Test Tema 47 #2

Actualizado el 13/04/2025

1. De entre las siguientes, la herramienta de análisis de riesgos desarrollada por el Centro Criptológico Nacional siguiendo la metodología MAGERIT es:

a) LORETO.

b) LUCÍA.

c) PILAR.

d) INES.

2. A la máxima cantidad de datos que se pueden perder en caso de desastres se le denomina:

a) RTO

b) RPO

c) SDO

d) RDO

3. Cual es la función principal del conjunto de herramientas "PILAR" desarrollado por el CCN- CERT:

a) Gestión de Ciberincidentes en las entidades del ámbito de aplicación del ENS

b) Almacenamiento virtual de información (archivos, muestras, aplicaciones, etc.)

c) Análisis y gestión de riesgos de un sistema de información

d) Auditoría de cumplimiento con el ENI

4. Se entiende por integridad de la información, según la norma ISO 27002:

a) Que cada persona accederá únicamente a la información que le corresponda.

b) Disposición de los servicios a ser usados cuando sea necesario.

c) Característica que previene contra la denegación no autorizada de acceso a activos del dominio.

d) La salvaguarda de la precisión y completitud de la información y sus métodos de proceso.

5. Respecto al análisis y gestión en un proyecto informático, indique cuál de las siguientes afirmaciones es correcta:

a) Las medidas preventivas están encaminadas a reducir los daños que puedan causar determinados incidentes

b) El plan de contingencia contendrá las medidas preventivas adoptadas

c) El plan de emergencia recoge las normas de actuación durante o inmediatamente después de cada fallo o daño

d) Las medidas de corrección van encaminadas a reducir la probabilidad de ocurrencia de incidentes

6. En temas de seguridad informática, una de las siguientes afirmaciones es falsa:

a) La prioridad de actuación viene dada por el producto impacto x vulnerabilidad

b) Los costes de seguridad se clasifican en directos (inversiones en equipos, mantenimiento, personal de seguridad) e indirectos (dificultad de uso, restricciones de servicios, reducción de prestaciones)

c) La política de seguridad es un documento oficial de la organización de carácter confidencial

d) El punto de equilibrio financiero será el que represente el coste mínimo sumando el coste de seguridad y el de pérdidas por incidentes o materializaciones de amenazas

7. Si un equipo tiene una avería ¿cuál de los siguientes indicadores nos da información sobre el tiempo medio requerido para reparar dicha avería?

a) MTBF

b) MTBR

c) MTTR

d) MTTF

8. Tras la realización de un análisis de riesgos de acuerdo con MAGERIT 3.0, el informe que detalla los activos, sus dependencias, las dimensiones en que son valiosos y la estimación de dicho valor, se denomina:

a) modelo de valor.

b) declaración de aplicabilidad.

c) mapa de riesgos.

d) estado de riesgo.

9. La probabilidad de explosión por escape de gas en una fábrica es de 0'0001. Si llega a producirse se sabe que morirán al menos diez empleados y se producirán pérdidas materiales por al menos de 100 millones de euros. ¿Cuál es riesgo cuantitativo asociado a la amenaza de explosión?

a) 10000 euros

b) 100 millones de euros

c) No se puede valorar porque la pérdida de vidas humanas no es cuantificable (salvo para las compañías de seguros)

d) Muy alto

10. ¿Cuál es una metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas, emitida por el Consejo Superior de Informática del ministerio de administraciones públicas de España?

a) COBIT.

b) MAGERIT.

c) METRICA.

d) REDSIS.

11. Dentro del conjunto de normas de la familia ISO 27000, ¿cual de las siguientes afirmaciones es la INCORRECTA?

a) ISO/IEC 270001 define los requisitos a cumplir para implantar un Sistema de Gestión de Seguridad de Información certificable conforme a la norma 27000.

b) ISO/IEC 270002 se usa para crear la estructura de la seguridad de la información en la organización e ISO/IEC 270001 define controles de manera mucho más detallada.

c) ISO/IEC 270002 define buenas prácticas para la Gestión de la Seguridad de los sistemas de información de una organización.

d) ISO/IEC 270001 sigue un modelo PDCA (Plan-Do-Check-Act).

