Test Tema 127 #1

Actualizado el 13/04/2025

1. Indique cuál de las siguientes no es una función del Centro de Operaciones de Ciberseguridad de la AGE y sus OOPP:

a) Prestación de servicios horizontales de ciberseguridad

b) Aumentar la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de la Administración

c) Facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad

d) Mejora de su capacidad de respuesta ante cualquier ataque

2. Según la arquitectura orgánica de la ciberseguridad que establece la Estrategia Nacional de Ciberseguridad 2019, ¿qué órgano facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad?

a) Consejo Nacional de Ciberseguridad

b) Comisión Permanente de Ciberseguridad

c) Foro Nacional de Ciberseguridad

d) Consejo de Seguridad Nacional

3. ¿Qué herramienta del CCN-Cert permite una gestión de ciberincidentes?:

a) LUCIA

b) CORINTO

c) CARMEN

d) PLATA

4. De las siguientes funciones del Consejo de Seguridad Nacional, conforme al artículo 5 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, indique aquella que es INCORRECTA:

a) Comunicar a la Comisión Europea la lista de los operadores de servicios esenciales nacionales establecidos para cada sector y subsector e informar a los puntos de contacto único de otros Estados sobre la intención de identificación de un operador de servicios esenciales de otro Estado miembro que ofrezca servicios en España.

b) Comunicar oportunamente a la Comisión Nacional para la Protección de las Infraestructuras Críticas las actualizaciones derivadas de cambios de operadores en la provisión de servicios esenciales básicos, que activarán las correspondientes notificaciones de alta o baja como operadores con incidencia en la Defensa Nacional tanto a los propios operadores como a sus equipos de respuesta a incidentes de seguridad de referencia.

c) Recabar de las autoridades competentes un informe anual sobre el tipo y número de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea.

d) Elaborar un informe anual resumido sobre las notificaciones recibidas para remitir al grupo de cooperación antes del 15 de febrero de cada año y, posteriormente, a las autoridades competentes y a los equipos de respuesta a incidentes de seguridad de referencia, para su conocimiento.

5. ¿Cuál de las siguientes no es una medida de la Estrategia Nacional de Ciberseguridad 2019?

a) Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público

b) Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible

c) Desarrollar el Centro de Operaciones de Ciberseguridad de la AGE que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local

d) Modificar el Esquema Nacional de Seguridad para incluir medidas relacionadas con la defensa del ciberespacio en el ámbito del Sector Público

6. En relación con la ciberseguridad, los pasos de una estrategia proactiva para evitar ataques antes de que ocurran son:

a) Determinar el daño que se puede producir, descubrir los puntos débiles y reducir las vulnerabilidades.

b) Evaluación de los daños producidos, determinación de la causa y reparación del daño.

c) Los definidos en el plan de contingencia aprobado.

d) No se pueden definir los pasos porque no es posible evitar ataques antes de que ocurran.

7. El Centro de Seguridad en Internet para menores de edad en España es:

a) IS4K

b) Better Internet for Kids

c) CyberCamp

d) OSI

8. El Consejo Nacional de Ciberseguridad lo preside:

a) El Director del Departamento de Seguridad Nacional.

b) La Ministra de Defensa.

c) El Secretario de Estado de Seguridad.

d) El Secretario de Estado director del Centro Nacional de Inteligencia y director del Centro Criptológico Nacional.

9. ¿En qué año se aprobó la actual Estrategía de Seguridad Nacional?

a) 2017

b) 2015

c) 2021

d) 2019

10. Seleccione la orden que aprueba la Estrategia Nacional de Ciberseguridad 2019:

a) Orden PCI/487/2019

b) Orden PCI/487/2020

c) Orden PRA/1267/2019

d) Orden PRA/1267/2020

11. ¿Cuál es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales?

