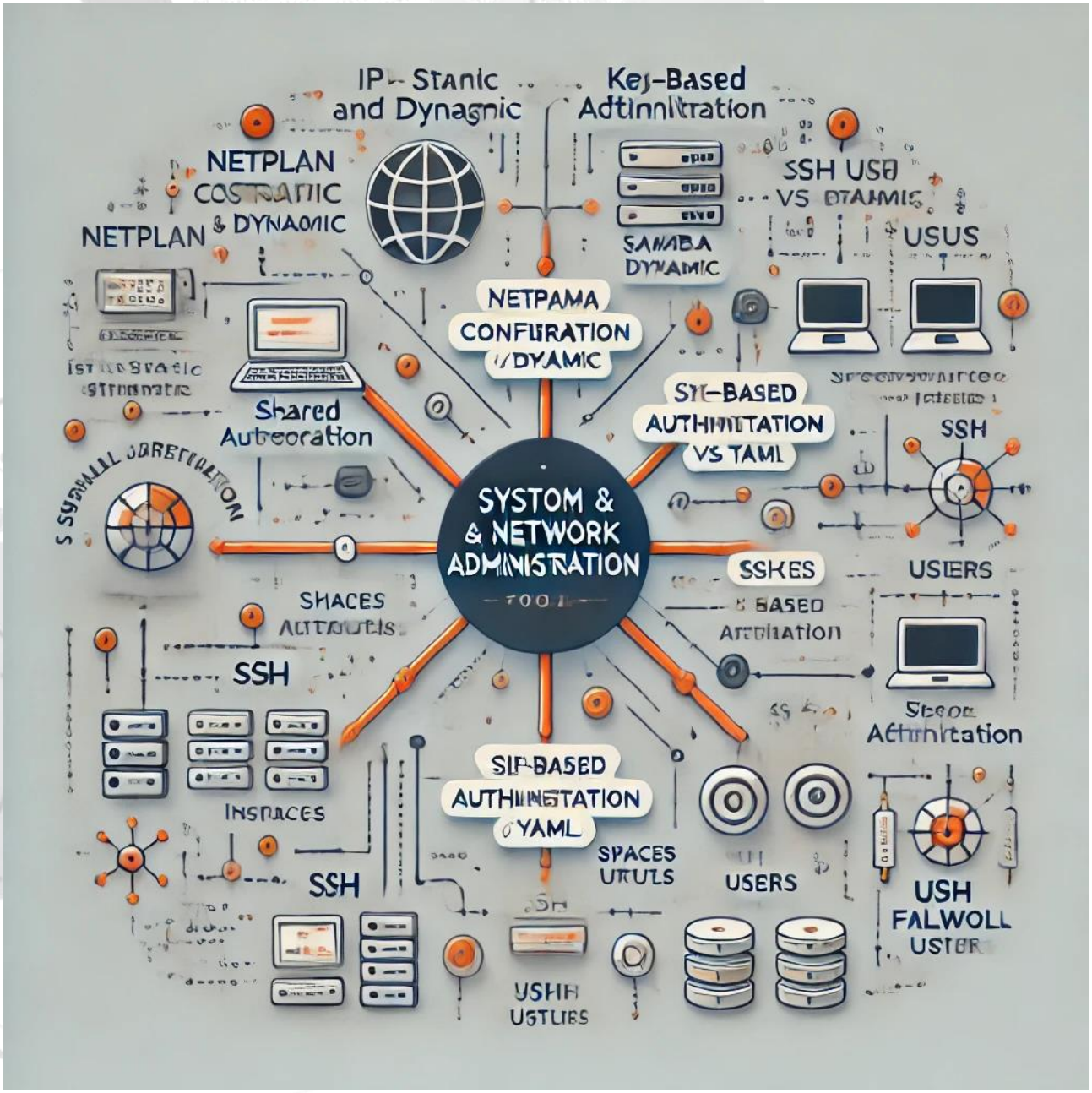
Preparación de Examen

CFGS Desarrollo de aplicaciones web

Sistemas informáticos

Eduardo de Lorenzo Ramos



Contenido

UT01 - Hardware de un sistema informático

UT01 – 1. Secuencia abreviada de instalación

ID	Descripción	Explicación
1	**Escoge una placa base compatible con procesadores Intel o AMD según el socket.**	Este paso es fundamental porque el procesador debe encajar físicamente y ser compatible electrónicamente con la placa base. Elegir una placa base con el socket adecuado asegura que los componentes clave funcionen correctamente.
2	**Usa el manual de la placa para verificar compatibilidad entre procesador y socket.**	Los procesadores tienen requisitos específicos, como el tipo de socket y chipset. Verificar la compatibilidad asegura que el procesador sea reconocido por la placa y que se aprovechen sus funciones.
3	**Coloca el procesador alineando el triángulo dorado según las instrucciones del manual.**	Es vital alinear correctamente el procesador porque sus pines o contactos deben encajar con precisión en el socket. Una colocación incorrecta puede dañar el procesador o la placa base.
4	**Aplica pasta térmica y monta el disipador con ventilador correctamente orientado.**	La pasta térmica mejora la transferencia de calor entre el procesador y el disipador, evitando el sobrecalentamiento. Montar el disipador correctamente asegura una disipación eficiente del calor generado.
5	**Instala módulos de memoria RAM compatibles, asegurando orientación correcta.**	La memoria RAM debe insertarse en las ranuras específicas y con la orientación adecuada para que la placa base pueda detectarla. Este paso es crucial para garantizar el correcto funcionamiento del sistema.
6	**Fija la placa base dentro de la carcasa alineando orificios y tornillos.**	La placa base debe asegurarse físicamente en la carcasa para proporcionar estabilidad y para que todos los demás componentes (como discos y cables) se puedan conectar correctamente.
7	**Instala la fuente de alimentación adecuada (mínimo 650W) conectando componentes.**	Una fuente de alimentación adecuada proporciona energía suficiente para todos los componentes del sistema. Este paso asegura que la computadora pueda operar de manera estable bajo carga.
8	**Monta discos M.2, SSD o HDD según las instrucciones del manual.**	Instalar el almacenamiento en este momento permite conectar los cables de datos y alimentación sin interferir con otros componentes que se puedan montar más adelante.
9	**Conecta cables de botones, luces y puertos frontales de la carcasa a la placa base.**	Este paso permite que los controles externos de la carcasa (como el botón de encendido) y los puertos frontales funcionen, haciendo el equipo operable desde el exterior.
10	**Conecta todos los cables de la fuente de alimentación a los dispositivos correspondientes.**	Este paso final asegura que todos los componentes reciban la energía necesaria para funcionar, completando el ensamblaje del sistema. Sin esto, la computadora no puede arrancar.

UT01 – 2. Listado de conectores por grupo

Grupo	Nombre	Función
Conectores de almacenamiento	**Puerto IDE**	Permite la conexión de discos duros y unidades ópticas antiguas mediante cables planos.
	Conectores SATA	Conectan discos duros HDD, SSD y unidades ópticas modernas para la transferencia de datos.
	Puertos eSATA	Facilitan la conexión de discos duros externos con transferencia de alta velocidad.
Conectores de energía	**Conector ATX de alimentación**	Proporciona energía principal a la placa base y todos sus componentes.
	Conector ATX 12V	Suministra energía de 12V específica para la CPU.

