TEMA 1

1) Análisis forense trata de saber
- **a.** Quién, cuándo, cómo y por qué se produjo un incidente de seguridad.
- **b.** Quién, cuándo, a qué hora, cómo y por qué se produjo un incidente de seguridad.
- **c.** Quién, cuándo, dónde, cómo y por qué se produjo un incidente de seguridad.
- **d.** Quién, dónde, cómo, en qué sitio y por qué se produjo un incidente de seguridad.

2) La cadena de custodia de una evidencia digital garantiza
- **a.** Confidencialidad, autenticidad, disponibilidad, repetitividad, trazabilidad e integridad de la evidencia.
- **b.** Confidencialidad, autenticidad, veracidad, disponibilidad, trazabilidad e integridad de la evidencia.
- **c.** Confidencialidad, completitud, autenticidad, disponibilidad e integridad de la evidencia.
- **d.** Confidencialidad, autenticidad e integridad de la evidencia.

3) Principio de intercambio de Locard:
- **a.** Cuando dos objetos entran en contacto solo uno transfiere material que incorpora al otro.
- **b.** Cuando dos objetos entran en contacto siempre transfieren material que incorporan al otro.
- **c.** Se puede obtener el estado de un sistema sin alterarlo.
- **d.** No se puede obtener el estado de un sistema sin alterarlo.

4) Según el principio de Locard, al detectar un incidente de seguridad es conveniente:
- **a.** Las respuestas b y c son correctas.
- **b.** Realizar un apagado lógico y físico de los equipos involucrados.
- **c.** Realizar muchas operaciones antes de decidir si se realiza un duplicado forense.
- **d.** Realizar pocas operaciones antes de decidir si se realiza un duplicado forense.

5) Principio de indeterminación de Heisenberg:
- **a.** Cuando dos objetos entran en contacto solo uno transfiere material que incorpora al otro.
- **b.** Cuando dos objetos entran en contacto siempre transfieren material que incorporan al otro.
- **c.** Se puede obtener el estado de un sistema sin alterarlo.
- **d.** No se puede obtener el estado de un sistema sin alterarlo.

6) Cómo auditor forense constato una conexión de origen no conocida en el fichero de conexiones del ordenador comprometido
   - **a.** Aplica el principio de Locard.
   - **b.** Aplica el principio de indeterminación de Heisenberg.
   - **c.** Las repuestas A y B son correctas siempre que analice una copia del disco del ordenador comprometido.
   - **d.** Las respuestas A y B son correctas.

7) Cómo auditor forense ejecuto PMPDUMP-LIST en el ordenador comprometido
   - **a.** Aplica el principio de Locard.
   - **b.** Aplica el principio de indeterminación de Heisenberg.
   - **c.** Las repuestas A y B son correctas siempre que analice una copia del disco del ordenador comprometido.
   - **d.** Las respuestas A y B son correctas.

8) Cuándo un administrador detecta un incidente relacionado con el robo de información debe proceder inmediatamente a:
   - **a.** Notificar el incidente y observar el atacante.
   - **b.** Cambiar las contraseñas de los usuarios administradores.
   - **c.** Apagar el equipo cortafuegos.
   - **d.** Apagar el equipo cortafuegos.

9) Las evidencias constatadas en un disco vienen de una volatilidad menor que las evidencias constatadas en la memoria principal:
   - **a.** Verdad.
   - **b.** Si el disco está configurado en RAID-5: Verdad.
   - **c.** Falso.
   - **d.** Si la memoria principal tiene un mecanismo de corrección de errores basada en paridad: Falso.

10) Todas las evidencias digitales siguientes tienen una naturaleza volátil:
   - **a.** Procesos de ejecución, conexiones abiertas y puertos, información del portapapeles y usuarios conectados local o remotamente.
   - **b.** Procesos en ejecución, conexiones abiertas y puertos, información del portapapeles y metadatos.
   - **c.** Procesos en ejecución, conexiones abiertas y puertos, información del portapapeles y ficheros ocultos.
   - **d.** Entradas en logs del sistema, conexiones abiertas y puertos, información del portapapeles y usuarios conectados local o remotamente.

11) Todas las evidencias digitales siguientes tienen una naturaleza persistente:
   - **a.** Entradas en logs del sistema, ficheros modificados o accedidos, procesos en ejecución, ejecutables camuflados y ficheros ocultos.
   - **b.** Entradas en logs del sistema, ficheros modificados o accedidos, metadatos, ejecutables camuflados y conexiones abiertas y puertos.
   - **c.** Entradas en logs del sistema, ficheros modificados o accedidos, metadatos, información del portapapeles y ficheros ocultos.
   - **d.** Entradas en logs del sistema, ficheros modificados o accedidos, metadatos, ejecutables camuflados y ficheros ocultos.

12) La integridad de una evidencia digital se puede garantizar:

- **a.** Comprobando que el hash obtenido con un algoritmo de cifrado de la evidencia en la fase de adquisición coincide con el de la fase de análisis.
- **b.** Comprobando que el hash MD5 de la evidencia en la fase de adquisición coincide con el de la fase de análisis.
- **c.** Comprobando que el hash MD5 de la evidencia en la fase de evaluación coincide con el de la fase de análisis.
- **d.** Comprobando que el hash MD5 de la evidencia en la fase de adquisición coincide con el de la fase información.

