Test Tema 38 #1

Actualizado el 13/04/2025

1. ¿Qué es una auditoría de regularidad?

a) Es la que evalúa la eficacia en la consecución de objetivos y la eficiencia en los recursos empleados para alcanzarlos.

b) Es aquella orientada a verificar el cumplimiento de la normativa aplicable.

c) Es la especializada en descubrir fraudes y delitos.

d) Ninguna de las anteriores.

2. ¿Cuál de las siguientes palabras no se corresponde con la definición 'información que recoge el sistema informático sobre las operaciones efectuadas, y que permiten contrastar los resultados procedentes de dicho sistema con los documentos originales a los que se refieren'?

a) Evidencias de auditoría

b) Trazas de auditoría

c) Registros de auditoría

d) Pistas de auditoría

3. ¿Cuál de las siguientes respuestas referidas a las auditorías de control de calidad es cierta?

a) Es un procedimiento habitual de control de calidad del software

b) Es un procedimiento extraordinario al que se pueden someter los proyectos que tengan especial magnitud

c) Su objetivo es proceder al refinamiento sucesivo en la definición de las especificaciones finales del proyecto

d) Ninguna de las respuestas anteriores es cierta

4. Señale la verdadera:

a) Si el impacto de un hallazgo según su materialidad es bajo se refleja en el informe como posible debilidad del sistema de control

b) Si el impacto de un hallazgo según su materialidad es medio se describe dicho hallazgo como una vulnerabilidad a la que se expone el sistema

c) Si el impacto de un hallazgo según su materialidad es bajo se describe dicho hallazgo como una vulnerabilidad a la que se expone el sistema

d) Si el impacto de un hallazgo según su materialidad es medio se identifica como una debilidad que debe compensarse o anularse con más controles, o haciendo los existentes más estrictos

5. En el ámbito de la auditoría de eficiencia, ésta es máxima…:

a) Cuando los costes de desarrollo, mantenimiento y operación del sistema son los más bajos posibles

b) Cuando se cumplen todos los requisitos de los usuarios y los objetivos del organismo

c) Cuando el personal de sistemas de información trabaja con la máxima diligencia

d) Cuando se alcanzan los objetivos de los usuarios con los mínimos recursos posibles

6. ¿Cuál es la diferencia entre una auditoría de vulnerabilidades y un test de penetración?

a) Un test de penetración identifica los servicios en ejecución. Una auditoría de vulnerabilidades proporciona una mayor información sobre las vulnerabilidades.

b) Un test de penetración enumera los recursos, una auditoría de vulnerabilidades enumera las vulnerabilidades.

c) Un test de penetración aprovecha las vulnerabilidades, una auditoría de vulnerabilidades encuentra las vulnerabilidades.

d) Los dos son lo mismo.

7. Que afirmación de las siguientes acerca de la auditoria informática es incorrecta:

a) Debe ser realizada por una empresa externa.

b) Debe velar por la eficacia y eficiencia del sistema informático.

c) Debe verificar la calidad de los sistemas de información.

d) Debe supervisar los mecanismos de control interno establecidos en los centros de proceso de datos.

8. De acuerdo con la guía CCN-STIC-802, de auditoría del ENS, señale cuál es 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 desarrollada por personal diferente al que administra el sistema.

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

9. Generalmente el auditor informático:

a) Informa a la Dirección General de Organización.

b) Informa a la Dirección del Departamento de Informática.

c) El alcance de sus funciones es sólo sobre el Departamento de Informática.

d) Analiza los controles en el día a día.

10. Señale la falsa:

a) La auditoría requiere una planificación a tres niveles: qué, cuándo y cómo auditar

b) Si el área ya ha sido auditada con anterioridad debe revisarse la documentación previa

c) Aunque el área ya haya sido auditada con anterioridad es necesario realizar la auditoría al completo sin tener en cuenta la documentación previa pues ésta puede no ser ya consistente con la situación actual

d) Una de las ventajas del uso de herramientas de auditoría informática es la disminución del riesgo propio del proceso de auditoría en la recolección de datos y la mayor independencia

11. En el contexto de una investigación forense:

a) Se debe trabajar con el disco duro original para dejar constancia del trabajo realizado

b) Se debe trabajar con una copia de los ficheros del disco duro realizada desde el sistema operativo y configurando el acceso a disco en modo de sólo lectura

c) Se debe trabajar con un clonado o copia bit a bit del disco duro

d) Se debe trabajar con el disco duro original pero realizando previamente una imagen forense y dejando constancia mediante el cálculo del hash

12. Diremos que un sistema de información es efectivo cuando:

a) Utiliza el mínimo de recursos para producir las salidas requeridas.

b) Cuando alcanza sus objetivos.

c) Cuando proteja los activos de todas las amenazas posibles.

d) Cuando conserve la completitud, robustez, pureza y veracidad de los datos.

13. Los objetivos de alto nivel de la auditoria informática son, con carácter general: I) Dar a la Dirección garantía suficiente del cumplimiento de los objetivos de control. II) Sustanciar los riesgos resultantes, si se detectan debilidades de control significativas. III) Aconsejar a la Dirección sobre el curso de acciones correctivas.

a) Sólo I
b) Sólo II
c) I y II
d) I, II y III

14. ¿Cuál es la norma que regula el proceso de auditoría?

a) Aquella que se haya aprobado en el ámbito organizativo en el que se desarrolla la auditoría
b) COBIT
c) El mandato para la auditoría
d) La política de seguridad de la organización

15. ¿Cuántos niveles de evaluación están contemplados en los Criterios Comunes?

a) Siete
b) Son los mismos que los de ITSEC
c) Cinco
d) Seis

16. ¿Cuál de los siguientes es un control de acceso físico?