Grupo	Nombre	Función
	Conector adicional ATX (4 pines)	Garantiza un suministro extra de energía al procesador para mayor estabilidad.
Ranuras de expansión	**Ranuras PCI**	Permiten agregar tarjetas de expansión como sonido, red o video.
	Ranura PCIe x16	Diseñada para tarjetas gráficas modernas con mayor capacidad de transferencia de datos.
Conectores para periféricos	**Conector de panel frontal**	Habilita funciones como encendido, reinicio y conexión a puertos USB desde la parte frontal de la carcasa.
	Conectores USB 2.0 y USB 3.0	Proveen conectividad para dispositivos periféricos como teclados, ratones y discos externos.
	Conectores PS/2 (teclado y ratón)	Compatibles con hardware antiguo, permiten la conexión de teclado y ratón mediante puertos dedicados.
Conectores de audio y video	**Puerto VGA**	Transmite señales de video analógicas a monitores.
	Puerto HDMI	Transfiere señales de audio y video digital de alta definición.
	Puerto DVI	Compatible con señales digitales y analógicas para monitores.
	Conectores de audio (jack 3.5mm)	Facilitan la entrada y salida de señales de audio mediante auriculares y micrófonos.
	Conector S/PDIF óptico	Transfiere audio digital de alta calidad evitando interferencias electromagnéticas.
	Conector de audio coaxial	Conecta sistemas de sonido envolvente a través de señales de audio analógicas.
Conectores y puertos especializados	**Puerto FireWire (IEEE 1394)**	Diseñado para transferencias rápidas de datos en dispositivos multimedia como cámaras digitales.
	Puerto COM y LPT	Usados para conectar dispositivos industriales, impresoras de tickets o sensores antiguos.
	Puerto joystick/MIDI	Facilita la conexión de dispositivos MIDI e instrumentos musicales.
Componentes internos	**Socket CPU**	Conecta la CPU física y lógicamente a la placa base.
	Ranuras DIMM	Permiten instalar módulos de memoria RAM para tareas de procesamiento temporal.
	Batería CMOS	Mantiene la configuración del BIOS y la hora del sistema cuando el equipo está apagado.
	Chipset	Gestiona la comunicación entre la CPU, memoria RAM y otros dispositivos de la placa base.
Conectores auxiliares	**Conector de ventilador del chasis**	Controla y alimenta los ventiladores del sistema para la refrigeración del equipo.
	Puerto AAFP	Conecta puertos de audio frontales del chasis para auriculares y micrófonos.

UT03 - Introducción a los sistemas en red

UT03 – 1. Comparativa entre modelos OSI y TCP/IP

Capa (Modelo OSI)	Capa (Modelo TCP/IP)	Función principal
Capa 7: Aplicación	**Capa de Aplicación**	Proporciona servicios de red a las aplicaciones del usuario final (HTTP, FTP, SMTP, etc.).
Capa 6: Presentación		Traduce y formatea los datos para la capa de aplicación (cifrado, compresión, etc.).
Capa 5: Sesión		Gestiona las sesiones entre aplicaciones (establecimiento, mantenimiento y finalización).
Capa 4: Transporte	**Capa de Transporte**	Gestiona la transmisión de datos entre dispositivos. Usa protocolos como TCP (fiable) y UDP (rápido).
Capa 3: Red	**Capa de Internet**	Define cómo se enrutan los paquetes entre dispositivos a través de múltiples redes usando direcciones IP.
Capa 2: Enlace de datos	**Capa de Acceso a Red**	Gestiona la transferencia de datos dentro de una red local usando direcciones MAC.
Capa 1: Física		Define los medios físicos de transmisión (cables, señales eléctricas, etc.).

UT03 – 2. Topologías de red

Tipo de Topología	Descripción	Ventajas	Desventajas
Estrella	Todos los dispositivos están conectados a un nodo central, generalmente un switch o hub.	- Fácil de instalar y administrar. - Fallos en un dispositivo no afectan al resto de la red.	- Dependencia del nodo central; si falla, toda la red se cae.
Bus	Todos los dispositivos están conectados a un único cable principal (bus).	- Fácil de implementar en pequeñas redes. - Uso eficiente de cables.	- Difícil de solucionar problemas. - Si el cable principal falla, toda la red se cae.
Anillo	Cada dispositivo está conectado al siguiente, formando un bucle cerrado.	- Facilita la organización del flujo de datos. - El rendimiento es uniforme bajo cargas moderadas.	- Si un dispositivo falla, afecta a toda la red. - Añadir o quitar dispositivos interrumpe la red.
Malla	Todos los dispositivos están conectados entre sí directamente.	- Alta redundancia; si un enlace falla, hay otros caminos disponibles.	- Requiere mucho cableado. - Es compleja y costosa de implementar.
Árbol	Combina topologías en estrella, con una jerarquía donde los nodos superiores conectan a subredes.	- Escalable y bien estructurada. - Fácil de expandir.	- Si un nodo superior falla, afecta a todos los nodos dependientes.
Híbrida	Combinación de dos o más topologías (por ejemplo, estrella con bus o anillo).	- Adaptable a diferentes necesidades. - Ofrece flexibilidad.	- Puede ser compleja de diseñar e implementar.
Punto a Punto	Conexión directa entre dos dispositivos.	- Simple y rápido para comunicación entre dos nodos.	- Escalabilidad limitada. - No apta para redes grandes.

UT03 – 3. Tipos de cableado

UT03 - 3.1. Tabla de Tipos de Cableado (sin UTP)

Tipo de Cable	Descripción	Ventajas	Desventajas	Usos Comunes
Fibra Óptica	Transmite datos mediante pulsos de luz a través de filamentos de vidrio o plástico.	- Altas velocidades (hasta Tbps). - Distancias largas sin pérdida de señal.	- Costoso. - Instalación y mantenimiento complejos.	Redes WAN, enlaces troncales y conexión entre edificios.
Coaxial	Tiene un núcleo conductor, una capa aislante y un blindaje metálico.	- Menor pérdida de señal. - Resistente a interferencias.	- Limitado en velocidad. - Rígido y menos flexible.	Televisión por cable y redes antiguas.
Cable HDMI	Diseñado para transmisión de audio y video digital de alta definición.	- Transmisión de video y audio en un solo cable.	- No es apto para redes de datos.	Conexión de monitores, televisores y dispositivos multimedia.
Cable Coaxial RG-6	Variante moderna del coaxial, mejor adaptado para frecuencias altas.	- Resistente y adecuado para señales digitales.	- Similar al coaxial estándar en sus limitaciones de flexibilidad.	Televisión digital, satélites y aplicaciones de banda ancha.
Cable de Consola	Utilizado para configuración de dispositivos como routers y switches.	- Conexión directa a dispositivos de red para administración.	- No es para transmisión continua de datos.	Configuración inicial y administración de equipos de red.
Cable de Fibra Activa	Incluye electrónica integrada para amplificar señales.	- Ideal para distancias extremadamente largas.	- Caro y específico.	Redes de centros de datos y telecomunicaciones internacionales.

UT03 - 3.2. Tabla de Tipos de Cableado UTP

Categoría de Cable	Descripción	Velocidad Máxima	Distancia Máxima	Usos Comunes
Cat5e	Mejorado respecto a Cat5, soporta Gigabit Ethernet con reducción de interferencias.	Hasta 1 Gbps	100 metros	Redes LAN domésticas y empresariales.
Cat6	Diseñado para velocidades más altas y menor interferencia.	Hasta 10 Gbps	55 metros (10 Gbps)	Redes empresariales, especialmente en oficinas modernas.
Cat6a	Versión avanzada de Cat6, mejor blindaje para entornos ruidosos.	Hasta 10 Gbps	100 metros	Redes de centros de datos y aplicaciones de alta velocidad.
Cat7	Ofrece blindaje individual en cada par de cables y es compatible con Cat6.	Hasta 10 Gbps	100 metros	Redes industriales o de alta interferencia.
Cat8	Última generación, soporta conexiones para centros de datos con alta capacidad.	Hasta 40 Gbps	30 metros	Centros de datos y conexiones de servidores.

