Test Tema 48 #1

Actualizado el 13/04/2025

1. Según el Esquema Nacional de Seguridad, las Instrucciones Técnicas de Seguridad:

a) Son aspectos que pueden ser aplicados por parte de las Administraciones públicas.

b) Son aspectos que obligatoriamente deben ser aplicados por parte de las Administraciones Públicas.

c) Algunas Instrucciones de Seguridad son de aplicación preceptiva y otras de aplicación facultativa.

d) Ninguna de las anteriores.

2. Las medidas de seguridad que contempla el ENS se dividen en tres grupos. Medidas destinadas a proteger la operación del sistema, medidas para la protección de activos concretos y:

a) Medidas organizativas.

b) Medidas preventivas.

c) Medidas paliativas.

d) Medidas sancionadoras.

3. ¿Cuál de las siguientes NO es una dimensión de la seguridad en el Esquema Nacional de Seguridad?

a) Disponibilidad

b) Trazabilidad

c) Integridad

d) Escalabilidad

4. Señale cuál de las siguientes NO es una guía CCN-STIC:

a) CCN-STIC-804 - Medidas de implantación del Esquema Nacional de Seguridad.

b) CCN-STIC-820 - Protección Contra Denegación de Servicio.

c) CCN-STIC-823 - Seguridad en entornos Cloud.

d) CCN-STIC-830 - Medidas de seguridad en el puesto de trabajo (entorno ofimático).

5. ¿Qué serie CCN-STIC constituye un conjunto de normas desarrolladas para entornos basados en el sistema operativo Windows de Microsoft?

a) 500

b) 600

c) 700

d) 400

6. El soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las Administraciones de las Comunidades Autónomas corresponde a:

a) NCIBE-CERT

b) CCN-CERT

c) Al CERT correspondiente de la Comunidad Autónoma

d) Al CERT del Ministerio de Defensa

7. ¿Cuál de los siguientes no es un principio rector de la Estrategia de Ciberseguridad Nacional?

a) Unidad de acción

b) Resiliencia

c) Anticipación

d) Cooperación Internacional

8. Seleccione la opción correcta, de entre las siguientes, respecto al ámbito de aplicación del Esquema Nacional de Seguridad:

a) Es de aplicación única y exclusivamente al sector público.

b) Es de aplicación al sector público y, en determinadas circunstancias, también a sistemas de información del sector privado.

c) Es de aplicación al sector privado únicamente.

d) Es de igual aplicación tanto al sector público como al privado, en todos los casos y circunstancias.

9. ¿Cuál es la guía referente a Auditoría del Esquema Nacional de Seguridad?

a) CCN-STIC-801

b) CCN-STIC-802

c) CCN-STIC-803

d) CCN-STIC-804

10. La herramienta del CCN-CERT para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos es:

a) CARMEN.

b) ELENA.

c) IRIS.

d) GLORIA.

11. Indique cual de los siguientes NO es un principio básico en el ENS

a) Reevaluación periódica

b) Vigilancia continua

c) Seguridad como proceso integral

d) Prevención, reacción y recuperación

12. Según la guía CCN-STIC-827 Gestión y uso de dispositivos móviles:

a) La gestión de dispositivos móviles puede realizarse mediante el envío de mensajes SMS reconocibles por el software propietario de la marca instalado en el dispositivo o el Sistema Operativo.

b) La gestión de dispositivos móviles puede realizarse aplicando Mobile Device Management (MDM) con un producto de terceros.

c) Mobile Application Management (MAM) se dirige a gestionar una o varias aplicaciones específicas dentro de cada dispositivo móvil, en vez de gestionar la totalidad del dispositivo.

d) Todas las anteriores son correctas.

13. ¿Cuál es la herramienta de borrado seguro incluida en el catálogo de productos y servicios TIC, Guía CCN/STIC 105?:

a) Eraser DX.

b) Olvido Windows.

c) HDShredder.

d) Olivia.

14. Respecto a las declaraciones y certificaciones de conformidad con el ENS

a) La declaración de conformidad es de aplicación a los sistemas de categoría BÁSICA

b) La certificación de conformidad es obligatoria para los sistemas de categoría MEDIA y ALTA

c) El Distintivo de Certificación de Conformidad deberá estar firmado electrónicamente por la Entidad de Certificación responsable de la auditoría de certificación, y el Distintivo de Declaración de Conformidad estará firmado o sellado electrónicamente por la entidad responsable del sistema de información

d) Todas las anteriores son correctas.

15. Señale la respuesta INCORRECTA, el ámbito de aplicación del ENS incluye:

a) A las Universidades Públicas

b) Sólo a la Administración General del Estado, a las Administraciones de las Comunidades Autónomas y a las entidades de la Administración Local

c) A las entidades del sector privado cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades administrativas

d) A las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas

16. El trashing es una técnica que afecta a la dimensión de:

a) Disponibilidad

b) Confidencialidad

c) Trazabilidad

d) Integridad

17. En el Esquema Nacional de Seguridad, las dimensiones de seguridad se adscribirán a uno de los siguientes niveles:

a) Bajo, Medio o Alto

b) Limitado, Grave o Muy Grave

c) Básico, Medio o Alto

d) Básico, Medio, Alto o Muy Alto

18. El Esquema Nacional de Seguridad establece que las líneas de defensa han de estar constituidas por medidas de distinto tipo, ¿Cuál de las siguientes no es una de ellas?

a) Organizativa

b) Semántica

c) Lógica

d) Física

19. ¿Cuál de las siguientes guías del CCN-STIC trata la definición de roles y responsabilidades en la seguridad de la información?

a) 801

b) 835

c) 827

d) 806

20. ¿Cuál de los siguientes principios básicos no aparece en el Esquema Nacional de Seguridad, Real Decreto 311/2022 del 3 de mayo?

a) Diferenciación de responsabilidades

b) Gestión de la seguridad basada en los riesgos

c) Función diferenciada

d) Reevaluación periódica

21. El Esquema Nacional de Seguridad, Real Decreto 311/2022, de 3 de mayo, en su artículo 31, indica que los sistemas de información de nivel medio serán objeto de una auditoría regular ordinaria que verifique el cumplimiento de los requerimientos en él definidos. ¿Cuál es la periodicidad obligatoria para la realización de la misma?

a) Al menos cada año.

b) Al menos cada dos años.

c) Cuando se produzcan modificaciones en el sistema de información.

d) Ninguna de las anteriores.