13) Un proceso de análisis forense sigue la secuencia de fases siguiente:

- **a.** Informar, evaluar, adquirir y analizar.
- **b.** Adquirir, analizar, evaluar e informar.
- **c.** Evaluar, analizar, adquirir e informar.
- **d.** Evaluar, adquirir, analizar e informar.

14) La integridad de una evidencia digital se puede garantizar:

- **a.** Comprobando que el hash obtenido con un algoritmo de cifrado de la evidencia en la fase de adquisición coincide con el de la fase de análisis.
- **b.** Comprobando que el hash MD5 de la evidencia en la fase de adquisición coincide con el de la fase de análisis.
- **c.** Comprobando que el hash MD5 de la evidencia en la fase de evaluación coincide con el de la fase de análisis.
- **d.** Comprobando que el hash MD5 de la evidencia en la fase de adquisición coincide con el de la fase información.

15) Respecto a PMDUMP y STRING:

- **a.** PMDUMP se utiliza en la fase de generación informe de evidencias y STRING en la fase de análisis.
- **b.** PMDUMP se utiliza en la fase de adquisición de evidencias y STRING en la fase de generación de informe.
- **c.** PMDUMP se utiliza en la fase de adquisición de evidencias y STRING en la fase de análisis.
- **d.** PMDUMP se utiliza en la fase de análisis de evidencias y STRING en la fase de adquisición.

16) Me despierto en clase y están hablando de ficheros de los o bitácora y del principio de:

- **a.** Heisenberg.
- **b.** Locard.
- **c.** Locard y Heisenberg.
- **d.** Heisenberg y quizás Locard.

17) En el análisis forense la ISO/IEC 27037 aplica a los subprocesos
- **a.** Evaluar, adquirir las evidencias e informar.
- **b.** Evaluar y adquirir las evidencias.
- **c.** Evaluar, adquirir y analizar las evidencias.
- **d.** Analizar e interpretas las evidencias.

18) En el análisis forense la ISO/IEC 27042 aplica a:
- **a.** Evaluar, adquirir las evidencias e informar.
- **b.** Evaluar y adquirir evidencias.
- **c.** Evaluar, adquirir y analizar las evidencias.
- **d.** Analizar e interpretar las evidencias.

19) En un análisis forense el rol Digital Evidence Specialist (DES) tiene asignadas las funciones de:
- **a.** Un perito digital menos la de analizar evidencias digitales.
- **b.** Un perito digital menos la de adquirir evidencias digitales.
- **c.** Adquirir y analizar.
- **d.** Un perito digital menos la de adquirir y analizar evidencias digitales.

20) En un análisis forense el rol "Digital Evidence First Responder (DEFR)" está:
- **a.** Autorizado, formado y habilitado para actuar en la escena de un incidente y así evaluar el escenario y adquirir las evidencias digitales con las debidas garantías.
- **b.** Un perito digital menos la de adquirir evidencias digitales.
- **c.** Adquirir y analizar evidencias digitales.
- **d.** Autorizado, formado y habilitado para actuar en la escena del incidente y así evaluar el escenario.

21) FOCA está orientado a:
- **a.** Adquisición de evidencias.
- **b.** Análisis de metadatos y adquisición de evidencias digitales.
- **c.** Análisis de metadatos.
- **d.** Duplicado forense.

22) PMDUMP es una herramienta orientada a:
- **a.** Adquisición de evidencias digitales no volátiles de un ordenador.
- **b.** Análisis de evidencias digitales no volátiles de un ordenador.
- **c.** Adquisición de evidencias digitales volátiles de un ordenador.
- **d.** Análisis de evidencias digitales volátiles de un ordenador.

23) Según el principio de Locard:
- **a.** No se puede obtener el estado de un sistema sin alterarlo.
- **b.** Es recomendable realizar pocas operaciones antes de decidir si se realiza un duplicado forense.
- **c.** El mero hecho de medir altera la magnitud medida.
- **d.** Se puede obtener el estado de un sistema sin alterarlo.

24) Según la ISO/IEC 27037, los principios que gobiernan la evidencia digital son:

- **a.** Relevancia y suficiencia de las evidencias y confiabilidad del proceso de análisis forense.
- **b.** Relevancia de las evidencias y confiabilidad del proceso de análisis forense.
- **c.** Suficiencia de las evidencias y confiabilidad del proceso de análisis forense.
- **d.** Relevancia y suficiencia de las evidencias, confiabilidad del proceso de análisis forense y disponibilidad del perito forense.

25) Autopsy es una herramienta orientada a:

- **a.** Adquirir evidencias.
- **b.** Analizar evidencias.
- **c.** Adquirir y analizar evidencias.
- **d.** Adquirir, generar copias forenses y analizar evidencias.

26) La ejecución de "netstat –an" está relacionada con:

- **a.** La adquisición de evidencias no volátiles.
- **b.** La adquisición de evidencias volátiles.
- **c.** El análisis de evidencias no volátiles.
- **d.** El análisis de evidencias volátiles.

27) La ejecución de "netstat –r" no está relacionada con:

- **a.** La adquisición de evidencias no volátiles.
- **b.** La adquisición de evidencias volátiles.
- **c.** El análisis de evidencias volátiles.
- **d.** La a y la c son correctas.

