UAM

Universidad Autónoma de Madrid

PRUEBAS SELECTIVAS PARA EL INGRESO EN LA ESCALA ESPECIAL SUPERIOR DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE MADRID.

CONVOCADO POR RESOLUCIÓN DE 13 DE ENERO DE 2026.

SEGUNDO EJERCICIO TEÓRICO

11 de junio de 2026

No pasar esta página hasta que lo indique el tribunal

1) **En el ENS, la seguridad se concibe como:**

a) La adopción periódica de herramientas y productos de seguridad según la evolución tecnológica.
b) Una obligación fundamentalmente documental orientada a justificar cumplimiento ante auditorías.
c) Un proceso integral, continuo y gestionado que debe mantenerse a lo largo del ciclo de vida del sistema.
d) Una responsabilidad operativa concentrada principalmente en el área de sistemas y administración técnica.

2) **En la estructura de roles del ENS, ¿qué afirmación es correcta?**

a) El responsable de la seguridad determina los fines y el uso del servicio.
b) El responsable del sistema no participa en la implantación ni supervisión de medidas de seguridad.
c) Los roles del ENS solo son exigibles en sistemas de categoría media o alta.
d) La segregación de responsabilidades reduce conflictos de interés y mejora el control sobre el sistema.

3) **La categoría de un sistema según el ENS se determina en función de:**

a) El impacto sobre la confidencialidad, la integridad y la disponibilidad de la información y los servicios.
b) El coste del proyecto y la tecnología implantada.
c) El tipo de dato personal tratado, con independencia del resto de dimensiones del sistema.
d) El nivel de exposición a ataques desde internet como criterio de categorización.

4) **Es una medida organizativa del ENS:**

a) La obligación de emplear cifrado asimétrico en todos los sistemas, con independencia de su contexto.
b) La definición de políticas, normas, procedimientos y responsabilidades.
c) La implantación de un firewall de nueva generación como sustituto del resto de controles.
d) La sustitución del análisis de riesgos por la sola existencia de una política de seguridad.

5) **En gestión de incidentes de seguridad, la fase de contención tiene como objetivo:**

a) Identificar el origen exacto del ataque y documentarlo completamente.
b) Eliminar definitivamente el malware del sistema afectado.
c) Limitar la propagación del incidente y reducir su impacto inmediato.
d) Restaurar los sistemas a su estado operativo normal.

6) **Una exigencia de NIS2 es:**

a) Mejorar indicadores generales de soberanía digital sin obligaciones concretas de gestión y notificación.
b) Prohibir el uso de servicios cloud en entidades esenciales y sustituirlos por infraestructuras propias.
c) Sustituir el ENS como marco de seguridad aplicable al sector público español.

d) Implantar medidas de gestión de riesgos y notificar incidentes significativos a la autoridad competente.

7) En un SOC, la priorización de alertas se realiza en función de:

a) El volumen de eventos generados por cada sistema.
b) El impacto potencial y la criticidad del activo afectado.
c) El número de herramientas implicadas en la detección.
d) El tiempo que lleva abierta la alerta.

8) En protección de datos, una EIPD o DPIA procede cuando:

a) Cualquier tratamiento se externaliza, con independencia de su naturaleza y nivel de riesgo.
b) El delegado de protección de datos lo recomienda, aunque no concurran criterios de alto riesgo.
c) Puede existir un alto riesgo para los derechos y libertades de las personas físicas.
d) Se cifra la base de datos, aunque el tratamiento no implique riesgo elevado.

9) La notificación de una brecha de datos personales debe valorarse según:

a) El riesgo para los derechos y libertades de las personas afectadas.
b) El volumen de datos afectados, con independencia del impacto real sobre las personas afectadas.
c) Si los datos exfiltrados son de carácter básico, sin valorar el contexto ni las consecuencias.
d) Si el tratamiento no figura en el registro de actividades de tratamiento.

10) El reglamento EIDAS se vincula con:

a) La clasificación de la información y el etiquetado de seguridad documental.
b) La seguridad del puesto de trabajo y el endurecimiento de estaciones de usuario.
c) La protección de datos personales y la privacidad como marco principal de cumplimiento.
d) La identidad electrónica y los servicios de confianza para transacciones electrónicas.

11) En el ENI, la interoperabilidad semántica tiene como finalidad principal que la información intercambiada entre sistemas y administraciones:

a) Se tramite siempre mediante una única plataforma común de intercambio entre administraciones.
b) Se conserve obligatoriamente en formatos ofimáticos normalizados para asegurar su archivo electrónico.
c) Mantenga un significado común, inequívoco y reutilizable para todos los sistemas que la procesan.
d) Circule exclusivamente a través de canales cifrados y con firma electrónica reconocida.

12) ¿Cuál es el principal riesgo de almacenar credenciales directamente en código fuente o scripts?

a) Aumento del consumo de CPU.
b) Dificultad para ejecutar el código en producción.
c) Exposición de credenciales si el código es accesible o se filtra.
d) Incompatibilidad con sistemas operativos modernos.

13) COBIT se emplea para:

a) Establecer un marco de gobierno y gestión de las TIC alineado con los objetivos del negocio y el control de riesgos.
b) Implantar exclusivamente controles técnicos de seguridad perimetral en redes y sistemas.
c) Regular el tratamiento de datos personales y garantizar el cumplimiento específico de la normativa de privacidad.
d) Definir formatos y mecanismos comunes para el intercambio automatizado de información entre sistemas.

14) ITIL 4 está orientado a:

a) La categorización formal de sistemas según impacto en confidencialidad, integridad y disponibilidad.
b) La regulación de la identidad electrónica y de los servicios de confianza cualificados.
c) La gestión de servicios TIC y la mejora del valor entregado al usuario y al negocio.
d) El intercambio estructurado de inteligencia de amenazas entre organizaciones y plataformas.

