CONVOCATORIA 191/21.

EJERCICIO PRUEBAS SELECTIVAS DE ACCESO AL CUERPO A2-02 SUPERIOR DE GESTIÓN EN INGENIERÍA TÉCNICA EN INFORMÁTICA DE LA ADMINISTRACIÓN DE LA GENERALITAT, SECTOR ADMINISTRACIÓN ESPECIAL, TURNO PROMOCIÓN INTERNA**.**

EL PLAZO PARA FORMULAR ALEGACIONES ES DE **5 DÍAS HÁBILES** DESDE LA PUBLICACIÓN

PLANTILLA DE RESPUESTAS

Nº	RESPUESTA	Nº	RESPUESTA
1	B	31	A
2	D	32	D
3	B	33	B
4	B	34	D
5	C	35	A
6	C	36	A
7	B	37	A
8	C	38	A
9	A	39	D
10	D	40	A
11	B	41	B
12	A	42	D
13	C	43	B
14	D	44	B
15	D	45	A
16	A	46	C
17	C	47	C
18	D	48	C
19	B	49	C
20	A	50	D
21	C	51	B
22	B	52	D
23	D	53	B
24	A	54	D
25	D	55	B
26	C	56	A
27	C	57	D
28	B	58	D
29	D	59	B
30	B	60	D

GENERALITAT VALENCIANA
Conselleria de Hacienda, Economía y Administración Pública

PRUEBAS SELECTIVAS DE ACCESO AL CUERPO A2-02 SUPERIOR DE GESTIÓN EN INGENIERÍA TÉCNICA EN INFORMÁTICA DE LA ADMINISTRACIÓN DE LA GENERALITAT, SECTOR ADMINISTRACIÓN ESPECIAL.

PROMOCIÓN INTERNA.

(PROCESO DE ESTABILIZACIÓN)

CONVOCATORIA 191/21

EJERCICIO ÚNICO

TIEMPO REALIZACIÓN:
(1 hora y 15 minutos, 75 minutos)

1. Indique cuál de los siguientes NO es un eje estratégico del plan GEN Digital 2025:

A) Gobierno sostenible.

B) Sostenibilidad climática.

C) Educación digital.

D) Justicia moderna.

2. Indique cuál de las siguientes líneas estratégicas NO se corresponde con el eje de gobierno inteligente del plan GEN Digital 2025:

A) Acercar la Administración a las personas.

B) Mejorar la eficiencia de la Administración.

C) Eliminar el papel del proceso administrativo.

D) Desarrollar un marco de vivienda sostenible.

3. En el marco ITIL v4, en el SVS (Service Value System), se definen como componentes núcleo o principales (indicar la opción CORRECTA):

A) Principios guía o básicos, gobernanza, cadena de valor del servicio, diseño y transición.

B) Principios guía o básicos, gobernanza, cadena de valor del servicio, prácticas.

C) Principios guía o básicos, gobernanza, cadena de valor del servicio, entrega y soporte.

D) Principios guía o básicos, gobernanza, cadena de valor del servicio, gestión del proyecto.

4. ITIL v4 presenta un modelo de gestión que se basa en lo que se denominan dimensiones. El número de dimensiones de dicho modelo es de (indique la opción CORRECTA):

A) 5 dimensiones.

B) 4 dimensiones.

C) 6 dimensiones.

D) 3 dimensiones.

5. En relación con las buenas prácticas en la dirección de proyectos, indique cuál de las siguientes opciones es la INCORRECTA:

A) Los riesgos son un aspecto de la incertidumbre.

B) En el alcance de un proyecto se debe definir qué se incluye y qué se excluye explícitamente.

C) Los interesados de un proyecto son aquellas personas o departamentos de tu organización que pueden verse afectados por el desarrollo del proyecto.

D) Alcance, tiempo y costes están relacionados en un proyecto. Cualquier cambio en una de ellas afectará al menos a una de las otras dos.

6. En relación con la gestión de riesgos en la dirección de proyectos, indique cuál de las siguientes opciones es la CORRECTA:

A) Ignorar los riesgos y esperar que no afecten el proyecto.

B) Transferir todos los riesgos a un tercero.

C) Mitigar los riesgos mediante la implementación de estrategias preventivas.

