examundo

Examen de práctica CISSP en español

50 preguntas con respuestas. Las guías y las traducciones las hizo y las revisó un software. Ninguna persona las ha revisado todavía.

Actualizado el 25 de noviembre de 2026 · examundo.tech/es/cissp/

Dominio 3: Arquitectura e ingeniería de seguridad

1. ¿Qué concepto criptográfico garantiza que el remitente no pueda negar haber enviado un mensaje?

Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. Confidencialidad
B. Integridad
C. No repudio
D. Autenticación

---

2. Un arquitecto de seguridad diseña un sistema para proteger datos gubernamentales clasificados. ¿Qué modelo de seguridad debe implementar para evitar que la información fluya de niveles de clasificación altos a niveles bajos?

A security architect is designing a system to protect classified government data. Which security model should be implemented to prevent information from flowing from higher classification levels to lower classification levels?

A. Modelo Bell-LaPadula
B. Modelo Clark-Wilson
C. Modelo Brewer-Nash
D. Modelo de integridad Biba

---

3. Una aplicación de comercio electrónico necesita intercambiar de forma segura claves de cifrado simétrico con los navegadores de los clientes. ¿Qué protocolo debe usar?

An e-commerce application needs to securely exchange symmetric encryption keys with customers' browsers. Which protocol should be used?

A. TLS con intercambio de claves Diffie-Hellman
B. IPsec en modo transporte con claves precompartidas
C. Kerberos con tickets de concesión de tickets (TGT)
D. S/MIME con cifrado basado en certificados

---

4. Una instalación segura exige integridad de dos personas (two-person integrity) para entrar a la sala de servidores. ¿Qué tipo de control de acceso físico cumple este requisito?

A secure facility requires two-person integrity for access to the server room. What type of physical access control implements this requirement?

A. Cerradura de código (cipher lock) con cambio trimestral del código
B. Lector de tarjetas con videovigilancia que graba todas las entradas
C. Lector biométrico con teclado PIN para autenticación multifactor
D. Esclusa de seguridad (mantrap) con doble autenticación que exige a dos personas autorizadas

---

5. ¿Cuál de los siguientes principios de seguridad describe MEJOR la defensa en profundidad (defense in depth)?

Defense in depth is BEST described as which of the following security principles?

A. Implementar varias capas de controles de seguridad para proteger los activos

B. Diseñar sistemas que fallen en un estado seguro cuando ocurren errores

C. Dar a los usuarios el acceso mínimo necesario para hacer su trabajo

D. Endurecer los sistemas quitando servicios y funciones innecesarios

---

6. ¿Qué tipo de control de seguridad física es una esclusa de seguridad (mantrap)?

A mantrap is classified as which type of physical security control?

A. Control preventivo

B. Control compensatorio

C. Control detectivo

D. Control correctivo

---

7. Un sistema financiero debe impedir que usuarios no autorizados modifiquen los registros de transacciones y, al mismo tiempo, permitir la lectura para auditoría. ¿Qué modelo de seguridad apoya MEJOR este requisito?

A financial system must prevent unauthorized users from modifying transaction records while allowing read access for auditing. Which security model BEST supports this requirement?

A. Modelo de confidencialidad Bell-LaPadula

B. Modelo Brewer-Nash (muralla china)

C. Modelo de integridad Biba

D. Modelo de control de acceso Graham-Denning

---

8. Una organización implementa un nuevo sistema criptográfico para proteger datos en reposo en la nube. El sistema debe cumplir los requisitos regulatorios de custodia de claves (key escrow) y mantener independencia operativa del proveedor de nube. ¿Qué enfoque cumple MEJOR ambos requisitos?

An organization is implementing a new cryptographic system to protect data at rest in a cloud environment. The system must support regulatory compliance requirements for key escrow while maintaining operational independence from the cloud provider. Which approach BEST satisfies both requirements?

A. Implementar cifrado del lado del cliente con claves administradas en un HSM local y dar copias en custodia a un servicio externo de key escrow

B. Implementar cifrado de sobre (envelope encryption) con claves administradas por el cliente y guardadas en el servicio de administración de claves del proveedor de nube

C. Implementar cifrado transparente de datos (TDE) en la capa de base de datos con las claves guardadas en la configuración de la aplicación

D. Usar el servicio de cifrado nativo del proveedor de nube con rotación automática de claves y respaldo en otra región de la nube

---

9. Un arquitecto de seguridad debe elegir un modelo de seguridad formal para un sistema de inteligencia militar que maneja documentos de varios niveles de clasificación. El requisito PRINCIPAL es impedir que la información fluya a niveles de clasificación más bajos. ¿Qué modelo es el MÁS adecuado?

A security architect must select a formal security model for a military intelligence system handling documents at multiple classification levels. The PRIMARY requirement is preventing information from flowing to lower classification levels. Which model is MOST appropriate?

A. Modelo de integridad Biba

B. Modelo de integridad Clark-Wilson

C. Modelo Bell-LaPadula

D. Modelo Brewer-Nash (muralla china)

---

10. En un centro de datos se rompe una tubería de agua sobre la sala de servidores. ¿Qué control ambiental habría evitado MEJOR el daño del agua a los equipos críticos?

A data center experiences a water pipe burst above the server room. Which environmental control would have BEST prevented water damage to critical equipment?

A. Sistemas de presión de aire positiva para evitar la entrada de humedad

B. Sensores de detección de agua con válvulas de cierre automático

C. Piso elevado para colocar los equipos por encima del nivel del suelo

D. Sistemas de climatización (HVAC) con monitoreo de humedad y alertas

---

Dominio 7: Operaciones de seguridad

11. ¿Qué práctica de administración de configuración (configuration management) detecta MEJOR los cambios no autorizados en las configuraciones de servidores de producción?

Which configuration management practice BEST detects unauthorized changes to production server configurations?

A. Comparar con regularidad las configuraciones reales con las líneas base aprobadas

B. Aprobar automáticamente los cambios hechos por administradores con privilegios

C. Revisar los registros de compra de hardware sin examinar la configuración de los servidores

D. Reemplazar las líneas base aprobadas por las configuraciones actuales después de cada escaneo

12. ¿Qué rol de un equipo de respuesta a incidentes es responsable de identificar y contener el incidente en un primer momento?

Which role in an incident response team is responsible for initially identifying and containing the incident?

A. Coordinador del incidente

B. Analista forense

C. Primer respondiente

D. Responsable de comunicaciones

13. ¿En qué nivel de gravedad se clasifica normalmente un incidente que causa una interrupción menor en sistemas no críticos, sin pérdida de datos?

