Test Tema 47 #1

Actualizado el 13/04/2025

1. De las siguientes normas, ¿cuál está referida al código de buenas prácticas en gestión de la seguridad de la Información?

a) ISO/IEC 13335-2.
b) ISO/IEC 27002:2022.
c) UNE 71502:2004.
d) ISO 10646.

2. ¿Qué norma corresponde a "Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información"?

a) UNE ISO/IEC 20000-1.
b) UNE-EN ISO 9001:2008.
c) ISO 14001.
d) UNE-EN ISO/IEC 27002:2017.

3. Qué norma UNE se ocupa de los sistemas de gestión de la seguridad de la información

a) UNE-ISO/IEC 20000-1:2018
b) UNE-ISO/IEC 27001:2017
c) UNE-ISO/IEC 19770-1:2008
d) -

4. El dominio de control "Seguridad ligada al personal" se corresponde con la dimensión de seguridad:

a) Organizativa.
b) Lógica.
c) Física.
d) Legal.

5. Una amenaza es, de acuerdo a MAGERIT:

a) Daño producido a una organización por un posible incidente
b) Resultado de una agresión
c) Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales
d) Posibilidad de ocurrencia de un incidente

6. En la metodología MAGERIT v3, el término que hace referencia a la medida del daño sobre un activo, derivado de la materialización de una amenaza es:

a) Impacto.
b) Riesgo.
c) Magnitud.
d) Contramedida.

7. Para determinar el nivel aceptable de seguridad hay que llegar a un equilibrio entre:

a) El coste de los daños versus el coste de sus consecuencias
b) El coste de las medidas de seguridad versus el presupuesto disponible
c) Los costes y la probabilidad de los daños versus el coste de las medidas y seguridad para evitarlos
d) El coste de los daños versus los daños que somos capaces de aceptar

8. Según MAGERIT, el conjunto de programas de seguridad que permite materializar las decisiones de gestión de riesgos es el:

a) mapa de riesgos

b) informe de insuficiencias

c) cuadro de mando

d) plan de seguridad

9. El período de tiempo tras un incidente dentro del cual se reanuda un producto, servicio o actividad o se recuperan recursos, se denomina:

a) Análisis de impacto al negocio (BIA).

b) Periodo máximo tolerable de interrupción (MTPD).

c) Objetivo de punto de recuperación (RPO).

d) Objetivo de tiempo de recuperación (RTO).

10. Un activo es, de acuerdo a MAGERIT:

a) Daño producido a una organización por un posible incidente

b) Resultado de una agresión

c) Evento que desencadena un incidente

d) Ninguno de los anteriores

11. En que norma de carácter internacional basa su terminología Magerit V3

a) ISO 14971

b) ISO 31000

c) ISO 17799

d) ISO 90003

12. La implantación de un sistema de single sign-on (SSO) implica que el riesgo de un acceso no autorizado:

a) Tendrá un mayor impacto

b) Tendrá un menor impacto

c) Tendrá una probabilidad mayor

d) Tendrá una probabilidad menor

13. 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

14. La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT, establece unas dimensiones canónicas de valoración de activos. Determine cuál de las siguientes respuestas es correcta:

a) Disponibilidad, integridad de los datos y confidencialidad de los datos.

b) Disponibilidad, integridad de los datos, confidencialidad de los datos, eficacia y eficiencia.

c) Eficacia, eficiencia, disponibilidad, integridad, confidencialidad, conformidad y fiabilidad.

d) Disponibilidad, integridad de los datos, confidencialidad de los datos, autenticidad de los usuarios del servicio, autenticidad del origen de los datos, trazabilidad del servicio, trazabilidad de los datos.

15. ¿Cuál de las siguientes amenazas de seguridad de Internet podría comprometer la integridad?

a) Robo de los datos desde el cliente

b) Exposición de la información de configuración de red

c) Un troyano en el navegador

d) Escuchas ilegales en la red

16. ¿Cuál de los siguientes conceptos NO es un elemento básico de MAGERIT?

a) activo

b) salvaguarda

c) amenaza

d) vulnerabilidad

17. Según la metodología MAGERIT versión 3.0, la dimensión de seguridad relativa al mantenimiento de las características de completitud y corrección de los datos es:

a) Trazabilidad

b) Autenticidad

c) Integridad

d) Disponibilidad

18. En el ámbito de las Tecnologías de la Información, señale de entre las siguientes, cuál se considera una amenaza según Magerit v3:

a) Ataques en Cascada.

b) Formación del Personal.

c) Ingeniería Social.

d) Inspecciones de Seguridad.