D) Evitar cualquier proyecto que presente riesgos.

7. En el framework SAFe versión 6.0, el acrónimo ART (Agile Release Train) se define como:

A) Sistema KANBAN utilizado para capturar y administrar nuevas funcionalidades.

B) Equipo de trabajo que desarrolla nuevas funcionalidades de manera incremental.

C) Período breve de tiempo fijo en el que un equipo de Scrum trabaja para completar una cantidad de trabajo establecida.

D) Software de gestión propuesto en SAFe V6 para aquellos proyectos en los que la configuración es *Large Solution, Portfolio o Full*.

8. ¿Cuál de los siguientes principios no forma parte de los 12 principios del Manifiesto Ágil (https://agilemanifesto.org/iso/es/principles.html)?

A) Aceptamos que los requisitos cambien, incluso en etapas tardías del desarrollo. Los procesos Ágiles aprovechan el cambio para proporcionar ventaja competitiva al cliente.

B) El software funcionando es la medida principal de progreso.

C) La simplicidad, o el arte de maximizar la cantidad de trabajo realizado, es esencial.

D) Nuestra mayor prioridad es satisfacer al cliente mediante la entrega temprana y continua de software con valor.

9. ¿Qué es el control de versiones de software?

A) Un sistema que registra los cambios realizados en un archivo o conjunto de archivos a lo largo del tiempo.

B) Un método para nombrar las versiones de software utilizando metodologías ágiles.

C) Un proceso para eliminar versiones antiguas de software.

D) Un sistema para rastrear el uso de software obsoleto por parte de los usuarios.

10. ¿Cuál de las siguientes opciones NO es una función clave de un ingeniero de DevOps?

A) Gestión de proyectos.

B) Diseñar y mejorar la infraestructura TI.

C) Revisión de desempeño y benchmarking.

D) Desarrollo de software.

11. Según el artículo 8 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), la Seguridad del Sistema debe contemplar las siguientes medidas (Indique la respuesta correcta):

A) Prevención, detección, evaluación y contención.

B) Prevención, detección, respuesta y conservación.

C) Mantenimiento, detección, evaluación y documentación.

D) Mantenimiento, evaluación, documentación y actuación.

12. Según el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), ¿qué organismo, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación? (Indique la respuesta correcta):

A) El Centro Criptológico Nacional.

B) La Secretaría de Estado de Digitalización e Inteligencia Artificial.

C) La Agencia de Protección de Datos.

D) La Comisión Sectorial de Administración Electrónica.

13. De acuerdo con el *Libro II – Catálogo de Elementos* de la metodología "MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" aquella información sometida a normativa específica de control de acceso y distribución, es decir aquella cuya confidencialidad es especialmente relevante se clasifica como:

A) Nivel alto, medio y bajo.

B) Nivel alto, medio y básico.

C) Nivel confidencial, difusión limitada, sin clasificar y de carácter público.

D) No define una clasificación concreta en esta materia, sino que establece la ley de secretos oficiales vigente en cada momento como el marco de referencia.

14. En la OWASP Testing Guide 4.0, y más concretamente en la sección: Pruebas de Seguridad de aplicaciones web, se detalla las pruebas que han de realizarse en 11 secciones. Indique cuál de las siguientes NO se encuentra en dicha relación

A) *Identity Management Testing* (Pruebas de administración de identidad).

B) *Session Management Testing* (Pruebas de administración de sesión).

C) *Cryptography* (Pruebas para Criptografía débil).

D) *Server Side Testing* (Pruebas en el lado del servidor).

15. La Guía de Seguridad de las TIC CCN-STIC 823: Utilización de servicios en la nube del centro criptográfico nacional, enuncia un decálogo de recomendaciones para la utilización de servicios en la nube. De las siguientes opciones cuál NO pertenece a dicho decálogo:

A) Elabora una normativa de seguridad específica para los usuarios de la nube.

B) Realizar un seguimiento periódico del cumplimiento de los Acuerdos de Nivel de Servicio (SLA), establecidos con el CSP.

C) Acogerse a un perfil de cumplimiento específico (en caso de que sea de aplicación).

D) En caso de que el CPD se encuentre fuera de la Comunidad Europea, se deberá realizar un análisis de riesgos, para identificar requisitos adicionales de seguridad, que se reflejarán en la declaración de aplicabilidad.

