examundo

Examen de práctica CompTIA Security+ en español

70 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/comptia-security-plus/

Operaciones de seguridad

1. Un administrador de red quiere identificar picos inusuales de ancho de banda saliente hacia un rango de IP en el extranjero, sin capturar ni almacenar el contenido completo de los paquetes en toda la empresa. ¿Qué fuente de registros es la MÁS adecuada para este objetivo?

A network administrator wants to identify unusual spikes in outbound bandwidth to a foreign IP range without capturing and storing full packet payloads across the enterprise. Which log data source is MOST appropriate for this goal?

A. Captura completa de paquetes (PCAP)
B. Registros de eventos de seguridad de Windows
C. Registros de consultas DNS
D. Datos de NetFlow

---

2. Un administrador revisa un servidor de base de datos recién aprovisionado y ve que Telnet y FTP están habilitados por defecto, junto con varias cuentas locales sin uso. ¿Qué principio de endurecimiento (hardening) se está violando?

An administrator is reviewing a newly provisioned database server and finds Telnet and FTP services enabled by default, along with several unused local user accounts. Which hardening principle is being violated?

A. Mínima funcionalidad (least functionality)
B. Separación de funciones (separation of duties)
C. Defensa en profundidad (defense in depth)
D. Mínimo privilegio (least privilege)

---

3. Un análisis de vulnerabilidades indica que un servidor Linux usa una versión antigua de OpenSSL, vulnerable a un CVE conocido. Al verificar a mano, el administrador confirma que en realidad está instalada la versión con el parche y que el escáner leyó mal la información del banner. Este caso describe un:

A vulnerability scan flags a Linux server as running an outdated OpenSSL version vulnerable to a known CVE. Upon manual verification, the administrator confirms the patched version is actually installed and the scanner misread the banner information. This scenario describes a:

A. Verdadero negativo (true negative)
B. Verdadero positivo (true positive)
C. Falso negativo (false negative)
D. Falso positivo (false positive)

---

4. Un investigador forense incauta una laptop sospechosa de contener evidencia de robo de datos por parte de un empleado, y llena un formulario de cadena de custodia (chain of custody) con cada persona que maneja el equipo. ¿Cuál es el propósito PRINCIPAL de esta documentación?

A forensic investigator seizes a laptop suspected of containing evidence of insider data theft and completes a chain-of-custody form documenting every individual who handles the device. What is the PRIMARY purpose of this documentation?

A. Determinar qué departamento debe pagar el reemplazo del equipo

B. Calcular el valor monetario del activo incautado para el seguro

C. Establecer un registro continuo que pruebe la integridad de la evidencia y su admisibilidad en procesos legales

D. Programar el mantenimiento rutinario del equipo cuando termine la investigación

---

5. Un disco duro incautado pasa de un analista forense a otro. Cada traspaso se anota con fecha, hora, nombre de la persona y motivo del acceso. ¿Qué se mantiene con esta documentación?

A seized hard drive is transferred between two forensic analysts. Each transfer is logged with the date, time, individual's name, and purpose of access. What is being maintained by this documentation?

A. Cadena de custodia (chain of custody)

B. Orden de volatilidad (order of volatility)

C. Retención legal (legal hold)

D. Política de retención de datos (data retention policy)

---

6. Un administrador de red quita los derechos de administrador local a las cuentas de usuario estándar y da acceso elevado solo cuando se necesita para una tarea específica. ¿Qué principio de seguridad ejemplifica esta práctica?

A network administrator removes local administrator rights from standard user accounts, granting elevated access only when required for a specific task. This practice exemplifies which security principle?

A. Defensa en profundidad (defense in depth)

B. Confianza cero (zero trust)

C. Mínimo privilegio (least privilege)

D. Separación de funciones (separation of duties)

---

7. Un analista de seguridad busca de forma proactiva en la telemetría de la empresa pruebas de una técnica de ataque nueva que aún no activó ninguna alerta del SIEM, a partir de una hipótesis basada en inteligencia de amenazas reciente. ¿Qué práctica describe MEJOR esta actividad?

A security analyst proactively searches enterprise telemetry for evidence of a novel attack technique that has not yet triggered any SIEM alert, based on a hypothesis derived from recent threat intelligence. This activity is BEST described as which practice?

A. Caza de amenazas (threat hunting)

B. Análisis de vulnerabilidades (vulnerability scanning)

C. Correlación automática de registros

D. Triaje de incidentes (incident triage)

---

8. Un equipo de seguridad quiere detectar un ataque de malware sin archivos (fileless) que usa PowerShell para inyectar código malicioso directamente en la memoria, sin escribir un ejecutable en el disco. ¿Qué herramienta de seguridad es la MÁS adecuada para detectar este comportamiento?

A security team wants to detect a fileless malware attack that uses PowerShell to inject malicious code directly into memory without writing an executable to disk. Which security tool is BEST suited to detect this behavior?

A. Agente de prevención de pérdida de datos (DLP)

B. Antivirus basado en firmas

C. Detección y respuesta en el endpoint (EDR)

D. Firewall de red

---

9. ¿Qué control protege MEJOR la confidencialidad de los datos sensibles guardados en el disco duro de una laptop robada?

Which control BEST protects the confidentiality of sensitive data stored on a stolen laptop's hard drive?

A. Sistema de detección de intrusiones
B. Autenticación multifactor
C. Cifrado de disco completo
D. Segmentación de red

---

10. Durante el endurecimiento (hardening) de un servidor, un técnico deshabilita Telnet, elimina la cuenta de invitado predeterminada y cierra todos los puertos de red sin uso. ¿Qué concepto de seguridad representa MEJOR esta actividad?

During server hardening, a technician disables Telnet, removes the default guest account, and closes all unused network ports. Which security concept does this activity BEST represent?

A. Establecer una línea base de seguridad (security baseline)
B. Aplicar el mínimo privilegio (least privilege)
C. Reducir la superficie de ataque (attack surface)
D. Implementar segmentación de red

---

11. Durante la respuesta a un incidente, un analista forense debe recolectar evidencia de un servidor comprometido que sigue encendido. Según el orden de volatilidad (order of volatility), ¿qué tipo de dato se debe recolectar PRIMERO?

During incident response, a forensic analyst must collect evidence from a compromised server that is still powered on. According to the order of volatility, which type of data should be collected FIRST?

A. El contenido de la RAM y los procesos en ejecución
B. Los registros archivados en un servidor de respaldo remoto
C. Los datos de configuración impresos en la documentación del sistema
D. Los archivos guardados en el disco duro local

---

12. ¿Qué técnica de endurecimiento (hardening) reduce la superficie de ataque de un servidor al deshabilitar puertos y servicios que no se usan?

Which hardening technique reduces a server's attack surface by disabling unused ports and services?

A. Activar el registro detallado (verbose logging)
B. Deshabilitar los servicios innecesarios
C. Instalar un antivirus
D. Configurar un honeypot

---

13. En una investigación forense, un analista lleva un disco duro incautado a un laboratorio forense para crear una imagen forense (imaging). ¿Qué documento debe acompañar al disco para mantener la integridad de la evidencia?

During a forensic investigation, an analyst transfers a seized hard drive to a digital forensics lab for imaging. Which document must accompany the drive to maintain evidentiary integrity?

A. Guía de respuesta a incidentes (incident response playbook)
B. Formulario de cadena de custodia (chain of custody)
C. Plan de continuidad del negocio
D. Política de retención de datos

---

14. Un analista de seguridad hace respuesta a incidentes en vivo en una estación de trabajo que sigue encendida y conectada a la red. Siguiendo el orden de volatilidad, ¿qué artefacto debe recolectar PRIMERO, antes que cualquier otra evidencia?

A security analyst is performing live incident response on a workstation that is still powered on and connected to the network. Following the order of volatility, which artifact should the analyst collect FIRST, before any other evidence?

A. Tablas de enrutamiento y caché ARP
B. El contenido de la RAM y los procesos en ejecución
C. Archivos temporales guardados en el disco local
D. Registros de la CPU y caché del procesador

Amenazas, vulnerabilidades y mitigaciones

15. Un administrador de red sospecha que un atacante intercepta y altera el tráfico entre los clientes internos y la puerta de enlace predeterminada al responder solicitudes ARP con una dirección MAC falsificada. ¿Qué mitigación resolvería MEJOR este ataque en particular?

A network administrator suspects an attacker is intercepting and altering traffic between internal clients and the default gateway by responding to ARP requests with a spoofed MAC address. Which mitigation would BEST address this specific attack?

A. Segmentación de red con VLAN
B. Implementar cifrado WPA3
C. Deshabilitar los puertos de switch sin uso
D. Inspección dinámica de ARP (Dynamic ARP Inspection, DAI)

16. Un empleado abre un archivo adjunto de un correo y poco después todos los archivos de la unidad compartida están cifrados, con una nota que exige un pago en criptomonedas para recuperar el acceso. ¿Qué tipo de malware causó este incidente?

An employee opens an email attachment and shortly afterward finds that all files on the shared drive have been encrypted, with a note demanding payment in cryptocurrency to restore access. Which type of malware caused this incident?

A. Rootkit
B. Bomba lógica (logic bomb)
C. Ransomware
D. Spyware

17. Un atacante llama a la mesa de ayuda de TI haciéndose pasar por un ejecutivo de la empresa que está "bloqueado" durante una llamada urgente con un cliente, y presiona al técnico para que restablezca una contraseña de inmediato sin verificar su identidad. ¿Qué técnica de ingeniería social se usa?

An attacker calls the IT help desk posing as a company executive who is 'locked out' during an urgent client call, pressuring the technician to reset a password immediately without verifying identity. Which social engineering technique is being used?

