *(Configuration Management Database).*
c. SIEM
d. *Firewall*

8. ¿Qué medida se implementa para proteger la seguridad del entorno en una organización?

a. Instalación de sistemas contra incendios.
b. Capacitación del personal en ciberseguridad.
c. Uso de sistemas de autenticación biométrica.
d. Configuración de un CMDB.

9. ¿Cuál es un ejemplo de control de acceso basado en el principio de privilegios mínimos?

a. Permitir que todos los empleados accedan a la base de datos financiera.
b. Limitar el acceso de un empleado de recursos humanos a datos financieros.
c. Garantizar que los administradores tengan acceso completo a todos los sistemas.
d. Compartir credenciales entre diferentes usuarios.

10. ¿Qué acción clave forma parte de la gestión de continuidad del negocio?

a. Desarrollar una política para la actualización de dispositivos móviles.
b. Implementar autenticación multifactorial.
c. Realizar simulaciones de ciberataques para los clientes.
d. Diseñar un plan de recuperación para procesos críticos.

Ejercicios de autoevaluación Unidad de Aprendizaje 4

1. **¿Cuál es el objetivo general de la estrategia de seguridad en una organización?**

    a. Reducir los costos operativos.
    b. Proteger los sistemas informáticos y la información crítica frente a amenazas.
    c. Incrementar la productividad a través de tecnología avanzada.
    d. Crear sistemas de acceso público.

2. **¿Qué principio sigue la estrategia de *Menor privilegio?***

    a. Dar acceso completo a todos los usuarios.
    b. Asignar a los usuarios solo los permisos necesarios para cumplir con sus responsabilidades.
    c. Limitar el acceso únicamente a los gerentes.
    d. Permitir el acceso de todos los dispositivos externos.

3. **¿Qué enfoque utiliza la estrategia de *Defensa en profundidad?***

    a. Proteger solo el núcleo del sistema.
    b. Implementar múltiples capas de protección en diferentes niveles.
    c. Confiar únicamente en el cifrado de datos.
    d. Reducir privilegios sin medidas adicionales.

4. **Según la estrategia de diversificación de la defensa, ¿qué elemento es fundamental?**

    a. Confiar en un único proveedor de seguridad.
    b. Limitar el uso de herramientas tecnológicas.
    c. Utilizar diferentes soluciones de seguridad de múltiples proveedores.
    d. Mantener sistemas separados sin interconexión.

5. ¿Qué técnica utiliza la estrategia del *Eslabón más débil* para explotar vulnerabilidades humanas?

a. Criptografía avanzada.
b. Actualización de sistemas obsoletos.
c. Ingeniería social.
d. Uso de *firewalls*.

6. ¿Cuál de las siguientes opciones es un ejemplo de medida preventiva en una estrategia de seguridad?

a. Recuperar datos tras un ataque.
b. Realizar simulaciones de ciberataques.
c. Implementar autenticación multifactorial y políticas de contraseñas robustas.
d. Desconectar temporalmente los sistemas.

7. ¿Qué herramienta protege aplicaciones web frente a ataques como inyecciones SQL o XSS?

a. *Endpoint protection*
b. *Web application firewall* (WAF)
c. Sistema de detección de intrusos (IDS)
d. Tecnología *hash*

8. ¿Cuál es el objetivo principal de la estrategia de *Simplicidad?*

a. Reducir vulnerabilidades y errores al simplificar los sistemas.
b. Implementar herramientas avanzadas en todas las áreas.
c. Crear sistemas complejos que dificulten los ataques.
d. Aumentar la cantidad de accesos disponibles.

9. ¿Qué define la estrategia de *Postura de negación?*

a. Permitir acceso solo a ciertos datos críticos.
b. Considerar que todo lo no permitido explícitamente debe estar bloqueado.
c. Compartir recursos con todos los usuarios.
d. Utilizar permisos establecidos por defecto.

10. ¿Cuál de las siguientes prácticas fomenta la estrategia de *Participación universal?*

a. Confiar únicamente en sistemas automatizados.
b. Restringir la capacitación a los administradores.
c. Empoderar a todos los empleados para contribuir a la seguridad de la organización.
d. Crear un sistema sin intervención humana.

