Osakidetza



TÉCNICO/A INFORMÁTICA

PREGUNTAS

1. **De los siguientes ordenadores personales, ¿cuál fue el que logró un éxito realmente notable en el mercado?**

   a) El PC Wozniak.
   b) IBM PC.
   c) Motorola PC 68K.
   d) Zilog Z c80.

2. **¿Qué material se emplea para fabricar un microprocesador?**

   a) Aluminio.
   b) Galenio.
   c) Silicio.
   d) Todas las anteriores son correctas.

3. **¿Qué son FPM y BEDO?**

   a) Tipos de memoria RAM.
   b) Tipos de zócalo para microprocesador.
   c) Ranuras de memoria.
   d) Tipos de disco duro.

4. **Seleccione la afirmación correcta acerca de los sistemas de firmware BIOS y UEFI utilizados en las placas base modernas:**

   a) Tipos de firmware que están incorporados en un chip de la placa base.
   b) Se encargan de arrancar el PC y de dar soporte para manejar ciertos dispositivos de entrada/salida.
   c) Ofrecen una interfaz gráfica para configurar parámetros básicos.
   d) Todas las anteriores son correctas.

5. **¿Qué dispositivo del ordenador realiza el procesamiento necesario para representar gráficos en pantalla?**

   a) La CPU.
   b) La GPU.
   c) La TFPU.
   d) NINGUNA de las anteriores es correcta.



6. ¿Qué se entiende por "resolución" de una pantalla?

a) La relación entre el tamaño horizontal y el tamaño vertical de la pantalla.
b) El número de pulgadas que hay en la diagonal de la pantalla.
c) El número de puntos individuales (pixel) que puede representar el monitor en forma de puntos horizontales por puntos verticales.
d) NINGUNA de las anteriores es correcta.

7. ¿Qué son SATA, SAS y PCIe?

a) Conectores de discos duros.
b) Interfaces de almacenamiento internas.
c) Ranuras de extensión para los discos duros.
d) Buses de datos.

8. ¿Qué tecnología realiza una grabación magnética asistida por calor?

a) HAMR.
b) SMR.
c) PMR.
d) HGST.

9. ¿Cuál de los siguientes se considera un formato de tarjeta de memoria?

a) SDHC.
b) QFast.
c) XQD.
d) La a) y c) son correctas.

10. ¿Cuáles de estos componentes incluyen los netbooks?

a) Sistemas operativos Chrome OS o Windows 10.
b) Microprocesadores sencillos, tipo atom, Celeron o algún ARM, pero mejorados y de hasta 4 núcleos.
c) Pantallas de como mínimo 11.6 pulgadas, LED y resolución "HD Ready" al menos.
d) Todas las anteriores son correctas.

11. ¿De qué se encarga la ALU?

a) Se encarga de ejecutar numerosos cálculos, como los realizados sobre números enteros o las operaciones lógicas.
b) Se encarga de realizar operaciones con números flotantes, así como de otras operaciones como la división de enteros.
c) Es el camino para los datos, que comunican las diversas partes del microprocesador.
d) De ella depende el tamaño máximo de memoria que puede manejar el microprocesador.



12. ¿Qué es la velocidad de acceso a memoria (ns)?

a) Es el número que expresa la velocidad de reloj del bus máximo que puede soportar de forma fiable.
b) Es el tiempo mínimo para realizar un ciclo mínimo de acceso a la memoria.
c) Es el tiempo de latencia, retraso o retardo en el acceso a memoria.
d) Es la máxima cantidad de memoria que podría trasladarse por segundo.

13. ¿Cuáles son los tipos de ranuras de memoria más comunes hoy en día?

a) FM2+ y LGA.
b) DIMM y SO-DIMM.
c) DDR2 y DDR3.
d) DIMM y DD2.

14. ¿Qué es la frecuencia de refresco en pantalla?

a) La memoria dedicada exclusivamente al uso de la GPU.
b) El número de colores que pueden representarse.
c) El número de veces que puede dibujarse la pantalla por segundo.
d) NINGUNA de las anteriores es correcta.

15. ¿Cuál de estas afirmaciones NO es una ventaja de las pantallas OLED/AMOLED?

a) Excelentes ángulos de visión.
b) Bajo consumo.
c) Fabricación costosa.
d) Elevado refresco y tiempo de respuesta.

16. ¿Con cuál de estas formas podría implementarse un sistema tipo RAID?

a) RAID software.
b) RAID hardware.
c) RAID firmware.
d) Todas las anteriores son correctas.

17. ¿Cuál de estas afirmaciones sobre los discos duros SSD es correcta?

a) El nivel de ruido de un disco SSD es muy elevado.
b) Un disco SSD tiene alta resistencia a impactos y vibraciones.
c) No es resistente a las condiciones climatológicas adversas.
d) Si no existe fragmentación los discos duros de alta velocidad de rotaciones son más rápidos que los discos duros SSD.



18. ¿Cuál de estos medios utiliza la tecnología del almacenamiento óptico?

a) MicroSD.
b) CD.
c) eSATA.
d) Disquete.

19. ¿En qué generación el tipo de sistema operativo era por procesamiento por lotes o batch?

a) 2º Generación.
b) 3º Generación.
c) 4º Generación.
d) 5º Generación.

20. ¿Cuál de los siguientes sistemas operativos es multiusuario y multitarea?

a) CTSS.
b) OS/360.
c) UNIX.
d) EXEC II.

21. ¿En qué tipos de sistemas operativos se utiliza la técnica que se conoce como tiempo compartido (*time sharing*)?

a) Sistemas operativos monousuario.
b) Sistemas operativos en tiempo real.
c) Sistemas operativos multiprogramación.
d) Sistemas operativos interactivos.

22. Si en un superordenador se instala un sistema operativo monotarea…

a) Ejecutará más de un proceso cada vez.
b) Solo ejecutará un proceso cada vez.
c) Dividirá en diferentes hebras (threads) el proceso.
d) Seleccionará los demás procesos para distribuir el trabajo.

23. ¿En qué tipos de sistemas el equipo informático NO comparte recursos?

a) En los sistemas centralizados.
b) En los sistemas en red.
c) En los sistemas distribuidos.
d) NINGUNA de las anteriores es correcta.



24. ¿En cuántos niveles se dividía el sistema operativo THE (Technische Hogeschool Eindhoven)?

a) En 4 niveles: del 0 al 3.
b) En 4 niveles: del 1 al 4.
c) En 5 niveles: del 0 al 4.
d) En 6 niveles: del 0 al 5.

25. ¿Qué son los procesos de usuario/a?

a) Son los procesos que generalmente se ejecutan al iniciar el sistema.
b) Son los procesos que manda ejecutar el/la usuario/a que entre en el sistema.
c) Son los procesos que el sistema operativo ejecuta en segundo plano.
d) Son los procesos que cada usuario necesita para un correcto funcionamiento del sistema operativo.

26. ¿Cómo se ejecutan los procesos en el algoritmo FIFO (first input first output)?

a) Los procesos se ejecutan en orden de llegada. El primero que llega empieza a ejecutar.
b) Se ejecuta el proceso más corto de los que están esperando para ejecutar la CPU.
c) El proceso se ejecuta en orden de prioridad de cada proceso.
d) Este algoritmo va dando tiempo de ejecución a cada proceso que esté en espera.

27. La técnica de gestión de memoria principal del sistema operativo por particionamiento …

a) Consiste en particionar la memoria en particiones de tamaño fijo o particiones de tamaño variable.
b) Solamente se pueden particionar a tamaño fijo.
c) Sirve para ejecutar programas que no están cargados totalmente en memoria.
d) Protege la zona de memoria asignada a cada proceso.

28. ¿Qué sistema de archivos son soportados por la mayoría de distribuciones de linux?

a) NTFS.
b) FAT32.
c) EXT2, EXT3, EXT4.
d) HFS.

29. ¿Cuál es la diferencia fundamental entre el modelo OSI y TCP/IP?

a) OSI tiene 4 capas prácticas; TCP/IP tiene 7 teóricas.
b) OSI es modelo teórico de referencia con 7 capas; TCP/IP es práctico de implementación con 4 capas.
c) TCP/IP define solo 3 capas físicas; OSI define 7 lógicas.
d) OSI se usa solo en LAN; TCP/IP en WAN.



30. Analizando las ventajas del uso de redes, la compartición de recursos software y de datos implica un cambio significativo en la gestión administrativa frente a sistemas aislados. ¿Cuál de los siguientes efectos es una consecuencia directa y positiva de esta centralización en un entorno LAN?

a) La eliminación total de la necesidad de realizar copias de seguridad debido a la redundancia del medio.
b) La capacidad de administrar centralizadamente los recursos compartidos. Lo que permite mantener la integridad de los datos mediante mecanismos de control de acceso y asegurar la coherencia de versiones de software mediante actualizaciones desplegadas desde el servidor.
c) El aumento exponencial del tráfico de red independientemente del número de personas usuarias que accedan al recurso.
d) La necesidad de replicar manualmente los archivos de datos en cada estación de trabajo para garantizar su disponibilidad, incrementando la probabilidad de inconsistencias y duplicidad de información.

31. En una red con tecnología de transmisión por difusión (broadcast), ¿qué característica es definitoria?

a) Cada enlace conecta exclusivamente dos nodos punto a punto.
b) Un único canal de comunicación es compartido por todos los dispositivos.
c) Requiere obligatoriamente conmutación de circuitos.
d) Solo permite transmisión en modo full-dúplex.

32. ¿Qué topología física de red ofrece mayor tolerancia a fallos en un enlace individual?

a) Topología en bus.
b) Topología en estrella.
c) Topología en anillo.
d) Topología en malla.

33. ¿Qué estándar IEEE 802 define específicamente la tecnología Ethernet para redes cableadas?

a) IEEE 802.11
b) IEEE 802.5
c) IEEE 802.3
d) IEEE 802.4

34. En transmisión de datos, ¿qué relación existe entre ancho de banda y velocidad de transmisión?

a) Son conceptos idénticos y completamente sinónimos.
b) La velocidad de transmisión determina el ancho de banda disponible.
c) No guardan relación directa en medios de transmisión digitales.
d) El ancho de banda limita la velocidad máxima teórica de transmisión.



35. ¿Qué medio de transmisión ofrece mayor inmunidad a interferencias electromagnéticas y permite mayores distancias sin necesidad de repetidores?

a) Par trenzado UTP Categoría 6.
b) Cable coaxial RG-6.
c) Fibra óptica monomodo.
d) Medio inalámbrico en banda de 5 GHz.

36. ¿Qué protocolo del nivel de internet en TCP/IP se encarga de la resolución de direcciones IP a direcciones MAC en una red local?

a) ICMP (Internet Control Message Protocol).
b) UDP (User Datagram Protocol).
c) ARP (Address Resolution Protocol).
d) DNS (Domain Name System).

