1 Principios de Seguridad en Windows XP

En la mayoría de los sistemas operativos actuales, aparecen dos conceptos relacionados con la seguridad del sistema: Autentificación y Autorización.

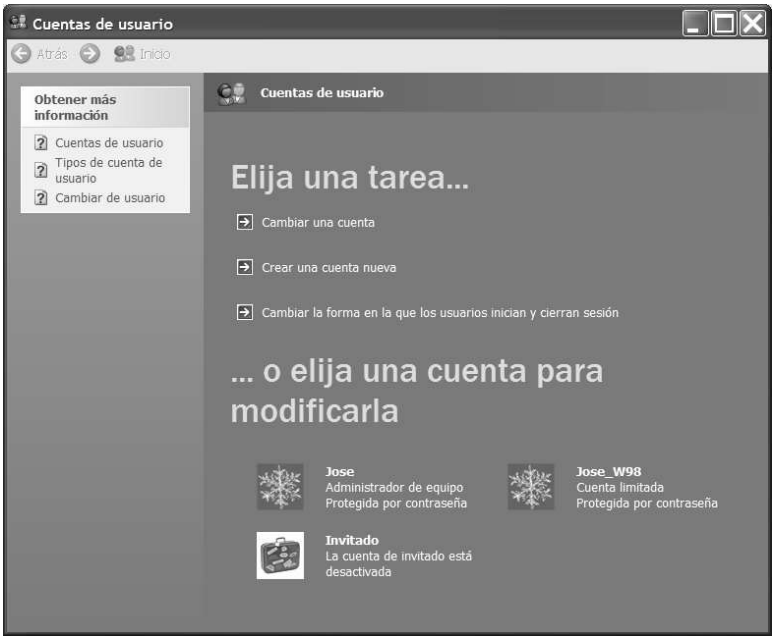
- Autentificación: Para usar el sistema es necesario abrir una sesión de trabajo (login) para lo cual tendremos que autentificarnos, proporcionando al sistema un nombre de usuario y una contraseña. En caso de no tener una cuenta de usuario abierta en el sistema, será imposible entrar en el mismo.
- Autorización: Una vez que el usuario se ha autentificado y abierto sesión, cada vez que quiera usar un recurso (un fichero, una carpeta, una impresora, etc) el sistema comprobará si esta autorizado o no para realizar esa acción. Los administradores del sistema pueden modificar estas autorizaciones mediante unas listas de acceso.

1.1 Gestión de Cuentas de Usuario y Grupos.

Podemos crear, borrar y modificar cuentas de usuario en Windows XP usando varios programas distintos.

- Asistente para cuentas de usuario desde Panel de Control.
- Gestión de cuentas de usuario mediante consola especial.
- Gestión de cuentas de usuario locales y grupo mediante consola.
- Desde el shell de texto.

Asistente para cuentas de usuario desde Panel de Control



Para abrir la herramienta Cuentas de usuarios, hay que abrir el Panel de control desde el menú Inicio y, a continuación, hacer doble clic en Cuentas de usuario.

Para crear una cuenta de usuario nueva, hay que seguir estos pasos:

1. Hacer clic en Crear una nueva cuenta en la lista desplegable Elija una tarea.
2. Escribir el nombre que deseamos utilizar para la cuenta y, después,

hacer clic en Siguiente.

3. Seleccionar el tipo de cuenta que deseamos y después hacer clic en Crear cuenta.

Para realizar cambios en una cuenta, hay que seguir estos pasos:

1. Hacer clic en Cambiar una cuenta en la lista desplegable Elija una tarea.
2. Hacer clic en la cuenta que desea cambiar.
3. Seleccionar el elemento que desea cambiar: (nombre, imagen, tipo, contraseña, borrado).

Nota: No se puede borrar una cuenta de un usuario si tiene sesión abierta en el sistema.

Gestión de cuentas de usuario mediante consola especial.

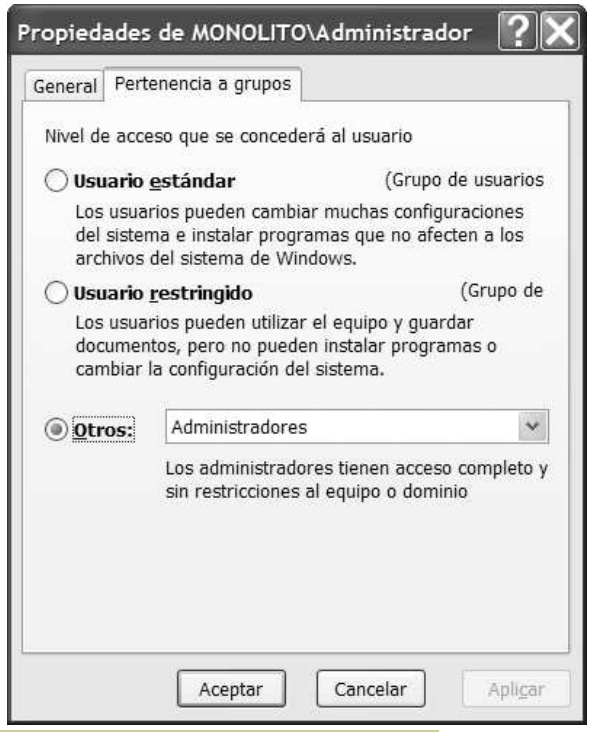
Podemos también gestionar las cuentas de usuario mediante una consola. Si estamos conectados a un dominio, este es el gestor de usuarios que usaremos por defecto. Para acceder a dicho gestor, hay que ejecutar la siguiente orden desde Inicio – Ejecutar, o bien desde una ventana del intérprete de comandos:

CONTROL USERPASSWORDS2

Con este gestor de cuentas de usuario, tenemos un control mucho mayor sobre las cuentas de usuario que el que obtenemos con el asistente.

La primera opción que vemos en pantalla, "Los usuarios deben escribir su nombre y contraseña para usar el equipo" nos permite indicar si queremos usar la autentificación o no. Si lo desactivamos, obtendremos un XP que se iniciará automáticamente con la cuenta que indiquemos sin mostrarnos siquiera la pantalla de bienvenida. Obviamente, esta opción solo debería usarse en ambientes domésticos donde solo un usuario usa el ordenador.

Para agregar cuentas de usuario usamos el botón agregar, para eliminar cuentas el botón quitar, etc. Si seleccionamos una cuenta de usuario y pulsamos el botón propiedades, pasamos a la siguiente pantalla.



Desde esta pantalla, podemos observar como podemos incluir al usuario en algún grupo de usuarios, bien uno de los dos incluidos en el gestor (usuarios estándar y usuarios restringidos) o bien seleccionando otro grupo como puede ser el de administradores, etc.

Vemos que este control de grupos es mucho más

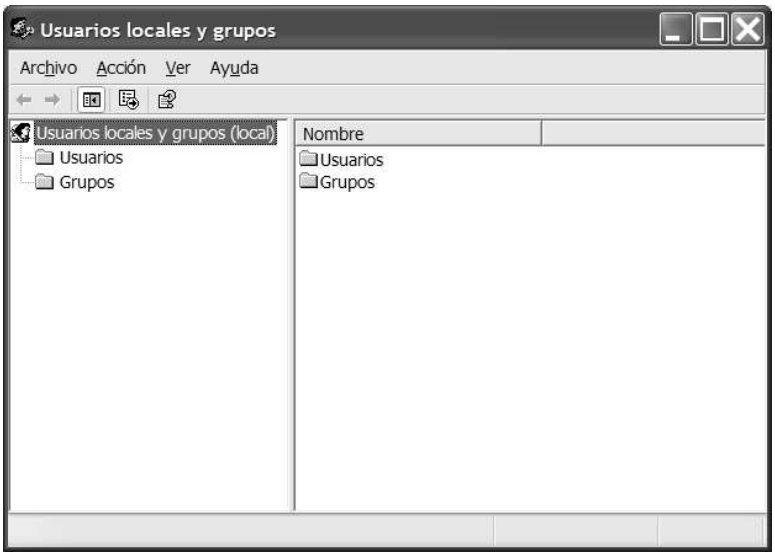
amplio que el que nos ofrece el asistente donde las opciones son usuarios administradores o usuarios restringidos.

En las distintas pestañas de este gestor, podemos ver opciones muy interesantes como el Passport de MSN, opciones para modificar el inicio del sistema, opciones para almacenar las contraseñas de nuestro equipo, etc.

Una opción muy interesante que nos podemos encontrar en la primera pantalla (y que es un fallo de seguridad tremendo por parte de Microsoft, que no seria admisible en un sistema servidor) es la posibilidad de cambiar la contraseña del Administrador. Para hacerlo, basta con que nos hayamos autentificado con una cuenta de usuario que pertenezca al grupo Administradores. Esta opción ha sido incluida ya que a veces los usuarios no recuerdan con el tiempo la contraseña que le asignaron a la cuenta de Administrador en el momento de la instalación del equipo.

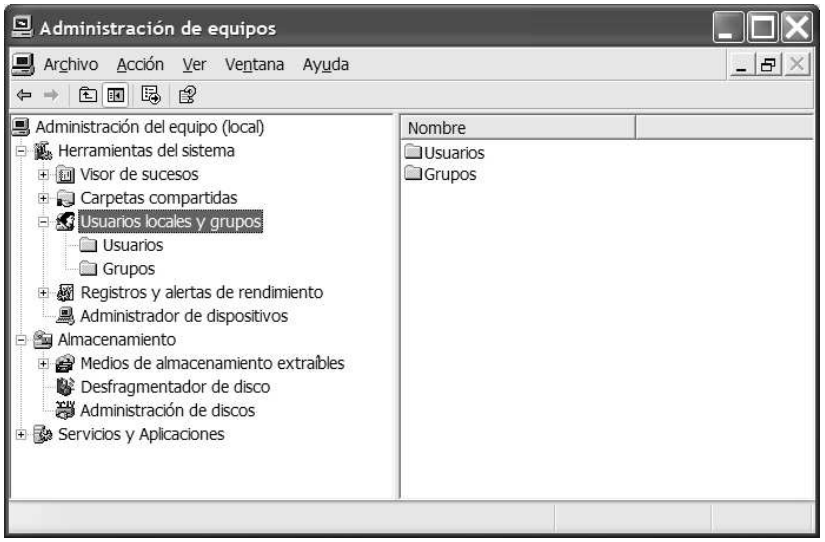
Gestión de cuentas de usuarios locales y grupo mediante consola.

La tercera opción que tenemos para gestionar cuentas de usuario, es la opción más interesante de todas las que nos ofrece XP. Es la consola de usuarios locales y grupos. Podemos llegar a dicha consola de varias formas.



- Podemos ejecutar desde Inicio – Ejecutar y escribir LUSRMGR.MSC.
- O desde Panel de Control – Herramientas Administrativas – Administración de Equipos y en ella escogemos la carpeta de usuarios locales y grupos.

Lleguemos desde donde lleguemos, veremos que tenemos dos carpetas, una para los usuarios y otra para los grupos. Podemos crear usuarios nuevos accediendo a las propiedades de la carpeta usuarios (botón derecho sobre ella) y seleccionando la opción de Usuario Nuevo. Podemos modificar un usuario accediendo a sus propiedades. Del mismo modo podemos crear nuevos grupos y modificar los ya existentes.

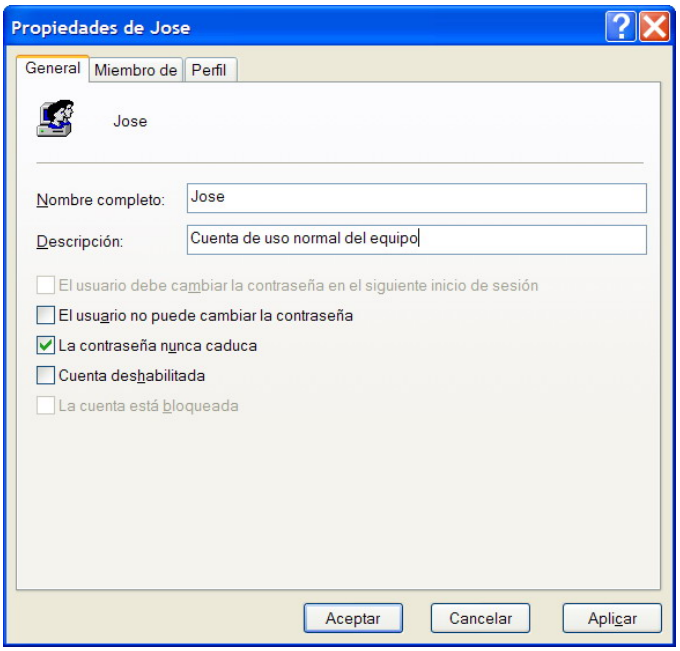


Podemos tanto asignar a un usuario varios grupos, como asignar a un grupo varios usuarios.

Podemos crear todas las cuentas de usuarios que deseemos, pero aparte de estas cuentas normales, existen dos cuentas de usuario especiales en Windows XP, ya creadas y que no pueden (no deben) ser modificadas o eliminadas.

- La cuenta del Administrador del sistema (Administrador). Todos los sistemas XP tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitados para que solo puedan ser ejecutadas por el Administrador. Es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador (integrándolas como miembros del grupo Administradores), aunque Administrador solo puede haber uno. Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema.
- La cuenta de Invitado. (Guest). Es la contraria a la cuenta de Administrador, esta totalmente limitada, no cuenta apenas con ningún permiso o derecho pero permite que cualquier usuario pueda entrar en nuestro sistema sin contraseña (lo que se denomina acceso anónimo) y darse un "paseo" por el mismo. Por defecto, en Windows XP Profesional esta cuenta esta desactivada. Es altamente recomendable nunca activar dicha cuenta, ya que representa un riesgo altísimo de seguridad.

