

1. Disponemos en nuestra organización de un Sistema de Gestión de la Seguridad de la Información (SGSI) que queremos certificar; para ello:
 - a. Auditores externos deberán determinar la conformidad del sistema con los requerimientos de ISO/IEC 27001, mientras que ISO/IEC 27002 contiene una guía de buenas prácticas y no es certificable
 - b. Auditores externos deberán determinar la conformidad del sistema con los requerimientos de ISO/IEC 27002, mientras que ISO/IEC 27001 contiene una guía de buenas prácticas y no es certificable
 - c. Auditores externos deberán determinar la conformidad del sistema con los requerimientos de ISO/IEC 27001, mientras que ISO/IEC 27002 contiene una guía de buenas prácticas y también es certificable
 - d. Tanto ISO/IEC 27001 como ISO/IEC 27002 son guías de buenas prácticas y no son certificables

2. De acuerdo con la ISO/IEC 20000, en el proceso de gestión de nivel de servicio:
 - a. Cada servicio ofrecido se debe definir, acordar y documentar en al menos tres acuerdos de nivel de servicio (SLAs)
 - b. Los SLAs deben estar bajo el control de la gestión de la configuración
 - c. Los SLAs se deben revisar periódicamente por las partes, para asegurar que se encuentran actualizados y continúan siendo eficaces
 - d. Las no conformidades se revisarán y las acciones de mejora definidas en este proceso generarán solicitudes para el cambio (RFCs) que se comunicarán al proceso de gestión del cambio

3. De acuerdo con metodología de gestión de proyectos PMBOK, ¿cual de las siguientes características sobre las fases de un proyecto no es correcta?
 - a. Las fases se pueden subdividir en subfases en función del tamaño, complejidad, etc...
 - b. La dirección del proyecto nunca lleva a cabo una revisión de la fase actual hasta que esta está totalmente cerrada
 - c. Una fase de un proyecto suele concluir con una revisión del trabajo logrado y los productos entregables
 - d. Se puede cerrar una fase sin la decisión de iniciar alguna otra fase

4. ¿Cual de lo siguientes organismos no es una Entidad de Certificación reconocida en España?
 - a. Red Académica y de Investigación Española que proporciona servicios a las universidades RedIRIS
 - b. Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía
 - c. Autoridad de Certificación de la Comunidad Valenciana-ACCV
 - d. CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)

5. De acuerdo a la Ley orgánica 15/1999, del 13 de diciembre, sobre protección de datos de carácter personal, no son funciones de la Agencia de Protección de Datos:
 - a. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos
 - b. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias
 - c. Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley
 - d. No atender las peticiones y reclamaciones formuladas por las personas afectadas

6. De acuerdo con el Real Decreto 1720/2007, de 21 de diciembre, en el que se aprueba el desarrollo de la Ley orgánica de protección de datos de carácter personal quedan excluidos los ficheros o tratamientos...
 - a. Ficheros realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas
 - b. Ficheros de las Fuerzas y Cuerpos de Seguridad
 - c. Ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad
 - d. Ficheros creados para realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas

7. De acuerdo con el artículo 3 de la Ley 25/2007, de 18 de octubre, de conservación de datos de comunicaciones electrónicas y de redes públicas de comunicación, los operadores no podrán conservar ningún dato que revele:
 - a. La fecha y hora de la conexión y desconexión del servicio de acceso a Internet
 - b. Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación
 - c. El servicio de Internet utilizado
 - d. El contenido de la comunicación

8. La ley 11/2007, del 22 de junio...
 - a. Reconoce el derecho de los ciudadanos para la custodia de los datos personales con las administraciones públicas recopilados por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa
 - b. Reconoce el deber de los ciudadanos a relacionarse con las administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas
 - c. Reconoce el derecho de los ciudadanos a relacionarse con las administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas
 - d. Reconoce el deber de los ciudadanos para ceder los datos personales con las administraciones Públicas recopilados por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa

9. De acuerdo con el artículo 52 de los Estatutos de la Universitat Politècnica de València (DECRETO 182/2011, de 25 de noviembre),
 - a. En caso de vacante, ausencia o enfermedad el Rector será sustituido por el vicerrector expresamente designado por el Rector o, en su defecto, por el vicerrector de mayor grado y antigüedad
 - b. En caso de vacante, ausencia o enfermedad el Rector será sustituido por el vicerrector que ostente las competencias de docencia e investigación
 - c. En caso de vacante, ausencia o enfermedad el Rector será sustituido por el Secretario General
 - d. En caso de vacante, ausencia o enfermedad el Rector será sustituido por el Gerente

10. De acuerdo con el artículo 157 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público, el procedimiento por el que todo empresario interesado podrá presentar una proposición, quedando excluida toda negociación de los términos del contrato con los licitadores se denomina:
 - a. Abierto
 - b. Restringido
 - c. Negociado
 - d. Diálogo competitivo

