Tema 5 – Sistemas informáticos en red

Modelo OSI

Determina las funciones de comunicación.

Cada nivel se corresponde con una capa que se comunica con su capa superior e inferior.

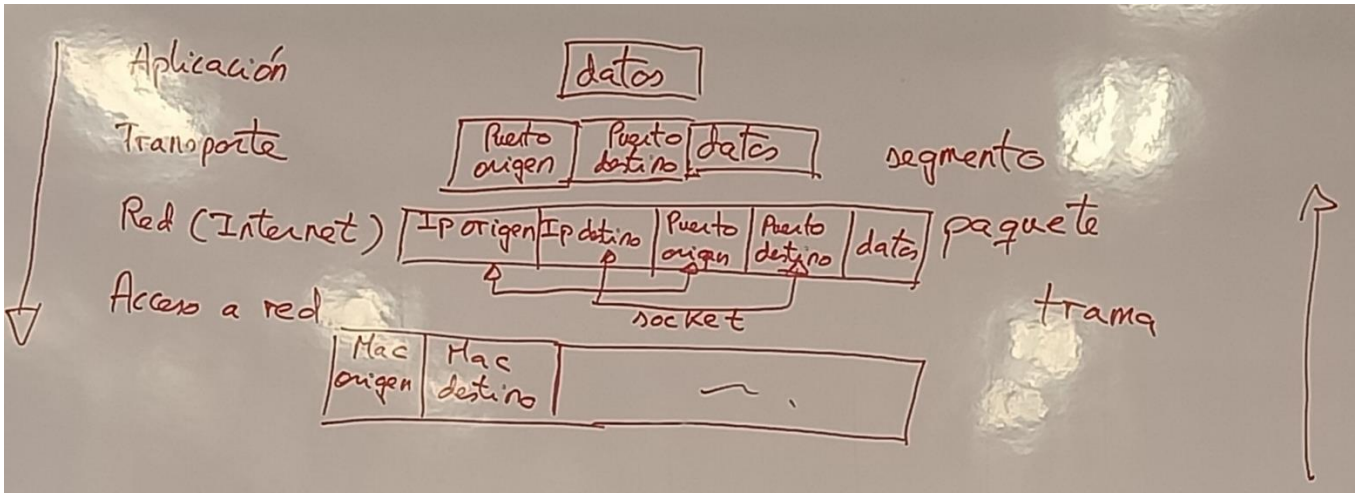
Encapsulamiento → Cada capa añade una traza con metainformación para que se interprete en el receptor, añade a los datos de la capa superior información asociada al protocolo que representa formado los PDU (paquete de datos).

7 capas :

- Aplicación: interfaz entre usuario y aplicaciones.
- Presentación: determina el formato de la información para transferir. Codifica los datos pudiendo comprimirlos o cifrarlos.
- Sesión: define los mecanismos para establecer, mantener y controlar el dialogo entre las aplicaciones emisora y receptora.
- Transporte: prepara y controla el flujo de datos. Encapsula en segmentos los datos de la capa de sesión.
- Red: selecciona la ruta entre el emisor y el receptor. Encapsula los segmentos de datos en paquetes.
- Enlace de datos: Establece mecanismos de detección y corrección de errores en la transmisión de datos. Encapsula los paquetes en tramas.
- Física: determina las especificaciones mecánicas, eléctricas y funcionales. La trama constituida por bits se traduce en señales eléctricas, electromagnéticas o pulsos de luz, hasta llegar al receptor donde son reconvertidas a binario para su interpretación.

Relacionadas con las aplicaciones del host

Transporte y control del flujo de datos



Correspondencia entre el modelo OSI y el modelo TCP/IP

Modelo OSI	Modelo TCP/IP
7. Aplicación	a) Aplicación
6. Presentación	
5. Sesión	
4. Transporte	b) Transporte
3. Red	c) Internet
2. Enlace de datos	d) Acceso a red
1. Física	

Protocolo Ethernet

Transmisión de datos por cable especificando las características del cableado, su señalización y el formato de las tramas de datos. Esta asociado a la capa física del modelo OSI.

Emplea un mecanismo CSMA/CD (acceso múltiple por detección de portadora y detección de colisiones). El host debe escuchar el medio antes de transmitir.

Bajo coste, flexibilidad, fácil de implementar y seguro ante accesos no permitidos.

Muy empleada en redes de área local LAN.

Protocolo WI-FI

Conjunto de especificaciones para redes de área local inalámbricas asociándose a la capa física del modelo OSI.

Emplean el mecanismo CSMA/CA (acceso múltiple por detección de portadora y prevención de colisiones) que antes de transmitir envía una notificación y si recibe autorización lo hace.

Fácil de instalar y móvil. Inseguro al ser un medio de transmisión abierto y se pueden saturar los canales.

Protocolo IPv4

Protocolo para la transferencia de datos entre las distintas redes en internet:

- Transmite datos a nivel de red.
- Transmitir el formato de la información de control asociada a dicho nivel.

Cada nivel de la pila de protocolos recibe los datos del nivel superior que, junto a la información de control (cabecera) del nivel correspondiente, forman la unidad de datos.

La unidad de datos del nivel de red IP se llama paquete o paquete IP. está formado por los datos del nivel de transporte, más la información de control (cabecera) del propio nivel de red.

- No garantiza que los paquetes lleguen a su destino en el mismo orden en el que son enviados. En IP cada paquete es enrutado o encaminado de manera independiente; por esta razón, cada paquete tiene que contener la dirección IP del destinatario.
- No se garantiza que los paquetes lleguen a su destino sin errores en los datos. detectar los errores que se producen en los propios datos de control del nivel de red, pero no puede detectar los errores que se producen en los datos de nivel superior.
- Ni siquiera se garantiza la entrega de los paquetes que se envían. Cuando hay mucho tráfico de paquetes, los routers pueden verse desbordados, eliminando los paquetes que ya no pueden almacenar.

Tiene que ser la capa de nivel superior, la capa de transporte, la que trate toda esta problemática si se quiere ofrecer a las aplicaciones un servicio más fiable.

Direcciones IP

La IP es un número de identificación único asociado a la tarjeta de red (NIC). Es única y ha de estar dentro del rango de direcciones del NIC. En las LAN privadas no hace falta.

Es la dirección de cada ordenador y puede cambiar en cualquier momento.

Cada dirección IP consta de 32 bits en 4 grupos de 8 bits.

Notación decimal de una dirección IP

Utilizamos las direcciones IP en formato decimal, pasando el valor binario de cada octeto al sistema decimal y separándolo con un punto. Cada uno de ellos varía entre 0 y 255.

Partes de una dirección IP

- Bits de red - Son los bits que identifican la red a la que está conectado el host. Es decir, todos los equipos que pertenecen a la misma red dentro de esa red tendrán el mismo identificador de red.
- Bits de host - Son los bits que identifican a un host particular dentro de una red. No puede haber, en la misma red, dos equipos con el mismo valor en el identificador de host de su dirección IP.

El número de bits de red no tiene por qué ser el mismo que el número de bits de host.

Direcciones unicast: direcciones que sirven para identificar a un equipo concreto.

Dirección MAC - dirección de control de acceso al medio

La dirección MAC se refiere al nombre de cada ordenador y siempre es el mismo (no cambia) se escribe en hexadecimal.

Todas las tarjetas de red disponen de un identificador exclusivo MAC que trabaja en la 2 capa (enlace de datos del modelo OSI).

Cualquier dispositivo conectado a una red necesita disponer de una MAC para identificarse a nivel de la Capa de Enlace

La dirección MAC está formada por 48 bits de los cuales los 24 primeros identifican al fabricante, y los 24 siguientes son el número de serie/referencia que el fabricante le ha asignado a la NIC.

Toda trama de información que circula por una red tiene encapsulada una MAC de origen y una de destino, debiendo llegar al dispositivo con dicha MAC.

Clases de redes

La dirección 127.0.0.1 es la dirección de loopback y apunta a tu pc desde tu pc, referencia al localhost.

- Clase A: redes muy grandes con muchos hosts. Tiene 126 redes.
- Clase B: redes de tamaño medio. Tiene 16.384 redes.
- Clase C: redes pequeñas, inferiores a 254 hosts. Tiene 2.097.152 redes.
- Clase D: identifican un grupo de host, se reservan para envíos múltiples (un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase). Tiene 16 redes.
- Clase E: se usa con fines experimentales. Tiene 15 redes.

Direcciones publicas

Son accesibles por cualquier “ordenador” conectado a “Internet”.

Hay que comunicar al NIC que clase de red se va a instalar y completar la IP añadiendo el número de host que se vayan instalando.

Direcciones privadas

Son accesibles desde “equipos privados” conectados en “redes locales”. las direcciones que colocaremos en cada equipo son irrelevantes, pues no establecerá conflicto con ningún otro ordenador del mundo. Son direcciones IP que no son utilizadas nunca en Internet. en la numeración hay que respetar siempre el mismo número de red para todos los equipos, solo iremos variando el número del host.

Ip reservadas para LAN privadas

- Clase A: desde 10.0.0.0 hasta 10.255.255.255
- Clase B: desde 172.16.0.0 hasta 172.31.255.255
- Clase C: desde 192.168.0.0 hasta 192.168.255.255

Estas redes podrán conectarse posteriormente a Internet mediante dispositivos Router o Proxy.

Mascara de red subred

Una máscara de subred es una secuencia de 32 bits que sirve para determinar cómo distinguir

lo que es red de lo que es host en una dirección IP y determina el tipo de clase de red.

La máscara de red la utilizan los routers y los switches para comprobar si dos equipos pertenecen o no a la misma red.

Dirección de broadcast → identifica a todos los equipos. Se pone todos los bits de host a 1.

Comprobar si dos equipos pertenecen a la misma red (comparten medio físico)

1. AND lógico entre IP1 y la máscara de red → obtendrá la red o subred.
2. AND lógico entre IP2 y la máscara de red.

3. XNOR a los resultados de las operaciones anteriores.

Resultado:

- Todo a 1: están en la misma red.
- 1 y 0: NO están en la misma red lógica.

Protocolo IPv6

Emplea 128 bits y se representa en hexadecimal en bloques de dos bytes.

Protocolo TCP (transcription transfer protocol) y UDP (user datagram protocol)

- Protocolo TCP: garantiza que todos los segmentos llegan al destino, es confiable pero lento. Usado por FTP y HTTP.
- Protocolo UDP: envía segmentos de manera rápida sin importar si llegan o no. Aplicaciones de streaming.

Protocolo TCP/IP

Parámetros

- Ip: Asigna una dirección ip a un adaptador de red, la ip es suministrada por el administrador de la red de la instalación.
- Máscara de subred: determina como distinguir la red del host y el tipo de clase de red.
- Puerta de enlace (gateway): es la dirección del enrutador local, reenvía el tráfico a destinos fuera de la red local.
- DNS: traduce direcciones de dominio a direcciones ip.
- Servidor DHCP: establece direcciones ip dentro del rango asignado.

Componentes interconexión de redes

Capa	Dispositivo	Función
Física	Repetidor	Regenera la señal entre dos puntos de una red. Existen inalámbricos o cableados.
	Hub	Replica la información entrante por uno de sus puertos al resto de puertos.
Enlace de datos	Switch	Conecta la información entrante por uno de sus puertos al puerto de destino única-mente.
	Punto de acceso	Extiende la red cableada mediante un medio inalámbrico. Pertenece a las capas 1 y 2 del modelo OSI.
Red	Router	Conecta redes diferentes.