a) Etiquetado de soportes en cinta
b) Uso de clave por teclado para entrar al CPD
c) Contraseñas para uso de aplicaciones, renovadas periódicamente
d) Todas

17. Dentro de los objetivos que se fijaría una auditoría sobre el grado de adecuación de las herramientas de software utilizadas a la información gestionada, ¿cuál de los siguientes considera que no sería relevante obtener del estudio?

a) Fiabilidad técnica
b) Cambio del modelo de datos utilizados
c) Estudio de opinión de los usuarios
d) Facilidad de mantenimiento y expansión

18. Un auditor informático deberá verificar:

a) Cumplimiento de objetivos de la organización
b) Adecuación de procedimientos de control
c) Uso de metodologías según estándares de la organización
d) Todas

19. Según la Guía de Seguridad CCN-STIC-802, ¿los hallazgos de no conformidad se clasificarán atendiendo a qué grados?:

a) No Conformidad Mayor, No Conformidad Menor, y Observación
b) No Conformidad Mayor, y No Conformidad Menor
c) No Conformidad Mayor, No Conformidad Menor y Alegación.
d) No Conformidad Mayor, No Conformidad Menor, Observación y Alegación.

20. ¿Cuál de las siguientes no es un requisito que debe cumplir una evidencia?

a) Suficiente
b) Eficiente
c) Relevante
d) Competente

21. En auditoría informática, los controles de salida contienen, entre otros, a:

a) Registro y almacenamiento de formularios negociables

b) Autorización de la distribución

c) Balanceo y conciliación

d) Todas las anteriores

22. ¿Cuál es el objetivo de la Auditoría de Sistemas de Información o Auditoría Informática?

a) Definir e implementar el Sistema de Gestión de Riesgos de la organización.

b) Establecer la política de control de las organizaciones.

c) La supervisión de los controles efectivamente implementados en una organización y la determinación de la eficiencia de los mismos.

d) Establecer la política de seguridad de las organizaciones.

23. Indique la afirmación verdadera sobre la auditoría informática:

a) Se lleva a cabo exclusivamente por empleados de la empresa auditada.

b) Se centra únicamente en la evaluación del desempeño de los empleados.

c) Se centra en evaluar la eficiencia del uso de todos y cada uno de los recursos de la empresa.

d) Se lleva a cabo para asegurar el cumplimiento de los estándares y regulaciones aplicables.

24. Los controles detectivos tienen como objeto:

a) Reducir el riesgo ante una debilidad existente

b) Predecir problemas potenciales antes de que ocurran

c) Solucionar problemas detectados por controles detectivos

d) Reportar errores

25. ¿Cuál de los siguientes no es un control de entrada de datos en una Revisión de Controles de Aplicación en una auditoría informática?

a) Controles por lote y balanceo

b) Validación y edición de datos

c) Balanceo y conciliación

d) Autorización de ingreso

26. ¿Cuándo es necesario disponer de un control compensatorio?

a) Cuando no esté previsto un control.

b) Cuando el coste de un control lo haga inabordable.

c) Cuando el control no esté efectivamente implantado o falle su aplicación.

d) Todas las anteriores son ciertas.

27. Cuál de las siguientes afirmaciones es falsa en lo que al "informe final de una auditoría" se refiere:

a) Si el informe es muy extenso, sería conveniente redactar un resumen ejecutivo.

b) Es conveniente que el informe esté perfectamente indexado con, al menos, tres apartados en función de a quién vaya dirigido (director de sistemas, equipo técnico de sistemas, equipo de calidad y auditoría).

c) El esquema típico de un informe de auditoría contendría entre otros los siguientes apartados: introducción, objetivos, metodología y resultados.

d) Un elemento sustancial para asegurar la calidad del informe y que éste sea completo y objetivo es conseguir que los responsables de la actividad realicen una revisión del borrador del informe y formulen las alegaciones y comentarios que consideren oportunos.

28. Cuál de los siguientes no es parte del contenido mínimo de un informe de auditoría:

a) Metodología

b) Alegaciones

c) Objetivo y alcance

d) Título

29. Señale la afirmación verdadera sobre las pruebas de cumplimiento:

a) Son aquellas que se aplican para detectar la presencia o ausencia de errores en los procesos o controles, basándose en muestreos estadísticos o buscando específicamente las operaciones de mayor riesgo

b) Son aquellas orientadas a comprobar que se cumplen determinados procedimientos de control o procesos establecidos

c) Son aquellas dedicadas exclusivamente a probar la existencia de controles

d) Un ejemplo de pruebas de cumplimiento es la observación de la ejecución de los procesos

30. Según el artículo 34 del Esquema Nacional de Seguridad, (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. consolidado), los sistemas de información a los que se refiere el RD serán objeto de una auditoria regular ordinaria que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad, al menos:

a) Cada año

b) Cada dos años

c) Cada cinco años

d) -

31. ISACA es:

a) la agencia gubernamental de Evaluación de Políticas Públicas y de la Calidad de los Servicios.

b) el estándar de calidad más extendido en la realización de auditorías informáticas.

c) una de las normas de la ISO 17799.

d) una asociación independiente que establece prácticas globalmente aceptadas para los profesionales de la auditoría informática.

32. Cuál de las siguientes no es una función del auditor de Sistemas de Información:

a) Análisis de requisitos y especificación funcional

b) Evaluación de los planes de implantación de sistemas y mejoras de los existentes

c) Evaluación de riesgos

d) Evaluación de controles en los sistemas de información

33. Cuál de las siguientes no es una norma básica en la auditoría de los sistemas de información:

a) Obtención de evidencia suficiente.

b) Estudio y evaluación del sistema de control interno.

c) Obtención de evidencia adecuada.

d) Todas las anteriores forman parte de las normas básicas en la auditoría de los sistemas de información.

