



## Cuestionario del primer ejercicio

Especialidad: A6 D4. Seguridad Informática.

Por favor, lea detenidamente antes de comenzar:

- **NO** abra el **CUESTIONARIO** ni empiece el examen hasta que se le indique.
- Para realizar este primer ejercicio se hace entrega de dos documentos:
  1. Cuadernillo con el **cuestionario de preguntas tipo test**, con cuatro respuestas alternativas sobre las materias del programa de esta convocatoria.
  2. **Hoja de respuestas** donde se consignará la respuesta correcta a cada pregunta.
- Al finalizar la prueba se hará entrega de la hoja de respuestas. El cuadernillo con el cuestionario se podrá utilizar como borrador y se podrá llevar por el opositor al finalizar el tiempo marcado para el ejercicio.
- Sólo se calificará las respuestas marcadas en la **HOJA DE RESPUESTAS**
- Una vez abierto el cuestionario, compruebe que consta de todas las páginas y preguntas y que sea legible. En caso contrario solicite uno nuevo al personal del aula.
- Verifique que el número de la solapa donde se recogen sus **datos personales coincide con el número de la hoja** de examen donde se consignan las respuestas.
- El examen se realizará con bolígrafo azul o negro. Si no dispone de uno, solicítelo al Tribunal.
- El cuestionario consta de **100 (CIEN) preguntas**, cada una de ellas con **cuatro respuestas alternativas**, de las cuales **sólo una de ellas es correcta, más 5 (CINCO) preguntas adicionales de reserva**, que serán valoradas en el caso de que se anule algunas de las 100 anteriores. **Marque con una equis la respuesta elegida** en la celda correspondiente a la pregunta, de forma clara (ver fig. 1).
- **Las respuestas múltiples, poco claras o dudosas, se considerarán como no contestadas.** Si desea corregir una respuesta, **rodee la opción incorrecta** con un círculo (ver fig. 2) y marque con una equis la nueva opción que elige.

1	A	B	C	D
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fig 1.

1	A	B	C	D
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fig 2.

- Todas las preguntas tendrán el mismo valor y **las contestaciones erróneas se penalizarán** con 1/3 del valor de una contestación correcta.
- **NO Separe** ninguna de las copias de la **HOJA DE RESPUESTAS**. Una vez finalizado, el personal del aula le indicará los pasos a seguir.
- **Dispone de 90 minutos**, máximo, para realizar este ejercicio.




Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025  
Primer Ejercicio


Fecha:  
10/05/2026  
Página: 2 de 32



1. ***En el contexto del R.D. 311/2022 por el que se regula el Esquema Nacional de Seguridad (ENS), ¿qué dimensión de la seguridad de los sistemas de información resulta crítica para garantizar la reproducibilidad científica de datos experimentales?***
  - A) Confidencialidad.
  - B) Disponibilidad.
  - C) Integridad.
  - D) Autenticidad.
  
2. ***Conforme al artículo 6 del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), ¿en qué caso será lícito el tratamiento de datos personales obtenido en ensayos clínicos de un Organismo Público de Investigación (OPI)?***
  - A) Desde que el interesado otorgue su mero consentimiento.
  - B) Si es necesario para proteger intereses vitales de una persona física distinta del interesado.
  - C) Para la publicación de los mismos en repositorios abiertos.
  - D) Cuando sea necesario para el cumplimiento de una misión en el ejercicio de poderes públicos conferidos al responsable de la seguridad.
  
3. ***En los OPI, la clasificación de datos clínicos de pacientes debe regirse concurrentemente por el Esquema Nacional de Seguridad (ENS) y por:***
  - A) La Ley 40/2015, de Régimen Jurídico del Sector Público.
  - B) El artículo 9 del RGPD sobre categorías especiales de datos.
  - C) La norma ISO/IEC 27001:2022.
  - D) El artículo 8 del RGPD sobre categorías de datos sensibles.
  
4. ***La federación de identidades eduGAIN, utilizada en redes académicas europeas, se basa en:***
  - A) OAuth 2.0.
  - B) LDAP cifrado.
  - C) SAML 2.0.
  - D) Kerberos

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025 Primer Ejercicio</p>	<p>Fecha: 10/05/2026 Página: 4 de 32</p>
---	--	--

5. ***La técnica anonimato-K aplicada a conjuntos de datos garantiza que ningún individuo sea:***
  - A) Capaz de identificar patrones estadísticos generales.
  - B) Distinguible de al menos  $k-1$  individuos adicionales en la misma clase de equivalencia.
  - C) Reconocible por combinación de atributos estadísticos.
  - D) Visible en agregaciones de al menos cinco registros.
  
6. ***El esquema Common Criteria (ISO/IEC 15408) evalúa la seguridad de sistemas informáticos mediante:***
  - A) Pruebas de estrés computacional promediado en el tiempo.
  - B) Validación de licencias de software utilizadas.
  - C) Niveles de evaluación basados en la rigurosidad de evaluación y pruebas.
  - D) Criterios comunes a todas las normas ISO relacionadas con la seguridad informática.
  
7. ***La métrica RPO (Recovery Point Objective) mide, en la evaluación de resiliencia:***
  - A) El tiempo máximo aceptable de interrupción del servicio.
  - B) Pérdida máxima de datos asumible entre la última copia de seguridad y la interrupción del servicio.
  - C) Porcentaje de disponibilidad anual del servicio.
  - D) Número mínimo de nodos redundantes para recuperar el servicio sin pérdida de rendimiento.
  
8. ***Las pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad de un servicio se realizarán obligatoriamente, según la medida op.cont.3.1 del Esquema Nacional de Seguridad:***
  - A) En sistemas de nivel alto.
  - B) En sistemas de nivel medio y alto.
  - C) En sistemas de nivel bajo, medio y alto.
  - D) El ENS no obliga en ningún caso a hacer pruebas periódicas del plan de continuidad, pero sí a tener uno.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 5 de 32</p>
---	---	---

9. *¿Qué evalúa el Static Application Security Testing (SAST) respecto del código fuente de una aplicación?*
- A) Su robustez en tiempo de ejecución.
  - B) Su resiliencia ante un ataque DDoS.
  - C) La existencia de vulnerabilidades.
  - D) Su rendimiento en producción.
10. *Del Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC), del Centro Criptológico Nacional (CCN), ¿qué productos y servicios son elegibles para su uso en sistemas que manejan información clasificada?*
- A) Productos y servicios aprobados.
  - B) Productos y servicios certificados.
  - C) Productos y servicios cualificados.
  - D) Ninguno de los anteriores.
11. *En el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) del software, una puntuación comprendida en el intervalo 7,0 - 8,9 representa una vulnerabilidad*
- A) Baja.
  - B) Media.
  - C) Alta.
  - D) Crítica.
12. *Las pruebas DAST (Dynamic Application Security Testing) se ejecutan para:*
- A) Detectar vulnerabilidades en el código fuente una vez compilado.
  - B) Monitorizar los flujos de datos de una aplicación.
  - C) Atacar la aplicación en funcionamiento sin conocer el código fuente.
  - D) Detectar vulnerabilidades en funciones o métodos concretos del código fuente.
13. *El artículo 13.3 del Esquema Nacional de Seguridad (ENS) explicita que el responsable de la seguridad será:*
- A) Distinto del responsable del sistema, sin excepciones.
  - B) Distinto del responsable del servicio, con excepciones.
  - C) Distinto del responsable del sistema, con excepciones.
  - D) Distinto del responsable del servicio, sin excepciones.



