U5 Sistemas Operativos Windows

PARTE II. Usuarios, redes, recursos compartidos y seguridad

Implantación de Sistemas Operativos

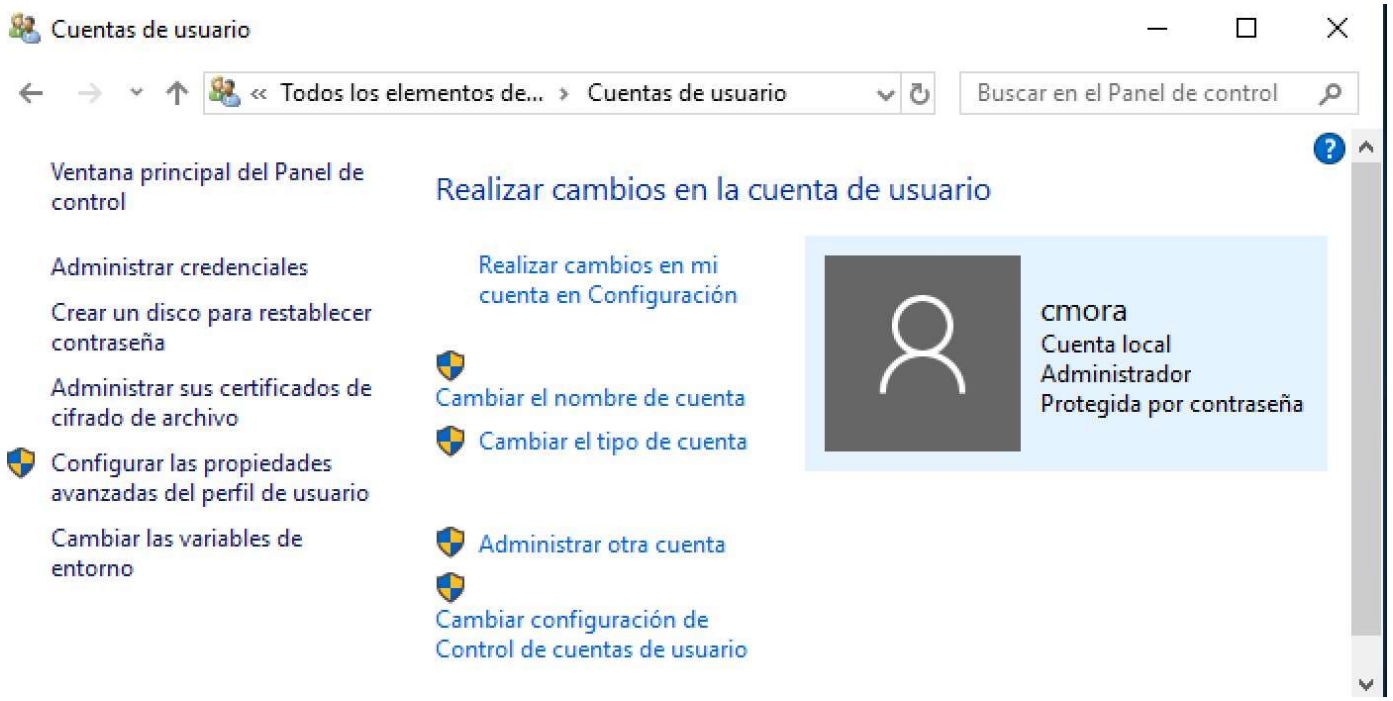
Usuarios y grupos locales

- Windows 10 admite:
  - 2 tipos básicos de cuenta: administrador y usuario estándar.
  - 2 tipos de usuario: local y de dominio

  ¿Qué es un dominio? El conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.
- Windows 10 asigna un identificador de seguridad (SID) a cada nueva cuenta de usuario.
- Si ejecutamos whoami /USER podemos ver el SID correspondiente a nuestro usuario. Por ejemplo: S-1-5-21-448539723-413027322-839522115-1003
  - La letra y primeros 3 grupos de dígitos identifican al tipo de objeto
  - Los 3 grandes números centrales identifican el dominio al que pertenece el usuario
  - Los últimos 4 dígitos identifican al usuario (suelen empezar por 1000 para usuario normal y por 500 para el Administrador)
- Ejecuta whoami /GROUPS para ver todos los grupos a los que pertenece el usuario

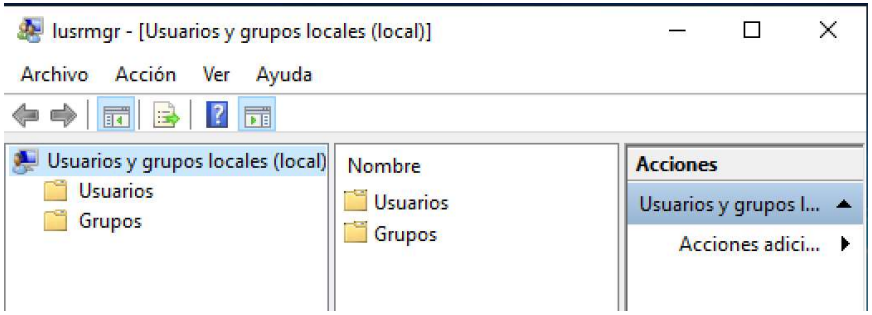
Gestionar cuentas de usuario

- Para gestionar las cuentas de usuario contamos con las opciones siguientes:
  1. El asistente para cuentas accesible desde el Panel de control