A. Búsqueda en la basura (dumpster diving)
B. Pretexting (pretexto)
C. Tailgating (seguir a alguien para entrar)
D. Espiar por encima del hombro (shoulder surfing)

18. Un atacante obtiene una lista grande de usuarios y contraseñas filtrada en una brecha previa de una empresa sin relación, y prueba de forma sistemática esos mismos pares de credenciales en varias plataformas de banca en línea. ¿Qué técnica de ataque se usa?

An attacker obtains a large list of usernames and passwords leaked from a previous breach at an unrelated company and systematically attempts to log in with those exact credential pairs across several different online banking platforms. Which attack technique is being used?

A. Ataque de diccionario (dictionary attack)
B. Ataque de fuerza bruta (brute-force attack)
C. Relleno de credenciales (credential stuffing)
D. Pulverización de contraseñas (password spraying)

---

19. Un usuario reporta que los archivos de una unidad de red compartida de repente tienen una extensión nueva y desconocida y no se pueden abrir. En cada carpeta afectada apareció un archivo de texto que exige un pago en criptomonedas a cambio de una clave de descifrado. ¿Qué amenaza es la MÁS probable?

A user reports that files on a shared network drive suddenly have a new, unfamiliar file extension and cannot be opened. A text file demanding cryptocurrency payment for a decryption key has appeared in each affected folder. Which threat is MOST likely responsible?

A. Rootkit
B. Bomba lógica (logic bomb)
C. Gusano (worm)
D. Ransomware

---

20. Un atacante llama a un empleado, dice ser de la mesa de ayuda de la empresa y le pide que le lea un código de un solo uso que acaban de enviar a su teléfono. ¿Qué vector de ingeniería social se usa?

An attacker calls an employee, claiming to be from the corporate help desk, and asks the employee to read back a one-time passcode that was just sent to their phone. Which social engineering vector is being used?

A. Vishing
B. Smishing
C. Espiar por encima del hombro (shoulder surfing)
D. Tailgating

---

21. Un actor de amenazas compromete un sitio web que visitan con frecuencia los empleados de un contratista de defensa e inserta JavaScript malicioso que solo se ejecuta cuando la IP del visitante coincide con el rango conocido del contratista. ¿Qué técnica de ataque se describe?

A threat actor compromises a website frequently visited by employees of a defense contractor and embeds malicious JavaScript that only executes when the visitor's IP address matches the contractor's known range. Which attack technique is being described?

A. Typosquatting
B. Envenenamiento de DNS (DNS poisoning)
C. Ataque de abrevadero (watering hole attack)
D. Cross-site scripting (XSS)

---

22. Varias estaciones de trabajo de una oficina empiezan a calentarse mucho, con los ventiladores a toda velocidad de forma continua, y las herramientas de monitoreo muestran un uso de CPU cercano al 100% incluso cuando los empleados no están trabajando. ¿Qué indicador de compromiso (IoC) es el MÁS coherente con este comportamiento?

Several workstations in an office begin running unusually hot with fans at full speed continuously, and monitoring tools show sustained CPU usage near 100% even when employees are not actively working. Which indicator of compromise is MOST consistent with this behavior?

A. Contenido bloqueado por un cambio en una regla del firewall

B. Registros fuera de ciclo de una tarea programada

C. Consumo de recursos de un malware de minería de criptomonedas

D. Registros faltantes de un SIEM comprometido

---

23. Un atacante registra un dominio casi idéntico al del sitio legítimo de un banco y compromete un resolvedor DNS público, de modo que los usuarios que escriben la URL correcta del banco son redirigidos en silencio al servidor del atacante. ¿Qué ataque describe esto?

An attacker registers a domain nearly identical to a bank's legitimate site and compromises a public DNS resolver so that users who type the correct bank URL are silently redirected to the attacker's server. Which attack does this describe?

A. Pharming

B. Pretexting

C. Vishing

D. Typosquatting

---

24. Un analista de seguridad investiga una brecha en la que el atacante usó exploits de día cero (zero-day) a la medida, mantuvo acceso persistente sin ser detectado durante ocho meses y extrajo datos de la oferta de un competidor en un contrato de defensa. ¿Qué tipo de actor de amenaza es el MÁS probable?

A security analyst investigates a breach in which the attacker used custom zero-day exploits, maintained undetected persistent access for eight months, and exfiltrated data tied to a competitor's defense contract bid. Which threat actor type MOST likely conducted this attack?

A. Aficionado que usa herramientas ajenas (script kiddie)

B. Amenaza interna no intencional (unintentional insider threat)

C. Hacktivista (hacktivist)

D. Amenaza persistente avanzada (APT) de un Estado-nación

---

25. El departamento de cuentas por pagar recibe un correo que parece venir de la cuenta del director ejecutivo (CEO) y que pide transferir fondos de urgencia a la cuenta de un proveedor nuevo. No hay malware ni enlaces maliciosos. ¿Qué tipo de ataque es?

The accounts payable department receives an email that appears to come from the CEO's account instructing them to urgently wire funds to a new vendor account. No malware or malicious link is involved. Which type of attack does this represent?

A. Relleno de credenciales (credential stuffing)

B. Ataque de abrevadero (watering hole attack)

C. Typosquatting

D. Compromiso de correo empresarial (business email compromise, BEC)

---

26. Un administrador de sistemas despedido hace poco usa credenciales que aún no habían sido desactivadas para entrar de forma remota y borrar archivos de respaldo críticos. ¿Qué categoría de actor de amenaza describe MEJOR a esta persona?

A systems administrator who was recently terminated uses credentials that had not yet been deactivated to log in remotely and delete critical backup archives. Which threat actor category BEST describes this individual?

A. Hacktivista (hacktivist)
B. Actor de un Estado-nación (nation-state)
C. Aficionado que usa herramientas ajenas (script kiddie)
D. Amenaza interna (insider threat)

---

27. Un equipo de seguridad nota miles de intentos de inicio de sesión exitosos en el portal de clientes de la empresa con combinaciones válidas de correo y contraseña que se filtraron antes en una brecha de un sitio de ventas no relacionado. ¿Qué ataque ocurre?

A security team notices thousands of successful login attempts against the company's customer portal using valid email and password combinations that were previously leaked in a breach of an unrelated retail website. Which attack is occurring?

A. Relleno de credenciales (credential stuffing)
B. Ataque con tablas arcoíris (rainbow table)
C. Pulverización de contraseñas (password spraying)
D. Ataque de fuerza bruta (brute-force)

---

28. Un atacante llama al departamento de cuentas por pagar, dice ser un auditor externo y pide los registros de facturas recientes para "verificar el cumplimiento", sin ofrecer ninguna prueba de identidad. ¿Qué técnica de ingeniería social se usa?

An attacker calls the accounts payable department, claiming to be an external auditor, and requests recent invoice records to 'verify compliance' before offering any proof of identity. Which social engineering technique is being used?

A. Tailgating
B. Baiting (cebo)
C. Pretexting (pretexto)
D. Quid pro quo

Gestión del programa de seguridad

29. La dirección de una organización declara que la empresa está dispuesta a aceptar hasta un 5% de probabilidad anual de una caída de un sistema crítico antes de que se requiera más inversión en seguridad. Esta declaración describe MEJOR su:

An organization's leadership states that the company is willing to accept up to a 5% chance of a critical system outage annually before additional security investment is required. This statement BEST describes the organization's:

A. Registro de riesgos (risk register)
B. Tolerancia al riesgo (risk tolerance)
C. Apetito de riesgo (risk appetite)
D. Excepción de riesgo (risk exception)

---

30. Una empresa SaaS con sede en EE. UU. aloja datos de gestión de relaciones con clientes (CRM) de un minorista europeo y los procesa estrictamente según las instrucciones escritas del minorista sobre su finalidad y retención. Según el GDPR, ¿qué rol tiene la empresa SaaS?

A US-based SaaS company hosts customer relationship management data on behalf of a European retailer, processing that data strictly according to the retailer's written instructions on purpose and retention. Under GDPR, which role does the SaaS company hold?

A. Titular de los datos (data subject)
B. Delegado de protección de datos (data protection officer)
C. Responsable del tratamiento (data controller)
D. Encargado del tratamiento (data processor)

---

31. Un cliente alemán envía un correo a una tienda en línea para pedir que se eliminen de forma permanente todos sus datos personales de los sistemas de la empresa. ¿Qué regulación le da al cliente el derecho legal de hacer esta solicitud?

A German customer emails an online retailer requesting that all of their personal data be permanently deleted from the company's systems. Which regulation grants this customer the legal right to make this request?

A. HIPAA
B. GDPR
C. PCI DSS
D. SOX

---

32. Una firma de servicios financieros identifica un riesgo residual en un sistema heredado de procesamiento de pagos que no se puede corregir del todo con el presupuesto. El CISO compra una póliza de ciberseguro para cubrir las posibles pérdidas de una brecha. ¿Qué estrategia de gestión de riesgos representa MEJOR esto?

A financial services firm identifies a residual risk from a legacy payment processing system that cannot be fully remediated within budget. The CISO purchases a cyber insurance policy to cover potential losses from a breach. Which risk management strategy does this BEST represent?

A. Transferencia del riesgo (risk transference)
B. Aceptación del riesgo (risk acceptance)
C. Evitación del riesgo (risk avoidance)
D. Mitigación del riesgo (risk mitigation)

---

33. Un cliente potencial pide pruebas de que los controles de seguridad de un proveedor de servicios en la nube han funcionado de forma efectiva durante 12 meses antes de firmar un contrato. ¿Qué tipo de informe de auditoría debe entregar el proveedor?

A prospective client requests evidence that a cloud service provider's security controls have operated effectively over a 12-month period before signing a contract. Which type of audit report should the provider supply?

A. Informe SOC 2 Tipo I
B. Informe SOC 2 Tipo II
C. Informe SOC 1 Tipo I
D. Atestación de cumplimiento (AOC) de PCI DSS

---

34. Una organización pide pruebas de la efectividad de los controles de seguridad de un proveedor de nube durante un período de operación de 12 meses, y no en un solo momento. ¿Qué tipo de informe cumple MEJOR este requisito?

