Configuración de sistemas Windows

Contenido

Gestión de usuarios 1
Usuarios 1
El administrador de usuarios 2
Directivas de seguridad local 7
Permisos 9

Gestión de usuarios

Las cuentas de usuario son una parte muy importante de la estructura de la seguridad de Windows ya que controlan el acceso a uno o varios ordenadores. Son la clave para conceder a los usuarios autorizados el acceso a los componentes dentro del entorno de Windows. Si se implantan correctamente, las cuentas proporcionan una forma cómoda y segura para permitir que los usuarios accedan a los recursos del sistema o de la red.

La administración de usuarios se realiza de dos formas diferentes dependiendo si el servidor es o no es un controlador de dominio:

- **El administrador de usuarios.** Administra la seguridad de las estaciones de trabajo y servidores miembro o servidores autónomos (no controladores del dominio).
- **El administrador de usuarios y equipos del Directorio Activo.** Administra la seguridad en el controlador principal o de reserva del dominio (controlador de dominio).

Las características de seguridad proporcionadas por el administrador de usuarios consisten en la creación de cuentas de usuarios y de grupo, la asignación de derechos de usuario y el establecimiento de relaciones de confianza entre diferentes dominios.

- Usuarios
- El administrador de usuarios
- Directivas de seguridad local

Usuarios

Una cuenta de usuario contiene toda la información que define a ese usuario en particular dentro del entorno de Windows. Todo lo que se necesita es asociarle un identificador de seguridad de usuario (SID). La seguridad de las cuentas de usuario puede incluir un nombre único de usuario, una contraseña y los permisos que el usuario tiene para utilizar el sistema y acceder a los recursos. Cada usuario del sistema posee una cuenta de usuario y una contraseña asociada para su uso individual.

Las cuentas de usuario pueden definirse en una máquina local o en el dominio. Las cuentas definidas en la máquina local sólo pueden utilizarse en esa máquina, mientras que las cuentas definidas en el dominio

pueden utilizarse en cualquier máquina que pertenezca a ese dominio o en algún dominio de confianza. Por defecto, Windows 2008 proporciona dos cuentas de usuario predefinidas:

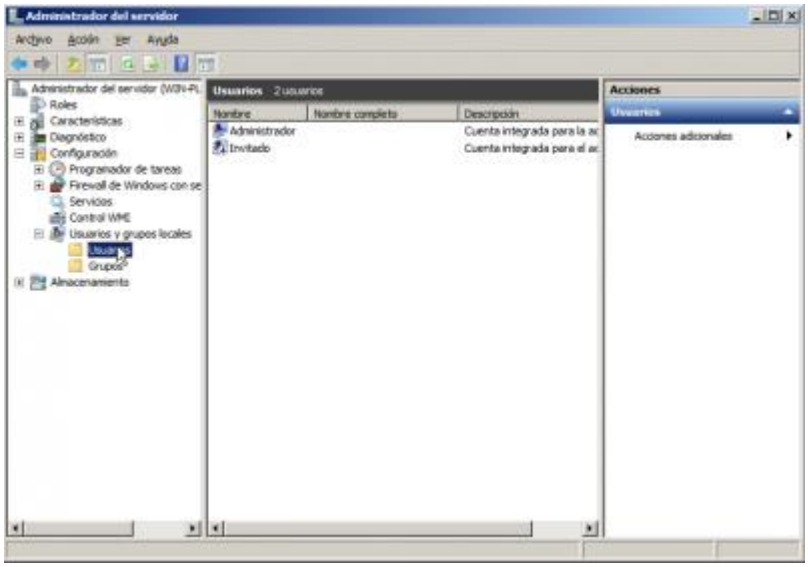
- **Administrador.** La cuenta administrador posee control total sobre las operaciones y la seguridad del sistema completo. Cualquiera que pueda iniciar una sesión como administrador posee control total sobre el sistema. Esto es un punto muy importante debido a que la cuenta Administrador y sus equivalentes deben ser totalmente de confianza.

La cuenta Administrador está pensada para el individuo que administra la configuración del sistema. Un mal uso de la cuenta puede ser desastroso debido a los derechos y permisos asociados.

- **Invitado.** Está pensada para los usuarios que se conecten muy ocasionalmente al sistema. Sin embargo, se recomienda que nunca se use la cuenta Invitado, sino que se creen cuentas temporales que proporcionen unos controles de responsabilidad y auditoria mejores. Por defecto, la cuenta está desactivada y configurada como miembro del grupo local Invitados. Posee una contraseña vacía y no se puede cambiar su perfil por el perfil de usuario predeterminado.