Si comprobáis el nombre de esta ultima consola, veréis que aparece la palabra local en el mismo. Esto es asi por que se distinguen dos ámbitos al hablar de usuarios: Los usuarios locales y los usuarios de dominio. Mientras no tengamos instalado un dominio (para lo cual necesitaremos algún servidor Windows de la familia NT) siempre estaremos trabajando con cuentas locales.



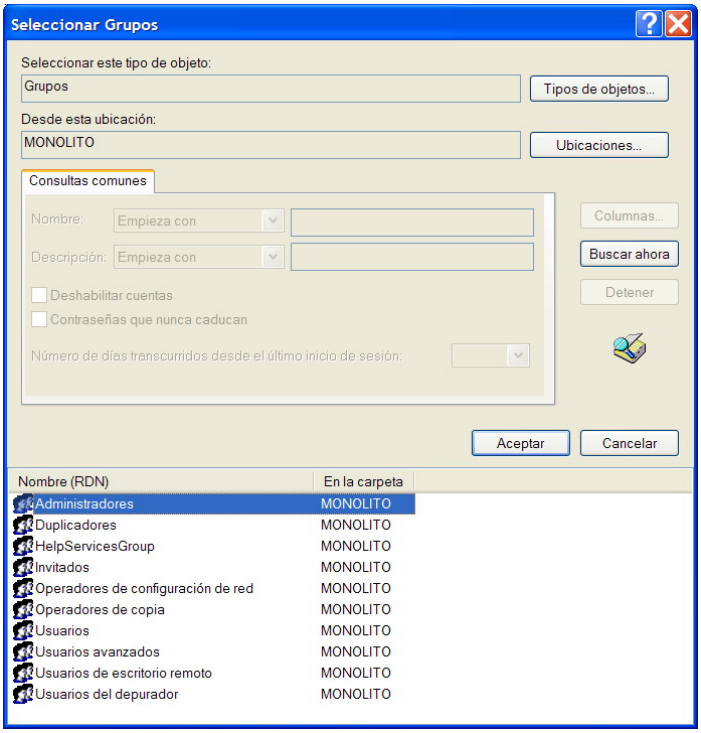
Si accedemos a las propiedades de un usuario, veremos como tenemos tres pestañas con las que trabajar:

- **General**: Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta.
  - El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.
  - El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.
  - La contraseña nunca caduca. Ya veremos como en Windows XP las contraseñas se consideran material fungible, es decir, que tras un cierto tiempo de uso el sistema obligará a cambiar dichas contraseñas. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque nunca.
  - Cuenta deshabilitada: No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.

- La cuenta esta bloqueada: Por determinados mecanismos de seguridad que ya veremos, se puede llegar a bloquear una cuenta, que implicará que dicha cuenta estará deshabilitada. Desde esta opción podemos volver a desbloquearla, simplemente desmarcando la casilla.

- **Miembro de**: Desde esta pestaña podemos introducir al usuario en grupos. Los grupos se usan para dar permisos y derechos a los usuarios fácilmente, sin tener que ir usuario por usuario. Asi por ejemplo, si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos los permisos del grupo Administradores.

  En la pestaña miembro de veremos todos los grupos a los que el usuario pertenece actualmente. Si le damos al botón **agregar** podremos escribir directamente el nombre de un grupo donde agregarlo. Si queremos escoger dicho grupo de una lista de los grupos posibles, hay que escoger la opción **Avanzada** y luego **Buscar ahora**, que nos mostrará una lista de todos los grupos del sistema. Basta con seleccionar el que queramos (o los que queramos) y pulsar aceptar.



- **Perfil**: Nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario. Como en un apunte posterior veremos el tema de perfiles, de momento lo dejamos pendiente.

Desde el shell de texto.

La ultima opción para gestionar las cuentas de usuario, es hacerlo directamente desde el Shell de texto. Esta opción puede parecer la más engorrosa, pero resulta ser la mas practica en muchísimas ocasiones, sobre todo si conocemos como hacer scripts de sistema.

Para ello disponemos de varias ordenes que nos permiten gestionar las cuentas de usuario:

- Net user

Agrega o modifica cuentas de usuario o muestra información acerca de ellas.

Sintaxis

`net user [`*nombreDeUsuario* `[`*contraseña* `| *] [`*opciones*`]] [/domain]`

`net user` *nombreDeUsuario* `{`*contraseña* `| *} /add [`*opciones*`] [/domain]]`

`net user [`*nombreDeUsuario* `[/delete] [/domain]]`

Parámetros

NombreDeUsuario Específica el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o ver. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

Contraseña Asigna o cambia una contraseña para la cuenta de usuario. Escriba un asterisco (*) si desea que se le pida la contraseña. Los caracteres de la contraseña no se muestran en la pantalla a medida que los escribe.

/domain Realiza la operación en el controlador principal del dominio principal del equipo.

opciones

Especifica una opción de la línea de comandos. La tabla siguiente enumera las opciones válidas de la línea de comandos que puede utilizar:

Sintaxis de las opciones de la línea de comandos	**Descripción**
`/active:{no | yes}`	Habilita o deshabilita la cuenta de usuario. Si no está activa, el usuario no puede tener acceso a los recursos del equipo. La opción predeterminada es **yes** (activa).
`/comment:"texto"`	Proporciona un comentario descriptivo acerca de la cuenta de usuario. Puede tener hasta 48 caracteres. Escriba el texto entre comillas.
`/countrycode:nnn`	Usa los códigos de país o región del sistema operativo para instalar los archivos de Ayuda y mensajes de error en el idioma especificado. 0 significa el código de país predeterminado.
`/expires:{{mm/dd/aaaa | dd/mm/aaaa | mmm,dd ,aaaa} | never}`	Provoca que la cuenta de usuario caduque si se especifica *fecha*. Las fechas de caducidad pueden tener el formato [*mm/dd/aaaa*], [*dd/mm/aaaa*] o [*mmm*,dd ,*aaaa*], según el código de país o región. Tenga en cuenta que la cuenta caduca al comienzo de la fecha especificada.
`/fullname:"nombre"`	Especifica un nombre de usuario completo en lugar de un nombre de usuario normal. Escriba dicho nombre entre comillas.
`/homedir:rutaDeAcceso`	Establece la ruta de acceso del directorio particular del usuario. Dicha ruta de acceso debe ser una ya existente.
`/passwordchg:{yes | no}`	Especifica si los usuarios pueden cambiar su contraseña. La opción predeterminada es **yes**.
`/passwordreq:{yes | no}`	Especifica si una cuenta de usuario debe tener una contraseña. La opción predeterminada es **yes**.

`/profilepath:[rutaDeAcceso]`	Establece una ruta de acceso al perfil de inicio de sesión del usuario. Esta ruta de acceso señala a un perfil de registro.
`/scriptpath:rutaDeAcceso`	Establece una ruta de acceso a la secuencia de comandos de inicio de sesión del usuario. El parámetro *rutaDeAcceso* no puede ser una ruta de acceso absoluta. *RutaDeAcceso* es relativa a *%raízSistema%*\System32\Repl\Import\Scripts.
`/times:{día[-día][,día[-día]] ,hora[-hora][,hora[-hora]] [;…] | all}`	Especifica las horas en las que se permite al usuario el uso del equipo. El parámetro *Hora* está limitado a incrementos de 1 hora. Para los valores de *día*, puede escribir el día o usar abreviaturas (L, Ma, Mi, J, V, S, D). Para las horas puede usar la notación de 12 horas o de 24 horas. Para el formato de 12 horas, use am, pm, a.m. o p.m. El valor **all** significa que un usuario puede iniciar una sesión en cualquier momento. Un valor nulo (en blanco) significa que un usuario nunca puede iniciar la sesión. Separe el día y la hora mediante comas y las unidades de día y hora con punto y coma (por ejemplo, **L,4AM-5PM;M,1AM-3PM**). No use espacios en la especificación de horas.
`/usercomment:"texto"`	Especifica que un administrador puede agregar o cambiar el "Comentario de usuario" de la cuenta. Escriba el texto entre comillas.
`/workstations:{nombreDeEquipo[,...] | *}`	Enumera hasta ocho estaciones de trabajo desde las que un usuario puede iniciar una sesión en la red. Separe los nombres de las estaciones con una coma. Si **/workstations** no es una lista o ésta es igual a un *, el usuario puede iniciar una sesión desde cualquier equipo.

net help *comando* Muestra ayuda para el comando **net** especificado.

Comentarios

Utilizado sin parámetros, net user muestra una lista de las cuentas de usuario en el equipo.

La contraseña debe tener la longitud mínima establecida con **net accounts /minpwlen**. Puede tener hasta 127 caracteres. Sin embargo, si utiliza Windows 2000 o Windows XP en una red en la que también hay equipos que utilizan Windows 95 o Windows 98, considere la posibilidad de utilizar contraseñas que no tengan más de 14 caracteres. Windows 95 y Windows 98 admiten contraseñas de hasta 14 caracteres. Si su contraseña tiene más caracteres, es posible que no pueda iniciar una sesión en la red desde esos equipos.

Ejemplos

Para mostrar una lista de todas las cuentas de usuario del equipo local, escriba:

```
net user
```

Para ver información acerca de la cuenta de usuario juanh, escriba:

```
net user juanh
```

Para agregar una cuenta de usuario para Enrique Pérez, con derechos de inicio de sesión desde las 8 a.m. a 5 p.m. de lunes a viernes (sin espacios en las especificaciones de las horas), una contraseña obligatoria (enriquep) y el nombre completo del usuario, escriba:

```
net user enriquep enriquep /add /passwordreq:yes /times:lunes-viernes,8am-5pm /fullname:"Enrique Pérez"
```

Obviamente la mayor potencia del shell de texto aparece cuando usamos scripts. Imaginemos el siguiente ejemplo:

Necesito crear una cuenta de usuario por cada uno de los alumnos del grupo, quiero indicar que solo puedan abrir sesión de lunes a viernes entre las 16 y las 22 horas, quiero usar como contraseña de cada usuario "caballo" pero obligando a cambiar dicha contraseña en el primer inicio de sesión del alumno.

Si tengo unos 40 alumnos entre varios grupos, esta claro que el tiempo que voy a usar en crear dichas cuentas va a ser importante. (Imaginad que ocurriría en una empresa con 600 empleados).

Podría solucionar todo el problema de la siguiente forma:

1. Creo un fichero de texto (alumnos.txt) donde en cada línea aparece el nombre del alumno (sin espacios en blanco). Dicho fichero naturalmente podría obtenerlo de la lista de clase, de un programa de horario, etc.
2. Creo un proceso por lotes que vaya leyendo dicho fichero de texto y vaya creando una cuenta de usuario por cada línea. Sería algo asi:

```
Rem ------ creacuen.bat -------
@Echo Off
Cls
Echo ------ Creando cuentas de usuario --------
For /F %%A In (.\ALUMNOS.TXT) Do (
        Echo ------ Creando cuenta para %%A
        NET USER %%A caballo /ADD /TIMES:LUNES-VIERNES,4PM-10PM
        )
Echo ------ Proceso Finalizado -----------------
```

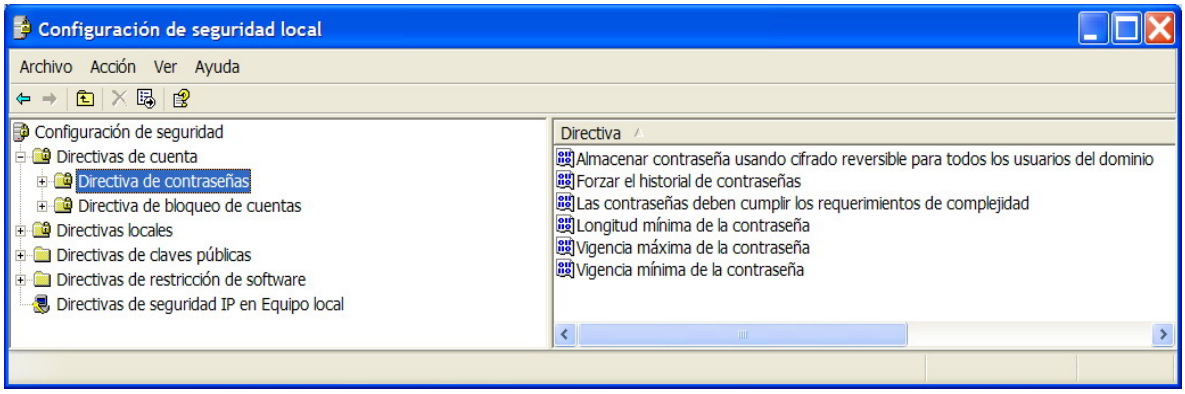
Si probamos este proceso, se nos crearán varias cuentas en el sistema. Para borrarlas automáticamente podríamos crear un script como el siguiente:

```
Rem ------ borracuen.bat -------
For /F %%A In (.\ALUMNOS.TXT) Do (NET USER %%A /DELETE)
```

Gestión de las contraseñas.

Windows XP es un sistema operativo muy configurable por parte del usuario. Aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales, y solo pueden ser modificadas desde las consolas del sistema.