An organization requests evidence of a cloud vendor's security control effectiveness over a 12-month operating period rather than at a single point in time. Which type of report BEST satisfies this requirement?

A. SOC 1: enfocado en controles relevantes para la información financiera, no en seguridad

B. Certificación ISO 27001: confirma que un sistema de gestión de seguridad de la información (ISMS) cumple la norma al momento de la auditoría

C. SOC 2 Tipo I: certifica que el diseño de los controles es adecuado en un solo momento

D. SOC 2 Tipo II: certifica la efectividad operativa de los controles durante un período de revisión extenso

---

35. Durante la negociación de un contrato con un proveedor de servicios en la nube, un oficial de cumplimiento quiere asegurar que la organización pueda verificar los controles de seguridad del proveedor en cualquier momento, sin necesitar el consentimiento previo del proveedor para programar la revisión. ¿Qué cláusula contractual se debe negociar en el SLA?

During contract negotiations with a cloud service provider, a compliance officer wants to ensure the organization can verify the vendor's security controls at any time without needing the vendor's advance consent to schedule the review. Which contractual clause should be negotiated into the SLA?

A. Cláusula de indemnización (indemnification)

B. Cláusula de derecho a auditar (right-to-audit)

C. Acuerdo de confidencialidad (NDA)

D. Cláusula de fuerza mayor (force majeure)

---

36. Un administrador de sistemas quiere aplicar un cambio de emergencia en una regla del firewall para bloquear la explotación activa de una vulnerabilidad crítica, fuera de la ventana de mantenimiento semanal normal. Según las prácticas estándar de gestión de cambios (change management), ¿qué debe ocurrir PRIMERO?

A systems administrator wants to deploy an emergency firewall rule change to block active exploitation of a critical vulnerability outside the normal weekly maintenance window. According to standard change management practices, what should occur FIRST?

A. Presentar el cambio por el proceso de cambio de emergencia para una aprobación acelerada

B. Esperar a la próxima reunión programada del comité asesor de cambios (CAB)

C. Aplicar el cambio de inmediato y documentarlo después

D. Avisar a los usuarios finales de la posible interrupción antes de hacer cualquier cambio

---

37. Una empresa que cotiza en bolsa contrata a una firma contable externa para verificar de forma independiente que sus controles de información financiera cumplen los requisitos regulatorios. ¿Qué tipo de auditoría se realiza?

A publicly traded company hires an outside accounting firm to independently verify that its financial reporting controls comply with regulatory requirements. Which type of audit is being performed?

A. Evaluación de vulnerabilidades (vulnerability assessment)

B. Auditoría interna (internal audit)

C. Autoevaluación de cumplimiento (compliance self-assessment)

D. Auditoría externa (external audit)

---

38. Un equipo de compras necesita una garantía independiente de que los controles de un proveedor SaaS sobre seguridad, disponibilidad y confidencialidad funcionaron de forma efectiva durante los últimos 12 meses antes de firmar un contrato. ¿Qué documento debe pedir al proveedor?

A procurement team needs independent assurance that a SaaS vendor's controls over security, availability, and confidentiality operated effectively over the past 12 months before signing a contract. Which document should the team request from the vendor?

A. Informe SOC 2 Tipo II

B. Cuestionario de autoatestación (self-attestation)

C. Resumen de una prueba de penetración (penetration test)

D. Análisis de impacto al negocio (BIA)

---

39. Una evaluación de riesgos en un banco regional identifica una vulnerabilidad con baja probabilidad de explotación y que causaría un impacto económico mínimo si ocurriera. El costo de implementar un control supera la pérdida potencial. ¿Qué respuesta al riesgo debe recomendar el equipo de seguridad a la gerencia?

A risk assessment at a regional bank identifies a vulnerability that has a low likelihood of exploitation and would cause minimal financial impact if realized. The cost of implementing a control exceeds the potential loss. Which risk response should the security team recommend to management?

A. Evitación del riesgo (risk avoidance)

B. Mitigación del riesgo (risk mitigation)

C. Aceptación del riesgo (risk acceptance)

D. Transferencia del riesgo (risk transference)

---

40. Una empresa recibe un aviso de un litigio pendiente por supuesta negligencia en una brecha de datos, y el equipo legal emite una retención legal (legal hold). ¿Qué acción se exige respecto a la política normal de retención de datos de la empresa?

A company receives notice of pending litigation involving alleged data breach negligence, and the legal team issues a legal hold. Which action is required regarding the company's standard data retention policy?

A. Entregar la custodia de los registros a los abogados de la contraparte para que los guarden

B. Suspender la destrucción rutinaria de los registros posiblemente relevantes hasta que se levante la retención

C. Borrar de inmediato todos los datos del caso para reducir el alcance del descubrimiento de pruebas (discovery)

D. Cifrar todos los registros sujetos a la retención y seguir con el calendario normal de retención

---

41. Después de implementar autenticación multifactor y segmentación de red para atender un riesgo de phishing, sigue existiendo algo de riesgo de compromiso de cuentas por la posibilidad de robo de tokens de sesión con un atacante en el medio (adversary-in-the-middle). ¿Qué término describe este riesgo restante?

After implementing multifactor authentication and network segmentation to address a phishing-related risk, some risk of account compromise still remains due to the possibility of adversary-in-the-middle session token theft. What term describes this remaining risk?

A. Riesgo residual (residual risk): el riesgo que queda después de aplicar controles

B. Riesgo de control (control risk): el riesgo de que un control no funcione como se diseñó

C. Riesgo inherente (inherent risk): el nivel de riesgo que existe antes de aplicar controles

D. Riesgo secundario (secondary risk): un riesgo nuevo que aparece como resultado directo de implementar un control

---

42. Un cliente potencial pide pruebas de que los controles de seguridad de un proveedor funcionaron de forma efectiva durante los seis meses anteriores, y no solo de que estaban bien diseñados en un momento dado. ¿Qué informe debe entregar el proveedor?

A prospective client requests evidence that a vendor's security controls have operated effectively over the preceding six months, not merely that they were properly designed at a single point in time. Which report should the vendor provide?

A. SOC 1 Tipo I
B. SOC 2 Tipo II
C. SOC 2 Tipo I
D. Certificado ISO 27001

Arquitectura de seguridad

43. Una empresa quiere usar una infraestructura en la nube provisionada exclusivamente para su organización y que no se comparta con ningún otro inquilino (tenant). ¿Qué modelo de despliegue en la nube describe esto?

A company wants to use cloud infrastructure that is provisioned exclusively for its own organization and is not shared with any other tenant. Which cloud deployment model does this describe?

A. Nube privada (private cloud)
B. Nube comunitaria (community cloud)
C. Nube híbrida (hybrid cloud)
D. Nube pública (public cloud)

44. Un administrador de red segmenta una red corporativa para que las estaciones del área de finanzas no puedan comunicarse directamente con los equipos del área de marketing. ¿Qué tecnología se implementa?

A network administrator segments a corporate network so that finance workstations cannot directly communicate with marketing department devices. Which technology is being implemented?

A. Balanceador de carga (load balancer)
B. VLAN
C. NAT
D. VPN

45. El navegador de un usuario muestra un error de certificado que dice que el certificado no es de confianza al visitar una aplicación web interna de la empresa. ¿Qué componente de la jerarquía PKI es MÁS probable que falte en el almacén de confianza (trust store) del cliente?

A user's browser displays a certificate error stating the certificate is not trusted when visiting an internal company web application. Which component of the PKI hierarchy is MOST likely missing from the client's trust store?

A. La clave privada del servidor web
B. El ticket de sesión del cliente
C. El certificado de la CA raíz
D. La clave de sesión simétrica

46. Un administrador de sistemas descarga un archivo ISO y quiere verificar que no se dañó ni se alteró durante la transferencia. ¿Qué método lo logra MEJOR?

A systems administrator downloads an ISO file and wants to verify that it was not corrupted or altered during transfer. Which method BEST achieves this?

A. Comparar el hash SHA-256 del archivo descargado con el hash publicado por el proveedor
B. Comparar el tamaño del archivo en bytes con el que aparece en el sitio del proveedor
C. Cifrar el archivo con AES-256 y confirmar que se descifra correctamente
D. Abrir el ISO e inspeccionar su contenido a simple vista

47. Un ingeniero de redes debe elegir un mecanismo de intercambio de claves de TLS que garantice que el tráfico de sesiones pasadas siga siendo confidencial aunque después se comprometa la clave privada de largo plazo del servidor. ¿Qué intercambio de claves ofrece esta propiedad?

A network engineer must select a TLS key exchange mechanism that ensures past session traffic remains confidential even if the server's long-term private key is later compromised. Which key exchange provides this property?

A. Intercambio de claves RSA estático

B. Intercambio de clave precompartida (PSK) sin parámetros efímeros

C. Diffie-Hellman efímero (DHE)

D. Intercambio de tickets de Kerberos

---

48. Un fabricante de sensores IoT con batería debe implementar cifrado para los datos en tránsito, pero los dispositivos tienen una capacidad de procesamiento y memoria extremadamente limitadas. ¿Qué factor debe influir MÁS en la elección del algoritmo criptográfico?

A manufacturer of battery-powered IoT sensors must implement encryption for data in transit but has extremely limited processing power and memory. Which factor should MOST influence the choice of cryptographic algorithm?

A. Criptografía ligera optimizada para dispositivos con recursos limitados

B. Algoritmos resistentes a la computación cuántica con claves grandes

C. El algoritmo más fuerte disponible, sin importar el consumo de recursos

D. DES heredado, por compatibilidad con sistemas anteriores

---

49. Una institución financiera aísla físicamente su red principal de procesamiento de transacciones para que no tenga ninguna conexión de red con internet ni con ninguna otra red. ¿Qué concepto de seguridad se aplica?