12. Según MAGERIT v3, ¿quiénes son participantes en la tarea PS.2 (Plan de ejecución) para llevar a cabo un Plan de Seguridad?

a) El equipo de proyecto, especialistas en seguridad y especialistas en áreas específicas de seguridad.

b) Departamento de desarrollo y departamento de compras.

c) El equipo de proyecto y personal especializado en la salvaguarda en cuestión.

d) El director de proyecto y el comité de seguimiento.

13. Cuál de los siguientes no es un activo en MAGERIT:

a) www

b) url

c) anon

d) edi

14. El riesgo se puede:

a) Eliminar, reducir, asumir o transferir.

b) Eliminar, reducir pero no asegurar.

c) Reducir, asumir, transferir pero nunca se puede eliminar del todo.

d) Eliminar, reducir, asumir, transferir o asegurar.

15. Según MAGERIT 3.0, el informe en el que se recogen los resultados de la identificación de las amenazas relevantes sobre el sistema a analizar, caracterizadas por las estimaciones de ocurrencia y daño causado, se denomina:

a) Estimación del riesgo.

b) Plan de salvaguardas.

c) Declaración de aplicabilidad.

d) Mapa de riesgos.

16. El punto objetivo de recuperación que marcará la frecuencia de copias de respaldo:

a) RTPO

b) RTO

c) DRP

d) RPO

17. En la terminología de recuperación de sistemas ante desastres, el tiempo que cuantifica la cantidad perdida de datos hasta el momento de la interrupción, se denomina:

a) MTBF (Tiempo Medio Entre Fallos)

b) RPO (Objetivo de Punto de Recuperación)

c) RTO (Objetivo de Tiempo de Recuperación)

d) SDO (Objetivo de Entrega del Servicio)

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

a) Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a 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) -

19. ¿Cuál de las siguientes opciones es una metodología de Análisis y Gestión de Riesgos?

a) SCRUM.

b) MAGERIT.

c) PMBOOK.

d) ISO 9000.

20. Indique la respuesta correcta: la metodología de análisis de gestión de riesgos "MAGERIT"…

a) No necesita de la intervención de los responsables de los sistemas de información.

b) Está desarrollada por Computer Emergency Response Tearn (CERT).

c) Fue creada por el Consejo Superior de Administración Electrónica.

d) Sigue la terminología de la norma ISO 41000.

21. ¿Cuál de las siguientes es una norma certificable?

a) ISO/IEC 27003

b) UNE-ISO/IEC 27002:2009

c) UNE-ISO/IEC 27001:2017

d) BS 7799-1

22. Dentro de la metodología MAGERIT la definición: "es el daño sobre el activo derivado de la materialización de la amenaza", corresponde a:

a) Amenazas

b) Vulnerabilidad

c) Impacto

d) Riesgo

23. La autenticación fuerte requiere dos de los tres atributos de autenticación, de entre los que se encuentran:

a) Algo que alguien sabe

b) Algo que alguien tiene

c) A y B son correctas

d) A y B son incorrectas

24. En las organizaciones basadas en la información es crítico que implanten un plan de continuidad y contingencia de negocio. En este contexto, se entiende como Recovery Point Objective (RPO):

a) La cantidad máxima de tiempo tolerable que se necesita para verificar el sistema y / o la integridad de los datos

b) Es el período de tiempo máximo que la organización considera tolerable, durante el que los datos están en riesgo de pérdida.