16. De las siguientes herramientas del CCN, indique cuál es una solución para la automatización de las tareas básicas realizadas por un auditor de seguridad sobre equipos de comunicaciones como enrutadores, conmutadores y cortafuegos:

A) ROCÍO.

B) REYES.

C) CLARA.

D) CARMEN.

17. ¿Cuál de las siguientes respuestas NO es una clasificación de los ciberincidentes registrada en la Guía para la Gestión de ciberincidentes del CCN-STIC-817?:

A) Intento de intrusión.

B) Compromiso de la información.

C) Criptografía.

D) Contenido abusivo.

18. Según el Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat, indique qué afirmación es INCORRECTA:

A) La política de seguridad regulada en el presente decreto deberá aplicarse a toda la información bajo la responsabilidad de la Administración de la Generalitat y sus entidades autónomas, así como al tratamiento del que pueda ser objeto. Esta consideración no se limita a los datos de carácter personal y es independiente de que el tratamiento sea manual o automatizado.

B) La presente política se desarrollará en un conjunto de documentos cuyo objetivo es facilitar que el tratamiento de información se realice de acuerdo con los objetivos y principios expuestos en los artículos anteriores.

C) Los responsables de seguridad incluirán en sus memorias anuales un apartado sobre el grado de cumplimiento y eficacia de esta normativa y otro proponiendo acciones de mejora. Estas memorias se presentarán al responsable en materia de seguridad de la información que corresponda para que apruebe las actuaciones oportunas.

D) El incumplimiento de la política de seguridad expresada en este decreto tendrá consecuencias penales, según lo dispuesto en el Código Penal.

19. El artículo 2 del Decreto 130/2012, de 24 de agosto, del Consell, establece que la organización de la seguridad regulada en el presente decreto es aplicable a las consellerias de la Generalitat, así como a sus entidades autónomas dependientes, a las que se refiere el artículo 5.1 del texto refundido de la Ley de hacienda pública de la Generalitat exceptuando:

A) las entidades locales.

B) La conselleria con competencias en sanidad y a la Agència Valenciana de Salut.

C) La conselleria con competencias en educación.

D) La conselleria con competencias en Sanidad y a la conselleria con competencias en Educación.

20. Podemos definir la inteligencia artificial distribuida como la disciplina o enfoque que:

A) Estudia la solución cooperativa de problemas mediante un conjunto de agentes distribuidos, donde ninguno posee toda la información para resolver el problema.

B) Estudia la solución cooperativa de problemas mediante un conjunto de agentes distribuidos, donde todos poseen toda la información para resolver el problema.

C) Estudia la solución de problemas mediante la ejecución secuencial de la verdad imparcial entre distintos agentes distribuidos en un centro de procesamiento de datos.

D) Estudia la solución de problemas que requieren del algoritmo estándar del reloj o de segunda oportunidad.

21. En los métodos de búsqueda ciegos o no informados, la búsqueda primero en profundidad es una estrategia:

A) En la que se busca primero en los estados menos prometedores (breath-first).

B) En la que se busca primero los estados siguiendo el Algoritmo A*, donde el coste = coste hasta ahora + Poda α-β.

C) Que sigue un camino del árbol hasta el final. Si no se encuentra la solución en ese camino se retrocede y se prueba con otro camino. Ese retroceso se denomina backtracking.

D) Que sigue un camino del árbol. Si no se encuentra la solución en ese camino se detiene y finaliza la búsqueda.

22. Concepto definido en 1959 por Arthur Samuel como campo de estudio que da a las computadoras la capacidad de aprender sin ser explícitamente programadas:

A) Aprendizaje profundo (Deep Learning).

B) Aprendizaje automático (Machine Learning).

C) Inteligencia artificial (Artificial Intelligence).

D) Red neuronal artificial (Artificial Neural Network).

23. En el campo de los métodos de aprendizaje supervisado, ¿cómo se denomina la red de neuronas artificiales más sencilla compuesta únicamente por una capa de neuronas de entrada y otra capa de neuronas de salida?

A) FOAF.

B) Red bayesiana de primer orden.

C) RETE.

D) Perceptrón.

