

SUPUESTO 1

El Centro de Proceso de Datos de una administración pública dispone de un armario de comunicaciones (rack) con los siguientes dispositivos físicos:

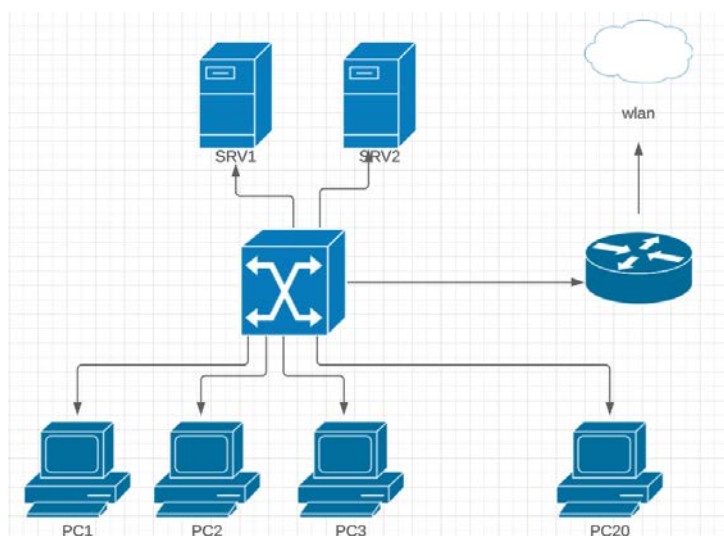
- 1 Switch 24 portGigabitEthernet + 2 SFP+
- 1 Router 4 portGigabitEthernet + 2 port SFP + WIFI
- 2 Servidores 2 CPU 8 cores + 128 GB RAM + 2 HD 500 GB
- 1 Sistema de alimentación interrumpida (SAI)

En dicha administración trabajan 20 empleados. Cada empleado dispone de un PC con sistema operativo Microsoft Windows 10. Dichos PC están conectados al switch del rack mediante cable ethernet puerto RJ45. Todos los empleados tienen conexión a internet.

La infraestructura de red dispone de 2 servidores con sistema operativo Microsoft Windows Server 2022. Estos servidores son los controladores de dominio (SRV1 y SRV2) basados en el directorio activo de Microsoft Windows Server (Active Directory) con el sistema de nombres de dominio activo (DNS). El nombre de dominio de la entidad se ha denominado *ayuntamiento.es*. Estos servidores están conectados al switch del rack mediante cable ethernet puerto RJ45. Los servidores tienen conexión a internet.

La topología lógica de la red es en estrella. Toda la red tiene el mismo direccionamiento IPv4. El enlace entre el switch y el router va cableado mediante fibra óptica. La conexión a internet es también mediante fibra óptica.

El diseño de la infraestructura de red de la administración pública es el siguiente:



PREGUNTAS SUPUESTO 1

1. ¿Cuál sería el direccionamiento IPv4 correcto para la red privada de la administración pública en formato CIDR?
 - a) 147.84.0.0/8
 - b) 237.10.0.0/24
 - c) 192.168.0.0/8
 - d) 172.28.0.0/12
2. En la topología en estrella del supuesto, ¿cuál es una característica?
 - a) Vulnerabilidad máxima en el nodo central
 - b) El coste del cableado puede ser alto
 - c) Permite aumentar o disminuir con sencillez el número de estaciones
 - d) Todas son características de una topología en estrella
3. El departamento de informática ha decidido segmentar la red en dos subredes lógicas: una para los empleados y otra para los servidores. ¿Qué tecnología de red utilizarías?
 - a) VLAN
 - b) FTTH
 - c) RADIUS
 - d) LAN
4. Recientemente se ha incorporado un nuevo trabajador a la plantilla de la administración pública. Indique los pasos a seguir para unir el PC del nuevo empleado al dominio `ayuntamiento.es`
 - a) Propiedades del sistema → Opciones avanzadas → Botón Cambiar
 - b) Configuración → Sistema → Pestaña "Nombre de equipo" → Botón Dominio
 - c) Propiedades del sistema → Pestaña "Nombre de equipo" → Botón Cambiar
 - d) Ninguna es correcta
5. Desde la consola de comandos de Windows, ¿cómo podemos mostrar equipos y recursos de uso compartido disponibles en el equipo PC3?
 - a) Netstat\\PC3
 - b) Net view \\PC3
 - c) Netuse\\PC3
 - d) Net stat\\PC3
6. Para la gestión de los dispositivos de la red (equipos, impresoras, switches...), la organización tiene contratado un software con el que lleva a cabo el inventario. ¿Qué protocolo hace que funcione este software?
 - a) SNMP
 - b) IPP
 - c) SMTP
 - d) TFTP

