

30 preguntas de práctica

Preparación para CompTIA Security+

👏 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
- ☑ 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.

Pregunta 1: ¿Qué tipo de control de seguridad está diseñado para disuadir o desanimar a los atacantes de intentar una violación de la seguridad?

A. Control Correctivo B. Control Directivo C. Control Disuasorio (*Deterrent*) D. Control Compensatorio

Respuesta Correcta: C. Control Disuasorio (*Deterrent*)

Explicación: Un **Control Disuasorio** (*Deterrent*) tiene como objetivo principal reducir la probabilidad de un ataque al hacer que parezca menos atractivo o más arriesgado (ej. una valla electrificada o avisos de videovigilancia). El Control Correctivo se utiliza después de un incidente (restauración), el Directivo establece la guía (política), y el Compensatorio se implementa cuando el control primario no puede cumplirse.

Pregunta 2: ¿Qué principio fundamental de seguridad se viola si un servidor de archivos no está disponible para los usuarios legítimos debido a un ataque de Denegación de Servicio (DoS)?

A. Confidencialidad B. Integridad C. No Repudio D. Disponibilidad

Respuesta Correcta: D. Disponibilidad

Explicación: La **Disponibilidad** se refiere a asegurar que los sistemas y los datos sean accesibles por los usuarios autorizados cuando sea necesario. Un ataque DoS, al sobrecargar el servidor, viola directamente este principio. La Confidencialidad se relaciona con la privacidad, y la Integridad con la exactitud de los datos.

Pregunta 3: El proceso de obtener la aprobación formal para implementar una nueva versión de un sistema operativo en la infraestructura de producción se realiza a través de:

A. Gestión de Riesgos (Risk Management) B. Gestión de Incidentes (Incident Management) C. Gestión de Cambios (Change Management) D. Gestión de Activos (Asset Management)

Respuesta Correcta: C. Gestión de Cambios (Change Management)

Explicación: La **Gestión de Cambios** es el proceso formal que define los procedimientos para manejar y documentar las modificaciones en el entorno de producción (incluyendo *upgrades* de SO) para minimizar el riesgo de interrupciones o vulnerabilidades no deseadas.

Pregunta 4: ¿Qué función de las soluciones criptográficas garantiza la autenticidad y la no modificación de un documento al utilizar la clave privada del remitente para crear un valor que solo puede ser verificado por su clave pública?

A. *Hashing* B. Obfuscación C. Cifrado simétrico D. Firma Digital

Respuesta Correcta: D. Firma Digital

Explicación: Una **Firma Digital** proporciona **Integridad** y **No Repudio**. Se crea al cifrar el *hash* del documento con la clave privada del remitente, probando la identidad del firmante (autenticidad) y que el documento no fue alterado (*hashing* solo verifica la integridad, pero no la identidad).

Pregunta 5: ¿Qué categoría de actor de amenaza tiene la motivación principal de obtener ganancias financieras al robar información de tarjetas de crédito o extorsionar con *ransomware*?

A. Hacktivistas B. Amenazas Internas (*Insider Threats*) C. Crimen Organizado D. Atacantes No Cualificados

Respuesta Correcta: C. Crimen Organizado

Explicación: El **Crimen Organizado** está motivado casi exclusivamente por el **beneficio económico** y opera con estructuras empresariales complejas para maximizar sus ganancias a través de estafas, robo de datos sensibles y el despliegue de *ransomware*. Los Hacktivistas buscan fines ideológicos o políticos.

Pregunta 6: Un atacante envía correos electrónicos fraudulentos masivos diseñados para engañar a cualquier empleado para que revele credenciales. Este es un ejemplo de un vector de ataque basado en:

A. Cadena de Suministro (*Supply Chain*) B. Red No Segura C. Mensajes (*Message-based*) D. Llamada de Voz (*Voice Call*)

Respuesta Correcta: C. Mensajes (*Message-based*)

Explicación: Los ataques de *phishing* por correo electrónico son el ejemplo más común de un vector de ataque **basado en mensajes**. El ataque a la Cadena de Suministro se centra en vulnerar a un proveedor, y la Llamada de Voz es *Vishing*.