UT03 – 4. Redes inalámbricas

UT03 - 4.1. Tabla de Tipos de Redes Inalámbricas

Tipo de Red	Descripción	Rango	Velocidad	Usos Comunes
Wi-Fi (IEEE 802.11)	Redes inalámbricas para dispositivos como laptops, smartphones y IoT.	Hasta 100 metros (interior)	Hasta 9.6 Gbps (Wi-Fi 6E)	Redes domésticas y empresariales.

Tipo de Red	Descripción	Rango	Velocidad	Usos Comunes
Bluetooth	Tecnología para conexiones de corto alcance entre dispositivos personales.	Hasta 10 metros (clase 2)	Hasta 2 Mbps (Bluetooth 5)	Auriculares, dispositivos portátiles, IoT.
WiMAX (IEEE 802.16)	Redes inalámbricas de banda ancha para áreas extensas.	Hasta 50 km	Hasta 1 Gbps	Proveedores de servicios de internet en áreas rurales.
ZigBee	Protocolos para dispositivos de baja potencia y redes de malla.	Hasta 100 metros (interior)	Hasta 250 Kbps	Domótica, sensores industriales y aplicaciones IoT.
NFC (Near Field Communication)	Tecnología de corto alcance para transferencia de datos entre dispositivos cercanos.	Hasta 4 cm	Hasta 424 Kbps	Pagos móviles, intercambio de datos entre dispositivos.
Li-Fi (Light Fidelity)	Tecnología basada en luz visible para transmisión de datos.	Hasta 10 metros (iluminación)	Hasta 1 Gbps	Aplicaciones industriales y entornos sensibles a interferencias.

UT03 - 4.2. Tabla de Seguridad en Redes Inalámbricas

Tipo de Seguridad	Descripción	Ventajas	Desventajas	Usos Comunes
WEP (Wired Equivalent Privacy)	Seguridad básica para redes Wi-Fi, basada en cifrado RC4.	Fácil de implementar.	Vulnerable a ataques. Obsoleto.	Redes antiguas o no críticas.
WPA (Wi-Fi Protected Access)	Introduce TKIP para mejorar la seguridad frente a WEP.	Más seguro que WEP.	Menos seguro que WPA2. Vulnerable a ataques avanzados.	Redes Wi-Fi domésticas antiguas.
WPA2 (Wi-Fi Protected Access 2)	Reemplaza TKIP con AES para un cifrado más robusto.	Amplia adopción. Seguridad fuerte frente a ataques estándar.	Vulnerable a ataques de fuerza bruta si se usa una contraseña débil.	Redes Wi-Fi modernas en hogares y empresas.
WPA3	Último estándar con mejoras en cifrado y protección contra ataques de fuerza bruta.	Cifrado avanzado. Protección contra ataques conocidos.	No es compatible con dispositivos antiguos.	Redes empresariales y domésticas avanzadas.
VPN (Virtual Private Network)	Crea un túnel seguro para la transmisión de datos a través de redes públicas.	Protege la privacidad y encripta datos en tránsito.	Dependiente de la configuración y del proveedor del servicio.	Acceso remoto seguro, especialmente en redes públicas.
MAC Filtering	Limita el acceso a la red solo a dispositivos con direcciones MAC específicas.	Control adicional sobre qué dispositivos acceden a la red.	Fácil de eludir con spoofing de MAC.	Redes pequeñas con acceso controlado.
Captive Portal	Sistema de autenticación para redes públicas, que requiere registro en un portal web antes de conectarse.	Fácil de implementar para redes públicas.	No asegura la transmisión de datos después de la autenticación.	Redes en hoteles, aeropuertos y cafeterías.

UT04 - Direccionamiento IP y servicios de red.

UT04 – 1. Tabla Resumen: Dirección IP y Servicios de Red

Tema	Descripción
Definición de Dirección IP	Identificador único que permite la comunicación entre dispositivos en una red. Se divide en: - **Parte de red:** Identifica la red. - **Parte de host:** Identifica el dispositivo en la red.
Unicidad de la IP	No pueden existir dos dispositivos con la misma dirección IP en una red, ya que generaría un conflicto que impediría la comunicación.
Tipos de IP	- **IPv4 (32 bits):** Más común, en formato decimal (ej. 192.168.1.1). - **IPv6 (128 bits):** Formato hexadecimal para mayor capacidad de direccionamiento.
Subnetting (Segmentación)	Proceso para dividir una red en subredes más pequeñas, optimizando el uso de direcciones y mejorando la gestión del tráfico.
Servicios de Red	- **DHCP:** Asigna direcciones IP automáticamente, simplificando la configuración. - **DNS:** Traduce nombres de dominio a direcciones IP. - **FTP:** Transferencia de archivos. - **HTTP/HTTPS:** Protocolo para navegación web.
Acceso Remoto	Herramientas como **VPN** y **RDP** permiten conectar a dispositivos y redes de forma segura desde ubicaciones remotas, facilitando el teletrabajo o la administración de sistemas.

UT04 – 2. Pasos para el cálculo de IP

Paso	Instrucción	Ejemplo	Direcciones no utilizables
1. Identificar la red base y su máscara	Define la dirección IP inicial y la máscara de red.	Dirección: 172.16.0.0/24	Ninguna. Es la base de cálculo.
2. Determinar el número de subredes	Usa la fórmula 2n2^n2n, donde nnn son los bits tomados de la parte de host.	24=162^4 = 1624=16 subredes.	Ninguna, este paso es teórico.
3. Calcular el tamaño de cada subred	Determina cuántos hosts caben en cada subred con 2bits de host−22^{\text{bits de host}} - 22bits de host−2 (se restan red y broadcast).	24−2=142^4 - 2 = 1424−2=14 hosts por subred.	Dirección de red y broadcast no pueden asignarse: Ejemplo: **172.16.0.0** y **172.16.0.15**.
4. Asignar rangos de direcciones	Divide la red base en subredes consecutivas según el incremento calculado.	Subred 1: **172.16.0.0 - 172.16.0.15**	Dirección de red: **172.16.0.0**. Broadcast: **172.16.0.15**.
5. Verificar IPs utilizables	Las direcciones válidas son todas las que no sean red ni broadcast dentro del rango asignado.	Rango válido: **172.16.0.1 - 172.16.0.14**.	Las direcciones de red y broadcast se excluyen, como en el ejemplo anterior.
6. Documentar resultados	Registra la dirección de red, máscara, broadcast y rango de direcciones IP asignables.	**Subred 1:** Red: 172.16.0.0/28 Máscara: 255.255.255.240 Válidas: **172.16.0.1 – 172.16.0.14**.	Ninguna adicional a las señaladas en los pasos anteriores

UT04 – 3. Tabla de Redes Privadas por Rango de IP

Tipo de Red	Rango de IP (Decimal)	Clase	Máscara por Defecto	Usos Comunes
Clase A	1.0.0.0 - 126.255.255.255	Clase A	255.0.0.0	Redes muy grandes como ISP y grandes empresas.
Clase B	128.0.0.0 - 191.255.255.255	Clase B	255.255.0.0	Redes medianas como campus universitarios y corporaciones.