22. Una solución del CCN-CERT para realizar tareas de sobreescritura y borrado seguro sobre los sistemas de archivos y discos es:

a) CAMELA

b) OLVIDO

c) CARLA

d) ANA

23. La herramienta PILAR sirve para:

a) Proporcionar una defensa preventiva frente a ataques de tipo ransomware mediante el despliegue de vacunas.

b) Realizar el análisis de riesgos según la metodología ISO 9001.

c) Realizar el análisis de coste/beneficio según la metodología APR.

d) Realizar el análisis de riesgos según la metodología Magerit e ISO/IEC 27005.

24. ¿Qué guía del CCN-STIC de seguridad versa acerca de la criptología de empleo en el ENS?

a) CCN-STIC 610

b) CCN-STIC 105

c) CCN-STIC 807

d) CCN-STIC 598

25. En el marco del CCN-CERT es FALSO:

a) Los servicios del CCN-CERT están dirigidos exclusivamente a la Administración General del Estado.

b) GLORIA es una plataforma del CCN-CERT para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos.

c) El CCN-CERT está adscrito al CNI (Centro Nacional de Inteligencia).

d) Se deben notificar al CCN-CERT todos aquellos incidentes que sean catalogados con un nivel de peligrosidad de Alto, Muy Alto y Crítico.

26. De acuerdo con el Esquema Nacional de Seguridad, el sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

d) Todas las anteriores.

27. Indique cuál de estas medidas de seguridad del Esquema Nacional de Seguridad corresponde al marco operacional:

a) Proceso de autorización.

b) Protección de las instalaciones e infraestructuras.

c) Protección de las aplicaciones informáticas.

d) Monitorización del sistema.

28. El Esquema Nacional de Seguridad lo aplica todo el Sector Público:

a) Asegurar el acceso, integridad, disponibilidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

b) garantizar la seguridad de los ciudadanos residentes en territorio nacional en el caso de agresión de una potencia extranjera, o de atentado terrorista.

c) garantizar la inviolabilidad de las comunicaciones electrónicas entre ciudadanos dentro del territorio nacional.

d) Proteger a los ciudadanos de posibles acosos por parte de los poderes del Estado.

29. ¿Cuál de las siguiente afirmaciones es cierta?:

a) Las dimensiones de seguridad en el Esquema Nacional de Seguridad son: disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad.

b) Las dimensiones de seguridad en el Esquema Nacional de Seguridad son: disponibilidad, integridad, confidencialidad, portabilidad y autenticidad.

c) Las dimensiones de seguridad en el Esquema Nacional de Seguridad son: disponibilidad, eficiencia, confidencialidad, trazabilidad y autenticidad.

d) Las dimensiones de seguridad en el Esquema Nacional de Seguridad son: disponibilidad, integridad, confidencialidad, trazabilidad y no repudio.

30. ¿Cuál de estas afirmaciones NO corresponde al CCN-CERT?

a) El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional.

b) Los servicios del CCN-CERT están dirigidos exclusivamente a la Administración General del Estado.

c) CARMEN, LUCIA e INÉS son herramientas desarrolladas por CCN-CERT.

d) Las funciones del CCN-CERT quedan recogidas en el RD 311/2022, de 3 de mayo, regulador del Esquema Nacional de Seguridad.

31. El Real Decreto 311/2022, en su disposición adicional segunda, dispone que las guías de seguridad de las tecnologías de la información y las comunicaciones para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad las elaborará y difundirá:

a) El Centro Criptológico Nacional.

b) La Agencia Española de Protección de Datos.

c) Cada organismo público que implante medidas de seguridad de acuerdo con el Esquema Nacional de Seguridad.

d) El Consejo Superior de Administración Electrónica.

32. Señale la sentencia correcta, en relación al principio de mínimo privilegio definido en el Esquema Nacional de Seguridad:

a) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue.

b) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

c) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

d) Todas las anteriores.

33. Según el Anexo A de la Guía de Seguridad de las TIC CCN-STIC 802, ¿cuál de los siguientes NO es un requisito que deba probar el Auditor Jefe?:

a) Acreditación de formación y experiencia en auditoría de cuentas

b) Conocimientos de seguridad y gestión de riesgos de seguridad.

c) Conocimiento de los requisitos del Esquema Nacional de Seguridad

d) Conocimientos de otra legislación aplicable cuando la auditoría incluya además otros requisitos o esquemas de seguridad

34. ¿Hay incidentes de obligada notificación al CCN-CERT?

a) Sí. Las Administraciones Públicas deben notificar al CCN-CERT todos aquellos incidentes que sean catalogados con un nivel de peligrosidad de Crítico

b) Sí. Las Administraciones Públicas deben notificar al CCN-CERT todos aquellos incidentes del tipo DoS, APT y Phishing

c) No

d) Sí. Las Administraciones Públicas deben notificar al CCN-CERT todos aquellos incidentes que sean catalogados con un nivel de peligrosidad de Alto, Muy Alto o Crítico

35. Indica cuál de las siguientes NO es una "dimensión de la seguridad" a tener en cuenta para establecer la categoría del sistema, según lo especificado en el Anexo I del Esquema Nacional de Seguridad (Real Decreto 311/2022):

a) Disponibilidad (D).

b) Trazabilidad (T).

c) Autenticidad (A).

d) Conservación (C).