- Switch: divide una red en subredes, evitando que colisionen paquetes de datos. Cada puerto es un segmento diferente.
- Router: pertenece a la capa de red del modelo OSI y conecta diferentes redes. Dispone de su propio sistema operativo. Utiliza tablas de enrutamiento para encaminar los paquetes.
- Hub: Dispositivo de red que trabaja en la capa física del modelo OSI. Solo cuenta con un dominio de colisión.

Topología física y lógica. Mapas

Los mapas establecen la organización física o lógica de los dispositivos y componentes implicados.

- Topología física: organización de los componentes y conexiones físicas.
    - Inalámbricas
        - Distribuida: emplea puntos de acceso para que el cliente se pueda mover libremente saltando de uno a otro.
        - Centralizada: utiliza puntos de acceso sin capacidad de gestión. Emplea switches WLAN que realizan el control y la gestión de la red wifi.
    - Cableadas
        - WAN: redes de área extensa
            - Punto a punto: dos equipos se comunican directamente.
            - Estrella: equipo central que conecta al resto.
            - Malla: los equipos están interconectados entre si.
        - LAN: redes locales
            - Estrella:
            - Estrella extendida: estrellas interconectadas entre si.
            - Bus: medio compartido.
            - Anillo: medio compartido cerrado.

- Topología lógica: establece la configuración de la comunicación y el acceso al medio.
    - WLAN: considera una conexión punto a punto entre dos equipos.
    - LAN: conjunto de reglas para controlar el medio compartido.
        - Método de acceso por contienda (redes Ethernet y wifi): escucha antes de enviar la trama para ver si el medio esta libre
        - Método de acceso controlado (redes físicas en anillo): establece un turno para enviar tramas.

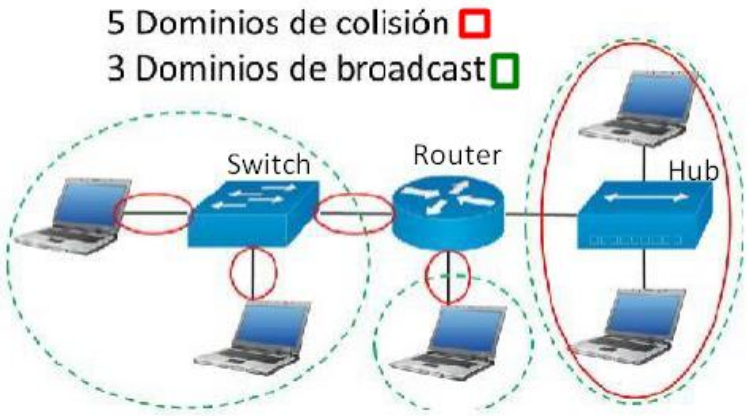
Dominios de colisión y difusión

Segmentar una red en dominios mejora la eficiencia y aumenta el ancho de banda. Los hubs extienden los dominios de colisión mientras que los switches y routers lo limitan.

- Dominio de colisión: área donde pueden colisionar paquetes.
    - Hub: solo cuenta con un dominio de colisión.

- Switch: cada puerto es un segmento de colisión.

- Dominios de difusión o broadcast: áreas donde se reciben tramas de broadcast. Es una separación lógica dentro de la red de ordenadores en la que los mensajes, normalmente paquetes de capa 3 en el modelo OSI, pueden ser difundidos. Los hub, switches y bridges no limitan estos dominios.



Tipos de redes

Según su tamaño:

- PAN redes de área personal: entorno usuario.
- LAN/WLAN redes de área local/ inalámbrica: poco alcance, un hogar, una oficina…
- MAN/WMAN redes de área metropolitana: constituida por varias redes LAN.
- WAN redes de área extensa: conecta redes LAN a largas distancias.

Según su transmisión:

- Redes punto a punto: de host de origen a host de destino a través de un medio.
- Redes multipunto: de un host de origen a múltiples destinos a través del mismo medio.

Según su función:

- Redes entre iguales: los hosts ofrecen y acceden por igual a los servicios.
- Redes cliente-servidor: unos host ofrecen servicios y recursos (servidores) y otros acceden a ellos (clientes).

Según los medios empleados:

- Inalámbricas: emplea ondas electromagnéticas para transmitir información por el aire.

- Cableada: utiliza un medio físico para transmitir señales (cable).
- Mixtas: ambos.

Acceso a redes WAN

Redes privadas

- Conmutación de circuitos: se establece un canal entre nodos y terminales.
- Conmutación de paquetes: divide los datos para transmitir en paquetes a través de una red compartida. Establece comunicación entre multitud de pares de nodos a través del mismo canal. Es la más económica.
- Dedicada: conexión directa y permanente entre dos nodos de la red WAN del proveedor de servicios. Coste muy elevado.

Redes públicas

- DSL (Digital Suscriber Line): accede a internet a través de cables de cobre.
- FTTH o fibra hasta el hogar: fibra óptica desde la red troncal hasta los clientes
    - OTL (Optical Line Termination): dispositivo activo del que parten las fibras a los diferentes usuarios.
    - Divisor óptico o splitter: divide la señal óptica entrante en partes iguales de menor potencia a diferentes ramas o usuarios.
    - ONT (Optical Network Terminal): convierte las señales ópticas en electicas y viceversa. Se integra en los routers SoHo.
- HFC o hibrido fibra-coaxial: fibra óptica desde la red troncal y cable coaxial hasta los hogares.
- Inalámbricas: utiliza ondas electromagnéticas. Son muy empleadas en redes WAN
    - WiMAX: para zonas sin cobertura por cable. Red de alta velocidad para redes MAN. Se necesitan dispositivos que emitan microondas y reciban esto.
    - Wi-fi: transmisión de datos a gran velocidad en redes locales. A menor frecuencia mayor alcance y menor ancho de banda.
    - WPAN
        - Bluetooth: facilita la transmisión entre dispositivos cercanos.
        - Zigbee: baja tasa de transferencia de datos. Control y monitorización a bajo coste.
    - LTE-A(4G) 5G: comunicación de redes WMAN y WWAN.

Tipologías de red

- Modo ad hoc (IBSS): dos clientes se conectan directamente sin emplear ningún dispositivo de infraestructura.
- Modo de infraestructura: los clientes se conectan a través de dispositivos de infraestructura (puntos de acceso inalámbrico) a un sistema de distribución (switches o routers). Hay 2 tipos:
    - BSS (conjunto servicios básicos): un punto de acceso con servicios básicos que cubre una zona determinada.
    - ESS (conjunto servicios extendidos): varios puntos de acceso conectados mediante un sistema de distribución ampliando la zona de cobertura.

Ficheros de configuración de red

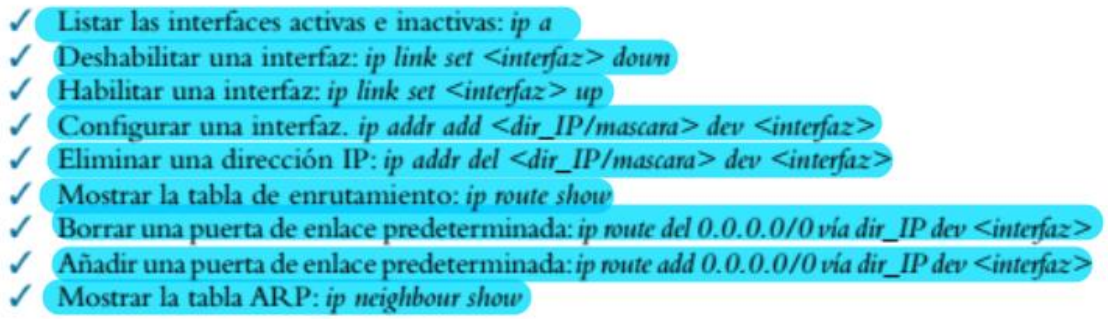
Ubuntu

- /etc/hosts → entrada con asignaciones entre direcciones IP y nombres de hosts. Este archivo tiene prioridad sobre la configuración DNS del equipo.

Windows

- C:\Windows\system32\drivers\etc\ → asociaciones entre IP y dominios.
- Ipconf → monitoreo interfaces red

Monitorización y verificación de una red mediante comandos



- Ping a la tarjeta de red: 127.0.0.1 comprobar que red interna funciona bien
- traceroute: da la ruta que sigue un paquete desde la ip de origen a la de destino. Busca fallos de conectividad.
- nmap: auditorias y funciones de seguridad.

Gestión de puertos

- Puerto físico:
- Puerto lógico: número que se asocia a la aplicación de origen o destino de una comunicación.
    - Bien conocidos: 0 al 1023 reservados para aplicaciones y servicios HTTP(80), FTP(20), HTTPS (443)
    - Registrados: 1024 al 49151 conectan aplicaciones de usuario a servidores
    - Dinámicos, privados o efímeros: aplicaciones de intercambio punto a punto.

Socket: combinación de ip y puerto de destino. Una comunicación entre dos host tiene una pareja de sockets. IP:Puerto.

Windows: netstat

Linux: ss

Mantenimiento

- Predictivo: utilidades de diagnostico
- Preventivo: acciones técnicas y procedimientos y su frecuencia
- Correctivo: método para diagnosticar y resolver averías.

Tema 6 – Gestión de recursos en red

Permisos

Security principals: grupo de usuarios identificados por SID

Permisos normales (pestaña seguridad)

Tipos	Permisos	Descripción
Permisos en carpetas	Mostrar el contenido de la carpeta	Posibilita listar el contenido de la carpeta
	Lectura	Permite ver el contenido de la carpeta, permisos, propietario y atributos
	Escritura	Posibilita crear nuevos archivos y subcarpetas, ver el propietario, modificar atributos y permisos
	Lectura y ejecución	Permite navegar por las subcarpetas más los permisos de lectura y mostrar el contenido
	Modificar	Posibilita eliminar la carpeta más los permisos de lectura y ejecución
	Control total	Permite cambiar permisos, eliminar subcarpetas y archivos, tomar posesión y todos los permisos anteriores
	Permisos especiales	Se habilita cuando se activa uno de ellos
Permisos en archivos	Lectura	Permite ver el contenido del archivo, propietarios, permisos y atributos
	Escritura	Posibilita modificar su contenido y sus atributos, así como ver el propietario, permisos y atributos
	Lectura y ejecución	Permite ejecutar el archivo más el permiso de lectura
	Modificar	Posibilita modificar y eliminar el archivos más los permisos de escritura, y lectura y ejecución
	Control total	Permite cambiar permisos, tomar posesión más todos los permisos anteriores
	Permisos especiales	Se habilita cuando se activa uno de ellos

Permisos especiales (opciones avanzadas)

Permiso especial	Descripción
Atravesar carpeta/ ejecutar archivo	Posibilita moverse por carpetas, aunque no se tenga permiso de acceso. En archivos, permite su ejecución
Mostrar carpeta/ leer datos	Permite visualizar los nombres de ficheros y subcarpetas de una carpeta. En archivos, posibilita leer su contenido
Leer atributos	Permite ver los atributos de un archivo o carpeta como lectura y oculto
Leer atributos extendidos	Permite ver los atributos extendidos de un archivo o carpeta. Los atributos extendidos están definidos por los programas y pueden variar según estos
Crear archivos/ escribir datos	En carpetas, permite crear archivos. En archivos, permite modificar su contenido
Crear carpetas/ anexar datos	En carpetas, permite crear carpetas. En archivos, posibilita añadir datos sin modificar los existentes
Escribir atributos	Permite modificar los atributos del archivo o carpeta
Escribir atributos extendidos	Permite modificar los atributos extendidos del archivo o carpeta
Eliminar	Permite eliminar el archivo o la carpeta
Permisos de lectura	Permite leer los permisos del archivo o la carpeta
Cambiar permisos	Permite modificar los permisos del archivo o de la carpeta
Tomar posesión	Permite tomar posesión de un archivo o carpeta

- Se pueden definir los permisos NTFS solo en las unidades con formato NTFS.
- Los permisos no permitidos explícitamente están implícitamente denegados.
- Los permisos se suman cuando un usuario pertenece a distintos grupos.
- La denegación de permisos tiene preferencia sobre la concesión.
- Los permisos sobre ficheros prevalecen sobre los de carpeta.