28) EndCase Imager es una herramienta orientada a:

- **a.** La adquisición de evidencias no volátiles.
- **b.** La adquisición de evidencias volátiles.
- **c.** La adquisición de evidencias volátiles y no volátiles.
- **d.** La generación del informe.

29) Me despierto en clase y están hablando de las cadenas de proxy Tor y del principio de:

- **a.** Heisenberg.
- **b.** Locard.
- **c.** Locard y ¿?
- **d.** Heisenberg y Locard.

30) Respecto a MD5:

- **a.** MD5 es un algoritmo para obtener un hash o resumen digital. Se utiliza en relación con la trazabilidad de la evidencia digital.
- **b.** MD5 es un algoritmo para cifrar una evidencia digital. Se utiliza en relación con la trazabilidad de la evidencia digital.
- **c.** MD5 es un algoritmo para cifrar una evidencia digital. Se utiliza en relación con la integridad de la evidencia digital.
- **d.** MD5 es un algoritmo para obtener un hash o resumen digital. Se utiliza en relación con la integridad de la evidencia digital.

31) Respecto a SHA-256:

- **a.** SHA-256 es un algoritmo para obtener un hash o resumen digital. Se utiliza en relación con la integridad de la evidencia digital.
- **b.** SHA-256 es un algoritmo para obtener un hash o resumen digital. Se utiliza en relación con la trazabilidad de la evidencia digital.
- **c.** SHA-256 es un algoritmo para cifrar una evidencia digital. Se utiliza en relación con la trazabilidad de la evidencia digital.
- **d.** SHA-256 es un algoritmo para cifrar una evidencia digital. Se utiliza en relación con la integridad de la evidencia digital.

32) La firma electrónica digital avanzada es el conjunto de datos en forma electrónica, consignados junto a otros asociados con ellos

- **a.** que pueden ser utilizados como medio de identificación del firmante y para detectar cambios en los datos del firmante.
- **b.** que puede ser utilizados como medio de identificación del firmante y pueden detectar cambios en los datos del firmante.
- **c.** que pueden ser utilizados como medio de identificación del firmante y para detectar cambios en los datos firmados.
- **d.** que pueden ser utilizados como medio de identificación del firmante y para detectar cambios en los datos del firmante.

33) Se considera firma electrónica reconocida a la firma electrónica:

- **a.** Avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- **b.** Basada en un certificado reconocido y generada mediante un dispositivo de creación de firma.
- **c.** Avanzada basada en el certificado y generada mediante un dispositivo seguro de creación de firma.
- **d.** Avanzada basada en un certificado reconocido y generada mediante un dispositivo de creación de firma.

34) La pregunta "¿Se conoce la tasa de error de las herramientas forenses informáticas utilizadas?" está relacionada con la propiedad de la evidencia digital:

- **a.** Relevancia.
- **b.** Suficiencia.
- **c.** Confiabilidad.
- **d.** Pertinente.

35) La pregunta "¿La evidencia recolectada valida un indicio de clave que permita esclarecer los hechos en un estudio?" está relacionada con la propiedad de la evidencia digital:

- **a.** Relevancia.
- **b.** Suficiencia.
- **c.** Confiabilidad.
- **d.** Pertinente.

36) La pregunta “¿Se ha analizado todos los elementos informáticos identificados en la escena del crimen?” está relacionado con la propiedad de la evidencia digital:

- **a.** Relevancia.
- **b.** Suficiencia.
- **c.** Confiabilidad.
- **d.** Pertinente.

37) Un analista forense puede utilizar la herramienta EnCase Imager en lugar de PMDUMP:

- **a.** Sí.
- **b.** No.
- **c.** Solo para copiar unidades de disco.
- **d.** Solo para copiar la memoria RAM completa.

TEMA 2

1) La LOPD se aplica a:
- **a.** Personas físicas y jurídicas.
- **b.** Personas físicas.
- **c.** Personas jurídicas.
- **d.** Personas físicas y a los DCP de las personas fallecidas.

2) Si una organización trata los DCP solo con recursos internos:
- **a.** El responsable del fichero actúa como encargado del tratamiento.
- **b.** No se aplica la LOPD.
- **c.** El responsable de seguridad actúa como encargado del tratamiento.
- **d.** No existe la figura del encargado de tratamiento.

3) El sistema NOTA es una herramienta de la AEPD que sirve para:
- **a.** Obtener un informe basado en las respuestas transmitidas por un RF o RS a preguntas relacionadas con el reglamento de medidas de seguridad de LOPD.
- **b.** Obtener un informe basado en las respuestas transmitidas por un RF a preguntas relacionadas con la adaptación legal a la LOPD.
- **c.** Obtener un nivel de madurez entre 0 y 5 sobre la adaptación de una organización a la LOPD.
- **d.** Realizar notificaciones electrónicas a la AEPD relacionadas con la inscripción de ficheros con datos de carácter personal.

4) Entre los principios por el RF con los DCP se encuentran:
- **a.** Deben de ser exactos y no es necesario que estén actualizados.
- **b.** Se recogen con fines indeterminados.
- **c.** Se conservan sólo durante el tiempo necesario para las finalidades del tratamiento para el que se han recogido.
- **d.** Se pueden conservar una vez finalizado el tratamiento para el que se han recogido.