36. Según el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, la política de seguridad de la información debe aplicar como requisito mínimo:

a) Líneas de defensa.

b) Mínimo privilegio

c) Seguridad integral.

d) Responsabilidad diferenciada

37. Respecto a los Mecanismos de Autenticación en los sistemas de categoría MEDIA:

a) Es obligatorio el doble factor de autenticación en cualquier caso

b) Es obligatorio el doble factor de autenticación para los usuarios de la organización

c) Para los usuarios de la organización, se admite un único factor de autenticación basado en contraseña cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas

d) Se admite un único factor de autenticación en cualquier caso

38. De acuerdo al Esquema Nacional de Seguridad, ¿cuál de las siguientes afirmaciones es CIERTA?:

a) La integridad es la propiedad o característica consistente en que el activo de información ha sido alterado de manera no autorizada.

b) La integridad es la propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

c) La integridad es la propiedad o característica consistente en que la degradación que sufre el activo no supera el riesgo asumible.

d) La integridad es la propiedad o característica consistente en que el activo de información no puede ser accesible por terceros sin autorización.

39. ¿Cuál es la guía referente al Plan de Adecuación del Esquema Nacional de Seguridad?

a) CCN-STIC-803

b) CCN-STIC-805

c) CCN-STIC-806

d) CCN-STIC-807

40. ¿Cuál de los siguientes no es un requisito mínimo de seguridad de los definidos en el Esquema Nacional de Seguridad?

a) Gestión de personal.

b) Integridad y actualización del sistema.

c) Prevención ante la continuidad de la actividad.

d) Incidentes de seguridad.

41. Según el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, señale la respuesta correcta respecto a la auditoría de seguridad:

a) Se realizará, al menos, cada dieciocho meses para los sistemas de todas las categorías, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

b) El equipo auditor, en el diseño de sus pruebas y revisiones, debe limitarse a la revisión de documentos facilitados por los responsables de la información, del servicio y de seguridad.

c) Cuando existan razones que lo justifiquen, dentro de las tareas de la auditoria de seguridad podrán incluirse además la ejecución de trabajos de consultoría.

d) El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados

42. Señale la respuesta FALSA. Según la Guía de Seguridad CCN-STIC-812 (Seguridad en entornos y aplicaciones web), entre las recomendaciones generales para un desarrollo seguro del software de aplicaciones web se encuentra:

a) De forma general, se recomienda el uso del método POST de HTTP sólo para la consulta de información, y el método GET para el intercambio y envío de información por parte de los clientes Web a la aplicación Web.

b) Las cabeceras HTTP pueden ser manipuladas fácilmente por un atacante y no deben emplearse como método de validación o de envío de información.

c) El almacenamiento de información sensible, tanto propia de la lógica de la aplicación como las credenciales de acceso, debe de almacenarse cifrada en todos los servidores, y especialmente en el de base de datos.

d) Todos los mecanismos de interacción entre los distintos componentes del entorno Web (servidor Web, de aplicación y base de datos) deben realizarse de forma segura.

43. El Esquema Nacional de Seguridad indica que un sistema de información será de categoría ALTA:

a) Si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Si todas sus dimensiones de seguridad alcanzan el nivel ALTO.

c) Si presta servicios a través de redes públicas de comunicación.

d) Si gestiona datos de carácter personal.

44. ¿Cómo se denomina la Comisión Delegada del Gobierno para la Seguridad Nacional que asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional?

a) El Consejo de Seguridad Nacional.

b) El Comité Especializado de Ciberseguridad.

c) El Comité Especializado de Situación.

d) El Consejo Ejecutivo de Ciberseguridad.

45. Según la Instrucción Técnica de Seguridad (ITS) de conformidad con el ENS, ¿se pueden certificar servicios?:

a) No, ya que la ITS especifica como su ámbito de aplicación, exclusivamente, los sistemas de información de las entidades del ámbito de aplicación del ENS, en cuanto tales sistemas desarrollen competencias estatutarias de la entidad pública de que se trate

b) Si, ya que ITS especifica como su ámbito de aplicación, tanto los sistemas de información como los servicios prestados por las entidades del ámbito de aplicación del ENS, en cuanto tales sistemas o servidcios desarrollen compentencias estatutarias de la entidad pública de que se trate

c) No, ya que se certifican entidades del ámbito de aplicación del ENS, no sistemas o servicios

d) Sí, siempre que se trate de servicios desarrollados por las entidades públicas en ejercicio de sus competencias estatutarias

46. ¿Cuál de los siguientes sistemas NO tiene la consideración de entorno inseguro para la información almacenada o en tránsito, de acuerdo con el Esquema Nacional de Seguridad?

a) Dispositivos portátiles o móviles

b) Comunicaciones sobre redes inalámbricas, incluso cuando la comunicación se realice con cifrado fuerte

c) Soportes de información y comunicaciones en redes abiertas

d) Dispositivos periféricos

47. La herramienta del CCN-CERT para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos es:

a) CARMEN

b) ELENA

c) IRIS

d) GLORIA

48. En el contexto del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, en las decisiones en materia de seguridad deberán tenerse en cuenta una serie de principios básicos. Indique cuáles son los principios básicos contemplados en el Esquema Nacional de Seguridad (ENS):

a) Seguridad integral, Gestión de riesgos, Prevención, detección, respuesta y conservación, Existencia de líneas de defensa, Vigilancia continua, Reevaluación periódica, Diferenciación de responsabilidades.

b) Análisis y gestión de los riesgos, Gestión de personal, Profesionalidad, Mínimo privilegio, Integridad y actualización del sistema, Continuidad de la actividad.

c) Mecanismos de control, Actualización permanente, Formación, Ciclo de vida de servicios y sistemas, Auditorías.

d) Ninguna de las respuestas anteriores es correcta.