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. ¿Cuál es el objetivo general de la gestión de seguridad en redes empresariales?

a. Maximizar la velocidad de transmisión.
b. Reducir el uso de *hardware* en la red.
c. Establecer bases de seguridad para gestionar amenazas e imprevistos.
d. Identificar canales de transmisión y proteger los activos de información.

2. ¿Qué es el entorno de red?

a. Un espacio físico para guardar información.
b. Un espacio virtual para conectar equipos informáticos de manera eficiente y segura.
c. Un espacio virtual donde se intercambia información y recursos.
d. Un sistema exclusivo de redes inalámbricas.

3. ¿Qué caracteriza una red alámbrica?

a. Usa señales no guiadas.
b. Requiere un cable físico para transmitir señales.
c. Está basada únicamente en wifi.
d. Depende de servidores externos.

4. ¿Qué ventaja ofrece una red inalámbrica?

a. Mayor seguridad que una red alámbrica.
b. Alta estabilidad en la transferencia de datos.
c. Conectividad sin limitaciones físicas.
d. Menor riesgo de intrusiones.

5. ¿Qué tipo de red inalámbrica cubre áreas metropolitanas?

a. W-MAN
b. W-LAN

c. W-PAN
d. W-WAN

6. ¿Qué herramienta permite analizar puertos abiertos y evaluar la seguridad de un sistema?

a. Wireshark
b. SCANLINE
c. SolarWinds
d. NMAP

7. ¿Qué fase en un ataque cibernético implica permanecer en el sistema sin ser detectado?

a. Escaneo
b. Mantenimiento del acceso
c. Eliminación de evidencias
d. Reconocimiento

8. ¿Qué paso inicial es fundamental para identificar elementos esenciales de una red?

a. Escaneo
b. Enumeración
c. Mantenimiento del acceso
d. Estudio de aplicaciones

9. ¿Qué ventaja ofrece un enfoque híbrido de red?

a. Reduce el costo de infraestructura.
b. Combina la estabilidad del cableado con la flexibilidad inalámbrica.
c. Evita la necesidad de implementar herramientas de auditoría.
d. Aumenta la velocidad de ambas redes simultáneamente.

10. ¿Qué característica tiene NMAP que lo hace destacar como herramienta de ciberseguridad?

a. Es *software* libre y accesible para cualquier empresa.
b. Solo es compatible con sistemas *Windows*.
c. Permite configuraciones exclusivas en cortafuegos.
d. Limita el análisis a redes locales.

Ejercicios de autoevaluación Unidad de Aprendizaje 6

1. ¿Qué es un ataque remoto?

a. Un ataque que requiere acceso físico al sistema.
b. Un ataque que no necesita conexión a internet.
c. Un ataque que requiere conexión a internet o un canal de telecomunicaciones.
d. Un ataque interno ejecutado por empleados.

2. ¿Cuál de las siguientes es una técnica de ataque local?

a. *Shoulder Surfing*
b. *Phishing*
c. *Ransomware*
d. *Man in the Middle*

3. ¿Qué técnica utiliza dispositivos olvidados como pendrives para engañar a la víctima?

a. *Tailgating*
b. *Dumpster Diving*
c. *Ciber-Baiting*
d. *Pretexting*

4. ¿Qué diferencia un ataque activo de un ataque pasivo?

a. Los activos son más discretos que los pasivos.
b. Los pasivos alteran datos, mientras que los activos no.
c. Los activos solo buscan recopilar datos.
d. Los pasivos recopilan datos sin modificar el sistema, mientras que los activos alteran información.

5. ¿Cuál es un ejemplo de ataque remoto?

a. *Dumpster Diving*
b. *Shoulder Surfing*
c. *Phishing*
d. *Pretexting*

6. ¿Qué técnica se utiliza para modificar nombres de dominio y redirigir a sitios falsos?

a. *IP Spoofing*
b. *DNS Spoofing*
c. *Replay Attack*
d. *SQL Injection*

7. ¿Qué herramienta permite capturar pulsaciones de teclado para obtener datos sensibles?

a. *Keymaker*
b. *Ransomware*
c. *Keylogger*
d. *Malware Script*

8. ¿Cuál es el objetivo principal de un ataque DoS?

a. Colapsar un sistema enviando una gran cantidad de solicitudes.
b. Interceptar comunicaciones.
c. Inyectar código malicioso en bases de datos.
d. Monitorear el tráfico de red sin ser detectado.