5) Entre los principios ARCO de la LOPD se encuentran:
- **a.** Acceso, rectificación, cancelación y oposición.
- **b.** Acceso, recuperación, cancelación y oposición.
- **c.** Acceso, rectificación, conocimiento y oposición.
- **d.** Aplicación, rectificación, cancelación y oposición.

6) Las medidas de seguridad recogidas en el RDLOPD pueden ser de:
- **a.** Nivel bajo, medio o alto.
- **b.** Nivel básico, mediano o alto.
- **c.** Nivel básico, medio o alto.
- **d.** Nivel básico, medio o crítico.

7) Los DCP relacionados con infracciones administrativas o penales, con temas financieros o relacionados con la personalidad o comportamiento son de nivel:
- **a.** Básico.
- **b.** Medio.
- **c.** Alto.
- **d.** Bajo.

8) Los DCP relacionados con nombre y apellidos o datos de contacto (dirección, teléfono, email, etc.) son de nivel:
- **a.** Básico.
- **b.** Medio.
- **c.** Alto.
- **d.** Bajo.

9) Los DCP relacionados con ideología, religión y creencias, salud y vida sexual, afiliación sindical o violencia de género son de nivel:
- **a.** Básico.
- **b.** Medio.
- **c.** Alto.
- **d.** Bajo.

10) La existencia de un RS es obligatoria si:
- **a.** Hay DCP de nivel sólo básico.
- **b.** Hay DCP de nivel básico, medio y alto.
- **c.** Hay DCP.
- **d.** No hay DCP.

11) Un auditor comprobará si hay un registro de acceso a los DCP si éstos son:
- **a.** De nivel medio.
- **b.** De nivel básico y/o medio.
- **c.** De nivel básico, medio y alto.
- **d.** De nivel medio o relacionados con nombre y apellidos o datos de contacto (dirección, teléfono, email, etc…).

12) Un auditor comprobará si se limita el número de accesos (identificación y autenticación) a los DCP si éstos son:
- **a.** De nivel básico.
- **b.** De nivel básico y/o medio.
- **c.** De nivel básico o relacionados con nombre y apellidos o datos de contacto (dirección, teléfono, email, etc…).
- **d.** Ninguna de las anteriores.

13) Un auditor comprobará si se almacenan copias de seguridad en ubicación alternativaa donde se tratan los datos si los DCP son:
- **a.** De nivel medio.
- **b.** De nivel básico y/o medio.
- **c.** Sobre ideología.
- **d.** De nivel medio.

14) Las comunicaciones con DCP se cifrarán si:

- **a.** Se transmiten DCP por redes púbicas o inalámbricas.
- **b.** Se transmiten DCP de nivel básico por redes públicas o inalámbricas.
- **c.** Se transmiten DCP de nivel medio por redes públicas o inalámbricas.
- **d.** Se transmiten DCP relacionados con ideología, religión y creencias, salud y vida sexual, afiliación sindical o violencia de género por redes públicas o inalámbricas.

15) La auditoría del RDLOPD es obligatoria si:

- **a.** Los DCP son de nivel medio y/o alto.
- **b.** Los DCP son de nivel básico.
- **c.** Los DCP son de nivel bajo y medio.
- **d.** Los DCP son de nivel básico, pero no de nivel medio.

16) El auditor de LOPD puede utilizar:

- **a.** La ISO/IEC 27001 como referente y la ISO 19011 como guía en el proceso de auditoría.
- **b.** La ISO 19011 como referente y la LOPD y su RDLOPD como guías en el proceso de auditoría.
- **c.** La LOPD y su RDLOPD como referentes y la ISO/IEC 27001 como guía en el proceso de auditoría.
- **d.** La LOPD y su RDLOPD como referentes y la ISO 19011 como guía en proceso de auditoría.

17) En una auditoría LOPD un auditor constata un listado de ficheros donde algunos pueden ser temporales debido a su nombre y a que su fecha de creación es de 2010.

- **a.** Es una evidencia, pero no constituye un hallazgo.
- **b.** Es un hallazgo, pero no constituye una evidencia.
- **c.** Es una evidencia y constituye un hallazgo.
- **d.** No es una evidencia, pero si constituye un hallazgo.

18) En una auditoría LOPD un auditor constata que el DS no está aprobado por la dirección:

- **a.** Es una evidencia y constituye un hallazgo.
- **b.** Es un hallazgo, pero no constituye una evidencia.
- **c.** Es una evidencia, pero no constituye un hallazgo.
- **d.** No es una evidencia, pero si constituye un hallazgo.

19) En una auditoría LOPD un auditor constata que el RF dispone de una relación de hace 16 meses donde figuran los usuarios con acceso autorizado y perfiles:

- **a.** Es un hallazgo, pero no constituye una evidencia.
- **b.** Es una evidencia, y constituye un hallazgo, pero no es necesario recomendar medidas correctoras ya que la relación está actualizada.
- **c.** Es una evidencia, constituye un hallazgo y recomienda que se genere la relación con una mayor frecuencia.
- **d.** Es una evidencia, no constituye un hallazgo y recomienda que se genere la relación con mayor frecuencia.

