Osakidetza



TÉCNICO/A SUPERIOR INFORMÁTICA

PREGUNTAS

1.- ¿Qué capa del modelo OSI se relaciona con la transmisión de bits puros a través de un canal de transmisión?

a) Enlace.

b) Transporte.

c) Física.

d) Red.

2.- ¿Qué capa del modelo OSI ofrece los servicios: control del diálogo, manejo de tokens y sincronización?

a) Transporte.

b) Sesión.

c) Presentación.

d) Aplicación.

3.- ¿Qué capa del modelo OSI determina cómo se encaminan los paquetes desde el origen al destino?

a) Enlace.

b) Red.

c) Transporte.

d) Sesión.

4.- ¿En qué capa del modelo TCP/IP se define el protocolo SMTP?

a) Enlace.

b) Sesión.

c) Transporte.

d) Aplicación.

5.- ¿Cuál de los siguientes protocolos encuadrarías en la capa interred del modelo TCP/IP?

a) IP.

b) DSL.

c) Ethernet.

d) DNS.

6.- ¿Qué capa del modelo OSI se encargaría de la siguiente tarea?: El emisor divide los datos de entrada en tramas de datos y transmite las tramas en forma secuencial.

a) Transporte.

b) Red.

c) Enlace.

d) Física.

7.- ¿Cuál de los siguientes protocolos encuadrarías en la capa de transporte del modelo de referencia TCP/IP?

a) IP.

b) UDP.

c) ICMP.

d) RTP.

8.- ¿Cuál es el orden correcto de las capas del modelo de referencia OSI?

a) Física, conexión o enlace, red, transporte, presentación, sesión, aplicación.

b) Física, conexión o enlace, red, transporte, presentación, aplicación, sesión.

c) Sesión, presentación, transporte, MAC, red, física.

d) Aplicación, presentación, sesión, transporte, red, conexión o enlace, física.

9.- ¿Qué capa del modelo de referencia OSI tiene como función principal dividir los datos que recibe de la capa de red en tramas que pueden ser transmitidas por la capa física?

a) Transporte.

b) Sesión.



c) Red.

d) Conexión o enlace.

10.- ¿A qué capa del modelo de referencia OSI corresponden los protocolos Ethernet y Point-to-Point Protocol (PPP)?

a) Red.

b) Conexión o enlace.

c) Transporte.

d) Sesión.

11.- En una arquitectura de comunicaciones como OSI y TCP/IP, ¿cómo se lleva a cabo la interacción entre entidades que están en la misma capa pero en diferentes equipos?

a) Mediante una interfaz de servicios.

b) Mediante un protocolo correspondiente a la capa inmediatamente superior.

c) Mediante un protocolo correspondiente a la capa inmediatamente inferior.

d) Mediante un protocolo correspondiente a esa capa.

12.- La arquitectura de protocolos OSI tiene 7 capas, mientras que la TCP/IP tiene solo 5. ¿Qué implica esta reducción?

a) Que en la capa de transporte de TCP/IP se realizan funciones que en OSI corresponden a las capas de sesión y presentación.

b) Que en la capa de aplicación de TCP/IP se realizan funciones que en OSI corresponden a las capas de sesión y presentación.

c) Que las aplicaciones basadas en TCP/IP tienen necesariamente una funcionalidad más reducida que las basadas en OSI.

d) Que en el modelo OSI se definieron capas que en realidad no sirven para nada.

13.- En el contexto del modelo OSI, la distinción entre "servicio", "interfaz" y "protocolo" implica que:

a) El protocolo define los servicios que una capa ofrece a la capa superior mediante su interfaz.

b) El servicio es la implementación concreta de las reglas de comunicación entre entidades homólogas.



c) La interfaz especifica cómo accede la capa superior a los servicios de la capa inferior, mientras que el protocolo define las reglas de comunicación entre entidades de la misma capa.

d) Servicio, interfaz y protocolo son términos equivalentes dentro de una arquitectura por capas.

14.- Las unidades de datos que se intercambian en el nivel 2 (capa de conexión o enlace de datos) se denominan:

a) Mensajes.

b) Datagramas.

c) Celdas.

d) Tramas.

15.- Para identificar unívocamente un servicio en un entorno de comunicaciones TCP/IP se requiere:

a) Una dirección IP, un protocolo (TCP o UDP) y un puerto.

b) Solo es necesaria una dirección IP.

c) Solo es necesario un puerto.

d) Solo es necesario indicar un protocolo (TCP o UDP).

16.- El modelo de referencia OSI para la interconexión de sistemas abiertos está estructurado en:

a) Un número variable de capas.

b) 5 capas.

c) 7 capas.

d) 9 capas.

17.- ¿Qué función realiza la capa de transporte en el modelo OSI?

a) Encaminar paquetes entre redes.

b) Controlar el acceso al medio físico.

c) Proporcionar comunicación extremo a extremo fiable.

d) Convertir señales analógicas en digitales.



18.- En el modelo OSI, la arquitectura por niveles tiene como objetivo principal:

a) Reducir la cantidad de protocolos necesarios en una red.

b) Permitir que cada capa pueda modificarse sin afectar necesariamente a las demás.

c) Garantizar que todas las redes utilicen los mismos medios físicos.

d) Aumentar la velocidad de transmisión de datos.

19.- En el proceso de encapsulación descrito en TCP/IP, el orden correcto al enviar datos desde una aplicación es:

a) Datos - Segmentos - Paquetes- Tramas

b) Datos - Segmentos - Tramas - Paquetes

c) Datos - Tramas - Segmentos - Paquetes

d) Segmentos - Datos - Tramas - Paquetes

20.- En el modelo OSI, la comunicación entre capas homólogas es:

a) Física y directa.

b) Lógica, mientras que la transmisión real se realiza a través de las capas inferiores.

c) Exclusiva del nivel físico.

d) Posible únicamente en redes locales.

21.- Según el modelo OSI, ¿cuál es la función principal del nivel de transporte?

a) Encaminamiento entre redes.

b) Control del acceso al medio físico.

c) Entrega extremo a extremo y control de flujo.

d) Traducción de formatos de datos.

22.- En la comparación estructural entre OSI y TCP/IP, una diferencia clave es que:

a) TCP/IP separa estrictamente sesión y presentación como capas independientes.

b) OSI no contempla el nivel de transporte.

c) TCP/IP agrupa en su capa de aplicación funciones que en OSI pertenecen a varias capas superiores.

d) OSI no define servicios.



23.- En el modelo OSI, el concepto de "servicio" hace referencia a:

a) Las reglas de comunicación entre entidades homólogas.

b) Lo que una capa ofrece a la capa inmediatamente superior.

c) El formato físico de las señales transmitidas.

d) El medio de transmisión utilizado.

24.- En TCP/IP, el protocolo IP pertenece al nivel que en el modelo OSI corresponde principalmente a:

a) Presentación.

b) Transporte.

c) Red.

d) Enlace de datos.

25.- En una LAN, ¿en qué tipo de transmisiones se utiliza el código de línea 4B5B?

a) Transmisiones en banda ancha 802.11a.

b) Transmisiones en banda ancha 802.11g.

c) Transmisiones en banda base Ethernet 100Base-T.

d) Transmisiones en banda base Ethernet 1000Base-T.

26.- ¿En qué topología de redes LAN cableadas tiene sentido la utilización de un switch?

a) Bus.

b) Árbol.

c) Anillo.

d) Estrella.

27.- ¿Qué medio de transmisión está permitido si se emplea el esquema de banda base 1000Base-SX?

a) Par trenzado UTP de categoría 5.

b) Par trenzado STP especial.

c) Fibra óptica monomodo.

d) Fibra óptica multimodo.

28.- ¿En qué variante de la norma IEEE 802.11 se usa MIMO (Multiple-Input Multiple-Output)?

a) 802.11a.

b) 802.11b.

c) 802.11g.

d) 802.11n.

29.- ¿Qué dos protocolos se definen en el denominado MAC inalámbrico de principio distribuido (DFWMAC – Distributed Foundation Wireless MAC) para realizar contención y sondeo a fin de posibilitar un acceso distribuido con un control central opcional?

a) TCP y IP.

b) DCF y PCF.

c) BSS y AP.

d) CSMA y ARP.

30.- ¿Cuál de estas técnicas sirve para corregir errores ocurridos durante la transmisión de una trama?

a) MAC.

b) Bit de paridad simple.

c) CRC.

d) FEC.

31.- ¿Qué campos contiene una trama 802.3?

a) Dirección IP origen, dirección IP destino, protocolo, datos, checksum.

b) Dirección MAC destino, dirección MAC origen, puerto destino, puerto origen, datos, CRC.

c) Dirección MAC destino, dirección MAC origen, longitud, datos, CRC.

d) Dirección MAC destino, dirección MAC origen, protocolo, datos, longitud de trama, checksum, CRC.

32.- ¿Cuál de estas afirmaciones acerca de las direcciones MAC es correcta?

a) Son identificadores únicos de 48 bits asignados por el fabricante.

b) Están formadas por cuatro octetos.

c) Solo se usan en tramas Ethernet.

d) Aportan información geográfica sobre la ubicación de un equipo.

33.- ¿Qué ofrece el protocolo de transporte UDP?

a) Intercambio de bytes, fiable, orientado a conexión.

b) Intercambio de mensajes, fiable, no orientado a conexión.

c) Intercambio de mensajes, no fiable, orientado a conexión.

d) Intercambio de mensajes, no fiable, no orientado a conexión.

34.- La familia de estándares IEEE 802.11 corresponde a:

a) Protocolos de comunicaciones Bluetooth.

b) Estándares de cables Ethernet.

c) Estándares de seguridad.

d) Protocolos de redes locales inalámbricas.

35.- ¿Cuál de estos protocolos ofrece un servicio de intercambio de paquetes (datagramas) entre dos equipos conectados a Internet?

a) TCP.

b) Ethernet.

c) SSL.

d) IP.

36.- En una red Ethernet capturamos una trama con información correspondiente a HTTP. ¿Cuál de estas afirmaciones es correcta?

a) Los datos HTTP van directamente en la parte de datos de la trama Ethernet, sin cabeceras adicionales.

b) Los datos HTTP van dentro de un segmento TCP, que a su vez va dentro de un datagrama IP, que a su vez va dentro de la trama Ethernet.



c) Los datos HTTP van dentro de un datagrama UDP, que a su vez va dentro de un datagrama IP, que a su vez va dentro de la trama Ethernet.

d) Los datos HTTP van dentro de un datagrama IP, que a su vez va dentro de un segmento TCP, que a su vez va dentro de la trama Ethernet.

37.- ¿Sobre qué medios físicos pueden funcionar las redes Ethernet (802.3)?

a) Todas las demás respuestas son correctas.

b) Par trenzado.

c) Fibra óptica.

d) Cable coaxial.

38.- Las tecnologías de transmisión Frame Relay y ATM se engloban dentro de:

a) Redes de conmutación de paquetes con servicio de datagramas.

b) Redes de conmutación de paquetes con servicio de circuitos virtuales.

c) Redes de conmutación de mensajes con servicio de datagramas.

d) Redes de conmutación de circuitos.

39.- Los métodos de conmutación más importantes en redes de comunicación de datos no incluyen:

a) Conmutación de circuitos.

b) Conmutación de paquetes.

c) Conmutación de mensajes.

d) Conmutación de frecuencias.

40.- ¿Qué característica distingue a una red LAN frente a una WAN?

a) Utiliza exclusivamente fibra óptica.

b) Cubre una extensión geográfica limitada.

c) Funciona únicamente con direccionamiento IP público.

d) No utiliza protocolos de enlace de datos.

41.- En una red Ethernet tradicional con CSMA/CD, una colisión se detecta cuando:

a) Dos equipos transmiten simultáneamente en el mismo medio compartido.

b) El switch rechaza un paquete.

c) Se supera el tamaño máximo de trama.

d) El CRC es incorrecto.

42.- En Ethernet conmutada en modo full-duplex:

a) Siguen produciéndose colisiones.

b) Se utiliza paso de testigo.

c) No se producen colisiones.

d) Se necesita un hub.

43.- ¿Cuál es la unidad de datos en el nivel de enlace de datos en Ethernet?

a) Segmento.

b) Datagram.

c) Trama.

d) Celda.

44.- En la conmutación de paquetes orientada a circuitos virtuales:

a) No existe establecimiento previo de conexión lógica.

b) Todos los paquetes siguen el mismo camino lógico.

c) No se utiliza direccionamiento.

d) Se basa en transmisión analógica.

45.- El protocolo TCP se caracteriza por ser:

a) No orientado a conexión y no fiable.

b) Orientado a conexión y fiable.

c) No orientado a conexión y fiable.

d) Orientado a conexión y no fiable.

46.- En una red Ethernet 802.3, el campo FCS (Frame Check Sequence) de la trama se utiliza para:

a) Identificar el protocolo de nivel superior.

b) Detectar errores en la transmisión.

c) Asignar prioridad al tráfico.

d) Indicar la longitud del segmento TCP.

47.- En una red IP, el campo TTL (Time To Live) de un paquete se utiliza para:

a) Medir el tiempo exacto de transmisión del paquete.

b) Limitar el número de saltos que puede atravesar un paquete.

c) Indicar la prioridad de la trama Ethernet.

d) Establecer la conexión TCP.

48.- ¿Cuál de los siguientes protocolos se utiliza típicamente en una red LAN Ethernet para el acceso al medio compartido?

a) CSMA/CD.

b) ARP.

c) OSPF.

d) TCP.

49.- ¿Cuál de las siguientes características puede aplicarse en la conmutación de paquetes mediante datagramas?

a) Previo a la transmisión de los datos, se establece una conexión a fin de elegir la ruta origen-destino a seguir por el mensaje, lo que implica la reserva de los recursos necesarios para posibilitar la comunicación.

b) Durante el proceso de transmisión de los paquetes, es necesario el envío previo de un paquete header conteniendo, entre otras, información relativa al destino al que van dirigidos el resto de paquetes.

c) Para evitar las demoras características de la conmutación de circuitos, la conmutación de paquetes se caracteriza porque cada nodo intermedio ni almacena temporalmente ni procesa cada paquete antes de transmitirlo, sino que efectúa su transmisión según lo recibe.

d) Cada paquete se transmite independientemente del resto, de forma que pueden seguir caminos distintos y, en consecuencia, recibirse de forma desordenada en el receptor.

50.- ¿Cuál de las siguientes características de los dispositivos de interconexión es correcta?

a) Repetidor (repeater): funciona a partir de la capa de red y permite la interconexión de sistemas cuya funcionalidad difiere a nivel 3.

b) Puente (bridge): opera hasta la capa de enlace a fin de posibilitar la interconexión de redes LAN de naturaleza diferente; por ejemplo, una red WLAN con una Ethernet.

c) Pasarela (gateway): trabaja en la capa física y es un mero amplificador de señal que solventa el problema de atenuación de la señal en su propagación hacia el destino.

d) Dispositivo de capa superior: trabaja por debajo de la capa de red para posibilitar la comunicación entre protocolos de la capa correspondiente.

51.- ¿Qué información utiliza principalmente un router para decidir por qué interfaz debe reenviar un paquete IP recibido?

a) La dirección MAC de destino contenida en la trama Ethernet.

b) La dirección IP de destino y su tabla de encaminamiento.

c) El número de puerto TCP o UDP.

d) El campo TTL del paquete.

52.- ¿Cuáles son las capas OSI en las que opera un router para la interconexión de dos sistemas?

a) Física, enlace y red.

b) Enlace, red y transporte.

c) Red, transporte y sesión.

d) Física, red y transporte.

53.- ¿Cuál de los siguientes es un tipo de VLAN válido?

a) VLAN de nivel 1: se asignan los hosts a una VLAN en función de la dirección MAC de aquellos.

b) VLAN de nivel 2 por dirección MAC: la VLAN viene determinada por el contenido del campo de tipo de protocolo de la trama MAC.

c) VLAN de nivel 3 por direcciones de subred: en este caso son los paquetes y no las estaciones finales quienes pertenecen a una VLAN u otra en función de su cabecera de nivel 3.



d) VLAN de niveles superiores: los miembros de la LAN se diferencian por el puerto al que están conectados al conmutador o medio físico que constituye la red.

54.- ¿Qué efecto tiene la incorporación de un router entre dos redes LAN distintas?

a) Se mantiene un único dominio de colisión y un único dominio de difusión.

b) Se separan los dominios de colisión, pero no los de difusión.

c) Se separan tanto los dominios de colisión como los de difusión.

d) Se unifican las direcciones MAC de ambas redes.

55.- ¿Cuál de estos dispositivos sirve para interconectar a nivel 3 (IP) dos o más LAN diferentes?

a) Un puente.

b) Un router o encaminador.

c) Un IDS.

d) Un punto de acceso Wi-Fi.

56.- Un ordenador A tiene dirección IP 192.168.2.12/24 y la pasarela por omisión P en su LAN es 192.168.2.1. A envía un datagrama IP al ordenador B, que tiene dirección IP 192.168.3.18. ¿Cuál de estas afirmaciones es cierta?

a) A usa ARP para averiguar la dirección física de su pasarela P y luego envía a P por la LAN una trama que contiene el datagrama.

b) A usa ARP para averiguar las direcciones físicas de B y de P y luego envía a P el datagrama, con la orden de que lo retransmita hacia B.

c) A no puede enviar datagramas IP a B porque están en LAN diferentes.

d) A usa ARP para averiguar la dirección física de B y luego envía a B por la LAN una trama que contiene el datagrama.

57.- ICMP es:

a) Un mecanismo utilizado por los routers para la notificación y el control de la congestión en redes IP.

b) Un protocolo de cifrado de paquetes que funciona sobre IP.

c) Un mecanismo utilizado por los hosts y routers para enviar al emisor notificaciones sobre problemas encontrados al procesar datagramas.

d) Un protocolo de encaminamiento para redes IP.

58.- ¿Qué campo de una trama Ethernet se utiliza para detectar errores?

a) Dirección MAC origen.

b) Longitud.

c) FCS (Frame Check Sequence).

d) Tipo.

59.- ¿Cuál de estas definiciones corresponde a un sistema autónomo (AS) de Internet?

a) Un AS es un grupo de redes IP que poseen una política de rutas propia e independiente. Se identifica con un número y se conecta a otros AS mediante routers y el protocolo BGP.

b) Un AS es un conjunto de equipos que comparten la misma dirección de subred y que están administrados por un organismo nacional de asignación de direcciones.

c) Un AS es una red que usa los mismos protocolos de Internet (TCP/IP) pero no está conectada a ella.

d) Un AS es una red doméstica cuyos equipos comparten una única dirección IP mediante la técnica NAT.

60.- ¿Cuál de estos protocolos no es un IGP (Interior Gateway Protocol), es decir, no realiza encaminamiento intradominio?

a) OSPF.

b) RIP.

c) IGRP.

d) BGP.

61.- ¿Cuál de estas afirmaciones sobre las direcciones IPv4 es cierta?

a) Tienen una longitud de 128 bits.

b) Se representan como seis parejas de dígitos hexadecimales.

c) Se estructuran en una parte dirección de red y otra dirección de host, de longitudes fijas.

d) Se estructuran en una parte dirección de red y otra dirección de host, de longitudes variables.



62.- Usando NAT, un ISP puede:

a) Traducir nombres de máquinas a sus correspondientes direcciones IP.

b) Ahorrar direcciones IP públicas.

c) Traducir direcciones IP a direcciones MAC.

d) Traducir direcciones IPv4 a direcciones IPv6 y viceversa.

63.- ¿Cuál de estas afirmaciones sobre las direcciones físicas (MAC) y lógicas (IPv4) es falsa?

a) Una interfaz conectada a una red tiene tanto una dirección IP como una dirección MAC.

b) La dirección MAC de una interfaz se averigua a partir de su dirección IP ejecutando ARP.

c) La dirección MAC de una interfaz se averigua haciendo un cálculo a partir de la dirección IP.

d) Las direcciones MAC se usan en la capa 2 (enlace de datos).

64.- ¿Cuál de los siguientes es un protocolo de enrutamiento?

a) OSPF.

b) DHCP.

c) DNS.

d) IPSec.

65.- ¿Por qué Internet utiliza enrutamiento jerárquico mediante sistemas autónomos?

a) Para reducir el número de cables.

b) Para evitar el uso de direcciones IP.

c) Para mejorar la escalabilidad del enrutamiento.

d) Para eliminar routers intermedios.

66.- ¿Cuál de estos tipos de direcciones no existen en IPv6?

a) Unicast.

b) Multicast.

c) Anycast.

d) Broadcast.

67.- ¿Cuál es la principal diferencia funcional entre un bridge y un router?

a) El bridge utiliza direcciones IP y el router direcciones MAC.

b) El bridge opera en la capa de enlace y el router en la capa de red.

c) El bridge permite interconectar redes WAN y el router solo LAN.

d) El router no necesita tablas de encaminamiento.

68.- En el encaminamiento basado en vector distancia, cada router:

a) Mantiene una visión completa de la topología de la red.

b) Comparte con sus vecinos el estado completo de sus enlaces.

c) Envía periódicamente su tabla de distancias a los routers vecinos.

d) Calcula rutas únicamente mediante el algoritmo de Dijkstra.

69.- En el direccionamiento IPv4 moderno (CIDR), ¿qué característica permite una mayor flexibilidad en la asignación de direcciones IP?

a) El uso exclusivo de clases A, B y C.

b) La división fija entre red y host.

c) La longitud variable del prefijo de red.

d) La utilización de direcciones MAC en lugar de IP.

70.- En una arquitectura TCP/IP, el protocolo ARP se utiliza cuando:

a) Un router necesita calcular la mejor ruta.

b) Un host necesita conocer la dirección MAC correspondiente a una dirección IP dentro de su red local.

c) Se establece una conexión TCP.

d) Se produce un error en la entrega de un datagrama.

71.- ¿Cuál de las siguientes direcciones IPv6 se utiliza para identificar a un conjunto de interfaces, enviando el paquete a la más cercana según el routing?

a) Unicast.

b) Multicast.

c) Anycast.



d) Broadcast.

