Tema 3

Windows NT

Cuentas de usuario

Para que cualquier usuario pueda acceder a un dominio NT es necesario que un administrador del dominio le asigne una cuenta de usuario. Todas las cuentas de usuario y sus datos asociados (de los que hablaremos en esta sección) se almacenan en la base de datos de usuarios (SAM). La creación de las cuentas de usuario se realiza mediante el Administrador de Usuarios para Dominios (Figura 1). En los siguientes apartados veremos los elementos de que consta una cuenta y que el administrador debe configurar.

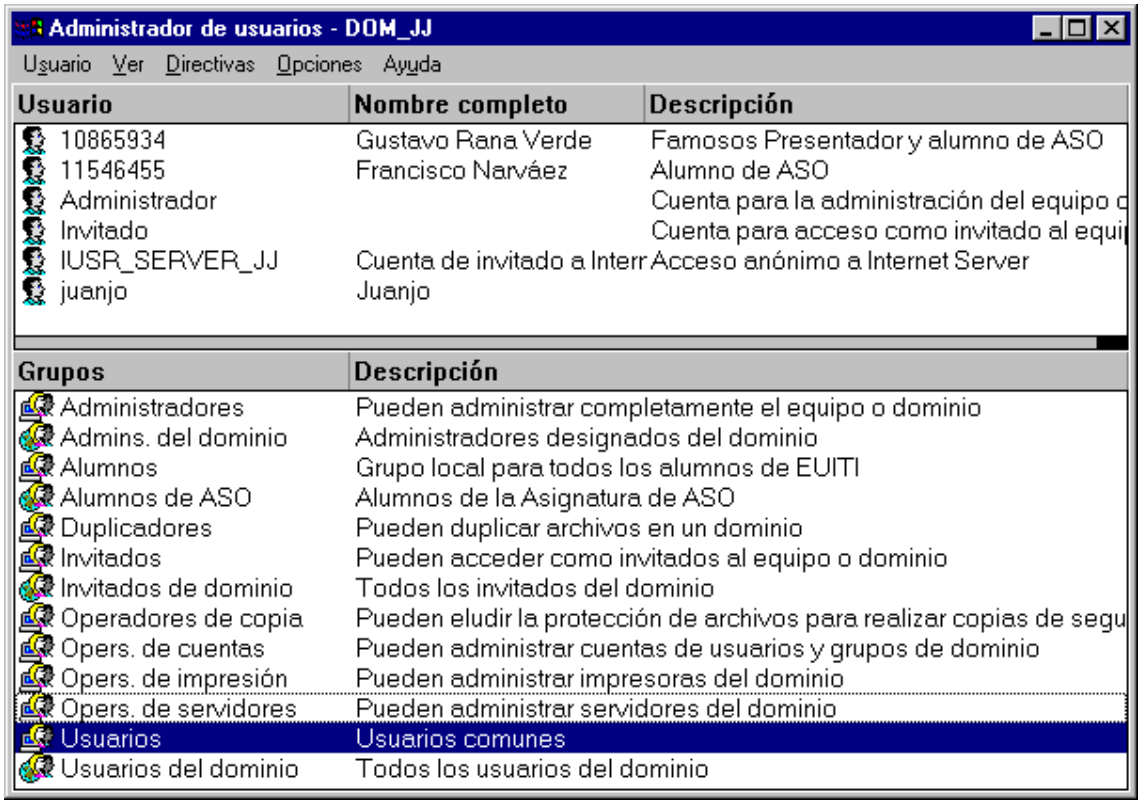


Figura 1 Administrador de Usuarios para Dominios

Crear y definir una cuenta de usuario

Para crear una cuenta de usuario se emplea el comando Nuevo Usuario que nos muestra la ventana de la Figura 2. A través de esa ventana se introducen los datos que permiten configurar una cuenta de usuario y que vamos a detallar en los siguientes apartados.

Nombre de usuario

Lo mínimo que se debe indicar para crear una cuenta de usuario, es el nombre que se le va a dar. Este nombre debe ser único dentro del dominio. Será el nombre que el usuario empleará para conectarse al sistema. Debe ser una cadena de caracteres de hasta 20 caracteres y en la que no pueden usarse los siguientes caracteres:

/ \ [ ] : ; | = , + * ? < >

Este nombre sólo tiene importancia de cara al usuario. Internamente NT usa un identificador único para cada usuario, este identificador es el SID (Security Identifier). El SID se crea a partir de tres elementos: el nombre del equipo en el que se crea, la fecha y hora de creación y el propio nombre que se le da al usuario. Esto garantiza que dos cuentas nunca tengan el mismo SID. Aunque volviéramos a crear una cuenta con el mismo nombre el SID sería distinto. El SID se emplea en la lista de Control de Acceso (ACL Access Control List) que determina los permisos de los usuarios sobre cada recurso.

Para la creación de los nombres de usuarios se debe seguir un método que garantice que a dos usuarios no se les da el mismo nombre. Alguno de los métodos que se pueden utilizar son los siguientes:

- **Utilizar el propio nombre o el apellido.** Por ejemplo, Juan, Paula o Felipe. El problema de este criterio es que es muy fácil que dos usuarios coincidan en su primer apellido o nombre. Sólo es válido en organizaciones muy pequeñas.
- **Nombre + Inicial del apellido.** JuanF, PaulaG o FelipeH. Este método provocaría menos colisiones que el anterior pero seguirían existiendo.
- **Inicial del nombre + Primer apellido.** JFernandez, PGonzalez, FHernandez. Tiene la misma probabilidad de coincidencia que el anterior.
- **Iniciales. JFS, PGP, FHA.** El problema de esta nomenclatura es que es más difícil reconocer de que usuario se trata, los nombres completos o los apellidos son más descriptivos.
- **Valor numérico (Hash).** Asignar a cada usuario un número que lo identifique. En este caso las coincidencias son imposibles, pero la representatividad del nombre es nula.

Nombre completo

Esta información es únicamente descriptiva de cara al administrador. De todas formas es importante ser rigurosos y anotar el nombre completo del usuario al que se le asigna la cuenta, sobre todo por motivos documentales.

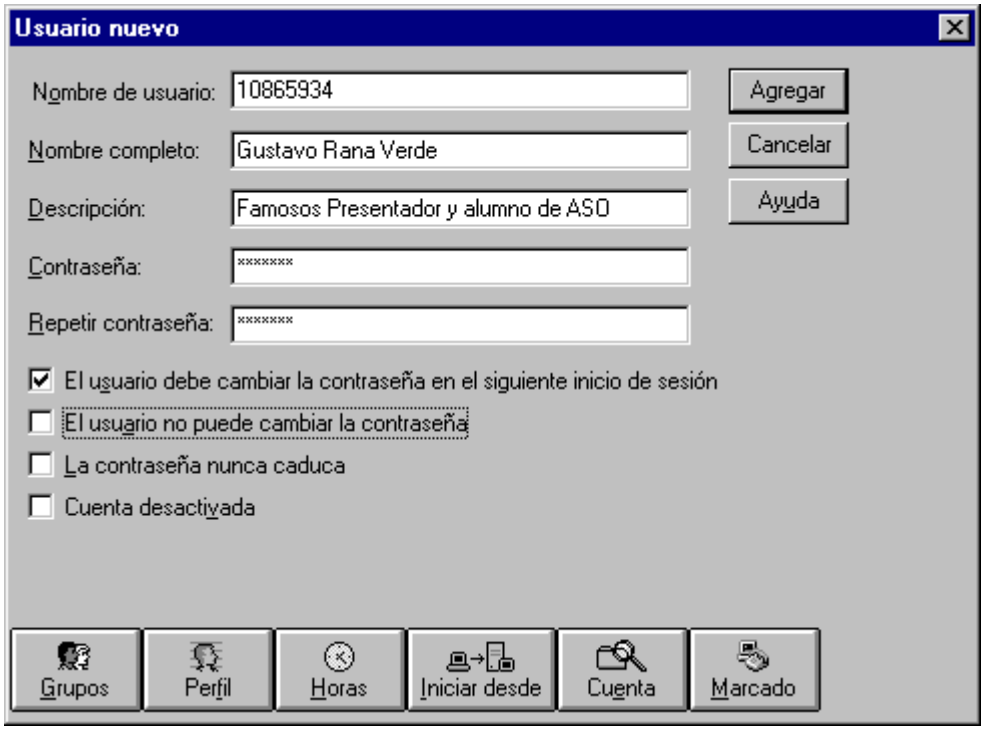


Figura 2 Crear una nueva cuenta de Usuario

Contraseña

Es la palabra secreta de acceso o password que utilizará el usuario para conectarse al sistema y que le sirve de garantía para que nadie acceda a su cuenta y sus datos. La palabra

de paso no la debe conocer ni el Administrador, aunque bien es cierto que la puede cambiar. Las palabras de paso pueden tener hasta 14 caracteres y se diferencia entre mayúsculas y minúsculas. Se guardan encriptadas y se usan de forma encriptada cuando se realiza la auntentificación en el login de un usuario. Alguna de las cosas que se pueden configurar de las palabras de paso son:

- **El usuario debe cambiar la contraseña en el siguiente inicio de sesión.** Cuando se marca esta opción, se fuerza a que el usuario cambia su palabra de paso la siguiente vez que entre en el sistema. Suele ser una opción que se marca siempre que se crea una cuenta, el administrador pone la primera password y deja que el usuario elija la que él desee la primera vez que se conecte. Por ello esta opción está seleccionada por defecto. Se suele utilizar para fijar passwords temporales.
- **El usuario no puede cambiar la contraseña.** Si seleccionamos esta opción el usuario no podrá cambiar su password. Por defecto no está fijada. Se suele marcar por ejemplo en la cuenta de Invitado, ya que esta cuenta debe ser común para los usuarios invitados del sistema y no es lógico permitir el cambio de la contraseña de esta cuenta.
- **La contraseña nunca caduca.** Cuando se marca esta opción la contraseña nunca "muere". El valor por defecto para esta opción es Falso para las nuevas cuentas. Sólo se debe emplear para cuentas comunes y no críticas, como por ejemplo la cuenta de Invitado. Otra cuenta que tiene esta opción marcada es la de Duplicador, ya que de esta forma se previene que los servicios de replicación dejen de funcionar simplemente porque la contraseña de la cuenta se hubiera extinguido.

Cuenta desactivada

Este campo sirve para deshabilitar una cuenta temporalmente. La cuenta seguirá existiendo en la SAM, pero el usuario no podrá conectarse al sistema con esa cuenta. Obviamente el valor por defecto para este campo en las nuevas cuentas es NO. Esta opción se suele utilizar cuando se crean plantillas que faciliten la posterior creación de cuentas. Las cuentas que se utilizan como plantillas se tienen deshabilitadas para evitar posibles usos fraudulentos de las mismas. La cuenta de Administrador no se puede deshabilitar, mientras que la cuenta de Invitado (en los NT Server, no así en NT Workstation) está inactiva por defecto.

Cuenta bloqueada

A diferencia de los campos anteriores, éste no puede ser fijado por el Administrador sino que las cuentas las bloquea directamente el sistema por determinadas circunstancias que así lo aconsejan. Por ejemplo, cuando un usuario teclea repetidamente mal su contraseña, el sistema bloquea la cuenta ya que esos errores seguramente los ha provocado un intruso al sistema. El Administrador no puede utilizar esta opción para bloquear una cuenta, tan solo la empleará para desbloquear cuentas bloqueadas, después de comprobar la causa por la que se bloqueo la cuenta[1].

Directorio particular

En este campo se indica el directorio que se asigna al usuario para que pueda guardar sus datos. En este directorio el usuario tendrá asignados todos los permisos. Para indicar este directorio hay que pulsar el botón Perfil (Figura 2). Aparecerá entonces la ventana de la Figura 3, donde indicaremos la ubicación exacta del directorio personal.

Puede ser local a la estación o estar situada en una de las unidades del servidor. Cuando se especifica un path de red se le asigna una unidad de red, lo que permitirá al usuario un acceso más rápido a su directorio (Z: en el ejemplo). Para los path de red se debe usar su nombre **UNC** (universal Naming Convention). El nombre UNC contiene el nombre de la máquina el nombre de la carpeta compartida[2] y el camino a partir de él hasta el fichero deseado. Por ejemplo

```
\\nombredelequipo\carpetacompartida\subdirectorios\fichero
```

[1] Si el Administrador desea bloquear una cuenta tiene que emplear la opción Cuenta Desactivada.

[2] Se pone el nombre con el que se comparte el recurso y no el nombre ni la unidad del directorio, aunque puede que coincidan

\\othello\Users\%USERNAME%

\\othello\Users\10865934

NT sustituye %USERNAME% por el nombre del usuario. Si el nombre del recurso compartido existe, NT crea automáticamente el directorio y asigna los permisos oportunos. El permiso que se asigna es Control Total para el usuario (véase sección Permisos en NTFS). Es habitual limitar el espacio en disco asignando una cuota que puede ocupar el directorio personal de los usuarios. Esta limitación previene que un usuario acapare para él un espacio excesivo de disco.

Login script

Similar a un fichero por lotes (bat) o programa ejecutable que se ejecuta cuando el usuario entra en el sistema. Estos ficheros suelen contener los comandos que configuran adecuadamente el entorno de trabajo del usuario (por ejemplo, mapeo de unidades de red). En NT la funcionalidad que tienen los login script las desempeñan los perfiles, aunque nada impide usarlos simultáneamente. La ubicación del login script también se indica desde el botón Perfil, es decir, se configura en la misma pantalla donde se establece el perfil y directorio particular (Figura 3).

Perfil

Fichero que contiene la descripción del entorno de trabajo del usuario. Dentro del perfil se incluyen los grupos de programas, colores de la pantalla, Menú Inicio, conexiones de red y todos los aspectos que definen el entorno de trabajo dentro de un sistema NT. Dada la importancia de los perfiles dentro de NT y las distintas variantes que tienen, dedicaremos una sección completa para describirlos exhaustivamente.