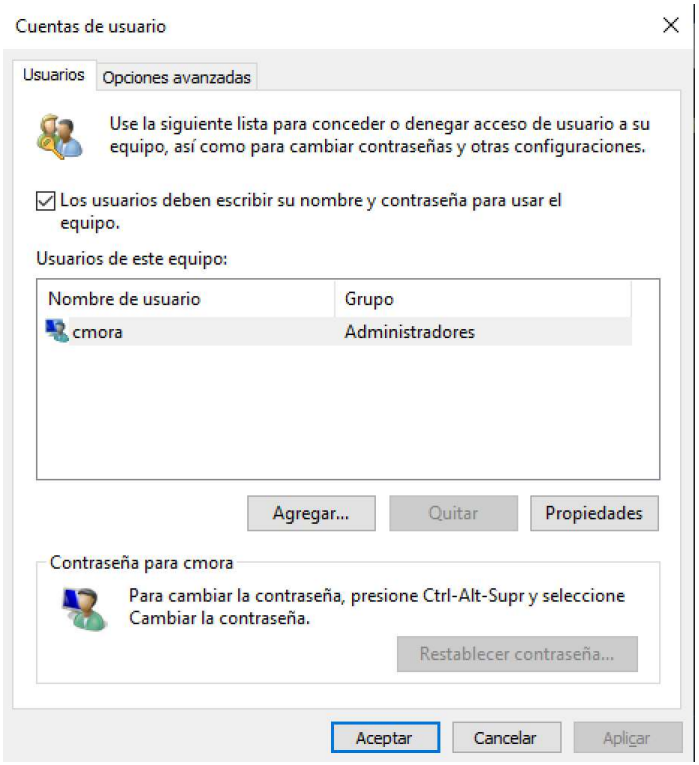


Gestionar cuentas de usuario

2. La consola específica para la gestión de usuarios mediante LUSRMGR.MSC



3. La consola especial mediante control userpasswords2 o ejecutando NETPLWIZ que permiten crear/eliminar usuarios, modificar los grupos a los que pertenecen y sus password (incluido el usuario Administrador) e incluye opciones no disponibles en la consola anterior.



Gestionar cuentas de usuario

4. El comando net user. Su sintaxis es la siguiente:

   *si deseamos que pida contraseña y [] indica que son parámetros opcionales

   - net user [nombredeusuario [contraseña | *] [opciones]] [/domain]
   - net user nombredeusuario [contraseña | *] /add [opciones] [/domain]]
   - net user [nombredeusuario [/delete] [/domain]]

- Add agrega
- Delete borra
- [/domain] realiza la acción en el controlador de dominio principal

- Ejemplos:
  - net user “usuario” /add → añade usuario
  - net user “usuario” “contraseña” /add → añade usuario con contraseña
  - net user “usuario” /delete → borra usuario

Gestionar cuentas de usuario

El comando net localgroup permite consultar los usuarios de un grupo, añadir un usuario al grupo o borrar un usuario del grupo.

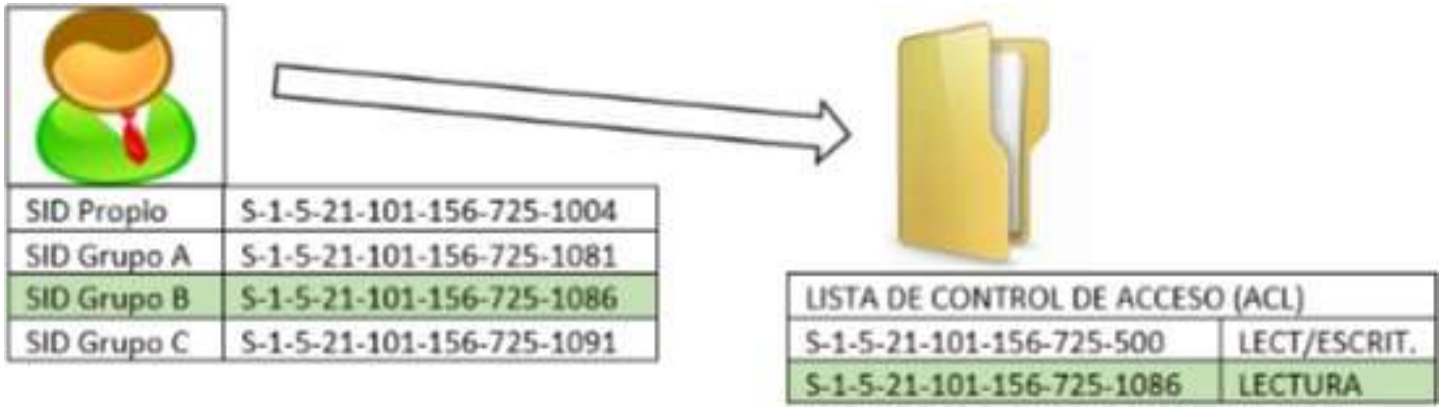
- Ejemplos:
  - net localgroup “administradores” → consulta los usuarios de un grupo, en este caso administradores.
  - net localgroup “grupo” “usuario” /add → añade un usuario al grupo
  - Net localgroup “grupo” “usuario” /delete → borra un usuario del grupo.

Usuarios y grupos locales

- Al instalar Windows 10 crea automáticamente las cuentas de usuario locales:
  - **Usuario inicial**: corresponde con la cuenta del usuario registrado que de forma predeterminada será del grupo Administradores
  - **Administrador**: deshabilitada por defecto, podemos habilitarla ejecutando en la consola la instrucción ***net user administrator /active:yes*** y ejecutamos ***control userpasswords2*** para asignarle un password o mediante la consola LUSRMGR.MSC pero no es recomendable por motivos de seguridad.
  - **DefaultAccount** (cuenta de usuario estándar empleada por el sistema)
  - **Invitado** (deshabilitada de forma predeterminada ya que permite la entrada sin un nombre y contraseñas únicos)
  - **HomeGroupUser$** se crea cuando se configura el grupo Hogar y sirve para la conexión a otros equipos de ese grupo.
  - **WDAGUtilityAccount** que se crea para Windows Defender Application Guard y está deshabilitada mientras Windows Defender no esté en uso.
- Podemos ejecutar una consola como otro usuario con ***runas /user:usuario_a_suplantar cmd***