72.- En el algoritmo de Dijkstra utilizado en protocolos de estado de enlace, el objetivo es:

a) Determinar el número máximo de saltos permitidos.

b) Construir un árbol de coste mínimo desde el router origen hacia el resto de nodos.

c) Traducir direcciones IP en direcciones MAC.

d) Asignar direcciones IP dinámicamente.

73.- En el diagrama Entidad/Relación (E/R), los conjuntos de entidades se representan mediante:

a) Rectángulos.

b) Rombos.

c) Elipses u óvalos.

d) Cuadrados.

74.- En el modelo relacional, los atributos principales tienen la restricción:

a) Primary Key, Unique, Not Null y Foreign key.

b) Primary Key, Not Null y Foreign key.

c) Primary Key, Unique, Not Null.

d) Unique, Not Null y Foreign key.

75.- En el modelo relacional, la operación del álgebra relacional que hace casar las tuplas, cuyos valores coinciden para los atributos que son comunes a ambas relaciones, se denomina:

a) Intersección de conjuntos.

b) Reunión natural.

c) División.

d) Producto cartesiano.



76.- En el diseño de un modelo Entidad/Relación (E/R), ¿cuál de las siguientes afirmaciones define mejor lo que es una clave candidata?

a) Es un atributo o conjunto mínimo de atributos que identifica de forma única a cada instancia de una entidad.

b) Es cualquier atributo que forma parte de la clave primaria de una entidad.

c) Es el atributo que el diseñador elige obligatoriamente para relacionar una entidad con otra (clave foránea).

d) Es un identificador que puede contener valores nulos siempre que no se repitan.

77.- ¿Cuál de las siguientes no es una base de datos relacional?

a) MySQL.

b) MariaDB.

c) MongoDB.

d) Oracle.

78.- En un modelo Entidad/Relación (E/R), si se desea almacenar la o las tarjetas bancarias de un cliente, se añadirá al tipo de entidad "Cliente" el atributo:

a) Principal "tarjeta".

b) Compuesto "tarjeta".

c) Multivaluado "tarjeta".

d) Simple "tarjeta".

79.- En el contexto del modelado de una base de datos relacional, se desea registrar las asignaturas que una facultad recomienda cursar con anterioridad para matricularse en una asignatura dada. Una asignatura puede tener N asignaturas recomendadas y una misma asignatura puede estar en la lista de recomendadas de varias asignaturas distintas. ¿cómo se denomina ese tipo de interrelación?

a) Reflexiva o recursiva.

b) Inflexiva.

c) Inclusiva.

d) Relativa.



80.- En el modelo Entidad/Relación(E/R), ¿Cómo se llama la entidad que no puede ser identificada de forma única por sus propios atributos?

a) Anónima.

b) Secundaria.

c) Huérfana.

d) Débil.

81.- ¿Quién introdujo el modelo Entidad/Relación (E/R)?

a) Alan Turing.

b) Peter Chen.

c) Larry Ellison.

d) Michael Stonebraker.

82.- ¿Cuál es el propósito del modelo Entidad/Relacion (E/R)?

a) Crear aplicaciones de software.

b) Optimizar la eficiencia de las bases de datos.

c) Representar y definir datos independientemente de la tecnología utilizada.

d) Diseñar interfaces de usuario.

83.- ¿Cuáles son las dos clases de entidades existentes en el modelo Entidad/Relación (E/R)?

a) Simples y compuestas.

b) Regulares y débiles.

c) Temporales y espaciales.

d) Primarias y secundarias.

84.- En el contexto del modelo Entidad/Relación (E/R) ¿qué es la cardinalidad de una relación?

a) El número de entidades que participan en la relación.

b) La cantidad máxima de atributos de las entidades que participan en la relación.

c) El número de ocurrencias en cada tipo de entidad que participa en la relación.

d) La cantidad de atributos que componen la clave primaria de una entidad fuerte.



85.- En un modelo relacional, ¿qué propiedad garantiza que cada valor de un atributo pertenece al dominio definido?

a) Integridad de entidad.

b) Integridad de dominio.

c) Integridad referencial.

d) Integridad de clave.

86.- ¿Cuál de las siguientes formas normales elimina dependencias parciales respecto a una clave compuesta?

a) 1.

b) 2.

c) 3.

d) 4.

87.- ¿Qué significa la propiedad 'D' en ACID?

a) Distribución.

b) Durabilidad.

c) Determinismo.

d) Dependencia.

88.- En el modelo Entidad/Relación (E/R), una entidad débil se identifica mediante:

a) Una clave candidata propia.

b) Una clave alternativa.

c) Una clave parcial y la clave de su entidad fuerte.

d) Una restricción CHECK.

89.- ¿Qué operación del álgebra relacional corresponde a seleccionar filas que cumplen un predicado?

a) Producto cartesiano (×).

b) Proyección (π).



c) Unión (∪).

d) Selección (σ).

90.- ¿Cuál es el objetivo de la minería de datos?

a) Establecer las estructuras relacionales necesarias para las grandes bases de datos.

b) Cruzar los datos con distintos niveles de agregación en bases de datos multidimensionales.

c) Buscar reglas y estructuras a partir de los datos almacenados en almacenes de datos.

d) Recolectar masivamente los datos y procesarlos en tiempo real.

91.- ¿Cuál es el objetivo principal del proceso de normalización en el diseño de bases de datos relacionales?

a) Aumentar la velocidad de las consultas (performance) y la eficiencia del hardware.

b) Asegurar que la base de datos sea compatible con múltiples sistemas operativos.

c) Eliminar la redundancia de los datos y prevenir anomalías de actualización, inserción y borrado.

d) Definir la interfaz de usuario para interactuar con los datos almacenados.

92.- En la notación de cardinalidad min-max (m,M) utilizada en el modelo E/R, ¿Qué representa el valor 'm'?

a) El número máximo de atributos en una entidad.

b) El número mínimo de ocurrencias de la entidad que participan en la relación.

c) El grado máximo de la relación (binaria, ternaria, etc.).

d) El número total de tuplas en la tabla resultante.

93.- ¿Qué término describe un atributo en una tabla (Entidad A) cuyos valores deben coincidir con los valores de la clave primaria de otra tabla (Entidad B)?

a) Clave primaria.

b) Clave candidata.

c) Clave foránea.

d) Clave principal.



94.- Cuál de los siguientes modelos de bases de datos es considerado el precursor histórico del modelo relacional, organizando los datos en una estructura de árbol?

a) Modelo de red.

b) Modelo jerárquico.

c) Modelo orientado a objetos.

d) Modelo NoSQL.

95.- ¿Qué es una transacción en una base de datos?

a) El proceso de mapear un modelo Entidad/Relación a un esquema relacional.

b) Una operación que garantiza la serializabilidad de múltiples accesos concurrentes a una misma tabla.

c) Un conjunto de operaciones que se gestionan como una sola unidad atómica para preservar la consistencia del sistema.

d) Una función del SGBD para definir la estructura física del almacenamiento de los datos.

96.- ¿Cuál es la diferencia fundamental entre una clave primaria y una clave candidata?

a) Una tabla puede tener varias claves primarias, pero solo una clave candidata.

b) Las claves candidatas pueden tener valores duplicados, mientras que la clave primaria debe ser única.

c) La clave primaria es la clave candidata elegida para identificar de forma única los registros, y no puede aceptar valores nulos.

d) No existe diferencia técnica; ambos términos son sinónimos y se usan indistintamente según el gestor de base de datos.

97.- ¿Cuál de los siguientes módulos de SAP permite realizar actividades relacionadas con el cumplimiento de las regulaciones financieras gubernamentales?

a) Finanzas (SAP ERP Financials).

b) Recursos humanos (SAP ERP Human Capital Management).

c) Servicios corporativos (SAP ERP Corporate Services).

d) Gestión de la experiencia de canal web (SAP Web Channel Experience Management).

98.- ¿Cuál de las siguientes opciones refleja una de las ventajas clave de las innovaciones de ventas en SAP S/4HANA?

a) Las comprobaciones de disponibilidad (ATP) pasan a ejecutarse únicamente mediante procesos batch nocturnos.

b) Las liquidaciones de contratos se desactivan para simplificar la gestión de precios.

c) Toda la gestión del cumplimiento de pedidos se centraliza en tiempo real mediante el *Sales Order Fulfillment Cockpit*.

d) Los estados de pedidos se almacenan en múltiples tablas agregadas para acelerar el reporting.

99.- ¿Qué aplicación SAP permite llevar a cabo la monitorización, administración y control de proyectos (desde el inicio hasta la implementación) dentro de una organización?

a) Planificación de recursos empresariales (SAP Enterprise Resource Planning).

b) Gestión de relaciones con los clientes (SAP Customer Relationship Management).

c) Gestión de relaciones con los proveedores (SAP Supplier Relationship Management).

d) Gestión del portfolio y proyecto (SAP Portfolio and Project Management).

100.- ¿Cuál de las siguientes afirmaciones es falsa respecto a SAP HANA?

a) SAP HANA es un sistema gestor de bases de datos relacionales.

b) SAP HANA opera completamente desde la memoria del dispositivo.

c) SAP HANA es una herramienta de análisis.

d) Por el momento las soluciones basadas en NetWeaver NO pueden utilizar SAP HANA como base de datos.

101.- ¿Cuál de las siguientes afirmaciones es falsa respecto a SAP HANA y la tecnología que utiliza?

a) SAP HANA se basa en un almacenamiento basado en columnas, que permite alcanzar mayor rapidez en el acceso a datos en memoria, a la vez que disminuye los requisitos de uso de memoria.

b) Dado que SAP HANA funciona manipulando datos almacenados en la memoria del dispositivo, necesita una máquina con al menos 1TB de memoria para poder funcionar.

c) La portabilidad de aplicaciones web basadas en SQL Server a SAP HANA es sencilla, precisando en muchos casos únicamente la actualización de la librería ODBC/JDBC de SQL Server a SAP HANA.



d) SAP HANA incluye un servidor propio de aplicaciones, SAP HANA XS, que utiliza Server-side JavaScript (XSJS) como lenguaje principal.

102.- ¿Qué sistema gestor de bases de datos está soportado por SAP S/4HANA?

a) Solamente SAP HANA.

b) Solamente Oracle.

c) Solamente PostgreSQL.

d) Cualquiera de los tres citados.

103.- En SAP S/4HANA, ¿Cómo se denomina el software que actúa como punto de acceso a los sistemas SAP a través de conexiones HTTP/S?

a) SAP Web Dispatcher.

b) SAP Fiori.

c) SAP Gateway.

d) Application Engine.

104.- En SAP S/4HANA, ¿qué componente proporciona la interfaz de usuario basada en aplicaciones?

a) SAP Fiori.

b) SAP Solution Manager.

c) SAProuter.

d) SAP NetWeaver Gateway.

105.- ¿Qué protocolo usa SAP Gateway para permitir consumir datos del sistema SAP S4/HANA?

a) ODBC.

b) OData.

c) ADO.NET.

d) JDBC.

106.- ¿Cuál es el tipo de sistema gestor base de datos nativo de SAP S/4HANA?

a) Documental, in-memory.



b) Documental, out-memory.

c) Relacional, in-memory.

d) Relacional, out-memory.

107.- ¿Qué es principalmente SAP S/4HANA?

a) Un sistema de gestión de bases de datos.

b) Una plataforma de desarrollo de aplicaciones móviles.

c) Un software de planificación de recursos empresariales.

d) Una herramienta de gestión de relaciones con los clientes.

108.- ¿Cuál de las siguientes NO es una opción de despliegue de SAP S/4HANA?

a) On-premise.

b) Public Cloud.

c) Private Cloud.

d) Private CRM.

109.- ¿Cuál es la función de Fiori Launchpad en SAP S/4HANA?

a) Gestionar las consultas a la base de datos.

b) Proporcionar un único punto de entrada a las aplicaciones SAP.

c) Automatizar procesos de negocio.

d) Generar informes financieros.

110.- ¿Qué característica distingue a SAP HANA frente a bases de datos tradicionales?

a) No soporta transacciones.

b) Solo soporta NoSQL.

c) Soporta almacenamiento orientado a objetos.

d) Soporta almacenamiento orientado a columnas.

111.- ¿Cuál es el propósito principal de SAP Vora dentro del ecosistema de análisis de datos en SAP S/4HANA?

a) Sustituir a SAP HANA como base de datos in-memory principal.



b) Actuar como repositorio de datos maestros central para S/4HANA.

c) Proporcionar capacidades de análisis sobre big data integrándose con Hadoop y Spark.

d) Servir como motor de transacciones OLTP para procesos críticos.

112.- ¿Qué significa CDS en el contexto de SAP S/4HANA?

a) Common Data Schema.

b) Central Directory System.

c) Cloud Deployment Service.

d) Core Data Services.

113.- ¿Cuál de las siguientes opciones describe correctamente el proceso de *HANAtization* durante una conversión a SAP S/4HANA?

a) Los ajustes obligatorios necesarios para ejecutar el código ABAP existente en una base de datos SAP HANA.

b) Reescribir completamente el código ABAP para eliminar todas las sentencias SQL.

c) Reemplazar todas las sentencias SELECT por llamadas RFC.

d) Sustituir el kernel de ABAP por un motor de ejecución basado únicamente en SAP S/4HANA.

114.- ¿Qué tecnología se usa en SAP Fiori para construir la mayoría de interfaces modernas?

a) PowerBuilder.

b) VSCode.

c) SAPUI5 (UI5).

d) VBScript.

115.- En S/4HANA, el concepto 'embedded analytics' se refiere a:

a) Analítica exportando a un Data Warehouse (DWS) externo.

b) Analítica en tiempo real sobre datos transaccionales.

c) Uso exclusivo de OLAP MOLAP.

d) Analítica offline.



116.- ¿Qué rol tiene ABAP en el ecosistema S/4HANA?

a) Desarrollo de interfaces gráficas.

b) Administración de red.

c) Cifrado.

d) Gestión de extensiones y lógica de negocio.

117.- ¿Cuál es una opción recomendada para extender S/4HANA minimizando modificaciones al core?

a) Extensibilidad in-app y side-by-side.

b) Modificar tablas estándar directamente.

c) Eliminar controles de autorización.

d) Desactivar actualizaciones.

118.- ¿Qué simplificación del modelo de datos ofrece SAP S/4HANA en el área financiera?

a) Mantener múltiples tablas históricas y de agregación para mayor precisión.

b) Eliminar el libro mayor general y reemplazarlo por vistas virtuales.

c) Unificar FI, CO, AA, ML y CO-PA en una tabla única llamada Universal Journal (ACDOCA).

d) Utilizar tablas duplicadas para versiones alternativas del mismo asiento.

119.- ¿Cuál de las siguientes opciones describe correctamente el conjunto completo de layers que conforman la arquitectura de Embedded Analytics en SAP S/4HANA?

a) Persistence Layer, BW Layer, InfoCube Layer, Visualization Layer.

b) Visualization Layer, ECC OLAP Layer, Aggregate Tables Layer, Data Aging Layer.

c) Visualization Layer, Analytics Layer, Access Layer, Virtualization/Modeling Layer, Persistence Layer.

d) Planning Layer, ETL Layer, Staging Layer, Semantic Layer.

120.- ¿Cuál de las siguientes afirmaciones describe correctamente el papel de SAP Leonardo dentro del ecosistema de SAP S/4HANA?

a) SAP Leonardo sustituye completamente al motor transaccional de SAP S/4HANA.

b) SAP Leonardo reemplaza a SAP HANA como base de datos in-memory.

c) SAP Leonardo es un módulo obligatorio para ejecutar procesos financieros centrales.

d) SAP Leonardo proporciona servicios de machine learning, IoT y big data que amplían las capacidades analíticas de SAP S/4HANA.

121.- En la metodología SCRUM, ¿Cuál de los siguientes roles busca aplicar las mejores prácticas y mejorar el trabajo en equipo?

a) Product owner.

b) Scrum master.

c) *Stakeholders.*

d) Coach.

122.- En la metodología SCRUM, ¿Qué sentencia es errónea?

a) La daily meeting debe ser una reunión breve.

b) La función principal del coach es formar, dirigir y aconsejar al SCRUM Team.

c) La review meeting se activa al concluir el Product Backlog.

d) La velocidad de un sprint se mide en Story Points.

123.- ¿Qué se entiende por épica en la metodología SCRUM?

a) Es un repositorio que recoge todo aquello que impide alcanzar los objetivos del proyecto.

b) La definición en lenguaje del negocio que hace el Product Owner de los requisitos del trabajo.

c) Un trabajo concreto, idealmente realizado por una persona dedicando entre medio día y tres días.

d) Agrupaciones de historias de usuario que definen grandes bloques operativos dentro de un proyecto.

124.- En la metodología SCRUM, ¿Cúal de las siguientes herramientas representa la evolución del trabajo durante un sprint?

a) *Time Sprint.*

b) *Time Boxing.*

c) *Burn-down chart.*

d) *Spring Planning.*

125.- En la metodología SCRUM, la lista de trabajos y tareas que van a desarrollarse en el transcurso del proyecto se conoce como:

a) *Product Backlog.*

b) *Planning Poker.*

c) *Sprint Planning.*

d) *Sprint Backlog.*

126.- En SCRUM, ¿Qué criterio se sigue para ordenarse los elementos primero?

a) Los que más riesgo impliquen.

b) Los más complejos de implementar, para reducir el riesgo.

c) Los que maximizan la entrega de valor.

d) Los elementos que menos riesgo impliquen.

127.- En SCRUM, ¿Cuál es la responsabilidad del rol Tester?

a) Crear escenarios y casos de test.

b) Encontrar errores/bugs en el producto.

c) Automatizar los tests.

d) En SCRUM no existe el rol Tester.

128.- En SCRUM, ¿Quién es el responsable de medir el rendimiento del proyecto?

a) El Equipo Scrum (Scrum Team).

b) El Gestor de Entregas (Delivery Manager).

c) El Líder del Proyecto (Scrum Master).



d) El Propietario del Producto (Product Owner).

129.- En SCRUM, ¿Qué muestra un gráfico BurnDown?

a) El progreso del proyecto.

b) La capacidad de los miembros del equipo.

c) Cantidad de trabajo restante con respecto al tiempo.

d) La velocidad general (en términos ágiles) del equipo.

130.- En SCRUM, ¿Qué se hace durante una reunión de revisión del Sprint (Sprint review)?

a) Discutir los problemas técnicos que se han encontrado durante el Sprint.

b) Analizar el progreso llevado a cabo respecto a los Objetivos del Sprint.

c) Presentar las tareas completadas a las partes interesadas (stakeholders).

d) El equipo discute las mejoras que se pueden aplicar para los próximos Sprints.

131.- ¿Qué es la metodología Agile?

a) Un enfoque estricto y prescriptivo de la gestión de proyectos.

b) Un enfoque flexible e iterativo de la gestión de proyectos.

c) Un enfoque lineal y secuencial de la gestión de proyectos.

d) Una metodología centrada únicamente en la documentación.

132.- ¿Cuáles son los roles que intervienen en SCRUM?

a) Scrum Master, Product Owner, Project Manager.

b) Scrum Master, Developer, Project Manager.

c) Scrum Master, Product Owner, Developer.

d) Scrum Master, Product Owner, Stakeholder.

133.- ¿Cuál de las siguientes preguntas NO es una de las tres que se formulan durante la reunión diaria de Scrum?

a) ¿Qué conseguí ayer?.

b) ¿Qué voy a hacer hoy?.

c) ¿Hay algún impedimento en mi camino?.

d) ¿Cómo podemos mejorar el producto?.

134.- ¿Cuál de las siguientes actividades de SCRUM tiene como objetivo permitir que el equipo inspeccione y adapte el proceso de desarrollo?

a) Reunión diaria de Scrum (Daily Stand-up).

b) Revisión del sprint (Sprint Review).

c) Retrospectiva del sprint (Sprint Retrospective).

d) Planificación del sprint (Sprint Planning).

135.- ¿Cuál es una de las características más importantes de un proyecto que sigue las prácticas Agile?

a) Al final de cada iteración se debe disponer de un producto funcional y mostrable a las partes interesadas.

b) Se debe esperar a terminar el proyecto para mostrar el producto final y concluido a las partes interesadas.

c) Deja libertad al equipo de desarrollo para que decida cuándo generar una versión funcional del producto, pudiendo terminar una iteración sin disponer aún del mismo.

d) La primera versión funcional del producto se genera a mitad del proyecto, disponiendo de una ceremonia especial donde se mostrará a las partes interesadas.

136.- ¿Por cuántos principios está respaldado el Manifiesto Agil?

a) 12.

b) 20.

c) 25.

d) 30.

137.- ¿Cuál de los siguientes principios no corresponde al Manifiesto Agil?

a) Aceptar los cambios en los requisitos, incluso si es en etapas tardías del desarrollo.

b) El software que funciona es la medida principal del progreso.

c) Promover un ritmo de desarrollo sostenible, constante a lo largo del tiempo.

d) Fomentar la documentación exhaustiva del proceso y del producto por encima del software funcional.

138.- ¿Qué métrica ágil se suele usar para predecir la capacidad futura del equipo basada en el histórico?

a) Throughput.

b) Velocidad.

c) ROI.

d) Lead time.

139.- ¿Cuál es la duración típica recomendada de un Sprint en Scrum?

a) 3 a 5 días.

b) 1 a 2 semanas.

c) 1 a 4 semanas.

d) Depende de la complejidad del Sprint.

140.- ¿Cuándo es preferible utilizar la metodología en cascada (Waterfall) en lugar de un marco de trabajo ágil como Scrum?

a) Cuando los requisitos del proyecto son altamente inciertos y se espera que evolucionen significativamente durante el desarrollo.

b) Cuando el equipo de desarrollo es multidisciplinar y requiere autonomía total para decidir cómo realizar el trabajo en ciclos cortos.

c) Cuando los requisitos están claramente definidos desde el inicio, son estables y el proyecto se desarrolla en un entorno con baja incertidumbre.

d) Cuando se necesita entregar valor de forma incremental y obtener retroalimentación constante del cliente para ajustar el producto final.

141.- ¿Cuándo NO es adecuado utilizar metodologías ágiles?

a) Cuando se necesita una alta flexibilidad para adaptarse a cambios frecuentes en los requisitos del proyecto.

b) Cuando el proyecto tiene requisitos muy estables, predecibles y la documentación exhaustiva inicial es un requisito legal o contractual innegociable.

c) Cuando se requiere una colaboración constante y feedback continuo por parte del cliente o del Product Owner.

d) Cuando el equipo de desarrollo es auto-organizado y se fomenta la comunicación directa y transparente entre sus miembros.