a) El Centro Criptológico Nacional (CCN)

b) El Centro Nacional para la Protección de Infraestructuras Críticas (CNPI

c) El INCIBE

d) La Secretaría de Estado de Seguridad

12. Según la arquitectura orgánica de la ciberseguridad que establece la Estrategia Nacional de Ciberseguridad 2019, ¿qué órgano asume la tarea de desarrollar el Plan Nacional de Ciberseguridad?

a) Consejo Nacional de Ciberseguridad

b) Comisión Permanente de Ciberseguridad

c) Foro Nacional de Ciberseguridad

d) Consejo de Seguridad Nacional

13. La plataforma de desafíos de ciberseguridad del CCN-CERT, en la que cualquier persona puede demostrar su conocimiento y destreza ante diferentes desafíos en la materia (criptografía, esteganografía, exploiting, forense, networking y reversing, entre otros), se denomina:

a) Ana.

b) Atenea.

c) CCNDroid.

d) Marta.

14. Según la Estrategia Nacional de Ciberseguridad 2019, ¿cuál de los siguientes principios no es un principio rector?

a) Unidad de acción

b) Eficacia

c) Anticipación

d) Resiliencia

15. ¿Cuántas líneas de acción tiene la Estrategia Nacional de Ciberseguridad 2019?

a) 5

b) 6

c) 7

d) 8

16. Según la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, ¿cuál de los siguientes principios no es un principio rector?

a) Eficacia.

b) Resiliencia.

c) Unidad de acción.

d) Anticipación.

17. Según la arquitectura orgánica de la ciberseguridad que establece la Estrategia Nacional de Ciberseguridad 2019, ¿qué órgano se crea como un elemento novedoso de colaboración público-privada?

a) Consejo Nacional de Ciberseguridad

b) Comisión Permanente de Ciberseguridad

c) Foro Nacional de Ciberseguridad

d) Consejo de Seguridad Nacional

18. ¿Cómo se denomina a la red neuronal diseñada para mejorar las capacidades de vigilancia y reducir la superficie de exposición de los sistemas frente a las amenazas del ciberespacio en tiempo real?

a) ANA

b) ANGELES

c) ADA

d) ESE

19. En el ámbito de las amenazas de seguridad, es CIERTO:

a) Una amenaza persistente avanzada (APT), no deja rastro en los sistemas una vez ha obtenido lo que buscaba, al guardarse en memoria RAM.

b) El eslabón más débil de un sistema de seguridad son los cortafuegos.

c) CARMEN es la herramienta del CCN-CERT para identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT).

d) Mantener los sistemas actualizados no ayuda a protegerse contra amenazas persistentes avanzadas (APT).

20. La relación completa de objetivos de una investigación forense en tecnologías de la información, tras un ataque o agresión es:

a) Reconocimiento de los métodos o los puntos débiles que posibilitaron la agresión. Determinación de los daños ocasionados. Identificación del autor. Aseguramiento de las evidencias.

b) Reconocimiento de los métodos o los puntos débiles que posibilitaron la agresión. Determinación de los daños ocasionados. Identificación del Autor. Denuncia ante la autoridad.

c) Reconocimiento de los métodos o los puntos débiles que posibilitaron la agresión. Determinación de los daños ocasionados. Aseguramiento de las evidencias. Registro y archivado de la incidencia.

d) Reconocimiento de los métodos o los puntos débiles que posibilitaron la agresión. Determinación de los daños ocasionados. Identificación del autor. Aseguramiento de las evidencias. Presentación de denuncia ante la autoridad competente.

21. Según el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, ¿cuál de las siguientes NO es una de las funciones que desempeñarán, como mínimo los CSIRT?

a) Supervisar incidentes a escala internacional

b) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados

c) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación

d) Responder a incidentes

22. En las pruebas de seguridad de la infraestructura WIFI se detectó un punto de acceso inalámbrico instalado sin la autorización explícita del administrador de red, se estaba investigando si lo había agregado un empleado con buenas intenciones o un atacante malintencionado. ¿Cómo se llama a este tipo de amenaza?

a) Rogue AP

b) SandBox AP

c) Hunter AP

d) Captive AP

23. En ciberseguridad, ¿a qué nos referimos con movimiento lateral?

a) Son las técnicas que emplea un intruso que ha roto el perímetro de seguridad de una organización para profundizar en su red en busca de activos valiosos.

b) Es el acto de explotar una vulnerabilidad para obtener acceso a elementos reservados a usuarios que tengan privilegios elevados.

c) Es un tipo de ataque de ingeniería social basado en explotar vulnerabilidades de personas del círculo del objetivo principal para suplantarlas.

d) Se refiere a la replicación de un virus informático desde un equipo infectado a otros equipos de la misma organización.