Tipo de Red	Rango de IP (Decimal)	Clase	Máscara por Defecto	Usos Comunes
Clase C	192.0.0.0 - 223.255.255.255	Clase C	255.255.255.0	Redes pequeñas como oficinas y hogares.
Clase D (Multicast)	224.0.0.0 - 239.255.255.255	Clase D	No aplica	Usada para transmisiones de multicast (streaming, conferencias).
Clase E (Experimental)	240.0.0.0 - 255.255.255.255	Clase E	No aplica	Reservada para propósitos experimentales y no usada comercialmente.

UT05 - Instalación y configuración (Windows I)

UT05 – 1. Configurar una Máquina Virtual Windows 10 en VirtualBox

Paso	Instrucción
1. Descargar e instalar VirtualBox	Descarga VirtualBox desde la página oficial junto con el Extension Pack. Instala ambos elementos en tu sistema operativo anfitrión.
2. Crear una nueva máquina virtual	Abre VirtualBox, selecciona "Nueva" o presiona **Ctrl + N**. Asigna un nombre a la máquina y selecciona "Windows 10 (64-bit)" como sistema operativo.
3. Configurar memoria RAM	Asigna al menos 4 GB de RAM (4096 MB) para un rendimiento óptimo.
4. Crear un disco duro virtual	Elige "Crear un disco duro virtual ahora", selecciona el formato VDI y ajusta el tamaño (recomendado: al menos 50 GB).
5. Configurar el almacenamiento ISO	Entra en la configuración de la máquina virtual y adjunta el archivo ISO de Windows 10 en la opción de "Almacenamiento".
6. Ajustar núcleos de CPU	En la sección "Sistema", asigna al menos 2 núcleos de CPU para un mejor rendimiento.
7. Configurar red (opcional)	Inicialmente desactiva el adaptador de red para acelerar la instalación. Posteriormente, habilítalo en modo NAT para acceso a Internet.
8. Guardar y comenzar	Guarda la configuración y haz clic en "Iniciar" para proceder con la instalación del sistema operativo.

UT05 – 2. Instalar Windows 10 en una Máquina Virtual y Añadir Guest Additions

Paso	Instrucción
1. Configurar máquina virtual	Sigue los pasos de la **Tabla 1** para configurar la máquina virtual en VirtualBox con el archivo ISO de Windows 10.
2. Iniciar instalación de Windows	Arranca la máquina virtual con el archivo ISO. Configura idioma, región y distribución del teclado en la pantalla inicial del asistente de instalación.
3. Elegir tipo de instalación	Selecciona la opción "Personalizada" y elige la partición creada en la configuración inicial.
4. Completar instalación	Sigue las instrucciones del asistente hasta que se reinicie el sistema y puedas crear el primer usuario con contraseña.
5. Habilitar red (opcional)	En VirtualBox, habilita el adaptador de red en modo NAT para permitir el acceso a Internet dentro de la máquina virtual.

Paso	Instrucción
6. Instalar Guest Additions	- En VirtualBox, selecciona "Dispositivos" > "Insertar imagen de CD de las Guest Additions". - En Windows, abre el disco virtual y ejecuta VBoxWindowsAdditions.exe.
7. Reiniciar la máquina virtual	Completa la instalación y reinicia la máquina virtual para aplicar las mejoras de las Guest Additions (como integración del ratón y resolución dinámica).

UT05 – 3. Configurar el Gestor de Arranque en Windows 10

Paso	Instrucción
1. Abrir el símbolo del sistema	Abre CMD como administrador desde el menú de inicio (busca "cmd", haz clic derecho y selecciona "Ejecutar como administrador").
2. Listar las opciones de arranque	Ejecuta el comando bcdedit /enum para listar todas las entradas de arranque disponibles.
3. Cambiar el nombre del arranque	Usa el comando bcdedit /set {ID} description "Primera instalación de Windows" reemplazando {ID} por el identificador correspondiente al sistema.
4. Ajustar tiempo de espera	Cambia el tiempo de espera para elegir el sistema operativo con bcdedit /timeout 60 (por ejemplo, para 60 segundos).
5. Establecer un arranque por defecto	Usa el comando bcdedit /default {ID} para establecer como predeterminado uno de los sistemas operativos listados.
6. Verificar cambios	Ejecuta nuevamente bcdedit /enum para confirmar que las modificaciones se aplicaron correctamente.
7. Probar configuración	Reinicia la máquina para comprobar que el nombre modificado y el tiempo de espera aparecen correctamente en el menú de arranque.

UT06 - Administración básica del sistema (Windows II)

UT06 – 1. Crear usuarios en Windows 10

Paso	Instrucción	Notas
1. Abrir Administración de equipos	Haz clic derecho en el botón de inicio de Windows y selecciona **Administración de equipos**.	Requiere permisos de administrador para acceder a esta herramienta.
2. Navegar a usuarios y grupos	En la ventana que se abre, ve a **Herramientas del sistema > Usuarios y grupos locales > Usuarios**.	Asegúrate de estar en la carpeta correcta antes de crear un usuario.
3. Crear un nuevo usuario	Haz clic derecho en el panel central y selecciona **Usuario nuevo**.	También puedes usar el menú superior para seleccionar "Acción > Usuario nuevo".
4. Completar el formulario	Rellena los campos: - **Nombre de usuario** (ej. jperez). - **Nombre completo** (ej. Juan Pérez). - **Descripción** (Departamento, cargo, etc.).	El nombre de usuario debe ser único en el sistema.

Paso	Instrucción	Notas
5. Asignar contraseña	Introduce una contraseña segura y desmarca la casilla **El usuario debe cambiar la contraseña en el próximo inicio de sesión** si no deseas esta opción.	Activa "La contraseña nunca caduca" si es una cuenta especial, como un servicio.
6. Guardar el usuario	Haz clic en **Crear** y luego en **Cerrar** para finalizar.	El usuario estará ahora en la lista de cuentas disponibles del sistema.
7. Asignar al usuario a un grupo	Haz clic derecho sobre el usuario recién creado, selecciona **Propiedades** y ve a la pestaña **Miembro de**.	Permite añadir el usuario a grupos específicos según su función (ej. Administradores, Usuarios).
8. Comprobar configuración	Asegúrate de que el usuario pueda iniciar sesión y tenga los permisos adecuados.	Usa el comando net user [nombre de usuario] en CMD para verificar la información del usuario.

UT06 – 2. Configurar Permisos en Carpetas en Windows 10

Paso	Instrucción	Notas
1. Seleccionar la carpeta	Haz clic derecho sobre la carpeta a la que deseas configurar permisos y selecciona **Propiedades**.	Asegúrate de tener permisos de administrador para realizar esta acción si es necesario.
2. Acceder a la pestaña de seguridad	En la ventana de Propiedades, selecciona la pestaña **Seguridad**.	Esta pestaña muestra los permisos actuales asignados a la carpeta.
3. Editar los permisos	Haz clic en el botón **Editar** para abrir la ventana de permisos.	Aquí puedes agregar o modificar permisos para usuarios y grupos.
4. Agregar un nuevo usuario o grupo	En la ventana de permisos, haz clic en **Agregar**.	Se abrirá una nueva ventana para seleccionar usuarios o grupos.
5. Buscar usuarios o grupos	En la ventana que aparece: - Introduce el nombre del usuario o grupo. - Haz clic en **Comprobar nombres** para validar la entrada.	Si el nombre es correcto, aparecerá subrayado; de lo contrario, verifica que esté escrito correctamente.
6. Asignar permisos específicos	Una vez agregado el usuario o grupo, selecciona los permisos que deseas asignar (lectura, escritura, control total, etc.).	Usa "Control total" solo si el usuario necesita acceso completo; evita esto para usuarios estándar.
7. Quitar permisos existentes (opcional)	Selecciona un usuario o grupo en la lista y haz clic en **Quitar** si deseas eliminar sus permisos sobre la carpeta.	Esto es útil para restringir el acceso de usuarios o grupos no autorizados.
8. Configurar opciones avanzadas	Haz clic en el botón **Opciones avanzadas** para acceder a configuraciones adicionales, como herencia de permisos.	Puedes desactivar la herencia si no deseas que los permisos de la carpeta padre se apliquen.
9. Aplicar y guardar cambios	Haz clic en **Aceptar** en todas las ventanas abiertas para aplicar los cambios realizados.	Los permisos se aplican inmediatamente, y los usuarios afectados verán los cambios en su acceso.
10. Validar configuración	Prueba acceder a la carpeta con una cuenta de usuario con los permisos configurados.	Asegúrate de que los permisos funcionen como esperas (acceso permitido o denegado).