14. ***Según el apartado 4.3 del Anexo de la Resolución de 8 de julio de 2014, de la Presidencia del CSIC, por la que se aprueba la política de seguridad de la información (PSI) de la Agencia Estatal Consejo Superior de Investigaciones Científicas, el órgano decisorio encargado de mantener actualizada y adaptada dicha PSI es:***
- A) El Comité Técnico de Seguridad de la Información.
  - B) Los Grupos de Trabajo de Seguridad de la Información.
  - C) El Grupo Técnico de Seguridad de la Información.
  - D) El Comité Corporativo de Seguridad de la Información.
15. ***¿Qué afirmación es cierta respecto del ámbito de aplicación (artículo 2) del Esquema Nacional de Seguridad (ENS)?***
- A) El ENS debe sustituirse obligatoriamente por la norma ISO/IEC 27001 en el caso de las entidades del sector privado.
  - B) El ENS se aplica también a los sistemas de información de las entidades del sector privado cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las personas físicas o jurídicas.
  - C) El ENS no es de aplicación a todo el sector público.
  - D) Ninguna de las anteriores.
16. ***¿A quién corresponde la determinación de la categoría de seguridad del sistema, según el artículo 41 del Esquema Nacional de Seguridad (ENS)?***
- A) Al responsable o responsables de la seguridad.
  - B) Al responsable o responsables del sistema.
  - C) Al responsable o responsables de la información.
  - D) Al máximo órgano jerárquico de la entidad correspondiente.
17. ***Las siglas SIEM corresponden a:***
- A) Security Integrated Equipment Management.
  - B) Security Information and Equipment Management.
  - C) Security Incident and Event Management.
  - D) Security Information and Event Management.



18. ***En relación con el personal, propio o ajeno, que utiliza los sistemas de información sujetos al Esquema Nacional de Seguridad (ENS), ¿qué opción refleja con mayor precisión sus obligaciones según el Real Decreto 311/2022?***
- A) Debe ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad, y su actuación, supervisada, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
  - B) Debe revisar periódicamente la política de seguridad de la información y proponer las modificaciones necesarias para mantener su alineamiento con el ENS.
  - C) Debe colaborar en los análisis de riesgos indicando los activos críticos y valorando el impacto de posibles incidentes, de forma que puedan determinarse los requisitos de seguridad aplicables al sistema.
  - D) Debe participar en la elaboración de los planes de concienciación y de formación en seguridad, definiendo contenidos y periodicidad de las acciones formativas para el conjunto de la organización.
19. ***¿Qué opción describe de forma más ajustada las funciones del responsable del sistema, de acuerdo con el artículo 13 del Esquema Nacional de Seguridad (ENS)?***
- A) Determinar los requisitos de los servicios prestados, incluyendo los niveles de calidad y seguridad que se ofrecerán a los usuarios externos.
  - B) Desarrollar la forma concreta de implementar la seguridad en el sistema y supervisar la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
  - C) Establecer los requisitos de la información tratada, considerando su sensibilidad y los impactos asociados.
  - D) Decidir qué medidas de seguridad del anexo II se consideran desproporcionadas y pueden no aplicarse al sistema.
20. ***El artículo 4.7 del Reglamento General de Protección de Datos (RGPD) define responsable del tratamiento como:***
- A) La persona física o jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios del tratamiento.
  - B) La persona jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
  - C) La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
  - D) La persona jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios del tratamiento.



21. ***El artículo 4.11 del Reglamento (UE) 2016/679 define «consentimiento del interesado» como una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de datos que le conciernen mediante:***
- A) Una declaración o una clara acción afirmativa.
  - B) La presunción tácita derivada de silencio o inactividad.
  - C) Una declaración escrita o acción tácita.
  - D) Una autorización verbal documentada.
22. ***¿Cuál es el conjunto de dimensiones de seguridad que, de acuerdo con el ENS, se deben considerar para categorizar un sistema de información que soporta servicios científicos críticos en una administración pública?***
- A) Confidencialidad, integridad, disponibilidad y anonimato.
  - B) Integridad, trazabilidad, disponibilidad y escalabilidad.
  - C) Disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.
  - D) Confidencialidad, integridad, disponibilidad y resiliencia.
23. ***En un proyecto científico se tratan datos de salud de participantes humanos, seudonimizados pero reidentificables, junto con resultados experimentales asociados. ¿Cuál de las siguientes afirmaciones describe mejor la clasificación que debería aplicarse a estos datos científicos en cuanto a sensibilidad?***
- A) Deberían clasificarse como datos de sensibilidad alta o crítica, al tratarse de datos personales de categorías especiales cuyo acceso no autorizado podría suponer un grave perjuicio para los interesados.
  - B) Pueden clasificarse como datos de sensibilidad baja, puesto que la seudonimización elimina cualquier riesgo relevante para los interesados.
  - C) Deberían considerarse datos públicos, ya que la investigación científica tiene interés general y ello justifica su difusión sin restricciones adicionales.
  - D) Bastaría con clasificarlos como datos de uso interno / sensibilidad media, porque las medidas de seguridad adicionales se reservan únicamente para datos personales no seudonimizados.





24. ***En relación con los principios de seguridad de la información aplicados a la gestión de accesos en un centro de investigación, ¿cuál de las siguientes prácticas se ajusta mejor al principio de «necesidad de saber» (need-to-know)?***
- A) Conceder acceso de lectura a todos los proyectos de investigación del centro a cualquier persona que disponga de contrato en vigor, con independencia de su unidad o función.
  - B) Otorgar a todo el personal investigador acceso completo a los repositorios de datos científicos, pero limitarles el acceso a información administrativa y económica.
  - C) Asignar a cada usuario únicamente los permisos estrictamente necesarios para desempeñar sus funciones en proyectos concretos, evitando accesos generalistas a otros datos o sistemas no relacionados.
  - D) Conceder permisos amplios por defecto y revisarlos solo cuando se detecte un incidente de seguridad o una fuga de información.
25. ***En un consorcio internacional de investigación se tratan datos personales y datos de categorías especiales (por ejemplo, salud) de participantes de varios Estados miembros de la UE. ¿Cuál de las siguientes afirmaciones describe mejor las obligaciones de seguridad y protección de datos para la institución pública española que participa en el proyecto?***
- A) Debe cumplir exclusivamente la normativa del país del socio coordinador, puesto que el proyecto es único y multinacional y no se aplican normativas nacionales adicionales.
  - B) Debe aplicar el Reglamento (UE) 2016/679 (RGPD) y la normativa española de desarrollo, aplicar medidas de seguridad basadas en un análisis de riesgos (incluyendo, en su caso, evaluaciones de impacto), y garantizar la licitud, confidencialidad, integridad y responsabilidad proactiva en los tratamientos de datos personales dentro del proyecto.
  - C) Puede prescindir del RGPD si se firma un acuerdo interno en el consorcio que regula la seguridad, dado que este acuerdo prevalece sobre las normas nacionales y europeas en el ámbito científico.
  - D) Solo está obligada a aplicar medidas de seguridad técnica (cifrado, copias de seguridad), sin necesidad de documentar políticas ni de justificar las decisiones en un análisis de riesgos, por tratarse de investigación científica de interés público.