24. ¿Cómo se da cumplimiento en España a la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, comúnmente conocida como Directiva NIS 1?:

a) No es una directiva, sino un reglamento comunitario, directamente aplicable en todos los Estados Miembros que por tanto no necesita ningún tipo de transposición.

b) Se transpone al ordenamiento jurídico en España a través del Real Decreto Ley 12/2018 de seguridad de las redes y los sistemas de información.

c) En España todavía no se ha finalizado el proceso de transposición de esta directiva NIS 1.

d) No es necesario dar cumplimiento a esta Directiva puesto que la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, comúnmente conocida como Directiva NIS 2, deroga la Directiva 2016/1148 a partir del 01.01.2023.

25. La herramienta proporcionada por el CCN-CERT para analizar las características de seguridad técnicas definidas a través del Esquema Nacional de Seguridad en el ámbito de la Administradón Electrónica se denomina:

a) INES
b) LUCIA
c) CLARA
d) CARMEN

26. Según la arquitectura orgánica de la ciberseguridad que establece la Estrategia Nacional de Ciberseguridad 2019, ¿qué órgano apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales?

a) Consejo Nacional de Ciberseguridad
b) Comisión Permanente de Ciberseguridad
c) Comité de Situación
d) Consejo de Seguridad Nacional

27. La Directiva 2016/1148/UE:

a) Se conoce como Directiva NIST.
b) Ha sido traspuesta mediante Real Decreto en 2018.
c) Prevé el establecimiento de medidas de seguridad en determinados operadores de la Unión Europea.
d) Ha modificado la Ley 8/2011, de protección de infraestructuras críticas.

28. En España, los CSIRT de referencia:

a) Atienden las notificaciones de incidencias de seguridad de todos los ámbitos de forma indistinta.
b) Funcionan de manera totalmente independiente.
c) Se integran en una red europea con ENISA al frente.
d) Son dos, el CCN-CERT e INCIBE-CERT.

29. La herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit se denomina:

a) PILAR
b) LUCIA
c) JUANA
d) MARIA ANTONIA

30. ¿Cuál de las siguientes respuestas NO es una fase de la gestión de ciberincidentes?

a) Verificación de la Política de Seguridad
b) Contención, mitigación y recuperación
c) Detección, análisis e identificación
d) Actividad post-ciberincidente

31. El cert nacional competente para la respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado es

a) INCIBE-CERT
b) CERT-CCN
c) OSI
d) CNI

32. ¿Cuál de los siguientes fines se recoge dentro del apartado "OBJETIVO GENERAL" de la Estrategia Nacional de Ciberseguridad 2019?:

a) Garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

b) Protección del ecosistema empresarial y social de los ciudadanos.

c) Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

d) Garantizar la conectividad universal y facilitar el libre flujo de información, servicios e ideas.

33. Según la arquitectura orgánica de la ciberseguridad que establece la Estrategia Nacional de Ciberseguridad 2019, ¿qué órgano asiste al presidente en la dirección de la política de Seguridad Nacional?

a) Consejo Nacional de Ciberseguridad

b) Comisión Permanente de Ciberseguridad

c) Foro Nacional de Ciberseguridad

d) Consejo de Seguridad Nacional

34. En relación a los equipos de respuesta a incidentes de seguridad informática (CSIRT), en lo relativo a las relaciones con los operadores de servicios esenciales, ¿en qué casos es necesario que los operadores reporten los incidentes al CCN-CERT?:

a) Cuando el operador es una entidad del ámbito subjetivo de aplicación de la ley 40/2015.

b) Cuando el operador es una entidad no incluida en el ámbito subjetivo de aplicación de la ley 40/2015.

c) En todos los casos, independientemente de la naturaleza del operador.

d) En todos los casos, independientemente de la naturaleza del proveedor, siempre que no sea necesario reportar al ESPDEF-CERT.