11. De acuerdo con el artículo 16 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, ¿quién deberá realizar una evaluación inicial de los riesgos para la seguridad y salud de los trabajadores, teniendo en cuenta, con carácter general, la naturaleza de la actividad, las características de los puestos de trabajo existentes y de los trabajadores que deban desempeñarlos?
- El trabajador
 - El empresario
 - La comunidad autónoma
 - El cuerpo de bomberos de la localidad
12. Respecto a la arquitectura de computadores, podemos decir que:
- Los procesadores CISC tienen un juego de instrucciones más complejo que los RISC, y por ello los CISC necesitan más memoria y un mayor número de instrucciones que los RISC para realizar tareas equivalentes
 - Según la clásica definición de Von Neumann, la Unidad Aritmético-Lógica (UAL) es un procesador adicional que, funcionando conjuntamente con la Unidad Central de Proceso (CPU), descarga a ésta de las operaciones aritméticas y lógicas complejas
 - La CPU se comunica con los periféricos externos por medio de módulos de Entrada/Salida, pudiendo utilizar para ello técnicas de interrupción o también procesadores específicos de entrada/salida
 - La memoria caché está estructurada en una jerarquía de niveles, de modo que la L1, también llamada interna o principal, es la situada entre la CPU y la RAM, mientras que la L2 está embebida en el dispositivo de almacenamiento y funciona a modo de *buffer* (caché de disco)
13. Sobre las diferentes tecnologías de almacenamiento podemos decir:
- El estándar iSCSI permite la transferencia de datos en bloque por medio de redes TCP/IP, por lo que presenta la ventaja de poder conformar redes de almacenamiento extensas o dispersas geográficamente, a la vez de beneficiarse del desarrollo e implantación de las tecnologías de red
 - El interfaz SAS (Serial Attached SCSI) es el sucesor del interfaz paralelo SCSI, orientado a aumentar las tasas de transferencia a partir de los 3 Gb/s. Mantiene la limitación de 16 dispositivos conectados, y el inconveniente es que se reparte la capacidad entre todos ellos, por lo que disminuye la tasa de transferencia con cada uno de ellos
 - El interfaz SATA es el sucesor del interfaz paralelo ATA, orientado a aumentar las tasas de transferencia a partir de los 150 MB/s. Una característica muy interesante es que el conector es el mismo que en la interfaz SAS, y permite utilizar estos discos duros con una controladora SATA
 - El canal de fibra o fibre channel (FC) es una tecnología de red utilizada para redes de almacenamiento, disponible primero a la velocidad de 1 Gbps y posteriormente a 2, 4 y 8 Gbps. El FCP (protocolo del canal de fibra) es el protocolo de interfaz de SATA sobre fibre channel

14. De los distintas tecnologías relacionadas con los sistemas almacenamiento podemos afirmar:

- a. Para superar las grandes limitaciones de la FAT de 16 bits, tales como el tamaño máximo de partición de 2 GB, se introdujo FAT32, que llevó ese límite a los 2 TB, además de permitir archivos de hasta 2 GB
- b. El sistema NTFS incorpora el empleo de un registro transaccional (journal) para garantizar la integridad del sistema de ficheros (aunque no la de cada archivo), así como cuotas de disco por usuario, puntos de montaje de volúmenes y cifrado de ficheros mediante EFS
- c. EXT4 introduce mejoras respecto de EXT3, tales como la desfragmentación online, el registro por diario (journaling), además de aumentar el tamaño máximo de archivo de 2 TB a 16 TB y el de volumen de 32 TB a 1 PB
- d. LVM (Logical Volume Manager) proporciona un método de asignación de espacio en los dispositivos de almacenamiento masivo que es más flexible que esquemas de particionamiento convencionales. Permite instantáneas de disco (snapshots) de lectura y escritura, y soporta niveles de RAID 0 hasta RAID 5

15. Sobre el control de cuentas de usuario (UAC) de MS-Windows podemos decir:

- a. Es un mecanismo de seguridad introducido en Windows Vista y 2008, para proteger el sistema ante posibles ejecuciones de software malicioso
- b. Sirve para auditar los inicios de sesión y acceso a objetos del sistema
- c. Es un software antivirus integrado en el sistema con una configuración particular según el usuario que inicia sesión
- d. Es un mecanismo para impedir la ejecución de determinadas aplicaciones, configurable para cada usuario mediante directivas de grupo

16. En un equipo con Windows Vista o Windows 7 en el que se ha eliminado accidentalmente un archivo, ¿cuál de estas alternativas NO serviría para recuperarlo?

- a. Utilizar la característica "versiones anteriores"
- b. Utilizar la herramienta de copia de seguridad que incluye Windows
- c. Utilizar una imagen del sistema creada anteriormente
- d. Utilizar un disco de reparación del sistema creado anteriormente

17. ¿Cuál de estas afirmaciones NO es cierta acerca de la instalación y despliegue de Windows Vista o Windows 7?

- a. La instalación se basa en imágenes y se utiliza el formato de archivo de imagen .wim (Windows Imaging)
- b. Ya no es posible emplear la utilidad sysprep para inicializar la información específica del equipo
- c. Para ayudar a la preparación e instalación de los equipos se puede utilizar Windows PE, que es un sistema operativo mínimo con servicios limitados
- d. En las ediciones de licencias por volumen los equipos se pueden activar conectándose a un servidor de licencias

18. ¿Cuál de estas afirmaciones NO es cierta sobre el servicio DNS de Windows 2008?
- Cuando se ejecuta en un controlador de dominio y se integra con Active Directory funciona en modo dinámico, permitiendo a los equipos registrarse automáticamente
 - Las zonas integradas en Active Directory se almacenan en la base de datos del AD y se replican junto a resto de datos del directorio
 - Todavía no incluye soporte para IPv6
 - Soporta registros del tipo CNAME, A, AAAA, MX, PTR y SRV
19. El esquema del Directorio Activo de Windows:
- Define las clases de objetos y atributos que pueden crearse en el directorio y es único para el bosque
 - Depende de las versiones de Windows instaladas en los DCs y determina las características disponibles en el dominio. Hay un nivel de esquema para el dominio y otro para el bosque
 - Es la base de datos donde se almacena el árbol de unidades organizativas del dominio
 - Es la política de seguridad que se aplica sobre las cuentas de usuario. Establece los requisitos de complejidad de las contraseñas
20. En un sistema Linux, se quiere acceder como root para reparar problemas o hacer pruebas en el sistema. ¿Con qué nivel de ejecución (runlevel) de los siguientes es más adecuado iniciar el sistema?
- 0
 - 1
 - 2
 - 3
21. En un sistema Linux con usuarios locales, tras habilitar la opción de “shadowed password”, ¿en qué fichero se almacenan los passwords de los usuarios?
- /usr/passwd
 - /usr/shadow
 - /etc/passwd
 - /etc/shadow
22. En un sistema Linux que utiliza gestión de paquetes mediante rpm, ¿con qué comando de los siguientes se podría verificar que el package MIPAQUETE está instalado?
- grep MIPAQUETE
 - find -q rpm | grep MIPAQUETE
 - rpm -qa | grep MIPAQUETE
 - find MIPAQUETE