24. En el ciclo de vida de un proyecto big data se encuentran las siguientes fases:

A) Adquisición o captura de datos, análisis, transformación, almacenamiento y explotación.

B) Planificación, desarrollo, pruebas y mantenimiento.

C) Inicio, planificación, ejecución, supervisión y cierre.

D) Análisis, síntesis, diseño e implantación.

25. Se entiende por big data un conjunto de datos que, por su volumen y complejidad, no pueden ser procesados por métodos tradicionales en computadoras tradicionales. Indique cuál es la opción correcta desde la perspectiva del procesamiento.

A) En el procesamiento por lotes (*batch*), su principal orientación es hacia el procesamiento de grandes volúmenes de datos dinámicos de manera no escalable.

B) En el procesamiento por lotes (*batch*), su principal orientación es hacia el procesamiento de grandes volúmenes de datos dinámicos de manera escalable.

C) En el procesamiento streaming, su principal orientación es hacia el procesamiento de un flujo continuo de datos, donde prima la velocidad. Son sistemas donde se debe asegurar una latencia alta.

D) En el procesamiento streaming, su principal orientación es hacia el procesamiento de un flujo continuo de datos, donde prima la velocidad. Son sistemas donde se debe asegurar una baja latencia.

26. Seleccione cuál de las siguientes afirmaciones NO es cierta sobre la tecnología RPA (Robotic Process Automation):

A) Es una tecnología donde los robots ejecutan procesos, simulando acciones humanas.

B) Las tareas que realiza un humano con un teclado y un ratón pueden ser reproducidas por un robot.

C) RPA permite realizar tareas de manera rápida y con un mínimo de errores, liberando el tiempo de las personas en actividades repetitivas y que requieran del juicio humano.

D) Un robot ejecuta uno o varios procesos automatizados. Un proceso automatizado realiza de forma automática las tareas manuales y repetitivas.

27. Seleccione cuál de las siguientes afirmaciones NO es cierta sobre la tecnología RPA (Robotic Process Automation):

A) La hiperautomatización contempla el uso de la tecnología RPA.

B) Tecnologías como el reconocimiento óptico de caracteres (OCR), procesamiento de lenguaje natural (NLP) e Inteligencia Artificial son usadas para ampliar las capacidades de RPA.

C) RPA es una tecnología intrusiva, donde los entornos y sistemas existentes deben adaptarse a esta tecnología.

D) Esta tecnología es candidata a ser aplicable en servicios de centro de atención telefónica (*call center* o *contact center)*.

28. Los centros de proceso de datos o *datacenters* deben cumplir una serie de características de seguridad física, ¿cuál de las siguientes NO es una buena medida de seguridad?

A) Instalación de un Circuito Cerrado de Televisión (CCTV).

B) Debe estar explícitamente señalizado.

C) Debe tener un control de acceso a las instalaciones.

D) Las puertas deben estar provistas de una cerradura.

29. ¿Cuál de las siguientes NO es una ventaja de la hiperconvergencia?

A) Simplificación de la gestión.

B) Mayor eficiencia.

C) Reducción de costos.

D) Aumento de la complejidad de la red.

30. ¿Qué es la hiperconvergencia?:

A) Un tipo de software antivirus.

B) Una tecnología que combina almacenamiento, computación y redes en una sola solución.

C) Un tipo de infraestructura de red.

D) Un protocolo de enrutamiento.

31. Cómo se denomina el tipo de servicio de informática en la nube que ofrece recursos esenciales de proceso, almacenamiento y redes a petición que son de pago por uso:

A) Infrastructure as a Service (IaaS).

B) Platform as a Service (PaaS).

C) Software as a Service (SaaS).

D) Analytics as a Service (AaaS).

32. Desde el punto de vista de la computación en la nube, Gmail ofrecido por Google es un ejemplo de:

A) PaaS (Platform as a Service).

B) CaaS (Communication as a Service).

C) IaaS (Infrastructure as a Service).

D) SaaS (Software as a Service).

33. Señale la opción CORRECTA según la Resolución de 28 de marzo de 2018, de la Dirección General de Tecnologías de la Información y las Comunicaciones, por la que se establecen los criterios de estandarización tecnológica y las políticas de uso correcto del puesto de trabajo normalizado de los usuarios TIC en la Administración de la Generalitat y de sus organismos autónomos, publicada en el DOGV el 23 de abril de 2018, en referencia a su punto sexto:

A) No se permite alterar la configuración del software ni del sistema operativo de los Puestos de Trabajo Normalizados, ni desinstalar o instalar aplicaciones, salvo que sean de software libre o gratuito.