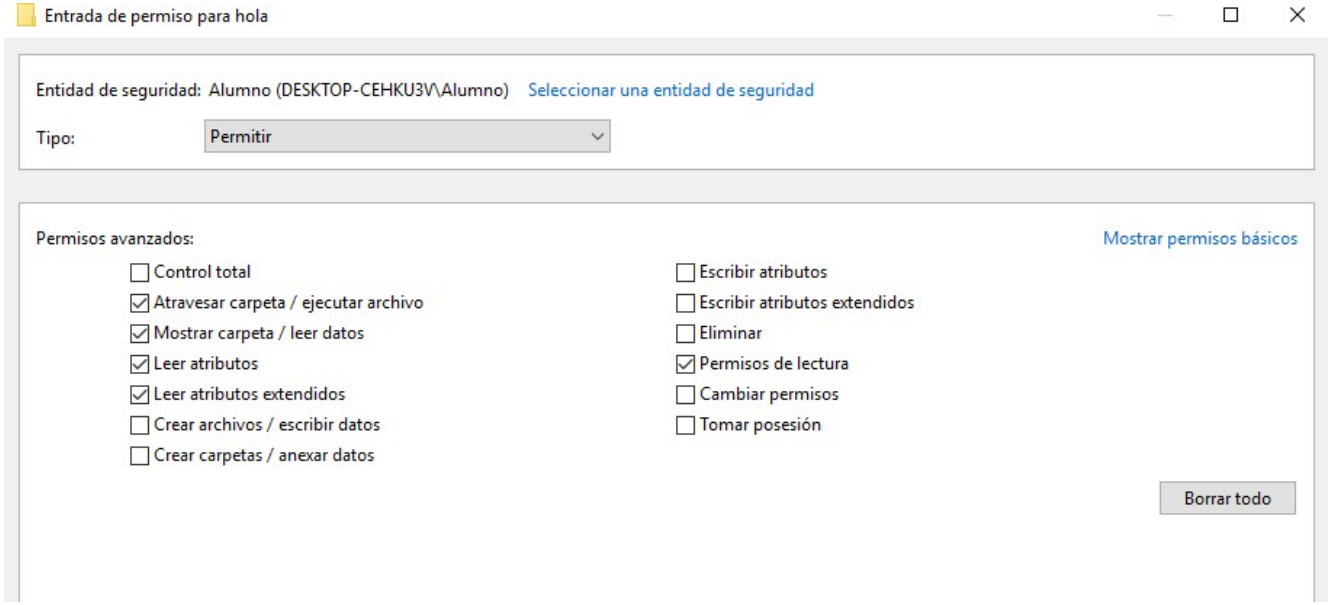
Listas de control de acceso (ACL)

- Por cada recurso del sistema (impresora, carpeta, fichero, conexión de red, etc) el sistema cuenta con una lista donde apunta los SID (usuarios o grupos) que sí tienen acceso a un recurso y qué tipo de acceso.
- También es posible una denegación implícita de permisos para un usuario o grupo.
- Si entran en contradicción 2 reglas en la ACL, tendrá más peso la denegación implícita de permisos.
- El sistema de ficheros debe ser NTFS para incorporar ACLs



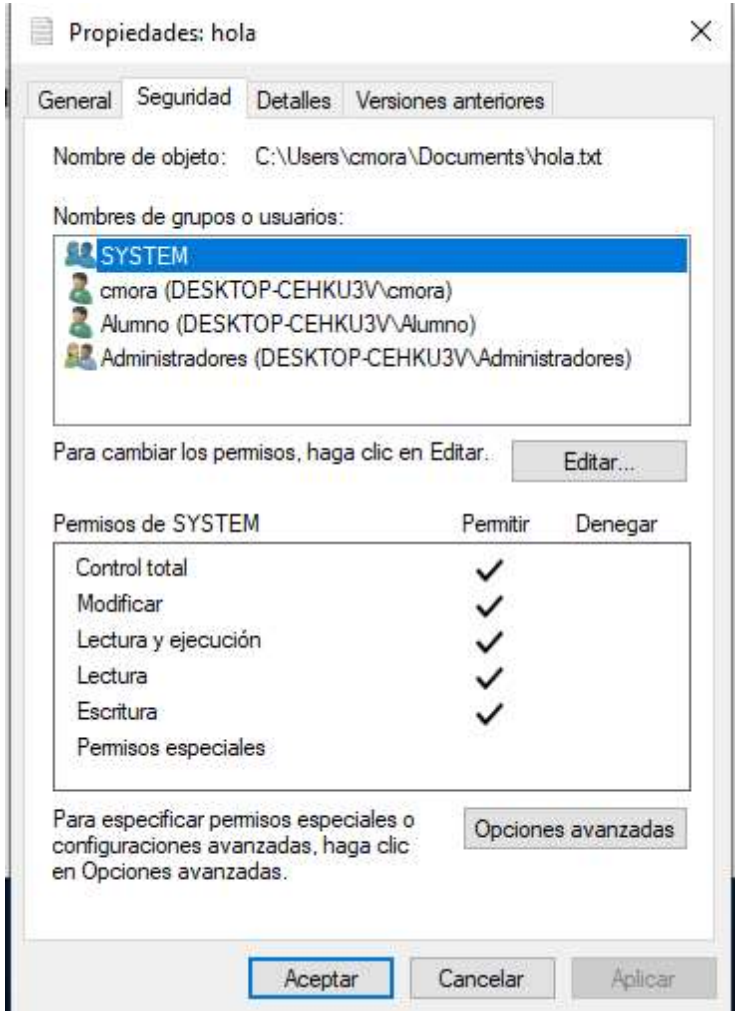
Listas de control de acceso (ACL)

- Los permisos que podemos aplicar para cada SID en la ACL no sólo son los básicos que aparecen en la lista de seguridad. Dentro de opciones avanzadas, podemos permitir o denegar la lista que se muestra (para que aparezca esta ventana hay que pulsar el botón agregar).
- Aunque deneguemos permisos a un Administrador, todos los miembros del grupo Administradores pueden tomar posesión de un recurso del sistema.



Listas de control de acceso (ACL)

- Podemos asignar las ACLs desde la pestaña de Seguridad disponible en las propiedades de los recursos.
- En el caso de ficheros y directorios, cualquier recurso que se crea, **hereda la configuración ACL** de su directorio padre.
- Si queremos que no se produzca herencia, tendremos que indicar que queremos deshabilitarla.
- Es importante **no eliminar totalmente la herencia** sino copiarla como permisos explícitos para no impedir que el sistema pueda acceder al recurso
- si deshabilitamos la herencia, **deshabilitaremos también la de los descendientes** si no indicamos lo contrario.



Listas de control de acceso (ACL)

Copia de recursos

- Si copiamos un fichero o directorio a otra unidad, aplicará los permisos correspondientes a la unidad destino.
- Si copiamos un fichero o directorio a la misma unidad, mantendrá los permisos que tenía el recurso de origen