19. En MAGERIT, el riesgo residual es …

a) el riesgo aceptado

b) el riesgo despreciable

c) el riesgo recomendable.

d) el riesgo que resultaría tras aplicar un conjunto determinado de controles

20. Según Magerit V3, en la fase de Análisis de Riesgos, para determinar el valor de un activo hay que considerar:

a) Lucro cesante: pérdida de ingresos

b) Frecuencia de uso del activo

c) Ubicación física

d) Probabilidad de que se materialice una amenaza que cause un impacto al mismo

21. ¿Cuál de los siguientes es un objetivo de la gestión de riesgos?

a) Aumentar el presupuesto de seguridad de Tecnologías de la Información

b) Transparencia hacia la empresa de los riesgos significativos

c) Conocimiento de las últimas herramientas en materia de seguridad

d) Conducir un análisis de riesgo detallado

22. Según la Norma UNE-ISO/IEC 27001:2017, la facultad de un control para lograr los objetivos de seguridad para la que fue diseñado se denomina:

a) Eficiencia de un control

b) Finalidad de un control

c) Idoneidad de un control

d) Eficacia de un control

23. Las medidas de seguridad necesarias para restaurar el servicio de forma rápida, eficiente y con el menor costo y pérdidas posibles se incluyen en:

a) Plan de Recuperación de Desastres

b) Plan estratégico

c) Plan de sistemas

d) Plan de seguridad física

24. ¿Cuál de las siguientes afirmaciones es falsa respecto de MAGERIT?

a) MAGERIT es un órgano encargado de establecer la política de seguridad de los sistemas de información en las Administraciones Públicas

b) MAGERIT es una metodología para análisis y gestión de riesgos de los sistemas de información de las Administraciones Públicas

c) MAGERIT defiende que la seguridad debe ser independiente del medio

d) El objetivo de MAGERIT es conseguir la confianza en la utilización de técnicas informáticas y telemáticas

25. La serie ISO 27000 contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Respecto a las diferentes normas de esta serie es CIERTO:

a) La ISO 27001 es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

b) El Anexo A de la ISO 27001 enumera en forma de resumen los objetivos de control y controles que desarrolla. Es obligatoria la implementación de todos los controles enumerados en dicho anexo.

c) La ISO 27002 es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados.

d) La ISO 27003 es la única norma certificable de la serie.

26. ¿Qué norma corresponde a "Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información"?

a) UNE-EN ISO/IEC 27002:2017

b) UNE ISO/IEC 20000-1

c) UNE-EN ISO 9001:2008

d) ISO 14001

27. En el ámbito de la disponibilidad de la información ¿qué es el RPO?

a) Es la cantidad máxima de información que puede perderse cuando el servicio es restaurado tras una interrupción del sistema.

b) Es la cantidad máxima de tiempo tolerable necesario para que todos los sistemas críticos vuelvan a estar en línea.

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

d) Es la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

28. Señale cuál de las siguientes herramientas utilizadas en informática forense es software propietario:

a) The Sleuth Kit

b) Oxygen Forensic Suite

c) Volatility

d) Santoku

29. Indique la respuesta INCORRECTA:

a) Las herramientas PILAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT.

b) El acrónimo PILAR significa: Procedimiento Integral Lógico para el Análisis de Riesgos.

c) Las herramientas PILAR disponen de una biblioteca estándar de propósito general.

d) Las herramientas PILAR son capaces de realizar calificaciones de seguridad respecto a ISO/IEC 27002 (2005, 2013) - Código de buenas prácticas para la Gestión de la Seguridad de la Información -.

30. ¿Con qué ámbito se relaciona COSO?

a) Con control de la calidad, es similar al EFQM

b) Con el marco de Seguridad de las Tecnologías de la Información, similar a la ISO 27000

c) Con el Análisis y Gestión de Riesgos generales de una organización

d) Con el control de los servicios de Tecnologías de la Información, similar a ITIL

31. El tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio sin afectar a la continuidad de negocio se denomina:

a) RPO (Recovery Point Objective).

b) MRT (Maximum Recovery Time).

c) RTO (Recovery Time Objective).

d) MTD (Maximum Tolerable Downtime).

32. La política de seguridad de alto nivel de la Organización:

a) Debe describir QUE se intenta proteger, POR QUE se debe hacer, sin entrar en detalles acerca del COMO.

b) Debe describir QUE se intenta proteger, POR QUE se debe hacer y COMO se debe implementar.

c) Debe describir QUE se intenta proteger, POR QUE se debe hacer, COMO se debe implementar y CUANDO hay que implementar los mecanismos de seguridad.

d) Debe describir QUE se intenta proteger, COMO se debe implementar y CUANDO hay que implementar los mecanismos de seguridad.

33. Si el equipo del proyecto decide que hay que seleccionar un proveedor más estable para el proyecto, ¿qué estrategia de respuesta a los riesgos está utilizando?

a) Evitar el riesgo.

b) Mitigar el riesgo.

c) Transferir el riesgo.

d) Aceptar el riesgo.