35. ¿Cuál de los siguientes es el objetivo general de la Estrategia Nacional de Ciberseguridad 2019?

a) Garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico

b) Protección del ecosistema empresarial y social y de los ciudadanos

c) Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

d) Garantizar la conectividad universal y facilita el libre flujo de información, servicios e ideas

36. Indique cómo se denomina el servicio desarrollado por el Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna de los organismos adscritos al servicio e Internet:

a) SAT RADAR

b) SAT INET

c) SDT RADAR

d) SDT INET

37. La Estrategia Nacional de Ciberseguridad 2019 se sustenta y se inspira en los principios rectores de la Seguridad Nacional. Entre ellos NO se encuentra la:

a) Unidad de acción.

b) Anticipación.

c) Eficacia.

d) Resiliencia.

38. ¿Qué elemento novedoso de colaboración público-privada se crea en la Estrategia Nacional de Ciberseguridad 2019?

a) Foro Nacional de Ciberseguridad

b) Comisión Permanente de Ciberseguridad

c) Centro de operaciones de ciberseguridad

d) Ninguno de los anteriores

39. ¿A quién corresponde el soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las Administraciones de las Comunidades Autónomas?

a) Al CCN-CERT

b) Al INCIBE-CERT

c) Al ESPDEF-CERT del Ministerio de Defensa

d) A la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

40. En la Estrategia Nacional de Ciberseguridad 2019, entre las medidas incluidas en la Línea de Acción 7: Desarrollar una cultura de ciberseguridad, NO se incluye:

a) Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.

b) Impulsar un sistema en favor de una información veraz y de calidad y que permita bloquear las noticias falsas y la desinformación.

c) Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.

d) Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

41. Según el Centro Nacional de Inteligencia, existen 4 tipos de autoridad que un CERT puede tener sobre su Comunidad:

a) autoridad completa, autoridad compartida, autoridad nula, autoridad indirecta.

b) autoridad total, autoridad parcial, autoridad nula, autoridad indirecta.

c) autoridad completa, autoridad compartida, autoridad directa, autoridad indirecta.

d) autoridad completa, autoridad parcial, autoridad nula, autoridad indirecta.

42. La herramienta desarrollada por el Centro Criptológico Nacional que permite a las Administraciones Públicas realizar el análisis y la gestión de riesgos, así como el análisis del impacto y la continuidad de operaciones para las Administraciones Públicas se denomina:

a) MAGERIT.

b) PILAR.

c) ANGELES.

d) LUCIA.

43. ¿A qué hace referencia las siglas SOC?

a) Security Operations Center

b) System Operations Center

c) System Operations Chief

d) System Operations Certificate

44. Según la Estrategia Nacional de Ciberseguridad 2019, ¿con qué frecuencia debe elaborarse un Informe de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos?

a) Cada seis meses

b) Anual

c) Cada dos años

d) No establece la frecuencia

45. Diga qué respuesta es CORRECTA, sobre la ciberseguridad:

a) La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, no incluye la ciberseguridad entre sus prioridades.

b) La última Estrategia de Ciberseguridad Nacional se aprobó el 28 de diciembre de 2021.

c) La Ley 36/2015 recoge la obligación de disponer de una Estrategia de Ciberseguridad Nacional.

d) La Estrategia Nacional de Ciberseguridad 2019 desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad.

46. La Estrategia Nacional de Ciberseguridad 2019:

a) Desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2015 en el ámbito de la ciberseguridad.

b) Desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2016 en el ámbito de la ciberseguridad.

c) Desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad.

d) Desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2018 en el ámbito de la ciberseguridad.