| | |
|---|---|
| **CONVOCATORIA** | FUNCIONARIO INTERINO SIN PLAZA PARA LA EJECUCIÓN DEL PROGRAMA DE CARÁCTER TEMPORAL "OFICINA TÉCNICA DE ASISTENCIA TECNOLÓGICA PARA LOS AYUNTAMIENTOS DE LA PROVINCIA" |
| **PLAZA/PUESTO** | COORDINADOR/A DE PROYECTOS |
| **TIPO** | PRIMER EJERCICIO –TEST |
| **FECHA** | 25/03/2025 |

**1. El artículo 9.3 de la Constitución Española de 1978 garantiza, entre otros, los principios de:**

a) Legalidad, jerarquía normativa e imparcialidad.
b) Seguridad jurídica, publicidad de las normas y celeridad.
c) Jerarquía normativa, legalidad y seguridad jurídica.
d) Retroactividad de las disposiciones sancionadoras, publicidad de las normas y jerarquía normativa.

**2. La competencia de la Diputación relativa a la prestación de servicios de administración electrónica y contratación centralizada se llevará a cabo:**

a) En los municipios con población inferior a 50.000 habitantes.
b) En los municipios con población inferior a 20.000 habitantes.
c) En los municipios con población superior a 50.000 habitantes.
d) En los municipios con población superior a 20.000 habitantes

**3. Corresponde en todo caso al Pleno de la Diputación:**

a) La alteración de la calificación jurídica de los bienes de dominio público.
b) Aprobar la oferta de empleo público.
c) Asegurar la gestión de los servicios propios de la Comunidad Autónoma cuya gestión ordinaria esté encomendada a la Diputación.
d) Ninguna es correcta.

**4. Son competencias propias de la Diputación,**

a) La prestación de los servicios de recogida de residuos en los municipios de menos de 5.000 habitantes, cuando éstos no procedan a su prestación.
b) La prestación de los servicios de prevención y extinción de incendios en los municipios de menos de 20.000 habitantes, cuando éstos no procedan a su prestación.
c) La prestación de los servicios de recogida de residuos en los municipios de más de 5.000 habitantes, cuando éstos no procedan a su prestación.
d) Son correctas a y b.

**5. En el ámbito de los funcionarios de carrera de la Administración Local, la Escala de Administración General se divide en las subescalas siguientes:**

a) Técnica, de gestión, administrativa, auxiliar y subalterna.
b) Técnica, de gestión, administrativa, auxiliar y de servicios especiales.
c) Técnica, de gestión, administrativa, auxiliar y de oficios.
d) Ninguna es correcta.

**6. Según la norma UNE-ISO 21500:2012, ¿cuál de las siguientes afirmaciones describe mejor el propósito de esta norma?:**

a) Proporcionar una guía sobre la gestión de proyectos, incluyendo conceptos y procesos de alto nivel aplicables a la mayoría de los proyectos.
b) Definir requisitos específicos para la certificación de proyectos y garantizar su éxito.
c) Establecer metodologías rígidas y obligatorias para la dirección de proyectos en cualquier industria.
d) Regular el uso de software de gestión de proyectos para garantizar su compatibilidad con estándares internacionales.

**7. En ITIL V3, ¿qué es un OLA?:**

a) Es un contrato entre un proveedor de servicios de TI con un único cliente externo a la organización.
b) Es un contrato entre departamentos de una misma organización.
c) Es un contrato entre un proveedor de servicios de TI que describe los servicios ofertados a varios clientes externos a la organización.
d) Es un contrato entre la administración y la empresa privada.

**8. En la metodología de gestión de servicios ITIL, ¿cuál es el término utilizado para describir la funcionalidad ofrecida por un servicio?:**

a) Riesgo.
b) Utilidad.
c) Garantía.
d) Coste.

**9. ¿Cuál de las siguientes afirmaciones describe correctamente el propósito principal de la Norma UNE-ISO 27001:2023?:**

a) Proporcionar directrices para la implementación de redes informáticas seguras en una organización.
b) Establecer un marco de referencia para la gestión de la seguridad de la información, incluyendo requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).

c) Definir estándares técnicos para la encriptación de datos en entornos empresariales.
d) Regular el cumplimiento legal de las empresas en materia de ciberseguridad en la Unión Europea.

**10. ¿En cuáles de los siguientes estados puede encontrarse el protocolo de acceso al medio Carrier Sense Multiple Access with Collision Detection (CSMA/CD)?:**

a) Período de espera, período de contienda, período de transmisión y período sin carga.
b) Período de espera, período de contienda, período de contención y período sin carga.
c) Período de espera, período de contención, período de transmisión y período sin carga.
d) Período de contienda, período de transmisión y período sin carga.