Permisos en red (pestaña compartir- carpetas)

En caso de conflicto se aplican los más restrictivos.

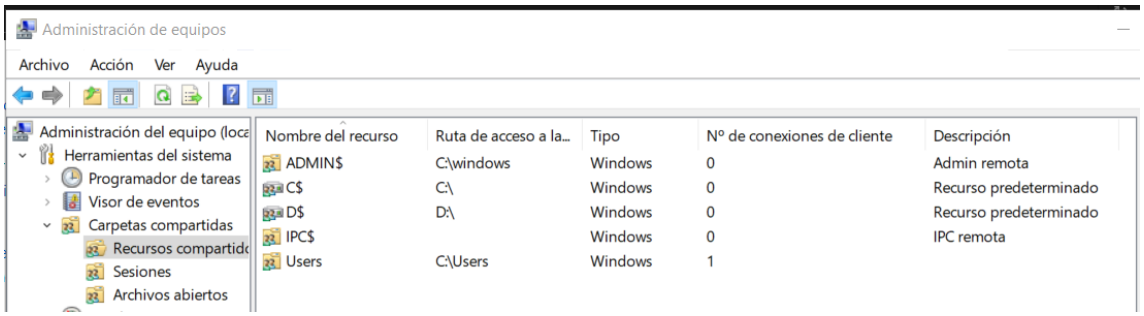
Compartir archivos o carpetas

- Equipos en la misma subred lógica
- Activar detección de redes y recursos compartidos
- Mismo grupo de trabajo en el equipo

Acceder a un recurso compartido:

- Carpeta red
- A través explorador en formato UNC: \\Equipo\\Recurso

- Red → conectar a una unidad de red.
- Explorador archivos → localhost
- Panel de control → sistema → herramientas administrativas → adm de equipos → carpetas compartidas → recursos compartidos



Se comparten las unidades, el directorio del sistema (admin), tuberías comunicación de procesos (IPCs)

Herencia

Permisos heredados: pasan de objetos primarios a secundarios. Controlada por propietario. Es dinámica (modificar la primaria afecta a la secundaria).

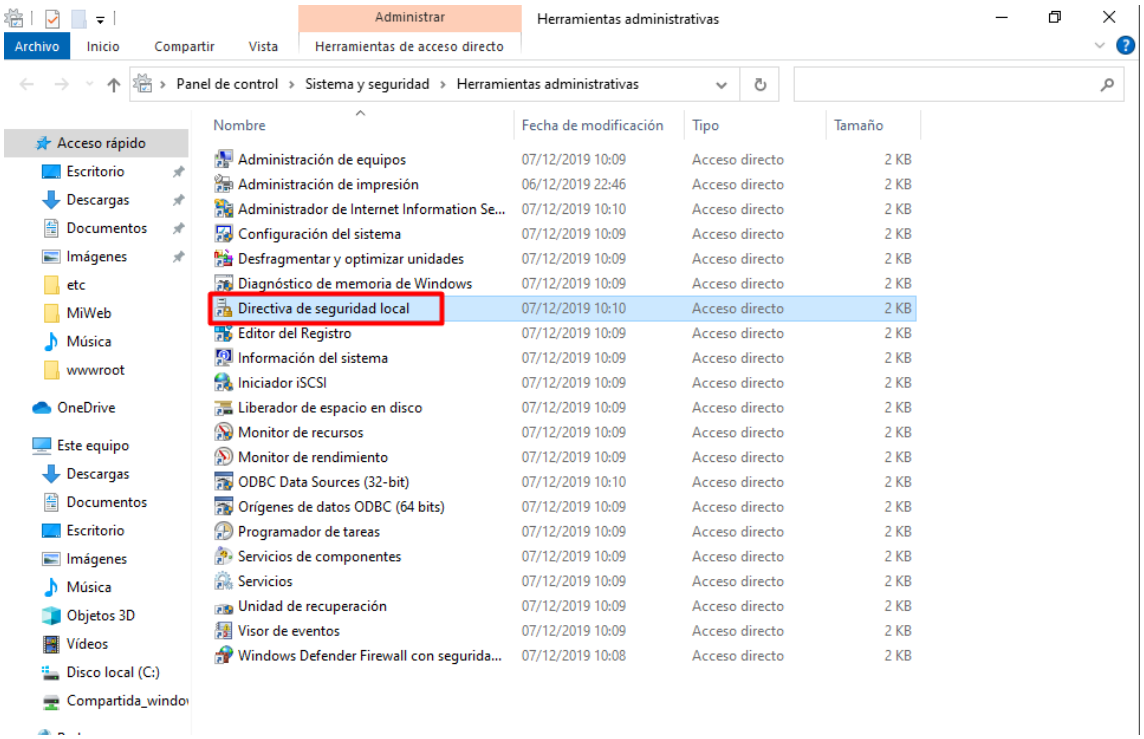
Opciones de seguridad avanzada → deshabilitar herencia

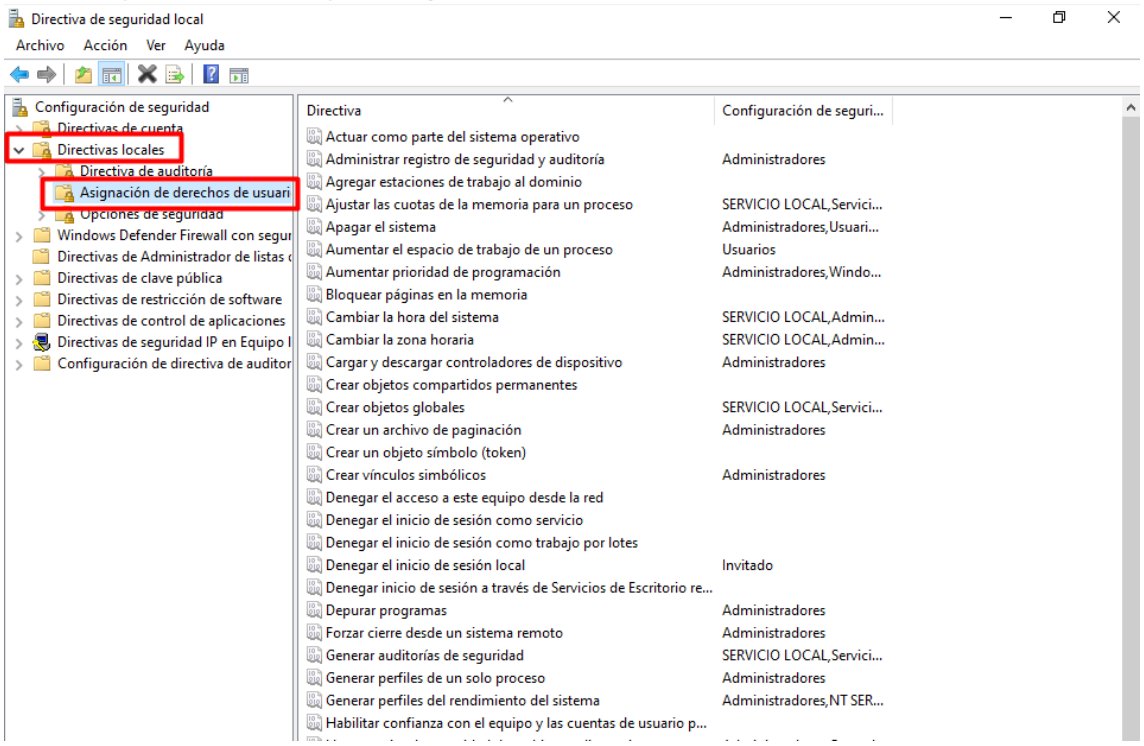
ACL lista de control de accesos

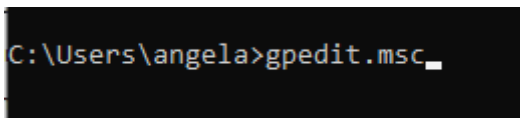
Para cada usuario o grupo existe una entrada de control de acceso (ACE) → pestaña seguridad

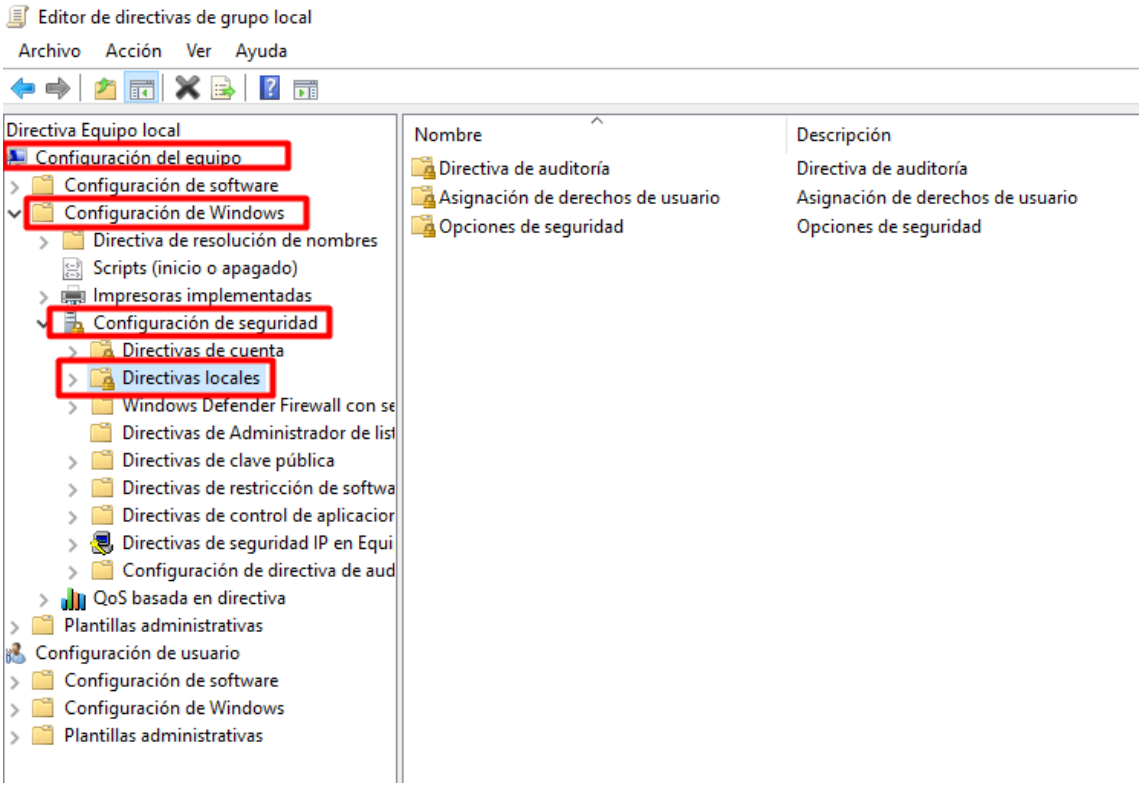
Derechos de usuario – privilegios

- Derechos de inicio de sesión: de qué modo y quien inicia sesión
- Privilegios específicos: derechos del usuario una vez ha accedido al sistema


