Expedient núm.: 2808/2020
Procediment: Seleccions de Personal i Provisions de Llocs de treball
Assumpte: Oposició per a cobrir de manera interina una plaça de personal funcionari Cap del departament d'Informàtica.

SEGUNDO EJERCICIO. PRUEBA TIPO TEST

De carácter obligatorio y eliminatorio.

Consistirá en responder por escrito un cuestionario tipo test de 50 preguntas más cinco preguntas de reserva, con cuatro respuestas alternativas, de las cuales solo una es correcta, referidas al temario que figura como anexo. Las personas aspirantes marcarán las contestaciones en las correspondientes hojas de examen.

Este ejercicio se calificará de 0 a 30 puntos, siendo eliminadas aquellas personas aspirantes que no obtengan la puntuación mínima de 15 puntos.

El criterio de corrección será el siguiente: cada pregunta respondida correctamente se valorará con 0,60 puntos; las preguntas no resueltas, tanto si figuran las cuatro opciones en blanco como si figuran con más de una respuesta, no se valorarán. Las preguntas con respuesta errónea se penalizarán con un cuarto del valor asignado a la respuesta correcta (-0,15).

En caso de que el tribunal acuerde la anulación de alguna o algunas de las preguntas, por haber detectado de oficio algún error manifiesto durante la realización del ejercicio o porque este se detecta como consecuencia de las alegaciones que posteriormente se presenten, se tendrán en consideración las preguntas de reserva. Estas se escogerán según el orden de prelación en que se encuentren en el propio ejercicio.

Si a consecuencia de las anteriores operaciones se agotan las preguntas de reserva y el tribunal acuerda anular alguna pregunta más, el valor de cada pregunta se ajustará para que la puntuación máxima sea de 30 puntos.

El tiempo para desarrollar este ejercicio será de 120 minutos.

No se corregirán anotaciones realizadas en los enunciados, sólo en la hoja de respuestas

1) **Las redes de comunicación inalámbricas se pueden clasificar según diferentes criterios. Uno de dichos criterios es el alcance geográfico máximo de la red. En este sentido, indique cuál es la afirmación que presenta los tipos de red de ordenadores ordenadas de menor a mayor alcance máximo de la red:**
   a) WBAN, WMAN, WLAN, WWAN
   b) WMAN, WPAN, WLAN, WWAN
   c) WBAN, WPAN, WWAN, WMAN
   d) Ninguna de las anteriores

2) **En el año 2019 se presentó un nuevo modelo comercial de un teléfono móvil que incorpora un chip que utiliza la tecnología UWB. Indique cuál es la respuesta correcta:**
   a) UWB hace referencia a una tecnología de transmisión de paquetes de datos que tiene como base de funcionamiento las tecnologías *spread spectrum* (SS).
   b) UWB hace referencia a un subconjunto de normas de la IEEE específicas para conexiones utilizando una WLAN.
   c) UWB es una tecnología WPAN que permite transmitir paquetes de información a distancias del orden de pocos metros.
   d) UWB es un estándar en el que se incorpora un dispositivo central que permite conectar los teléfonos y proporciona un ancho de banda entre los ordenadores conectados a una red inalámbrica.

3) **En la actualidad hay una tendencia a implantar servicios de telefonía IP, que posibilitan la utilización de las mismas redes para datos y voz. Indique cuál es la afirmación correcta:**
   a) El concepto de VoIP hace referencia a la tecnología que permite transmitir voz utilizando un protocolo de IP.
   b) La telefonía IP hace referencia los dispositivos necesarios para poder transmitir voz a través de la LAN, entre los cuales destacan el PDX y el protocolo SIP.
   c) La principal diferencia entre VoIP y VoLTE radica en la utilización de UWB como tecnología base en las comunicaciones.
   d) Ninguna de las anteriores.

4) **Uno de los principales inconvenientes de las redes inalámbricas es la presencia de ruido, que limita la capacidad de transmisión a través del canal. Considerando una red de ancho de banda H Hz y una señal de potencia S que se transmite en un canal con un ruido de potencia R, Shannon determinó que la capacidad máxima de un canal viene dada por la fórmula:**
   a) Número máximo de bits/s = H 10^2 Log (1+S/N)
   b) Número máximo de bits/s = H 10 Log_2 (1+S/N)
   c) Número máximo de bits/s = H Log_2 (1+S/N)
   d) Ninguna de las anteriores

5) En la transmisión de voz por IP existe una amplia variedad de protocolos de comunicación destinados a regular las comunicaciones. Indique la afirmación incorrecta:

a) El protocolo SCCP es propiedad de Cisco Systems y se define como un conjunto de mensajes que se envían entre los teléfonos IP y el *Call Manager*. Para el tráfico de datos se utilizan los protocolos RTP, UDP, IP.
b) El protocolo IAX2 es un protocolo utilizado por el programa de código abierto Asterisk. Soporta la funcionalidad denominada *Trunking (red)* que permite conectar dos *switch*, *routers* o servidores por medio de dos cables en paralelo en modo *half-duplex.*
c) El protocolo Jingle, en cuyo diseño participó Google, es una extensión del protocolo XMPP (*Extensive Messaging and Presence Protocol*) que permite la transferencia de información *peer-to-peer*.
d) El protocolo Skype utiliza software propietario y se caracteriza por mantener comunicaciones P2P y utilizar el algoritmo de cifrado AES de 256 bits para las transmisiones de voz, ficheros y mensajes. En la versión de pago se utiliza el algoritmo RSA para el acceso a correo de voz.

6) Las colisiones de mensajes en las transmisiones por red constituyen un problema que disminuye el rendimiento de la red. Indique cuál es la afirmación correcta:

a) El protocolo CSMA/CD consiste en que, cuando un equipo desea enviar una información, primer escucha el canal para saber si otro equipo está transmitiendo. Si el canal está ocupado, entonces espera hasta que el canal quede libre para empezar a transmitir. Dicho protocolo es propio de las redes inalámbricas.
b) El protocolo CSMA/CA consiste en que cada equipo anuncia su intención de transmitir antes de hacerlo, para evitar colisiones de datos entre los paquetes de datos. De esta manera, el resto de equipos de la red pueden saber cuándo hay colisiones. En este caso, en lugar de trasmitir la trama cuando el medio está libre, se espera un tiempo aleatorio antes de enviar las tramas.
c) El protocolo CSMA/CA, propio de las redes inalámbricas, se basa en la una asignación de tiempos de transmisión de los diferentes equipos, de manera que cada uno de ellos dispone de un tiempo limitado para realizar sus transmisiones. En caso de finalizar su asignación de tiempo, entonces incorpora un paquete de finalización intermedia.
d) Ninguna de las anteriores

7) El problema de las colisiones de transmisión en redes inalámbricas se hace especialmente importante a causa de algunos motivos. Indique cuál es la afirmación correcta:

a) El *hidden terminal problem*, que viene provocado por la insistencia en el envío de paquetes por un terminal emisor cuando el receptor no recibe correctamente la identificación del emisor, rechazando el mensaje. Dicho rechazo provoca un incremento en el número de mensajes que circulan y, por consiguiente, un incremento en el número de colisiones.
b) El *blocked terminal problem*, que viene provocado por obstáculos físicos en el espacio geográfico o la distancia. Entonces puede ocurrir que un equipo compruebe el canal, lo encuentre libre e inicie una transmisión hacia otro nodo que ya está recibiendo una trama desde otra estación.
c) El *fading*, que describe el problema que se provoca a causa de la atenuación de la señal cuando ésta se propaga a través del aire. La consecuencia es que dos estaciones pueden transmitir simultáneamente hacia el mismo nodo y provocar en el receptor colisiones no advertidas.
d) El *exposed node*, que consiste en que un nodo que ha sido designado como nodo repetidor inicia su transmisión al mismo tiempo que recibe un paquete para retransmitir. Entonces se produce la transmisión de dos mensajes al mismo tiempo, provocando una colisión.

8) Existe una equivalencia entre el modelo OSI y la especificación IEEE 802. Indique cuál de las siguientes es una afirmación incorrecta:

a) Las capas MAC y PHY equivalen de manera lógica con las funciones de las capas de enlace y física del modelo OSI.
b) Las funcionalidades de la capa de física del modelo OSI son equivalentes a las descritas en el protocolo 802.2.
c) Las capas MAC y PHY aparecen descritas en los protocolos 802.3 (Ethernet), 804.4 (Token Bus), 802.5 (Token Ring) y 802.11 (WLAN).
d) La capa de Control de Acceso Lógico (LLC) se describe en el estándar 802.2.

---

9) Una *Wireless Mesh Networks* (WMN) es un tipo de red inalámbrica. Indique cuál de las siguientes afirmaciones no es propia de una WMN:

a) Está formada por una estación base y sus puntos de acceso, que se comunican entre ellos para conformar una única red inalámbrica con el mismo SSID y contraseña, a la que se pueden conectar los clientes.
b) El tráfico se redirige por la red de manera que se dispone siempre de la mejor señal posible en la red. Las WMN determinan en cada momento el nodo idóneo al que conectarse.
c) El principal inconveniente de las WMN radica en la tolerancia a fallos, puesto que una caída de un nodo implica la caída de toda la red.
d) Al disponer de varios nodos en una misma zona, entonces las distancias a alcanzar en las transmisiones no son tan grandes, por lo que se puede tener una disminución de las interferencias y un ahorro de energía, puesto que no hace falta transmitir a tanta potencia.

---

10) El proyecto 802 define, además de la topología de red, un conjunto de reglas de acceso y transmisiones. El seguimiento del estándar es indispensable para asegurar la difusión de una tecnología, permitiendo que diversas empresas puedan fabricar y vender dispositivos con garantías de funcionamiento en entornos reales de redes de ordenadores. Indique qué subconjunto de normas se relaciona con la capa LLC del proyecto IEEE:

a) 802.2
b) 802.3
c) 802.4
d) 805.5

---

11) En redes de ordenadores aparece el concepto de *MAC address*. Indique cuál es la afirmación correcta en relación a dicho concepto:

a) El término *MAC address* hace referencia la capa de Acceso al Medio (Media Access Control) en las comunicaciones, de acuerdo al protocolo IEEE.
b) Es un número que identifica de manera biunívoca un conjunto de dispositivos de la red. Viene definido por el modelo clásico OSI.
c) También conocido como Dirección Física, es una colección de caracteres hexadecimales único para cada dispositivo de la red, y se relaciona con la capa 2 del modelo OSI.
d) Es una identificación de un dispositivo que se puede obtener, en Windows, por medio de la instrucción *ip link list*

---

12) Dentro del protocolo RFC se define el concepto de DHCP, que permite a dispositivos de red (clientes) la obtención de los parámetros necesarios para su conexión a una red. DHCP hace referencia a la gestión de direcciones IP y otros datos de configuración para toda una red. Indique cuál de las siguientes afirmaciones es verdadera:

a) La asignación de la IP se realiza de manera dinámica por un ordenador servidor, que asigna siempre la misma IP a cada uno de los dispositivos que se conectan a la red.
b) El servidor asigna una IP aleatoria a los equipos que se conectan a la red. Al ser una LAN en la que interviene un número limitado de dispositivos no hay problemas de duplicidad de IP dentro de la misma red.
c) El servidor DHCP asigna dinámicamente una IP y otros parámetros de configuración de red, con la finalidad de que puedan comunicarse con otras redes IP.
d) Ninguna de las anteriores.

---

13) En el caso de las redes es fundamental controlar la seguridad de las comunicaciones. Cuando se trata de redes inalámbricas aparecen riesgos adicionales que son inherentes a la naturaleza inalámbrica, de manera que cualquiera que se encuentre dentro del radio de alcance de la red podría llevar a cabo acciones maliciosas. Indique cuál de las siguientes afirmaciones es verdadera:

a) El *eavesdropping* consiste en realizar acciones de sobrecarga del sistema para provocar una caída del rendimiento.
b) El *MAC snooping*, que consiste en suplantar la *MAC Address* de un dispositivo permitido en la red.
c) *Man-in-the-middle* consiste en que el atacante se sitúa entre el emisor y el receptor, suplantando una de las partes y haciendo creer a la otra que está hablando con el legítimo interlocutor de la comunicación.
d) Ninguna de las anteriores

---

14) El término REST está relacionado con un esquema de aplicaciones basadas en la utilización de Servicios Web. De esta manera, el elemento principal en el que se basan estos servicios son las URL puesto que, en última instancia, un Web Service (WS) se relaciona directamente con la URL a la que se debe acceder para utilizar dicho WS. En relación a REST se puede decir que:

a) En REST siempre existe una transmisión de datos e informaciones utilizando el lenguaje XML
b) Existe un estándar en los mensajes, de manera que todos los servicios web deben ser llamados con los mismos parámetros y retornar ficheros XML o JSON con la misma estructura.
c) REST no posee restricciones en cuanto a la tecnología a utilizar, sólo se define la manera de transferir los datos entre los agentes interlocutores.
d) El código de programación de los WS es público, de manera que éste se puede incluir directamente en los programas del cliente para poder acceder a las funcionalidades disponibles en el servidor.