**11. ¿Cuáles de los siguientes protocolos se corresponden con un protocolo para la conexión entre sistemas autónomos?:**

a) SLP2 (Standalone Linking Protocol).
b) SGP2 (Standalone Gateway Protocol).
c) BGP4 (Border Gateway Protocol).
d) OSPF.

**12. ¿Cuál es el puerto por defecto para el servicio de Escritorio Remoto (RDP)?:**

a) 3389/TCP.
b) 3389/UDP.
c) 2389/TCP.
d) 2389/UDP.

**13. En referencia a los distintos servicios en la nube o cloud computing, ¿Cómo se llamaría el sistema en el cual se nos permite gestionar el entorno de virtualización?:**

a) SaaS.
b) PaaS.
c) IaaS.
d) On-site.

**14. ¿Cuáles son las categorías de Cloud en función del rol y el control que ejercen usuario y prestador?:**

a) Privada, pública, híbrida y en comunidad.
b) IaaS, PaaS y SaaS.
c) Agile, devops y container.
d) Ninguna de las respuestas anteriores es correcta.

**15. En un sistema de gestión de incidencias, ¿cuál de las siguientes opciones representa la mejor práctica para garantizar la trazabilidad y resolución eficiente de los problemas?:**

a) Resolver las incidencias de forma inmediata sin registrar detalles para agilizar el proceso.
b) Clasificar, priorizar y documentar cada incidencia, asegurando su seguimiento hasta su resolución.
c) Permitir que los usuarios resuelvan las incidencias por su cuenta sin intervención del equipo de soporte.
d) Cerrar automáticamente las incidencias que no se resuelvan en un plazo de 24 horas para mantener el sistema limpio.

**16. ¿Cuál de los siguientes corresponde al algoritmo de criptografía simétrica y cifrado por bloques diseñado, entre otros, por Bruce Schneier, que tiene un diseño simple y de tipo Feistel, que puede utilizarse en varias plataformas y en algunas versiones de PGP, que cuenta con una seguridad demostrada y no exhibe claves débiles, cuya longitud de bloque es de 128 bits y su longitud de clave es variable?:**

a) TWOFISH.
b) SERPENT.
c) RC6.
d) AES.

**17. En relación con las técnicas de detección de software malicioso mediante heurística, indique cuál es la afirmación correcta:**

a) Las técnicas heurísticas de tipo pasivo crean un entorno seguro donde ejecutar el código malicioso; de esta forma, se puede conocer cuál es el comportamiento del código. Este tipo de heurística se apoya en técnicas como el sandbox, la virtualización o la emulación.
b) Con las técnicas heurísticas de tipo activo, se exploran los archivos tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, se detecta como malicioso.
c) Con las técnicas heurísticas genéricas, se analiza cuán similar es un objeto a otro que ya se conoce como malicioso. Si un archivo es lo suficientemente similar a un código malicioso previamente identificado, será detectado como una posible variante.
d) Todas las afirmaciones son correctas.

**18. ¿Qué tipo de virus consiste en una combinación de virus de archivo, de macro y de sector de arranque, que realizan infecciones utilizando varias técnicas para instalarse en cualquiera de las ubicaciones posibles y se consideran muy peligrosos debido a su gran capacidad de infección?:**

a) Bimodales.
b) Parásitos.
c) Retrovirus.
d) Multimodo.

**19. ¿Cuál es la función principal de un Centro de Distribución de Claves (KDC) en un sistema de autenticación?:**

a) Generar y distribuir claves simétricas para la comunicación segura entre los usuarios y servicios.
b) Almacenar y gestionar las contraseñas de los usuarios en un directorio centralizado.
c) Cifrar los datos en tránsito para garantizar la confidencialidad en la comunicación.
d) Actuar como un firewall para proteger la red de accesos no autorizados.

**20. ¿Cuál de las siguientes tecnologías no sirve para la implementación de redes privadas virtuales?:**

a) SSH.
b) SLIP.
c) IPSEC.
d) SSL/TLS.

**21. ¿Cuál de las siguientes afirmaciones sobre la firma electrónica es correcta?:**

a) La firma electrónica se basa únicamente en el uso de contraseñas para autenticar al usuario.
b) La firma electrónica avanzada garantiza la integridad del documento y la identidad del firmante.
c) Una firma electrónica es siempre equivalente a una firma manuscrita en términos legales.
d) La firma electrónica avanzada garantiza la integridad del documento, pero no la identidad del firmante.