15) ¿Qué organismo está directamente asociado al apoyo y coordinación en ciberseguridad del sector público en España?

a) INE.
b) CCN-CERT.
c) ICO.
d) CNMC.

16) MAGERIT v3 se utiliza para:

a) Definir requisitos de desarrollo seguro específicos para aplicaciones web.
b) Implantar medidas obligatorias de privacidad y cumplimiento específico del RGPD.
c) Emitir certificados electrónicos cualificados y gestionar su revocación.
d) Analizar y gestionar riesgos sobre sistemas de información y sus activos.

17) En MAGERIT, un activo es:

a) Un componente físico inventariado, siempre que tenga identificación patrimonial.
b) El resultado de combinar amenaza, vulnerabilidad e impacto en un escenario de riesgo.
c) Cualquier elemento con valor para la organización y relevante para la prestación del servicio.
d) Exclusivamente la información clasificada o especialmente sensible tratada por el sistema.

18) ¿Cuál es la finalidad principal de una autoridad de certificación (CA) en una PKI?

a) Cifrar directamente los datos de los usuarios.
b) Emitir certificados digitales que vinculan identidad y clave pública.
c) Almacenar contraseñas de forma segura.
d) Gestionar el tráfico de red entre sistemas.

19) En análisis forense, ¿por qué es importante realizar una copia de la evidencia antes de analizarla?

a) Para mejorar el rendimiento del análisis.
b) Para evitar modificar la evidencia original.
c) Para reducir el tamaño de los datos.
d) Para acelerar la recuperación del sistema.

20) ¿Qué mecanismo se utiliza para conceder permisos temporales elevados a un usuario?

a) Hardening.
b) Privilegios permanentes.
c) Elevación de privilegios controlada (just-in-time).
d) Segmentación de red.

21) El objetivo de un DRP (Disaster Recovery Plan):

a) Prevenir incidentes de confidencialidad mediante controles criptográficos y de control de acceso.
b) Garantizar la continuidad de los procesos críticos de negocio durante la disrupción sin foco específico en la recuperación tecnológica.
c) Recuperar infraestructuras, sistemas y servicios tecnológicos tras una contingencia grave.
d) Clasificar activos de información y asignar niveles de criticidad patrimonial para su reposición.

22) ¿Qué característica define una copia de seguridad inmutable?

a) Puede modificarse por administradores autorizados.
b) Se replica automáticamente en múltiples ubicaciones.
c) No puede alterarse ni eliminarse durante un periodo definido.
d) Se almacena únicamente en la nube.

23) ¿Qué tecnología permite obtener visibilidad del tráfico de red sin intervenir directamente en él?

a) Firewall.
b) Switch de acceso.
c) Mirror/SPAN o TAP de red.
d) Balanceador de carga.

24) En auditoría de seguridad, la independencia del auditor favorece en:

a) Reducir la probabilidad de conflictos de interés y reforzar la objetividad de las conclusiones.
b) Incrementar automáticamente el número y la profundidad de las evidencias obtenidas.
c) Sustituir la necesidad de planificación, muestreo y contraste de evidencias durante la auditoría.
d) Limitar el uso de entrevistas y reuniones para evitar influencias del auditado sobre el auditor.

25) La privacidad desde el diseño implica:

a) Añadir controles de protección de datos al final del proyecto antes de pasar a producción.
b) Trasladar la responsabilidad de privacidad a un especialista externo independiente del tratamiento.
c) Incorporar requisitos y salvaguardas de privacidad desde la concepción del tratamiento y durante todo su ciclo de vida.
d) Sustituir la evaluación de impacto por controles técnicos avanzados siempre que exista cifrado robusto.

26) El principio de minimización de datos exige:

a) Conservar toda la información disponible por si pudiera resultar útil en tratamientos futuros.
b) Anonimizar obligatoriamente cualquier tratamiento que incluya datos personales identificativos.
c) Reducir el volumen de almacenamiento sin necesidad de revisar finalidad, base jurídica ni proporcionalidad.
d) Tratar solo los datos adecuados, pertinentes y limitados a lo necesario para la finalidad perseguida.

27) Una CMDB aporta valor porque:

a) Sustituye el registro de tratamientos y los análisis jurídicos necesarios en protección de datos.
b) Mantiene información estructurada sobre elementos de configuración y sus relaciones para apoyar operación, cambios e impacto.
c) Elimina la necesidad de procesos de control de cambios si la información técnica está correctamente inventariada.
d) Reemplaza el catálogo de servicios al describir activos técnicos, contratos y responsables de negocio en un único repositorio.

28) Un KPI se utiliza para medir:

a) La exposición residual al riesgo y su evolución para facilitar decisiones de tratamiento.
b) La probabilidad técnica de explotación de vulnerabilidades detectadas en activos expuestos.
c) El rendimiento, el nivel de servicio o el grado de consecución de objetivos definidos.
d) El nivel de apetito al riesgo definido o aprobado por la dirección.

29) ¿Qué indicador sería más adecuado como KPI en un SOC?

a) Número de ataques globales en internet.
b) Tiempo medio de detección de incidentes.
c) Número de empleados de la organización.
d) Capacidad total de almacenamiento.

30) En un enfoque Zero Trust, la premisa correcta es:

a) Confiar por defecto en la red interna y reforzar solo los accesos procedentes del exterior.
b) Validar explícitamente cada solicitud de acceso según identidad, contexto, dispositivo y nivel de riesgo.
c) Asumir que la autenticación inicial del usuario es suficiente para mantener acceso persistente a múltiples recursos.
d) Sustituir la gestión de identidades y privilegios por listas estáticas de confianza definidas por segmento de red.

