Ayuntamiento de Vitoria-Gasteiz
Vitoria-Gasteizko Udala
www.vitoria-gasteiz.org

CÓDIGO PRUEBA: TE9093011

TE9 - TÉCNICOS/AS. COMUNICACIONES

PRIMER EJERCICIO
SEGUNDA PRUEBA

Tiempo máximo: 50 minutos
Preguntas: 50.

MODELO / EREDUA:	**A**

INSTRUCCIONES

- No abra este cuadernillo hasta que se le indique.
- Siga leyendo estas instrucciones.
- Escriba: el DNI y la LETRA y rellene las casillas para su lectura óptica.
- Escriba: 1er APELLIDO, 2º APELLIDO, NOMBRE y FECHA.
- En EXAMEN escriba el Código de examen que aparece en la parte superior.
- Marque en su hoja de respuestas el MODELO de examen que le haya correspondido.
- Recuerde:
    - 50 preguntas con 4 alternativas de respuesta.
    - Una única alternativa válida. Si hay más de una, la más general o completa, excepto si en el enunciado se solicita "Seleccione el enunciado FALSO" en cuyo caso, tres serán ciertos y hay que marcar el que no lo es, el falso.
    - Duración de la prueba: 50 minutos.
    - Acierto: Un punto (1,00).
    - Errores, nulos, dobles o blancos: NO penalizan.
    - La ausencia de marca o la marca incorrecta en el modelo invalida prueba.
- No se entregaran nuevas hojas de respuesta en los últimos 5 minutos del ejercicio.
- Se podrán solicitar la recogida del examen transcurridos los primeros 30 minutos.
- Cuando se le indique, separe la hoja blanca de la copia amarilla de su hoja de respuestas. La blanca se entrega al personal de la organización.
- La copia amarilla y la hoja de instrucciones quedarán en su poder.
- Podrá descargar el cuadernillo de esta prueba en la página web de procesos selectivos, junto con la plantilla provisional de respuestas, cuando el Tribunal determine su publicación.

Gracias por su colaboración

1. ¿Cuál de estas denominaciones NO corresponde a un estándar Ethernet?

a) 100Base-T.

b) 10Base-SX.

c) 10GBase-T.

d) 1000Base-SX.

2. Sobre la seguridad de los navegadores:

a) Una página web no puede infectar un equipo por el mero hecho de visitarla.

b) Las cookies no pueden ser leídas por otra página distinta que aquella que la generó, por lo que no suponen un problema de seguridad sino sólo de privacidad.

c) No bloquear los elementos emergentes es una mala práctica.

d) El nivel de configuración de la seguridad y el de la privacidad no pueden configurarse de manera independiente y deben ser el mismo.

3. El estándar 802: (señale el enunciado FALSO)

a) Admite cableado apantallado y no apantallado.

b) Establece las velocidades admitidas por el medio de transmisión.

c) Puede utilizar PoE.

d) Admite fibra óptica, cable de cobre de par trenzado y radio.

4. Sobre DNS: (señale el enunciado FALSO)

a) El sistema de resolución de nombres de dominio en Internet es descentralizado.

b) Todos los servidores DNS contienen la base de datos completa de resolución de nombres de Internet.

c) Se puede utilizar cualquier servidor DNS de Internet disponible.

d) Los servidores DNS son los encargados de traducir una dirección web o dominio por la IP a la que corresponde para poder conectarnos a ella.

5. Para la gestión de infraestructuras TIC pueden utilizarse las siguientes herramientas: (señale el enunciado FALSO)

a) Equipos de analistas-programadores.

b) Recursos humanos propios de la organización.

c) Acuerdos de nivel de servicio.

d) Contratos de servicios gestionados.

6. Señale el enunciado FALSO sobre Spanning Tree Protocol:

a) RSTP evita la tormenta de broadcast.

b) STP o RSTP evitan bucles o loops en una red LAN que tenga enlaces redundantes.

c) STP utiliza las direcciones IP de las tramas para evitar enlaces redundantes.

d) Los modelos más recientes de Cisco IOS tienen por defecto RSTP en lugar de STP.

7. Son comandos de red CMD: (señale el enunciado FALSO)

a) Ipconfig.

b) sfc.

c) getmac.

d) tracert.

8. Respecto a los routers, sus protocolos y su configuración:

a) Los routers Cisco más recientes no admiten rutas estáticas debido a sus algoritmos mejorados.

b) La tabla de rutas indica cuál es el siguiente router en el camino.

c) RIP y OSPF son protocolos de cálculo de rutas.

d) Un router puede realizar traducción de direcciones de red (NAT) estática y dinámica.