26. *Desde la perspectiva de la gestión de riesgos y las guías de interconexión basadas en el ENS, ¿qué principio resulta especialmente relevante al diseñar el intercambio de datos científicos entre la red académica de una universidad y sistemas externos (por ejemplo, infraestructuras de otros países o nubes comerciales)?*
- A) Presuponer que todos los sistemas conectados son igualmente confiables, de manera que el control de seguridad puede delegarse completamente en la red académica.
  - B) Aplicar el principio de «nodo autoprotegido», tratando los sistemas externos como potencialmente no fiables y estableciendo un control local de los datos que entran y salen mediante perímetros, proxies y filtrado.
  - C) Permitir que los usuarios creen túneles cifrados directos (VPN personales) sin pasar por los perímetros institucionales, para no interferir con la confidencialidad de sus comunicaciones de investigación.
  - D) Reducir al mínimo los registros de actividad asociados al intercambio de datos, para evitar un crecimiento excesivo del almacenamiento y posibles problemas de privacidad.
27. *En el modelo CMMI (Capability Maturity Model Integration), ¿cuántos niveles de madurez de una organización se definen?*
- A) Siete.
  - B) Cinco.
  - C) Cuatro.
  - D) Seis.
28. *Entre las novedades introducidas por el Real Decreto 311/2022 en la actualización del Esquema Nacional de Seguridad (ENS), ¿cuál de las siguientes recoge correctamente uno de los cambios relevantes en los principios básicos aplicables al sector público?*
- A) Se elimina el principio de gestión basada en el riesgo.
  - B) Se suprime el principio de responsabilidades diferenciadas.
  - C) Se incorpora el principio de seguridad integral.
  - D) Se introduce el principio de vigilancia continua.




29. ***¿Qué es el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información?***
- A) Un reglamento nacional español.
  - B) Una norma promulgada a iniciativa del Congreso de los Diputados.
  - C) La transposición al ordenamiento jurídico español de un Reglamento de la Unión Europea.
  - D) La transposición al ordenamiento jurídico español de una Directiva de la Unión Europea.
30. ***Según la norma ISO/IEC 25010 sobre calidad del producto software, ¿cuál de las siguientes listas contiene exclusivamente características de calidad del modelo de producto?***
- A) Adecuación funcional, eficiencia de rendimiento, compatibilidad, usabilidad, fiabilidad, escalabilidad, seguridad y mantenibilidad.
  - B) Adecuación funcional, eficiencia de rendimiento, compatibilidad, usabilidad, fiabilidad, seguridad, portabilidad y mantenibilidad.
  - C) Adecuación funcional, eficiencia de rendimiento, compatibilidad, usabilidad, fiabilidad, accesibilidad, seguridad y mantenibilidad.
  - D) Adecuación funcional, eficiencia de rendimiento, compatibilidad, usabilidad, fiabilidad, interoperabilidad, seguridad y mantenibilidad.
31. ***Respecto a la relación entre el Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001 en la acreditación de sistemas informáticos, ¿cuál de las siguientes afirmaciones es más precisa?***
- A) El ENS exige obligatoriamente que todos los sistemas de información de las administraciones públicas estén certificados en ISO/IEC 27001 para considerarse conformes.
  - B) La certificación ISO/IEC 27001 es indiferente, ya que sus requisitos son incompatibles con la estructura de categorías y medidas del ENS.
  - C) El ENS no obliga a certificarse en ISO/IEC 27001, pero reconoce que esta norma establece un sistema de gestión de seguridad certificable que puede utilizarse como marco de referencia.
  - D) La aplicación de ISO/IEC 27001 sustituye por completo la necesidad de realizar auditorías periódicas de cumplimiento del ENS.



32. ***En el contexto de la gestión de la seguridad de la información y la continuidad de negocio, ¿qué definición describe mejor el concepto de resiliencia de un sistema?***
- A) La capacidad del sistema para proporcionar y mantener un nivel aceptable de servicio ante la ocurrencia de fallos o desafíos a la operación normal, incluyendo su recuperación en un tiempo compatible con los objetivos de la organización.
  - B) El porcentaje de tiempo durante el cual un sistema está disponible sin interrupciones a lo largo de un periodo de referencia.
  - C) La capacidad de un sistema para protegerse frente a accesos no autorizados, garantizando la confidencialidad de la información.
  - D) El conjunto de medidas dirigidas exclusivamente a prevenir la ocurrencia de incidentes de seguridad, sin considerar la recuperación.
33. ***En un enfoque de desarrollo y despliegue continuo (CI/CD) de aplicaciones que soportan investigación científica, ¿cuál es el modo más adecuado de integrar las pruebas de seguridad?***
- A) Al final del proyecto, justo antes del primer despliegue.
  - B) Integrar pruebas automatizadas de seguridad (por ejemplo, SAST y DAST) en distintas etapas del pipeline CI/CD.
  - C) Ejecutar pruebas funcionales automatizadas, pues si el sistema cumple correctamente con su funcionalidad se considera suficientemente seguro.
  - D) Reservar las pruebas de seguridad exclusivamente para entornos de producción, con el fin de probar el sistema en condiciones reales.
34. ***¿Cuál es la diferencia fundamental entre la anonimización y la seudonimización según el RGPD y las técnicas descritas?***
- A) La seudonimización elimina permanentemente cualquier posibilidad de reidentificación, mientras que la anonimización es reversible.
  - B) La anonimización es irreversible y destruye la vinculación técnica de forma permanente, mientras que la seudonimización permite revertir el proceso mediante una "llave".
  - C) Ambos procesos son idénticos y eximen a los datos de las restricciones de privacidad del RGPD.
  - D) La anonimización solo se aplica a identificadores directos (nombres), mientras que la seudonimización se aplica a identificadores indirectos.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 13 de 32</p>
---	---	--


35. *¿Cuál es la ventaja de un firewall con capacidad DPI frente a uno tradicional para proteger un instrumento como criostato o un secuenciador?*
- A) Entiende el protocolo específico del instrumento y puede bloquear comandos inusuales (como un apagado de emergencia) fuera de parámetros normales.
  - B) Aumenta la velocidad de transmisión al ignorar los paquetes que ya han sido cifrados por el broker MQTT.
  - C) Permite que el dispositivo funcione sin necesidad de una dirección IP, operando exclusivamente en la capa de enlace.
  - D) Garantiza que el software del instrumento se actualice automáticamente desde servidores externos no verificados.
36. *¿Qué beneficio específico aporta la política de "Aislamiento de Puerto" (Private VLANs) en una red de sensores de laboratorio?*
- A) Permite que los sensores de una misma subred compartan datos de calibración automáticamente.
  - B) Cifra el tráfico de capa 2 utilizando el estándar IEEE 802.1AE (MACsec).
  - C) Facilita que el personal administrativo acceda a los instrumentos sin necesidad de una VPN.
  - D) Impide que los dispositivos de la misma VLAN se comuniquen entre sí, evitando que un atacante escanee sensores adyacentes si logra comprometer uno.
37. *¿Cuál es la función específica de la DMZ (Zona Desmilitarizada) de datos en el diseño de una infraestructura de red segmentada para investigación?*
- A) Actuar como un "intercambiador" donde residen los brokers o proxies, evitando conexiones directas entre los sistemas exteriores y servidores de análisis.
  - B) Proporcionar acceso WiFi abierto para que los investigadores utilicen sus dispositivos personales sin supervisión.
  - C) Almacenar de forma permanente la propiedad intelectual más sensible para que sea accesible desde internet.
  - D) Servir como la puerta de enlace predeterminada (Gateway) para que los sensores de la red de instrumentación accedan a actualizaciones externas.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 14 de 32</p>
---	---	--