Pregunta 7: ¿Qué tipo de vulnerabilidad se presenta cuando un desarrollador no valida correctamente las entradas de los usuarios antes de ejecutar un comando, lo que permite la inyección de código malicioso en la aplicación web?

A. Vulnerabilidad de Hardware B. Vulnerabilidad de Sistema Operativo (OS) C. Vulnerabilidad de Aplicación Web D. Vulnerabilidad de Virtualización

Respuesta Correcta: C. Vulnerabilidad de Aplicación Web

Explicación: Las fallas de validación de entrada (como *Cross-Site Scripting* o Inyección SQL) son los defectos más comunes en el código de las **Aplicaciones Web**, lo que permite a los atacantes modificar el comportamiento de la aplicación a través del navegador.

Pregunta 8: ¿Qué tipo de ataque se basa en la interceptación y manipulación de la comunicación entre dos partes que creen estar comunicándose directamente entre sí?

A. Ataque de Denegación de Servicio (DoS) B. Ataque de *Man-in-the-Middle* (MITM) C. Ataque de *Birthday* D. Ataque de Fuerza Bruta

Respuesta Correcta: B. Ataque de *Man-in-the-Middle* (MITM)

Explicación: En un ataque **MITM**, el atacante se posiciona secretamente entre dos usuarios, interceptando y a menudo alterando el tráfico. El cifrado (TLS/SSL) es la principal defensa contra los MITM.

Pregunta 9: La práctica de desactivar servicios innecesarios, cerrar puertos sin usar y aplicar las configuraciones más seguras a un sistema operativo o servidor se conoce como:

A. Parcheo (*Patching*) B. Segmentación C. *Hardening* (Endurecimiento) D. Aislamiento

Respuesta Correcta: C. *Hardening* (Endurecimiento)

Explicación: El **Hardening** es un proceso de **Mitigación** centrado en reducir la superficie de ataque de un sistema mediante la eliminación de funciones innecesarias y la aplicación de configuraciones de seguridad muy estrictas (*secure baselines*).

Pregunta 10: ¿Qué modelo de arquitectura se utiliza para gestionar la infraestructura de IT (ej. servidores, redes, *load balancers*) utilizando archivos de definición legibles por máquina, aplicando las mismas prácticas de control de versiones que el código de *software*?

A. Internet de las Cosas (IoT) B. Sistemas de Control Industrial (ICS) C. Virtualización D. Infraestructura como Código (IaC)

Respuesta Correcta: D. Infraestructura como Código (IaC)

Explicación: **IaC** utiliza código (ej. Terraform o Ansible) para automatizar la gestión y el aprovisionamiento de la infraestructura, garantizando que la seguridad sea **consistente, rastreable y auditable**.

Pregunta 11: Al aplicar principios de seguridad a la infraestructura empresarial, ¿qué tecnología se utiliza para garantizar que un dispositivo que intenta acceder a la red (ej. un portátil) cumpla con una política de seguridad mínima (ej. tener antivirus actualizado) antes de que se le conceda el acceso?

A. VPN B. DNS Filtering C. NAC (*Network Access Control*) D. IDS/IPS

Respuesta Correcta: C. NAC (*Network Access Control*)

Explicación: **NAC** es un control de seguridad que comprueba el **estado de salud** de un *endpoint* antes de permitirle acceder a la red, aplicando políticas de seguridad para el cumplimiento (*compliance*) y la **higiene de seguridad**.

Pregunta 12: ¿Qué clasificación de datos requiere el más alto nivel de protección y restricción de acceso, ya que su divulgación causaría el daño más severo a la organización o a la nación?

A. Pública B. Confidencial C. Sensible D. Secreta/Clasificada

Respuesta Correcta: D. Secreta/Clasificada

Explicación: La clasificación **Secreta/Clasificada** (*Top Secret/Classified*) se utiliza para información cuya divulgación no autorizada podría causar un **daño excepcionalmente grave** o catastrófico, superando el impacto de la información Confidencial o Sensible.

Pregunta 13: ¿Qué estrategia de recuperación garantiza la **Disponibilidad** de un sistema al mantener un sitio secundario que se mantiene constantemente actualizado con el sitio primario, lo que permite un *failover* casi instantáneo?