An incident that causes minor disruption to non-critical systems with no data loss would typically be classified as what severity level?

A. Crítico

B. Alto

C. Bajo

D. Emergencia

14. En una revisión posterior a un incidente, el equipo descubre que el atacante mantuvo persistencia durante 87 días antes de ser detectado. ¿Qué mejora de operaciones de seguridad reduciría MÁS eficazmente el tiempo de permanencia (dwell time) en el futuro?

During a post-incident review, the team identifies that the attacker maintained persistence for 87 days before detection. Which security operations improvement would MOST effectively reduce future dwell time?

A. Exigir capacitación obligatoria de concientización en seguridad para todos los empleados cada trimestre

B. Instalar más firewalls en los límites de segmentación de red

C. Aumentar la frecuencia de los escaneos de vulnerabilidades de mensual a semanal

D. Implementar monitoreo continuo de seguridad con analítica de comportamiento y búsqueda de amenazas

15. La defensa en profundidad en seguridad física suele incluir varias capas. ¿Cuál es el orden CORRECTO, de la capa más externa a la más interna?

Defense in depth for physical security typically includes multiple layers. Which of the following represents the CORRECT order from outermost to innermost layer?

A. Cercado perimetral, control de acceso al edificio, control de acceso a la sala, candados en los equipos

B. Candados en los equipos, control de acceso a la sala, control de acceso al edificio, cercado perimetral

C. Control de acceso a la sala, candados en los equipos, cercado perimetral, control de acceso al edificio

D. Control de acceso al edificio, cercado perimetral, candados en los equipos, control de acceso a la sala

---

16. ¿Qué tipo de evidencia consiste en copias o reproducciones de la evidencia original?

Which type of evidence consists of copies or reproductions of original evidence?

A. Evidencia secundaria

B. Mejor evidencia (best evidence)

C. Evidencia de oídas (hearsay)

D. Evidencia corroborante

---

17. Una organización define sus objetivos de recuperación ante desastres. El negocio exige que los sistemas críticos se restauren dentro de las 4 horas posteriores a un desastre. ¿Qué métrica de recuperación define este requisito?

An organization is defining its disaster recovery objectives. The business requires that critical systems must be restored within 4 hours of a disaster. This requirement defines which recovery metric?

A. Tiempo medio de reparación (MTTR)

B. Tiempo máximo tolerable de inactividad (MTD)

C. Objetivo de tiempo de recuperación (RTO)

D. Objetivo de punto de recuperación (RPO)

---

18. El plan de recuperación ante desastres de una organización exige un objetivo de tiempo de recuperación (RTO) de 4 horas y un objetivo de punto de recuperación (RPO) de 1 hora para su base de datos de clientes. ¿Qué estrategia de respaldo cumple MEJOR estos requisitos?

An organization's disaster recovery plan requires a recovery time objective (RTO) of 4 hours and a recovery point objective (RPO) of 1 hour for its customer database. Which backup strategy BEST meets these requirements?

A. Respaldos diferenciales cada 4 horas almacenados en el sitio

B. Respaldos incrementales cada 6 horas con almacenamiento en cinta fuera del sitio

C. Respaldos completos semanales con respaldos incrementales diarios

D. Respaldos completos cada noche con replicación continua de la base de datos a un sitio tibio

---

19. Un primer respondiente llega a un servidor de producción comprometido que sigue encendido y procesando transacciones. Según la guía RFC 3227, ¿qué fuente de datos se debe recolectar PRIMERO durante la adquisición de evidencia en vivo?

A first responder arrives at a compromised production server that is still powered on and actively processing transactions. Per RFC 3227 guidelines, which data source should be collected FIRST during live evidence acquisition?

A. Registros de la CPU y memoria caché

B. Contenido de la RAM del sistema (memoria principal)

C. Caché ARP y entradas de la tabla de enrutamiento

D. Sistema de archivos temporal y datos del espacio de intercambio (swap)

---

20. Un departamento de TI sigue un proceso formal de administración de cambios. ¿Qué paso de autorización debe ocurrir ANTES de implementar un cambio en los sistemas de producción?

An IT department follows a formal change management process. Which authorization step should occur BEFORE implementing a change to production systems?

A. Probar el cambio en un entorno que no sea de producción
B. Aprobación del Comité Asesor de Cambios (CAB)
C. Documentar el cambio en la base de datos de administración de configuración (CMDB)
D. Comunicar el cambio a todas las partes interesadas afectadas

---

Dominio 4: Seguridad de comunicaciones y redes

21. Una organización implementa 802.1X para el control de acceso a la red. ¿Qué componente actúa como intermediario entre el suplicante (supplicant) y el servidor de autenticación?

An organization implements 802.1X for network access control. Which component acts as the intermediary between the supplicant and the authentication server?

A. Autoridad de certificación
B. Controlador de red
C. Autenticador
D. Proxy RADIUS

---

22. Una organización implementa WPA3-Enterprise para su seguridad inalámbrica. ¿Qué marco de autenticación usa WPA3-Enterprise?

An organization implements WPA3-Enterprise for wireless security. What authentication framework does WPA3-Enterprise use?

A. 802.1X con EAP
B. Filtrado de direcciones MAC
C. Clave precompartida (PSK)
D. LEAP

---

23. Una organización necesita dar acceso remoto seguro a personal de campo que se conecta desde varios países con una conexión a internet poco confiable. La solución debe admitir tráfico TCP y UDP y funcionar a través de la mayoría de los firewalls. ¿Qué protocolo de VPN es el MÁS adecuado?

An organization needs to provide secure remote access for field personnel who connect from various international locations with unreliable internet connectivity. The solution must support both TCP and UDP traffic and work through most firewalls. Which VPN protocol is MOST appropriate?

A. PPTP
B. VPN SSL/TLS
C. L2TP/IPsec
D. IPsec en modo túnel

---

24. La aplicación web de una empresa recibe un aumento repentino de tráfico desde muchas fuentes que satura la capacidad del servidor para responder. ¿Qué ataque es el MÁS probable?

A company's web application experiences a surge in traffic from multiple sources, overwhelming the server's ability to respond. Which attack is MOST likely occurring?

A. Hombre en el medio (Man-in-the-Middle, MitM)
B. Falsificación de solicitudes entre sitios (CSRF)
C. Secuestro de sesión (session hijacking)
D. Denegación de servicio distribuida (DDoS)

---

25. ¿Qué capa del modelo OSI es responsable de la entrega confiable de datos de extremo a extremo, el control de flujo y la recuperación de errores entre los hosts que se comunican?