34. En una auditoría de un sistema EDI, ¿cuáles son las principales áreas de revisión y evaluación, en las que los auditores y el personal especializado de soporte deben centrarse?

a) Conocimiento del negocio, evaluación de controles y pruebas

b) Conocimiento del negocio, evaluación del riesgo, evaluación de los controles generales, evaluación de los controles de operación, pruebas, uso de herramientas asistidas por ordenador (CAAT)

c) Conocimiento del negocio, evaluación del riesgo, evaluación de controles y pruebas

d) Conocimiento del negocio, controles administrativos y de gestión, evaluación del riesgo, evaluación del los controles de operación, pruebas y uso de herramientas asistidas por ordenador (CAAT)

35. Las auditorías técnicas que tienen por objeto participar en la investigación de fraudes, en actos conscientes y voluntarios en los cuales se eluden las normas legales se llaman

a) Auditorías forenses

b) Auditorías de gestión

c) Auditorías policiales

d) Auditorías de regularidad

36. Señale la falsa:

a) La evidencia obtenida de una tercera parte independiente es menos competente que la ofrecida por el área auditada

b) La evidencia obtenida de un sistema con un control efectivo es más competente que la ofrecida por un sistema con un control débil

c) La evidencia obtenida por el equipo auditor directamente en una inspección física es más competente que la obtenida indirectamente

d) Todas las afirmaciones anteriores son ciertas

37. ¿Cuál de las siguientes afirmaciones es falsa respecto a la auditoría?

a) Independientemente del tipo de auditoría informática que pretenda realizarse, la finalidad última es emitir un juicio acerca del estado de los sistemas

b) Del fin de la auditoría habrán de obtenerse los medios y las acciones de investigación que se estimen necesarios para su consecución

c) La auditoría siempre recomendará la toma de acciones correctivas, independientemente del examen de situación realizado

d) Cuando la tarea del auditor sea muy compleja, se llevará a cabo una división de funciones de forma arborescente

38. Las siglas CAAT en relación con los Sistemas de Información significan:

a) Computed Audit Assisted Techniques

b) Campaign Against Automotive Trenes

c) Centro para la Administración de Alternativas Tecnológicas

d) Computer-Assisted Advanced Tools

39. En la ejecución de un proyecto de auditoría informática sobre un sistema de información, el uso de procedimientos estadísticos de muestreo ayudará a minimizar el riesgo:

a) De muestreo.

b) De detección.

c) Inherente.

d) De control.

40. ¿En qué fase del ciclo de vida se deben contemplar los controles de aplicación por primera vez?

a) Diseño

b) Análisis

c) Construcción

d) Pruebas de aceptación

41. En una auditoría informática, ¿quién debe presentar recomendaciones de auditoría?

a) Los usuarios del servicio auditado

b) El equipo de auditoría

c) La dirección de la unidad auditada

d) La entidad certificadora

42. Señale la afirmación FALSA:

a) Los procedimientos señalan el marco de actuación en los distintos campos de las TIC para resolver situaciones concretas

b) Deben ser desarrollados por la unidad responsable de su implementación

c) Un ejemplo de procedimiento es la política de seguridad de la organización, que deberá ser conocido por todos los usuarios

d) Los procedimientos deben estar documentados y mantenerse actualizados

43. ¿En cuál de las fases de la planificación de una auditoria informática pueden surgir ciertos problemas por coincidir las fechas de trabajo del personal de la empresa auditora con otros clientes?

a) fase de planificación estratégica

b) fase de planificación administrativa

c) fase de planificación técnica

d) fase de planificación operativa

44. Según las pautas de conducta en el proceso de auditoria, los auditores pueden o deben hacer:

a) escribir los procedimientos

b) realizar gestión de perfiles de usuarios

c) realizar la documentación

d) verificar que se evalúan periódicamente riesgos o bien evaluarlos

45. El código ético definido por ISACA resultará de aplicación a:

a) Solamente a las personas certificadas como CISA y CISM.

b) A los profesionales certificados CISA y CISM y a los miembros de la ISACA.

c) A los miembros de la ISACA, que obligatoriamente serán profesionales con las certificaciones CISA y CISM, en lo que se refiere a la aplicación de las prácticas definidas dentro de COBIT.

d) A todos los profesionales que trabajen realizando auditorías de sistemas de información y que para ello empleen como referencia los manuales del COBIT.

46. 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 Real Decreto 3/2010.

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

47. Las conclusiones que se reflejen en un informe de auditoría deberán estar basadas en una evidencia:

a) Suficiente.

b) Contundente.

c) Prudente.

d) Demostrable.

48. ¿Cómo se llaman a las auditorías especializadas en descubrir fraudes y delitos, en obtener evidencias válidas para su uso por las autoridades competente, policiales o judiciales?

a) Auditorías de regularidad

b) Auditorías operativas o de gestión

c) Auditorías forenses

d) Auditorías de los sistemas de información

49. En una auditoría de comunicaciones al realizar un análisis detallado de los costes operativos, no será relevante considerar:

a) Volumen de datos transmitidos
b) Tiempos de duración de conexión
c) Protocolo de comunicación
d) Facilidades estáticas y dinámicas de conexión

50. El borrador del informe de auditoría se comienza a redactar en la fase de:

a) Planificación de la auditoría
b) Ejecución de la auditoría
c) Comunicación de los resultados
d) Seguimientos de las recomendaciones

51. ¿Cuándo es mejor realizar una auditoría de vulnerabilidades que un test de penetración?

a) Normalmente es necesario ejecutar ambos
b) Cuando buscas una visión más amplia del entorno en lugar de una visión más concreta de un punto
c) Cuando los tests de penetración están llenos de falsos positivos
d) Cuando los tests de penetración pueden, potencialmente, dañar equipos críticos