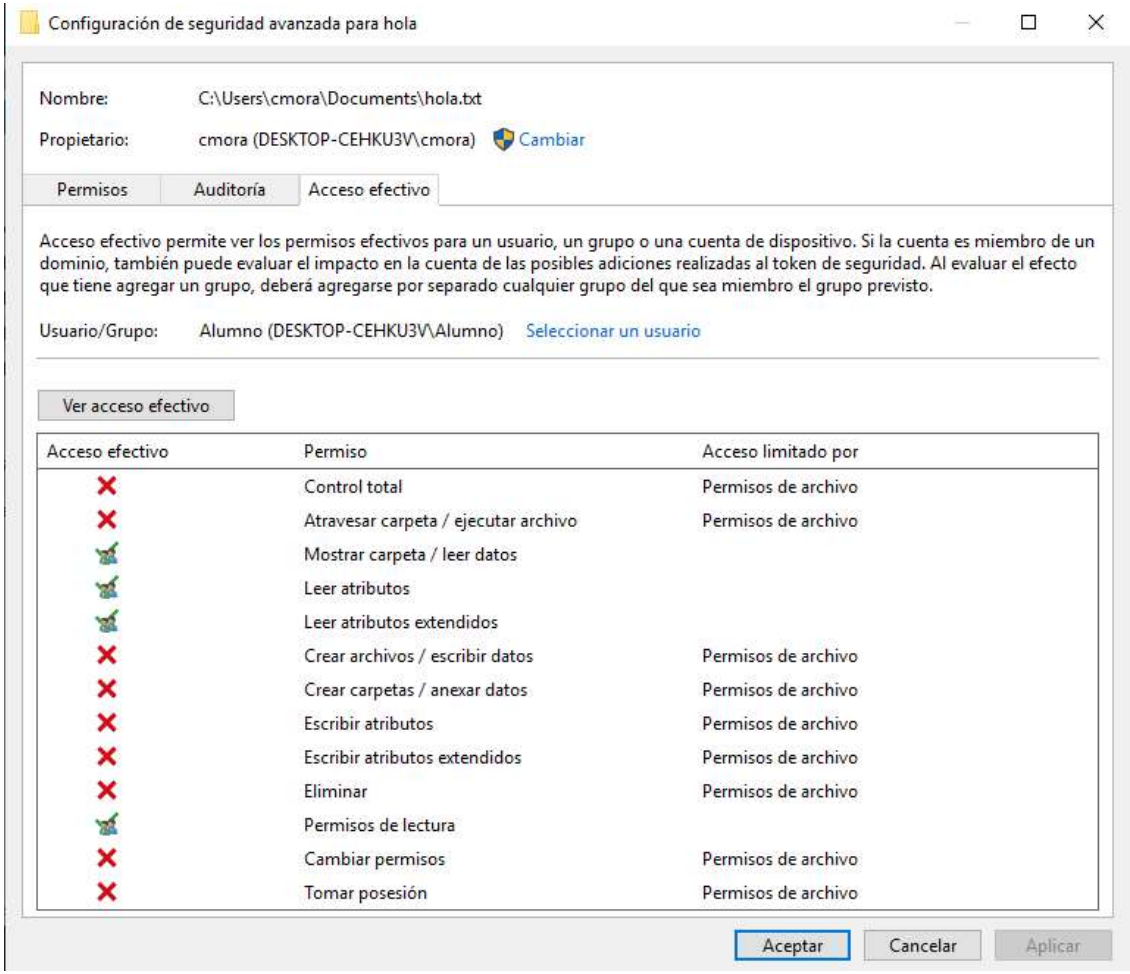
Dueño de recursos

- En Windows todo recurso tiene un propietario que normalmente es el usuario que creó dicho recurso.
- Aunque el propietario no cuente con una entrada en la ACL, podrá retocar las ACLs siempre.
- Podemos **cambiar el propietario** de un recurso dentro de las Opciones avanzadas de la pestaña Seguridad.
- El comando **dir /q** permite listar el propietario de los ficheros.

- El comando icacls permite consultar y configurar las ACLs por consola

Listas de control de acceso (ACL)

- La pestaña de acceso efectivo es especialmente útil para conocer para un SID concreto, el detalle de acceso para todos los permisos y el origen de esa limitación (herencia o permiso explícito)



Seguridad

- Las opciones de seguridad que proporciona el sistema son:
  - **Firewall de Windows**, monitoriza el tráfico de entrada y salida, permite la activación de reglas preestablecidas por perfiles y la creación de reglas a medida.
  - **Control de Cuentas de Usuario (UAC),** ayuda a impedir que el potencial malware realice cambios en los equipos
  - **Windows Defender**, es un software que protege contra virus, malware, spyware y otras amenazas.
  - Encriptación **Bitlocker**, permite cifrar particiones
  - **Windows Hello**, autenticación biométrica (huellas, escáner del rostro)
  - Cuenta con la posibilidad de crear **copias de seguridad, puntos de restauración e imágenes**
- A diferencia de sus predecesores, Windows 10 Home no permite desactivar las actualizaciones.
- Podemos cambiar las políticas de seguridad locales en la pantalla de configuración secpol.msc. Por ejemplo, podemos fijar directrices aplicables a las contraseñas de los usuarios.

Seguridad

Puntos de restauración

- Los **puntos de restauración** son copias de seguridad que el sistema operativo hace cuando detecta algún cambio en el sistema, al instalar programas nuevos, al desinstalarlos, etc.
- Podemos forzar la creación de puntos de restauración dentro de Panel de control > Recuperación.
  - En primer lugar tendremos que Activar la protección del sistema
  - Una vez activada, creamos un puntos de restauración
- La restauración se realiza en la misma ventana descrita anteriormente seleccionando en Recuperar el nombre de un punto de restauración.
- Esta restauración sólo almacena y vuelca la configuración misma del sistema. No afecta a los datos almacenados en el sistema