En concreto, desde la consola de Configuración de Seguridad Local, podemos gestionar varios aspectos sobre las contraseñas. (Inicio – Ejecutar – SecPol.msc – Configuración de Seguridad – Directivas de Cuenta – Directivas de Contraseñas)

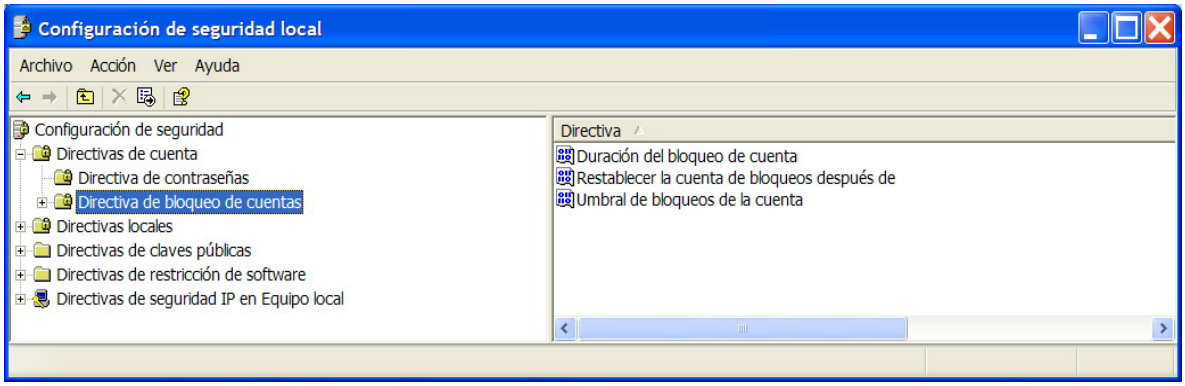


Las configuraciones más útiles que podemos gestionar desde aquí son:

- Forzar el historial de contraseñas. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuantas contraseñas recordará XP.
- Las contraseñas deben cumplir los requerimientos de complejidad. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.
- Longitud minina de la contraseña. Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.
- Vigencia máxima de la contraseña. Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
- Vigencia minina de la contraseña. Indica cuanto tiempo debe transcurrir desde que un usuario se cambia la contraseña, hasta que puede volver a cambiarla. Esta configuración de seguridad local se usa para evitar que un usuario cambie continuamente su contraseña a fin de volver a quedarse con su contraseña original caducada.

Bloqueo de las cuentas.

Desde secpol.msc también podemos gestionar un comportamiento de las cuentas de usuario relacionado con las contraseñas, y es el bloquear las cuentas si se intenta acceder al sistema con las mismas pero usando contraseñas incorrectas. Esta configuración la encontramos en (Inicio – Ejecutar – SecPol.msc – Configuración de Seguridad – Directivas de Cuenta – Directivas de Bloqueo de Cuentas)



Aquí podemos configurar:

- Duración del bloqueo de cuenta. (Durante cuanto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).
- Restablecer la cuenta de bloqueos después de. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).
- Umbral de bloqueo de la cuenta. (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

1.2 SID

Imaginad que creamos una cuenta en nuestro equipo con nombre PACO y contraseña P1c4. Creamos varias carpetas que solo le pertenecen a el, ciframos archivos para que solo los pueda leer el, etc. Un día sin embargo por error borramos la cuenta PACO y todas esas informaciones quedan "huérfanas". Ni cortos ni perezosos decidimos crear otra vez la cuenta PACO con contraseña P1c4, para intentar acceder a dichos ficheros y carpetas. Pues bien, comprobaremos que nuestro sistema sabe perfectamente que ese nuevo PACO no tiene nada que ver con el antiguo PACO, y los considera usuarios totalmente distintos.

Esto es asi por que el sistema operativo no usa para referirse a las cuentas su nombre o su contraseña, esos son campos que usamos nosotros, al igual que nos llamamos entre nosotros con nuestro nombre, no con nuestro DNI. El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID. (Security IDentifier o Identificador de Seguridad).

Un SID esta formado de la siguiente manera:

S-1-5-21-448539723-413027322-839522115-1003

El ultimo número, en este caso 1003 se conoce como RID (identificador relativo del usuario) y todo lo que esta delante del mismo identifica el dominio al que pertenece ese usuario. En concreto, esos tres grandes números que se observan (448539723-413027322-839522115) se generan automáticamente y al azar cada vez que instalamos un XP, y aparecerán en todas las cuentas que creemos en dicho sistema. (Esta es la razón por la que no se debe simplemente "clonar" o copiar un XP entero de una maquina a otra, puesto que este número será igual y esos sistemas no podrán trabajar adecuadamente en red).

La parte del SID S-1-5-21 nos da información sobre el objeto con el que estamos trabajando. Asi por ejemplo si hablamos de algunos grupos o usuarios especiales tenemos:

S-1-1-0 es el SID del grupo Todos (Everyone)

S-1-2-0 es el SID del grupo Usuarios locales

S-1-3-1 es el SID de Creator – Owner

S-1-5 Este inicio de SID nos indica que estamos trabajando con un usuario o grupo normal. Dentro de este grupo algunos SID conocidos son:

S-1-5-32-544 SID del grupo Administradores

S-1-5-32-545 SID del grupo Usuarios

Desde Windows XP es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden **`whoami.exe`**, sin embargo si intentáis ejecutar esta orden en vuestro Windows XP os dirá que dicho comando no existe. Esto es asi por que esta orden no es de las que vienen incluidas en una instalación típica de Windows XP, para instalar esta orden (y otras varias también bastante interesantes) debéis instalar las herramientas de soporte de Windows XP.

Para ello, introducid el CD de Windows XP Profesional en la unidad de CD con el sistema en marcha, explorad dicho CD y ejecutar el programa SETUP que esta en la carpeta \SUPPORT\TOOLS. Esto instalará en vuestro sistema varias herramientas, entre las cuales estará el comando WHOAMI.EXE.

Una vez instalado, abrid un shell, y ejecutad la siguiente orden:

```
M:\Archivos de programa\Support Tools>whoami /USER /SID
```

Que os responderá algo como lo siguiente:

```
[User]="SIS\Joan"  S-1-5-21-448539723-413027322-839522115-1003
```

Podemos ver aquí como nos dice el nombre de nuestro usuario actual y además nos indica que SID le ha sido otorgado por el sistema.

Si queremos ver no solo el SID que se le ha otorgado a nuestro usuario, sino el SID de todos los grupos a los que pertenece nuestro usuario, usad la orden con los parámetros /USER /SID /GROUPS.

Whoami solo nos muestra información sobre el usuario actual, asi que si queremos ver los SID de distintos usuarios, tendremos que ejecutar dicha orden como dichos usuarios. Aprovecho aquí para comentaros una orden que a veces es muy util. En lugar de tener que ir cerrando y abriendo sesión con cada usuario, podemos "hacernos pasar" por dicho usuario sin tener que cerrar sesión, ni abrir sesión, ni nada. Para ello usaremos la orden runas (ejecutar como si fuera).

Para ellos, abrid un shell y ejecutad la orden: `RunAs /user:usuario_a_suplantar cmd`

Con esto conseguiremos abrir una nueva shell en la que seremos el usuario que estamos suplantando, por lo que si ejecutamos en dicha ventana whoami nos responderá con el nuevo usuario.

Abrimos una nueva sesión de cmd ya que si ejecutamos directamente runas whoami se ejecutaría la orden, pero no veríamos nada.

1.3 Recursos Locales. Gestión de ACL

Llamamos recursos de un sistema a los distintos elementos con los que ese sistema cuenta para que sean usados por los usuarios. Así, una impresora, una carpeta, un MODEM, un fichero, una conexión de red, son recursos.

Bien, pues cada recurso cuenta con una lista donde aparecen los usuarios que pueden usar dicho recurso y de que forma pueden usarlo.

Ya hemos visto que el sistema no ve usuarios y grupos, realmente ve Identificadores de Seguridad (SID), de modo que dicha lista realmente tendrá en su interior una serie de SIDs y los permisos que cada uno de esos SIDs tiene sobre el recurso.

Esta lista con la que cuenta cada recurso se conoce como ACL (Access Control List, o Lista de Control de Acceso).

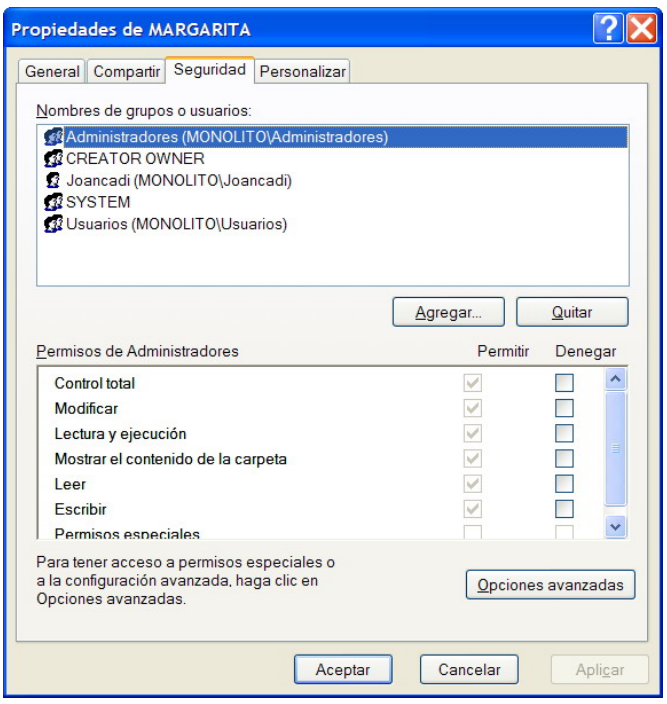
Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.

Si no aparece en la ACL ningún SID del usuario, el recurso niega el acceso al usuario.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc) esta permitida para ese SID en su ACL, si lo esta le autoriza para hacerlo, en caso contrario se lo impide.

Puede ocurrir que un usuario tenga permisos contradictorios… imaginemos que en el ACL de la carpeta margarita aparece que el SID del usuario PACO puede escribir en la carpeta, pero PACO pertenece al grupo PROFESORES que aparece en el ACL de margarita como que no tiene derecho a escribir. Bien, en este caso se aplica la siguiente regla:

1. Lo que mas pesa en cualquier ACL es la denegación implícita de permisos. Si un permiso esta denegado, no se sigue mirando, se deniega inmediatamente.
2. Basta con que un permiso este concedido en cualquier SID para que se considere concedido. (A excepción de la regla 1, es decir, que no este denegado implícitamente en ningún sitio)



Esto se entiende mejor gestionando el ACL de algún recurso.

Por ejemplo, creemos en el raíz de nuestro volumen (en NTFS) una carpeta con nombre MARGARITA. Una vez creada, accedemos a sus propiedades y en ellas a la pestaña Seguridad:

Podemos ver como en la parte superior tenemos las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID. Si veis las dos columnas por cada permiso, podemos tanto Permitir como Denegar un permiso. La denegación de un permiso es la que mas pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos, a menos que sea absolutamente necesario.

Puede ocurrir que en las propiedades de vuestro recurso no aparezca la pestaña Seguridad. Esto ocurre por que aún tendréis activado el uso compartido simple de archivos de Windows XP, que es una forma de olvidarnos de las ACL y trabajar de una forma muy simple, indicada para usuarios que no desean preocuparse por estos temas.

Para desactivar este uso compartido simple, accedemos a Mi PC, y allí en el menú Herramientas – Opciones de carpeta – Ver accedemos al final de la lista y allí encontramos dicha opción que hay que desactivar.

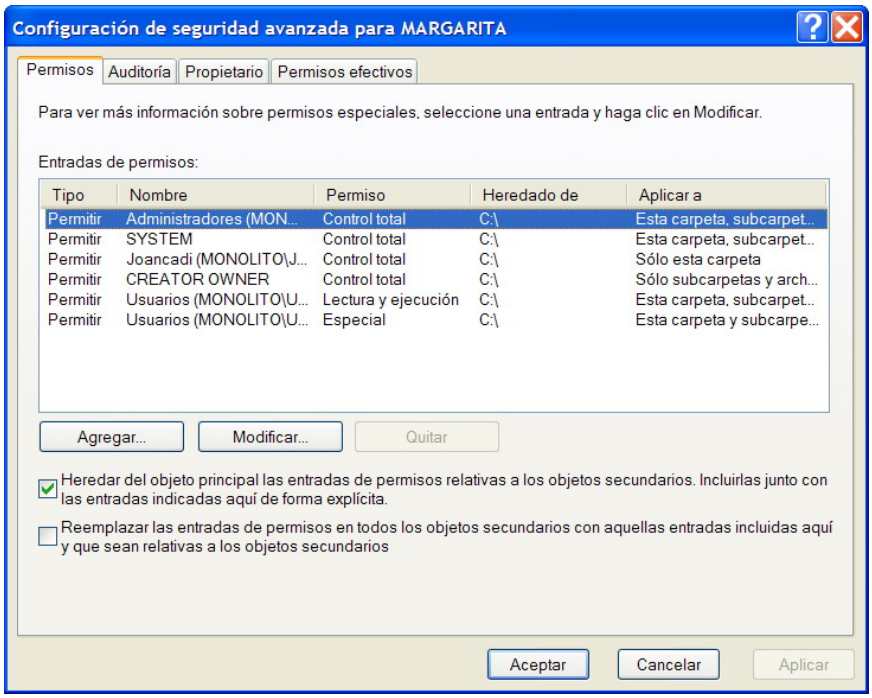
Más o menos todo lo que se ve en la ACL deberíais entenderlo sin problemas. Con los botones agregar y quitar podemos añadir o quitar SID de la ACL.

En la parte inferior podemos pulsar en las casillas de Permitir y Denegar para dar y quitar permisos.

