Test Tema 82 #1

Actualizado el 13/04/2025

1. Algunas de las ventajas a la hora de utilizar software general para la realización de las auditorías son:

a) Economicidad

b) Coste inicial alto

c) No se verifican procesos particulares sino genéricos

d) Todas las respuestas anteriores son incorrectas

2. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público:

a) notificarán sin dilaciones indebidas dicha violación a la AEPD

b) notificarán en el plazo de 36h dicha violación a la AEPD

c) notificarán sin dilaciones indebidas dicha violación a la AEPD y también al abonado si pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular

d) notificarán en el plazo de 36h dicha violación a la AEPD y también al abonado si pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular

3. En el RGPD Reglamento (UE) 2016/679:

a) hay artículos sobre la obligatoriedad de la realización de auditorías periódicas

b) hay artículos sobre la obligatoriedad y la periodicidad de la realización de auditorías periódicas

c) a y b son correctas

d) a y b son incorrectas

4. Señale cuál no es una herramienta de auditoría:

a) SAS

b) WinAudit

c) MNAP

d) ACL

5. La notificación de una brecha de seguridad en un sistema de información a la Agencia Española de Protección de Datos (AEPD) debe realizarla:

a) El responsable de seguridad.

b) El delegado de protección de datos.

c) El responsable del tratamiento de datos.

d) -

6. En el trabajo de auditor:

a) Se distinguen de forma general tres etapas

b) Una de las etapas se denomina proceso, donde se realiza el análisis cuantitativo y cualitativo de la información recabada

c) A y B son correctas

d) A y B son incorrectas

7. El Reglamento Europeo de Protección de Datos 2016/679, indica (señale la incorrecta):

a) se debe realizar siempre una evaluación de impacto al modificar significativamente una aplicación

b) se debe realizar siempre un análisis de riesgos al modificar significativamente una aplicación

c) se deben tomar medidas para garantizar la confidencialidad

d) se deben tomar medidas de manera propocionada

8. El proceso que consiste en la conversión de datos personales en datos que no se pueden utilizar para identificar a ningún individuo se denomina:

a) Anonimización.

b) Cifrado.

c) Reidentificación.

d) Categorización.

9. Un tipo de software libre que lleva al cabo una auditoría de todo el software y hardware que se encuentra en una red de una manera sencilla, además de eficiente es:

a) MAPILab Reports:

b) Network Inventory Advisor

c) Visual audit. X4

d) Todas las respuestas anteriores son correctas

10. En la herramienta PILAR, los activos esenciales son:

a) La información, los servicios ofrecidos por los sistemas y los equipos hardware o de comunicaciones que los soportan.

b) La información, las personas que manejan los sistemas y los servicios que proporcionan los sistemas.

c) La información y los servicios manejados por los sistemas.

d) -

11. Sobre las actividades de tratamiento de datos personales:

a) se registran para analizar su riesgo

b) se almancenan en un fichero

c) nunca requieren consentimiento

d) es gestionada por el delegado de protección de datos

12. Según la nueva Ley Orgánica 3/2018, LOPDGDD, en lo relativo al tratamiento de datos personales en relación con la notificación de incidentes de seguridad:

a) Las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes.

b) Las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

c) Las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes.

d) Las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

13. En los pliegos de contratación:

a) se deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos, según el Real Decreto-ley 14/2019.

b) no se pueden mencionar la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos, según el Real Decreto-ley 14/2019.

c) se deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos, según el Real Decreto-ley 17/2019.

d) no se pueden mencionar la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos, según el Real Decreto-ley 17/2019.

14. El tipo de control de acceso a usuarios que establece que todo recurso del sistema tiene una etiqueta de seguridad compuesta por el nivel de seguridad y el recurso al que se quiere acceder, se denomina:

a) DAC

b) RBAC

c) MAC

d) Ninguno de los anteriores

15. Según la nueva Ley Orgánica 3/2018, LOPDGDD en lo relativo a las medidas de seguridad en el Sector Público:

a) En caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado el Esquema Nacional de Seguridad (ENS) incluirá las medidas que sean necesarias, sin necesidad de tener en cuenta nada más.

b) En caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado, se requerirá informe del CCN-CERT y de la AEPD quienes determinarán las medidas que sean necesarias.

c) En caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado el Esquema Nacional de Seguridad (ENS) incluirá las medidas que sean necesarias, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el RGPD.

d) En caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado, se requerirá únicamente de un informe del CCN-CERT para determinar las medidas que sean necesarias.

