Preguntas de Prácticas

Fundamentos esenciales de Ciberseguridad

👏 Felicitaciones por invertir en tu desarrollo profesional. Esta decisión demuestra tu compromiso con el crecimiento en el sector TIC, una mentalidad que te diferenciará y abrirá nuevas oportunidades en tu carrera tecnológica.

Contenido

- ☑ Preguntas de prácticas basadas en conocimientos esenciales de ciberseguridad generalmente solicitados en certificaciones de entrada
- ☑ Enfoque en dominios clave de seguridad informática
- ☑ Respuestas con explicaciones detalladas

Público

👨‍🎓👩‍🎓 Este material está diseñado específicamente para técnicos de soporte y sistemas, estudiantes y profesionales del sector IT que buscan adquirir conocimientos fundamentales en ciberseguridad y seguridad de la información. Es ideal tanto para quienes desean iniciar su especialización en el ámbito de la seguridad informática como para aquellos que buscan fortalecer sus competencias en la protección de sistemas y datos.

Cómo sacar el máximo provecho a este material

Una certificación profesional no es solo un título - es la validación concreta de tus habilidades y un diferenciador clave en el competitivo mercado tecnológico. Este material está diseñado bajo el principio de que el aprendizaje activo a través de preguntas y respuestas explicadas es una de las metodologías más efectivas para la retención del conocimiento.

Cuando estudias no solo la respuesta correcta, sino también el "por qué" las otras opciones son incorrectas, desarrollas una comprensión más profunda de los conceptos. Este enfoque te prepara no solo para recordar información, sino para aplicar el conocimiento en escenarios reales como los que encontrarás en el examen y en tu trabajo diario.

No te limites a memorizar respuestas. Analiza cada explicación, investiga los conceptos que no comprendas completamente y aplica este conocimiento en ejercicios prácticos. Así transformarás la teoría en competencias duraderas.

Versión 1.0 - Noviembre/2025
© Picolo Trainings

CC BY-NC 4.0

Pregunta 1: ¿Cuál de los siguientes términos describe una debilidad en un sistema o red que podría ser explotada por una amenaza?

A. Riesgo

B. Explotación

C. Amenaza

D. Vulnerabilidad

Respuesta Correcta: D. Vulnerabilidad

Explicación: Una **vulnerabilidad** es una debilidad o un fallo en el diseño, la implementación o la configuración de un sistema que, al ser aprovechado por una **amenaza** mediante un **exploit**, puede resultar en una violación de la seguridad. El **riesgo** es la probabilidad de que la amenaza explote la vulnerabilidad, resultando en un impacto.

Pregunta 2: Si una base de datos sufre una corrupción de datos debido a un fallo en el disco, pero los datos se restauran completamente y de forma precisa desde una copia de seguridad verificada, ¿qué principio de la triada CIA se ha conservado?

A. Confidencialidad

B. Disponibilidad

C. Integridad

D. No Repudio

Respuesta Correcta: C. Integridad

Explicación: La **Integridad** se refiere a la exactitud, consistencia y fiabilidad de los datos a lo largo de su ciclo de vida. Aunque la **Disponibilidad** fue interrumpida temporalmente, la restauración precisa de los datos desde una copia de seguridad asegura que el principio de Integridad se mantiene.

Pregunta 3: ¿Qué tipo de ataque de ingeniería social utiliza mensajes de texto SMS para engañar a las víctimas y hacer que revelen información confidencial?

A. Vishing

B. Tailgating

C. Phishing

D. Smishing

Respuesta Correcta: D. Smishing

CC BY-NC 4.0
© Picolo Trainings

Explicación: El **Smishing** es una técnica de *phishing* que emplea mensajes de texto (SMS) o mensajería instantánea para manipular a las víctimas. El **Vishing** utiliza llamadas de voz (VOIP o teléfono), mientras que el *phishing* general utiliza correo electrónico.

Pregunta 4: ¿Qué tipo de *malware* se propaga automáticamente por la red explotando vulnerabilidades de *software* sin requerir la interacción del usuario o un archivo huésped?