52. ¿Qué se entiende por control interno?

a) Cualquier actividad automática empleada para prevenir o corregir errores que puedan afectar al funcionamiento de un sistema
b) Cualquier actividad manual empleada para prevenir o corregir errores que puedan afectar al funcionamiento de un sistema
c) Cualquier actividad manual o automática empleada para prevenir o corregir errores que puedan afectar al funcionamiento de un sistema
d) Ninguna de las anteriores

53. En la auditoría de sistemas EFT son las iniciales de:

a) Electronic Fundation Transfer
b) Electronic Fundation Testing
c) Electronic Funds Transfer
d) Electronic Funds Testing

54. Las herramientas que permiten realizar técnicas de auditoría asistidas por ordenador se conocen como:

a) CASEs
b) CAATs
c) CATEs
d) CAdES

55. ¿Cuál de los siguientes no es un órgano especializado en el control de la Administración Pública?

a) Tribunal de Cuentas
b) IGAE
c) Agencia Estatal de Evaluación de Políticas Públicas y de la Calidad de los Servicios
d) Todos lo son

56. El estudio de la información, su calidad, flujo y seguridad es característico de:

a) La auditoría informática
b) La planificación estratégica
c) La planificación de capacidad del sistema
d) Las técnicas de control de proyectos

57. Los auditores que han participado en el desarrollo de un sistema podrían haber perdido su independencia si:

a) Realizan una revisión del desarrollo del sistema

b) Recomiendan medidas de mejora

c) Realizan una evaluación independiente de la aplicación después de su puesta en producción

d) Participan activamente en el diseño e implementación del sistema de aplicación

58. La auditoría de economía, eficacia y eficiencia, o triple E, ha sido bautizada por la United Kingdom Audit Office como:

a) VFN

b) VAN

c) TIR

d) VFM

59. En la auditoría informática se conocen como pruebas sustantivas:

a) Sirven para obtener una comprensión de cuáles son los controles administrativos que están establecidos.

b) Sirven para ver si los controles están bien diseñados y funcionan eficazmente.

c) Se utilizan para determinar si se cumplen los objetivos de salvaguarda de los activos, integridad de los datos, eficacia y eficiencia.

d) Estas pruebas se utilizan para sacar consecuencias del análisis de determinada información.

60. ¿Por qué no puede considerarse cierto que la correcta aplicación y gestión de parches es la solución a la mayoría de los problemas de seguridad?

a) Los parches siempre abren nuevas vulnerabilidades

b) Los parches crean problemas de interoperabilidad

c) Los parches solo tratan los fallos software conocidos

d) Los parches pueden arreglar problemas de mala configuración

61. ¿Cómo se llama a las auditorías informáticas especializadas en descubrir fraudes y delitos, en obtener evidencias válidas para su uso por las autoridades competentes, policiales o judiciales?:

a) Auditorías forenses.

b) Auditorías de regularidad.

c) Auditorías operativas o de gestión.

d) Auditorías de los sistemas de información.

62. El conjunto de las reglas generales que desarrollan las políticas y que son de obligada aplicación se recogen en:

a) Normativas

b) Procedimientos

c) Instrucciones

d) Declaraciones de conformidad

63. ¿Cuál de las siguientes afirmaciones acerca de la auditoría informática es falsa?

a) La finalidad de la auditoría informática es emitir un juicio acerca del estado de los sistemas

b) La auditoría informática llega siempre a una valoración o diagnóstico final, positivo o negativo

c) La auditoría informática propone acciones a realizar

d) La auditoría informática analiza tanto la infraestructura física y lógica como la estructura organizativa

64. Desde el punto de vista de un auditor de seguridad indique cuál de las siguientes premisas, sobre control interno de acceso lógico, es inadecuada:

a) El sistema debe obligar al usuario a cambiar de contraseña cada cierto tiempo

b) El registro o log de acceso al sistema puede desactivarse a petición del responsable de seguridad

c) Es conveniente que la autenticación de entrada al sistema se haga una única vez

d) El sistema debe rechazar el acceso a los usuarios después de una serie de intentos fallidos

65. ¿Qué se entiende por control concomitante?

a) Un control a priori.

b) Un control en paralelo con el proceso.

c) Un control a posteriori.

d) Ninguna de las anteriores.

66. La declaración de intenciones de alto nivel que refleja los objetivos de la organización es la definición de:

a) Normativa

b) Política

c) Instrucción

d) Procedimiento

67. ISACA hace referencia a:

a) A una asociación que promueve un estándar de auditoría y control de los sistemas de información

b) Nada relacionado con la informática

c) Un protocolo de acceso remoto a datos a través de Internet

d) Un organismo internacional de estandarización de sistemas de virtualización de infraestructuras

68. Según la ISACA, una "auditoría de sistemas" se puede definir como:

a) Auditoría que abarca la revisión y evaluación de todos los aspectos de los sistemas automáticos de procesamiento de la información (o una parte de ellos), incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

b) Conjunto de actividades, técnicas, procedimientos y herramientas que nos permiten el control y mejora de los procesos de la organización en el campo de los sistemas de información.

c) ISACA no ha dado una definición de Auditoría porque es una organización sin ánimo de lucro que centra su actividad en la seguridad de los sistemas de información.

d) La auditoría que centra su actividad sobre los sistemas de una organización, incluyendo los sistemas eléctricos, electrónicos e informáticos, aplicando en los controles la normativa europea dictada por los organismos: CEN, CENELEC, EIS y ETSI.