Administrar
Herramientas administrativas
Archivo
Inicio
Compartir
Vista
Herramientas de acceso directo
Panel de control › Sistema y seguridad › Herramientas administrativas
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
etc
MiWeb
Música
wwwroot
OneDrive
Este equipo
Descargas
Documentos
Escritorio
Imágenes
Música
Objetos 3D
Vídeos
Disco local (C:)
Compartida_windo
Nombre
Fecha de modificación
Tipo
Tamaño
Administración de equipos 07/12/2019 10:09 Acceso directo 2 KB
Administración de impresión 06/12/2019 22:46 Acceso directo 2 KB
Administrador de Internet Information Se... 07/12/2019 10:10 Acceso directo 2 KB
Configuración del sistema 07/12/2019 10:09 Acceso directo 2 KB
Desfragmentar y optimizar unidades 07/12/2019 10:09 Acceso directo 2 KB
Diagnóstico de memoria de Windows 07/12/2019 10:09 Acceso directo 2 KB
Directiva de seguridad local 07/12/2019 10:10 Acceso directo 2 KB
Editor del Registro 07/12/2019 10:09 Acceso directo 2 KB
Información del sistema 07/12/2019 10:09 Acceso directo 2 KB
Iniciador iSCSI 07/12/2019 10:09 Acceso directo 2 KB
Liberador de espacio en disco 07/12/2019 10:09 Acceso directo 2 KB
Monitor de recursos 07/12/2019 10:09 Acceso directo 2 KB
Monitor de rendimiento 07/12/2019 10:09 Acceso directo 2 KB
ODBC Data Sources (32-bit) 07/12/2019 10:10 Acceso directo 2 KB
Orígenes de datos ODBC (64 bits) 07/12/2019 10:09 Acceso directo 2 KB
Programador de tareas 07/12/2019 10:09 Acceso directo 2 KB
Servicios de componentes 07/12/2019 10:09 Acceso directo 2 KB
Servicios 07/12/2019 10:09 Acceso directo 2 KB
Unidad de recuperación 07/12/2019 10:09 Acceso directo 2 KB
Visor de eventos 07/12/2019 10:09 Acceso directo 2 KB
Windows Defender Firewall con segurida... 07/12/2019 10:08 Acceso directo 2 KB


Directiva de seguridad local
Archivo
Acción
Ver
Ayuda
Configuración de seguridad
Directivas de cuenta
Directivas locales
Directiva de auditoría
Asignación de derechos de usuari
Opciones de seguridad
Windows Defender Firewall con segur
Directivas de Administrador de listas
Directivas de clave pública
Directivas de restricción de software
Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo
Configuración de directiva de auditor
Directiva
Configuración de seguri...
Actuar como parte del sistema operativo
Administrar registro de seguridad y auditoría Administradores
Agregar estaciones de trabajo al dominio
Ajustar las cuotas de la memoria para un proceso SERVICIO LOCAL,Servici...
Apagar el sistema Administradores,Usuari...
Aumentar el espacio de trabajo de un proceso Usuarios
Aumentar prioridad de programación Administradores,Windo...
Bloquear páginas en la memoria
Cambiar la hora del sistema SERVICIO LOCAL,Admin...
Cambiar la zona horaria SERVICIO LOCAL,Admin...
Cargar y descargar controladores de dispositivo Administradores
Crear objetos compartidos permanentes
Crear objetos globales SERVICIO LOCAL,Servici...
Crear un archivo de paginación Administradores
Crear un objeto símbolo (token)
Crear vínculos simbólicos Administradores
Denegar el acceso a este equipo desde la red
Denegar el inicio de sesión como servicio
Denegar el inicio de sesión como trabajo por lotes
Denegar el inicio de sesión local Invitado
Denegar inicio de sesión a través de Servicios de Escritorio re...
Depurar programas Administradores
Forzar cierre desde un sistema remoto Administradores
Generar auditorías de seguridad SERVICIO LOCAL,Servici...
Generar perfiles de un solo proceso Administradores
Generar perfiles del rendimiento del sistema Administradores,NT SER...
Habilitar confianza con el equipo y las cuentas de usuario p...


C:\Users\angela>gpedit.msc



Directivas de seguridad. Objeto y ámbito de directivas

Reglas de seguridad para administrar usuarios y equipos – directivas de grupo (GPO).

- GPO locales: equipos que no forman parte de un dominio. Actúa sobre el propio equipo local.
    - Directivas de configuración de equipo: modificaciones se aplican en el arranque de sistema.
    - Directivas de configuración de usuario: modificaciones se aplican en cada inicio de sesión del usuario.
    - Configuración y actualización de software
    - Configuración de Windows
    - Plantillas administrativas: configuración y ajustes del equipo. Es la más importante.
- GPO no locales: orientadas al servicio de Active Directory.

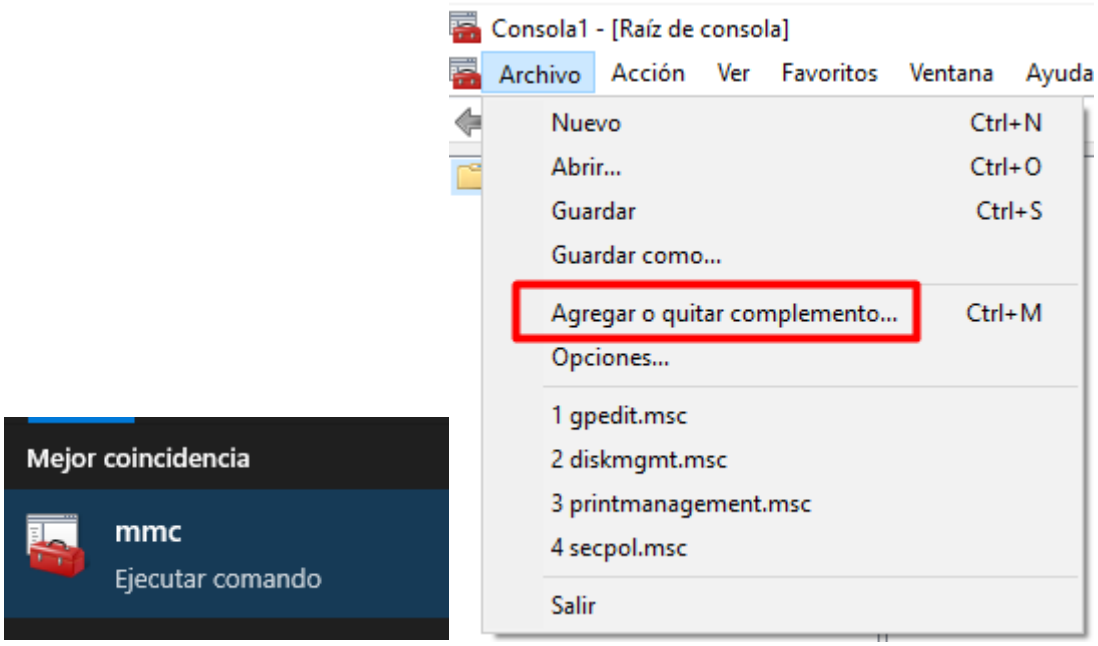
Listar GPO → gpresult /r (sistema) o gpresult /user angela /v

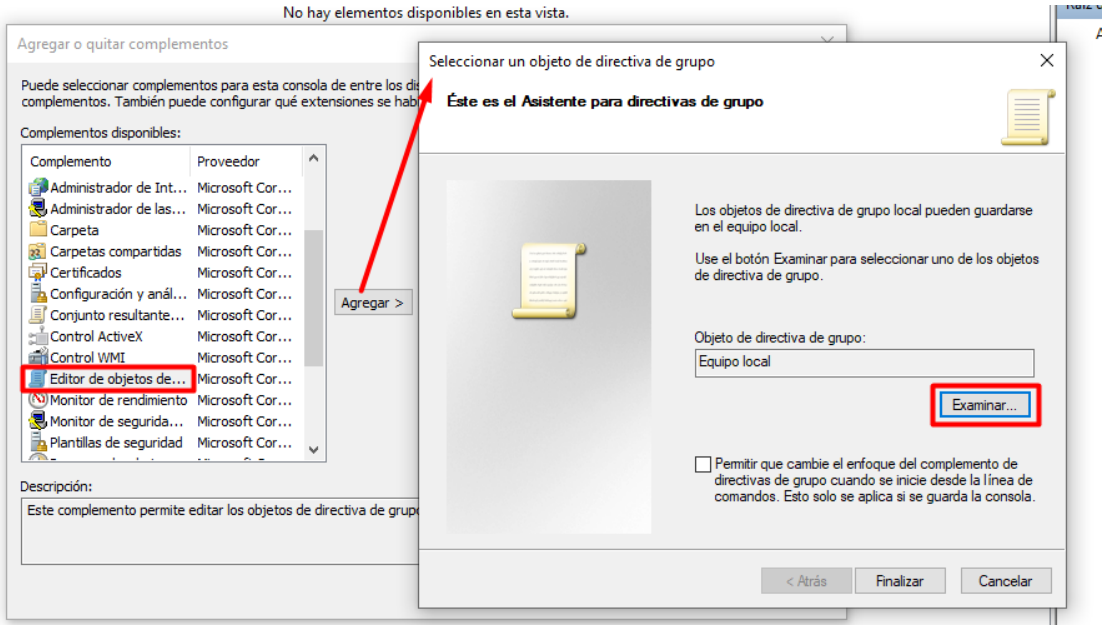
Plantillas

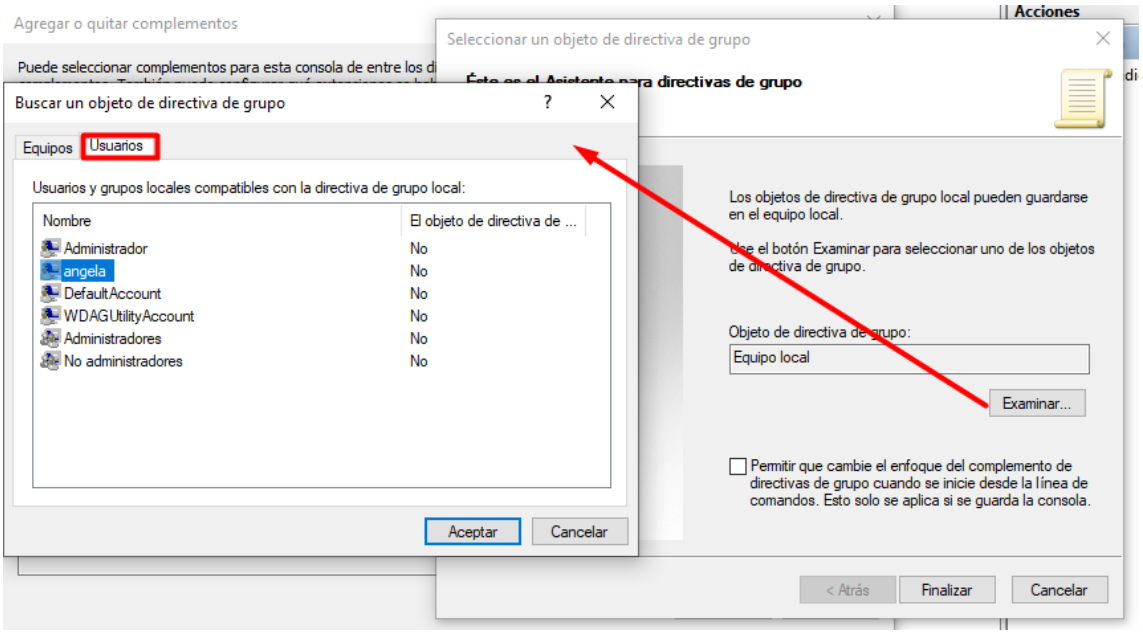
Definen configuración registro Windows para administrar aplicaciones o características del sistema operativo o aplicaciones de terceros.