---

15) En las transmisiones en redes de ordenadores es fundamental mantener unos altos niveles de seguridad que protejan los datos e informaciones, en relación a amenazas, riesgos y vulnerabilidades. En relación a la seguridad de la información se describen varios pilares. Indique cuál de las siguientes afirmaciones es falsa:

a) Confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde. Así, cada sistema automático o individual solo podrá usar los recursos que necesita para ejercer sus tareas.
b) Integridad consiste en asegurar que la información no se pierde ni se ve comprometida voluntaria e involuntariamente.
c) Disponibilidad consiste en asegurar que la información esté disponible y completa para las personas que la necesiten.
d) Gestión de usuarios consiste en disponer de un buen sistema de seguridad en la creación de contraseñas y en asegurar que los usuarios dispongan de formación específica en temas de generación de contraseñas.

---

16) En las configuraciones de los *routers*, normalmente, se ofrecen varias modalidades de cifrado, a efectos de mejorar la seguridad de la red. Indique cuál de las siguientes afirmaciones es cierta:

a) WEP (*Wireless Equivalent Privacy*) es un método de seguridad de cifrado incluido en el estándar IEEE 802.11 para redes cableadas. Utiliza una clave compartida (PSK) de seguridad para cifrar todas las comunicaciones. Usa el algoritmo de encriptación RC4.
b) WPA (*Wifi Protected Access*) es una variante mejorada de WEP que aumenta la seguridad de una clave compartida única con claves dinámicas (TKIP) y protege las identidades de los usuarios mediante la autenticación con clave compartida (PSK). Usa el algoritmo de encriptación AES con integración de claves EAP
c) WPA2 (*Wifi Protected Access 2*) aparece en 2005 con un algoritmo de encriptación EPSA e integración de claves EAP, con 128 bits de clave secreta.
d) WPA3 es la versión de WPA que aparece en 2018, con una clave de cifrado de 192 bits en la versión *Enterprise*, que incrementa la seguridad con respecto a su antecesor WPA2.

---

17) La seguridad de las redes inalámbricas se basa en la aplicación de algunos protocolos, como WEP y WAP, en sus diferentes versiones. Indique la afirmación correcta:

a) El protocolo WEP aparece en 1999, con integración de claves y con un algoritmo de encriptación RC4 con clave secreta de 40 a 104 bits.
b) El protocolo WAP aparece en 2001, con algoritmo de encriptación RC4 y clave secreta de 64 a 128 bits, con integración de claves EAP.
c) El protocolo WAP2 aparece en 2005, con algoritmo de encriptación AES y clave secreta de 256 bits, con integración de claves EAP.
d) Ninguna de las anteriores

---

18) El CCN es un organismo español adscrito del CNI que dispone de un CERT dedicado a la gestión de medidas de gestión de la seguridad informática, con el objetivo de mitigar el riesgo de ataques contra redes y sistemas informáticos. Indique cuál es la afirmación correcta en relación al *ransomware*:

a) *Ransomware* es un tipo de ciberataque que tiene como objetivo el robo de información, de tecnología o de cualquier tipo de información.
b) *Ransomware* utiliza diversos métodos para conseguir las credenciales de los usuarios, como el *phising*, o por obtención de credenciales disponibles en la *dark web*.
c) Los ataques *ransomware* tienen como objetivo congestionar las redes inalámbricas, pero en ningún caso provocan robos de información.
d) Ransomware es un tipo de ciberdelito que busca principalmente beneficios económicos por medio de la extorsión, derivados de imposibilitar el acceso a la información por parte de las víctimas del ciberdelito.

---

19) En una red se definen las vulnerabilidades como fallos o errores del sistema, que constituyen puertas abiertas que se pueden aprovechar por parte de los delincuentes cibernéticos. Indique cuál es la afirmación correcta:

a) Las vulnerabilidades físicas se refieren a problemas de acceso a la red informática por parte de personas ajenas a la organización.

b) Las vulnerabilidades físicas se refieren a problemas de configuración de los equipos físicos. Con una buena configuración es posible minimizarlos o evitarlos.
c) Las vulnerabilidades lógicas se refieren al control de acceso a dependencias que contengan los *Data Warehouse*, dado que el control debe seguir la lógica de acceso propia de la organización
d) Las vulnerabilidades físicas incluyen consideraciones de acceso físico a los dispositivos de almacenamiento de datos por parte de personas no autorizadas.

---

20) La Ley 59/2003, artículo 3, versa sobre la consideración de la firma electrónica y los documentos firmados electrónicamente. Indique cuál de las siguientes afirmaciones no se corresponde con el contenido del citado artículo:

a) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
b) Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.
c) La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel, siempre que ésta se presente como alternativa a la versión en papel.
d) El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio

---

21) La Ley 59/2003, artículos 6 y 7, versa sobre la consideración de certificado digital y sobre las personas que pueden disponer de certificado digital. Indique cuál de las siguientes afirmaciones es cierta:

a) Un firmante es la persona que posee un dispositivo de creación de firma y que actúa exclusivamente en nombre propio.
b) Las personas que pueden solicitar certificados electrónicos de personas jurídicas son sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.
c) Los certificados electrónicos de las personas jurídicas afectan considerablemente al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.
d) La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, si bien su identificación no se debe incluir en el propio certificado electrónico.

---

22) En la certificación digital toman especial importancia los aspectos de identificación y autenticación por parte de las Administraciones Públicas (AAPP). Así, en la Ley 39/2015, capítulo II, se indican las formas de identificación y firma. Indique la afirmación inco-

rrecta en relación a la identificación electrónica de los interesados, así, éstos podrán identificarse mediante:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezcan.
d) Todos los certificados que suministre una empresa con solvencia suficiente y credibilidad demostrable son considerados válidos, a todos los efectos, en cualquier proceso de certificación digital en entornos cerrados de comunicación en los que intervenga la Administración Pública, conforme a lo específicamente acordado entre las partes.

23) En diagnóstico de funcionamiento de dispositivos en una red de comunicaciones se puede utilizar el comando *ping*. Indique cuál de las siguientes es una afirmación verdadera en relación al comando *ping*:

a) Es un acrónimo de *Packet Interchange Groper* disponible en entornos *Windows* y *Linux*.
b) Es un comando de diagnóstico que permite realizar una verificación del estado de una determinada conexión por medio del envío de 5 solicitudes de eco, en su ejecución predeterminada.
c) Por medio del tiempo de espera de la respuesta al envío de información se determina el tiempo de retraso de dicha respuesta.
d) Ninguna de las anteriores

24) La Ley 03/2018 de Protección de Datos Personales y garantía de los derechos digitales regula el tratamiento de datos personales, como derecho fundamental protegido por la Constitución española. En dicha ley se indica que Internet se ha convertido en una realidad omnipresente tanto en la vida personal como colectiva. Sin embargo, el uso de Internet posee múltiples riesgos, y es competencia del sector público la protección de datos y la transparencia y acceso a la información pública. Indique cuáles de las siguientes afirmaciones no es correcta:

a) El tratamiento de los datos está basado en el consentimiento del afectado, entendiendo como tal consentimiento toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, mediante una declaración o clara acción afirmativa, el tratamiento de datos personales que le conciernen.
b) El tratamiento de los datos personales de un menor de edad sólo puede fundarse en su consentimiento cuando la persona sea mayor de catorce años, excepto en los casos en los que contempla la ley, relacionados con la tutela.
c) El responsable del tratamiento de los datos, siempre que éstos sean obtenidos del afectado, debe facilitar al mismo la identidad del responsable del tratamiento y de su representante, la finalidad del tratamiento y la posibilidad de ejercer sus derechos en relación con los datos.
d) Con la finalidad de tratamientos con fines de videovigilancia, sólo las personas jurídicas de naturaleza pública pueden llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras en las que se capten imágenes de la vía pública, siempre con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

25) Un sistema de RAID permite una mejora del rendimiento en el almacenamiento externo. Así, RAID permite elegir la mejor forma de utilizar el dispositivo, de acuerdo a las necesidades de la organización. Indique cuál de las asignaciones es correcta:

a) RAID 0 es el sistema más rápido. Se necesita un mínimo de cuatro unidades, de manera que los datos se distribuyen en cada disco. Es ideal para los usuarios que necesitan la máxima velocidad y capacidad, como en procesos de edición de vídeo. No es tolerante a fallos y no es un sistema recomendado como solución de copias de seguridad. Responde al concepto de *disk stripping*.
b) RAID 1 es un modo seguro que requiere un mínimo de 2 unidades, que trabaja con pares de unidades, replicando los datos. Proporciona la máxima seguridad de los datos en el caso de un fallo de disco único. Sin embargo, el rendimiento se reduce durante la escritura. Es una excelente elección cuando la seguridad es más importante que la velocidad. Responde al concepto de *disk mirroring*.
c) RAID 0+1 es un modo RAID compuesto de un duplicado de conjuntos distribuidos de datos. Es una combinación de RAID 0 y RAID 1 y requiere disponer de un mínimo de dos discos, si bien sólo la mitad de ellos se utiliza para el almacenamiento de datos. Este sistema proporciona buenas velocidades, si bien todos los discos deben tener la misma capacidad.
d) RAID 3 es un sistema que realiza la distribución de datos a nivel de byte, entre varios discos, con un disco adicional dedicado a almacenar información de paridad. Es un sistema tolerante a fallos, pero no es un sistema que proporcione seguridad de datos en entornos donde se leen archivos largos y secuenciales, como archivos de vídeo.

---

26) En 1985, Richard Stallman publica el Manifiesto GNU, que es una explicación y definición de las metas del Proyecto GNU, anunciado por el propio Stallman en 1983. GNU se relaciona directamente con el software libre, de manera que se afirma que los usuarios disponen de libertades esenciales, entre las que no se encuentra:

a) La libertad de ejecutar el programa en las condiciones que describa de manera específica el autor del programa.
b) La libertad de estudiar el funcionamiento de un programa y modificarlo de modo que realice las tareas como el usuario desee. Para ello es indispensable disponer del código fuente del programa.
c) La libertad de redistribuir copias para ayudar a los demás usuarios.
d) La libertad de distribuir copias de sus versiones modificadas a otras personas, dando a toda la comunidad la oportunidad de beneficiarse de sus cambios.

---

27) La IEEE ha definido diferentes estándares de funcionamiento para los diferentes tipos de red y tecnologías usadas. Indique cuál es la afirmación incorrecta en cuanto a vinculación de tipo de red y código de normativa según la IEEE:

a) IEEE 802.15 con la WPAN
b) IEEE 802.11 con la WLAN
c) IEEE 802.16 con la WMAN
d) IEEE 802.20 con la WBAN

---

28) Un Servicio de Directorios (SD) es, en esencia, una aplicación o conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores. Con dicha información, los administradores pueden gestionar el acceso de los

usuarios a los recursos de dicha red. Indique cuál de las siguientes afirmaciones es falsa en relación a LDAP:

a) LDAP es un protocolo basado en X.500, que se ejecuta sobre TCP/IP u otros servicios de transferencia orientados a conexión.
b) LDAP define una organización de las entradas de la base de datos en forma de estructura jerárquica en árbol.
c) LDAP está basado en el modelo cliente – servidor, donde el servidor posee los datos que conforman la información del directorio.
d) LDAP es una base de datos que en la que las entradas son los servicios del SD, que poseen atributos que se relacionan con una única clave.

29) De la misma manera que la seguridad es muy importante en las redes de comunicación, en un Servicio de Directorios (SD) es sumamente importante mantener los niveles de seguridad, puesto que pueden contener datos e información sensible. Indique cuál de las siguientes afirmaciones no es correcta:

a) La autenticación anónima es útil para el caso de accesos de tipo *read-only* al directorio, siempre que los datos no sean sensibles.
b) SASL es un marco que proporciona múltiples mecanismos de autenticación y encriptación para protocolos orientados a conexión.
c) En la implementación de LDAPv3 se permite una autenticación anónima, de manera que el cliente sólo se debe autenticar en caso de realizar accesos de alteración de los servicios.
d) La Autenticación Básica proporciona facilidades de autenticación en los datos de identificación del cliente que son transmitidos por la red con texto claro, si bien este sistema no se recomienda en redes abiertas en las que no hay autenticación o encriptación en capas inferiores, como SSL.