69. Ética del Auditor. Cuatro afirmaciones: -El Auditor sirve con diligencia, lealtad y honradez los intereses de empleados, accionistas, clientes y público en general. No participará en ninguna actividad ilegal o impropia - Garantiza la confidencialidad de la información obtenida en el ejercicio de sus funciones. No la usará en beneficio propio, ni dejará que llegue a terceros. -Evita actividades que pongan en entredicho su independencia. -Fomenta la formación de los directivos de la empresa, sus clientes, incluso del público en general, para que sepan de que va la Auditoría y los Sistemas de Información:

a) Las tres primeras afirmaciones son correctas, la cuarta no

b) Todas son correctas

c) La cuarta es correcta, las otras tres son afirmaciones obvias

d) Son correctas, pero de ellas no se desprende nada práctico

70. La auditoría de sistemas de información se puede considerar como:

a) Una auditoría de eficiencia

b) Una auditoría de eficacia

c) Una auditoría operativa

d) Una auditoría de legalidad

71. Le han encargado realizar una auditoría informática de un centro de proceso de datos en el que, entre otros, se procesan datos fiscales de todas las empresas españolas. Indique que recomendaría solucionar con más urgencia:

a) Las aplicaciones informáticas están insuficientemente documentadas

b) Los equipos no están alimentados con fuentes de alimenta ininterrumpida (U.P.S.)

c) Las copias de seguridad en cinta se guardan junto con las cintas de datos

d) El equipamiento utilizado no responde a la filosofía de 'sistemas abiertos'

72. ¿Cuál de las siguientes no es una de las cinco funciones de la auditoría informática?

a) Velar por la eficacia y eficiencia del sistema informático

b) Verificar el cumplimiento de las normas y estándares vigentes en la organización

c) Verificar la calidad de los sistemas de información, y proponer e implantar mejoras en los mismos

d) Supervisar los mecanismos de control interno

73. ¿Cuál de los siguientes no es un requerimiento general de la labor de un auditor?

a) Proporcionar una garantía razonable de que se alcanzan los objetivos de control

b) Supervisar que la Dirección aborda obligatoriamente las acciones recomendadas

c) Identificar si existen debilidades significativas en los controles

d) Sustanciar el riesgo que puede estar asociado a las debilidades identificadas

74. La auditoría moderna es un proceso metódico y como tal tiene un esquema de progreso común a todos los proyectos. Este esquema se resume en las siguientes cinco fases:

a) Toma de contacto, Revisión, Planificación, Desarrollo de la auditoría y Conclusiones

b) Toma de contacto, Planificación, Revisión, Diagnóstico y Conclusiones

c) Toma de contacto, Planificación, Desarrollo de la auditoría, Diagnóstico y Conclusiones

d) Planificación, Revisión, Desarrollo de la auditoría, Diagnóstico y conclusiones

75. Entre los organismos que recogen buenas prácticas de auditoría no se encuentra:

a) ISACA

b) NIST

c) CNI/CCN

d) IDEA

76. La auditoría es:

a) Actividad que tiene por objeto la evaluación de conformidad de diseños, productos software, procesos o sistema

b) Proceso por el que el sistema de calidad de una empresa es auditado para comprobar el cumplimiento de determinadas normas

c) Descripción completa de un producto software y las interrelaciones de sus elementos

d) Estructura organizativa, procedimientos, actividades y recursos que juntos aseguran que los productos software satisfacen las necesidades implícitas o establecidas en contrato por los clientes

77. Las pruebas de auditoria que permiten medir el riesgo por deficiencia de los controles existentes o por su ausencia se denominan:

a) de cumplimiento
b) de verificación
c) de adecuación
d) sustantivas

78. Generalmente el auditor informático elevará su informe a:

a) La dirección de la Organización
b) La dirección de Informática
c) La dirección del departamento que este auditando
d) Al Departamento de Asuntos Económicos

79. Las auditorías de cumplimiento del Esquema Nacional de Seguridad y de la normativa sobre protección de datos personales:

a) Pueden realizarse a la vez si así se establece en la declaración de alcance.
b) Deben realizarse de manera ordinaria cada dos años, una inmediatamente a continuación de la otra.
c) Deben realizarse de manera ordinaria cada dos años alternando anualmente una y otra.
d) Pueden realizarse conjuntamente sólo cuando tengan carácter extraordinario.

80. ¿Cuál de los siguientes derechos, si es asignado a un operador de ordenador, debería hacer sospechar a un auditor informático, cuando se realiza una auditoría de derechos de acceso?

a) Leer acceso a datos.
b) Borrar acceso a archivos de datos de transacción.
c) Acceso de leer/ejecutar a programas.
d) Actualizar acceso a archivos de lenguaje/script de control de trabajo.

81. ¿Cuál de las siguientes no es una tarea típica de la auditoría informática?

a) Reorganización de los recursos humanos del Departamento de Sistemas de Información
b) Revisión de aplicaciones
c) Revisión de instalaciones informáticas
d) Revisión de sistemas bajo desarrollo

82. En el ámbito de la auditoría de sistemas se denominan hallazgos a:

a) Las tareas orientadas a comprobar que se cumplen determinados procesos de control o procedimientos establecidos.
b) Los criterios, condiciones y efectos que permiten documentar los problemas encontrados.
c) Las tareas que permiten al equipo auditor entender el entorno de los sistemas a auditar.
d) Los métodos aplicados para conseguir el objetivo de la auditoría.