7. Se ha decidido por parte de la jefatura del departamento de informática utilizar la asignación automática direcciones IP para la red de la administración pública, ¿cuál es el rol o característica que debería tener activo los servidores SRV1 y SRV2?
- a) DNS
 - b) ICMP
 - c) DHCP
 - d) VPN
8. En la infraestructura de red de la administración, seleccione la opción incorrecta en relación con los dispositivos de interconexión utilizados.
- a) El router opera en la Capa 2 o Nivel de Enlace del modelo OSI
 - b) El enrutamiento de paquetes es una característica de los routers y switches multicapa
 - c) Un router permite interconectar redes heterogéneas o redes diferentes
 - d) El switch es utilizado para conectar varios dispositivos en una LAN
9. Para realizar tareas de soporte y mantenimiento, se le pide como operador de informática que debe habilitar la herramienta 'Escritorio remoto' de Windows 10 en los PCs de los trabajadores. ¿Cómo debería proceder para habilitar dicha herramienta?
- a) Configuración → Personalización → Escritorio Remoto
 - b) Configuración → Red e Internet → Ethernet → Escritorio Remoto
 - c) Configuración → Sistema → Características opcionales → Habilitar el botón
 - d) Configuración → Sistema → Escritorio Remoto → Habilitar el botón
10. El administrador de sistemas ha realizado un cambio en la configuración de las directivas de grupo (GPO) dentro del dominio. Se le pide que actualice la configuración de las directivas de grupo a los equipos de los empleados. ¿Cómo debería actuar para aplicar la configuración de directiva?
- a) gpresult /pc1
 - b) nslookup /pc1
 - c) gpupdate /force
 - d) No se pueden actualizar puesto que es una directiva de dominio
11. El departamento de informática ha decidido utilizar el siguiente direccionamiento IPv4 para la infraestructura de red: 172.16.0.0/24 y máscara de subred 255.255.255.0/24. Indicar cuál sería la dirección de red, la dirección de difusión y el rango de direcciones utilizado.
- a) Dirección de red 172.16.0.1; Dirección de difusión 172.16.0.255; Rango de direcciones 172.16.0.2 - 172.16.0.254

- b) Dirección de red 172.16.0.0; Dirección de difusión 172.16.0.255; Rango de direcciones 172.16.0.1 - 172.16.0.254
- c) Dirección de red 172.16.1.0; Dirección de difusión 172.16.1.254; Rango de direcciones 172.16.1.1 - 172.16.1.253
- d) Ninguna de las anteriores

12. En cuanto a la tecnología WIFI a utilizar se está valorando utilizar la tecnología que proporcione mayores velocidades, se decide que debe operar dentro de la banda de los 5Ghz. ¿Cuál de las siguientes proporciona las mayores velocidades teniendo en cuenta dichos requisitos?

- a) 802.11i
- b) 802.11n
- c) 802.11ac
- d) 802.11ad

13. En la entidad local se va a implantar la red WIFI segura, de forma que el acceso a la misma no esté basado en una clave compartida entre todos los usuarios. ¿Qué protocolos y estándares se utilizarán para proporcionar la autenticación y cifrado en dicha red WIFI?

- a) WEP-TKIP
- b) WPA-TKIP
- c) WPA2-AES
- d) WPS-AES

14. ¿Qué comando utilizarías en uno de los equipos para mostrar la información de su conexión, incluyendo su dirección IP, máscara de subred, puerta de enlace y servidores DNS?