30) El sistema de información de un Ayuntamiento debe seguir la normativa que dicte la legislación estatal. En el caso de la facturación se debe tener en cuenta la normativa en relación a la factura electrónica. Según el sitio web del Ministerio de Hacienda, una factura electrónica es una factura que se expide y recibe en formato electrónico y posee los mismos efectos legales que una factura en papel. Indique la afirmación correcta:

a) La factura electrónica está regulada por el RD 1619/2012, en el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.
b) Las facturas electrónicas, por el hecho diferencial de ser electrónicas, deben posee obligatoriamente un formato electrónico estructurado, con lenguajes como XML. No se aceptan, bajo ningún concepto, facturas presentadas en forma de imagen o PDF.
c) La factura electrónica proporciona beneficios como: acortar los ciclos de tramitación, reduce errores humanos, elimina costes de impresión. Sin embargo, no resuelve la problemática de mejorar el espacio físico de almacenamiento, puesto que se requieren unidades de almacenamiento de datos.
d) El único requisito de formato de las facturas electrónicas que utilicen las Administraciones Públicas es que estén escritas en un lenguaje informático determinado, que sea Facturae 3.2 ó 3.2.1

31) En relación al *cloud computing* existen distintas formas de servicio, que proporcionan diversos niveles de flexibilidad o sencillez a la hora de generar y mantener las aplicaciones. Indique cuál de las siguientes afirmaciones es verdadera:

a) SaaS se refiere a un modelo de *cloud computing* que proporciona a los usuarios acceso al software basado en *cloud* de un proveedor. Los usuarios pueden descargar e instalar el software las veces que haga falta, sin limitación provocada por el número de licencias.
b) PaaS se refiere a un modelo de *cloud computing* que proporciona a los usuarios un entorno de *cloud* en el que pueden desarrollar, gestionar y distribuir sus propias aplicaciones.
c) IaaS se refiere a un modelo de *cloud computing* en la que un proveedor proporciona a los usuarios acceso a recursos de cálculo como servidores, almacenamiento y redes. Los usuarios sólo tienen que adquirir el hardware y la empresa de *cloud computing* se encarga del mantenimiento de los diferentes equipos hardware
d) Ninguna de las anteriores

---

32) A raíz de la crisis provocada por el virus Covid-19, algunas organizaciones se han visto obligadas a tomar medidas y adoptar soluciones para afrontar las necesidades surgidas. Una de ellas está relacionada con la utilización de SaaS para poder operar en remoto. Indique cuál de los siguientes no es un proveedor de Saas:

a) Microsoft
b) Amazon
c) ERP
d) IBM

---

33) Los modelos de despliegue de soluciones en *cloud computing* pueden adoptar varias modalidades. Indique cuál de las siguientes es la afirmación verdadera:

a) El modelo de despliegue de nube pública ofrece el servicio a varios clientes desde un mismo centro de cálculo y computación, de manera que los clientes comparten recursos de almacenamiento y procesamiento.
b) El modelo de despliegue de nube privada permite que los recursos sean entregados de forma exclusiva y privada al cliente, de manera que éste posee el control sobre el servicio que contrata. Sin embargo, el control de los datos sigue recayendo en el proveedor de servicios.
c) El modelo de nube híbrida es una combinación de nube pública y privada, en la que el cliente decide los servicios que desea contratar. Ofrece mayores niveles de seguridad que la nube privada, con una reducción de costos
d) Ninguna de las anteriores

---

34) Existen dos soluciones básicas en relación con la utilización de software: *cloud software* y *software on premise*. Indique cuál es la afirmación verdadera:

a) En el caso del *cloud software*, las aplicaciones software se instalan en los ordenadores locales a partir de una descarga de ficheros desde la propia nube.
b) En el caso del *software on premise* la empresa no necesita disponer de sistemas de seguridad de datos y programas, puesto que la empresa que vende el software es la responsable del buen funcionamiento de las aplicaciones.
c) La modalidad de software en la nube requiere de la instalación de ordenadores y servidores locales muy potentes, para poder soportar mucha carga de conexiones web.
d) Ninguna de las anteriores.

---

35) Uno de las necesidades, cuando se quiere seguir una estrategia digital que incluya la presencia en la WWW, es disponer de un espacio para alojar las páginas web del sitio dentro de un servidor web. Aparece entonces el concepto de Web Hosting. Existen va-

rias alternativas para cubrir las distintas necesidades de alojamiento. Indiquen cuál es la afirmación falsa:

a) El hosting compartido es un tipo de alojamiento consistente en que el proveedor alquila espacio de almacenamiento de memoria a varios sitios web dentro de un mismo servidor. Los clientes comparten los recursos del servidor.
b) Un servidor dedicado es un tipo de web hosting de uso exclusivo de un único cliente, que no comparte recursos con otros clientes. Al no compartir recursos, el rendimiento del sitio web no se ve afectado por el tráfico.
c) Un VPS es un tipo de alojamiento web en el que el servidor web está compartido por varios clientes, pero utilizando una tecnología de compartición de otros recursos (como CPU del servidor) siguiendo una política de asignación de CPU que provoca que se tenga la impresión de que el servidor está totalmente dedicado a uno de los clientes.
d) El cloud hosting consiste en ejecutar desde una nube todos los recursos necesarios para el funcionamiento de un sitio web

36) La Ley 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, en su apartado de Autoridades de protección de datos (TÍTULO VII), indica que la Agencia Española de Protección de Datos es una autoridad administrativa en protección de datos. En este sentido se realizan algunas afirmaciones a partir del contenido de la Ley. Indique cuál es la afirmación verdadera:

a) La Agencia Española de Protección de Datos es una autoridad administrativa dependiente del Consejo General del Poder Judicial, que realiza acciones de protección de datos.
b) Corresponde a la Agencia Española de Protección de Datos la supervisión de la aplicación de la Ley 03/2018, así como de desempeñar las funciones y potestades que se le atribuyan a partir de otras leyes o normas de Derecho de la Unión Europea.
c) Se recomienda que las Administraciones Públicas, entre las que se incluyen las tributarias y de la Seguridad Social, proporcionen a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación, si bien dicha colaboración no es, bajo ningún concepto, una obligación.
d) La Agencia Española de Protección de Datos es una organización de carácter público que desempeña sus acciones con una limitación geográfica limitada a las fronteras del estado español, de manera que no puede realizar sus funciones a nivel exterior. Las acciones de protección de datos en el exterior sólo las puede llevar a cabo el Ministerio de Exteriores.

37) En el diseño de Bases de Datos se intenta conseguir la mayor calidad de datos, en relación a eliminación de redundancias y facilitar tareas de modificación de datos, eliminar problemas de integridad referencial y generar una estructura fácilmente comprensible y con posibilidades de escalabilidad. Para tales efectos se define el concepto de Normalización de Datos, con varias Formas Normales. Indique la afirmación incorrecta:

a) Se dice que una tabla de una Base de Datos está en primera forma normal cuando todos los atributos contienen un único dato, todos los atributos de la clave están definidos y todos los atributos dependen de la clave primaria.
b) Se dice que una tabla de una Base de Datos está en segunda forma normal cuando no incluye dependencias parciales de la clave primaria.
c) Se dice que una tabla de una Base de Datos está en tercera forma normal cuando no contiene dependencias transitivas.
d) Se dice que una tabla de una Base de Datos está en cuarta forma normal cuando cada uno de los determinantes es una clave candidata.

38) En Bases de Datos se denomina con el acrónimo ACID a determinadas características que cumplen algunos modelos de Bases de Datos. Indique cuál de las siguientes no es una de las propiedades ACID mencionadas:

a) *Atomicity*, que se refiere a que las transacciones en Bases de Datos deben ser ejecutadas en su totalidad: o bien se ejecutan de manera completa, o bien no se ejecutan.

b) *Completity*, que se refiere a asegurar que las transacciones realicen los bloqueos de todos los registros de las tablas con las que va a trabajar, de manera que se asegure que las transacciones concurrentes no interaccionan entre sí.
c) *Isolation*, que se refiere a que la realización dos transacciones sobre el mismo conjunto de datos deben ser independientes, de manera que no se genere ningún tipo de error ni inconsistencia entre ellas.
d) *Durability*, que se refiere a que, una vez realizada la operación, ésta persistirá y no se podrá deshacer.

---

39) El tipo de cable más común en las LAN es el par trenzado, adoptado como solución para conectar redes reutilizando el cableado existente de redes telefónicas. Indique cuál de las siguientes es una afirmación verdadera:

a) El cable par trenzado necesita unos conectores específicos para asegurar su correcta instalación. Se pueden destacar el RJ-45 y el RJ-49, con ocho conexiones de cable, correspondientes a cuatro pares trenzados.
b) Existen varios tipos de cable de par trenzado: el STP (que no posee ningún tipo de protección adicional a la recubierta de PVC), el UTP (que va recubierto por una malla conductora que actúa de pantalla frente a interferencias y ruido electrónico) y el FTP (que posee una pantalla global de aluminio que mejora la protección).
c) Los cables se pueden clasificar por categorías, así, la categoría 5b corresponde a un tipo de cable que posee una frecuencia máxima de 250 MHz, es cable UTP o STP y posee conectores RJ-45 o RJ-49
d) Ninguna de las anteriores

---

40) Una copia de seguridad es un proceso mediante el cual se duplica, de un soporte a otro, un determinado volumen de datos. El objetivo es poder recuperarlos en caso de fallo en el alojamiento original de los datos. En las copias de seguridad es importante determinar la información que se debe respaldar y la periodicidad del respaldo. En este sentido, se definen varios tipos de copia de seguridad. Indique cuál de las siguientes es una afirmación incorrecta:

a) La copia de seguridad en espejo o RAID1 consiste en realizar una copia de seguridad realizando una copia de los datos en tiempo real. Estas copias aseguran que se puede recuperar la información en cualquier momento posterior a la copia en el espejo, dado que la copia siempre es un reflejo del original.
b) La copia de seguridad completa consiste en realizar una copia de todos los datos en un soporte distinto al original. Este sistema permite una fácil restauración de datos, pero requiere mayores necesidades de almacenamiento y coste económico frente a otros tipos de copia. Estas copias se suelen realizar en horarios que no conlleven carga sobre el servidor.
c) La copia de seguridad diferencial consiste en realizar una copia de todos los datos que han sufrido alguna variación respecto de la anterior copia de seguridad completa, o bien que se han creado desde la última copia de seguridad completa. El *backup* diferencial siempre parte de un *backup* completo.
d) La copia de seguridad incremental consiste en copiar los datos que han variado desde la última copia realizada. De esta manera sólo se copian los cambios que no son redundantes. Este tipo de copia de seguridad posee menos problemas de espacio que la copia completa, pero el tiempo de recuperación de datos de la incremental es mayor en la completa

---

41) El objetivo principal de las copias de seguridad es la preservación de los datos para garantizar la continuidad del Sistema de Información ante posibles fallos en los mismos. El procedimiento que se sigue a un fallo es la restauración de la copia de seguridad. Indique cuál es la afirmación correcta en relación a los siguientes conceptos relacionados con la restauración de copias de seguridad:

a) El *Recovery Time Objective* se define como el tiempo que se tarda en recuperar un nivel de servicio mínimo tras una caída del servicio sin afectar a la continuidad de la operatoria de la organización

b) El *Maximum Tolerable Downtime* es el tiempo máximo que ha estado caído un proceso o sistema antes de recuperar un determinado nivel de servicio.
c) El *Revised Operating Level* es el nivel mínimo de recuperación que debe tener una actividad para que se considere como recuperada, aunque el nivel de servicio no sea el óptimo.
d) Ninguna de las anteriores

---

42) En la planificación de las copias de seguridad es crítico seleccionar el soporte idóneo para salvaguardar la información. De esta manera, se pueden definir varios sistemas o arquitecturas de almacenamiento. Indique cuál es la afirmación incorrecta:

a) Se utiliza el término DAS cuando se utiliza, para almacenar la copia de seguridad, un dispositivo de almacenamiento directo del ordenador.
b) Se utiliza el término NAS para hacer referencia a la arquitectura de copias de seguridad en la que se utiliza un dispositivo de almacenamiento de copias de seguridad que es común a todos los ordenadores que están conectados a una LAN
c) Se utiliza el término HAS al sistema híbrido en el que los ordenadores de una red realizan copias de seguridad en almacenamientos de conexión directa al ordenador, o bien en un dispositivo común a todos los ordenadores.
d) Se utiliza el término SAN cuando se utiliza un conjunto de varios dispositivos de almacenamiento para almacenar las copias de seguridad de los ordenadores de una red.