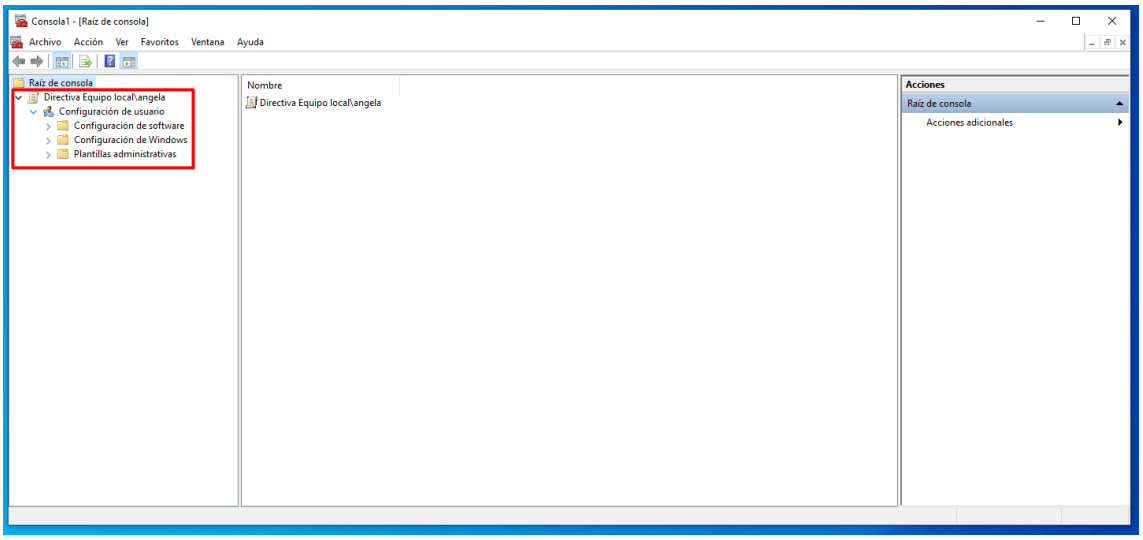
Requisitos de seguridad del sistema y de los datos. Seguridad a nivel de usuario y de equipos

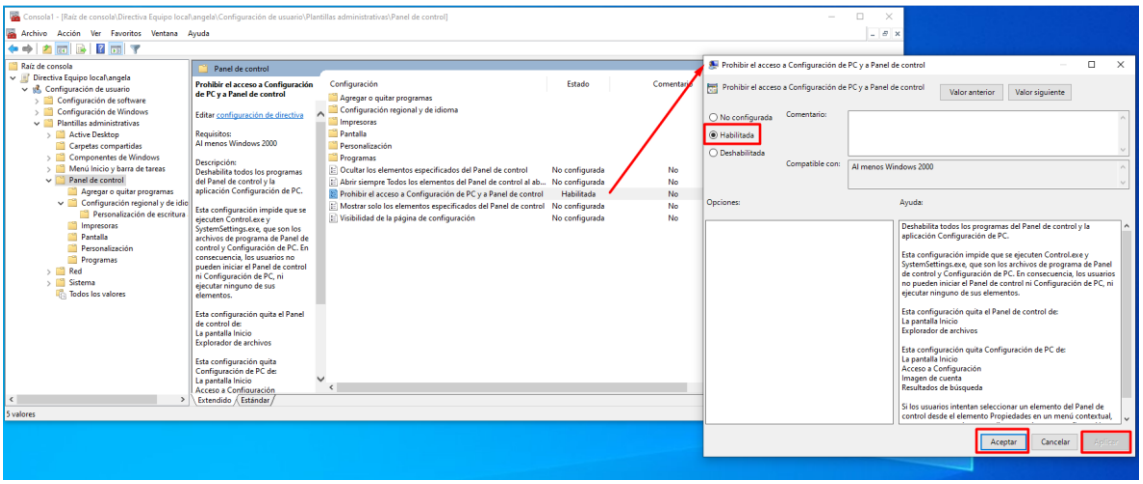
Permite crear consolas personalizadas que aumenten la productividad y se adapten a las preferencias individuales.

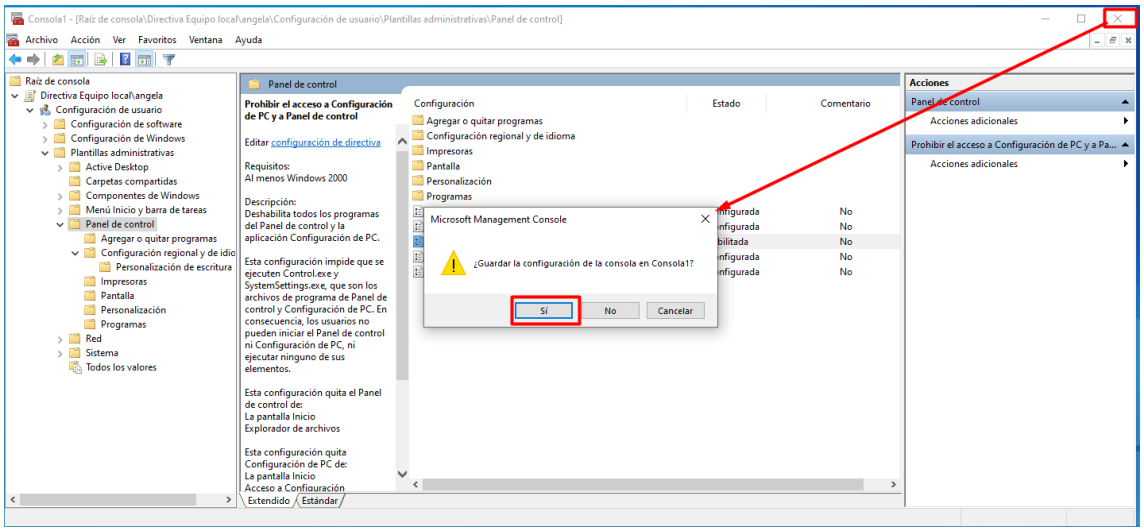

Consola1 - [Raíz de consola]
Archivo
Acción
Ver
Favoritos
Ventana
Ayuda
Nuevo Ctrl+N
Abrir... Ctrl+O
Guardar Ctrl+S
Guardar como...
Agregar o quitar complemento... Ctrl+M
Opciones...
1 gpedit.msc
2 diskmgmt.msc
3 printmanagement.msc
4 secpol.msc
Salir
Mejor coincidencia
mmc
Ejecutar comando


No hay elementos disponibles en esta vista.
Agregar o quitar complementos
Puede seleccionar complementos para esta consola de entre los di
complementos. También puede configurar qué extensiones se hab
Complementos disponibles:
Complemento
Proveedor
Administrador de Int... Microsoft Cor...
Administrador de las... Microsoft Cor...
Carpeta Microsoft Cor...
Carpetas compartidas Microsoft Cor...
Certificados Microsoft Cor...
Configuración y anál... Microsoft Cor...
Conjunto resultante... Microsoft Cor...
Control ActiveX Microsoft Cor...
Control WMI Microsoft Cor...
Editor de objetos de... Microsoft Cor...
Monitor de rendimiento Microsoft Cor...
Monitor de seguridad... Microsoft Cor...
Plantillas de seguridad Microsoft Cor...
Agregar >
Descripción:
Este complemento permite editar los objetos de directiva de grup
Seleccionar un objeto de directiva de grupo
Éste es el Asistente para directivas de grupo
Los objetos de directiva de grupo local pueden guardarse en el equipo local.
Use el botón Examinar para seleccionar uno de los objetos de directiva de grupo.
Objeto de directiva de grupo:
Equipo local
Examinar...
Permitir que cambie el enfoque del complemento de directivas de grupo cuando se inicie desde la línea de comandos. Esto solo se aplica si se guarda la consola.
< Atrás
Finalizar
Cancelar


Agregar o quitar complementos
Puede seleccionar complementos para esta consola de entre los di
Buscar un objeto de directiva de grupo
Equipos
Usuarios
Usuarios y grupos locales compatibles con la directiva de grupo local:
Nombre
El objeto de directiva de ...
Administrador
No
angela
No
DefaultAccount
No
WDAGUtilityAccount
No
Administradores
No
No administradores
No
Aceptar
Cancelar
Seleccionar un objeto de directiva de grupo
Éste es el Asistente para directivas de grupo
Los objetos de directiva de grupo local pueden guardarse en el equipo local.
Use el botón Examinar para seleccionar uno de los objetos de directiva de grupo.
Objeto de directiva de grupo:
Equipo local
Examinar...
Permitir que cambie el enfoque del complemento de directivas de grupo cuando se inicie desde la línea de comandos. Esto solo se aplica si se guarda la consola.
< Atrás
Finalizar
Cancelar
Acciones


Consola1 - [Raíz de consola]
Archivo
Acción
Ver
Favoritos
Ventana
Ayuda
Raíz de consola
Directiva Equipo local\angela
Configuración de usuario
Configuración de software
Configuración de Windows
Plantillas administrativas
Nombre
Directiva Equipo local\angela
Acciones
Raíz de consola
Acciones adicionales


Panel de control
Prohibir el acceso a Configuración de PC y a Panel de control
Habilitada
Deshabilitada
No configurada
Aceptar
Cancelar



Servidores

Permiten compartir recursos en red.

- Debe estar activo y en funcionamiento para acceder a los recursos
- Escalabilidad. Debe posibilitar el crecimiento del sistema
- Mantenimiento. Tareas de mantenimiento sin mermar su disponibilidad.

Servidor de ficheros

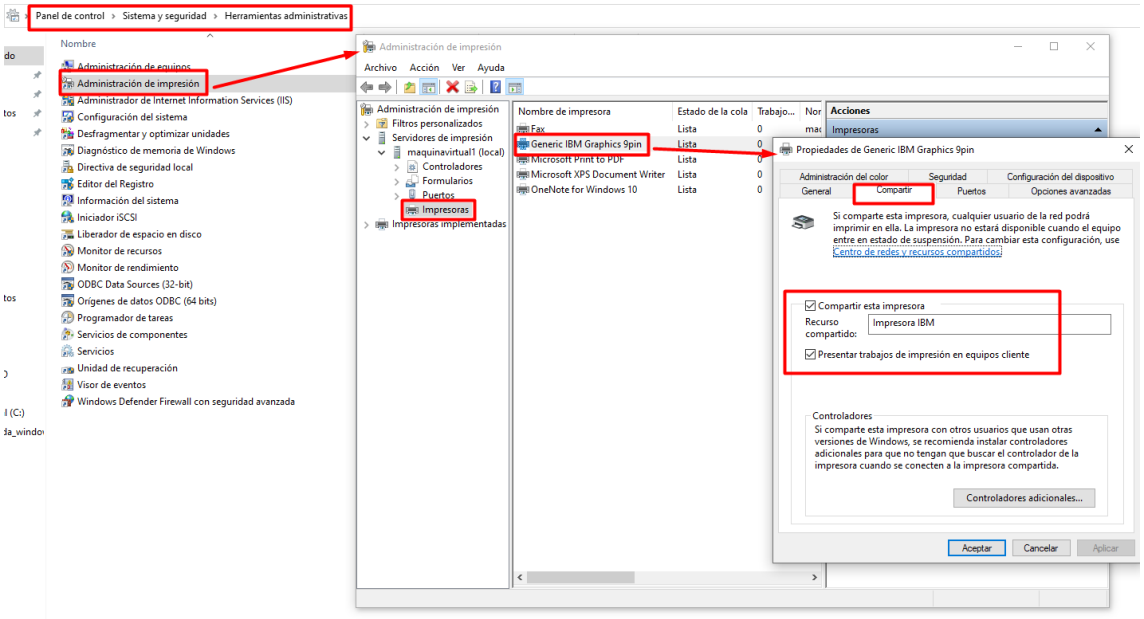
Gestiona el almacenamiento controlado de ficheros en diferentes clientes.