142.- ¿Cuál de los siguientes NO es un principio explícito en Kanban?

a) Comenzar con lo que se está haciendo ahora.

b) Aspirar a perseguir cambios incrementales y evolutivos

c) Priorizar al cliente por encima de los procesos actuales.

d) Fomentar actos de liderazgo a todos los niveles.

143.- Durante la planificación del Sprint, ¿cuáles son las dos preguntas principales que se deben responder?

a) ¿Qué pretendemos completar?, ¿Cómo se hará para completar los objetivos?.

b) ¿Qué hice ayer?, ¿Qué haré hoy?.

c) ¿Cuánto costará?, ¿Cuándo terminaremos?.

d) ¿Qué falló?, ¿Qué podemos mejorar?.

144.- En Kanban, ¿qué práctica anima a los equipos a terminar las tareas que tienen entre manos, antes de comprometerse con otras nuevas?

a) Timeboxing.

b) Limitación del trabajo en curso.

c) Sprint Goal.

d) Burndown.

145.- ¿Cuál de las siguientes fases no es fundamental en la ingeniería del software?

a) Especificación del Requisitos.

b) Diseño e implementación.

c) Validación.

d) Reingeniería.

146.- ¿Cómo se denomina a los requisitos que capturan los servicios que el sistema debe proveer, cómo deberá reaccionar a entradas particulares y cómo deberá comportarse en situaciones específicas?

a) Requisitos funcionales.

b) Requisitos NO funcionales.



c) Requisitos externos.

d) Requisitos de la organización.

147.- ¿Cuál de los siguientes NO es un tipo de diagrama en UML?

a) Diagrama de caso de uso.

b) Diagrama de flujo.

c) Diagrama de secuencia.

d) Diagrama de estado.

148.- ¿Cómo se denomina al proceso de probar componentes del programa, como métodos o clases de objetos?

a) Pruebas de unidad.

b) Pruebas de componente.

c) Pruebas del sistema.

d) Pruebas de versión.

149.- ¿Qué tipos de pruebas se incluyen dentro de las pruebas de desarrollo?

a) Pruebas de unidad, de componente y de rendimiento.

b) Pruebas de unidad, de componente y de usuario.

c) Pruebas de unidad, de componente y del sistema.

d) Pruebas de unidad, de componente y de escenario.

150.- Realizar cambios en el código de un programa sin alterar su comportamiento, se considera un mantenimiento

a) Correctivo.

b) Preventivo.

c) Modificativo.

d) Adaptativo.



151.- ¿Cuál de los siguientes es un orden correcto para especificar el ciclo de vida del desarrollo software?

a) Captura y Análisis de requisitos, Diseño, Implementación, Despliegue, Testing, Mantenimiento.

b) Diseño, Captura y Análisis de requisitos, Implementación, Integración, Explotación, Mantenimiento.

c) Captura y Análisis de requisitos, Diseño, Implementación, Integración, Mantenimiento, Explotación.

d) Captura y Análisis de requisitos, Diseño, Implementación, Integración, Explotación, Mantenimiento.

152.- En el ámbito de la ingeniería software, se distinguen varios tipos de mantenimiento. ¿Cuál de los siguientes no es uno de ellos?

a) Correctivo.

b) Adaptativo.

c) Perfectivo.

d) Modificativo.

153.- Durante el proceso de desarrollo de software, ¿En qué fase se generará el diagrama de secuencia de un caso de uso?

a) Diseño.

b) Análisis.

c) Pruebas.

d) Implementación.

154.- ¿Cuál de los siguientes procesos, metodologías o frameworks establece cuatro fases (incepción o inicio, elaboración, construcción y transición) para dividir un proyecto en el tiempo?

a) Proceso Unificado.

b) Agile.

c) Scrum.

d) Waterfall (Cascada).



155.- ¿En qué fase del ciclo de vida del desarrollo de software se especifica cómo se va a desarrollar el sistema a implementar?

a) Análisis.

b) Implementación.

c) Concepción.

d) Diseño.

156.- ¿Cuál de los siguientes NO es uno de los modelos de creación de prototipos de software?

a) Prototipado rápido.

b) Prototipado evolutivo.

c) Prototipado en espiral.

d) Prototipado en cascada.

157.- En el modelo de ciclo de vida en espiral, ¿qué representa la dimensión angular en los ejes cartesianos?

a) Las diferentes áreas de conocimiento involucradas en el proyecto.

b) La secuencia de las cuatro clases de actividades en cada ciclo.

c) El nivel de complejidad de las actividades en cada cuadrante.

d) El progreso relativo en el desarrollo de las actividades de cada cuadrante.

158.- ¿En qué fase del ciclo de vida del software se produce el documento de requisitos del software?

a) Análisis.

b) Diseño.

c) Codificación.

d) Integración.

159.- ¿Qué es un SRD (Software Requirements Document) en el ciclo de vida del software?

a) Una descripción detallada del código fuente a usar en el sistema.

b) Un conjunto de programas fuente en el lenguaje de programación elegido.

c) Una especificación precisa y completa de lo que debe hacer el sistema.



d) Un documento que describe el procedimiento de integración.

160.- En el contexto de las fases del ciclo de vida del software, ¿qué documento suele tener la siguiente estructura: información sobre el problema detectado, descripción de la solución adoptada y modificaciones realizadas sobre el sistema?

a) Documento de cambios.

b) Documento de requisitos.

c) Documento de diseño.

d) Documento de problemas.

161.- ¿Cuáles son las fases del Proceso Unificado?

a) Inicio, Elaboración, Construcción, Test.

b) Inicio, Elaboración, Construcción, Transición,.

c) Requisitos, Análisis, Diseño, Implementación.

d) Requisitos, Análisis, Diseño, Implementación,Test.

162.- En UML, ¿Qué diagrama se utiliza para modelar el modelo del dominio del sistema?

a) Diagrama de clases.

b) Diagrama de datos.

c) Diagrama de información.

d) Diagrama de estados.

163.- ¿Cuál de las siguientes NO es una prueba funcional?

a) Pruebas de integración.

b) Pruebas de desempeño.

c) Pruebas unitarias.

d) Pruebas de humo.

164.- ¿Qué técnica de diseño reduce el acoplamiento y aumenta la cohesión?

a) Ley de Demeter.

b) Variables globales.



c) Dependencias circulares.

d) Herencia múltiple.

165.- ¿Qué es una refactorización (refabricación)?

a) Añadir nuevas funcionalidades a un componente.

b) Modificar el código de un componente sin cambiar su comportamiento.

c) Reducir la cobertura de pruebas, pero manteniendo la rama principal.

d) Modificar el diseño, utilizando patrones de diseño.

166.- ¿Qué técnica NO se utiliza en las pruebas de caja negra?

a) Partición de equivalencia (Equivalence Partitioning).

b) Análisis de valores límite (*Boundary Value Analysis*).

c) Cobertura de sentencias (Statement Coverage).

d) Pruebas de tabla de decisión (*Decision Table Testing*).

167.- ¿Qué técnica NO se utiliza en las pruebas de caja blanca?

a) Cobertura de sentencias (Statement Coverage).

b) Cobertura de ramas (Branch Coverage).

c) Análisis de valores límite (Boundary Value Analysis).

d) Cobertura de caminos (Path Coverage).

168.- ¿Qué es la complejidad ciclomática de un programa?

a) El tiempo que tarda en ejecutarse.

b) El número de línea del programa.

c) El número de rutas de ejecución independientes del programa.

d) Un número que determina lo complejo que es entender el código del programa.

169.- ¿Cuál de los siguientes no es un elemento en la definición de un proyecto?

a) Estado.

b) Requisitos.

c) Alcance.



d) Riesgos.

170.- El método de estimación que se basa en la opinión de un grupo de cinco o seis expertos para llegar a un consenso de valores estimados, se conoce como:

a) Técnica PERT.

b) Técnica Delphi.

c) Método Montecarlo.

d) Método EDT.

171.- En la planificación de un proyecto, selecciona cuál de los siguientes elementos no es clave para elaborar un calendario:

a) Estimación del trabajo.

b) Relaciones de dependencia entre tareas.

c) Disponibilidad de los recursos.

d) Estándares de calidad.

172.- ¿En qué categoría de riesgo se encontraría clasificado el hecho de contar con unos requisitos vagos?

a) Riesgo externo.

b) Riesgo técnico.

c) Riesgo organizativo.

d) Riesgo de gestión del proyecto.

173.- En el seguimiento de un proyecto, la relación entre el valor ganado y el coste real, se denomina:

a) IRE. Índice de rendimiento de la estimación.

b) IRR. Índice de rendimiento real.

c) IRC. Índice de rendimiento del coste.

d) IRP. Índice de rendimiento de la programación.

174.- Indica las 5 fases en las que se divide un proyecto en el ciclo de vida:

a) Licitación, Planificación, Ejecución, Monitorización y Control, Cierre.

b) Inicio, Planificación, Monitorización y Control, Ejecución, Cierre.

c) Análisis, Planificación, Evaluación, Ejecución, Cierre.

d) Análisis, Planificación, Monitorización y Control, Ejecución, Cierre.

175.- ¿En qué fase del ciclo de vida de un proyecto se llevan a cabo las siguientes actividades: Elaborar el Acta de Constitución (Project Charter) e Identificar las partes interesadas (stakeholders)?

a) Inicio.

b) Licitación.

c) Análisis.

d) Planificación.

176.- ¿En qué fase del ciclo de vida de un proyecto se lleva a cabo la actividad de desarrollar el plan de dirección del proyecto?

a) Análisis.

b) Planificación.

c) Inicio.

d) Ejecución.

177.- ¿A qué término corresponde la siguiente definición? "Relación entre la cantidad de tiempo que se requiere para realizar una tarea en función del número de personas que la van a trabajar"

a) Duración.

b) Actividad.

c) Esfuerzo.

d) Holgura.

178.- En el contexto de la gestión de proyectos, ¿Qué significa EDT?

a) Estructura de desarrollo transversal.

b) Estructura de desglose del trabajo.

c) Estructura de despliegue transitoria.

d) Estructura de desglose de tareas.

179.- ¿En qué se diferencia el ciclo de vida de un proyecto del cronograma del mismo?

a) El ciclo de vida se compone de etapas sucesivas mientras que el cronograma se compone de tareas.

b) El ciclo de vida es aplicable a proyectos pequeños mientras que el cronograma es aplicable solo a proyectos grandes.

c) El ciclo de vida y el cronograma son términos que se refieren a lo mismo.

d) El ciclo de vida se compone de fases mientras que el cronograma se compone de etapas.

180.- ¿Cuál es el objetivo de la división del proyecto en etapas?

a) Mejorar la eficiencia y la gestión del equipo del proyecto.

b) Reducir el riesgo del proyecto al subordinar nuevas inversiones a la consecución de objetivos específicos.

c) Proveer flexibilidad al proyecto al permitir que cada etapa afecte a la planificación de la siguiente o del proyecto completo.

d) Todas las demás respuestas son correctas.

181.- ¿Qué es una etapa en el ciclo de vida de un proyecto?

a) Una tarea que permite avanzar hacia el objetivo final del proyecto.

b) Un conjunto de tareas que generan un resultado con significado propio.

c) Una fase del análisis del proyecto que divide su ejecución en períodos específicos.

d) Una oportunidad de inversión en el proyecto que permite demostrar su viabilidad.

182.- ¿En qué consiste la fase de Planificación en la gestión de proyectos?

a) Es la fase donde se ejecutan las tareas planificadas.

b) Es la fase donde se verifica el código fuente de la aplicación.

c) Es la fase donde se desarrollan los diferentes planes de gestión.

d) Es la fase donde se ejecutan el análisis, diseño y codificación de la aplicación.

183.- En la gestión de proyectos, ¿en qué fase se llevan a cabo las tareas planificadas para completar los entregables?

a) Inicialización.

b) Planificación.

c) Seguimiento y control.

d) Ejecución.

184.- ¿Por qué es posible que las fases de gestión de proyectos se ejecuten ligeramente en paralelo?

a) Porque no es necesario controlar ni seguir el progreso del proyecto hasta que se complete la fase de Ejecución.

b) Porque algunos aspectos dentro de las fases suelen desarrollarse de forma progresiva, a medida que existe información para ello.

c) Porque la planificación y la ejecución son dos fases que deben llevarse a cabo simultáneamente.

d) Porque la fase de Cierre debe solaparse con la fase de Seguimiento y Control para garantizar que se han conseguido los entregables.

185.- ¿Qué se utiliza para representar tareas a lo largo del tiempo y su calendario?

a) Cronograma

b) Matriz RACI.

c) Diagrama de tareas.

d) Burndown.

186.- ¿Qué restricción NO forma del análisis de viabilidad de un proyecto interno?

a) Tareas.

b) Alcance.

c) Presupuesto.

d) Plazo.

187.- ¿Qué técnica se utiliza específicamente para identificar la secuencia de actividades que determina la duración mínima de un proyecto?

a) Método de la Duración Mínima.

b) Método del Camino Crítico.

c) Método del Camino Mínimo.

d) Método de la Duración Crítica.

188.- ¿Qué documentación NO se prepara en la fase de planificación del proyecto?

a) El cronograma del proyecto.

b) La línea base de costes.

c) El diccionario de la WBS junto con la lista de entregables.

d) El análisis de requisitos del proyecto.

189.- ¿Cuál de estas técnicas NO se utiliza en el cálculo de un presupuesto?

a) Estimación por analogía.

b) Estimación por niveles.

c) Estimación por juicio de expertos.

d) Estimación paramétrica.

190.- ¿Cuál es la unidad más baja de una EDT/WBS donde se puede estimar el costo y la duración?

a) Entregable Principal.

b) Actividad.

c) Paquete de Trabajo.

d) Tarea.

191.- ¿Qué significa la matriz de responsabilidad RACI?

a) Revisar, Aprobar, Consultar, Informar..

b) Rápido, Agil, Constante, Iterativo.

c) Responsable, Aprobador, Consultor, Informado.

d) Recursos, Actividades, Costos, Ingresos.

192.- ¿Cuál de las siguientes técnicas NO se utiliza para la detección de riesgos en un proyecto?

a) Brainstorming.

b) Método MoSCoW.

c) Método DELPHI.

d) Método DAFO.

193.- En ITIL la unidad organizativa que tiene recursos y medios propios y es responsable de producir un resultado es:

a) Un servicio.

b) Un proceso.

c) Una función.

d) Un rol.

194.- En ITIL la gestión de los servicios es:

a) Una serie de acciones y actividades que permiten alcanzar un objetivo.

b) Un conjunto de disposiciones especializadas (funciones y procesos) que permiten proporcionar valor a los clientes en forma de servicios.

c) Un medio de proporcionar valor a los clientes, facilitando los resultados que desean obtener, sin asumir toda la responsabilidad de los costes o riesgos.

d) El resultado de trabajos en talleres que presentan los beneficios y las ventajas de determinadas acciones, en sectores y contextos diferentes.

195.- ¿Dentro de la Estrategia de Servicios de ITIL, qué proceso de gestión es el responsable de generar el plan estratégico (o roadmap) que guía la dirección de TI?

a) La gestión de la estrategia.

b) La gestión del portfolio de servicios.

c) La gestión de la demanda.

d) La gestión de la relación comercial.

196.- ¿Cuál de los siguientes procesos no pertenece a la fase de diseño de servicios en ITIL?

a) Proceso de gestión de la capacidad.

b) Proceso de gestión de proveedores.

c) Proceso de coordinación del diseño.

d) Proceso de gestión de activos de servicio y configuraciones.

197.- En ITIL, ¿qué proceso tiene por objetivo restaurar el servicio lo más rápido posible en el plazo establecido cuando un servicio se para o pierde calidad?

a) Gestión de eventos.

b) Gestión de incidentes.

c) Gestión de problemas.

d) Gestión de restauraciones.

198.- Los componentes principales del sistema de valor del servicio ITIL son: los principios rectores (guía), la gobernanza (dirección), la cadena de valor de los servicios, las prácticas y la… (elige la opción correcta)

a) Mejora completa.

b) Mejora total.

c) Mejora continua.

d) Mejora iterativa.

199.- ¿Qué elementos de ITIL crean la base para la cultura y el comportamiento de una organización, desde la toma de decisiones estratégicas hasta las operaciones cotidianas?

a) Los principios rectores/directores.

b) La cadena de valor de servicio.

c) Las prácticas.

d) Las actividades de gobernanza.

200.- ¿Cuál de las siguientes opciones describe mejor un servicio en el marco de ITIL?

a) El resultado de seguir un proceso.

b) Un medio para entregar valor a los clientes.

c) El resultado de la realización de una actividad.

d) Una oferta de un proveedor de servicios de TI.

201.- En el marco de ITIL, ¿qué principio rector/director se ocupa principalmente de comprender quién es el consumidor del servicio y cuál es su necesidad?

a) Mantener la sencillez y la practicidad.

b) Centrarse en el valor.

c) Progresar de forma iterativa con retroalimentación.

d) Optimizar y automatizar.

202.- En el marco de ITIL, ¿qué principio rector/director recomienda evaluar el estado actual y decidir qué se puede reutilizar?

a) Progresar de forma iterativa con la retroalimentación.

b) Empezar por donde se está.

c) Colaborar y promover la visibilidad.

d) Centrarse en el valor.

203.- ¿Cuál es el primer principio director de las buenas prácticas ITIL 4?

a) Focalizarse en la tecnología utilizada.

b) Focalizarse en el coste financiero para la empresa.

c) Focalizarse siempre en el valor proporcionado a las partes integrantes.

d) Focalizarse en los riesgos para la empresa.

204.- El tercer principio de ITIL4, "Implementar las buenas prácticas por iteraciones sucesivas", indica que debe seguirse el método de 4 etapas "plan, do, check, act". A dicho método se le conoce como la rueda de:

a) Deming.

b) Fleming.

c) Lenin.

d) Manning.

205.- ¿Cuál de los siguientes NO es un principio director de las buenas prácticas ITIL 4?

a) La automatización.

b) El pragmatismo.

c) El enfoque holístico.

d) La reestructuración.

206.- ¿Qué es lo primero que se debe hacer si un proceso, servicio, acción o indicador no proporciona valor según las buenas prácticas ITIL 4?

a) Automatizarlo.

b) Eliminarlo.

c) Añadir más etapas.

d) Continuar utilizándolo sin cambios.

207.- ¿Cuántos principios rectores (o directores) se definen oficialmente en las buenas prácticas de ITIL 4?

a) 4.

b) 5.

c) 7.

d) 34.

208.- ¿Cuál es la recomendación fundamental del segundo principio rector de ITIL 4, denominado "Empezar donde se está"?

a) Ignorar los procesos y herramientas actuales para diseñar una solución completamente nueva y sin fallos previos.

b) Identificar y medir los servicios y métodos existentes para determinar qué se puede reutilizar o mejorar antes de descartarlos.

c) Priorizar la automatización inmediata de todas las tareas manuales para acelerar el cambio organizacional.

d) Solicitar retroalimentación constante al cliente antes de realizar cualquier pequeña modificación en la infraestructura.

209.- ¿Cuál es la diferencia principal entre incidente y problema en ITIL?

a) Un problema está compuesto por varios incidentes.

b) Un incidente es la causa de uno o más problemas.

c) Un problema es la causa de uno o más incidentes.

d) No hay diferencias.

210.- En ITIL 4, la "cadena de valor del servicio" incluye actividades como:

a) Planificar, Mejorar, Participar, Diseño y transición, Obtener/construir, Entrega y soporte.

b) Diseño y transición, Desarrollar, Compilar, Testear, Entrega y soporte.

c) Diseño y transición, Desarrollar, Compilar, Ejecutar, Testear, Entrega y soporte.

d) Planificar, Mejorar, Diseño y transición, Compilar, Obtener/crear, Entrega y soporte.

211.- En ITIL, ¿Qué práctica se centra en reducir la probabilidad y el impacto de incidentes, identificando las causas reales y potenciales de los incidentes y gestionando soluciones alternativas y errores conocidos?

a) Gestión de problemas.

b) Gestión de errores.

c) Gestión de incidencias.

d) Gestión de riesgos.

212.- ¿Qué es un SLA en el contexto ITIL?

a) Un acuerdo documentado entre un proveedor de servicios y un cliente que identifica los servicios requeridos y el nivel esperado de los mismos.

b) Un contrato legal y técnico que define las sanciones financieras que el proveedor debe pagar en caso de una caída del sistema.

c) Un conjunto de objetivos técnicos utilizados internamente por el equipo de TI para medir el rendimiento de los servidores y la red.

d) Un documento que describe los pasos detallados que el equipo de soporte debe seguir para resolver un incidente específico.

213.- ¿Cuál es la premisa fundamental del quinto principio rector de ITIL 4, denominado "Pensar y trabajar de manera integral"?

a) En unificar los procesos en toda la organización.

b) En entender que todas las partes deben integrarse para crear valor.

c) En centrarse únicamente en la tecnología y olvidar los procesos.

d) En utilizar todos los departamentos la misma tecnología.

214.- ¿Cuál es el objetivo principal del principio "Colaborar y promover la visibilidad"?

a) Centralizar la toma de decisiones en un único director para evitar discusiones.

b) Ocultar los fallos internos para no preocupar a los clientes.

c) Eliminar los "silos" de trabajo y asegurar que todos entiendan los objetivos.

d) Reducir el número de reuniones para que el equipo trabaje más rápido.

215.- ¿En qué situación es más recomendable comenzar a utilizar el marco de referencia ITIL en una organización?

a) Únicamente cuando la empresa decide cambiar todos sus servidores físicos por servicios en la nube (Cloud).

b) Cuando una organización necesita un modelo para la creación, entrega y mejora continua de servicios.

c) Solo si el departamento de Recursos Humanos detecta conflictos interpersonales entre los programadores.

d) Cuando la empresa quiere eliminar por completo el uso de procesos y centrarse solo en la programación ágil.

