Test Tema 48 #2

Actualizado el 13/04/2025

1. 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

2. Señale qué herramienta del CCN-CERT permite el Intercambio de información de ciberamenazas:

a) LUCIA

b) CARMEN

c) ROCIO

d) REYES

3. El RD 311/2022 define la dimensión de Trazabilidad como la propiedad o característica consistente en que:

a) Una entidad es quien dice ser o bien garantiza la fuente de la que proceden los datos

b) Las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

c) Las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad

d) La información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados

4. El RD 311/2022 establece que en la organización prestataria de servicios externalizados deberá designar un Punto o Persona de Contacto (POC) para la seguridad de la información tratada y el servicio prestado que:

a) Debe contar con el apoyo de los órganos de dirección

b) Canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información

c) Será el propio Responsable de Seguridad de la organización contratada

d) Todas son correctas

5. Indique cual de los siguientes NO es un requisito mínimo que desarrollará la Política de Seguridad

a) Profesionalidad

b) Protección de las instalaciones

c) Seguridad por defecto

d) Mínimo privilegio

6. 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) -

7. Respecto a los Perfiles de Cumplimiento Específicos (PCE), señale la respuesta INCORRECTA:

a) Se podrán implementar en determinado tipo de entidades (entidades locales, universidades, etc) o sectores de actividad concretos (servicios en la nube, etc)

b) uCeENS es una metodología para la obtención de la Certificación de Conformidad en el ENS en base a un Perfil de Cumplimiento Específico (PCE)

c) Cualquier entidad del sector público podrá elaborar un Perfil de Cumplimiento Específico

d) El CCN validará y publicará los correspondientes perfiles de cumplimiento

8. La herramienta web del CCN que nos permite realizar auditorías de seguridad sobre configuraciones de equipos de comunicaciones es:

a) CLARA

b) INES

c) ROCIO

d) VANESA

9. Según la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el Responsable de Seguridad y Enlace:

a) Es designado por el Ministerio del Interior y los operadores críticos deben facilitar a este el acceso a sus infraestructuras.

b) Es designado por los operadores críticos y debe contar con la habilitación del Director de Seguridad.

c) Es una figura independiente tanto de los operadores críticos como del Ministerio de Interior y su designación se lleva a cabo a través de selección competitiva.

d) Es personal al servicio de la Administración General del Estado, salvo en los casos de País Vasco y Navarra donde será un funcionario de la administración autonómica de esas comunidades, si bien en todo caso deberá contar con la habilitación expresa del Director de Seguridad.

10. ¿Cuál de los siguientes principios no aparece como básico en el Esquema Nacional de Seguridad, Real Decreto 311/2022?

a) Seguridad integral

b) Análisis de riesgos

c) Reevaluación periódica

d) Función diferenciada

11. ¿Cuál de los siguientes NO es un objetivo de la Estrategia Nacional de Ciberseguridad?

a) Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.

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

c) Seguridad del ciberespacio en el ámbito internacional

d) Protección del derecho a la ciberintimidad de la ciudadanía

12. Respecto de el Plan de Continuidad, medida de seguridad recogida en el Anexo II del Esquema Nacional de Seguridad, indique la respuesta INCORRECTA:

a) Aplica a categoría MEDIA

b) Afecta sólo a la dimensión de seguridad de Disponibilidad

c) Es una medida del Marco operacional

d) Será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad

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

a) Interoperabilidad.

b) Transparencia.

c) Legitimidad.

d) Trazabilidad.

14. ¿Cuál de los siguientes responsables no aparece definido en el Esquema Nacional de Seguridad?

a) Responsable del fichero

b) Responsable de la información

c) Responsable del servicio

d) Responsable de seguridad

15. Un Sistema de Gestión de Seguridad de la Información con certificación vigente en la norma ISO/IEC 27001 implica directamente cumplimiento del Esquema Nacional de Seguridad

a) No

b) Sí, siempre

c) Sí, excepto por las medidas de seguridad referidas al marco operacional para el que habría que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo

d) -

16. ¿Cada cuánto tiempo serán objeto de una auditoría regular ordinaria los sistemas de información a los que se refiere el Esquema Nacional de Seguridad?

a) Cada dos años

b) Al menos, cada dos años

c) Cada año

d) Al menos, una vez al año

17. En una auditoría interna relativa al cumplimiento del Esquema Nacional de Seguridad, el informe de auditoría deberá dictaminar sobre la adecuación de las medidas implantadas, identificar sus deficiencias y, además:

a) Abstenerse de proponer medidas correctivas.

b) Identificar a los causantes de las deficiencias.

c) Remitirse a la Agencia Española de Protección de Datos.

d) Proponer medidas correctivas o complementarias.