Utilizan protocolos FTP, FTPS y SFTP.

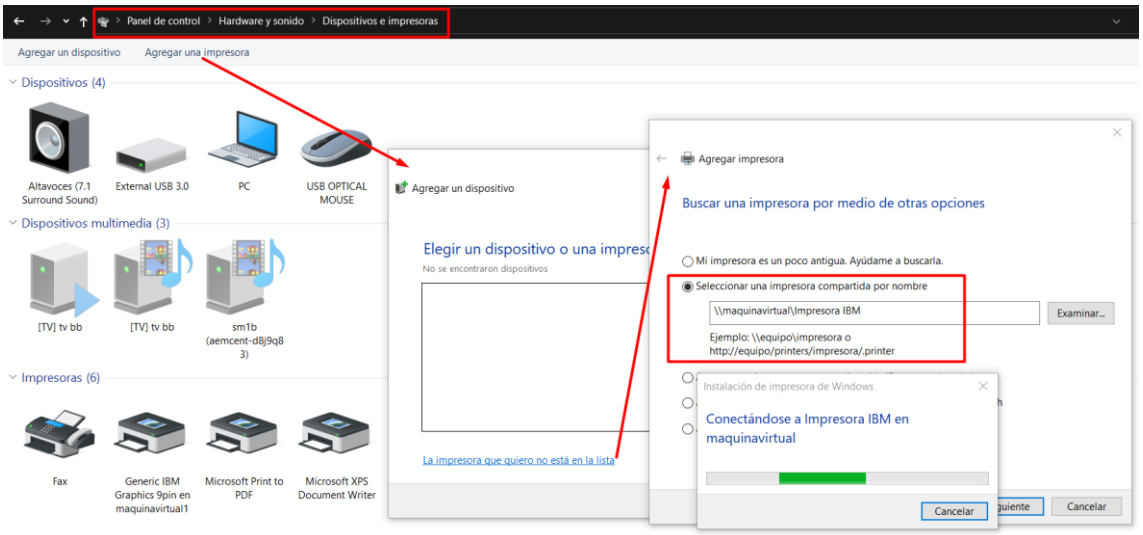
Cliente FTP: Filezilla. Explorador Windows → ftp:\\ip

Servidor de impresión

Posibilita conectividad con impresoras sin depender de host.



Clientes de impresión



Servidor de aplicaciones

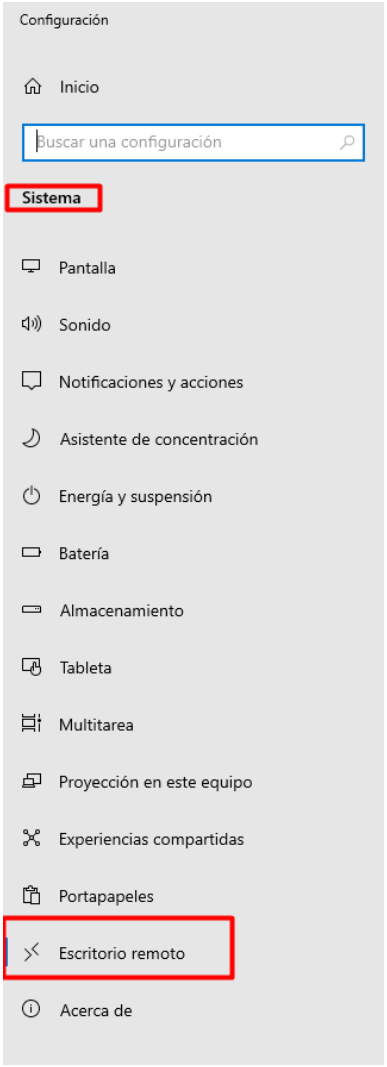
Alojan y ejecutan programas a petición de los clientes.

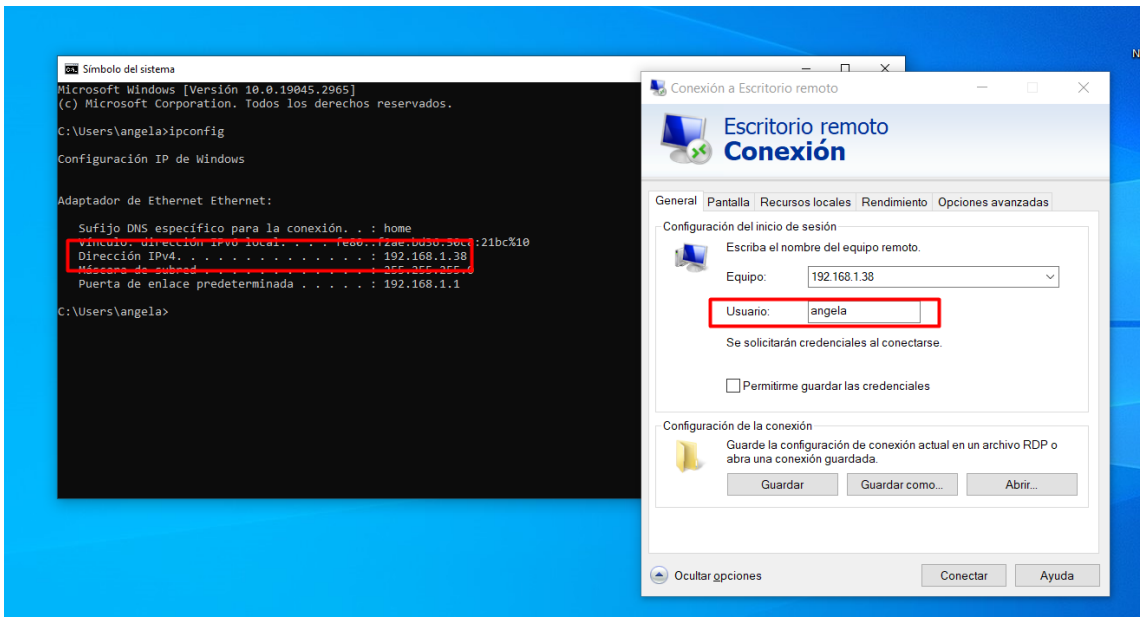
Se utiliza para reducir la complejidad y el tamaño de las aplicaciones, dirigir el flujo de datos para aumentar el rendimiento o controlar la seguridad de los datos.

Arquitectura en 3 capas:

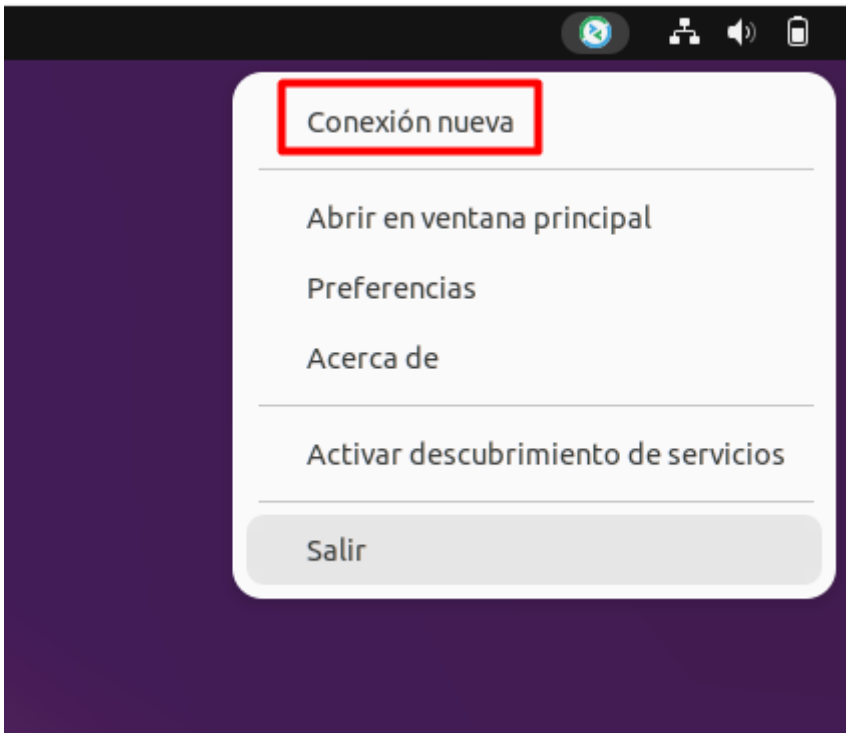
- Nivel 1 presentación: interfaz gráfica GUI del lado del cliente a través de la que se conecta al servidor.
- Nivel 2 aplicación: ejecuta el procesamiento de la información. Intermediario entre cliente y datos.
- Nivel 3 datos: aloja datos para procesar las peticiones del cliente.