- a) ipconfig /all
- b) ipconfig /interfaces
- c) ipconfig -a
- d) a) y c) son correctas

15. El Centro de Proceso de datos de la administración tiene un nivel Tier IV. ¿Qué afirmación no es correcta con respecto al CPD?

- a) Cada servidor dispone de doble fuente de alimentación
- b) Tiene una disponibilidad superior al 99,99%
- c) Los SAIs están duplicados
- d) Dispone de una línea de distribución eléctrica

SUPUESTO 2

Usted se ha incorporado a la plantilla de una entidad local como operador de informática. El jefe del departamento de informática le hace saber que la entidad cumple con las especificaciones y requisitos de seguridad exigidas por la legislación vigente en materia de seguridad de la información y protección de datos.

Con el objeto de garantizar la protección y seguridad de la infraestructura frente a posibles amenazas y vulnerabilidades, la entidad tiene implementadas las siguientes medidas de seguridad en sus sistemas de información:

- Sistema de identificación y autenticación de usuarios mediante contraseñas y certificados digitales
- Firewall 8 GE SFP + UnifiedThreatProtection (UTP)
- Antivirus corporativo
- Sistema de copias de seguridad
- Sistema de acceso remoto a los servicios y programas de la red corporativa para los teletrabajadores

También se le comunica que recientemente se ha implantado un servidor web en la infraestructura de red de la entidad local en una zona desmilitarizada (DMZ). Este servidor es el portal principal de la entidad y está basado en un gestor de contenidos (Joomla) que contiene información corporativa e institucional de la entidad.

PREGUNTAS SUPUESTO 2

1. Con la implantación del teletrabajo se ha facilitado a los usuarios portátiles para trabajar desde casa. Si se quieren conectar desde su casa a la red de la empresa, para que la conectividad del trabajador se pueda realizar de forma segura, ¿qué tipo de acceso implantaría?
 - a) Permitir conexiones directas a las aplicaciones corporativas a través de internet
 - b) Utilizar un switch virtual FTTH del operador de telecomunicaciones
 - c) Establecer túneles VPN a través de internet hacia la red corporativa
 - d) Utilizar https para facilitar el acceso a través de un navegador web

2. Para mejorar la seguridad, se quiere permitir en el firewall los puertos seguros SSL. ¿Qué protocolo seguro de comunicación y qué puerto tendrían que abrirse para el servidor web, el servidor de correo entrante y para el saliente?
- a) html-443, smtps 465, imaps 993
 - b) html-443, smtps 993, imaps 143
 - c) https-993, smtps 443, imaps 465
 - d) https-443, smtps 465, imaps 993
3. Las copias de seguridad son un aspecto importante para la entidad y forman parte de las tareas cotidianas de los administradores de sistemas. La entidad cuenta con la siguiente política de seguridad: los domingos se realiza una copia completa y a diario una copia diferencial. Si se produce un ataque el miércoles, en el caso de querer restaurar la información, ¿qué debería restaurar?
- a) Únicamente es necesaria la copia del martes
 - b) La copia del domingo y la del martes
 - c) La copia del domingo, la del lunes y la del martes
 - d) La copia del domingo y la del lunes
4. El secretario de la entidad tiene instalado en su ordenador un certificado digital para la firma de documentos oficiales. Se le pide hacer una copia de seguridad y para ello se dispone a exportarlo del almacén de certificados del navegador. ¿Qué extensión tendrá el archivo que contiene la clave privada y sirve como copia de seguridad del certificado digital?
- a) der
 - b) pfx o p12
 - c) pwp
 - d) cero crt
5. Un usuario de la entidad ha solicitado a la FNMT el certificado digital de empleado público y cuando ha recibido el mensaje para poder descargarlo se genera el siguiente error: "Error: No se ha encontrado la clave privada". ¿A qué puede deberse?
- a) Que no esté utilizando el mismo equipo o con los que obtuvo el código de solicitud.
 - b) Que no haya introducido la contraseña correcta que protege la solicitud.
 - c) a) y b) son correctas
 - d) Ninguna es correcta. El error se debe a un problema en la descarga de FNMT