49. Se ha designado un POC (Punto o Persona de Contacto) en el proveedor para la seguridad de la información tratada y el servicio prestado, y entre sus funciones se encuentra la de gestión de los incidentes de seguridad para el ámbito de dicho servicio. ¿A partir de qué nivel de impacto es obligatorio notificar al CCN-CERT un incidente de seguridad según la Guía CCN- STIC 817 y la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC?

a) Igual o superior a MUY ALTO

b) Igual o superior a ALTO

c) Igual o superior a MEDIO

d) Es obligatorio notificar todos los incidentes al CCN-CERT independientemente de su impacto o peligrosidad

50. Según el Esquema Nacional de Seguridad, ¿qué elementos debe identificar un Análisis de Riesgos Informal?

a) Activos, amenazas, salvaguardas y riesgos residuales

b) Vulnerabilidades e impacto

c) Impacto, riesgo calculado y riesgo intrínseco

d) -

51. Según se establece en el Esquema Nacional de Seguridad (ENS) señale cual NO es un principio básico en las decisiones en materia de seguridad:

a) Diferenciación de responsabilidades.

b) Enfoque de soluciones multilaterales.

c) Gestión de riesgos.

d) Líneas de defensa.

52. En relación con las categorías de los sistemas del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, es CORRECTO:

a) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO.

b) A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad: Autenticidad, Confidencialidad, Integridad y Disponibilidad.

c) Para determinar el nivel requerido de una dimensión de seguridad, si dicha dimensión no se ve afectada, no se adscribirá a ningún nivel.

d) Para determinar el nivel requerido de una dimensión de seguridad el nivel ALTO se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave.

53. Según el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, el análisis y gestión de riesgos es una parte esencial del proceso de seguridad, debiendo mantenerse permanentemente actualizado. Para ello, el propio ENS establece que se debe realizar un análisis de riesgos formal para los sistemas de:

a) Categoría básica

b) Categoría media

c) Categoría alta

d) Categoría media y alta

54. De acuerdo con la Guía de Seguridad para la auditoría del ENS, señale cuál es uno de los requisitos mínimos para los integrantes del equipo de auditoría:

a) En ningún caso los integrantes del equipo auditor, deben haber participado o detentado responsabilidades previas a la auditoría, al menos en los tres últimos años, en el sistema de información auditado

b) El Auditor Jefe debe probar conocimientos de seguridad y gestión de riesgos de seguridad (certificación y experiencia probada de al menos 4 años en estos elementos)

c) Todos los miembros del equipo auditor deben probar acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional o internacional.

d) Todos los miembros del equipo auditor deben probar conocimiento de los requisitos del RD 4/2010

55. En seguridad de la información, ¿a qué hace referencia el término “autenticidad”?

a) Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

b) La capacidad de demostrar la veracidad de una información.

c) Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

d) -

56. Las dimensiones de seguridad de la información pueden resumirse en:

a) Disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad

b) Integridad, autenticación, confidencialidad, precisión, portabilidad

c) Disponibilidad, confidencialidad, autenticación, portabilidad, integración

d) Autenticación, disponibilidad, integridad, escalabilidad, portabilidad

57. De acuerdo a lo dispuesto por el RD 311/2022 por el que se regula el Esquema Nacional de Seguridad, ¿cuál de los siguientes NO es un requisito mínimo a tener en cuenta a la hora de desarrollar la política de seguridad?:

a) Análisis y gestión de riesgos.

b) Gestión de personal.

c) Autorización y control de los accesos.

d) Definición de las dimensiones básicas de seguridad de la información.

58. Los sistemas de información bajo el ámbito del Esquema Nacional de Seguridad serán objeto de una auditoría regular ordinaria que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad. ¿Cada cuánto tiempo, al menos, se ha de realizar dicha auditoría?

a) Cada tres años

b) Cada dos años

c) Cada año para sistemas de categoría Media o Alta, y cada dos años para Básica

d) Cada año

59. ¿Cuántos anexos incluye el RD 311/2022 (ENS)?

a) Ninguno

b) 1

c) 2

d) 4

60. Indique la respuesta INCORRECTA en relación con la determinación de la conformidad dentro del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS):

a) Los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad.

b) Los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad y obligatoriamente cada dos años una auditoría de certificación.

c) Los sujetos responsables de los sistemas de información que hayan superado el proceso de certificación o de autoevaluación anterior, darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la Instrucción Técnica de Seguridad de conformidad con el ENS.

d) -

61. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, se aplicarán las medidas de seguridad indicadas en el Anexo II, que se dividen en tres grupos. Indicar cuál de ellos NO es el correcto:

a) Marco estratégico [est]. Constituido por el conjunto de medidas relacionadas con la misión, visión, posicionamiento y estrategia de la organización.

b) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

c) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

d) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

62. El CCN publica Guías CCN-STIC de Seguridad agrupadas en series. ¿Qué serie se dedica al Esquema Nacional de Seguridad?

a) Serie CCN-STIC 200.

b) Serie CCN-STIC 400.

c) Serie CCN-STIC 800.

d) -

63. Indique cómo se denomina el documento que desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad:

a) Plan Nacional de Ciberseguridad 2019

b) Plan Nacional de Ciberseguridad 2021

c) Estrategia Nacional de Ciberseguridad 2019

d) Estrategia Nacional de Ciberseguridad 2021

64. El soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las Administraciones de las Comunidades Autónomas corresponde a:

a) INCIBE-CERT

b) CCN-CERT

c) Al CERT correspondiente de la Comunidad Autónoma

d) Al CERT del Ministerio de Defensa.