216.- ¿Qué es un flujo de valor en el contexto de ITIL 4?

a) Un diagrama técnico que muestra únicamente cómo viajan los datos a través de los servidores de la empresa.

b) Una serie de pasos que una organización realiza para crear y entregar productos y servicios a un consumidor.

c) Un proceso financiero utilizado para calcular el valor monetario de los activos de hardware al final de su vida útil.

d) Una jerarquía estricta de mando que determina quién debe aprobar los cambios en la infraestructura de TI.

217.- En el proceso KDD, ¿en qué etapa se aplican una serie de técnicas de preprocesado de datos?

a) Recopilación de datos.

b) Selección, limpieza y transformación de datos.

c) Minería de datos.

d) Interpretación y evaluación de modelos.

218.- En los sistemas OLAP, el operador drill-down consiste en:

a) Crear un subcubo especificando valores determinados en varias dimensiones.

b) Rotar el cubo para obtener diferentes perspectivas de los datos.

c) Tomar un subconjunto de un cubo eligiendo un valor concreto para una de las dimensiones.

d) Navegar desde una vista con menor detalle a otra con más nivel de detalle en las dimensiones.

219.- Con respecto a business intelligence, indique la sentencia correcta:

a) En business intelligence la información es la protagonista y está orientada a la toma de decisiones.

b) En minería de datos se parte del conocimiento y, mediante un proceso deductivo, se obtienen datos de calidad.

c) Los data warehouse están pensados exclusivamente para realizar operaciones de minería de datos sobre ellos.

d) Los datos que entran a la fase de selección, limpieza y transformación de datos son los datos que se van a minar.

220.- Dentro de las tareas de data mining, ¿qué se entiende por clustering?

a) Encontrar objetos que manifiesten características significativamente diferentes a las del resto de los objetos del conjunto.

b) Dividir una población heterogénea de objetos en grupos homogéneos, de forma que los objetos de cada grupo sean similares entre sí.

c) Encontrar reglas que muestran la relación que existe entre los distintos atributos de los datos analizados.

d) Encontrar un modelo que, aplicado a un ejemplo sin clasificar, lo clasifique dentro de un conjunto predefinido de clases.

221.- En Business Intelligence, ¿cuál de las siguientes técnicas de evaluación de modelos emplea la métrica conocida como MAE (mean absolute error)?

a) Evaluación de clasificadores.

b) Evaluación de modelos de regresión.

c) Evaluación de agrupamientos.

d) Evaluación de reglas de asociación.



222.- ¿A qué software se refiere la siguiente definición? Framework de programación basado en Java que soporta el procesamiento de grandes conjuntos de datos en un entorno informático distribuido

a) Apache Hadoop.

b) Apache Groovy.

c) Python.

d) R.

223.- En el contexto del tratamiento de datos para su análisis, ¿qué significan las siglas ETC?

a) Extraer, Transferir, Cargar.

b) Ejecutar, Transformar, Cargar

c) Extraer, Transformar, Cargar

d) Ejecutar, Transferir, Cargar

224.- En el área de la minería de datos, ¿qué significa KDD?

a) Knowledge Data Distribution.

b) Knowledge Data Definition.

c) Knowledge, Development and Dissemination.

d) Knowledge Data Discovery.

225.- De las siguientes opciones, ¿cuál refleja mejor el contenido de un data warehouse?

a) Histórico de datos internos de la organización.

b) Datos operacionales (actuales) de la organización.

c) Datos históricos integrados, obtenidos de fuentes internas y externas.

d) Datos externos a la organización que se integran con los operacionales.

226.- ¿Qué es un cubo OLAP?

a) Una base de datos multi-dimensional, orientada a la realización efectiva de transacciones ACID.

b) Una base de datos multi-dimensional, adecuada para el análisis instantáneo de grandes cantidades de datos.

c) Una superposición de tablas bidimensionales en un SGBD relacional.

d) Una tabla de múltiples columnas, estructuradas a su vez en sub-columnas, en un SGBD No-SQL.

227.- ¿Cuál de estas arquitecturas NO corresponde a un sistema OLAP?

a) MOLAP: OLAP multidimensional.

b) ROLAP: OLAP relacional.

c) HOLAP: OLAP híbrida.

d) TOLAP: OLAP transaccional.

228.- Una de las herramientas de código abierto más populares para la minería de datos es:

a) WEKA.

b) SPSS Modeler.

c) SAS Miner.

d) Kaggle.

229.- En el contexto de la visualización de datos para "business analytics", ¿qué es un mapa de calor?

a) Es una representación de datos de temperatura sobre un mapa geográfico.

b) Es un método para la visualización de datos jerárquicos mediante el uso de rectángulos anidados.

c) Es una representación gráfica de datos, donde los valores individuales contenidos en una matriz se representan como colores.

d) Es un mapa en el que se presentan datos estadísticos por regiones, colocando un número o coloreando las diferentes zonas, en función del dato que representa.

230.- El proceso que utiliza técnicas matemáticas, estadísticas y de Inteligencia Artificial para extraer datos, identificar información útil y conocimientos posteriores en forma de patrones, se denomina:

a) Minería de datos.

b) Big Data.



c) Business Intelligence.

d) Todas las demás respuestas son correctas.

231.- ¿Cuál de las siguientes afirmaciones refleja mejor la diferencia entre un Data Mart y un Data Warehouse?

a) Un Data Mart es una base de datos operacional, mientras que un Data Warehouse almacena datos históricos.

b) Un Data Mart es un subconjunto especializado de un Data Warehouse, orientado a un área o departamento, mientras que el Data Warehouse integra datos de toda la organización.

c) Un Data Mart almacena únicamente datos externos, mientras que un Data Warehouse almacena solo datos internos.

d) No hay diferencia; ambos términos son equivalentes.

232.- ¿Cuál de las siguientes afirmaciones describe mejor un Data Lake?

a) Es un repositorio centralizado que almacena únicamente datos estructurados de manera organizada para análisis rápido.

b) Es un sistema que almacena grandes volúmenes de datos en su formato original, sean estructurados, semiestructurados o no estructurados, permitiendo flexibilidad para análisis futuros.

c) Es un subconjunto de un Data Warehouse orientado a un área específica de la empresa.

d) Es una base de datos relacional optimizada para transacciones OLTP.

233.- ¿Cuál de las siguientes NO es una característica de un cartograma?

a) Ajusta el tamaño de las áreas geográficas según los valores de una variable.

b) Representa datos espaciales de manera visual y proporcional.

c) Mantiene la escala geográfica exacta de los territorios.

d) Permite identificar patrones y distribuciones sobre un mapa.

234.- En el aprendizaje por refuerzo, el agente aprende principalmente a través de:

a) Un conjunto de datos etiquetados que le indican la respuesta correcta.

b) La identificación de patrones repetitivos en datos históricos sin interacción con el entorno.

c) La interacción con un entorno, recibiendo recompensas mayores o menores según sus acciones.



d) La combinación de varias reglas de asociación predefinidas.

235.- ¿Cuál de las siguientes afirmaciones describe correctamente la relación entre Deep Learning y Machine Learning?

a) Machine Learning es un subconjunto de Deep Learning.

b) Deep Learning es un subconjunto de Machine Learning que utiliza redes neuronales profundas para aprender de grandes volúmenes de datos.

c) Machine Learning y Deep Learning son conceptos completamente independientes sin relación jerárquica.

d) Deep Learning reemplaza por completo a Machine Learning en cualquier tipo de análisis de datos.

236.- ¿Cuál de las siguientes afirmaciones describe mejor el Cognitive Computing?

a) Es un sistema que sigue reglas estrictas y predefinidas para procesar datos sin adaptarse a nueva información.

b) Son sistemas que simulan procesos de pensamiento humano, aprendiendo, razonando y tomando decisiones a partir de datos complejos.

c) Son sistemas que combinan inteligencia artificial, análisis de datos y aprendizaje automático para asistir en la toma de decisiones.

d) Son plataformas diseñadas para analizar grandes volúmenes de datos empresariales y generar insights accionables mediante técnicas avanzadas de IA.

237.- ¿Cuál de los siguientes NO es un componente típico de un sistema de Business Intelligence?

a) Fuente de datos

b) Infraestructura de datos

c) Escalado de Infraestructuras

d) Interfaz de usuario

238.- ¿Cuál de las siguientes afirmaciones describe mejor la Web Mining?

a) Es el proceso de diseñar bases de datos relacionales para aplicaciones web.

b) Es el análisis de datos disponibles en la web para extraer conocimiento útil, incluyendo contenido, estructura y patrones de uso.

c) Es la creación de sitios web utilizando lenguajes de programación como HTML, CSS y JavaScript.



d) Es el análisis de patrones de navegación y comportamiento de usuarios en sitios web para mejorar servicios o recomendaciones.

239.- ¿Qué es la ciencia de datos?

a) Un conjunto de principios fundamentales que dirigen la extracción de conocimiento a partir de los datos.

b) Un software específico diseñado únicamente para crear bases de datos empresariales.

c) Un método específico de almacenamiento masivo de información en la nube.

d) Una disciplina interdisciplinar que combina estadística, programación y conocimiento del dominio para analizar datos y apoyar la toma de decisiones.

240.- En función del origen y la forma en que se generan los datos, ¿cuáles son los dos principales modos de captura en los sistemas de información?

a) Batch y Streaming

b) Estructurados y no estructurados

c) Internos y externos

d) Históricos y transaccionales

241.- En caso de que se impugne un documento electrónico en el que se utilizó un servicio de confianza cualificado, y las comprobaciones realizadas arrojan un resultado negativo para quien impugnó, ¿qué consecuencia prevé la Ley?

a) Las costas se reparten por mitad entre las partes.

b) Las costas las asume el órgano jurisdiccional.

c) Las costas son a cargo de quien formuló la impugnación.

d) No se prevé ninguna consecuencia económica para el impugnante.

242.- El plazo máximo para resolver el procedimiento de verificación previa de cumplimiento de requisitos para incluir a un prestador en la lista de confianza es de 6 meses. ¿Qué efecto produce el silencio administrativo transcurrido dicho plazo?

a) Se entiende estimada la solicitud (silencio positivo).

b) El procedimiento se suspende automáticamente.

c) Se puede entender desestimada la solicitud (silencio negativo).

d) El prestador puede iniciar la actividad de forma provisional.

243.- Según la Ley 6/2020, ¿en qué supuesto queda exento de personación física el/la solicitante de un certificado cualificado?

a) Cuando acredite su identidad mediante videoconferencia homologada.

b) Cuando ya sea cliente del prestador desde hace más de dos años.

c) Cuando su firma en la solicitud haya sido legitimada en presencia notarial.

d) Cuando aporte copia compulsada del DNI ante el prestador.

244.- Un prestador cualificado expide certificados de sello electrónico a personas jurídicas. Además de los datos habituales y datos que permitan identificar a la persona física a la que se entregaron dichos certificados, ¿qué información adicional debe registrar obligatoriamente?

a) El domicilio fiscal de la persona jurídica.

b) Los datos del/la representante legal inscrito en el Registro Mercantil, si lo hubiera.

c) Las respuestas a) y b) son correctas.

d) No tiene obligación de registrar información adicional más allá del NIF de la entidad.

245.- Según la Ley 6/2020, ¿cuándo puede un prestador de servicios de confianza suspender la vigencia de un certificado electrónico, a diferencia de revocarlo?

a) a), b), y c) son correctas.

b) Por solicitud del titular o resolución judicial/administrativa.

c) En casos de duda sobre la violación del secreto de los datos de creación o falsedad de los datos del certificado.

d) Por inseguridad en los mecanismos criptográficos

246.- Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el periodo de vigencia de los certificados cualificados no será superior a:

a) 2 años.

b) 5 años.

c) 4 años.

d) 3 años.

247.- ¿Qué propiedades garantiza la firma electrónica, adecuadamente implementada?

a) Confidencialidad e integridad de los datos firmados, y no repudio por parte del/la firmante.

b) Integridad de los datos firmados, autenticación del/la receptor/a y no repudio por parte del receptor/a.

c) Confidencialidad e integridad de los datos firmados, y no repudio por parte del receptor/a.

d) Integridad de los datos firmados, autenticación del/la firmante, y no repudio por parte del/la firmante.

248.- Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, los certificados de autenticación de sitio web expedidos a personas jurídicas consignan la identidad del titular utilizando:

a) El URL del sitio web.

b) Su denominación o razón social y su número de identificación fiscal.

c) Únicamente su número de identificación fiscal.

d) Únicamente su denominación o razón social.

249.- Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, un prestador de servicios electrónicos de confianza tiene una de estas obligaciones:

a) Eliminar la información relativa a los servicios prestados en el momento de la extinción del certificado o la finalización del servicio prestado.

b) Disponer de un servicio de consulta accesible al público sobre el estado de validez o revocación de los certificados emitidos.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo al órgano de supervisión con una antelación mínima de dos semanas al cese efectivo de la actividad, sin que sea necesario comunicarlo a los clientes.

d) Almacenar de forma permanente todos los datos de creación de firma, sello o autenticación de sitio web de las personas físicas o jurídicas a las que haya prestado sus servicios.

250.- Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, la expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular es considerada una infracción:

a) Grave.

b) Muy grave.

c) El hecho indicado no constituye una infracción.

d) Leve.

251.- ¿Cuál de estas funciones no es ofrecida por los sistemas de correo electrónico seguro, como S/MIME o PGP?

a) Confidencialidad de los mensajes.

b) Integridad de los mensajes

c) Autenticación del emisor.

d) Entrega garantizada

252.- ¿Qué requisito establece el Reglamento Europeo de Identificación Digital (eIDAS) para la firma electrónica avanzada?

a) Estar vinculada al firmante de manera única.

b) a), c) y d) son correctas

c) Haber sido creada utilizando datos de creación de la firma electrónica que el firmante. puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

d) Permitir la identificación del firmante.

253.- ¿Qué es necesario para que una firma electrónica sea "cualificada" de acuerdo al reglamento eIDAS?

a) Que haya sido emitida usando claves simétricas de 256 bits, frente a los 128 de otros tipos de firma.

b) Que haya sido emitida utilizando algoritmos de clave pública.

c) Que haya sido realizada con un certificado emitido por un prestador cualificado de servicios de confianza.

d) Que vaya acompañada de una firma manuscrita.

254.- Con respecto a la autenticación de sitios web, el reglamento eIDAS:

a) No se contempla, se ciñe a la autenticación de personas.

b) Se contempla, pero solo para sitios web oficiales de los gobiernos de los estados miembros.

c) Considera la autenticación de sitios web utilizando certificados cualificados, que incluyan la identificación del sitio web, además de la identificación del proveedor de servicios de confianza.



d) Recomienda la autenticación de sitios web utilizando certificados auto-firmados.

255.- ¿Cuál de estas opciones NO corresponde a un requisito de los certificados cualificados de firma electrónica?

a) Que incluya el nombre del/la firmante, o un seudónimo.

b) Que incluya los datos relativos al inicio y final del período de validez del certificado.

c) Que incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor.

d) Que contenga el número de serie del dispositivo cualificado usado para almacenar la firma.

256.- La definición "datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos" corresponde a:

a) Sello electrónico.

b) Firma electrónica.

c) Documento electrónico.

d) Identificación electrónica.

257.- ¿Cuál de estas infracciones es considerada leve?

a) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control.

b) No extinguir la vigencia de los certificados electrónicos en los supuestos señalados en esta Ley.

c) La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de diez días desde que aquellos se hubieren producido.

d) La resistencia, obstrucción, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

258.- Según la Ley 6/2020, ¿cuál es el período mínimo durante el cual los prestadores cualificados deben conservar la información relativa a los servicios prestados?

a) Cinco años.

b) Diez años.

c) Quince años.



d) Veinte años.

259.- Según la Ley 6/2020, ¿qué plazo máximo tiene la Administración para dictar y notificar resolución en el procedimiento de verificación previa para la cualificación de un prestador de servicios de confianza?

a) Tres meses.

b) Seis meses.

c) Nueve meses.

d) Doce meses

260.- Según la Ley 6/2020, ¿qué cuantía mínima debe tener el seguro de responsabilidad civil de un prestador cualificado de servicios electrónicos de confianza?

a) 500.000 euros.

b) 1.000.000 euros.

c) 1.500.000 euros.

d) 2.000.000 euros.

261.- Según la Ley 6/2020, ¿en qué plazo deben los prestadores de servicios de confianza no cualificados comunicar al Ministerio competente el inicio de su actividad?

a) En el plazo de un mes.

b) En el plazo de dos meses.

c) En el plazo de tres meses.

d) Antes de iniciar la actividad.

262.- Según la Ley 6/2020, ¿qué órgano ejerce la función de supervisión y control de los prestadores de servicios electrónicos de confianza en España?

a) La Agencia Española de Protección de Datos

b) El Ministerio de Asuntos Económicos y Transformación Digital

c) El Centro Criptológico Nacional

d) La Comisión Europea

263.- Según la Ley 6/2020, ¿qué sucede si un prestador cualificado no remite el informe de evaluación de la conformidad en los términos previstos por el Reglamento (UE) 910/2014?

a) Se le impone automáticamente una multa.

b) Se suspende provisionalmente su actividad hasta la subsanación del incumplimiento.

c) Se inicia automáticamente un procedimiento sancionador por infracción grave.

d) Se retira la cualificación al prestador y al servicio, eliminándolo de la lista de confianza.

264.- Según la Ley 6/2020, cuando en un certificado cualificado se consigne un pseudónimo en lugar del nombre real del/la titular:

a) b), c), y d) son falsas

b) El prestador debe constatar la verdadera identidad del/la titular y conservar la documentación acreditativa.

c) Solo podrá utilizarse pseudónimo en certificados no cualificados.

d) La identidad real únicamente podrá revelarse con autorización del propio titular.

265.- Indique cuál de los siguientes es un derecho del/la interesado/a, según el reglamento europeo de protección de datos.

a) Derecho de indagación.

b) Derecho de repudio.

c) Derecho al olvido.

d) Derecho de publicidad.

266.- Según el reglamento europeo de protección de datos, indique cuál de los siguientes NO se considera dentro de las categorías especiales de datos personales.

a) Datos bancarios.

b) Datos genéticos.

c) Derecho biométricos.

d) Derecho relativos a la salud.

267.- El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un/a interesado/a sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable, en el reglamento europeo de protección de datos se entiende por:

a) Datos personales.

b) Seudonimización.

c) Elaboración de perfiles.

d) Tratamiento de datos.

268.- ¿Por quién estará compuesto el comité europeo de protección de datos?

a) Por un/a delegado/a de protección de datos de cada Estado miembro y por el/la Supervisor/a Europeo de Protección de Datos o sus representantes respectivos.

b) Por un/a encargado/a del tratamiento de datos de una administración pública de cada Estado miembro y por el/la Supervisor/a Europeo de Protección de Datos o sus representantes respectivos.

c) Por un/a delegado/a de protección de datos de cada Estado miembro y por el/la Delegado/a Europeo de Protección de Datos o sus representantes respectivos.

d) Por el/la director/a de una autoridad de control de cada Estado miembro y por el/la Supervisor/a Europeo de Protección de Datos o sus representantes respectivos.

269.- ¿A cuánto puede ascender cómo máximo las sanciones que impone el reglamento europeo de protección de datos, cuando se comete una infracción?

a) A una multa administrativa de 20.000.000 EUR o, tratándose de una empresa, de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior.

b) A una multa administrativa de 50.000.000 EUR o, tratándose de una empresa, de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior.

c) A una multa administrativa de 20.000.000 EUR o, tratándose de una empresa, de una cuantía equivalente al 5% del volumen de negocio total anual global del ejercicio financiero anterior.

d) A una multa administrativa de 50.000.000 EUR o, tratándose de una empresa, de una cuantía equivalente al 5% del volumen de negocio total anual global del ejercicio financiero anterior.



270.- Según la legislación actual sobre protección de datos, una persona tiene derecho a no aportar documentos que ya se encuentren en poder de la administración actuante o hayan sido elaborados por cualquier otra administración. La administración actuante podrá consultar o recabar dichos documentos salvo que la persona interesada se opusiera a ello. Además, (seleccione la opción más adecuada):

a) No cabrá la oposición únicamente cuando la aportación del documento se exigiera en el marco del ejercicio de potestades de inspección.

b) La persona interesada puede oponerse a que la administración recabe dichos documentos en cualquier caso.

c) No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

d) No cabrá la oposición únicamente cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras.

271.- El artículo 9 de la Ley Orgánica 3/2018 sobre protección de datos establece como categorías especiales algunos datos personales. ¿Cuál de los siguientes no está considerado como especial?

a) Vida sexual.

b) Afiliación sindical.

c) Nombre y Apellidos.

d) Creencias.

272.- Según el artículo 5 de la Ley Orgánica 3/2018 sobre protección de datos, los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad. Este deber de confidencialidad, ¿hasta cuándo se mantendrá?

a) Tendrá efecto mientras se mantenga la relación de la persona obligada con el responsable o encargado del tratamiento.

b) Se mantendrá aun cuando hubiese finalizado la relación de la persona obligada con el responsable o encargado del tratamiento.

c) La ley no especifica este aspecto.

d) Lo decidirá la persona obligada a mantener ese deber de confidencialidad.

273.- La Ley Orgánica 3/2018, aprobada por las Cortes Generales de España que tiene por objeto adaptar el derecho interno español al Reglamento General de Protección de Datos ¿cuál de estos acrónimos tiene?

a) LOGSE

b) LOPD

c) RGPD

d) LOPDGDD

274.- ¿Debe publicar la Administración de la Comunidad Autónoma del País Vasco un inventario de sus actividades de tratamiento de datos personales?

a) No tiene obligación ni de crearlo ni de publicarlo.

b) Sí, en cualquier caso.

c) No, debe crearlo y custodiarlo pero no tiene obligación de publicarlo.

d) Sí, cuando se hayan tratado datos personales de categoría especial.

275.- En el marco de la Ley Orgánica 3/2018, de 5 de diciembre ¿a partir de qué edad puede un menor de edad dar su consentimiento para el tratamiento de sus datos personales?

a) 12 años.

b) 14 años.

c) 16 años.

d) 18 años.