El administrador de usuarios

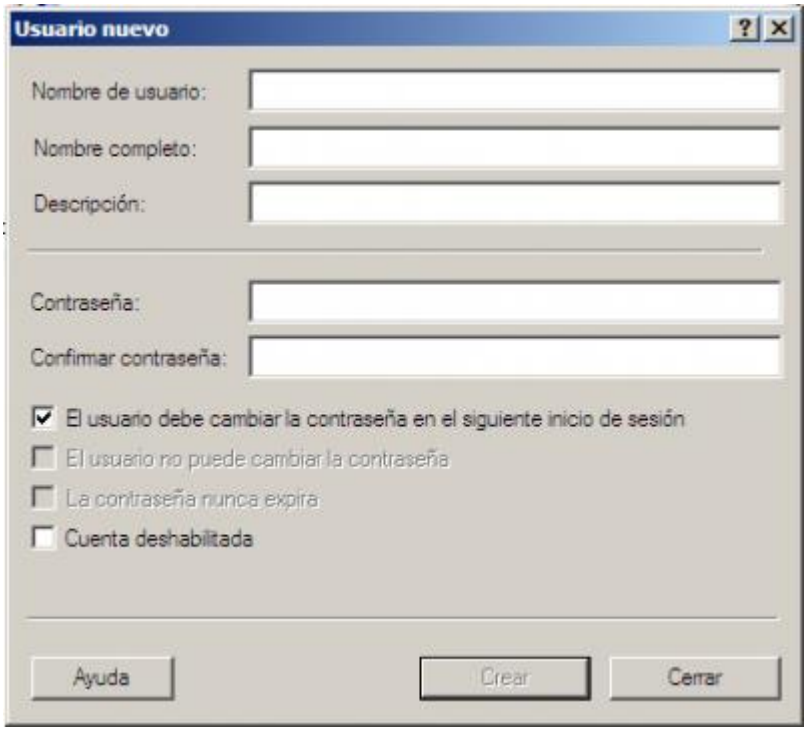
El administrador de usuarios permite gestionar de una manera fácil los usuarios y los grupos de usuarios del sistema. Para utilizar el administrador de usuarios en el menú de inicio pulse el botón derecho del ratón sobre *Equipo*, seleccione *Administrar* y luego *Usuarios y grupos locales* que se encuentra en la categoría *Configuración del Administrador del servidor* (véase la figura 2-1). Otra forma de acceder a la administración de usuarios y grupos locales es a través de la herramienta *Administración de equipos*, dentro de la categoría *Herramientas del sistema.*



- **Crear una cuenta de usuario**

Para crear una nueva cuenta de usuario hay que hacer los siguientes pasos:

- Seleccione el menú *Usuarios* de la barra de menús (en *Usuarios y grupos locales*) y dentro de este menú seleccione la opción *Usuario nuevo...* haciendo clic con el botón derecho.
- En la ventana que aparece (véase la figura 2-2) debe indicar los datos de la nueva cuenta de usuario, siendo el único campo obligatorio el referente al nombre de usuario. El resto de los campos que aparecen son: *nombre de usuario, nombre completo, descripción, contraseña y confirmar contraseña.*