Which OSI model layer is responsible for end-to-end reliable data delivery, flow control, and error recovery between communicating hosts?

A. Capa 2: Enlace de datos
B. Capa 4: Transporte
C. Capa 3: Red
D. Capa 5: Sesión

---

26. Una organización sufre ataques de inundación SYN (SYN flood) contra su servidor web. ¿Qué técnica de defensa sería la MÁS eficaz?

An organization is experiencing SYN flood attacks against its web server. Which defensive technique would be MOST effective?

A. Desactivar las marcas de tiempo (timestamps) de TCP
B. Implementar filtrado de direcciones MAC
C. Limitar la tasa de paquetes ICMP
D. Cookies SYN (SYN cookies)

---

27. Al implementar TLS en una aplicación web, ¿qué versión debe considerarse el estándar MÍNIMO aceptable para nuevas implementaciones?

When implementing TLS for a web application, which version should be considered the MINIMUM acceptable standard for new deployments?

A. TLS 1.0
B. SSL 3.0
C. TLS 1.2
D. TLS 1.1

---

28. Una institución financiera exige autenticación mutua entre clientes y servidores. ¿Qué función de TLS ofrece esta capacidad?

A financial institution requires mutual authentication between clients and servers. Which TLS feature provides this capability?

A. Reanudación de sesión (session resumption)
B. Autenticación con certificado de cliente
C. Confidencialidad directa perfecta (Perfect Forward Secrecy, PFS)
D. Indicación de nombre de servidor (Server Name Indication, SNI)

---

29. Un sistema de detección de intrusiones (IDS) genera muchas alertas por patrones de tráfico normales. ¿Qué tipo de error ocurre?

An intrusion detection system (IDS) is generating numerous alerts for normal traffic patterns. What type of error is occurring?

A. Falso positivo
B. Falso negativo
C. Verdadero negativo
D. Verdadero positivo

---

30. Una corporación multinacional sufre interrupciones de enrutamiento en internet. La investigación revela que un ISP extranjero anuncia por BGP el espacio de direcciones IP de la empresa. ¿Qué ataque es el MÁS probable y cuál es la diferencia PRINCIPAL con el envenenamiento de rutas (route poisoning)?

A multinational corporation experiences Internet routing disruptions. Investigation reveals that a foreign ISP is advertising the company's IP address space via BGP. Which attack is MOST likely occurring, and what is the PRIMARY difference from route poisoning?

A. Secuestro de BGP (BGP hijacking); apunta a la propiedad del prefijo y no a las métricas de la ruta

B. Envenenamiento de rutas; afecta el enrutamiento externo y no los protocolos internos de vector de distancia

C. Oscilación de rutas (route flapping); causa interrupciones intermitentes y no una redirección persistente del tráfico

D. Anteposición de AS path (AS path prepending); manipula los números de sistema autónomo para influir en las decisiones de enrutamiento

---

Dominio 2: Seguridad de activos

31. La línea base de seguridad (baseline) de una empresa de servicios financieros exige cifrado AES-256 para todos los datos de clientes. Una evaluación de riesgos revela que ciertos sistemas heredados no admiten AES-256. ¿Qué proceso debe aplicar el arquitecto de seguridad para resolver esta limitación?

A financial services firm's baseline security standard requires AES-256 encryption for all customer data. A risk assessment reveals that certain legacy systems cannot support AES-256. What process should the security architect apply to address this constraint?

A. Adaptación (tailoring)

B. Controles compensatorios

C. Delimitación del alcance (scoping)

D. Aceptación del riesgo

32. Según la política de clasificación del gobierno de EE. UU., ¿qué etiqueta se aplica a la información cuya divulgación no autorizada se podría esperar razonablemente que cause 'daño grave' (serious damage) a la seguridad nacional?

Under U.S. government classification policy, which label applies to information whose unauthorized disclosure could reasonably be expected to cause 'serious damage' to national security?

A. Secreto (Secret)

B. Información no clasificada controlada (CUI)

C. Confidencial (Confidential)

D. Alto secreto (Top Secret)

33. ¿Quién es el responsable final de determinar el nivel de clasificación de los datos dentro de una organización?

Who is ultimately responsible for determining the classification level of data within an organization?

A. Custodio de los datos (data custodian)

B. Propietario de los datos (data owner)

C. Administrador de seguridad

D. Director de seguridad de la información (CISO)

34. Una organización debe conservar cierta documentación de cumplimiento de HIPAA por un mínimo de 6 años según HIPAA y un mínimo de 10 años según una ley estatal aplicable. ¿Qué período de retención debe recomendar el gerente de seguridad para esa documentación?

An organization must retain certain HIPAA compliance documentation for a minimum of 6 years under HIPAA and a minimum of 10 years under an applicable state law. What retention period should the security manager recommend for that documentation?

A. 8 años, como punto medio entre los requisitos
B. 10 años, para cumplir el requisito más estricto
C. Retención indefinida para evitar riesgos de cumplimiento
D. 6 años, para cumplir el requisito federal de HIPAA

---

35. Una corporación multinacional guarda datos de clientes de la UE en centros de datos en la nube. Los clientes franceses temen que entidades de fuera de la UE puedan obligar legalmente a entregar sus datos. ¿Qué principio atiende MEJOR esta preocupación?

A multinational corporation stores EU customer data in cloud data centers. French customers are concerned about their data being legally compelled from non-EU entities. Which principle BEST addresses this concern?

A. Soberanía de los datos (data sovereignty)
B. Localización de datos (data localization)
C. Redundancia geográfica
D. Residencia de datos (data residency)

---

36. La política de retención de datos de una organización exige conservar los registros de transacciones de clientes durante siete años. Al terminar ese período, ¿cuál es el PRIMER paso del proceso de eliminación?

An organization's data retention policy requires keeping customer transaction records for seven years. At the end of this period, what is the FIRST step in the disposal process?

A. Verificar que no se aplique ninguna retención legal
B. Sobrescribir los datos con una herramienta compatible con DoD 5220.22-M
C. Destruir físicamente todos los medios de almacenamiento que contienen los datos
D. Eliminar todas las copias de respaldo del almacenamiento fuera del sitio

---

37. ¿Qué rol es el responsable PRINCIPAL de determinar el nivel de clasificación asignado a un activo de datos de la organización?

Which role is PRIMARILY responsible for determining the classification level assigned to an organizational data asset?