16. ¿La notificación de una brecha de seguridad en un sistema de información a la AEPD la realiza?

a) El Delegado de Protección de Datos de la organización

b) El jefe de área de Seguridad de la organización

c) El responsable del tratamiento de datos personales de la organización

d) El encargado del tratamiento de datos personales de la organización

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

a) proponer medidas correctivas o complementarias.

b) abstenerse de proponer medidas correctivas.

c) identificar a los causantes de las deficiencias.

d) remitirse a la Agencia Española de Protección de Datos.

18. El responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas:

a) estadísticas, técnicas y organizativas apropiadas

b) estadísticas, tácticas y organizativas apropiadas

c) técnicas y organizativas apropiadas

d) estadísticas, técnicas, tácticas y organizativas apropiadas

19. ¿Cuál de las siguientes respuestas NO es obligatoria para adaptarse al RGPD?:

a) Obligación de informar al ciudadano sobre el tratamiento de los datos personales.

b) Designar un Delegado de Protección de Datos en los supuestos contemplados en la normativa de protección de datos.

c) Mantener un registro de actividades de tratamiento en el que se detalle quien trata los datos, finalidad y base jurídica.

d) Que los administradores de las BB.DD estén certificados por la AEPD.

20. El RGPD incorpora el concepto:

a) compliance, siempre tiene que estar reflejado en la auditoría el nivel de cumplimiento respecto a derechos de protección de datos

b) accountability', siempre tiene que haber una rendición de cuentas de las organizaciones respecto a las medidas relativas protección de datos

c) avalability, siempre tiene que estar disponible para la autoridad de control la última auditoria de datos realizada

d) avalability, siempre tiene que estar disponible para el delegado de protección de datos la última auditoria de datos realizada

21. La norma ISO/IEC 27002 es un conjunto de controles de seguridad para sistemas de información genéricos. Esta norma está relacionada con el Esquema Nacional de Seguridad (ENS). Señale la opción INCORRECTA:

a) Numerosas medidas de seguridad del ENS coinciden con controles de ISO/IEC 27002.

b) El ENS es más preciso que la norma ISO/IEC 27002 y establece un sistema de protección proporcionado a la información y servicios a proteger para racionalizar la implantación de medidas de seguridad y reducir la discrecionalidad.

c) La norma ISO/IEC 27002 carece de la proporcionalidad del ENS, quedando a la mejor opinión del auditor que certifica la conformidad con ISO/IEC 27001. La certificación de la conformidad con ISO/IEC 27001 no es obligatoria en el ENS.

d) Tanto la norma ISO/IEC 27002 como el ENS contemplan diversos aspectos relativos a la firma o la autenticación electrónica.

22. Una de las siguientes condiciones no es suficiente para que un tratamiento de datos personales sea lícito según el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (RGPD):

a) El tratamiento es necesario para la ejecución de un contrato sea el interesado parte de él o no.

b) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

c) El tratamiento es necesario para el cumplimiento de una obligación legal del responsable.

d) -

23. Sobre las herramientas de análisis de riesgos, señale la opción correcta:

a) Permite hacer una clasificación inicial por sector (sanidad, crédito, telecomunicaciones, etc…)

b) Análisis previo de detección de datos de alto nivel de riesgo de tratamiento

c) Detección de si las condiciones son válidas para la utilización de la herramienta Facilita

d) Todas las anteriores

24. La realización de la auditoría, dentro de las medidas de seguridad de nivel medio, de acuerdo al RD 1720/2007 debe llevarse a cabo:

a) Por personal externo

b) Por personal interno a la organización

c) Por profesionales en materia de protección de datos

d) Todas las respuestas anteriores son incorrectas

25. ¿Cuál de las herramientas de la AEPD (Agencia Española de Protección de Datos) está diseñada para el análisis de necesidad de una Evaluación de Impacto en Protección de Datos?:

a) Facilita RGPD.

b) Comunica-Brecha RGPD.

c) Gestiona RGPD.

d) Evalua-Riesgo RGPD.