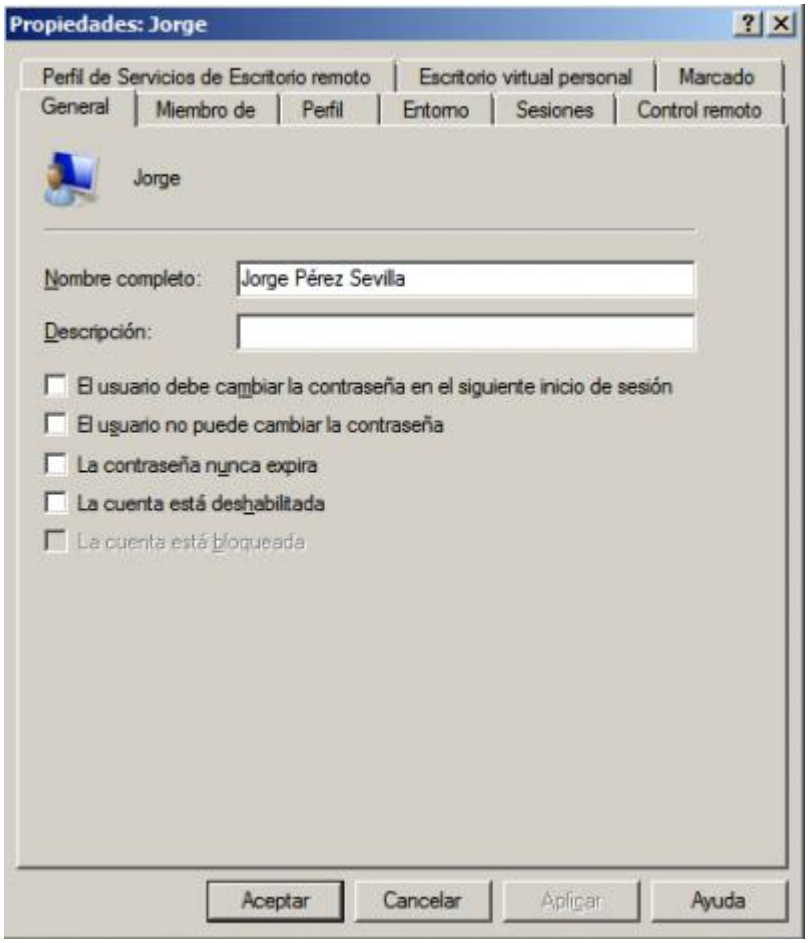
Dar de alta un usuario

Además de estos campos, el cuadro de diálogo Usuario nuevo contiene una serie de casillas de verificación referentes a la contraseña y a la disponibilidad de la cuenta. Estas casillas y su significado son las siguientes: *El usuario debe cambiar la contraseña en el siguiente inicio de sesión, El usuario no puede cambiar la contraseña, La contraseña nunca caduca y Cuenta deshabilitada.*

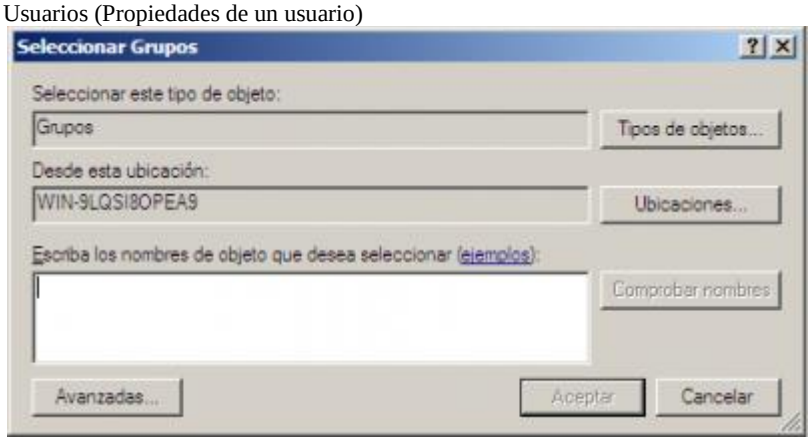
- **Propiedades de un usuario**

Para ver las propiedades de un usuario pulse dos veces sobre el usuario y aparecerá la ventana *Propiedades* (véase la figura 2-3). El número de pestañas que aparece en la ventana *Propiedades* varía dependiendo de los servicios instalados en el sistema. A continuación se van a ver las pestañas más utilizadas:

- La pestaña *General* muestra la información suministrada a la hora de crear un nuevo usuario.
- En la pestaña *Miembro de* aparece el listado de grupos al que pertenece el usuario. Para modificar los grupos a los que pertenece un usuario utilice los botones *Agregar o Quitar*. Si pulsa *Agregar* aparece un cuadro de diálogo (véase la figura 2-4) que permite escribir los nombres de los grupos a los que pertenece. Si no se acuerda de los nombres de los grupos puede verlos pulsando el botón *Avanzadas*.