34. Según MAGERIT versión 3 en un proyecto de análisis de gestión de riesgos, qué producto de salida de los citados a continuación NO se genera en la tarea de Planificación del proyecto:

a) Relación de participantes en los grupos de interlocutores.

b) Plan de entrevistas.

c) Informe de recursos necesarios.

d) Especificación detallada de los objetivos del proyecto.

35. Señale qué dos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema según la metodología Magerit versión 3:

a) Información y aplicaciones.

b) Información y servicios.

c) Aplicaciones e instalaciones.

d) Información y personal.

36. El volumen de datos en riesgo de pérdida que la organización considera tolerable es:

a) RPO (Recovery Point Objective)

b) RTO (Recovery Time Objective)

c) DRP (Disater Recovery Plan)

d) Business Impact Analysis (BIA)

37. Entre la documentación de la Seguridad de la Organización nos podremos encontrar:

a) La Política de Seguridad Corporativa será elaborada por el Responsable de Seguridad Corporativa y aprobada por el Comité de Seguridad Corporativa y por la Alta Dirección.

b) La Política de Seguridad de las TIC que debe estar alineada en todo momento con el Mantenimiento de los Sistemas de Información.

c) El Documento de Seguridad que ha de estar presente en toda documentación de la seguridad de la información.

d) Todas las respuestas anteriores son correctas.

38. La evaluación del riesgo es:

a) subjetiva

b) objetiva

c) Matemática

d) Estadística

39. Los mecanismos de salvaguarda, de acuerdo a MAGERIT son:

a) Un dispositivo lógico que reduce el riesgo

b) Un dispositivo físico que reduce el riesgo

c) Aquellos que operan de forma preventiva sobre la vulnerabilidad

d) Todas las respuestas anteriores son correctas

40. ¿Cómo se denomina la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC?

a) MAGERIT

b) Pilar

c) COBIT

d) ISO 31000

41. ¿Cuál de los siguientes no es un tipo de control?

a) Preventivo.

b) Detectivo.

c) Cognitivo.

d) Todos los anteriores lo son.

42. Un plan de emergencia es un plan por el que...

a) se realiza una nueva puesta en marcha del negocio tras un incidente.

b) disminuye el riesgo de aparición de incidentes menores.

c) se fuerza la indisponibilidad de los recursos críticos de información.

d) se prepara el entorno de continuidad en condiciones precarias.

43. En la metodología MAGERIT la definición "eventos que pueden desencadenar un incidente en la organización" corresponde a:

a) Riesgo

b) Impacto

c) Amenaza

d) Vulnerabilidad

44. La técnica de MAGERIT v3 que se utiliza para modelar las diferentes formas de alcanzar un objetivo se denomina:

a) Análisis logarítmico.
b) Árboles de ataque.
c) Valoración Delphi.
d) Gráficos de radar.

45. Indique la opción correcta, de entre las siguientes, respecto al objetivo de la metodología MAGERIT:

a) La eliminación completa de los riesgos físicos a los que se exponen los activos de una organización.

b) Facilitar información sobre incidentes de ciberseguridad.
c) Proporcionar una guía para analizar y gestionar el riesgo de sistemas TIC.
d) Reducir el número de activos para reducir la exposición de la organización a ciberataques.

46. ¿Cuáles son las dimensiones de seguridad según CobiT?

a) Confidencialidad, Disponibilidad, Integridad y Autenticidad.
b) Confidencialidad, Integridad y Disponibilidad.
c) Confidencialidad, Integridad, Disponibilidad y Autenticación.
d) Confidencialidad, Integridad, Disponibilidad e Interoperabilidad.

47. ¿Cómo define la Norma UNE ISO IEC 27002 la seguridad de la información?

a) La preservación de la confidencialidad y la integridad
b) La preservación de la confidencialidad, la integridad y la disponibilidad
c) La obtención de la autenticación y la preservación de la confidencialidad, la integridad y la disponibilidad

d) La obtención de la autenticación y el no repudio y la preservación de la confidencialidad, la integridad y la disponibilidad

48. Cuál de las siguientes es unna norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una organización. Es certificable.

a) ISO 27000
b) ISO 27001
c) ISO 27002
d) ISO 33000

49. Se entiende por disponibilidad de la información:

a) La información utilizada será la última, exacta, autorizada y completa.
b) Que cada persona accederá únicamente a la que le corresponda.
c) Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

d) Procedimiento o mecanismo tecnológico que reduce el riesgo.

50. Ignorar quien accede a que dato y cuando lo hace, afecta a la dimensión de la seguridad denominada:

a) confidencialidad
b) disponibilidad
c) integridad
d) trazabilidad

51. ¿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 Esquema Nacional de Seguridad.

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 Esquema Nacional de Interoperabilidad.