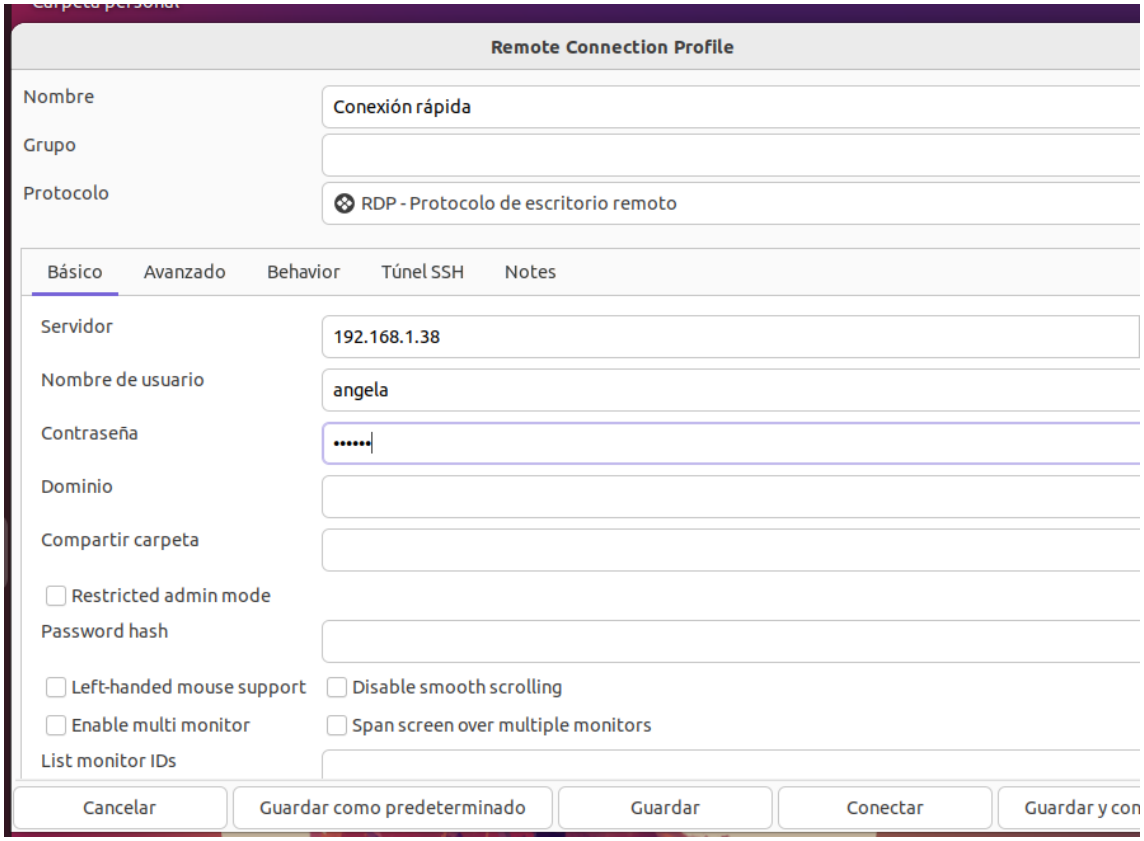
Conexión remota

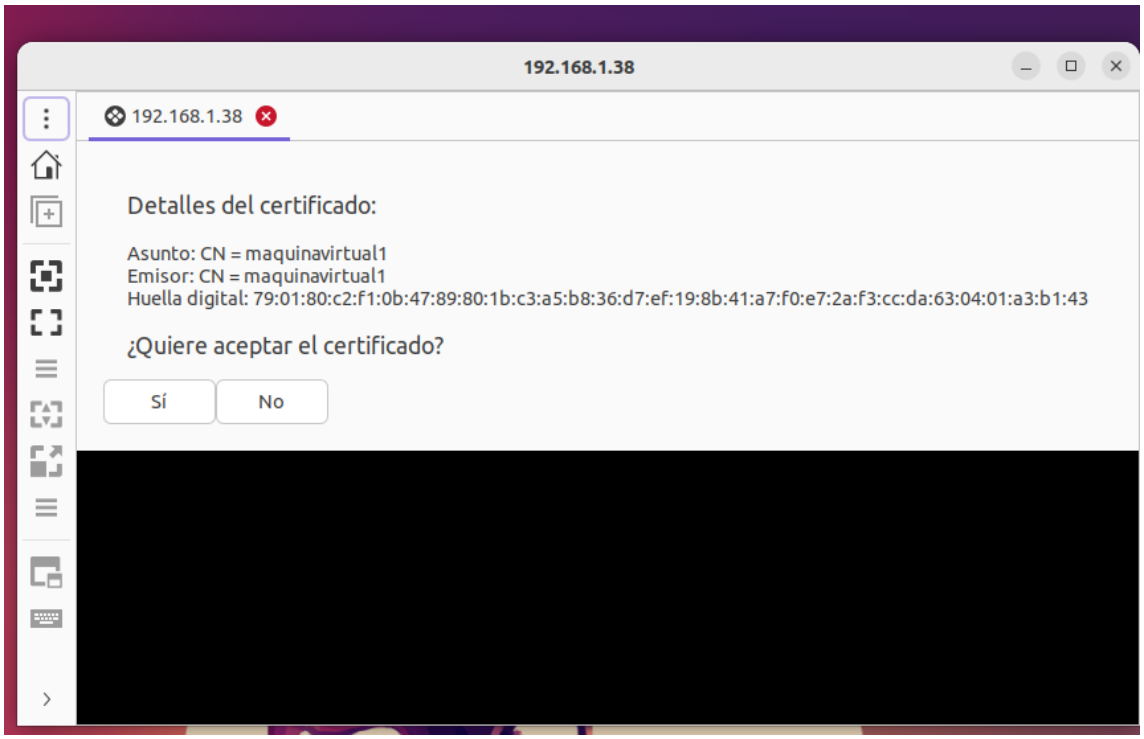




Ubuntu


Conexión nueva
Abrir en ventana principal
Preferencias
Acerca de
Activar descubrimiento de servicios
Salir


Remote Connection Profile
Nombre
Conexión rápida
Grupo
Protocolo
RDP - Protocolo de escritorio remoto
Básico
Avanzado
Behavior
Túnel SSH
Notes
Servidor
192.168.1.38
Nombre de usuario
angela
Contraseña
Dominio
Compartir carpeta
Restricted admin mode
Password hash
Left-handed mouse support
Disable smooth scrolling
Enable multi monitor
Span screen over multiple monitors
List monitor IDs
Cancelar
Guardar como predeterminado
Guardar
Conectar
Guardar y con



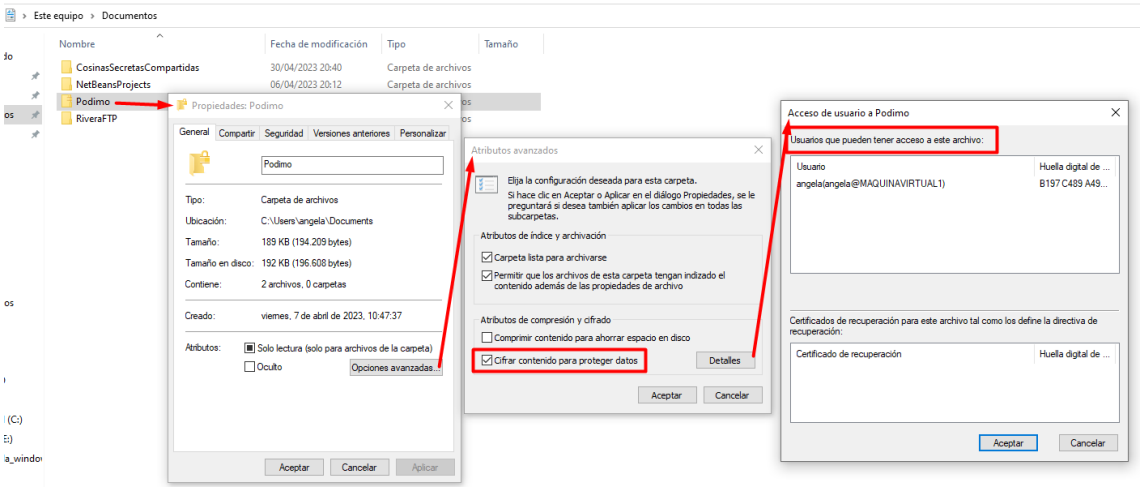
Herramientas de seguridad

Cifrado

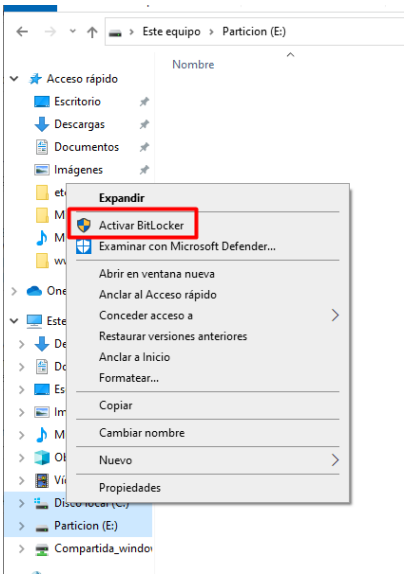
Garantiza la confidencialidad, autenticidad e integridad de los datos a través de la codificación.

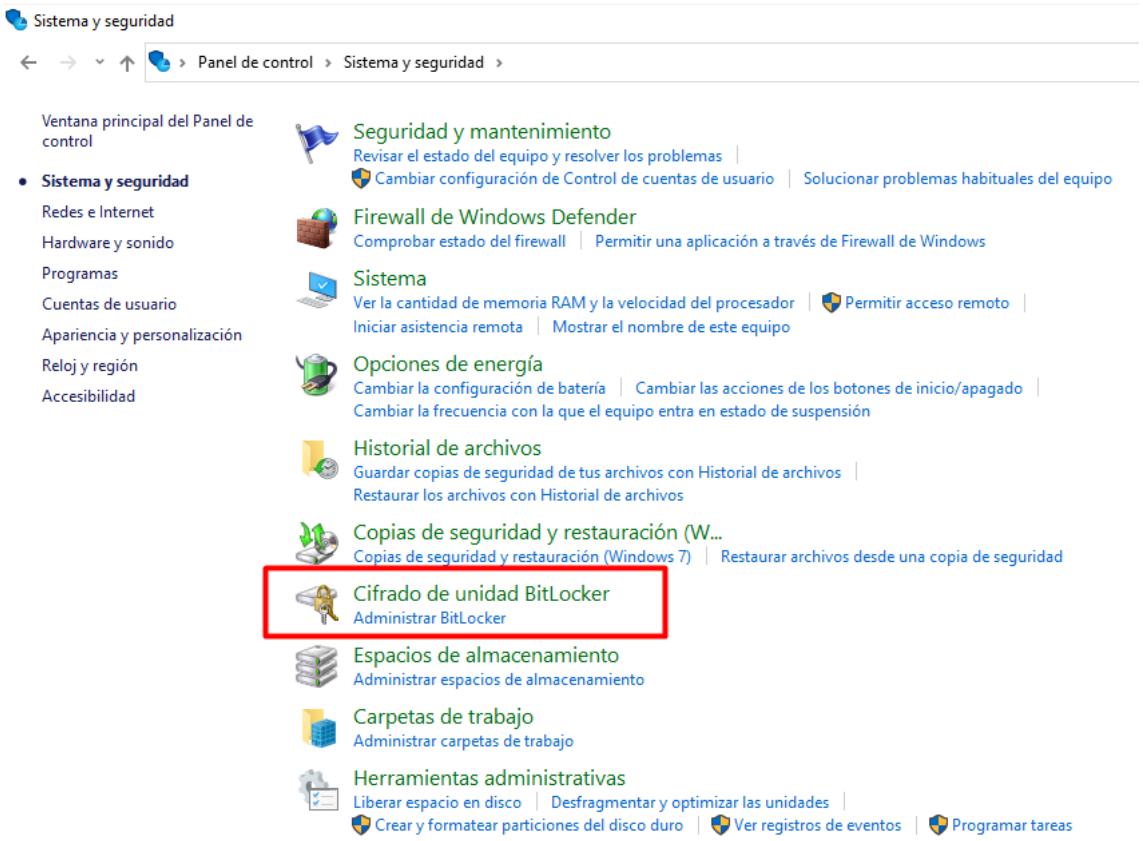
Cifrado EFS: los archivos están disponibles para el usuario que lo cifro pero no para el resto.

- Cifrado EFS



- BitLocker: cifra volúmenes





- Seahorse-nautilus: Ubuntu (contraseñas

Cortafuegos

Controla el trafico entrante y saliente de una red. Filtra las amenazas externas evitando accesos no autorizados. Filtra:

- Paquetes por direcciones IP o MAC.
- Aplicaciones atendiendo al número de puerto.
- Direcciones URL.

Emplea protocolo NAT para ocultar direcciones privadas en dispositivos protegidos.

Tipos de implementación:

- Firewall dedicado: dispositivo hardware especifico que analiza el tráfico a gran velocidad
- Firewall integrado: implementado en dispositivos hardware que agrupan varias funciones como los routers SoHo.
- Firewall por software: aplicaciones software propias o de terceros:
    - Firewall de servidor: orientado a sistemas operativos en red con ámbito sobre los equipos cliente que gobierna.
    - Firewall personal: filtra el trafico entre el equipo y el resto de la red.