31) La arquitectura ZTNA tiene como objetivo:

a) Cifrado simétrico de copias de seguridad para reforzar la protección de la información en reposo.
b) Automatización de respuestas del SOC mediante playbooks y orquestación entre herramientas.
c) Acceso remoto y segmentado basado en identidad, contexto y verificación continua del acceso.
d) Autenticación de acceso a red cableada o inalámbrica mediante 802.1X y validación del dispositivo.

32) SASE combina de forma característica:

a) Servicios de red y capacidades de seguridad entregados de forma convergente desde la nube.
b) Infraestructuras PKI corporativas y gestión centralizada del ciclo de vida de claves y certificados.
c) Copias de seguridad inmutables y planes de recuperación ante desastres integrados con orquestación.
d) Capacidades de análisis forense, threat hunting y sandboxing unificadas para investigación avanzada.

33) En una estrategia multicloud, un reto de seguridad y gobierno es:

a) Depender de un único proveedor para todos los servicios críticos, reduciendo la capacidad de negociación y resiliencia.
b) Carecer de mecanismos nativos de cifrado, control de acceso y registro en las plataformas cloud actuales.
c) No poder aplicar segmentación lógica ni definir redes virtuales aisladas en entornos cloud modernos.
d) Mantener políticas, identidades, configuraciones y registros coherentes entre distintos proveedores y servicios.

34) En cloud, el control plane hace referencia a:

a) El cableado físico, la refrigeración y la distribución eléctrica interna del centro del proveedor.
b) La capa de administración, orquestación y control de recursos y servicios de la plataforma.
c) El conjunto de repositorios dedicados exclusivamente a copias offline y recuperación ante desastres.
d) El plano dedicado únicamente al tránsito de datos de usuario entre zonas, regiones o redes virtuales.

35) Desde una perspectiva de seguridad, la segmentación de red, incluida la microsegmentación, tiene como objetivo:

a) Simplificar la administración de direccionamiento y reducir cambios operativos en la topología de red.
b) Sustituir los controles de identidad, autenticación y autorización al imponer aislamiento suficiente entre segmentos.
c) Limitar los movimientos laterales y aplicar políticas de comunicación más granulares entre sistemas, servicios o cargas de trabajo.
d) Evitar la necesidad de cifrado en tránsito al quedar el tráfico restringido a dominios internos considerados de confianza.

36) Una arquitectura de alta disponibilidad se basa en:

a) Un único nodo sobredimensionado, configurado para absorber picos y mantener continuidad por capacidad.
b) Segmentación lógica de red suficiente para aislar fallos, sin necesidad de redundar componentes críticos.
c) Escalado vertical de un único sistema crítico como mecanismo principal de continuidad del servicio.
d) Redundancia de componentes y mecanismos de conmutación para sostener el servicio ante fallos.

37) Cuál de las siguientes medidas deben estar presentes en la seguridad física de un CPD:

a) Controlar el acceso físico y mantener condiciones ambientales seguras para proteger equipos y servicio.
b) Desplegar redes inalámbricas seguras específicas para mantenimiento, con cobertura amplia en toda la sala técnica.
c) Aplicar políticas documentales de clasificación sobre soportes físicos como medida principal de protección del CPD.
d) Centralizar la monitorización de eventos para sustituir controles de acceso, videovigilancia y protección ambiental.

38) MITRE ATT&CK se utiliza para:

a) Redactar y mantener planes de continuidad de negocio y recuperación ante desastres.
b) Modelar tácticas, técnicas y procedimientos observados en el comportamiento de adversarios.
c) Puntuar vulnerabilidades con una métrica estandarizada de severidad técnica y contexto ambiental.
d) Definir protocolos concretos de defensa y topologías de red recomendadas frente a cada técnica atacante.

39) MITRE D3FEND complementa a ATT&CK porque:

a) Sustituye la necesidad de detecciones al proporcionar controles suficientes frente a cualquier técnica adversaria.
b) Puntúa de forma financiera el impacto del incidente para priorizar inversiones y planes de aseguramiento.
c) Describe técnicas defensivas y contramedidas que ayudan a mapear y reforzar la respuesta frente a TTPs adversarias.
d) Evita el uso de TTPs como referencia y se centra exclusivamente en métricas de cumplimiento normativo.

40) Según el ENS, además de confidencialidad, integridad y disponibilidad, un atributo de la seguridad de la información es:

a) Escalabilidad.
b) Autenticidad.
c) Rendimiento.
d) Redundancia.

41) Una función hash criptográfica se caracteriza por:

a) Producir una huella normalmente de longitud fija, siendo determinista y diseñada para dificultar colisiones e inversión.
b) Ser reversible siempre que se disponga de una clave de descifrado suficientemente robusta.
c) Sustituir por sí sola a la firma digital al garantizar autenticidad, integridad y no repudio.
d) Cifrar información mediante criptografía de clave pública para proteger su confidencialidad.

42) En cifrado asimétrico, lo correcto es afirmar que:

a) Utiliza una única clave compartida para cifrado, descifrado y firma.
b) No permite mecanismos de firma digital y se limita a proteger la confidencialidad del mensaje.
c) Emplea un par de claves relacionado matemáticamente, una pública y otra privada, con usos complementarios.

d) Debe implementarse obligatoriamente con curvas elípticas para ser considerado seguro.

43) En una PKI, OCSP y CRL se utilizan para:

a) Autenticar usuarios de forma interactiva sin necesidad de validar el ciclo de vida del certificado.
b) Comprobar el estado de revocación de certificados emitidos por una autoridad de certificación.
c) Emitir tokens criptográficos de tipo JWT para sesiones web y APIs federadas.
d) Evaluar la fortaleza criptográfica del certificado a partir del algoritmo y la longitud de clave utilizados.