20) En una auditoría LOPD un auditor constata que las contraseñas se cifran con un algoritmo propietario basado en el cifrado de Julio Cesar 4.

- **a.** Es un hallazgo y constituye una evidencia.
- **b.** Es una evidencia, constituye un hallazgo y recomienda que se sustituya el algoritmo del cifrado.
- **c.** Es una evidencia, no constituye un hallazgo y recomienda que se sustituya el algoritmo de cifrado.
- **d.** Es una evidencia, constituye un hallazgo y recomienda que se mantenga el algoritmo de cifrado.

21) En una auditoría LOPD un auditor constata que no se dispone de registro de acceso, aunque el RF es la única persona que accede a los DCP:

- **a.** Es una evidencia, constituye un hallazgo y recomienda que se implemente un registro de acceso.
- **b.** Es una evidencia, constituye un hallazgo y no recomienda que se implemente un registro de acceso.
- **c.** Es un hallazgo y constituye una evidencia.
- **d.** Es una evidencia y constituye un hallazgo.

22) En una auditoría LOPD un auditor constata que el departamento de RRHH escanea los informes médicos y almacena los PDF correspondientes en una memoria USB. ¿Qué pregunta haría como auditor al responsable del departamento?

- **a.** ¿Desde cuándo?
- **b.** ¿Cuántos informes?
- **c.** ¿Se cifran?
- **d.** ¿Cuántos GB tiene la memoria USB?

23) En una auditoría LOPD un auditor constata que las imágenes de las maras de vídeo vigilancia se visualizan, pero no se graban:

- **a.** Es una evidencia, constituye un hallazgo y recomienda que se graben.
- **b.** El RF no está obligado a garantizar los derechos de ARCO.
- **c.** Es una evidencia, constituye un hallazgo y recomienda que se inscriba el fichero correspondiente en la AEPD.
- **d.** No es necesario comprobar si están dados de alta los ficheros correspondientes en la AEPD.

24) En una auditoría LOPD un auditor constata que se han instalado varias cámaras falsas en las entradas del edificio y no se ha registrado en el fichero correspondienteen la AEPD:

- **a.** No es necesario comprobar si están dados de alta los ficheros correspondientes en la EPD y el RF no está obligado a garantizar los derechos ARCO.
- **b.** El RF no está obligado a garantizar los derechos ARCO.
- **c.** Es una evidencia, constituye un hallazgo y recomienda que se inscriba el fichero correspondiente en la AEPD:
- **d.** Es una evidencia, constituye un hallazgo y recomienda que se graben.

TEMA 3

1) La calidad del software depende de la calidad de los siguientes elementos:
- **a.** El proceso de desarrollo software, el proyecto, el equipo y el producto software.
- **b.** El proceso de explotación del software, las herramientas, el equipo y el producto software.
- **c.** El proceso de desarrollo software, el proyecto y el producto software.
- **d.** El proceso de pruebas del software, el equipo y el producto software.

2) El proceso de desarrollo software se puede implementar según el referente:
- **a.** ISO/IEC 15504.
- **b.** Familia ISO/IEC 25000.
- **c.** ISO/IEC 27001.
- **d.** ISO/IEC 12207.

3) Un auditor puede evaluar la capacidad de los procesos de la ISO/IEC 12207 utilizando:
- **a.** ISO/IEC 15504.
- b. ISO 19011.
- c. ISO/IEC 14598.
- d. Familia ISO/IEC 25000.

4) El modelo de la calidad de los procesos software según la ISO está formado por:
- **a.** CCMDI-DEV e ISO/IEC 15504.
- **b.** ISO/IEC 12207, ISO/IEC 15504 y CCMI-DEV.
- **c.** ISO/IEC 12207 e ISO/IEC 15504.
- **d.** ISO/IEC 12207 e ISO/IEC 27001.

5) Respecto a la ISO/IEC 12207:
- **a.** Especifica que procesos hay que implementar en un proceso de desarrollo de software.
- **b.** Especifica cómo hay que implementar los procesos de desarrollo software.
- **c.** Especifica cómo se evalúan los procesos de desarrollo software.
- **d.** Especifica cómo se evalúa la calidad del producto software.

6) Si un auditor ha definido que una factoría software está en nivel de madurez 1, ha revisado los siguientes procesos:

- **a.** De un suministro de gestión del modelo de ciclo de vida y gestión de la configuración software.
- **b.** De un suministro, de planificación del proyecto y gestión de la configuración software.
- **c.** De suministro, de gestión del modelo de ciclo de vida y gestión de la configuración software.
- **d.** De aseguramiento de la calidad, de gestión del modelo de ciclo de vida y gestión de la configuración software.

7) Si un auditor ha definido que una organización de desarrollo software está en el nivel de madurez 2, ha comprobado que la capacidad de los procesos correspondientes es:

- **a.** Al menos dos para la mitad de los mismos.
- **b.** Al menos dos para los más importantes.
- **c.** Dos.
- **d.** Uno para la cuarta parte, dos para la mitad y tres para la cuarta parte.