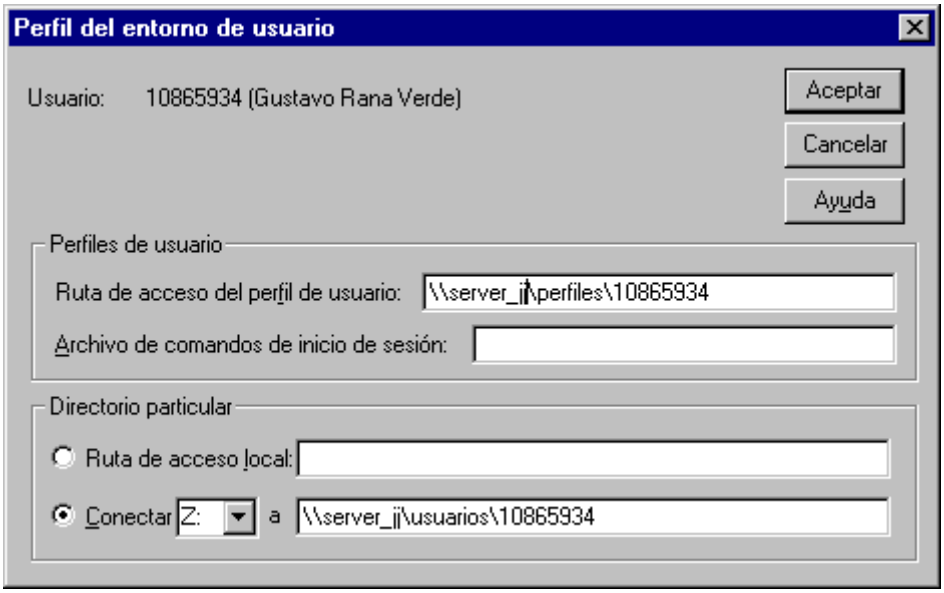


Figura 3 Directorio particular y perfil de un usuario

Tipo de cuenta

Una cuenta puede ser local o global. Las cuentas que habitualmente se crean son globales. Las cuentas locales se suelen utilizar en las siguientes situaciones:

- Permitir a usuarios de NT el acceso a servidores LAN Manager
- Permitir a usuarios de otros sistemas el acceso a Windows NT Server
- Permitir el acceso a aquellos usuarios que tienen sus cuentas globales en un dominio en el que no se confía o que no ejecuta NT Server.

Las cuentas locales permiten iniciar sesión desde una estación y pueden recibir derechos y permisos. Sin embargo, las cuentas locales de un dominio no se pueden usar en un dominio

que confíe en el anterior. Para indicar el tipo de cuenta y la caducidad de la misma se emplea el botón Cuenta en la ventana de configuración de la cuenta y nos muestra la ventana de la Figura 4. Lo normal es emplear cuentas globales, las locales son de poca utilidad.

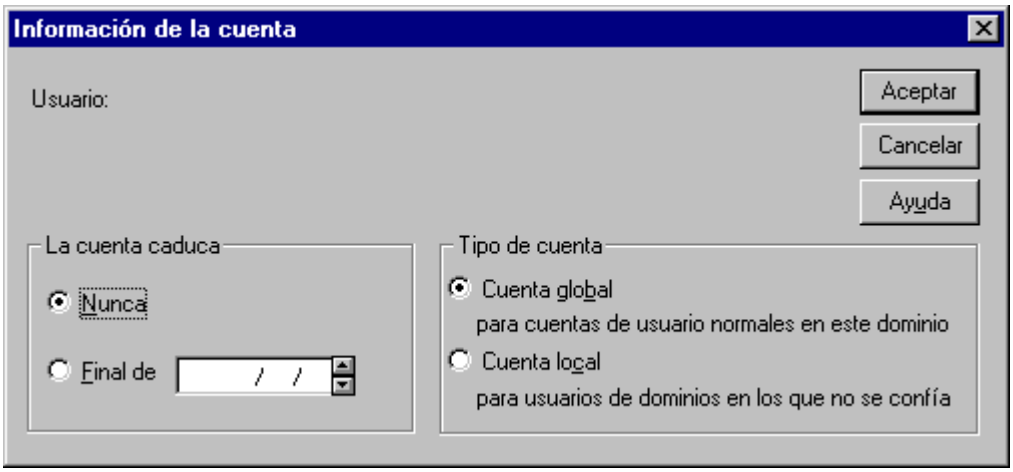


Figura 4 Tipo y caducidad de una cuenta de usuario

Horario de conexión

En esta sección se puede configurar las horas y los días de la semana en los que el usuario podrá acceder al sistema. Por ejemplo, los usuarios de una oficina puede tener permitido el acceso de Lunes a Viernes de 8 de la mañana a 7 de la tarde y tener prohibido el acceso fuera de esas horas. La granularidad mínima es de una hora y por defecto está permitido el acceso las 24 horas del los 7 días de la semana. Si el usuario trata de conectarse en horas en las que no le está permitido, su conexión dependerá de las directivas de seguridad del sistema (véase apartado sobre Directivas de seguridad).

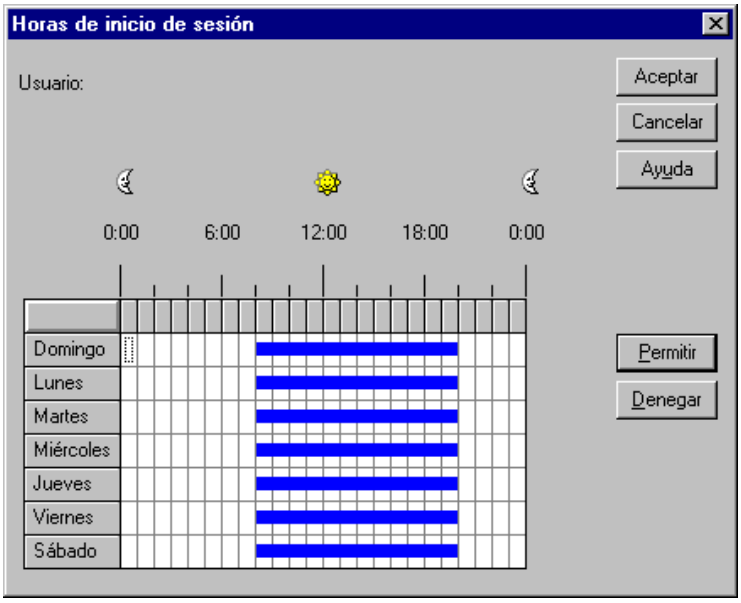


Figura 5 Horario de inicio de sesión

Estaciones de conexión

Aquí se indicarán la lista de estaciones desde la que el usuario podrá conectarse al dominio. Como máximo se pueden indicar 8 estaciones. Por defecto no existen restricciones, con lo que el usuario puede conectarse desde cualquier estación del dominio[3].

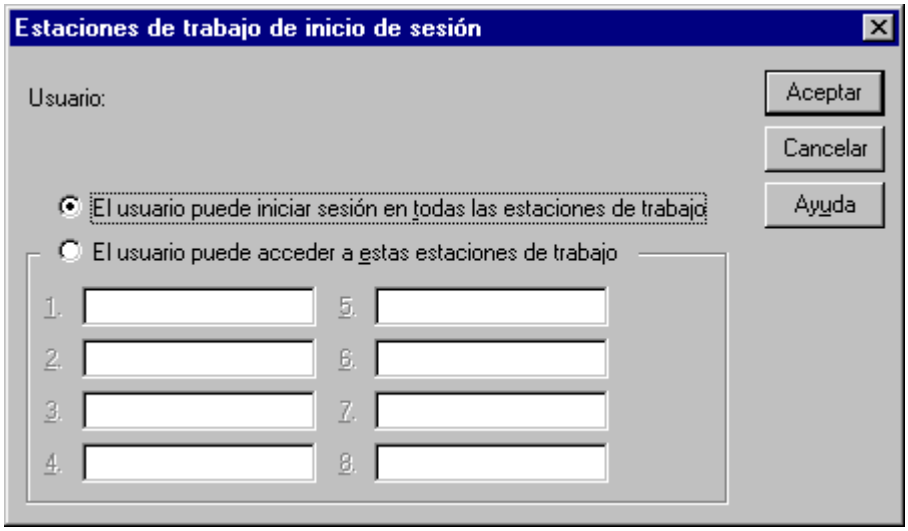


Figura 6 Estaciones desde las que el usuario puede iniciar sesión

Marcado

La opción de Marcado (Dialin) permite al usuario el acceso remoto al sistema. En este caso el administrador puede especificar cual será el método de "call back" o rellamada.

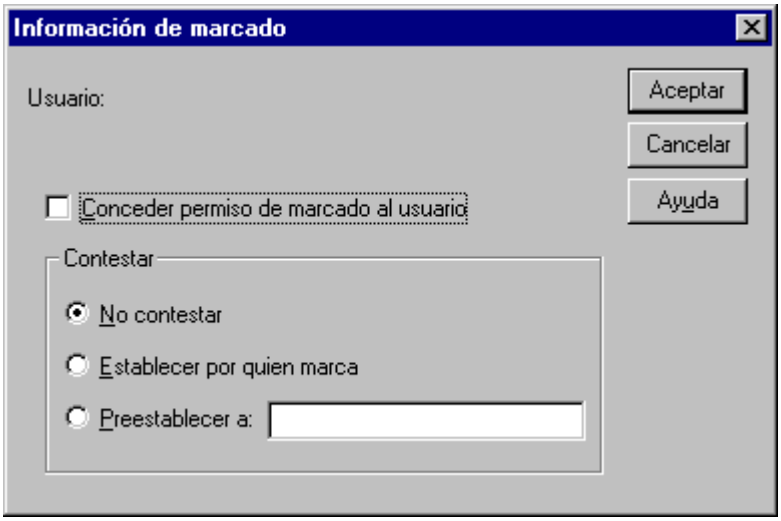


Figura 7 Información de marcado

- **No contestar (No call back).** Cuando el usuario llama, el controlador de dominio le solicita la cuenta y la contraseña. Si los datos son correctos, el usuario tendrá acceso al sistema. No se produce una rellamada. Es la opción por defecto.
- **Establecer por quien marca** (User defined call back). Cuando el usuario llama al sistema, éste le pregunta desde que número está realizando la llamada. Entonces el servidor hace un llamada a ese número y se inicia el proceso de conexión con la consiguiente petición de nombre de usuario y contraseña. Se emplea cuando los usuarios

[3] Ojo, no puede conectarse desde los controladores del dominio, a no ser que el usuario le otorgue explícitamente ese Derecho, véase Derechos de Usuarios.

no tienen un punto fijo para conectarse remotamente. Es una opción más segura que la anterior, pero menos que la siguiente.

- **Preestablecer a (Preset to).** Call back predefinida. El usuario llama y el sistema hace una rellamada a un número previamente predefinido y que debe corresponder con el número de teléfono desde el que se suele conectar el usuario. Es la forma más segura de acceso remoto, ya que para que un intruso pudiera acceder a la cuenta de ese usuario, no sólo tendría que saber la contraseña, sino que tendría que llamar desde el número de teléfono del usuario.

Fecha de expiración

En este campo se indica la fecha a partir de la cual la cuenta se deshabilitará automáticamente. Por ejemplo, en el caso de las cuentas de los alumnos en nuestra red, se puede indicar que las cuentas se deshabiliten al final de curso. Por defecto, ninguna nueva cuenta tiene fecha de expiración (Figura 4).

Grupos

Aquí habrá que indicar todos aquellos grupos de los que forme parte el usuario. Un usuario puede pertenecer simultáneamente a varios grupos. Las nuevas cuentas pertenecen por defecto al grupo Usuarios del dominio. Además de fijar la lista de grupos a los que pertenece el usuario se puede indicar cual es su grupo primario. El grupo primario, que debe ser un grupo global, se emplea cuando el usuario se conecta desde un Macintosh o cuando ejecuta aplicaciones POSIX. Nunca se puede borrar a un usuario de su grupo primario. Para hacerlo previamente hay que asignarle un nuevo grupo primario y luego borrarlo del primario anterior.

Para establecer la pertenencia a un grupo se emplea el botón Grupos. Nos aparecerá la ventana de la Figura 8 donde podremos Agregar todos los grupos a los que deba pertenecer el usuario. Si se observa la ventana, el usuario tiene un grupo primario que debe ser global.

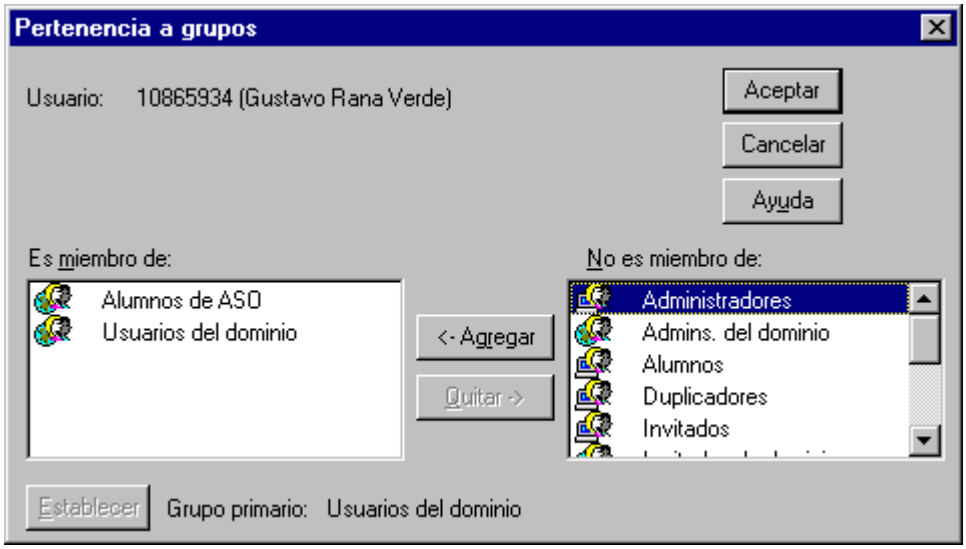


Figura 8 Grupos de un usuario

Borrado de una cuenta de usuario

Para borrar una cuenta de usuario, simplemente hay que seleccionar la cuenta que se quiere borrar y presionar la tecla *Sup*. Hay que tener en cuenta que cuando se borra una cuenta, aunque se cree una nueva con el mismo nombre, no tendrá los privilegios que hayamos asignado a la primera. Lo que identifica una cuenta es su SID (Security Identifier), no el nombre del usuario. Para advertirnos de ello, el sistema nos muestra el mensaje de error de la Figura 9. El borrado es una acción irreversible.