83. ¿Quién debe presentar recomendaciones en una auditoría?

a) El equipo de auditoría
b) La dirección estratégica de la unidad auditada
c) La dirección técnica de la unidad auditada
d) Las entidades certificadoras

84. Los informes de auditoría:

a) Deben ser enviados al órgano auditado para que establezca observaciones o alegaciones

b) No será sometido a las observaciones o alegaciones del órgano auditado porque esto pondría en peligro la independencia del procedimiento

c) Incluirá los hechos, hallazgos, conclusiones y recomendaciones que se consideren más relevantes por parte de los auditores

d) Ninguna de las anteriores es correcta

85. ¿Cuál de las siguientes afirmaciones es falsa?

a) Un control de desarrollo es el que comprueba que el resultado obtenido concuerda con las especificaciones iniciales.

b) Un control de proceso asegura que la explotación se realiza con las versiones adecuadas de los programas y de los datos.

c) Un control de continuación determina que se evita la pérdida o corrupción de información efectuando las salvaguardas y recuperaciones necesarias.

d) Un control de configuración asegura que la explotación se realiza con las versiones adecuadas de los programas y de los datos.

86. Indique cuál de los siguientes es un estándar de auditoría informática:

a) UNE EN ISO/IEC 27020

b) ISACA SI 1002

c) RFC 4253

d) IEEE 802.11a

87. En el transcurso de una auditoría informática, uno de los auditores descubre que existe un incumplimiento grave en un control informático que podría llevar a la realización de un fraude importante por parte de un grupo de empleados, con pérdidas económicas y de imagen para la empresa auditada. El auditor debe:

a) Reunir todas las evidencias de esta deficiencia grave y convocar una reunión urgente con los responsables de la empresa para que conozcan este hecho y puedan tomar medidas preventivas.

b) Contactar al grupo de empleados que pueden cometer el fraude y advertirles de lo descubierto para que no comentan el posible fraude.

c) Reunir todas las pruebas y exponerlas todas juntas en el informe al final de la auditoría, aunque dicho informe se entregue con posterioridad de la posibilidad de realización del fraude, ya que una auditoría no debe interrumpirse por ninguna causa.

d) Llamar a ISACA para informar de que se ha producido una violación del código ético de conducta que se propone en COSO (Marco de Gobierno Corporativo).

88. ¿Cuál de las siguientes es una norma básica en la auditoría de los sistemas de información?

a) Planificación y supervisión

b) Estudio y evaluación del sistema de control interno

c) Obtención de evidencia suficiente y adecuada

d) Todas las anteriores

89. Entre las tareas del auditor no se incluye:

a) Comprender y evaluar la metodología seguida en el proceso de desarrollo

b) Identificar las fases de la metodología de desarrollo

c) Revisar el cumplimiento de estándares y normas de control interno

d) Desarrollar e implantar los cambios necesarios para el cumplimiento con estándares y normas

90. ¿Cuál de las siguientes no es una fase en un proceso de auditoría de la gestión de la seguridad informática de una instalación?

a) Evaluación de la adecuación de los controles establecidos

b) Realización de entrevistas a usuarios

c) Adquisición del conocimiento necesario mediante la identificación y documentación del entorno y de la gestión

d) Ejecución de pruebas sustantivas

91. El proceso de auditoría de sistemas de información se considera como un proceso:

a) Estratégico

b) Operativo

c) Táctico

d) Tecnológico

92. Que afirmación de las siguientes acerca de la auditoria informática NO es correcta:

a) Debe velar por la eficacia y eficiencia del sistema informático.

b) Debe verificar la calidad de los sistemas de información.

c) Debe supervisar los mecanismos de control interno establecidos en los centros de proceso de datos.

d) Debe ser realizada por una empresa externa.

93. La auditoría bienal de cumplimiento de la LOPD y la realización de pruebas de hacking ético tienen las siguientes similitudes y diferencias, marcar la respuesta verdadera:

a) El hacking ético no es una herramienta de auditoría ya que lo realizan los hackers solamente, mientras que la auditoría LOPD lo realizan siempre juristas o personal de perfil TAC.

b) El hacking ético es una técnica para probar los controles de seguridad de las aplicaciones y sirve para que un auditor de seguridad IT pueda encontrar deficiencias. Si la aplicación maneja datos LOPD, la información del estado de estos controles puede servir de apoyo a la auditoría de cumplimiento del reglamento asociado a la LOPD que también debe verificarse en la auditoría bienal, que incluirá tanto aspectos organizativos como técnicos.

c) La Auditoría LOPD es una auditoría IT estrictamente hablando, ya que no debe entrar a valorar aspectos organizativos y procedimentales mientras que el hacking ético entra a valorar los valores éticos de la empresa de cara al tratamiento de la información, en particular los datos de carácter personal.

d) El hacking ético requiere de personal técnico exclusivamente (hackers o no) mientras que la auditoría de cumplimiento de la LOPD sólo debe contar con personal jurista y los responsables funcionales de las aplicaciones LOPD involucradas pero no a técnicos.

94. Cuál de las siguientes puede ser objeto de una 'Auditoría de la Seguridad':

a) Redes de área local

b) Inventario

c) Intercambio de información con el exterior

d) Prácticas comunes de seguridad

95. Según la Guía de Seguridad CCN-STIC-802, ¿cuándo las No Conformidades detectadas en una auditoría pueden causar que el dictamen sea desfavorable?:

a) Cuando el número de No Conformidades mayores sea muy elevado

b) Cuando el número de No Conformidades Mayores y Menores sea muy elevado

c) Cuando exista un número significativo de No Conformidades Mayores cuya solución no pueda evidenciarse a través de un Plan de Acciones Correctivas y requiere la comprobación in-situ de su correcta implantación a través de una auditoría extraordinaria

d) Ninguna de las anteriores es cierta

96. La auditoría informática tiene entre sus normas generales:

a) Exigencia de evidencia

b) Hacer partícipe al usuario

c) Formar parte de la empresa auditada

d) Informar a las autoridades judiciales

97. Uno de los estudios a realizar en la auditoria de la seguridad lógica de los sistemas de información es:

a) La implementación de controles de acceso a las librerías de programas (jerarquía de permisos y privilegios), a los datos, a los sistemas gestores de bases de datos y a los sistemas de comunicaciones.

b) El estado de la documentación de procedimientos de respaldo y recuperación.

c) La clasificación de las dependencias en función de su valor crítico.

d) Los puntos de control para determinar la seguridad operativa frente a caída de líneas, averías.