37. ¿Cuál es la forma más comprimida posible de la siguiente dirección IPv6? 2001:db8:0:0:0:1:2:3

a) 2001:db8::1:2:3
b) 2001:db8:0::0:1:2:3
c) 2001:db8:0:0::1:2:3
d) 2001:db8:::1:2:3

38. ¿Qué dispositivo de interconexión opera principalmente en el nivel físico y repite la señal a todos sus puertos sin filtrar tramas?

a) Switch (conmutador).
b) Router (encaminador).
c) Hub (concentrador).
d) Bridge (puente).

39. Se tiene la dirección IPv4 192.168.10.0/26. ¿Cuál de las siguientes afirmaciones es correcta respecto a esta subred?

a) El rango de hosts va de 192.168.10.0 a 192.168.10.63.
b) La dirección de broadcast es 192.168.10.63.
c) Se pueden crear 64 subredes a partir de esta máscara.
d) Cada subred tiene 128 hosts utilizables.

40. Se tiene la dirección IPv4 10.20.30.0/27. ¿Cuál de las siguientes afirmaciones es correcta?

a) Cada subred tiene 32 direcciones totales y 30 hosts utilizables.
b) La dirección de broadcast de la primera subred es 10.20.30.32.
c) La segunda subred comienza en 10.20.30.33.
d) La máscara de subred es 255.255.255.128.



41. En la configuración básica de un router para interconectar redes, ¿qué tabla es esencial para la toma de decisiones de encaminamiento?

a) Tabla ARP (Address Resolution Protocol).
b) Tabla de conmutación MAC.
c) Tabla de enrutamiento (routing table).
d) Tabla de sesiones TCP activas.

42. ¿Cuál es la razón técnica principal por la que Zigbee resulta especialmente adecuado para despliegues IoT con gran número de dispositivos distribuidos?

a) Porque ofrece altas velocidades de transmisión comparables a Wi-Fi.
b) Porque combina bajo consumo energético, topologías en malla y buena escalabilidad.
c) Porque requiere infraestructuras cableadas dedicadas.
d) Porque está diseñado exclusivamente para comunicaciones multimedia.

43. ¿Qué características comparten los tres tipos de conexiones (M2M, M2P y P2P) que existen entre los elementos IoT?

a) Solo pueden iniciarse desde una máquina.
b) Solo pueden iniciarse desde una persona.
c) Son unidireccionales.
d) Son bidireccionales y cualquiera de los elementos puede iniciar la comunicación.

44. ¿Qué ocurre cuando evoluciona de forma drástica un elemento de una capa del modelo OSI?

a) Todas las demás capas deben modificarse para adaptarse.
b) Las capas inferiores dejan de funcionar.
c) Las demás capas no necesitan conocer el cambio ni modificar su comportamiento.
d) Se altera la estructura completa del modelo.

45. ¿Qué combinación de características explica la creciente adopción de Bluetooth Low Energy (BLE) en aplicaciones IoT?

a) Conexión punto a punto y transmisión de vídeo y audio en tiempo real.
b) Incorporación de topologías Broadcast y Mesh junto con mayor distancia de comunicación en la versión 5.
c) Uso de cableado estructurado y dependencia de infraestructura física dedicada.
d) Mayor velocidad de transferencia que WiFi y compatibilidad exclusiva con redes metropolitanas.



46. Un sensor instalado en los neumáticos de un vehículo mide de forma constante la presión y transmite automáticamente ese valor al panel de control del automóvil para su supervisión. ¿Qué tipo de comunicación representa este caso?

a) Comunicación P2P (persona a persona).
b) Comunicación M2P (máquina a persona).
c) Comunicación M2M (máquina a máquina).
d) Comunicación WAN (red de área amplia).

47. ¿Qué situación NO es un ejemplo de comunicación P2P (persona a persona)?

a) Telemetría.
b) Redes Sociales.
c) Servicios de salud.
d) Call centers.

48. ¿Cuál es la diferencia más importante entre las etiquetas RFID activas y pasivas?

a) Las activas requieren que lector y etiqueta se "vean", mientras que las pasivas NO.
b) Las activas NO disponen de fuente de alimentación, mientras que las pasivas SÍ.
c) La diferencia más importante es el uso de una fuente de energía.
d) Las pasivas permiten mayores distancias de lectura que las activas.

49. ¿Qué estándar de Ethernet permite transmisión a 10 Gbps exclusivamente en full dúplex utilizando par trenzado (UTP) (Cat5e, 6 o 7) con una distancia máxima de 100 metros?

a) 1000BaseSX.
b) 10GBaseT.
c) 10GBaseSR.
d) 100BaseTX.

50. ¿Cuáles son los cuatro elementos que permiten que el Internet de todo (Internet of Everything (IoE)) se convierta en una realidad?

a) Dispositivos, redes, protocolos y servicios.
b) Objetos, datos, procesos y personas.
c) Sensores, actuadores, nube y aplicaciones.
d) Hardware, software, conectividad y seguridad.

51. ¿Qué combinación de características describe correctamente a LoRaWAN?

a) Utiliza frecuencias por debajo de 1 GHz, permite alcances de hasta 20 km y está orientada a bajo consumo energético.
b) Opera por encima de 2,4 GHz, ofrece altas tasas de Mbps y está orientada a comunicaciones de corto alcance.
c) Funciona exclusivamente en entornos urbanos, con alcances máximos de 2 km y alto consumo de energía.



d) Requiere licencia propietaria y ofrece velocidades comparables a WiFi.

52. ¿Cuál de las siguientes opciones NO corresponde a una necesidad típicamente cubierta por las tecnologías NFC y RFID?

a) Sistemas de prepago con tarjeta en transporte público.
b) Control de acceso mediante tarjetas de identificación.
c) Logística y transporte.
d) Redes de área amplia para comunicaciones de largo alcance.

53. Si pensamos en el riego automático del césped de un jardín, ¿cuál es la secuencia correcta del flujo de funcionamiento de un sistema IoT?

a) El actuador analiza los datos → el sensor decide la acción → el sistema central ejecuta la orden.
b) El actuador mide la humedad → el sensor ejecuta la acción → el sistema central almacena los datos.
c) El sistema de predicción meteorológica habilita el actuador para que éste mida la humedad.
d) El sensor mide la humedad → los datos se envían a un sistema de control → se activa el actuador si es necesario.

54. ¿Cuáles son las fases en el proceso de desarrollo de software?

a) Análisis, diseño, codificación, integración y mantenimiento.
b) Análisis, diseño, codificación, pruebas y mantenimiento.
c) Análisis, codificación, integración y mantenimiento.
d) Diseño, codificación, integración, pruebas y mantenimiento.

55. ¿En qué consiste la fase de análisis en el ciclo de vida del software?

a) En esta fase se elabora un diseño donde se contemplan los elementos necesarios para que el sistema funcione.
b) En esta fase se procede a analizar las necesidades que tienen los/las usuarios/as del futuro sistema y que deben quedar satisfechas mediante el funcionamiento del mismo.
c) Esta fase no forma parte del ciclo de desarrollo aunque sí influye en el resto de fases.
d) Esta fase permite la optimización de los recursos en la producción del mismo.

56. ¿En cuántos documentos se describen los trabajos realizados en cada una de las fases del ciclo de vida del software?

a) En 5 documentos: requisitos del software, diseño del software, código fuente, documento de pruebas y documento de cambios.
b) En 3 documentos: requisitos del software, diseño del software, documento de cambios.



c) En 5 documentos: requisitos del software, diseño del software, código fuente, sistema de software y documento de cambios.
d) En 3 documentos: requisitos del software, documento de pruebas, documento de cambios.

57. ¿En qué consiste el ciclo de vida de software en V?

a) Se basa en la secuenciación de las distintas fases de la producción del software que se han descrito.
b) Se basa en una secuencia de fases análoga a la del modo en cascada pero se da especial importancia a la visión jerarquizada que se va teniendo de las distintas partes del sistema a medida que se avanza en el desarrollo.
c) Se basa en una forma de desarrollo lineal, en la que cada fase tiene una duración limitada en el tiempo.
d) Se basa en un sistema auxiliar que permite probar experimentalmente ciertas soluciones parciales a las necesidades de la persona usuaria.

58. La revisión de la fase de codificación en el ciclo de vida en cascada se realiza sobre…

a) El documento de análisis.
b) El documento de diseño.
c) El código fuente.
d) El sistema de explotación.

59. ¿Qué elemento distintivo introduce el modelo en espiral respecto a otros modelos de ciclo de vida?

a) El análisis intermedio.
b) El análisis de prueba.
c) El análisis de riesgo.
d) El análisis inicial.

60. ¿En qué cuatro valores se basa la Programación Extrema (XP) según Beck?

a) Sencillez, Comunicación, Retroalimentación y Valentía.
b) Planificación, Comunicación, Análisis y Evaluación.
c) Rapidez, Análisis, Comunicación y Retroalimentación.
d) Análisis, Codificación, Comunicación y Retroalimentación.

61. ¿Cuál de estos aspectos debe contemplar el Plan de Garantía de Calidad de software?

a) Organización de equipos de personas y la dirección y seguimiento del desarrollo.
b) Modelo de ciclo de vida a seguir, con detalle de sus fases y actividades.
c) Revisiones y auditorías que se llevarán a cabo durante el desarrollo, para garantizar que las actividades y documentos son correctos y aceptables.
d) Todas las anteriores son correctas.



62. ¿En qué consiste el control de cambios?

a) Consiste en almacenar de forma organizada las sucesivas versiones de cada elemento de la configuración.
b) Consiste en garantizar que las diferentes configuraciones del software se componen de elementos compatibles entre sí, y que constituyen un conjunto coherente.
c) Consiste en diseñar y almacenar de forma organizada los archivos de registro (.log) correspondientes a las distintas versiones de la configuración.
d) NINGUNA de las anteriores es correcta.

63. ¿Cuál de las siguientes NO es una norma estándar del desarrollo del software?

a) DoD.
b) ESA.
c) ISO.
d) IDEE.

64. Según el estándar ISO 12207, de Procesos del Ciclo de vida del software [ISO,IEC,2017] se establece que:

a) El mantenimiento de software es la modificación de un producto software después de haber sido entregado.
b) El propósito del proceso de mantenimiento es conservar la capacidad del sistema de proporcionar un servicio.
c) La fase de mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno del software, y a cambios debidos a las mejoras producidas por los requisitos cambiantes del cliente.
d) Hay 4 tipos de mantenimiento del software: correctivo, adaptativo, perfectivo y preventivo.

65. ¿En qué consiste el mantenimiento perfectivo?

a) El mantenimiento perfectivo incluye cambios en la especificación, normalmente debidos a cambios en los requisitos de un producto software.
b) El mantenimiento perfectivo consiste en la modificación del software para mejorar sus propiedades.
c) El mantenimiento perfectivo consiste en la modificación de un programa debido a cambios en el entorno.
d) El mantenimiento perfectivo consiste en localizar y eliminar posibles defectos de los programas.