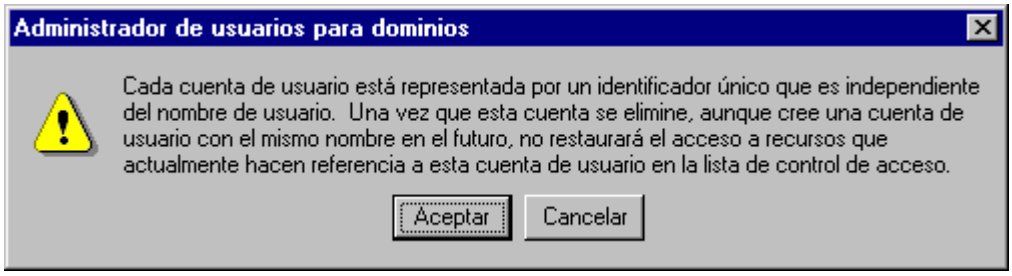


Figura 9 Aviso al borrar un usuario.

Cuentas predefinidas

Cuando se instala una máquina NT, ya sea en su versión servidor o estación, se crean ciertas cuentas predefinidas. En concreto se crean dos cuentas de usuario: Administrador e Invitado. Ambas cuentas pueden verse en la Figura 1.

Administrador

Es la cuenta del administrador del dominio y, por tanto, se emplea para realizar las tareas de administración. Es posible crear cuentas con los mismo privilegios que la cuenta de Administrador, y es incluso recomendable tener una cuenta adicional con privilegios de administrador y dejar la cuenta de Administrador en reserva. La cuenta de Administrador es especial y por ello no se puede borrar, aunque si se puede renombrar (no altera su SID). No está mal renombrar esta cuenta ya que previene el ataque contra intrusos. La cuenta de Administrador tiene las siguientes capacidades:

- Crear/borrar/editar cuentas de usuario y grupos (locales y globales).
- Asignar derechos y permisos a los usuarios.
- Bloquear el servidor y echarlo abajo.
- Formatear el disco duro del servidor.
- Gestión de perfiles.
- Compartir/dejar de compartir recursos (carpetas e impresoras).

Invitado

La cuenta de invitado tiene un conjunto de privilegios limitado y tiene un uso ocasional. Se suele utilizar cuando se necesita permitir el acceso a nuestro sistema a un usuario no habitual y que necesite realizar tareas muy básicas. Es una cuenta súper peligrosa y si se tiene habilitada hay que ponerle contraseña. Uno de sus peligros es que puede permitir conexiones si no tiene contraseña. Si por ejemplo un intruso se intenta conectar al dominio mediante una cuenta inexistente, el propio sistema tras denegar el primer acceso, trata de conectar al usuario mediante la cuenta de invitado y si ésta no tiene contraseña, el intruso podrá acceder al sistema. Por motivos de seguridad esta cuenta está deshabilitada por defecto en las versiones NT Server (sí se habilita en las Workstation). Por defecto no tiene contraseña, así que si se habilita hay que recordar ponerle su palabra de paso.

Grupos de usuarios

Es muy importante planificar cuidadosamente la administración de las cuentas de usuario y, sobre todo, planificar los grupos de usuarios que se necesitan crear. Los grupos de usuarios tienen como objetivo principal simplificar las labores de administración; es más sencillo y más rápido asignar permisos a un grupo de usuarios, que hacerlo de forma individual a cada uno de los usuarios que forman el grupo. El mantenimiento de los permisos y derechos de un grupo es más sencillo que el de varias cuentas de usuario. Generalmente usaremos los

grupos para administrar el acceso a los recursos (puestos, archivos, impresoras, etc.) y hacer más sencilla su gestión. Vamos a ver unos pequeños consejos:

- Es obvio que sobre el directorio personal de un usuario aplicaremos permisos específicos para dicho usuario (Control Total), pero si necesitamos que varios usuarios de distintos o de un mismo grupo accedan al mismo recurso es recomendable crear un nuevo grupo para tal fin, ya que un usuario puede pertenecer a varios grupos.
- Muchas veces creamos grupos utilizando el mismo esquema de nuestra empresa u organización, sin embargo también es aconsejable pensar en los grupos de usuarios en función de los recursos que van a necesitar.
- Cambiaremos los permisos proporcionados a un conjunto de usuarios utilizando la cuenta del grupo pero no modificaremos cada cuenta individualmente.
- Intentaremos aprovechar los grupos predefinidos de Windows NT, a los que se han asignado conjuntos de derechos y capacidades muy útiles.

Las ventajas que se derivan del uso de grupos son:

- Los permisos se pueden asignar/eliminar para todos los miembros del grupo.
- Si un usuario se elimina de un grupo, automáticamente pierde todos los permisos asignados al grupo.
- Si un usuario se añade a un grupo, automáticamente adquiere todos los permisos asignados al grupo.

En un dominio de Windows NT Server se pueden mantener dos tipos de grupos: grupos locales y grupos globales. La diferencia entre ambos se centra fundamentalmente en su ámbito de actuación. Para comprender las características de cada uno de ellos, vamos a analizarlos con detenimiento.

Grupos locales y globales

En NT existen dos tipos de grupos de usuarios: globales y locales. Las características de ambos tipos de grupos son las siguientes:

Grupo Global

Los grupos globales también se denominan grupos de dominio. Un grupo global contiene una serie de cuentas de usuario de un dominio que están agrupadas bajo un nombre de cuenta de grupo. Un grupo global sólo puede contener cuentas de usuario del dominio donde se creó. Se mantienen en el controlador primario de dominio y se replican de forma automática a los controladores secundarios.

Una vez que se crea un grupo global, se le puede asignar permisos y derechos en su propio dominio sobre estaciones de trabajo o servidores, o sobre dominios que confían. Su ámbito de actuación se extiende a todo el dominio, esto es, pueden recibir permisos para acceder a los recursos de todo el dominio. Sin embargo, lo mejor es asignar derechos y permisos a grupos locales, y usar el grupo global como método para agregar usuarios a grupos locales.

Los grupos globales se pueden agregar a grupos locales del mismo dominio, en dominios que confían en dicho dominio, o en servidores o estaciones que ejecuten Windows NT Workstation en el mismo dominio o en uno que confía. No se puede crear un grupo global en un equipo que ejecute Windows NT Workstation o en un equipo que ejecute Windows NT Server como servidor miembro.

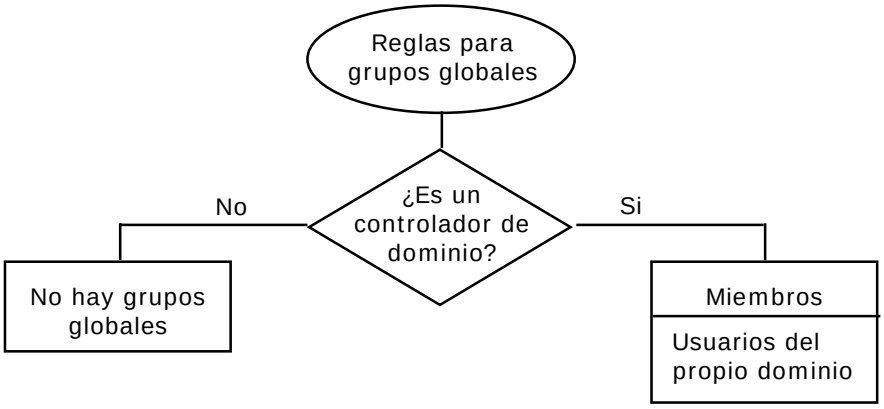
La palabra "globales" en "grupos globales" indica que el grupo está disponible para recibir derechos y permisos en múltiples dominios (globales). Un grupo global sólo puede contener cuentas de usuario; no puede contener grupos locales ni otros grupos globales.

Propiedades de los grupos globales

- Está formado únicamente por cuentas de usuario de un mismo dominio, del dominio en el que se crea.

- No puede contener otros grupos, ni locales[4] ni globales.
- El término global indica que el grupo puede recibir derechos y permisos para utilizar recursos de múltiples dominios, del dominio en el que se crea y de los dominios que confían en él.
- Puede formar parte de un grupo local.
- Se administran desde un controlador de dominio.

Lo forman	Usuarios globales del dominio
No lo forman	Grupos locales, usuarios locales, grupos globales, cuentas de otros dominios
Ámbito	Dominio local y todos los dominios que en él confían



Grupo Local

Un grupo local contiene cuentas de usuario y cuentas de grupo globales de uno o más dominios, agrupados bajo un nombre de cuenta de grupo. Los usuarios y los grupos globales de fuera del dominio local sólo se pueden agregar al grupo local si pertenecen a un dominio en el que se confía. Los grupos locales hacen posible la rápida asignación de derechos y permisos sobre los recursos de un dominio (es decir, el dominio local) a usuarios y grupos de dicho dominio y de otros dominios en los que se confíe.

Cuando un grupo de usuarios deba tener el mismo acceso a un recurso, entonces debe crearse un grupo que contenga a esos usuarios y asignar el permiso al grupo. Lo mismo ocurre si varios grupos globales necesitan tener los mismos permisos sobre un recurso, se pueden agrupar todos ellos en un grupo local y dar el permiso al grupo local. Al dar los permisos en el grupo local, automáticamente los heredan los usuarios que a él pertenecen, bien directamente, o indirectamente a través de su pertenencia a un grupo global que a su vez pertenezca al grupo local. La otra solución, asignar los permisos individualmente a los usuarios, provoca una sobrecarga de trabajo para el Administrador y hace que las lista de control de acceso para ese recurso sean más grandes.

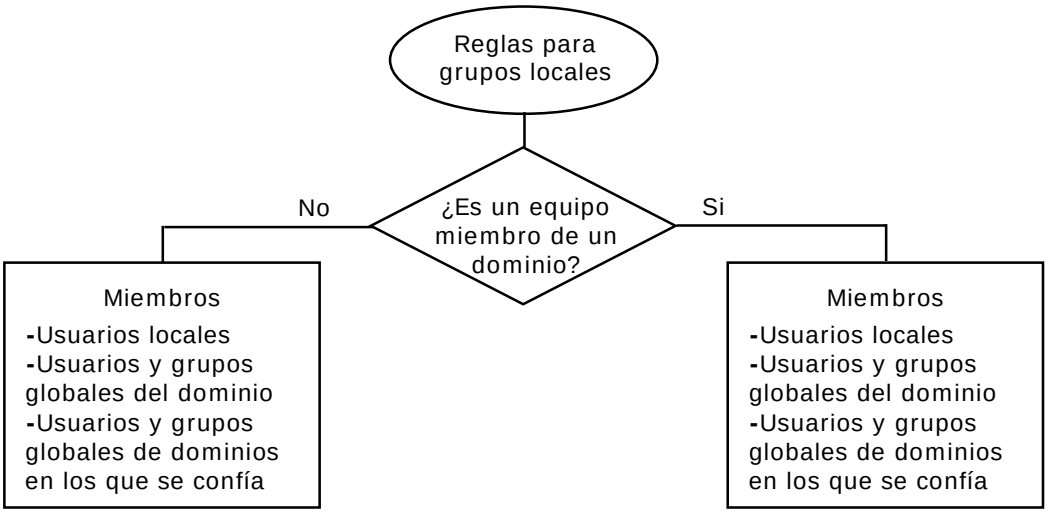
Los grupos locales también existen en servidores miembro y equipos que ejecutan Windows NT Workstation, y pueden contener cuentas de usuario y grupos globales. Un grupo local no puede contener otros grupos locales. La palabra "locales" indica que el grupo está disponible para recibir derechos y permisos localmente. Es decir, si se definen en una estación o un servidor NT, pueden recibir permisos en esa máquina. Si por el contrario se definen en un controlador de dominio, podrán recibir permisos sobre todos los recursos de ese dominio.

[4] Si un grupo global contuviera un grupo local o un usuario local, podría ocurrir que ese usuario local obtuviera permisos en recursos del dominio, violando la definición de usuario local, por la cual este tipo de usuarios sólo pueden recibir permisos sobre recursos locales.

Propiedades de los grupos locales

- Está formado por cuentas de usuario, grupos globales del dominio en el que se crea y de dominios en los que se confía.
- No puede contener otros grupos locales.
- El término local indica que el grupo sólo puede recibir derechos y permisos para utilizar los recursos del dominio o equipo en él que se crean.
- Se administran desde un controlador de dominio o un servidor miembro o estación.
- No puede ser miembro de ningún otro grupo.

Lo forman	Usuarios locales, grupos globales, usuarios del dominio o de dominios que confían y grupos globales de dominios que confían
No lo forman	Otros grupos locales
Ámbito	Recursos locales del equipo o dominio en el que se crean



Grupos locales de estaciones y del dominio

Al igual que pasa con las cuentas de usuario, también existen grupos locales en cada estación o servidor NT y grupos locales que pertenecen a todo el dominio. Los grupos locales de las estaciones NT se guardan en la SAM de las propias estaciones Esos grupos locales tendrán como ámbito de trabajo la propia máquina y no afectará a otras máquinas. Es decir, el grupo local de una estación no puede tener permisos sobre ningún recurso fuera del equipo en el que se definen. Los miembros que pueden formar parte de los grupos locales de las estaciones son:

- Cuentas de usuarios locales de la estación en la que son definidos
- Cuentas de usuarios y grupos globales del dominio al que pertenece la estación.
- Cuentas de usuarios y grupos globales de dominios en los que confía el dominio de la estación.

Los grupos locales del dominio tendrán como ámbito el dominio y se crean dentro del Administrador de Usuarios para dominios de los servidores NT. Los grupos locales del dominio podrán acceder a los recursos de los controladores del dominio, no a los de las estaciones NT. Pueden estar formados por:

- Cuentas de usuarios y grupos globales del dominio al que pertenece la estación.
- Cuentas de usuarios y grupos globales de dominios en los que confía el dominio de la estación.