276.- En el marco de la Ley Orgánica 3/2018, de 5 de diciembre, ¿qué categoría de datos no puede ser tratada basándose solo en el consentimiento de la persona afectada para evitar situaciones discriminatorias?

a) Datos de contacto.

b) Datos sobre afiliaciones políticas.

c) Datos sobre ideología.

d) Datos sobre nivel educativo.



277.- En el marco de la Ley Orgánica 3/2018, de 5 de diciembre, ¿cuál de las siguientes afirmaciones sobre el tratamiento de datos personales relativos a condenas e infracciones penales es verdadera?

a) Solo pueden ser tratados por abogados y procuradores.

b) Pueden ser tratados libremente sin necesidad de una norma de rango legal.

c) Solo pueden ser tratados para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

d) Solo pueden ser tratados cuando se encuentre amparado en una norma de Derecho de la Unión, en la ley orgánica o en otras normas de rango legal.

278.- En el marco de la Ley Orgánica 3/2018, de 5 de diciembre, ¿cuándo puede llevarse a cabo el registro completo de los datos referidos a condenas e infracciones penales?

a) Solo cuando los datos sean proporcionados directamente por la persona afectada.

b) Cuando se realice conforme con lo establecido en la regulación del Sistema de Registros Administrativos de Apoyo a la Administración de Justicia.

c) Siempre que lo autorice la persona afectada.

d) Cuando los datos sean utilizados para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

279.- En el marco de la Ley Orgánica 3/2018, de 5 de diciembre, ¿cuándo debe informarse a la persona afectada sobre su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar?

a) Siempre que se trate de datos personales.

b) Cuando los datos personales obtenidos de la persona afectada sean tratados para la elaboración de perfiles.

c) Cuando los datos personales no hayan sido obtenidos de la persona afectada.

d) Siempre que se trate de datos personales relativos a condenas e infracciones penales.

280.- Según la Ley Orgánica 3/2018, ¿cuál es la obligación del responsable del tratamiento respecto a los datos personales de las personas empleadas de una empresa?

a) Solo debe recabar los datos estrictamente necesarios para la relación laboral y garantizar su confidencialidad.

b) Puede tratar libremente todos los datos que considere relevantes para la gestión interna.



c) Solo está obligado a recabar datos sobre salud, pero no sobre desempeño laboral.

d) No tiene ninguna obligación específica mientras los datos se utilicen dentro de la empresa.

281.- ¿Qué principio establece que los datos personales deben ser exactos y, si es necesario, actualizados?

a) Principio de minimización de datos.

b) Principio de exactitud.

c) Principio de confidencialidad.

d) Principio de limitación de finalidad.

282.- ¿Cuál de los siguientes NO es un derecho de las personas interesadas según la Ley Orgánica 3/2018?

a) Derecho de acceso.

b) Derecho de supresión.

c) Derecho a la neutralidad.

d) Derecho de portabilidad.

283.- Según la Ley Orgánica 3/2018, ¿quién es responsable del cumplimiento del tratamiento de datos personales en una empresa?

a) El/la delegado/a de protección de datos exclusivamente.

b) El/la responsable del tratamiento.

c) Solo el/la administrador/a de sistemas.

d) La propia persona interesada.

284.- ¿Qué obligación tienen, según la Ley Orgánica 3/2018, los encargados del tratamiento respecto a las instrucciones del responsable?

a) Cumplir estrictamente las instrucciones documentadas del responsable.

b) Actuar según su criterio personal.

c) Solo notificar errores, pero no cumplir instrucciones.

d) No tienen obligación legal.

285.- Según la Ley Orgánica 3/2018, ¿qué medida debe adoptar un/a responsable para garantizar la seguridad de los datos personales?

a) Medidas técnicas y organizativas adecuadas.

b) Solo medidas técnicas, no organizativas.

c) Solo medidas organizativas, no técnicas.

d) Ninguna medida es obligatoria.

286.- Según la Ley Orgánica 3/2018, ¿cuál es la autoridad competente para supervisar el cumplimiento de la normativa de protección de datos en España?

a) El Ministerio de Justicia.

b) La Agencia Española de Protección de Datos.

c) El Tribunal Supremo.

d) El Defensor del Pueblo.

287.- Según el artículo 9 del ENS (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), ¿qué tipo de medidas deben constituir las líneas de defensa en un sistema de información?

a) Medidas de naturaleza humana, económica y social.

b) Medidas de naturaleza organizativa, física y lógica.

c) Medidas de naturaleza física.

d) Medidas de naturaleza ofensiva.

288.- Según el ENS, ¿qué permite la vigilancia continua?

a) La detección de actividades o comportamientos anómalos y su oportuna respuesta.

b) La detección de riesgos mínimos y las medidas de prevención de los mismos.

c) La detección y corrección de fallos en el hardware.

d) La detección y corrección de problemas en el software.

289.- Según el ENS, en la organización e implantación del proceso de seguridad el Responsable del Servicio debe determinar:

a) Los requisitos de la información tratada.

b) Los requisitos de los servicios prestados.

c) Las decisiones para satisfacer los requisitos de seguridad.

d) La forma de implementar la seguridad en el sistema.

290.- Según el ENS, ¿con qué frecuencia mínima deben realizarse auditorías de seguridad regulares ordinarias en los sistemas de información?

a) Cada año.

b) Cada dos años.

c) Cada tres años.

d) Cada cinco años.

291.- El ENS está constituido por principios básicos y requisitos mínimos para garantizar la protección adecuada de la información. ¿Cuál de las siguientes dimensiones de seguridad NO está explícitamente mencionada en dicho artículo?

a) Confidencialidad, integridad y disponibilidad.

b) Trazabilidad y autenticidad.

c) Acceso y conservación de los datos.

d) Resiliencia operativa ante ciberataques.

292.- En virtud del artículo 2.3 del Real Decreto 311/2022, las entidades del sector privado que presten servicios al sector público también quedan sujetas al ENS. ¿Qué obligación específica se extiende además a la cadena de suministro de dichos contratistas?

a) Obtener la certificación ISO 27001 en todos sus sistemas de información.

b) Presentar un análisis de riesgos conforme al artículo 24 del RGPD.

c) Cumplir los requisitos ENS necesarios según los resultados del análisis de riesgos correspondiente.

d) Designar un Responsable de Seguridad de la Información independiente del contratista principal.

293.- Conforme al artículo 28 del Real Decreto 311/2022, las medidas de seguridad del Anexo II podrán ser sustituidas por otras compensatorias. ¿Qué condición exige expresamente el precepto para que dicha sustitución sea válida?

a) Que las medidas alternativas estén aprobadas previamente por el CCN (Centro de Criptlogía Nacional) mediante instrucción técnica.

b) Que se justifique documentalmente que la protección aportada es, al menos, equivalente, y que satisfacen los principios básicos y requisitos mínimos.

c) Que sean objeto de una auditoría extraordinaria por un organismo externo acreditado.

d) Que el responsable del sistema informe a la Agencia Española de Protección de Datos antes de su aplicación.

294.- El artículo 30 del Real Decreto 311/2022 introduce el concepto de «perfil de cumplimiento específico». ¿Qué organismo tiene competencia para aprobar dichos perfiles según el real decreto?

a) La Comisión Sectorial de Administración Electrónica.

b) El Ministerio de Asuntos Económicos y Transformación Digital.

c) El Centro Criptológico Nacional.

d) La Agencia Española de Protección de Datos.

295.- Según el artículo 31 del Real Decreto 311/2022, las entidades del sector público incluidas en el ámbito del ENS deben someterse a auditorías de seguridad periódicas. ¿Cuál es la periodicidad ordinaria máxima establecida para dichas auditorías?

a) Anual.

b) Cada dos años.

c) Cada tres años.

d) Cada cinco años.

296.- El artículo 40 del Real Decreto 311/2022 define las categorías de seguridad de los sistemas de información. ¿Qué determina la categoría de seguridad de un sistema conforme al Anexo I?

a) El número de personas usuarias que acceden al sistema y el volumen de datos almacenados.

b) El mayor nivel de seguridad requerido en cualquiera de las dimensiones de seguridad afectadas.

c) El presupuesto asignado a la seguridad del sistema en el ejercicio presupuestario en curso.

d) La clasificación del organismo responsable dentro de la estructura de la Administración General del Estado.



297.- La disposición transitoria única establece un plazo para que los sistemas de información preexistentes a la entrada en vigor del RD 311/2022 alcancen su plena adecuación al ENS. ¿Cuál es ese plazo?

a) Veinticuatro meses desde la entrada en vigor.

b) Doce meses desde la entrada en vigor.

c) Dieciocho meses desde la entrada en vigor.

d) Treinta y seis meses desde la entrada en vigor.

298.- Respecto a los incidentes de seguridad, los artículos 33 y 34 del RD 311/2022 regulan la capacidad de respuesta. ¿A qué entidades se extiende la prestación de servicios de respuesta a incidentes prevista en el artículo 34?

a) Exclusivamente a las entidades de la Administración General del Estado.

b) Únicamente a los operadores de infraestructuras críticas designados conforme a la normativa sectorial.

c) A todas las empresas privadas con más de 250 personas empleadas que operen en territorio español.

d) A las entidades del sector público y a las organizaciones del sector privado que les presten servicios.

299.- Conforme a la disposición adicional segunda del artículo 34 del Real Decreto 311/2022, ¿qué tipo de carácter tienen las instrucciones técnicas de seguridad reguladas en dicho precepto?

a) Carácter de obligado cumplimiento.

b) Carácter orientativo y recomendatorio para las entidades del sector público.

c) Carácter vinculante solo para la Administración General del Estado, no para las comunidades autónomas.

d) Carácter vinculante exclusivamente cuando así lo determine el CCN (Centro Criptológico Nacional) en cada instrucción concreta.

300.- El artículo 3 del RD 311/2022 establece la relación entre el ENS y la normativa de protección de datos personales. Cuando un sistema de información trata datos personales, ¿qué obligación específica recae sobre la persona responsable o encargada del tratamiento además del cumplimiento del ENS?

a) Notificar obligatoriamente al CCN (Centro Criptológico Nacional) la existencia del tratamiento antes de su puesta en marcha.



b) Realizar un análisis de riesgos conforme al artículo 24 del RGPD y, en su caso, una evaluación de impacto según el artículo 35 del mismo reglamento.

c) Obtener la certificación de conformidad con el ENS antes de iniciar cualquier tratamiento de datos de carácter personal.

d) Designar a un/a delegado/a de protección de datos con funciones exclusivas de auditoría del ENS.

301.- El preámbulo del RD 311/2022 indica que las entidades del sector público que desplieguen redes 5G deben aplicar, además del ENS, otra norma específica. ¿A qué artículo de qué norma se refiere expresamente?

a) Artículo 5 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad de redes y sistemas de información.

b) Artículo 17 del Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de redes 5G.

c) Artículo 10 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

d) Artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

302.- El artículo 12 del Real Decreto 311/2022 regula la política de seguridad de las entidades del sector público. En el caso de las entidades del sector privado que presten servicios al sector público, ¿quién debe aprobar dicha política?

a) El/la Responsable de Seguridad designado por la entidad.

b) El órgano que ostente las máximas competencias ejecutivas de la entidad privada.

c) El Centro Criptológico Nacional, previo informe del contratista.

d) El órgano contratante de la Administración Pública correspondiente.

303.- Según el artículo 6 del Real Decreto 311/2022, el principio de «seguridad integral» implica que la seguridad se aborda desde una perspectiva global. ¿Qué elemento resulta esencial para este principio según el precepto?

a) Que la seguridad quede exclusivamente en manos del personal técnico especializado de cada entidad.

b) Que el análisis de riesgos se realice como paso previo y único a cualquier decisión de seguridad.

c) Que se establezcan cortafuegos perimetrales en todos los sistemas de categoría alta

d) Que todos los elementos del sistema —personas, tecnología y procesos— sean considerados de forma integrada.

304.- El artículo 11 del Real Decreto 311/2022 recoge el principio de «diferenciación de responsabilidades». ¿Cuál de las siguientes afirmaciones describe mejor su contenido?

a) Cada entidad debe disponer de un organigrama de seguridad donde consten todos los/las responsables de cada activo.

b) La responsabilidad de la seguridad de los sistemas recae sobre el/la responsable del servicio, no sobre el/la responsable del sistema.

c) Se exige que el/la responsable de la información, el/la responsable del servicio y el/la responsable del sistema sean personas o entidades distintas.

d) El personal de operaciones no podrá tener acceso a funciones de auditoría interna bajo ninguna circunstancia.

305.- El artículo 32 del Real Decreto 311/2022 regula el informe del estado de la seguridad. ¿Qué órgano tiene encomendado, según dicho artículo, recopilar la información necesaria para elaborar dicho informe con carácter general?

a) La Comisión Sectorial de Administración Electrónica.

b) El Ministerio de Hacienda y Función Pública.

c) El Centro Criptológico Nacional.

d) La Agencia Española de Protección de Datos.

306.- Conforme al artículo 35 del Real Decreto 311/2022, la «conformidad con el ENS» en el ámbito de la Administración Digital implica que los sistemas de información deben alcanzar y mantener la conformidad. ¿Cómo se acredita dicha conformidad para los sistemas de categoría ALTA?

a) Mediante una certificación de conformidad expedida por una entidad de certificación acreditada.

b) Mediante una declaración de conformidad suscrita por el/la responsable de seguridad de la entidad.

c) Mediante un informe favorable del CCN tras auditoría directa realizada por sus equipos.

d) Mediante la superación del cuestionario INES (Informe Nacional del Estado de la Seguridad).

307.- El artículo 39 del Real Decreto 311/2022 establece la obligación de «actualización permanente» del ENS. ¿Cuál de los siguientes factores NO figura expresamente en dicho artículo como motivo que obliga a esa actualización?

a) Las resoluciones dictadas por la Agencia Española de Protección de Datos en materia de brechas de seguridad.

b) La evolución de la tecnología y los estándares en materia de seguridad.

c) Las nuevas amenazas y vectores de ataque que se identifiquen.

d) El marco jurídico vigente en cada momento.

308.- El Anexo II del Real Decreto 311/2022 estructura las medidas de seguridad en tres grupos. ¿Cuál es la denominación correcta de los tres grupos y su descripción funcional según el real decreto?

a) Marco preventivo, marco reactivo y marco normativo.

b) Medidas técnicas, medidas organizativas y medidas jurídicas.

c) Marco estratégico, marco táctico y marco operativo.

d) Marco organizativo, marco operacional y medidas de protección.

309.- El artículo 29 del Real Decreto 311/2022 promueve el uso de infraestructuras y servicios comunes de las administraciones públicas. ¿Cuál es la finalidad principal que persigue expresamente este artículo?

a) Lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo en materia de seguridad.

b) Reducir el gasto en personal técnico especializado mediante la externalización de los servicios de seguridad.

c) Garantizar que todos los sistemas de información compartan una misma plataforma tecnológica homologada.

d) Evitar la duplicidad de auditorías de seguridad entre entidades de la misma comunidad autónoma.

310.- El algoritmo de cifrado DES (Data Encryption Standard) es un algoritmo de:

a) Clave hash.

b) Clave asimétrica.

c) Clave simétrica.

d) Clave pública.

311.- ¿Cuál de los siguientes es un algoritmo de cifrado de clave pública?

a) NSA.

b) RSA.

c) RC4.

d) AES.

312.- ¿Cuál de los siguientes es un estándar UIT-T aplicado en el marco del modelo PKI (Public Key Infrastructure)?

a) X.505.

b) X.507.

c) X.508.

d) X.509.

313.- ¿Cómo se define una PKI (Public Key Infrastructure)?

a) El conjunto de herramientas, políticas, personas y recursos necesarios para permitir la puesta en marcha de un entorno de seguridad basado en criptografía de clave pública, donde las personas usuarias pueden disponer de los servicios de integridad y no repudio.

b) El conjunto de herramientas, políticas, personas y recursos necesarios para permitir la puesta en marcha de un entorno de seguridad basado en criptografía de clave pública, donde las personas usuarias pueden disponer de los servicios de autenticación y no repudio.

c) El conjunto de herramientas, políticas, personas y recursos necesarios para permitir la puesta en marcha de un entorno de seguridad basado en criptografía de clave pública, donde las personas usuarias pueden disponer de los servicios de autenticación e integridad.

d) El conjunto de herramientas, políticas, personas y recursos necesarios para permitir la puesta en marcha de un entorno de seguridad basado en criptografía de clave pública, donde las personas usuarias pueden disponer de los servicios de autenticación, integridad y no repudio.

314.- ¿Cuál de los siguientes no es un algoritmo hash utilizado en criptografía?

a) HDA-3.

b) MD5.

c) SHA-1.

d) SHA-2.

315.- ¿Cuál de las siguientes afirmaciones sobre el funcionamiento de HTTPS es CIERTA?

a) HTTPS sustituye completamente al protocolo HTTP utilizando un nuevo formato de datos.

b) HTTPS utiliza HTTP sobre una conexión cifrada mediante SSL/TLS.

c) HTTPS solo proporciona autenticación, pero no cifrado de la información.

d) HTTPS funciona únicamente en redes locales.

316.- ¿Qué tipo de algoritmo es SHA-2?

a) Criptografía de clave pública.

b) Función de resumen criptográfico (hash).

c) Criptografía simétrica.

d) Firma digital.

317.- ¿Cuál de estos sistemas usa criptografía para incorporar seguridad en la capa 3 de la arquitectura TCP/IP?

a) IPSec.

b) SSL.

c) TLS.

d) WPA.

318.- ¿Qué contiene el chip criptográfico incorporado en el DNIe?

a) La identidad del titular en formato electrónico firmada por la FNMT.

b) Una clave privada del/la ciudadano/a.

c) Un certificado digital del/la ciudadano/a.

d) Dos certificados digitales del/la ciudadano/a con sus correspondientes claves privadas.

319.- ¿Cuál es la principal ventaja de la criptografía simétrica frente a la asimétrica?

a) Proporciona no repudio de forma directa.

b) Es computacionalmente más eficiente.

c) No requiere intercambio de claves.

d) Utiliza certificados digitales.

320.- En un sistema de criptografía de clave pública, la confidencialidad se garantiza cuando el mensaje se cifra con:

a) La clave privada del emisor.

b) La clave pública del emisor.

c) La clave pública del receptor.

d) La clave privada del receptor.

321.- ¿Cuál es la función principal de una función hash criptográfica?

a) Cifrar información de forma reversible.

b) Generar una huella digital única del mensaje.

c) Establecer una clave secreta compartida.

d) Firmar digitalmente documentos.

322.- Una función hash criptográfica segura debe cumplir principalmente:

a) Que sea reversible.

b) Que sea rápida de invertir.

c) Que sea resistente a colisiones.

d) Que utilice clave pública.

323.- En una firma digital basada en criptografía asimétrica, el emisor firma un documento utilizando:

a) La clave pública del receptor.

b) Su propia clave privada.

c) Su propia clave pública.

d) La clave privada del receptor.

324.- El objetivo principal del servicio de no repudio es:

a) Garantizar la confidencialidad del mensaje.

b) Evitar la modificación del mensaje en tránsito.

c) Impedir que el emisor niegue haber enviado el mensaje.



d) Acelerar el proceso de cifrado.

325.- ¿Qué entidad dentro de una PKI es responsable de emitir certificados digitales?

a) Autoridad de certificación (CA).

b) Autoridad de registro (RA).

c) Usuario final.

d) Servidor DNS.

326.- Un certificado digital X.509 contiene principalmente:

a) La clave privada del/la titular.

b) La clave pública del/la titular firmada por una CA.

c) El algoritmo hash del mensaje original.

d) La contraseña del/la usuario/a.

327.- En el protocolo TLS, la criptografía asimétrica se utiliza principalmente para:

a) Cifrar todo el tráfico de datos de la sesión.

b) Establecer de forma segura una clave simétrica de sesión.

c) Generar códigos de estado HTTP.

d) Reemplazar completamente la criptografía simétrica.

328.- ¿Qué propiedad garantiza que un mensaje no ha sido alterado durante la transmisión?

a) Confidencialidad.

b) Disponibilidad.

c) Integridad.

d) Autorización.

329.- En IPSec, el protocolo AH (Authentication Header) proporciona principalmente:

a) Confidencialidad mediante cifrado.

b) Integridad y autenticación del paquete.

c) Traducción de direcciones IP.



d) Compresión de datos.

330.- ¿Cuál es el propósito del intercambio de claves Diffie-Hellman?

a) Firmar digitalmente documentos.

b) Compartir de forma segura una clave secreta a través de un canal inseguro.

c) Generar funciones hash.

d) Emitir certificados digitales.

331.- ¿Qué diferencia fundamental existe entre autenticación y autorización?

a) Son términos equivalentes.

b) La autenticación verifica identidad; la autorización determina permisos.

c) La autorización cifra datos; la autenticación no.

d) La autenticación se realiza solo con hash.

332.- ¿Cuál de los siguientes algoritmos es de cifrado simétrico?

a) RSA.

b) AES.

c) DSA.

d) Diffie-Hellman.

333.- En una firma digital, el hash del documento se cifra para:

a) Reducir el tamaño del archivo.

b) Aumentar la velocidad de transmisión.

c) Garantizar integridad y autenticidad.

d) Ocultar la identidad del/la firmante.

334.- En seguridad informática, ¿cuál de las siguientes sentencias es errónea respecto a los requisitos que deben cumplir las políticas de seguridad de una organización?

a) Aplicación del principio de defensa en profundidad.

b) Configuración robusta ante fallos.

c) Cumplimiento de las exigencias del entorno legal.

d) Asignación de los máximos privilegios.

335.- El nivel RAID 6 proporciona:

a) Acceso independiente con paridad distribuida.

b) Acceso síncrono con un disco dedicado a paridad.

c) Acceso independiente con doble paridad.

d) Acceso independiente con un disco dedicado a paridad.

336.- En la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), ¿en qué etapa se crea el comité de seguridad?

a) Establecer un programa de mejora de la seguridad.

b) Definición de las políticas de seguridad y del alcance del SGSI.

c) Definición de responsabilidades y asignación de recursos.

d) Ejecutar las recomendaciones de la auditoría.

337.- En seguridad informática, la realización de copias de seguridad se considera una medida:

a) Preventiva.

b) Correctiva.

c) Activa.

d) Detectiva.