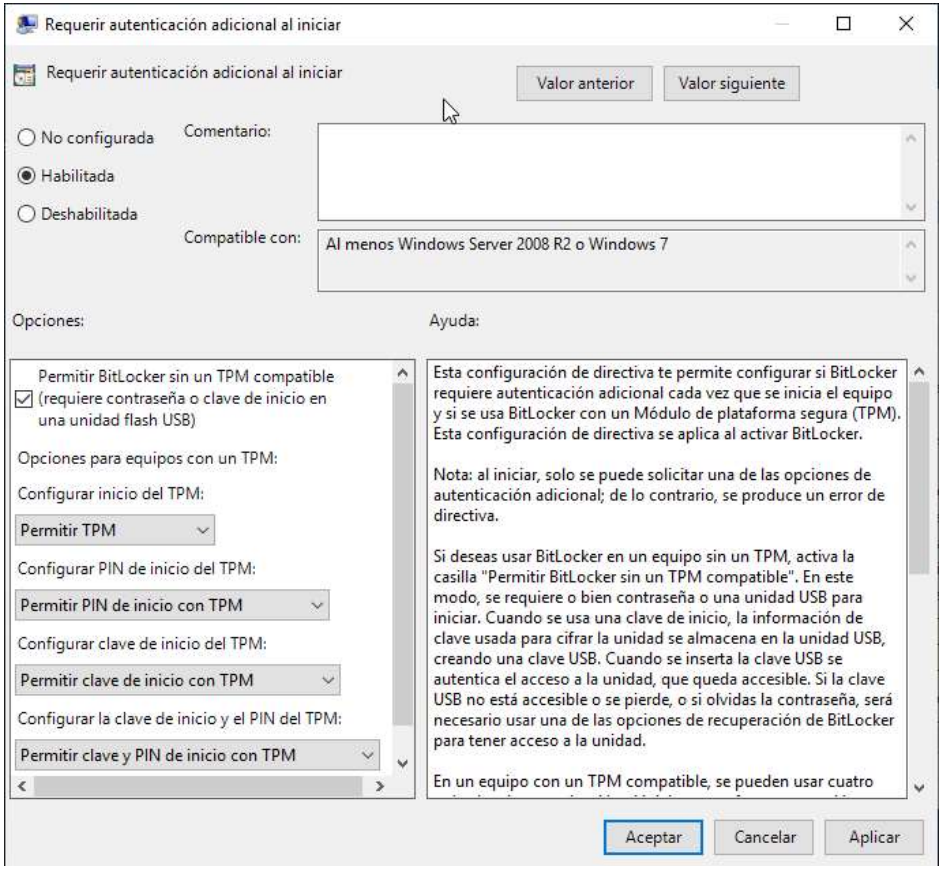
Seguridad

BitLocker

- **Bitlocker** necesita de un Módulo de plataforma fiable o TPM. Se trata de un chip que crea y guarda las claves de cifrado con medidas de seguridad mucho más restrictivas que el almacenaje de información de cualquier otra área de memoria.
- Al no disponer de TPM, podremos configurar el acceso al contenido, una vez cifrado, mediante una **contraseña**, o a través de una **smart card** que necesitaremos tener conectada cada vez que arranquemos el **ordenador**.
- La opción de activación de BitLocker está disponible directamente en el menú contextual de las unidades del sistema.
- Si ciframos una unidad de Windows que no contiene el sistema, el cifrado se ejecutará en segundo plano. Si en cambio es la del sistema, será necesario el reinicio antes de que empiece el cifrado.

Seguridad

- Si nuestro equipo no cuenta con el TPM podemos usar BitLocker modificando la directiva relacionada. Para ello:
  - Accedemos a las políticas de grupo del sistema con gpedit.msc.
  - A continuación, nos situamos en la ruta "Directiva equipo local / Configuración del equipo / Plantillas administrativas / Componentes de Windows / Cifrado de unidad BitLocker / Unidades del sistema operativo" y hacemos doble click en "Requerir autenticación adicional al iniciar". Tenemos que habilitar esta opción y dejar marcado el check "Permitir BitLocker sin un TPM compatible".

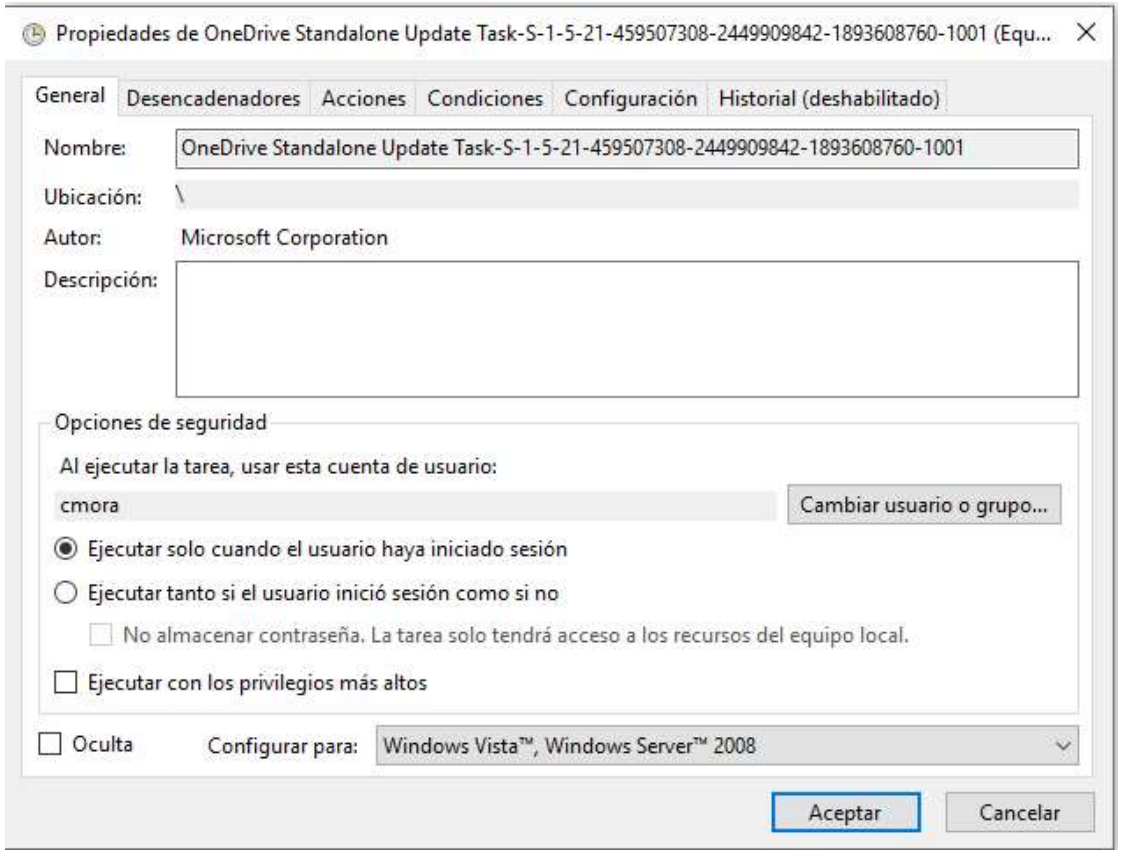


Seguridad

- El sistema operativo cuenta con utilidades para realizar **imágenes** de discos y **copias de seguridad** en Panel de control > Copias de seguridad y restauración
  - Las **imágenes del disco** se pueden crear con la opción de incluir los ficheros necesarios para crear un disco de reparación del sistema que evita el uso del disco de instalación para una futura restauración
  - Las **copias de seguridad**, pueden programarse y realizarse localmente o en red.