**22. ¿Cuál de las siguientes afirmaciones sobre la tecnología Fibre Channel es correcta?:**

a) Fibre Channel es un protocolo de red diseñado principalmente para la transmisión de voz sobre IP.
b) Fibre Channel utiliza exclusivamente cableado de fibra óptica, sin posibilidad de emplear otros medios físicos.
c) Fibre Channel permite la conexión de dispositivos de almacenamiento a alta velocidad y se usa comúnmente en SAN (Storage Area Networks).
d) Fibre Channel es un protocolo de red que reemplazó completamente a Ethernet en entornos empresariales.

**23. En una infraestructura SAN, ¿cuál de los siguientes elementos es fundamental para garantizar la redundancia y disponibilidad del almacenamiento?:**

a) El uso de discos duros SSD en todos los nodos de almacenamiento.
b) La implementación de múltiples caminos (multipathing) entre los servidores y los dispositivos de almacenamiento.
c) La conexión de la SAN a una red Wi-Fi de respaldo para evitar interrupciones.
d) La configuración de un único switch Fibre Channel con enlaces de alta velocidad.

**24. En un sistema operativo multitarea, con 8 Kbytes de espacio lógico de proceso, con páginas de 1 Kbytes y 32 Kbytes de memoria física y sin memoria virtual, la tabla de páginas ocupará:**

a) 8*5 bits.
b) 32*3 bits.
c) 32*5 bits.
d) 8*3 bits.

**25. Por las características del sistema de almacenamiento necesario para nuestra organización, se va a implementar en las cabinas de almacenamiento un sistema RAID 101. ¿Cuántos discos rígidos serán necesarios como mínimo para poder formar este grupo RAID?:**

a) 4.
b) 6.
c) 8.
d) No existe el RAID 101.

**26. En un sistema de almacenamiento basado en arquitectura Scale-Out, ¿cuál de los siguientes mecanismos es fundamental para garantizar la coherencia de los datos y el equilibrio de carga entre nodos?:**

a) Implementación de un sistema de hashing distribuido (DHT) para la asignación de bloques de datos entre nodos.
b) Uso de un único nodo maestro que gestiona todas las operaciones de lectura y escritura en el sistema.
c) Dependencia exclusiva de un RAID tradicional para gestionar la redundancia y distribución de datos.
d) Configuración de un servidor centralizado que almacena metadatos y dirige todas las peticiones de acceso a los nodos de almacenamiento.

**27. ¿Cuál de los siguientes métodos de detección utiliza un antivirus para identificar software malicioso basado en su comportamiento en lugar de firmas específicas?:**

a) Análisis heurístico.
b) Comparación de firmas digitales.
c) Lista blanca de aplicaciones.
d) Escaneo basado en hashes criptográficos.

**28. ¿Cuál de los siguientes protocolos de tunelización es ampliamente utilizado en VPNs debido a su seguridad y capacidad de cifrado de extremo a extremo?:**

a) PPTP (Point-to-Point Tunneling Protocol).
b) L2TP/IPSec (Layer 2 Tunneling Protocol con IPSec).

c) FTP (File Transfer Protocol).
d) SNMP (Simple Network Management Protocol).

**29. ¿Cuál es la principal diferencia entre un hipervisor de tipo 1 y un hipervisor de tipo 2?:**

a) Un hipervisor de tipo 1 se ejecuta directamente sobre el hardware, mientras que un hipervisor de tipo 2 se ejecuta sobre un sistema operativo anfitrión.
b) Un hipervisor de tipo 1 siempre requiere una conexión a Internet para funcionar, mientras que un hipervisor de tipo 2 puede operar sin conexión.
c) Un hipervisor de tipo 1 es utilizado solo en entornos domésticos, mientras que un hipervisor de tipo 2 es exclusivo para servidores empresariales.
d) Un hipervisor de tipo 1 necesita un sistema operativo base para gestionar las máquinas virtuales, mientras que un hipervisor de tipo 2 se ejecuta directamente sobre el hardware.

**30. En un entorno de virtualización con hipervisores de tipo 1, ¿qué técnica se utiliza para reducir la sobrecarga de traducción de direcciones de memoria y mejorar el rendimiento de las máquinas virtuales?:**

a) VT-d (Intel Virtualization Technology for Directed I/O), que permite la virtualización de dispositivos de entrada/salida para mejorar el rendimiento de los accesos directos.
b) SLAT (Second Level Address Translation), que optimiza la gestión de la memoria virtual al reducir la sobrecarga en la tabla de páginas del hipervisor.
c) Ballooning Memory, que permite al hipervisor asignar dinámicamente memoria entre máquinas virtuales según la demanda.
d) Nested Virtualization, que habilita la ejecución de un hipervisor dentro de una máquina virtual para entornos de pruebas.