UT06 – 3. Cifrar Archivos en Windows 10

Paso	Instrucción	Notas
1. Seleccionar el archivo	Haz clic derecho sobre el archivo que deseas cifrar y selecciona **Propiedades**.	Asegúrate de tener permisos para modificar el archivo.
2. Acceder a Opciones Avanzadas	En la ventana de Propiedades, ve a la pestaña **General** y haz clic en **Opciones avanzadas**.	Aquí se encuentran las configuraciones adicionales del archivo.
3. Activar el cifrado	En la ventana de **Atributos avanzados**, marca la casilla **Cifrar contenido para proteger datos** y haz clic en **Aceptar**.	El cifrado está basado en el usuario, solo accesible por el creador.
4. Aplicar el cifrado	Haz clic en **Aceptar** en la ventana de Propiedades y confirma si deseas aplicar el cifrado solo al archivo o también a la carpeta contenedora.	El sistema aplicará el cifrado automáticamente.
5. Exportar el certificado (opcional)	Si necesitas compartir el archivo, haz clic en la notificación emergente para exportar el certificado de cifrado.	Guarda el archivo en un lugar seguro y protégelo con una contraseña.
6. Verificar acceso	Intenta abrir el archivo cifrado con otro usuario para confirmar que solo es accesible para el usuario que lo cifró.	Importa el certificado en otros usuarios si deseas compartir acceso al archivo cifrado.

UT06 – 4. Configurar Directivas de Contraseña en Windows 10

Paso	Instrucción	Notas
1. Abrir el Editor de Directivas de Seguridad Local	Escribe secpol.msc en el cuadro de búsqueda de Inicio y presiona Enter.	Esta herramienta requiere permisos de administrador.
2. Navegar a Directiva de contraseñas	Ve a **Directivas de cuenta > Directiva de contraseñas**.	Aquí puedes configurar todas las políticas relacionadas con contraseñas.
3. Configurar el historial de contraseñas	Haz doble clic en **Exigir el historial de contraseñas**, introduce el valor (ej. 4) y haz clic en **Aceptar**.	Esto evita que el usuario reutilice las últimas contraseñas.
4. Habilitar contraseñas complejas	Haz doble clic en **Las contraseñas deben cumplir con los requisitos de complejidad** y selecciona **Habilitar**.	Requiere letras mayúsculas, minúsculas, números y caracteres especiales.
5. Establecer la vigencia máxima de la contraseña	Haz doble clic en **Duración máxima de la contraseña**, introduce el valor (ej. 30 días) y haz clic en **Aceptar**.	Define el tiempo máximo antes de que la contraseña deba cambiarse.
6. Configurar la longitud mínima	Haz doble clic en **Longitud mínima de la contraseña**, introduce el valor (ej. 10 caracteres) y haz clic en **Aceptar**.	Establece el número mínimo de caracteres requeridos.
7. Configurar el umbral de bloqueo	Haz doble clic en **Umbral de bloqueo de cuenta**, introduce el valor (ej. 3 intentos) y haz clic en **Aceptar**.	Especifica el número de intentos fallidos antes de que la cuenta sea bloqueada.

UT06 – 5. Configurar un Análisis Diario en Windows 10

Paso	Instrucción	Notas
1. Abrir el Programador de Tareas	Escribe "Programador de Tareas" en la barra de búsqueda de Inicio y selecciona la herramienta.	Requiere permisos de administrador.
2. Crear una nueva tarea	En el panel derecho, haz clic en **Crear tarea**.	Asigna un nombre descriptivo, como "Análisis rápido diario".
3. Configurar disparadores	Ve a la pestaña **Desencadenadores**, haz clic en **Nuevo** y selecciona la opción **Diariamente**.	Establece la hora deseada (ej. 00:00:00 para medianoche).

Paso	Instrucción	Notas
4. Configurar acciones	Ve a la pestaña **Acciones**, haz clic en **Nueva** y selecciona **Iniciar un programa**.	En el campo Programa, introduce la ruta de **MpCmdRun.exe** y el argumento -Scan -ScanType 1.
5. Guardar y verificar	Haz clic en **Aceptar** y valida la tarea con credenciales de administrador.	Comprueba que la tarea aparece en la Biblioteca del Programador de Tareas.

UT06 – 6. Optimizar y Desfragmentar el Disco en Windows 10

Paso	Instrucción	Notas
1. Abrir la herramienta de desfragmentación	Haz clic en **Inicio**, escribe "Optimizar unidades" y selecciona la herramienta.	No requiere permisos especiales para su uso.
2. Seleccionar la unidad	En la ventana que aparece, selecciona el disco que deseas desfragmentar o analizar.	Se recomienda optimizar discos HDD; no es necesario para SSD modernos.
3. Analizar el disco	Haz clic en **Analizar** para verificar si la unidad necesita ser desfragmentada.	El sistema mostrará un porcentaje de fragmentación.
4. Optimizar el disco	Haz clic en **Optimizar** para iniciar el proceso de desfragmentación.	El tiempo necesario depende del tamaño y estado del disco.
5. Configurar optimización programada	Haz clic en **Cambiar configuración** y establece un horario regular para optimizar las unidades automáticamente.	Esto garantiza un mantenimiento constante sin intervención manual.

UT07 - Administración de redes. (Windows III)

UT07 – 1. Configuración de Parámetros de Red

Paso	Instrucción	Notas
1. Abrir configuración de red	Ve a **Configuración** > **Red e Internet** > **Estado** y selecciona **Cambiar opciones de adaptador**.	Aquí puedes ver todos los adaptadores de red disponibles.
2. Configurar la IP fija	Haz clic derecho sobre el adaptador puente y selecciona **Propiedades**. Doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)**.	Ingresa la IP, máscara de subred (ej. 255.255.255.0), puerta de enlace y DNS (ej. 8.8.8.8).
3. Probar conectividad interna	Abre CMD y ejecuta ping 127.0.0.1 para verificar la funcionalidad del adaptador interno.	Si no responde, revisa la configuración del adaptador.
4. Probar conectividad externa	Ejecuta ping 8.8.8.8 para confirmar acceso a internet.	Asegúrate de que el adaptador NAT esté habilitado para acceso externo.
5. Verificar comunicación entre máquinas	En una máquina, ejecuta ping [IP de la otra máquina] para validar la conectividad entre ambas.	Ambas máquinas deben responder sin pérdida de paquetes.