Programación de tareas

- Como hemos visto en las copias de seguridad, existe la opción de la programación de tareas también en Windows.
- El acceso a su configuración está en Panel de control > Herr. Administrativas > Programador de tareas o bien empleando taskschd.msc



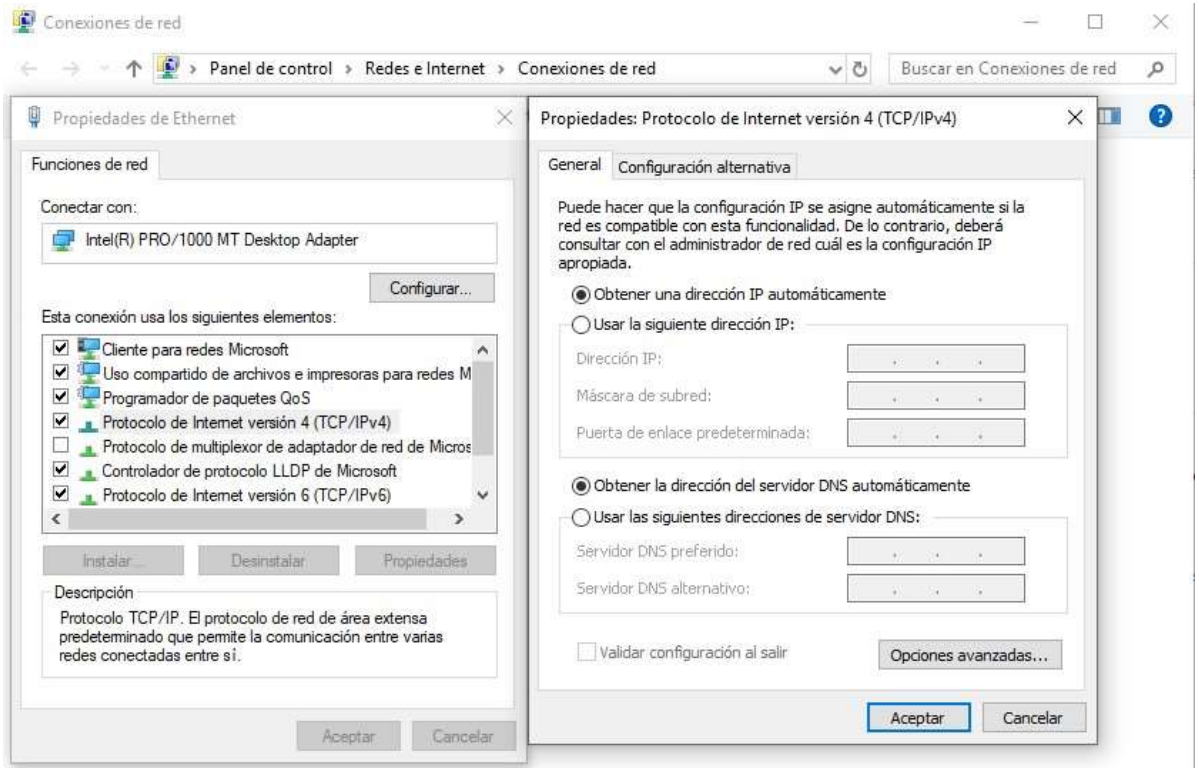
Redes

- Hay 2 tipos de redes Microsoft:
  - Redes **basadas en dominio**: son redes basadas en un esquema jerarquizado en el que los servidores Active Directory (controladores de dominio) mantienen la información de las cuentas de usuario en una BBDD centralizada.
  - Redes **basadas en grupo de trabajo**: son redes basadas de igual a igual. La seguridad es mucho más difícil de mantener y administrar.
    - Permite la compartición de recursos (impresoras y archivos) de manera que la instalación de un recurso por parte de un miembro del grupo proporciona dicho recurso al resto.
    - Más información: https://www.xataka.com/basics/como-crear-red-local-windows-10-utilizar-grupo-hogar

- Las redes basadas en **grupo Hogar** eran un tipo particular de redes basadas en grupo de trabajo pero esta opción **desaparece** a partir de la versión 1803 de Windows 10 (principios de 2018)**.**

Redes

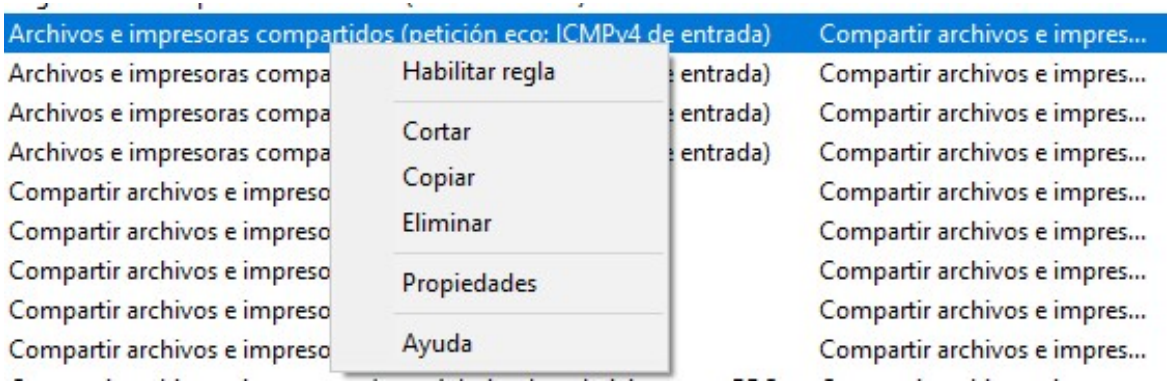
Desde Panel de control > Redes e Internet > Conexiones de red podemos configurar el interfaz de red.