A financial institution physically isolates its core transaction-processing network so it has no network connection to the internet or any other network. Which security concept is being applied?

A. Microsegmentación (micro-segmentation)

B. Aislamiento físico (air gap)

C. Subred filtrada (screened subnet)

D. Confianza cero (zero trust)

---

50. Un administrador de un centro de datos debe evitar el movimiento lateral entre dos máquinas virtuales que comparten la misma VLAN y subred, aunque el tráfico este-oeste (east-west) entre ellas es necesario para que la aplicación funcione. ¿Qué control logra MEJOR este objetivo?

A data center administrator must prevent lateral movement between two virtual machines that share the same VLAN and subnet, even though east-west traffic between them is required for the application to function. Which control BEST achieves this goal?

A. Implementar un IDS de red en modo promiscuo

B. Crear una VLAN nueva para cada máquina virtual

C. Activar la seguridad de puertos (port security) en el switch físico

D. Microsegmentación con políticas de firewall en el host

---

51. Una empresa de comercio electrónico exige que sus servidores web sigan disponibles aunque falle uno de ellos, sin que los usuarios sufran una caída. ¿Qué arquitectura apoya MEJOR este requisito?

An e-commerce company requires its web servers to remain available even if one server fails, without users experiencing downtime. Which architecture BEST supports this requirement?

A. Cifrado de disco completo en cada servidor

B. Un servidor de respaldo aislado (air gap) y apagado

C. Balanceo de carga activo-pasivo con conmutación automática por falla

D. Un único punto de presencia con procedimientos de reinicio manual

---

52. Una empresa quiere asegurar que el proveedor que publicó una actualización de software firmada no pueda negar después haberla publicado. ¿Qué concepto criptográfico ofrece MEJOR esta garantía?

A company wants to ensure that a signed software update cannot later be disputed by the vendor who published it. Which cryptographic concept BEST provides this assurance?

A. Ofuscación solo con hash
B. No repudio mediante firma digital
C. Disponibilidad mediante balanceo de carga
D. Confidencialidad mediante cifrado simétrico

---

53. Una empresa de energía mantiene una red totalmente aislada, sin conexiones físicas ni inalámbricas con la red de TI corporativa, para sus sistemas de control SCADA. ¿Qué control de seguridad representa esto?

A power utility maintains a completely isolated network with no physical or wireless connections to the corporate IT network for its SCADA control systems. Which security control does this represent?

A. Subred filtrada (screened subnet)
B. Aislamiento físico (air gap)
C. Servidor de salto (jump server)
D. Red privada virtual (VPN)

---

54. Una evaluación de seguridad de un edificio inteligente encuentra varios termostatos IoT que aún usan las credenciales de administrador de fábrica y están conectados al mismo segmento de red que las estaciones de finanzas. ¿Qué acción atiende el MAYOR riesgo inmediato?

A security assessment of a smart building finds several IoT thermostats still using factory-default administrator credentials and connected to the same network segment as finance workstations. Which action addresses the GREATEST immediate risk?

A. Activar la geocerca (geofencing) en la aplicación móvil
B. Deshabilitar SNMP en las estaciones de finanzas
C. Cambiar las credenciales predeterminadas y colocar los dispositivos IoT en una VLAN aislada
D. Aumentar la frecuencia de actualización del firmware del termostato

---

55. Un administrador web quiere verificar el estado de revocación de los certificados para clientes TLS sin exponer a la autoridad certificadora (CA) los patrones de navegación de cada cliente y sin agregar un viaje de ida y vuelta extra a la negociación TLS (handshake). ¿Qué enfoque cumple MEJOR estos requisitos?

A web administrator wants to verify certificate revocation status for TLS clients without exposing individual client browsing patterns to the certificate authority and without adding an extra round trip to the TLS handshake. Which approach BEST meets these requirements?

A. OCSP stapling
B. Consulta OCSP estándar enviada directamente a la CA
C. Verificación con lista de revocación de certificados (CRL)
D. Fijación de certificados (certificate pinning)

---

56. En la arquitectura de referencia empresarial de Purdue (Purdue Enterprise Reference Architecture), usada para segmentar redes de control industrial, ¿en qué nivel están normalmente los controladores lógicos programables (PLC) y las unidades terminales remotas (RTU) que se conectan directamente con sensores y actuadores de campo?

In the Purdue Enterprise Reference Architecture used to segment industrial control networks, at which level do programmable logic controllers (PLCs) and remote terminal units (RTUs) that directly interface with field sensors and actuators typically reside?

A. Nivel 3 - Operaciones del sitio
B. Nivel 1 - Control básico
C. Nivel 2 - Control supervisorio de área
D. Nivel 0 - Proceso físico

Conceptos generales de seguridad

57. Un comité asesor de cambios (change advisory board) revisa una solicitud para aplicar un cambio crítico en una regla del firewall durante una ventana de mantenimiento programada. ¿Qué elemento de la solicitud de cambio es el MÁS importante para minimizar el tiempo de caída si el cambio causa una interrupción inesperada del servicio?

A change advisory board is reviewing a request to deploy a critical firewall rule change during a scheduled maintenance window. Which element of the change request is MOST important for minimizing downtime if the change causes an unexpected service disruption?

A. Firma de aprobación del cambio
B. Análisis del impacto en las partes interesadas
C. Plan de reversión (rollback o backout)
D. Resultados de pruebas en un entorno aislado (sandbox)

---

58. Un centro de datos instala alarmas activadas por movimiento que avisan al personal de seguridad cada vez que se detecta movimiento no autorizado dentro de una sala de servidores restringida fuera del horario laboral. ¿Qué tipo de control representa este sistema de alarma?

A data center installs motion-activated alarms that alert security personnel whenever unauthorized movement is detected within a restricted server room after hours. Which type of control does this alarm system represent?

A. Control preventivo (preventive)
B. Control correctivo (corrective)
C. Control disuasorio (deterrent)
D. Control detectivo (detective)

---

59. Un administrador de un centro de datos instala fuentes de poder redundantes, arreglos RAID 10 y un clúster de conmutación por falla (failover) para un servidor de base de datos crítico. ¿Qué principio de la tríada CIA está atendiendo PRINCIPALMENTE el administrador?

A data center administrator deploys redundant power supplies, RAID 10 arrays, and a failover cluster for a critical database server. Which principle of the CIA triad is the administrator PRIMARILY addressing?

A. No repudio (non-repudiation)
B. Disponibilidad (availability)
C. Integridad (integrity)
D. Confidencialidad (confidentiality)

---

60. Una empresa exige que el empleado que inicia una orden de compra no pueda ser el mismo que aprueba el pago de esa orden. ¿Qué principio de seguridad se aplica?

A company requires that the employee who initiates a purchase order cannot be the same employee who approves payment for that order. Which security principle is being enforced?

A. Separación de funciones (separation of duties)
B. Mínimo privilegio (least privilege)
C. Vacaciones obligatorias (mandatory vacation)
D. Rotación de puestos (job rotation)

---

61. En el modelo de seguridad AAA, ¿qué proceso determina qué acciones puede realizar en un sistema un usuario ya verificado?

In the AAA security model, which process determines what actions an already-verified user is permitted to perform on a system?

A. Identificación (identification)
B. Contabilidad (accounting)
C. Autenticación (authentication)
D. Autorización (authorization)

---

62. Una organización adopta un modelo de seguridad en el que cada solicitud de acceso, sea de un empleado interno o de un socio externo, debe autenticarse y autorizarse sin importar la ubicación de red de quien la hace. ¿Qué modelo de seguridad adoptó la organización?

An organization migrates to a security model in which every access request, whether from an internal employee or an external partner, must be authenticated and authorized regardless of the requester's network location. Which security model has the organization adopted?

A. Confianza cero (zero trust)
B. Control de acceso basado en roles (RBAC)
C. Defensa en profundidad (defense in depth)
D. Defensa basada en el perímetro (perimeter-based defense)

---

63. Un atacante intercepta una solicitud de transferencia bancaria entre el servidor de aplicaciones de un banco y su base de datos, y cambia el número de la cuenta de destino antes de que termine la transacción. ¿Qué principio de la tríada CIA se vulneró PRINCIPALMENTE?

An attacker intercepts a wire transfer request between a bank's application server and its database, altering the destination account number before the transaction completes. Which tenet of the CIA triad has been PRIMARILY violated?

A. Confidencialidad (confidentiality)
B. Disponibilidad (availability)
C. No repudio (non-repudiation)
D. Integridad (integrity)

---

64. Antes de instalar un parche crítico en servidores de producción, una organización exige la revisión y la aprobación de un grupo designado. ¿Cuál es el propósito PRINCIPAL de este grupo en el proceso de gestión de cambios?

Before deploying a critical patch to production servers, an organization requires review and sign-off by a designated group. What is the PRIMARY purpose of this group in the change management process?

A. Redactar el plan de respuesta a incidentes
B. Hacer la instalación técnica del parche
C. Evaluar el riesgo y aprobar o rechazar los cambios propuestos
D. Dar la capacitación anual de concientización sobre seguridad

---

65. Durante un cambio programado en las reglas del firewall, el cambio aprobado por el equipo de redes causa una caída crítica en servicios de cara a los clientes. Según la práctica estándar de gestión de cambios, ¿qué se debió preparar ANTES de la implementación para minimizar el impacto de esta falla en el negocio?

During a scheduled firewall rule change, the network team's approved change causes a critical outage affecting customer-facing services. According to standard change management practice, what should have been prepared BEFORE implementation to minimize the business impact of this failure?