8) Un auditor concluirá que un proceso de la ISO/IEC 12207 alcanza el nivel de capacidad 1 si constata que:

- **a.** Se generan los "outcomes" o resultados del proceso según la ISO/IEC 15504.
- **b.** Se generan los "outcomes" o resultados del proceso según la ISO/IEC 12207.
- **c.** Se generan los "outcomes" o resultados del proceso según la ISO/IEC 14598.
- **d.** Se generan al menos la mitad de los "outcomes" o resultados del proceso según la ISO/IEC 12207.

9) Una certificación de la calidad de los procesos software (una evaluación CMMI por ejemplo):

- **a.** Siempre asegura un producto de calidad software.
- **b.** No tiene relación con un producto de calidad de software.
- **c.** No existe el concepto de certificación de la calidad de los procesos software.
- **d.** No siempre asegura un producto de calidad de software.

10) SPICE es el método para realizar auditorías de procesos de desarrollo software relacionado con:

- **a.** ISO/IEC 12207.
- **b.** CMMI-DEV.
- **c.** SQUARE.
- **d.** ISO/IEC 9126.

11) SCAMPI es el método para realizar auditorías de procesos de desarrollo software relacionado con:

- **a.** ISO/IEC 12207.
- **b.** CMMI-DEV.
- **c.** SPICE.
- **d.** ISO/IEC 9126.

12) CMMI-DEV es similar a:

- **a.** ISO/IEC 15504.
- **b.** ISO/IEC 9126.
- **c.** ISO/IEC 12207.
- **d.** ISO/IEC 14598.

13) En una auditoría de proceso software un auditor AENOR utiliza los siguientes estándares:

- **a.** ISO 19011, ISO/IEC 9126 e ISO/IEC 15504.
- **b.** ISO 19011, ISO/IEC 12207 y CMMI-DEV.
- c. ISO 19011, ISO/IEC 12207 e ISO/IEC 14598.
- d. ISO 19011, ISO/IEC 12207 e ISO/IEC 15504.

14) En relación con el proceso de desarrollo software, la ISO/IEC 12207 especifica:

- **a.** Cómo se debe hacer (metodología) y lo que se debe hacer.
- **b.** Lo que se debe hacer.
- **c.** Cómo se evalúa la capacidad de los procesos que describe.
- **d.** Cómo se debe hacer (metodología).

15) Tras auditar el proceso de desarrollo software una factoría software, el auditor asigna:

- **a.** Un nivel de capacidad a la factoría y un nivel de madurez a los procesos auditados.
- **b.** Un nivel de capacidad a la factoría.
- **c.** Un nivel de madurez a la factoría.
- **d.** Un nivel de madurez a la factoría y un nivel de madurez a los procesos auditados.

16) Para que un proceso de la ISO/IEC 12207 alcance el nivel de capacidad 2:

- **a.** No es necesario que se generen todos los “outcomes” o resultados del proceso según la ISO/IEC 12207.
- **b.** Es necesario que se generen al menos la mitad de los “outcomes” o resultados del proceso según la ISO/IEC 12207.
- **c.** Es necesario que se generen todos los “outcomes” o resultados del proceso según la ISO/IEC 15504.
- **d.** Es necesario que se generen todos los “outcomes” o resultados del proceso según la ISO/IEC 12207.

17) Si el auditor constata que los 3 procesos del nivel de madurez 1 y los 7 niveles de madurez 2 alcanzan el nivel de capacidad 2 puede concluir que:

- **a.** La organización auditada se encuentra en un nivel de capacidad 2 y en un nivel de madurez 2.
- **b.** La organización auditada se encuentra en un nivel de madurez 2.
- **c.** La organización auditada se encuentra en un nivel de capacidad 2 para los 3 procesos del nivel de madurez 1 y los 7 procesos del nivel de madurez 2.
- **d.** La organización auditada se encuentra en un nivel de capacidad 2.

18) Las evidencias directas en una auditoría SPICE pueden ser:

- **a.** El propio producto que se obtiene de un "outcome" o un AP.
- **b.** Correos, actas de reunión, planes, hitos, fechas, etc.
- **c.** El propio producto que se obtiene de un "outcome".
- **d.** El propio producto que se obtiene de un "outcome" o un PA.

19) Las evidencias indirectas de una auditoría SPICE pueden ser:

- **a.** El propio producto que se obtiene de un "outcome" o un AP.
- **b.** Correos, actas de reunión, planes, hitos, fechas, etc.
- **c.** Correos, actas de reunión, planes, hitos, "outcomes", etc.
- **d.** Correos, AP, PA, planes, hitos, fechas, etc.

20) Las evidencias de tipo afirmaciones en una auditoría se pueden obtener en:

- **a.** Entrevistas con distintos actores de la organización y en "outcomes".
- **b.** Entrevistas con distintos actores de la organización auditada y en evidencias indirectas.
- **c.** Entrevistas con distintos actores de la organización auditada y en correos.
- **d.** Entrevistas con distintos actores de la organización.

21) ¿Qué estándar ha adoptado ISACA para evaluar los procesos de COBIT 5?

- **a.** ISO/IEC 15504.
- **b.** ISO/IEC 12207.
- **c.** CMMI-DEV.
- **d.** ISO/IEC 14598.