9. Se denomina comúnmente resolución Full HD a:

a) 1280 x 720 píxeles (16:9).

b) 1920 x 1080 píxeles (16:9).

c) 3840 x 2160 píxeles (16:9).

d) 7680 x 4320 píxeles (16:9).

10. Los radioenlaces punto a punto se pueden utilizar en general para: (señale el enunciado FALSO)

a) El acceso a Internet.

b) Conectar dos segmentos Ethernet de cobre.

c) Conectar a Ethernet múltiples dispositivos mediante protocolo 802.11.

d) Conectar dos segmentos Ethernet de fibra.

11. Respecto a firewalls stateful y stateless: (señale el enunciado FALSO)

a) Los firewalls stateless pueden detectar cuando se están utilizando datos ilícitos para infiltrarse en la red.

b) Los firewalls Stateful examinan el comportamiento de los paquetes y si parece anómalo, pueden filtrar los datos sospechosos.

c) Un firewall stateful se puede utilizar en el interior de una red.

d) Un firewall stateful puede ser comprometido por alguna vulnerabilidad, a no ser que se mantenga actualizado con las últimas actualizaciones.

12. ¿Cuál de las siguientes NO es una tecnología de telefonía móvil?:

a) HSPA.

b) GPRS.

c) HSDPA.

d) CSMA/CD.

13. En cuanto a comunicaciones móviles:

a) las redes de comunicaciones de telefonía móvil dividen el territorio en pequeñas celdas, donde despliegan antenas repetidoras.

b) Una de las ventajas de 5G es la reducción de la latencia.

c) La tecnología 5G no podrá utilizarse para IoT.

d) La tecnología UMTS utiliza ondas de la banda en torno a 2100 MHz.

14. Los puntos de acceso inalámbricos de Aruba: (señale el enunciado FALSO)

a) Existen para interiores, exteriores, remoto.

b) Ofrecen funciones avanzadas como segmentación estática.

c) Utilizan cifrado para usuarios e invitados.

d) Soportan diversos estándares Wi-Fi.

15. Respecto a la configuración del correo electrónico en el móvil: (señale el enunciado FALSO)

a) POP3 permite consultar el correo descargado incluso sin acceso a red.

b) Los puertos por defecto para POP3 son: 110 (no cifrado) y 995 (cifrado).

c) El tipo de seguridad a aplicar en la configuración viene determinado por el tipo de cliente de correo móvil que se decida utilizar.

d) IMAP permite consultar el correo descargado incluso sin acceso a red si se activa tal opción de configuración.

16. Las extensiones del navegador Microsoft Edge son:

a) Barras de botones que se pueden instalar en el navegador.

b) Compatibles con todos los demás navegadores del mercado.

c) El lugar donde se almacenan los certificados digitales en Microsoft Edge.

d) Pequeños programas que un desarrollador usa para agregar o modificar características de Microsoft Edge.

17. En la configuración de un dispositivo móvil: (señale el enunciado FALSO)

a) Bluetooth no se considera suficientemente seguro por no poder utilizar cifrado.

b) Una vez asignado, es posible cambiar el nombre del dispositivo en protocolo Bluetooth.

c) En WiFi, el dispositivo tiene una dirección MAC.

d) En WiFi, el dispositivo tiene una dirección IP.

18. Señale el framework para VoIP no propietario (open source):

a) Alcatel-Lucent.

b) Asterisk.

c) Cisco.

d) Avaya.

19. En cuanto a VoIP: (señale el enunciado FALSO)

a) Es un protocolo.

b) Permite realizar llamadas a través de cualquier tipo de conexión.

c) Requiere una centralita on-premise.

d) Se puede utilizar en teléfonos fijos.

20. El comando para mostrar la configuración TCP/IP de un PC con Windows 10 es:

a) Ipconfig.

b) netsh show ip.

c) netstat.

d) tracert.

21. En cuanto a switches de capa 2 y switches de capa 3:

a) Los switches de Capa 3 manejan el inter-VLAN routing.

b) Un switch de Capa 2 puede asignar VLANs a puertos de switches específicos que a su vez se encuentran presentes en diferentes subredes de la Capa 3.

c) Un switch de Capa 3 dispone de una tabla de direcciones MAC y de una tabla de enrutamiento IP.

d) La Capa 2 proporciona transferencia directa de datos entre dos dispositivos dentro de una red LAN.

22. El protocolo “spanning tree” (STP) tiene como objetivo…:

a) Evitar bucles.

b) Detectar bucles.

c) Eliminar paquetes duplicados.

d) Seleccionar el camino adecuado entre 2 bucles.