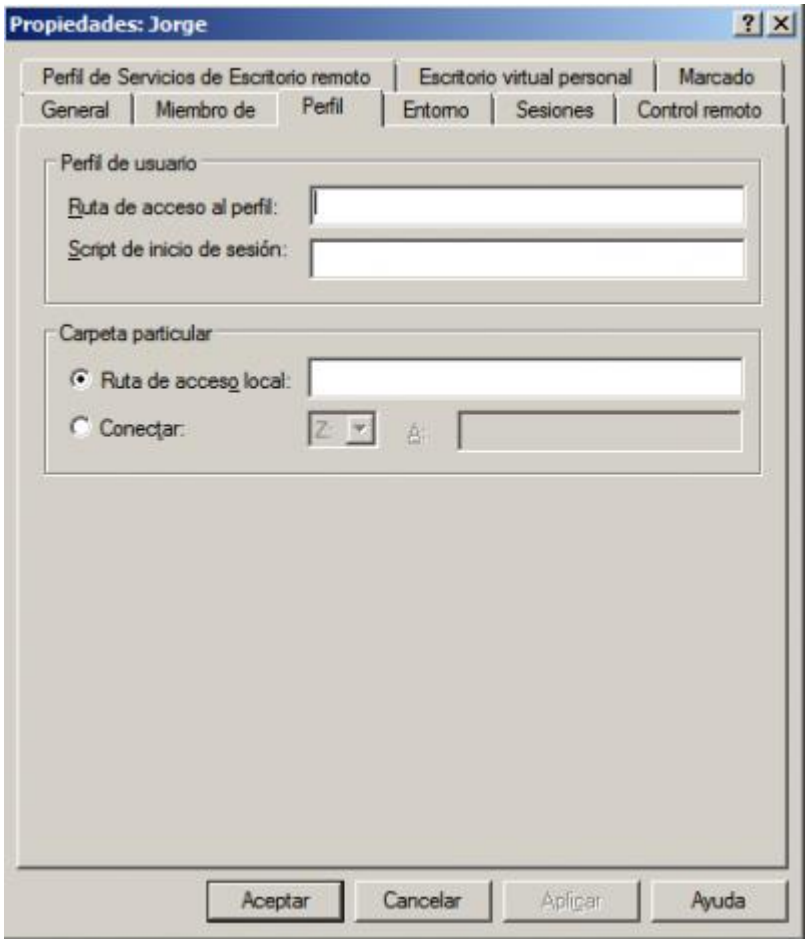


Usuarios (Propiedades de un usuario)



Gestión de grupos

- En la pestaña *Perfil* (véase la figura 2-5) puede establecer el perfil y el directorio particular de un usuario.



Pestaña “Perfil” de la carpeta “Propiedades de usuario”

A la hora de definir la *Carpeta particular* para un usuario, el administrador debe tener en cuenta si la ubicación del directorio es local o no. Si es local, entonces el directorio es visible cuando el usuario se conecte desde la máquina en la que se ha definido, mientras que si utiliza un directorio de red, éste es visible independientemente de dónde se establezca la conexión.

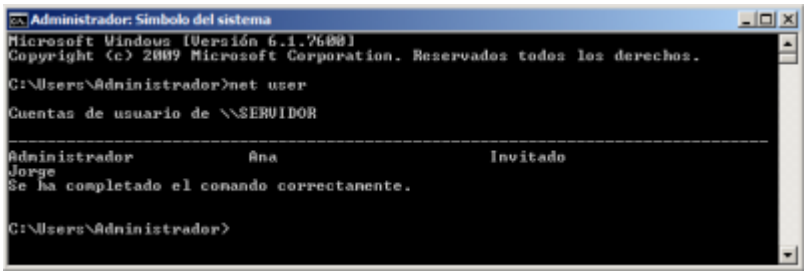
Para definir estos directorios, basta con escribir el camino completo junto con el nombre de éste en el cuadro de texto apropiado, que será el cuadro titulado *Ruta de acceso local.* En el caso de tratarse de un directorio compartido debe seleccionarse la opción Conectar a; además, debe indicar la letra de la unidad en la que quiere asignar el directorio y en el cuadro de texto escribir la dirección (*Nombre_máquina**nombre_recurso_compatido*\).

- **Comandos**

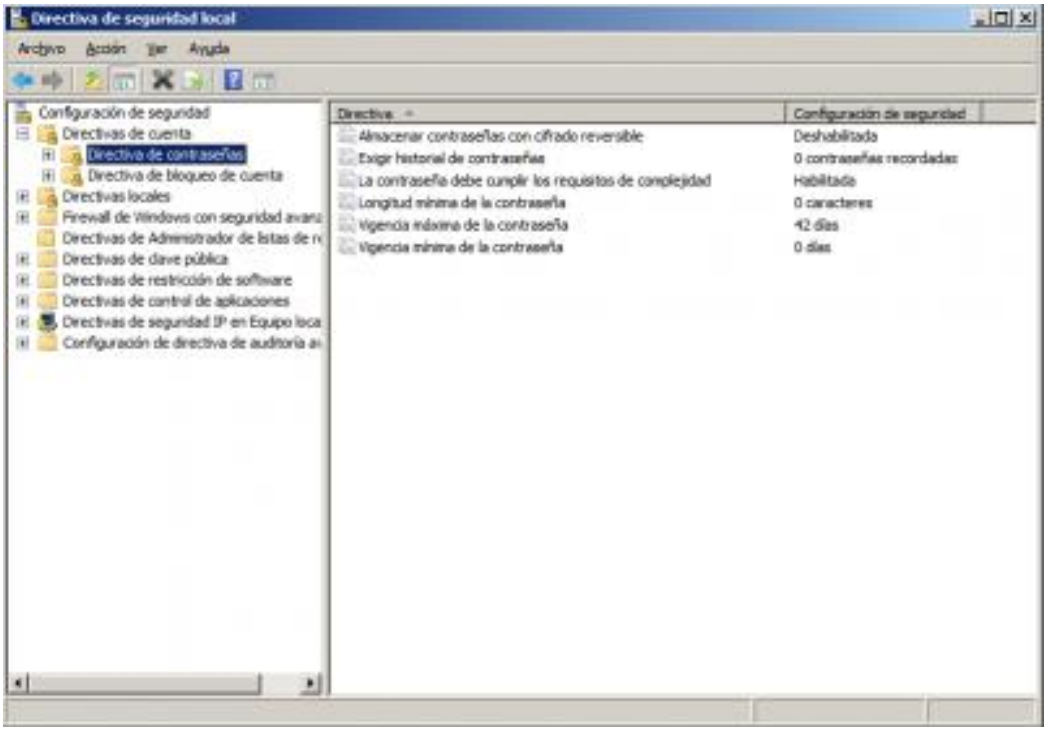
Aunque lo normal es utilizar el entorno gráfico, también puede administrar los usuarios del sistema utilizando el Símbolo del sistema. En la tabla 2-1 se muestran los comandos más utilizados.

