PUBLICACIÓN DE LA PLANTILLA DE CORRECCIÓN DEL EXAMEN TIPO TEST DE LA PRIMERA FASE DE LA CONVOCATORIA ESPECÍFICA DE SELECCIÓN DE PERSONAL PARA EL ACCESO LIBRE A LAS VACANTES CORRESPONDIENTES A LA TASA DE REPOSICIÓN DE LA S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, M.P., S.A. (INCIBE)

INC-DO02E-25001. Perfil de Técnico Senior de Laboratorio de Tecnologías

En aplicación del principio de transparencia, se hace pública la plantilla de corrección junto con las respuestas correctas correspondientes al examen tipo test celebrado el pasado 21 de noviembre de 2025, para la cobertura de la plaza indicada en el Anexo I de la convocatoria específica de selección de personal para el acceso libre a las vacantes correspondientes a la tasa de reposición de la S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE).

Se informa a las personas aspirantes que, a partir de la fecha de esta publicación, disponen de un plazo de tres días naturales para presentar las alegaciones que estimen oportunas.

El plazo para la presentación de alegaciones finalizará el **27 de noviembre de 2025 a las 23:59 horas (CEST)**. Las alegaciones deberán enviarse por correo electrónico a la dirección **convocatorias@incibe.es**, indicando en el cuerpo del mensaje el **nombre y apellidos de la persona candidata, DNI y motivo de la alegación**.

Todas las alegaciones recibidas en plazo serán debidamente analizadas y resueltas por el **Tribunal Calificador**.

ANEXO I. PERFIL DE TÉCNICO SENIOR DE LABORATORIO DE TECNOLOGÍAS.

Se procede a publicar la plantilla de respuestas , así como preguntas y respuestas correctas

PLANTILLA DE RESPUESTAS

1	B
2	C
3	B
4	B
5	B
6	B
7	C
8	C
9	B
10	A
11	D
12	C
13	B
14	B
15	B

PREGUNTAS DE RESERVA:

16	B
17	C
18	B

PREGUNTAS Y RESPUESTAS CORRECTAS

1. ¿Cuál de las siguientes afirmaciones sobre el ámbito de aplicación (artículo 2) del Reglamento (UE) 2024/2847 es **incorrecta**?

    a. El Reglamento no se aplica a los productos con elementos digitales desarrollados o modificados exclusivamente con fines de seguridad nacional o defensa ni a los productos diseñados específicamente para el tratamiento de información clasificada.

    b. El Reglamento no se aplica a productos que no tengan conectividad directa a Internet, aunque puedan comunicarse con otros dispositivos.

    c. El Reglamento no es aplicable a los productos con elementos digitales que hayan sido certificados de conformidad con el Reglamento (UE) 2018/1139.

    d. El Reglamento no se aplica a las piezas de recambio que se comercialicen para reemplazar componentes idénticos en productos con elementos digitales y que se fabriquen con arreglo a las mismas especificaciones que los componentes a los que están destinadas a sustituir.

2. ¿Cuál de las siguientes afirmaciones sobre los requisitos de ciberseguridad relativos a las propiedades de los productos con elementos digitales (Parte I del Anexo I), del Reglamento (UE) 2024/2847 es **incorrecta**?

    a. protegerán la integridad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, los comandos, los programas y la configuración frente a toda manipulación o modificación no autorizada por el usuario, e informarán sobre los casos de corrupción de datos.

    b. tratarán únicamente los datos personales o de otro tipo que sean adecuados, pertinentes y limitados a lo que sea necesario para la finalidad prevista del producto con elementos digitales («minimización de datos»).

    c. protegerán la confidencialidad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, aplicando técnicas de anonimización ante posibles accesos no autorizados.

    d. garantizarán la protección contra el acceso no autorizado mediante mecanismos de control adecuados, incluidos, entre otros, sistemas de gestión de la autenticación, la identidad o el acceso, e informarán de posibles accesos no autorizados.