338.- ¿Cuáles son los tres principios fundamentales de la seguridad de la información en la nube?

a) Confidencialidad, integridad y privacidad.

b) Integridad, privacidad y disponibilidad.

c) Confidencialidad, integridad y disponibilidad.

d) Integridad, autenticación y privacidad.

339.- ¿Cuál de los siguientes no es un principio fundamental de la seguridad de la información?

a) Continuidad.

b) Disponibilidad.

c) Integridad.

d) Confidencialidad.

340.- Para cumplir los objetivos principales de seguridad informática, una organización debe contemplar cuatro planos de actuación:

a) Técnico, humano, psicológico, integral.

b) Técnico, legal, humano, organizativo.

c) Técnico, legal, humano, integral.

d) Técnico, legal, empresarial, organizativo.

341.- ¿A qué servicio de seguridad corresponde la definición: "Garantiza que cada mensaje transmitido o almacenado solo pueda ser leído por su legítimo/a destinatario/a"?

a) Autorización.

b) Confidencialidad.

c) Disponibilidad.

d) Autenticación.

342.- ¿Qué servicio de seguridad garantiza que la identidad del creador de un mensaje es legítima?

a) Autorización.

b) Autenticación.

c) Confidencialidad.

d) Disponibilidad.

343.- El principio consistente en implantar varios niveles de seguridad dentro de un sistema se denomina:

a) Defensa colateral.

b) Defensa perimetral.

c) Defensa en niveles.

d) Defensa en profundidad.

344.- ¿Es posible reducir el riesgo de un sistema hasta riesgo cero?

a) Sí, en activos físicos pero no en lógicos.

b) Sí, aunque el coste sería muy elevado.

c) No, siempre existirá un riesgo residual.

d) Sí, aplicando medidas técnicas y legales.

345.- ¿Cuál de las siguientes medidas se considera un control de seguridad organizativo?

a) Configuración de un firewall.

b) Instalación de un antivirus.

c) Formación en seguridad para empleados/as.

d) Cifrado de discos duros.

346.- ¿Cuál de las siguientes razones justifica la implantación de estándares de seguridad?

a) Transmitir confianza a usuarios/as y consumidores.

b) Definir métricas de evaluación y certificación.

c) Suministrar normas a fabricantes.

d) Todas las anteriores.

347.- ¿Qué agencia europea se encarga de la seguridad de redes y sistemas de información?

a) ENISA.

b) EDPS.

c) EASA.

d) EFSA.

348.- Una declaración de intenciones que establece las bases de la seguridad y delimita responsabilidades se denomina:

a) Plan de seguridad.

b) Manual de seguridad.

c) Política de seguridad.

d) Procedimiento de seguridad.

349.- Desde el punto de vista de la seguridad física, en un edificio deben definirse:

a) Tres zonas: públicas, internas y de acceso restringido.

b) Dos zonas: públicas y privadas.

c) Cuatro zonas: públicas, internas, restringidas y prohibidas.

d) Intranet, DMZ y extranet.

350.- ¿Qué nivel RAID ofrece acceso paralelo con un disco dedicado a paridad?

a) RAID 1.

b) RAID 0.

c) RAID 3.

d) RAID 5.

351.- El Plan de Continuidad de Negocio (BCP) tiene como objetivo principal:

a) Evitar cualquier tipo de ataque informático.

b) Garantizar la recuperación y continuidad de los servicios críticos tras un incidente.

c) Eliminar la necesidad de copias de seguridad.

d) Sustituir el SGSI.

352.- ¿Qué concepto describe la capacidad de un sistema para seguir funcionando ante fallos o incidentes graves?

a) Integridad.

b) Resiliencia.

c) Confidencialidad.

d) Autenticación.

353.- La auditoría de seguridad en una organización tiene como finalidad principal:

a) Sustituir las políticas de seguridad existentes.

b) Detectar y sancionar a los usuarios incumplidores.

c) Evaluar el cumplimiento de las políticas y controles establecidos.

d) Incrementar la disponibilidad de los sistemas.

354.- ¿Qué documento describe las acciones concretas a seguir ante un incidente de seguridad?

a) Política de seguridad.

b) Procedimiento de seguridad.

c) Plan de continuidad de negocio.

d) Declaración de aplicabilidad.

355.- El principio de mínimo privilegio establece que:

a) Los/las usuarios/as deben tener acceso completo para evitar bloqueos.

b) Se deben asignar únicamente los permisos estrictamente necesarios para realizar una tarea.

c) Los/las administradores deben tener todos los privilegios posibles.

d) El acceso debe ser anónimo para mayor seguridad.

356.- En la gestión de riesgos, el riesgo se define habitualmente como:

a) Activo x disponibilidad.

b) Amenaza x impacto.

c) Vulnerabilidad x impacto.

d) Probabilidad x impacto.

357.- ¿Cuál es el objetivo principal de un análisis de riesgos en seguridad informática?

a) Eliminar completamente todas las amenazas.

b) Identificar activos, amenazas y vulnerabilidades para estimar el nivel de riesgo.

c) Implantar directamente medidas técnicas.

d) Garantizar el cumplimiento legal automático.

358.- ¿Cuál de las siguientes afirmaciones es FALSA respecto a SOA?

a) SOA se basa en el principio de homogeneización de la semántica propia de la organización.

b) SOA persigue la obtención de un mapa de sistemas de información desacoplado, escalable y ágil.

c) SOA persigue la independencia del negocio respecto de la tecnología.



d) SOA busca una orientación a eventos de negocio, que disparan la orquestación de los servicios
mediante mensajería preferentemente síncrona.

359.- ¿Cuál de las siguientes afirmaciones contradice los principios básicos a seguir a la hora de implantar una estrategia SOA?

a) Los equipos implicados en los sistemas a integrar deben hablar y ponerse de acuerdo sobre el formato de los datos necesario para el intercambio de información.

b) En el lado tecnológico, el punto de comunicación para el envío y recepción de la mensajería debe ser la infraestructura SOA de la organización.

c) La estrategia SOA debe facilitar la integración de todos los sistemas participantes con el menor impacto posible.

d) Abstraer el diseño de los servicios de su entorno y de los sistemas que los usan garantiza su autonomía, aumenta su reusabilidad y disminuye su acoplamiento.

360.- A la hora de implantar SOA es conveniente:

a) Implantarlo desde el primer momento en el cien por cien de la organización.

b) Implantarlo deprisa y pensando en el corto plazo y los resultados que producirá.

c) Plantearlo como un cambio estratégico que, aplicado de forma constante e iterativa, extenderá con el tiempo bastantes de sus beneficios y mejoras al resto de la organización.

d) Plantearlo como la solución inmediata a todos los problemas de integración horizontal entre sistemas de la organización.

361.- ¿Cuál de las siguientes tareas NO corresponde a la gobernanza en SOA?

a) Seleccionar, entre las herramientas tecnológicas existentes, las más adecuadas para soportar la evolución hacia un mapa de sistemas con bajo acoplamiento, alta escalabilidad y eficiente en costes.

b) Dar soporte a la coordinación de proyectos TIC para ayudar a que se sigan las directrices estratégicas.

c) Definir los tipos de datos que participan en la semántica del negocio.

d) Identificar nuevos servicios, nuevas composiciones o nuevas versiones de los existentes.

362.- A la hora de implantar SOA, el establecimiento de las especificaciones en materia de seguridad en el intercambio de información en el mapa de sistemas se definen desde:

a) La gobernanza.

b) Las políticas.

c) Los estándares.

d) El catálogo de servicios.

363.- ¿Cuál de las siguientes afirmaciones es FALSA respecto al catálogo de servicios en una estrategia SOA?

a) La obtención de un Catálogo de Servicios mediante el enfoque Bottom up (de abajo arriba) es más inmediata y asequible que la estrategia Top down (de arriba abajo).

b) El enfoque Bottom up (de abajo arriba) es más indicada para nuevos sistemas y para nuevos requerimientos.

c) El enfoque Top down (de arriba abajo) es más costoso en recursos y en plazos, puesto que se necesitan conocimientos en modelado de procesos de negocio.

d) El enfoque Bottom up (de abajo arriba) intenta cambiar el patrón "petición-respuesta" por el de "proveedor-consumidor" mediante listas de suscripción.

364.- En una estrategia SOA el producto más tangible de la implementación es:

a) La gobernanza.

b) Las políticas.

c) Los estándares.

d) El catálogo de servicios.

365.- ¿Cuál de los siguientes es un conocido servidor para el registro y localización de microservicios, balanceo de carga y tolerancia a fallos desarrollado por Netflix?

a) Flutter.

b) Spring.

c) Nginx.

d) Eureka.

366.- ¿Cuál de los siguientes NO es un método HTTP?

a) POST.

b) PUT.

c) REMOVE.



d) PATCH.

367.- En el área de microservicios, se usan comúnmente APIs REST. ¿Qué significa REST?

a) Randomized Explicit State Translation

b) Representational State Transfer

c) Relational Environment Safe Token

d) Request Extended Secure Transfer

368.- En una arquitectura de microservicios, ¿cuál es una de las ventajas del escalado por partición de datos?

a) Reduce el consumo de memoria.

b) Aumenta la complejidad de implementación.

c) Resuelve los problemas del carácter monolítico de la aplicación.

d) Presenta problemas similares a los del escalado horizontal.

369.- Cuando se estructura un servicio global en microservicios, en lo que se refiere al despliegue de nuevas versiones, ¿qué afirmación es correcta?

a) Requiere un corte en el servicio global para realizar actualizaciones.

b) Permite desplegar nuevas versiones de un microservicio de manera independiente al resto de microservicios.

c) Limita la autonomía de la cadena de despliegue.

d) Una actualización de un microservicio siempre afecta al resto de los microservicios.

370.- ¿Cuál es una de las características básicas de una arquitectura de microservicios?

a) Independencia de los microservicios entre sí.

b) Gestión centralizada de datos.

c) Los microservicios comparten una base de datos común.

d) Fuerte acoplamiento entre los servicios.

371.- ¿Qué significa que los microservicios están débilmente acoplados?

a) Que cada microservicio contiene su propia lógica de negocio y se despliega conjuntamente con el resto.



b) Que cada microservicio puede estar desarrollado usando una tecnología diferente.

c) Que cada equipo de desarrollo es responsable de todo el ciclo completo de un microservicio.

d) Que los fallos en un microservicio no se propagan en la cadena de servicios.

372.- ¿Cuál de los siguientes patrones se utiliza para evitar que un fallo en un microservicio colapse toda la cadena de llamadas?

a) API Gateway.

b) Circuit Breaker.

c) Service Registry.

d) Event Sourcing.

373.- ¿Cuál de las siguientes afirmaciones describe mejor el patrón API Gateway en una arquitectura de microservicios?

a) Es un servicio que replica los datos entre microservicios.

b) Es un punto de entrada único que centraliza las peticiones de los clientes y las redirige al microservicio correspondiente.

c) Es una base de datos compartida por todos los microservicios.

d) Es un mecanismo de autenticación interno entre microservicios.

374.- ¿Cuál de las siguientes afirmaciones es FALSA respecto a la comunicación entre microservicios?

a) La comunicación síncrona mediante REST es la única válida en arquitecturas de microservicios.

b) La comunicación asíncrona mediante mensajería reduce el acoplamiento temporal entre servicios.

c) El uso de colas de mensajes permite que un microservicio continúe funcionando aunque el destinatario esté caído.

d) La elección entre comunicación síncrona y asíncrona depende de los requisitos del negocio.

375.- ¿Cuál de los siguientes NO es un beneficio del uso de contenedores Docker en una arquitectura de microservicios?

a) Portabilidad entre entornos de desarrollo, pruebas y producción.

b) Aislamiento de dependencias entre microservicios.

c) Despliegue rápido e independiente de cada microservicio.

d) Eliminación completa de la necesidad de orquestación.

376.- ¿Cuál de los siguientes enfoques es el más adecuado para gestionar transacciones que abarcan múltiples microservicios?

a) Transacciones ACID distribuidas mediante un gestor central.

b) Patrón SAGA, mediante una secuencia de transacciones locales coordinadas.

c) Base de datos compartida entre los microservicios implicados.

d) Llamadas síncronas encadenadas entre todos los microservicios participantes.

377.- ¿Qué problema principal introduce el uso de un registro de servicios como Eureka en una arquitectura de microservicios?

a) Aumenta el acoplamiento entre microservicios.

b) Impide el escalado horizontal de los servicios.

c) Introduce un punto único de fallo si no se despliega con alta disponibilidad.

d) Obliga a usar comunicación síncrona entre todos los servicios.

378.- ¿Cuál de las siguientes afirmaciones describe mejor el concepto de "bounded context" en el diseño de microservicios?

a) Es el límite físico de despliegue de un microservicio en un contenedor.

b) Es el número máximo de instancias que puede tener un microservicio escalado horizontalmente.

c) Es el protocolo de comunicación acordado entre dos microservicios.

d) Es el límite lógico dentro del cual un modelo de dominio tiene un significado consistente y bien definido.

379.- ¿Cuál de los siguientes es un inconveniente real de las arquitecturas de microservicios frente a las monolíticas?

a) Dificultad para escalar componentes de forma independiente.

b) Mayor complejidad operacional al gestionar múltiples servicios desplegados de forma distribuida.

c) Imposibilidad de usar diferentes tecnologías en cada servicio.

d) Mayor acoplamiento entre los componentes del sistema.

380.- ¿Cuál de las siguientes afirmaciones describe correctamente la diferencia entre orquestación y coreografía en microservicios?

a) En la orquestación un coordinador central dirige el flujo, mientras que en la coreografía cada microservicio reacciona a eventos de forma autónoma.

b) En la orquestación cada microservicio conoce y coordina al resto, mientras que en la coreografía un coordinador central dirige el flujo.

c) Orquestación y coreografía son dos términos distintos para referirse al mismo patrón de comunicación.

d) La coreografía requiere siempre comunicación síncrona mientras que la orquestación usa mensajería asíncrona.

381.- ¿Qué modelo de despliegue en la nube ofrece al usuario capacidad para ejecutar software específico que puede incluir sistemas operativos y aplicaciones?

a) SaaS.

b) PaaS.

c) IaaS.

d) AaaS.

382.- ¿Cuál de las siguientes afirmaciones es FALSA respecto a los beneficios de la computación en la nube?

a) Las aplicaciones se actualizan automáticamente.

b) Los recursos hardware se pueden incrementar bajo demanda, lo que facilita una reducción de costes.

c) El consumidor NO necesita instalación ni mantenimiento del software.

d) La empresa tiene un coste fijo mensual independiente del uso y personas usuarias que tenga la plataforma, lo que permite hacer una planificación más ajustada de los costes de explotación.

383.- ¿Cuál de las siguientes afirmaciones es FALSA respecto a los modos de despliegue de computación en la nube?

a) Una nube comunitaria puede ser administrada por la organización u organizaciones constituyentes o por terceras partes.

b) Una nube híbrida -formada por la unión de dos o más nubes- NO permite portar datos o aplicaciones entre las nubes que la conforman.



c) La infraestructura de una nube privada es gestionada íntegramente por una organización.

d) Una nube comunitaria es la forma menos habitual de despliegue de computación en la nube, siendo el NIST el único que suele recoger este modelo de despliegue.

384.- En la computación en la nube, Google Drive es un ejemplo del modelo de servicio:

a) SaaS.

b) PaaS.

c) IaaS.

d) AaaS.

385.- A la hora de considerar la seguridad en computación en la nube, un evento o actividad que tiene el potencial de producir daño a los sistemas de información o a las redes se considera:

a) Una vulnerabilidad.

b) Una amenaza.

c) Un riesgo.

d) Un incidente.

386.- En la estrategia de seguridad respecto al BYOD (bring your own device), el enfoque de virtualización:

a) Supone mantener la seguridad en el propio dispositivo mediante un sistema MDM instalado por el fabricante.

b) Supone que la red controla qué dispositivos acceden al sistema.

c) Se basa en una plataforma software que monitoriza y gestiona todos los dispositivos móviles.

d) Permite a las aplicaciones funcionar en servidores back-end en vez de en los dispositivos móviles.

387.- ¿Qué modelo de despliegue en la nube ofrece al usuario control sobre la aplicación aunque no de toda la infraestructura subyacente?

a) SaaS.

b) PaaS.

c) IaaS.

d) AaaS.

388.- Si quisiera utilizar servicios interactivos o de tiempo real ¿cuál sería la técnica de conmutación que elegiría en base a su menor latencia?

a) Conmutación de paquetes mediante datagramas.

b) Conmutación de paquetes mediante circuitos virtuales.

c) Conmutación de circuitos.

d) Conmutación de circuitos mediante paquetes virtuales.

389.- ¿A qué término corresponde la siguiente definición: "Proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de software, proporcionando una capa adicional de abstracción y automatización de virtualización de aplicaciones"?

a) Docker.

b) Hypervisor.

c) Ribbon.

d) VirtualBox.

390.- ¿Qué códigos de estado HTTP corresponden a una redirección?

a) 3XX.

b) 2XX.

c) 5XX.

d) 4XX.

391.- ¿Qué es Docker Compose?

a) Una herramienta para la compartición de datos entre diferentes contenedores.

b) Una herramienta para la interconexión de servicios dentro de un mismo contenedor.

c) Una herramienta para definir contenedores que implementan múltiples servicios.

d) Una herramienta para definir y ejecutar aplicaciones multi-contenedor.

392.- Los proveedores cloud ofrecen soluciones orientadas a:

a) Conectividad (servicios de red).

b) Procesamiento de información (cómputo).

c) Almacenamiento de información.

d) a), b), y c) son correctas.

393.- ¿Cuál de los siguientes es un software de virtualización?

a) Vagrant.

b) Vmware.

c) Kubernetes.

d) Docker.

394.- Gmail puede utilizarse para la gestión personalizada del correo electrónico de una organización. ¿De qué tipo de servicio en la nube estamos hablando?

a) SaaS.

b) PaaS.

c) IaaS.

d) AaaS.

395.- ¿Cuál de estas afirmaciones sobre la computación cloud es FALSA?

a) La computación cloud permite el acceso a los recursos desde cualquier parte a través de Internet.

b) Usando computación cloud se paga en función del uso que se hace de los recursos.

c) La computación cloud permite incrementar y reducir rápidamente los recursos utilizados.

d) La computación cloud exige que todas las aplicaciones corporativas sean portadas a la plataforma del proveedor.

396.- ¿Qué intenta garantizar un acceso web mediante HTTPS, frente a un acceso HTTP?

a) Confidencialidad de los datos, integridad de los datos, autenticación del servidor.

b) Confidencialidad de los datos.

c) Autenticación de cliente y servidor.

d) Integridad de los datos.

397.- ¿Cuál de estas características NO se corresponde a lo que entendemos por computación en la nube?

a) Autoservicio bajo demanda.

b) Elasticidad rápida.

c) Almacenamiento local con procesamiento remoto.

d) Servicio y facturación flexible.

398.- ¿Cuál o cuáles de estas técnicas requieren la modificación del sistema operativo cliente que se ejecuta en una máquina virtual?

a) Virtualización completa.

b) Paravirtualización.

c) Virtualización completa y paravirtualización.

d) Virtualización de aplicaciones.

399.- Las funciones fundamentales para conseguir una computación segura en la nube son:

a) Gestión de identidad y control de acceso.

b) Cifrado de los datos en tránsito.

c) Cifrado de los datos almacenados en la nube.

d) Replicación de los datos.

400.- Los principales beneficios de la computación en la nube para las empresas NO incluyen:

a) Rapidez y facilidad para desplegar aplicaciones y servicios.

b) Foco en el núcleo del negocio, dedicando menos recursos a la gestión de los sistemas de información.

c) Ventaja tecnológica, pudiendo aprovechar de forma inmediata las últimas funcionalidades disponibles.

d) Independencia del proveedor, al poder migrar fácilmente de un proveedor cloud a otro.

401.- ¿Cuál de las siguientes afirmaciones sobre microservicios es correcta?

a) Los microservicios requieren necesariamente el uso de máquinas virtuales dedicadas para cada servicio.



b) Los microservicios permiten escalar servicios de forma independiente.

c) Todos los microservicios deben compartir la misma base de datos.

d) Los microservicios eliminan la necesidad de monitoreo y gestión de fallos.

402.- ¿Cuál es la principal ventaja de utilizar contenedores frente a máquinas virtuales en entornos cloud?

a) Los contenedores incluyen un sistema operativo completo, lo que los hace más seguros.

b) Los contenedores permiten ejecutar aplicaciones de forma ligera y portable, compartiendo el mismo núcleo del sistema operativo.

c) Los contenedores no requieren orquestación para escalar.

d) Los contenedores reemplazan la necesidad de infraestructura de red en la nube.

403.- ¿Cuál de los siguientes mecanismos se utiliza en la nube para garantizar alta disponibilidad y tolerancia a fallos?

a) Replicación de datos y balanceo de carga entre múltiples servidores o regiones.

b) Uso exclusivo de máquinas físicas locales.

c) Evitar la virtualización para no depender del hipervisor.

d) Ejecutar todas las aplicaciones en un único servidor potente.

404.- ¿Qué característica define mejor la elasticidad en la nube?

a) Capacidad de las personas usuarias para instalar cualquier software en los servidores del proveedor.

b) Garantizar que todos las personas usuarias compartan los mismos recursos fijos.

c) Ejecutar únicamente aplicaciones críticas en la nube.

d) Posibilidad de aumentar o reducir recursos automáticamente según la demanda.

405.- En el modelo IaaS, ¿qué controla el usuario y qué gestiona el proveedor?

a) La persona usuaria controla toda la infraestructura, el proveedor solo provee soporte técnico.

b) La persona usuaria no controla nada, el proveedor gestiona todo.

c) La persona usuaria controla solo las aplicaciones y datos, el proveedor gestiona infraestructura, virtualización y red.

d) La persona usuaria controla la red y almacenamiento, el proveedor solo el cómputo.

406.- ¿Cuál es una de las funciones principales de un sistema IDS (Intrusion Detection System)?

a) Cifrar automáticamente todos los datos de la red.

b) Sustituir los mecanismos de autenticación de usuarios.

c) Detectar actividades sospechosas analizando el tráfico de red.

d) Gestionar direcciones IP dentro de la red.