A. *Hot Site* B. *Cold Site* C. *Warm Site* D. *Backup* (Copia de seguridad)

Respuesta Correcta: A. *Hot Site*

Explicación: Un **Hot Site** es un sitio de recuperación completamente equipado, duplicado en tiempo real o casi real (alta disponibilidad), que permite una conmutación por error con el **tiempo de inactividad más bajo posible**, en contraste con un *Cold Site* (básico) o *Warm Site* (parcialmente equipado).

Pregunta 14: ¿Qué práctica se aplica a los recursos informáticos para asegurar que todos los sistemas similares se configuren con la misma configuración mínima de seguridad aprobada por la organización?

A. Cifrado B. Sandboxing C. Aplicación de Líneas Base Seguras (*Secure Baselines*) D. *Patching*

Respuesta Correcta: C. Aplicación de Líneas Base Seguras (*Secure Baselines*)

Explicación: Las **Líneas Base Seguras** (*Secure Baselines*) son configuraciones mínimas estandarizadas y endurecidas que se aplican a todos los sistemas. Esto garantiza la **consistencia** en la seguridad y evita el "desvío de configuración" (*configuration drift*).

Pregunta 15: ¿Qué paso en el ciclo de vida de la Gestión de Activos es crucial para eliminar de forma segura los datos sensibles de un dispositivo de almacenamiento antes de que el *hardware* sea desechado o reutilizado?

A. Adquisición B. Asignación C. Monitoreo/Seguimiento D. Disposición

Respuesta Correcta: D. Disposición

Explicación: La **Disposición** es el proceso de retirar o desechar un activo. En este paso, las técnicas como la desmagnetización (*Degaussing*) o la destrucción física son obligatorias para garantizar que la información sensible no sea recuperable.

Pregunta 16: En la Gestión de Vulnerabilidades, una vez que se ha identificado y clasificado una vulnerabilidad, ¿qué paso se lleva a cabo para determinar el tiempo, los recursos y las acciones necesarias para corregir o mitigar la debilidad?

A. Identificación B. Validación C. Remediación D. Análisis

Respuesta Correcta: D. Análisis

Explicación: El **Análisis** de la vulnerabilidad ocurre después de la identificación y clasificación (ej. puntuación CVSS). En esta fase se evalúa el riesgo real, se determina la causa raíz y se planifican los pasos de **Remediación** (la acción de corregir).

Pregunta 17: ¿Qué herramienta de monitoreo se utiliza principalmente para recopilar, normalizar, correlacionar y analizar datos de registro (*logs*) de múltiples fuentes (sistemas operativos, *firewalls*, *routers*) para detectar incidentes de seguridad en tiempo real?

A. *Packet Capture* B. IDS (*Intrusion Detection System*) C. SIEM (*Security Information and Event Management*) D. EDR (*Endpoint Detection and Response*)

Respuesta Correcta: C. SIEM (*Security Information and Event Management*)

Explicación: El **SIEM** es la solución centralizada para la gestión de *logs* (información) y eventos. Su función de **correlación** permite identificar patrones de ataque que son invisibles para un solo dispositivo.

Pregunta 18: ¿Qué tecnología de seguridad de red inspecciona el contenido de los paquetes en busca de firmas de ataque conocidas o comportamientos anómalos y tiene la capacidad de bloquear o interrumpir activamente el tráfico malicioso?

A. *Firewall* de Filtrado de Paquetes B. IDS (*Intrusion Detection System*) C. IPS (*Intrusion Prevention System*) D. DLP (*Data Loss Prevention*)

Respuesta Correcta: C. IPS (*Intrusion Prevention System*)

Explicación: Un **IPS** es un control en línea (*in-line*) que puede prevenir o bloquear el ataque activamente (por eso se llama "Prevention System"). Un **IDS** solo detecta y alerta, mientras que un *Firewall* básico filtra por dirección y puerto, no por contenido malicioso.

Pregunta 19: ¿Qué solución de gestión de identidad se utiliza para obligar a los administradores y otros usuarios privilegiados a acceder a sus cuentas a través de una bóveda de contraseñas, lo que minimiza la exposición de credenciales de alto nivel?