38. *¿Qué medidas de seguridad críticas introduce el estándar MQTTS para mitigar las vulnerabilidades del protocolo MQTT base en el ámbito científico?*
- A) Aumenta la disponibilidad del servicio permitiendo conexiones anónimas sin restricciones de ancho de banda.
  - B) Implementa cifrado AES y autenticación mutua mediante certificados digitales X.509, asegurando que los datos sean ilegibles si se interceptan.
  - C) Elimina la necesidad de un servidor central (broker) mediante una arquitectura descentralizada de punto a punto.
  - D) Reduce la latencia de red al transmitir las credenciales en texto plano para evitar el overhead de procesamiento
39. *¿Qué limitación estratégica presenta una arquitectura de seguridad que confía exclusivamente en un firewall de perímetro?*
- A) Es incapaz de proteger dispositivos "silenciosos" como impresoras 3D o sensores que carecen de potencia de procesamiento.
  - B) Crea un riesgo pues una vez superada la barrera, el movimiento lateral hacia datos críticos es trivial.
  - C) Impide la identificación de aplicaciones específicas (capa 7) que podrían ser utilizadas para la exfiltración de datos.
  - D) Obliga a que todas las reglas de filtrado se gestionen de forma individual en cada estación de trabajo mediante GPOs.
40. *¿Cuál es la función crítica del servidor RADIUS dentro del estándar IEEE 802.1X?*
- A) Emitir la señal electromagnética de radio para que los dispositivos se conecten al WiFi.
  - B) Actuar como servidor de autenticación centralizado para validar identidades contra una base de datos como LDAP.
  - C) Cifrar el tráfico de los sensores IoT que no tienen capacidad de inicio de sesión manual.
  - D) Proporcionar un portal cautivo para que los invitados acepten los términos de uso sin contraseña.



41. ***¿Qué característica define al protocolo EAP-TLS como el método de autenticación más robusto para entornos de investigación?***
- A) La obligatoriedad de presentar certificados digitales tanto en el servidor como en el dispositivo del usuario.
  - B) El uso de una contraseña compartida (PSK) que debe rotarse cada 24 horas por todos los investigadores.
  - C) La capacidad de permitir el acceso basándose exclusivamente en la dirección MAC del hardware.
  - D) La eliminación del cifrado en la capa de enlace para priorizar la velocidad de transferencia de datos.
42. ***En una infraestructura de "red plana" (flat network), ¿qué riesgo crítico se facilita tras el compromiso de una estación de trabajo?***
- A) La optimización automática del tráfico de broadcast en todos los segmentos físicos.
  - B) El movimiento lateral, permitiendo al atacante saltar de sistemas de baja seguridad a activos críticos.
  - C) La desconexión inmediata y segura de todos los nodos de almacenamiento de datos.
  - D) La imposibilidad técnica de realizar escaneos de red para identificar vulnerabilidades.
43. ***¿En qué consiste la amenaza de hardware denominada "BadUSB" dentro de los riesgos de dispositivos extraíbles?***
- A) En el extravío accidental de unidades USB que contienen datos científicos sensibles sin cifrar.
  - B) En la exfiltración silenciosa de terabytes de información por parte de personal interno.
  - C) En la reprogramación del microcontrolador del dispositivo para que actúe como un teclado y ejecute comandos maliciosos.
  - D) En la inestabilidad técnica provocada por el uso de periféricos inteligentes en redes aisladas (air-gapped).
44. ***¿Para qué se utiliza específicamente el Cifrado Preservador de Formato (FPE) en el contexto del procesamiento de datos?***
- A) Para añadir una "sal" aleatoria a las funciones hash y evitar ataques de diccionario.
  - B) Para agrupar registros similares y reemplazar sus valores por el promedio del grupo.
  - C) Para garantizar que el dato seudonimizado mantenga la estructura original (por ejemplo, que un número de 16 dígitos siga teniendo 16 dígitos) y evitar errores de esquema en las herramientas.
  - D) Para añadir ruido estadístico controlado a las respuestas de las consultas y proteger la presencia de individuos en el conjunto de datos.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 16 de 32</p>
---	---	--

45. *¿En qué situación es imperativo realizar una Evaluación de Impacto en Protección de Datos (DPIA) en el ámbito de la investigación científica que utiliza uso de IA y Big Data?*
- A) En todos los proyectos de investigación, independientemente del tipo de datos.
  - B) Únicamente cuando el proyecto cuenta con financiación internacional.
  - C) Cuando se prevea un "alto riesgo" para los interesados, como en el tratamiento de datos sensibles a gran escala o el uso de tecnologías innovadoras.
  - D) Solo si el número de investigadores participantes supera la decena.
46. *¿Cómo clasifica el Reglamento General de Protección de Datos (RGPD) a los datos de salud, perfiles genéticos y variables sociodemográficas profundas?*
- A) Como datos de carácter meramente administrativo.
  - B) Como activos de información de bajo riesgo.
  - C) Como "categorías especiales de datos".
  - D) Como información de dominio público.
47. *¿Cuál es la principal característica que distingue a un ataque pasivo de uno activo?*
- A) El ataque pasivo busca interrumpir la disponibilidad de los servicios del sistema.
  - B) El ataque activo no deja huella operativa y es extremadamente difícil de detectar.
  - C) El ataque pasivo se limita a observar o monitorear las transmisiones sin alterar los recursos.
  - D) El ataque activo se basa únicamente en el análisis de tráfico para inferir patrones.
48. *¿Por qué las amenazas internas (insider threats) representan un riesgo crítico para las organizaciones?*
- A) Porque son ataques ejecutados exclusivamente desde redes públicas fuera del control de la empresa.
  - B) Porque el atacante ya posee acceso legítimo y ha superado los controles de seguridad perimetrales.
  - C) Porque siempre son ataques accidentales causados por la falta de formación del personal.
  - D) Porque requieren meses de reconocimiento externo antes de poder acceder a la red local.






49. *¿Qué define a un ataque dirigido (“targeted attack”) frente a uno de carácter indiscriminado?*
- A) Su éxito se basa en el envío masivo de correos de \*phishing\* genéricos a miles de usuarios.
  - B) El uso de herramientas automatizadas para identificar cualquier sistema vulnerable en internet.
  - C) La orientación específica hacia una institución mediante un perfilado profundo y persistencia en el tiempo.
  - D) El objetivo de propagar ransomware común para obtener un lucro económico rápido de forma masiva.
50. *¿Cuál es la característica principal que define el objetivo de una Amenaza Persistente Avanzada (APT)?*
- A) Obtener un rédito económico inmediato mediante el envío masivo de correo no deseado.
  - B) Realizar ataques oportunistas e indiscriminados contra cualquier sistema vulnerable en la red.
  - C) Ejecutar una campaña de intrusión dirigida de larga duración para el espionaje estratégico o la exfiltración de propiedad intelectual.
  - D) Utilizar virus comunes que pueden ser detectados fácilmente por las firmas de los antivirus tradicionales.
51. *En el contexto de la defensa contra APTs, ¿en qué se basa la detección mediante el análisis del comportamiento (UEBA)?*
- A) En la búsqueda de firmas de malware conocido en una base de datos global.
  - B) En la prohibición total del intercambio de archivos y la colaboración internacional.
  - C) En la identificación de anomalías operativas, como una conexión inusual a altas horas de la madrugada hacia un servidor sensible.
  - D) En asumir que el perímetro de red es impenetrable y no requiere monitorización interna.