98. En el contexto de la auditoria informática, el Plan Estratégico de Sistemas de Información se considera un control de tipo:

a) General en el ámbito organizativo.

b) De desarrollo, adquisición y mantenimiento de sistemas de información.

c) De explotación de sistemas de información.

d) Los planes estratégicos de sistemas de información no se consideran controles.

99. Cuál de las siguientes certificaciones profesionales NO pertenecen a ISACA:

a) CISSP

b) CISA

c) CRISC

d) CISM

100. El primer resultado de la fase de Planificación de una auditoria es la enunciación de los objetivos y alcance de la auditoría, que será recogido en un documento formal denominado:

a) Plan de auditoria

b) Informe de auditoria

c) Plan de sistemas

d) Plan estratégico

101. Cuál de los siguientes debe ser el primer paso en una Auditoría de Sistemas:

a) Crear un diagrama de flujo de las ramas de decisión

b) Comprender el entorno a estudiar

c) Realizar una evaluación de riesgos

d) Desarrollar un plan de auditoría

102. En auditoría informática, el objeto de una "prueba de cumplimiento" es:

a) Verificar el cumplimiento de la legislación y la normativa vigente en las operaciones de un sistema de información, especialmente en el capítulo de compras y gestión de personal

b) Sustanciar la probabilidad de que los objetivos de control no se alcancen

c) Determinar si los controles se están aplicando de la forma descrita en la documentación o de la forma descrita por el usuario o directivo

d) Verificar que todos los usuarios se adhieren voluntaria u obligatoriamente a la política sobre usos de recursos informáticos implantada por la Dirección

103. Respecto al contenido del informe de auditoría, indicar cuál de las siguientes recomendaciones es correcta:

a) El informe final de una auditoria sólo contendrá recomendaciones relativas a los incumplimientos o puntos débiles detectados en el área auditada.

b) El informe final incluirá las alegaciones de los auditados, indicando la opinión de los auditores sobre ellas, y si no se incluyen las alegaciones, deberá indicarse el motivo.

c) El informe final de una auditoria operativa debe contener la opinión de los auditores y sugerencias generales sobre cómo aplicar los controles para evaluar el funcionamiento del área auditada.

d) En el informe final de una auditoria operativa se deben señalar las debilidades y fortalezas observadas en relación con los controles implementados en el área auditada.

104. En relación con la auditoría de economía, eficacia y eficiencia, ¿cuál de las siguientes afirmaciones es verdadera?

a) Al contrario de lo que ocurre en el sector privado, en el sector público es muy sencillo realizar comparaciones entre los distintos servicios y administraciones públicas

b) La auditoría de economía consiste en medir los costes de desarrollo, mantenimiento y operación de un sistema de información, incluyendo equipos y personal

c) La auditoría de eficacia es una medida de la correcta utilización de los equipos, instalaciones y personal que participan en el sistema de información. Es una medida de la calidad técnica del sistema de información

d) La eficiencia se evalúa determinando si los requisitos del diseño se han cumplido y los usuarios están satisfechos con el sistema

105. Los procedimientos se detallan técnicamente a través de:

a) Normativas

b) Políticas

c) Indicaciones

d) Ninguna de las anteriores

106. Indique cuál es la denominación de la modalidad de auditoria dirigida a verificar las distintas fases del ciclo de vida del desarrollo de un proyecto:

a) Auditoría de la dirección de tecnologías de la información.

b) Auditoría de equipamiento informático.

c) Auditoría de la contratación de bienes y servicios TIC.

d) Auditoría de los desarrollos y mantenimiento de los sistemas de información.

107. ¿Cuál es el órgano especializado en el control interno y en la evaluación de los servicios de cada uno de los Ministerios y de sus organismos públicos dependientes?

a) La IGAE

b) La Inspección General de los Servicios de cada Ministerio

c) La Inspección General del Ministerio de Hacienda y Administraciones Públicas

d) La Agencia Estatal de Evaluación de Políticas Públicas y de la Calidad de los Servicios

108. En la realización de una auditoría de redes, ¿cuál debe ser la primera etapa?

a) Realizar un análisis de vulnerabilidades.

b) Identificación de la configuración de red física.

c) Reunión inicial de los auditores con el equipo de gestión de redes de la organización.

d) Realizar un análisis de situación revisando la anterior auditoría de seguridad.

109. Cuál de los siguientes enunciados no pertenece al código ético definido para los perfiles de auditor por la ISACA:

a) Apoyar la implantación y estimular el cumplimiento de estándares, procedimientos y controles apropiados en los sistemas de información.

b) Mantener la protección de la intimidad y la confidencialidad de la información a la que se tenga acceso, dentro del marco de la Directiva Europea en materia de protección de datos de carácter personal (transpuesta en España a través de la Ley Orgánica 15/1999).

c) Apoyar la formación profesional de las partes legítimamente interesadas, mejorando su comprensión de la seguridad y control de los sistemas de información.

d) Informar a las partes apropiadas de los resultados del trabajo realizado, revelando todos los hechos significativos que obren en su conocimiento.