66. ¿De qué dos clases pueden ser los cambios en el entorno a los que se refiere el mantenimiento adaptativo?

a) Entorno de los datos y el entorno de la programación.
b) Entorno de los procesos y el entorno del sistema operativo.
c) Entorno del hardware y el entorno del software.



d) Entorno de los datos y el entorno de los procesos.

67. ¿Cuál de estas afirmaciones sobre el coste del mantenimiento del software es correcta?

a) El mantenimiento es la fase más costosa del ciclo de vida del software.
b) Detectar y corregir un error es más barato en las fases iniciales que en las finales.
c) El mantenimiento puede costar más del doble que el desarrollo.
d) Todas las anteriores son correctas.

68. Según las Leyes de Lehman sobre el mantenimiento del software, la Ley de Continuidad del Cambio establece que:

a) Que tan pronto como un programa ha sido escrito, está ya desfasado.
b) Que cuando hay cambios en un programa la estructura se hace más compleja.
c) Que la evolución de un programa es un proceso autorregulado.
d) Que a lo largo del tiempo de vida de un programa, la carga que supone el desarrollo del programa es constante.

69. ¿Cuáles de los siguientes son métodos empleados en el mantenimiento del software?

a) Ingeniería Inversa.
b) Modernización.
c) Reestructuración.
d) Todas las anteriores son correctas.

70. Según la norma ISO/IEC 12207 ¿Cuáles son las principales actividades que agrupan los procesos de ciclo de vida del software?

a) Procesos de software, procesos de hardware y procesos de colaboración.
b) Procesos de colaboración, procesos organizacionales y procesos de gestión técnica.
c) Procesos de acuerdo, procesos organizacionales de proyecto, procesos de gestión técnica, y procesos técnicos.
d) NINGUNA de las anteriores es correcta.

71. ¿Cuál es el propósito del proceso de adquisición?

a) Obtener el producto o servicio de acuerdo a los requisitos de la persona compradora.
b) Proveer un producto o servicio a la persona compradora, que cumpla con los requisitos acordados.
c) Proveer la infraestructura y los servicios de los proyectos.
d) a) y b) son correctas.



72. ¿Cuál de estas tareas pertenece a la fase de implementación del proceso de la estructura de mantenimiento que propone la norma ISO/IEC 14764?

a) Desarrollar, documentar y ejecutar planes y procedimientos para dirigir las actividades y tareas del proceso de mantenimiento.
b) Definir procedimiento para recibir, almacenar y controlar los informes de problemas y solicitudes de modificación de las personas usuarias, y proporcionar a éstas retroalimentación.
c) Implementar o establecer una interfaz con el proceso de gestión de configuración, para gestionar las modificaciones del sistema existente.
d) Todas las anteriores son correctas.

73. ¿Cuál de las siguientes tareas forma parte del proceso de planificación de proyectos?

a) Proporcionar un marco analítico y estructurado para identificar alternativas.
b) Producir y coordinar planes realistas y efectivos.
c) Monitorizar de manera continua los riesgos.
d) Controlar los elementos y las configuraciones del sistema.

74. ¿Qué actividad se encarga de obtener los recursos necesarios para soportar el sistema de software durante todo su ciclo de vida?

a) Preparación del mantenimiento.
b) Ejecución del mantenimiento.
c) Soporte logístico.
d) Gestión de resultados del mantenimiento.

75. ¿Cuándo se realiza la migración de un software?

a) Cuando el software ha llegado al final de su vida útil.
b) Cuando el sistema debe adaptarse para funcionar en un nuevo entorno (hardware, sistema operativo, plataforma, infraestructura…).
c) Cuando es necesario analizar el software para decidir si debe retirarse o no.
d) NINGUNA de las anteriores es correcta.

76. En Windows 11, ¿qué característica de Microsoft Edge bloquea sitios maliciosos?

a) Navegación InPrivate.
b) Filtro Microsoft Defender SmartScreen.
c) Windows Defender Credential Guard.
d) Firewall de Windows Defender.



77. En un escenario de migración a Windows 11 a gran escala donde se quiere preservar el perfil de la persona usuaria, ¿qué herramienta recomienda Microsoft?

a) Windows Configuration Designer para exportar e importar perfiles durante el aprovisionamiento.
b) User State Migration Tool (USMT) incluida en el Windows Assessment and Deployment Kit.
c) Windows Deployment Services (WDS) utilizando imágenes de arranque personalizadas para transferir automáticamente los perfiles.
d) Microsoft Deployment Toolkit (MDT) usando una tarea de actualización in-place para migrar los perfiles.

78. En Windows 11, ¿cómo se llama el tipo de autenticación en el que la persona usuaria solo introduce una contraseña?

a) Autenticación fuerte.
b) Autenticación SSO.
c) Autenticación simple.
d) Autenticación biométrica.

79. La contraseña de imagen en Windows 11 se basa en:

a) Una secuencia de números PIN.
b) Gestos (círculos, líneas, puntos) sobre una imagen.
c) Reconocimiento facial obligatorio.
d) Una tarjeta inteligente conectada por USB.

80. En Windows 11, ¿qué característica de WDS permite instalar múltiples equipos simultáneamente?

a) Multidifusión.
b) Activación PXE.
c) Instalación desatendida.
d) Imágenes de inicio.

81. En Windows 11, ¿qué herramienta generaliza una instalación de referencia eliminando datos específicos del equipo?

a) DISM.
b) Sysprep.
c) DiskPart.
d) BCDBoot.

82. ¿Qué permite el SideLoading de aplicaciones en Windows 11?

a) Instalar apps de la tienda oficial.
b) Crear cuentas empresariales.



c) Gestionar actualizaciones de drivers.
d) Instalar aplicaciones de prueba sin certificación.

83. En Windows 11, ¿cuál es la principal consecuencia de la reorientación de Cortana hacia los servicios de productividad de Microsoft 365?

a) Pierde funciones como la administración de dispositivos conectados y la reproducción de música.
b) Gana funcionalidades domóticas.
c) Se limita exclusivamente a la traducción de idiomas.
d) Requiere licencia Enterprise para cualquier uso.

84. En Windows 11 ¿Qué herramienta gestiona el almacén central de controladores?

a) Administrador de dispositivos.
b) Almacén central de controladores.
c) DISM.
d) PnPUtil.

85. En Windows 11, ¿qué herramienta de línea de comandos permite crear, eliminar y administrar particiones y volúmenes en discos físicos o virtuales?

a) DiskPart.
b) Deployment Image Servicing and Management.
c) PnPUtil.
d) Netsh.

86. En Windows 11, ¿qué tecnología permite compartir contenido en redes locales sin saturar el ancho de banda?

a) BranchCache.
b) DirectAccess.
c) RemoteFX.
d) Wi-Fi Direct Printing.

87. ¿Qué conjunto de herramientas permite administrar servidores en Windows 11?

a) Microsoft Management Console (MMC).
b) Windows PowerShell.
c) Herramientas de administración RSAT.
d) ServerScope.

88. En Windows 11, ¿qué herramienta controla la ejecución de aplicaciones basándose en reglas?

a) Windows Defender SmartScreen.
b) AppLocker.



c) Device Guard.
d) Credential Guard.

89. En Windows Server 2022, ¿cuál de las siguientes opciones NO es un rol FSMO de Active Directory?

a) Schema Master.
b) RID Master.
c) PDC Emulator Master.
d) Network Domain Controller.

90. En un entorno con Windows Server 2022, en un servidor DHCP, ¿qué representa el ámbito (scope)?

a) Un rango de direcciones IP que el servidor puede asignar.
b) El tiempo de concesión de las direcciones.
c) Las opciones de configuración del servidor.
d) La lista de exclusiones de direcciones.

91. En un entorno con Windows Server 2022, en un servidor DHCP, ¿qué es una reserva?

a) Un rango de direcciones excluidas del ámbito (scope).
b) Una configuración de opciones específicas para una persona usuaria del dominio.
c) Una dirección IP específica asignada permanentemente a un dispositivo según su MAC.
d) Un tiempo de concesión de direcciones extendido.

92. En un entorno con Windows Server 2022 y un dominio basado en Active Directory, ¿qué tipo de grupo permite incluir miembros de cualquier dominio del bosque y asignar permisos en cualquier dominio del mismo bosque?

a) Grupo Global.
b) Grupo Local de Dominio.
c) Grupo Universal.
d) Grupo Local.

93. En Windows Server 2022, ¿qué componente es el responsable de mantener el canal seguro (secure channel) entre el equipo cliente y el controlador de dominio?

a) Servicio Kerberos.
b) Servicio Netlogon.
c) Servicio DNS.
d) Servicio Active Directory.



94. En Windows Server 2022, en un dominio de Active Directory, una persona usuaria pertenece a una Unidad Organizativa (OU) llamada "Pediatría". Existen las siguientes Directivas de Grupo (GPO):

- **Una GPO vinculada al Sitio que configura el fondo de pantalla en azul.**
- **Una GPO vinculada al Dominio que configura el fondo de pantalla en verde.**
- **Una GPO vinculada a la OU "Pediatría" que configura el fondo de pantalla en rojo.**

No hay herencia bloqueada ni "Enforced" activado en NINGUNA GPO. ¿Cuál será el color del fondo de pantalla que recibirá la persona usuaria?

a) Depende del controlador de dominio que autentique a la persona usuaria.
b) Azul.
c) Verde.
d) Rojo.

95. En Windows Server 2022, ¿qué función tiene el rol PDC Emulator en Active Directory?

a) Administrar el esquema de Active Directory.
b) Sincronizar la hora del dominio con un servidor de tiempo.
c) Asignar identificadores relativos (RID).
d) Mantener las referencias entre dominios.

96. En Windows Server 2022, en Active Directory, ¿cuál es la función principal del Catálogo Global?

a) Almacenar copias de seguridad de todos los objetos del dominio.
b) Contener información parcial de todos los objetos del bosque para búsquedas rápidas.
c) Gestionar las relaciones de confianza entre dominios.
d) Replicar completamente todos los objetos entre controladores de dominio.

97. En el modelo de seguridad de Windows Server 2022, ¿cuál de las siguientes afirmaciones describe correctamente la relación entre el token de acceso de una persona usuaria y la DACL de un recurso?

a) La DACL se almacena dentro del token de acceso de la persona usuaria y se genera en el momento del inicio de sesión.
b) El token de acceso contiene los SID de la persona usuaria y sus grupos, y se comparan con los de la DACL cuando se intenta acceder a un recurso.
c) El token de acceso solo se utiliza para autenticación, mientras que la DACL solo interviene en la auditoría.
d) La DACL determina qué grupos aparecerán en el token de acceso durante el inicio de sesión.