---

43) En criptografía, una unidad de cifrado por bloques es una unidad de cifrado de clave simétrica que opera en grupos de bits de longitud fija, llamados bloques, aplicándoles una transformación. Existen varios algoritmos de cifrado por bloques. Indique cuál es la afirmación correcta:

a) El algoritmo DES (*Data Encryption Standard*), diseñado por IBM, usa una clave de 64 bits y trabajo con bloques de 72 bits. De éstos, 8 bits se destinan para funciones de control de paridad.
b) El algoritmo AES (*Advanced Encryption Standard*), también conocido como algoritmo Rijndael, posee un cifrado simétrico que permite cifrar bloques de 128 bits, utilizando claves de 128, 192 ó 256 bits.
c) El algoritmo 3AES (triple AES) fue desarrollado como una mejora del algoritmo AES, extendiendo la aplicación del algoritmo hasta tres veces consecutivas, con tres claves diferentes. El tamaño de la clave combinada es de 168 bits.
d) Ninguna de las anteriores

---

44) Se entiende por Calidad de Servicio (QoS) la posibilidad de asegurar, principalmente, una determinada tasa de transmisión de datos en la red, un retardo y una variación de retardo. Existen variables de medida de la QoS. Indique cuál de las siguientes no es una afirmación correcta, en relación a parámetros que afectan a la QoS:

a) Los Retardos, también conocidos como *delay*, son incrementos en el tiempo de recepción de paquetes por parte del receptor. Se pueden deber a motivos diversos, como la permanencia en colas de paquetes o por seguir rutas menos directas para prevenir la congestión de la red.

b) La Latencia, también conocida como *jitter*, hace referencia al tiempo que tarda en transmitirse un paquete dentro de la red. Factores que generan mayor *jitter* son la tecnología de acceso a Internet, la distancia entre los puntos emisor y receptor y la propia capacidad del dispositivo emisor.
c) En ocasiones se producen alteraciones en el orden de entrega de los paquetes de un mensaje, debido principalmente a que éstos han permanecido en colas distintas o porque han seguido rutas distintas del resto de paquetes del mensaje. Este problema requiere de un protocolo que permita reordenar los paquetes en el dispositivo receptor.
d) Durante la transmisión de paquetes se pueden producir errores, por ser mal dirigidos o por corromperse durante su encaminamiento. Estos errores pueden provocar una disminución de la QoS.

---

45) Los administradores de Bases de Datos pueden utilizar diferentes sistemas para asegurar la integridad de datos y para encapsular procedimientos y definiciones de tabla. Indique cuál es la afirmación incorrecta:

a) Un TRIGGER de SQL define una acción que se debería realizar en la Base de Datos siempre que ocurra un determinado acontecimiento en la aplicación. En general, dichos acontecimientos van asociados a acciones de INSERT, UPDATE o DELETE en tablas.
b) Un STORED PROCEDURE es un tipo de subprograma que se puede programar a nivel de administración de la base de datos. Pueden ser invocados por otros programas y recibir datos por parámetro.
c) La diferencia entre los PROCEDURE y las FUNCTION radica en el tipo de datos de los parámetros de retorno.
d) Una TRANSACTION es la unidad básica de ejecución en una base de datos. Puede ser un programa o parte de un programa, o una sentencia, de manera que se deben realizar todas las acciones que incluye la TRANSACTION. En caso contrario, se debe asegurar que se retorna a la situación de la base de datos anterior al inicio de la ejecución de la TRANSACTION

---

46) El diseño del software tiende a ser cada vez más modular. Así, las aplicaciones se componen de una serie de componentes (servicios) reutilizables, que se pueden encontrar distribuidos a lo largo de una serie de máquinas conectadas en red. Indique la afirmación incorrecta:

a) Un servicio web, según la W3C, es un software diseñado para soportar interacciones máquina a máquina a través de la red. De esta manera, proporcionan una forma estándar de interoperar entre aplicaciones que se ejecutan en diferentes plataformas.
b) En una arquitectura orientada a servicios, cualquier interacción punto a punto implica dos *endpoints*: uno que proporciona un servicio, que corresponde al servicio web, y otro que lo consume
c) Los servicios basados en SOAP utilizan mensajes para intercomunicarse. La descripción delas operaciones ofrecidas por el servicio se pueden escribir en un lenguaje denominado WSDL.
d) El lenguaje de programación que se utiliza en la codificación de un servicio web debe ser el mismo que el del programa que lo invoca. De esta manera se asegura la máxima eficiencia en la interacción entre ambos programas

---

47) La Ley 39/2015 trata sobre el Procedimiento Administrativo Común de las Administraciones Públicas. En dicha Ley se trata el tema de la acreditación en materia de representación, con el apartado del apoderamiento. Indique la afirmación incorrecta:

a) La representación se puede acreditar por medio de cualquier medio válido en Derecho que deje constancia fidedigna de su existencia. A estos efectos, se entiende como acreditada la representación efectuada por comparecencia electrónica en la correspondiente sede electrónica.
b) La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales deben disponer de un registro electrónico general de apoderamientos.

c) Los registros electrónicos, con el objeto de garantizar la seguridad y preservación de la información, deben mantener una visibilidad limitada a los dispositivos de la Administración en la que se ha realizado el registro electrónico.
d) Los registros de apoderamiento que se realicen en los registros electrónicos deben contener, como mínimo, el nombre y apellidos o denominación o razón social, DNI, NIF o documento equivalente (en todos los casos, tanto del poderdante como del apoderado), la fecha de inscripción, el periodo de tiempo por el cual se otorga el poder y el tipo de poder según las facultades que otorgue.

---

48) La Ley 40/2015 establece y describe los principios de actuación y funcionamiento del sector público. En su Capítulo V trata sobre el funcionamiento electrónico del sector público. Indique cuál de las siguientes es una afirmación incorrecta:

a) Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.
b) Todos los documentos utilizados en las actuaciones administrativas se deben almacenar por medios electrónicos, excepto cuando no sea posible.
c) Se describe la sede electrónica o portal de internet como aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública o bien a uno o varios organismos públicos o entidades de Derecho Público.
d) Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, padrones municipales y otros registros de población, datos fiscales y datos de los usuarios del sistema de salud deben ubicarse dentro del territorio de la Unión Europea

---

49) El Real Decreto RD 3/2010 regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Dentro de los Principios Básicos, el RD indica que la seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección. Indique cuál es la afirmación correcta:

a) Las medidas de detección deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema.
b) Las medidas de prevención estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
c) Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a situaciones en las que un incidente de seguridad inhabilite los medios habituales.
d) Ninguna de las anteriores

---

50) Se entiende por virtualización el concepto de creación, a través de software, de una representación virtual de un recurso tecnológico. La virtualización aporta algunas oportunidades, como hacer funcionar varios sistemas operativos en un mismo ordenador, reducir costes de adquisición de hardware, aprovechar mejor los equipos. Indique cuál es la afirmación correcta en relación a la virtualización de servidores:

a) En la virtualización de servidores, también conocida como virtualización de plataforma o virtualización de hardware, se dispone de un software denominado hipervisor o VMM, que crea una capa de abstracción del hardware de la máquina física, generando una máquina virtual.

b) La virtualización con un hipervisor tipo 1, también denominado *hosted*, consiste en la ejecución de un software que se ejecuta sobre el sistema operativo del servidor, como una aplicación más, para ofrecer la funcionalidad específica.
c) La virtualización con un hipervisor tipo 2, también denominado nativo o *unhosted*, consiste en la ejecución del software directamente sobre el hardware del servidor. Dicho software se instala directamente sobre el servidor, haciendo las funciones tanto de sistema operativo como de virtualización.
d) Ninguna de las anteriores

PREGUNTAS DE RESERVA:

RESERVA 1. En un sistema de almacenamiento de tipo RAID 1, si se considera que N es el número de discos y D la capacidad de cada disco, indique la afirmación que contiene la fórmula correcta para calcular la capacidad disponible de almacenamiento:

a) N*D
b) N*D/2
c) (N-1)*D
d) Ninguna de las anteriores

RESERVA 2. El Real Decreto RD 3/2010, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en su ANEXO I, determina la categoría de un sistema en relación a la seguridad, con varias dimensiones de la seguridad. Se define el nivel ALTO cuando se produce un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Indique cuál de las siguientes no es una afirmación verdadera en relación a la consideración de perjuicio muy grave:

a) La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales.
b) El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
c) Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
d) El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

RESERVA 3. La encriptación de datos es una técnica que permite incrementar la seguridad en las transmisiones de datos, de manera que los mensajes aparecen codificados, con la finalidad de ocultar su contenido. Indique cuál es la afirmación correcta en relación a los tipos de encriptación:

a) La criptografía simétrica utiliza una única clave para cifrar y descifrar los mensajes. Dicha clave debe ser conocida previamente por el emisor y el receptor.
b) La criptografía asimétrica se basa en el uso de dos claves privadas para incrementar la seguridad en las transmisiones.
c) La criptografía híbrida se basa en utilizar un sistema que combine la criptografía simétrica con la asimétrica en la emisión de mensajes, de manera que se puede elegir entre usar una clave pública o dos privadas.
d) Ninguna de las anteriores.

RESERVA 4. La tendencia actual en bases de datos pasa por la acumulación de grandes volúmenes de datos. En este sentido, indique cuál es la afirmación falsa.

a) El término VLDB se utiliza para referirse a bases de datos que contienen tablas con un número especialmente elevado de registros.
b) Se entiende por Big Data a grandes conjuntos de información, que superan la capacidad del software convencional de bases de datos para procesar datos en un tiempo razonable.
c) Las bases de datos relacionales proporcionan más potencia, robustez, funcionalidad y estandarización y capacidades de escalabilidad de datos que las NoSQL, pero éstas, al no respetar las normas ACID, son más rápidas en cuanto a extracción de información.

d) Las bases de datos documentales son un tipo de bases de datos NoSQL que permiten almacenar datos de documentos utilizando codificaciones como a JSON o XML.

RESERVA 5. En relación a la reutilización de aplicaciones y transferencia de tecnologías. Indique cuál de las siguientes afirmaciones es incorrecta:

a) Las Administraciones Públicas deben mantener directorios actualizados de aplicaciones para su libre reutilización.
b) La Administración General del Estado debe promover la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de las actividades propias de dicha administración.
c) Las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios, podrán ser declaradas como de fuentes abiertas, cuando se derive una mayor transparencia en el funcionamiento de la Administración Pública. Quedan exceptuadas las aplicaciones desarrolladas a través de contratación.
d) La Administración General del Estado, a través de un centro para la transferencia de la tecnología, debe mantener un directorio general de aplicaciones para su reutilización, prestando asistencia técnica para la libre reutilización de aplicaciones.

Expedient núm.: 2808/2020
Procediment: Seleccions de Personal i Provisions de Llocs de treball
Assumpte: Oposició per a cobrir de manera interina una plaça de personal funcionari Cap del departament d'Informàtica.

SEGON EXERCICI. PROVA TIPUS TEST

De caràcter obligatori i eliminatori.

Consistirà a respondre per escrit un qüestionari tipus test de 50 preguntes més 5 preguntes de reserva, amb quatre respostes alternatives, de les quals només una és correcta, referides al temari que figura com a annex. Les persones aspirants marcaran les contestacions en els corresponents fulls d'examen.

Aquest exercici es qualificarà de 0 a 30 punts, i seran eliminats aquells aspirants que no obtinguin la puntuació mínima de 15 punts.

El criteri de correcció serà el següent: cada pregunta resposta correctament es valorarà amb 0,60 punts; les preguntes no resoltes, tant si figuren les quatre opcions en blanc com si figuren amb més d'una resposta, no es valoraran. Les preguntes amb resposta errònia es penalitzaran amb un quart del valor assignat a la resposta correcta, (-0,15).

En cas que el tribunal acordi l'anul·lació d'alguna o algunes de les preguntes, per haver detectat d'ofici algun error manifest durant la realització de l'exercici o perquè aquest es detecta com a conseqüència de les al•legacions que posteriorment es presentin, es tendran en consideració les preguntes de reserva. Aquestes s'escolliran segons l'ordre de prelació en què es trobin en el propi exercici.

Si a conseqüència de les anteriors operacions s'esgoten les preguntes de reserva, el tribunal acorda anul·lar alguna pregunta més, el valor de cada pregunta s'ajustarà perquè la puntuació màxima sigui de 30 punts.

El temps per desenvolupar aquest exercici serà de 120 minuts.

No es corregiran anotacions fetes als enunciats, només al full de respostes

1) **Les xarxes de comunicació sense fils es poden classificar segons diversos criteris. Un d'aquests criteris és l'abast geogràfic màxim de la xarxa. En aquest sentit, indiqui quina és l'afirmació que presenta els tipus de xarxa d'ordinadors ordenats de menys a més abast màxim de la xarxa:**
   a) WBAN, WMAN, WLAN, WWAN
   b) WMAN, WPAN, WLAN, WWAN
   c) WBAN, WPAN, WWAN, WMAN
   d) Cap de les anteriors

2) **L'any 2019 es va presentar un nou model comercial d'un telèfon mòbil que incorpora un xip que utilitza la tecnologia UWB. Indiqueu quina és la resposta correcta:**
   a) UWB fa referència a una tecnologia de transmissió de paquets de dades que té com a base de funcionament les tecnologies *spread spectrum* (SS).
   b) UWB fa referència a un subconjunt de normes de la IEEE específiques per a connexions utilitzant la WLAN.
   c) UWB és una tecnologia WPAN que permet transmetre paquets d'informació a distàncies de l'ordre de pocs metres.
   d) UWB és un estàndard en el qual s'incorpora un dispositiu central que permet connectar els telèfons i proporciona una amplada de banda entre els ordinadors connectats a una xarxa sense fils.