23. ¿Qué utilidad, que forma parte de SAMBA, permite el acceso desde Linux a recursos CIFS mediante instrucciones similares a las del programa ftp?
- cifsutil
 - smbclient
 - smbftp
 - cifsmanager
24. Se pretende validar usuarios desde un equipo Linux contra un dominio de Microsoft Active Directory mediante kerberos. ¿Dónde configuraremos el KDC en la máquina cliente unix?
- En kerberos.conf
 - En krb5.conf
 - En kinit.defaults
 - En la variable de entorno KDC
25. Utilizamos como servidor de SMTP de una red un equipo Linux con una configuración estándar de sendmail. Debido a un problema de conectividad externa, los mensajes de correo salientes han sido retenidos y encolados en él. Una vez restablecida la conectividad deseamos reprocessar estos mensajes cuanto antes. ¿Qué orden podemos utilizar para ello?
- sendmail -q
 - mqueue -r
 - mailq
 - dispatch
26. En un entorno Linux, ¿cual es el fichero donde se realiza la correspondencia entre los números de puerto y protocolo con los nombres de servicio?
- /etc/portmap
 - /etc/friendly
 - /etc/services
 - /etc/mapping
27. Podemos afirmar a propósito de ServiceGuard:
- Es un sistema de clúster de alta disponibilidad, en el cual las aplicaciones se recuperan en nodos alternativos en menos de 0,6 segundos
 - Su funcionamiento se basa en reservar uno de los nodos en estado latente, a la espera de que entre en funcionamiento en caso de caída de uno de los nodos activos
 - Se reconfigura de manera automática e inteligente tras el fallo de un nodo, sin interacción del usuario
 - Es necesario que el usuario sepa en todo momento en qué nodo del clúster se está ejecutando su aplicación para poder lanzar las órdenes oportunas

28. Se dispone de un gestor de colas NQS. ¿Qué programa utilizaremos para administrar las peticiones, colas, dispositivos y los parámetros globales de funcionamiento?
- qadm
 - qmgr
 - nqsadmin
 - nqsctl
29. En un sistema ORACLE correctamente configurado, ¿qué fichero residente en los clientes contiene las direcciones de las bases de datos accesibles por red?
- Listener.ora
 - tnsnames.ora
 - names.ora
 - sqlnetwork.ora
30. En un sistema ORACLE 11g, ¿cuál de las siguientes afirmaciones es correcta?
- El administrador no asigna privilegios del sistema a los usuarios, solo él tiene acceso a los mismos
 - Los privilegios sobre los objetos solo los puede asignar el administrador
 - Los privilegios del sistema los asigna cualquier usuario propietario
 - El propietario de un objeto puede asignar grants sobre el mismo a otros usuarios
31. En ORACLE 11g, ¿qué información sobre TABLESPACES es correcta?
- Cualquier usuario de la base de datos puede crear un Tablespace
 - El tablespace SYSTEM contiene información básica, como un diccionario de la base de datos y el segmento de rollback
 - No es posible aumentar el tamaño de un tablespace sin ponerlo offline ni de añadir otro fichero
 - El tablespace SYSTEM se puede desactivar con el comando ALTER TABLESPACE SYSTEM OFFLINE
32. ¿Cuál es el comando genérico de administración de MySQL por línea de comandos?
- mysqladmin
 - mysqldb
 - mqladmin
 - adminsqli
33. ¿Cuál de los siguientes tipos de sentencias del intérprete de comandos PostgreSQL es de tipo DDL?
- INSERT
 - CREATE
 - UPDATE
 - DELETE

34. ¿Qué cuenta con derechos administrativos es la creada inicialmente por Microsoft SQL Server?

- a. administrador_sql
- b. sa
- c. root
- d. dba

35. La respuesta de un servidor HTTP con un código 3XX significa:

- a. Error del cliente
- b. Error del servidor
- c. Redirección
- d. Informativo

36. ¿Qué directiva de Apache nos permite configurar el que un cliente pueda realizar más de una petición por conexión?

- a. timeout
- b. timeoutclient
- c. keepalive
- d. reuseconnection

37. Microsoft IIS, para Windows Server 2008, se puede instalar:

- a. Solamente con la herramienta gráfica Administrador del servidor
- b. Solamente con la herramienta gráfica Administrador del servidor y con la de línea de comandos Server Manager CMD
- c. Solamente con la herramienta gráfica Administrador del servidor, con la de línea de comandos Server Manager CMD, y con la utilidad en modo texto PkgMgr
- d. Con la herramienta gráfica Administrador del servidor, con la de línea de comandos Server Manager CMD, con la utilidad en modo texto PkgMgr y con la herramienta OC Setup

38. ¿Cuál es el resultado que aparece por consola al ejecutar el siguiente programa escrito en el lenguaje javascript?

```
var mes, año, numDías, esNoBisiesto;
mes= 2;
año= 2012;
esNoBisiesto= ((año % 4 == 0) && (año % 100 != 0)) || (año % 400 == 0);
numDías= (esNoBisiesto)? 29: 28;
WScript.Echo (numDías);
WScript.StdIn.ReadLine();
```

- a. 28
- b. 29
- c. 1
- d. esNoBisiesto

39. En un script bash, ¿qué obtendríamos con la siguiente expresión:

```
echo 232 |tr 3 \\n |paste -sd+ -|bc
```

- a. 0
- b. 1
- c. 4
- d. 22

40. ¿Cuál es el número mágico de un script ejecutable Linux?

- a. x
- b. #!
- c. 555
- d. Unix no utiliza números mágicos en los scripts

41. ¿Cómo se llama la implementación de Microsoft de ECMAScript?

- a. ActionScript
- b. JScript
- c. .NET
- d. JavaScript

42. ¿Qué es CPAN?

