

Preguntas

- 1) Según lo que se refiere en el apartado “9. Gestión del plan de prevención” del mismo, el Plan de prevención de la Universitat Politècnica de València debe ser aprobado por:
 - a. La Secretaría General de la UPV
 - b. La Gerencia de la UPV
 - c. El Consejo de Gobierno de la UPV
 - d. El Comité de Seguridad y Salud de la UPV
- 2) ¿Qué tiene en común todos los residuos generados en la UPV?
 - a. Que el gestor que los recoge es siempre el mismo.
 - b. Que los gestores que los recogen son siempre autorizados por la administración competente.
 - c. Que tienen el mismo procedimiento de gestión.
 - d. Que todos se generan en los tres campus de la UPV (Alcoi, Gandia y Vera).
- 3) ¿Qué debes hacer si en tu unidad se genera un residuo que no sabes cómo se debe gestionar?
 - a. Contactar con la Unidad de Medio Ambiente para que me informen de cómo debo hacerlo.
 - b. Contactar con la Conselleria con competencias en Medio Ambiente para que me informen de cómo debo hacerlo.
 - c. Depositarlo en el contenedor de basura orgánica ya que los residuos sufren un proceso de separación previo antes de depositarlo en el vertedero.
 - d. Tirarlo por el WC.
- 4) La unidad de medida de la potencia de cálculo de un microprocesador es:
 - a. Gigabyte
 - b. Flops
 - c. FPS
 - d. FBS
- 5) Según el IEEE, ¿cuál es la máxima velocidad de un puerto USB 3.0?
 - a. 4,8 Gbps
 - b. 480 Mbps
 - c. 12 Mbps
 - d. 1,8 Mbps

- 6) ¿Cuál de las siguientes afirmaciones es incorrecta?
- a. El RAID 6 considera dos discos de paridad..
 - b. Para crear un RAID 5 necesitaremos al menos 5 discos
 - c. El RAID 0 no tiene redundancia.
 - d. El RAID 1 es bastante caro porque utiliza el doble de discos de los que serían necesarios para almacenar la misma información sin redundancia.
- 7) El parámetro *alien crosstalk* o diafonía con otros cables adyacentes, es característico ¿de qué tipo de cableado UTP es característico?
- a. Categoría 5
 - b. Categoría 5e
 - c. Categoría 6a
 - d. Categoría 6e
- 8) ¿Cuál de las siguientes categorías de fibra óptica corresponde a fibra monomodo?
- a. OM3
 - b. OS1
 - c. OM4
 - d. OM5
- 9) El cableado U/FTP:
- a. Es *unshielded*, que significa que no lleva pantalla exterior, y *foiled*, que indica que cada par sí lleva apantallamiento propio.
 - b. Es *unshielded*, que significa que no lleva tipo de pantalla alguno y *foiled*, que indica que los cables están contruidos utilizando aluminio y no cobre.
 - c. La *U* indica que es el cable de cobre de toda la vida y, la *F*, que dispone de apantallamiento, tanto externo como interno, en cada par.
 - d. No existe un cableado U/FTP, solamente cables UTP o FTP.
- 10) ¿Cuál de los siguientes dispositivos de conexión de redes funciona a nivel 3 de la capa OSI?
- a. *Hubs*
 - b. *Switches* (conmutadores)
 - c. *Bridges* (puentes)
 - d. *Routers* (encaminadores)