98. En un dominio con Windows Server 2022, un administrador copia nuevos archivos .admx y .adml al almacén central (Central Store) de directivas de grupo.
¿Cuál de las siguientes afirmaciones describe correctamente la función y diferencia entre estos archivos?

a) Los archivos .admx contienen la configuración de idioma y los adml definen las políticas aplicables al sistema.
b) Los archivos .admx definen la estructura y configuración de las plantillas administrativas, mientras que los adml contienen los recursos específicos de idioma.
c) Ambos archivos son idénticos, pero uno se usa para equipos y otro para personas usuarias.
d) Los archivos adml solo se utilizan cuando el dominio está en nivel funcional 2022.

99. En un dominio de Windows Server 2022, existen las GPO predeterminadas: Default Domain Policy y Default Domain Controllers Policy.
¿Cuál de las siguientes afirmaciones describe correctamente la diferencia principal entre ellas?

a) Default Domain Policy se aplica únicamente a los controladores de dominio, mientras que Default Domain Controllers Policy se aplica a todas las personas usuarias y equipos del dominio.
b) Default Domain Controllers Policy se aplica a nivel de sitio, mientras que Default Domain Policy solo se aplica a OUs específicas.
c) Default Domain Policy se aplica a todos los objetos del dominio y generalmente configura directivas de contraseña y bloqueo de cuenta, mientras que Default Domain Controllers Policy se aplica solo a los controladores de dominio y suele configurar directivas de auditoría y de inicio de sesión.
d) Ambas políticas son idénticas y se aplican de forma redundante a todos los objetos del dominio.

100. En Windows Server 2022, al configurar RAID, ¿qué característica principal de RAID 5 garantiza la tolerancia a fallos?

a) Duplica todos los datos en otro disco, tolerando fallos de hasta dos discos.
b) Requiere solo 2 discos y mantiene rendimiento de escritura igual a lectura.
c) Aumenta capacidad sin tolerancia a fallos, como RAID 0.
d) Distribuye datos y paridad entre los discos, permitiendo que el sistema siga operativo si falla un disco.



101. En una organización, la persona administradora gestiona los permisos de acceso a los documentos almacenados en OneDrive para la Empresa. Una persona trabajadora quiere compartir un archivo con algunos/as compañeros/as, pero mantenerlo inaccesible para el resto de la empresa. Según el funcionamiento descrito, ¿cuál de las siguientes afirmaciones refleja correctamente cómo se gestionan estos permisos?

a) Una vez subido un archivo a OneDrive para la Empresa, automáticamente todas las personas de la organización tienen acceso de lectura, sin posibilidad de restricciones individuales.
b) El sistema no permite compartir archivos de forma selectiva; únicamente se pueden compartir bibliotecas completas con toda la organización.
c) Las personas usuarias pueden guardar sus archivos profesionales y decidir compartirlos o no con sus colaboradores/as, pero los derechos y autorizaciones sobre el contenido de la biblioteca son gestionados por el/la administrador/a del sitio SharePoint.
d) Las personas usuarias pueden guardar sus archivos profesionales, pero tanto la decisión de poder compartir con otros colaboradores/as como los derechos y autorizaciones sobre el contenido de la biblioteca son gestionados por la persona administradora del sitio SharePoint.

102. Al abrir una carpeta en OneDrive para Empresas, la ruta de acceso se representa visualmente en la parte superior de la ventana mostrando la jerarquía completa, por ejemplo: Mis archivos > Documentos > ENI. ¿Cómo se denomina esta forma de representar la ruta de navegación?

a) Se denomina hilo de navegación.
b) Se denomina hilo de Ariadna.
c) Se denomina árbol de directorios.
d) Se denomina ruta de acceso rápido.

103. De todos los criterios de ordenación disponibles en OneDrive a través de la lista Organizar, alguno de ellos está disponible únicamente en la versión para Empresas. ¿Cuáles son esos criterios exclusivos?

a) La ordenación por tamaño y tipo de archivo.
b) La ordenación por modificado por y fecha de modificación.
c) La ordenación por tipo de archivos y por nombre de autor.
d) La ordenación por tamaño de archivo y fecha de modificación.

104. Una persona responsable de TI de una empresa está evaluando si el Almacén personal de OneDrive puede ser utilizado por los/as empleados/as para guardar documentación sensible corporativa. ¿En qué planes de suscripción está disponible esta funcionalidad?

a) En los planes Microsoft 365 Familia y Personal, no en OneDrive para la Empresa ni en suscripciones para grandes empresas o educativas.
b) En todos los planes de Microsoft 365, incluyendo OneDrive para la Empresa y los planes educativos.



c) En los planes Microsoft 365 Empresa Básico y Empresa Estándar, pero no en los planes personales ni familiares.
d) En los planes Microsoft 365 Empresa únicamente si el administrador del tenant de Microsoft 365 lo habilita expresamente desde el centro de administración corporativo.

105. Una persona usuaria de OneDrive necesita dar acceso a un archivo a una persona sin cuenta Microsoft. ¿Es esto posible?

a) No es posible, ya que OneDrive exige que todas las personas destinatarias dispongan de una cuenta Microsoft activa para poder acceder a cualquier archivo compartido.
b) No es posible de forma directa, dado que OneDrive solo admite el uso compartido entre personas usuarias que pertenezcan al mismo tenant o inquilino de Microsoft 365.
c) Sí es posible, pero la persona destinataria deberá crear obligatoriamente una cuenta Microsoft antes de poder visualizar el archivo compartido.
d) Sí es posible, siempre que la persona administradora haya autorizado compartir con personas usuarias externas, que recibirán el acceso mediante un vínculo por correo electrónico como invitadas anónimas.

106. Una empresa necesita crear un sitio SharePoint para gestionar grandes volúmenes de datos entrantes, configurar reglas que dirijan automáticamente esos archivos a ubicaciones específicas, y administrar modificaciones sobre los datos una vez añadidos al sistema. ¿Qué tipo de sitio SharePoint cubre estas necesidades?

a) Un centro de documentos, ya que está diseñado para la gestión centralizada de documentos de la empresa y permite configurar reglas de enrutamiento para dirigir los archivos a las ubicaciones correspondientes.
b) Un centro de datos, ya que permite crear un sitio diseñado para la gestión de datos, configurar tablas de enrutamiento para enviar archivos entrantes a ubicaciones específicas y administrar la eliminación o modificación de datos tras añadirlos al sistema de referencia.
c) Un sitio de proyecto, ya que reúne todos los estados y artefactos del proyecto en un entorno único, incluyendo herramientas para gestionar y redirigir los datos entrantes de forma automatizada.
d) Un centro de investigación de base, ya que proporciona funciones avanzadas de búsqueda y clasificación de datos, permitiendo además configurar reglas para dirigir automáticamente los archivos a las ubicaciones definidas.

107. Varias personas de un equipo necesitan modificar el mismo archivo almacenado en una biblioteca de documentos SharePoint. ¿Qué es preferible hacer para evitar que varias personas usuarias realicen modificaciones simultáneas sobre el mismo archivo?

a) Extraer el archivo del repositorio antes de abrirlo, de forma que ninguna otra persona usuaria pueda modificarlo mientras esté extraído, e insertarlo de nuevo una vez guardados los cambios para que todas puedan ver las modificaciones.

b) Abrir el archivo directamente desde la biblioteca y activar el modo de edición exclusiva desde las opciones del documento, que bloqueará automáticamente el acceso al resto de personas usuarias mientras esté abierto.
c) Crear una copia local del archivo, realizar las modificaciones necesarias y subir la nueva versión a la biblioteca, sobreescribiendo la anterior para que el resto de personas usuarias accedan a la versión actualizada.
d) Compartir el archivo con permisos de solo lectura para el resto de personas usuarias mientras una persona del equipo lo edita, y restablecer los permisos de edición una vez finalizados los cambios.

108. Una persona usuaria de SharePoint quiere configurar un sistema de notificaciones para un archivo de la biblioteca de documentos. ¿Qué opciones de notificación tiene disponibles?

a) Puede recibir notificaciones únicamente a través del correo electrónico corporativo asociado a su cuenta de Microsoft 365.
b) Puede recibir notificaciones a través de una ventana emergente en el propio sitio SharePoint o mediante una notificación push en la aplicación móvil de Microsoft 365.
c) Puede configurar un resumen semanal de todos los cambios realizados en la biblioteca completa, sin posibilidad de filtrar las notificaciones por archivo específico.
d) Puede recibir un aviso por correo electrónico o por SMS cada vez que se realice una modificación en dicho archivo, tras crear una alerta sobre el mismo.

109. Una persona usuaria está gestionando las tareas de un proyecto en SharePoint y observa que algunas tareas aparecen representadas de forma diferente en la escala de tiempo. ¿De qué depende la forma geométrica con la que se representa cada tarea?

a) Depende de la persona usuaria asignada: las tareas con persona responsable asignada se representan con un círculo y las tareas sin asignar se representan con un rectángulo en la escala de tiempo.
b) Depende de las fechas introducidas: si se han definido tanto la fecha de inicio como la de vencimiento se representa con un rectángulo, y si solo se ha introducido una de las dos fechas se representa con un rombo en la escala de tiempo.
c) Depende de la prioridad asignada a la tarea: las tareas de alta prioridad se representan con un triángulo y las de baja prioridad, con un círculo en la escala de tiempo.
d) Depende del estado de la tarea: las tareas completadas se representan con un rombo y las pendientes con un círculo en la escala de tiempo.

110. Una persona usuaria acaba de crear un nuevo sitio Wiki en SharePoint y observa que al acceder a él se muestra automáticamente una página por defecto. ¿Cómo se denomina técnicamente esta página y qué características tiene?

a) Se denomina Home.aspx; es la primera página del sitio que aparece al acceder a él y, aunque al crear el sitio se propone una versión estándar, puede modificarse o eliminarse y sustituirse por otra.



b) Se denomina Index.aspx; es la primera página del sitio que aparece al acceder a él y, aunque al crear el sitio se propone una versión estándar, puede modificarse o eliminarse y sustituirse por otra.
c) Se denomina Index.aspx y es una página generada automáticamente que recoge un índice de todos los contenidos del sitio, pudiendo ser modificada pero no eliminada.
d) Se denomina Home.aspx y es una página generada automáticamente que recoge un índice de todos los contenidos del sitio, pudiendo ser modificada pero no eliminada.