52. 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) -

53. Según MAGERIT v3, en el desarrollo de sistemas de información:

a) La seguridad debe estar embebida en el sistema desde su primera concepción.

b) La seguridad comenzará a considerarse formalmente cuando finalice el proceso de implantación de sistemas de información.

c) La seguridad del sistema de información es más económica implantarla una vez puesto en producción el sistema de información que tenerla en consideración durante el desarrollo del sistema.

d) La seguridad sólo ralentiza el proceso de desarrollo de sistemas de información por lo que sólo se debe considerar en aquellos sistemas que usen datos económicos.

54. 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

55. Según MAGERIT v3, 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) Evaluación de salvaguardas

c) Declaración de aplicabilidad

d) Mapa de riesgos

56. Indique cuál de los siguientes estándares se aplica a la seguridad de los sistemas informáticos:

a) ISO 12207

b) ISO 2167

c) ISO 27002

d) ISO 9004

57. Según la Norma UNE-ISO/IEC 27001:2017, la facultad de un control para lograr los objetivos de seguridad para la que fue diseñado se denomina:

a) eficacia de un control

b) eficiencia de un control

c) idoneidad de un control

d) finalidad de un control

58. Un honeypot es:

a) Un ataque sofisticado de phishing.

b) Un ramsomware bancario.

c) Un tipo de malware que explota vulnerabilidades 0day.

d) Un sistema hardware o herramientas software que simulan ser equipos vulnerables para poder exponerlos sin ningún riesgo y permitir el análisis de todos los ataques efectuados sobre ellos.

59. En cuanto a la gestión de incidencias según ISO 27001, ¿qué afirmación es FALSA?

a) El trabajo de gestión de una incidencia se termina una vez que la incidencia se ha resuelto o mitigado

b) El proceso de gestión de una incidencia da comienzo con la notificación de la misma por parte de la persona que la detecta.

c) Una vez detectado el incidente, se debe proceder a su clasificación.

d) Una vez el incidente se ha resuelto, se informará sobre su cierre a la persona que lo ha notificado

60. La capacidad de proporcionar y mantener un nivel aceptable de servicio ante la ocurrencia de fallos y desafíos a la operación normal se conoce como:

a) Disponibilidad.

b) Seguridad.

c) Resiliencia.

d) Mantenibilidad.

61. Respecto al análisis y gestión de riesgos:

a) En la gestión de riesgos, ningún riesgo identificado puede declararse como asumible ya que la metodología trata de evitar cualquier daño en nuestra organización

b) Si tenemos implementadas salvaguardas en nuestro sistema, no tiene sentido disponer de planes de continuidad pues las amenazas no llegarán a materializarse

c) Un led que indique el mal funcionamiento de un disco de un RAID puede considerarse como una salvaguarda

d) Cualquier amenaza afecta a todas las dimensiones de un activo

62. El impacto es, de acuerdo a MAGERIT:

a) Daño sobre el activo derivado de la materialización de la amenaza

b) Lo que podría pasar

c) Las respuestas 'a' y 'b' son correctas

d) Lo que probablemente pase

63. Los criterios comunes (criterios de evaluación unificados para la seguridad de los productos IT) se corresponden con la norma:

a) ISO 15408

b) ANSI 14508

c) CEN 15408

d) IEEE 14508

64. ¿A qué se denomina riesgo en MAGERIT versión 3?

a) Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

b) Al suceso que puede afectar a un activo y causarle un daño.

c) A la medida del daño sobre un activo derivado de la materialización de una amenaza.

d) Al recurso del sistema de información expuesto a un ataque.

65. En relación con la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT). Señale cuál de las opciones siguientes NO es correcta:

a) MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA (European Network and Information Security Agency).

b) El modelo normativo de MAGERIT se apoya en tres submodelos: análisis, gestión y procesos.

c) Uno de los objetivos de MAGERIT consiste en preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación.

d) PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos.

66. Algunos de los elementos tecnológicos que intervienen en la seguridad perimetral corporativa son:

a) En la seguridad perimetral corporativa sólo intervienen enrutadores y switches.

b) Switches, servidores y aplicaciones departamentales.

c) Enrutadores, cortafuegos y sistemas VPN.

d) Servidores, tecnologías inalámbricas, sistemas de usuarios y aplicaciones departamentales.

67. Señale la que no sea una de las técnicas específicas para el análisis de riesgos que establece MAGERIT:

a) Análisis de procesos.

b) Análisis mediante tablas.

c) Análisis algorítmico.

d) Árboles de ataque.

68. Una de las diferencias entre un Plan de Recuperación ante desastres (PRD o DRP en inglés) y un Plan de Contingencia es que:

a) El PRD debe ser realizado antes que el Plan de Contingencia.

b) El Plan de Contingencia debe ser realizado antes que el PRD.

c) El Plan de Contingencia realiza acciones para poder continuar con las actividades críticas del negocio aunque sea en modo manual o semi automático mientras que el PRD, en paralelo al Plan de Contingencia, trata de recuperar las aplicaciones y la información dañada para volver a la normalidad.

d) El PRD realiza acciones para poder continuar con las actividades críticas del negocio aunque sea en modo manual o semi automático mientras que el Plan de Contingencia trata de recuperar las aplicaciones y la información dañada para volver a la normalidad.