407.- En la gestión de la seguridad informática, ¿qué aspecto es fundamental para permitir la integración y comunicación entre distintos sistemas y proveedores?:

a) La utilización de estándares e interoperabilidad entre sistemas.

b) El uso de sistemas propietarios cerrados.

c) La eliminación de interfaces entre aplicaciones.

d) El uso exclusivo de un único proveedor tecnológico.

408.- Con respecto a los pasos a seguir en un ciberataque, indique la respuesta correcta:

a) Antes de instalar un programa antivirus se deben modificar las contraseñas.

b) La realización de un análisis completo del sistema precede a la instalación de un programa antivirus.

c) Una vez realizada una limpieza manual se procede a modificar las contraseñas.

d) La realización de un análisis completo del sistema precede a la modificación de contraseñas.

409.- En las etapas en la gestión de la ciberseguridad, el control de accesos y gestión de identidades quedaría enmarcado en la etapa de:

a) Respuesta.

b) Inteligencia.

c) Detección.

d) Prevención.

410.- Uno de los siguientes NO es un tipo de sistema anti-intrusión. ¿Cuál?

a) SIDS.

b) NIDS.

c) HIDS.

d) IPS.

411.- Un Centro de Operaciones de Ciberseguridad ofrece los siguientes servicios:

a) Detección y gestión de respuestas.

b) Mantenimiento de hardware de persona usuaria.

c) a) y b) son correctas.

d) Capacitación general en ofimática.

412.- ¿Cuál de estos protocolos de seguridad para Wi-Fi requiere el uso de un servidor de autenticación (como RADIUS)?

a) WPA/WPA2 Enterprise.

b) WEP.

c) WPA/WPA2 Personal.

d) Todos los citados.

413.- ¿Cuáles son los tres objetivos primordiales de la ciberseguridad?

a) Autenticación, Autorización, Acceso.

b) Trazabilidad, No repudio, Control de acceso.

c) Certificados, Firmas Digitales, Sellos Digitales.

d) Confidencialidad, Integridad, Disponibilidad.

414.- ¿Cuál de estos métodos ayuda a preservar la confidencialidad de la información?

a) Cifrado.

b) Gestión de permisos de archivos.

c) a), b), y d) son correctas.

d) Controles y registros de accesos.

415.- ¿Cuál de estos mecanismos NO está específicamente diseñado para preservar la disponibilidad de los sistemas informáticos?

a) Resúmenes criptográficos utilizando funciones hash.

b) Redundancia en redes y servicios.

c) Realización de copias de seguridad.

d) Replicación de datos.

416.- Un ataque consistente en entregar una dirección IP falsa cuando se procesa una solicitud de resolución de un nombre, se denomina:

a) ARP poisoning.

b) ARP reversing.

c) DNS poisoning.

d) DNS reversing.

417.- ¿Qué técnica se utiliza para detectar intrusiones mediante comparación de patrones conocidos de ataques?

a) Detección basada en anomalías.

b) Detección basada en firmas.

c) Encriptación de datos.

d) Gestión de identidades.

418.- ¿Qué tipo de malware se oculta dentro de programas legítimos y se ejecuta sin que el usuario lo note?

a) Virus.

b) Troyano.

c) Gusano.

d) Rootkit.

419.- En la seguridad de redes, ¿qué función cumple un firewall?

a) Filtrar tráfico según reglas de seguridad.

b) Monitorizar cambios en archivos del sistema.



c) Proteger únicamente las contraseñas de usuarios.

d) Encriptar la información de la red.

420.- ¿Cuál de los siguientes ataques explota vulnerabilidades en aplicaciones web para insertar código malicioso en un navegador?

a) SQL Injection.

b) Cross-Site Scripting.

c) DDoS.

d) Phishing.

421.- ¿Cuál de los siguientes ataques se basa en saturar un sistema con tráfico para interrumpir su disponibilidad?

a) Phishing.

b) Malware.

c) DDoS.

d) Man-in-the-middle.

422.- ¿Qué tipo de ataque engaña a las personas usuarias para que revelen información confidencial mediante correos o sitios falsos?

a) Phishing.

b) SQL Injection.

c) Rootkit.

d) Spoofing.

423.- ¿Qué técnica se utiliza para proteger datos sensibles al transformarlos en un formato ilegible sin la clave correcta?

a) Hashing.

b) Cifrado.

c) Compresión.

d) Tokenización.

424.- ¿Qué tipo de malware se propaga automáticamente entre sistemas sin intervención de la persona usuaria?

a) Troyano.

b) Gusano (Worm).

c) Rootkit.

d) Spyware.

425.- ¿Cuál de los siguientes mecanismos ayuda a mantener la confidencialidad de los datos?

a) Gestión de permisos.

b) Registro de accesos.

c) Cifrado.

d) Todas las anteriores.

426.- ¿Qué tipo de malware se instala de manera oculta y permite al atacante tomar control completo del sistema?

a) Rootkit.

b) Troyano.

c) Gusano.

d) Spyware.

427.- ¿Qué ataque aprovecha vulnerabilidades en la configuración de routers o switches para interceptar tráfico interno de la red?

a) ARP poisoning.

b) Phishing.

c) SQL Injection.

d) Cross-Site Scripting.

428.- Dentro del Big Data, ¿cuál de los siguientes rasgos NO está incluido en lo que se conoce como las tres uves?

a) Velocidad.

b) Virtualización.

c) Variedad.

d) Volumen.

429.- En la jerarquía del conocimiento, ¿qué elementos ocupan la base y la cúspide respectivamente?

a) Base: Datos Cúspide: Conocimiento.

b) Base: Información Cúspide: Conocimiento.

c) Base: Información Cúspide: Sabiduría.

d) Base: Datos Cúspide: Sabiduría.

430.- En la arquitectura funcional de un sistema de big data, ¿en qué capa están los datos descritos en todas sus dimensiones?

a) Privacidad y seguridad.

b) Gestión de los datos.

c) Gobierno de los datos.

d) Infraestructura tecnológica.

431.- En la gestión de los datos, ¿cuál de las siguientes sentencias es verdadera?

a) Las bases de datos en las que se sustenta un ERP (Enterprise Resource Planning) es un sistema OLTP.

b) Los sistemas que almacenan las operaciones que se llevan a cabo en un cajero automático es un sistema OLAP.

c) Los sistemas que dan soporte a las herramientas operativas de la empresa se les conoce como sistemas OLAP.

d) Los sistemas de apoyo al proceso de toma de decisiones de los directivos es un sistema OLTP.

432.- Indique la sentencia correcta con respecto a las implementaciones de un sistema olap en un data warehouse.

a) La aproximación MOLAP emplea una base de datos relacional para almacenar los hechos.

b) La aproximación HOLAP emplea únicamente una base de datos multidimensional para almacenar la información.



c) La aproximación HOLAP es más ineficiente que la aproximación MOLAP en cuanto al espacio utilizado.

d) La aproximación ROLAP utiliza menos espacio de almacenamiento que la aproximación MOLAP.

433.- ¿Cuál de estos sistemas de almacenamiento distribuido ha sido diseñado específicamente para el almacenamiento fiable de macrodatos (Big Data)?

a) HDFS.

b) SMB.

c) NTFS.

d) NFS.

434.- Cuando hablamos de Big Data nos referimos a conjuntos de datos cuyas características dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales. ¿De qué características hablamos?

a) Tamaño.

b) Velocidad de crecimiento.

c) Tamaño, complejidad y velocidad de crecimiento.

d) Complejidad.

435.- ¿Cuál de los siguientes es un sistema almacenamiento para Big Data que permite su gestión mediante un lenguaje basado en SQL?

a) Ext4.

b) S3.

c) Hbase.

d) Hive.

436.- Dentro del ecosistema Apache Hadoop, ¿qué es Pig?

a) Un sistema de gestión de bases de datos documentales**.**

b) Un sistema de gestión de bases de datos NoSQL orientado a columnas.

c) Un lenguaje para especificar programas de análisis de datos y un compilador para convertirlos en procesos MapReduce.

d) Una interfaz web para Apache Spark.

437.- En el ciclo de vida de la analítica de datos, el responsable de construir y refinar modelos analíticos es:

a) El administrador del data warehouse.

b) El científico de datos.

c) El analista de negocio.

d) El analista de inteligencia de negocio.

438.- En el ecosistema Hadoop, ¿qué es HBase?

a) Un sistema de gestión de bases de datos no relacional.

b) Un sistema de gestión de bases de datos relacional, sin capacidad para OLTP.

c) Un sistema de gestión de bases de datos relacional, con capacidad para OLTP.

d) Un sistema de ficheros distribuido y tolerante a fallos.

439.- Las arquitecturas para procesamiento big data incluyen soluciones de estos tipos:

a) Para procesamiento por lotes (batch).

b) Para procesamiento de flujos (streaming).

c) Procesamiento por lotes y procesamiento en streaming, usando herramientas diferenciadas para cada tipo de procesamiento.

d) Procesamiento por lotes y procesamiento en streaming, existiendo herramientas que pueden usarse para ambos tipos de procesamiento.

440.- En el ecosistema Hadoop, una de estas herramientas está diseñada para analizar grandes conjuntos de datos usando SQL:

a) HDFS.

b) HBase.

c) Hive.

d) YARN.

441.- ¿Cuál de los siguientes NO es un nivel del Índice de Madurez de los Modelos de Negocio de los Big Data?

a) Monitorización empresarial**.**

b) Metamorfosis empresarial**.**

c) Digitalización empresarial.

d) Monetización de los datos.

442.- ¿Cuál NO forma parte del ciclo vital de la analítica de datos?

a) Descubrimiento.

b) Preparación de los datos.

c) Puesta en marcha.

d) Todas las fases forman parte del ciclo vital de la analítica de datos.

443.- El concepto de "la muerte del porqué" hace referencia a:

a) La sustitución de causalidad por correlación en algunos análisis.

b) El abandono del método científico.

c) La falta de métricas financieras.

d) La eliminación de hipótesis en estadística.

444.- ¿Cuál es uno de los cuatro factores motrices del valor de los Big Data?

a) Acceso a datos históricos agregados.

b) Acceso a datos sin estructurar.

c) Reducción de costes operativos.

d) Incremento del presupuesto de TI.

445.- Hadoop MapReduce se utiliza principalmente para:

a) Procesamiento distribuido de grandes volúmenes de datos.

b) Gestión de metadatos en entornos de almacenamiento distribuido.

c) Orquestación de flujos de trabajo analíticos en tiempo real.

d) Consulta interactiva SQL sobre datos estructurados.

446.- La federación de datos se basa en la idea de que:

a) El almacenamiento es el nuevo ETC.

b) La consulta es el nuevo ETC.



c) El ETL desaparece.

d) Todo debe estar en un único servidor.

447.- El mantenimiento predictivo es un ejemplo de:

a) Optimización operativa basada en analítica descriptiva histórica.

b) Uso estratégico de analítica predictiva integrada en procesos operativos.

c) Implementación de arquitecturas MPP para acelerar el data warehouse.

d) Aplicación de modelos de segmentación para campañas de marketing.

448.- El principal desafío de introducir Big Data en un entorno tradicional de data warehouse es:

a) Sustituir completamente el sistema anterior.

b) Eliminar procesos ETL.

c) Integrar nuevas arquitecturas con sistemas existentes.

d) b) y c) son correctas.

449.- El enriquecimiento de datos en arquitectura Big Data consiste en:

a) Integrar datos de distintas fuentes para facilitar el preprocesado de los datos.

b) Transformar y limpiar datos durante procesos ETL tradicionales.

c) Optimizar almacenamiento para acelerar consultas.

d) Combinar múltiples fuentes para mejorar análisis.

450.- Un error común en toma de decisiones basada en datos es:

a) Automatizar decisiones sin supervisión humana en contextos críticos.

b) Sobreajustar los modelos analíticos a datos históricos sin validar su generalización.

c) Priorizar indicadores financieros de corto plazo frente a métricas estratégicas de largo plazo.

d) Ignorar sesgos cognitivos.

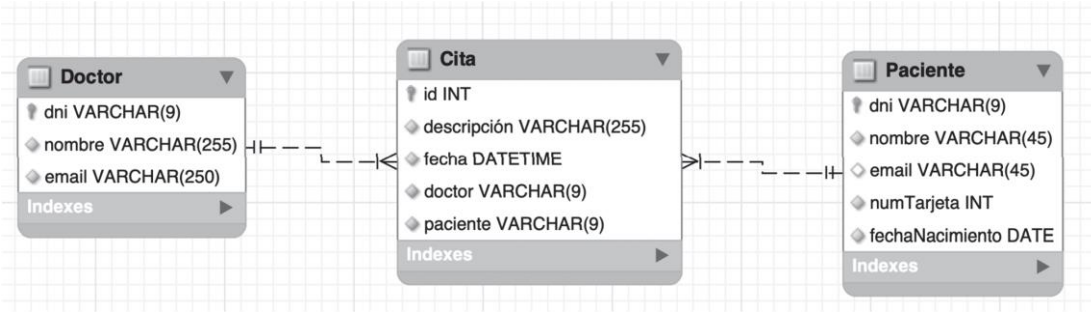
CASO PRÁCTICO 1

GESTIÓN DE PACIENTES

DESCRIPCIÓN DEL CASO

El sistema sanitario OsaNet (nombre ficticio) quiere mejorar su proceso de gestión de pacientes creando un sistema digital que pueda realizar un seguimiento de los historiales médicos y las citas de los pacientes. El sistema también debe permitir a los médicos actualizar los historiales de los pacientes y programar citas.

OsaNet necesita desarrollar un diagrama entidad/relación para garantizar que la base de datos refleje con precisión las relaciones entre las distintas entidades implicadas en el proceso de gestión de pacientes, doctores/as y citas. Se ha comenzado con el siguiente diseño de tablas y relaciones.



OsaNet dispone también de un sistema online, dentro de su intranet, que permite conocer la disponibilidad de agenda de un/a doctor/a. Este sistema, accesible desde el dominio (ficticio) intranet.osanet.eus, se ha implementado como un microservicio al que puede accederse vía API REST por HTTPS. Antes de asignar una nueva cita a un doctor/a se puede realizar una consulta GET para conocer la disponibilidad del facultativo.

El sistema OsaNet está considerando implementar nuevas funcionalidades para su intranet. Para gestionar el proyecto de desarrollo se seguirá el framework Scrum, generando entre otros artefactos, un backlog de producto y un backlog de sprint.

PREGUNTAS: 451-475

451.- Según el diagrama E/R anterior, ¿cuál de las siguientes afirmaciones es correcta?

a) En la entidad Cita, la columna doctor es clave foránea, la columna paciente es clave primaria y la columna id es clave foránea.

b) En la entidad Cita, la columna doctor es clave foránea, la columna paciente es clave foránea y la columna id es clave foránea.

c) En la entidad Cita, la columna doctor es clave foránea, la columna paciente es clave foránea y la columna id es clave primaria.

d) En la entidad Cita, la columna doctor es clave primaria, la columna paciente es clave primaria y la columna id es clave foránea.

452.- Según el diagrama E/R anterior, ¿cuál de las siguientes afirmaciones es correcta?

a) Hay una relación 1:N entre Doctor y Cita. También hay una relación 1:N entre Cita y Paciente.

b) Hay una relación 1:N entre Doctor y Cita. También hay una relación 1:N entre Paciente y Cita.

c) Hay una relación 1:1 entre Doctor y Cita. También hay una relación 1:1 entre Cita y Paciente.

d) Hay una relación N:M entre Doctor y Cita. También hay una relación N:M entre Cita y Paciente

453.- Realizando pruebas sobre el servicio web de disponibilidad de agenda, una persona usuaria ha recibido el siguiente error "HTTP Status Code:500". ¿A qué se debe un código de error de estado 500 en el protocolo HTTP?

a) A que la página a la que ha intentado acceder la persona usuaria no existe.

b) El error con código de estado 500 no existe en el protocolo HTTP.

c) Es un problema con el navegador de la persona usuaria, borrando las cookies y volviendo a intentar la petición probablemente se solucione.

d) Es un error interno en la parte del servidor.



454.- Se quiere implementar un nuevo microservicio que permita al personal facultativo guardar en el sistema OsaNet comentarios médicos obtenidos tras una consulta. Estos comentarios pasarán a formar parte del historial médico de la persona paciente. Por ejemplo, "La persona paciente XXXX indica dolores continuos en la zona abdominal. Se ha solicitado para esta persona la realización de análisis de heces y sangre.". Esta información es confidencial. ¿Qué verbo o método de consulta HTTP es necesario usar para transmitir este tipo de información de la forma más segura posible?

a) GET.

b) POST.

c) GET o POST indistintamente.

d) PUSH.

455.- Se está considerando añadir un campo contraseña en la tabla Doctor del esquema E/R presentado en el enunciado. Por cuestiones de seguridad no se quiere guardar la contraseña en claro. En su lugar se ha decidido guardar un hash (resumen criptográfico). En cuanto a su nivel de seguridad, ¿cuál de las siguientes funciones hash es más robusta?

a) MD5.

b) SHA-1.

c) SHA-256.

d) DRAGON-512.

456.- Para gestionar el proyecto usando el framework Scrum, el equipo del proyecto OsaNet ha generado, entre otros artefactos, un backlog de producto y un backlog de sprint. ¿Cuáles son las definiciones correctas y qué rol de Scrum gestiona dichos artefactos?

a) Backlog del sprint: es una lista priorizada de características, mejoras y correcciones de errores que definen los requisitos del producto. La gestiona el Product Owner. Backlog del producto: contiene un subconjunto de elementos del backlog del sprint. Lo gestiona el Equipo de Desarrollo.

b) Backlog del producto: es una lista priorizada de características, mejoras y correcciones de errores que definen los requisitos del producto. La gestiona el Product Owner. Backlog del sprint: contiene un subconjunto de elementos del backlog del producto. Lo gestiona el Equipo de Desarrollo.

c) Backlog del sprint: es una lista priorizada de características, mejoras y correcciones de errores que definen los requisitos del producto. La gestiona el Equipo de Desarrollo. Backlog del producto: contiene un subconjunto de elementos del backlog del sprint. Lo gestiona el Product Owner.



d) Backlog del producto: es una lista priorizada de características, mejoras y correcciones de errores que definen los requisitos del producto. La gestiona el Equipo de Desarrollo. Backlog del sprint: contiene un subconjunto de elementos del backlog del producto. Lo gestiona el Product Owner.

457.- Siguiendo el framework Scrum el Equipo de Desarrollo de OsaNet se reúne cada mañana para celebrar la reunión diaria de Scrum (el Daily Scrum). ¿A qué tres preguntas clave debe responder cada miembro del equipo?

a) ¿Cuándo terminarás tu tarea o proyecto? ¿Cuántas horas trabajaste ayer? ¿Cuál es el estado general del proyecto?

b) ¿Qué hiciste desde la última reunión diaria? ¿Qué planeas hacer hasta la próxima reunión diaria? ¿Hay algún impedimento o bloqueo que te impida cumplir con tu trabajo?

c) ¿Cuándo terminarás tu tarea o proyecto? ¿Cuántas horas trabajaste ayer? ¿Hay algún impedimento o bloqueo que te impida cumplir con tu trabajo?

d) ¿Qué hiciste desde la última reunión diaria? ¿Cuántas horas trabajaste ayer? ¿Cuál es el estado general del proyecto?

458.- Se quiere lanzar una consulta HTTP para conocer la disponibilidad de un/a doctor/a. Si el dominio (ficticio) del servicio es intranet.osanet.eus, ¿cuál de las siguientes peticiones GET con parámetros es sintácticamente correcta?

a) https://intranet.osanet.eus/agenda&dni=12345678A&fecha=151120231100

b) https://intranet.osanet.eus/agenda?dni=12345678A&fecha=151120231100

c) https://intranet.osanet.eus/agenda&dni=12345678A?fecha=151120231100

d) https://intranet.osanet.eus/agenda dni=12345678A fecha=151120231100

459.- La tabla Cita tiene una clave primaria “id”. ¿Qué ventaja presenta respecto a usar una clave primaria compuesta (doctor/a, paciente, fecha)?

a) Reduce la necesidad de índices.

b) Permite claves extranjeras más simples y estables.

c) Asegura que no existan citas duplicadas.

d) Evita almacenar fecha y hora.



460.- El microservicio de disponibilidad devuelve información sobre las horas libres de un/a doctor/a. ¿Qué característica debe tener esa operación para evitar efectos secundarios?

a) Debe ser idempotente.

b) Debe ser un POST.

c) Debe modificar la base de datos.

d) Debe eliminar la disponibilidad anterior.

461.- Si una persona paciente se elimina pero mantiene citas activas, ¿qué debe hacer la base de datos al intentar borrar su registro?

a) Borrarlo igualmente.

b) Sustituir el DNI por NULL.

c) Rechazar la operación mediante restricción clave extranjera (FK)

d) Eliminar solo su email.

462.- El microservicio de disponibilidad usa HTTPS. ¿Qué ocurriría si un atacante intentara interceptar la comunicación?

a) Podría leer los datos con dificultad.

b) No podría ver el contenido porque va cifrado.

c) Podría modificar la tabla Cita.

d) Podría autenticar clientes sin permiso.

463.- En Abbott, "el sistema OsaNet quiere mejorar su proceso de gestión" debe interpretarse como:

a) Añadir la Tabla Sistema

b) No genera tablas nuevas tablas

c) Método gestionar() en la tabla Doctor

d) Atributo booleano en la tabla Doctor.



464.- Abbott sugiere que sinónimos como "doctor/a" y "facultativo/a" deben:

a) Crear tablas distintas

b) Ser ignorados

c) Agruparse en la misma tabla

d) Convertirse en métodos

465.- En el E/R, la entidad Cita tiene claves extranjeras a Paciente y Doctor/a. En Orientación a Objetos esto se traduce en:

a) Dos atributos primitivos (idDoctor, idPaciente) dentro de Cita.

b) Dos asociaciones: Cita → Paciente y Cita → Doctor.

c) Dos asociaciones: Paciente → Cita y Doctor → Cita.

d) Una herencia desde Paciente y Doctor a Cita.

466.- La relación 1:N entre Paciente y Cita se convierte en Orientación a Objetos en:

a) Un atributo Cita en Paciente.

b) Una lista de Citas dentro de Paciente.

c) Herencia Cita→Paciente.

d) Una lista de Pacientes dentro de Cita.