44) El protocolo estandarizado se utiliza para automatizar la emisión y renovación de certificados es:

a) REST como protocolo estándar específico de validación, emisión y renovación automática.
b) REST y SCEP combinados como estándar universal para cualquier PKI pública o privada.
c) TTLS junto con interfaces REST de administración genéricas.
d) ACME.

45) El principio de mínimo privilegio persigue:

a) Limitar cada acceso o permiso a lo estrictamente necesario para desempeñar la función autorizada.
b) Conceder permisos amplios inicialmente y reducirlos solo si se detecta un uso indebido.
c) Homogeneizar perfiles para simplificar administración, aunque se concedan permisos no necesarios.
d) Asignar privilegios temporales de baja prioridad sin relación directa con las tareas reales del usuario.

46) En un modelo RBAC, los permisos se asignan en función de:

a) La dirección IP o el segmento de red desde el que accede el usuario.
b) Una combinación dinámica de atributos del sujeto, recurso y contexto de acceso.
c) Decisiones individuales definidas caso por caso para cada usuario sin intermediación de roles.
d) El rol o función asignada al usuario dentro de la organización.

47) ABAC permite tomar decisiones de acceso basadas en:

a) Una lista cerrada de administradores autorizados a conceder o denegar accesos manualmente.
b) Atributos del sujeto, del recurso, de la acción y del contexto en el momento del acceso.
c) Direcciones MAC exclusivamente, como identificador suficiente para autorizar cualquier acceso.
d) Roles predefinidos y la categoría ENS del sistema como únicos criterios de autorización.

48) El SSO federado con SAML se utiliza para:

a) Compartir claves simétricas entre aplicaciones para evitar autenticaciones repetidas del usuario.
b) Intercambiar tokens de autorización delegada entre APIs sin necesidad de autenticación del usuario final.
c) Autenticar usuarios entre dominios o aplicaciones mediante aserciones de identidad intercambiadas entre proveedor de identidad y proveedor de servicio.
d) Propagar atributos de identidad sin requerir autenticación previa del usuario ante un proveedor de identidad.

49) OpenID Connect (OIDC) se basa en:

a) OAuth 2.0, al que añade una capa de identidad y autenticación.
b) DNSSEC, utilizando registros firmados para validar identidad y sesión del usuario.
c) Kerberos, como protocolo base obligatorio para cualquier implementación de identidad federada moderna.
d) SAML 2.0, del que hereda directamente el formato de token y los flujos de autenticación.

50) FIDO2 y las passkeys tienen como objetivo:

a) Sustituir de forma general el uso de certificados digitales en cualquier escenario de identidad o confianza.
b) Resolver principalmente problemas de autorización entre aplicaciones corporativas y APIs de terceros.
c) Obligar al uso de biometría como único factor válido para cualquier autenticación moderna.
d) Reforzar la autenticación y reducir la dependencia de contraseñas tradicionales mediante credenciales resistentes al phishing.

51) Un SOC tiene como misión central:

a) Definir el modelo corporativo de gobierno de seguridad y aprobar la política de riesgos.
b) Verificar el cumplimiento normativo de proveedores y custodiar evidencias para auditorías periódicas.
c) Centralizar la monitorización, el análisis de alertas y la coordinación de la respuesta ante incidentes.
d) Operar herramientas de seguridad y escalar eventos técnicos sin asumir funciones de coordinación.

52) Un SIEM aporta valor porque:

a) Normaliza, agrega y correlaciona eventos de múltiples fuentes para facilitar detección e investigación.
b) Consolida la administración de sondas de red y reemplaza la visibilidad de tráfico este-oeste.

c) Traslada la retención de registros al origen, por lo que reduce la necesidad de políticas centralizadas de conservación.
d) Inspecciona tráfico en línea y aplica bloqueo automático sobre sesiones maliciosas a nivel de aplicación.

53) UEBA resulta útil para:

a) Establecer canales cifrados y autenticados entre cargas de trabajo para reducir exposición lateral.
b) Identificar desviaciones respecto a patrones habituales de comportamiento de usuarios y otros activos relevantes.
c) Emitir y validar credenciales de acceso delegadas para aplicaciones y APIs de confianza.
d) Comprobar desviaciones de configuración en plantillas de infraestructura antes de su promoción a producción.

54) Un SOAR se asocia con:

a) La distribución inteligente de tráfico entre sedes y regiones para sostener continuidad de servicio.
b) La planificación y ejecución de políticas de copia, retención y restauración sobre infraestructuras críticas.
c) La emisión y el ciclo de vida de credenciales de máquina y certificados para servicios corporativos.
d) La orquestación de flujos y la automatización de acciones de respuesta apoyadas en playbooks.

55) En gestión de vulnerabilidades, CVSS v4 se usa para:

a) Mantener una taxonomía operativa de activos y dependencias para apoyar el análisis de impacto.
b) Cuantificar el coste potencial de remediación y exposición para priorizar inversiones en ciberseguridad.
c) Estimar la severidad técnica de una vulnerabilidad mediante una métrica estandarizada que puede complementarse con contexto ambiental.
d) Determinar la sensibilidad regulatoria de la información tratada para aplicar salvaguardas proporcionales.

56) En un ejercicio de Red Team, el objetivo principal es:

a) Identificar vulnerabilidades técnicas de forma puntual.
b) Evaluar la capacidad global de detección y respuesta de la organización.
c) Comprobar únicamente la configuración de los sistemas.
d) Validar el cumplimiento normativo.

57) En pruebas ofensivas, las reglas de enfrentamiento sirven para:

a) Documentar exclusivamente las vulnerabilidades explotadas con evidencia técnica.
b) Permitir ampliar objetivos durante la ejecución si aparecen nuevos vectores viables.
c) Sustituir la aprobación formal previa cuando el ejercicio esté acotado técnicamente.
d) Definir alcance, autorizaciones, restricciones y condiciones de ejecución del ejercicio.