52. *¿Por qué los atacantes suelen priorizar los sistemas administrativos y financieros en lugar de atacar directamente la infraestructura de investigación (High Performance Computing)?*
- A) Porque los sistemas administrativos contienen la propiedad intelectual más valiosa del centro.
  - B) Porque la infraestructura de investigación no tiene conexión alguna con la red de internet.
  - C) Porque los sistemas administrativos suelen tener una postura de seguridad inferior y sirven para escalar privilegios hacia el interior de la red.
  - D) Porque es imposible comprometer los sistemas de computación de alto rendimiento mediante ataques remotos.
53. *¿En qué consiste específicamente la técnica de "envenenamiento del entrenamiento" (Data Poisoning) en modelos de IA?*
- A) En saturar los servidores de procesamiento con peticiones masivas para provocar una denegación de servicio.
  - B) En introducir datos maliciosos o etiquetas erróneas durante la fase de aprendizaje para manipular la lógica interna del modelo.
  - C) En el uso de IA generativa para eliminar errores gramaticales en campañas de phishing y hacerlas más convincentes.
  - D) En la alteración del código de un antivirus en tiempo real para que no pueda ejecutarse en sistemas operativos modernos.
54. *¿Qué implica la estrategia de ataque denominada "Grabar ahora, Descifrar después" (Harvest Now, Decrypt Later)?*
- A) Recolectar hardware cuántico hoy para venderlo en el mercado negro cuando la tecnología madure.
  - B) Almacenar datos ya cifrados con algoritmos de cifra moderna hoy para descifrarlos en el futuro cuando existan computadoras cuánticas suficientemente potentes.
  - C) Infectar sistemas con malware latente que solo se activará tras detectar un procesador cuántico en la red.
  - D) Utilizar el algoritmo de Shor para acelerar la minería de criptomonedas antes de que se estandarice la criptografía post-cuántica.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 19 de 32</p>
---	---	--

**55. *En el contexto de la migración a la Criptografía Post-Cuántica (PQC), ¿qué define a la "Agilidad Criptográfica"?***

- A) La velocidad a la que un algoritmo cuántico puede factorizar números primos grandes en tiempo polinómico.
- B) El uso de redes (lattices) y funciones hash para que la IA detecte anomalías en milisegundos.
- C) La automatización de la respuesta a incidentes (SOAR) para reducir el tiempo de contención de horas a milisegundos.
- D) La capacidad de una infraestructura para cambiar algoritmos de cifrado de manera rápida y transparente sin interrumpir las operaciones.

**56. *¿Cuál es el principio fundamental que rige una Arquitectura de Confianza Cero (Zero Trust Architecture)?***

- A) Conceder acceso total a cualquier usuario que se conecte desde dentro del perímetro de la red corporativa.
- B) Delegar la seguridad exclusivamente en el uso de herramientas de inteligencia artificial generativa.
- C) Basar la protección en el principio de "nunca confiar, siempre verificar", independientemente de la ubicación del usuario.
- D) Eliminar las capas de cifrado para acelerar el procesamiento de datos en la nube.

**57. *¿Por qué el compromiso de la cadena de suministro (Supply Chain Attack) se ha vuelto una tendencia predominante?***

- A) Porque permite obtener acceso a miles de clientes finales al comprometer un solo componente de confianza, como una actualización de software.
- B) Porque es una técnica más sencilla que requiere menos conocimientos técnicos que un ataque directo.
- C) Porque los proveedores de servicios suelen carecer de cualquier tipo de medida de ciberseguridad.
- D) Porque el objetivo principal es sabotear la logística física de entrega de componentes de hardware.




58. ***En el contexto del fortalecimiento o bastionado técnico de una estación científica, ¿qué implica la "minimización de la superficie de ataque"?***
- A) Reducir el número de investigadores que tienen acceso físico al laboratorio de computación.
  - B) Configurar el firewall local para permitir todo el tráfico entrante de instituciones colaboradoras.
  - C) Eliminar todas las capas de cifrado de disco para mejorar el rendimiento de los análisis estadísticos.
  - D) Seguir una "política de lista blanca" instalando solo el software necesario y deshabilitando servicios superfluos.
59. ***Siguiendo la regla "3-2-1" para la gestión de backups en servidores científicos, ¿qué característica es fundamental para protegerse contra el ransomware?***
- A) Mantener las copias cifradas en origen y en una ubicación lógicamente aislada e inmutable
  - B) Almacenar todas las copias en el mismo servidor principal para un acceso inmediato.
  - C) Realizar las copias de seguridad sin cifrar para reducir el tiempo de restauración.
  - D) Utilizar un único soporte físico para todas las copias para simplificar la gestión.
60. ***¿Cuál es la limitación crítica de la detección basada en firmas en los sistemas antivirus tradicionales?***
- A) Consume una cantidad excesiva de recursos de CPU y memoria en comparación con otras técnicas.
  - B) Es intrínsecamente reactiva y no ofrece protección contra el malware de "día cero" (zero-day).
  - C) Solo es capaz de detectar software malicioso diseñado para sistemas operativos móviles.
  - D) Requiere que el usuario tenga privilegios de administrador para poder identificar cualquier archivo.
61. ***¿Qué diferencia fundamental define a las soluciones de Detección y Respuesta en los Puntos Finales (EDR) frente al antivirus tradicional?***
- A) El EDR se basa exclusivamente en el escaneo de archivos estáticos almacenados en el disco duro.
  - B) El EDR permite que los usuarios operen siempre con privilegios de administrador para facilitar el análisis.
  - C) El EDR solo funciona si el malware ya ha infectado el núcleo del sistema operativo.
  - D) El EDR analiza "qué hace" un proceso (comportamiento) en lugar de buscar "qué es" el archivo (firma).



62. *¿Qué factor es más determinante para la robustez de una contraseña frente a ataques de fuerza bruta?*
- A) La inclusión obligatoria de caracteres especiales y símbolos complejos.
  - B) El cambio frecuente y obligatorio de la clave cada 30 días.
  - C) La longitud de clave y el uso de frases de paso (passphrases) compuestas por palabras aleatorias.
  - D) La reutilización de patrones predecibles para facilitar el recuerdo por parte del investigador.
63. *¿Qué enfoque de control de aplicaciones prohíbe todo por defecto y solo permite la ejecución de software verificado mediante su Hash (SHA-256) o firma digital?*
- A) El enfoque reactivo basado en listas negras (blacklisting).
  - B) El enfoque proactivo basado en listas blancas (whitelisting).
  - C) El modelo de informática en la sombra (shadow IT).
  - D) El paradigma de seguridad perimetral basado en firewalls.
64. *En una arquitectura ZTA para un laboratorio de microscopía remota, ¿cuál es la función del PEP respecto al tráfico de datos?*
- A) Almacenar de forma segura las claves maestras de cifrado de todos los dispositivos.
  - B) Actuar como el agente que intercepta, establece y supervisa la conexión entre el sujeto y el instrumento tras la decisión del motor de políticas.
  - C) Generar los certificados de identidad digital para los nuevos sensores que se añaden a la red de forma dinámica.
  - D) Realizar el análisis de integridad de los datos científicos para descartar ruido experimental.
65. *Un infostealer ha robado las 'cookies de sesión' de un funcionario autenticado en el cloud mediante su certificado de empleado público. ¿Qué riesgo supone esto, aunque el certificado esté protegido?*
- A) Ninguno, ya que el proveedor cloud pedirá el certificado de nuevo para cada clic.
  - B) Permite al atacante realizar un 'Session Hijacking', accediendo al cloud sin poseer el certificado físico.
  - C) El atacante podrá usar la cookie para emitir nuevos certificados oficiales a su nombre.
  - D) La sesión se cerrará automáticamente en el momento en que el malware toque el archivo de cookies.