- 11) Disponemos de una red con un único conmutador de 24 puertos y configuramos los 12 primeros en una VLAN (VLAN 1) y los 12 últimos en otra VLAN (VLAN 2). No existe otro dispositivo de red adicional. ¿Cuál de las siguientes afirmaciones **no** es correcta?
- a. Todas las estaciones podrán comunicarse entre ellas.
 - b. Las estaciones de la VLAN 1 podrán comunicarse entre ellas, pero no con las de la VLAN 2.
 - c. Las tramas *broadcast* que emita una estación de la VLAN 2 serán visibles solamente en los puertos que pertenecen a la VLAN 2.
 - d. La tabla de direcciones MAC es única, incluyendo direcciones aprendidas en las dos VLAN.
- 12) ¿En qué consiste el *flooding* (inundación) en un *switch*?
- a. Es el fenómeno que ocurre cuando se llena la tabla MAC y que tiene como consecuencia que el *switch* no funcione correctamente.
 - b. Es el fenómeno que ocurre cuando se desbordan los buffers de los puertos del *switch* y no se puede enviar tráfico por ellos.
 - c. Es la manera en que el *switch* envía las tramas dirigidas a una estación cuando la dirección MAC de la estación de destino no se encuentra en la tabla, enviando la trama a todos los puertos menos a aquel por el que se recibió.
 - d. Solamente ocurre en los *switches* que no son *wire-speed* y consiste en que todas las estaciones conectadas a él envían tráfico a la vez, no habiendo disponibilidad de canal para todo el tráfico y por tanto el *switch* se colapsa.
- 13) La dirección IP que se puede configurar en un *switch*...
- a. Es una dirección que nos permite gestionar el *switch* a través de la red.
 - b. Es necesaria para poder encaminar el tráfico de las estaciones.
 - c. No se puede configurar una dirección IP en un *switch* puesto que funcionan solamente a nivel 2.
 - d. Es obligatorio que sea de rango privado.
- 14) ¿Cómo se denomina la técnica empleada por los *switches* para solucionar la formación de bucles?
- a. *Networking*
 - b. *Tunneling*
 - c. *Spanning tree*
 - d. *Bridging*

15) ¿En qué consiste el NAT?

- a. Mapea direcciones físicas a direcciones IP.
- b. Mapea direcciones IP a direcciones MAC.
- c. Realiza el filtrado de paquetes a nivel de red.
- d. Sustituye las direcciones de una red interna por la dirección pública del *host* bastión.

16) Disponemos de una única roseta de conexión a la red cableada y necesitamos conectar más de un equipo. Como tenemos un *router* Wi-Fi con ADSL casero viejo que tiene al menos cuatro puertos Ethernet y que aún funciona, desconectamos el equipo que tenemos en la roseta, conectamos uno de los puertos del *router* a la roseta y disponemos de tres puertos para conectar estaciones, donde puedo conectar el equipo que tenía anteriormente en la roseta y añadir más. A partir de ese momento, el equipo que tenía conectado en la roseta deja de funcionar correctamente. ¿Cuál es la razón más probable?

- a. Se trata de un *router* y no de un *switch*, y por tanto, no sirve la solución.
- b. Hay que cambiar la configuración de enrutamiento porque el protocolo de enrutamiento no es el mismo en la red del despacho que en la red de casa.
- c. El servidor DHCP interno del *router* está repartiendo direcciones IP que no son las mismas que funcionan en el despacho, afectando a los equipos conectados a él y al resto de la red del despacho.
- d. Los puertos Ethernet del *router* son FastEthernet y la roseta está conectada a un puerto Gigabit en el bastidor (*rack*) de comunicaciones, o viceversa.

17) El protocolo IEEE 802.3an corresponde a...

- a. 10Gigabit Ethernet sobre Fibra óptica (10Gbase-SR y 10Gbase-LR)
- b. Gigabit Ethernet sobre UTP (1000baseT)
- c. Gigabit Ethernet sobre fibra óptica multimodo (1000base-SX)
- d. 10Gigabit Ethernet sobre UTP (10GbaseT)

18) El protocolo TCP...

- a. Es un protocolo IP no orientado a conexión que funciona en el puerto 6 del nivel IP.
- b. Es un protocolo orientado a conexión que funciona en el puerto 6 del nivel IP.
- c. Es un protocolo IP no orientado a conexión que funciona en el puerto 17 del nivel IP.
- d. Es un protocolo orientado a conexión que funciona en el puerto 17 del nivel IP.

19) La máscara 255.255.255.240 también puede representarse como

- a. /8
- b. /16
- c. /24
- d. /28

20) El protocolo ARP (*address resolution protocol*) nos permite:

- a. Obtener la dirección IP de un equipo al que queremos enviar información sabiendo su dirección MAC.
- b. Obtener la dirección MAC de un equipo sabiendo su dirección IP.
- c. Obtener la dirección IP de un equipo sabiendo su nombre NetBIOS.
- d. Obtener la dirección MAC de un equipo sabiendo su nombre DNS.