69. La norma ISO/IEC 27001:2022:

a) Es un estándar comúnmente aceptado para la gestión de riesgos de seguridad de la información.

b) Disponer de una certificación bajo esta norma ISO supone el cumplimiento del Esquema Nacional de Seguridad, ya que existe una equivalencia entre ambos estándares formalmente reconocida en el RD 311/2022 por el que se regula el Esquema Nacional de Seguridad.

c) No es certificable.

d) Es un estándar comúnmente aceptado para la implantación de sistemas de gestión de seguridad de la información, o ISMS - information security management systems por sus siglas en inglés.

70. Según MAGERIT V3, todas las dimensiones de la Seguridad son:

a) Disponibilidad, integridad y confidencialidad.

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

c) Disponibilidad, integridad, confidencialidad y auditabilidad.

d) Disponibilidad e integridad.

71. La seguridad de la información, según la ISO 27001, se basa en la preservación de su:

a) Accesibilidad - Disponibilidad - Invulnerabilidad.

b) Accesibilidad - Integridad - Disponibilidad.

c) Confidencialidad - Integridad - Disponibilidad.

d) Confidencialidad - Integridad - Inviolabilidad.

72. Seleccione la respuesta verdadera sobre los términos empleados para definir la estrategia de continuidad y recuperación en un sistema de información:

a) El objetivo de Punto de recuperación RPO determina la pérdida aceptable de datos en caso de interrupción.

b) El objetivo de Tiempo de Recuperación RTO es el tiempo máximo que el sistema puede estar interrumpido.

c) Cuanto más bajo es el RTO más baja es la tolerancia al desastre y más elevado será el coste de las estrategias de recuperación.

d) Todas las anteriores son verdaderas.

73. Señale cuál de las siguientes normas se debe tener en cuenta en el Área de Seguridad de una organización:

a) ISO 19799.

b) ISO 14508 sobre perfiles de protección.

c) ISO 14848.

d) ISO 27002.

74. Según la Norma UNE-ISO/IEC 27002:2017cuál de los siguientes aspectos NO está incluido en el control de accesos:

a) seguridad de los servicios de red

b) sincronización de relojes

c) responsabilidades del usuario

d) control de acceso a la librería de programa as fuente

75. Indica cuál de las siguientes afirmaciones es CORRECTA:

a) Las contramedidas se implementan sin tener en cuenta los riesgos identificados.

b) La gestión del riesgo se basa exclusivamente en el análisis de los indicadores relativos al número de intrusiones que se han detectado en cada periodo.

c) La gestión de riesgos se basa siempre en una escala cuantitativa.

d) Ninguna de las anteriores.

76. ISACA:

a) Es la Information Security Audit and Control Association

b) Posee una metodología basada en COBIT, de cara a obtener los controles a aplicar durante la auditoría y en CMMI, de cara a obtener un modelo de desarrollo sobre el que basarse para auditar el existente

c) Posee una metodología propia, que no se basa ni en COBIT ni en CMMI

d) Ninguna de las anteriores

77. Según Magerit v3, quién NO es un participante en un proyecto de análisis y gestión de riesgos:

a) Comité de Gestión.

b) Grupos de Interlocutores.

c) Comité de Seguimiento.

d) Equipo de Proyecto.

78. El Plan de Contingencias:

a) implica un análisis de los posibles riesgos

b) debe incluir un Plan de Recuperación de Desastres

c) las dos primeras son ciertas

d) las dos primeras son falsas

79. Un plan de contingencia corresponde a:

a) Evitar el riesgo de daños

b) Minimizar los daños producidos

c) Planificar las situaciones de emergencia

d) Establecer medidas de recuperación

80. ¿Cuál de las siguientes satisface una autenticación de usuario de dos factores?

a) Escaneo de iris y de huella dactilar

b) Identificador de usuario y sistema GPS

c) Smartcard que requiere un código PIN

d) Identificador de usuario más contraseña

81. Acorde a MAGERIT v3, una vez identificado y valorado el riesgo residual actual, se procede a su tratamiento. ¿Cuál NO es una estrategia de tratamiento del riesgo?

a) Mitigar.

b) Asumir.

c) Compartir/transferir.

d) Todas son estrategias de tratamiento del riesgo.

82. ¿Cuál de los siguientes no se considera un riesgo de origen accidental?

a) Huelga del personal

b) Errores en la utilización de los datos

c) Averías en las instalaciones eléctricas

d) Interrupción de suministro de energía

83. Atendiendo al estándar ISO 22301 en un Plan de Recuperación ante Desastres, el Objetivo de Punto de Recuperación (Recovery Point Objective RPO) es:

a) el nivel de servicios a proporcionar en modo alterno hasta que se recupere la situación normal.

b) el tiempo que la organización puede soportar desde que se produce el fallo hasta que se recuperan los servicios críticos.

c) el tiempo máximo tolerable de interrupción.

d) la pérdida máxima de datos tolerable en caso de interrupción.