66. ***En un entorno 'Multi-Party Computation', ¿qué mecanismo permite la mayor granularidad sin crear usuarios en cada organización?***
- A) Listas de Control de Acceso (ACL) basadas en el ID de cuenta.
  - B) Políticas de bucket públicas filtradas por dirección IP.
  - C) Federación de identidades mediante roles de IAM con condiciones de contexto (Contextual Conditions).
  - D) Uso de una clave secreta compartida (PSK) para todos los centros de investigación.
67. ***Para garantizar la integridad de datasets masivos (ej. genómica) frente a corrupción silenciosa, ¿cuál es la mejor práctica de arquitectura?***
- A) Confiar exclusivamente en las sumas de comprobación (checksums) automáticas del proveedor tras la subida.
  - B) Implementar 'Content-Addressable Storage' (CAS) con validación de hashes end-to-end y Object Lock.
  - C) Utilizar exclusivamente discos persistentes con redundancia local (LRS).
  - D) Habilitar el versionado de objetos sin controles de acceso granulares.
68. ***En un entorno de computación científica, ¿cuál es el propósito principal del flujo OBO cuando un servicio de análisis necesita acceder a un repositorio de datos protegido?***
- A) Permitir que el servicio de análisis use sus propias credenciales de administrador para acceder a cualquier dato.
  - B) Evitar que el usuario tenga que iniciar sesión en el portal científico original.
  - C) Cifrar los datos científicos antes de que salgan del repositorio hacia la nube pública.
  - D) Intercambiar el token de acceso del usuario por un nuevo token que permita al servicio intermedio llamar a un servicio de backend.
69. ***En el contexto de detección de anomalías en redes de transferencia de datos científicos, ¿por qué los modelos basados en firmas suelen ser insuficientes?***
- A) Debido a que el uso de cifrado impide la lectura de los encabezados de capa 4.
  - B) Porque los investigadores científicos siempre utilizan protocolos propietarios no documentados.
  - C) Porque las firmas de Snort no pueden analizar archivos de más de 1GB.
  - D) Porque el tráfico legítimo en el ámbito científico a menudo imita el comportamiento de un ataque de exfiltración o de DoS.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 23 de 32</p>
---	---	--

70. *¿Cuál es la función principal de un 'Network Tap' frente a un puerto 'SPAN' en la monitorización de alta precisión para seguridad científica?*
- A) El TAP permite filtrar tráfico de capa 7 antes de enviarlo al sensor.
  - B) El TAP es un dispositivo activo que puede inyectar paquetes para mitigar ataques en tiempo real.
  - C) SPAN es superior porque mantiene la sincronización temporal de hardware mejor que un TAP.
  - D) El TAP garantiza la entrega de todos los paquetes físicos, incluyendo errores de CRC, sin descartarlos por saturación de la CPU del switch.
71. *Si una plataforma obliga a usar el número de identidad (DNI/NIE) como nombre de usuario visible, ¿qué principio del Artículo 5 del RGPD se está vulnerando principalmente?*
- A) Integridad y Confidencialidad.
  - B) Interoperabilidad transnacional.
  - C) Exactitud.
  - D) Seguridad por diseño y por defecto.
72. *En un entorno de investigación de alto nivel, ¿cuál es la justificación técnica primordial para implementar una separación estricta mediante el uso de identidades federadas (como EduGAIN) y proveedores de identidad (IdP) distintos para la actividad académica y la personal?*
- A) Habilitar la indexación automática en bases de datos bibliográficas como Scopus o WoS.
  - B) Mitigación del riesgo de escalada de privilegios y el control de la superficie de ataque mediante el principio de compartimentación.
  - C) El cumplimiento estricto de la Ley de Propiedad Intelectual sobre los borradores de documentos compartidos.
  - D) La optimización del ancho de banda institucional al filtrar el tráfico de redes sociales personales.
73. *En autenticación mTLS, ¿qué ocurre inmediatamente después de que el servidor envía su certificado al cliente?*
- A) El servidor cierra la conexión para evitar ataques de denegación de servicio.
  - B) El cliente genera una clave simétrica y la envía sin cifrar al servidor.
  - C) El servidor solicita el certificado digital del cliente para validar su identidad.
  - D) El cliente cifra todo el tráfico con su clave privada antes de recibir respuesta.



74. ***Un entorno científico utiliza tokens de hardware basados en FIDO2/WebAuthn. ¿Qué propiedad técnica fundamental impide los ataques de 'man-in-the-middle' (MitM) en este protocolo?***
- A) El uso de algoritmos de hashing simétricos como SHA-256 para la transmisión de secretos.
  - B) La rotación automática de claves privadas después de cada acceso a sistema.
  - C) El enlace criptográfico del origen (domain binding) firmado por el autenticador.
  - D) La implementación obligatoria de biometría como único factor de desbloqueo del token.
75. ***Al implementar RBAC sobre una arquitectura de Microservicios, ¿cuál es el propósito de utilizar tokens firmados (como JWT) que incluyan el 'claim' de roles?***
- A) Garantizar que el usuario no pueda cerrar sesión sin el permiso del administrador.
  - B) Permitir la autorización descentralizada sin que cada microservicio consulte constantemente al servicio de identidad central.
  - C) Cifrar la base de datos de usuarios para que los desarrolladores no vean las contraseñas.
  - D) Reemplazar completamente el protocolo TLS/SSL en las comunicaciones de red.
76. ***Bajo la política de 'Separación Dinámica de Deberes' (DSoD), ¿cuándo se aplica la restricción de conflicto entre dos roles?***
- A) Únicamente cuando el usuario intenta acceder a la base de datos de auditoría.
  - B) En el momento de asignación del usuario al rol por parte del administrador.
  - C) Cuando el sistema de archivos detecta una colisión de identidades federadas.
  - D) En el momento de la activación de los roles dentro de una misma sesión de usuario.
77. ***Desde la perspectiva de cumplimiento (Compliance), ¿cuál es el desafío legal de mayor impacto al procesar datos genómicos sujetos a GDPR en una modalidad de teletrabajo internacional?***
- A) La transferencia internacional de datos a jurisdicciones sin una "Decisión de Adecuación" de la CE o sin "Cláusulas Contractuales Tipo" (SC válidas).
  - B) El elevado coste de mantenimiento de las licencias de software de seguridad para investigadores residentes en países en vías de desarrollo.
  - C) La imposibilidad técnica de realizar auditorías físicas presenciales en los domicilios particulares de los investigadores contratados.
  - D) La diferencia de husos horarios que dificulta la monitorización de los logs de seguridad en tiempo real por parte del DPO.