21) Para comprobar los parámetros de configuración IP que tiene una estación Windows, ejecutamos la orden:

- a. ipconfig /all
- b. ifconfig /all
- c. configip /all
- d. checkip /all

22) Para comprobar la configuración, servidor DNS asignado y correcto funcionamiento del DNS, desde una estación Windows ejecutamos el comando:

- a. dnsconfig
- b. dnslookup
- c. ipconfig /dns
- d. nslookup

23) Desde un equipo con dirección 172.16.1.5/24 intentamos hacer un PING a otro equipo con dirección 172.16.5.5/24 y no contesta. Suponiendo que ninguno de los dos equipos tenga configurado un cortafuegos que evite el tráfico ICMP entre ellos, ¿cuál es la causa más probable y cuál sería la primera acción a realizar?

- a. El *switch* en el que se encuentran no tiene aprendida la MAC del equipo de destino. Hay que comprobar la tabla MAC del *switch* de destino.
- b. Ambas son direcciones privadas y no se puede encaminar el tráfico entre direcciones privadas.
- c. Se trata de subredes distintas, por lo que es necesario pasar por un *router*. Intentaría hacer PING al *router* predeterminado desde cada una de ellas a ver si se alcanza, porque si no es así, el tráfico no puede salir de la subred correspondiente.
- d. El ARP que lanza la estación 172.16.1.5 no ha sido contestado por la estación 172.16.5.5 y por tanto hay que revisar la configuración de esta última.

- 24) Desde una estación con dirección IP 10.2.3.4/255.255.255.0 intentamos conectarnos a una página web en Internet, pero la conexión falla. Esto puede deberse a que...
- a. La máscara de red no corresponde a la de una clase A, mientras que la dirección IP sí lo es.
 - b. La dirección es de un rango privado y por tanto nunca voy a poder acceder a Internet desde ella.
 - c. La página web tiene filtros para impedir el acceso desde algunas direcciones, posiblemente incluyendo la de ese equipo.
 - d. La dirección es de un rango privado y no debe haber en la red un servidor intermedio (*proxy*) o un elemento que haga NAT y permita dicha conexión.
- 25) El uso de la banda de 5 GHz en las redes Wi-Fi:
- a. Es privativo de los Estados Unidos y está prohibido en Europa.
 - b. Solamente está soportado en el estándar 802.11a en Europa.
 - c. Solamente está soportado en el estándar 802.11g en Europa.
 - d. Se soporta a partir del estándar 802.11n en Europa.
- 26) La máxima velocidad teórica alcanzable cuando se usa el estándar 802.11n en las redes Wi-Fi es de...
- a. 600 Mbps
 - b. 54 Mbps
 - c. 11 Mbps
 - d. 1 Gbps
- 27) El ancho de banda máximo que puede usarse en los canales para el estándar Wi-Fi 802.11ac es de:
- a. 20 MHz
 - b. 40 MHz
 - c. 80 MHz
 - d. 160 MHz
- 28) ¿Qué es el WPA2?
- a. Mecanismo estándar definido por la norma IEEE 802.11 para medir la energía de la señal RF.
 - b. Protocolo de seguridad empleado por WLAN.
 - c. Control de acceso basado en el propio puerto, ya sea de un conmutador o un acceso inalámbrico.
 - d. Cambio de punto de acceso de un cliente WLAN al moverse y pasar al campo de cobertura de otro punto de acceso.

29) El protocolo más seguro para conectarse a una red Wi-Fi es:

- a. WPA2-PSK
- b. WPA2-Enterprise
- c. WPA-PSK
- d. WEP2

30) Si realizamos un túnel VPN desde un equipo para conectarnos a la red interna de una empresa, ¿cuál de las siguientes afirmaciones es **falsa**?

- a. El equipo pasa a tener dos direcciones IP: la dirección real correspondiente a la red a la que está conectada realmente el equipo y una dirección interna de la red de la empresa a la que hacemos el túnel.
- b. Todo el tráfico entre el equipo y la red interna de la empresa va cifrado por el túnel.
- c. Si al configurar el túnel marcamos la casilla “Usar la puerta de enlace predeterminada en la red remota”, todo el tráfico que sale del equipo a Internet lo hace desde la dirección interna de la empresa y no la real del adaptador.
- d. El tráfico entre el equipo y elementos que estén en Internet y, por tanto, fuera de la empresa, pasará necesariamente por el túnel.

31) ¿Qué puerto es el que se utiliza normalmente para las comunicaciones web seguras?