26. Según la nueva Ley Orgánica 3/2018, LOPDGDD recoge como obligación general de los responsables y encargados del tratamiento de datos:

a) Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la ley orgánica 3/2018, sus normas de desarrollo y la legislación sectorial aplicable, y valorarán si procede la realización de la evaluación de impacto en la protección de datos.

b) Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la ley orgánica 3/2018, sus normas de desarrollo y la legislación sectorial aplicable, sin necesidad de tener que valorar si procede realizar una evaluación de impacto en la protección de datos.

c) Los responsables, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la ley orgánica 3/2018, sus normas de desarrollo y la legislación sectorial aplicable, y valorarán si procede la realización de la evaluación de impacto en la protección de datos.

d) Los encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la ley orgánica 3/2018, sus normas de desarrollo y la legislación sectorial aplicable, sin necesidad de tener que valorar si procede realizar una evaluación de impacto en la protección de datos.

27. ¿Qué artículo de la Ley Orgánica 3/2018, LOPDGDD, define los supuestos en que puede considerarse que se producen mayores riesgos para la protección de datos?

a) La LOPDGDD no define supuestos. Los supuestos hay que tomarlos del Esquema Nacional de Seguridad.

b) En el artículo 28 de la LOPDGDD.

c) En el artículo 17 de la LOPDGDD.

d) La LOPDGDD no define supuestos. Los supuestos hay que tomarlos delas recomendaciones de las recomendaciones de la AEPD.

28. En cuanto al acceso a datos personales a través de redes de comunicaciones:

a) Debe llevarse a cabo a través de técnicas de cifrado

b) Deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local

c) Debe permitir el registro de todos los accesos a los datos, guardando, hora, fecha, usuario y fichero accedido

d) Todas las respuestas anteriores son correctas

29. Señale cuál es una herramienta de cifrado:

a) TCE, Transparent Content Encryption

b) TDE, Transparent Data Encryption

c) TKE, Transparent Key Encryption

d) TSE, Transparent Server Encryption

30. Señale la respuesta correcta, respecto assirgpd:

a) Es un herramienta de destinada a AA.PP para facilitar el cumplimiento del RGPD y gestión de los tratamientos de datos personales

b) Es una herramienta comercial para realizar auditorias de protección de datos segun el RGPD

c) Es un herramienta de auditoria open source relativo a protección de datos segun el RGPD

d) Es un herramienta de destinado a AA.PP para facilitar el cumplimiento del RGPD sin incluir análisis de riesgos

31. ¿Indique cuáles son herramientas para comprobación del cumplimiento de la normativa vigente de protección de datos?

a) LUCIA, PILAR, InformaRGPD

b) PILAR, FacilitaRGPD

c) PILAR, FacilitaRGPD, InformaRGPD

d) LUCIA, PILAR, FacilitaRGPD, InformaRGPD

32. Las medidas para el cumplimiento de RGPD y LOPDGDD, se basan en:

a) las guías CCN-STIC y FacilitaRGPD

b) el ENS y FacilitaRGPD

c) las guías CCN-STIC y el ENS

d) FacilitaRGPD y las guías CCN-STIC

33. ¿Cuál no es software relativo a protección de datos?

a) Data Privacy Solution

b) PrivateLOPD

c) Privacy Driver

d) Pridatec

34. La protección de datos desde el diseño y por defecto debe tener en cuenta:

a) El estado de la organización

b) El estado de la técnica

c) El coste de la auditoría

d) La duración del tratamiento

35. ¿Cuál de las siguientes respuestas es CORRECTA referente a las auditorías que se plantean en el RGPD?:

a) Hay obligación de realizar auditorías periódicas preventivas según dispone el RGPD.

b) Solo se tendrán que realizar auditorías cuando lo exija la AEPD.

c) Pueden realizarse auditorías de cumplimiento a decisión de la organización sin que las haya solicitado la AEPD.

d) Las auditorías del RGPD tienen que ser siempre realizadas por un auditor certificado.