A. Troyano

B. Adware

C. Gusano (Worm)

D. Rootkit

Respuesta Correcta: C. Gusano (*Worm*)

Explicación: Un **Gusano** (*Worm*) es un *malware* autorreplicante y autodifusor que utiliza la red y sus vulnerabilidades para propagarse sin necesidad de inyectarse en un archivo legítimo (como lo haría un virus) ni depender del engaño del usuario (como un troyano).

Pregunta 5: El proceso de verificar que un usuario que solicita acceso a un sistema es, de hecho, quien dice ser, se conoce como:

A. Autorización

B. Auditoría

C. Autenticación

D. Contabilización (Accounting)

Respuesta Correcta: C. Autenticación

Explicación: La **Autenticación** es el proceso de verificar la identidad. La **Autorización** se produce después y determina qué recursos puede acceder el usuario, y la **Contabilización** registra las acciones realizadas.

Pregunta 6: ¿Cuál de los siguientes combina al menos dos **factores diferentes** de autenticación (algo que sabes, algo que tienes, algo que eres)?

A. Autenticación de Paso Único (SPA)

B. Autenticación Única (Single Sign-On - SSO)

C. Autenticación Multifactor (MFA)

D. Contraseña de Uso Único (One-Time Password - OTP)

Respuesta Correcta: C. Autenticación Multifactor (MFA)

CC BY-NC 4.0
© Picolo Trainings

Explicación: La **Autenticación Multifactor (MFA)** requiere que el usuario presente credenciales de **múltiples categorías de factores** independientes (ej. contraseña + huella dactilar, o contraseña + *token* de seguridad) para conceder el acceso.

Pregunta 7: ¿Qué método de cifrado utiliza un par de claves matemáticamente relacionadas (una pública y una privada) para proteger la confidencialidad de los datos?

A. Cifrado simétrico

B. Hashing

C. Steganography

D. Cifrado asimétrico

Respuesta Correcta: D. Cifrado asimétrico

Explicación: El **Cifrado Asimétrico** (o de clave pública) utiliza dos claves diferentes: la clave **pública** (que se comparte) para cifrar, y la clave **privada** (que se mantiene secreta) para descifrar, y viceversa para las firmas digitales.

Pregunta 8: ¿Qué tecnología se encarga de emitir, gestionar, revocar y distribuir certificados digitales utilizados para autenticar sitios web y firmar digitalmente documentos?

A. SSL/TLS

B. Protocolo de Transferencia de Hipertexto (HTTP)

C. Infraestructura de Clave Pública (PKI)

D. VPN

Respuesta Correcta: C. Infraestructura de Clave Pública (PKI)

Explicación: La **Infraestructura de Clave Pública (PKI)** es el sistema de roles, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales y gestionar el cifrado de clave pública.

Pregunta 9: ¿Qué protocolo carece de mecanismos de verificación de conexión y es vulnerable a ataques de inundación debido a que no requiere un *handshake* de tres vías para el envío de paquetes?

A. TCP (Transmission Control Protocol)

B. HTTP (Hypertext Transfer Protocol)

C. ARP (Address Resolution Protocol)

D. UDP (User Datagram Protocol)

CC BY-NC 4.0
© Picolo Trainings

Respuesta Correcta: D. UDP (*User Datagram Protocol*)

Explicación: UDP es un protocolo sin conexión (*connectionless*) que no realiza el *handshake* de tres vías (SYN, SYN-ACK, ACK), lo que lo hace muy rápido, pero propenso a ataques de inundación (*flood*) ya que los atacantes pueden enviar un gran volumen de datos sin verificar la sesión.

Pregunta 10: ¿Qué tecnología permite que múltiples dispositivos en una red privada (usando direcciones IP privadas, ej. 192.168.x.x) compartan una única dirección IP pública para acceder a Internet?

A. VPN (Virtual Private Network)

B. DMZ (Demilitarized Zone)

C. NAT (Network Address Translation)

D. VLAN (Virtual Local Area Network)

Respuesta Correcta: C. NAT (*Network Address Translation*)

Explicación: La **NAT** es un proceso que modifica la información de la dirección IP en las cabeceras de los paquetes mientras están en tránsito, permitiendo que las direcciones **privadas** se "traduzcan" a una dirección **pública** única al comunicarse con Internet.