111. Microsoft Teams es una plataforma de trabajo colaborativo que pone a disposición de sus personas usuarias una serie de herramientas y servicios. ¿Cuál de las siguientes opciones describe correctamente las tareas que pueden realizar las personas de un equipo en Teams?

a) Conversar por mensajería instantánea, gestionar el correo electrónico corporativo, transferir archivos, administrar los permisos de acceso a documentos y planificar reuniones de equipo.
b) Acceder a información del equipo, transferir archivos, consultar el historial de conversaciones, crear sitios SharePoint y administrar las suscripciones de Microsoft 365 del equipo.
c) Conversar por mensajería instantánea, acceder a información del equipo, transferir archivos personales o compartidos, consultar el historial de conversaciones, planificar reuniones y colaborar en la edición de archivos compartidos.
d) Conversar por mensajería instantánea, transferir archivos, consultar el historial de conversaciones, gestionar las licencias de usuario y coeditar historiales compartidos del equipo.

112. La persona propietaria de un equipo en Microsoft Teams quiere revisar qué aspectos puede gestionar desde la configuración del equipo. ¿Cuál de las siguientes opciones describe correctamente las posibilidades que ofrece dicha configuración?

a) Modificar la imagen asociada al equipo, gestionar el calendario compartido, administrar las autorizaciones de las personas miembro y configurar las notificaciones de correo electrónico del equipo.
b) Administrar las autorizaciones de las personas miembro, gestionar el calendario compartido, configurar los canales privados, gestionar las reuniones programadas del equipo y autorizar el uso de emojis y GIF animados y pegatinas.
c) Modificar la imagen asociada al equipo, gestionar el calendario compartido, administrar las licencias de Microsoft 365 de las personas miembro, activar o desactivar las menciones y gestionar el almacenamiento de archivos del equipo.
d) Modificar la imagen asociada al equipo, administrar las autorizaciones de las personas miembro, activar o desactivar las menciones a equipos y canales, y autorizar el uso de emojis, GIF animados y pegatinas.



113. Microsoft Teams establece una serie de límites en la gestión de canales dentro de un equipo. ¿Cuál de las siguientes afirmaciones describe correctamente dichos límites?

a) Se puede añadir hasta 200 canales por equipo, sin contar los canales eliminados que se pueden restaurar en un plazo de 30 días.
b) Se puede añadir hasta 200 canales por equipo, incluidos los canales eliminados que se pueden restaurar en un plazo de 30 días.
c) Se puede añadir hasta 300 canales por equipo, sin contar los canales eliminados que se pueden restaurar en un plazo de 60 días.
d) Se puede añadir hasta 300 canales por equipo, incluidos los canales eliminados que se pueden restaurar en un plazo de 60 días.

114. Según la norma ISO/IEC 17799, ¿cómo se define la Seguridad de la Información?

a) Como un conjunto de herramientas de software para proteger la red.
b) Como la preservación de su confidencialidad, su integridad y su disponibilidad.
c) Como un proceso de auditoría externa para certificar la calidad de los datos.
d) Como la eliminación de todas las amenazas externas que afectan al hardware.

115. ¿Cómo define la norma ISO 7498 la Seguridad Informática?

a) Como un sistema de gestión basado en el control de acceso físico.
b) Como una metodología para el análisis de riesgos en la administración pública.
c) Como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.
d) Como el uso de técnicas criptográficas para garantizar el anonimato de la persona usuaria.

116. Dentro de los objetivos de seguridad, ¿qué comprende el plano de actuación "Humano"?

a) Instalación, configuración y actualización de soluciones de hardware.
b) Sensibilización y formación de personas empleadas y personas directivas, definición de funciones y obligaciones del personal.
c) Definición e implantación de políticas de seguridad, planes, normas y procedimientos.
d) Cumplimiento y adaptación a la legislación vigente como la LOPD y el Código Penal.

117. ¿Qué garantiza el servicio de "Confidencialidad"?

a) Que la identidad de la persona creadora de un mensaje o documento es legítima.
b) Que un mensaje o fichero no ha sido modificado desde su creación.
c) Que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario.
d) Que el sistema sea lo suficientemente robusto frente a ataques e interferencias.



118. ¿En qué consiste el objeto del servicio de "No repudiación"?

a) En implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje.
b) En controlar el acceso de las personas usuarias a los distintos equipos y servicios ofrecidos.
c) En registrar y monitorizar la utilización de los distintos recursos del sistema.
d) En probar que un contenido digital pertenece a una persona titular de derechos de autor.

119. ¿Cómo se define el principio de "Defensa en Profundidad"?

a) Como el uso de un único cortafuegos para proteger el perímetro de la red.
b) Como el diseño e implantación de varios niveles de seguridad dentro del sistema informático de la organización.
c) Como la actualización diaria de los parches publicados por fabricantes.
d) Como el cifrado de todos los datos sensibles transmitidos por Internet.

120. En los niveles de madurez de la gestión, ¿qué caracteriza a la Etapa 1?

a) La certificación de la gestión basada en estándares internacionales como ISO 27001.
b) La implantación de medidas básicas de seguridad por “sentido común”.
c) La gestión global de la seguridad mediante la definición de políticas y planes.
d) La adaptación a los requisitos del marco legal y de las exigencias de los/las clientes.

121. Técnicamente, ¿qué es una "vulnerabilidad"?

a) Cualquier evento accidental o intencionado que pueda ocasionar algún daño.
b) La probabilidad de que una amenaza se materialice sobre un recurso.
c) Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.
d) La medición y valoración del daño que produciría un incidente de seguridad.

122. ¿Cómo se define de forma simplificada un "Incidente de Seguridad"?

a) El impacto económico derivado de la falta de medidas preventivas.
b) La materialización de una amenaza.
c) Una debilidad en los sistemas físicos o lógicos de la empresa.
d) Un medio empleado para eliminar o reducir un riesgo identificado.



123. ¿Qué es una medida de seguridad "pasiva"?

a) Aquella utilizada para anular el riesgo antes de que ocurra el incidente.
b) Cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad.
c) Un procedimiento para detectar un ataque durante su ejecución.
d) Una técnica para monitorizar los registros de actividad de los equipos.

124. En la jerarquía de conceptos de seguridad, ¿qué elemento constituye la base de la pirámide y sirve para dejar constancia de las tareas realizadas?

a) Procedimientos de Seguridad.
b) Planes de Contingencia.
c) Registros / Evidencias.
d) Políticas de Seguridad.

125. ¿Qué principio establece que las personas usuarias deben tener asignadas solo los servicios y aplicaciones estrictamente necesarios para sus tareas?

a) Principio de Configuración Robusta y Segura.
b) Defensa en Profundidad (Layered Security).
c) Asignación de los mínimos privilegios.
d) Control de Acceso Discrecional por Propietario/a.

126. ¿Cómo se define el nivel RAID 0 en cuanto a su tolerancia a fallos?

a) Ofrece una alta disponibilidad mediante el uso de espejado
b) Utiliza códigos Hamming para la corrección de errores en tiempo real.
c) Este nivel no ofrece tolerancia a fallos.
d) Requiere un disco dedicado exclusivamente para el almacenamiento de paridad.

127. ¿Qué nivel de RAID se destaca por ofrecer actualmente la mejor "relación rendimiento-coste" para aplicaciones empresariales?

a) RAID 0+1 / RAID 10
b) RAID 6 (Acceso independiente con doble paridad)
c) RAID 2 (Acceso síncrono con código de errores)
d) RAID 5

128. ¿Qué acción debe realizarse de forma inmediata en el sistema cuando un/una empleado/a causa baja en la organización?

a) Auditoría de las últimas sesiones de acceso de la persona usuaria.
b) Transferencia de sus ficheros personales a un soporte desmagnetizado.



c) Cancelación o bloqueo inmediato de las cuentas de una persona usuaria.
d) Cambio de contraseña de acceso al BIOS de su estación de trabajo.

129. Dentro de los factores de autenticación, ¿cuál es un ejemplo textual de "Lo que se sabe"?

a) Tarjeta inteligente (smartcard) o token USB.
b) Características biométricas como el iris o la voz.
c) Firma manuscrita.
d) Contraseñas (passwords) y PINs.

130. ¿Cómo se clasifica la información cuya divulgación podría ocasionar "daños significativos" para la organización?

a) Información de uso interno.
b) Información secreta o reservada.
c) Información desclasificada.
d) Información confidencial.

131. En las conexiones VPN, ¿qué propiedades se garantizan mediante el uso de algoritmos criptográficos?

a) Escalabilidad, disponibilidad y redundancia de la red.
b) Confidencialidad, autenticidad e integridad de los datos.
c) Mayor ancho de banda y menor latencia en conexiones remotas.
d) Encapsulamiento de protocolos no enrutables mediante túneles.

132. ¿Cómo se denomina al intervalo de tiempo transcurrido desde que se hace pública una vulnerabilidad hasta que se presenta la correspondiente actualización o parche de seguridad?

a) Días de riesgo.
b) Periodo de exposición.
c) Ventana de vulnerabilidad.
d) Tiempo de respuesta técnica.

133. ¿Qué técnica de espionaje empresarial consiste en la búsqueda de información sensible en copias generadas en papel que han sido descartadas?

a) Trash scanning.
b) Paper tracking.
c) Dumpster diving.
d) Scraping físico.



134. Según la Ley General de Telecomunicaciones de España (32/2003), ¿qué obligación puede imponer el Estado a los organismos públicos o fabricantes en relación con el cifrado?

a) Entregar copias de seguridad de todas las claves privadas.
b) Utilizar exclusivamente algoritmos de cifrado de flujo.
c) Prohibir el uso de longitudes de clave superiores a 128 bits.
d) Facilitar sin coste alguno los aparatos de cifrado a efectos de su control.

135. ¿En qué fase del ciclo de vida de un sistema es más común la introducción accidental de puertas traseras?

a) Durante las fases de desarrollo.
b) Durante la auditoría de certificación.
c) Durante la fase de despliegue en producción.
d) Durante el mantenimiento correctivo.

136. ¿Cómo se conoce al fenómeno de acceso y control remoto de teléfonos móviles y agendas electrónicas a través de la tecnología Bluetooth?

a) Bluejacking masivo.
b) Snarfing o Bluesnarfing.
c) Bluetooth capturing.
d) Remote cell control.

137. ¿Qué estándar se define como un manual con una serie de secciones compuestas por módulos que incluyen las distintas pruebas para realizar una auditoría técnica de seguridad?

a) OSSTMM.
b) Owasp
c) NIST SP 800-42
d) EISPP

138. ¿Cuál es el nombre del lenguaje propietario utilizado por la herramienta Nessus para que la persona usuaria pueda definir sus propias pruebas de vulnerabilidades?

a) Nessus Scripting Tool (NST).
b) NASL (Nessus Attack Scripting Language).
c) Vulnerability Definition Language (VDL).
d) Nessus Core Script.