Unos consejos

- Los grupos globales son la forma más eficiente de agregar usuarios a grupos locales.
- Es posible agregar grupos globales a grupos locales del mismo dominio, o de dominios que confían o a equipos con NT Workstation o NT Server que funcionen como servidores miembro del mismo dominio o de dominios que confían.
- Aunque un grupo global puede recibir derechos y permisos, es preferible conceder los derechos y permisos a grupos locales. Los grupos globales se emplearán para agregar sus cuentas a los grupos locales.

¿Qué tipo de grupo elegir?

- Si el grupo necesita operar en un solo dominio: **Local**
- Si el grupo tiene que contener usuarios de distintos dominios: **Local**
- Si el grupo tiene que contener otros grupos: **Local**
- Si el grupo necesita derechos y permisos de otro dominio: **Global**

Un ejemplo práctico

Como hemos dicho al principio, el dominio sirve para administrar de una manera lógica los recursos, servidores y estaciones de una red fácilmente. Por ejemplo, supongamos una facultad en la que hay departamentos: Informática y Economía. En cada departamento hay servidores, estaciones y recursos. Podemos crear un dominio por departamento. En cada departamento, elegiremos un servidor que actuará como PDC y donde se darán de alta los usuarios de ese departamento.

En el dominio del departamento Informática tenemos tres grupos globales: los Profesores, los Becarios y los Proyectantes, ya que identifican perfectamente los tres grupos de usuarios del dominio; sus responsabilidades y necesidades son distintas y tendrán distinto acceso a los recursos disponible. A la hora de dar de alta un nuevo usuario en el departamento, basta meterlo en el grupo correspondiente para que tenga los permisos por defecto de ese grupo. En el departamento de Economía sólo hay dos grupos globales: los Profesores y los Becarios.

Recientemente el Departamento de Informática ha adquirido una impresora Láser muy rápida para que los profesores puedan imprimir sus trabajos. ¿Cómo hay que proceder para asignar los permisos sobre esa impresora? Pues muy sencillo, se crea un grupo local Impresora_Laser y se le asignan los permisos oportunos para que sus miembros puedan imprimir trabajos en ella. Como la idea es que sólo los profesores la puedan emplear, simplemente habrá que incluir el grupo global Profesores dentro del grupo local Impresora_Laser.

Por desgracia se ha averiado la impresora del Departamento de Economía. Como el Departamento de Informática es muy solidario, decide que permita a los profesores de Economía imprimir en la maravillosa impresora láser. Lo primero que habría que hacer es establecer una relación de confianza, de forma que el dominio de Informática confíe en el de Economía. Una vez establecida la relación de confianza, simplemente tendremos que añadir el grupo global Profesores del dominio Economía en el grupo local Impresora_Laser del dominio de Informática. Si se contrata un nuevo profesor en cualquiera de los dominios y se le incluye, como es lógico, en el grupo global respectivo de Profesores, automáticamente podrá imprimir sus trabajos en la impresora Láser.

Como se puede ver, los permisos sobre la impresora se han asignado al grupo local y hemos utilizado los grupos globales para incluir usuarios dentro de ese grupo local. De esta manera el número de sitios donde se tienen que dar los permisos disminuye y es más fácil realizar la administración del sistema. En resumen, los grupos globales se deben emplear para organizar los usuarios y los locales para asignar permisos sobre los recursos.

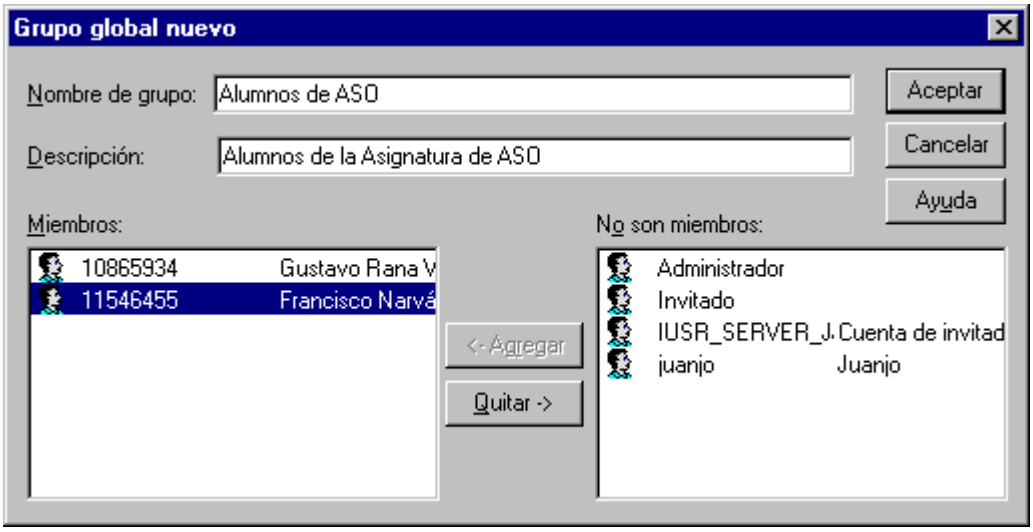


Figura 10 Creación del Grupo Global Alumnos de ASO

Creación de grupos globales y locales

Para crear, editar y borrar los grupos, tanto locales como globales, se emplea el Administrador de Usuarios para dominios (Figura 1). Como siempre los borrados son lo más simple de todo; escogeremos el grupo que deseemos y ejecutaremos el comando *Eliminar* o pulsaremos la tecla *Suprimir*. Al igual que ocurre con el borrado de cuentas de usuario, está acción es irreversible y se nos muestra un mensaje similar al de la Figura 9, donde se indica que aunque creemos un nuevo grupo con ese nombre no tendrá los permisos que se asignaron al grupo previamente borrado.

Para crear un nuevo grupo global se utiliza el comando *Grupo global nuevo*. En el ejemplo de la Figura 10 creamos un grupo global que agrupa a todos los alumnos de la asignatura. Como puede verse cuenta entre sus miembros con dos cuentas de usuario identificadas por su DNI. Para añadir miembros al grupo se emplea el botón *Agregar*. Una vez creado ese grupo podríamos darle los permisos que necesiten los alumnos de la asignatura, aunque en realidad es más lógico dar los permisos a grupos locales. Para ello, podríamos crear un grupo local Alumnos mediante el comando *Grupo local nuevo*. Como se puede apreciar en la figura siguiente, dentro de ese grupo hemos incluido el grupo global Alumnos de ASO. Cualquier permiso que se otorgue al grupo local Alumnos, lo heredarán automáticamente los miembros del grupo global Alumnos de ASO. Para añadir otros grupos globales se emplea el botón Agregar; sus miembros heredarán también los permisos del grupo local Alumnos.

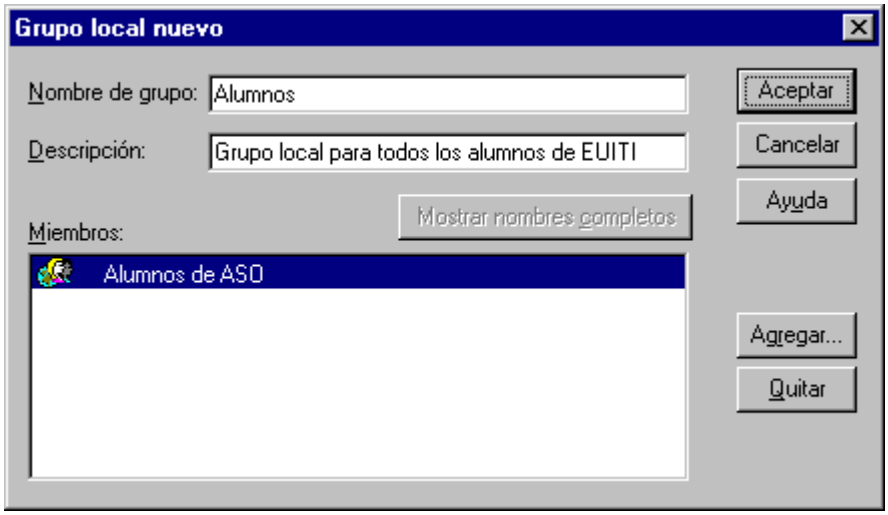


Figura 11 Creación del grupo local Alumnos

Grupo globales predefinidos

NT Server crea al instalarse en un PDC una serie de grupos globales predefinidos (véase Figura 1) que sirven de plataforma inicial para la planificación de los grupos globales de nuestro dominio. En la siguiente tabla se pueden ver esos grupos globales predefinidos.

Grupo	Miembros predefinidos	¿Quién puede modificarlos?
Administradores del dominio	Administrador	Administradores del Dominio
Usuarios del dominio	Administrador	Administradores y Operadores de Cuenta
Invitados del dominio	Invitado	Administradores y Operadores de Cuenta

Tabla 1 Grupos Globales predefinidos

Administradores del dominio

Un miembro de este grupo tiene derechos administrativos sobre:

- el dominio en el que está definido
- estaciones y servidores de ese dominio
- los dominios que confían en él

La cuenta Administrador pertenece a este grupo. A su vez este grupo está asignado al grupo local Administradores. Si no queremos que los Administradores del dominio controlen una estación o un servidor miembro tendremos que borrar el grupo Administradores del domino del grupo local Administradores de ese servidor o estación. Sólo un administrador, es decir un miembro del grupo, puede hacer cambios sobre el grupo Administradores del dominio.

Usuarios del dominio

Contiene a todos los usuarios con cuenta en el dominio. Cuando se crea una nueva cuenta se añade automáticamente a este grupo. Todos sus miembros tienen acceso a las estaciones de dominio. Este grupo forma parte del grupo local Usuarios. Si no queremos que los usuarios del grupo Usuarios del dominio accedan a una determinada estación o servidor habrá que borrarlo del grupo local Usuarios. Sólo los miembros de los grupos locales Administradores y Operadores de cuenta pueden hacer cambios en este grupo.

Invitados del dominio

Formado por todas las cuentas de invitado. Inicialmente sólo contiene la cuenta Invitado. Forma parte del grupo local Invitados. La norma es incluir en este grupo aquellos usuarios que tienen menos permisos y derechos que los usuarios normales del dominio. Tendremos que borrarlos del grupo Usuarios del dominio e incluirlos en este otro grupo. Sólo los miembros de los grupos locales Administradores y Operadores de cuenta pueden hacer cambios en este grupo.

Grupos locales predefinidos

Los equipos con NT Server, ya sean controladores de dominio o servidores miembro, y con NT Workstation tiene predefinidos una serie de grupos locales. Los grupos definidos dependerán del papel que ese ordenador desempeñe dentro de la red.

Controlador de dominio	Servidor o estación NT
Administradores	Administradores
Operadores de cuenta	Operadores de copia
Operadores del servidor	Usuarios avanzados
Operadores de impresión	Usuarios
Operadores de copia	Invitados
Usuarios	Duplicadores
Invitados	
Duplicadores	

Tabla 2 Grupos locales predefinidos de acuerdo con el papel del equipo

Administradores

Si es el grupo local Administradores de un dominio tienen control total sobre todo el dominio. Si es el grupo local de la estación solamente sobre esa estación. Los miembros de este grupo pueden realizar todas las tareas administrativas:

- Crear/borrar/editar cuentas de usuario
- Crear/borrar/editar grupos locales y globales
- Asignar derechos y permisos a los usuarios y a los grupos
- Controlar recursos compartidos e impresoras
- Instalar el archivos del sistema operativo y aplicaciones
- Formatear el disco duro
- Echar abajo el sistema
- Hacer copias de seguridad y restaurarlas.

Por defecto los miembros de este grupo tanto para un dominio como para un servidor o estación, son el Administrador (del dominio o de la estación) y el grupo global Administradores del Dominio (del dominio).

Grupo	Miembros predefinidos	¿Quién puede modificarlos?
Administradores	Cuenta Administrador y Administradores del Dominio	Administradores
Usuarios	Administrador y Usuarios del dominio	Administradores y Operadores de Cuenta
Invitados	Cuenta Invitado e Invitados del dominio	Administradores y Operadores de Cuenta
Operadores del Servidor	Ninguno	Administradores y Operadores de Cuenta
Operadores de Impresión	Ninguno	Administradores
Operadores de Copia	Ninguno	Administradores
Operadores de Cuenta	Ninguno	Administradores
Duplicadores	Ninguno	Administradores, Operadores de Cuenta y Operadores del Servidor

Tabla 3 Tabla de grupos locales predefinidos en un controlador primario

Operadores de Cuenta

Este grupo solamente existe en los servidores NT que actúan como controladores de dominio. Los miembros de este grupo pueden controlar casi todas las cuentas de usuario del dominio y los grupos. Un operador de cuenta puede crear, borrar y definir todas las cuentas y grupos, excepto aquellas creadas por los miembros del grupo Administradores. Tampoco pueden modificar los grupos Administradores del dominio, Administradores, Operadores del Servidor, Operadores de Cuenta, Operadores de Impresión y Operadores de Copia, ni las cuentas que a ellos pertenezcan. Los Operadores de Cuenta tampoco pueden asignar derechos a los usuarios, ni administrar planes de seguridad. Sin embargo, si pueden iniciar sesiones en servidores del dominio, pueden apagarlos y pueden agregar equipos a un dominio. Por defecto, no hay ningún usuario perteneciente a este grupo.

Operadores de Copia

Los miembros de este grupo pueden inicial sesiones locales y realizar copias de seguridad. Obviamente también pueden restaurar copias de seguridad antiguas. Pueden realizar esas actividades aunque no tengan permiso de lectura o escritura sobre los ficheros y directorios que se guardan/recuperan en las copias de seguridad. Además, pueden mantener perfiles locales y echar abajo el sistema.

Por defecto, no hay ningún usuario que pertenezca a este grupo. En el caso de que sea el grupo local de un dominio, su poder para realizar copias de seguridad se extiende a todo el dominio; si es el grupo local de una estación, sólo podrá hacerlo sobre la estación.

Operadores de Impresión

Sólo existen en los servidores NT que actúan como controladores primarios. Los usuarios de este grupo pueden compartir impresoras, definir la forma en la que las comparten y dejar de compartirlas. En resumen pueden manejar cualquier aspecto relacionada con las impresoras del dominio. Además pueden iniciar sesiones locales en los servidores y echarlos abajo. Por defecto no tiene miembros.