UT07 – 2. Configuración de un Grupo de Trabajo

Paso	Instrucción	Notas
1. Abrir configuración de red	Ve a **Configuración** > **Red e Internet** > **Estado** y selecciona **Cambiar opciones de adaptador**.	Aquí puedes ver todos los adaptadores de red disponibles.
2. Configurar la IP fija	Haz clic derecho sobre el adaptador puente y selecciona **Propiedades**. Doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)**.	Ingresa la IP, máscara de subred (ej. 255.255.255.0), puerta de enlace y DNS (ej. 8.8.8.8).

Paso	Instrucción	Notas
3. Probar conectividad interna	Abre CMD y ejecuta ping 127.0.0.1 para verificar la funcionalidad del adaptador interno.	Si no responde, revisa la configuración del adaptador.
4. Probar conectividad externa	Ejecuta ping 8.8.8.8 para confirmar acceso a internet.	Asegúrate de que el adaptador NAT esté habilitado para acceso externo.
5. Verificar comunicación entre máquinas	En una máquina, ejecuta ping [IP de la otra máquina] para validar la conectividad entre ambas.	Ambas máquinas deben responder sin pérdida de paquetes.

UT07 – 3. Configuración de un Servidor FTP

Paso	Instrucción	Notas
1. Activar IIS	Ve a **Panel de Control** > **Programas y características** > **Activar o desactivar características de Windows**. Activa **IIS** y su componente FTP.	Esta función es necesaria para configurar el servidor FTP.
2. Crear un directorio FTP	Crea una carpeta llamada **FTP-Compartido** en C: o D:.	Asigna permisos adecuados para usuarios autorizados (lectura/escritura).
3. Configurar un nuevo sitio FTP	Abre el Administrador de IIS, haz clic en **Sitios** y selecciona **Agregar sitio FTP**.	Define el nombre del sitio, selecciona la carpeta creada y asigna IP y puerto (ej. 21).
4. Configurar autenticación	Habilita la **Autenticación básica** y asigna permisos específicos a usuarios o grupos.	Puedes usar usuarios locales creados en el sistema para autenticación.
5. Verificar acceso desde cliente	Usa un cliente FTP como FileZilla en otra máquina (W2) para conectarte al servidor FTP configurado en W1.	Proporciona la IP del servidor, el puerto 21, y las credenciales del usuario autorizado.

UT07 – 4. Bloquear Chrome con el Firewall

Paso	Instrucción	Notas
1. Abrir el Firewall de Windows	Escribe "Firewall de Windows con seguridad avanzada" en la barra de búsqueda de Inicio y ábrelo.	Necesitas permisos de administrador para crear nuevas reglas.
2. Crear una nueva regla de salida	En el panel izquierdo, selecciona **Reglas de salida** y haz clic en **Nueva regla** en el panel derecho.	Las reglas de salida controlan las aplicaciones que pueden acceder a internet.
3. Seleccionar programa	Selecciona la opción **Programa** y especifica la ruta del ejecutable de Chrome (ej. C:\Program Files\Google\Chrome\Application\chrome.exe).	Esto asegura que la regla afecte solo a Chrome.
4. Bloquear conexión	Selecciona **Bloquear la conexión** cuando la aplicación intente acceder a internet.	Aplica esta regla para los perfiles de dominio, privado y público.
5. Verificar funcionamiento	Intenta abrir Chrome y accede a una página web. Deberías recibir un error de conexión.	Otros navegadores como Edge o Firefox deben seguir funcionando correctamente.

UT07 – 5. Configurar Análisis Programado en Windows Defender

Paso	Instrucción	Notas
1. Abrir el Programador de Tareas	Escribe "Programador de Tareas" en el cuadro de búsqueda de Inicio y selecciona la herramienta.	Necesitas permisos de administrador para crear tareas.
2. Crear una nueva tarea	Haz clic en **Crear tarea básica** y asigna un nombre como "Análisis Semanal Windows Defender".	Usa un nombre descriptivo para identificar fácilmente la tarea.
3. Configurar desencadenador	Selecciona un **desencadenador diario o semanal** y establece la hora deseada para ejecutar el análisis.	Configura el horario en un momento de baja actividad del sistema.

Paso	Instrucción	Notas
4. Configurar la acción	Selecciona **Iniciar un programa** y escribe el comando: MpCmdRun.exe con argumentos -Scan -ScanType 2.	Esto realiza un análisis completo del sistema.
5. Guardar y verificar	Haz clic en **Finalizar** y revisa que la tarea aparece en la Biblioteca del Programador de Tareas.	Puedes forzar la ejecución para comprobar que funciona correctamente.

UT08 - Instalación y configuración (Linux I)

UT08 – 1. Instalación de Ubuntu

Paso	Instrucción	Notas
1. Descargar Ubuntu ISO	Descarga la imagen ISO desde la página oficial de Ubuntu.	Asegúrate de elegir la versión 24.04 LTS.
2. Crear máquina virtual	Configura una máquina virtual en VirtualBox con 4 GB de RAM, 2 núcleos, disco de 40 GB y red NAT.	Selecciona "Ubuntu (64-bit)" como sistema operativo.
3. Iniciar desde el GRUB	Arranca la máquina virtual y selecciona la opción **Try or Install Ubuntu** en el menú GRUB.	Asegúrate de que el archivo ISO esté montado en el almacenamiento de la máquina virtual.
4. Configurar idioma y teclado	Selecciona idioma, distribución del teclado y conexión de red en el asistente de instalación.	Estas configuraciones pueden ajustarse más tarde desde el sistema operativo.
5. Configurar particiones	Selecciona instalación manual y crea las siguientes particiones: - **/boot:** 500 MB. - **/swap:** 8 GB. - **/**: 15 GB. - **/var:** 5 GB. - **/home:** 14 GB.	Asegúrate de asignar los tamaños y puntos de montaje adecuados según las necesidades del sistema.
6. Completar instalación	Define el nombre de usuario, contraseña y zona horaria.	La contraseña debe ser compleja para mayor seguridad.
7. Instalar Guest Additions	Inserta la imagen de las Guest Additions desde **Dispositivos** en VirtualBox, monta el disco y ejecuta VBoxLinuxAdditions.run.	Esto habilita la resolución dinámica y mejor integración con el h

UT08 – 2. Creación de Usuarios

Paso	Instrucción	Notas
1. Abrir terminal	Abre una terminal con privilegios de administrador.	Puedes usar Ctrl + Alt + T para abrir rápidamente una terminal.
2. Crear un nuevo usuario	Ejecuta el comando: sudo adduser [nombre_usuario].	Sigue las instrucciones para establecer contraseña y datos adicionales.
3. Cambiar al nuevo usuario	Usa el comando su - [nombre_usuario] para iniciar sesión como el nuevo usuario.	Verifica que el entorno del usuario esté configurado correctamente.
4. Salir del usuario	Usa el comando exit para volver al usuario administrador.	Esto te permite regresar al entorno inicial.

UT08 – 3. Actualización del Sistema

Paso	Instrucción	Notas
1. Abrir terminal	Inicia una terminal con privilegios de administrador.	Puedes usar Ctrl + Alt + T.

Paso	Instrucción	Notas
2. Actualizar repositorios	Ejecuta el comando: sudo apt update.	Esto sincroniza los repositorios de software disponibles.
3. Instalar actualizaciones	Usa el comando: sudo apt upgrade -y.	Este paso actualiza los paquetes instalados.
4. Actualización completa	Ejecuta: sudo apt full-upgrade -y.	Realiza una actualización completa del sistema operativo.
5. Limpiar el sistema	Usa: sudo apt autoremove -y && sudo apt clean.	Esto elimina paquetes obsoletos y libera espacio en disco.