A. Administrador de datos (data steward)
B. Propietario de los datos (data owner)
C. Custodio de los datos (data custodian)
D. Procesador de datos (data processor)

---

38. Una organización de salud da de baja laptops que guardaban historiales médicos de pacientes sin cifrar. ¿Qué método de sanitización da la MAYOR garantía de que los datos no se puedan recuperar?

A healthcare organization is decommissioning laptops that stored unencrypted patient health records. Which sanitization method provides the HIGHEST assurance of data irrecoverability?

A. Destrucción física mediante trituración o incineración
B. Borrado criptográfico de las claves de cifrado
C. Sobrescritura de siete pasadas con datos aleatorios
D. Desmagnetización (degaussing) con un desmagnetizador Tipo I o Tipo II

---

39. Una organización clasifica una nueva base de datos con evaluaciones de desempeño, información salarial e información de identificación personal (PII) de empleados. La divulgación no autorizada podría causar desventaja competitiva y responsabilidad legal. ¿Qué nivel de clasificación es el MÁS adecuado?

An organization is classifying a new database containing employee performance reviews, salary information, and personally identifiable information (PII). The unauthorized disclosure could result in competitive disadvantage and potential legal liability. What classification level is MOST appropriate?

A. Secreto
B. Confidencial
C. Solo uso interno
D. Público

---

40. Una organización de salud debe determinar quién responde por que los historiales de los pacientes se clasifiquen bien, se conserven según los requisitos regulatorios y solo los vea personal autorizado. ¿Quién tiene la responsabilidad PRINCIPAL de estas decisiones?

A healthcare organization must determine accountability for ensuring patient health records are properly classified, retained according to regulatory requirements, and accessible only to authorized personnel. Who has PRIMARY responsibility for these decisions?

A. Procesador de datos
B. Director de seguridad de la información (CISO)
C. Propietario de los datos
D. Custodio de los datos

Dominio 1: Seguridad y gestión de riesgos

41. Un analista de seguridad descubre que un empleado ha accedido a archivos confidenciales de recursos humanos sin justificación de negocio. El rol del empleado no requiere acceso a datos de RR. HH. ¿Qué principio de seguridad se violó con MÁS probabilidad?

A security analyst discovers an employee has been accessing confidential HR files without business justification. The employee's role does not require access to HR data. Which security principle was MOST likely violated?

A. Necesidad de saber (need-to-know)
B. Defensa en profundidad
C. Separación de funciones (separation of duties)
D. Privilegio mínimo (least privilege)

---

42. El CISO de una organización quiere alinear el programa de seguridad con los objetivos del negocio. ¿Qué marco es el MÁS adecuado para este propósito?

An organization's CISO wants to align the security program with business objectives. Which framework is BEST suited for this purpose?

A. ISO 27002
B. COBIT
C. CIS Controls
D. NIST SP 800-53

---

43. Una organización de salud sufre un ataque de ransomware que cifra los historiales de pacientes. El CISO informa del incidente a la junta directiva. ¿Qué concepto demuestra el CISO?

A healthcare organization suffers a ransomware attack that encrypts patient records. The CISO reports the incident to the board. Which concept is the CISO demonstrating?

A. Debida diligencia (due diligence)
B. Separación de funciones
C. Regla del hombre prudente (prudent man rule)
D. Debido cuidado (due care)

---

44. Un CISO explica a la junta directiva la relación entre la planificación de continuidad del negocio (BCP) y la planificación de recuperación ante desastres (DRP). ¿Qué afirmación es la MÁS precisa?

A CISO is explaining the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) to the executive board. Which statement is MOST accurate?

A. El BCP solo abarca los sistemas y datos de TI, y el DRP cubre todas las operaciones del negocio

B. BCP y DRP son términos intercambiables para el mismo proceso de planificación

C. El DRP es el plan estratégico más amplio que contiene al BCP como componente

D. El BCP es el plan estratégico más amplio, y el DRP es un subconjunto táctico enfocado en la recuperación de TI

---

45. Durante un ejercicio de recuperación ante desastres se descubre que las cintas de respaldo no se pueden leer. ¿Qué fase del ciclo de vida de BCP/DRP se descuidó con MÁS probabilidad?

During a disaster recovery exercise, the backup tapes are found to be unreadable. Which phase of the BCP/DRP lifecycle was MOST likely neglected?

A. Evaluación de riesgos

B. Análisis de impacto al negocio (BIA)

C. Desarrollo del plan

D. Pruebas y ejercicios

---

46. Un analista de riesgos determina que un servidor de archivos tiene una probabilidad anual del 20% de ser comprometido por ransomware, con una pérdida estimada de $50,000 por incidente. ¿Cuál es la expectativa de pérdida anualizada (ALE)?

A risk analyst determines that a file server has a 20% annual probability of being compromised by ransomware, with an estimated loss of $50,000 per incident. What is the Annualized Loss Expectancy (ALE)?

A. $10,000

B. $50,000

C. $40,000

D. $250,000

---

47. El equipo de seguridad de una organización está redactando una nueva política de control de acceso. ¿Qué tipo de documento debe ser el MÁS restrictivo y dar acciones obligatorias específicas?

An organization's security team is developing a new access control policy. Which document type should be MOST restrictive and provide specific mandatory actions?

A. Procedimiento

B. Estándar

C. Guía

D. Política

---

48. Una empresa implementa los principios de Privacidad desde el Diseño (Privacy by Design) para una nueva plataforma de datos de clientes. ¿Qué enfoque demuestra MEJOR este principio?

A company is implementing Privacy by Design principles for a new customer data platform. Which approach BEST demonstrates this principle?

A. Agregar cifrado y controles de acceso para proteger los datos de los clientes antes del despliegue en producción

B. Incorporar controles de privacidad en la arquitectura del sistema desde el diseño inicial, con minimización de datos y configuraciones de privacidad predeterminadas

C. Capacitar a los desarrolladores en requisitos de privacidad y hacer revisiones de código para verificar el cumplimiento

D. Hacer una evaluación de impacto de privacidad después del desarrollo del sistema para identificar y corregir riesgos

---

49. Una empresa quiere transferir el riesgo financiero asociado con una brecha de datos. ¿Qué estrategia está usando?

A company wants to transfer financial risk associated with a data breach. Which strategy is being employed?

A. Mitigación del riesgo
B. Transferencia del riesgo
C. Aceptación del riesgo
D. Evitación del riesgo

---

50. Durante un incidente de seguridad con acceso no autorizado a sistemas financieros, ¿qué rol es el responsable PRINCIPAL de determinar si se debe notificar a las fuerzas del orden (law enforcement)?