¿Pero… por que aparece la columna de Permitir en gris y no nos deja cambiarla? Bien, ha llegado el momento de hablar de la herencia.

Imaginemos que creamos una carpeta por ejemplo CONTABLES, y la preparamos minuciosamente para que pueden leer y escribir en ella los usuarios que sean miembros del grupo CONTABLES, para que solo puedan leer los del grupo JEFES pero no escribir, y que los demás usuarios no puedan ni leer en ella ni escribir. Bien, si ahora dentro de la carpeta CONTABLES creamos una nueva carpeta INFORMES, ¿no sería lógico que esta carpeta INFORMES "heredara" la ACL de su carpeta madre CONTABLES para que no tuviera que configurarla nuevamente?

Pues precisamente eso es lo que hace Windows XP, cualquier recurso que creemos, heredará automáticamente la ACL de su recurso padre si es que existe. En nuestro caso, la carpeta MARGARITA ha heredado la ACL de la raíz de nuestro volumen. De modo que no podremos quitar usuarios, quitar permisos, etc.



Para realizar cambios en la ACL de nuestra carpeta MARGARITA, debemos indicarle que "rompa" la herencia, es decir, que deseamos retocar manualmente su ACL.

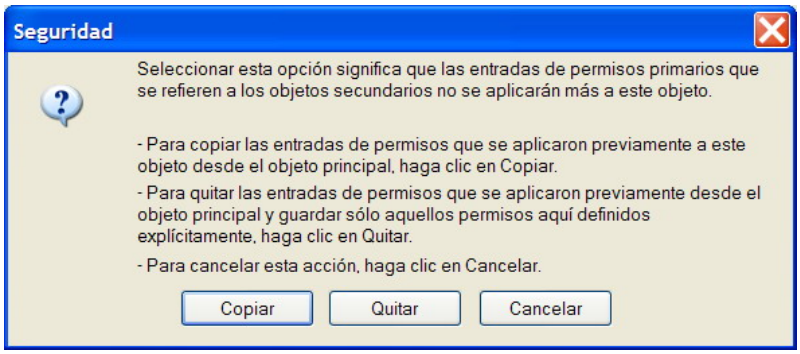
Para ello, accedemos al botón de Opciones Avanzadas que esta en la pestaña Seguridad.

Podemos ver en estas opciones avanzadas 4 pestañas, de momento nos quedamos en la primera, permisos.

Vemos como en la parte inferior de esta ventana, podemos ver como esta marcada la opción de "Heredar del objeto principal las entradas de permiso relativas a los objetos secundarios. Incluirlas junto con las entradas indicadas aquí de forma explicita". Si desmarcamos dicha opción mataremos la relación de herencia de nuestro recurso, y podremos gestionar su ACL "a pelo". Hagámoslo.

Cuidado ahora, una vez quitada la herencia, el sistema nos da a elegir entre dos opciones:

Si escogemos la opción Copiar, la herencia se interrumpirá, y podremos retocar la ACL como nos plazca, pero dicha ACL será la que ahora mismo tiene el recurso, heredada de su objeto principal.



Si escogemos la opción Quitar, la ACL se borrará totalmente, se interrumpirá la herencia y la podremos crear desde cero.

Si elegimos quitar y empezar desde cero, hay que tener en cuenta que en las ACL no solo deben aparecer nuestras SID normales, sino que grupos como Creator Owner o System son necesarios para que el sistema pueda trabajar sin problemas con dichas carpetas. Si quitamos estos SID tendremos problemas en el futuro (copias de seguridad, auditorias, etc).

Vemos como debajo de la opción de Heredar del objeto principal, tenemos otra opción que nos permite activar que los objetos por debajo del nuestro hereden las modificaciones que hagamos en nuestra ACL. Esto es importante tenerlo en cuenta si queremos que los cambios que hagamos en la ACL se repliquen en los objetos hijos del nuestro, ya que hemos roto la herencia y a veces tendremos que forzar dichos cambios.

Realizad el siguiente ejercicio:

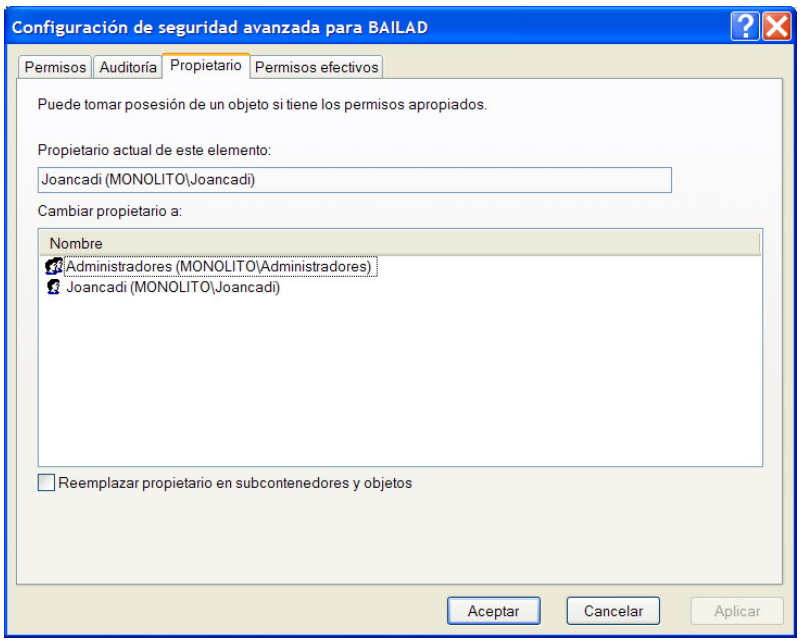
1. Cread 4 usuarios con nombre MELINDA, BELINDA, ROSALINDA y DESIDERIA.
2. Introducid los 4 usuarios anteriores en el grupo DANZA.
3. Cread una carpeta en la raíz de vuestro volumen con nombre BAILE. Modificad su ACL para que sólo puedan leer y escribir en dicha carpeta los miembros del grupo BAILE. Quitad el grupo Administradores, Usuarios, etc. Dejad los que aparecen en mayúsculas (creator owner y system) para que no tengamos problemas con la carpeta.
4. Comprobad abriendo sesión con los usuarios nuevos que efectivamente ellos pueden entrar y escribir en dicha carpeta y los demás usuarios del sistema no. (Podéis hacerlo bien cerrando y abriendo sesión o con Runas, lo que os resulte más cómodo).

Ahora bien, esa entrada en la ACL que se ve como Creator Owner indica el usuario que creó la carpeta y que por lo tanto es su propietario. Si dicha carpeta la creamos por ejemplo con el usuario Jose, el usuario Jose veremos como tiene permisos sobre dicha carpeta. Para evitar esto, repetid el ejercicio pero cread la carpeta con MELINDA por ejemplo. (En vez de con una carpeta BAILE hacedlo con la carpeta BAILAD por ejemplo).

Bien, ahora tendremos una carpeta donde ni los miembros del grupo Administradores ni el Administrador pueden entrar, leer o escribir. Es solamente para los usuarios del grupo DANZA… ¿o no?

Es imposible que un usuario en un sistema impida que el Administrador realice alguna función, (siempre que el Administrador sepa lo que es Administrar un sistema, claro). En este caso como Administrador (o miembro del grupo Administradores) podemos hacer lo siguiente. Accedemos a las propiedades de la carpeta "rebelde", si bien en ella no podemos modificar nada si podemos acceder a sus propiedades avanzadas, y dentro de dichas propiedades accedemos a Propietario.

Podéis ver como desde aquí podemos cambiar el propietario actual del objeto, e indicar que el propietario actual es el grupo Administradores (o el usuario actual si es del grupo Administradores). Basta con que seleccionemos el grupo Administradores y marquemos abajo Reemplazar propietario en subcontenedores y objetos y demos aplicar – aceptar. Seremos propietarios de la carpeta.



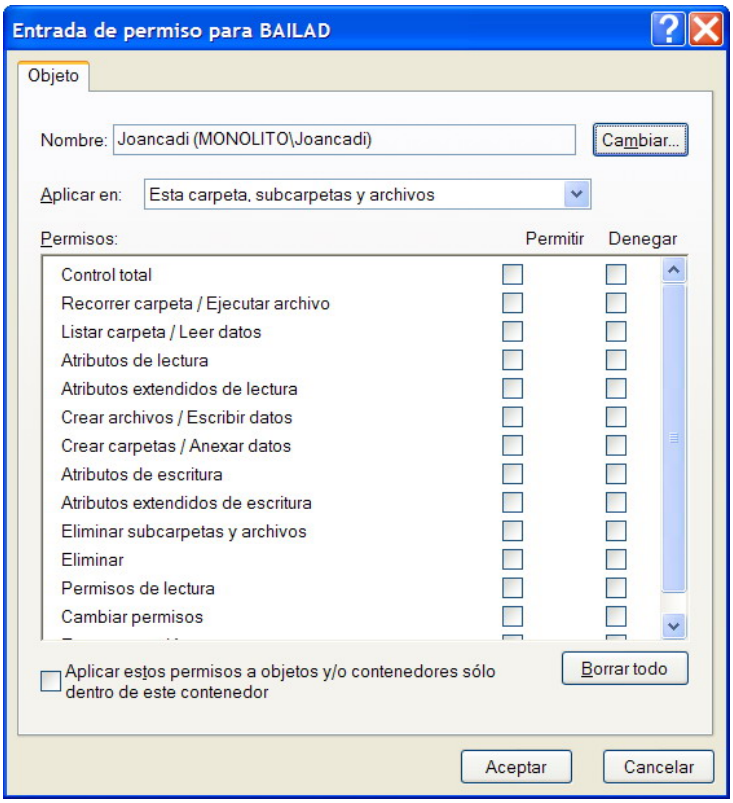
Basta con que actualicemos la ventana de permisos y ya podremos modificar la ACL del recurso como queramos.

Ojo, esto no nos permite acceder a la carpeta directamente, nos permite modificar su ACL, donde tendremos que introducir el SID del grupo Administradores para asi si, poder acceder a la carpeta con los permisos que indiquemos.

Otro ejercicio más para comprobar todo lo visto hasta ahora:

- Crear 20 usuarios con nombre Al_ASI_01, Al_ASI_02…… Al_ASI_20 (os aconsejo que lo hagáis desde shell de texto y con un proceso por lotes).
- Crear un grupo AL_ASI e introducid dentro los 20 usuarios anteriores
- Abrid sesión como AL_ASI_01 y cread una carpeta en el raíz de vuestro volumen con nombre A_S_I.
- Modificad sus permisos para que solo los miembros del grupo AL_ASI puedan leer, escribir, etc, en dicha carpeta. Quitad todas las demás SID de su ACL, incluidas las SID especiales.
- Comprobad que nadie fuera del grupo AL_ASI puede acceder a la carpeta A_S_I
- Cread un usuario con nombre HACKER y hacedlo miembro del grupo Administradores pero no del grupo A_S_I
- Abrid sesión como el usuario HACKER y modificar los permisos de A_S_I para que se DENIEGUE el acceso a los miembros del grupo AL_ASI y se permita el acceso total al grupo Todos.

Los distintos permisos que se pueden aplicar para cada SID en la ACL no son únicamente los que vemos en las propiedades de la carpeta, si entramos en opciones avanzadas y allí en permisos – agregar veremos como podemos indicar otro tipo de permisos.



- el permiso Recorrer carpeta permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas).
- El permiso Atributos de lectura permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS..
- El permiso Atributos de escritura permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.
- El permiso Leer permisos permite o impide que el usuario lea permisos del archivo o de la carpeta, como Control total, Leer y Escribir.
- El permiso Tomar posesión permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

Un permiso muy especial es el de Control Total. Si este permiso se lo otorgamos a un usuario en una carpeta, este usuario podrá eliminar cualquier cosa que haya en esa carpeta, incluso si le denegamos el permiso de eliminación en esos recursos. Hay que tener mucho cuidado al conceder este permiso.

También podemos gestionar las ACL desde shell de texto, con la instrucción XCACLS.EXE que viene incluida en las herramientas de soporte del cd de Windows XP (se ha debido instalar al mismo tiempo que instalamos whoami). También es posible usar la orden CACLS que es prácticamente igual que CACLS, aunque un poco menos potente.

Usando xcacls al mismo tiempo que runas, podemos crear carpetas usando varios usuarios, modificar sus permisos, etc. Si esto mismo lo hacemos abriendo y cerrando las distintas sesiones nos ocupará mucho más tiempo.

Veamos como se usa esta orden mediante un pequeño ejercicio.

1) Creamos un usuario desde shell de texto con nombre Nami y contraseña 1234.

```
NET USER NAMI 1234 /ADD
```

2) Creamos un usuario desde shell de texto con nombre Zoro y contraseña 1234.

```
NET USER ZORO 1234 /ADD
```

3) Lanzamos un shell de texto usando la cuenta de usuario Nami. (A partir de aquí todo lo realizaremos desde este shell, usando la cuenta Nami).

```
RUNAS /USER:NAMI CMD
```

4) Creamos una carpeta TESORO. (Puede que nos tengamos que ir al raíz para tener permisos para crear carpetas).

```
MKDIR TESORO
```

5) Visualizamos los permisos de dicho carpeta, su ACL.

```
XCACLS TESORO
```

6) Indicamos con xcacls que añadimos al usuario Zoro a la ACL de la carpeta, con permisos de lectura.

```
XCACLS TESORO /G ZORO:R /E
```

7) Comprobamos que se han modificado los permisos.

```
XCACLS TESORO
```

8) Le quitamos a los Administradores los permisos sobre esta carpeta.

```
XCACLS TESORO /R ADMINISTRADORES /E
```

9) Comprobamos que se han modificado los permisos.