B) Todo software privativo debe tener su licencia legal asociada, al corriente de pago y custodiada por la DGTIC.

C) Los equipos informáticos están destinados al uso personal del usuario.

D) Al terminar la jornada laboral el usuario TIC no es necesario apagar completamente el Puesto de Trabajo Normalizado y todos sus periféricos conectados o relacionados con él ya que hay rutinas que lo hacen automáticamente.

34. Señale la opción CORRECTA según la Resolución de 28 de marzo de 2018, de la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) por la que se establecen los criterios de estandarización tecnológica y las políticas de uso correcto del puesto de trabajo normalizado de los usuarios TIC en la Administración de la Generalitat y de sus organismos autónomos, publicada en el DOGV el 23 de abril de 2018, en referencia a su punto tercero:

A) La DGTIC mantendrá en su portal www.dgtic.gva.es una lista de elementos software estándares para el Puesto de Trabajo Normalizado, dicha lista no podrá sufrir revisiones ni actualizaciones.

B) Para conocer las versiones de cada software que forman parte del Puesto de Trabajo Normalizado, se tendrá en cuenta el plan de versiones o *release plan* en los portales web de cada producto, aceptándose en el Puesto de Trabajo Normalizado la versión actual y las dos anteriores con soporte en cada momento.

C) Para los puestos normalizados de pruebas se permitirá cualquier versión para pruebas y diagnósticos, siempre que cuente con la autorización del jefe de servicio.

D) Excepcionalmente, y previa autorización por parte de la DGTIC, se permitirá la existencia de un software en versiones no actualizadas, siempre y cuando no afecte a la arquitectura del Puesto de Trabajo Normalizado en su versión actual en lo que se refiere a la interacción con otras aplicaciones o herramientas.

35. ¿Cuál de las siguientes características es un inconveniente de la Virtualización de escritorio (VDI)?

A) Disminución del rendimiento.

B) Administración simplificada.

C) Ahorro de Espacio.

D) Alta Disponibilidad.

36. ¿Qué componente de la Virtualización de escritorio (VDI) se encarga de ejecutar las máquinas virtuales del escritorio?

A) El hipervisor.

B) El cortafuegos.

C) El conmutador de red.

D) El servidor DNS.

37. Según el Reglamento UE 2016/679 de 27 de abril, en lo que se refiere a su ámbito de aplicación material, según lo indicado en el artículo 2, este reglamento no se aplica al tratamiento de datos personales (indique la opción CORRECTA):

A) 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.

B) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones administrativas o de ejecución de sanciones administrativas, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

C) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones administrativas y penales o de ejecución de sanciones administrativas y penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

D) Por parte de las autoridades competentes con fines de prevención, monitorización, detección o enjuiciamiento de infracciones administrativas y penales o de ejecución de sanciones administrativas y penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

38. Con relación a la Agencia Española de Protección de Datos y su consejo consultivo, (indique la respuesta CORRECTA):

A) El consejo consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

B) El consejo consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al trimestre.

C) El consejo consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al año.

D) El consejo consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, bimensualmente.

39. Según el Real Decreto 203/2021, la carpeta ciudadana es (indique la respuesta CORRECTA):

A) Un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información y al seguimiento de los trámites administrativos que afecten a sus familiares de segundo grado.

B) Permite el acceso a sus comunicaciones, pero no a las notificaciones de los trámites administrativos.

C) Permite el seguimiento del estado de tramitación de los procedimientos en los que tenga curiosidad, sea o no interesado.

D) Un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente.

40. De acuerdo con el RD 203/2021 (indique la respuesta CORRECTA):

A) El sistema de código seguro de verificación deberá garantizar, entre otros, el origen e integridad de los documentos mediante el acceso a la sede electrónica o sede electrónica asociada correspondiente.

B) Los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas no están obligados a relacionarse electrónicamente en el ejercicio de dicha representación.

C) La capacidad de representación nunca podrá acreditarse mediante certificado electrónico cualificado de representante.