3) **A l'actualitat hi ha una tendència a implantar serveis de telefonia IP, que fan possible la utilització de les mateixes xarxes per a dades i veu. Indiqueu quina és l'afirmació correcta:**
   a) El concepte de VoIP fa referència a la tecnologia que permet transmetre veu utilitzant un protocol d'IP.
   b) La telefonia IP fa referència als dispositius necessaris per poder transmetre veu a través de la LAN, entre els quals destaquen el PDX i el protocol SIP.
   c) La principal diferència entre VoIP i VoLTE està en la utilització d'UWB com a tecnologia base en les comunicacions.
   d) Cap de les anteriors.

4) **Un dels principals inconvenients de les xarxes sense fils és la presència de renou, que limita la capacitat de transmissió a través de canal. Considerant una xarxa d'amplada de banda H Hz i un senyal de potència S que es transmet a un canal amb un renou de potència R, Shannon va determinar que la capacitat màxima d'un canal ve donada per la fórmula:**
   a) Nombre màxim de bits/s = H 10^2 Log (1+S/N)
   b) Nombre màxim de bits/s = H 10 Log_2 (1+S/N)
   c) Nombre màxim de bits/s = H Log_2 (1+S/N)
   d) Cap de les anteriors

5) A la tranmisión de veu per IP ha una varietat de protocols de comunicació destinats a regular les comunicacions. Indiqueu quina és l'afirmació incorrecta:

a) El protocol SCCP és propietat de Cisco Systems i es defineix com un conjunt de missatges que s'envien entre els telèfons IP i el *Call Manager*. Per al trànsit de dades s'utilitzen els protocols RTP, UDP, IP.

b) El protocol IAX2 és un protocol utilitzat pel programa de codi obert Asterisk. Suporta la funcionalitat anomenada *Trunking (red)* que permet connectar dos *switch*, *routers* o servidors per mitjà de dos cables en paral·lel en mode half-duplex.

c) El protocol Jingle, en el disseny del qual va participar Google, és una extensió del protocol XMPP (*Extensive Messaging and Presence Protocol*) que permet la transferència d'informació *peer-to-peer*.

d) El protocol Skype utilitza software propietari i es caracteritza per mantenir comunicacions P2P i utilitzar l'algoritme de xifrat AES de 256 bits per a les transmissions de veu, fitxers i missatges. En la versió de pagament s'utilitza l'algoritme RSA per l'accés a correu de veu.

6) Les col·lisions de missatgeria en les transmissions per xarxa constitueixen un problema que disminueix el rendiment de la xarxa. Indiqueu quina és l'afirmació correcta:

a) El protocol CSMA/CD consisteix en què, quan un equip vol enviar una informació, primer escolta el canal per saber si un altre equip està transmetent. Si el canal està ocupat, llavors espera fins que el canal quedi lliure per començar a transmetre. Aquest protocol és propi de les xarxes sense fils.

b) El protocol CSMA/CA consisteix en què cada equip anuncia la seva intenció de transmetre abans de fer-ho, per evitar col·lisions de dades entre els paquets de dades. D'aquesta manera, la resta d'equips de la xarxa poden saber quan hi ha col·lisions. En aquest cas, en lloc de transmetre la trama quan el medi està lliure, s'espera un temps aleatori abans d'enviar les trames.

c) El protocol CSMA/CA, propi de les xarxes sense fils, es basa en la una assignació de temps de transmissió dels diferents equips, de manera que cada un d'ells disposa d'un temps limitat per realitzar les seves transmissions. En cas de finalitzar la seva assignació de temps, llavors incorpora un paquet de finalització intermèdia.

d) Cap de les anteriors

7) El problema de les col·lisions de transmissió en xarxes sense fils es fa especialment important a causa d'alguns motius. Indiqueu quina és l'afirmació correcta:

a) El *hidden terminal problem*, que ve provocat per la insistència en l'enviament de paquets per un terminal emissor quan el receptor no rep correctament la identificació de l'emissor, rebutjant el missatge. Dit rebuig provoca un increment en el nombre de missatges que circulen i, per tant, un increment en el nombre de col·lisions.

b) El *blocked terminal problem*, que ve provocat per obstacles físics a l'espai geogràfic o la distància. Llavors pot passar que un equip comprovi el canal, el trobi lliure i iniciï una transmissió cap a un altre node que ja està rebent una trama des d'una altra estació.

c) El *fading*, que descriu el problema que es provoca a causa de l'atenuació del senyal quan aquesta es propaga a través de l'aire. La conseqüència és que dues estacions poden transmetre simultàniament cap al mateix node i provocar en el receptor col·lisions no advertides.

d) El *exposed node*, que consisteix en que un node que ha estat designat com a node repetidor inicia la seva transmissió a el mateix temps que rep un paquet per retransmetre. Llavors es produeix la transmissió de dos missatges al mateix temps, provocant una col·lisió.

8) Hi ha una equivalència entre el model OSI i l'especificació IEEE 802. Indiqueu quina de les següents és una afirmació incorrecta:

a) Les capes MAC i PHY equivalen de manera lògica amb les funcions de les capes d'enllaç i física del model OSI.

b) Les funcionalitats de la capa d'física del model OSI són equivalents a les descrites al protocol 802.2.

c) Les capes MAC i PHY apareixen descrites en els protocols 802.3 (Ethernet), 804.4 (Token Bus), 802.5 (Token Ring) i 802.11 (WLAN).

d) La capa de Control d'Accés Lògic (LLC) es descriu a l'estàndard 802.2.

9) Una Wireless Mesh Networks (WMN) és un tipus de xarxa sense fils. Indiqueu quina de les següents afirmacions no és pròpia d'una WMN:

a) Està formada per una estació base i els seus punts d'accés, que es comuniquen entre ells per conformar una única xarxa sense fils amb el mateix SSID i contrasenya, a la qual es poden connectar els clients.

b) El trànsit es redirigeix per la xarxa de manera que es disposa sempre de la millor senyal possible a la xarxa. Les WMN determinen en cada moment el node idoni al qual connectar-se.

c) El principal inconvenient de les WMN està en la tolerància a fallades, ja que una caiguda d'un node implica la caiguda de tota la xarxa.

d) Pel fet de disposar de diversos nodes en una mateixa zona, les distàncies a aconseguir en les transmissions no són tan grans, de manera que es pot tenir una disminució de les interferències i un estalvi d'energia, ja que no fa falta transmetre a tanta potència.

10) El projecte 802 defineix, a més de la topologia de xarxa, un conjunt de regles d'accés i transmissions. El seguiment de l'estàndard és indispensable per assegurar la difusió d'una tecnologia, permetent que diverses empreses puguin fabricar i vendre dispositius amb garanties de funcionament en entorns reals de xarxes d'ordinadors. Indiqueu quin subconjunt de normes es relaciona amb la capa LLC de el projecte IEEE:

a) 802.2
b) 802.3
c) 802.4
d) 805.5

11) En el món de les xarxes d'ordinadors apareix el concepte de MAC address. Indiqueu quina és l'afirmació correcta en relació a aquest concepte:

a) El terme *MAC address* fa referència la capa d'Accés al Medi (*Media Access Control*) a les comunicacions, d'acord amb el protocol IEEE.

b) És un nombre que identifica de manera biunívoca un conjunt de dispositius de la xarxa. Ve definit pel model clàssic OSI.

c) També conegut com a Direcció Física, és una col·lecció de caràcters hexadecimals únic per a cada dispositiu de la xarxa, i es relaciona amb la capa 2 del model OSI.

d) És una identificació d'un dispositiu que es pot obtenir, en *Windows*, per mitjà de la instrucció *ip link list*

12) Dins el protocol RFC es defineix el concepte de DHCP, que permet als dispositius de xarxa (clients) l'obtenció dels paràmetres necessaris per a la seva connexió a una xarxa. DHCP fa referència a la gestió d'adreces IP i altres dades de configuració per a tota una xarxa. Indiqueu quina de les següents afirmacions és vertadera:

a) L'assignació de la IP es realitza de manera dinàmica per un ordinador servidor, que assigna sempre la mateixa IP a cada un dels dispositius que es connecten a la xarxa.

b) El servidor assigna una IP aleatòria als equips que es connecten a la xarxa. Pel fet de ser una LAN en la qual intervé un nombre limitat de dispositius, no hi ha problemes de duplicitat d'IP dins de la mateixa xarxa.

c) El servidor DHCP assigna dinàmicament una IP i altres paràmetres de configuració de xarxa, amb la finalitat que puguin comunicar-se amb altres xarxes IP.

d) Cap de les anteriors.

13) En el cas de les xarxes és fonamental controlar la seguretat de les comunicacions. Quan es tracta de xarxes sense fil apareixen riscos addicionals que són inherents a la naturalesa sense fils, de manera que qualsevol que es trobi dins del radi d'abast de la xarxa podria dur a terme accions malicioses. Indiqueu quina de les següents afirmacions és vertadera:

a) *Eavesdropping* consisteix a realitzar accions de sobrecàrrega de sistema per provocar una caiguda del rendiment.

b) *MAC Snooping* consisteix en suplantar la MAC Address d'un dispositiu permès a la xarxa.

c) *Man-in-the-middle* consisteix en què l'atacant se situa entre l'emissor i el receptor, suplantant una de les parts i fent creure a l'altra que està parlant amb el legítim interlocutor de la comunicació.

d) Cap de les anteriors

14) El terme REST està relacionat amb un esquema d'aplicacions basades en la utilització de Serveis Web. D'aquesta manera, l'element principal en el qual es basen aquests serveis són les URL ja que, en última instància, un Web Service (WS) es relaciona directament amb la URL a la qual s'ha d'accedir per utilitzar aquest WS. En relació a REST es pot dir que:

a) En REST sempre hi ha una transmissió de dades i informacions utilitzant el llenguatge XML

b) Hi ha un estàndard en els missatges, de manera que tots els serveis web han de ser cridats amb els mateixos paràmetres i retornar fitxers XML o JSON amb la mateixa estructura.

c) REST no té restriccions pel que fa a la tecnologia a utilitzar, només es defineix la manera de transferir les dades entre els agents interlocutors.

d) El codi de programació dels WS és públic, de manera que aquest es pot incloure directament en els programes de client per poder accedir a les funcionalitats del servidor.

15) A les transmissions en xarxes d'ordinadors és fonamental mantenir uns alts nivells de seguretat que protegeixin les dades i informacions, en relació a amenaces, riscos i vulnerabilitats. Quant a la seguretat de la informació es descriuen diversos pilars. Indiqueu quina de les següents afirmacions és falsa:

a) Confidencialitat consisteix a assegurar que només el personal autoritzat accedeix a la informació que li correspon. Així, cada sistema automàtic o individual només podrà usar els recursos que necessita per exercir les seves tasques.

b) Integritat consisteix a assegurar que la informació no es perd ni es veu compromesa voluntària i involuntàriament.

c) Disponibilitat consisteix a assegurar que la informació estigui disponible i completa per a les persones que la necessitin.

d) Gestió d'usuaris consisteix a disposar d'un bon sistema de seguretat en la creació de contrasenyes i en assegurar que els usuaris disposin de formació específica en temes de generació de contrasenyes.

16) A les configuracions dels *routers*, normalment, s'ofereixen diverses modalitats de xifrat, a efectes de millorar la seguretat de la xarxa. Indiqueu quina de les següents afirmacions és certa:

a) WEP (*Wireless Equivalent Privacy*) és un mètode de seguretat de xifrat inclòs en l'estàndard IEEE 802.11 per xarxes cablejades. Utilitza una clau compartida (PSK) de seguretat per xifrar totes les comunicacions. Utilitza l'algoritme d'encriptació RC4.

b) WPA (*Wifi Protected Access*) és una variant millorada de WEP que augmenta la seguretat d'una clau compartida única amb claus dinàmiques (TKIP) i protegeix les identitats dels usuaris mitjançant l'autenticació amb clau compartida (PSK). Utilitza l'algoritme d'encriptació AES amb integració de claus EAP

c) WPA2 (*Wifi Protected Access 2*) apareix en 2005 amb un algoritme d'encriptació EPSA i integració de claus EAP, amb 128 bits de clau secreta.

d) WPA3 és la versió de WPA que apareix en 2018, amb una clau de xifrat de 192 bits en la versió *Enterprise*, que incrementa la seguretat en comparació amb el seu antecessor WPA2.