78. *Al implementar un modelo de acceso para investigadores remotos, ¿qué ventaja técnica diferencial ofrece un esquema de "Zero Trust Network Access" (ZTNA) frente a una VPN "Full-Tunnel" tradicional?*
- A) Elimina la necesidad de cifrar el tráfico de datos, ya que la confianza se establece únicamente a nivel de identidad del investigador.
  - B) Reduce drásticamente la latencia de red al permitir que el tráfico de los experimentos viaje por canales UDP sin verificación de integridad.
  - C) Permite el uso de dispositivos personales (BYO sin necesidad de instalar agentes de cumplimiento o verificaciones de postura (Health Checks).
  - D) Proporciona acceso granular basado en aplicaciones y contexto, evitando que un endpoint comprometido realice escaneo de red o movimiento lateral.
79. *Al definir el MAO para una línea de investigación clínica o experimental, ¿cuál es el criterio técnico de mayor criticidad que debe prevalecer?*
- A) El impacto en la reputación institucional y la confianza de los organismos financiadores.
  - B) La ventana temporal máxima antes de que la interrupción en la monitorización de experimentos invalide la significación estadística de la serie de datos.
  - C) El coste operativo prorrateado de los salarios del personal investigador durante el tiempo de inactividad.
  - D) La capacidad técnica de los sistemas de backup de IT para replicar el estado actual de las máquinas virtuales.
80. *Al realizar un fuzzing de protocolos en una interfaz de hardware de alta velocidad (como USB 4.0 o PCIe), ¿cuál es el riesgo crítico derivado de un fallo en la Máquina de Estados?*
- A) Una degradación progresiva en el ancho de banda efectivo del bus de datos.
  - B) El sobrecalentamiento físico de los rastros de cobre en la placa de circuito impreso.
  - C) La generación de una interrupción que fuerce al sistema operativo a solicitar una actualización de drivers.
  - D) La transición forzada del hardware hacia estados de depuración (debug) o privilegios elevados no documentados.
81. *¿Qué vulnerabilidad de hardware explota el fenómeno de acoplamiento capacitivo entre líneas de memoria para inducir una inversión de bits (bit-flipping) sin tener permisos de escritura?*
- A) Spectre v2.
  - B) Rowhammer.
  - C) Buffer Overflow de nivel 0 (Kernel heap).
  - D) Meltdown.



82. ***En un ejercicio de "Lecciones Aprendidas", el equipo analiza el Dwell Time. ¿Qué representa exactamente esta métrica en la gestión de incidentes de seguridad?***
- A) El tiempo que tarda el equipo de IT en restaurar un servidor crítico desde el último backup disponible.
  - B) El tiempo acumulado que los empleados dedican a visualizar los contenidos de la plataforma de formación continua.
  - C) La latencia de red medida entre el servidor colector de logs (SIEM) y los agentes instalados en los equipos finales.
  - D) El tiempo total que el atacante permaneció en la red desde la intrusión inicial hasta su detección y expulsión.
83. ***Durante un ataque de Ransomware activo, el equipo de respuesta decide aplicar una "Contención Estratégica" mediante el aislamiento de la red en lugar de apagar físicamente los servidores. ¿Cuál es la justificación técnica primordial según RFC 3227?***
- A) Evitar el desgaste mecánico y posibles fallos de sectores en los discos duros ante un reinicio forzado.
  - B) Preservar artefactos en memoria RAM, como llaves de cifrado simétrico (AES) y procesos inyectados (beacons).
  - C) Permitir que el atacante termine de cifrar archivos no críticos para identificar su patrón de conducta y TTPs.
  - D) Cumplir estrictamente con la normativa GDPR que prohíbe el apagado de servidores que contienen bases de datos.
84. ***¿Qué herramienta de código abierto es considerada el estándar para capturar e inspeccionar el tráfico de red a nivel de paquetes?***
- A) Nmap.
  - B) Metasploit Framework.
  - C) Wireshark.
  - D) Putty SSH Client.
85. ***En Windows, ¿qué herramienta centralizada se utiliza para configurar qué eventos de éxito o error (como inicios de sesión o acceso a objetos) deben registrarse?***
- A) Administrador de Tareas.
  - B) Editor de Directivas de Grupo (gpedit.msc / GPM).
  - C) Panel de Control de Cuentas de Usuario (UA).
  - D) Editor del Registro (regedit).




86. ***En la fase de 'Planificación y Preparación' de la ISO/IEC 27035, ¿cómo se debe integrar la formación para mitigar ataques de BEC?***
- A) Instruyendo exclusivamente al SOC en la creación de reglas de correo electrónico para bloquear palabras clave.
  - B) Capacitando al personal de departamentos clave en procesos de verificación fuera de banda para transacciones críticas.
  - C) Automatizando el cambio de contraseñas cada 15 días para todos los empleados del área contable.
  - D) Prohibiendo el uso de correos electrónicos externos para cualquier comunicación con proveedores.
87. ***Tras un incidente grave originado en un terminal BYOD, ¿cuál sería la medida correctiva más adecuada en la fase de Post-incidente?***
- A) Eliminar el programa BYOD y obligar a todos a usar solo ordenadores de sobremesa.
  - B) Revisar y actualizar la política de uso aceptable y mejorar el despliegue de soluciones de segmentación.
  - C) Sancionar económicamente al empleado por el coste del tiempo de inactividad del servidor.
  - D) Publicar el nombre del empleado en el boletín interno para concienciar al resto de la plantilla.
88. ***Bajo el marco de la CRA de la UE, ¿qué obligación crítica recae sobre el fabricante durante las fases de recuperación y post-incidente tras detectarse una vulnerabilidad explotada?***
- A) Notificar la vulnerabilidad a ENISA en un plazo de 24 horas desde que se tiene constancia de su explotación.
  - B) Esperar a que CEN/CENELEC publiquen una nueva norma ISO antes de aplicar el parche.
  - C) Delegar la responsabilidad de la recuperación exclusivamente en el usuario final del producto.
  - D) Desactivar el producto permanentemente para evitar cualquier responsabilidad legal futura.
89. ***¿Cuál es la principal ventaja de la regla de respaldo 3-2-1?***
- A) Asegurar que el tiempo de restauración sea siempre inferior a una hora.
  - B) Eliminar puntos únicos de fallo al diversificar las copias y los soportes físicos.
  - C) Evitar la necesidad de realizar copias de seguridad completas de forma periódica.
  - D) Centralizar todos los datos en un único proveedor de nube para reducir costes.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 28 de 32</p>
---	---	--


90. *¿Qué combinación de métricas define mejor la diferencia de objetivos entre un SOC y un CSIRT?*
- A) El SOC mide el volumen de logs procesados y el CSIRT el número de Parches instalados.
  - B) El SOC se centra en el MTTD y el CSIRT en el MTTR.
  - C) El SOC mide la disponibilidad del servidor y el CSIRT el ancho de banda recuperado.
  - D) El SOC evalúa el coste por licencia y el CSIRT el número de empleados por turno.
91. *¿Cuál es el enfoque principal que define la actividad diaria de un SOC?*
- A) La vigilancia continua, monitorización de alertas y detección de amenazas en tiempo real.
  - B) La respuesta ante desastres naturales y continuidad de negocio.
  - C) La creación de leyes y normativas de ciberseguridad a nivel nacional.
  - D) La investigación forense profunda de incidentes que ya han finalizado.
92. *En el contexto de medidas correctivas, ¿qué diferencia a una 'corrección' de una 'acción correctiva'?*
- A) La corrección elimina la causa raíz y la acción correctiva elimina el síntoma.
  - B) No existe diferencia; ambos términos se refieren a reparar el daño de forma inmediata.
  - C) La corrección es para incidentes leves y la acción correctiva para graves.
  - D) La corrección elimina el incumplimiento detectado, mientras que la acción correctiva elimina la causa de dicho incumplimiento.
93. *¿Cuál es el objetivo principal de realizar una revisión post-incidente (PIR)?*
- A) Identificar y sancionar a los responsables del error.
  - B) Analizar qué sucedió y cómo mejorar la respuesta futura.
  - C) Justificar el aumento de presupuesto ante la dirección.
  - D) Documentar el incidente únicamente para cumplir con normativas legales.