c) El tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

d) -

25. Indique cuál de las siguientes afirmaciones NO es correcta en relación a MAGERIT:

a) En MAGERIT 3, vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo

b) Se permite estructurar el conjunto de activos en capas

c) Se consideran activos esenciales, la información que se maneja y los servicios prestados

d) Define que los activos están expuestos a amenazas que interesan por su valor

26. Según la Metodología de Análisis y Gestión de Riesgos (MAGERIT) indicar a qué concepto corresponde la siguiente definición "toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial":

a) Salvaguarda

b) Riesgo

c) Impacto

d) Vulnerabilidad

27. ¿Cuál de las siguientes no es una fuente principal para que una Organización identifique sus necesidades de seguridad física en el área de sistemas de información?

a) Los requisitos legales, estatutarios y contractuales a los que esté obligada la Organización

b) Los principios, objetivos y requisitos para el tratamiento de la información que la Organización ha desarrollado para soportar sus operaciones

c) El nivel de madurez en la gestión de la seguridad física, medido de acuerdo con el Computer Maturity Model

d) La valoración de los riesgos de la Organización

28. En la metodología MAGERIT, el evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, se denomina:

a) Impacto

b) Vulnerabilidad

c) Amenaza

d) Riesgo

29. ¿Cuál de las siguientes situaciones NO puede considerarse un incidente?

a) Fallo hardware.

b) Un uso no autorizado de la cuenta de un usuario.

c) Un evento cuyo impacto no genere una interrupción prolongada del servicio.

d) Todos los anteriores se considerarían incidentes.

30. Las dimensiones canónicas de la seguridad son:

a) Disponibilidad, confidencialidad y trazabilidad

b) Confidencialidad, autenticidad y disponibilidad

c) Integridad, trazabilidad y autenticidad

d) Confidencialidad, integridad y disponibilidad

31. ¿Cuál de los siguientes libros NO forma parte de MAGERIT v3?

a) Método.

b) Catálogo de elementos.

c) Catálogo de riesgos.

d) Guía de Técnicas.

32. En relación con la seguridad de los sistemas de información, seleccione la respuesta correcta:

a) Amenaza es la debilidad de un sistema de información que puede ser explotada mediante un ataque

b) Impacto es la probabilidad de que se produzca un daño en la organización

c) Mecanismos de Seguridad son las acciones llevadas a cabo encaminadas a reducir el riesgo sobre alguna vulnerabilidad

d) Vulnerabilidad es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales

33. Si se estima en un 20% la probabilidad de un incidente que provoca una pérdida de 10.000 euros, se está hablando de:

a) Un riesgo

b) Un impacto

c) Ninguna de las anteriores

d) a) y b)

34. La norma ISO 27002:

a) es un estándar de facto para la prestación de servicios de seguridad de la Tecnología de la Información.

b) tiene como objetivo proporcionar una base común para la gestión de la seguridad dentro de las organizaciones.

c) establece 36 dominios de control para la gestión de la seguridad.

d) establece un sistema de certificación adecuado a la norma.

35. Dentro de la familia de estándares ISO 27000, ¿qué norma se encarga de ayudar a las organizaciones a medir, a informar y, por lo tanto, a mejorar sistemáticamente la eficacia de su Sistema de Información de Gestión de la Seguridad (SGSI)?

a) ISO 27001.

b) ISO 27002.

c) ISO 27003.

d) ISO 27004.

36. Indique cuál es la norma española en base a la cual se certifica un Sistema de Gestión de la Seguridad de la Información:

a) ISO/IEC TR 13335

b) UNE 71501 IN

c) UNE-ISO/EIC 17799

d) UNE-ISO/IEC 27001

37. ¿Qué tipos de tratamiento del riesgo contempla MAGERIT v3?

a) Eliminación, Mitigación, Compartición, Financiación.

b) Eliminación, Reducción, Compartícón, Financiación.

c) Exterminación, Mitigación, Compartición, Financiación.

d) Compartición, Reducción, Traspaso, Compartición.

38. La norma ISO 27002 recoge:

a) Buenas prácticas para la gestión de la seguridad de la información.

b) La reglamentación de interconexión segura de redes inalámbricas (WIFI).

c) Normativa aplicable para el desarrollo de aplicaciones militares.

d) Estándares de desarrollo de aplicaciones de uso dual (civil y militar).