Pregunta 11: En la arquitectura de seguridad, ¿qué zona se utiliza para albergar servidores que deben ser accesibles desde la red pública de Internet, pero que deben estar separados de la red interna de la organización?

A. Red Privada Virtual (VPN)

B. Red de Área Local (LAN)

C. Zona Desmilitarizada (DMZ)

D. Honeypot

Respuesta Correcta: C. Zona Desmilitarizada (DMZ)

Explicación: La **DMZ** actúa como una subred neutral y aislada que aloja servicios públicos (servidores web, correo, etc.), protegiendo la red interna de posibles ataques si los servicios públicos son comprometidos.

Pregunta 12: ¿Qué estándar de seguridad inalámbrica proporciona la protección más robusta contra ataques de descifrado actualmente?

A. WEP

B. WPA

C. WPA2 con TKIP

CC BY-NC 4.0
© Picolo Trainings

D. WPA3

Respuesta Correcta: D. WPA3

Explicación: WPA3 es el estándar más reciente y más seguro. Soluciona debilidades conocidas en WPA2 (como los ataques KRACK) y ofrece un cifrado más fuerte y una mejor protección contra ataques de fuerza bruta *offline*.

Pregunta 13: ¿Qué tecnología se utiliza principalmente para establecer un túnel seguro y cifrado sobre una red pública (como Internet) para permitir el acceso remoto seguro?

A. ACL (Access Control List)

B. VPN (Virtual Private Network)

C. NAC (Network Access Control)

D. Firewall

Respuesta Correcta: B. VPN (*Virtual Private Network*)

Explicación: Una **VPN** crea un túnel seguro y cifrado entre dos puntos, lo que permite que los datos viajen de forma confidencial y con integridad a través de redes que no son de confianza.

Pregunta 14: ¿Qué concepto de seguridad ocurre cuando un atacante o *malware* eleva sus permisos de usuario en un sistema comprometido, por ejemplo, de un usuario estándar a privilegios de administrador o *root*?

A. Hardening

B. Desbordamiento de búfer

C. Escalada de privilegios

D. Denial of Service (DoS)

Respuesta Correcta: C. Escalada de privilegios

Explicación: La **Escalada de Privilegios** es el acto de explotar una vulnerabilidad o fallo de configuración para obtener niveles de acceso que no deberían estar disponibles para la cuenta o proceso comprometido.

Pregunta 15: ¿Qué herramienta de línea de comandos se utiliza habitualmente para mostrar las conexiones de red activas, las tablas de enrutamiento y las estadísticas de la interfaz en un *endpoint*?

A. ping

B. nslookup

CC BY-NC 4.0
© Picolo Trainings

C. netstat

D. tcpdump

Respuesta Correcta: C. netstat

Explicación: El comando **netstat** (*Network Statistics*) es la utilidad estándar para auditar el estado de las conexiones de red (entrantes, salientes y puertos de escucha) en el sistema local.

Pregunta 16: ¿Qué marco de cumplimiento normativo de EE. UU. exige que las organizaciones protejan la información personal de salud (PHI) de los pacientes?

A. GDPR

B. PCI DSS

C. FERPA

D. HIPAA

Respuesta Correcta: D. HIPAA

Explicación: HIPAA (*Health Insurance Portability and Accountability Act*) es la ley federal de EE. UU. que establece las normas nacionales para proteger la información de salud sensible del paciente.

Pregunta 17: La práctica esencial de aplicar actualizaciones a los *drivers* de dispositivos y al *firmware* de hardware se conoce generalmente como:

A. Virtualización

B. Patching (Parcheo)

C. Hardening

D. Provisioning

Respuesta Correcta: B. *Patching* (Parcheo)

Explicación: El ***Patching*** (Parcheo) es el proceso de aplicar actualizaciones de *software*, *drivers* y *firmware* para corregir fallos, vulnerabilidades de seguridad o mejorar la funcionalidad.