94. ***En una incautación forense, ¿cuál es la diferencia más crítica al preservar un HDD rotacional frente a un SSD NVMe respecto a la modificación inadvertida de datos al encender el equipo intervenido?***
- A) Solo en HDD se modifican metadatos SMART al encender, mientras que en SSD NVMe jamás se alteran metadatos internos sin una orden explícita de escritura.
  - B) En ambos (HDD y SSD NVMe), el encendido nunca modifica datos si no se inicia el sistema operativo original del usuario.
  - C) En SSD NVMe, el firmware puede ejecutar garbage collection y TRIM al recibir energía, alterando bloques lógicos, mientras que en HDD los cambios automáticos en el plato son mínimos si no hay escritura activa.
  - D) En HDD, el simple encendido activa rutinas internas de garbage collection que reescriben sectores, mientras que en SSD NVMe no ocurre ningún cambio automático.
95. ***En una diligencia de incautación, ¿cuál es la principal diferencia práctica al manipular un disco duro rotacional frente a un SSD o NVMe respecto al riesgo de pérdida de datos relevantes como evidencia?***
- A) El disco duro rotacional borra automáticamente sectores dañados al desconectarlo, mientras que SSD y NVMe nunca hacen operaciones internas sin orden judicial.
  - B) No existe ninguna diferencia relevante: todos los soportes se comportan igual frente a golpes, desconexiones y escrituras accidentales.
  - C) El disco duro rotacional es más sensible a golpes físicos, mientras que SSD y NVMe son más sensibles a escrituras lógicas inadvertidas que pueden activar borrado o sobreescritura interna.
  - D) SSD y NVMe son más vulnerables a campos magnéticos externos, mientras que los discos duros rotacionales son inmunes a ellos.
96. ***Durante el análisis forense de un teléfono móvil incautado, el perito debe trabajar sobre una copia de los datos y no directamente sobre el dispositivo original. ¿Cuál es la razón jurídica y técnica principal para esta práctica dentro de la cadena de custodia?***
- A) Evitar el uso de equipos costosos del laboratorio, ya que la copia es siempre más económica.
  - B) Proteger la integridad de la evidencia original y poder repetir el análisis sin alterar los datos.
  - C) Agilizar el proceso judicial reduciendo la cantidad de documentos en el expediente.
  - D) Impedir que el perito conozca toda la información personal del titular del dispositivo.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 30 de 32</p>
---	---	--

97. *Al utilizar Sysmon en Windows, ¿qué Event ID es imprescindible monitorizar para rastrear posibles movimientos laterales entre máquinas?*
- A) Event ID 1.
  - B) Event ID 3.
  - C) Event ID 5.
  - D) Event ID 255.
98. *¿Cuál es la diferencia fundamental entre un Indicador de Compromiso (IoC) y un Indicador de Ataque (IoA) durante la fase de Detección y Análisis?*
- A) El IoC es una evidencia puramente digital, mientras que el IoA hace referencia a un evento físico o de ingeniería social.
  - B) Los IoC son exclusivos de sistemas Windows, mientras que los IoA se aplican únicamente a entornos Linux y Cloud.
  - C) El IoC se centra en la evidencia forense post-mortem (hashes, IPs); el IoA identifica la intención y el comportamiento en tiempo real.
  - D) La normativa ISO 27035 establece que solo los IoC tienen validez legal como evidencia en un proceso judicial.
99. *Tras un desastre, ¿qué procedimiento de validación de datos es indispensable antes de declarar el "Retorno a la Normalidad" y reanudar una investigación interrumpida?*
- A) Ejecutar pruebas de control con materiales de referencia certificados para descartar derivas o descalibraciones en los instrumentos de precisión.
  - B) Revisar exhaustivamente los registros de acceso físico (logs) para confirmar que nadie accedió al laboratorio durante la evacuación.
  - C) Solicitar a los investigadores principales que firmen una declaración de conformidad basada en su inspección visual de los datos recuperados.
  - D) Comparar exclusivamente el volumen total de datos (en G antes y después del incidente para asegurar que no hay pérdida de archivos.
100. *¿Qué técnica es más utilizada durante la evaluación post-incidente para llegar a la causa origen?*
- A) La técnica de los cinco porqués.
  - B) Evaluación de vulnerabilidades.
  - C) Matriz de riesgos de probabilidad e impacto.
  - D) Análisis de impacto en el negocio o BIA (Business Impact Analysis).

	Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025 Primer Ejercicio	Fecha: 10/05/2026 Página: 31 de 32
---	--	--

## PREGUNTAS DE RESERVA

- 101.** *La medida de seguridad op.acc.1 del Anexo II del Esquema Nacional de Seguridad se refiere a:*
- A) El proceso de gestión de derechos de acceso.
  - B) La segregación de funciones y tareas.
  - C) Los requisitos de acceso.
  - D) La identificación.
- 102.** *Conforme al artículo 12.6 del Esquema Nacional de Seguridad (ENS), no es un requisito mínimo para el desarrollo de la política de seguridad:*
- A) Análisis y gestión de los riesgos.
  - B) Profesionalidad.
  - C) Mejora continua del proceso de seguridad
  - D) Protección de los sistemas.
- 103.** *¿Cuál es la función principal de inotify en la gestión de logs en Linux?*
- A) Rotar archivos de log según su tamaño.
  - B) Cifrar los logs antes de escribirlos en disco.
  - C) Bloquear el acceso a archivos auditados.
  - D) Notificar eventos del sistema de archivos en tiempo real a las apps.
- 104.** *Para prevenir el movimiento lateral dentro de una red que conecta instrumentos de precisión (como un sincrotrón o un criomicroscopio), ¿qué técnica de segmentación se considera la más robusta bajo un enfoque de defensa en profundidad?*
- A) Implementación de VLANs basadas en puertos físicos para separar los diferentes laboratorios dentro del mismo edificio.
  - B) Adopción de Microsegmentación mediante el uso de identidades de carga de trabajo (Workload Identity) y mTLS entre cada sensor y el servidor de datos.
  - C) Configuración de listas de control de acceso (ACL) estáticas en el router de núcleo (Core) de la infraestructura científica.
  - D) Filtrado estricto de direcciones MAC en todos los switches de la capa de acceso para impedir la conexión de dispositivos no inventariados.



105. *Durante la fase de Contención de un incidente que afecta a un smartphone personal (BYOD) con datos corporativos, ¿cuál es la medida técnica más equilibrada para proteger la empresa sin vulnerar la privacidad del empleado?*
- A) Realizar un borrado de fábrica remoto de todo el dispositivo.
  - B) Solicitar al empleado que entregue el terminal físicamente para un análisis forense completo de sus fotos y mensajes.
  - C) Ejecutar un borrado selectivo de las aplicaciones y contenedores corporativos gestionados por el MDM.
  - D) Bloquear el acceso a internet de toda la vivienda del empleado hasta que el incidente se resuelva.

\*\*\*\*\* FIN DEL CUESTIONARIO \*\*\*\*\*