Los pasos para permitir que un operador de impresión controle impresoras que no se encuentren en el controlador primario serían los siguientes:

1. Crear un grupo global.

2. Incluir en ese grupo a los Operadores de Impresión que deseemos.

3. En cada servidor NT que tenga impresoras compartidas, habrá que hacer que el grupo global que contiene las cuentas de los Operadores de Impresión pertenezcan al grupo local Usuarios Avanzados.

Operadores del Servidor

Sólo existen el los servidores NT que actúan como controladores primarios. Su principal misión es mantener los servidores funcionando. Pueden realizar muchas de las operaciones propias de los Administradores, pero no pueden modificar ningún aspecto relacionado con la seguridad del sistema. Las tareas que pueden realizar son:

- Iniciar sesiones locales en los servidores y apagarlos.
- Pueden bloquear y desbloquear servidores.
- Compartir y configurar recursos compartidos: tanto impresoras como directorios.
- Hacer copias de seguridad y restaurarlas.
- Formatear el disco y cambiar la hora del sistema.

Duplicadores

Existen tanto en los controladores primarios como en los servidores y estaciones. Sus miembros soportan las funciones de duplicación de directorios. No tiene inicialmente miembros. En realidad sólo debe tener una cuenta de usuario. Esa cuenta permitirá iniciar sesiones en el servicio Duplicador del controlador principal del dominio y de los controladores

reserva. Este servicio sirve para mantener las mismas versiones de determinados ficheros guardados en ciertos directorios. Se configura un servidor como exportador y los demás como importadores. El exportador exportará unos directorios a los importadores, es decir, cuando la versión de esos ficheros cambie en el exportador se transmitirá dinámicamente esa nueva versión a cada uno de los importadores. Como exportador sólo pueden funcionar equipos con NT Server mientras que como importadores pueden trabajar equipos con NT Server y NT Workstation.

Grupo	Miembros predefinidos	¿Quién puede modificarlos?
Administradores	Cuenta Administrador	Administradores
Usuarios	Cuenta de usuario especificada durante la instalación de la estación (si no pertenece a un dominio)	Administradores y Usuarios Avanzados
Invitados	Cuenta Invitado	Administradores y Usuarios Avanzados
Usuarios Avanzados	Ninguno	Administradores y Usuarios Avanzados
Operadores de Copia	Ninguno	Administradores
Duplicadores	Ninguno	Administradores

Tabla 4 Tabla de grupos locales predefinidos en una estación NT y en servidores que no sean controladores de dominio

Usuarios

Existe en todos los equipos NT (servidores o estaciones). Proporciona a los usuarios los derechos para realizar sus tareas diarias. Sus miembros no pueden iniciar sesiones locales en el servidor pero si pueden trabajar en las estaciones. En estaciones NT, pueden realizar las siguientes operaciones:

- Entrar al sistema a través de una estación y acceder a la red.
- Ejecutar aplicaciones
- Usar impresoras de red y locales
- Tener un perfil personal y guardarlo localmente en la estación
- Echar abajo y bloquear la estación

Los miembros de este grupo en un controlador de dominio son el grupo global Usuarios del Dominio y el usuario Administrador. En estaciones o servidores NT no hay miembros predefinidos.

Invitados

Los miembros del grupo local Invitados, tienen un conjunto de privilegios muy limitados. Pertenecerán a este grupo los usuarios ocasionales de nuestro sistema. Permite que esos usuarios no habituales inicien sesiones interactivas en las estaciones de trabajo (inicio de sesión local) o de forma remota en la cuenta incorporada Invitado de un dominio (inicio de sesión de red. No tienen derechos en los servidores del dominio. Sin embargo tienen ciertos derechos sobre las estaciones. Las pueden echar abajo. De forma predeterminada el grupo global Invitados del dominio pertenecen a este grupo.

Usuarios Avanzados

Sólo existen en las estaciones NT o en servidores NT que no sean controladores de dominio. Pueden hacer lo mismo que los miembros del grupo Usuarios y además:

- Pueden crear cuentas de usuario y modificarlas.

- Añadir cualquier cuenta a los grupos Usuarios, Invitados y Usuarios Avanzados.
- Compartir y configurar recursos compartidos (impresoras y directorios).

Dado que no existen en los dominios, se recomienda seguir la siguiente estrategia. Hacer que el usuario habitual de una estación, pertenezca al grupos Usuarios Avanzados. Eso hace que ese usuario tenga un mayor control sobre su propia estación, lo que le permitirá compartir sus recursos con otros usuarios. Si se quiere que tenga menos privilegios, se debe incluir simplemente dentro del grupo Usuarios; si se les quieren dar todos los derechos debe pertenecer al grupo local Administradores.

Grupos especiales

NT incluye grupos especiales que son empleados para indicar como un determinado usuario está usando NT. En otras palabras, estos grupos no tienen miembros, la pertenencia a ellos depende del tipo de acceso que tenga el usuario sobre el sistema. No aparecen en el Administrador de usuarios (la herramienta para definir cuentas de usuario) pero si cuando se asignan permisos a directorios, archivos e impresoras. Esos grupos son los siguientes:

- **Todos.** Todas las cuentas de usuarios. Interactivo + Red.
- **Interactivo.** Cualquier usuario que use el equipo localmente.
- **Red.** Todos los usuarios conectados al equipo o recurso a través de la red.
- **Sistema.** Esta entidad representa al sistema operativo. Al instalar el sistema se asignan permisos al sistema. No es habitual que el administrador asigne permisos a este grupo.
- **Creador/Propietario.** Cualquiera que crea un fichero, un directorio o un trabajo de impresión. En un directorio, si se asignan derechos a este grupo, el creador de un subdirectorio o un archivo tendrá esos derechos. Para un impresora los permisos asignado al grupo Creador/Propietario se transferirán a los usuarios que envíen un trabajo de impresión y los tendrán sobre ese trabajo.

Si el Administrador se conecta al dominio desde el PDC, durante esa sesión pertenecerá al grupo Interactivo. Si lo hace desde una estación, pertenecerá al grupo Red. En cualquiera de los dos casos pertenecerá al grupo Todos. Además durante cualquier sesión pertenecerá al grupo Creador/Propietario respecto de aquellos objetos de los que sea Propietario.

Derechos y permisos

Aunque en algunos SOs muchas veces estas dos palabras se utilizan indistintamente para referirnos al nivel de acceso que los usuarios tienen sobre un recurso, como por ejemplo un fichero, en NT estos dos conceptos, el derecho y el permiso son cosas diferentes.

- **Permisos.** Se aplican sobre objetos concretos del sistema: un archivo, una carpeta, una impresora.... El permiso es una regla asociada con un objeto que regula los usuarios que pueden tener acceso al objeto y de qué manera. Los permisos sobre cada objeto se representan a través de su lista de control de acceso (ACL Access Control List). En las ACL, aparecen los SIDs de los usuarios y grupos que tienen acceso al objeto y el tipo de acceso que tienen. El encargado de asignar los permisos sobre un objeto, será el creador del mismo o el propietario.
- **Derechos (user rights)**. Es una acción que los usuarios pueden hacer y que afecta a todo el equipo, es decir, no se refiere a un objeto particular, como leer fichero o imprimir un trabajo, sino a acciones sobre todo el sistema, por ejemplo hacer copias de seguridad o apagar el equipo. Los derechos permiten a los usuarios realizar tareas administrativas. Los derechos se asignan a través del Administrador de Usuarios. Hay que indicar que los derechos son de mayor rango que los permisos y si hay conflicto entre ellos prevalece el derecho. Por ejemplo, si a un usuario se le da el derecho de poder hacer copias de seguridad, le permitirá hacer backups incluso de ficheros o directorios sobre los que no tenga permiso de lectura. Existen dos tipos de derechos: normales y avanzados.

- **Capacidades predefinidas**. Además de los derechos, los grupos predefinidos tiene asignados una serie de capacidades predefinidas que son los que marcar las funciones que esos grupos de usuarios pueden realizar. A diferencia de los derechos, están capacidades no se pueden asignar a través del Administrador de Usuarios para Dominios ya que son acciones administrativas que deben desempeñar los miembros de los grupos predefinidos con labores concretas como pueden ser Administradores o los distintos tipos de Operadores existentes.

Derechos de usuario

Dejando a un lado los permisos (los analizaremos en los apartados que tratan sobre los sistemas de archivos), en los siguientes apartados, hablaremos de los distintos derechos que existen en NT y de las capacidades predefinidas.

Derechos Normales

Como se ha dicho anteriormente, existen dos tipos de derechos: normales y avanzados. Los primeros son los que se suelen emplear más habitualmente ya que son los que más afectan al usuario tipo. Son los siguientes:

D1 **Inicio de sesión local.** Permite al usuario acceder al equipo desde el propio equipo.

D2 **Acceder a este equipo desde la red.** Permite iniciar una sesión remota, es decir, conectarse a través de la red.

D3 **Tomar posesión de archivos y otros objetos.** Esto permite a los usuarios convertirse en propietario de un objeto y poder asignar los permisos que desee.

D4 **Administrar los registros de auditoría y seguridad.** Especificar los aspectos de seguridad y los eventos que el sistema va a auditar.

D5 **Cambiar la hora del sistema.** Permite cambiar la fecha y la hora.

D6 **Apagar el sistema.** Apagar el equipo y echarlo abajo.

D7 **Forzar el apagado desde un sistema remoto.** Este derecho permite que un usuario "rebote" un servidor a través de la red.

D8 **Hacer copias de seguridad de archivos y directorios.** Permite realizar backups o copias de archivos y directorios. Este derecho prevalece sobre los permisos sobre directorios y archivos.

	Administradores	O. del Servidor	O. de Cuenta	O. de Impresión	O. de Copia	Todos	Usuarios	Invitados
D1	SI	SI	SI	SI	SI			
D2	SI				SI	SI		
D3	SI							
D4	SI							
D5	SI	SI						
D6	SI	SI	SI	SI	SI			
D7	SI	SI						
D8	SI	SI			SI			
D9	SI	SI			SI			
D10	SI							
D11	SI							

Tabla 5 Asignación de derechos en controladores de Dominio

D9 **Restaurar archivos y directorios.** Derecho complementario al anterior. Nos permite recuperar copias de seguridad antiguas.

D10 **Cargar y descargar controladores de dispositivos.** Permite instalar y desinstalar controladores de los dispositivos del equipo.

D11 **Agregar equipos al dominio.** Necesario para poder incluir todos los equipos del dominio. La estación reconocerá las cuentas de usuario del dominio.

	Administradores	Usuarios Avanzados	Usuarios	Invitados	Todos	O. de Copia
D1	SI	SI	SI	SI	SI	SI
D2	SI	SI			SI	
D3	SI					
D4		SI				
D5	SI	SI				
D6	SI	SI	SI		SI	SI
D7	SI	SI				
D8	SI	SI			SI	
D9	SI				SI	
D10	SI				SI	
D11		SI				

Tabla 6 Asignación de derechos en estaciones NT y servidores NT

En las tablas anteriores se resumen los derechos que se asignan por defecto a los grupos predefinidos. Como se puede ver, aunque el grupo Invitados no tienen asignado el derecho para echar abajo el sistema, lo pueden hacer ya que ese derecho lo tiene el grupo Todos.

Para asignar derechos normales a los usuarios se emplea el Administrador de usuarios para dominios y dentro de él, el comando *Derechos de Usuario* en el menú Directivas. El proceso para asignarlo es bastante simple Como puede verse en la figura, dentro de la lista desplegable se selecciona el Derecho que queremos asignar y mediante los botones *Agregar* y *Quitar* se eligen los usuarios a los que se asigna ese derecho. El botón *Agregar* nos lleva a la ventana de la Figura 13, donde se pueden seleccionar cualquier grupo o cualquier usuario, tanto del dominio en el que nos encontremos como de dominios en los que confiemos.