During a security incident involving unauthorized access to financial systems, which role is PRIMARILY responsible for determining whether law enforcement should be notified?

A. El líder del equipo de respuesta a incidentes, porque tiene la información más actualizada del incidente
B. El director de seguridad de la información (CISO), porque es responsable de todos los asuntos de seguridad
C. La alta dirección o el asesor legal, porque es una decisión de negocio y legal con implicaciones regulatorias
D. El enlace con las fuerzas del orden, porque mantiene la relación con las agencias externas

---

Respuesta correcta

1. C El no repudio (non-repudiation) impide que alguien niegue una acción y normalmente se logra con firmas digitales. La clave privada del remitente crea la firma y su clave pública la verifica, lo que prueba el origen. La autenticación confirma la identidad, pero no siempre da una prueba que nadie pueda negar. La confidencialidad protege contra la divulgación. La integridad muestra que los datos no se alteraron, pero no prueba quién los creó.

2. A Bell-LaPadula protege la confidencialidad con la propiedad simple (no leer hacia arriba) y la propiedad * (no escribir hacia abajo). Así la información no se filtra de un nivel alto a uno bajo. Biba y Clark-Wilson se enfocan en la integridad. Brewer-Nash (muralla china, Chinese Wall) evita conflictos de interés en el entorno comercial.

3. A TLS con Diffie-Hellman permite que dos partes creen un secreto compartido en un canal inseguro, como en HTTPS. Las variantes efímeras (DHE/ECDHE) dan confidencialidad directa perfecta (perfect forward secrecy). IPsec se usa sobre todo en VPN y requiere configuración previa. S/MIME es para correo y Kerberos necesita un KDC y confianza previa, así que no sirven para clientes públicos.

4. D La integridad de dos personas exige que dos personas autorizadas estén presentes para entrar, de modo que nadie actúe solo. La esclusa de seguridad (mantrap) con doble autenticación obliga a que ambas se autentiquen. El biométrico con PIN es multifactor para una sola persona. La videovigilancia solo detecta, y con una cerradura de código cualquiera que sepa el código entra solo.

5. A La defensa en profundidad (también llamada seguridad por capas) usa varias capas independientes de controles, de modo que si una falla, las demás siguen protegiendo. Por ejemplo: firewalls, IDS/IPS, controles de acceso, cifrado y barreras físicas. Quitar servicios es endurecimiento (hardening), dar el acceso mínimo es el privilegio mínimo (least privilege) y fallar de forma segura es diseño fail-safe o fail-secure.

6. A Una esclusa de seguridad (mantrap, también llamada vestíbulo de control de acceso) es un control preventivo. Exige autenticarse en dos puertas sucesivas y solo una está abierta a la vez, lo que frena el acceso no autorizado antes de que ocurra. Los controles detectivos identifican incidentes después (CCTV, sensores) y los correctivos reparan el daño. Los compensatorios sustituyen a un control principal que no está disponible.

7. C Biba protege la integridad con “no escribir hacia arriba” (los sujetos de baja integridad no pueden dañar objetos de alta integridad) y “no leer hacia abajo”. Así se evita la modificación no autorizada de los registros. Bell-LaPadula trata la confidencialidad, Brewer-Nash los conflictos de interés y Graham-Denning no se centra en la integridad. El requisito habla de impedir modificaciones, o sea integridad.

8. A El cifrado del lado del cliente con claves en un HSM local da independencia del proveedor, y un tercero puede guardar copias de las claves para cumplir la norma. El servicio nativo de la nube crea dependencia del proveedor. El cifrado de sobre con claves en la nube sigue atando el acceso a las claves al proveedor. TDE con claves en la configuración de la aplicación no las protege bien ni resuelve la custodia.

9. C Bell-LaPadula aplica control de acceso obligatorio para la confidencialidad con dos reglas: la propiedad simple (no leer hacia arriba) y la propiedad * (no escribir hacia abajo). Impide el flujo de información de niveles altos a bajos, justo lo que se pide. Biba y Clark-Wilson tratan la integridad. Brewer-Nash restringe el acceso entre empresas competidoras y no controla el flujo por clasificación.

10. B Los sensores de detección de agua con válvulas de cierre automático detectan la fuga, activan alarmas y cortan el suministro, lo que limita el daño. El sensor es detectivo y el cierre automático es correctivo. El piso elevado ayuda con inundaciones desde abajo, no con una tubería que se rompe arriba. La presión positiva y el monitoreo de humedad no detienen el agua de una tubería rota.

11. A Comparar con regularidad las configuraciones reales con las líneas base aprobadas (baselines) detecta la desviación de configuración (configuration drift) y permite investigar cambios sin autorización. Aprobar automáticamente los cambios de administradores se salta la autorización. Reemplazar las líneas base tras cada escaneo normaliza cambios no autorizados. Las compras de hardware no muestran cambios en los servidores.

12. C El primer respondiente (first responder) es el primer punto de contacto: identifica el incidente y toma medidas inmediatas de contención para evitar más daño. El coordinador dirige el proceso general de respuesta. El analista forense reúne y analiza la evidencia. El responsable de comunicaciones maneja los mensajes internos y externos sobre el incidente.

13. C Un incidente de gravedad baja implica interrupciones menores en sistemas no críticos, sin pérdida de datos ni impacto importante en el negocio. Los incidentes críticos afectan operaciones centrales o implican brechas de datos. Los de gravedad alta afectan sistemas importantes, pero no vitales. El nivel de emergencia es para amenazas inmediatas a la vida, a la seguridad de las personas o a la infraestructura crítica.

14. D El tiempo de permanencia (dwell time) se reduce con detección activa, no solo con controles preventivos. La analítica de comportamiento y la búsqueda de amenazas (threat hunting) encuentran actividad anómala que indica un compromiso. Los escaneos buscan debilidades, no amenazas activas. La capacitación y los firewalls previenen, pero no detectan lo que ya está dentro. El monitoreo continuo reduce el tiempo medio de detección (MTTD).

15. A La defensa en profundidad física va de afuera hacia adentro: controles del perímetro (cercas, portones, guardias), controles de entrada al edificio (lectores de credenciales, recepción), controles de las salas (sala de servidores) y, al final, controles del activo (gabinetes con llave, candados de cable). Así el atacante debe superar varias barreras. Las demás opciones tienen un orden incorrecto.