65. En el Real Decreto 311/2022, Esquema Nacional de Seguridad, se define como "la propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad" a la:

a) Confidencialidad.

b) Integridad.

c) Autenticidad.

d) Trazabilidad.

66. Si en un fichero aplicamos el algoritmo de resumen SHA1 destinado a detectar cualquier cambio no autorizado en la información contenida, ¿qué principio de seguridad informática estaremos aplicando?

a) Trazabilidad.

b) Confidencialidad.

c) Disponibilidad.

d) Integridad.

67. Atendiendo al Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, señale la opción correcta sobre la realización de auditorías de seguridad en los sistemas de información de categoría básica:

a) No necesitan realizar una auditoría.

b) Deben ser objeto de una auditoría al menos anualmente.

c) Deben ser objeto de una auditoría al menos cada dos años.

d) Deben ser objeto de auditoría cuando se produzcan modificaciones sustanciales en el sistema de información.

68. Las medidas de seguridad recogidas en el anexo II del Esquema Nacional de Seguridad serán proporcionales a:

a) El criterio del Responsable de la Información

b) Las dimensiones de seguridad relevantes en el sistema a proteger y la categoría del sistema de información a proteger

c) El resultado de la auditoría de seguridad

d) El análisis de vulnerabilidades realizado por el DPD

69. ¿Qué solución desarrollada por el CCN-CERT es un sistema de auditoría continua que tiene por objetivo incrementar la capacidad de vigilancia, reducir los tiempos en la gestión de la seguridad, mediante una gestión eficiente de la detección de vulnerabilidades y de la notificación de alertas, así como ofrecer recomendaciones para un tratamiento oportuno de las mismas?

a) MARIA

b) ANA

c) GLORIA

d) CARMEN

70. Según el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para determinar la conformidad con el Esquema Nacional de Seguridad se exige:

a) Superar una auditoría de conformidad o realizar una autoevaluación, en el caso de sistemas de categoría básica.

b) Superar una auditoría de conformidad en cualquier caso.

c) Preparar y aprobar la política de seguridad, categorizar los sistemas, implantar las medidas de seguridad y realizar un análisis de riesgos.

d) -

71. ¿Quién tiene la potestad para aprobar los niveles de seguridad de los servicios?

a) Responsable del Sistema

b) Responsable de la información

c) Responsable de seguridad

d) Responsable del Servicio

72. (reserva)Si implantamos herramientas de seguridad informática para proteger los sistemas de invasiones, intrusiones y accesos por parte de personas no autorizadas, estaremos aplicando el principio de:

a) Pitágoras.

b) Transparencia.

c) Resalencia.

d) Confidencialidad.

73. Según el Esquema Nacional de Seguridad, ¿qué elementos debe identificar un Análisis de Riesgos Informal?

a) Activos, amenazas, salvaguardas y riesgos residuales.

b) Vulnerabilidades e impacto.

c) Impacto, riesgo calculado y riesgo intrínseco.

d) -

74. Respecto al CCN-CERT, ¿qué respuesta es CORRECTA?:

a) Ofrece los servicios de sistemas de alerta temprana de la Red SARA y de Internet.

b) Tiene por misión resolver los incidentes de las entidades financieras de cualquier tamaño.

c) Es una entidad que depende del Ministerio de Defensa, en concreto del Mando Conjunto de Ciberdefensa.

d) La Oficina de Coordinación Cibernética depende del CCN-CERT.

75. ¿Cuál de los siguientes es un principio del Esquema Nacional de Seguridad?

a) Enfoque de soluciones de seguridad multilaterales

b) Carácter multidimensional de la seguridad

c) Reevaluación periódica

d) Todos los anteriores

76. ¿Cuál es el objetivo general de la Estrategia de Ciberseguridad Nacional?

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

b) La coordinación, por parte del Gobierno de España, de la ciberseguridad en el país.

c) Potenciar el uso seguro de las tecnologías de la información y, en particular, las que ofrecen un valor añadido a empresas y administraciones.

d) El establecimiento de un mando único en materia de ciberseguridad, que asuma la responsabilidad íntegra en dicha materia.

77. Respecto a la notificación de incidentes de ciberseguridad, señale la INCORRECTA

a) El CCN ejerce la coordinación nacional de la respuesta técnica de los CSIRT en materia de seguridad de las redes y sistemas de información del sector público

b) Todas las entidades, del sector público o privado, deberán notificar al CCN aquellos incidentes que tenga un impacto significativo

c) Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior

d) Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán los incidentes de seguridad al INCIBE-CERT

78. Según el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ¿a quién corresponde articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información?

a) A la Agencia Española de Protección de Datos.

b) Al Centro Criptológico Nacional.

c) Al Consejo Nacional de Seguridad lnformática.

d) Al Comité Sectorial de Administración Electrónica.

79. ¿Es de aplicación el Esquema Nacional de Seguridad a los sistemas que tratan información declarada como información clasificada de acuerdo con la Ley 9/1968 de Secretos Oficiales?

a) Sí, sin perjuicio de la aplicación de la Ley 9/1968 de Secretos Oficiales y otra normativa oficial, sin ser necesario adoptar medidas complementarias de seguridad

b) No, pues los sistemas que tratan información clasificada están excluídos del ámbito de aplicación del ENS

c) Sí, sin perjuicio de la aplicación de la Ley 9/1968 de Secretos Oficiales y otra normativa especial, pudiendo resultar necesario adoptar medidas complementarias de seguridad

d) Sí, pero solo para las materias clasificadas como difusión limitada

80. Según el Real Decreto 311/2022 sobre el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ¿qué organismo es el encargado de actuar ante cualquier agresión recibida en los sistemas de información de las entidades del sector público?

a) El CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team).

b) El GDT (Grupo de Delitos Telemáticos).

c) La BIT (Brigada de Investigación Tecnológica).

d) El CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones).

81. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad establece los requisitos mínimos que debe contener la Política de Seguridad de una organización. Entre estos requisitos mínimos NO se encuentra:

a) Gestión del personal.

b) Máximo privilegio.

c) Adquisición de productos de seguridad y contratación de servicios de seguridad.

d) Incidentes de seguridad.

82. Uno de los requisitos mínimos del ENS es el mínimo privilegio, según el cual...

a) las actuaciones en materia de seguridad deben basarse en el análisis de los defectos del sistema.

b) las actuaciones en materia de seguridad deben ser de naturaleza reactiva, de modo que los incidentes descubran las vulnerabilidades.

c) las consideraciones relativas a la seguridad deben retrasarse hasta las últimas fases del desarrollo del sistema para que su análisis sea lo más próximo posible a la realidad y se puedan minimizar los defectos.

d) se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

83. Indique cuál de los siguientes es un principio básico del Esquema Nacional de Seguridad:

a) Proporcionalidad.

b) Respeto al derecho de protección de datos de carácter personal.

c) Derecho a la garantía de seguridad y confidencialidad.

d) Gestión de la seguridad basada en los riesgos.

84. Según el Real Decreto 311/2022, para determinar la conformidad con el Esquema Nacional de Seguridad se exige:

a) Superar una auditoría de conformidad, o realizar una autoevaluación, en el caso de sistemas de categoría básica.

b) Superar una auditoría de conformidad, en cualquier caso.

c) Preparar y aprobar la política de seguridad, categorizar los sistemas e implantar las medidas de seguridad.

d) Preparar y aprobar la política de seguridad, categorizar los sistemas, implantar las medidas de seguridad y realizar un análisis de riesgos.

85. En relación a lo dispuesto en el Esquema Nacional de Seguridad, un sistema de información será de categoría MEDIA cuando:

a) Las dimensiones de seguridad definidas como críticas son, en su mayoría, de nivel MEDIO.

b) Alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna es de nivel inferior.

c) Alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

d) Las dimensiones de seguridad son, en su mayoría, de nivel MEDIO.

86. Uno de los requisitos mínimos del Esquema Nacional de Seguridad es el de la seguridad por defecto, según el cual …

a) las actuaciones en materia de seguridad deben basarse en el análisis de los defectos del sistema

b) las actuaciones en materia de seguridad deben ser de naturaleza reactiva, de modo que los incidentes descubran las vulnerabilidades

c) las consideraciones relativas a la seguridad deben retrasarse hasta las últimas fases del desarrollo del sistema para que su análisis sea lo más próximo posible a la realidad y se puedan minimizar los defectos

d) el uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario

87. ¿En qué caso sería suficiente una autoevaluación como auditoría al sistema de información según el RD 311/2022?

a) La autoevaluación no está prevista en el RD 311/2022

b) En sistemas de información de categoría básica

c) En sistemas de información de categoría básica o media

d) Cuando así lo decida el responsable de seguridad competente

88. En un Plan de Adecuación al ENS, ¿qué tarea se realiza habitualmente después de la Declaración de Aplicabilidad provisional y antes de la Declaración de Aplicabilidad Definitiva?

a) Identificar activos

b) Realizar un análisis de riesgos

c) Valorar/Categorizar el sistema

d) -

89. ¿Cuál es la norma principal de la serie ISO que contiene los requisitos del Sistema de Gestión de Seguridad de la Información?

a) No existe una norma ISO, pero el ENS define con detalle todos los conceptos necesarios.

b) ISO 9004:2018.

c) ISO 14001:2015.

d) ISO 27001:2022.

90. Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito del RD 311/2022 contemplarán los requisitos necesarios para asegurar la conformidad con el ENS:

a) De los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS

b) De los contratistas, tales como las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS

c) Sólo en el caso de que se admita la subcontratación a terceros

d) El RD 311/2022 no aplica a los sistemas de información del sector privado

91. Según el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren se denomina:

a) Autenticidad

b) Confidencialidad

c) Disponibilidad

d) Trazabilidad

92. El artículo 13 del ENS (Esquema Nacional de Seguridad) establece que el responsable de seguridad:

a) Determinará los requisitos de la información tratada.

b) Detallará las atribuciones de cada responsable y los mecanismos de coordinación, seguridad y resolución de conflictos.

c) Determinará los requisitos de los servicios prestados.

d) Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

93. Indique cuál de los siguientes términos NO corresponde a una de las dimensiones de la seguridad definidas en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

a) Resiliencia

b) Trazabilidad

c) Disponibilidad

d) Confidencialidad

94. ¿Cuál de los siguientes no se incluye en la Estructura Orgánica definida en la Estrategia de Ciberseguridad Nacional?

a) El Consejo de Seguridad Nacional.

b) El Consejo Nacional de Ciberseguridad.

c) El Foro Nacional de Ciberseguridad.

d) El Consejo Ejecutivo de Ciberseguridad.

95. Las dimensiones de la seguridad que contempla el Esquema Nacional de Seguridad son Disponibilidad, Autenticidad, Integridad, Confidencialidad y una opción de entre las siguientes:

a) Interoperabilidad.

b) Transparencia.

c) Legitimidad.

d) Trazabilidad.

96. Norma ISO relacionada con el sistema de gestión de la seguridad de la información:

a) ISO/IEC 19770.

b) ISO 9000.

c) ISO/IEC 27001.

d) ISO 38500.