A. Una plantilla de informe posterior al incidente para el equipo de seguridad
B. Un inventario de activos actualizado con todos los firewalls afectados
C. Un plan de continuidad del negocio revisado que cubra todo el centro de datos
D. Un plan de reversión documentado y probado para la ventana del cambio

---

66. Unos investigadores demuestran que se pueden crear dos archivos ejecutables distintos que producen el mismo resumen SHA-1. Cuando se usa SHA-1 para verificar la autenticidad de un paquete de software descargado, ¿qué propiedad de seguridad debilita PRINCIPALMENTE esta vulnerabilidad de colisión?

Researchers demonstrate that two different executable files can be crafted to produce an identical SHA-1 digest. When SHA-1 is used to verify the authenticity of a downloaded software package, this collision vulnerability PRIMARILY undermines which security property?

A. Integridad (integrity)
B. Autorización (authorization)
C. Confidencialidad (confidentiality)
D. Disponibilidad (availability)

---

67. En una arquitectura de confianza cero (zero trust) basada en el modelo NIST SP 800-207, ¿qué componente evalúa el algoritmo de confianza con varias fuentes de datos, como la identidad, el estado del dispositivo y la inteligencia de amenazas, para tomar la decisión final de conceder o negar el acceso a un recurso?

In a zero trust architecture based on the NIST SP 800-207 model, which component evaluates the trust algorithm using multiple data sources such as identity, device posture, and threat intelligence to render the final decision to grant or deny access to a resource?

A. Motor de políticas (policy engine)
B. Sistema de diagnóstico y mitigación continuos (CDM)
C. Punto de aplicación de políticas (policy enforcement point)
D. Administrador de políticas (policy administrator)

---

68. Una empresa de servicios financieros quiere que las decisiones de acceso consideren el departamento del usuario, la clasificación de sensibilidad del archivo solicitado, la hora del día y el estado de cumplimiento del dispositivo antes de conceder el acceso. ¿Qué modelo de autorización cumple MEJOR este requisito?

A financial services company wants access decisions to consider the user's department, the sensitivity classification of the requested file, the time of day, and the device's compliance status before granting access. Which authorization model BEST satisfies this requirement?

A. Control de acceso basado en atributos (ABAC)
B. Control de acceso obligatorio (MAC)
C. Control de acceso basado en roles (RBAC)
D. Control de acceso discrecional (DAC)

---

69. A un técnico nuevo de la mesa de ayuda se le otorgan derechos de administrador local solo en las estaciones de trabajo del departamento de soporte, y no acceso de administrador en todo el dominio. ¿Qué principio de seguridad refleja esta configuración?

A new help desk technician is granted local administrator rights to only the workstations in the support department rather than domain-wide administrator access. Which security principle does this configuration reflect?

A. Confianza cero (zero trust)
B. Separación de funciones (separation of duties)
C. Mínimo privilegio (least privilege)
D. Defensa en profundidad (defense in depth)

---

70. Una gerente de finanzas firma digitalmente con su clave privada la aprobación de una transferencia bancaria, para que después no pueda negar haberla autorizado. ¿Qué concepto de seguridad ilustra MEJOR este caso?

A finance manager digitally signs a wire transfer approval using her private key so that she cannot later deny having authorized the transaction. Which security concept does this scenario BEST illustrate?

A. Autenticación (authentication)
B. No repudio (non-repudiation)
C. Confidencialidad (confidentiality)
D. Integridad (integrity)

Respuesta correcta

1. D NetFlow registra metadatos de cada conversación: IP de origen y destino, puerto, protocolo, bytes y duración. Por eso permite ver tendencias de volumen de tráfico sin el costo de almacenar el contenido. La captura completa (PCAP) da todo el detalle, pero es impráctica para vigilar de forma continua a toda la empresa. Los registros DNS no muestran cuántos datos se transfieren. Los eventos de Windows son de autenticación y acceso en el equipo.

2. A La mínima funcionalidad (least functionality) exige que un sistema ejecute solo los servicios, protocolos y cuentas necesarios para su función. Telnet, FTP y cuentas viejas sin uso amplían la superficie de ataque sin necesidad. El mínimo privilegio limita los permisos de una cuenta, no los servicios activos. La separación de funciones reparte tareas críticas entre varias personas para evitar fraude. La defensa en profundidad pone varias capas de control.

3. D Un falso positivo (false positive) ocurre cuando el escáner reporta una vulnerabilidad que no existe, como aquí, donde la verificación manual mostró que la versión con el parche sí estaba instalada. Un falso negativo es lo contrario: una vulnerabilidad real que no se detecta. Un verdadero positivo sería detectar una vulnerabilidad real, y un verdadero negativo, reportar correctamente que no hay ninguna.

4. C La cadena de custodia crea un registro continuo y verificable de quién tuvo acceso a la evidencia y cuándo, y así prueba que no fue alterada. Eso es esencial para que se admita en procesos legales o disciplinarios. El valor para el seguro y la responsabilidad económica de un departamento son temas administrativos. Los equipos incautados se conservan tal como se obtuvieron, sin mantenimiento rutinario, porque cualquier cambio dañaría la evidencia.

5. A La cadena de custodia es el registro documentado y continuo de quién manejó la evidencia, cuándo y por qué, y sirve para probar que no se alteró y que sigue siendo admisible en un proceso legal. Una retención legal es un aviso para conservar datos relevantes en un litigio. La política de retención define cuánto tiempo se guardan los datos. El orden de volatilidad indica en qué orden se recolecta evidencia en un sistema activo.

6. C El mínimo privilegio (least privilege) limita cada cuenta a los derechos de acceso necesarios para su trabajo, y da permisos elevados solo de forma temporal cuando hay justificación. La separación de funciones reparte tareas críticas entre varias personas para evitar fraude. La defensa en profundidad usa varias capas de control. La confianza cero es un modelo más amplio que verifica cada solicitud, y el mínimo privilegio es uno de sus principios.

7. A La caza de amenazas (threat hunting) es una búsqueda proactiva, basada en hipótesis, de amenazas no detectadas, con inteligencia y experiencia del analista. No es solo detección reactiva. El análisis de vulnerabilidades busca debilidades conocidas, no señales de compromiso. La correlación automática es una función pasiva del SIEM, basada en reglas. El triaje ocurre cuando ya existe una alerta o un evento reportado; la caza empieza sin alerta.

8. C El EDR (endpoint detection and response) vigila de forma continua el comportamiento de procesos, la actividad de línea de comandos y las operaciones en memoria del equipo, y por eso puede marcar un uso anómalo de PowerShell o una inyección en memoria aunque ningún archivo malicioso toque el disco. El antivirus por firmas busca patrones conocidos; la telemetría de comportamiento del EDR encaja mejor aquí. Un firewall de red no ve procesos locales. El DLP evita la fuga de datos.

9. C El cifrado de disco completo (full disk encryption) deja ilegibles todos los datos del disco sin la clave de descifrado, así que siguen siendo confidenciales aunque se saque el disco y se lea sin conexión. La segmentación de red limita el movimiento lateral, pero no protege un disco extraído. La autenticación multifactor protege el inicio de sesión, pero se evita montando el disco en otro equipo. Un IDS detecta actividad de red sospechosa, no protege datos en reposo.

10. C Deshabilitar servicios innecesarios, quitar cuentas predeterminadas y cerrar puertos sin uso elimina posibles puntos de entrada para un atacante, y eso es reducir la superficie de ataque. La segmentación divide la red en zonas aisladas, no desactiva funciones de un equipo. El mínimo privilegio limita los permisos de los usuarios. La línea base es la configuración estándar documentada; aquí se hace el endurecimiento hacia esa línea base.

11. A El orden de volatilidad prioriza la evidencia según qué tan rápido se pierde. El contenido de la RAM, las conexiones de red activas y los procesos en ejecución se pierden en cuanto se apaga el equipo, así que se capturan primero. Los archivos del disco persisten tras el apagado y pueden esperar. Los registros en un respaldo remoto ya están a salvo fuera del equipo. La documentación impresa es estática y de menor prioridad.

12. B Deshabilitar servicios innecesarios y cerrar puertos que no hacen falta reduce directamente la cantidad de puntos de entrada explotables, un paso básico del endurecimiento. El registro detallado mejora la visibilidad para detectar, pero no reduce la superficie de ataque. Un antivirus puede prevenir, detectar y eliminar malware, pero no quita servicios expuestos. Un honeypot es un sistema señuelo para estudiar atacantes, no una medida de endurecimiento.

13. B El formulario de cadena de custodia anota a cada persona que manejó la evidencia, con la fecha, la hora y el motivo de cada traspaso. Apoya la integridad y la admisibilidad de la evidencia, aunque no prueba por sí solo que no se alteró. La guía de respuesta (playbook) orienta las acciones, pero no registra el manejo de evidencia. El plan de continuidad trata de resiliencia operativa. La política de retención define cuánto se guardan los datos.

14. D RFC 3227 pone en primer lugar los registros de la CPU y la caché del procesador, porque el estado del procesador cambia muy rápido y se pierde al quitar la energía. El contenido de la RAM y los procesos, junto con las tablas de enrutamiento y la caché ARP, están en el siguiente nivel, con las estadísticas del kernel; el RFC no fija un orden separado entre ellos. Los archivos temporales del disco suelen ir después, aunque también pueden cambiar durante la adquisición.

15. D La inspección dinámica de ARP (DAI) valida los paquetes ARP contra la tabla de vinculación de DHCP snooping y descarta las respuestas ARP falsificadas, justo lo que frena este ataque de intermediario (on-path). Las VLAN limitan el alcance del dominio de difusión, pero no validan el ARP dentro de la misma VLAN. Deshabilitar puertos sin uso reduce la superficie física, pero no valida ARP en los puertos activos. WPA3 protege el wifi, no el ARP de una red cableada.