- a. 8080
- b. 434
- c. 443
- d. 344

32) Se dispone de un cliente de red configurado para obtener una dirección IP automáticamente. ¿Qué tipo de servidor es consultado para obtener dicha dirección?

- a. Un servidor de WINS
- b. Un servidor de HTTP
- c. Un servidor de DHCP
- d. Un servidor de TCP/IP

33) El protocolo SSTP normalmente utiliza...

- a. El puerto UDP 1701
- b. El puerto TCP 443
- c. Los puertos 50 y 51 en la cabecera IP
- d. El puerto TCP 1720

- 34) ¿Cuál de los siguientes protocolos **no** es un protocolo para hacer VPN?
- a. L2TP
 - b. NTP
 - c. PPTP
 - d. SSTP
- 35) ¿Qué herramienta de Windows emplearías para clonar máquinas con el sistema operativo Windows con una configuración compatible?
- a. Active Directory
 - b. Sysprep
 - c. El servicio de replicación de Active Directory
 - d. Delete C: /all
- 36) En un bosque de AD (Active Directory) existen los dominios A, B y C; A es el padre de B y éste lo es de C. Los usuarios de A necesitan acceder frecuentemente a los recursos de C. ¿Qué se puede hacer para mejorar la eficacia de los inicios de sesión remotos de los usuarios de A?
- a. Crear una relación de confianza entre A y B y entre B y C. Al ser transitivas, A confiará en C.
 - b. Nada, pues los usuarios de A acceden a los recursos de C con la ruta de confianza más corta.
 - c. Crear una relación de confianza de acceso directo entre A y C.
 - d. Crear una relación de confianza externa entre A y C.
- 37) ¿Cuál de estas **no** sería una utilidad para gestionar la instalación de paquetes en sistemas Linux?
- a. dpkg
 - b. rpm
 - c. yum
 - d. wget
- 38) El servicio de escritorio remoto en Windows 10...
- a. por defecto está habilitado; todos los usuarios tienen acceso y escucha en el puerto 3389.
 - b. por defecto está deshabilitado; sólo los usuarios administradores tienen acceso y escucha en el puerto 1189.
 - c. por defecto está deshabilitado; sólo los usuarios administradores tienen acceso y escucha en el puerto 3389.
 - d. por defecto está habilitado, sólo los usuarios administradores tienen acceso y escucha en el puerto 1189.

- 39) En un equipo Windows, ¿cómo podemos ver una lista de las aplicaciones y procesos en ejecución?
- Con el Administrador de tareas
 - Desde el panel de notificaciones
 - Con el comando NETSTAT
 - Desde en panel de control > Administrador de dispositivos
- 40) Desde un Mac con OS X, ¿cómo conectarías al recurso compartido “mi-recurso” servido desde en un equipo Windows de nombre “equipo.upv.es”?
- Desde Preferencias del Sistema > Compartir > Conectar a recurso compartido y escribir “\\equipo.upv.es\mi-recurso”.
 - Desde el Finder > Ir > Conectarse al servidor... y escribir la dirección “smb://equipo.upv.es/mi-recurso”.
 - Desde el Finder > Ir > Conectarse al servidor... y escribir la dirección “afp://equipo.upv.es/mi-recurso”.
 - Desde el navegador Safari, escribiendo en la URL “\\equipo.upv.es\mi-recurso”.
- 41) ¿Qué servicios se utilizan en los equipos Windows para la resolución de nombres de máquina?
- WINS y DNS
 - DHCP y WINS
 - DNS y MAPI
 - WINS y Bonjour
- 42) ¿Cómo podríamos instalar Windows en un ordenador Mac de modo que tuviéramos un arranque doble con Windows y OS X?
- Con el asistente Boot Camp incluido en OS X.
 - No se puede.
 - Modificando el gestor de arranque con el comando BCDEDIT.
 - Creando una partición de tipo “Windows” con la utilidad de discos.
- 43) ¿Cómo se llama la característica de Windows que permite cifrar los datos de los discos duros para evitar su exposición en caso de pérdidas o robo?
- Device Guard
 - Bitlocker
 - Applocker
 - Defender