84. Señale cuál de las siguientes versiones de PILAR es una versión reducida, destinada a la realización de análisis de riesgos muy rápidos:

a) PILAR Basic

b) PILAR Mini

c) .PILAR

d) RMAT

85. El primer paso a la hora de desarrollar un Plan de Continuidad de Negocio es:

a) Clasificar los sistemas según su importancia

b) Establecer una estrategia de recuperación de desastres

c) Determinar el tiempo crítico de recuperación

d) Realizar una clasificación del riesgo

86. Según MAGERIT V3, la relación de amenazas a las que están expuestas los activos se llama:

a) Modelo de amenazas.

b) Informe de suficiencias.

c) Mapa de riesgos.

d) Listado de vulnerabilidades.

87. Señale de las siguientes cuál es una técnica específica dentro de un proyecto de análisis y gestión de riesgos, según la guía de Técnicas de MAGERIT v3:

a) Sesiones de trabajo.

b) Valoraciones Delphi.

c) Histogramas.

d) Árboles de ataque.

88. ¿Qué es una estructura de desglose de riesgos (RBS)?

a) Una representación jerárquica de los riesgos según sus categorías.

b) Una matriz que vincula la probabilidad de ocurrencia de cada riesgo con su impacto.

c) Un diagrama de influencias.

d) Un diagrama de Ishikawa.

89. En MAGERIT ¿cuál de las siguientes opciones NO es cierta?

a) Riesgo es la posibilidad de que suceda un daño o perjuicio

b) Impacto es el evento que puede desencadenar un incidente en la organización

c) Existen tres submodelos: elementos, eventos y procesos

d) La información es un activo

90. Según la norma ISO/IEC 27002, el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados, es el concepto de:

a) Seguridad.

b) Integridad.

c) Disponibilidad.

d) Confidencialidad.

91. En MAGERIT, el riesgo residual es...

a) el riesgo aceptado.

b) el riesgo despreciable.

c) el riesgo recomendable.

d) el riesgo que resultaría tras aplicar un conjunto determinado de controles.

92. Un centro alternativo de tratamiento de la información:

a) Debe ser identificable desde el exterior, para que sea fácilmente localizado en caso de emergencia.

b) Debe tener las mismas restricciones de acceso físico que la instalación principal.

c) Debe estar ubicado en las proximidades de la instalación principal, así se puede poner en operación inmediatamente.

d) No necesita disponer del mismo nivel de supervisión ni controles ambientales que la instalación principal, porque los costes serían prohibitivos.

93. El término MAGERIT es un acrónimo que procede de los siguientes términos, o significa lo siguiente:

a) Mercado Abierto y Gratuito a la Exportación de Recursos Informáticos y de Telecomunicaciones

b) Sistema Informático propio, financiado y desarrollado por la Comunidad Autónoma de Madrid (de aquí el nombre de: "MAGERIT")

c) Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

d) Methot Aid for Gradual Employ Resource of Information Technology

94. Según Magerit v3 cuál de las siguientes tareas NO forma parte de la actividad de caracterización de los activos en el Análisis de Riesgos:

a) Identificación de los activos.

b) Dependencias entre activos.

c) Auditoría de los activos.

d) Valoración de los activos.

95. El RPO (Recovery Point Objective) de una organización son 2 horas. ¿Cuál de las siguientes afirmaciones es cierta?

a) No más de 2 horas de datos de producción se pueden perder en caso de desastre.

b) No más de 4 horas de datos de producción se pueden perder en caso de desastre.

c) El tiempo para recuperar los sistemas en producción de nuevo no puede ser más de 2 horas.

d) El tiempo para recuperar los sistemas en producción de nuevo no puede ser más de 4 horas.

96. MAGERIT es:

a) Una metodología de Análisis y gestión de riesgos de sistemas de información.

b) Una metodología de Análisis y gestión de centros de recuperación de desastres de sistemas de información.

c) Una metodología de Análisis y gestión de sistemas de archivo de sistemas de información.

d) Una metodología de Análisis y gestión de evaluación de rendimiento de sistemas de información.