Pregunta 18: ¿Qué mecanismo de registro centralizado permite a varios dispositivos de red (servidores, *routers*, *firewalls*) enviar sus mensajes de eventos a un repositorio central para su análisis?

A. Visor de Sucesos (Event Viewer)

B. Audit Logs

C. Syslog

CC BY-NC 4.0
© Picolo Trainings

D. Packet Capture

Respuesta Correcta: C. Syslog

Explicación: Syslog es el protocolo estándar de la industria que permite la gestión y transmisión estandarizada de mensajes de registro de eventos desde dispositivos y sistemas a un servidor de registro centralizado.

Pregunta 19: ¿Qué término describe mejor el proceso continuo de identificar, clasificar, priorizar y corregir o mitigar las debilidades en un sistema o red?

A. Exploración de Puertos (Port Scanning)

B. Gestión de Vulnerabilidades

C. Detección de Intrusos (IDS)

D. Auditoría de Cumplimiento

Respuesta Correcta: B. Gestión de Vulnerabilidades

Explicación: La **Gestión de Vulnerabilidades** es el ciclo de vida completo que abarca la detección de debilidades (*scanning*), su análisis de riesgo, la priorización y la aplicación de soluciones (*patching* o *mitigación*).

Pregunta 20: ¿Qué repositorio proporciona un diccionario de nombres comunes y estandarizados para identificar vulnerabilidades de ciberseguridad conocidas públicamente, permitiendo la comunicación consistente entre analistas?

A. TTP (Tactics, Techniques, and Procedures)

B. CVE (Common Vulnerabilities and Exposures)

C. SIEM (Security Information and Event Management)

D. TAXII (Trusted Automated eXchange of Indicator Information)

Respuesta Correcta: B. CVE (*Common Vulnerabilities and Exposures*)

Explicación: CVE es la lista universalmente aceptada de identificadores para vulnerabilidades de seguridad conocidas, facilitando la identificación y el seguimiento de los fallos por parte de los profesionales de seguridad.

Pregunta 21: Una empresa decide contratar una póliza de seguro contra desastres naturales que puedan afectar su centro de datos. ¿Qué estrategia de gestión de riesgos está aplicando la empresa?

A. Elusión de Riesgos

B. Mitigación de Riesgos

CC BY-NC 4.0
© Picolo Trainings

C. Aceptación de Riesgos

D. Transferencia de Riesgos

Respuesta Correcta: D. Transferencia de Riesgos

Explicación: La **Transferencia de Riesgos** implica trasladar la responsabilidad financiera o el impacto de un riesgo a un tercero, como una compañía de seguros.

Pregunta 22: ¿Qué plan de seguridad se centra en asegurar que las **funciones y procesos críticos del negocio** puedan continuar operando durante y después de un evento catastrófico?

A. Plan de Respuesta a Incidentes (IRP)

B. Plan de Continuidad del Negocio (BCP)

C. Plan de Recuperación ante Desastres (DRP)

D. Plan de Contingencia

Respuesta Correcta: B. Plan de Continuidad del Negocio (BCP)

Explicación: El **BCP** se enfoca en mantener la **funcionalidad del negocio**, mientras que el **DRP** se centra en la **recuperación de la infraestructura** de IT. El BCP tiene una visión más amplia.

Pregunta 23: Un analista de seguridad recibe una alerta del SIEM sobre una conexión de red saliente a un servidor de Comando y Control (C2) conocido. En el contexto de la gestión de alertas, ¿cómo se clasifica este evento?

A. Falso Negativo

B. Verdadero Negativo

C. Falso Positivo

D. Verdadero Positivo

Respuesta Correcta: D. Verdadero Positivo

Explicación: Un **Verdadero Positivo** es una alerta correcta sobre una actividad maliciosa real. Este tipo de alerta debe ser escalada inmediatamente para iniciar el proceso de respuesta a incidentes.

Pregunta 24: ¿En qué orden de volatilidad se debe recopilar la evidencia digital en una investigación forense?