97. De entre las siguientes opciones, indique la que corresponda con la aplicación a través de la cual se puede realizar el reporte de incidentes al centro CCN-CERT:

a) LORETO.

b) LUCIA.

c) INES.

d) PILAR.

98. Cuando se utilicen servicios en la nube suministrados por terceros:

a) Deberán ser autorizados por la Secretaría General de Administración Digital en cualquier caso

b) Deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información

c) Sólo es posible usar servicios en la nube bajo la modalidad SaaS

d) No es necesario que cumplan con las medidas de seguridad definidas en las guías CCN-STIC

99. ¿Cuál de los siguientes aspectos NO está recogido como una Instrucción Técnica de Seguridad según el Esquema Nacional de Seguridad?

a) Informe de Estado de Seguridad

b) Auditoría de Seguridad

c) Notificación de Incidentes de Seguridad

d) Protocolo de Comunicaciones Seguras

100. Según la guía CCN-STIC-803, Valoración de los sistemas, un RTO mayor de 5 días ¿con qué nivel se corresponde?

a) Bajo

b) Medio

c) Alto

d) No Aplicable.

101. De acuerdo al ENS, ¿cuál de las siguientes medidas de protección debe aplicarse en un CPD que preste servicio a un sistema con Disponibilidad de nivel Bajo?

a) Protección frente a inundaciones

b) Análisis de impacto

c) Protección frente a la denegación de servicio

d) Protección frente a incendios

102. 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

103. Señale cuál de los siguientes NO es un principio básico del Esquema Nacional de Seguridad (ENS):

a) Diferenciación de responsabilidades.

b) Prevención, detección, respuesta y conservación.

c) Líneas de defensa.

d) Continuidad de la actividad.

104. ¿Qué Real Decreto define el Esquema Nacional de Seguridad?

a) RD 4/2010

b) RD 3/2022

c) RD 4/2009

d) RD 311/2022

105. Las dimensiones de la seguridad que contempla el Esquema Nacional de Seguridad son Disponibilidad, Autenticidad, Integridad, Confidencialidad y:

a) Interoperabilidad.

b) Transparencia.

c) Trazabilidad.

d) Legitimidad.

106. ¿Cuál de los siguientes NO es un requisito mínimo de seguridad según el artículo 12 del Esquema Nacional de Seguridad?

a) Líneas de defensa.

b) Profesionalidad.

c) Análisis y Gestión de Riesgos.

d) Mínimo privilegio

107. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en el apartado 6 del artículo 12 sobre la política de seguridad y requisitos mínimos de seguridad, recoge que: "La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos". Indique de la siguiente lista, cual NO corresponde a un requisito mínimo de los detallados en el Real Decreto:

a) Mínimo privilegio.

b) Mejora continua del proceso de seguridad.

c) Optimizar los datos de acceso permitiendo compartirlos entre un mismo grupo de usuarios.

d) -

108. Según se establece en el Real Decreto 311/2022, ¿qué órgano recogerá la información que permita elaborar un perfil general del estado de la seguridad en las Administraciones Públicas?

a) El Centro Criptológico Nacional.

b) El Consejo Superior de Administración Electrónica.

c) El Comité Sectorial de Administración Electrónica.

d) La Comisión Interministerial de Administración Electrónica.

109. Según el Centro Criptológico Nacional (CCN), el análisis de riesgos es fundamental en la gestión de incidentes de seguridad, puesto que sus resultados se emplearán para la implantación de medidas de seguridad, lo que corresponde a la fase de:

a) Preparación.

b) Detección, análisis, identificación.

c) Contención, mitigación, recuperación.

d) Post-incidente.

110. ¿En qué año se publicó la última Estrategia de Ciberseguridad Nacional?

a) 2013

b) 2015

c) 2017

d) 2019

111. De acuerdo con lo establecido en el Esquema Nacional de Seguridad, en su Anexo I, las dimensiones de la seguridad son las siguientes:

a) Disponibilidad, autenticidad, integridad y confidencialidad.

b) Disponibilidad, autenticidad, integridad, confidencialidad y no repudio.

c) Disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

d) -

112. Uno de los requisitos mínimos del Esquema Nacional de Seguridad (ENS) es el "mínimo privilegio", según el cual:

a) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

b) Las actuaciones en materia de seguridad deben basarse en el análisis de los defectos del sistema.

c) Las actuaciones en materia de seguridad deben ser de naturaleza reactiva, de modo que los incidentes descubran las vulnerabilidades.

d) Las consideraciones relativas a la seguridad deben retrasarse hasta las últimas fases del desarrollo del sistema para que su análisis sea lo más próximo posible a la realidad y se puedan minimizar los defectos.

113. El art. 32.1 ENS, habla de un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2. La elaboración de dicho perfil es competencia de:

a) Comité Sectorial de Administración Electrónica

b) Centro Criptológico Nacional

c) INCIBE

d) Consejo de Ministros

114. 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

115. Indique la opción INCORRECTA en relación con el Esquema Nacional de Seguridad (ENS):

a) Los sistemas de información a los que se refiere el ENS serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos expuestos en el ENS.

b) Gestión de riesgos, diferenciación de responsabilidades y reevaluación periódica son 3 de los principios básicos que deberán tenerse en cuenta en las decisiones en materia de seguridad.

c) El INCIBE, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de la seguridad de las tecnologías de la información y las comunicaciones.

d) Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS

116. Para adquirir productos para sistemas de categoría MEDIA o ALTA:

a) Se utilizará el Catálogo de Productos y Servicios de Seguridad de las TIC (CPSTIC)

b) Si no existen productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo al artículo 19 del ENS.

c) Si no existen productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, es posible recurrir a productos o servicios certificados conforme a los Common Criteria u otra certificación reconocida internacionalmente

d) Todas son correctas

117. ¿Cuál de las siguientes medidas de seguridad NO pertenece al grupo Medidas de protección [mp] según el RD 311/2022 (Esquema Nacional de Seguridad)?

a) Detección de intrusión.

b) Formación.

c) Desarrollo de aplicaciones

d) Energía eléctrica.