6. La 2FA o doble factor de autenticación, supone en Seguridad Informática:

- a) Añadir dos caracteres alfanuméricos a nuestra contraseña habitual y cambiarla periódicamente, añadiendo así una capa adicional de seguridad.
- b) Identificarse en una cuenta de usuario utilizando dos pasos en lugar de uno, confirmando así que el usuario es realmente el propietario de la cuenta.
- c) Añadir un mayor nivel de seguridad al acceso a las cuentas, al solicitarse, además de la contraseña habitual, un código de seguridad.
- d) b) y c) son correctas

7. ¿En qué consiste la estrategia 3-2-1 para diversificar las copias de seguridad?

- a) En mantener 3 copias de cualquier fichero, 2 almacenadas en distintos soportes y 1 cifrada
- b) En mantener 3 copias de cualquier fichero, 2 almacenadas de forma cifrada y 1 almacenada en la nube
- c) En mantener 3 copias de cualquier fichero, 2 almacenadas fuera de la organización y 1 cifrada
- d) En mantener 3 copias de cualquier fichero, 2 almacenadas en distintos soportes y 1 fuera de la organización o en la nube

8. ¿Cómo se conoce a un tipo de ataque en el cual se cifra la información contenida en los sistemas de almacenamiento y exigen una cantidad económica para desbloquearlo?

- a) Adware
- b) Ransomware
- c) Smurf
- d) Hoax

9. Indique la respuesta correcta que resume el funcionamiento de la firma digital con criptografía de clave pública, garantizando autenticidad del origen, el no repudio en origen y la integridad

- a) El emisor calcula un hash del mensaje, lo cifra con su clave pública y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza la clave privada del emisor para descifrar el criptograma
- b) El emisor calcula un hash del mensaje, lo cifra con su clave privada y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza su clave privada para descifrar el criptograma
- c) El emisor calcula un hash del mensaje, lo cifra con su clave pública y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza su clave privada para descifrar el criptograma

- d) El emisor calcula un hash del mensaje, lo cifra con su clave privada y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza la clave pública del emisor para descifrar el criptograma

10. ¿A qué dimensión de seguridad afecta un ataque realizado con un sniffer?

- a) Integridad
- b) Disponibilidad
- c) Autenticación
- d) Confidencialidad

11. Las extensiones son paquetes de software que extienden la instalación Joomla predeterminada. Indicar cual de las siguientes es una extensión en Joomla

- a) Componente
- b) Idioma
- c) Modulo
- d) Todas las anteriores son extensiones en Joomla

12. Por seguridad, la entidad hace copia de seguridad de la web municipal cada mes. Teniendo en cuenta que no se tiene instalado en Joomla ningún plugin que realice esa tarea, ¿cómo harías la copia de seguridad manualmente?

- a) Copiar la base de datos en la que se apoya el sitio web y la estructura de directorios y archivos del sitio web
- b) Copiar el archivo configuration.php y la estructura de directorios y archivos del sitio web
- c) Copiar solo el archivo configuration.php y la base de datos
- d) No se puede realizar la copia manualmente

13. Indicar cual de las afirmaciones es cierta en relación al cortafuegos

- a) Redirige el tráfico a la zona desmilitarización evitando que se acceda a la red local
- b) Bloquea accesos no autorizados a un ordenador, mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados
- c) Monitoriza el tráfico de internet entrante y saliente mediante un proxy
- d) Todas las anteriores son correctas

14. Indique cual de los siguientes no es un formato de firma avanzada admitido, atendiendo a la política de seguridad de la entidad

- a) XAdES
- b) CAdES
- c) PAdES

d) TAdES

15. ¿Cuál de las siguientes afirmaciones relativas a la VPN no es correcta?

- a) Utiliza los protocolos de comunicación L2TP/IPSec
- b) La velocidad de acceso es mayor que el de una conexión tradicional
- c) Utiliza los protocolos de cifrado AES-256
- d) Las VPN reducen los costos y son sencillas de usar