- a. Un repositorio en la red de módulos y distribuciones de perl
- b. Un compilador de php
- c. Un compilador de C ANSI
- d. Una especificación de computación en paralelo

43. Disponemos de un equipo linux de kernel 2.6 con una distribución estándar y acceso a un almacenamiento externo FC. Desde un servidor externo FC le asignamos para su uso una nueva LUN. ¿Qué podríamos ejecutar desde una shell del equipo para reconocer el nuevo disco y poder utilizarlo sin reiniciar el sistema?

- a. No es necesario hacer nada. El reconocimiento debe ser automático
- b. `rmmod -F scsi ; insmod scsi`
- c. `for i in /sys/class/scsi_host/host*/scan; do echo - - - >$i; done`
- d. `ioscan -fn`

44. ¿Qué es imprescindible en un certificado digital?

- a. Una identidad y la clave privada de esa entidad, todo ello firmado por una autoridad de certificación
- b. Una identidad y la clave pública de esa entidad, todo ello firmado por esa misma entidad
- c. El cifrado con la clave pública de la autoridad de certificación de la identidad y la clave pública de quien es certificado
- d. El cifrado con la clave privada de la autoridad de certificación de la identidad y la clave pública de quien es certificado

45. ¿Qué es el protocolo OCSP?

- a. Un protocolo de certificación de sistema abierto
- b. Un protocolo de seguridad de listas de correo electrónico
- c. Un protocolo que utilizan los navegadores modernos para comprobar que el certificado es válido
- d. Un protocolo de seguridad para la creación de certificados digitales

46. En un sistema Linux, ¿qué hace el comando siguiente?

```
find /etc -type f | xargs openssl md5 > /usr/secure/sigs.txt
```

- a. Crea un archivo `/usr/secure/sigs.txt` con el hash MD5 de todos los archivos del directorio `/etc`
- b. Crea un archivo `/usr/secure/sigs.txt` con la lista de todos los archivos del directorio `/etc` con un valor MD5 correcto
- c. Chequea el hash MD5 de todos los archivos del directorio `/etc` contra el fichero `openssl` y deja el resultado en `/usr/secure/sigs.txt`
- d. Chequea el hash MD5 de todos los archivos del directorio `/etc` contra el fichero `xargs` y deja el resultado en `/usr/secure/sigs.txt`

47. El proceso de análisis de riesgos informáticos consiste en:

- a. Identificación de los activos informáticos (datos, software, hardware, servicios), sus vulnerabilidades y amenazas a las que se encuentran expuestas, así como su probabilidad de ocurrencia, y el impacto de todas ellas. Con ello obtenemos la matriz de riesgo, que nos sirve para determinar el riesgo asumible y el residual
- b. Identificación de los activos informáticos (datos), sus vulnerabilidades y amenazas a las que se encuentran expuestas, así como su probabilidad de ocurrencia, y el impacto de todas ellas. Con ello obtenemos la matriz de riesgo, que nos sirve para determinar las medidas de protección necesarias para eliminar completamente el riesgo residual
- c. Identificación de los activos informáticos (datos y software), sus vulnerabilidades y amenazas a las que se encuentran expuestas, así como su probabilidad de ocurrencia. Con ello obtenemos la matriz de riesgo, que nos sirve para determinar el riesgo asumible y el residual
- d. Identificación de los activos informáticos (hardware, servicios), sus vulnerabilidades y amenazas a las que se encuentran expuestas y el impacto de todas ellas. Con ello obtenemos la matriz de riesgo, que nos sirve para determinar el riesgo residual

48. ¿Cuál es el orden adecuado de las siguientes fases en un análisis forense de seguridad?
- 1ª. Identificación del incidente. 2ª. Recopilación de evidencias. 3ª. Preservación de la evidencia. 4ª. Análisis de la evidencia. 5ª. Documentación y presentación de los resultados
 - 1ª. Recopilación de evidencias. 2ª. Preservación de la evidencia. 3ª. Identificación del incidente. 4ª. Análisis de la evidencia. 5ª. Documentación y presentación de los resultados
 - 1ª. Identificación del incidente. 2ª. Análisis de la evidencia. 3ª. Recopilación de evidencias. 4ª. Preservación de la evidencia. 5ª. Documentación y presentación de los resultados
 - 1ª. Identificación del incidente. 2ª. Recopilación de evidencias. 3ª. Análisis de la evidencia. 4ª. Preservación de la evidencia. 5ª. Documentación y presentación de los resultados
49. ¿Qué es SNORT?
- Un sistema de detección de intrusiones sobre red
 - Un entorno abierto de ejecución de aplicaciones de simulación de tiempo real en red
 - Un estándar de calidad de diseño de aplicaciones informáticas
 - Una herramienta de gestión de la capacidad de sistemas
50. ¿Cuál de los siguientes protocolos puede ser utilizado específicamente para conectarse a servicios de terminal, por ejemplo en un entorno VMware?
- H.225
 - RTSP
 - RDP
 - XBMP
51. En el entorno de virtualización de VMware, ¿cuál es la funcionalidad de la utilidad VMotion?
- Es la suite completa de virtualización
 - Permite mover máquinas virtuales en ejecución desde un servidor físico ESX a otro
 - Es la interfaz web del servicio de consola
 - Es un switch virtual para el enrutamiento del tráfico entre máquinas virtuales
52. En el entorno de virtualización, ¿qué es un hipervisor?
- Es una capa de software que se ejecuta directamente sobre el hardware en sustitución del sistema operativo, o sobre un sistema operativo host y permite ejecutar múltiples máquinas virtuales
 - Es una máquina virtual que tiene acceso directo al hardware para la gestión de los sistemas operativos invitados
 - Es un software instalado en un equipo externo a un sistema de máquinas virtuales y que permite ofrecer funcionalidades de gestión conjunta
 - Es un software comercial de Xen Corporation