- 44) Sobre las ediciones de Windows 10 de 32 y 64bits, ¿cuál de estas afirmaciones es cierta?
- a. Podemos actualizar una edición de 32bits a una de 64bits.
 - b. Las ediciones de 32bits sólo pueden ejecutar aplicaciones de 32bits y las de 64 bits sólo pueden ejecutar aplicaciones de 64bits.
 - c. Para instalar una edición de 64bits, el equipo debe tener una CPU con soporte para 64bits y al menos 8GB de RAM.
 - d. Las ediciones de 64bits requieren versiones de 64 bits de los controladores (*drivers*) de los dispositivos hardware.
- 45) Las directivas de grupo en un Active Directory se utilizan para...
- a. Crear grupos dinámicos basados en los atributos de los usuarios.
 - b. Restringir el ámbito de un grupo dentro del bosque.
 - c. Aplicar configuraciones a equipos y usuarios.
 - d. Definir reglas para controlar el acceso a archivos en recursos compartidos.
- 46) ¿Cuál es el directorio habitual de instalación de OpenGnSys?
- a. /opt/opengnsys
 - b. /usr/local/pornngnsys
 - c. /opengnsys/bin
 - d. /etc/default/opengnsys
- 47) Para realizar operaciones de clonación y particionado en OpenGnSys:
- a. Seleccionamos el ordenador y lanzamos la orden de clonar.
 - b. Los ordenadores de una unidad organizativa deben asociarse a una entidad.
 - c. Los ordenadores de una entidad deben asociarse a un aula.
 - d. Los ordenadores de una unidad organizativa deben asociarse a un repositorio.
- 48) ¿Cuál de las siguientes **no** es una tecnología o característica que permite en los navegadores web ejecutar aplicaciones del lado cliente?
- a. ActiveX
 - b. Javascript
 - c. Java Applets
 - d. Cookies
- 49) ¿Cuáles son los números de puerto que se utilizan por defecto en los protocolos de correo electrónico POP, IMAP y SMTP?
- a. POP 110, IMAP 143 y SMTP 25
 - b. POP 143, IMAP 995 y SMTP 21
 - c. POP 993, IMAP 995 y SMTP 25
 - d. POP 143, IMAP 110 y SMTP 25

50) ¿Cómo se denominan los dispositivos dedicados de almacenamiento que se conectan directamente a la red para ofrecer servicios de archivos?

- a. NAS
- b. SAN
- c. LUN
- d. RAID

51) En cuanto al software antivirus de cliente:

- a. No existen antivirus para sistemas operativos Mac OS X, ya que no es necesario al no existir ataques de virus para este sistema operativo.
- b. Ningún software antivirus de cliente incorpora un módulo de cortafuegos (*firewall*), ya que los sistemas operativos ya disponen de cortafuegos propio.
- c. Muchos antivirus disponen de herramientas que permiten cargar el antivirus en el arranque, pero no deben usarse en ningún caso, cuando un equipo ya ha sido infectado.
- d. Las bases de datos de antivirus, llamadas también *firmas de antivirus*, aseguran que el equipo esté protegido contra las últimas amenazas conocidas por cada antivirus, por lo que es muy importante que estén actualizadas.

52) ¿Cuál de estas afirmaciones sobre el cortafuegos de Windows 10 **no** es cierta?

- a. Distingue entre redes de dominio, privadas y públicas.
- b. Permite reglas de entrada, de salida y de seguridad de conexión.
- c. Permite reglas para controlar las conexiones de un programa o de un puerto.
- d. No se puede desactivar excepto si se instala otra aplicación antivirus que lo sustituya.

53) ¿Qué deberíamos hacer para evitar ataques de tipo *phishing*?

- a. Tener siempre activado el firewall de nuestro equipo.
- b. Dudar de los enlaces a páginas web en los correos electrónicos y comprobar cada vez que nos conectemos a una página que solicita información privada, que la URL sea correcta, que se utilice el protocolo HTTPS y que el certificado sea válido.
- c. Mantener tanto nuestro equipo como el software que utilicemos siempre actualizado con las últimas versiones y parches de seguridad.
- d. Utilizar claves largas, que no incluyan palabras comunes y que contengan combinaciones de varios tipos de caracteres, como números, mayúsculas y signos de puntuación.