D) Cualquier modificación del documento generado dará lugar a un nuevo documento con el mismo código seguro de verificación, que su predecesor.

41. La arquitectura de microservicios se define como un estilo de arquitectura para el desarrollo de SW que consiste en construir una aplicación como un conjunto de pequeños servicios, los cuales se ejecutan en su propio proceso y se comunican con mecanismos ligeros. Cuál de las siguientes características NO es correcta:

A) Bajo acoplamiento.

B) El componente de negocio es acordado entre todos los microservicios.

C) Mantenibilidad.

D) Los microservicios son independientes entre sí.

42. Indique cuál de los siguientes se trata de un principio guía que defina reglas básicas para el desarrollo, mantenimiento y uso de arquitecturas SOA:

A) Conceptualización.

B) Alta dependencia de recursos externos.

C) Contrato de caja blanca.

D) Reutilización.

43. Un CMS (Content Management System)

A) Dispone una única parte, la CMA.

B) Dispone de dos partes: la parte web pública y la parte web privada.

C) Dispone de dos partes: la parte visible LMS y la de MHV.

D) Dispone de una única parte: la parte web pública, a la que se accede mediante usuario y contraseña.

44. Entre las principales características de un portafirmas se encuentra:

A) No poder utilizar flujos desde aplicaciones externas mediante servicios web.

B) La capacidad de crear peticiones o flujos de firma incluyendo diferentes firmantes que pueden firmar en paralelo o en cascada, y usuarios que otorgan visto bueno.

C) Calcular un resumen o *hash* digital de longitud variable a partir del contenido parcial de los pies de firma del documento a firmar.

D) Volver a calcular el resumen o *hash* a partir del contenido del documento a firmar.

45. Según se indica en el artículo 11 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, las Administraciones públicas (Indique la respuesta CORRECTA):

A) Usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

B) Sólo podrán utilizar estándares abiertos para que todos los ciudadanos puedan acceder a estos.

C) Podrán utilizar los estándares no abiertos que considere el responsable de gestión de documentos.

D) Utilizarán los formatos que sean de uso común entre los ciudadanos y no estarán obligadas a admitir otros formatos al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología.

46. La Plataforma Autonómica de Interoperabilidad se constituye en una pieza fundamental para la modernización de la Administración pública, al facilitar: (Indique la respuesta CORRECTA)

A) Impermeabilización de los sistemas de intercambio de información.

B) Minimización del trabajo no realizado en el proceso de solicitudes.

C) Independencia de los orígenes de información (interlocutor único).

D) Aumento de la información solicitada al ciudadano.

47. El Sistema de Interconexión de Registros (SIR) es la Plataforma que permite el intercambio de asientos electrónicos de registro entre todas las Administraciones Públicas, cuál de las siguientes afirmaciones NO es cierta:

A) El intercambio de información se realiza de forma segura y con conformidad legal.

B) Las aplicaciones o servicios de registro deben estar certificados en SICRES 3.0 y utilizar el directorio común DIR3.

C) La conexión e intercambio de registros en SIR solo puede realizarse usando servicios comunes en red, como ORVE o GEISER.

D) En caso de no utilizar Servicios comunes en red y se utilicen aplicaciones propias estas deben superar un proceso de certificación que verifique el cumplimiento de la norma y otros requisitos técnicos de conexión con SIR.

48. Los sistemas de identificación permitidos en la plataforma Cl@ve son:

A) Claves concertadas (Cl@ve ocasional y Cl@ve permanente), certificados electrónicos (incluyendo certificados ACCV) y tarjeta de coordenadas.

B) Únicamente certificados electrónicos (incluyendo el DNI-e y certificados ACCV).

C) Claves concertadas (Cl@ve ocasional y Cl@ve permanente) y certificados electrónicos (incluyendo el DNI-e).

D) Únicamente claves concertadas (Cl@ve ocasional y Cl@ve permanente).

49. De acuerdo con el "PAE Portal Administración Electrónica" con relación a "Firmas Longevas", los formatos AdES (forma genérica de llamar a los formatos CAdES, XAdES y PAdES) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional que garantiza la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. En ese contexto, ¿cómo se denomina el formato de firma que añade sellos de tiempo al formato "AdES C"?

A) AdES T.