53. Se dispone de un equipo servidor con dos procesadores de dos núcleos cada uno y una cantidad en total de 64GB de RAM. Está instalado el VMware vSphere Hypervisor ESXi versión 5 y sólo se dispone de licenciamiento gratuito. Se pretende disponer de varias máquinas virtuales con la misma versión de sistema operativo y 4GB de RAM cada una. ¿Cuántas máquinas virtuales simultáneas podremos utilizar como máximo en este servidor?
- 4
 - 8
 - 16
 - Más de 16
54. Un sistema CRM es, de entre las siguientes opciones:
- Un sistema informático de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing
 - Una plataforma tecnológica orientada a facilitar servicios al cliente
 - Un sistema de almacenamiento, recogida y análisis de ficheros de datos
 - Software de información geográfica orientado a ubicar e integrar la mayoría de los procesos de negocio
55. En una organización, ¿para cuál de las siguientes funciones NO se puede utilizar un sistema IVR?
- Para proporcionar información de forma automática
 - Para recoger y firmar de forma electrónica documentos
 - Para encaminar llamadas a partir de los dígitos que marque un usuario
 - Para encuestas y aplicaciones de televoto
56. Las centrales de tránsito sin abonados propios a las que se conectan otras centrales y que no pertenecen a la red jerárquica, se conocen como:
- Locales
 - Tándem
 - Primarias
 - Directas
57. El protocolo de señalización SIP utiliza por defecto el puerto:
- 5060
 - 5080
 - 4569
 - 80
58. En la telefonía móvil GSM, los centros de conmutación móvil se conocen por el acrónimo:
- MSC
 - BTS
 - BSC
 - BS

59. Las tarjetas de identificación de usuario (SIM) almacenan en su interior un número de identificación internacional de usuario conocido por:
- IMEI
 - IMSI
 - PIN
 - PUK
60. En un sistema de comunicaciones móviles UMTS, se entiende por UTRAN a:
- Equipos de usuario
 - La red de acceso radio
 - Controladores de la red
 - Los nodos B
61. En un sistema de codificación de vídeo, ¿qué es el chroma subsampling?
- Es una técnica de codificación que permite corregir el virado a rojo de los CCDs domésticos
 - Es una técnica de codificación en la que se implementa menor resolución de la información de crominancia que de la información de luminancia del vídeo
 - Es una técnica de codificación en la que se codifican por separado las líneas pares y las líneas impares de la información de crominancia del vídeo
 - Es una técnica de codificación que mezcla el canal de audio estéreo con la información de crominancia del vídeo
62. ¿Cuál de los siguientes formatos de vídeo de la ITU implementa una resolución mayor?
- QCIF
 - CIF
 - 4CIF
 - 16CIF
63. ¿Cuál es el protocolo ITU de señalización de llamada que se suele utilizar en las comunicaciones de videoconferencia H.323?
- G.711
 - H.261
 - H.225
 - SIP
64. ¿Cuál de los siguientes es un estándar específico de streaming de audio y vídeo?
- RTSP
 - UDP
 - WMV
 - FLV

65. ¿Cuál de los siguientes protocolos se utiliza específicamente para la gestión de dispositivos domóticos a través de líneas eléctricas?
- X10
 - PLC
 - 802.11n
 - UPnP
66. ¿Qué acción debe realizar un administrador de un servidor Xenserver para permitir el control de acceso basado en roles (RBAC)?
- Crear un nuevo pool
 - Habilitar la autenticación LDAP
 - Configurar la autenticación contra un Directorio Activo
 - Instalar las Xenserver tools en el controlador del dominio
67. Con respecto a la utilización de la fibra óptica como medio de transmisión podemos decir:
- Proporciona un menor caudal de datos frente a los cables coaxiales y pares trenzados
 - La fibra multimodo se utiliza por la ventaja que tiene sobre la monomodo al presentar menor dispersión modal
 - Un ejemplo de propagación monomodo puede ser el de una fibra formada por un revestimiento de 125 μm y un núcleo de 9 μm por el interior del cual se transmite axialmente un único modo
 - En las transmisiones multimodo no se suelen utilizar fuentes láser
68. Respecto de los sistemas de transmisión por satélite, podemos decir que:
- En los sistemas geoestacionarios (GEO), al estar el satélite a distancias del orden de 36.000 km se introduce en el sistema un retraso de unos 25 s que obligan a utilizar protocolos modificados
 - En los sistemas de satélite de órbita baja (LEO) para conseguir grandes coberturas se recurre a la utilización coordinada de varios satélites; por ejemplo, el sistema Teledesic para conseguir una cobertura de todo el globo utiliza una constelación de 3 satélites
 - Los terminales de usuario de los sistemas GEO suelen ser más pequeños que los LEO, gracias que no es necesario incorporar el sistema de seguimiento automático del satélite
 - En el enlace ascendente se suelen utilizar mayores frecuencias, a pesar de su mayor atenuación, pues podemos tener mayor potencia; en el enlace descendente, para evitar interferencias, se suele utilizar canales próximos con distinta polarización

69. De acuerdo con la norma UNE-EN 50173, ¿qué categoría de cableado de par trenzado admite frecuencias de hasta 250 MHz?
- Categoría 3
 - Categoría 5
 - Categoría 5e
 - Categoría 6
70. Uno de los parámetros de certificación de fibras ópticas es la atenuación, sobre la cual podemos afirmar:
- Depende únicamente de la distancia
 - Es la pérdida de señal en el extremo emisor debido al comportamiento del medio físico
 - Se espera que supere un determinado valor mínimo
 - Se espera que no supere un determinado valor máximo y se mide en dB/Km
71. Respecto de los distintos dispositivos que se utilizan para la conformación y conexión de redes, podemos decir:
- Hay conmutadores (o switches) que utilizan la técnica de Almacenar-Transmitir (Store-and-Forward) para minimizar la propagación de errores, mientras que otros optan por la técnica de Cortar-Continuar (Cut-Through) para disminuir la latencia
 - Los concentradores (hubs) separan dominios de colisión aislando el tráfico de broadcast, y pueden cambiar de protocolo o de velocidad entre puertos
 - Los puentes transparentes (bridges) permiten unir redes de distinto tipo, como por ejemplo Ethernet con Token-Ring
 - Los encaminadores (routers) permiten la conexión de redes diferentes por medio de protocolos como el spanning tree, VLANs o Multicast
72. Según el modelo de referencia ISO/OSI, son funciones del nivel de Transporte:
- Compresión y cifrado de datos
 - Conexión de extremo a extremo, control de circuitos virtuales, multiplexación
 - Detección de errores, distribución ordenada de tramas y control del flujo
 - Direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final
73. Sobre el protocolo 802.1Q para redes virtuales (VLANs) podemos afirmar:
- Está basado en la dirección física (port-based) y se permiten 12 VLANs
 - Está basado en protocolo (port-based), y añade 4 bits a la trama original
 - Está basado en puerto (port-based) y utiliza 12 bits para identificar la VLAN
 - Está basada en el protocolo de Internet (IP-based) y los puertos de un conmutador sólo pueden ser todos tagged o todos untagged