16. C El ransomware cifra los archivos de la víctima y exige un pago, normalmente en criptomonedas, a cambio de la clave de descifrado: justo el caso descrito. El spyware recopila datos en secreto sin cifrar archivos. Un rootkit oculta procesos maliciosos de las herramientas de detección, pero no extorsiona con cifrado. Una bomba lógica activa código destructivo por una condición o fecha, y no se define por exigir un rescate. Las copias de seguridad y la recuperación sin conexión son la defensa principal.

17. B El pretexting consiste en inventar un escenario creíble o una identidad falsa, aquí un ejecutivo bloqueado con urgencia, para manipular a alguien y que se salte los procedimientos normales de verificación. El tailgating es seguir físicamente a una persona autorizada por una puerta segura. El shoulder surfing es mirar a alguien mientras escribe sus credenciales. El dumpster diving es sacar de la basura material sensible desechado.

18. C El relleno de credenciales (credential stuffing) reutiliza pares de usuario y contraseña ya filtrados contra varios servicios sin relación, y aprovecha que la gente repite contraseñas. La pulverización de contraseñas (password spraying) prueba una o pocas contraseñas comunes en muchos usuarios para evitar bloqueos, sin pares válidos conocidos. La fuerza bruta adivina combinaciones. El ataque de diccionario usa una lista de contraseñas probables, no pares ya confirmados.

19. D El ransomware cifra los archivos de la víctima, cambia sus extensiones y muestra una nota de rescate que exige un pago, normalmente en criptomonedas, por la clave de descifrado: justo este caso. Un gusano se propaga solo por las redes, pero no cifra archivos ni pide pagos por sí mismo. Un rootkit busca persistencia oculta y escalar privilegios, no cifrar. Una bomba lógica activa una carga destructiva por una condición o fecha, sin extorsión.

20. A El vishing es phishing por voz, hecho en una llamada telefónica. Aquí el atacante usa una llamada en vivo para que el empleado revele un código de un solo uso, una técnica clásica para burlar la autenticación multifactor (MFA) en tiempo real. El smishing es phishing por mensajes SMS, no por llamadas. El shoulder surfing es mirar información por encima del hombro. El tailgating es seguir a alguien para entrar a un área segura.

21. C Un ataque de abrevadero (watering hole) apunta a un grupo específico al comprometer un sitio legítimo que ese grupo visita con frecuencia, y entrega contenido malicioso solo a las víctimas buscadas, como en este caso. El typosquatting registra dominios mal escritos para atrapar errores de tecleo. El XSS puede ser el mecanismo, pero describe solo la técnica de inyección, no la estrategia dirigida. El envenenamiento de DNS altera registros de resolución.

22. C Un uso sostenido y alto de CPU con calor excesivo en horas sin actividad es una señal clásica de malware de minería de criptomonedas (cryptomining), que usa en silencio la capacidad de procesamiento para minar a favor del atacante. Un cambio en el firewall bloquearía o alteraría tráfico, no subiría la CPU. Los registros faltantes del SIEM indican manipulación o una falla de registro. Los registros fuera de ciclo son entradas con horario inesperado, no síntomas de rendimiento.

23. A El pharming redirige a las víctimas a un sitio malicioso mediante manipulación a nivel de DNS, aunque el usuario escriba la URL correcta. En el typosquatting, en cambio, la redirección depende de que el usuario escriba mal el dominio. El pretexting es una técnica de ingeniería social basada en un escenario o una identidad inventada. El vishing es phishing por voz en llamadas. Como aquí se compromete un resolvedor DNS, el término preciso es pharming.

24. D Los grupos APT (advanced persistent threat) de un Estado-nación tienen mucho financiamiento, herramientas de día cero a la medida y paciencia para operaciones largas y sigilosas con fines económicos o políticos estratégicos, como los ocho meses de permanencia y la extracción dirigida de este caso. Un script kiddie no tiene la destreza para crear día cero. Un hacktivista busca disrupción pública por una causa. Una amenaza interna no intencional implica una exposición accidental.

25. D El compromiso de correo empresarial (BEC) es un ataque dirigido en el que se usa la cuenta de correo falsificada o comprometida de un ejecutivo para engañar a empleados y que transfieran fondos o datos sensibles. No hace falta malware. El typosquatting usa dominios mal escritos para llevar a sitios falsos. El abrevadero compromete un sitio que visita el objetivo. El relleno de credenciales usa pares robados de usuario y contraseña.

26. D Una amenaza interna (insider threat) es un empleado actual o antiguo que abusa de su acceso legítimo o de su conocimiento de los sistemas internos para hacer daño, como este administrador despedido con credenciales aún activas. Un hacktivista actúa por causas políticas o sociales. Un actor de Estado-nación tiene operaciones patrocinadas por un gobierno y muchos más recursos. Un script kiddie tiene poca destreza y usa herramientas ya hechas, no acceso interno legítimo.

27. A El relleno de credenciales (credential stuffing) usa pares de usuario y contraseña ya robados en una brecha anterior sin relación y los prueba en otros sitios, aprovechando que se repiten las contraseñas. La fuerza bruta adivina combinaciones desconocidas. La pulverización prueba pocas contraseñas comunes en muchas cuentas. Las tablas arcoíris son una técnica sin conexión para revertir hashes de contraseñas, no un inicio de sesión en línea con credenciales filtradas.

28. C El pretexting consiste en inventar un escenario o una identidad falsa, como un auditor, para ganarse una confianza falsa y lograr que la víctima revele información sensible. El baiting atrae a la víctima con un objeto físico o digital tentador, como una memoria USB etiquetada. El tailgating es seguir físicamente a una persona autorizada a un área segura. En el quid pro quo se ofrece un servicio o beneficio a cambio de información, y aquí no ocurre.

29. B La tolerancia al riesgo (risk tolerance) define el nivel aceptable de variación para un indicador de riesgo específico y medible, aquí un umbral de 5% de probabilidad anual de caída. El apetito de riesgo es la postura estratégica y más amplia sobre cuánto riesgo se está dispuesto a asumir para lograr los objetivos, sin un límite numérico específico. El registro de riesgos lista los riesgos identificados. La excepción de riesgo es una desviación aprobada de una política en un caso concreto.

30. D El encargado del tratamiento (data processor) maneja datos personales solo en nombre y según las instrucciones del responsable (data controller), que decide los fines y los medios del tratamiento, aquí el minorista europeo. El minorista, y no la empresa SaaS, es el responsable. El titular (data subject) es la persona a la que se refieren los datos. El delegado de protección de datos es un rol de supervisión que exige el artículo 37 del GDPR en ciertos casos.

31. B El Reglamento General de Protección de Datos (GDPR) de la UE da a los titulares el derecho de supresión ("derecho al olvido") en su artículo 17, para pedir que se eliminen sus datos personales en ciertas condiciones. HIPAA regula la información médica protegida en el sector salud de EE. UU. PCI DSS es un estándar de seguridad para datos de tarjetas de pago, no de derechos de los titulares. SOX regula la exactitud de la información financiera de empresas públicas.

32. A Comprar un ciberseguro para compensar la pérdida económica de un riesgo que no se puede corregir del todo es la definición típica de transferencia del riesgo: el impacto económico pasa a un tercero, la aseguradora. La mitigación implicaría agregar controles técnicos o de procedimiento. La evitación significa eliminar la actividad riesgosa, como retirar el sistema heredado. La aceptación es tolerar el riesgo sin ninguna acción, y aquí sí se transfiere la exposición.

33. B El SOC 2 Tipo II evalúa la efectividad operativa de los controles durante un período largo, normalmente de 6 a 12 meses, justo lo que pide el cliente: garantía histórica y no una foto de un momento. El SOC 2 Tipo I solo evalúa el diseño de los controles en un punto del tiempo. El SOC 1 se enfoca en controles de la información financiera. El AOC de PCI DSS certifica el cumplimiento de tarjetas de pago, no la seguridad general.

34. D El informe SOC 2 Tipo II evalúa si los controles operaron de forma efectiva durante una ventana de observación definida, normalmente de seis a doce meses, como se pide aquí. El SOC 2 Tipo I solo revisa si los controles están bien diseñados en un momento, sin probar su efectividad en el tiempo. El SOC 1 trata controles que afectan los estados financieros de los clientes. La ISO 27001 certifica el cumplimiento a la fecha de la auditoría, no es una atestación sobre un período.

35. B Una cláusula de derecho a auditar (right-to-audit) da a la organización la autoridad contractual de inspeccionar los controles de seguridad del proveedor y las pruebas de cumplimiento por iniciativa propia, sin que el proveedor tenga que aceptar un calendario, algo clave para supervisar el riesgo de terceros. Un NDA solo limita la divulgación de información. La fuerza mayor trata hechos fuera de control, como desastres naturales. La indemnización reparte responsabilidad por pérdidas, no da acceso de auditoría.

36. A Los marcos maduros de gestión de cambios incluyen un procedimiento de cambio de emergencia que permite una revisión y aprobación aceleradas fuera del ciclo normal, para equilibrar la urgencia con la responsabilidad. Saltarse la aprobación debilita el control de cambios y los registros de auditoría, incluso con prisa. Esperar al CAB deja el sistema expuesto e ignora la vía de emergencia que existe para esto. Avisar a los usuarios es un paso posterior a autorizar el cambio, no previo.

37. D Una auditoría externa la hace un tercero independiente ajeno a la organización, para dar garantía objetiva a reguladores, accionistas y otras partes, como al contratar una firma contable externa. Una auditoría interna la hace la propia área de auditoría de la organización y beneficia sobre todo a su dirección. Una autoevaluación de cumplimiento es una revisión interna informal, sin verificación independiente. Una evaluación de vulnerabilidades busca debilidades técnicas, no el cumplimiento financiero.