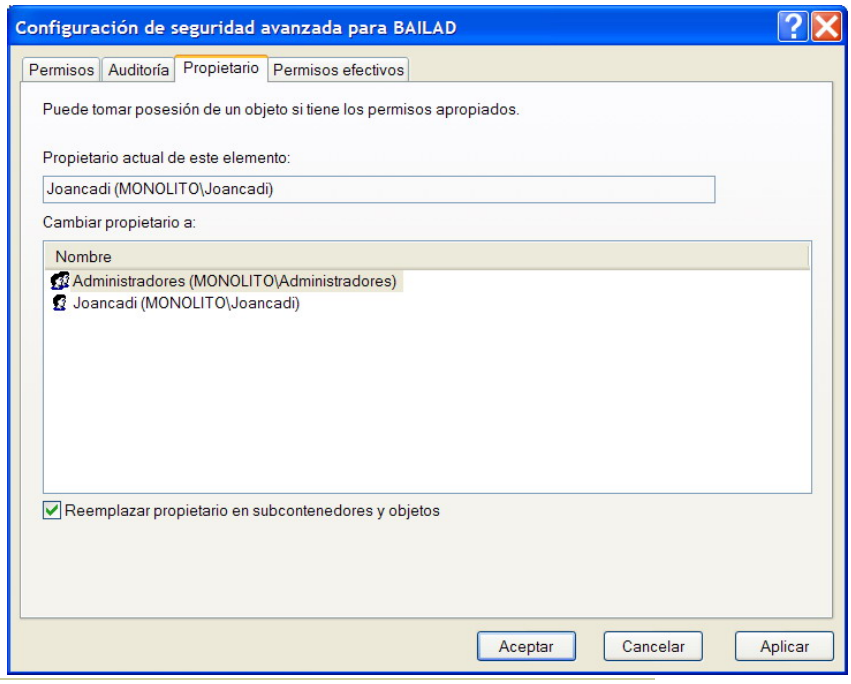
```
XCACLS TESORO
```

Lo último que vamos a ver sobre las ACL es el concepto de Creator Owner. El propietario de un recurso es aquel usuario que creó el recurso, y este propietario siempre tiene el poder ultimo sobre el recurso. No importa que dicho usuario desaparezca de su ACL, o incluso que se le deniegue el acceso al recurso; su propietario siempre podrá modificar su ACL.

Uno de los principales poderes del Administrador del sistema (y de hecho, de cualquier miembro del grupo Administradores) es que puede tomar posesión de cualquier recurso. Es decir, que el Administrador puede indicarle a cualquier recurso que él es el creador o propietario del recurso, por lo que pasa a tener todos los poderes sobre el mismo.

Para conseguir esto, tenemos que entrar en las opciones avanzadas de la pestaña Seguridad del recurso, y allí irnos a la pestaña Propietario.

Veremos como aunque no tengamos ningún permiso sobre el recurso, desde esta pestaña podemos indicar que el propietario del recurso será el grupo Administradores (recomendado antes que asignar el propietario al usuario individual), bastará entonces actualizar las propiedades del recurso para ver como pasamos a tener todos los poderes.



Como ejercicio, cread un usuario nuevo en el sistema, abrid sesión como dicho usuario (o usar runas), crear una carpeta cualquiera y configurad su ACL para que únicamente el usuario nuevo tenga algún permiso sobre dicha carpeta. Abrid sesión ahora como un miembro del grupo de Administradores y conseguid acceder a la carpeta, para por ejemplo crear un archivo dentro. (Tendremos que tomar posesión de la carpeta para el grupo Administradores, y posteriormente modificar su ACL para insertar nuestra cuenta con permisos de escritura).

1.4 Recursos Compartidos.

En el punto anterior hemos visto como podemos modificar las ACL de los recursos para que sean usadas por los usuarios y grupos LOCALES, es decir, aquellos que residen en nuestra propia maquina.

Vamos a ver ahora como modificamos esas ACL para permitir el uso por parte de usuarios y grupos que no pertenecen a nuestra propia maquina, sino que van a entrar en nuestro sistema a través de la red.

Windows presenta dos posibilidades a la hora de usar una red, trabajar en lo que se conoce como grupo de trabajo en la que todas las maquinas son iguales en derechos y obligaciones (red entre pares, o peer to peer) o bien trabajar en una red centralizada, donde existe una maquina que ejecuta un rol de control sobre las demás y que corre un sistema operativo servidor como Windows 2003 (Dominio).

Dejaremos el tema de cómo trabajar en un Dominio para los apuntes sobre Windows 2003, y nos centraremos ahora en los grupos de trabajo.

Obviamente para poder trabajar en un grupo de trabajo, debemos tener nuestro Windows XP bien configurado para trabajar en red. Para ello comprobad que:

1) Aseguraros que en propiedades de red, estáis usando una conexión TCP/IP, y que se encuentra en ella configurada una dirección IP valida, una mascara de red, una puerta de enlace y un servidor DNS correctos. (Panel de control – Conexiones de Red – Propiedades de nuestra conexión – Propiedades de TCP/IP).
2) Aseguraros que vuestra maquina tiene un nombre descriptivo, y que estáis trabajando en el mismo grupo de trabajo que el resto de vuestros compañeros. (Propiedades de Mi PC – Nombre de Equipo)
3) Aseguraros que no estáis corriendo ningún cortafuego que impida el acceso a vuestra maquina desde la red. En el caso de usar el cortafuegos incorporado en Windows XP, aseguraros que esta permitida la comparición en red. (Panel de Control – Centro de Seguridad).

Para comprobar si hemos metido bien los datos podemos usar la orden IPCONFIG, que nos muestra nuestros valores de configuración en la red.

```
IPCONFIG
```

Para asegurarnos que estamos en red, podemos utilizar la orden PING, que envía paquetes a una dirección IP y nos responde si dichos paquetes llegan a su destino y vuelven sin problemas.

```
PING Dirección-IP-destino
```

Si todas las maquinas responden al PING, sabemos que al menos la red TCP/IP esta trabajando sin problemas.

Por favor, huid siempre que sea posible de acceder a la red desde el explorador de archivos. Es un sistema que precisa para su buen funcionamiento un servidor WINS en la red, y si este no existe es un procedimiento enormemente lento y engorroso. Mucho mejor el PING para comprobar si estamos conectados. (Windows usa su propio protocolo para compartir recursos en un grupo de trabajo, este protocolo es conocido como NetBios y usa un localizador para encontrar los nombres de las maquinas conocido como Wins. Si estamos en un Dominio, el protocolo usado es únicamente TCP/IP y el localizador es DNS).

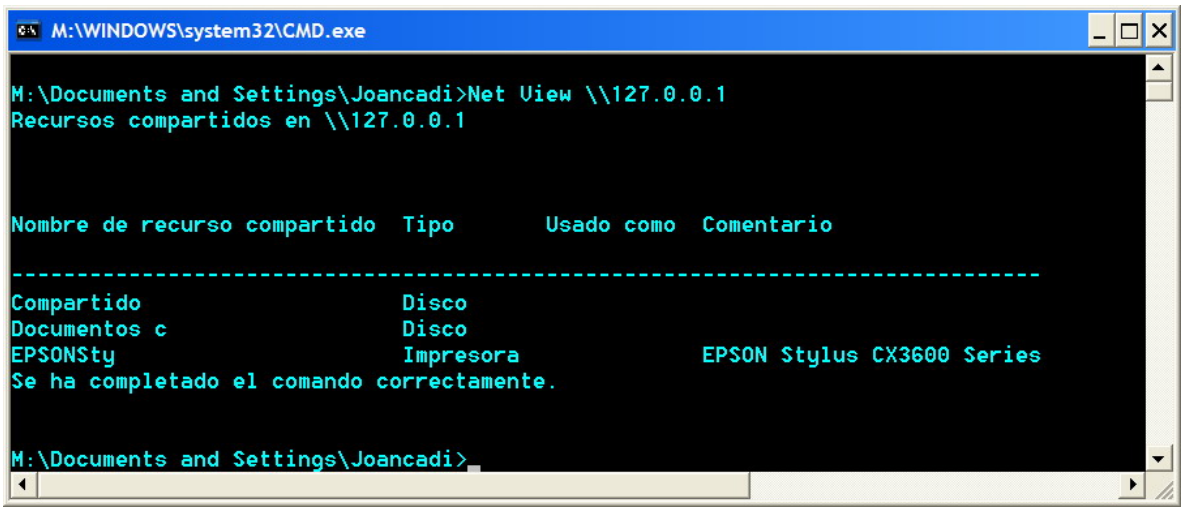
Una vez que estamos en red, podemos intentar acceder a las otras maquinas de la red para comprobar si están compartiendo algún tipo de información en la red, e intentad acceder a el.

Para ver los nombres de las maquinas NetBios que son conocidas por nuestro sistema en la red, escribid la orden NET VIEW.

```
Net View
```

Es probable que la unica maquina que podamos ver sea la nuestra, esto es asi por que estos son nombres NetBios y no estamos usando un servidor Wins. Podemos forzar a Net View a que busque una maquina en concreto para mostrarnosla:

```
Net View \\Nombre_Maquina
Net View \\Dirección_IP_remota
```



Podemos ver como Net View (en este caso la dirección IP es 127.0.0.1 que se conoce como localhost, es decir, nuestra propia maquina) nos muestra que recursos compartidos tiene esa maquina en la red, y de que tipo son. Esos son los recursos a los que podemos acceder de forma "normal".

Es posible que en este punto ya no funcionen algunas cosas… vayamos por partes:

- Si al hacer un net view \\127.0.0.1 (localhost) nos dice que no hay entradas en lista, es evidente que no estamos compartiendo nada. Compartid alguna carpeta (propiedades de carpeta, compartir) y comprobadlo de nuevo.
- Si aun compartiendo cosas, somos incapaces de ver nada, comprobad de nuevo el estado del cortafuegos (Panel de Control – Cortafuegos – Excepciones – Compartir).

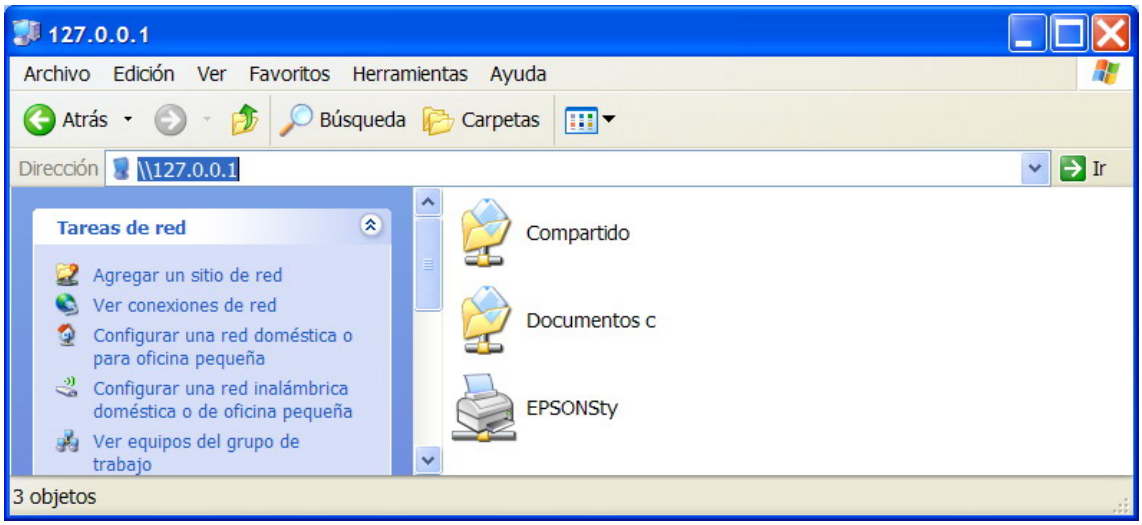
- Comprobad que vuestra configuración IP es correcta, dirección IP, mascara de red, etc.
- Comprobad que el cable de red esta correcto, que tenéis conexión a Internet, etc.

Obviamente, para acceder a un recurso desde la red, debemos recibir autorización. Es decir, al igual que vimos en el punto anterior, el usuario que intenta usar el recurso debe estar incluido en la ACL del recurso.

Asi, es seguro que si intentamos acceder directamente a otro equipo con Net View recibiremos el error 5 probablemente, acceso denegado. Esto es asi por que el equipo remoto no nos autoriza a ver sus contenidos compartidos. Esto es asi por que Windows XP no permite por defecto que alguien entre por la red al equipo si no se autoriza, mediante un nombre de usuario y contraseña correctos.

Al igual que usamos Net View para ver lo que un equipo comparte, podemos hacerlo desde el explorador de archivos. Para ello, iros al explorador y escribid en su barra de direcciones

```
\\Nombre_Maquina
\\Dirección_IP_remota
```



Vemos como obtenemos el mismo resultado que desde Net View, pero de forma gráfica (Por favor, intentad no entrar en esa opción de Ver equipos del grupo de trabajo, os reitero que es lenta, engorrosa y genera errores).

Esta maquina nos ha dado permiso por que es la nuestra, claro (127.0.0.1, localhost) pero ¿que ocurre si le damos la dirección de otra maquina?

Pensemos un poco…. El equipo remoto al que queremos conectarnos tiene sus recursos, con sus ACL y demás como vimos anteriormente. De repente ve como un usuario intenta acceder, autorizarse, pero no desde el equipo local (con su SID y demás) sino desde la red. Es obvio que en este ambiente no se pueden usar las SID (recordar que la SID incluye dentro un numero aleatorio que depende de cada equipo, por lo que una maquina no reconoce los SID normales de otra maquina).