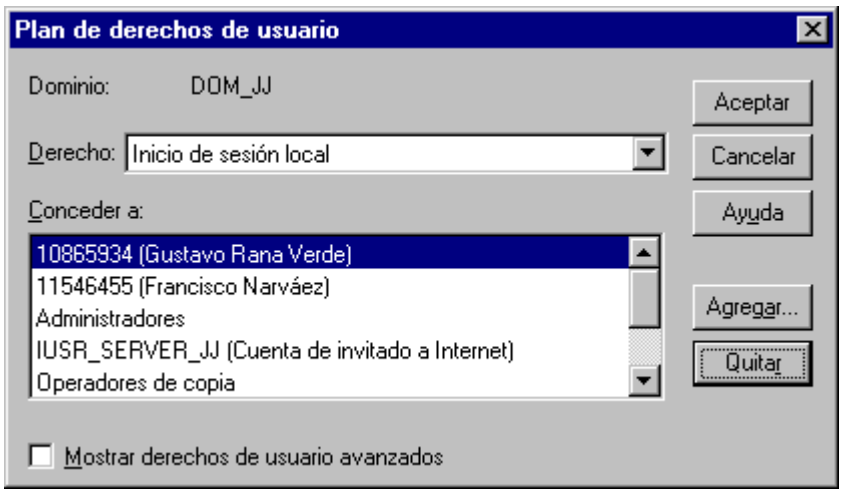


Figura 12 Derechos de usuario

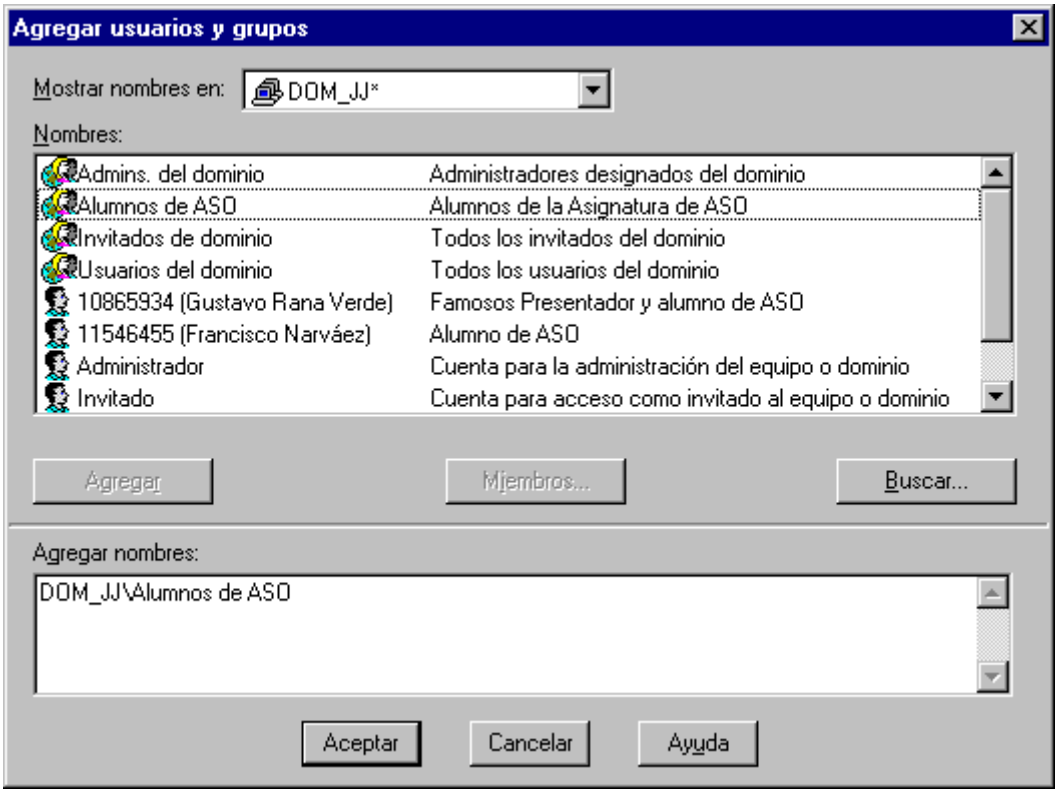


Figura 13 Cuadro de diálogo para Agregar Usuarios

Esta última ventana se emplea en todas las ocasiones en las que es necesario asignar algún privilegio. Como puede verse, en el ejemplo se va a agregar el grupo local Alumnos de ASO. Antes del nombre del grupo, siempre se añade el nombre del dominio, ya que existe la posibilidad de escoger usuarios y grupos de otros dominios. Si sólo se añadiera el nombre del usuario podría dar lugar a ambigüedades.

Derechos Avanzados

Además de los derechos comentados en el apartado anterior, existen otros derechos que son menos empleados y que tienen usos que van más allá de los que necesitan los usuarios "normales". Están enfocados a usuarios que por ejemplo desarrollen aplicaciones para NT. Algunos de ellos son los siguientes:

- DA1 **Actuar como parte del sistema operativo.** El usuario podrá hacer operaciones como si fuera una parte del SO. Este derecho se asigna a los subsistemas.
- DA2 **Saltarse la comprobación de recorrido.** Permite al usuario cambiar de directorio aunque no tenga permisos sobre ese árbol de directorios.
- DA3 **Crear un fichero de intercambio.** Permite al usuario la creación de ficheros de intercambio. Lo pueden hacer los Administradores.
- DA4 **Depurar programas.** Permite al usuario depurar objetos de bajo nivel, como los threads. Lo pueden hacer los Administradores.
- DA5 **Incrementar cuotas.** Permite incrementar las cuotas de algunos objetos. También lo tienen asignado los Administradores.
- DA6 **Iniciar sesión como servicio.** El usuario puede entrar en el sistema como un servicio que se ejecuta en background (replicación). Ese servicio debe habilitarse a través de programa Servicios dentro del Panel de Control.

Capacidades predefinidas

Además de los derechos, tanto normales como avanzados, existen otras acciones que pueden desarrollar los grupos y usuarios predefinidos. Estas acciones son capacidades

predefinidas y, a diferencia de los derechos, no pueden ser cambiadas por el Administrador. Estas acciones predefinidas son las siguientes:

- A1 **Crear y administrar cuentas de usuario.**
- A2 **Crear y administrar grupos de usuario globales.**
- A3 **Crear y administrar grupos de usuario locales.**
- A4 **Asignar derechos de usuarios,** los derechos que hemos visto en los apartados anteriores.
- A5 **Gestión de auditorías y ficheros de registro.** Permite controlar las auditorías que realiza el sistema y observar los ficheros de registro.
- A6 **Bloquear el servidor.** Bloquea el servidor e impide que otro usuario entre en sesión.
- A7 **Desbloquear el servidor.**
- A8 **Formatear el disco duro.** Es decir, poder realizar operaciones sobre los discos duros del servidor, operaciones como el formateo o la creación de volúmenes.
- A9 **Crear grupos de programa.**
- A10 **Mantener perfiles locales.** Permitir que se guarde una copia local del perfil del usuario. Esa copia se suele mantener en %SYSTEMROOT%\Profiles.
- A11 **Compartir y dejar de compartir carpetas.** Permite que un usuario decida compartir una carpeta con otros usuarios y cómo la va a compartir.
- A12 **Compartir y dejar de compartir impresoras.** Idéntico al anterior pero cuando el recurso compartido es una impresora.

	Administradores	O. del Servidor	O. de Cuenta	O. de Impresión	O. de Copia	Todos	Usuarios	Invitados
A1	SI		SI					
A2	SI		SI					
A3	SI		SI					
A4	SI							
A5	SI							
A6	SI	SI			SI			
A7	SI	SI						
A8	SI	SI						
A9	SI	SI						
A10	SI	SI	SI	SI	SI			
A11	SI							
A12	SI	SI		SI				

Tabla 7 Asignación de acciones predefinidas en controladores de Dominio

	Administradores	Usuarios Avanzados	Usuarios	Invitados	Todos	O. de Copia
A1	SI	SI				
A3	SI	SI	SI			
A4	SI					
A5		SI				
A6	SI	SI			SI	
A7	SI					
A8	SI					
A9	SI	SI				
A10	SI	SI	SI		SI	
A11	SI	SI				
A12	SI	SI				

Tabla 8 Asignación de acciones predefinidas en estaciones NT y servidores NT

Los Usuarios Avanzados pueden modificar sólo las cuentas que ellos crean. Pueden además crear grupos locales, pero solamente pueden añadir/borrar usuarios de los grupos que ellos creen y de los grupos locales Usuarios Avanzados, Usuarios e Invitados. Los Usuarios Avanzados no pueden modificar los grupos Administradores y Operadores de Copia[5].

Políticas sobre Cuentas de Usuario

Sobre las cuentas de los usuarios se pueden fijar normas, políticas o directivas que los usuarios deben cumplir y que servirán para aumentar la seguridad del sistema. Las cuentas de usuarios serán más difíciles de violar y el sistema tendrá unas mejores medidas de seguridad. Este conjunto de normas, afectan en su mayoría a las contraseñas y se establecen desde el Administrador de Usuarios para Dominios y son las siguientes:

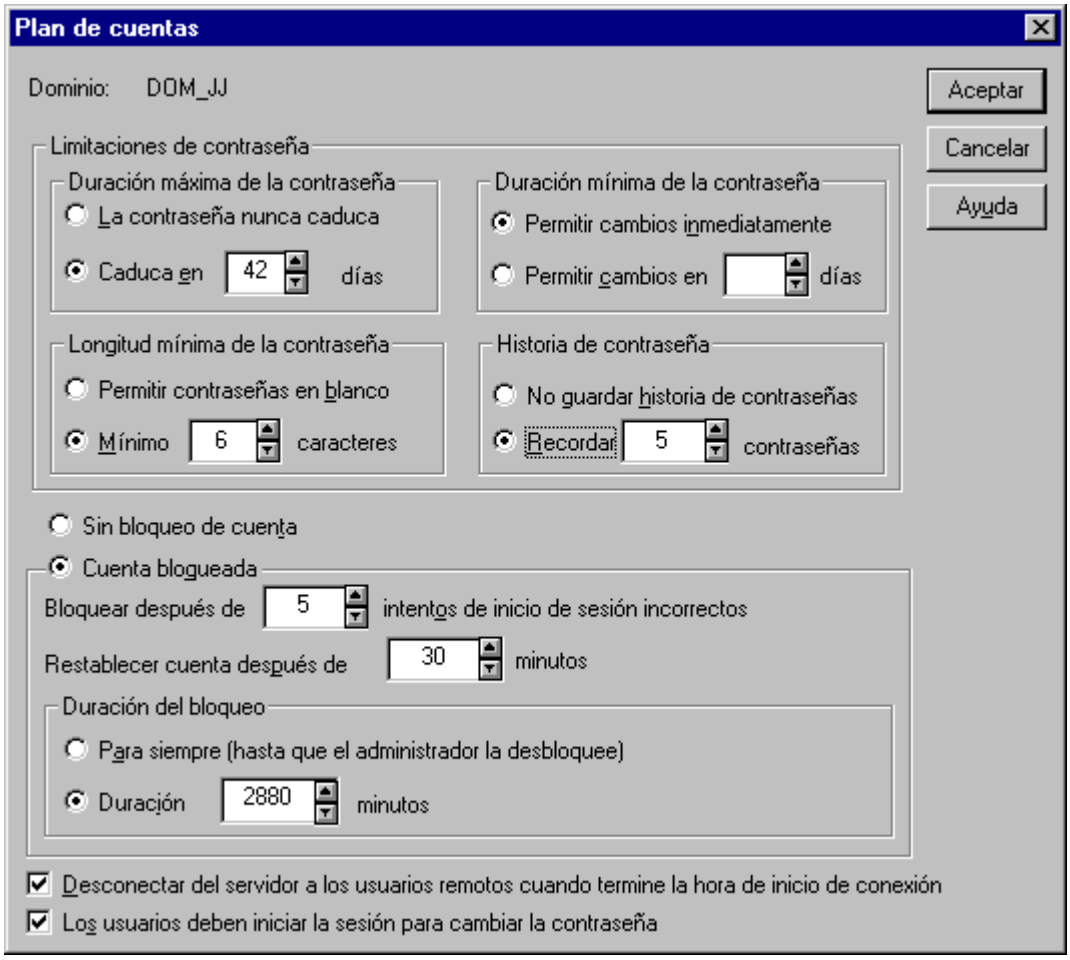


Figura 14 Plan de Cuentas

Limitaciones de la contraseña

- **Máxima duración de una contraseña.** Indica el número de días máximo durante los que el sistema permite que un usuario mantenga la misma contraseña. Se puede hacer que la contraseña no caduque nunca, o hacer que tenga una duración máxima entre 1 y 999 días.
- **Mínima duración de una contraseña.** Cantidad de tiempo que debe pasar antes de que el sistema permita a un usuario cambiar su contraseña. Puede hacerse que esos

[5] Se cumple que ningún usuario puede dar o quitar privilegios (permisos y derechos) de lo que carezcan.

cambios se permitan siempre (lo normal) o indicar el número de días que deben transcurrir entre cambios (entre 1 y 999 días).

- **Contraseñas únicas.** Mediante esta norma se especifica el número de nuevas contraseñas que el usuario debe tener antes de permitirle volver a usar una contraseña que ya tuvo en el pasado. Por defecto el sistema no recuerda las contraseñas antiguas, por lo que los usuarios pueden usar la misma contraseña cuando el sistema les solicita una nueva. Hay que indicarle que recuerde un cierto número de contraseñas (entre 1 y 24), esto impedirá que los usuarios vuelvan a usar la misma contraseña.
- **Mínima longitud de las contraseñas.** Indica el número mínimo de caracteres que debe tener una palabra de paso. Esto previene contra contraseñas vacías (se pueden permitir si se desean). La longitud puede variar entre 1 y 14 caracteres, aunque no deberían permitirse nunca contraseñas de menos de 6 caracteres.

Bloqueo de cuentas

- **No bloquear cuentas.** Cuando se habilita esta opción, no se bloquea ninguna cuenta aunque el usuario realice muchos logins incorrectos. Esta opción sólo se debe habilitar en situaciones en las que la seguridad no sea un requisito o cuando el bloqueo de cuentas genere un trabajo excesivo (demasiados usuarios que olvidan sus contraseñas).
- **Bloquear cuentas de usuario.** Esta opción permite que el sistema bloquee una cuenta de usuario si se introduce mal varias veces la contraseña. En esta opción se especifica el número mínimo de veces en las que el usuario se puede equivocar (entre 1 y 999). Tiene varias subopciones más:
  - **Resetear el número de logins incorrectos.** Se puede indicar el número de minutos máximo (entre 1 y 99999) entre dos logins incorrectos. Pasado ese tiempo se considera que el usuario no ha realizado ningún login incorrecto.
  - **Durante cuanto tiempo permanecerá bloqueada la cuenta.** Entre 1 y 99999 minutos.

  Como medida de seguridad, la cuenta de Administrador no debe bloquearse nunca. Eso impide que un intruso que intente violar la cuenta del Administrador provoque que ésta sea bloqueada. Además, de esta forma el Administrador siempre podrá desbloquear la cuenta de otros usuarios.

Horarios de conexión

- **Forzar a desconectar a los usuarios remotos cuando se excedan sus horarios de conexión.** Si se activa esta opción, si un usuario está conectado y en ese momento sobrepasa su horario de conexión, se le desconecta. Si no se habilita la opción, el usuario podrá seguir conectado, aunque no podrá hacer nuevos logins.
- **Los usuarios deben estar conectados para cambiar su contraseña.** Con esta opción se obliga a que los usuarios entren en sesión para cambiar sus contraseñas. Si la contraseña ha caducado, tendrá que cambiar la contraseña el Administrador. Si no está habilitada la opción, los usuarios podrán cambiar su contraseña aunque esta haya caducado.

Para fijar un Plan de Cuentas se utiliza el Administrador de Usuarios para dominios. Dentro de la herramienta deberemos ejecutar el comando *Cuentas* del menú *Directivas*. Nos mostrará la ventana de la Figura 14, en la que podremos configurar todos los aspectos explicados en este apartado.