Tema 4

1) ¿Quién está interesado en evaluar la calidad?
   a. Organismos o empresas que adquieren productos software y organismos o empresas que externalizan total o parcialmente su proceso de desarrollo software.
   b. Factorías y empresas desarrolladoras de software y organismos o empresas que externalizan total o parcialmente su proceso de desarrollo software.
   c. Factorías y empresas desarrolladoras de software, organismos o empresas certificadoras de calidad ambiental y organismos o empresas que externalizan total o parcialmente su proceso de desarrollo software.
   d. Factorías y empresas desarrolladoras de software, organismos o empresas que adquieren productos software y organismos o empresas que externalizan total o parcialmente su proceso de desarrollo software.

2) Factorías y empresas desarrolladoras de software, ¿están interesadas en evaluar la calidad de su software?
   a. No, porque hoy los clientes compran software basándose exclusivamente en el precio.
   b. Sí, porque así venden más.
   c. …
   d. …

3) La deuda técnica hace referencia a:
   a. Consecuencias y costes en que incurre una empresa por externalizar software con debilidades.
   b. Consecuencias y costes en que incurre una empresa por comprar software con debilidades.
   c. Consecuencias y costes en que incurre una empresa por desarrollar software con debilidades.
   d. Consecuencias y costes en que incurre una empresa por desarrollar software sin debilidades.

4) La deuda técnica no intencionada viene dada por:
   a. Código de baja calidad por un programador junior o asumir un equipo de baja calidad o adquisición de una empresa con deuda técnica.
   b. Código de baja calidad por un programador junior o de adquisición de una empresa con deuda técnica.
   c. Código de baja calidad por un programador junior, o adquisición de una empresa con deuda técnica o presión de fechas <<Time to market>>.
   d. Código de baja calidad por un programador junior o asumir un equipo de baja calidad.

5) La deuda técnica intencionada viene dada por:

a. Código de baja calidad por un programador junior o asumir un equipo de baja calidad.
b. Código de baja calidad por un programador junior o subprocesos de desarrollo de baja calidad o presión de fechas <<Time to market>> o pruebas y testing pobres.
c. Subprocesos de desarrollo de baja calidad o presión de fechas <<Time to market>> o adquisición de una empresa con deuda técnica.
d. Subprocesos de desarrollo de baja calidad o presión de fechas <<Time to market>> o pruebas y testing pobres.

6) La deuda técnica es:

a. Es visible y genera valores negativos.
b. Es invisible y genera valores negativos.
c. Es visible y genera valores positivos.
d. Es invisible y genera valores positivos.

7) Las características según el modelo de calidad del producto software recogidas en la ISO/IEC 9126 son:

a. Funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.
b. Funcionalidad, fiabilidad, usabilidad, confidencialidad, mantenibilidad y portabilidad.
c. Funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y trazabilidad.
d. Racionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.

8) Según el modelo de calidad del producto software de la ISO/IEC 9126 las métricas internas:

a. Son aplicables a la utilización del software por parte de los usuarios.
b. Son aplicables el software en ejecución.
c. No dependen de la ejecución del software y son, por lo tanto, medidas estáticas.
d. No dependen de la ejecución del software y son, por tanto, medidas dinámicas.

9) Según el modelo de calidad del producto software de la ISO/IEC 9126 las métricas externas:

a. Son aplicables a la utilización del software por parte de los usuarios.
b. Son aplicables al software en ejecución.
c. No dependen de la ejecución del software y son, por lo tanto, medidas estáticas.
d. Son aplicables al software en ejecución y la utilización del software por parte de los usuarios.

10) Según el modelo de calidad del producto software de la ISO/IEC 9126 las métricas en uso:

a. Son aplicables a la utilización del software por parte de los usuarios.
b. Son aplicables al software en ejecución.
c. No dependen de la ejecución de software y son, por lo tanto, medidas estáticas.
d. Son aplicables a la utilización del software por parte de los usuarios y no es necesario que el software esté en ejecución.

11) La ISO/IEC 14598 es un marco de trabajo para:

a. Evaluar la calidad de los procesos de desarrollo software.
b. Evaluar la calidad de los productos de software.
c. Evaluar la calidad de los productos de software y de los procesos de desarrollo software.
d. Definir un modelo de calidad del producto software.

12) El referente que usara un auditor para evaluar la calidad de un producto software es:

a. ISO/IEC 25000.
b. ISO/IEC 14598.
c. ISO/IEC 15504.
d. ISO/IEC 19011.

13) En una auditoría de producto software un auditor de AENOR utiliza los siguientes estándares:

a. ISO/IEC 19011, ISO/IEC 9126 e ISO/IEC 27001.
b. ISO/IEC 15504, ISO/IEC 9126 e ISO/IEC 14598.
c. ISO/IEC 19011, ISO/IEC 9000 e ISO/IEC 14598.
d. ISO/IEC 19011, ISO/IEC 9126 e ISO/IEC 14598.

14) La calidad del producto software se puede interpretar como:

a. El grado en que dicho producto satisface los requisitos del CEO y CIO aportando de esta manera un valor.
b. El grado en que dicho producto satisface los requisitos de sus desarrolladores aportando de esta manera un valor.
c. El grado en que dicho producto satisface los requisitos de sus usuarios aportando de esta manera un valor.
d. El grado en que dicho producto satisface los requisitos de sus usuarios.