97. En la metodología MAGERIT, se define vulnerabilidad como:

a) El daño producido a la organización por un posible incidente

b) La posibilidad de que se produzca un impacto dado en la organización

c) Cualquier activo del sistema

d) Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza

98. En relación con la versión 3 de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), podemos afirmar que:

a) Es una actualización realizada por el CCN (Centro Criptológico Nacional), con el fin de adaptar la versión anterior a los requerimientos exigidos en el Esquema Nacional de Seguridad.

b) Fue elaborada por el antiguo Consejo Superior de Administración Electrónica, pero ha dejado de tener validez dado que no se adapta a los requerimientos exigidos en el Esquema Nacional de Seguridad.

c) El CCN ha desarrollado una herramienta denominada PILAR que implementa la metodología MAGERIT

d) -

99. Indicar cuál de los siguientes NO está entre los objetivos que persigue MAGERIT v3:

a) Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

b) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

c) Establecer una norma de obligado cumplimiento para todos los organismos de las Administraciones Públicas españolas a la hora de analizar y gestionar los riesgos.

d) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

100. Documento que indica por escrito como una organización planea proteger los recursos físicos e informáticos:

a) Acuerdo de Licencia de Usuario Final (EULA)

b) Política de Seguridad

c) Acuerdo de nivel de servicio (SLA)

d) Gestión de relaciones entre socios (PRM)

101. (reserva)Según la norma ISO/IEC 27002, el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados, es el concepto de:

a) Seguridad.

b) Integridad.

c) Disponibilidad.

d) Confidencialidad.

102. Según Magerit v3, un riesgo es:

a) Consecuencia que sobre un activo tiene la materialización de una amenaza.

b) Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus archivos.

c) Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

d) Debilidad en la seguridad de un sistema de información. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

103. La primera tarea a realizar en un plan de continuidad de negocio es:

a) Duplicar los equipos críticos

b) Hacer una copia de seguridad de todos los datos

c) Realizar un análisis de la criticidad de los diferentes recursos ante posibles situaciones de emergencia

d) Evaluar la habilidad del personal para responder adecuadamente a situaciones de emergencia

104. ¿Qué respuesta es CORRECTA respecto a la herramienta de análisis y gestión de riesgos PILAR?:

a) Es un entorno de análisis de riesgos abierto a todo tipo de usuarios.

b) Su desarrollo es responsabilidad del Centro de Operaciones de Ciberseguridad de la AGE.

c) Se basa en la metodología MAGERIT.

d) Sólo está disponible para la Administración General del Estado.

105. ¿Qué dos activos de entre los siguientes considera esenciales MAGERIT versión 3.0 en su Catálogo de Elementos?:

a) Equipos y comunicaciones.

b) Software y hardware.

c) Tangibles e intangibles.

d) Información y servicios.

106. Se entiende por integridad de la información:

a) Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada.

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

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

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

107. El contenido de la norma ISO 27001 se divide en secciones, ¿cuál de las siguientes NO se corresponde con una sección de la misma?

a) Mejora del SGSI.

b) Auditorías internas.

c) Responsabilidad de la dirección.

d) Plan de seguridad.

108. Según MAGERIT v3 los elementos del análisis de riesgos son:

a) Impacto, riesgos calculados y riesgos intrínsecos.

b) Activos, amenazas y salvaguardas.

c) Vulnerabilidades, riesgos e impacto.

d) Entorno, sistema de información, información, funciones y otros.

109. El riesgo es, de acuerdo a MAGERIT:

a) Daño producido a una organización por un posible incidente

b) Resultado de una agresión

c) Posibilidad de ocurrencia de un incidente

d) Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización causando daños o perjuicios a la misma

110. MAGERIT:

a) Es una metodología de análisis de riesgos

b) Es una metodología de gestión de riesgos

c) Es una metodología de gestión de proyectos

d) Las respuestas ‘a’ y ‘b’ son correctas

111. ¿Cuál es el nombre con que se conoce en MAGERIT versión 3 a la persona de la organización, con buen conocimiento de personas y unidades implicadas en el proyecto de Análisis de Gestión de Riesgos, que tiene la capacidad para conectar al equipo de proyecto con el grupo de usuarios?

a) Promotor

b) Enlace operacional

c) Director de proyecto

d) Responsable de servicios internos

112. ¿En qué se diferencia el Plan de Continuidad de Negocio y el Plan de Recuperación ante Desastres?

a) No existe ninguna diferencia, son términos equivalentes.

b) El Plan de Continuidad de Negocio se centra en la parte reactiva de las TIC mientras que el de Recuperación ante Desastres afecta a todos los departamentos de la organización.

c) El Plan de Recuperación ante Desastres se centra en la parte reactiva y es un subconjunto del Plan de Continuidad de Negocio.

d) Ninguna de las anteriores.

113. En el análisis algorítmico descrito en la guía de técnicas de Magerit v3, el coeficiente denominado 'grado de dependencia', es un coeficiente aplicado a las dependencias entre:

a) activos en el modelo cualitativo, que varía entre 0,0 (activos independientes) y 1,0 (activos con dependencia absoluta).

b) activos en el modelo cuantitativo, que varía entre 0,0 (activos independientes) y 1,0 (activos con dependencia absoluta).

c) activos en el modelo cualitativo, que varía entre 0,0 (activos con dependencia absoluta) y 1,0 (activos independientes).

d) activos en el modelo cuantitativo, que varía entre 0,0 (activos con dependencia absoluta) y 1,0 (activos independientes).