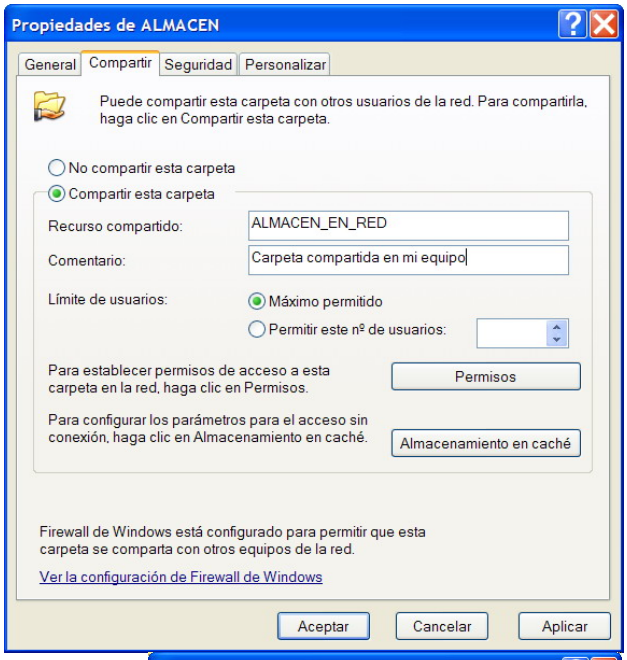
Asi que la maquina remota a la que intentamos acceder, insiste en autorizarnos, y lo hace de la siguiente forma:

1) Comprueba el nombre de usuario y la contraseña que esta usando en su maquina el usuario que intenta colarse por la red. Si ese **nombre de usuario y contraseña coinciden** con un **nombre de usuario y contraseña locales** de la propia maquina, supone que es el usuario indicado y le deja pasar.

2) En caso de que el punto 1 no se cumpla, comprueba si en la maquina que intenta entrar esta **activa la cuenta de Invitado** y el sistema esta configurado para permitir que se use la cuenta Invitado para red, y los permisos de red y la seguridad del recurso también lo permiten.

3) Si no se cumplen el punto 1 ni 2, aparece una pantalla como la indicada arriba que pregunta directamente un nombre de usuario y contraseña para entrar en el equipo.

Un punto importante que hay que conocer: Una vez que un equipo nos deja acceder al mismo nos concede una credencial, esta credencial no se borra inmediatamente, sino que es recordada en el equipo durante un tiempo. Esto es importante saberlo por que podremos encontrarnos con un equipo que nos concede el paso, borramos la cuenta que permite ese paso, y sin embargo al volver a probar resulta que seguimos entrando sin problemas. Simplemente ocurre que las credenciales siguen estando activas, aunque la situación que las genero haya desaparecido. Para actualizar estas credenciales la forma más segura es reiniciando el equipo.



Recursos compartidos mediante cuenta local.

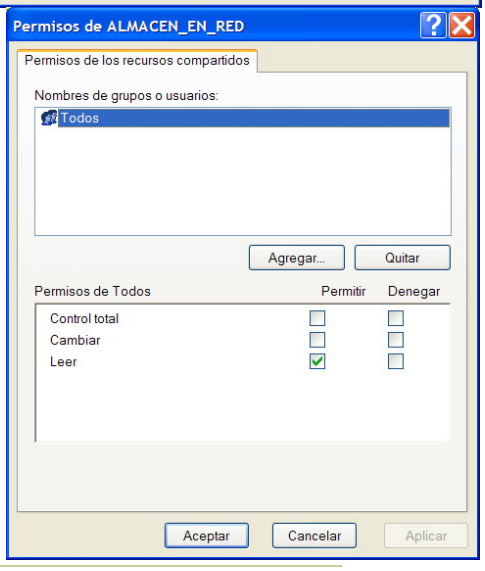
Bien, creemos una carpeta y compartámosla en red, para ir viendo punto por punto como se realiza esta acción.

1) Creamos un usuario en nuestro sistema con el nombre RINO y contraseña 1234.

2) Cread una carpeta ALMACEN en la raíz de vuestro volumen.

3) Accedemos a sus propiedades y a la pestaña Compartir. (Si no se ve esta pestaña, es que tenéis activado la opción de uso compartido simple de archivos y habrá que desactivarla (Mi PC – Herramientas – Opciones de Carpeta – Ver – ultima opción).

4) Allí indicamos que queremos compartir el archivo, le ponemos un nombre y un comentario, y entramos en la opción de Permisos. Esta opción será la que nos indique que usuarios pueden entrar desde la red a dicho recurso.



5) Agregamos al usuario RINO en Permisos, con control total.
6) Accedemos a la pestaña Seguridad de ALMACEN. Añadimos al usuario Rino con todos los permisos (No es suficiente con añadir al usuario en Permisos, también hay que añadirlo en Seguridad).
7) Ahora que le hemos concedido al usuario RINO el derecho a entrar en la carpeta ALMACEN, nos situamos en otro ordenador.
8) Creamos la cuenta RINO con contraseña 1234
9) Abrimos sesión con dicha cuenta RINO en esa maquina.
10) Desde shell de texto escribid lo siguiente (vale el nombre de la maquina o su dirección IP):

```
Net View \\Nombre_Maquina_donde_esta_Almacen
```

Deberiamos ver el recurso compartido ALMACEN_EN_RED

Escribimos:

```
Net Use X: \\Nombre_Maquina_Almacen\ALMACEN_EN_RED
```

Si lo hemos realizado todo bien, con esto veremos que tenemos un nuevo volumen en el sistema, con la letra X y que corresponde al recurso compartido.

11) Para hacer lo mismo desde el explorador, escribid en la barra de direcciones del explorador \\Nombre_Maquina_Almacen
12) Hacemos click con el botón derecho en la carpeta ALMACEN_EN_RED y escogemos la opción conectar a unidad de red, con lo que crearemos otro volumen para dicho recurso en nuestro sistema.
13) Si escribimos directamente \\Nombre_Maquina_Almacen\ALMACEN_EN_RED accederemos al recurso, sin crear ninguna letra de volumen.

Veremos como accedemos usando la cuenta del usuario RINO, ya que le hemos dado los permisos necesarios, tanto en permisos como en seguridad.

Si queremos que esos volúmenes (X) que hemos creado se conecten automáticamente cada vez que iniciemos sesión, añadimos el parámetro /persistent:yes desde shell de texto en el net use, o bien indicamos volver a conectar si lo hacemos desde el explorador.

```
Net Use X: \\Nombre_Maquina_Almacen\ALMACEN_EN_RED /persistent:yes
```

Si queremos borrar la asociación del recurso con la letra, basta con escribir NET USE * /DELETE y los borrara todos. (Si solo queremos uno, en lugar de * poned su nombre).

Recursos compartidos y acceso anónimo.

Hasta aquí hemos visto como acceder usando una cuenta de usuario común en los dos equipos. Veamos ahora como podemos activar el acceso de usuarios anonimos usando la cuenta Invitado. Esto nos permitirá ofrecer recursos compartidos en red para que pueda usarlo cualquier maquina sin preocuparnos de las cuentas locales que dicha maquina tenga.

Para ello, realizamos lo siguiente:

1) Compartimos un recurso en nuestra maquina.

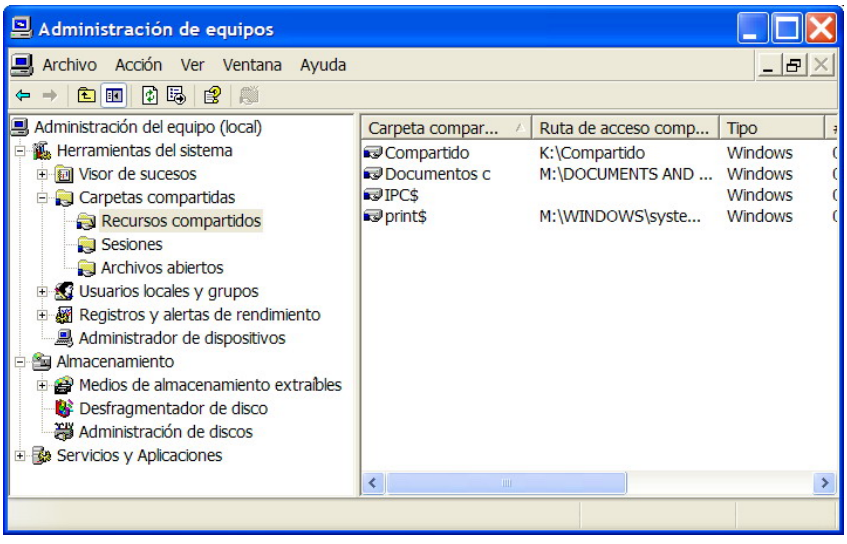
2) Nos aseguramos de que la cuenta Invitado esta activa.
3) Accedemos a secpol.msc para tocar algunas directivas de grupo que deben ser cambiadas para permitir el acceso anónimo de usuarios:
4) Desde directivas locales – Asignación de derechos de usuario:
    a. Denegar el acceso desde la red a este equipo. Nos aseguramos que la cuenta Invitado no esta incluida en esta directiva.
    b. Tener acceso a este equipo desde la red. Nos aseguramos que la cuenta Invitado esta incluida en esta directiva.
5) Desde directivas locales – Opciones de seguridad.
    a. Acceso de red: deja los permisos de Todos para aplicarse a usuarios anónimos. Si la habilitamos, basta con que en permisos al compartir agreguemos el grupo Todos. Si esta deshabilitado el grupo Todos no incluye la cuenta Invitado, por lo que habrá que agregar específicamente la cuenta Invitado.

Con estos pasos, conseguiremos un sistema en el cual, si compartimos un recurso, en sus propiedades en permisos indicamos que puede ser usada por Todos y en su seguridad incluimos el usuario Invitado, cualquier usuario de la red podrá entrar en el recurso con los permisos que indiquemos para la cuenta Invitado. Esto se conoce como acceso anónimo.

Modificando otras directivas de grupo, es posible crear otros esquemas de compartición y trabajo en red, pero este es uno de los más útiles y simples, ya que permite recursos nominales y recursos anónimos.

La forma de crear un recurso compartido oculto en Windows es muy simple, basta con terminar el nombre de dicho recurso con el símbolo $. Asi, si creamos una carpeta VIDEOS y la compartimos en red con AVI$, dicha carpeta no será visible ni con Net View ni desde el explorador, sin embargo dicho recurso se podrá usar sin ningún problema indicando su nombre completo \\Equipo\Avi$.

De hecho, Windows comparte de forma predeterminada TODOS nuestros volúmenes completos, con los nombres C$, D$, etc. Estos recursos compartidos se usan desde la Administración de sistemas, y no deben ser desactivados. Esta forma de trabajar es muy cómoda, puesto que un Administrador siempre podrá acceder a sus equipos desde red, sin tener que compartir implícitamente ningún recurso.



Si queremos ver nuestros recursos compartidos, incluidos algunos ocultos, lo podemos hacer desde la consola COMPMGMT.MSC.

Desde esta consola también podemos ver las sesiones abiertas por usuarios remotos en nuestro equipo (e incluso desconectar dichas sesiones y también podemos

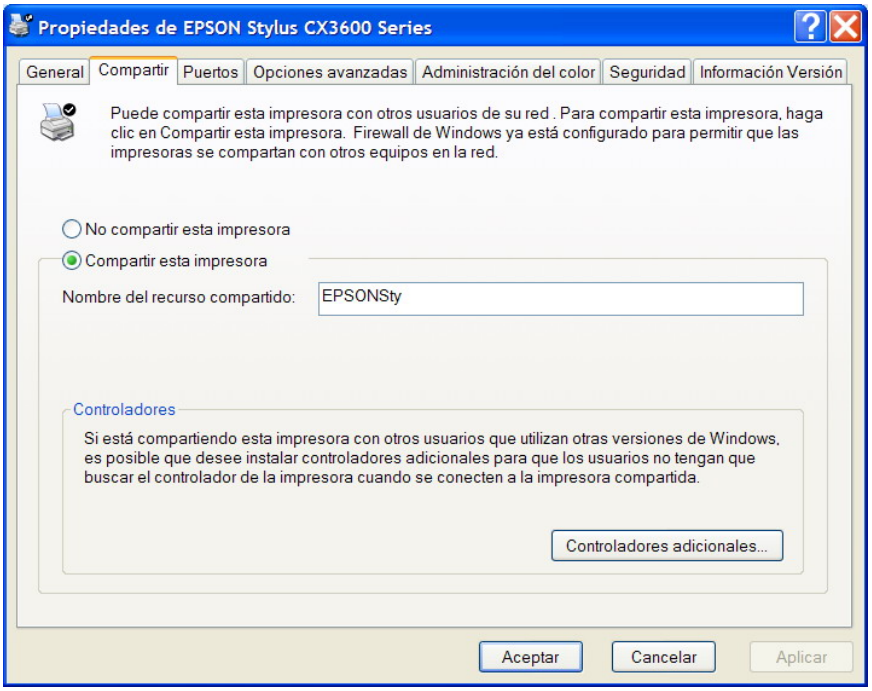
ver que archivos están abiertos por dichas sesiones).

El recurso compartido IPC$ es un recurso utilizado para funciones avanzadas de Administración de sistemas.

Recursos compartidos. Impresoras.