74. Respecto del protocolo de Spanning Tree (STP) podemos afirmar:

- a. Está diseñado para evitar que se produzca una saturación en la red cuando se cierra un bucle entre tres o más routers
- b. Los elementos de red intercambian paquetes de control por broadcast para detectar el bucle, ver la posición de cada uno de ellos en el anillo, y acordar el sentido de rotación en que se transmitirá la información
- c. Una vez definida la topología los puentes envían la información repartida entre todos los caminos que se ha deducido que llegan al destino, y el algoritmo de spanning tree determina la cantidad que se envía por cada puerto dependiendo de la velocidad de cada una de los caminos posibles
- d. Con la proliferación de elementos de conexión en los que cada puerto atiende a una única estación se ideó el protocolo Rapid Spanning Tree (RSTP, 802.1w), que permite marcar esos puertos para evitar el problema de tener que recalcular el spanning tree cada vez que una estación se apaga o se enciende

75. Respecto de los protocolos 10Gigabit Ethernet, podemos decir:

- a. A diferencia de Gigabit Ethernet (GBE) no es capaz de soportar trunking 802.3ad (Link Aggregation Control Protocol, LACP)
- b. Utiliza el mismo formato y tamaño de trama que Gigabit Ethernet
- c. En su versión 10GBASE-LX4 funciona en primera ventana (850 nm) y utiliza la codificación 8B/10B
- d. En su versión 10GBASE-LX4 funciona en segunda ventana (1310 nm) y utiliza la codificación 64B/66B y 4 longitudes de onda

76. Sobre la tecnología Asynchronous Transfer Mode (ATM) podemos decir:

- a. Soporta nativamente el multicast
- b. Permite establecer circuitos virtuales permanentes (PVC) o conmutados (SVC); los SVCs se crean manualmente asignando entradas en la tabla de conmutación mientras que para establecer los PVCs utiliza señalización Q2931 a través de los circuitos reservados
- c. Es una tecnología que ha sustituido completamente a POS (Packet over Sonet) por reducir mucho la complejidad y el overhead
- d. Ofrece 4 categorías de tráfico: CBR para capacidad constante, VBR para un tráfico medio pero permitiendo ráfagas, ABR que fija un mínimo garantizado y un máximo orientativo y UBR que opera sin garantías

77. Respecto de Asymmetric Digital Subscriber Line (ADSL) podemos afirmar:

- a. La técnica Discrete Multi Tone (DMT) divide el espectro de frecuencia en canales de 4,3 kHz
- b. Trabaja en un rango de frecuencias de 2 kHz a 4 kHz en el sentido del usuario a la red, y entre 25 kHz y 150kHz de la red al usuario
- c. La comunicación es Half-Dúplex
- d. En cada hogar conectado hay un Digital Subscriber Line Access Multiplexer (DSLAM) que es el encargado de multiplexar los canales de voz, datos y televisión por una única línea de comunicación

78. ¿Cuál de las siguientes direcciones IPv4 no corresponde a un rango de direccionamiento privado?

- a. 10.28.128.186
- b. 126.145.12.216
- c. 172.30.32.224
- d. 192.168.192.55

79. ¿Cuál de las siguientes combinaciones de dirección IP y máscara pertenece a una subred mayor, esto es, con más direcciones IP?

- a. 10.28.128.186/255.255.255.0
- b. 126.145.12.216/16
- c. 172.30.32.225/255.255.255.252
- d. 192.168.192.55/24

80. Entre los protocolos TCP/IP el denominado Open Shortest Path First (OSPF) se clasifica como:

- a. Exterior Gateway Protocol, pues se intercambia información de encaminamiento entre sistemas autónomos
- b. Internal Gateway Protocol, que utiliza exclusivamente la métrica del vector distancia
- c. Internal Gateway Protocol, que utiliza el estado del enlace
- d. External e Internal Gateway Protocol, de encaminamiento híbrido interno y entre sistemas autónomos

81. Respecto de IPv6 podemos afirmar:

- a. La base de su funcionamiento es la utilización de datagramas de tipo broadcast, y desaparece del mismo los multicast
- b. El espacio de direcciones es prácticamente inagotable, pues es de 128 bytes
- c. Debido a su completa incompatibilidad con IPv4 en un mismo equipo, la transición de una a otra ha de ser mediante la sustitución ordenada de todo el equipamiento por zonas
- d. Se pueden utilizar los últimos bytes de la dirección para incluir una parte local única, como por ejemplo la MAC

82. Respecto de algunos protocolos TCP/IP, podemos decir:

- a. Se utiliza el protocolo ARP para conocer la dirección IP para una MAC dada, para lo que necesariamente debe consultar una tabla estática de correspondencias
- b. Los mensajes ICMP están encapsulados y se envían dentro de datagramas IP con el campo protocolo con valor 4
- c. El protocolo UDP es no orientado a conexión, por lo que es menos fiable y no puede ser utilizado para aplicaciones en tiempo real
- d. El protocolo TCP es orientado a conexión, estableciéndola mediante una negociación en tres pasos (SYN, SYN/ACK y ACK)

83. ¿Qué tipo de registro del DNS ayuda a combatir el Spam, especificando cual o cuales hosts están autorizados a enviar correo desde el dominio dado?