15) La ISO/IEC 25000 hereda la característica de calidad de la ISO/IEC 9126 y añade:

a. Compatibilidad y seguridad.
b. Compatibilidad, usabilidad y seguridad.
c. Compatibilidad, portabilidad y seguridad.
d. Compatibilidad, seguridad y adecuación funcional.

16) En el marco de la ISO/IEC 25000 la interoperabilidad es una subcaracterística de:

a. La fiabilidad.
b. La seguridad.
c. La mantenibilidad.
d. La compatibilidad.

17) En el marco de la ISO/IEC 25000 la reusabilidad es una subcaracterística de:

a. La mantenibilidad.
b. La seguridad.
c. La fiabilidad.
d. La compatibilidad.

18) En el marco de la ISO/IEC 25000 la mantenibilidad es:

a. La capacidad del producto software para ser modificado debido a necesidades evolutivas, correctivas o perfectivas.
b. La capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidad evolutivas, correctivas o perfectivas.
c. La capacidad del producto software para ser probado efectiva y eficientemente, debido a necesidad evolutivas, correctivas o perfectivas.
d. Capacidad de dos o más sistemas o componentes para intercambiar información y/o llevar a cabo sus funciones requeridas cuando comparten el mismo entorno hardware o software.

19) En el marco de la ISO/IEC 25000 la compatibilidad es:

a. La capacidad del producto software para ser modificado debido a necesidades evolutivas, correctivas o perfectivas.
b. La capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidad evolutivas, correctivas o perfectivas.
c. La capacidad del producto software para ser probado efectiva y eficientemente, debido a necesidad evolutivas, correctivas o perfectivas.
d. Capacidad de dos o más sistemas o componentes para intercambiar información y/o llevar a cabo sus funciones requeridas cuando comparten el mismo entorno hardware o software.

20) En el marco de la ISO/IEC 25000 la complejidad ciclomática está relacionada con:

a. La seguridad.
b. La compatibilidad y mantenibilidad.
c. La mantenibilidad.
d. La usabilidad y la compatibilidad.

21) En el marco de la ISO/IEC 25000 la complejidad ciclomática está relacionada con:

a. Esfuerzo necesario para poder probar todos los caminos en un código fuente.
b. Esfuerzo necesario para poder probar todos los bucles en un código fuente.
c. Esfuerzo necesario para poder probar todas las funciones en un código fuente.
d. Esfuerzo necesario para poder probar todas las estructuras condicionalidades en un código fuente.

22) En el marco de la ISO/IEC 25000 la complejidad ciclomática se define como:

a. v(G) = e – n + 2, donde n representa el número de aristas y e el número de nodos.
b. v(G) = e – n + 2, donde e representa el número de líneas del código que no son comentarios y n el número de líneas de comentarios.
c. v(G) = e – n + 2, donde e representa el número de nodos y n el número de aristas.
d. v(G) = e – n + 2, donde e representa el número de aristas y n el número de nodos.

23) Según Tomas McCabe un valor de complejidad ciclomática mayor de 20 implica un riesgo:

a. Alto o altísimo en la capacidad de ser analizado un código fuente.
b. Moderado en la capacidad de ser analizado un código fuente.
c. Alto en la capacidad de ser analizado un código fuente.
d. Despreciable en la capacidad de ser analizado un código fuente.

24) Según Tomas McCabe un valor de complejidad ciclomática mayor de 50 implica un riesgo:

a. Alto o altísimo en la capacidad de ser analizado un código fuente.
b. Moderado en la capacidad de ser analizado un código fuente.
c. Altísimo en la capacidad de ser analizado un código fuente.
d. Despreciable en la capacidad de ser analizado un código fuente.

25) En el marco de la ISO/IEC 25000 la densidad de código repetido indica la relación entre la cantidad de:

a. Comentarios de un producto y su tamaño (sin incluir comentarios).
b. Código repetido de un producto y su tamaño (sin contar comentarios).
c. Código repetido de un producto y su tamaño (contando comentarios).
d. Comentarios de un producto y su tamaño (obviamente, incluyendo comentarios).

26) En el marco de la ISO/IEC 25000 la densidad de comentarios indica la relación entrela cantidad de:

a. Comentarios de un producto y su tamaño (sin incluir comentarios).
b. Código repetido de un producto y su tamaño (sin contar comentarios).
c. Código repetido de un producto y su tamaño (contando comentarios).
d. Comentarios de un producto y su tamaño (obviamente, incluyendo comentarios).

27) En el marco de la ISO/IEC 25000 la accesibilidad es una dimensión de la:

a. Usabilidad.
b. La mantenibilidad.
c. La seguridad.
d. La complejidad ciclomática

28) Para evaluar el nivel de accesibilidad de una aplicación web, un auditor usará como referente:

a. La UNE 139803:2012 de ENAC.
b. La UNE 139803:2012 de ISO.
c. La UNE 139803:2012 de AENOR.
d. La UNE 139803:2012 de BSI.

29) Según la UNE 139803:2012 los niveles de conformidad respecto a la accesibilidad de una aplicación web son:

a. A, AA, AAA y AAAA.
b. A, AA y AAA.
c. A y AAA.
d. A, BB y CCC.

30) Respecto a una aplicación web, TAWDIS es un test para evaluar su nivel de conformidad respecto a la:

a. Usabilidad.
b. Mantenibilidad.
c. Accesibilidad.
d. Modularidad.