UT08 – 4. Instalación y Uso de Webmin

Paso	Instrucción	Notas
1. Actualizar dependencias	Ejecuta: sudo apt update && sudo apt install software-properties-common apt-transport-https curl.	Asegúrate de tener permisos de administrador.
2. Agregar repositorio	Agrega la clave GPG con: `curl -fsSL https://download.webmin.com/developers-key.asc	sudo gpg --dearmor -o /usr/share/keyrings/webmin.gpg. Añade el repositorio: echo "deb [signed-by=/usr/share/keyrings/webmin.gpg] https://download.webmin.com/download/newkey/repository stable contrib"
3. Instalar Webmin	Ejecuta: sudo apt update && sudo apt install webmin.	Esto instala Webmin y habilita su servicio automáticamente.
4. Acceder a Webmin	Abre un navegador y ve a https://[IP]:10000.	Usa un usuario con permisos de sudo para iniciar sesión.

UT10 - Administración de la red (Linux III)

UT10 – 1. Configurar un Equipo con Netplan para Dos Tarjetas de Red

Paso	Instrucción	Notas
1. Verificar las interfaces de red	Usa el comando ip addr show para listar las interfaces de red disponibles. Identifica las tarjetas NAT (por DHCP) y Adaptador Puente (por IP estática).	Por ejemplo: **enp0s3** (NAT) y **enp0s8** (estática).
2. Crear una copia de seguridad	Antes de modificar, crea una copia del archivo con: sudo cp /etc/netplan/50-cloud-init.yaml /etc/netplan/50-cloud-init.backup.	Esto asegura que puedes revertir cambios en caso de errores.
3. Editar el archivo de Netplan	Abre el archivo de configuración con sudo nano /etc/netplan/50-cloud-init.yaml.	Utiliza un editor que soporte YAML para evitar problemas con la sintaxis.
4. Configurar DHCP en la tarjeta NAT	Configura la tarjeta **enp0s3** para recibir la IP por DHCP:	YAML es sensible a los espacios, asegúrate de seguir correctamente la tabulación y la estructura:
	network:	La clave **network** está completamente alineada a la izquierda.
	version: 2	**version** tiene dos espacios de tabulación respecto a **network**.
	ethernets:	**ethernets** también está alineada con dos espacios respecto a **network**.
	enp0s3:	**enp0s3** tiene dos espacios más respecto a **ethernets**.
	dhcp4: true	Habilita DHCP para esta interfaz.
5. Configurar IP estática en	Añade la configuración para **enp0s8** en el mismo archivo:	El ejemplo asigna una IP estática al adaptador puente.
	enp0s8:	Define la segunda tarjeta de red.

Paso	Instrucción	Notas
la segunda tarjeta	dhcp4: false	Desactiva DHCP.
	addresses: [192.168.1.100/24]	Asigna una IP estática con su máscara de red.
	gateway4: 192.168.1.1	Especifica la puerta de enlace para el acceso a internet.
	nameservers:	Configura los servidores DNS.
	addresses: [8.8.8.8, 8.8.4.4]	Usa servidores DNS públicos, como los de Google.
6. Aplicar los cambios	Guarda el archivo con **Ctrl+O** y cierra con **Ctrl+X**. Aplica los cambios ejecutando sudo netplan apply.	Si hay un error de sintaxis, revisa el archivo con sudo netplan try antes de aplicar los cambios.
7. Verificar conectividad	- Verifica la IP dinámica de **enp0s3** con ip addr show enp0s3. - Prueba la IP estática de **enp0s8** con ping 192.168.1.1.	Si las tarjetas no responden, revisa la configuración del archivo YAML y asegúrate de que el formato sea correcto.

UT10 - 1.1. Ejemplo de configuración de archivo de netplan

```
network:                    # Nivel 0, sin espacios (alineado a la izquierda)
  version: 2                # Nivel 1, 2 espacios
  ethernets:                # Nivel 1, 2 espacios
    enp0s3:                 # Nivel 2, 4 espacios
      dhcp4: true           # Nivel 3, 6 espacios
    enp0s8:                 # Nivel 2, 4 espacios
      dhcp4: false          # Nivel 3, 6 espacios
      addresses:            # Nivel 3, 6 espacios
        - 192.168.1.100/24  # Nivel 4, 8 espacios
      gateway4: 192.168.1.1 # Nivel 3, 6 espacios
      nameservers:          # Nivel 3, 6 espacios
        addresses:          # Nivel 4, 8 espacios
          - 8.8.8.8         # Nivel 5, 10 espacios
          - 8.8.4.4         # Nivel 5, 10 espacios
```

UT10 - 1.2. Ejemplo de configuración de archivo de netplan

Nivel	Indentación (Espacios)	Clave o Elemento	Funcionalidad	Ejemplo
Nivel 0	0 espacios	network:	Define el inicio de la configuración de red. Es la clave raíz del archivo YAML en Netplan.	network:
Nivel 1	2 espacios	version:	Define la versión de Netplan (normalmente 2) y las interfaces de red a configurar (ethernets).	version: 2
		ethernets:		ethernets:
Nivel 2	4 espacios	Nombre de la interfaz	Especifica cada interfaz de red, como enp0s3 (NAT) o enp0s8 (estática). Cada interfaz debe ser única.	enp0s3:
Nivel 3	6 espacios	Configuraciones de interfaz	Define parámetros dentro de cada interfaz, como DHCP, direcciones IP estáticas, puerta de enlace y DNS.	dhcp4: true
Nivel 4	8 espacios	Subparámetros	Detalla valores específicos de configuraciones, como direcciones IP o nombres de servidores.	addresses:
Nivel 5	10 espacios	Listas de valores	Proporciona valores múltiples para configuraciones como direcciones IP o DNS en formato de lista.	192.168.1.100/24

Consistencia en espacios: Cada nivel debe usar exactamente 2 espacios. Tabuladores o espacios inconsistentes provocan errores de sintaxis.
Validación del archivo: Usa sudo netplan try para validar los cambios antes de aplicarlos. Los errores suelen indicar líneas problemáticas con mensajes como: YAMLException: bad indentation.

UT10 – 3. Instalación y Configuración de Samba

Paso	Instrucción	Notas
1. Instalar Samba	Ejecuta sudo apt update && sudo apt install samba samba-common-bin -y.	Esto instala los paquetes necesarios para el servicio Samba.
2. Crear el directorio compartido	Usa sudo mkdir -p /srv/samba/public para crear la carpeta compartida.	Asigna permisos con sudo chmod -R 0777 /srv/samba/public.
3. Configurar el archivo smb.conf	Edita el archivo con sudo nano /etc/samba/smb.conf y agrega:	Asegúrate de hacer una copia de seguridad antes de modificar este archivo.
	[public]	Nombre del recurso compartido.
	Path = /srv/samba/public	Ruta del directorio compartido.
	Browseable = yes	Permite que otros usuarios vean la carpeta.
	Writable = yes	Permite que los usuarios escriban en el directorio.
	Guest ok = yes	Permite acceso sin autenticación.
4. Reiniciar el servicio Samba	Ejecuta sudo systemctl restart smbd.	Verifica que el servicio esté activo con sudo systemctl status smbd.