Política de seguridad:

- Denegar por defecto: prohíbe todo lo no explícitamente autorizado.
- Aceptar por defecto: prohíbe cualquier comunicación definida explícitamente.

Ubuntu → UFW a través de la interfaz gráfica Gufw.

Sistemas de detección de intrusión IDS

Monitorizan actividades o eventos en una red o host en busca de intentos de acceso sin permiso.

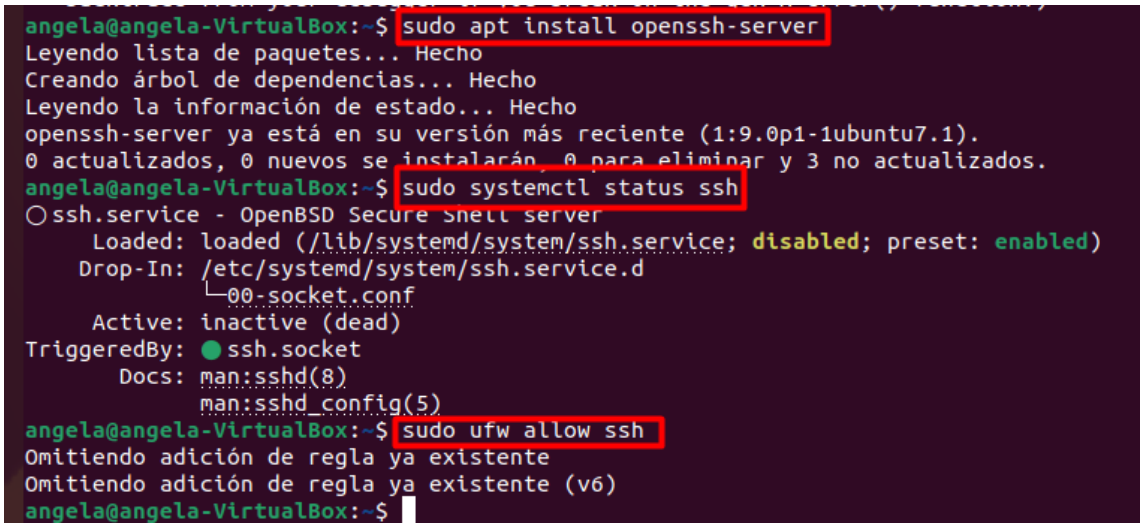
Catalogación:

- Sistema de detección o análisis de intrusiones
    - Detección mediante firmas: coteja el trafico de la red con patrones de reconocimiento predefinidos o firmas de ataques conocidos.
    - Detección mediante anomalías. Compara el comportamiento normal de la red con respecto a alteraciones de los mismos objetos.
- Según respuesta ante ataque:
    - Pasivos: informa a administradores o personal responsable para que tomen medidas.
    - Activos: actúa automáticamente. Informa al personal, recopila información y trata de parar o responder al ataque.
- Según fuente de análisis
    - Sistemas de detección de intrusiones en red (NIDS): analiza el trafico de la red en segmentos estratégicos.
    - Sistemas de detección de intrusiones de host (HIDS): analiza la actividad interna del host a través de archivos de registros, conexiones de red o programas instalados.

OpenSSH

Secure Shell (SSH) y OpenSSH(protocol OpenSSL) permite acceder de forma remota y segura a otro equipo.

Ubuntu:



Modificar archivo /etc/ssh/sshd_config → reiniciar servidor sudo service ssh restart

Para conectar ssh -p <puerto< <usuario>@<ip>

Windows: Putty

Tema 7 – Aplicaciones informáticas

Tipos de software

Por licencia

- Libre: puede ser gratuito o no. Esta mas orientado a la ética.
  El usuario dispone de 4 libertades:
  - Libertad 0: ejecutar el programa con cualquier propósito.
  - Libertad 1: tener acceso al código fuente para estudiarlo y adaptarlo.
  - Libertad 2: distribuir copias.
  - Libertad 3: modificación y mejora.
- Propietario o privativo: prohíbe o se debe autorizar su uso, distribución o modificación.
- Copyleft: garantiza una distribución sin restricciones añadidas. Las licencias presentan un conjunto de cláusulas para su distribución. El software distribuido copiado permanece con el mismo tipo de licencia que su antecesor.
- Dominio público: no tiene derechos de autor. Es software libre sin copyleft que podría degenerar en privativo.
- Sin copyleft o con licencia permisiva: el software distribuido o copiado no tiene que permanecer con la misma licencia que su antecesor.
  - Licencia BSD:
  - Licencia MIT:
  - Licencia Apache:
- Mozilla Public License (MPL): se distribuye el código, pero sin perder el derecho de sus creaciones
- Código abierto open source: es pragmático y deben cumplirse 10 términos.
- Shareware: limita el uso del software hasta su pago.
- Freeware: gratuito y sin limitaciones.
- Licencia OEM: ligada a un equipo físico concreto. Asociada al fabricante del equipo.
- Licencia retail: está destinada a un único equipo pero tiene validez aunque se cambia el hardware.
- Licencias de volumen: activación de múltiples equipos con una licencia.

Por propósito

- Software base o de sistema: aplicaciones, programas o software que actúan de intermediario, gestor o administrador entre usuario y hardware.
- Software de desarrollo de aplicaciones: software para diseñar, desarrollar o implementar software de sistema o de aplicación (editores, compiladores, depuradores e IDE).
- Software de aplicación: realizar tareas concretas por parte del usuario final.

Herramientas de internet

Correo electrónico

- Protocolo SMTP (Simple Mail Transfer Protocol): envía y recibe correos entre buzones (de servidor a servidor de correo o desde un cliente a un servidor).

- Protocolo POP3: accede y descarga los correos desde los buzones del servidor a las aplicaciones de correo. Se descarga localmente y se eliminan del servidor.
- Protocolo IMAP4: accede y descarga los correos desde los buzones del servidor a las aplicaciones de correo. Los correos no se eliminan por lo que se pueden utilizar desde diferentes máquinas.

Gestores:

- Basados en aplicación: Outlook.
- Basados en web: Gmail.

Mensajería instantánea

Una aplicación cliente solicita autenticación por parte de un usuario. Una vez conectado el sistema habilita su lista de contactos indicando quien se encuentra en línea.

- Según tipo de comunicación
  - Síncronos: usuarios deben estar conectados durante la comunicación.
  - Asíncronos: usuarios acceden al sistema de comunicación recibiendo los mensajes almacenados durante su desconexión.
- Según tipo de información transmitida
  - Texto
  - Vox
  - Video
  - Mixtos

Transferencia de ficheros – P2P

Las redes Peer to Peer o redes entre iguales actúan como cliente y servidor al mismo tiempo.

Características:

- Escalabilidad: se añaden fácilmente nodos a la red aumentando su robustez y mejorando su funcionamiento.
- Anonimato: restringe la identificación a la necesaria para gestionar la comunicación
- Descentralización:
  - Descentralizada: distribuye los recursos entre todos los nodos.
  - Centralizada: un servidor central administra el funcionamiento de la red y almacena los contenidos
  - Hibrido: nodos que actúan de servidores controlando la estructura de la red sin almacenar o distribuir contenidos.

Usos:

- Calculo en investigaciones científicas
- Implementar sistemas de ficheros distribuidos (CFS)
- Telefonía VoIP
- Transacciones de monedas virtuales
- Compartir ancho de banda y acceso a internet
- Enrutamientos anónimos para redes seguras

Computación y almacenamiento en la nube

Modelo formado por un conjunto de servicios ofrecidos sobre una red que atiende a clientes remotamente. Tecnologías que permiten acceder a los clientes a los servicios y la efectividad necesaria para cada uno bajo demanda.

Ventajas:

- Cliente no tiene que descargar aplicaciones para acceder a los servicios
- Gran flexibilidad y eficiencia de los recursos al ajustar los servicios a la demanda
- Alta disponibilidad desde cualquier localización y dispositivo
- Seguridad y protección de datos al desvincularlos de los clientes
- Reducción del coste de computación por parte de los clientes

Modelos según los servicios gestionados por los usuarios a nivel de arquitectura de computación:

- Software as a Service SaaS: modelo en el que una aplicación es alojada en un servicio para usuarios. el usuario solo puede usar las aplicaciones del proveedor. El proveedor se encarga del soporte, mantenimiento, servidores, SO, almacenamiento y configuración.
- Platform as a Service (PaaS): modelo orientado a desarrolladores de aplicaciones que alojan sus programas en la plataforma del proveedor. Entorno para desarrollar y despliega aplicaciones.
- Infraestructure as a Service (IaaS): los proveedores ofrecen la infraestructura (red, almacenamiento y servidores) a clientes para que exploten sus necesidades.

Virtualización: a partir de unos recursos e infraestructura común se ofrecen soluciones adaptadas y flexibles a diferentes clientes, servicios y necesidades.

Desventajas:

- Pérdida de control sobre los datos y los servicios
- Necesidad de disponer de acceso a internet
- Sujeto a políticas de privacidad, seguridad, actualización, escalabilidad y flexibilidad de los proveedores

Software antimalware

Aplicaciones que intentan evitar la acción de distintos tipos de amenazas. Pretenden detectar y erradicar el software malicioso.

- Phishing: suplantación de identidad con el objetivo de extraer datos valiosos del usuario para que el atacante pueda actuar en nombre de este.
- Sniffing: trata de capturar el trafico de la red para obtener información valiosa.
- DoS Denial of Service: se colapsa un sistema interrumpiendo los servicios por una gran afluencia de tráfico. Si proviene de varios puntos de conexión simultáneamente se denomina denegación de servicio distribuido.
- Hijacking: consiste en secuestrar un navegador y redirigir la navegación para obtener datos de los usuarios.

Tipos de malware:

- Virus: software que trata de alterar el funcionamiento de un sistema informático o red. Según su propagación:
    - Gusano: emplea la memoria de los equipos para propagarse a través de la red a gran velocidad.
    - Virus: ficheros ejecutable o adjuntos a ficheros que se propagan al ser copiados o ejecutados.
- Troyano: software que se hace pasar por una aplicación autentica para acceder al equipo a través de puertas traseras
- Spyware: software que recopila información sobre el usuario para enviarla a terceros.
- Adware: programa que muestra publicidad a través de ventanas emergentes, navegadores, barras de herramientas etc.
- Ransomware: programa que bloquea o restringe el acceso al sistema, datos o información exigiendo un rescate.
- Keylogger: software que registra las pulsaciones de teclado y las envía a terceros.
- Botnet: conjunto de sistemas infectados por malware que actúan de manera conjunta para realizar alguna acción malintencionada.

Clonación y copias de seguridad

Clonaciones

Permite copiar datos contenidos en particiones o discos y almacenarlos en particiones u otros medios creando una copia exacta.

Imagen: archivo o conjuntos de archivos que contienen la estructura y el contenido del origen facilitando su manejo para la posterior clonación.

Al realizar una clonación los discos implicados no pueden estar en funcionamiento. Al finalizar la clonación de un disco con sistema operativo se debe configurar el “nuevo sistema” de manera que se eviten duplicidades que puedan causar errores.

Copias de seguridad

Maneja archivos concretos facilitando su restauración individual.

Las políticas de backup determinan la frecuencia y el conjunto de archivos sobre los que se efectúan las copias de seguridad.

Tipos:

- Total: copia todos los archivos seleccionados.
- Incremental: copia solamente aquellos archivos que han cambiado desde la ultima copia de seguridad total o incremental.
- Diferencial: copia los archivos que hayan cambiado desde la ultima copia de seguridad total.