18. Atendiendo al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, indique cuál de las siguientes respuestas es INCORRECTA en relación con un sistema de información de categoría alta:

a) Será objeto de una auditoría regular ordinaria, al menos cada dos años.

b) Deberá realizarse una auditoría extraordinaria siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

c) Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes.

d) Los informes de auditoría serán analizados por el responsable del sistema.

19. Según el artículo 31 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria que verifique el cumplimiento de los requerimientos del ENS:

a) Al menos cada dieciocho meses, pudiendo extenderse durante seis meses adicionales cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

b) Al menos cada dos años, sin posibilidad de extensión.

c) Al menos cada dos años, pudiendo extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

d) Al menos cada doce meses, pudiendo extenderse en periodos de seis meses hasta un máximo de treinta y seis cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

20. El centro de respuesta ante incidentes de seguridad para el sector público se llama CCN-CERT, mientras que el centro de respuesta ante incidentes de seguridad para el sector privado se llama:

a) IRIS-CERT.

b) OSI.

c) INCIBE-CERT.

d) ESP-DEF-CERT.

21. La guía CCN-STIC 887G trata sobre la configuración segura y gestión de las cargas de trabajo en:

a) AWS.

b) AZURE.

c) IBM Cloud.

d) Google Cloud.

22. El Real Decreto 311/2022, de 3 de mayo, regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. En el mismo, la seguridad se entenderá como:

a) Un proceso específicamente tecnológico, contemplando exclusivamente elementos técnicos.

b) Un proceso integral teórico que comprende únicamente tas medidas de prevención y detección de amenazas, quedando fuera del ámbito del ENS las de corrección, a implantar particularmente en cada caso.

c) Un proceso específicamente tecnológico, que comprende únicamente las medidas concretas de detección y corrección de amenazas, quedando fuera del ámbito del ENS las de prevención, como propias de cada caso particular.

d) Un proceso integral constituido por elementos humanos, materiales, técnicos, jurídicos y organizativos

23. ¿Cuál de los siguientes grupos de medidas de seguridad no se define en el anexo II del Esquema Nacional de Seguridad, Real Decreto 311/2022 del 3 de mayo?

a) Medidas de protección

b) Marco organizativo

c) Marco operacional

d) Marco tecnológico

24. En el contexto del Real Decreto 311/2022, de 3 de mayo, 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) Análisis y gestión de los riesgos, Gestión de personal, Profesionalidad, Mínimo privilegio, Integridad y actualización del sistema, Continuidad de la actividad.

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

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

d) Ninguna de las respuestas anteriores es correcta.

25. Según el Esquema Nacional de Seguridad (ENS), Real Decreto 311/2022, en lo relativo a la auditoría:

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.

b) Los sistemas de información de categoría MEDIA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.

c) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada en cualquier caso por personal de seguridad ajeno al que administra el sistema de información.

d) El ENS no considera suficiente una autoevaluación en ningún sistema de información de categoría BÁSICA, MEDIA o ALTA.

26. Indique cuál no es un principio básico según el RD 311/2022:

a) Prevención, reactivación y revisión

b) Seguridad Integral

c) Reevaluación periódica

d) Líneas de defensa

27. ¿Cuál de los siguientes no es un grupo de medidas de seguridad de los establecidos en el Esquema Nacional de Seguridad?

a) Marco de gestión

b) Marco organizativo

c) Marco operacional

d) Medidas de protección

28. De acuerdo con el Esquema Nacional de Seguridad, la disponibilidad de medios alternativos cuando los habituales no estén disponibles, es obligatoria:

a) En todos los sistemas y con los mismos requisitos.

b) En todos los sistemas, pero con diferentes requisitos según la categoría del sistema.

c) Sólo en sistemas de categoría MEDIA y ALTA.

d) Sólo en sistemas de categoría ALTA.

29. ¿Cuál de los siguientes aspectos no están recogidas en una Instrucción Técnica de Seguridad?

a) La declaración la conformidad.

b) La definición de roles y responsabilidades.

c) La auditoría.

d) La gestión de incidentes.

30. ¿Qué guía del CCN hace referencia a la criptografía de empleo en el Esquema Nacional de Seguridad?

a) CCN-STIC-802

b) CCN-STIC-403

c) CCN-STIC-807

d) CCN-STIC-823

31. Según el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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 cinco dimensiones de la seguridad. Cuál de las siguientes NO es correcta:

a) Disponibilidad [D]

b) Accesibilidad [A]

c) Integridad [I]

d) Confidencialidad [C]

32. La serie de normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones, se denomina:

a) CCN-STIC.

b) CCN-SOC.

c) CCN-RFC.

d) CCN-ENS.