9. ¿Qué medida preventiva es esencial para evitar ataques en sistemas *UNIX?*

a. Eliminar contraseñas complejas.
b. Permitir privilegios de administrador a todos los usuarios.
c. Mantener el sistema operativo actualizado con parches de seguridad.
d. Usar cuentas de usuario genéricas.

10. ¿Qué acción clave ayuda a prevenir ataques en redes públicas inseguras?

a. Usar Telnet para conexiones seguras.
b. Evitar compartir información confidencial en redes wifi públicas.
c. Deshabilitar los *firewalls* del sistema.
d. Confiar en configuraciones predeterminadas.

Ejercicios de autoevaluación
Unidad de Aprendizaje 7

1. ¿Cuál es el principal objetivo de las redes inalámbricas en una empresa?

a. Reducir los costes asociados a la implementación de redes físicas.
b. Garantizar una transferencia segura y eficiente de datos en tiempo real.
c. Eliminar la necesidad de routers en la conectividad.
d. Sustituir completamente las redes alámbricas.

2. ¿Qué característica describe mejor al estándar IEEE 802.11?

a. Conexiones solo mediante cables.
b. Gestión de datos exclusivamente locales.
c. Infraestructura inalámbrica estructurada en el modelo OSI.
d. Uso limitado a redes domésticas.

3. ¿Cuál de los siguientes estándares pertenece a la familia IEEE 802.11?

a. Wifi 7
b. 802.11ax (WiFi 6)
c. LTE Advanced
d. Ethernet 5G

4. ¿Qué topología se caracteriza por conectar todos los dispositivos en una línea central?

a. Malla
b. Estrella
c. Bus
d. Anillo

5. ¿Cuál de los siguientes es un mecanismo de cifrado obsoleto?

a. WPA3
b. WPA2-*Enterprise*

c. TKIP
d. WEP

6. ¿Qué función realiza la capa de red en el modelo OSI?

a. Garantizar la encriptación y desencriptación de datos.
b. Gestionar el enrutamiento y entrega de datos entre redes.
c. Sincronizar los dispositivos conectados.
d. Establecer conexiones físicas entre nodos.

7. ¿Cuál es una vulnerabilidad típica de redes abiertas?

a. Alta velocidad de conexión.
b. Facilidad para ataques de tipo *Man in the Middle.*
c. Complejidad en la configuración.
d. Mayor coste de implementación.

8. ¿Qué significa SSID en el contexto de redes inalámbricas?

a. Sistema de seguridad inalámbrico dinámico.
b. Identificador del conjunto de servicios de una red WLAN.
c. Protocolo de conexión segura para redes wifi.
d. *Software* de supervisión de identidades digitales.

9. ¿Cuál es una de las mejoras que ofrece WPA3 frente a WPA2?

a. Mayor resistencia frente a ataques de fuerza bruta.
b. Incremento de la velocidad de transmisión.
c. Uso exclusivo en redes domésticas.
d. Sustitución del modelo OSI.

10. ¿Qué topología de red es ideal para empresas que necesitan una expansión flexible?

a. Árbol
b. Anillo
c. Bus
d. Estrella

Ejercicios de autoevaluación Unidad de Aprendizaje 8

1. ¿Cuál es el objetivo principal de la criptografía?

a. Compartir información pública.
b. Proteger información mediante técnicas de cifrado.
c. Garantizar la confidencialidad de los datos.
d. Aumentar la velocidad de transmisión.

2. ¿Qué significa el concepto de criptoanálisis?

a. Análisis del uso de claves privadas.
b. Descifrar mensajes sin conocer la clave utilizada.
c. Identificar vulnerabilidades en sistemas de cifrado.
d. Monitorear la transmisión de datos cifrados.