Tabla 2-1. Comandos para la administración de usuarios

Comando	Ejemplo	Descripción
net user	net user	Muestra los usuarios del sistema (véase la figura 2-6).
net user <login> <pass> /add	net user encarni hola00== /add	Añade un usuario con una determinada contraseña.
net user <login> <pass>	net user encarni hola00==	Cambia la contraseña del usuario.
net user <login> /del	net user encarni /del	Borra un usuario.
net localgroup <grupo> <usuario> /add	net localgroup Administradores encarni /add	Añade un usuario dentro del grupo
net view	net view	Mostrará los equipos de la red
net view	net view\\puesto1	Muestra los recursos compartidos para el pc puesto1



Net user



Directivas de seguridad local

Uno de los puntos más importantes de un sistema es la fortaleza de las contraseñas de los usuarios. Si un usuario que tiene muchos privilegios utiliza como contraseña “hola”, entonces el sistema corre un grave peligro. Quizá la organización tenga una seguridad casi perfecta, pero una contraseña débil puede suponer revelar los secretos de la organización, su uso para iniciar un ataque por denegación de servicio o incluso sabotear la red. Salvo que se utilicen métodos de autentificación de varios factores para todos los usuarios en la red (p.ej., huella dactilar, tarjeta), debe implementar las opciones de seguridad de contraseña.

Dentro de *Inicio, Herramientas administrativas* puede ejecutar la herramienta *Directivas de seguridad local* para establecer los requisitos que deben cumplir las contraseñas de los usuarios (véase la figura 2-7).

Existen tres tipos de directivas de cuentas: las directivas de contraseñas, las directivas de bloqueo de cuentas, y las directivas Kerberos. Las directivas de contraseña permiten indicar cómo es la contraseña de los usuarios. Las directivas de contraseña que puede establecer son las siguientes:

- **Forzar el historial de las contraseñas.** Permite obligar a los usuarios a que no repitan las últimas contraseñas utilizadas anteriormente.
- **Vigencia máxima y mínima de la contraseña.** Permite establecer el tiempo máximo de la contraseña (vigencia máxima) y el tiempo mínimo que debe tener el usuario la contraseña (vigencia mínima). Al finalizar el período de vigencia de la contraseña el sistema le obliga al usuario a que cambie su contraseña.
- **Longitud mínima de la contraseña.** Determina el número mínimo de caracteres que un usuario debe utilizar en su contraseña. Cuanto más larga sea la contraseña, más difícil será comprometerla. No obstante, uno de los efectos colaterales de exigir contraseñas largas es que los usuarios utilizan contraseñas fáciles de averiguar o que las escriban en algún lugar.
- **Las contraseñas deben cumplir los requerimientos de complejidad.** Si activa esta opción se exige que todas las contraseñas tengan, al menos, seis caracteres de longitud y que incluyan caracteres de tres de estas cuatro categorías: letras mayúsculas, letras minúsculas, números o símbolos.

Además, la contraseña no puede contener ni el nombre de cuenta del usuario ni parte del nombre completo del usuario en más de dos caracteres consecutivos. También puede utilizar otros caracteres en las contraseñas como ½ (Alt+233). Además, si la organización tiene sus propios requisitos de seguridad de las contraseñas, podrá crear un filtro de contraseñas personalizado e instalarlo en cada controlador del dominio. El fichero que proporciona el filtro integrado es passfilt.dll.

- **Almacenar contraseñas usando cifrado reversible para todos los usuarios del dominio.** Activar esta opción debilita significativamente la seguridad de las contraseñas y sólo se debe hacerlo si es totalmente necesario.