A. SSO (*Single Sign-On*) B. MFA (*Multifactor Authentication*) C. PAM (*Privileged Access Management*) D. Provisioning

Respuesta Correcta: C. PAM (*Privileged Access Management*)

Explicación: **PAM** se enfoca específicamente en la protección y el monitoreo de cuentas con privilegios elevados (*root*, administrador), proporcionando controles más estrictos que el MFA o el SSO estándar, como el acceso a través de un *jump box* o la rotación automática de contraseñas.

Pregunta 20: ¿Qué beneficio principal se obtiene de la orquestación y automatización de seguridad, especialmente cuando se integra con el SIEM/XDR?

A. Reducción de la superficie de ataque del sistema operativo. B. Mejora significativa en el **Tiempo Medio de Respuesta** (*Mean Time To Respond - MTTR*). C. Disminución de los falsos negativos en la detección. D. Eliminación de la necesidad de *patching* de *firmware*.

Respuesta Correcta: B. Mejora significativa en el **Tiempo Medio de Respuesta** (*Mean Time To Respond - MTTR*).

Explicación: El objetivo primordial de la **Automatización** y **Orquestación** (SOAR) es reducir drásticamente el tiempo que transcurre entre la detección de una amenaza y el momento en que se contiene o se resuelve, mejorando directamente el MTTR.

Pregunta 21: ¿Qué fase del proceso de Respuesta a Incidentes se centra en la erradicación de la causa raíz de la intrusión (ej. cerrar el *exploit* o eliminar el código malicioso) antes de restaurar el sistema?

A. Contención B. Erradicación C. Recuperación D. Detección y Análisis

Respuesta Correcta: B. Erradicación

Explicación: La **Contención** (aislamiento) es lo primero para detener la propagación. La **Erradicación** es el paso donde se identifica y elimina la **causa raíz** del compromiso, asegurando que el atacante no pueda volver a entrar. La Recuperación viene después, cuando se restauran los sistemas limpios.

Pregunta 22: Un analista forense está investigando un incidente. ¿Qué fuente de datos debe priorizar por su volatilidad para su recopilación inmediata antes de que se pierda?

A. Contenido de RAM B. Contenido del disco duro C. Registros del *firewall* D. Copias de seguridad archivadas

Respuesta Correcta: A. Contenido de RAM

Explicación: El contenido de la **Memoria de Acceso Aleatorio (RAM)** es el más volátil, ya que se pierde inmediatamente si el dispositivo se apaga o se reinicia. El principio forense es recopilar la evidencia de la más volátil a la menos volátil.

Pregunta 23: ¿Qué documento de gobernanza de seguridad proporciona la guía de más alto nivel para toda la organización, estableciendo la postura de seguridad y el propósito del programa de seguridad?

A. Estándar B. Procedimiento C. Política D. Directiva

Respuesta Correcta: C. Política

Explicación: Una **Política** de seguridad es un documento de alto nivel y amplio que establece las reglas y la postura de seguridad de la organización. Los **Estándares** definen los requisitos técnicos para cumplir la política, y los **Procedimientos** son las instrucciones paso a paso.

Pregunta 24: ¿Qué documento de gestión de riesgos se utiliza para analizar y priorizar los procesos de negocio en función de la criticidad, el tiempo máximo de interrupción tolerable (MTD) y el impacto potencial, guiando así la inversión en continuidad?

A. Registro de Riesgos (*Risk Register*) B. Matriz de Controles C. Análisis de Impacto en el Negocio (BIA) D. Matriz de Evaluación de Proveedores

Respuesta Correcta: C. Análisis de Impacto en el Negocio (BIA)

Explicación: El **BIA** (*Business Impact Analysis*) es el proceso clave para determinar qué procesos de negocio son críticos, estimar el impacto financiero/operacional de su pérdida y definir el RTO y el RPO necesarios para los planes de recuperación.

Pregunta 25: En la Gestión de Riesgos, una empresa decide aceptar el riesgo de un ciberataque de baja probabilidad y bajo impacto, en lugar de gastar fondos en controles de mitigación. Esta estrategia se conoce como:

A. Transferencia B. Aceptación C. Elusión (*Avoidance*) D. Reducción

Respuesta Correcta: B. Aceptación

Explicación: La **Aceptación de Riesgos** ocurre cuando el costo de mitigar el riesgo es mayor que el impacto potencial del riesgo en sí, o cuando el riesgo se considera insignificante para las operaciones del negocio.