A. Contenido de Disco Fijo > Contenido de RAM > Copias de Seguridad

B. Contenido de RAM > Contenido de Disco Fijo > Copias de Seguridad

C. Copias de Seguridad > Contenido de RAM > Contenido de Disco Fijo

CC BY-NC 4.0
© Picolo Trainings

D. Contenido de RAM > Copias de Seguridad > Contenido de Disco Fijo

Respuesta Correcta: B. Contenido de RAM > Contenido de Disco Fijo > Copias de Seguridad

Explicación: La evidencia se recopila de lo **más volátil a lo menos volátil**. La **RAM** se pierde si el sistema se apaga (la más volátil), el **Disco Fijo** es semi-persistente, y las **Copias de Seguridad** son las más estables.

Pregunta 25: Según el marco de respuesta a incidentes de NIST, ¿qué documento detalla los pasos técnicos exactos a seguir (ej. cómo aislar un *host* infectado o cómo aplicar un *parche* de emergencia)?

A. Directiva de Respuesta a Incidentes

B. Plan de Continuidad del Negocio

C. Plan de Respuesta a Incidentes

D. Procedimientos de Respuesta a Incidentes

Respuesta Correcta: D. Procedimientos de Respuesta a Incidentes

Explicación: Los **Procedimientos** son documentos detallados y específicos (manuales técnicos de "cómo hacer") que se ejecutan durante la respuesta. La **Directiva** establece la autoridad (alto nivel), y el **Plan** define los roles y el alcance (nivel medio).

CC BY-NC 4.0
© Picolo Trainings

¿Esto te ha sido útil?

Es solo el principio. Únete al Club Guerreros de la TIC y lleva tu preparación al siguiente nivel. En nuestro club encontrarás tu tribu: más materiales, cursos y la motivación para conquistar tu certificación.



¡Te esperamos!

https://www.picolotrainings.com/es/guerrerosdelatic

LICENCIA © Picolo Trainings - 2025

Este trabajo está licenciado bajo la Licencia Creative Commons Reconocimiento-NoComercial 4.0 Internacional (CC BY-NC 4.0).

Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc/4.0/deed.es

Eres libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato.

Adaptar — remezclar, transformar y construir a partir del material.

Bajo los siguientes términos:

Atribución (BY) — Debes dar crédito apropiado a Picolo Trainings, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de Picolo Trainings.

NoComercial (NC) — No puede utilizar el material para fines comerciales.

No es necesario que obtengas un permiso adicional del autor para los usos permitidos por esta licencia.

AVISOS LEGALES IMPORTANTES

1. Origen del Contenido y Descargo de Responsabilidad

Las preguntas y respuestas de este material fueron elaboradas por el autor con asistencia de herramientas de Inteligencia Artificial y posteriormente curadas y validadas, tomando como referencia los temarios oficiales públicos de las certificaciones correspondientes. Picolo Trainings no ofrece exámenes antiguos ni preguntas de exámenes reales. Este material no forma parte de, ni está avalado, patrocinado o aprobado por entidades certificadoras.

2. Naturaleza del Contenido

El contenido tiene fines exclusivamente informativos y educativos. No constituye asesoramiento profesional ni sustituye la formación técnica especializada en ciberseguridad. Dada la naturaleza del proceso de creación, Picolo Trainings no garantiza la exactitud, exhaustividad o actualidad de la información. El material se ofrece "tal cual" ("as is") y el usuario asume todo el riesgo de su uso.

3. Limitación de Responsabilidad

En la máxima medida permitida por la ley, Picolo Trainings no asume responsabilidad alguna por errores u omisiones en el contenido, ni por ningún daño directo, indirecto, incidental, especial o consecuente que pudiera derivarse del uso o la imposibilidad de uso de este material y la información contenida en el mismo.

4. Marcas Registradas

Todas las referencias a marcas comerciales, nombres de productos y entidades certificadoras que puedan aparecer en el material se realizan con fines meramente ilustrativos y didácticos. Cualquier marca mencionada es propiedad de sus respectivos titulares. Su posible uso en este material no implica afiliación, patrocinio, respaldo o relación comercial alguna con Picolo Trainings.

Legislación aplicable: Este material digital se rige e interpreta de acuerdo con la legislación española y de la Unión Europea.