58) OSINT consiste en:

a) Recopilar y analizar información obtenida de fuentes públicamente accesibles para generar inteligencia útil.
b) Desarrollar o emplear capacidades de explotación no divulgadas para comprometer sistemas sin parche disponible.
c) Capturar evidencias volátiles del sistema para preservar artefactos útiles en un análisis forense.
d) Aplicar mecanismos criptográficos para proteger el contenido y determinados metadatos en comunicaciones electrónicas.

59) STIX y TAXII se emplean para:

a) Aplicar autenticación de acceso a red basada en intercambio seguro de credenciales entre cliente y autenticador.
b) Modelar, intercambiar y transportar inteligencia de amenazas en formatos estructurados y mecanismos normalizados.
c) Firmar y validar el origen de mensajes de correo mediante mecanismos de autenticación de dominio.
d) Registrar y verificar evidencias de integridad en canalizaciones de entrega continua para asegurar la trazabilidad del despliegue.

60) Un IoC es:

a) Un mecanismo de protección criptográfica aplicado a volúmenes para garantizar confidencialidad en reposo.
b) Un identificador operativo usado para asignar responsabilidades formales dentro del modelo de seguridad.
c) Un artefacto observable que puede señalar la posible presencia de una intrusión o actividad maliciosa.
d) Una directriz de continuidad que establece criterios de copia, retención y restauración de información.

61) En la respuesta a incidentes, la secuencia de gestión correcta es:

a) Clasificación, comunicación, escalado y cierre administrativo.
b) Recuperación, detección, contención, análisis y cierre.
c) Detección, análisis, contención, erradicación y recuperación.
d) Aislamiento, restauración del servicio y cierre del incidente.

62) En el ámbito del ENS, la notificación de incidentes al CCN-CERT debe hacerse usando la siguiente herramienta:

a) Reyes.
b) Pilar.
c) Lucía.
d) Claudia.

63) En un entorno de análisis forense, la cadena de custodia garantiza:

a) La segmentación lógica de redes mediante VLAN.
b) La obtención, conservación y presentación de evidencias digitales.
c) La autenticación federada entre aplicaciones y dominios.
d) El control del inventario y uso de licencias de software.

64) La adquisición de memoria RAM en análisis forense es valiosa porque puede contener:

a) Únicamente archivos ya guardados de forma permanente en disco.
b) Solo registros de autenticación del directorio activo.
c) Paquetes de red ya capturados y almacenados por herramientas de monitorización.
d) Información volátil como procesos en ejecución, conexiones activas y posibles claves en memoria.

65) Una solución DLP tiene como objetivo principal:

a) Sustituir al cifrado de disco.
b) Incrementar el ancho de banda WAN.
c) Prevenir fugas de información por distintos canales.
d) Realizar correlación de eventos de seguridad.

66) Un EDR se orienta a:

a) Aplicar políticas de administración y contención sobre dispositivos móviles y aplicaciones corporativas.
b) Proporcionar visibilidad, detección y capacidades de respuesta sobre la actividad de estaciones de trabajo y servidores.
c) Decidir el acceso a la red en función de la identidad del usuario y del estado de cumplimiento del equipo.
d) Automatizar la emisión y renovación de credenciales y certificados de máquina en entornos distribuidos.

67) Un XDR pretende integrar:

a) La agregación centralizada de registros de múltiples fuentes con foco principal en búsqueda, correlación y conservación de eventos.
b) La visibilidad y respuesta sobre estaciones de trabajo y servidores mediante sensores desplegados en los propios endpoints.
c) La inspección de tráfico y flujos para detectar anomalías de red y movimientos laterales desde sensores o taps dedicados.
d) Telemetría, analítica y capacidad de respuesta coordinada sobre múltiples dominios como endpoint, identidad, correo, red y nube.

68) El hardening de un sistema consiste en:

a) Deshabilitar componentes innecesarios, aplicar configuraciones seguras y reducir la superficie de exposición del sistema.
b) Mantener el sistema plenamente actualizado mediante la instalación continua de parches y nuevas versiones.
c) Centralizar registros y telemetría para facilitar la detección temprana de anomalías operativas y de seguridad.
d) Aislar servicios críticos en segmentos diferenciados para limitar la propagación de incidentes entre entornos.

69) MDM y MAM se relacionan con:

a) El control del acceso a la red en función de la identidad del usuario y del estado del equipo.
b) La captura y análisis de tráfico para detectar anomalías y movimientos laterales en la red.
c) El análisis automatizado de archivos sospechosos en entornos aislados para observar su comportamiento.
d) La administración, protección y aplicación de políticas sobre dispositivos móviles y aplicaciones corporativas.

70) En un escenario BYOD, una medida especialmente relevante es:

a) Prohibir cualquier conexión desde redes domésticas, aunque se use acceso seguro corporativo.
b) Separar el ámbito corporativo del personal mediante contenedorización, políticas y control de acceso.
c) Utilizar cuentas compartidas para simplificar soporte y acceso desde distintos terminales.
d) Prescindir de la autenticación multifactor para reducir fricción en dispositivos personales.

71) ¿Cuál es una medida eficaz para reducir ataques de phishing en el correo electrónico?

a) Aumentar el tamaño de los buzones de usuario.
b) Deshabilitar el cifrado TLS en el correo.
c) Implantar controles como SPF, DKIM y DMARC.
d) Permitir cualquier dominio externo sin validación.

72) Un ataque BEC se caracteriza por:

a) Denegación de servicio dirigida contra servidores DNS autoritativos.
b) Explotación de vulnerabilidades en el firmware de un switch troncal de red.
c) Exfiltración de información mediante dispositivos USB.
d) Fraude basado en la suplantación o manipulación del correo empresarial para inducir pagos o acciones indebidas.