110. Los controles preventivos tienen como objeto:

a) Reducir el riesgo ante una debilidad existente

b) Predecir problemas potenciales antes de que ocurran

c) Solucionar problemas detectados por controles detectivos

d) Reportar errores

111. ¿Cuál de los siguientes sería el encuadre orgánico preferible de la auditoria informática interna?

a) Se adscribiría al Departamento de Sistemas de Información, ya que el personal especializado necesario solo esta disponible en ese Departamento.

b) Dependería orgánicamente del Departamento de SI y funcionalmente del Departamento Financiero, por su labor auxiliar en la auditoria financiera de la organización.

c) No debería existir, ya que al ser interna seria imposible que fuera independiente con respecto a los auditados.

d) Se encuadraría dentro del staff, es decir, dentro de los órganos de apoyo a la dirección existentes en la estructura organizativa, con el fin de garantizar la independencia necesaria.

112. ¿Cuál de los siguientes no se considera un motivo para ordenar una auditoría?

a) Para determinar el origen del malfuncionamiento de una aplicación.

b) Para determinar el estado del sistema ante un cambio importante.

c) Para determinar cual es el motivo del malfuncionamiento del sistema.

d) Para determinar si los proyectos transcurren según lo establecido, en cuanto a recursos, objetivos, etc.

113. La auditoría informática es:

a) El estudio de los programas para detectar bucles erróneos

b) La revisión de las operaciones realizadas por los sistemas informáticos de una organización para determinar su correcto funcionamiento

c) La auditoría completa de los accesos indebidos a los sistemas de información e identificación de los causantes

d) La realización de los planes de sistemas de una organización

114. Señale la afirmación verdadera:

a) El modelo organizativo en el que los auditores forman parte de los órganos de control de la organización permite una mayor independencia

b) El modelo organizativo en el que los auditores se integran dentro de los propios centros informáticos permite una mayor independencia

c) El modelo organizativo en el que los auditores se integran dentro de los propios centros informáticos ofrece una implicación más directa en las tareas destinadas a mejorar la calidad

d) La a) y la c) son correctas

115. ¿Qué requisitos son necesarios para obtener y mantener una certificación CISA?

a) Aprobar el examen sobre las materias establecidas por la ISACA

b) La a) y además acreditar una experiencia profesional adecuada

c) La b) y además aceptar un código de ética profesional

d) La c) pero acreditando periódicamente una formación continua

116. El nivel EAL4 de Criterios Comunes significa:

a) Diseñado, probado y revisado metódicamente

b) Estructuralmente probado

c) Probado y verificado metódicamente

d) Diseño verificado y probado formalmente

117. Dentro del marco de la auditoría de sistemas de información, los "controles" en función del momento en que actúan podrían clasificarse en:

a) Proactivos, reactivos, concurrentes y recurrentes.

b) Recurrentes, instantáneos, previos y posteriores.

c) Concomitantes, recurrentes, duraderos e instantáneos.

d) Reactivos, preventivos y concurrentes o concomitantes.

118. ¿Cuál de las siguientes afirmaciones describe mejor el propósito de una auditoría informática de nivel experto?:

a) Evaluar el rendimiento de la infraestructura técnica de una organización.

b) Identificar vulnerabilidades y riesgos de seguridad en los sistemas de información.

c) Revisar la gestión financiera de la empresa en relación con la tecnología.

d) Supervisar el cumplimiento de las políticas de recursos humanos en TI.

119. Entre las funciones de un auditor informático están:

a) Revisión de sistemas bajo desarrollo, instalaciones informáticas y aplicaciones

b) Soporte a auditores no informáticos

c) La a) y la b) son correctas

d) La a) y la b) son incorrectas

120. Una entidad estatal emplea a 3.000 personas (250 en el departamento TIC), gestiona un presupuesto de gastos de 1.000 millones de Euros, tiene una base de datos central de 4.000 millones de registros, y registra un volumen de 45 millones de transacciones anuales. Una autoevaluación de riesgos realizada recientemente ha concluido en la necesidad de establecer una unidad/función de auditoría informática. La ubicación orgánica más adecuada de esta nueva unidad sería:

a) Dentro del Departamento TIC, en dependencia directa del Director de Sistemas de Información.

b) Dentro del Departamento TIC, dependiendo del Administrador Corporativo de Seguridad.

c) Dentro de la Unidad de Auditoría Interna.

d) Dentro de la Secretaría General o unidad de servicios generales.

121. Los controles correctivos tienen como objeto:

a) Reducir el riesgo ante una debilidad existente

b) Predecir problemas potenciales antes de que ocurran

c) Solucionar problemas detectados por controles detectivos

d) Reportar errores

122. En relación con la auditoría informática señalar cuál de las siguientes afirmaciones es falsa:

a) El informe final deberá estar compuesto por las entrevistas en profundidad y datos recopilados durante las fases de revisión y verificación.

b) Se entrevistará al mayor número de usuarios posible.

c) Las entrevistas no tendrán una duración superior a dos horas y media.

d) Para la validación de la carga de trabajo se utilizarán cuestionarios y entrevistas planificadas.

123. Los controles compensatorios tienen como objetivo:

a) Reducir el riesgo ante una debilidad existente

b) Predecir problemas potenciales antes de que ocurran

c) Solucionar problemas detectados por controles detectivos

d) Reportar errores

124. ¿Cuál de las actuaciones siguientes corresponde a una auditoría informática?

a) Recomendar situaciones

b) Planes estratégicos de seguridad

c) Planes de aseguramiento de calidad

d) Reorganización de los recursos humanos del departamento informático

125. Según la Guía de Seguridad CCN-STIC-408, a las pruebas de auditoria para comprobar la correcta aplicación y configuración de contramedidas de seguridad en los dispositivos de información y comunicaciones, para alertar de posibles desviaciones detectadas, se les llama:

a) Pruebas de regresión.

b) Pruebas de trampa (honeypot).

c) Pruebas de penetración o (pentesting).

d) Pruebas de forense.