16. A La evidencia secundaria incluye copias, fotografías o reproducciones del original, y en un tribunal se prefiere menos que la mejor evidencia (best evidence), que es el original. La evidencia corroborante apoya o confirma otra evidencia, pero no tiene que ser una copia. La evidencia de oídas (hearsay) es el testimonio de lo que dijo otra persona y normalmente no se admite.

17. C El objetivo de tiempo de recuperación (Recovery Time Objective, RTO) es el tiempo meta para restaurar un sistema o proceso tras una interrupción. Las 4 horas son un RTO típico. El RPO es la pérdida de datos aceptable medida en tiempo. El MTD es la interrupción máxima que el negocio tolera, y el RTO debe caber dentro de él. El MTTR es una métrica operativa del tiempo promedio de reparación.

18. D El RTO (4 horas) es el tiempo de inactividad aceptable y el RPO (1 hora) es la pérdida de datos aceptable. La replicación continua puede cumplir el RPO de 1 hora, y un sitio tibio (warm site) bien preparado y probado puede cumplir el RTO de 4 horas. Los respaldos cada 4 o 6 horas incumplen el RPO (guardarlos solo en el sitio crea además un punto único de falla), y los semanales o diarios pierden hasta 24 horas de datos. Hay que probar que la activación cumpla el RTO.

19. A RFC 3227 da un orden de volatilidad que empieza con registros y caché. Sigue un grupo con tablas de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel y memoria. Después vienen los archivos temporales, el disco, los registros remotos, la configuración física y la topología de red, y los medios de archivo. Entre las opciones, los registros de la CPU y la caché van primero. La RAM y la caché ARP están en el mismo grupo.

20. B La aprobación del Comité Asesor de Cambios (Change Advisory Board, CAB) es el paso de autorización que debe darse antes de implementar. Evalúa el riesgo del cambio y su alineación con el negocio. Probar el cambio y avisar a los afectados también suelen hacerse antes, pero no autorizan nada. La CMDB se actualiza después para reflejar el estado ya implementado.

21. C En 802.1X, el autenticador (authenticator), normalmente un switch o punto de acceso inalámbrico, es el intermediario. Reenvía las solicitudes del suplicante (el dispositivo cliente) al servidor de autenticación, casi siempre con RADIUS, y aplica la decisión del servidor. Un proxy RADIUS puede estar en la ruta, pero no es el intermediario definido. La autoridad de certificación emite certificados y el controlador de red no es un componente estándar de 802.1X.

22. A WPA3-Enterprise usa 802.1X con el Protocolo de Autenticación Extensible (EAP) para autenticar a cada usuario contra un servidor RADIUS con credenciales individuales. WPA3-Personal, en cambio, usa SAE (autenticación simultánea de iguales). Las claves precompartidas son del modo Personal. El filtrado MAC es débil porque las direcciones se falsifican fácilmente, y LEAP es un protocolo de Cisco obsoleto y vulnerable que no es parte de WPA3.

23. B La VPN SSL/TLS es la mejor opción porque puede usar el puerto TCP 443, que casi siempre atraviesa firewalls y NAT. Sus túneles pueden llevar tráfico TCP y UDP, y muchas usan un canal de datos UDP con respaldo en TCP. IPsec en modo túnel y L2TP/IPsec dependen de que se permita el tráfico IPsec (por ejemplo UDP 500 y 4500), que los firewalls restrictivos pueden bloquear. PPTP tiene vulnerabilidades conocidas.

24. D Un ataque DDoS usa muchas fuentes distribuidas para inundar el objetivo con tráfico, agotar sus recursos y negar el servicio a usuarios legítimos. Las pistas son el aumento de tráfico desde varias fuentes y el agotamiento de recursos. El MitM intercepta la comunicación sin inundarla. El secuestro de sesión y el CSRF abusan de sesiones autenticadas y no generan picos de tráfico.

25. B La capa de Transporte (capa 4) da servicios de comunicación de extremo a extremo. TCP logra la confiabilidad con secuenciación, confirmaciones, retransmisión de segmentos perdidos y control de flujo con ventanas deslizantes. UDP, en la misma capa, ofrece entrega sin conexión y sin garantías. Enlace de datos entrega entre nodos con direcciones MAC, Red enruta entre redes con IP y Sesión controla el diálogo entre aplicaciones.

26. D Las cookies SYN evitan que el servidor reserve recursos durante la negociación TCP (handshake) hasta verificar la conexión, lo que elimina el agotamiento de estado. El servidor codifica los datos de la conexión en el número de secuencia en lugar de guardar conexiones semiabiertas. Limitar ICMP combate otro vector. El filtrado MAC es de capa 2 y no sirve contra ataques de capa 4 desde internet. Quitar las marcas de tiempo no frena el agotamiento de recursos.

27. C TLS 1.2 es la versión mínima aceptable para nuevas implementaciones según estándares de NIST y PCI DSS. Ofrece conjuntos de cifrado fuertes, soporte obligatorio de SHA-256 y protección contra ataques conocidos. TLS 1.0 y 1.1 están en desuso por sus vulnerabilidades. SSL 3.0 tiene fallas críticas (ataque POODLE) y nunca debe usarse. TLS 1.3 mejora más, pero TLS 1.2 sigue siendo la base mínima.

28. B La autenticación con certificado de cliente exige que el cliente presente un certificado X.509 durante la negociación TLS (handshake). Así ambas partes verifican la identidad de la otra (autenticación mutua). El TLS estándar solo autentica al servidor. SNI permite alojar varios sitios TLS en una IP, pero no cambia quién se autentica. La reanudación acelera reconexiones y PFS protege las claves de sesión, pero ninguna da autenticación mutua.

29. A Un falso positivo ocurre cuando el IDS identifica por error tráfico legítimo como malicioso y alerta sobre actividad normal. Esto causa fatiga de alertas y hace perder tiempo a los analistas. Un falso negativo es tráfico malicioso que pasa sin detectar. Un verdadero positivo detecta un ataque real y un verdadero negativo no alerta ante tráfico legítimo. Los falsos positivos se corrigen ajustando firmas, umbrales o listas blancas.

30. A En el secuestro de BGP (BGP hijacking), un sistema autónomo (AS) no autorizado anuncia prefijos que no le pertenecen y otros AS envían el tráfico hacia el atacante. El envenenamiento de rutas es una técnica legítima de convergencia en protocolos de vector de distancia como RIP, que anuncia una métrica infinita para quitar una ruta caída. La anteposición de AS path es ingeniería de tráfico legítima y la oscilación de rutas es inestabilidad, no redirección deliberada.