114. ¿Cuál de los siguientes elementos no se considera un activo de una organización?

a) Recursos físicos: equipos, sistemas, cableado…

b) Utilización de recursos: uso de CPU, de ancho de banda, de disco duro…

c) Imagen y reputación pública y profesional de la empresa y sus empleados

d) Todos los anteriores son activos de una organización

115. Según MAGERIT v3, ¿qué concepto se correspondería con la definición: "proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios"?

a) Auditoría.

b) Acreditación.

c) Certificación.

d) Evaluación.

116. ¿Cuál de los siguientes pasos será el último en un Proceso de Gestión de Riesgos, según se establece en la Guía de Seguridad de las TIC CCN-STIC 801?

a) Implementar las medidas de seguridad.

b) Obtener la autorización para operar.

c) Monitorizar.

d) Evaluar la seguridad del sistema de información.

117. La versión actual de la metodología de análisis y gestión de riesgos MAGERIT es:

a) 1

b) 2

c) 3

d) 4

118. Los cuatro pasos del Ciclo de Deming son:

a) Planificar, Medir, Monitorizar, Informar

b) Planificar, Revisar, Reaccionar, Implementar

c) Planificar, Hacer, Actuar, Auditar

d) Planificar, Hacer, Revisar, Actuar

119. En cuanto a la dependencia entre activos, a la hora de evaluar riesgos:

a) La seguridad del activo superior depende de la del inferior.

b) El activo superior puede ser atacado a través del inferior.

c) La relación indica que el activo inferior es necesario para que el superior funcione.

d) La a) y la b) son correctas.

120. Según la metodología MAGERIT versión 3 (y 2), el riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información se denomina:

a) Riesgo retenido.

b) Riesgo acumulado.

c) Riesgo residual.

d) Riesgo supervisado.

121. Respecto a la metodología MAGERIT y la gestión de riesgos, el riesgo calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él se denomina:

a) Riesgo inherente

b) Riesgo repercutido

c) Riesgo acumulado

d) Riesgo total

122. ¿Qué NO debe incluir la implementación de un plan de continuidad de negocio dentro de un Sistema de Gestión de la Seguridad de la Información?

a) Designar y formar a las personas que deben intervenir en cada caso

b) Documentar y construir procedimientos de actuación en cada caso

c) Aportar una definición del alcance del Sistema de Gestión de la Seguridad de la Información

d) Establecer una estructura de gestión y sus niveles de competencia dentro del plan de continuidad

123. En el contexto de Magerit es FALSO:

a) El libro de Método incluye la guía Valoración Delphi.

b) La herramienta PILAR soporta el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

c) El análisis de riesgos considera los siguientes elementos: activos, amenazas y salvaguardas.

d) Las dependencias entre activos son la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

124. Respecto a la metodología MAGERIT y la gestión de riesgos, el riesgo calculado, tomando en consideración el valor propio de un activo y el valor de los activos que dependen de él, se denomina:

a) Riesgo inherente.

b) Riesgo repercutido

c) Riesgo acumulado.

d) Riesgo total.

125. El análisis de las necesidades de la organización, la implantación y ejecución de controles y medidas para gestionar la capacidad de la organización frente a incidentes, la supervisión y revisión del rendimiento y la mejora continua son los pilares de:

a) La planificación de sistemas.

b) La gestión de la configuración.

c) La gestión de cambios.

d) La gestión de la continuidad del negocio.

126. La seguridad física de los sistemas de información:

a) Debido a la segregación de tareas, es labor exclusiva de los guardias de seguridad

b) Debe alcanzar también a los equipos que estén fuera de los locales de la Organización (equipos en teletrabajo, dispositivos móviles, etc.)

c) Es una preocupación que se evita al externalizar las funciones de explotación del sistema de información

d) Es notablemente superior en aquellas Organizaciones que disponen de sótanos bunkerizados

127. Para desarrollar un plan de continuidad de negocio de éxito es fundamental la participación del usuario final durante el proceso de:

a) Estrategias de recuperación
b) Desarrollo del plan detallado
c) Análisis de impacto al negocio (BIA)
d) Mantenimiento y pruebas

128. Un evento con consecuencias en detrimento de la seguridad del sistema de información se denomina, según MAGERIT v.3:

a) Incidente
b) Incidencia
c) Contingencia
d) Impacto

129. Como medidas de tipo físico, en seguridad informática, podemos hablar de:

a) Seguridad de datos y de software
b) Seguridad organizativo-administrativa y de software
c) Seguridad de hardware y de datos
d) Adecuación de locales y seguridad de accesos

130. Magerit es una herramienta de:

a) Gestión de tiempos de proyectos
b) Gestión de recursos
c) Gestión operativa
d) Gestión de riesgos