- Hay un conjunto de comandos de redes que pueden ser útiles
  - ipconfig: permite configurar el interfaz de red.
  - ping: realiza peticiones de eco
  - Tracert: permite seguir la pista de paquetes que vienen desde un host
  - nslookup: consulta la resolución de nombres del servidor DNS

Redes

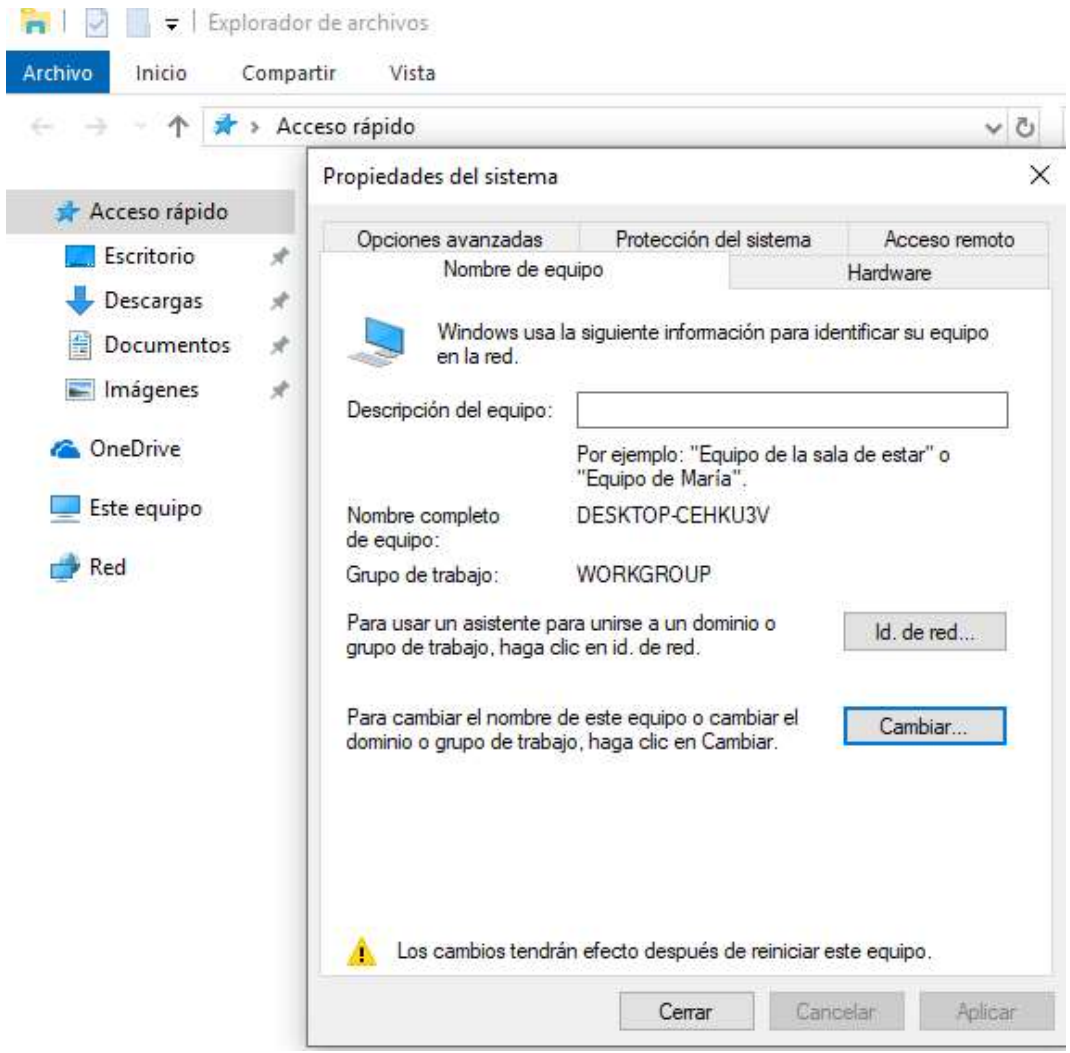
- Es posible que el Firewall impida la ejecución de la instrucción del ping. Para habilitar la repuesta a los ecos en el cortafuego, debemos seguir estos pasos:
  - Abrimos en el Panel de control el Firewall de Windows y escogemos la Configuración avanzada
  - Seleccionamos en las reglas la entrada la entrada relativa al protocolo ICMP. Concretamente, escogemos la regla que pone "**Archivos e impresoras compartidos (petición eco ICMPv4 de entrada)**", y si utilizamos IPv6, pues deberemos activar la regla correspondiente. Escogemos habilitar regla.



  - Comprobamos que podemos hacer ping

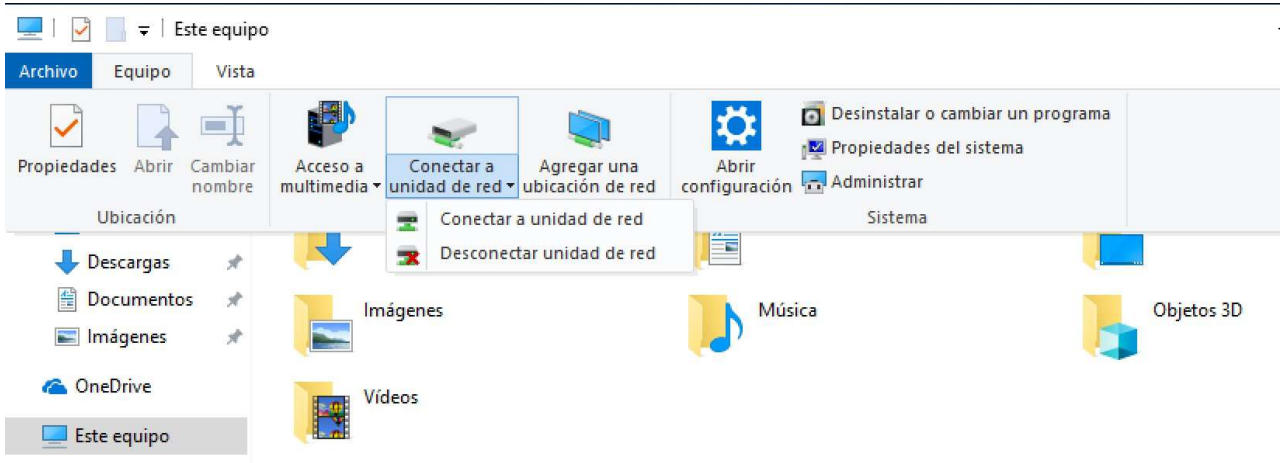
Redes

- Una vez que sabemos que el interfaz está correctamente conectado, podemos cambiar el nombre del equipo o el grupo de trabajo al que pertenece.
- Para ello, consultamos las propiedades de este equipo desde el explorador de archivos y tenemos acceso a esta opción



Recursos compartidos

- Podemos montar recursos compartidos de la red como unidades de volumen en nuestro equipo. Esto lo podemos hacer bien utilizando el comando NET USE o bien desde el explorador de archivos.