3. ¿Cuál de las siguientes afirmaciones sobre la gestión de vulnerabilidades en productos con elementos digitales (Parte II del Anexo I), del Reglamento (UE) 2024/2847 es **incorrecta**?

a. Los fabricantes deben identificar y documentar vulnerabilidades conocidas y razonablemente previsibles que puedan afectar la seguridad del producto.

b. Los fabricantes deben diseñar medidas de mitigación que solo se apliquen a vulnerabilidades críticas detectadas antes de la comercialización del producto.

c. Cuando los fabricantes consideren que los riesgos para la seguridad de la publicación superan los beneficios en materia de seguridad, podrán retrasar la publicación de información sobre una vulnerabilidad solucionada hasta que se haya dado a los usuarios la posibilidad de aplicar el parche correspondiente.

d. Los fabricantes deben establecer procedimientos que permitan la detección, evaluación y gestión de vulnerabilidades durante todo el ciclo de vida del producto.

4. ¿Cuál de las siguientes opciones describe un procedimiento válido y que incluye las condiciones suficientes para descifrar tráfico HTTPS que, una aplicación que está siendo auditada y que está instalada en un equipo informático del que se tienen permisos de administración, envía a servicios web legítimos de terceros?

a. Usar un proxy para forzar tráfico HTTP y capturar el tráfico ya descifrado con wireshark.

b. Obtener los secretos de sesión durante el proceso de negociación inicial, por ejemplo, usando SSLKEYLOGFILE, capturar el tráfico mediante *tcpdump* y descifrarlo con las claves TLS obtenidas previamente

c. Capturar el tráfico HTTPs en cualquier momento de la comunicación permitirá descifrarlo, ya que se tienen permisos de administración y por tanto se tiene acceso a los secretos de sesión TLS.

d. Instalar la aplicación en un docker y utilizar tcpdump permitirá capturar todo el tráfico en la interfaz de red del docker, incluidas las claves TLS.

5. ¿Cuál de las siguientes afirmaciones es **correcta** respecto al comando “nmap -sU -p- <dirección IP objetivo>” de la herramienta Nmap?

a. Realiza, sobre la dirección IP objetivo, un envío muy rápido de tráfico anómalo y segmentado.

b. Realiza, sobre la dirección IP objetivo, un escaneo UDP de todos los puertos del objetivo, genera mucho tráfico y se desaconseja por ser lento e intrusivo.

c. Escanea, sobre la dirección IP objetivo, los puertos UDP más comunes (0–1023) y es seguro en entornos de producción.

d. Solo analiza si el host en la dirección IP objetivo está activo, sin enviar paquetes a puertos específicos.

6. Si se quiere ejecutar un escaneo de vulnerabilidades, con una herramienta como Nessus, desde una máquina virtual (VM) en VirtualBox contra un equipo de la misma red que el equipo anfitrión (host), ¿cómo se debe configurar la interfaz de red de la VM para que Nessus pueda comunicarse correctamente con la red?

    a. Configurar la interfaz de red de la VM en modo NAT, ya que permite que la VM acceda a internet y descubra automáticamente los equipos de la red.

    b. Configurar la interfaz de red de la VM en modo puente (Bridged), para que la VM tenga una dirección IP en la misma red que el host y pueda escanear otros equipos.

    c. Habilitar un *Port Mirror* entre la interfaz del host y la de la máquina virtual.

    d. Configurar la VM en modo NAT con puerto redirigido, lo cual permite escanear automáticamente todas las IP de la red local.

7. ¿Qué parámetro debe habilitarse en Linux para permitir el reenvío de paquetes entre dos redes, es decir, para que el sistema actúe como router?

    a. rp_filter

    b. accept_redirects

    c. net.ipv4.ip_forward

    d. conntrack_forward

8. ¿Cuál de las siguientes afirmaciones sobre directorios relativos a la estructura del sistema de archivos de Linux, es **incorrecta**?

    a. /dev contiene ficheros del sistema representando los dispositivos que estén físicamente instalados en el ordenador.

    b. /etc está reservado para los ficheros de configuración del sistema.

    c. /proc contiene programas que son únicamente accesibles al superusuario o "root".

    d. /var contiene información temporal de los programas.