118. Según el Esquema Nacional de Seguridad, la medida de seguridad op.exp.8 Registro de la actividad aplica en la categoría...

a) Solo en la categoría del sistema alta

b) Esta medida de seguridad aplica cuando así lo decida el responsable de los servidores

c) Baja, media y alta de la dimensión trazabilidad

d) En todos los casos anteriores

119. ¿Cuál de las siguientes medidas se debe aplicar en un sistema de información de categoría alta según el Esquema Nacional de Seguridad?

a) Previsión de la disponibilidad de medios alternativos para continuar prestando servicio cuando los medios habituales no estén disponibles

b) Asignar un identificador singular para cada entidad que accede al sistema

c) Cifrado de la información tanto durante su almacenamiento como durante su transmisión

d) Todas las anteriores

120. De acuerdo con la guía CCN-STIC 802, de auditoría de ENS, señale la respuesta correcta:

a) Los sistemas de categoría básica y media requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada dos años, o cuando se produzcan modificaciones sustanciales en el sistema

b) Los sistemas de categoría básica requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada año, o cuando se produzcan modificaciones sustanciales en el sistema

c) Los sistemas de categoría básica requerirán de una autoevaluación para su declaración de la conformidad que deberá ser realizada por personal diferente al que administra el sistema

d) Los sistemas de categoría básica se pueden someter a una auditoría formal de certificación de conformidad, siendo ésta la posibilidad siempre deseable

121. Tomando como referencia un contexto de uso de dispositivos móviles desplegados en un organismo público que puedan contener información corporativa o acceder a recursos corporativos o de otros organismos públicos, cuál de las siguientes medidas de securización del puesto cliente NO se corresponde con un nivel de seguridad alto según el Esquema Nacional de Seguridad:

a) Auto-bloqueo del dispositivo tras cierto tiempo de inactividad.

b) Auto-borrado en caso de varios intentos fallidos de autenticación del usuario.

c) Borrado seguro, en caso de reutilización del dispositivo.

d) Se permite la descarga sólo de aquellas aplicaciones previamente aceptadas por el organismo (de fuentes aceptadas).

122. De acuerdo con el Esquema Nacional de Seguridad, ¿cada cuánto tiempo es necesario realizar una auditoría ordinaria en los sistemas de información de la Administración Autonómica?

a) Todos los años

b) Al menos cada 2 años

c) Al menos cada 5 años

d) Solo es necesario realizar auditorías cuando se produzcan modificaciones sustanciales en los sistemas de información

123. ¿Cuál de los siguientes es un principio básico del Esquema Nacional de Seguridad?

a) Proporcionalidad

b) Respeto al derecho de protección de datos de carácter personal

c) Derecho a la garantía de seguridad y confidencialidad

d) Gestión de la seguridad basada en los riesgos

124. Según la guía CCN-STIC-827 Gestión y uso de dispositivos móviles, señale la INCORRECTA:

a) La autenticación del usuario se realizará con una contraseña/pin del dispositivo y/u otro tipo de autenticación antes de acceder a los recursos del organismo.

b) Los dispositivos deben bloquearse automáticamente después de un determinado periodo de inactividad.

c) El uso de un modelo BYOD (Bring Your Own Device) está intensamente desaconsejado.

d) Bajo la potestad del administrador de seguridad, podrá bloquearse de forma remota el dispositivo si se sospecha que ha podido ser dejado en un estado no seguro o en una ubicación no segura.

125. Si un servidor hardware dispone de 2 fuentes de alimentación redundantes conectadas a un SAI diferente cada una de ellas, ¿qué principio de seguridad informática estoy aplicando?

a) Ninguno, pues los principios de seguridad informática solo aplican al software y no al hardware.

b) Disponibilidad.

c) Trazabilidad.

d) Autenticidad.

126. La protección contra Denegación de servicio se recoge en la Guía CCN-STIC:

a) 828

b) 817

c) 820

d) 823

127. Según el Esquema Nacional de Seguridad, todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que debe desarrollarse aplicando una serie de requisitos mínimos. Indique cuál de los siguientes NO es uno de estos requisitos mínimos:

a) Almacenamiento encriptado de todos los datos.

b) Continuidad de la actividad.

c) Prevención ante otros sistemas de información interconectados.

d) Gestión de personal.

128. El Esquema Nacional de Seguridad establece que los sistemas comprendidos en el ámbito de aplicación han de ser objeto de una auditoría regular. ordinaria, al menos:

a) Cada 6 meses.

b) Cada año.

c) Cada 2 años.

d) El Esquema Nacional de Seguridad no especifica nada respecto a los plazos de realización de auditorías.

129. ¿Cuál no es una línea de acción de la Estrategia de Ciberseguridad Nacional?

a) Establecimiento de un mando único en materia de ciberseguridad

b) Desarrollar una cultura de ciberseguridad

c) Impulsar la ciberseguridad de ciudadanos y empresas

d) Garantizar la seguridad y resiliencia de los activos estratégicos para España

130. En virtud de la Disposición Transitoria del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, dispondrán de:

a) Veinticuatro meses para alcanzar su plena adecuación al ENS, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2.

b) Veinticuatro meses para alcanzar su plena adecuación al ENS, a excepción de aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2.

c) Dieciocho meses para alcanzar su plena adecuación al ENS, a excepción de aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2.

d) Doce meses para alcanzar su plena adecuación al ENS, a excepción de aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2.