- a. CNAME
- b. SOA
- c. LOC
- d. SPF

84. Respecto de algunos protocolos TCP/IP, se puede decir:

- a. FTP es un protocolo sin cifrar que usa el puerto 21, y su contrapartida con cifrado, SSH File Transfer Protocol (SFTP) utiliza el puerto 20
- b. HTTP es un protocolo en el que el cliente se comunica con el servidor por medio de un determinado método (HEAD, GET, POST, PUT, etc.); los datos que intercambian lo hacen precedidos de determinados encabezados específicos (Host, Server, Content-Length, Content-Type, etc.) que indican cosas como las acciones requeridas, tipos de datos, códigos de estado, etc
- c. SMTP utiliza exclusivamente el puerto 25 a través de UDP para enviar mensajes
- d. El protocolo DHCP permite asignar direcciones IP de forma dinámica pero, a diferencia de BootP, no permite la asignación estática o automática

85. De los protocolos WPA y WPA2 podemos decir:

- a. WPA2 incluye el cifrado completo estandarizado en 802.11i con cifrado AES
- b. WPA2 está basado en el estándar 802.11i mientras que WPA no incluye cifrado
- c. WPA sólo autentica con clave compartida preestablecida (PSK) y por eso también se le conoce por WPA-Personal
- d. El protocolo de cifrado WEP, que utiliza un vector de inicialización de 24 bits, es fácil de romper mientras que WEP2, que lo utiliza de 48 bits, es seguro a día de hoy

86. Sobre la especificación 802.11n podemos afirmar:

- a. Utiliza las bandas de 2,45 y 5,8 GHz, y construye canales de 400 MHz por combinación de dos de 200 MHz
- b. Utiliza Multiplexación por División de Frecuencias Ortogonales (OFDM) con mejoras respecto a sus predecesoras
- c. La utilización de la técnica MIMO (Multiple Inputs, Multiple Outputs), hace que pueda usar hasta dos antenas simultáneamente, por lo cual consigue tasas de 600 Mbps
- d. Introduce la desagregación MAC, que consiste en dividir cada trama en pequeñas celdas, que se transmiten mucho más rápidamente que las tramas originales. En la estación de destino se deben volver a juntar todas para volver a reconstruir la trama original

87. Sobre la autenticación en redes inalámbricas podemos decir:

- a. La especificación 802.1X determina un sistema que se compone de una estación cliente, un punto de acceso inalámbrico y un servidor de autenticación. Es aplicable a las redes inalámbricas pero no a las cableadas
- b. Un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP es RADIUS (Remote Authentication Dial-In User Server), el cual comprueba que la información del usuario es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP y, si es aceptado, el servidor le autorizará el acceso al sistema
- c. El gran inconveniente de la autenticación RADIUS es que no se pueden implementar servicios de roaming
- d. Los protocolos EAP (Extensible Authentication Protocol) como EAP-TLS, EAP-TTLS y EAP-PEAP utilizan todas ellas credenciales de nombre y contraseña para autenticar al usuario, y de certificado digital para el servidor, y se diferencian entre sí por el método de cifrado

88. A propósito del protocolo SNMP podemos decir:

- a. Gestiona dispositivos conectados a la red bien por sondeo de los mismos o por notificación de eventos, para lo que utiliza los puertos TCP 161 en el gestor de eventos y 162 en el agente que lleva a cabo las operaciones de gestión
- b. Accede a una Base de Información de Administración (MIB), que es una colección de variables a controlar que, al no estar estandarizada, puede ostentar una organización cualquiera, siendo lo más usual una jerarquía en tres niveles
- c. Opera en el nivel de Transporte de OSI. La comunicación entre gestores y agentes se realiza por medio de mensajes SNMP tales como: GetRequest, SetRequest, GetNextRequest, GetBulkRequest, Response, Trap e InformRequest, y contempla hasta cuatro tipos de datos: Entero, Cadena de octetos, Dirección física, y Contador
- d. En su versión 3 incorpora mejoras de seguridad, tales como cifrado de los paquetes, integridad de los mensajes y autenticación de la fuente

89. A propósito de RMON (Remote Network MONitoring) podemos decir:

- a. RMON es una extensión de SNMP; define nuevos objetos de gestión y funciona de modo que los agentes RMON recopilan periódicamente la información sobre ellos. El gestor recoge la información estadística de la red con lecturas SNMP de los objetos RMON, lo que implica que para que RMON funcione SNMP debe estar habilitado
- b. RMON es una alternativa a SNMP; define objetos de gestión y funciona de modo que los agentes RMON recopilan periódicamente la información sobre ellos. El gestor recoge la información estadística de la red con lecturas de los objetos RMON y de los equivalentes SNMP, lo que implica que para que RMON funcione SNMP debe estar deshabilitado
- c. RMON es protocolo de gestión necesario para el funcionamiento de SNMP, pues su funcionamiento se basa en que el gestor recoge la información estadística de la red con lecturas RMON de los objetos SNMP, lo que implica que para que SNMP funcione RMON debe estar habilitado
- d. Los objetos de gestión se organizan en varios grupos, los cuales son opcionales aunque con dependencias: el grupo hostTopN requiere la implementación del grupo host, el grupo event requiere la implementación del grupo alarm, y el grupo filtre requiere la implementación del grupo capture

90. Podemos afirmar, a propósito de los cortafuegos:

- a. En todas las arquitecturas existe lo que se llama un host bastión, que consiste en un sistema que ofrece servicios a los usuarios de la red interna pero que ha de ser invisible desde el exterior
- b. En arquitecturas de doble cortafuegos uno de ellos independiza la red externa de la red interna, y el segundo de ellos la red interna de la denominada zona desmilitarizada (DMZ); es decir, que para acceder a la DMZ desde el exterior hay que forzar la seguridad de los dos cortafuegos
- c. Aquellos que funcionan por filtrado de paquetes mantienen listas de acceso con determinadas reglas. Sus limitaciones son que no pueden operar por puertos u otra característica del paquete, ni tampoco aplicar reglas de aceptar todo, sólo de descartar
- d. Los cortafuegos de inspección de estados (stateful firewalls) tiene en cuenta además la posición del paquete en el flujo de datos, de modo que si al de comienzo de una sesión se le aplica una regla, a todos los demás del mismo flujo se les aplicará la misma regla