33. De acuerdo con lo establecido en el RD 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad:

a) Todos los sistemas de información serán objeto de una auditoría regular ordinaria con carácter anual.

b) Los sistemas de información de categoría básica no precisan ser auditados.

c) La auditoría de los sistemas de categoría media puede ser sustituida por una autoevaluación realizada por el mismo personal que administra el sistema.

d) No es necesario que los informes de autoevaluación sean conocidos por el responsable de seguridad competente. Basta con que los conozca el responsable del sistema.

34. ¿Cuál de los siguientes NO es un objetivo de la Estrategia Nacional de Ciberseguridad?

a) Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

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

c) Seguridad del ciberespacio en el ámbito internacional

d) Protección del derecho a la ciberintimidad de la ciudadanía

35. ¿Cuál de los siguientes es un requisito mínimo de seguridad según el artículo 12 del Esquema Nacional de Seguridad?

a) Líneas de defensa.

b) Análisis y gestión de los riesgos.

c) Seguridad integral.

d) Detección ante otros sistemas de información interconectados.

36. De acuerdo al art. 27 del Esquema Nacional de Seguridad, la relación de medidas de seguridad que aplican las Administraciones Públicas para cumplir los requisitos mínimos de seguridad teniendo en cuenta los activos de un sistema, su categoría y las decisiones para gestionar los riesgos identificados se formaliza en:

a) La Política de Seguridad de la Información.

b) El Documento de Seguridad.

c) El Informe de Auditoría

d) La Declaración de Aplicabilidad.

37. ¿Es obligatoria la certificación de conformidad con el ENS?

a) No, sólo es obligatorio realizar auditorías ordinarias cada 2 años en el caso de sistemas de categoría MEDIA o ALTA, y una autoevaluación para los sistemas de categoría BÁSICA

b) Sí, los sistemas de categoría ALTA precisarán de una auditoría para la certificación de su conformidad

c) Sí, los sistemas de categoría MEDIA y ALTA precisarán de una auditoría para su certificación de conformidad, sin perjuicio de la auditoría prevista en el artículo 31 que podrá servir asimismo para los fines de certificación

d) Sí, todos los sistemas con independencia de su categoría deberán ser objeto de una auditoría de certificación de conformidad

38. De acuerdo al art. 28 del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, la relación de medidas de seguridad que aplican las Administraciones Públicas para cumplir los requisitos mínimos de seguridad teniendo en cuenta los activos de un sistema, su categoría y las decisiones para gestionar los riesgos identificados se formaliza en:

a) La Política de Seguridad de la Información.

b) La Declaración de Aplicabilidad.

c) El Documento de Seguridad.

d) El Informe de Auditoría.

39. En relación con las medidas de seguridad 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) Las medidas de seguridad se dividen en 2 grupos: marco organizativo y marco operacional.

b) La medida org.2 Normativa de seguridad se incluye dentro del marco operacional.

c) El número de medidas de seguridad definidas por el ENS es 50.

d) La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad de seguridad.

40. ¿Qué serie CCN-STIC establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad?

a) 500

b) 600

c) 700

d) 800

41. El empleo de algoritmos de firma electrónica acreditados por el Centro Criptológico Nacional:

a) Es una medida del Esquema Nacional de Seguridad para la dimensión de confidencialidad.

b) Es una medida de nivel medio del Esquema Nacional de Seguridad.

c) Es una recomendación de la Agencia Española de Protección de Datos.

d) Ninguna de las anteriores.

42. El Esquema Nacional de Seguridad establece que los sistemas 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 auditorías

43. ¿Qué Guía CCN-STIC de seguridad versa acerca de la Gestión y uso de dispositivos móviles?

a) CCN-STIC 820.

b) CCN-STIC 822.

c) CCN-STIC 823.

d) CCN-STIC 827.

44. Los sistemas de información de categoría media conforme al Esquema Nacional de Seguridad, aprobado por Real Decreto 311/2022, de 3 de mayo, serán objeto de una auditoría regular ordinaria:

a) Una vez al año cuando contengan datos personales de acuerdo al Reglamento General de Protección de Datos.

b) Cada tres años si no contienen datos personales.

c) Al menos cada dos años y con carácter extraordinario siempre que se produzcan modificaciones sustanciales que puedan repercutir en las medidas de seguridad requeridas.

d) Trimestralmente.

45. En relación a la medida de seguridad Mecanismo de autenticación para usuarios de la organización recogida en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, señale cuál de las siguientes opciones NO es de aplicación a un sistema con un nivel de confidencialidad ALTO:

a) Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

b) Las credenciales se suspenderán tras un periodo definido de no utilización.

c) Se exigirá el uso de al menos tres factores de autenticación.

d) Doble factor para acceso desde o a través de zonas no controladas.