Compartir una impresora es prácticamente igual que compartir una carpeta. Basta con que accedamos a nuestra impresora (Inicio – Impresoras y Faxes, o bien accedemos desde Panel de Control), y en sus propiedades indiquemos compartir.

Desde esta opción podemos compartir la impresora, indicar un nombre de recurso compartido, y podemos instalar en nuestro sistema controladores adicionales. Estos controladores permiten que cuando una maquina remota quiera acceder a nuestra impresora no tenga que instalar ningún driver (controlador) adicional, sino que se los bajara automáticamente desde nuestra propia maquina.



Recursos compartidos. Ejercicios.

Se propone ahora un ejercicio completo sobre compartición de recursos.

a) Crear la cuenta de usuario PAVO.

b) Crear una carpeta en el raíz de nuestro volumen con nombre AVE.

c) Preparad dicha carpeta para que el usuario PAVO pueda acceder desde la red (para lo cual tendrá que abrir sesión como PAVO en una maquina remota) y tenga permisos totales sobre dicha carpeta.

d) Probad que efectivamente el usuario PAVO puede entrar desde otra maquina a la carpeta AVE. Preparad dicha maquina para que de forma predeterminada cada vez que el usuario PAVO abra sesión en dicha maquina se conecte a la carpeta AVE y la muestre como unidad Y:

e) Crear en el primer equipo una carpeta en el raíz de nuestro volumen con nombre P2P.

f) Preparad dicha carpeta para que cualquier usuario de cualquier maquina pueda acceder desde la red a la carpeta P2P, con permisos de solo lectura.

g) Cread un fichero de texto en la carpeta P2P, ahora comprobad que desde cualquier maquina de la red y desde cualquier usuario se puede conectar a la carpeta P2P del primer equipo y se puede leer el fichero de texto.

1.5 Perfiles de Usuario.

Un perfil de usuario contiene todas las características y ficheros que forman parte de entorno de trabajo de un usuario. Esto incluye los parámetros especiales de ese usuario en el registro del sistema para multitud de aspectos, desde el aspecto del cursor del ratón, a la forma en que configura el Word, las cookies que utiliza, los favoritos de Internet, sus carpetas de documentos, accesos directos a carpetas de red, etc.

Por defecto, cada usuario que inicia sesión en nuestra maquina cuenta con un perfil de usuario, que se crea cuando dicho usuario inicia sesión por primera vez en nuestra maquina. Los perfiles de usuario locales se almacenan bajo la carpeta DOCUMENTS AND SETTINGS que se crea en el mismo volumen donde instalamos Windows XP, y en una carpeta con el nombre de la cuenta del usuario. Podemos usar la variable de entorno %SystemDrive% que indica en que volumen se instaló Windows XP. La variable %UserName% nos devuelve el nombre de usuario actual, con lo que nuestro perfil estará almacenado en %SystemDrive%\Documents And Settings\%UserName%. Toda esta ruta esta también almacenada en una variable de entorno que es la de %UserProfile%.

Dentro de cada perfil de usuario, encontramos una jerarquía de directorios o carpetas. El raíz de dicho perfil (es decir, la carpeta dentro de Documents And Settings que tiene como nombre el nombre del usuario) contiene un fichero NTUSER.DAT, que contiene la porción de información del registro del sistema inherente a dicho usuario. Dentro del perfil se incluyen las siguientes carpetas:

- Datos de programa. Esta carpeta oculta contiene datos específicos para programas, comos los diccionarios de los procesadores de textos, bases de datos de los CDs, certificados de Internet Explorer, etc. La información que se almacena en esta carpeta depende de los programas.
- Cookies. Esta carpeta contiene las cookies del Internet Explorer. (Galletas, pequeños ficheros de textos usados por las páginas Web para proporcionar diversos servicios).
- Favoritos. Los favoritos del Internet Explorer.
- Configuración Local. Esta carpeta oculta contiene configuraciones y ficheros que no se mueven con el perfil del usuario, bien por que sean específicos de la maquina local o por que sean excesivamente grandes y no merezcan la pena ser mantenidos junto con el perfil. Por ejemplo, aquí se encuentran los históricos de Internet Explorer, los ficheros temporales del mismo, etc.

- Mis Documentos. Esta carpeta es la que realmente se usa, cuando en cualquier programa almacenamos algo en la carpeta Mis Documentos. Así, si en un programa almacenamos algo en Documentos de Ana, por ejemplo, lo estamos almacenando en la carpeta Mis Documentos del perfil Ana. Si almacenamos algo en Mis Documentos directamente, lo estamos almacenando en la carpeta Mis Documentos del perfil del usuario actual.
- Entorno de Red. Tenemos aquí los accesos directos que aparecen en Mis sitios de Red.
- Impresoras. Tenemos aquí accesos directos a impresoras y faxes.
- Documentos Recientes. Accesos directos a los últimos documentos con los que hemos trabajado.
- Send To. (Enviar a) Esta carpeta contiene accesos directos a las carpetas y aplicaciones que aparecen en el menú contextual de un objeto en el explorador de archivos, bajo la opción Enviar a. Podemos añadir en esta carpeta, nuevos destinos para nuestros programas y documentos.
- Menú Inicio. Esta carpeta contiene los objetos personales (como accesos directos a aplicaciones y documentos) que vemos aparecer en el Menú Inicio.
- Plantillas. Tenemos aquí accesos directos a plantillas de documentos. Estas plantillas son usadas por el comando Nuevo en el explorador.
- Escritorio. Tenemos en esta carpeta los accesos directos que se muestran en el escritorio del usuario.

Perfiles comunes.

En la carpeta de perfiles (%SystemDrive%\Documents And Settings) podemos encontrar dos perfiles que no están asociados a ninguna cuenta de usuario en particular. Estos son All Users (Todos los usuarios) y Default User (Usuario por defecto). La carpeta Default User está oculta.

- Perfil All Users. El contenido de este perfil, se añade a los contenidos de los perfiles de cada usuario. Por ejemplo, si ponemos algún acceso directo en All Users\Escritorio, este acceso le aparecerá a todos nuestros usuarios en sus escritorios. Por defecto, solo los administradores pueden añadir objetos al escritorio y al menú inicio del perfil All Users. Sin embargo, todos los usuarios pueden añadir objetos en la carpeta de documentos compartidos.
- Perfil Default User. Cuando un usuario inicia sesión en nuestro sistema por primera vez (y no tiene un perfil móvil u obligatorio), Windows crea un nuevo perfil local para dicho usuario, copiando el contenido de la carpeta Default User a una nueva carpeta con el nombre del usuario. Por lo tanto, podemos configurar los perfiles de nuestros nuevos usuarios, modificando el contenido de la carpeta Default User. Por defecto, solo los administradores pueden hacer cambios en esta carpeta.

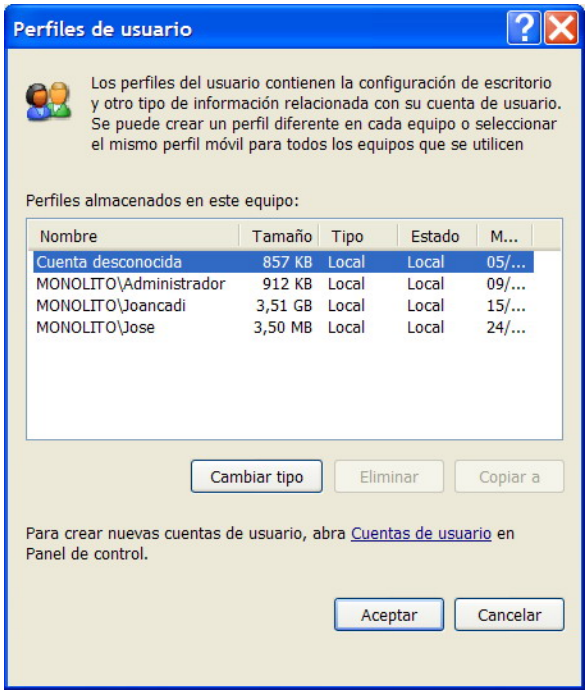
Es interesante conocer bien el funcionamiento de estos perfiles especiales, ya que pueden simplificar enormemente la vida a los administradores. Podemos, por ejemplo, incluir enlaces directos a las páginas Web de la empresa, a documentos donde se expliquen las características de seguridad que se han de seguir, etc.

Hay que tener cuidado con un error que se suele cometer con los permisos de los ficheros al usar estos perfiles. Si **copiamos** un fichero a la carpeta de perfil para Default User, este fichero obtiene los permisos de la carpeta. Sin embargo, si **movemos** un fichero a la carpeta de perfil para Default User, este fichero conserva sus permisos propios. Esto hace que si como administrador creamos un fichero y lo movemos a la carpeta Default User (o a cualquier carpeta en realidad) este fichero nos pertenecerá a nosotros, y es muy probable que el usuario no tenga permiso ni siquiera para verlo.

Gestionando Perfiles.

Una vez comprendido que es un perfil y donde se encuentran ubicados, es tentador para un administrador gestionarlos directamente desde el explorador de archivos, copiarlos, borrarlos, etc.

Sin embargo, esta no es una práctica recomendada, ya que se corre el riesgo de dejar perfiles inutilizables. De hecho, salvo las carpetas escritorio y menú inicio, las demás carpetas no deben ser modificadas desde el explorador de archivos.



Para gestionar estos perfiles, debemos usar el formulario de perfiles de usuario que XP incorpora. Para llegar a este formulario debemos ir al formulario Sistema (Panel de Control – Sistema o Propiedades de Mi PC) y allí Opciones Avanzadas – Perfiles de Usuario: Configuración.

Los miembros que no sean miembros del grupo Administrador no podrán ver otros perfiles diferentes al suyo, y no pueden modificar ningún perfil. No se puede gestionar un perfil que tenga sesión abierta en el sistema.

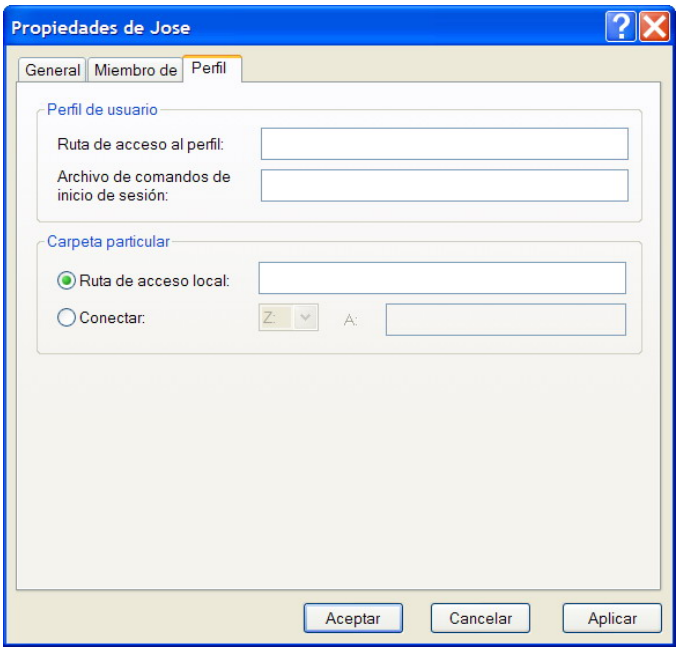
Desde aquí podemos borrar perfiles dejando el registro del sistema actualizado, copiar perfiles de un usuario a otro y cambiar el tipo de dicho perfil, pasándolo de local a móvil, etc.

El concepto de cambiar tipo de local a móvil, etc, lo veremos con posterioridad.

Asignando Perfiles.

Normalmente, cuando creamos una nueva cuenta de usuario su perfil se crea automáticamente la primera vez que dicha cuenta de usuario inicia sesión en nuestro sistema (es ese rato largo que se llevan las nuevas cuentas en las que aparece en pantalla algo como aplicando su configuración personal). Sin embargo, como Administrador del sistema podemos asignar directamente un perfil a una cuenta de usuario. Para ello debemos usar la consola LUSRMGR.MSC. Si desde allí escogemos un usuario y hacemos doble clic, veremos como nos aparecen las propiedades de dicho usuario, y tenemos una pestaña para gestionar su perfil.

Desde este formulario, podemos configurar lo siguiente:



- Ruta de acceso al perfil. Si no queremos que el perfil este localizado en su ubicación por defecto, podemos indicar aquí donde queremos que se cree dicho perfil. Hay que tener en cuenta que el usuario que use el perfil debe tener derechos totales sobre dicha carpeta. De esta forma veremos como podemos crear tres tipos distintos de perfiles: locales, móviles y obligatorios.
- Archivo de comandos de inicio de sesión. Aquí podemos colocar el nombre y localización de un fichero de comandos (Script) que se ejecutará cada vez que el usuario inicie sesión.
- Carpeta particular (Home). Ruta de acceso local. La carpeta particular (Home) es una carpeta en la que el usuario puede almacenar sus ficheros y programas. Aunque la mayoría de los programas usan la carpeta Mis Documentos para almacenar los ficheros del usuario, podemos necesitar crear una carpeta alternativa para dicho usuario. Si hemos creado un Script de inicio de sesión para el usuario, su directorio por defecto inicial es esta carpeta Home. Aquí indicamos en que directorio de nuestro sistema hemos creado la carpeta para dicho usuario.
- Carpeta particular (Home). Conectar. Desde aquí podemos indicar una carpeta particular para ese usuario, e indicar una letra de volumen para que dicha carpeta sea referenciada.