91. Respecto de los protocolos utilizados para establecer redes privadas virtuales (VPN) podemos afirmar:

- a. PPTP (Point to Point Tunneling Protocol) se utiliza para encapsular tramas PPP sobre IP; utiliza el puerto 172 para la gestión del túnel y es muy seguro puesto que exige el uso de infraestructura PKI
- b. IPSec determina que antes de intercambiar información segura ambos equipos acuerden por el método IKE el password a utilizar en la comunicación; tras ello ya se pueden usar los protocolos ESP o AH (mejor este último pues permite el cifrado)
- c. SSTP (Secure Socket Tunneling Protocol) proporciona un mecanismo de encapsulación de tráfico PPP sobre el canal SSL del protocolo HTTPS, por lo que obtiene de éstos la seguridad a nivel transporte con negociación de claves mejorada, cifrado y comprobación de integridad
- d. L2TP (Layer 2 Tunneling Protocol) permite túneles en conexiones tanto de red a red como de usuario a red. Funciona encapsulando los paquetes en tramas PPP, que cifra y comprime para encapsularlas después en paquetes TCP por el puerto 1700. Es multiprotocolo y permite NAT pero su gran pega es no permitir multicast

92. De acuerdo con el artículo 148 de la Constitución Española de 1978, las comunidades autónomas podrán asumir competencias en materia de:

- a. Ordenación del territorio, urbanismo y vivienda
- b. Régimen aduanero y arancelario
- c. Legislación sobre pesas y medidas, determinación de la hora oficial
- d. Fomento y coordinación general de la investigación científica y técnica

93. De acuerdo con el artículo 29 del Estatuto de Autonomía de la Comunidad Valenciana,

- a. La Diputación es el órgano colegiado de gobierno de la Generalitat, que ostenta la potestad ejecutiva y reglamentaria
- b. Los miembros del Consell que reciben el nombre de diputados son designados por el president de la Generalitat
- c. La sede del Consell será la ciudad de Valencia
- d. Todas las normas, disposiciones y actos emanados del Consell, que por su naturaleza lo exijan, serán publicados en el Boletín Oficial del Estado

Preguntas de Reserva

94. ¿Cuál de estos comandos NO serviría para crear una cuenta para el usuario "test" en el dominio upvnet.upv.es, ejecutándolo en un Windows 2008 que es controlador de dicho dominio?

- a. dsadd user "cn=test,cn=Users,dc=upvnet,dc=upv,dc=es"
- b. powershell "Import-Module Active Directory; New-ADUser -Path 'cn=Users,dc=upvnet,dc=upv,dc=es' -Name 'test'"
- c. net user test * /add
- d. Idifde -d upvnet.upv.es -u test

95. En un pool de servidores XenServer, se quiere migrar una VM (máquina virtual) de un servidor a otro pero al intentar hacer esta operación, el administrador se da cuenta que esta opción no está disponible. ¿ A qué puede ser debida esta situación ?
- La VM no tiene instaladas las XenServer Tools.
 - Word Load Balancing no está habilitado.
 - La VM está ejecutándose en el servidor maestro del pool.
 - La VM fue creada utilizando fast cloning en vez de full copy
96. ¿Que es OC4J?
- Un compilador java de código abierto
 - Un entorno de desarrollo de applets java
 - Un entorno de desarrollo de javascript
 - Una implementación de un servidor de aplicaciones J2EE
97. Deseamos ver el estado de los nodos en cluster HP-UX Service Guard. ¿Qué instrucción deberíamos utilizar?
- clustat
 - lsnodes
 - sgnodes
 - cmviewcl
98. Respecto de las arquitecturas complejas orientadas a la computación podemos decir que:
- OpenMP es una interfaz de programación de aplicaciones (API) para la programación multiproceso de memoria compartida en múltiples plataformas
 - Un clúster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, que presenta un alto rendimiento y alta disponibilidad pero a costa de la escalabilidad, no pudiendo presentar por tanto balanceo de carga
 - Los distintos nodos que forman un clúster se interconectan mediante una red que puede ser Ethernet o Myrinet, y disponen de un Middleware llamado InfiniBand que supone una capa de abstracción para el usuario
 - Las técnicas del multihilo o *multithreading* son las que permiten a los procesadores multinúcleo realizar las tareas en paralelo

99. De acuerdo con el artículo 4 de la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal, respecto de la calidad de los datos:
- Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido
 - Los datos de carácter personal objeto de tratamiento no podrán usarse con fines históricos, estadísticos o científicos
 - Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado
 - Los datos de carácter personal no serán cancelados cuando hayan dejado de ser pertinentes para la finalidad para la cual hubieran sido recabados o registrados, y deberán usarse con fines históricos, estadísticos o científicos
100. De acuerdo con el artículo 11 de la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal, respecto de la comunicación de datos, será necesario el consentimiento previo del interesado para la comunicación de los datos de carácter personal objeto de tratamiento:
- Para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario
 - Cuando se trate de datos recogidos de fuentes accesibles al público
 - Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos
 - Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica
101. En un centro de la Universitat Politècnica de València se retira un equipo informático estropeado de tamaño pequeño, que no se puede reutilizar. De acuerdo con el sistema de gestión de los residuos no peligrosos, para gestionar la recogida del residuo se debe hacer lo siguiente:
- Dejarlo en la papelera más próxima
 - Llevarlo al contenedor amarillo, ya que cada día los equipos electrónicos llevan más componentes de plástico
 - Depositarlo en el contenedor gris
 - Depositarlo en el servicio de informática