**31. En un entorno de virtualización con un hipervisor de tipo 1, ¿qué mecanismo permite la comunicación eficiente entre máquinas virtuales sin necesidad de pasar por la capa de red física?:**

a) SR-IOV (Single Root I/O Virtualization), que permite a las máquinas virtuales acceder directamente a dispositivos de red físicos compartidos sin intervención del hipervisor.
b) VMDq (Virtual Machine Device Queues), que mejora la eficiencia del procesamiento de paquetes de red en entornos virtualizados mediante colas de hardware.
c) VMX (Virtual Machine Extensions), que habilita la ejecución de instrucciones privilegiadas en entornos virtualizados con menor sobrecarga.
d) VSwitch (Virtual Switch), que permite la interconexión de máquinas virtuales dentro del hipervisor sin depender de hardware de red físico.

**32. Dentro del ciclo de mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001, ¿cuál es la fase en la que se implementan los controles de seguridad y se ejecutan las políticas definidas?:**

a) Plan (Planificar) – Se identifican los riesgos y se establecen políticas de seguridad.
b) Do (Hacer) – Se implementan los controles de seguridad y se ejecutan las políticas establecidas.
c) Check (Verificar) – Se monitorizan y auditan los controles para evaluar su eficacia.
d) Act (Actuar) – Se realizan correcciones y mejoras basadas en los resultados de las auditorías.

**33. En el marco de ITIL, ¿cuál es el principal objetivo del proceso de Gestión del Cambio?:**

a) Garantizar que todas las solicitudes de cambio (RFC) sean aprobadas automáticamente para agilizar la implementación de servicios.
b) Controlar el ciclo de vida de los cambios para minimizar riesgos e interrupciones en los servicios de TI.
c) Desarrollar nuevos servicios sin necesidad de documentación ni aprobación formal.
d) Eliminar la necesidad de pruebas en los cambios para acelerar la entrega de nuevas funcionalidades.

**34. Según ITIL, ¿qué tipo de cambio requiere una evaluación completa de riesgos, pruebas, planificación y aprobación antes de su implementación?:**

a) Cambio estándar – Se trata de un cambio preautorizado con bajo riesgo y repetitivo.
b) Cambio normal – Necesita una evaluación completa y aprobación formal antes de su implementación.
c) Cambio de emergencia – Se implementa con rapidez debido a una incidencia crítica.
d) Cambio operacional – Se refiere a ajustes menores que no requieren una evaluación de riesgos.

**35. El EtherType del protocolo FCoE (Fiber Channel Over Ethernet) es:**

a) 0x8906.
b) 0x0806.
c) 0x0906.
d) 0x89DD.

**PREGUNTAS DE RESERVA**

**36. El artículo 7 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales, establece que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de:**

a) Doce años
b) Catorce años

c) Quince años
d) Dieciséis años

**37. ¿Cuál de las siguientes opciones representa una amenaza para la seguridad física de un centro de procesamiento de datos (CPD)?:**

a) Un ataque de malware a un servidor.
b) Un incendio en la sala de servidores.
c) Un error en la configuración de un firewall.
d) Una brecha de seguridad en una base de datos.

**38. ¿Cuál de las siguientes afirmaciones es correcta respecto a la diferencia entre la criptografía de clave simétrica y asimétrica?:**

a) En la criptografía de clave simétrica, se usan dos claves diferentes: una para cifrar y otra para descifrar.
b) La criptografía de clave asimétrica es más eficiente en términos de velocidad que la criptografía de clave simétrica.
c) En la criptografía de clave asimétrica, se utiliza un par de claves (pública y privada) para cifrar y descifrar los datos.
d) La criptografía de clave simétrica es más segura que la criptografía de clave asimétrica para el intercambio de claves.

**PROCESO SELECTIVO CONVOCADO PARA O NOMEAMENTO INTERINO SEN PRAZA DUN/HA COORDINADOR/A DE PROXECTOS PARA A EXECUCIÓN DO PROGRAMA DE CARÁCTER TEMPORAL "OFICINA TÉCNICA DE ASISTENCIA TECNOLÓXICA PARA OS CONCELLOS DA PROVINCIA"**

**RESPOSTAS DO TEST**

| | | | |
|---|---|---|---|
| **1** | C | **21** | B |
| **2** | B | **22** | C |
| **3** | A | **23** | B |
| **4** | B | **24** | A |
| **5** | A | **25** | C |
| **6** | A | **26** | A |
| **7** | B | **27** | A |
| **8** | B | **28** | B |
| **9** | B | **29** | A |
| **10** | D | **30** | B |
| **11** | C | **31** | D |
| **12** | A | **32** | B |
| **13** | D | **33** | B |
| **14** | A | **34** | B |
| **15** | B | **35** | A |
| **16** | A | **RESERVA** | |
| **17** | C | **36** | B |
| **18** | A | **37** | B |
| **19** | A | **38** | C |
| **20** | B | | |