17) La seguretat de les xarxes sense fils es basa en l'aplicació d'alguns protocols, com WEP i WAP, en les seves diferents versions. Indiqueu l'afirmació correcta:

a) El protocol WEP apareix a 1999, amb integració de claus i amb un algoritme d'encriptació RC4 amb clau secreta de 40 a 104 bits.

b) El protocol WAP apareix a 2001, amb algoritme d'encriptació RC4 i clau secreta de 64 a 128 bits, amb integració de claus EAP.

c) El protocol WAP2 apareix a 2005, amb algoritme d'encriptació AES i clau secreta de 256 bits, amb integració de claus EAP.

d) Cap de les anteriors

18) El CCN és un organisme espanyol adscrit de l'CNI que disposa d'un CERT dedicat a la gestió de mesures de gestió de la seguretat informàtica, amb l'objectiu de mitigar el risc d'atacs contra xarxes i sistemes informàtics. Indiqueu quina és l'afirmació correcta en relació a *ransomware*:

a) *Ransomware* és un tipus de ciberatac que té com a objectiu el robatori d'informació, de tecnologia o de qualsevol tipus d'informació.

b) Ransomware utilitza diversos mètodes per aconseguir les credencials dels usuaris, com el *phising*, o per obtenció de credencials disponibles a la *dark web*.

c) Els atacs *ransomware* tenen com a objectiu congestionar les xarxes sense fils, però en cap cas provoquen robatoris d'informació.

d) *Ransomware* és un tipus de ciberdelicte que cerca principalment beneficis econòmics per mitjà de l'extorsió, derivats d'impossibilitar l'accés a la informació per part de les víctimes del ciberdelicte.

19) A una xarxa es defineixen les vulnerabilitats com fallides o errors de sistema, que constitueixen portes obertes que es poden aprofitar per part dels delinqüents cibernètics. Indiqueu quina és l'afirmació correcta:

a) Les vulnerabilitats físiques es refereixen a problemes d'accés a la xarxa informàtica per part de persones alienes a l'organització.

b) Les vulnerabilitats físiques es refereixen a problemes de configuració dels equips físics. Amb una bona configuració és possible minimitzar-los o evitar-los.

c) Les vulnerabilitats lògiques es refereixen a el control d'accés a dependències que continguin els *Data Warehouse*, atès que el control ha de seguir la lògica d'accés pròpia de l'organització

d) Les vulnerabilitats físiques inclouen consideracions d'accés físic als dispositius d'emmagatzematgent de dades per part de persones no autoritzades.

---

20) La Llei 59/2003, article 3, tracta sobre la consideració de la signatura electrònica i els documents signats electrònicament. Indiqueu quina de les següents afirmacions no es correspon amb el contingut de l'esmentat article:

a) La signatura electrònica avançada és la signatura electrònica que permet identificar el signant i detectar qualsevol canvi ulterior de les dades signades, que està vinculada al signant de manera única i a les dades a què es refereix, i que ha estat creada per mitjans pels quals el signant pot mantenir sota el seu exclusiu control.

b) Es considera document electrònic el redactat en suport electrònic que incorpori dades que estiguin signades electrònicament.

c) La signatura electrònica reconeguda tindrà respecte de les dades consignades en forma electrònica el mateix valor que la signatura manuscrita en relació amb els consignats en paper, sempre que aquesta es presenti com a alternativa a la versió en paper.

d) El suport en què es trobin les dades signades electrònicament és admissible com a prova documental a un judici

---

21) La Llei 59/2003, articles 6 i 7, tracta sobre la consideració de certificat digital i sobre les persones que poden disposar de certificat digital. Indiqueu quina de les següents afirmacions és certa:

a) Un signant és la persona que té un dispositiu de creació de signatura i que actua exclusivament en nom propi.

b) Les persones que poden sol·licitar certificats electrònics de persones jurídiques són els seus administradors, representants legals i voluntaris amb poder suficient a aquests efectes.

c) Els certificats electrònics de les persones jurídiques afecten considerablement a el règim de representació orgànica o voluntària regulat per la legislació civil o mercantil aplicable a cada persona jurídica.

d) La custòdia de les dades de creació de signatura associades a cada certificat electrònic de persona jurídica serà responsabilitat de la persona física sol·licitant, si bé la seva identificació no s'ha d'incloure en el propi certificat electrònic.

---

22) En el certificat digital prenen especial importància els aspectes d'identificació i autenticació per part de les Administracions Públiques (AP). Així, a la Llei 39/2015, capítol II, s'indiquen les maneres d'identificació i firma. Indiqui l'afirmació incorrecta en relació a la identificació electrònica dels interessats, així, els interessats es podran identificar mitjançant:

a) Sistemes basats en certificats electrònics qualificats de signatura electrònica expedits per prestadors inclosos a la «Llista de confiança de prestadors de serveis de certificació».

b) Sistemes basats en certificats electrònics qualificats de segell electrònic expedits per prestadors inclosos a la «Llista de confiança de prestadors de serveis de certificació».

c) Sistemes de clau concertada i qualsevol altre sistema que les administracions públiques considerin vàlid en els termes i condicions que s'estableixin

d) Tots els certificats que subministri una empresa amb solvència suficient i credibilitat demostrable són considerats vàlids, a tots els efectes, en qualsevol procés de certificació digital en entorns tancats de comunicació en els quals intervingui l'Administració Pública, d'acord amb l'específicament acordat entre les parts.

23) En accions de diagnòstic de funcionament de dispositius en una xarxa de comunicacions es pot utilitzar l'ordre *ping*. Indiqueu quina és una afirmació certa en relació a l'ordre *ping*:

a) És un acrònim de *Packet Interchange Groper* disponible en entorns *Windows* i *Linux*.

b) És una instrucció de diagnòstic que permet realitzar una verificació de l'estat d'una determinada connexió per mitjà de l'enviament de 5 sol·licituds d'eco, a la seva execució per defecte.

c) Per mitjà de el temps d'espera de la resposta a l'enviament d'informació es determina el temps de retard d'aquesta resposta.

d) Cap de les anteriors

24) La Llei 03/2018 de Protecció de Dades Personals i garantia dels drets digitals regula el tractament de dades personals, com a dret fonamental protegit per la Constitució espanyola. En aquesta llei s'indica que Internet s'ha convertit en una realitat omnipresent tant en la vida personal com col·lectiva. No obstant això, l'ús d'Internet té múltiples riscos, i és competència del sector públic la protecció de dades i la transparència i accés a la informació pública. Indiqueu quines de les següents afirmacions no és correcta:

a) El tractament de les dades està basat en el consentiment de l'afectat, entenent com a tal consentiment tota manifestació de voluntat lliure, específica, informada i inequívoca per la qual aquest accepta, mitjançant una declaració o clara acció afirmativa, el tractament de dades personals que li concerneixen.

b) El tractament de les dades personals d'un menor d'edat només pot fundar-se en el seu consentiment quan la persona sigui major de catorze anys, excepte en els casos en què preveu la llei, relacionats amb la tutela.

c) El responsable del tractament de les dades, sempre que aquestes siguin obtingudes de l'afectat, ha de facilitar al mateix la identitat del responsable del tractament i del seu representant, la finalitat del tractament i la possibilitat d'exercir els seus drets en relació amb les dades.

d) Amb la finalitat de tractaments amb fins de videovigilància, només les persones jurídiques de naturalesa pública poden dur a terme el tractament d'imatges a través de sistemes de càmeres o videocàmeres en què es captin imatges de la via pública, sempre amb la finalitat de preservar la seguretat de les persones i béns, així com de les seves instal·lacions.

25) Un sistema de RAID permet una millora del rendiment en l'emmagatzematgent extern. Així, RAID permet triar la millor forma d'utilitzar el dispositiu, d'acord a les necessitats de l'organització. Indiqui quina de les assignacions és correcta:

a) RAID0 és el sistema més ràpid. Es necessita un mínim de quatre unitats, de manera que les dades es distribueixen en cada disc. És ideal per als usuaris que necessiten la màxima velocitat i capacitat, com a processos d'edició de vídeo. No és tolerant a fallides i no és un sistema recomanat com a solució de còpies de seguretat. Respon a el concepte de *disk stripping*.

b) RAID1 és una manera segura que requereix un mínim de 2 unitats, que treballa amb parells d'unitats, replicant les dades. Proporciona la màxima seguretat de les dades en el cas d'una fallida de disc únic. No obstant això, el rendiment es redueix durant l'escriptura. És una elecció ideal quan la seguretat és més important que la velocitat. Respon al concepte de *disk mirroring*.

c) RAID 0 + 1 és un sistema RAID compost d'un duplicat de conjunts distribuïts de dades. És una combinació de RAID 0 i RAID 1 i requereix disposar d'un mínim de dos discos, si bé només la meitat d'ells s'utilitza per a l'emmagatzematgent de dades. Aquest sistema proporciona bones velocitats, si bé tots els discos han de tenir la mateixa capacitat.

d) RAID 3 és un sistema que realitza la distribució de dades a nivell de byte, entre diversos discos, amb un disc addicional dedicat a emmagatzemar informació de paritat. És un sistema tolerant a fallides, però no és un sistema que proporcioni seguretat de dades en entorns on es llegeixen arxius llargs i seqüencials, com arxius de vídeo.

26) A 1985, Richard Stallman publica el Manifest GNU, que és una explicació i definició dels objectius de GNU, anunciat pel propi Stallman en 1983. GNU es relaciona directament amb el programari lliure, de manera que s'afirma que els usuaris disposen de llibertats essencials, entre les quals no es troba:

a) La llibertat d'executar el programa en les condicions que descrigui de manera específica l'autor de el programa.

b) La llibertat d'estudiar el funcionament d'un programa i modificar-lo de manera que realitzi les tasques com l'usuari desitgi. Per a això és indispensable disposar del codi font del programa.

c) La llibertat de redistribuir còpies per ajudar els altres usuaris.

d) La llibertat de distribuir còpies de les seves versions modificades a altres persones, donant a tota la comunitat l'oportunitat de beneficiar-se dels seus canvis.

27) La IEEE ha definit diferents estàndards de funcionament per als diferents tipus de xarxa i tecnologies emprades. Indiqueu quina és l'afirmació incorrecta pel que fa a vinculació de tipus de xarxa i codi de normativa segons la IEEE:

a) IEEE 802.15 amb la WPAN
b) IEEE 802.11 amb la WLAN
c) IEEE 802.16 amb la WMAN
d) IEEE 802.20 amb la WBAN

28) Un Servei de directoris (SD) és, en essència, una aplicació o conjunt d'aplicacions que emmagatzema i organitza la informació sobre els usuaris d'una xarxa d'ordinadors. Amb aquesta informació, els administradors poden gestionar l'accés dels usuaris als recursos d'aquesta xarxa. Indiqueu quina de les següents afirmacions és falsa en relació a LDAP:

a) LDAP és un protocol basat en X.500, que s'executa sobre TCP / IP o altres serveis de transferència orientats a connexió.

b) LDAP defineix una organització de les entrades de la base de dades en forma d'estructura jeràrquica en arbre.

c) LDAP està basat en el model client-servidor, on el servidor té les dades que conformen la informació de directori.

d) LDAP és una base de dades que en la qual les entrades són els serveis de la SD, que tenen atributs que es relacionen amb una única clau.

29) De la mateixa manera que la seguretat és molt important en les xarxes de comunicació, en un Servei de directoris (SD) és sumament important mantenir els nivells de seguretat, ja que poden contenir dades i informació sensible. Indiqueu quina de les següents afirmacions no és correcta:

a) L'autenticació anònima és útil per al cas d'accessos de tipus *read-only* al directori, sempre que les dades no siguin sensibles.

b) SASL és un marc que proporciona múltiples mecanismes d'autenticació i encriptació per protocols orientats a connexió.

c) A la implementació de LDAPv3 es permet una autenticació anònima, de manera que el client només s'ha de autenticar en cas de realitzar accessos d'alteració dels serveis.

d) La Autenticació Bàsica proporciona facilitats d'autenticació a les dades d'identificació de client que són transmeses per la xarxa amb text clar, tot i que aquest sistema no es recomana a xarxes obertes en les què no hi ha autenticació o encriptació en capes inferiors, com SSL.