23. Los equipos WiFi cumplen con el estándar IEEE:

a) 802.1

b) 802.2

c) 802.3

d) 802.11

24. Las VLAN: (señale el enunciado FALSO)

a) están aisladas entre sí.

b) son redes virtuales mediante las cuales una red física existente puede dividirse en varias redes lógicas.

c) su uso no afecta a la seguridad de la red.

d) en las VLAN basadas en puertos, cada puerto no puede asignarse a varias VLAN.

25. Un ataque en el que un ciberdelincuente trata de obtener nombres de usuario y contraseña, haciendo que su víctima introduzca información confidencial en un sitio web falso que tiene el aspecto de uno legítimo es un ataque de tipo:

a) Man-in-the-middle.

b) Phishing.

c) Mail spoofing.

d) Zero day.

26. En la clasificación TIER:

a) Las definiciones de TIER establecen opciones de diseño específicas para cumplir los requisitos del TIER.

b) En un centro de datos de TIER I se dispone de depósitos de combustible.

c) Los TIER son progresivos: cada nivel contiene las especificaciones del anterior.

d) En un centro de datos de TIER II, un apagado imprevisto no afectará al sistema.

27. Nagios permite monitorizar el tráfico para el/los siguiente/s protocolo/s:

a) SMTP, POP3.

b) HTTP, HTTPS.

c) SNMP.

d) Todos los anteriores.

28. Según el Esquema nacional de seguridad:

a) El análisis de riesgos no se debe realizar para sistemas de categoría BASICA.

b) La función diferenciada es un principio básico.

c) Para reducir, eliminar, mitigar o transferir los riesgos se aplicarán preferentemente medidas compensatorias.

d) La reducción de los niveles de riesgo se consigue con la realización del análisis de riesgos.

29. ¿Cuál de estas medidas o sistemas de seguridad es reactiva?:

a) Encriptación.

b) Antivirus de endpoint.

c) Backup.

d) Firewall.

30. Técnicamente, respecto a certificado digital y firma digital:

a) Para firmar un documento digitalmente es necesario disponer de un certificado digital.

b) La firma digital es un medio para demostrar la identidad del titular de una determinada transacción electrónica.

c) Los certificados digitales válidos para operar con la administración son emitidos por prestadores de servicios de certificación, mientras que las firmas digitales no.

d) Certificado digital y firma digital es lo mismo.

31. Sobre la seguridad en el correo electrónico: (señale el enunciado FALSO)

a) Los filtros antispam de cliente de correo son incompatibles con los de servidor.

b) Si hay un enlace incluido en un correo, se recomienda inspeccionarlo previamente, acercando el ratón.

c) Es conveniente desactivar HTML en el cliente de correo.

d) Un ciberdelincuente puede ocultar su identidad, falsificando su dirección como remitente con la de otro usuario real.

32. ¿Cómo protegerse ante amenazas zero day?: (señale el enunciado FALSO)

a) Mediante un antivirus instalado en el endpoint y correctamente actualizado.

b) Manteniendo los PC actualizados.

c) Mediante sistemas basados en análisis de comportamiento.

d) Manteniendo políticas de instalar sólo el software necesario.

33. En anti-spoofing: (señale el enunciado FALSO)

a) Firewalls, routers o gateways pueden tener instaladas herramientas anti-spoofing que examinen paquetes entrantes.

b) Las herramientas anti-spoofing pueden permitir exclusiones de pares de direcciones “IP origen-IP destino”.

c) Un ataque de IP spoofing da al atacante acceso al tráfico de datos.

d) Las herramientas anti-spoofing aumentan la protección contra ataques DoS y DDoS.

34. Una solución de filtrado web: (señale el enunciado FALSO)

a) Puede utilizar blacklists y whitelists.

b) Funciona en base a palabras clave restringidas.

c) No requiere administración, pues el algoritmo automatiza la gestión.

d) Puede formar parte de la solución general de seguridad.

35. VPN Ipsec vs VPN SSL: (señale el enunciado FALSO)

a) VPN SSL requiere un software de usuario dedicado.

b) IPSec es un protocolo de nivel de red.

c) La aplicación ideal es que la empresa conecte la sede y las sucursales a través de la VPN IPSec, y el servicio de acceso VPN SSL se proporcione para empleados de oficinas móviles o empleados en viajes de negocios.

d) IPSec proporciona un mecanismo de seguridad de alta calidad y basado en cifrado que se puede usar en conjunto para la red IPv4 / IPv6.

36. Para poder utilizar con la mayor seguridad posible una VPN desde un equipo, es recomendable: (señale el enunciado FALSO)

a) Mantener el sistema operativo del equipo cliente actualizado.

b) Utilizar la cuenta habitual del usuario para conectarse.

c) Mantener actualizado el cliente VPN del equipo.

d) Conectar por cable cuando sea posible para reforzar la seguridad.