B) AdES CT.

C) AdES X.

D) AdES A.

50. ¿Cuál de los siguientes tipos de archivos se utiliza comúnmente en los SIG?

A) Archivos de texto.

B) Archivos de audio.

C) Archivos de imagen.

D) Archivos geoespaciales.

51. ¿Cuáles son los tipos de objetos vectoriales utilizados en un Sistema de Información Geográfica?

A) Puntos, líneas y eventos.

B) Puntos, líneas y polígonos.

C) Líneas y proyecciones.

D) Líneas, polígonos y recorridos.

52. ¿Cuál de los siguientes NO es un componente de SD-WAN?

A) Controller.

B) Orchestrator.

C) Edge.

D) Core.

53. Según el CNAF (Cuadro Nacional de Atribución de Frecuencias) ¿Qué subbandas de frecuencias se destinan para redes de servicios de seguridad de las Fuerzas y Cuerpos de Seguridad del Estado y redes de servicios de emergencia en todo el territorio nacional? (Indique la respuesta CORRECTA):

A) 328,600 MHz a 335,400 MHz.

B) 380-385 MHz y 390-395 MHz.

C) 406,1-430 MHz y 440-470 MHz.

D) 433,050 MHz a 434,790 MHz.

54. Las redes de comunicaciones de emergencias dispondrán de las siguientes características (Indique la respuesta INCORRECTA):

A) Fiabilidad y disponibilidad las 24 horas del día.

B) Respaldo de los sistemas de energía y de transporte redundantes para garantizar la continuidad del servicio.

C) Capacidad de priorización del tráfico de las llamadas de emergencia.

D) Integrar sistemas tipo Söll, o análogos, para facilitar las comunicaciones entre las distintas flotas de una red de emergencias.

55. Las siguientes características están relacionadas con 5G (Indique la respuesta INCORRECTA):

A) Velocidad de descarga de hasta 10 Gbps.

B) Latencia de hasta 50 ms.

C) Bajo consumo de energía: 90% menor respecto a 4G.

D) Alta disponibilidad de 99,999%.

56. Las siguientes afirmaciones están relacionadas con 5G (Indique la respuesta INCORRECTA):

A) Alcance: Las celdas 5G tienen un alcance en entorno urbano entre 10 y 20 km. A partir de 6,65 km comienza a haber degradación de forma lineal.

B) Aplicaciones en telemedicina: Posibilidad realizar monitorización y asistencia quirúrgica remota de pacientes en tiempo (casi) real.

C) Uso de espectro de ondas milimétricas (mmWave) que permite ofrecer una velocidad de descarga teórica de 20 gigabits por segundo.

D) Ciudades inteligentes - IoT: Capaz de soportar 1 millón de dispositivos en 1 Km2.

57. Indique cuál de los siguientes protocolos NO es un protocolo de autenticación autorización y accounting:

A) RADIUS.

B) DIAMETER.

C) TACACS.

D) AES.

58. En el contexto de la seguridad inalámbrica. ¿Cuál de los siguientes protocolos usados en la seguridad en el acceso a una red WiFi es el menos seguro y por ello el menos recomendado para su uso?

A) WPA.

B) WPA2.

C) WPA3.

D) WEP.

59. Las VPN de nivel de transporte implementan mecanismos de seguridad para proteger las comunicaciones de cualquier tipo de aplicación. Esto permite establecer comunicaciones seguras sin necesidad de realizar ninguna modificación en el software de aplicación. Uno de los protocolos de seguridad más empleados por las VPN en el nivel de transporte es (indicar la opción CORRECTA):

A) IPSec.

B) TLS.

C) SSH.

D) SNMP.

60. En IPsec, el protocolo AH (indique la opción CORRECTA):

A) Aporta confidencialidad (cifrado) en la carga útil (*payload*) mediante el cálculo de un valor MAC (Message Authentication Code).

B) Aporta confidencialidad (cifrado) en la carga útil (*payload*) mediante el uso de un algoritmo AEAD (Authenticated Encryption with Associated Data).

C) Aporta confidencialidad (cifrado) en la carga útil (*payload*) mediante el uso de un valor ICV (Integrity Check Value).

D) El protocolo AH no cifra el contenido del paquete y, por lo tanto, no aporta confidencialidad.