31. A La adaptación (tailoring) ajusta los controles de una línea base a los límites de la organización y sus sistemas, justo lo que hace falta cuando un control no puede implementarse como está escrito. La delimitación (scoping) define a qué sistemas se aplica la línea base, no cómo adaptarla. Los controles compensatorios pueden elegirse como parte de la adaptación. La aceptación del riesgo exige autorizar el riesgo residual y no sustituye los requisitos aplicables.

32. A La Orden Ejecutiva 13526 define tres niveles de información clasificada. Secreto (Secret) se aplica cuando la divulgación podría causar “daño grave” a la seguridad nacional. Alto secreto (Top Secret) es para daño “excepcionalmente grave” (exceptionally grave) y Confidencial (Confidential) para “daño” sin el calificativo “grave”. La CUI no es un nivel clasificado, sino una categoría aparte para información sensible no clasificada. El orden ascendente es Confidential, Secret, Top Secret.

33. B El propietario de los datos (data owner), normalmente un gerente o ejecutivo de negocio, es el responsable final de definir la clasificación porque conoce el valor y la sensibilidad de los datos y acepta el riesgo. Los custodios aplican los controles técnicos, pero no definen la clasificación. Los administradores de seguridad hacen cumplir políticas ajenas. El CISO define el marco y la política general, pero no clasifica cada activo de datos.

34. B Conservar la documentación 10 años cumple el requisito más estricto y también los dos mínimos aplicables. El requisito estatal de 10 años no reemplaza la obligación federal, pero 10 años satisface ambas. Con 6 años se violaría la ley estatal y con 8 años tampoco se cumpliría. La retención indefinida es innecesaria, cara y crea riesgos de privacidad por guardar datos más tiempo del exigido.

35. A La soberanía de los datos significa que los datos están sujetos a las leyes y la jurisdicción del país donde se encuentran, incluidos los gobiernos que pueden exigir acceso. Atiende el temor a requerimientos legales de fuera de la UE (por ejemplo, la CLOUD Act de EE. UU.). La residencia indica dónde se guardan físicamente, pero no quién puede exigir acceso. La localización es una medida para lograr soberanía y la redundancia geográfica es de disponibilidad.

36. A Antes de eliminar datos hay que confirmar que ninguna retención legal (legal hold), litigio activo, auditoría regulatoria u otra obligación exija conservarlos. Destruir datos bajo retención legal puede traer sanciones graves por destrucción de evidencia y cargos por obstrucción. Solo después se destruyen técnicamente. Sobrescribir, destruir medios y quitar respaldos son pasos válidos, pero posteriores. Primero va el riesgo legal y de cumplimiento.

37. B El propietario de los datos (data owner), normalmente un gerente senior o ejecutivo de una unidad de negocio, asigna el nivel de clasificación y lo revisa periódicamente. El custodio (data custodian), a menudo personal de TI, implementa los controles que indica el propietario, como respaldos, listas de acceso y cifrado. El administrador (steward) cuida la calidad y el gobierno de los datos, y el procesador los trata por cuenta de otro. El propietario decide y el custodio implementa.

38. A La destrucción física da la mayor garantía porque deja el medio inutilizable e irrecuperable. El borrado criptográfico solo sirve si los datos estaban cifrados, y aquí no lo estaban. La sobrescritura de siete pasadas es eficaz, pero deja posibilidades teóricas de recuperación (firmware, sectores defectuosos, espacio de sobreaprovisionamiento) y es menos fiable en SSD. La desmagnetización sirve en medios magnéticos, pero no funciona en SSD, que usan memoria flash NAND.

39. B Confidencial es el nivel comercial adecuado para datos cuya divulgación no autorizada causaría daño grave a la organización, como desventaja competitiva y responsabilidad legal. La combinación de PII, salarios y evaluaciones cumple ese umbral. “Solo uso interno” es demasiado débil cuando hay riesgo legal. “Secreto” es un nivel gubernamental que casi no se usa en empresas y “Público” no es apropiado para datos sensibles de empleados.

40. C El propietario de los datos (data owner), normalmente un gerente o ejecutivo de negocio, decide la clasificación, los requisitos de retención y quién tiene acceso. Responde por el valor de negocio y la protección de los datos. Los custodios implementan los controles técnicos, pero no toman decisiones de política. Los procesadores tratan datos por cuenta de otro. El CISO orienta y gobierna la seguridad, pero no es propietario de los datos.

41. A La necesidad de saber (need-to-know) indica que solo se da acceso si una función del puesto lo requiere, aunque el usuario tenga el nivel de autorización (clearance). El sistema pudo permitir el acceso, pero el empleado no tenía necesidad de negocio. El privilegio mínimo se refiere al nivel mínimo de permisos, no a si el acceso se justifica. La separación de funciones previene fraude y la defensa en profundidad no es un principio de acceso.

42. B COBIT está diseñado para alinear el gobierno de TI con las metas del negocio y ofrece un marco de administración. ISO 27002 es un código de prácticas de controles técnicos y operativos, no de gobierno. NIST SP 800-53 da controles detallados para sistemas federales. Los CIS Controls son acciones priorizadas, tácticas y no estratégicas. Si la pregunta habla de alinear con el negocio, piensa en COBIT: primero gobierno, luego controles.

43. D El debido cuidado (due care) es actuar de la forma correcta y a tiempo, como lo haría una persona razonable. Informar de la brecha a la junta (y a los reguladores, si corresponde) es un ejemplo. La debida diligencia (due diligence) es investigar los riesgos y verificar de forma continua que las medidas siguen siendo eficaces. La regla del hombre prudente es el deber fiduciario de proteger los activos, pero aquí la acción es informar. La separación de funciones no aplica.

44. D El BCP es un marco estratégico amplio que asegura la continuidad de todas las funciones críticas del negocio durante y después de una interrupción: personas, procesos, instalaciones, cadena de suministro, comunicaciones y tecnología. El DRP es más acotado y táctico, y define cómo restaurar sistemas, datos e infraestructura de TI tras un desastre. El DRP es parte del BCP, no al revés. Son complementarios, no intercambiables.

45. D Las pruebas y ejercicios periódicos validan que los procedimientos de recuperación funcionan, incluida la integridad de los respaldos. Si las cintas no se leen en un ejercicio, las pruebas fueron insuficientes o no existieron. El análisis de impacto al negocio (BIA) identifica sistemas críticos y RTO, pero no valida medios de respaldo. La evaluación de riesgos no prueba controles. Tener un plan no basta: hay que probarlo.