- 54) En la criptografía asimétrica (indicad la opción correcta)...
- a. Se usan un par de claves. Ambas claves deben ser conocidas por todos ya que una se usa para cifrar y otra para descifrar.
 - b. Se usan un par de claves que únicamente las conoce el propietario.
 - c. Se usan un par de claves. Una clave pública que puede ser conocida por todos y una clave privada que únicamente debe conocer el propietario y que debe conservarla de forma segura.
 - d. Se usa la misma clave tanto para cifrar como para descifrar.
- 55) En el cliente de correo Outlook 2016, podemos configurar un certificado electrónico personal...
- a. Sólo para firmar correos, ya que el propio cliente de correo ya incorpora mecanismos cifrar los correos.
 - b. Sólo para cifrar, ya que el propio cliente de correo ya incorpora mecanismos para firmar los correos.
 - c. Firmar y cifrar los correos.
 - d. No es necesario configurar un certificado electrónico personal, ya que el propio cliente de correo ya incorpora mecanismos para firmar y cifrar los correos.
- 56) ¿Cuál de estos aspectos **no** podemos garantizar si únicamente firmamos digitalmente un documento?
- a. El no repudio
 - b. La autenticidad
 - c. La confidencialidad
 - d. La integridad
- 57) Si en un Windows 10, estamos instalando un certificado electrónico personal en el almacén de certificados del sistema, y no queremos que pueda ser usado por un tercero en caso de que el usuario se deje la sesión abierta, ¿qué opción deberíamos tener en cuenta?
- a. No es necesario realizar ninguna acción ya que el certificado ya tiene protegida la clave privada con contraseña.
 - b. Debemos habilitar la protección segura de clave privada y elegir posteriormente el nivel de seguridad alto, para proteger su uso con contraseña.
 - c. Debemos Habilitar la protección segura de clave privada y elegir posteriormente el nivel de seguridad medio, para proteger su uso con contraseña.
 - d. Debemos Habilitar la protección segura de clave privada y elegir posteriormente el nivel de seguridad bajo, para proteger su uso con contraseña.

- 58) Según la Política de firma electrónica y certificados de la Administración, para que una firma electrónica pueda ser considerada firma electrónica avanzada, deben inferirse los siguientes requisitos:
- a. Identificación, confidencialidad y no repudio
 - b. Identificación y no repudio
 - c. Identificación e integridad
 - d. Identificación, integridad y no repudio
- 59) ¿Cuál sería el nivel mínimo de iluminación aceptable en un entorno de trabajo, en el que las exigencias visuales sean de tipo *despacho/oficina*?
- a. 500 lux
 - b. 700 lux
 - c. 800 lux
 - d. 1.000 lux
- 60) En trabajos esporádicos de manipulación de cargas, para un trabajador sano y entrenado, el peso permitido puede llegar hasta los:
- a. 25 kg.
 - b. 30 kg.
 - c. 40 kg.
 - d. No hay peso máximo permitido, dependerá del entrenamiento del trabajador

Preguntas de reserva

- 61) Si necesitamos realizar una conexión a 40 Gbps entre dos equipos con fibra óptica, podremos utilizar...
- a. Solamente fibra multimodo
 - b. Solamente fibra monomodo
 - c. Solamente fibras multimodo de categoría OM1
 - d. Fibras monomodo y fibras multimodo a partir de la categoría OM4
- 62) La dirección 192.168.5.63 con máscara de red 255.255.255.192:
- a. Es la dirección de un equipo normal de la red 192.168.5.0/255.255.255.192
 - b. Es la dirección de la subred 192.168.5.63/255.255.255.192
 - c. Es la dirección de *broadcast* de la subred 192.168.5.0/255.255.255.192
 - d. No es una dirección válida puesto que las redes 192.168.x.x tienen como máscara válida solamente la 255.255.255.0

63) ¿Cuál de estas afirmaciones **no** es cierta sobre las cuentas de usuario en un dominio de Active Directory?

- a. Pueden ser miembros de más de un grupo.
- b. Pueden residir en más de una unidad organizativa.
- c. Se les puede definir las horas permitidas para iniciar sesión.
- d. Se les puede definir una fecha de expiración.

64) El *contador de programa* de una CPU contiene...

- a. la instrucción a ejecutar en código ASCII
- b. la instrucción a ejecutar en código binario
- c. la dirección de la instrucción a ejecutar
- d. la dirección en la que dejar el resultado