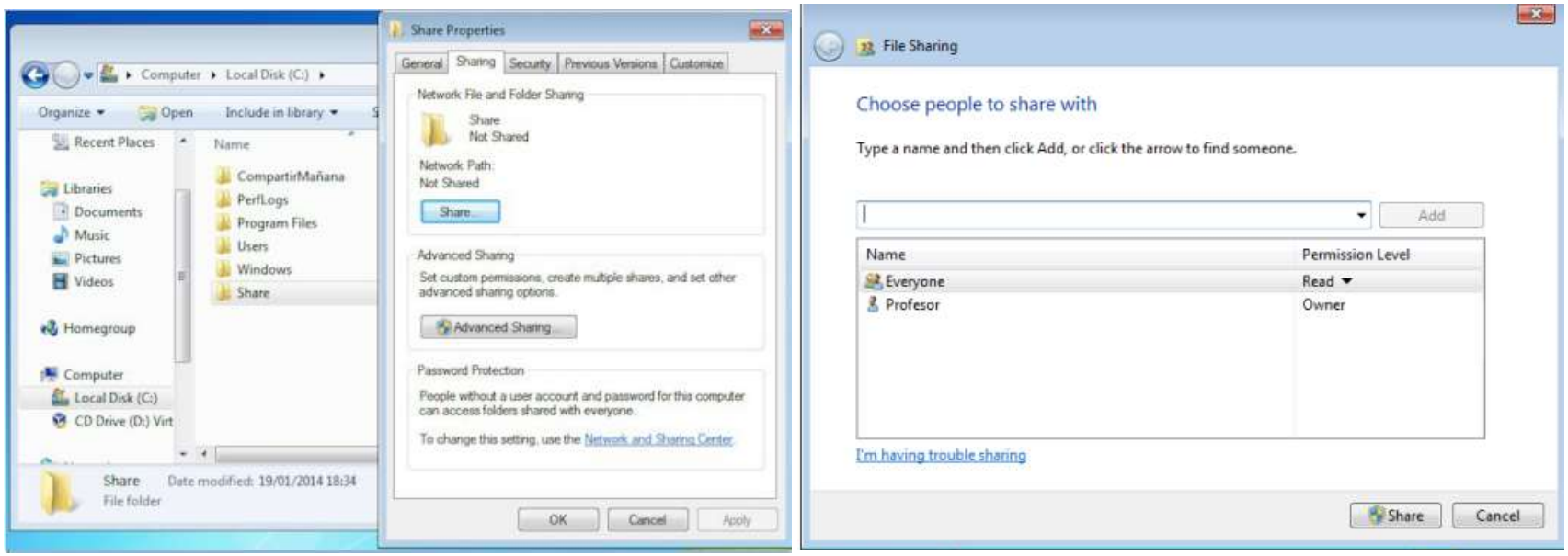
- Así, si por ejemplo queremos que el recurso compartido \\192.168.102.46\Almacen esté montado en nuestra máquina como el volumen X: de manera persistente, la orden sería:

  Net use x: \\192.168.102.46\Almacen /PERSISTENT:YES

Recursos compartidos

Compartir carpetas en Windows.

- Si queremos compartir una carpeta, debemos pulsar con el botón derecho del ratón sobre la carpeta → Propiedades. Entonces seleccionaremos la pestaña de compartir. En ésta tendremos disponibles las opciones de compartir. En las opciones avanzadas tendremos disponibles los permisos sobre usuarios y grupos.



Recursos compartidos

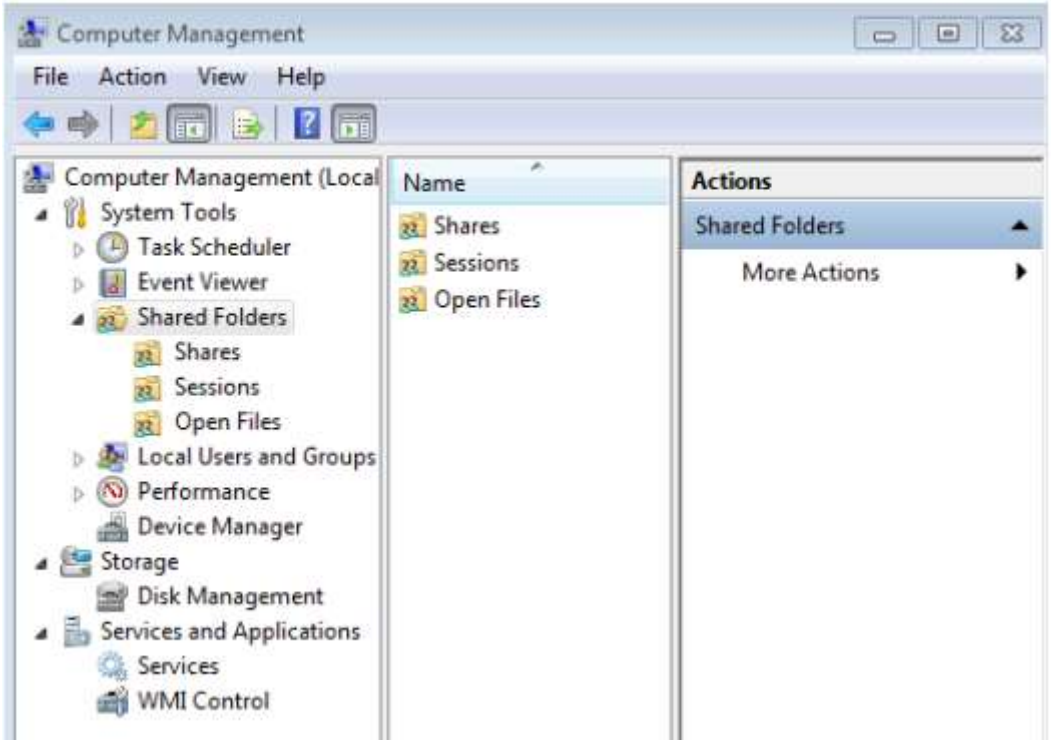
Acceder a la carpeta compartida.

- Podemos acceder a la carpeta compartida a través de la ruta UNC (Universal Naming Convention) \\Nombre_NetBios o \\Server_IP. Dependido de la configuración del servidor se podrá mostrar una ventana de autentificación. Una vez que tengamos acceso veremos una pantalla como la de la imagen siguiente y en ellas podremos explorar la carpeta compartida.
- También podremos añadir una unidad de red para no tener que establecer el UNC cada vez que quedamos acceder a la carpeta compartida.

Recursos compartidos

Gestión de los recursos compartidos.

- Podemos acceder a la información sobre las carpetas compartidas a través de diferentes herramientas.
  - Administración de equipos (Panel de control → Herramientas administrativas → Administración de equipos)



Recursos compartidos

Gestión de los recursos compartidos.

- Centro de redes y recursos compartidos en el panel de control.