El Script de inicio de sesión, es un programa que se ejecuta automáticamente cada vez que el usuario inicia sesión en nuestra maquina. Cualquier fichero ejecutable (bat, cmd, vbs, js, wsf, exe, com,..) puede ser usado como Script de inicio. Normalmente estos scripts se pueden utilizar para conectarnos a sitios de red, para iniciar ciertos programas de control, etc. Este es simplemente uno de los sitios donde podemos obligar a las cuentas de usuario a ejecutar un programa, en XP tenemos varios lugares más desde donde hacer esto. Podemos obligar a que se ejecuten programas cuando un usuario inicia sesión, cuando la cierra, cuando se enciende el sistema, cuando se apaga, a intervalos de tiempo, a horas programadas, etc.

Toda esta gestión de perfiles que hemos visto, solo funciona adecuadamente si estamos unidos a un dominio. En un ámbito de grupo de trabajo, no es recomendable trabajar con perfiles que no sean locales.

Tipos de perfiles.

Windows admite tres tipos distintos de perfiles.

- Perfiles de usuarios locales. Son los que se almacenan en %SystemDrive%\Documents And Settings en el disco duro local. Si un usuario cambia algo en su perfil, esos cambios solo se registran en nuestra maquina local, como es obvio. Es el único tipo de perfil usado si no estamos en un dominio.

- Perfiles de usuario móviles. Estos perfiles no se almacenan en el disco duro local de la maquina, sino en un servidor de red. Esto implica que esos perfiles están disponibles para los usuarios sin importar en que maquina abran sesión, siempre que dichas maquinas tengan acceso a ese servidor. El perfil se encuentra almacenado en un servidor, de modo que al iniciar sesión se copia dicho perfil a la maquina en la que se encuentre el usuario. Si el usuario modificar algo del perfil, dichos cambios son introducidos también en el servidor. Estos perfiles móviles pueden ser utilizados si contamos con un servidor en la red que cuente con Windows Server (2000, 2003, etc).
- Perfiles de usuario Obligatorios. Estos perfiles solo pueden ser cambiados por los administradores. Inicialmente, es igual que un perfil de usuario móvil, ya que el perfil se encuentra almacenado en un servidor, y se crea una copia de dicho perfil en la maquina en la que el usuario inicia sesión. Pero a diferencia el perfil móvil, los cambios que el usuario efectué en su perfil no se copian en el servidor. Es decir, aunque el usuario puede cambiar su perfil una vez abierta sesión, la próxima vez que inicie otra sesión verá que no se han almacenado ninguno de los cambios que ha introducido. Una ventaja de los perfiles de usuario obligatorios, es que pueden ser usados por múltiples usuarios sin que se afecten los unos a los otros. Obviamente, el administrador si puede modificar estos perfiles como le parezca.

Todo este tema de perfiles esta pensando principalmente para trabajar en un dominio, usando un servidor Windows donde estén almacenados dichos perfiles. Intentar trabajar con ellos en un ámbito de grupo de trabajo es altamente desaconsejable.

1.6 Directivas de Grupo.

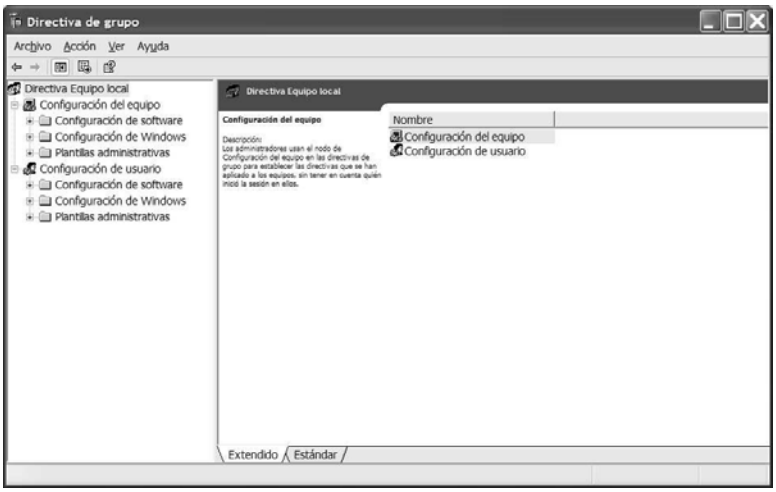
Las directivas de grupo forman parte de la estructura de Windows 2000, Windows XP y Windows 2003. En estos sistemas, las políticas de grupo son una herramienta muy poderosa que permite a los administradores configurar equipos de forma local o remota, instalando aplicaciones, restringiendo los derechos de los usuarios, eliminando aplicaciones, instalando y ejecutando scripts, y redirigiendo carpetas del sistema a red o viceversa. Pero también tienen utilidad las políticas de grupo en entornos pequeños, incluso en una sola maquina. Usando las políticas de grupo en una maquina corriendo Windows XP, podemos:

- Modificar políticas que se encuentran en el registro del sistema. El registro del sistema es una gran base de datos en la que se configuran cientos de comportamientos de Windows XP. Desde las políticas de grupo podemos acceder a estas características y modificarlas, de una forma mucho más simple que mediante la edición pura del registro.
- Asignar scripts que se ejecutaran automáticamente cuando el sistema se encienda, se apague, un usuario inicie sesión o cierre sesión.
- Especificar opciones especiales de seguridad.

Si estamos trabajando bajo un dominio (con un servidor en la red administrando dicho dominio) las políticas de grupo cobran mayor protagonismo. En un ambiente de grupo de

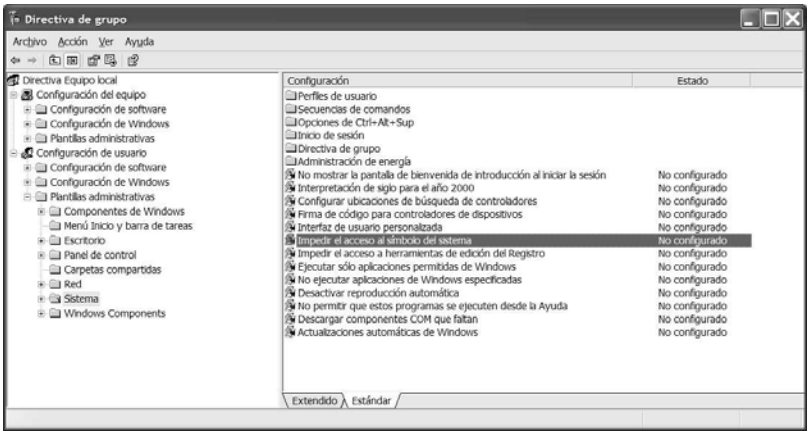
trabajo, las políticas de grupo de cada maquina, controlan los aspectos únicamente de dicha maquina y en algunos casos es imposible sacarles el rendimiento esperado.

La consola desde donde podemos gestionar las directivas de grupo es el gpedit.msc. (Inicio – Ejecutar – gpedit.msc).



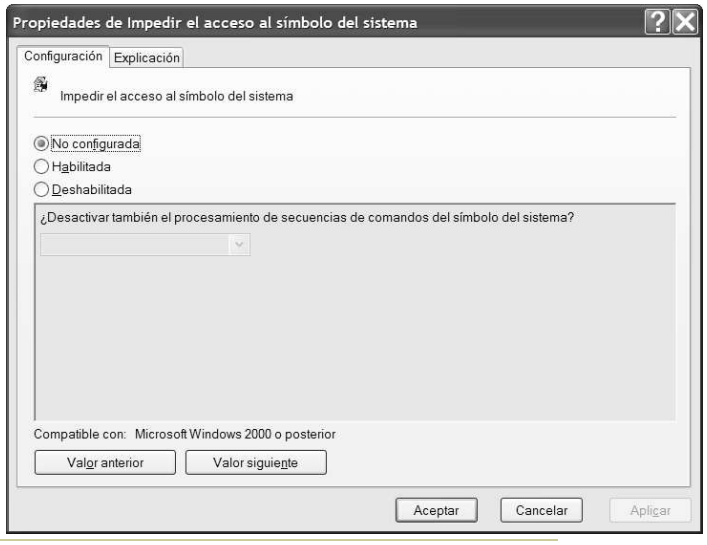
Para poder trabajar con el gpedit.msc necesitamos estar usando una cuenta de usuario que pertenezca al grupo Administradores. Esta consola es muy configurable, permitiéndonos añadir y quitar opciones según deseemos. De momento, vamos a trabajar con las opciones que aparecen por defecto.

Si nuestro equipo esta unido a un dominio, podemos configurar directivas del dominio completo, que afectaran a varias maquinas. Sin embargo, nos vamos a centrar aquí en las directivas locales, ya que no estamos trabajando en un dominio de momento.



Principalmente, veremos que dentro las directivas de grupo locales tenemos dos opciones: Configuración del equipo y Configuración del usuario. En el caso de estar trabajando en grupo de trabajo es prácticamente indistinto trabajar con una opción u otra.

La mejor forma de comprender que podemos hacer desde esta herramienta, es ir leyendo todas las posibles configuraciones que nos permiten las directivas de grupo. Contamos con más de 240 configuraciones que podemos perfilar para la configuración del equipo, y más de 440 configuraciones o directivas que podemos asignar para los usuarios. Obviamente, la gran mayoría de estas directivas pueden ser ignoradas por su escasa utilidad.



Para aprender más de una directiva en concreto, simplemente tendremos que seleccionarla con el ratón, y veremos una descripción detallada de dicha directiva en el panel central.

Algunas directivas aparecen tanto en la

configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.

Para modificar el estado o configuración de una directiva, simplemente tenemos que realizar doble clic sobre dicha directiva para que nos aparezca el cuadro de dialogo que nos permite modificar dicha directiva. Si en dicho cuadro de dialogo pulsamos sobre la pestaña Explicación, nos mostrará una explicación de la funcionalidad de dicha directiva.

Si escogemos la pestaña Configuración, veremos como podemos:

- **No configurar la directiva**, con lo que se comportará según el criterio por defecto para dicha directiva.
- **Habilitarla**, con lo que la pondremos en marcha en el sistema.
- **Deshabilitarla**, con lo que impediremos que se ponga en marcha dicha directiva.

Algunas directivas especiales permiten especificar otras informaciones.

Hay que tener cuidado en leer muy bien la directiva y su explicación antes de modificarla, ya que podemos entender justo lo contrario de lo que hace. Por ejemplo, si habilitamos la directiva que deshabilita el contenido extra en el escritorio, estamos deshabilitando dicha opción. (¿Esta claro, no?).

Probad a deshabilitar la directiva que hemos tomado como ejemplo (gpedit.msc – Configuración de Usuario – Plantillas Administrativas – Sistema - Impedir el acceso al símbolo del sistema) e intentad ejecutar una ventana de símbolo de comandos (cmd.exe)

Como ejercicio, probad a habilitar la directiva (gpedit.msc – Configuración de Usuario – Plantillas Administrativas – Sistema – No ejecutar aplicaciones de Windows especificadas) e insertar en la lista de aplicaciones prohibidas el solitario de Windows (sol.exe) y el block de notas Windows (notepad.exe). Probad a ejecutar cualquiera de estos programas.

Vemos como desde las directivas de grupo podemos modificar el comportamiento de Windows, dándonos una gran potencia en la administración del equipo.

Ahora bien, habremos notado que cuando activamos directivas de grupo, tanto desde configuración del equipo, como desde configuración del usuario, estas directivas se aplican a todos los usuarios, incluidos nosotros mismos. Esto esta bien si lo que queremos es proteger una maquina de un ciber, por ejemplo, pero si estamos en una maquina que usamos normalmente nos interesa buscar un método que nos permita "saltarnos" las directivas.

Para conseguir esto, tenemos que tener en cuenta lo siguiente:

- Las directivas de grupo se almacenan en una carpeta de nuestro sistema, concretamente en la carpeta %SystemRoot&\System32\GroupPolicy.
- Cada vez que un usuario inicia sesión en nuestro equipo, el usuario lee automáticamente las directivas que encuentre en dicha carpeta
- Todas las directivas que son leídas desde dicha carpeta se aplican al usuario que acaba de entrar en el sistema.

¿Teniendo en cuenta lo anterior, se os ocurre alguna manera de impedir que las directivas se apliquen, por ejemplo, a los miembros del grupo Administradores?

Es bastante simple, basta con impedir que los usuarios del grupo Administradores puedan leer dicha carpeta. Es decir, modificamos los permisos de seguridad de la carpeta donde están las directivas, %SystemRoot&\System32\GroupPolicy de modo que impidamos que los Administradores tengan permiso de lectura. (Aquí usamos por primera vez la entrada DENEGAR de los permisos).

Cerrar sesión y volver a abrirla como un usuario del grupo Administradores. Podremos comprobar como a dicho usuario ya no se le aplican las directivas, dado que no puede leerlas.

De este modo, podemos conseguir que las directivas del sistema no se nos apliquen, pero si nos damos cuenta, al denegarnos a nosotros mismos los permisos sobre la carpeta GroupPolicy, estamos consiguiendo también que sea imposible que modifiquemos las directivas de grupo. Esto implica que siempre que vayamos a modificar una directiva de grupo tendremos que tomar el control sobre la carpeta GroupPolicy, para poder leer y escribir en ella antes de poder modificar la directiva, y una vez que hayamos modificado la directiva, volver a quitarnos el permiso de lectura sobre dicha carpeta. Todo esto lo tenemos que hacer sin cerrar sesión, ya que podemos correr importantes riesgos en caso contrario.

Esta complejidad de los permisos sobre GroupPolicy vienen dados por que en cierta forma estamos "forzando" el uso de las directivas, que están pensadas para trabajar generalmente en un dominio, y no en un grupo de trabajo.