139. ¿A qué tipo de tratamiento de datos personales resultará de aplicación el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas?

a) Al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
b) Al tratamiento realizado en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.
c) Al tratamiento efectuado por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
d) Al tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

140. ¿Qué exige el principio de «integridad y confidencialidad» respecto al tratamiento de datos personales según el Reglamento (UE) 2016/679?

a) Que los datos sean exactos y, si fuera necesario, se mantengan actualizados, adoptando todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
b) Que los datos sean tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
c) Que los datos sean mantenidos de forma que se permita la identificación de las personas interesadas durante un plazo indefinido, sin atender a la necesidad del tratamiento de los datos personales ni a las medidas técnicas y organizativas que impone el presente Reglamento.
d) Que los datos sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados ulteriormente de manera incompatible con dichos fines, salvo que se traten con fines de archivo en interés público, de investigación científica o histórica.

141. Bajo el Reglamento (UE) 2016/679, ¿qué condición debe cumplirse para que el tratamiento de datos de un niño o niña sea lícito en relación con la oferta directa de servicios de la sociedad de la información?

a) Que la niña o el niño tenga como mínimo 14 años, sin que los Estados miembros puedan establecer por ley una edad inferior a tales fines.
b) Que el servicio sea gratuito y no implique la elaboración de perfiles comerciales.
c) Que el niño o la niña haya leído y aceptado las condiciones de privacidad de forma autónoma, siempre que tenga como mínimo 14 años de edad.
d) Que la niña o el niño tenga como mínimo 16 años, o si es menor a dicha edad, que el consentimiento lo diera o autorizara el titular de la patria potestad o tutela.



142. ¿Qué información debe facilitar, entre otras, la persona responsable del tratamiento en el momento en que obtenga datos personales directamente del interesado, conforme al Reglamento (UE) 2016/679?

a) La fuente de la que proceden los datos personales y si estos proceden de fuentes de acceso público.
b) Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
c) Las categorías de datos personales de que se trate y el historial de tratamientos anteriores de la persona interesada.
d) La descripción general de las medidas técnicas y organizativas de seguridad adoptadas para garantizar la resiliencia de los sistemas de tratamiento de datos.

143. ¿Qué información específica, entre otras, tiene derecho a obtener la persona interesada del responsable del tratamiento cuando ejerce su derecho de acceso al amparo del Reglamento (UE) 2016/679?

a) Las personas destinatarias o las categorías de personas destinatarias a las que se comunicaron o serán comunicados los datos personales, en particular personas destinatarias en terceros u organizaciones internacionales.
b) Cuando los datos personales no se hayan obtenido de la persona interesada, los datos personales de la persona representante de la persona destinataria.
c) La identificación pormenorizada de la ubicación física de los servidores y la dirección del centro de procesamiento de datos donde se encuentran alojados sus datos personales.
d) La descripción técnica del estándar de seguridad y el algoritmo de cifrado específico aplicado para garantizar la resiliencia de sus datos personales.

144. En el marco del Reglamento (UE) 2016/679, ¿en qué supuesto NO será de aplicación el derecho de supresión («el derecho al olvido») por ser el tratamiento de los datos necesario?

a) Cuando los datos personales hayan sido tratados ilícitamente.
b) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.
c) Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
d) Cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

145. De acuerdo con el texto del Reglamento (UE) 2016/679, ¿en qué formato tendrá derecho a recibir la persona interesada sus datos personales al ejercer el derecho a la portabilidad?

a) En cualquier formato que el responsable considere oportuno, siempre que sea legible por el interesado.
b) Únicamente en formato papel certificado y compulsado para garantizar su autenticidad.



c) En un formato estructurado, de uso común y lectura mecánica.
d) En un formato cifrado que solo pueda ser abierto por autoridades de control.

146. Conforme al Reglamento (UE) 2016/679, ¿cuál es el contenido mínimo que debe incluir la notificación de una violación de la seguridad de los datos personales a la autoridad de control competente?

a) La identificación nominal y el documento de identidad de cada una de las personas interesadas afectadas, así como la ubicación física exacta de los servidores vulnerados.
b) La naturaleza de la violación, los datos de contacto de la persona delegada de protección de datos, las posibles consecuencias y las medidas adoptadas o propuestas por el o la responsable para poner remedio a la violación.
c) Una copia íntegra del registro de actividades de tratamiento y la descripción técnica detallada de los algoritmos de cifrado que fallaron durante el incidente.
d) El dictamen vinculante del Comité Europeo de Protección de Datos sobre la gravedad de la infracción y la propuesta de sanción administrativa correspondiente.

147. En el marco del Reglamento (UE) 2016/679, ¿en qué circunstancia NO resulta obligatoria la comunicación individual de una violación de la seguridad de los datos personales a la persona interesada, a pesar de que sea probable que dicha violación entrañe un alto riesgo para sus derechos y libertades?

a) Cuando la persona responsable demuestre haber aplicado medidas de protección técnicas y organizativas, en particular las que hagan los datos personales ininteligibles para cualquier persona no autorizada a su acceso, como el cifrado.
b) Siempre que la persona responsable haya procedido a la notificación obligatoria a la autoridad de control competente en el plazo máximo de 72 horas.
c) Cuando la violación afecte exclusivamente a datos personales que hayan sido objeto de un tratamiento de seudonimización previo al incidente.
d) Cuando el tratamiento de los datos personales afectados se encuentre amparado por una obligación legal o una misión de interés público.

148. De acuerdo con el Reglamento (UE) 2016/679, ¿cuál de las siguientes funciones debe desempeñar la persona delegada de protección de datos como parte de sus cometidos mínimos?

a) Asumir la representación legal y la responsabilidad jurídica de la persona responsable del tratamiento ante cualquier reclamación judicial interpuesta por las personas interesadas.
b) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
c) Realizar de forma autónoma la evaluación de impacto relativa a la protección de datos en lugar de la persona responsable del tratamiento.
d) Validar técnicamente las aplicaciones y auditar el estándar de cifrado específico aplicado a las bases de datos de la persona responsable.



149. ¿En qué lugar tiene derecho a presentar una reclamación ante una autoridad de control una persona interesada que considere que el tratamiento de sus datos personales infringe el Reglamento (UE) 2016/679?

a) Exclusivamente en el Estado miembro donde la persona responsable del tratamiento tenga su administración central o su establecimiento principal.
b) En el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción.
c) Únicamente en el Estado miembro donde se haya designado a la persona representante de quien es responsable del tratamiento no establecido en la Unión.
d) Ante la autoridad de control del Estado miembro donde se localice el servidor físico que aloja los datos personales objeto de la controversia.

150. De acuerdo con lo establecido en el Reglamento (UE) 2016/679, ¿de quién tiene derecho a recibir una indemnización toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de dicho Reglamento?

a) De la Persona Delegada de Protección de Datos.
b) De la Agencia Española de Protección de Datos.
c) De la persona responsable o encargada del tratamiento.
d) Del Comité Europeo de Protección de Datos.

151. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en lo relativo al ejercicio de derechos sobre los datos personales de personas fallecidas, ¿qué regla prevalece en caso de existir una prohibición expresa del o de la causante para el acceso a su información?

a) La prohibición es absoluta y vinculante para todas las personas legitimadas, incluidas las personas herederas, ya que el derecho fundamental a la protección de datos exige el respeto íntegro a la voluntad de control sobre la propia información incluso tras el fallecimiento.
b) La prohibición impide el acceso, rectificación o supresión con carácter general, pero no puede afectar al derecho de las personas herederas a acceder a los datos de carácter patrimonial del o de la causante.
c) El ejercicio de los derechos de acceso y supresión decae únicamente si la prohibición ha sido inscrita en el registro de mandatos e instrucciones previsto por la Ley, siendo ineficaz cualquier otra manifestación de voluntad que no conste en documento público.
d) En caso de fallecimiento de personas con discapacidad, la prohibición expresa del o de la causante podrá ser siempre revocada por el Ministerio Fiscal de oficio si considera que el acceso a los datos beneficia el interés superior de las personas herederas.



152. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿quién tiene la potestad legal para ejercer los derechos de acceso, rectificación, cancelación u oposición en nombre de un o una menor de catorce años?

a) Las personas titulares de la patria potestad, quienes podrán ejercitar tales derechos en nombre y representación del o de la menor, así como cualquier otra persona que pudiera corresponderle en el contexto de la normativa de protección de datos.
b) El Ministerio Fiscal, con carácter exclusivo y de oficio, para garantizar la neutralidad y la protección del interés superior de la o del menor frente a posibles usos comerciales de sus datos por parte de sus representantes legales.
c) El o la propia menor de edad de forma autónoma, siempre que la persona responsable del tratamiento implemente mecanismos de verificación de madurez que demuestre que la persona afectada comprende las consecuencias del tratamiento de su información.
d) Únicamente la persona Delegada de Protección de Datos de la institución educativa o entidad donde se traten los datos, actuando como tutora o tutor digital para evitar conflictos de intereses entre el o la menor y sus progenitores.

153. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, en relación con los tratamientos con fines de videovigilancia, ¿quiénes podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones?

a) Tanto las personas físicas o jurídicas como las públicas o privadas.
b) Únicamente personas físicas o jurídicas.
c) Únicamente personas públicas o privadas.
d) Únicamente las asociaciones y organismos que creen sistemas de información generales o sectoriales.

154. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿cuál de las siguientes afirmaciones es válida en relación con el bloqueo de los datos?

a) El bloqueo es una medida facultativa que permite a la persona responsable del tratamiento seguir utilizando la información para fines estadísticos o de investigación interna, siempre que los datos se mantengan en un servidor independiente del principal.
b) Los datos bloqueados deben ser objeto de una eliminación física inmediata e irreversible de todos los soportes lógicos, debiendo el responsable emitir un certificado de destrucción para su remisión obligatoria a la Agencia Española de Protección de Datos.
c) Consiste en la identificación y reserva de los datos para impedir su tratamiento y visualización, excepto para ponerlos a disposición de jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes para la exigencia de posibles responsabilidades durante el plazo de prescripción.
d) El bloqueo implica una suspensión temporal del acceso a los datos durante un plazo fijo de un año, transcurrido el cual, si la persona afectada no ha reiterado su solicitud de supresión, los datos volverán a estar activos para el tratamiento original.



155. De acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿a través de qué departamento ministerial se relaciona la Agencia Española de Protección de Datos (AEPD) con el Gobierno?

a) El Ministerio del Interior.
b) El Ministerio de la Presidencia.
c) El Ministerio de Justicia.
d) El Ministerio de Economía y Empresa.

156. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿sobre qué tipos de tratamientos pueden ejercer sus funciones y potestades las autoridades autonómicas de protección de datos?

a) Sobre cualquier tratamiento de datos personales realizado por empresas privadas siempre que su domicilio social o su actividad principal se desarrolle dentro del territorio de la respectiva Comunidad Autónoma.
b) Sobre los tratamientos de datos de personas físicas realizados en el ejercicio de actividades exclusivamente personales o domésticas dentro del ámbito geográfico de la autonomía.
c) Sobre tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.
d) Exclusivamente como órganos de consulta y asesoramiento del Gobierno autonómico, careciendo de potestad para dictar circulares o ejercer las funciones de inspección y sanción previstas en el Reglamento (UE) 2016/679.

157. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿en qué supuestos debe la Agencia Española de Protección de Datos (AEPD) acordar obligatoriamente la inadmisión a trámite de una reclamación presentada por una o un ciudadano?

a) Únicamente cuando la reclamante sea una persona jurídica, dado que el derecho fundamental a la protección de datos ampara exclusivamente a las personas físicas y no a las organizaciones o empresas.
b) Cuando la reclamación se presente de forma presencial en papel y la persona interesada sea una persona obligada a relacionarse electrónicamente con las Administraciones Públicas, de acuerdo con la Ley 39/2015
c) Cuando el objeto de la queja sea una infracción cuya sanción económica prevista sea inferior a 3.000 euros, considerándose en tal caso que no existe un interés público relevante para iniciar el procedimiento.
d) Cuando las reclamaciones presentadas no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.



158. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿cuál de las siguientes conductas es tipificada como una infracción muy grave?

a) La exigencia del pago de un canon para atender las solicitudes de ejercicio de derechos de las personas afectadas cuando el ejercicio sea repetitivo, si la cuantía cobrada excede el importe de los costes de facilitar la información.
b) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas de seguridad que la persona responsable hubiese implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.
c) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.
d) No poner a disposición de la autoridad de protección de datos el registro de actividades de tratamiento cuando éste sea solicitado en el marco de una investigación.

159. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, ¿durante cuánto tiempo debe estar paralizado el expediente sancionador por causas no imputables a la presunta persona infractora para que se reinicie el plazo de prescripción de la infracción?

a) Durante más de 1 mes.
b) Durante más de 12 meses.
c) Durante más de 3 meses.
d) Durante más de 6 meses.

160. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ¿cuál de las siguientes afirmaciones NO se corresponde lo dispuesto para garantizar el derecho de acceso universal a Internet?

a) El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.
b) Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
c) Se procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso de las personas mayores.
d) El derecho de acceso universal implica la obligación de las personas proveedoras de red de suministrar conexión gratuita de banda ancha a toda la ciudadanía residente en entornos rurales con baja densidad demográfica.

161. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, ¿cuál de las siguientes afirmaciones se corresponde con lo dispuesto en relación con el derecho a la desconexión digital en el ámbito laboral?

a) El derecho a la desconexión faculta a la persona trabajadora para interrumpir de forma discrecional el uso de herramientas tecnológicas durante la jornada laboral



efectiva, siempre que se acredite un riesgo de fatiga informática conforme a la normativa de prevención de riesgos laborales.

b) La persona empleadora, previa audiencia de los y las representantes de las personas trabajadoras, debe elaborar una política interna que defina las modalidades de ejercicio de este derecho y las acciones de formación y sensibilización sobre un uso razonable de las herramientas tecnológicas.

c) Dada la naturaleza de este derecho, su obligatoriedad y el deber empresarial de definir protocolos de desconexión se circunscriben exclusivamente a las personas trabajadoras que prestan servicios a distancia o mediante teletrabajo.

d) En defecto de previsiones específicas en la negociación colectiva, la persona empresaria podrá establecer de forma unilateral las condiciones de la desconexión digital, siendo suficiente la notificación informativa a los y las representantes de las personas trabajadoras para su validez.

162. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, en relación con la protección de menores en Internet, ¿qué deben cumplir los centros educativos o entidades que desarrollen actividades con menores para publicar o difundir datos personales de estos en redes sociales?

a) Debido a la misión de interés público que desempeñan los centros docentes, estos están facultados para difundir imágenes de actividades escolares sin necesidad de consentimiento, siempre que no se identifique al o a la menor con nombres y apellidos.

b) La difusión o publicación de dichos datos en redes sociales o servicios equivalentes requiere obligatoriamente el consentimiento del o de la propia menor o de sus representantes legales, según lo dispuesto en las reglas generales de la Ley sobre consentimiento de menores.

c) Para garantizar la seguridad de la o del menor, la normativa prohíbe taxativamente a los centros educativos el uso de redes sociales abiertas, permitiendo la difusión de datos únicamente a través de plataformas educativas cerradas y de acceso restringido a las familias.

d) El centro educativo podrá publicar la información basándose en el "interés superior de la o del menor", bastando con informar previamente a sus tutores legales y dándoles un plazo de diez días para que manifiesten su oposición expresa antes de la subida del contenido.

163. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, en relación con el ejercicio del derecho al olvido en servicios de redes sociales y servicios equivalentes, ¿cuál de las siguientes afirmaciones es correcta respecto a la supresión de datos facilitados durante la minoría de edad?

a) El prestador del servicio sólo está obligado a suprimir los datos si la persona afectada demuestra que la información es inexacta, no pertinente o excesiva, siguiendo los criterios de ponderación aplicables a los datos facilitados por terceras personas en la edad adulta.

b) El derecho de supresión sobre contenidos de la etapa de minoría de edad decae automáticamente si la persona afectada, una vez alcanzada la mayoría de edad, realiza nuevas publicaciones en el mismo servicio, entendiéndose como una validación tácita de su historial previo.



c) En caso de que el derecho se ejercitase por una persona afectada respecto de datos que hubiesen sido facilitados al servicio, por ella o por terceras personas, durante su minoría de edad, la persona prestadora del servicio deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran otras circunstancias.
d) Las personas prestadoras de servicios de redes sociales están exentas de suprimir datos de menores si acreditan que dicha información se utiliza únicamente para fines estadísticos.

164. ¿Cuál es el objeto de la Ley 6/2020?.

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo.
b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.
c) Regular determinados aspectos de los servicios electrónicos de confianza.
d) El derecho fundamental de las personas físicas a la protección de datos personales amparado por el artículo 18.4 de la Constitución.

165. ¿A qué personas prestadoras establecidas fuera de España les resulta de aplicación la Ley 6/2020?

a) A todas las personas prestadoras residentes o domiciliadas en otro Estado que operen en España, independientemente de su supervisión.
b) A las personas prestadoras residentes o domiciliadas en otro Estado con establecimiento permanente en España, siempre que sus servicios no estén supervisados por la autoridad competente de otro país de la UE.
c) A las personas prestadoras residentes o domiciliadas en otro Estado con establecimiento permanente en España, siempre que sus servicios estén supervisados por la autoridad competente de otro país de la UE.
d) A las personas prestadoras públicas y privadas de servicios electrónicos de confianza establecidos en España.

166. Según la Ley 6/2020, ¿qué valor y eficacia jurídica tienen los documentos electrónicos?

a) Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.
b) Los documentos electrónicos públicos y administrativos, tienen el valor y la eficacia jurídica que se le otorgue en el ordenamiento jurídico español del Reglamento (UE) 2016/679.
c) Los documentos electrónicos públicos y privados, tienen el valor y la eficacia jurídica que corresponda a su copia no cualificada según el artículo 3 y la disposición segunda del Reglamento.
d) Los documentos electrónicos públicos y privados, tienen el valor y la eficacia jurídica que se le otorgue en el ordenamiento jurídico español del Reglamento (UE) 2016/679.



167. Conforme a la Ley 6/2020, ¿cuál es el período máximo de vigencia de un certificado electrónico cualificado?

a) 2 años.
b) 4 años.
c) 5 años.
d) 6 años.

168. De acuerdo con la Ley 6/2020, ¿qué ocurre si se viola o pone en peligro el secreto de los datos de creación de firma o de sello?

a) Que se le pondrá una multa a la persona responsable de haber puesto en peligro dichos datos.
b) Que se renovará el certificado electrónico con otro firmante.
c) Que se modificará la identidad de la persona titular del certificado electrónico.
d) Que se revocará el certificado electrónico.

169. Con arreglo a la Ley 6/2020, ¿qué información debe incluir la persona prestadora de servicios electrónicos de confianza en la comunicación a la persona titular cuando revoca o suspende un certificado electrónico?

a) Únicamente la fecha en la que el certificado quedará sin efecto, sin necesidad de justificación adicional.
b) Los motivos, la fecha y la hora en los que el certificado quedará sin efecto.
c) El procedimiento para recurrir la revocación y el plazo máximo para hacerlo.
d) La identidad de la autoridad competente que ha ordenado la revocación o suspensión.

170. En el supuesto de certificados cualificados de firma electrónica expedidos a personas físicas, ¿cómo se consigna la identidad del titular según lo previsto en la Ley 6/2020?

a) Por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca.
b) Por su nombre y apellidos junto con su dirección postal y fecha de nacimiento y/o mediante un pseudónimo.
c) Por su denominación o razón social y su número de identificación fiscal.
d) Por su Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o denominación o razón social y su número de identificación fiscal.



171. ¿En qué caso puede prescindirse de la personación física ante las personas encargadas de verificar la identidad de un solicitante de un certificado cualificado con arreglo a la Ley 6/2020?

a) Cuando la persona solicitante aporte una copia compulsada de su Documento Nacional de Identidad junto con una declaración responsable.
b) Cuando la firma de la persona solicitante en la solicitud de expedición del certificado cualificado haya sido legitimada en presencia notarial.
c) Cuando la persona solicitante haya obtenido previamente otro certificado cualificado en vigor expedido por el mismo prestador.
d) Cuando un representante legal acuda en su nombre con el certificado cualificado compulsado por el departamento competente.

172. Según la Ley 6/2020, ¿puede utilizarse la videoconferencia como método de identificación para solicitar un certificado cualificado y, en caso afirmativo, bajo qué condición?

a) No, la videoconferencia nunca está permitida ya que la identificación a distancia no garantiza la fiabilidad exigida para los certificados cualificados.
b) Sí, pero únicamente cuando la persona solicitante resida en el extranjero y no pueda desplazarse a territorio español y se haga en la Embajada Española correspondiente al país en el que reside.
c) No, únicamente se admite la personación física o la legitimación notarial de la firma, sin que se pueda usar ningún método de identificación a distancia.
d) Sí, siempre que aporte una seguridad equivalente en términos de fiabilidad a la presencia física, según evaluación de un organismo de evaluación de la conformidad, y bajo las condiciones técnicas fijadas por Orden Ministerial.

173. Con arreglo a la Ley 6/2020, ¿qué obligación tienen los prestadores de servicios electrónicos de confianza cuando consignan un pseudónimo en un certificado electrónico?

a) Comunicar el pseudónimo utilizado a la autoridad competente para su registro y validación previa.
b) Garantizar que el pseudónimo no coincida con el de ningún otro certificado expedido por el mismo prestador.
c) Constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.
d) No es posible usar pseudónimo en este tipo de certificados electrónicos.