38. A El informe SOC 2 Tipo II lo prepara un auditor independiente y evalúa la efectividad operativa de los controles del proveedor durante un período largo, normalmente de seis a doce meses, justo lo que se pide. El cuestionario de autoatestación se basa en lo que dice el propio proveedor, sin validación independiente. La prueba de penetración evalúa la explotabilidad técnica en un momento, no el entorno de controles. El análisis de impacto al negocio es un documento interno de planificación.

39. C La aceptación del riesgo es apropiada cuando la probabilidad y el impacto son bajos y el costo del control supera la pérdida potencial: la gerencia reconoce el riesgo de manera formal y no hace nada más. Evitar el riesgo sería eliminar la actividad, algo innecesario con tan poca exposición. Transferir pasa el impacto económico a un tercero, como un seguro, pero aquí lo más adecuado es aceptar. Mitigar agregaría controles, y el caso dice que no son rentables.

40. B Una retención legal (legal hold) obliga a la organización a suspender los calendarios normales de retención y destrucción para conservar los registros que pueden ser relevantes en el litigio, y así evitar la destrucción de pruebas (spoliation). Borrar datos bajo una retención es ilegal y puede traer sanciones. Cifrar los registros y seguir destruyéndolos no cumple con la conservación de los datos. La custodia sigue en la organización, no en la contraparte, para mantener una cadena de custodia defendible.

41. A El riesgo residual (residual risk) es justo el riesgo que queda después de aplicar controles de mitigación, como la MFA y la segmentación; aquí, la posibilidad de robo de tokens de sesión. El riesgo inherente es la exposición antes de cualquier control. El riesgo secundario aparecería si los propios controles causaran un problema nuevo, como los ataques de fatiga de MFA. El riesgo de control es que un control falle, no una brecha que el control nunca estuvo diseñado para cerrar.

42. B El informe SOC 2 Tipo II certifica la efectividad operativa de los controles durante un período extenso, normalmente de seis a doce meses, mientras que el SOC 2 Tipo I solo confirma que los controles estaban bien diseñados en un momento concreto. Los informes SOC 1 tratan controles de información financiera, no de seguridad. El certificado ISO 27001 confirma que hay un sistema de gestión de seguridad certificado, pero no ofrece una auditoría de efectividad operativa por período.

43. A Una nube privada ofrece infraestructura dedicada a una sola organización, alojada en sus instalaciones o por un tercero, con control exclusivo y aislamiento de otros inquilinos. Una nube pública comparte la infraestructura entre muchos clientes por internet. Una nube comunitaria se comparte entre varias organizaciones con intereses comunes, como requisitos de cumplimiento. Una nube híbrida combina dos o más modelos, lo que contradice la descripción de un solo inquilino.

44. B Una VLAN (red de área local virtual) separa de forma lógica los dominios de difusión en la capa 2 y permite aislar departamentos en los mismos switches físicos, de modo que el tráfico entre ellos requiere enrutamiento y se puede controlar o bloquear. Una VPN protege el tráfico en redes no confiables como internet, no segmenta internamente. NAT traduce direcciones IP, no controla el acceso. Un balanceador de carga reparte tráfico entre servidores y no crea segmentos aislados.

45. C El error indica que el cliente no puede armar una cadena de confianza hasta una raíz de confianza, es decir, falta el certificado de la CA raíz (root CA) en su almacén de confianza; sin él, el navegador no puede validar la cadena de emisión aunque el certificado del servidor sea válido. La clave privada nunca sale del servidor y no influye en el almacén del cliente. El ticket de sesión es un recurso de reanudación de TLS. La clave de sesión simétrica se negocia después de establecer la confianza.

46. A Un hash criptográfico produce un valor único de longitud fija a partir del contenido del archivo; cualquier cambio, aunque sea de un bit, lo cambia por completo. Si coincide con el valor que publica el proveedor, se confirma la integridad. El tamaño puede coincidir aunque el contenido esté dañado. Inspeccionar un ISO binario a simple vista no es práctico. Cifrar y descifrar prueba el cifrado, no si los bytes originales se alteraron antes.

47. C DHE (y su variante de curva elíptica ECDHE) genera un par de claves nuevo y propio de cada sesión en cada negociación y descarta la clave privada efímera después, así que comprometer más adelante la clave estática del certificado del servidor no permite descifrar sesiones ya capturadas. Eso es la confidencialidad directa perfecta (perfect forward secrecy). Con RSA estático se descifra todo el pasado al obtener la clave. Una PSK sin DH efímero reutiliza el mismo secreto. Kerberos es de autenticación.

48. A La criptografía ligera (lightweight cryptography) está diseñada para dar seguridad adecuada con poca carga de cómputo, poco gasto de batería y poca memoria, algo clave para dispositivos embebidos e IoT con recursos limitados. Elegir el algoritmo más fuerte sin pensar en los recursos puede agotar la batería y causar fallas de rendimiento. Los algoritmos poscuánticos suelen necesitar claves más grandes y más procesamiento. DES está obsoleto y roto.

49. B Un air gap aísla físicamente un sistema o una red, sin conexión por cable ni inalámbrica a ninguna otra red, y hace imposibles los ataques remotos por red contra ese segmento. Una subred filtrada mantiene conectividad controlada mediante firewalls, a diferencia de un air gap real. La confianza cero es una filosofía de acceso que verifica cada conexión, no un aislamiento físico. La microsegmentación crea zonas lógicas finas dentro de una red conectada, lo opuesto a no tener conexión.

50. D La microsegmentación aplica políticas de firewall detalladas a nivel de carga de trabajo, que permiten el tráfico este-oeste necesario entre las dos máquinas virtuales y a la vez bloquean el movimiento lateral no autorizado, aunque compartan VLAN y subred. Crear una VLAN por máquina rompería el requisito de la misma subred y no escala. Un IDS en modo promiscuo solo detecta. La seguridad de puertos controla las MAC del puerto físico, no la comunicación de aplicaciones.

51. C El balanceo de carga activo-pasivo con failover automático mantiene un servidor en espera listo para tomar el control cuando falla el activo, lo que apoya la alta disponibilidad con una interrupción mínima. Las configuraciones activo-activo reparten el tráfico entre varios servidores activos. El cifrado de disco protege la confidencialidad, no la disponibilidad. Un solo punto de presencia con reinicio manual causa caídas y es un punto único de falla. Un respaldo apagado no puede tomar el control solo.

52. B Las firmas digitales usan la clave privada del firmante, así que solo ese proveedor pudo crearlas. Al verificarlas con su clave pública se prueba el origen y se le impide negar la autoría: eso es el no repudio (non-repudiation). El cifrado simétrico protege la confidencialidad, no prueba el origen, y usa una clave compartida que ambas partes podrían usar. El balanceo de carga trata de la disponibilidad. Un hash solo verifica integridad, no identidad, porque cualquiera puede calcularlo.

53. B Un air gap aísla una red de forma física y lógica de todas las demás, incluidos internet y la TI corporativa, y elimina las rutas de ataque remoto. Es un control común en entornos críticos SCADA/ICS, donde la disponibilidad y la seguridad pesan más que la conectividad. Una subred filtrada sigue permitiendo conectividad externa controlada por firewalls. Un servidor de salto es un punto de acceso controlado, que implica que hay conexión. Una VPN crea un túnel cifrado, lo contrario del aislamiento.

54. C Las credenciales predeterminadas junto con una red plana, al lado de sistemas financieros sensibles, son el mayor riesgo inmediato de compromiso y movimiento lateral. Cambiar las credenciales y aislar los dispositivos IoT en su propia VLAN cierra a la vez la brecha de autenticación y la exposición de red. Actualizar el firmware con más frecuencia es buena práctica, pero no atiende el riesgo inmediato. Deshabilitar SNMP en finanzas no arregla el IoT. La geocerca no se relaciona con este riesgo de red.

55. A Con OCSP stapling, el servidor web consulta a la CA cada cierto tiempo y adjunta a la negociación TLS la respuesta OCSP firmada y con sello de tiempo. El cliente nunca contacta a la CA, así que no se revela qué sitios visita y se evita el viaje extra. La consulta OCSP estándar obliga al cliente a preguntar a la CA en tiempo real, con fuga de patrones y más demora. Las CRL son grandes, se actualizan poco y el cliente debe descargarlas. El certificate pinning define en qué certificado se confía, no cómo se entrega la revocación.

56. B El nivel 1 (control básico) es donde están los PLC, las RTU y otros controladores que ejecutan lógica de control en tiempo real y se comunican directamente con los dispositivos del nivel 0. El nivel 0 es el proceso físico en sí: sensores, válvulas y motores, no los controladores. El nivel 2 cubre funciones de supervisión de área, como HMI y software supervisorio SCADA que agrupan varios controladores del nivel 1. El nivel 3 maneja las operaciones de todo el sitio, como la programación de producción.

57. C Un plan de reversión define los pasos exactos para devolver el sistema al último estado en que funcionaba bien, y eso determina directamente qué tan rápido se restablece el servicio cuando hay una interrupción. El análisis de impacto dice quién resulta afectado, pero no da un procedimiento de recuperación. La firma de aprobación es un trámite de gobierno. Las pruebas en sandbox reducen la probabilidad de falla antes, pero no ayudan cuando el cambio ya causó una caída en producción.

58. D Los controles detectivos (detective) identifican un evento de seguridad y alertan mientras ocurre o después, justo lo que hace una alarma de movimiento al avisar al personal cuando hay un movimiento no autorizado. Un control preventivo evitaría la entrada, como una puerta con cerradura o un lector de credenciales. Un control correctivo actúa después de un incidente para restaurar o arreglar sistemas. Un control disuasorio desanima al atacante, como un letrero de advertencia visible.

59. B La energía redundante, el RAID 10 y el clúster de failover eliminan puntos únicos de falla para que el sistema siga accesible ante una falla de hardware, y eso es la disponibilidad. La confidencialidad no aplica, porque ninguno de estos controles limita quién puede ver los datos. La integridad no aplica, porque no verifican que los datos no se alteraron. El no repudio no forma parte de la tríada CIA y trata de la prueba de una acción, no del tiempo de actividad.