37. En la gestión de incidencias: (señale el enunciado FALSO)

a) Pueden existir varios niveles de escalado.

b) El registro de la incidencia debe realizarse una vez resuelta la misma.

c) Las métricas se utilizan para evaluar y mejorar la calidad del servicio.

d) Su objetivo es prevenir o restaurar en el menor tiempo posible cualquier interrupción no planificada o retraso que afecte a la calidad del servicio.

38. La diferencia entre IDS e IPS es:

a) IPS emite alertas, mientras que IDS mitiga la intrusión.

b) IDS sólo detecta ataques repetitivos, mientras que IPS detecta cualquier tipo de ataque.

c) IPS es vulnerable a un ataque DDoS, mientras que IDS no.

d) IPS puede descartar paquetes y desconectar conexiones, mientras que IDS no.

39. Una solución que permite a la organización realizar un seguimiento y regular el acceso a sitios web en función de sus categorías de contenido es una solución de tipo:

a) Antispam.

b) IPS.

c) Filtrado Web.

d) Control de aplicaciones.

40. Son buenas prácticas de seguridad en la configuración del correo electrónico: (señale el enunciado FALSO)

a) Marcar la opción de “Recordar contraseña” en los accesos a webmail.

b) Desactivar HTML.

c) Desactivar la ejecución de macros.

d) Configurar para el uso de estándares de cifrado como PGP o S/MIME.

41. Una solución antispam: (señale el enunciado FALSO)

a) Puede detener el correo malicioso antes de que llegue al buzón del destinatario.

b) Puede eliminar el código malicioso en un correo electrónico antes de entregarlo.

c) Puede detener el correo malicioso antes de que llegue al servidor de correo.

d) Puede estar incorporada en sistemas antivirus y en firewalls.

42. La monitorización de las comunicaciones: (señale el enunciado FALSO)

a) Requiere la definición de métricas iniciales de comportamiento normal.

b) Requiere la definición del ámbito de sistemas o servicios a monitorizar en la red.

c) Requiere herramientas específicas.

d) Requiere un SIEM.

43. En cuanto a los sistemas de control de aplicaciones: (señale el enunciado FALSO)

a) Ejecutan a nivel de endpoint.

b) Pueden controlar las aplicaciones que se ejecutan en un servidor.

c) Protegen contra amenazas Zero-Day.

d) Permiten la ejecución de goodware, aunque no esté autorizado en la política.

44. Un acuerdo de nivel de servicio:

a) Debe ser único para todos los servicios de la organización.

b) Debe establecer indicadores medibles.

c) No puede contemplar penalizaciones económicas.

d) Consiste en la definición de los tiempos-objetivo de resolución de incidencias.

45. ¿Cuál de las siguientes NO es una función del Servicio de Explotación y comunicaciones?:

a) Garantizar el correcto funcionamiento de los sistemas tras su implantación, mediante el mantenimiento correctivo, adaptativo y evolutivo de los mismos.

b) Elaborar políticas tecnológicas y de seguridad de la red.

c) Gestionar el acceso y autorizaciones a los sistemas.

d) Gestionar el parque de equipos de usuario, su inventario y mantenimiento.

46. Para distribuir en entorno Windows un paquete de software de usuario por primera vez se puede utilizar: (señale el enunciado FALSO)

a) WSUS.

b) Herramientas comerciales como ProactivaNet.

c) Instalaciones manuales en cada PC.

d) Una GPO de Active Directory.

47. Son herramientas que ayudan al diagnóstico y solución de averías en comunicaciones de red: (señale el enunciado FALSO)

a) Ping.

b) Wireshark.

c) Defrag.

d) tracert.

48. Para configurar TCP/IP en un PC que se comunicará con otras redes y que está en un entorno donde NO existe servidor DHCP, es necesario configurar:

a) Dirección IP, máscara de subred, puerta de enlace predeterminada, dirección MAC.

b) Dirección IP, máscara de subred, dirección MAC, nombre de equipo.

c) Dirección IP, máscara de subred, puerta de enlace predeterminada, servidores DNS.

d) Dirección IP, máscara de subred, servidor DNS preferido, servidor DNS alternativo.

49. Tipos de mantenimiento de sistemas informáticos: (señale el enunciado FALSO)

a) Sustractivo.

b) Preventivo.

c) Correctivo.

d) Evolutivo.

50. Comparando un switch de capa 3 y un router: (señale el enunciado FALSO)

a) Ambos pueden ejecutar enrutamiento estático y dinámico.

b) Ambos enrutan paquetes hacia la IP de destino.

c) Ambos pueden utilizarse como dispositivo único de ruteo hacia Internet.

d) Ambos son dispositivos que operan en el nivel de red.