3. ¿Qué ciencia engloba tanto la criptografía como el criptoanálisis?

a. Cibernética
b. Criptología
c. Algoritmia avanzada
d. Seguridad informática

4. ¿Qué principio básico de la criptografía busca detectar o evitar ataques criptográficos?

a. Temporalidad
b. Redundancia
c. Cifrado simétrico
d. Integridad

5. ¿Qué caracteriza a la criptografía clásica?

a. Uso de múltiples claves públicas.
b. Algoritmos complejos y largos.
c. Algoritmos sencillos y simétricos.
d. Exclusiva aplicación en sistemas informáticos.

6. ¿Qué ventaja ofrece el cifrado de "relleno de una sola vez"?

a. Su algoritmo simétrico es simple.
b. Es considerado inquebrantable si la clave no se reutiliza.
c. Puede usarse sin necesidad de clave.
d. No requiere sincronización entre emisor y receptor.

7. ¿Cuál es una de las desventajas del algoritmo de "relleno de una sola vez"?

a. Requiere claves públicas y privadas.
b. La sincronización entre emisor y receptor es crítica.
c. No garantiza la confidencialidad del mensaje.
d. Es fácilmente descifrable con herramientas modernas.

8. ¿Qué diferencia a la criptografía moderna de la clásica?

a. El uso exclusivo de claves públicas.
b. La generación automática de claves privadas.
c. La complejidad y longitud de los algoritmos.
d. La dependencia de claves compartidas.

9. ¿Qué protocolo se utiliza comúnmente para proteger comunicaciones en internet mediante cifrado?

a. IPSec
b. DES
c. RSA
d. IDEA

10. ¿Qué función cumple el componente ESP dentro del protocolo IPSec?

a. Proporcionar integridad al mensaje.
b. Verificar la identidad del emisor.
c. Garantizar confidencialidad y autenticación de datos.
d. Generar claves públicas automáticamente.

Ejercicios de autoevaluación Unidad de Aprendizaje 9

1. ¿Cuál es el objetivo principal de la autenticación en la seguridad informática empresarial?

a. a. Evitar la creación de nuevas cuentas de usuario.
b. b. Facilitar el acceso a todos los recursos de la red.
c. Garantizar que los usuarios que acceden a los sistemas sean quienes afirman ser.
d. Minimizar el número de usuarios activos.

2. ¿Qué diferencia clave existe entre identificación y autenticación?

a. La identificación confirma la identidad del usuario, mientras que la autenticación la declara.
b. La autenticación declara la identidad, y la identificación verifica que sea legítima.
c. La identificación declara quién es el usuario, y la autenticación confirma la legitimidad de esa declaración.
d. No existe diferencia entre ambos conceptos.

3. ¿Qué tipo de red permite el acceso sin necesidad de autenticación?

a. Privada
b. Cifrada
c. Multifactorial
d. Pública

4. ¿Qué método combina credenciales tradicionales con métodos biométricos y *tokens* digitales?

a. Validación de clave compartida
b. Protocolo Diffie-Hellman
c. Autenticación multifactorial (MFA)
d. Claves de cifrado asimétricas

5. Según el protocolo AAA, ¿qué acción se realiza tras la autenticación de un usuario?

a. Confirmación de integridad de los datos
b. Autorización para acceder a recursos específicos
c. Registro de anomalías en la red
d. Generación de claves públicas y privadas

6. ¿Cuál de los siguientes no es un principio fundamental del proceso de validación de identificación?

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

7. ¿Qué protocolo utiliza un centro de distribución de claves (KDC) para garantizar la seguridad en la red?

a. IPSec
b. Kerberos
c. KDC
d. IKE

8. ¿Qué vulnerabilidad se asocia al uso de claves compartidas?

a. Alta velocidad de transmisión
b. Posible almacenamiento en texto plano
c. Generación de claves automáticas
d. Falta de compatibilidad con redes públicas

9. ¿Qué protocolo establece una clave compartida entre dos participantes sin contacto previo?

a. Kerberos
b. KDC
c. Diffie-Hellman
d. IPSec

10. ¿Qué asegura el componente ESP del protocolo IPSec?

a. La integridad de los datos.
b. La autenticación del emisor.
c. La confidencialidad, autenticación e integridad de los datos.
d. La negociación automática de claves.