174. Según lo previsto en la Ley 6/2020, ¿cuál es el importe mínimo del seguro de responsabilidad civil que deben constituir los prestadores cualificados de servicios electrónicos de confianza?

a) 1.000.000 de euros, incrementándose en 250.000 euros por cada servicio cualificado adicional que se preste.
b) 1.500.000 euros, salvo para los prestadores del sector público, añadiéndose 500.000 euros más por cada tipo de servicio cualificado adicional.
c) 1.500.000 euros para cualquier prestador, pudiéndose reducir 500.000 euros si se presta un único servicio cualificado en el sector privado.
d) 2.000.000 de euros como importe base, con independencia del número de servicios cualificados que se presten.

175. En virtud de la Ley 6/2020, ¿qué tipo de infracción comete un prestador que no adopta medidas suficientes para resolver incidentes de seguridad en sus productos, redes y sistemas de información?

a) Infracción muy grave, si no se resuelve en el plazo de cinco días desde que se produjeron.
b) Infracción grave, si no se resuelve en el plazo de veinte días desde que se produjeron
c) Infracción grave, si no se resuelve en el plazo de diez días desde que se produjeron.
d) Infracción leve, si no se resuelve en el plazo de diez días desde que se produjeron.

176. En la Gestión de cambios de la tecnología ITIL4, un cambio abarca: Una modificación de uno o más elementos de configuración que componen el sistema de información…

a) o de uno o más servicios proporcionados por este sistema de información.
b) pero no de servicios proporcionados por este sistema de información.
c) siempre y cuando tenga un impacto en un proceso de negocio
d) o de la modificación de un dato.

177. En la metodología ITIL 4 el tipo de cambio estándar:

a) Requiere una evaluación completa y una autorización antes de llevarse a cabo.
b) Concierne a los cambios autorizados con antelación, que seguirán procedimientos predefinidos.
c) Requiere una reacción más rápida de lo previsto para limitar el impacto en la actividad empresarial.
d) Concierne a los cambios autorizados con antelación, que requerirán una evaluación completa.

178. En la metodología ITIL 4 el gestor de cambios: Indica la afirmación que NO es correcta.

a) Es el actor principal en la práctica Gestión de cambios.
b) Actúa como secretario del CAB.
c) Es mejor que sea una persona desconocida en la empresa.



d) Debe tener la posibilidad de decir NO a un cambio.

179. En la gestión de cambios de la metodología ITIL 4, los miembros permanentes del CAB (Change Advisory Board) son:

a) Un gestor de cambios y una persona representante de cada departamento.
b) Un gestor de cambios, la persona propietaria del servicio concernido y una única persona representante entre los diferentes departamentos de la entidad.
c) La persona propietaria del servicio concernido, expertos técnicos/as y subcontratistas.
d) Un gestor de cambios, el propietario del servicio concernido y un/una representante de la práctica Gestión de lanzamiento.

180. En la metodología ITIL 4, los objetivos de la práctica Gestión de incidentes son:

a) Restablecer el servicio.
b) Restablecer el servicio, minimizar el impacto y encontrar la causa.
c) Restablecer el servicio y minimizar el impacto.
d) Restablecer el servicio y encontrar la causa.

181. En la metodología ITIL 4, para codificar un incidente se deberá determinar la prioridad. Para ello deberemos identificar:

a) La urgencia y la gravedad.
b) El impacto y la urgencia.
c) La gravedad y el impacto.
d) Para codificar un incidente NO es necesario determinar la prioridad.

182. La diferencia entre los estados normal (o estándar) y degradado, de un servicio en la metodología ITIL 4 son:

a) El normal funciona tal y como fue concebido y el degradado no.
b) El normal funciona según el acuerdo de servicio (SLA) y el degradado no.
c) El normal funciona tal y como fue concebido y el degradado funciona con un nivel de calidad inferior.
d) El normal funciona según el acuerdo de servicio (SLA) y el degradado funciona con un nivel de calidad inferior.

183. En las mejores prácticas de la metodología ITIL 4, se han identificado dos tipos de escalada:

a) Escalada funcional y escalada vertical.
b) Escalada vertical y escalada orgánica.
c) Escalada orgánica y escalada jerárquica.
d) Escalada funcional y escalada jerárquica.



184. Entre las tareas de la práctica Gestión de cambios en la metodología ITIL 4 encontramos:

a) Asegurarse de que los procedimientos y métodos utilizados para procesar los cambios sean eficaces.
b) Asegurarse de que los cambios realizados en los elementos de configuración durante una modificación se registren en la base de datos apropiada.
c) Mantener un plan de trabajo completo de todos los cambios actuales y futuros.
d) Todas las anteriores son correctas.

185. En la metodología ITIL 4:

a) La práctica Gestión de incidentes se ocupa de las causas de las situaciones a posteriori.
b) La práctica Gestión de incidentes se ocupa de las situaciones en tiempo real.
c) La práctica Gestión de problemas se ocupa de las situaciones en tiempo real.
d) NINGUNA de las anteriores es correcta.

186. Cuál de las siguientes tareas NO pertenece a la práctica Gestión de problemas en la metodología ITIL 4:

a) Analizar situaciones de incidentes que pueden convertirse en problemas.
b) Detectar situaciones ya registradas como problemas.
c) Descartar errores conocidos.
d) Gestionar incidentes graves que se transformaron en problemas.

187. En la metodología ITIL 4, proporcionar un canal privilegiado para que las personas usuarias emitan y tramiten sus pedidos a la informática, es un objetivo:

a) De la práctica gestión de incidentes.
b) De la gestión de escalada de incidentes.
c) De la separación de roles.
d) De la práctica Gestión de solicitudes de servicio.

188. Uno de los objetivos de la práctica Gestión de solicitudes de servicio en la metodología ITIL 4 es:

a) Proporcionar un canal para escalar las quejas de las personas usuarias a la Dirección de informática.
b) Restablecer el servicio en el plazo contractual.
c) Minimizar el impacto del incidente.
d) Asignar y asegurar el presupuesto para la mejora continua.

189. ¿Cuál es el objeto principal del Esquema Nacional de Seguridad (ENS)?

a) Regular exclusivamente la protección de datos de carácter personal en el sector público.



b) Establecer los principios básicos y requisitos mínimos para una protección adecuada de la información tratada y los servicios prestados.
c) Sustituir la Ley de Procedimiento Administrativo Común en materia de administración digital.
d) Definir los estándares técnicos de interoperabilidad entre administraciones europeas.

190. ¿A qué entidades del sector privado les es de aplicación el cumplimiento del Esquema Nacional de Seguridad (ENS)?

a) A todas las entidades tecnológicas que operen en territorio español.
b) Únicamente a aquellas entidades que traten datos de nivel alto según el RGPD.
c) A las que presten servicios a entidades del sector público para el ejercicio de sus competencias y potestades administrativas.
d) A NINGUNA entidad del sector privado, ya que el ENS solo vincula a la Administración Pública.

191. Indica cuál de los siguientes NO es un principio básico del Esquema de Seguridad Nacional:

a) Seguridad integral.
b) Gestión de la seguridad basada en los riesgos.
c) Externalización obligatoria de servicios de auditoría.
d) Vigilancia continua y reevaluación periódica.

192. ¿Qué contenido mínimo debe incluir el instrumento que apruebe la política de seguridad en el Esquema de Seguridad Nacional?

a) Los roles o funciones de seguridad y la definición de sus deberes y responsabilidades.
b) El inventario completo de todos los activos de hardware de la organización
c) El presupuesto detallado anual para ciberseguridad
d) La lista nominativa de todas las personas usuarias con acceso a datos de la organización

193. En el Esquema de Seguridad Nacional, ¿qué implica el requisito mínimo de "Mínimo privilegio"?

a) Que las funciones de operación, administración y registro de actividad serán las de por defecto, sin restricciones de horario ni puntos de acceso facultados.
b) Reducir el número de administradores del sistema a uno solo por cada departamento.
c) Que solo el personal con rango de directivo puede acceder a la configuración del sistema.
d) Que los sistemas proporcionen la funcionalidad imprescindible para alcanzar los objetivos de la organización.



194. Para dar cumplimiento a los requisitos mínimos establecidos en el Esquema de Seguridad Nacional, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes. ¿En qué documento se debe formalizar la relación de medidas de seguridad seleccionadas para un sistema?

a) En el Informe Nacional del Estado de la Seguridad (INES).
b) En el Manual de Personas Usuarias del sistema de información.
c) En el pliego de prescripciones técnicas del contrato.
d) En la Declaración de Aplicabilidad.

195. En el Esquema de Seguridad Nacional, ¿con qué periodicidad mínima debe realizarse una auditoría regular ordinaria de seguridad?

a) Al menos cada dos años.
b) Anualmente.
c) Cada cuatro años, coincidiendo con la renovación de cargos.
d) Solo cuando se detecte un incidente de seguridad grave.

196. Los sistemas de información competentes serán objeto de un proceso para determinar su conformidad con el Esquema de Seguridad Nacional. En este ámbito, ¿qué requiere un sistema de categoría básica?

a) Un informe favorable emitido directamente por el Centro Criptológico Nacional.
b) Únicamente una autoevaluación para su declaración de conformidad.
c) Una auditoría de certificación obligatoria por una entidad acreditada.
d) No requiere NINGÚN procedimiento de determinación de conformidad.

197. En el Esquema de Seguridad Nacional, ¿quién es el órgano competente para validar y publicar los "perfiles de cumplimiento específicos"?

a) La Agencia Española de Protección de Datos (AEPD).
b) El Centro Criptológico Nacional (CCN).
c) El Ministerio de Hacienda y Función Pública.
d) La Secretaría de Estado de Digitalización e Inteligencia Artificial.

198. En el Esquema de Seguridad Nacional a fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información, ¿qué dimensiones de la seguridad se tendrán en cuenta?

a) Solo la confidencialidad y la disponibilidad.
b) Costo de reposición, tiempo de recuperación, hardware afectado y software afectado.
c) Disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.
d) Solo costo de reposición y tiempo de recuperación.



199. Según el Esquema de Seguridad Nacional, ¿cuáles son los grupos en los que se estructuran las medidas de seguridad?

a) Marco organizativo, Marco operacional y Medidas de protección.
b) Físicas, Lógicas y Organizativas.
c) Prevención, Detección y Respuesta.
d) Básicas, Medias y Altas.

200. Según el Esquema de Seguridad Nacional, ¿qué facultad tiene el CCN-CERT para el cumplimiento de sus funciones de soporte y coordinación en la resolución de incidentes?

a) Puede sancionar económicamente a las entidades que no hayan aplicado las medidas de seguridad preventivas.
b) Tiene la potestad de sustituir al personal técnico de la entidad afectada hasta que el incidente esté resuelto.
c) Puede recabar informes, registros de auditoría, configuraciones de los sistemas afectados y cualquier otra información o soporte necesario para la investigación.
d) Todas las anteriores son correctas.