60. A La separación de funciones reparte las tareas críticas entre varias personas, de modo que nadie pueda completar solo un proceso de alto riesgo, lo que reduce las oportunidades de fraude y error. El mínimo privilegio limita el acceso de un usuario a lo que necesita su rol, pero no divide un proceso entre dos personas. La rotación de puestos cambia a los empleados de rol para descubrir fraudes con el tiempo. Las vacaciones obligatorias permiten que otros revisen el trabajo; es una medida detectiva.

61. D La autorización ocurre después de verificar la identidad y define los permisos o derechos de acceso concretos de un usuario, a menudo con control de acceso basado en roles (RBAC). La autenticación solo confirma la identidad declarada con credenciales. La contabilidad (accounting) registra la actividad del usuario para auditoría, no decide permisos. La identificación es solo la declaración inicial de identidad, como escribir un nombre de usuario, antes de cualquier verificación.

62. A Confianza cero (zero trust) funciona con "nunca confiar, siempre verificar": exige autenticación y autorización continuas en cada solicitud de acceso, venga de dentro o de fuera del límite tradicional de la red. La defensa perimetral confía de forma implícita en quien ya está dentro del borde, lo contrario. La defensa en profundidad describe capas de controles, no un modelo de confianza. El RBAC es un método de autorización que se usa dentro de zero trust, no el modelo general.

63. D Alterar datos en tránsito es una modificación no autorizada de la información, que es la definición de una violación de integridad. La confidencialidad se vería afectada si el atacante solo hubiera visto o extraído los datos sin cambiarlos. La disponibilidad trata de la negación de acceso o servicio; la transacción se procesó, pero con datos alterados. El no repudio no es uno de los tres principios de la tríada CIA, sino un concepto de responsabilidad relacionado.

64. C Esto describe un comité asesor de cambios (CAB, Change Advisory Board), cuyo papel principal es evaluar el riesgo, el impacto y el plan de reversión de los cambios propuestos antes de aprobarlos o rechazarlos, para reducir las caídas imprevistas. La instalación técnica corresponde a los administradores de sistemas. El plan de respuesta a incidentes es otra función de planificación. La capacitación de concientización es un control operativo ajeno al control de cambios.

65. D Un plan de reversión documentado y probado para la ventana del cambio se evalúa antes de implementar y está pensado para restaurar con rapidez el estado anterior conocido si el cambio falla, lo que reduce la caída. Un plan de continuidad ayuda ante interrupciones, pero sirve menos para revertir este cambio concreto. El inventario ayuda a identificar sistemas afectados, pero no reduce el impacto de una falla. La plantilla de informe posterior es reactiva y no mitiga durante la falla.

66. A Una colisión de hash permite que un atacante reemplace el archivo legítimo por uno malicioso que produce el mismo resumen, y así anula el propósito del hash de probar que el archivo no fue alterado: eso es la integridad. La confidencialidad trata de la divulgación no autorizada de datos, que una colisión no afecta. La disponibilidad se refiere al tiempo de actividad de los sistemas. La autorización define lo que un sujeto autenticado puede hacer, y no tiene relación con verificar el contenido de un archivo.

67. A El motor de políticas (policy engine) es el componente que decide dentro del punto de decisión de políticas: ejecuta el algoritmo de confianza con datos como la identidad, el cumplimiento del dispositivo y la inteligencia de amenazas, y da la decisión de permitir o negar. El punto de aplicación de políticas es el guardián que abre o cierra la conexión según esa decisión, pero no decide. El administrador de políticas genera las credenciales de sesión. El CDM solo aporta datos del estado del dispositivo.

68. A El ABAC evalúa varios atributos dinámicos del sujeto, del recurso y del entorno (departamento, clasificación del archivo, hora y cumplimiento del dispositivo) para dar una decisión de acceso en tiempo real, y es base de zero trust. El RBAC solo considera el rol asignado, sin ese detalle de contexto. En el DAC, el dueño del recurso fija los permisos a su criterio, sin evaluar atributos del entorno. El MAC usa etiquetas y autorizaciones fijas, sin tener en cuenta el dispositivo ni la hora.

69. C El mínimo privilegio limita los derechos de acceso de un usuario a lo mínimo necesario para su trabajo, como limitar al técnico a las estaciones de su departamento y no a todo el dominio. La separación de funciones divide una tarea entre varias personas, no acota el acceso de una sola. La defensa en profundidad pone varias capas independientes de controles. La confianza cero es un modelo más amplio que verifica cada solicitud, distinto de solo minimizar los derechos otorgados.

70. B El no repudio usa mecanismos criptográficos, como las firmas digitales ligadas a una clave privada, para probar el origen de una acción e impedir que el firmante niegue después su participación. La confidencialidad no aplica, porque el caso no trata de ocultar la transferencia a terceros. La integridad solo asegura que el mensaje no se alteró, no que el emisor sea responsable. La autenticación verifica identidad u origen, pero el no repudio es lo que evita la negación de una acción firmada.

Palabras clave en inglés

CIA triad	tríada CIA	Confidencialidad, integridad y disponibilidad: las tres metas de la seguridad.
authentication	autenticación	Comprobar que alguien es quien dice ser.
authorization	autorización	Decidir qué puede hacer un usuario ya autenticado.

accounting	contabilidad, registro de actividad	Guardar qué hizo cada usuario y cuándo. Tercera A de AAA.
non-repudiation	no repudio	Prueba que impide negar que enviaste o firmaste algo.
zero trust	confianza cero	Modelo que no confía por defecto y verifica cada acceso.
compensating control	control compensatorio	Control alternativo cuando no puedes aplicar el principal.
change management	gestión de cambios	Proceso para aprobar, probar y documentar cambios en los sistemas.
least privilege	mínimo privilegio	Dar solo los permisos necesarios para hacer el trabajo.
multifactor authentication (MFA)	autenticación multifactor	Inicio de sesión con dos o más factores de tipo distinto.
threat actor	actor de amenaza	Persona o grupo que realiza o intenta un ataque.
insider threat	amenaza interna	Riesgo que viene de alguien con acceso dentro de la organización.
attack surface	superficie de ataque	Todos los puntos por donde un atacante podría entrar.
zero-day vulnerability	vulnerabilidad de día cero	Falla que se ataca antes de que exista un parche.
social engineering	ingeniería social	Engañar a personas para obtener datos o acceso.
phishing	phishing, suplantación de identidad	Mensaje falso que busca robar datos o instalar malware.
business email compromise (BEC)	compromiso del correo empresarial	Fraude con una cuenta de correo de trabajo falsificada o controlada por el atacante.
typosquatting	typosquatting, dominio con error tipográfico	Registrar un dominio casi igual al real para engañar.
ransomware	ransomware, secuestro de datos	Malware que cifra datos y pide un pago.
indicator of compromise (IoC)	indicador de compromiso	Señal de que un sistema pudo haber sido vulnerado.
patch	parche	Actualización que corrige una falla del software.
hardening	endurecimiento	Reducir riesgos al quitar servicios, accesos y ajustes inseguros.
SIEM	gestión de información y eventos de seguridad	Reúne y correlaciona registros de muchas fuentes.
SOAR	orquestación, automatización y respuesta de seguridad	Automatiza los pasos de respuesta ante un incidente.
EDR	detección y respuesta en endpoints	Vigila computadoras y servidores y puede aislar un equipo.

DLP	prevención de pérdida de datos	Detecta y frena la salida de datos sensibles.
IDS / IPS	sistema de detección / prevención de intrusiones	El IDS avisa de un ataque; el IPS puede bloquearlo.
incident response	respuesta a incidentes	Proceso ordenado para manejar un ataque y recuperarse.
containment	contención	Limitar el daño para que el incidente no se extienda.
chain of custody	cadena de custodia	Registro de quién tuvo la evidencia, cuándo y para qué.
false positive	falso positivo	Alerta sobre algo que en realidad no es un problema.
encryption	cifrado	Transformar datos para que no se puedan leer sin la clave.
hashing	hashing, función hash	Crea una huella de los datos para comprobar su integridad.
digital signature	firma digital	Prueba quién firmó y que el contenido no cambió.
public key infrastructure (PKI)	infraestructura de clave pública	Sistema que emite, administra y revoca certificados digitales.
CRL / OCSP	lista de revocación de certificados / protocolo de estado de certificados en línea	CRL reúne los certificados revocados; OCSP consulta el estado de uno.
segmentation	segmentación	Dividir la red en partes para limitar el movimiento del atacante.
RPO (recovery point objective)	objetivo de punto de recuperación	Cuántos datos puedes perder, medido en tiempo.
RTO (recovery time objective)	objetivo de tiempo de recuperación	Tiempo máximo previsto para que el sistema vuelva a funcionar.
risk register	registro de riesgos	Documento con cada riesgo, su nivel, responsable y respuesta.
threat hunting	caza de amenazas	Búsqueda proactiva de amenazas no detectadas, a partir de una hipótesis.
pretexting	pretexting (pretexto)	Engaño con una identidad o un escenario inventado para obtener información.
watering hole attack	ataque de abrevadero	Compromete un sitio legítimo que visita el grupo objetivo.
credential stuffing	relleno de credenciales	Prueba pares de usuario y contraseña filtrados en otros servicios.
residual risk	riesgo residual	Riesgo que queda después de aplicar los controles.

risk tolerance	tolerancia al riesgo	Nivel de riesgo específico y medible que la organización acepta.
air gap	aislamiento físico (air gap)	Red sin ninguna conexión con otras redes.
ABAC	control de acceso basado en atributos	Decide el acceso según atributos del usuario, del recurso y del entorno.
legal hold	retención legal	Orden de conservar registros relevantes para un litigio.

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/comptia-security-plus/