UT10 - 3.1. Creación de Usuarios en Samba

Paso	Instrucción	Notas
1. Crear un usuario en el sistema	Usa el comando sudo adduser [nombre_usuario] para crear un usuario en el sistema operativo.	Completa el proceso de configuración asignando una contraseña. Este usuario será base para Samba.
2. Configurar contraseña de Samba	Usa el comando sudo smbpasswd -a [nombre_usuario] para asignar una contraseña de Samba al usuario.	La contraseña de Samba es independiente de la contraseña del sistema.
3. Habilitar el usuario en Samba	Ejecuta el comando sudo smbpasswd -e [nombre_usuario] para habilitar al usuario en Samba.	Esto asegura que el usuario pueda autenticarse en los recursos compartidos.
4. Crear un directorio personal	Usa sudo mkdir -p /srv/samba/[nombre_usuario] para crear un directorio de uso exclusivo del usuario.	El directorio puede personalizarse según los permisos que desees otorgar.
5. Asignar permisos al directorio	Cambia la propiedad del directorio con sudo chown [nombre_usuario]:[nombre_usuario] /srv/samba/[nombre_usuario].	Asegúrate de que el usuario tenga control total de su carpeta.
6. Configurar el recurso compartido en Samba	Edita el archivo de configuración de Samba: sudo nano /etc/samba/smb.conf. Agrega la siguiente sección:	Este archivo define cómo y dónde estarán los recursos compartidos.
	[nombre_usuario]	Nombre del recurso compartido.
	path = /srv/samba/[nombre_usuario]	Ruta al directorio asignado al usuario.
	valid users = [nombre_usuario]	Define quién puede acceder al recurso.
	read only = no	Permite que el usuario tenga acceso de lectura y escritura.
	browseable = yes	Hace visible el recurso en la red.

Paso	Instrucción	Notas
7. Reiniciar el servicio Samba	Usa el comando sudo systemctl restart smbd para aplicar los cambios.	Asegúrate de que no haya errores en el archivo /etc/samba/smb.conf.
8. Probar el acceso al recurso	Desde un cliente Samba (Linux o Windows), intenta acceder al recurso compartido:	En Linux: smb://[IP_del_servidor]/[nombre_usuario]. En Windows: \\[IP_del_servidor]\[nombre_usuario].

UT10 – 4. Configuración del Servicio SSH

Paso	Instrucción	Notas
1. Instalar SSH	Ejecuta sudo apt install openssh-server -y.	Esto habilita el servicio SSH en el sistema.
2. Activar y verificar SSH	Usa los comandos: - sudo systemctl enable ssh - sudo systemctl start ssh - sudo systemctl status ssh.	Verifica que el servicio esté activo y habilitado para reinicios automáticos.
3. Habilitar SSH en el firewall	Ejecuta sudo ufw allow ssh para permitir conexiones SSH.	Esto asegura que las conexiones no sean bloqueadas.
4. Probar conexión SSH	Desde otro sistema, usa: ssh usuario@IP_servidor.	Reemplaza **usuario** e **IP_servidor** por los valores correspondientes.

UT10 - 4.1. Creación de Usuarios en Samba

Paso	Instrucción	Notas
1. Crear un usuario en el sistema	Usa el comando sudo adduser [nombre_usuario] para crear un usuario en el sistema.	Completa la configuración proporcionando una contraseña. Este usuario será utilizado para SSH.
2. Probar la cuenta localmente	Cambia al nuevo usuario con su - [nombre_usuario] para confirmar que su entorno está configurado correctamente.	Usa exit para regresar al usuario original tras la verificación.
3. Habilitar acceso SSH	Asegúrate de que el servicio SSH está activo. Usa los comandos:	Si el servicio no está instalado, ejecuta sudo apt install openssh-server -y.
	- sudo systemctl enable ssh	
	- sudo systemctl start ssh	
	- sudo systemctl status ssh	
4. Configurar directorios SSH del usuario	Cambia al usuario creado con su - [nombre_usuario] y crea la carpeta .ssh en su directorio personal:	La carpeta .ssh almacena claves y configuraciones relacionadas con SSH. Asegúrate de que solo el usuario tiene acceso a esta carpeta.
	``bash	
	mkdir -p ~/.ssh	
	chmod 700 ~/.ssh	
5. Configurar acceso con clave pública (opcional)	Si deseas usar claves públicas en lugar de contraseñas:	Esto mejora la seguridad y elimina la necesidad de contraseñas al conectarse. Usa ssh-copy-id usuario@IP_servidor desde el cliente para transferir la clave pública. Agrega la clave pública generada previamente al archivo y asigna permisos correctos.
	- Copia la clave pública al usuario:	
	- O, manualmente, edita el archivo ~/.ssh/authorized_keys:	

Paso	Instrucción	Notas
	``bash echo "clave_publica" >> ~/.ssh/authorized_keys chmod 600 ~/.ssh/authorized_keys ```	
6. Verificar configuración SSH	Desde otro cliente SSH, prueba conectarte usando el comando: ssh [nombre_usuario]@[IP_servidor].	Si todo está configurado correctamente, el cliente podrá iniciar sesión.
7. Opcional: Configurar restricciones de usuario	Para restringir accesos o limitar comandos, edita el archivo /etc/ssh/sshd_config.	Por ejemplo, puedes definir el acceso por grupos o deshabilitar el acceso por contraseña.
	- Para permitir solo usuarios específicos: ```bash AllowUsers [nombre_usuario] ``` - Reinicia el servicio SSH: sudo systemctl restart ssh.	Agrega esta línea al final del archivo.

UT10 – 5. Modificar, Habilitar y Deshabilitar el Firewall en Ubuntu

Paso	Instrucción	Notas
1. Verificar el estado del firewall	Usa el comando sudo ufw status para verificar si el firewall está habilitado o deshabilitado.	Si el estado es **inactive**, significa que el firewall está deshabilitado.
2. Habilitar el firewall	Ejecuta el comando sudo ufw enable para activar el firewall.	Este comando bloqueará todo el tráfico entrante excepto las reglas explícitamente permitidas.
3. Deshabilitar el firewall	Usa el comando sudo ufw disable para desactivar el firewall.	Esto elimina todas las restricciones de tráfico configuradas por UFW.
4. Permitir un puerto específico	Para habilitar el tráfico en un puerto, ejecuta: sudo ufw allow [puerto].	Ejemplo: sudo ufw allow 22 habilita conexiones SSH.
5. Bloquear un puerto específico	Usa sudo ufw deny [puerto] para denegar tráfico en un puerto.	Ejemplo: sudo ufw deny 80 bloquea conexiones HTTP.
6. Permitir tráfico desde una IP específica	Ejecuta sudo ufw allow from [IP] para permitir tráfico de una dirección IP específica.	Ejemplo: sudo ufw allow from 192.168.1.100 permite tráfico desde esta IP a todos los puertos.
7. Permitir tráfico a un puerto desde una IP específica	Usa sudo ufw allow from [IP] to any port [puerto].	Ejemplo: sudo ufw allow from 192.168.1.100 to any port 22 permite conexiones SSH solo desde esa IP.
8. Eliminar una regla específica	Usa el comando sudo ufw delete [número_regla] o sudo ufw delete allow/deny [puerto].	Verifica el número de la regla actual con sudo ufw status numbered.
9. Resetear el firewall	Para borrar todas las reglas y reiniciar la configuración predeterminada, usa: sudo ufw reset.	Útil si deseas empezar desde cero.
10. Activar el registro del firewall	Usa sudo ufw logging on para habilitar los logs del firewall.	Los logs se guardan en /var/log/ufw.log.
11. Configurar un rango de puertos	Usa sudo ufw allow [puerto_inicio]:[puerto_fin]/[protocolo] para abrir un rango de puertos.	Ejemplo: sudo ufw allow 1000:2000/tcp abre el rango de puertos entre 1000 y 2000 para TCP.
12. Verificar reglas activas	Ejecuta sudo ufw status para listar las reglas activas.	Si usas sudo ufw status verbose, obtendrás información adicional como el nivel de registro.