73) Las pruebas controladas de DDoS deben:

a) Realizarse sin aviso previo para comprobar la reacción real del servicio.
b) Planificarse, autorizarse y ejecutarse con salvaguardas técnicas y operativas.
c) Sustituir las pruebas de continuidad y recuperación si el servicio mantiene disponibilidad.
d) Ejecutarse sin monitorización para no alterar las métricas del ejercicio.

74) El Blue Team se centra en:

a) La simulación ofensiva de ataques para comprometer sistemas y validar exposición.
b) La evaluación de ofertas y la contratación de servicios de ciberseguridad.
c) La monitorización, la detección de amenazas y la respuesta defensiva ante incidentes.
d) La automatización de despliegues de infraestructura como código en entornos productivos.

75) El Purple Team aporta valor porque:

a) Facilita la colaboración entre capacidades ofensivas y defensivas para mejorar detección, respuesta y cobertura de control.
b) Sustituye la necesidad de telemetría y monitorización si el ejercicio ofensivo está bien planteado.
c) Elimina la necesidad de casos de uso de detección al centrarse en la validación manual de técnicas adversarias.
d) Reduce la utilidad de los ejercicios de Red Team al priorizar únicamente la coordinación interna del SOC.

76) El spear phishing se diferencia del phishing masivo en que:

a) Se distingue por usar de forma predominante llamadas o mensajería móvil en lugar de correo electrónico.
b) Requiere normalmente que exista una intrusión previa para personalizar el ataque con datos internos comprometidos.
c) Persigue principalmente suplantar cualquier identidad legítima de una organización con un mensaje general que engañe al mayor número de víctimas.
d) Selecciona objetivos concretos y adapta el señuelo al contexto, rol o relaciones de la víctima.

77) En programación segura en PYTHON, una buena práctica es:

a) Ejecutar la aplicación con privilegios elevados para evitar fallos de acceso a recursos del sistema.
b) Validar entradas, manejar excepciones de forma segura y mantener dependencias actualizadas y revisadas.
c) Ocultar errores y desactivar el registro para no exponer información al atacante.
d) Registrar el menor detalle posible para reducir impacto en rendimiento y volumen de trazas.

78) Un gestor de incidencias contribuye a:

a) Sustituir los procesos de alta, baja y modificación de cuentas en los sistemas corporativos.
b) Emitir y renovar certificados digitales de servicio para aplicaciones e infraestructuras.
c) Registrar, priorizar, asignar y seguir incidencias con trazabilidad hasta su resolución.
d) Aplicar validaciones de autenticidad de correo durante el tránsito entre servidores.

79) Un firewall de nueva generación se diferencia de un firewall tradicional porque incorpora:

a) Filtrado estático basado en puertos, protocolos y direcciones, sin visibilidad real de la aplicación.
b) Registro de logs de conexiones protegidas por el firewall.
c) Incapacidad para generar telemetría útil o integrarse con procesos de monitorización y análisis.
d) Identificación de aplicaciones, control más granular del tráfico e integración con funciones de prevención y detección.

80) Un WAF protege frente a:

a) Incidencias de suministro eléctrico o climatización en el centro de proceso de datos.
b) Ataques dirigidos a aplicaciones web, como inyecciones, manipulación de peticiones o explotación de lógica HTTP.
c) Secuestro de rutas y otros problemas de validación en el enrutamiento entre dominios.
d) Eliminación o cifrado malicioso de repositorios de copia para impedir la recuperación.

81) Cuando implementas DNSSEC mejoras la seguridad por:

a) Cifrado del canal DNS entre cliente y servidor de nombres para evitar la inspección del tráfico.
b) Autenticidad e integridad de los datos DNS mediante validación criptográfica de las respuestas.
c) Bloqueo o redirección automática de dominios maliciosos mediante políticas de respuesta.
d) Anonimización de las consultas DNS para ocultar el origen y contenido sin mecanismos adicionales.

82) En seguridad cloud, el modelo de responsabilidad compartida implica que:

a) La externalización del servicio elimina la necesidad de trazabilidad, monitorización y evidencia de cumplimiento.
b) El proveedor asume por completo la seguridad del servicio, incluidos datos, identidades y configuraciones del cliente.
c) El cliente conserva toda la responsabilidad de seguridad incluso cuando la plataforma o la infraestructura son gestionadas.
d) Proveedor y cliente asumen controles diferentes según el tipo de servicio cloud y la capa tecnológica implicada.

83) En directorios como Active Directory o Entra ID, una mala práctica sería:

a) Aplicar autenticación multifactor a las cuentas con privilegios elevados.
b) Separar las cuentas de administración de las utilizadas para el trabajo ordinario.
c) Registrar y auditar los accesos y cambios relevantes en el directorio.
d) Mantener cuentas privilegiadas activas sin revisión periódica ni control de necesidad.

84) SNMP y Netflow se usan para:

a) Autenticar usuarios entre dominios y aplicaciones mediante federación de identidad.
b) Supervisar el estado de dispositivos y obtener visibilidad del tráfico y de los flujos de red.
c) Emitir y renovar certificados de servicio para componentes y aplicaciones internas.
d) Cifrar el almacenamiento compartido de cabinas para proteger datos en reposo.

85) Una SQLi se produce cuando:

a) Un resolvedor no puede validar la autenticidad e integridad de respuestas DNS firmadas.
b) Una relación de federación pierde validez al no poder verificarse la identidad del emisor.
c) Entradas no validadas o consultas mal construidas permiten modificar la lógica de acceso a la base de datos.
d) La consola de administración de virtualización queda expuesta sin segmentación ni controles de acceso adecuados.