30) El sistema d'informació d'un Ajuntament ha de seguir la normativa que dicti la legislació estatal. En el cas de la facturació s'ha de tenir en compte la normativa en relació a la factura electrònica. Segons el lloc web del Ministeri d'Hisenda, una factura electrònica és una factura que s'expedeix i rep en format electrònic i té els mateixos efectes legals que una factura en paper. Indiqueu l'afirmació correcta:

a) La factura electrònica està regulada pel RD 1619/2012, en el qual s'aprova el reglament pel qual es regulen les obligacions de facturació.

b) Les factures electròniques, pel fet diferencial de ser electròniques, han de tenir obligatòriament un format electrònic estructurat, amb llenguatges com XML. No s'accepten, baix cap concepte, factures presentades en forma d'imatge o PDF.

c) La factura electrònica proporciona beneficis com: acurçar els cicles de tramitació, redueix errors humans, elimina costos d'impressió. Ara bé, no resol la problemàtica de millorar l'espai físic d'emmagatzematgent, ja que es requereixen unitats d'emmagatzematgent de dades.

d) L'únic requisit de format de les factures electròniques que utilitzin les administracions públiques és que estiguin escrites en un llenguatge informàtic determinat, que sigui Facturae 3.2 o 3.2.1

31) En relació al *cloud computing* hi ha diverses formes de servei, que proporcionen diversos nivells de flexibilitat o senzillesa a l'hora de generar i mantenir les aplicacions. Indiqueu quina de les següents afirmacions és vertadera:

a) SaaS es refereix a un model de *cloud computing* que proporciona als usuaris accés al software basat en *cloud* d'un proveïdor. Els usuaris poden descarregar i instal·lar el software les vegades que vulguin, sense limitació provocada pel nombre de llicències
b) PaaS es refereix a un model de *cloud computing* que proporciona als usuaris un entorn de *cloud* en el qual poden desenvolupar, gestionar i distribuir les seves pròpies aplicacions.
c) IaaS es refereix a un model de *cloud computing* en el qual un proveïdor proporciona als usuaris accés a recursos de càlcul com servidors, emmagatzemament i xarxes. Els usuaris només han d'adquirir el hardware i l'empresa de *cloud computing* s'encarrega del manteniment dels diversos equipaments hardware
d) Cap de les anteriors

32) Arran de la crisi provocada pel virus Covid-19, algunes organitzacions s'han vist obligades a prendre mesures i adoptar solucions per afrontar les necessitats sorgides. Una d'elles està relacionada amb la utilització de SaaS per poder operar en remot. Indiqui quin dels següents no és un proveïdor de Saas:

a) Microsoft
b) Amazon
c) ERP
d) IBM

33) Els models de desplegament de solucions en *cloud computing* poden adoptar diverses modalitats. Indiqueu quina de les següents és l'afirmació certa:

a) El model de desplegament de núvol públic ofereix el servei a diversos clients des d'un mateix centre de càlcul i computació, de manera que els clients comparteixen recursos d'emmagatzematgent i processament.
b) El model de desplegament de núvol privat permet que els recursos siguin lliurats de forma exclusiva i privada a el client, de manera que aquest té el control sobre el servei que contracta. Ara bé, el control de les dades segueix recaient en el proveïdor de serveis.
c) El model de núvol híbrid és una combinació de núvol públic i privat, en la qual el client decideix els serveis que desitja contractar. Ofereix majors nivells de seguretat que el núvol privat, amb una reducció de costos
d) Cap de las anteriors

34) Hi ha dues solucions bàsiques quant a la utilització de programari: *cloud software* i *software on premise*. Indiqueu quina és l'afirmació certa:

a) En el cas del cloud software, les aplicacions software s'instal·len en els ordinadors locals a partir d'una descàrrega de fitxers des del propi núvol.
b) En el cas del *software on premise* l'empresa no necessita disposar de sistemes de seguretat de dades i programes, ja que l'empresa que ven el software és la responsable del bon funcionament de les aplicacions.
c) La modalitat de software en el núvol requereix de la instal·lació d'ordinadors i servidors locals molt potents, per poder suportar molta càrrega de connexions web.
d) Cap de les anteriors.

35) Un de les necessitats, quan es vol seguir una estratègia digital que inclogui la presència a la WWW, és disposar d'un espai per allotjar les pàgines web del lloc dins d'un servidor web. Apareix llavors el concepte de Web Hosting. Existeixen diverses alternatives per cobrir les diferents necessitats d'allotjament. Indiquin quina és l'afirmació falsa:

a) El hosting compartit és un tipus d'allotjament consistent en què el proveïdor lloga espai d'emmagatzematgent de memòria a varis llocs web dins d'un mateix servidor. Els clients comparteixen els recursos del servidor.

b) Un servidor dedicat és un tipus de web hosting d'ús exclusiu d'un únic client, que no comparteix recursos amb altres clients. Pel fet de no compartir recursos, el rendiment del lloc web no es veu afectat pel tràfic.

c) Un VPS és un tipus d'allotjament web en el qual el servidor web està compartit per diversos clients, però utilitzant una tecnologia de compartició d'altres recursos (com CPU de servidor) seguint una política d'assignació de CPU que provoca que es tingui la impressió de què el servidor està totalment dedicat a un dels clients.

d) El cloud hosting consisteix a executar des d'un núvol tots els recursos necessaris per al funcionament d'un lloc web

36) La Llei 3/2018, de Protecció de Dades Personals i garantia dels drets digitals, en el seu apartat d'Autoritats de protecció de dades (TÍTOL VII), indica que l'Agència Espanyola de Protecció de Dades és una autoritat administrativa en protecció de dades. En aquest sentit es realitzen algunes afirmacions a partir del contingut de la Llei. Indiqueu quina és l'afirmació certa:

a) L'Agència Espanyola de Protecció de Dades és una autoritat administrativa depenent del Consell General de Poder Judicial, que realitza accions de protecció de dades.

b) Correspon a l'Agència Espanyola de Protecció de Dades la supervisió de l'aplicació de la Llei 03/2018, així com d'exercir les funcions i potestats que se li atribueixin a partir d'altres lleis o normes de Dret de la Unió Europea.

c) Es recomana que les administracions públiques, entre les quals s'inclouen les tributàries i de la Seguretat Social, proporcionin a l'Agència Espanyola de Protecció de Dades les dades, informes, antecedents i justificants necessaris per dur a terme la seva activitat de recerca, si bé aquesta col·laboració no és, de cap manera, una obligació.

d) L'Agència Espanyola de Protecció de Dades és un organització de caràcter públic que desenvolupa les seves accions amb una limitació geogràfica limitada a les fronteres de l'estat espanyol, de manera que no pot realitzar les seves funcions a nivell exterior. Les accions de protecció de dades a l'exterior només les pot dur a terme el Ministeri d'Exteriors.

37) En el disseny de Bases de Dades s'intenta aconseguir la major qualitat de dades, en relació a eliminació de redundàncies i facilitar tasques de modificació de dades, eliminar problemes d'integritat referencial i generar una estructura fàcilment comprensible i amb possibilitats d'escalabilitat. Per a tals efectes es defineix el concepte de Normalització de Dades, amb diverses Formes Normals. Indiqui l'afirmació incorrecta:

a) Es diu que una taula d'una base de dades està en primera forma normal quan tots els atributs contenen una única dada, tots els atributs de la clau estan definits i tots els atributs depenen de la clau primària.

b) Es diu que una taula d'una base de dades està en segona forma normal quan no inclou dependències parcials de la clau primària.

c) Es diu que una taula d'una base de dades està en tercera forma normal quan no conté dependències transitives.

d) Es diu que una taula d'una base de dades està en quarta forma normal quan cada un dels determinants és una clau candidata.

38) A Bases de Dades es denomina amb l'acrònim ACID a determinades característiques que compleixen alguns models de Bases de Dades. Indiqueu quina de les següents no és una de les propietats ACID esmentades:

a) *Atomicity*, que es refereix al fet que les transaccions en Bases de Dades han de ser executades en la seva totalitat: o bé s'executen de manera completa, o bé no s'executen.

b) *Completity*, que es refereix a assegurar que les transaccions realitzin els bloquejos de tots els registres de les taules amb les que va a treballar, de manera que s'asseguri que les transaccions concurrents no interaccionen entre sí.

c) *Isolation*, que es refereix al fet que la realització dues transaccions sobre el mateix conjunt de dades han de ser independents, de manera que no es generi cap tipus d'error ni inconsistència entre elles.

d) *Durability*, que es refereix al fet que una vegada realitzada l'operació, aquesta persistirà i no es podrà desfer.

39) El tipus de cable més comú en les LAN és el parell trenat, adoptat com a solució per connectar xarxes reutilitzant el cablejat existent de xarxes telefòniques. Indiqueu quina de les següents és una afirmació vertadera:

a) El cable parell trenat necessita uns connectors específics per assegurar la seva correcta instal·lació. Es poden destacar el RJ-45 i RJ-49, amb vuit connexions de cable, corresponents a quatre parells trenats.

b) Hi ha diversos tipus de cable de parell trenat: el STP (que no posseeix cap tipus de protecció addicional a la recoberta de PVC), el UTP (que va recobert per una malla conductora que actua de pantalla davant interferències i renou electrònic) i el FTP (que posseeix una pantalla global d'alumini que millora la protecció).

c) Els cables es poden classificar per categories, així, la categoria 5b correspon a un tipus de cable que té una freqüència màxima de 250 MHz, és cable UTP o STP i té connectors RJ-45 o RJ-49

d) Cap de les anteriors

40) Una còpia de seguretat és un procés mitjançant el qual es duplica, d'un suport a un altre, un determinat volum de dades. L'objectiu és poder recuperar-las en cas de fallida a l'allotjament original de les dades. A les còpies de seguretat és important determinar la informació que s'ha de respaldar i la periodicitat de la còpia. En aquest sentit, es defineixen diversos tipus de còpia de seguretat. Indiqueu quina de les següents és una afirmació incorrecta:

a) La còpia de seguretat en mirall o RAID1 consisteix a realitzar una còpia de seguretat realitzant una còpia de les dades en temps real. Aquestes còpies asseguren que es pot recuperar la informació en qualsevol moment posterior a la còpia en el mirall, atès que la còpia sempre és un reflex de l'original.

b) La còpia de seguretat completa consisteix a realitzar una còpia de totes les dades en un suport diferent a l'original. Aquest sistema permet una fàcil restauració de dades, però requereix majors necessitats d'emmagatzematgent i cost econòmic enfront d'altres tipus de còpia. Aquestes còpies es solen realitzar en horaris que no comportin càrrega sobre el servidor.

c) La còpia de seguretat diferencial consisteix a realitzar una còpia de totes les dades que han patit alguna variació respecte de l'anterior còpia de seguretat completa, o bé que s'han creat des de la darrera còpia de seguretat completa. El backup diferencial sempre parteix d'un backup complet.

d) La còpia de seguretat incremental consisteix a copiar les dades que han variat des de l'última còpia realitzada. D'aquesta manera només es copien els canvis que no són redundants. Aquest tipus de còpia de seguretat té manco problemes d'espai que la còpia completa, però el temps de recuperació de dades de la incremental és més gran a la completa

41) L'objectiu principal de les còpies de seguretat és la preservació de les dades per garantir la continuïtat de el Sistema d'Informació davant de possibles errades en els mateixos. El procediment que se segueix a una fallida és la restauració de la còpia de seguretat. Indiqueu quina és l'afirmació correcta en relació als següents conceptes relacionats amb la restauració de còpies de seguretat:

a) El *Recovery Time Objective* es defineix com el temps que es triga a recuperar un nivell de servei mínim després d'una caiguda del servei sense afectar la continuïtat de l'operatòria de l'organització

b) El *Maximum tolerable Downtime* és el temps màxim que ha estat caigut un procés o sistema abans de recuperar un determinat nivell de servei.

c) El *Revised Operating Leve*l és el nivell mínim de recuperació que ha de tenir una activitat perquè es consideri com recuperada, encara que el nivell de servei no sigui l'òptim.

d) Cap de les anteriors

42) A la planificació de les còpies de seguretat és crític seleccionar el suport idoni per salvaguardar la informació. D'aquesta manera, es poden definir diversos sistemes o arquitectures d'emmagatzematgent. Indiqueu quina és l'afirmació incorrecta:

a) S'utilitza el terme DAS quan s'utilitza, per emmagatzemar la còpia de seguretat, un dispositiu d'emmagatzematgent directe de l'ordinador.

b) S'utilitza el terme NAS per fer referència a l'arquitectura de còpies de seguretat en la que s'utilitza un dispositiu d'emmagatzematgent de còpies de seguretat que és comú a tots els ordinadors que estan connectats a una LAN

c) S'utilitza el terme HAS a sistema híbrid en el qual els ordinadors d'una xarxa realitzen còpies de seguretat en emmagatzemaments de connexió directa a l'ordinador, o bé en un dispositiu comú a tots els ordinadors.

d) S'utilitza el terme SAN quan s'utilitza un conjunt de diversos dispositius d'emmagatzematgent per emmagatzemar les còpies de seguretat dels ordinadors d'una xarxa.