467.- Si en E/R existe una relación Doctor–Paciente solo a través de Cita, en Orientación a Objetos:

a) Doctor tiene lista de Pacientes.

b) Paciente tiene lista de Doctores.

c) Ambos pueden tener listas si el sistema lo necesita.

d) No hay relación directa.

468.- En un diagrama de casos de uso, la comunicación entre Doctor y "Programar cita" se representa como:

a) Herencia

b) Asociación (línea simple)

c) “extends”.

d) “include”.

469.- ¿En cuál de los siguientes casos es apropiado modelar un caso de uso “extends” en el sistema OsaNet?

a) El caso de uso “Actualizar historial del paciente” siempre ejecuta “Validar identidad del doctor”.

b) El caso de uso “Consultar disponibilidad” se ejecuta siempre dentro de “Programar cita”.

c) El caso de uso “Programar cita” ejecuta “Solicitar confirmación al doctor” solo si la nueva cita modifica otra ya existente.

d) El caso de uso “Registrar paciente” siempre llama a “Crear tarjeta sanitaria”.

470.- Para validar que OsaNet funciona tras introducir nuevas funcionalidades en la intranet, se deben ejecutar:

a) Pruebas exploratorias.

b) Pruebas de regresión.

c) Pruebas estáticas.

d) Pruebas de localización.

471.- El microservicio consultar Citas devuelve JSON corrupto. Quieres probar que el sistema de citas lo maneja correctamente. ¿Qué tipo de prueba haces?

a) Caja negra con entradas inválidas.

b) Depuración interna del microservicio.

c) Revisión de logs.

d) Caja blanca sobre el front-end.

472.- En una prueba funcional, simulas que el/la doctor/a intenta crear una cita con una fecha anterior al día actual. ¿Qué tipo de prueba es?

a) Caja blanca.

b) Caja negra.

c) Integración.

d) Estática.

473.- ¿Qué tipo de cobertura utilizar para comprobar que todas las rutas del método consultarCitas() de la clase Paciente se ejecutan?

a) Cobertura de ramas.

b) Cobertura de humo.

c) Cobertura funcional.

d) Cobertura de datos.

474.- OsaNet quiere registrar "PacienteAdulto" y "PacienteMenor", donde los/las menores requieren autorización de tutor/a, pero ambos comparten datos personales y tarjeta sanitaria. ¿Qué diseño OO es adecuado?

a) Crear solo la clase Paciente y usar un atributo booleano "esMenor".

b) Crear PacienteAdulto y PacienteMenor heredando de Paciente

c) Crear dos clases independientes sin relación entre ellas.

d) Crear una relación 1:N entre Paciente y Tutor.

475.- En OsaNet se desea diferenciar entre dos tipos de doctores/as: doctores/as de atención primaria y doctores/as especialistas. Ambos comparten los mismos datos básicos (nombre, DNI, número de colegiado/a), pero cada tipo añade atributos propios. ¿Cuál sería la solución OO más adecuada?

a) Duplicar las clases DoctorPrimaria y DoctorEspecialista sin relación entre ellas.

b) Añadir todos los atributos en una única clase Doctor y dejar algunos vacíos según el tipo.

c) Crear una clase base Doctor y derivar de ella DoctorPrimaria y DoctorEspecialista mediante herencia

d) Crear una relación N:M entre Doctor y TipoDoctor.

Osakidetza



CASO PRÁCTICO 2

INFRAESTRUCTURA DE CLAVE PÚBLICA EN EL MARCO DE UNA ORGANIZACIÓN SANITARIA

DESCRIPCIÓN DEL CASO

Para dar soporte a las necesidades de nuestra organización sanitaria, ponemos en marcha una infraestructura de clave pública (**PKI**) cuya pieza central es una autoridad de certificación (**AC**) que emite certificados para:

- Personal de la organización sanitaria.
- Servidores web: portal del paciente, servidores de imágenes médicas, etc.
- Dispositivos IoT: monitores de pacientes, monitores de edificios, dispositivos de captación de imágenes médicas, etc.

Dicha AC es totalmente autónoma, partiendo de un certificado auto-firmado.

La AC tiene dos modos de emisión de certificados:

- **Modo 1** (**simplificado**). El titular del certificado acredita su identidad. La AC la verifica y genera una pareja de claves pública-privada para ese titular. Se emite el certificado y se le entrega conjuntamente con la clave privada.
- **Modo 2** (**avanzado**). El titular del certificado genera por su cuenta una pareja de claves pública-privada. Solicita el certificado acreditando su identidad y entregando la clave pública. La AC verifica la identidad y la validez de la clave, entregando al titular el certificado.

Nuestra PKI también incluye un servicio para comprobar online la validez de un certificado.

Se describen a continuación tres casos de uso de nuestra PKI, a los cuales corresponden las preguntas de este caso práctico.



> **Nota importante**: en todo este caso práctico se entiende que un certificado digital incluye la identidad del titular y la clave pública del mismo. La clave privada correspondiente se puede distribuir conjuntamente con el certificado (como se indica al describir el modo de emisión 1), pero no forma parte del mismo.

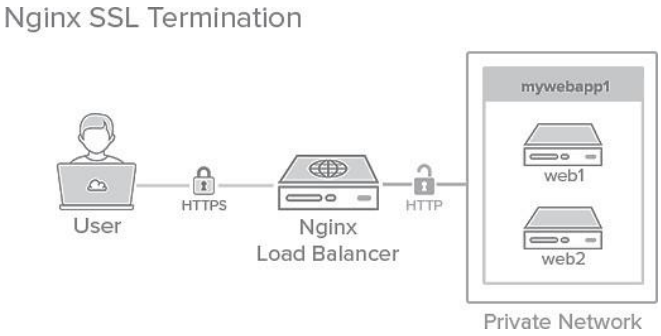
USO 1: FIRMA DIGITAL

La disponibilidad de esta PKI permite implementar procedimientos de firma digital sobre aquellos documentos digitales que lo requieran. Los procesos de firma de documentos se realizan de manera off-line (fuera del navegador web): para firmar un documento en formato PDF tiene que estar en el ordenador de un usuario/a. Dicho usuario/a utiliza programas como “Autofirma” (Gobierno de España) o “Adobe Acrobat” para generar la versión firmada del documento. Suponemos que nuestros/as usuarios/as utilizan ordenadores corporativos con Windows y tienen instalados los elementos criptográficos indicados previamente (que incluyen, pero no están limitados a, certificado del/la usuario/a, clave privada asociada, certificado de la AC).

USO 2: SERVIDORES WEB HTTPS

Los servidores web de la organización sanitaria han sido configurados, usando certificados emitidos para ello por nuestra AC, para que el acceso a los mismos sea siempre usando HTTPS. Todos los PCs corporativos de la organización sanitaria llevan instalado el certificado de la AC, lo que evita errores de acceso. Sin embargo, la AC no está reconocida por ordenadores no corporativos, externos a la organización sanitaria.

En la organización sanitaria, el servicio web de imágenes médicas tiene como dirección (ficticia) https://imagenes.os.org. Debido al gran volumen de accesos y tráfico que tiene, dicho servicio está implementado con 8 servidores físicos, y la distribución de carga entre ellos se realiza usando round-robin DNS. Decidimos cambiar la implementación de este servicio, haciendo que el nombre "imagenes.os.org" corresponda a una única dirección IP, asociada a una máquina en la que está instalado **Nginx** haciendo de equilibrador de carga (*load balancer*), tal como se muestra en la figura. Detrás del equilibrador de carga están los 8 servidores físicos que implementan realmente el servicio. Implementamos un sistema *Nginx SSL Termination*: las comunicaciones externas con el servicio de imágenes médicas son HTTPS, las internas (la distribución de la carga a los servidores reales) son HTTP "plano" (véase la figura).



SSL Termination y equilibrado de carga. Nótese que solo se representan dos servidores físicos, pero en el caso descrito se usan 8, que están en la red privada. Imagen tomada de https://www.digitalocean.com/community/tutorials/how-to-set-up-nginx-load-balancing-with- ssl-termination, con licencia CC-BY-NC-SA.

USO 3: CERTIFICADOS DE DISPOSITIVOS IOT

La instalación de certificados en los dispositivos IoT permite la comunicación segura (usando TLS) entre y con dichos dispositivos. Hay que tener en cuenta que los dispositivos IoT pueden estar en lugares no fácilmente accesibles, y ser muy numerosos.

USO 4: SERVIDORES PARA ALMACENAMIENTO DE DATOS AVANZADO

Los servidores de la Organización sanitaria van a cumplir la funcionalidad de almacenamiento de datos generados por los distintos centros y se están planteando distintas arquitecturas para poder proporcionar distintos servicios a empleado/as y pacientes de los centros sanitarios. Responda a las siguientes preguntas

PREGUNTAS: 476-500

476.- ¿Qué ventajas tiene el modo de emisión de certificados 1 (simplificado) con respecto al 2 (avanzado)?

a) La AC mantiene una copia de seguridad de la clave privada, que puede recuperarse en caso necesario.

b) El usuario no tiene que preocuparse de aspectos técnicos de emisión de claves.

c) No se requiere validar que el usuario posee la clave privada asociada a su clave pública, puesto que ambas han sido generadas de forma controlada por la AC.

d) a), b) y c) son correctas.

477.- ¿Qué inconvenientes tiene el modo de emisión de certificados 1 (simplificado), con respecto al 2 (avanzado)?

a) La clave privada deja de serlo totalmente, ya que hay que confiar en el buen uso de la misma por parte de la AC.

b) Se requiere que la persona usuaria acredite su identidad.

c) Es necesario validar que hay una correspondencia entre la clave pública y la privada.

d) No se puede excluir del certificado la clave privada de la persona usuaria.

478.- ¿Cuál de estos protocolos permite la verificación online de la validez de un certificado digital ante la entidad emisora?

a) SSL.

b) TLS.

c) OCSP.

d) HTTPS.

479.- En el proceso de firma digital de un documento PDF mediante herramientas como Autofirma o Adobe Acrobat, ¿cuál de las siguientes afirmaciones es CORRECTA?

a) El documento completo se cifra con la clave privada de la persona usuaria firmante.

b) Se calcula un resumen digital del documento, que es firmado con la clave privada de la persona usuaria.

c) El certificado de la persona usuaria se utiliza para cifrar el documento antes de enviarlo.

d) La firma digital consiste en añadir únicamente el certificado de la persona usuaria al documento.

480.- Una persona usuaria firma un documento digital utilizando su certificado, pero su clave privada ha sido comprometida sin que él lo sepa. ¿Cuál es la consecuencia principal?

a) Ninguna, porque no posee la clave pública.

b) La firma no podrá ser verificada correctamente.

c) Un tercero podría generar firmas válidas en nombre de la persona usuaria.

d) El documento firmado se descifrará automáticamente al detectarse el compromiso.



481.- ¿Cuál de las siguientes condiciones es necesaria para que un/a receptor/a pueda verificar correctamente una firma digital?

a) Disponer de la clave privada del/la firmante.

b) Disponer del certificado del/la firmante y confiar en la AC emisora.

c) Tener acceso al sistema donde se generó la firma.

d) Disponer del certificado de todas las personas usuarias de la organización.

482.- Definimos como "usuario/a corporativo" a un/a usuario/a de nuestra organización sanitaria, que utiliza un PC corporativo. Definimos como "usuario/a externo" a un/a usuario/a de fuera de nuestra organización que utiliza un PC no corporativo. ¿Cuál de estos escenarios es válido, asumiendo que todos los certificados son válidos, cuando haya un intento de acceso desde un navegador a un servidor web de nuestra organización sanitaria?

a) El usuario/a corporativo/a podrá conectar su navegador sin problemas usando HTTPS. Sin embargo, el usuario/a externo/a recibirá un aviso indicando que no es posible autenticar al servidor; el navegador bloqueará la conexión con el mismo y no será posible continuar la navegación con ese sitio web.

b) El usuario/a corporativo/a podrá conectar su navegador sin problemas usando HTTPS. Sin embargo, el usuario/a externo/a recibirá un aviso indicando que no es posible autenticar al servidor. El navegador dará al usuario/a externo/a la posibilidad de comunicarse con el servidor a su cuenta y riesgo, pero la conexión no estará cifrada.

c) Tanto el usuario/a corporativo/a como el externo/a podrán conectarse al servidor usando HTTPS, con autenticación del servidor y cifrado de la conexión.

d) El usuario/a corporativo/a podrá conectar su navegador sin problemas usando HTTPS. Sin embargo, el usuario/a externo/a recibirá un aviso indicando que no es posible autenticar al servidor. El navegador dará al usuario/a externo/a la posibilidad de comunicarse con el servidor a su cuenta y riesgo y la conexión estará cifrada.

483.- Actualizamos nuestro servicio "portal del paciente". El acceso sigue siendo HTTPS, pero se requiere autenticación de los clientes. ¿Cuál de estas alternativas es la correcta? Suponemos que el servidor tiene instalados los certificados de nuestra AC, así como de todas las AC con reconocimiento oficial.

a) Validación mediante envío de certificado digital y firma. El/la cliente envía su certificado; el servidor comprueba que es válido; el servidor envía un texto aleatorio (un "reto") al cliente, que lo devuelve firmado con su clave privada. Se valida la firma, lo que indica que el/la cliente posee una pareja de claves pública-privada correcta. Así se da por comprobada la identidad del/la cliente.

b) Validación mediante envío de certificado digital. El/la cliente envía su certificado, el servidor comprueba que es válido. Así se da por comprobada la identidad del/la cliente.



c) Validación mediante envío de certificado digital y firma. El servidor envía un texto aleatorio (un "reto") al cliente, que lo devuelve firmado con su clave pública. Se valida la firma, lo que indica que el/la cliente posee una pareja de claves pública-privada correcta. Así se da por comprobada la identidad del cliente.

d) Al abrir la conexión TLS (HTTPS), el proceso de autenticación del servidor lleva implícita la autenticación del cliente.

484.- Un/a usuario/a externo/a accede con frecuencia a los servidores de nuestra organización sanitaria. Tiene ya instalado en su PC un certificado de ciudadano emitido por la FNMT (Fábrica Nacional de Moneda y Timbre). Sin embargo, cada vez que accede a nuestros servidores, recibe un aviso en el navegador. ¿Qué tiene que hacer para evitar el aviso?

a) Instalar en su PC el certificado de nuestra AC y la clave privada asociada al mismo.

b) Pedirnos que instalemos en nuestros servidores su certificado de ciudadano.

c) Instalar en su PC el certificado de nuestra AC.

d) Instalar en su PC el certificado de la FNMT.

485.- La clave privada no deja de ser un archivo que su poseedor usa en diferentes operaciones criptográficas. Identifica cuál de estas afirmaciones es correcta:

a) La clave privada no sirve de nada sin la clave pública, por lo que puede ser almacenada sin especial cuidado en cualquier almacén de archivos (disco duro, unidad USB, etc.).

b) El usuario debe ser muy cuidadoso con la clave privada. Se recomienda almacenarla en un sitio o soporte seguro, y protegerla con una contraseña-PIN que sea imprescindible usar cada vez que se use.

c) La clave privada está desde el momento de su generación protegida por una contraseña, que debe facilitarse para poder usarla.

d) La clave privada va ligada al hardware del dispositivo en el que está instalada. Por lo tanto, un robo de la misma es inútil porque no funcionará en otro dispositivo.

486.- Identifica cuál de estas afirmaciones sobre firma digital es CIERTA . Sea "D" el documento a firmar. H=hash(D) su resumen digital.

a) El/la usuario/a firmante calcula el resumen digital del documento y lo firma con su clave privada. Junto al documento firmado se incluye su certificado digital, lo que permite verificar la firma y la identidad del firmante. El resultado es un documento en claro (no cifrado).

b) El/la usuario/a firmante calcula el resumen digital del documento y lo cifra con su clave privada. El resultado es un documento completamente cifrado que solo puede ser leído por quien tenga la clave pública del firmante.



c) El/la usuario/a firmante utiliza la clave pública de la AC para firmar el resumen digital del documento, garantizando así la autenticidad del firmante.

d) El/la usuario/a firmante cifra el documento completo con la clave pública de la AC y añade su certificado digital, lo que garantiza la autenticidad e integridad del documento.

487.- En el contexto de la comunicación con el servicio https://imagenes.os.org utilizando un sistema NGINX SSL Termination, identifica ¿cuál de estas afirmaciones es FALSA?

a) Solo es necesario configurar correctamente el servicio HTTPS (TLS) en una máquina.

b) Los 8 servidores internos tendrán menos carga de trabajo, al no tener que lidiar con cifrado/descifrado de información, validaciones, etc.

c) Solo es necesaria una dirección IP pública.

d) Sigue siendo necesario usar round-robin DNS sobre el nombre "imágenes.os.org" para distribuir la carga entre los 8 servidores reales.

488.- En el contexto del servicio https://imagenes.os.org con NGINX SSL Termination, ¿qué función realiza el equilibrador de carga?

a) Cifra las comunicaciones internas entre los servidores backend.

b) Gestiona las conexiones HTTPS externas y distribuye el tráfico a los servidores internos.

c) Genera certificados digitales para los servidores internos.

d) Verifica la identidad de los usuarios que acceden al servicio.

489.- Un/a usuario/a corporativo/a accede al servicio web y observa que el certificado del servidor ha expirado. ¿Qué ocurrirá?

a) El navegador permitirá la conexión sin mostrar ningún aviso.

b) La conexión será rechazada automáticamente sin posibilidad de continuar.

c) El navegador mostrará un aviso de seguridad indicando que el certificado no es válido.

d) El servidor renovará automáticamente el certificado sin intervención.

490.- ¿Cuál es una ventaja de utilizar HTTPS en los servicios web de la organización sanitaria?

a) Reduce el consumo de ancho de banda al comprimir los datos.

b) Permite autenticar al servidor y proteger la confidencialidad de la comunicación.

c) Evita la necesidad de utilizar certificados digitales.



d) Garantiza que los usuarios estén autenticados en todos los casos.

491.- En el contexto de usar los servicios de nuestra PKI para conseguir que la comunicación de/con los dispositivos IoT de nuestra organización sanitaria sea segura, identifica ¿cuál de estas afirmaciones es FALSA?

a) TLS con certificados IoT proporciona cifrado fuerte y protege la información confidencial compartida entre dispositivos IoT.

b) TLS con certificados IoT aporta autenticación e integridad a las comunicaciones entre dispositivos IoT.

c) Cuando un certificado IoT queda invalidado, solo se necesita que la AC genere uno nuevo y sea enviado al dispositivo por la red, sin necesidad de cifrar nada, porque la información transferida no es sensible.

d) Las plataformas CMS (Certificate Management System) están diseñadas para gestionar todo el ciclo de vida de los certificados IoT (instalación, revocación, renovación, etc.).

492.- En el contexto de dispositivos IoT que utilizan certificados digitales para comunicarse mediante TLS, ¿cuál de las siguientes afirmaciones es CORRECTA?

a) Los certificados permiten establecer comunicaciones cifradas y autenticar los dispositivos.

b) Los certificados se utilizan únicamente para cifrar los datos, pero no para autenticación.

c) TLS elimina la necesidad de gestionar certificados en los dispositivos IoT.

d) Solo es necesario instalar certificados en los servidores, no en los dispositivos.

493.- Dado que los dispositivos IoT pueden ser numerosos y de difícil acceso físico, ¿cuál es una práctica adecuada en la gestión de sus certificados?

a) Evitar la revocación de certificados para simplificar la gestión.

b) Utilizar sistemas centralizados para la gestión del ciclo de vida de los certificados.

c) Compartir el mismo certificado entre todos los dispositivos para facilitar la configuración.

d) No renovar los certificados para evitar interrupciones del servicio.

494.- ¿Qué problema de seguridad puede surgir si un dispositivo IoT utiliza siempre el mismo certificado sin renovación?

a) Aumenta el rendimiento del sistema.

b) Se reduce la latencia de las comunicaciones.

c) Se incrementa el riesgo si la clave privada es comprometida durante largos periodos.



d) Se evita la necesidad de confiar en la AC.

495.- Señala la afirmación FALSA si decidiéramos implementar un sistema federado sobre esta arquitectura,

a) Podría haber datos almacenados en el servidor central.

b) Podría haber datos almacenados en los dispositivos IoT.

c) Necesitaríamos una herramienta como Apache Hadoop para gestionar la distribución de los datos.

d) a), b), y c) son correctas

496.- ¿Qué tipo de datos podríamos encontrarnos en este sistema?

a) De baja latencia, por ejemplo, los monitores de los pacientes.

b) De baja latencia, por ejemplo, una base de datos con historiales médicos de pacientes.

c) No estructurados, como una base de datos MySQL con datos personales de pacientes.

d) Apache HBase.

497.- ¿Qué tipo de procesamiento de datos sería más adecuado para los datos generados por un dispositivo IoT?

a) OLTP.

b) Apache Hadoop.

c) Apache Hive.

d) a), b), y c) son correctas

498.- Si decidiéramos migrar el sistema descrito a la nube,

a) Podríamos migrar solo el almacenamiento de los datos, realizando el procesado en servidores locales.

b) Podríamos migrar solo el procesado de los datos, realizando el almacenamiento en servidores locales.

c) Podríamos migrar tanto el procesado como el almacenamiento de los datos.

d) No podríamos realizar el migrado, puesto que los datos provienen de fuentes distintas, generando así datos no estructurados, incompatibles con la nube.



499.- Un ejemplo de aplicación Big Data con objetivo de mantenimiento predictivo podría consistir en

a) El uso de técnicas Big Data para mantener la coherencia de los datos de los distintos dispositivos IoT.

b) El uso de técnicas Big Data para la predicción de problemas en los pacientes.

c) El uso de técnicas Big Data para la predicción de problemas en los monitores de los pacientes.

d) El uso de técnicas Big Data para mantener las previsiones de uso de recursos hospitalarios estables.

500.- ¿Cuál de estos sistemas podría ser adecuado para el almacenamiento de los datos generados por los dispositivos IoT?

a) Apache Hbase.

b) MapReduce.

c) Apache Pig.

d) Support Vector Machines.