Tabla 2-2. Configuración predeterminada de directiva de contraseña

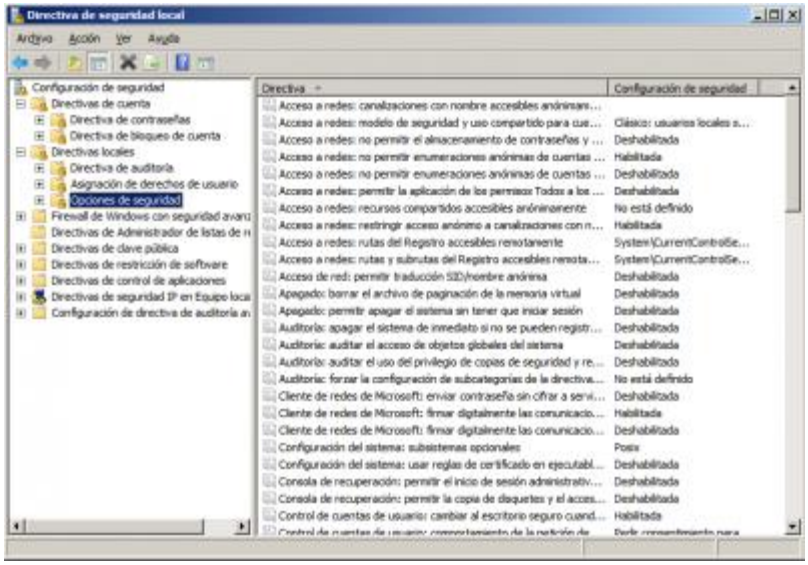
Configuración	Valor predeterminado	Intervalo
Exigir historial de contraseñas.	Se recuerdan 24 contraseñas en controladores de dominio, 0 en servidores independientes.	0 a 24.
Vigencia máxima de la contraseña.	42 días.	0 a 998.
Vigencia mínima de la contraseña.	1 día en controladores de dominio, 0 en servidores independientes.	0 a 998.
Longitud mínima de la contraseña.	7 caracteres en controladores de dominio, 0 en servidores independientes.	0 a 14.
Las contraseñas deben cumplir los requerimientos de complejidad.	Habilitado en controladores de dominio, deshabilitado en servidores independientes.	Habilitado o deshabilitado.
Almacenar contraseñas haciendo uso de cifrado reversible para todos los usuarios del dominio.	Deshabilitado	Habilitado o deshabilitado.

También puede definir directivas de bloqueo de cuentas para todo el dominio o para cuentas locales en equipos individuales mediante las directivas de seguridad. En la tabla 2-3 puede ver la configuración predeterminada de bloqueo de cuentas.

Tabla 2-3. Configuración predeterminada de bloqueo de cuenta

Configuración	Valor predeterminado	Intervalo
Duración del bloqueo de cuenta.	No se puede aplicar.	1 – 99.999 minutos (un valor de 0 nunca reestablecerá el número de intentos erróneos realizados en un determinado intento de inicio de sesión).
Umbral de bloqueo de cuenta.	0 intentos de inicio de sesión incorrectos (deshabilitado).	0 a 999 intentos.
Reestablecer el bloqueo de cuenta después de..	No se puede aplicar.	1 – 99.999 minutos (un valor de 0 necesitará que un administrador desbloquee la cuenta).

Las directivas locales del equipo permiten indicar qué se puede hacer en el equipo y quién lo puede hacer. Por ejemplo, con las directivas locales puede establecer quién puede apagar el ordenador, quién puede utilizar la unidad CD-ROM, etc..