86) IPSEC se asocia con:

a) Proteger el flujo de voz y multimedia en telefonía IP mediante SRTP.
b) Gestionar autorización delegada entre aplicaciones y APIs con OAuth 2.0.
c) Validar el origen de rutas en BGP para reforzar la seguridad del enrutamiento mediante RPKI.
d) Proteger el tráfico a nivel IP mediante autenticación, integridad y, cuando procede, cifrado, por ejemplo en VPN.

87) Con respecto a WireGuard identifique la respuesta correcta:

a) Es un protocolo/software de VPN orientado a establecer túneles seguros con una configuración sencilla y una base criptográfica moderna.
b) Es un estándar orientado a reforzar la autenticidad y el transporte seguro del correo electrónico.
c) Actúa como pasarela de seguridad para filtrar y proteger peticiones dirigidas a aplicaciones web.
d) Reemplaza los mecanismos de autenticación de acceso a red como 802.1X en entornos cableados.

88) En telefonía IP, SRTP se utiliza para:

a) Comprobar el estado de revocación de certificados digitales mediante consultas OCSP.
b) Proteger el flujo de voz y otros medios en tiempo real mediante cifrado, integridad y autenticación.
c) Separar el tráfico de voz del de datos mediante la asignación de VLAN de voz.
d) Detectar desviaciones de comportamiento de usuarios y entidades mediante analítica UEBA.

89) La estrategia 3-2-1-1-0 en backup establece que debe:

a) Mantener varias copias sincronizadas en línea para asegurar disponibilidad, aunque dependan del mismo entorno lógico.
b) Cifrar las copias y ampliar su periodo de retención para reducir el riesgo, sin necesidad de diversificar soportes.
c) Disponer de varias copias en soportes distintos, conservar al menos una copia offline o inmutable y verificar que no existan errores de respaldo.
d) Priorizar la rapidez de recuperación y comprobar las copias solo cuando sea necesario restaurar.

90) Son medidas de protección efectivas contra el ransomware:

a) Priorizar la alta disponibilidad del servicio y la replicación síncrona entre cabinas como defensa principal.
b) Centralizar registros y umbrales de alerta para detectar antes incidentes de disponibilidad y rendimiento.

c) Confiar en la restauración posterior y en el aislamiento manual una vez iniciado el cifrado para minimizar el impacto.
d) Disponer de copias offline o inmutables, segmentar entornos y reforzar el endurecimiento y la gestión de privilegios.

91) En virtualización, proteger el plano de gestión es crítico porque:

a) Un compromiso del plano de gestión puede otorgar control transversal sobre múltiples hosts, redes virtuales y máquinas invitadas.
b) Concentra sobre todo información operativa y estadística, por lo que su impacto en seguridad suele ser limitado.
c) Su acceso desde redes amplias o poco segmentadas favorece la administración distribuida sin aumentar de forma significativa el riesgo.
d) Al ser una capa técnica de soporte, suele quedar fuera del alcance prioritario del análisis de riesgos y de continuidad.

92) En Kubernetes, el escaneo de imágenes pretende:

a) Sustituir la protección en tiempo de ejecución si las imágenes han sido validadas previamente.
b) Detectar vulnerabilidades, componentes inseguros y errores de configuración antes de desplegar imágenes en el clúster.
c) Reemplazar la gestión de identidades, permisos y políticas de acceso al clúster.
d) Sustituir la revisión de manifiestos, políticas de admisión y controles de despliegue del clúster.

93) Una defensa válida frente a CSRF es:

a) Permitir solicitudes cross-site si viajan por HTTPS y proceden de navegadores actualizados.
b) Emplear tokens anti-CSRF y validar el origen o el contexto de la petición antes de aceptar acciones sensibles.
c) Desactivar por completo el uso de cookies para evitar que el navegador envíe credenciales en peticiones autenticadas.
d) Confiar en el uso exclusivo de HTTPS como medida suficiente para impedir peticiones forjadas entre sitios.

94) La observabilidad moderna (observability) integra de forma efectiva:

a) Únicamente registros del sistema operativo y del middleware básico para detectar fallos de servicio.
b) Exclusivamente alarmas del hipervisor y eventos de infraestructura física subyacente.
c) Copias de seguridad, replicación y procedimientos de recuperación ante desastres.
d) Logs, métricas y trazas para comprender el comportamiento del sistema y diagnosticar incidencias.

95) En seguridad de APIs, una mala práctica es:

a) Aplicar limitación de tasa para reducir abuso y proteger la disponibilidad del servicio.
b) Comprobar la autorización de forma granular según recurso, operación y contexto.
c) Devolver información excesiva en las respuestas o exponer más datos de los estrictamente necesarios.
d) Validar entradas, formatos y esquemas de petición antes de procesar la solicitud.

96) Una solución NDR se basa en:

a) Autenticación federada entre aplicaciones mediante SAML y un proveedor externo de identidad.
b) Sensores de red, metadatos de tráfico y análisis de flujos para detectar anomalías y actividad sospechosa.
c) Inspección y bloqueo en línea del tráfico para aplicar políticas de seguridad a nivel de aplicación.
d) Cifrado de repositorios de código y control de acceso a ramas en plataformas de desarrollo.

97) RPKI y route origin validation sirven para:

a) Validar la autenticidad del dominio remitente y aplicar políticas frente a suplantación en correo electrónico.
b) Proteger el establecimiento de sesiones y el transporte multimedia en entornos de voz sobre IP.
c) Validar el origen autorizado de prefijos anunciados y reforzar la seguridad del enrutamiento BGP.
d) Reforzar la seguridad de cuentas privilegiadas y controladores en servicios de directorio corporativo.