9. En una comunicación que sigue el modelo OSI, ¿qué capa es responsable de la cifrado y compresión de datos?

    a. Capa de sesión.

    b. Capa de presentación.

    c. Capa de aplicación.

    d. Capa de red.

10. ¿Qué desafío se presenta en la integración de datos provenientes de dispositivos IoT en un sistema SIEM?

a. **La falta de normalización en los formatos de los logs generados por los dispositivos IoT, que dificultan la correlación y el análisis de eventos.**

b. La escasa cantidad de logs generados por los dispositivos IoT, lo que hace difícil identificar patrones de comportamiento anómalo.

c. La necesidad de incorporar inteligencia artificial para filtrar datos irrelevantes de IoT sin afectar la detección de amenazas.

d. La incapacidad de los dispositivos IoT para generar eventos significativos que puedan ser aprovechados por el sistema SIEM para realizar análisis de seguridad.

11. ¿Cuál de las siguientes técnicas o sub-técnicas se encuentra dentro de las tácticas de Movimiento Lateral (Lateral Movement) en la matriz MITRE ATT&CK (Enterprise Matrix)?

    a. Setuid and Setgid.

    b. Port Knocking.

    c. Winlogon Helper DLL.

    d. RDP Hijacking.

12. ¿Cuál de los siguientes es el nombre de una herramienta que se podría utilizar para capturar una señal Bluetooth emitida por un dispositivo IoT doméstico?

    a. Aircrack-ng Suite

    b. OpenBLE

    c. HackRF One

    d. BT-Hunter

13. ¿Cuál es el principio fundamental que garantiza la seguridad de la criptografía cuántica en la distribución de claves (QKD)?

    a. La dificultad computacional de factorizar números primos grandes.

    b. La imposibilidad de medir un estado cuántico sin alterarlo.

    c. El uso de algoritmos de cifrado simétrico avanzados como AES-256.

    d. La resistencia de las funciones hash frente a colisiones.

14. ¿Cuál es la función principal de una Autoridad Certificadora (CA) dentro de una infraestructura de clave pública (PKI)?

    a. Generar claves simétricas para cifrado de datos en tránsito.

    b. Emitir y validar certificados digitales que vinculan claves públicas con identidades.

c. Asegurar la confidencialidad de los mensajes mediante cifrado asimétrico.

d. Almacenar certificados en la nube.

15. En el uso de Inteligencia Artificial y, en concreto, LLMs (Large Language Models), ¿qué técnica se debe utilizar para generar respuestas basadas en información actualizada y específica sin necesidad de reentrenar el modelo?

    a. Fine-Tuning del modelo con datos históricos.

    b. Retrieval-Augmented Generation (RAG)

    c. Reinforcement Learning from Human Feedback (RLHF).

    d. Mixture of Contextual Prompts (MCP).

Preguntas de reserva:

16. En relación con los servidores de redes privadas virtuales (VPN), señale la respuesta **correcta**:

    a. Un concentrador VPN puede establecer conexiones seguras (túneles) con dispositivos de usuario, pero no con otros servidores VPN.

    b. La autenticación mutua entre los extremos del túnel VPN se lleva a cabo, en general, mediante certificados de clave pública X.509.

    c. La tecnología "VPN as a Service" (VPNaaS) no puede utilizarse para establecer conexión a los recursos de la red interna corporativa (on-premise).

    d. Las VPN basadas en IPSec tienen como ventaja la ausencia de problemas de compatibilidad con la traslación de direccionamiento IP (NAT).

17. ¿Cuál de las siguientes afirmaciones sobre la tecnología Zigbee es **incorrecta**?

    a. Usa topología en malla.

    b. Se basa en el estándar IEEE 802.15.4.

    c. Su consumo eléctrico es mayor que el estándar IEEE 802.15.1 (Bluetooth).

    d. Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

18. ¿Cuál es el estándar OASIS para el intercambio de mensajes sobre TCP pensado para dispositivos de baja potencia en aplicaciones IoT?

a. DDS.

b. MQTT.

c. CoAP.

d. STOMP.

La Presidenta del Tribunal

En León, a 24 de noviembre de 2025

S.M.E. Instituto Nacional de Ciberseguridad de España M.P