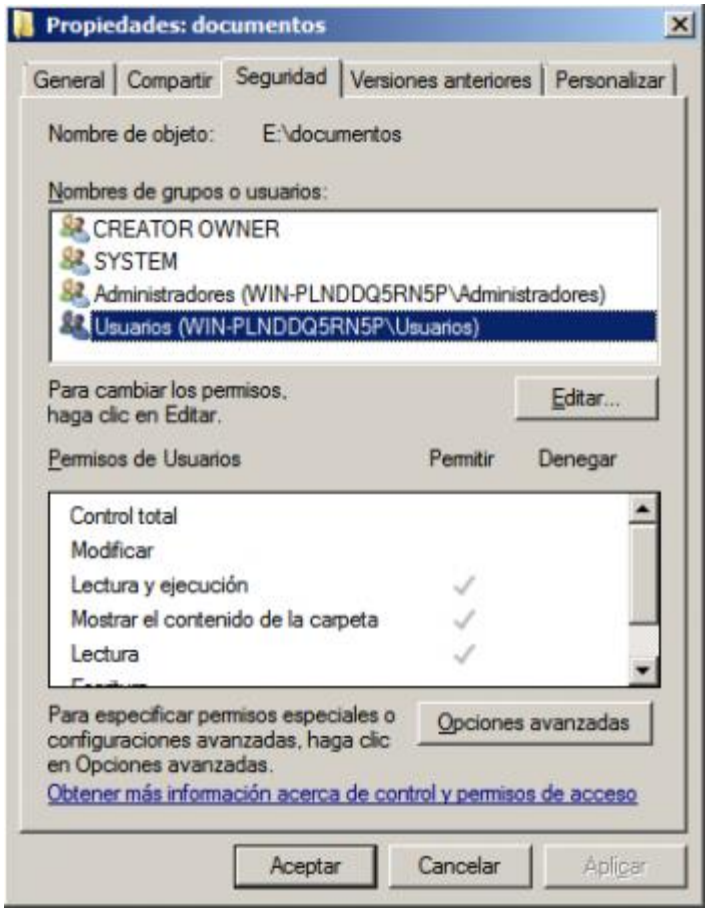
Directivas locales

Permisos

Los sistemas Windows ofrecen una gran libertad para establecer los permisos de acceso a un sistema de ficheros o carpetas ya que permiten establecer los permisos para cualquier usuario o grupo de usuarios.

Los permisos que se pueden establecer para un usuario o grupo son: *Control total*, *Modificar*, *Lectura y ejecución*, *Mostrar el contenido de la carpeta*, *Lectura*, *Escritura y Permisos especiales.* Lo mejor es clasificar los permisos en dos grupos: *Lectura y Escritura.* Los permisos de lectura son *Lectura y ejecución, Mostrar el contenido de la carpeta y Lectura.* Y los permisos de escritura son todos aquéllos que implican poder cambiar el contenido de la carpeta o archivo. Si desea permitir en un recurso la escritura lo mejor es activar el permiso *Control total.*

Para ver los permisos de acceso a un recurso (p.ej., carpeta o disco duro) hay que seleccionar la carpeta, pulse el botón derecho y seleccione *Propiedades.* Tal y como puede ver en la figura 2-14, en la pestaña *Seguridad* se muestran los permisos de la carpeta. En la parte superior se muestra el listado de los usuarios y grupos. Si selecciona un usuario o grupo en la parte inferior se muestran sus permisos.



Permisos de una carpeta

NTFS almacena una lista de control de acceso (access control list, ACL) con cada archivo y carpeta en una partición NTFS. La lista ACL contiene un listado de todas las cuentas de usuario, grupos y equipos a los que se ha concedido acceso al archivo o carpeta, y el tipo de acceso concedido. Para que un usuario pueda acceder a un archivo o carpeta, la lista ACL debe contener una entrada, denominada entrada de control de acceso (access control entry, ACE), para la cuenta de usuario, grupo o equipo al que pertenece el usuario. La entrada debe permitir específicamente el tipo de acceso solicitado por el usuario para que éste pueda tener acceso al archivo o carpeta. Si no existe ninguna entrada ACE en la lista ACL, Windows denegará al usuario el acceso al recurso.

Por defecto, cuando concedemos permisos a usuarios y grupos sobre una carpeta, los usuarios o grupos tienen acceso a las subcarpetas y archivos que ésta contiene. Es importante entender el modo en que las subcarpetas y los archivos heredan los permisos de NTFS desde las carpetas padre para poder utilizar la herencia en la propagación de permisos a archivos y carpetas.
Si concedemos permisos sobre un archivo o carpeta a una cuenta de usuario individual o a un grupo al que pertenezca el usuario, el usuario obtendrá varios permisos sobre el mismo recurso .

Los permisos son acumulativos .Los permisos efectivos de un usuario sobre un recurso son la combinación de los permisos de NTFS concedidos a la cuenta de usuario individual y los concedidos a los grupos a los que pertenece el usuario. Por ejemplo, si un usuario tiene permiso de Lectura sobre una carpeta y pertenece a un grupo con permiso de Escritura sobre la misma carpeta, el usuario tendrá ambos permisos, Lectura y Escritura, sobre esa carpeta.

Los permisos de archivo son independientes de los permisos de carpeta. Los permisos de archivo de NTFS tienen prioridad respecto a los permisos de carpetas de NTFS. Por ejemplo, un usuario con el permiso Modificar para un archivo podrá modificar el archivo aunque únicamente disponga del permiso de Lectura sobre la carpeta que contiene dicho archivo.

Denegar invalida otros permisos. Se puede denegar el acceso a un determinado archivo o carpeta aplicando la denegación del permiso a la cuenta de usuario o grupo. Aunque un usuario tenga permiso para acceder al archivo o carpeta como miembro de un grupo, denegar el permiso al usuario bloquea cualquier otro permiso de que éste disponga. Por tanto, la denegación de permiso es una excepción a la regla acumulativa. Es aconsejable evitar la denegación de permiso ya que es más fácil permitir el acceso a usuarios y grupos que denegar el acceso específicamente.
Ese preferible estructurar grupos y organizar recursos en carpetas de forma que otorgar permisos sea suficiente.