98) Devsecops tiene como objetivo:

a) Mantener la seguridad como función separada para no interferir en la velocidad de entrega del desarrollo.
b) Reservar las verificaciones de seguridad para la fase de cierre antes de la liberación final.
c) Integrar controles y validaciones de seguridad de forma continua en desarrollo, despliegue y operación.
d) Concentrar la automatización de seguridad en producción para evitar fricción durante el desarrollo.

99) En infraestructura como código, una buena práctica es:

a) Mantener credenciales y variables sensibles embebidas en plantillas para simplificar la promoción entre entornos.
b) Integrar control de versiones, revisión de cambios, validación previa y policy-as-code en el ciclo de despliegue.

c) Realizar ajustes manuales sobre cada entorno una vez desplegado para acelerar correcciones puntuales.
d) Posponer comprobaciones de seguridad y conformidad hasta después del despliegue para reducir tiempos de entrega.

100) 802.1x y NAC se utilizan para:

a) Cifrar discos o perfiles de usuario en estaciones virtuales para proteger datos en reposo.
b) Proteger APIs y sesiones web mediante tokens firmados y mecanismos de autorización delegada.
c) Controlar el acceso a la red en función de la identidad del usuario y del estado o cumplimiento del dispositivo.
d) Emitir, distribuir y renovar certificados de servicio para portales y aplicaciones corporativas.

PREGUNTAS DE RESERVA

101) En un S-SDLC, el modelado de amenazas sirve para:

a) Seleccionar proveedores o servicios tecnológicos en función de criterios generales de homologación.
b) Anticipar escenarios de abuso, identificar riesgos y definir controles de seguridad desde fases tempranas del diseño.
c) Sustituir las pruebas de seguridad dinámicas y las revisiones de código si el diseño ya ha sido analizado.
d) Mantener el inventario de activos y dependencias técnicas para su registro en la CMDB.

102) MTA-STS y DANE buscan mejorar:

a) La detección y contención de actividad sospechosa en estaciones de trabajo y servidores.
b) La autorización delegada y el consentimiento de acceso entre aplicaciones y APIs.
c) La gestión, elevación y supervisión de accesos privilegiados en sistemas críticos.
d) La autenticidad de la política y la protección del transporte TLS entre servidores de correo.

103) SAST, DAST e IAST se diferencian en:

a) El formato de informe o exportación de resultados que genera cada herramienta.
b) Que solo una de estas técnicas permite identificar y corregir vulnerabilidades de forma efectiva.
c) El sistema operativo o la plataforma sobre la que se ejecuta la aplicación analizada.
d) El momento, el contexto y la forma en que evalúan la aplicación durante el ciclo de desarrollo y ejecución.

104) Un SBOM proporciona:

a) Una taxonomía para clasificar amenazas, técnicas adversarias y su criticidad relativa.
b) Un inventario estructurado de componentes software, versiones y dependencias que componen una aplicación o producto.
c) Un registro formal de evidencias y artefactos conservados para su análisis forense o judicial.
d) Una matriz de funciones, responsabilidades y conflictos de interés para reforzar el control interno.

105) En entornos ICS/OT, una consideración imprescindible es:

a) Priorizar la disponibilidad y las restricciones operativas del proceso antes de aplicar cambios que puedan afectar a la producción.
b) Aplicar correcciones y reinicios en cuanto estén disponibles, aunque no exista ventana operativa validada.
c) Mantener credenciales comunes entre operadores y técnicos para simplificar la continuidad del servicio.
d) Reducir la segmentación entre redes industriales y corporativas para agilizar diagnóstico y mantenimiento.

106) En el uso de JWT, es un riesgo:

a) Limitar la vigencia del token y ajustar su tiempo de vida al contexto de uso.
b) Registrar eventos relevantes de autenticación y validación para facilitar trazabilidad y detección.
c) Proteger el intercambio del token mediante TLS para reducir exposición durante el transporte.
d) Aceptar tokens sin verificar correctamente la firma, el algoritmo admitido o la validez temporal.

107) El uso de mTLS en un service MESH aporta:

a) Filtrado de spam y validación de autenticidad en el intercambio de correo saliente entre dominios.
b) Firma biométrica avanzada para validar la identidad del usuario en operaciones de alto riesgo.
c) Autenticación mutua y cifrado del tráfico entre servicios para reforzar la confianza en comunicaciones internas.
d) Clasificación estructurada de indicadores y artefactos para intercambio de inteligencia de amenazas.

108) WPA3-Enterprise mejora la seguridad de una red wifi corporativa porque:

a) Convierte la red inalámbrica en anónima y oculta por defecto la identidad de usuarios y dispositivos frente a cualquier infraestructura de autenticación.
b) Elimina la necesidad de autenticación individual y de un backend de control de acceso al basarse solo en el cifrado del canal inalámbrico.
c) Refuerza la autenticación empresarial y la protección del acceso inalámbrico mediante mecanismos más robustos y adecuados para entornos corporativos.
d) Sustituye por completo los controles de acceso a red basados en identidad, postura del dispositivo o segmentación lógica.

109) Una RPZ puede emplearse para:

a) Firmar y validar criptográficamente zonas DNS para garantizar autenticidad e integridad de las respuestas.
b) Reforzar la seguridad del transporte SMTP entre servidores mediante políticas y validación de certificados.
c) Bloquear, redirigir o responder de forma controlada ante consultas a dominios considerados maliciosos.
d) Realizar validación criptográfica del origen de rutas en BGP para reducir secuestros de prefijos.

110) CSPM y CWPP se relacionan con:

a) La evaluación continua de configuraciones y postura de seguridad en cloud, junto con la protección de cargas de trabajo en ejecución.
b) La autenticación fuerte de usuarios y la emisión de credenciales de identidad digital cualificada.
c) La validación del origen de prefijos y la protección del enrutamiento interdominio en BGP.
d) El control de acceso físico, monitorización ambiental y continuidad operativa del centro de proceso de datos.