Login scripts

Los login scripts son ficheros de comandos que se ejecutan cuando un usuario se conecta al sistema. Sirven para configurar el entorno de trabajo de los usuarios. El uso de los login script es opcional, de hecho si nos conectamos desde una estación NT, toda la funcionalidad que tienen la proporcionan de forma más intuitiva los perfiles de usuario. Si la estación no es NT (pe. un estación MS-DOS), se precisa de los login script para establecer conexiones de red y ejecutar los comandos necesarios para definir el entorno de trabajo de los usuarios.

Login Scripts	Perfiles
Disponible para todo tipo de clientes	Disponible sólo en equipos NT
Se pueden utilizar para crear conexiones de red e iniciar aplicaciones; no sirven para configurar la apariencia del entorno de trabajo.	Pueden configurar todos los aspectos del entorno de trabajo, incluyendo la apariencia del mismo, así como crear conexiones de red e iniciar aplicaciones.
Cualquier editor de texto se puede usar para crear y editar los login scripts.	Se debe usar una herramienta especial para crear los perfiles, o se crean a partir de una cuenta de usuario.
Se puede usar como un fichero batch (lo normal) o un programa ejecutable.	Existen diferentes tipos de perfiles: local, personal, obligatorio y por defecto. Tienen distintos niveles de control e interaccionan unos con otros.

Tabla 9 Login Script vs Perfiles

¿Cuándo se debe usar un login script?

Aunque los perfiles NT pueden hacer lo mismo que los login scripts, sin embargo hay situaciones en las que se deben emplear estos últimos:

- Estamos empleando estaciones no-NT: MS-DOS, clientes LAN Manager...
- Sólo se desean fijar las conexiones de red y ejecutar aplicaciones; no queremos definir el entorno de trabajo de los usuarios.
- Se desea compartir un mismo login script para varios usuarios.
- Son más sencillos de mantener que los perfiles
- Nuestra red NT se ha integrado con una red Lan Manager existente que emplea login scripts.

Comandos de un login script

Los login script suelen tener extensión .BAT o .CMD. La diferencia entre ambos es que los primeros serán interpretados por el procesador de comandos de DOS y los segundos por un intérprete de comandos NT. Los comandos que se pueden usar son cualquier comando NT. El comando más empleado es el comando NET que tiene la siguiente sintaxis:

NET comando parámetros

En función del comando indicado, la funcionalidad es una u otra. El más empleado y el más útil de todos es USE y su sintaxis es:

NET USE [devicename | *] [\\computername\sharename[\volume] [password | *]]
[/USER:[domainname\][username]
[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE [devicename | *] [password | *] [/HOME]

NET USE [/PERSISTENT:{YES | NO}]

NET USE conecta o desconecta un equipo con un recurso compartido. Si se usa sin parámetros, lista las conexiones del equipo. El significado de los parámetros es:

- **devicename**: asigna un nombre para la conexión con el recurso o desconecta el recurso. Habitualmente hay dos tipos de nombres para dispositivos: letra de unidad (desde D: hasta Z:) y puertos para impresoras (LPT1: hasta LPT3:). Si se pone un asterisco se emplea el siguiente nombre libre.
- **\\computername**: es el nombre del equipo que contiene el recurso compartido.
- **\\sharename**: el nombre del recurso compartido

- **\volume**: especifica el volumen NetWare del servidor. No se emplea en entornos NT que no dispongan de equipos Novell NetWare.
- **password**: la contraseña necesaria para el acceso al recurso. Si se pone * eso indica que aparecerá una ventana pidiendo la contraseña al usuario.
- **/USER**: especifica un nombre de usuario diferente al del usuario que está en sesión.
- **domainame**: especifica un dominio diferente. Si se omite el dominio se considera el dominio en el que está conectado
- **username**, especifica el nuevo nombre usuario con el que conectarnos.
- **/DELETE**, cancela una conexión de red y la borra de la lista de conexiones permanentes.
- **/PERSISTENT**, indica si la conexión va a ser permanente o no. Por defecto se usa la última empleada.
- **/HOME**, conecta a un usuario con su directorio personal.

Ejemplo:

NET USE F: /DELETE

NET USE G: /DELETE

NET USE F: \\PDC\APPS

NET USE G: \\PDC\DATA

*NET USE * /HOME*

NET USE

Los dos primeros comandos borran las conexiones en las unidades F: y G:. Después se crean dos unidades de red, una, la F:, que apunta al recurso compartido APPS dentro de la máquina PDC, y la segunda, la G:, que corresponde al recurso DATA de la misma máquina. El penúltimo comando, asigna la siguiente letra al directorio personal del usuario. El último muestra por pantalla la lista de unidades disponible.

Variables en los login script

Es habitual que en los login script de cualquier sistema operativo se incluyan variables que sirven para hacer estos ficheros más generales y para que puedan ser compartidos por varios usuarios. Estas variables toman distintos valores en función del usuario o de la estación desde la que el usuario se conecta al sistema. Concretamente en los login script de NT se pueden incluir las siguientes variables:

- **%HOMEDRIVE%** la letra de la unidad donde se encuentra el directorio particular del usuario.
- **%HOMEPATH%** el path (sin letra de unidad) donde está el directorio particular del usuario.
- **%HOMESHARE%** el nombre del recurso compartido que contiene el directorio particular del usuario.
- **%OS%** el sistema operativo que se ejecuta en la estación del usuario.
- **%PROCESSOR_ARCHITECTURE%** el tipo de procesador de la estación del usuario.
- **%USER_DOMAIN%** el nombre del dominio que contiene la cuenta del usuario.
- **%USERNAME%** el nombre de la cuenta de usuario.
- **%SYSTEMROOT%** directorio donde se encuentra instalado el sistema operativo.

Variables de entorno

Las variables de entorno son cadenas de texto que se evalúan a un valor. El sistema operativo y las aplicaciones pueden leer estas variables y darles un valor para controlar el comportamiento del sistema y de las aplicaciones. NT distingue dos tipos de variables de entorno:

- Variables de entorno del sistema
- Variables de entorno del usuario

Las primeras existen para todos los usuarios, mientras las segundas las crean cada usuario. Dado que los usuarios pueden asignar valores a las variables de entorno, pueden existir conflicto entre ellas. NT resuelve los posibles conflictos dando prioridad a los valores que el usuario asigna a esas variables. Luego los valores que da el usuario prevalece sobre el que da el sistema y el que se asigna en el AUTOEXEC.BAT (este fichero también sirve para dar valor a las variables de entorno). Es decir, si una variables de entorno se fija primero por el sistema y el usuario sobreescribe esa variable prevalece el valor del usuario. Si además esa misma variable se trata de fijar en el AUTOEXEC.BAT ese valor se descarta. Por ejemplo:

Sistema SET APPL=\System\appl

Usuario SET APPL=\User\Appl

AUTOEXEC.BAT SET APPL=AUTOEXEC

El valor que prevalece en ese caso es el que da el usuario. La única excepción es la variable PATH. Es este caso el valor que dé el usuario se añade al que da el propio sistema, no se sobreescribe. También se añade el path especificado en el AUTOEXEC.BAT.

Las variables de entorno se pueden salvar dentro de los perfiles de usuario. Para hacerlo se emplea la aplicación Sistema dentro del Panel de Control.

Variable	Tipo	Descripción
ComSpec	Sistema	Especifica la localización del intérprete de comandos de NT, el CMD.EXE
OS2LibPath	Sistema	Indica donde se encuentran las DLLs de OS2 y que necesitan las aplicaciones de este SO
Path	Sistema	Especifica los directorios en los que se buscarán los programas ejecutables.
windir	Sistema	Indica el directorio donde está instalado NT
tmp o temp	Usuario	Especifica el directorio por defecto donde las aplicaciones guardarán los ficheros temporales. Se necesitan los dos porque hay aplicaciones que usan uno u otro

Tabla 10 Lista de variables de entorno

Uso de los login scripts

Un login script puede ser compartido por varias cuentas de usuario o por varios grupos. Dentro del Administrador de Usuarios para dominios hay que especificar donde se encuentra el login script del usuario (véase Figura 3). Si no se indica un path para el fichero, se considera que se encuentra en %SystemRoot%\System32\Repl\Import\Scripts (recurso compartido NETLOGON), directorio que se suele emplear para guardarlo. Si los login script se encuentran en otro directorio hay que indicar el path completo.

Normalmente los login scripts, se descargan desde el servidor que valida la entrada del usuario, el controlador primario o uno secundario. Por ellos es habitual hacer que ese directorio se replique entre el PDC y los BDCs del dominio. La copia maestra estará en el PDC (exportador) que exportará copias automáticamente a los BDCs (importadores). En el caso de replicar los login script hay que ser especialmente cuidadoso con la indicación de los paths, ya que aunque dupliquemos un login script del PDC al BDC, si en el cuerpo del script empleamos rutas que apuntan al PDC, cuando el PDC no esté activo, esas rutas serán inaccesibles. Por ello no está de más hacer cosas como la siguiente:

SET TEMP_SERVER=BDC

IF EXIST \\PDC\NETLOGON SET TEMP_SERVER=PDC

NET USE F: \\%TEMP_SERVER%\APPS

Perfiles de usuario

Windows NT proporciona varias formas de configurar el entorno de trabajo de los usuarios. En el apartado anterior ya hablamos de los login script como el método de configurar entornos en clientes no NT. En este apartado vamos a hablar de la forma mejor de determinar el entorno de trabajo de los usuarios cuando nuestras estaciones son NT. Ese método son los perfiles de usuario[6].

El entorno de trabajo de los usuarios incluye entre otras cosas la organización del Menú Inicio, la configuración de la barra de tareas, las conexiones de red, o la configuración de la pantalla y del ratón.

Características

Como ya se ha dicho, los perfiles de usuario solamente se pueden emplear en equipos que ejecuten Windows NT Workstation o NT Sever. También se pueden utilizar en equipos con Windows 95/98, aunque para este tipo de clientes la configuración resulta más compleja. (véase más adelante el apartado Perfiles con Windows 95). Para otro tipo de clientes, como DOS, UNIX o OS/2, los perfiles no se pueden utilizar.

El funcionamiento general de los perfiles es el siguiente. Cuando un usuario se conecta por primera vez desde un equipo NT, se le da la configuración de un perfil por defecto (Default User). Durante todas las sesiones, incluida la primera, los cambios que el usuario realiza en su entorno de trabajo se guardan dentro del perfil local de ese usuario. Esa configuración será especifica del equipo en el que el usuario se conectó. Si le usuario se conecta desde otra estación no tendrá disponible su perfil. Sin embargo, el administrador puede elegir un tipo de perfil, el perfil móvil, que permite que el usuario puede emplear el mismo perfil y, por tanto, la misma configuración, independientemente de la estación que utilice.

Ventajas

El empleo de perfiles proporciona ventajas tanto para los propios usuarios como para los administradores. Las ventajas de los usuarios son evidentes:

- Cuando el usuario se conecta al equipo, mantiene la configuración del entorno de trabajo que más se adapta a sus necesidades, lo que mejora su integración con el sistema y le hace más agradable y sencillo realizar su trabajo.
- Varias personas pueden usar el mismo equipo, y cada uno tendrá configurado su entorno de trabajo como más le guste.
- Si el perfil se almacena en un servidor (perfil móvil), el usuario tendrá el mismo entorno independientemente del equipo o estación desde la que se conecte.

Aunque quizá sean menos obvias, los administradores también se benefician del empleo de perfiles de usuario:

- El administrador puede crear perfiles especiales para usuarios poco expertos, o que se equivocan o distraen con facilidad. Estos perfiles no tendrán elementos extraños para los usuarios y se adaptarán perfectamente a sus necesidades sin que los propios usuarios tengan que configurarlos.
- Se puede crear y utilizar un mismo perfil para un grupo de usuarios.
- Se pueden asignar perfiles obligatorios que los usuarios no pueden cambiar.
- Se pueden ocultar ciertos recursos a los usuarios, asignando perfiles que mantengan restricciones de seguridad sobre esos objetos. Es decir, permiten implementar una política de seguridad.
- Se puede hacer accesible un nuevo recurso o aplicación a muchos usuarios de una sola vez, tan solo habrá que cambiar el perfil común de ese grupo de usuarios.

---

[6] Existe una tercera forma de configuración de entornos que es el Editor de Directivas del Sistema, que se discutirá más adelante.

Componentes de un perfil

Los componentes de un perfil, es decir, las cosas que un usuario puede configurar dentro de un perfil son los siguientes:

- **Explorador.** Todas aquellas opciones que pueden configurar el usuario dentro del Explorador de NT.
- **Barra de Tareas.** Configurar los grupos de programas, los elementos dentro de cada grupo y los aspectos que se pueden configurar dentro de la barra de tareas.
- **Impresoras.** Definición de las impresoras a las que se puede acceder desde el equipo.
- **Panel de Control.** Configuración del ratón, color, teclado, cursores, sonidos... y todo aquello que se puede configurar desde esta aplicación. Dentro de la aplicación Sistema se pueden fijar las variables de entorno.
- **Accesorios.** Configuración de las aplicaciones que se encuentran dentro de Accesorios: Notepad, Paint, HyperTerminal, Clock...
- **Prompt de comandos.** Incluye todos los aspectos configurables para las ventanas de comandos: fuentes, posición de la ventana, colores, buffers....
- **Ayuda.** Bookmarks a la ayuda de NT.
- **Aplicaciones NT.** Los programas escritos para NT están diseñados de forma que cada usuario puede tener una configuración propia para esas aplicaciones. El perfil de un usuario guarda la configuración para cada una de las aplicaciones NT.