Pregunta 26: ¿Qué marco de cumplimiento se aplica a cualquier entidad global que procese datos personales de ciudadanos de la Unión Europea, independientemente de la ubicación de la entidad?

A. PCI DSS B. FISMA C. GDPR D. FERPA

Respuesta Correcta: C. GDPR

Explicación: El **GDPR** (*General Data Protection Regulation*) de la UE tiene un alcance extraterritorial, lo que significa que rige la privacidad y el manejo de datos personales de los ciudadanos de la UE por cualquier organización en el mundo.

Pregunta 27: ¿Qué tipo de evaluación de seguridad implica la simulación de un ataque real, incluyendo la explotación activa de vulnerabilidades para intentar obtener acceso no autorizado a los sistemas?

A. Auditoría Interna B. Pruebas de Penetración (*Penetration Testing*) C. Evaluación de Vulnerabilidades (*Vulnerability Scanning*) D. Evaluación de Controles

Respuesta Correcta: B. Pruebas de Penetración (*Penetration Testing*)

Explicación: El **Pentesting** va más allá de la mera detección de fallos (*Vulnerability Scanning*); de hecho, intenta **explotar** activamente esas vulnerabilidades para demostrar el impacto real en el negocio y probar la capacidad de defensa de la organización.

Pregunta 28: El objetivo principal de implementar un programa de concienciación de seguridad es mitigar el riesgo de ataques basados en:

A. Fallos de *firmware* B. Vulnerabilidades de la red C. Error humano y engaño (*Social Engineering*) D. Ataques criptográficos

Respuesta Correcta: C. Error humano y engaño (*Social Engineering*)

Explicación: La **Concienciación de Seguridad** busca educar a los usuarios para que sean la primera línea de defensa, reconociendo y reportando ataques de **Ingeniería Social** (como *phishing*), que explotan el error humano.

Pregunta 29: ¿Cuál de los siguientes es el proceso de crear, modificar y eliminar las identidades de usuario y sus derechos de acceso a través de las diferentes aplicaciones de la organización?

A. Autenticación B. Autorización C. *Provisioning* (Aprovisionamiento) D. *De-provisioning*

Respuesta Correcta: C. *Provisioning* (Aprovisionamiento)

Explicación: El ***Provisioning*** es el proceso automatizado de gestionar el ciclo de vida de una cuenta de usuario, asegurando que el acceso se otorgue correctamente al inicio y se revoque de manera oportuna (el *De-provisioning* es la parte de eliminación) a lo largo del tiempo. El proceso completo de Identity Lifecycle Management, donde “crear, modificar y eliminar identidades” abarca tanto provisioning como de-provisioning. Si la pregunta dice explícitamente “crear, modificar y eliminar”, una respuesta más precisa sería Gestión de Identidades (Identity and Access Management – IAM) o Ciclo de Vida de Identidades, pero Provisioning es aceptable si se interpreta como el conjunto.

Pregunta 30: ¿Qué tecnología unifica los datos de seguridad de *endpoints*, correo electrónico, *cloud* y red para proporcionar una detección y respuesta de incidentes más rápida y con mayor contexto?

A. SIEM (*Security Information and Event Management*) B. IPS (*Intrusion Prevention System*) C. XDR (*eXtended Detection and Response*) D. DLP (*Data Loss Prevention*)

Respuesta Correcta: C. XDR (*eXtended Detection and Response*)

Explicación: **XDR** es la evolución que extiende la visibilidad más allá del *endpoint* (EDR) para correlacionar eventos de seguridad de forma holística en toda la infraestructura, facilitando la **identificación de la cadena de ataque** completa.

¿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 © Pico 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 Pico 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 Pico 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. Pico 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, Pico 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, Pico 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

Este material de preparación no está afiliado, patrocinado ni autorizado por CompTIA. CompTIA® y Security+® son marcas registradas de Computing Technology Industry Association, Inc.

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 Pico Trainings.

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