Un aspecto importante que hay que tener en cuenta es que los permisos se pueden establecer directamente a la carpeta o ser heredados de una carpeta superior. Por ejemplo, en la figura anterior puede ver que los Usuarios tienen permisos de lectura en la carpeta e:\Documentos. Como los permisos aparecen sombreados, los permisos se heredan de la carpeta superior, que en este caso es E:. Si desea cambiar estos permisos puede cambiarlos directamente en E:. Pero si desea en algún momento “romper” la herencia, entonces tiene que pulsar el botón Opciones avanzadas y en la ventana que aparece en la figura siguiente desactive la casilla **Incluir todos los permisos heredables del objeto primario de este objetivo** y automáticamente el sistema pregunta si desea copiar o eliminar los permisos del objeto superior.

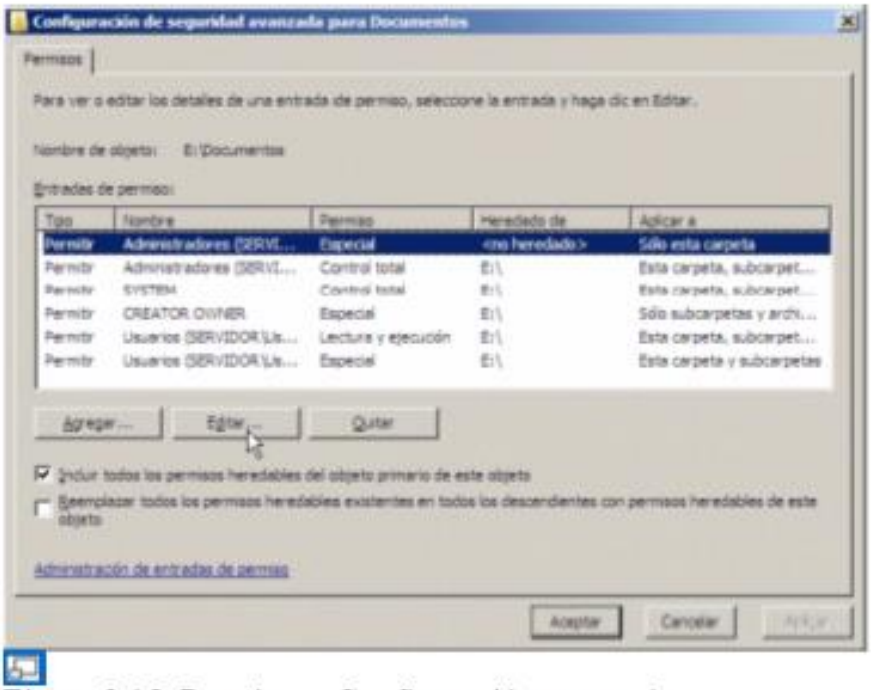


Figura 2 15. Permisos - Configuración avanzada

Para modificar los permisos pulse el botón **Editar** y en la ventana que aparece en la figura anterior puede añadir los usuarios o grupos a los que quiere establecer los permisos de acceso.

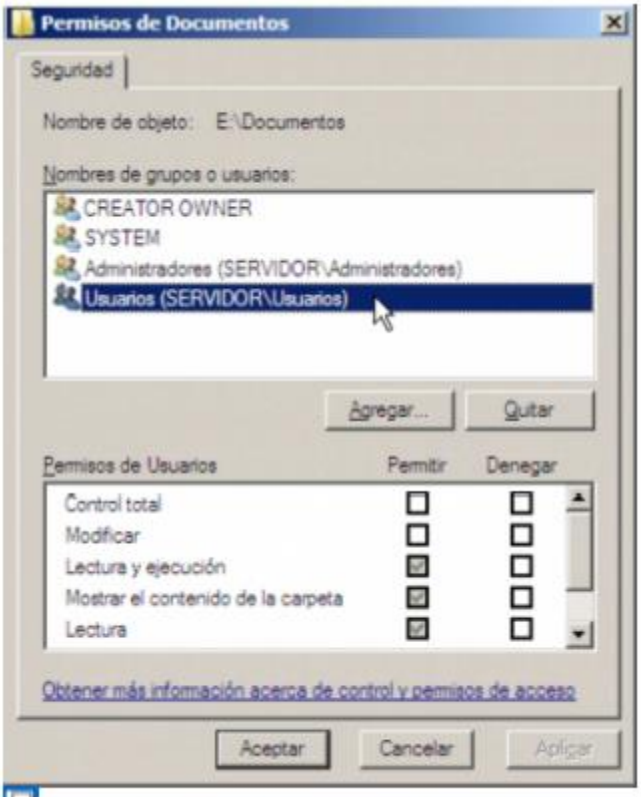


Figura 2 16. Permisos de una carpeta

Comandos

Net share	Crea, elimina o muestra recursos compartidos.	net share recurso_compartido