46. A ALE = SLE × ARO. La expectativa de pérdida única (SLE) es la pérdida esperada por un evento: $50,000. La tasa anualizada de ocurrencia (ARO) es la frecuencia esperada por año: 0.20 (20%). Entonces ALE = $50,000 × 0.20 = $10,000. Los $50,000 son solo el SLE y no consideran la frecuencia anual. Los $250,000 salen de multiplicar por 5 por error, y los $40,000 no salen de los datos.

47. B Un estándar (standard) exige configuraciones, ajustes o requisitos específicos (por ejemplo, “todas las contraseñas deben tener 12 caracteres o más”). Es táctico y de cumplimiento obligatorio. Las políticas son declaraciones generales de la intención de la dirección, menos específicas. Los procedimientos describen los pasos para aplicar políticas y estándares, y también pueden ser obligatorios. Las guías son recomendaciones, no obligaciones.

48. B Privacidad desde el Diseño exige integrar la privacidad en la arquitectura desde el principio, con minimización de datos (recopilar solo lo necesario) y privacidad por defecto (los ajustes más protectores como valor predeterminado). Una evaluación de impacto después del desarrollo es reactiva. Cifrar antes del despliegue atiende la seguridad, pero no minimiza la recopilación. La capacitación ayuda, pero no garantiza que la privacidad esté en la arquitectura.

49. B La transferencia del riesgo traslada el impacto financiero a un tercero, normalmente con un seguro (póliza de responsabilidad cibernética) o contratos (SLA de un proveedor de nube con penalizaciones). No es evitación, que elimina la actividad que causa el riesgo. Tampoco es mitigación, que aplica controles para reducir la probabilidad o el impacto, ni aceptación, que lo reconoce y documenta sin actuar. Transferir no elimina el riesgo, solo traslada la carga financiera.

50. C Involucrar a las fuerzas del orden es una decisión de negocio y legal que requiere la aprobación de la alta dirección o del asesor legal, por las obligaciones regulatorias, los riesgos de litigio, la divulgación pública y el impacto en el negocio. El equipo de respuesta aporta los datos técnicos, pero no toma esta decisión estratégica. El CISO asesora, pero la decisión implica exposición legal y cumplimiento. El enlace facilita el contacto, pero no decide si se inicia.

Palabras clave en inglés

due care	debido cuidado	Aplicar los controles que una persona razonable aplicaría.
due diligence	debida diligencia	Investigar riesgos y verificar de forma continua que los controles funcionen.
risk acceptance	aceptación del riesgo	Quedarse con el riesgo residual a sabiendas y con autorización.
risk transference	transferencia del riesgo	Pasar el impacto financiero a otro, como una aseguradora.
risk avoidance	evitación del riesgo	Dejar de hacer la actividad que causa el riesgo.
risk mitigation	mitigación del riesgo	Usar controles para bajar la probabilidad o el impacto.
residual risk	riesgo residual	El riesgo que queda después de aplicar los controles.
single loss expectancy (SLE)	expectativa de pérdida única	Dinero que se espera perder en un solo incidente.
annualized rate of occurrence (ARO)	tasa anualizada de ocurrencia	Cuántas veces por año se espera que pase el incidente.
annualized loss expectancy (ALE)	expectativa de pérdida anualizada	Pérdida esperada por año: SLE multiplicado por ARO.
business continuity plan (BCP)	plan de continuidad del negocio	Plan amplio para mantener las funciones críticas durante una interrupción.
disaster recovery plan (DRP)	plan de recuperación ante desastres	Plan táctico para restaurar sistemas y datos de TI.
business impact analysis (BIA)	análisis de impacto al negocio	Identifica los sistemas críticos y sus tiempos de recuperación.
recovery time objective (RTO)	objetivo de tiempo de recuperación	Tiempo meta para restaurar un sistema después de una interrupción.
recovery point objective (RPO)	objetivo de punto de recuperación	Pérdida de datos aceptable, medida en tiempo.
maximum tolerable downtime (MTD)	tiempo máximo tolerable de inactividad	Lo máximo que el negocio aguanta sin el servicio.
need-to-know	necesidad de saber	Acceso solo si tu trabajo requiere esa información.
least privilege	privilegio mínimo	Dar solo los permisos mínimos para hacer el trabajo.
separation of duties	separación de funciones	Dividir tareas entre varias personas para prevenir fraude.
defense in depth	defensa en profundidad	Varias capas de control que se respaldan entre sí.
data owner	propietario de los datos	Directivo que decide clasificación, retención y acceso a los datos.

data custodian	custodio de los datos	Persona de TI que aplica los controles que pide el propietario.
data steward	administrador de datos	Cuida la calidad, el origen y el gobierno de los datos.
data sovereignty	soberanía de los datos	Los datos quedan sujetos a las leyes del país donde residen.
legal hold	retención legal	Orden de conservar datos por un juicio o una investigación.
data sanitization	sanitización de datos	Eliminar datos de un medio para que no se recuperen.
tailoring	adaptación de controles	Ajustar los controles de la línea base a tu sistema.
scoping	delimitación del alcance	Decidir a qué sistemas se aplica una línea base.
baseline	línea base	Conjunto mínimo aprobado de configuraciones o controles.
non-repudiation	no repudio	Nadie puede negar una acción que sí realizó.
digital signature	firma digital	Firma con clave privada que se verifica con la clave pública.
key escrow	custodia de claves por un tercero	Guardar copias de claves de cifrado con un tercero.
mantrap	esclusa de seguridad	Dos puertas seguidas; solo una se abre a la vez.
compensating control	control compensatorio	Protección alternativa cuando el control principal no se puede usar.
detective control	control detectivo	Identifica un incidente cuando ocurre o después, como cámaras o registros.
order of volatility	orden de volatilidad	Orden para recoger evidencia, primero la que se pierde más rápido.
dwell time	tiempo de permanencia	Tiempo que un atacante está dentro sin ser detectado.
change advisory board (CAB)	comité asesor de cambios	Grupo que aprueba los cambios antes de pasarlos a producción.
false positive	falso positivo	Alerta por tráfico o actividad que en realidad es legítima.
mutual authentication	autenticación mutua	El cliente y el servidor verifican la identidad del otro.

Examundo es independiente. No está afiliado con los organismos que hacen estos exámenes ni tiene su aprobación. Las preguntas son originales, no son del examen real. examundo.tech/es/cissp/