43) A la criptografia, una unitat de xifrat per blocs és una unitat de xifrat de clau simètrica que opera en grups de bits de longitud fixa, anomenats blocs, aplicant una transformació. Hi ha diversos algoritmes de xifrat per blocs. Indiqueu quina és l'afirmació correcta:

a) L'algoritme DES (*Data Encryption Standard*), dissenyat per IBM, fa servir una clau de 64 bits i treball amb blocs de 72 bits. D'aquests, 8 bits es destinen per a funcions de control de paritat.

b) L'algoritme AES (*Advanced Encryption Standard*), també conegut com algorisme Rijndael, posseeix un xifrat simètric que permet xifrar blocs de 128 bits, utilitzant claus de 128, 192 o 256 bits.

c) L'algoritme 3AES (triple AES) va ser desenvolupat com una millora de l'algoritme AES, estenent l'aplicació de l'algoritme fins a tres vegades consecutives, amb tres claus diferents. La mida de la clau combinada és de 168 bits.

d) Cap de les anteriors

44) S'entén per Qualitat de Servei (QoS) la possibilitat d'assegurar, principalment, una determinada taxa de transmissió de dades a la xarxa, un retard i una variació de retard. Hi

ha variables de mesura de la QoS. Indiqueu quina de les següents no és una afirmació correcta, en relació a paràmetres que afecten la QoS:

a) Els Retards, també coneguts com a *delay*, són increments en el temps de recepció de paquets per part del receptor. Es poden deure a motius diversos, com la permanència a cues de paquets o per seguir rutes menys directes per prevenir la congestió de la xarxa.

b) La Latència, també coneguda com a *jitter*, fa referència al temps que es tarda per transmetre un paquet dins de la xarxa. Factors que generen més *jitter* són la tecnologia d'accés a Internet, la distància entre els punts emissor i receptor i la pròpia capacitat de el dispositiu emissor.

c) En ocasions es produeixen alteracions en l'ordre de lliurament dels paquets d'un missatge, a causa principalment pel fet de que aquests han estat en cues diferents o perquè han seguit rutes diferents de la resta de paquets del missatge. Aquest problema requereix d'un protocol que permeti reordenar els paquets al dispositiu receptor.

d) Durant la transmissió de paquets es poden produir errors, per ser mal dirigits o per corrompre's durant el seu encaminament. Aquests errors poden provocar una disminució de la QoS.

---

45) Els administradors de bases de dades poden utilitzar diferents sistemes per assegurar la integritat de dades i per encapsular procediments i definicions de taula. Indiqueu quina és l'afirmació incorrecta:

a) Un TRIGGER de SQL defineix una acció que s'hauria de realitzar a la base de dades sempre que ocorri un determinat esdeveniment en l'aplicació. En general, aquests esdeveniments van associats a accions de INSERT, UPDATE o DELETE a taules.

b) Un STORED PROCEDURE és un tipus de subprograma que es pot programar a nivell d'administració de la base de dades. Poden ser invocats per altres programes i rebre dades per paràmetre.

c) La diferència entre els PROCEDURE i les FUNCTION està en el tipus de dades dels paràmetres de retorn.

d) Una TRANSACTION és la unitat bàsica d'execució a una base de dades. Pot ser un programa o part d'un programa, o una sentència, de manera que s'han de realitzar totes les accions que inclou la TRANSACTION. En cas contrari, s'ha d'assegurar que es retorna a la situació de la base de dades anterior a l'inici de l'execució de la TRANSACTION

---

46) El disseny de software tendeix a ser cada vegada més modular. Així, les aplicacions es componen d'una sèrie de components (serveis) reutilitzables, que es poden trobar distribuïts al llarg d'una sèrie de màquines connectades en xarxa. Indiqui l'afirmació incorrecta:

a) Un servei web, segons la W3C, és un software dissenyat per suportar interaccions màquina a màquina a través de la xarxa. D'aquesta manera, proporcionen una manera estàndard d'interoperar entre aplicacions que s'executen a diferents plataformes.

b) A una arquitectura orientada a serveis, qualsevol interacció punt a punt implica dos *endpoints*: un que proporciona un servei, que correspon al servei web, i un altre que el consumeix

c) Els serveis basats en SOAP utilitzen missatges per intercomunicar-se. La descripció de les operacions que ofereix el servei es poden escriure en un llenguatge anomenat WSDL.

d) El llenguatge de programació que s'utilitza en la codificació d'un servei web ha de ser el mateix que el del programa que l'invoca. D'aquesta manera s'assegura la màxima eficiència a la interacció entre els dos programes

47) La Llei 39/2015 tracta sobre el procediment administratiu comú de les administracions públiques. A aquesta Llei es tracta el tema de l'acreditació en matèria de representació, amb l'apartat de l'apoderament. Indiqui l'afirmació incorrecta:

a) La representació es pot acreditar per mitjà de qualsevol medi vàlid en Dret que deixi constància fidedigna de la seva existència. A aquests efectes, s'entén com a acreditada la representació efectuada per compareixença electrònica a la seu electrònica corresponent.

b) L'Administració General de l'Estat, les comunitats autònomes i les entitats locals han de disposar d'un registre electrònic general d'apoderaments.

c) Els registres electrònics, amb l'objecte de garantir la seguretat i preservació de la informació, han de mantenir una visibilitat limitada als dispositius de l'Administració en la qual s'ha realitzat el registre electrònic.

d) Els registres d'apoderament que es realitzin en els registres electrònics han de contenir, com a mínim, el nom i cognoms o denominació o raó social, DNI, NIF o document equivalent (en tots els casos, tant de l'apoderdant com de l'apoderat), la data d'inscripció, el període de temps pel qual s'atorga el poder i el tipus de poder segons les facultats que otorgui.

48) La Llei 40/2015 estableix i descriu els principis d'actuació i funcionament del sector públic. En el seu capítol V tracta sobre el funcionament electrònic del sector públic. Indiqueu quina de les següents és una afirmació incorrecta:

a) Les administracions públiques poden identificar-se mitjançant l'ús d'un segell electrònic basat en un certificat electrònic o qualificat que reuneixi els requisits exigits per la legislació de signatura electrònica.

b) Tots els documents utilitzats a les actuacions administratives s'han d'emmagatzemar per mitjans electrònics, excepte quan no sigui possible.

c) Es descriu la seu electrònica o portal d'internet com aquella adreça electrònica, disponible per als ciutadans a través de xarxes de telecomunicacions, amb titularitat d'una administració pública o bé d'un o diversos organismes públics o entitats de dret públic.

d) Els sistemes d'informació i comunicacions per a la recollida, emmagatzematgent, processament i gestió del cens electoral, padrons municipals i altres registres de població, dades fiscals i dades dels usuaris de sistema de salut han de situar-se dins el territori de la Unió Europea

49) El Reial Decret RD 3/2010 regula l'Esquema Nacional de Seguretat a l'àmbit de l'Administració Electrònica. Dins dels Principis Bàsics, el RD indica que la seguretat del sistema ha de contemplar els aspectes de prevenció, detecció i correcció. Indiqueu quina és l'afirmació correcta:

a) Les mesures de detecció han d'eliminar o reduir la possibilitat de que les amenaces arribin a materialitzar-se amb perjudici per al sistema.

b) Les mesures de prevenció estaran acompanyades de mesures de reacció, de manera que els incidents de seguretat es tallin a temps.

c) Les mesures de recuperació permetran la restauració de la informació i els serveis, de manera que es pugui fer front a situacions en què un incident de seguretat inhabiliti els mitjans habituals.

d) Cap de les anteriors

50) S'entén per virtualització el concepte de creació, a través de software, d'una representació virtual d'un recurs tecnològic. La virtualització aporta algunes oportunitats, com fer funcionar diversos sistemes operatius en un mateix ordinador, reduir costos d'adquisició de hardware, aprofitar millor els equips. Indiqueu quina és l'afirmació correcta en relació a la virtualització de servidors:

a) A la virtualització de servidors, també coneguda com virtualització de plataforma o virtualització de hardware, es disposa d'un software anomenat hipervisor o VMM, que crea una capa d'abstracció de maquinari de la màquina física, generant una màquina virtual.
b) La virtualització amb un hipervisor tipus 1, també denominat *hosted*, consisteix en l'execució d'un software que s'executa sobre el sistema operatiu de servidor, com una aplicació més, per oferir la funcionalitat específica.
c) La virtualització amb un hipervisor tipus 2, també anomenat nadiu o *unhosted*, consisteix en l'execució del software directament sobre el hardware del servidor. Aquest software s'instal·la directament sobre el servidor, fent les funcions tant de sistema operatiu com de virtualització.
d) Cap de les anteriors

PREGUNTES DE RESERVA:

RESERVA 1. En un sistema d'emmagatzematgent de tipus RAID 1, si es considera que N és el nombre de discos i D la capacitat de cada disc, indiqui l'afirmació que conté la fórmula correcta per calcular la capacitat disponible d'emmagatzematgent:

a) N*D
b) N*D/2
c) (N-1)*D
d) Cap de les anteriors

RESERVA 2. El Reial Decret RD 3/2010, que regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, a l'ANNEX I, determina la categoria d'un sistema en relació a la seguretat, amb diverses dimensions de la seguretat. Es defineix el nivell ALT quan es produeix un perjudici molt greu sobre les funcions de l'organització, sobre els seus actius o sobre els individus afectats. Indiqueu quina de les següents no és una afirmació certa en relació a la consideració de perjudici molt greu:

a) L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals.
b) L'incompliment material d'alguna llei o regulació, o l'incompliment formal que no tingui caràcter de subsanable.
c) Causar un perjudici greu a algun individu, de difícil o impossible reparació.
d) El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.

RESERVA 3. L'encriptació de dades és una tècnica que permet incrementar la seguretat en les transmissions de dades, de manera que els missatges apareixen codificats, amb la finalitat d'ocultar el seu contingut. Indiqueu quina és l'afirmació correcta en relació als tipus d'encriptació:

a) La criptografia simètrica utilitza una única clau per xifrar i desxifrar els missatges. Aquesta clau ha de ser coneguda prèviament per l'emissor i el receptor.
b) La criptografia asimètrica es basa en l'ús de dues claus privades per incrementar la seguretat en les transmissions.
c) La criptografia híbrida es basa en utilitzar un sistema que combini la criptografia simètrica amb la asimètrica en l'emissió de missatges, de manera que es pot triar entre utilitzar una clau pública o dues privades.

d) Cap de les anteriors.

RESERVA 4. La tendència actual en bases de dades passa per l'acumulació de grans volums de dades. En aquest sentit, indiqui quina és l'afirmació falsa.

a) El terme VLDB s'utilitza per referir-se a bases de dades que contenen taules amb un nombre especialment elevat de registres.

b) S'entén per Big Data a grans conjunts d'informació, que superen la capacitat del software convencional de bases de dades per processar dades en un temps raonable.

c) Les bases de dades relacionals proporcionen més potència, robustesa, funcionalitat i estandardització i capacitats d'escalabilitat de dades que les NoSQL, però aquestes, pel fet de no respectar les normes ACID, són més ràpides pel que fa a extracció d'informació.

d) Les bases de dades documentals són un tipus de bases de dades NoSQL que permeten emmagatzemar dades de documents utilitzant codificacions com a JSON o XML.

RESERVA 5. En relació a la reutilització d'aplicacions i transferència de tecnologies. Indiqueu quina de les següents afirmacions és incorrecta:

a) Les administracions públiques han de mantenir directoris actualitzats d'aplicacions per a la seva lliure reutilització.

b) L'Administració General de l'Estat ha de promoure la formació de personal al seu servei en la utilització de mitjans electrònics per al desenvolupament de les activitats pròpies d'aquesta administració.

c) Les administracions titulars dels drets de propietat intel·lectual d'aplicacions, desenvolupades pels seus serveis, podran ser declarades com de fonts obertes, quan es derivi una major transparència en el funcionament de l'Administració Pública. Queden exceptuades les aplicacions desenvolupades a través de contractació.

d) L'Administració General de l'Estat, a través d'un centre per a la transferència de la tecnologia, ha de mantenir un directori general d'aplicacions per a la seva reutilització, prestant assistència tècnica per a la lliure reutilització d'aplicacions.

Ajuntament d'Inca

IDENTIFICACIÓ DE L'OPOSITOR: _____

Expedient: 2808/2020 **Procediment:** Seleccions de Personal i Provisions de Llocs de treball
Assumpte: Oposició per a cobrir de manera interina una plaça de personal funcionari Cap del departament d'Informàtica.

Posin una X a la resposta que considerin correcta. No emplenar les caselles amb fons gris

Preg	a	b	c	d	Cor	Inc	Blc	Nul
1				**d**				
2			**c**					
3	**a**							
4			**c**					
5		**b**						
6		**b**						
7			**c**					
8		**b**						
9			**c**					
10	**a**							
11			**c**					
12			**c**					
13			**c**					
14			**c**					
15				**d**				
16				**d**				
17		**b**						
18				**d**				
19				**d**				
20			**c**					
21		**b**						
22				**d**				
23			**c**					
24				**d**				
25		**b**						

Preg	a	b	c	d	Cor	Inc	Blc	Nul
26	**a**							
27				**d**				
28				**d**				
29			**c**					
30	**a**							
31		**b**						
32			**c**					
33	**a**							
34				**d**				
35			**c**					
36		**b**						
37	**a**							
38		**b**						
39	**a**							
40	**a**							
41			**c**					
42			**c**					
43		**b**						
44		**b**						
45			**c**					
46				**d**				
47			**c**					
48			**c**					
49			**c**					
50	**a**							

Preguntes de reserva / Preguntas de reserva

Preg	a	b	c	d	Cor	Inc	Blc	Nul
R1		**b**						
R2		**b**						
R3	**a**							
R4			**c**					
R5			**c**					

Concepte	Total	Nota
Correctes		
Incorrectes		
Blanc		
Nul		