Anatomía de los perfiles de usuario

Los perfiles locales (o las copias locales de los perfiles, si empleamos perfiles móviles) se guardan en %SystemRoot%\Profiles. Dentro de ese directorio existirá un subdirectorio por cada perfil local que se haya creado. Los perfiles de cada usuario se guardan en un subdirectorio que coincide con el nombre del usuario. Por tanto existirá un subdirectorio por cada usuario que tenga un perfil local, aunque un usuario puede tener más de un directorio si se ha conectado desde esa estación a varios dominios. En ese caso, los directorios tienen extensión 000, 001... (véase Figura 15). Además de los perfiles locales de los usuarios, siempre encontraremos otros dos subdirectorios:

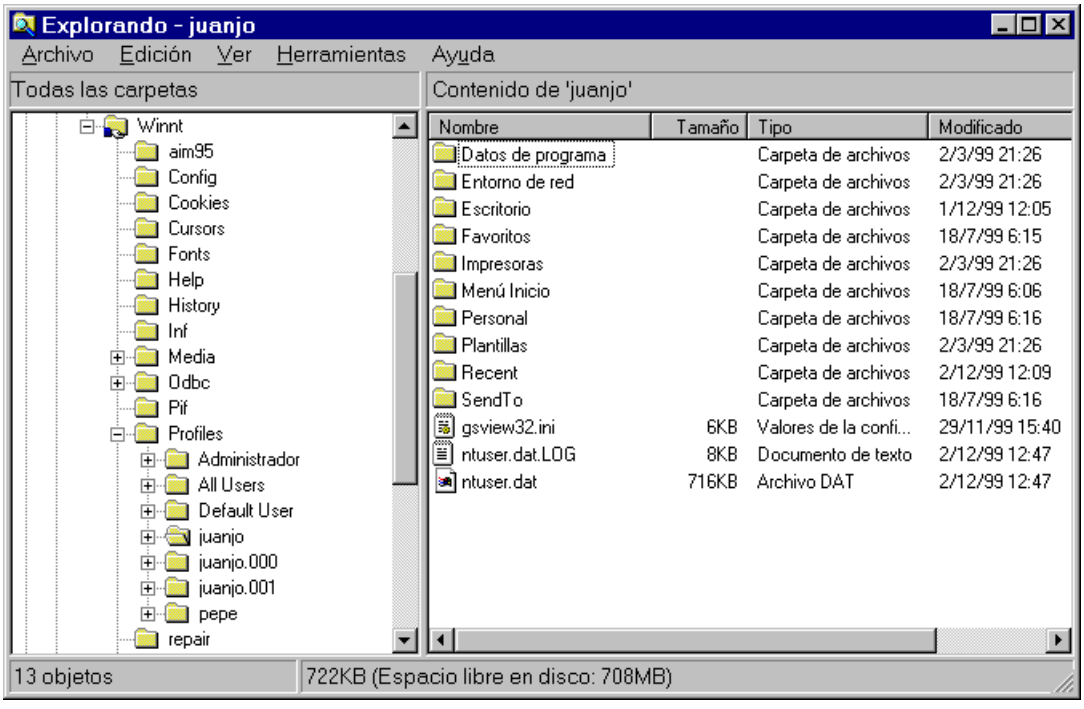


Figura 15 Directorio de Perfiles

- **Default User**. Guarda un perfil por defecto. Sirven para darle un perfil a los usuarios que no lo tienen ya que se conectan por primera vez al sistema.
- **All Users**. Guarda cosas comunes para todos los usuarios: grupos de programas y accesos directos. Concretamente tiene dos subdirectorios: Escritorio y Menú Inicio. Sólo el administrador puede crear estos grupos de programas comunes.

Dentro del perfil de cada usuario existen una serie de subdirectorios que contienen la información de configuración de ese usuario:

- **Datos de programa.** Algunas aplicaciones guardan las preferencias de los usuarios en ficheros. Estos ficheros se almacenan en este subdirectorio.
- **Escritorio.** Fichero y accesos directos que aparecen en el escritorio.
- **Favoritos.** Accesos directos a programas o localizaciones favoritas, en nuestro equipo o en nuestra red o incluso en Internet (páginas Web). También se pueden guardar bookmarks a páginas de ayuda.
- **Entorno de Red** (Oculto). Contiene los accesos directos a máquinas. Al igual que se establecen accesos directos para ficheros o aplicaciones, también se pueden crear para equipos.
- **Personal.** Se almacenan elementos de programas. Es un mini-directorio personal.
- **Impresoras** (Oculto). Accesos directos a las impresoras configuradas en el equipo. Aparece un acceso directo por cada una de ellas.
- **Recent** (Oculto). Accesos directos a los ficheros que se han abierto más recientemente.
- **Send To**. (Enviar A) Guarda accesos directos a los programas o elementos a los que se puede enviar un fichero. Aparecen cuando pulsamos el botón derecho del ratón sobre un fichero.
- **Menú Inicio**. Todos los grupos de programas y accesos directos que aparecen en el Menú Inicio.
- **Plantillas** (Oculto). Acceso directo a plantillas que usan programas como el Word o el PowerPoint.

Ficheros

NT 4.0	NTUSER.DAT	NTUSER.DAT.LOG	NTUSER.MAN
NT (previas)	USERNAME.USR		USERNAME.MAN
W95	USER.DAT	USER.DA0	USER.MAN

NTUSER.DAT: guarda los valores del registro.

NTUSER.DAT.LOG: para la tolerancia de fallos (registro transaccional). Evita cualquier fallo mientras NT actualiza NTUSER.DAT.

NTUSER.MAN: (solo lectura) se emplea para crear los perfiles obligatorios.

Los datos del perfil del usuario se guardan en un fichero llamado NTUSER.DAT. Los cambios que se van a hacer en ese fichero se reflejan en otro de nombre NTUSER.DAT.LOG, que es un fichero transaccional y que se emplea para evitar que un fallo en el sistema deje con inconsistencias el fichero NTUSER.DAT. En el caso de cualquier error durante una transacción, se puede reconstruir el fichero NTUSER.DAT a partir de la información contenida en NTUSER.DAT.LOG.

Tipos de perfiles

A pesar de que existen muchas variaciones respecto a los perfiles, en realidad se puede decir que existen tres tipos diferentes de perfiles:

Perfil Personal Local. Este perfil está disponible y se guarda en la máquina que emplea el usuario. Si el usuario emplea otro equipo no tendrá accesible su configuración. El usuario

puede cambiar cualquier elemento de su entorno de trabajo. El administrador no puede aplicar ninguna restricción a través del perfil.

Perfil Personal Móvil. El usuario mantiene el mismo perfil aunque se conecte desde distintas estaciones ya que la información del perfil se guarda en un controlador primario. Las opciones pueden ser cambiadas por el usuario y el administrador no puede aplicar restricciones.

Perfil Móvil Obligatorio. El perfil también se guarda en un servidor, por lo que es accesible desde cualquier estación. El usuario no puede cambiar la configuración. El administrador determina así le entorno de trabajo de los usuarios.

Es fundamental escoger el tipo de perfil más oportuno en función de los tipos de usuarios que tengamos, de la movilidad de los mismos, de su capacidad informática y de las restricciones que, como administradores, queramos fijar.

Perfil Personal Local

El perfil se crea y se mantiene localmente en cada equipo. Si un mismo equipo lo usa varios usuarios, se mantendrá un perfil por cada uno de los usuarios. Esos perfiles se guardan dentro de la carpeta %SYSTEMROOT%\Profiles, con lo que el perfil de un usuario estará en %SYSTEMROOT%\Profiles\%USERNAME%. Dentro de ese directorio se crea una carpeta para el perfil local de cada usuario, carpeta que tiene como nombre el nombre del usuario.

La primera vez que un usuario entra en sesión, el contenido del perfil Default User (también se encuentra en el directorio Profiles) y los grupos de programas comunes de All Users (también en Profiles) se combinan para crear los datos del perfil del nuevo usuario. Cuando el usuario salga de sesión, los cambios que haya hecho durante la misma en la configuración de su entorno de trabajo se salvan el directorio de su perfil. Cuando el usuario vuelva a entrar en sesión, la configuración de su entorno de trabajo será la que está almacenada en su perfil, es decir, la que dejó cuando salió de la sesión anterior.

Perfil Personal Móvil

En este caso los usuarios también mantienen un perfil personal, pero, a diferencia de los perfiles locales, el usuario mantendrá la misma configuración independientemente de la estación desde la que se conecte. Dado que el perfil debe ser accesible desde distintas estaciones, normalmente se guarda en un controlador del dominio.

Para crear un perfil móvil hay que indicar el path de ese perfil en la definición de la cuenta del usuario (Figura 3). Los cambios de configuración que el usuario realice durante una sesión se guardarán en ese perfil remoto cuando el usuario se desconecte. Aunque el perfil se mantiene en el servidor, **siempre se guarda una copia local**, por si existen problemas de red o en el servidor. Por tanto, el perfil se guarda en dos sitios: en el servidor y en la estación desde la que se conecta el usuario.

Cuando un usuario se conecta, la fecha del perfil almacenado en el servidor se compara con la de la copia que se guarda localmente. Si la versión más reciente es la del servidor, se emplea directamente; lógico ya que eso significa que el usuario se conectó más recientemente desde otra estación. Si por el contrario la versión más nueva es la local, se pregunta al usuario que configuración quiere emplear. Está última situación se produce cuando el usuario se desconecta y por cualquier causa (servidor caído, falta de permisos de escritura por sobrepasar cuotas...) no se ha podido salvar el perfil en el servidor. En ese caso y si hemos hecho cambios en nuestro perfil, puede interesarnos más cargar la copia local ya que será más reciente.

Para crear un perfil móvil hay que indicar en la cuenta del usuario el directorio donde se guardará la copia remota del perfil del usuario (Figura 3).

Pasos para crear perfiles móviles

1 Se comparte el directorio en el que pensemos guardar los perfiles con el nombre PROFILE$[7] y se le da permiso de Cambio o Control Total a TODOS.

[7] Al poner al final del nombre $ se evita que el recurso se pueda ver a través del entorno de Red.

2 No es necesario crear los directorios para cada usuario, se crean automáticamente.

3 En la cuenta de cada usuario se indica el path donde se va a guardar remotamente el perfil: \\SERVIDOR\PROFILES\nombre_del_usuario

4 La primera vez que se conecta un usuario, se crea el perfil (igual que los perfiles locales, con Default User y All Users) y se copia en el servidor.

5 En las siguientes veces que el usuario se conecte se comprobarán las dos versiones: la del servidor y la local, y se empleará la más reciente.

6 En caso de que el perfil local sea más reciente que el remoto, se pregunta al usuario cuál quiere emplear.

7 La copia local sirve para evitar problemas con la red o en el servidor.

Perfil Móvil Obligatorio

En este tipo de perfil, además de ser móvil, es decir, estar disponible desde cualquier estación, el usuario no puede guardar los cambios en la configuración de su entorno de trabajo, son perfiles de solo lectura. A diferencia de los dos tipos anteriores, el perfil móvil obligatorio no se establece cuando el usuario se conecta por primera vez. Para establecer un perfil obligatorio, hay que crearlo, esto es, establecer la configuración del entorno de trabajo, y después hay que asignárselo al usuario a través de la definición de su cuenta, en el campo correspondiente al perfil de usuario. Para garantizar que el usuario no pueda modificar su perfil hay que cambiar la extensión del fichero NTUSER.DAT y renombrarlo como **NTUSER.MAN** (MAN de mandatory).

Lo normal es emplear perfiles obligatorios para grupos de usuarios, de forma que varios usuarios usen el mismo perfil y no lo puedan modificar. En ese caso, si queremos cambiar cualquier aspecto del entorno para ese grupo de usuarios (pe. añadir los accesos directos o los grupos de programas para una nueva aplicación) sólo tendremos que actualizar el perfil que comparten.

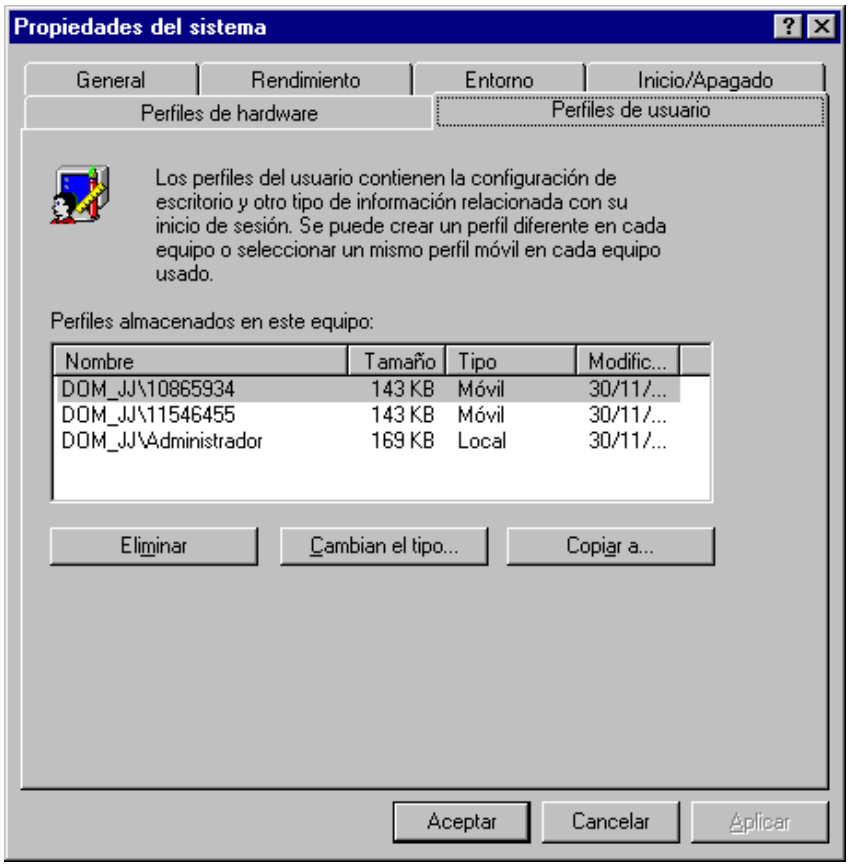


Figura 16 Aplicación Sistema

Como se ha dicho con anterioridad, es necesario crear primero el perfil (o lo que es lo mismo, configurar un entorno de trabajo) y luego asignar ese perfil al grupo de usuarios. El proceso podía ser más o menos el siguiente:

1. Se define una cuenta ficticia que emplearemos para predefinir el perfil (FICTICIA en adelante).
2. Nos conectamos con esa cuenta y configuramos el entorno de trabajo para ese hipotético usuario.
3. Salimos de esa sesión y entramos con la cuenta de Administrador.
4. Entramos en el directorio %SYSTEMROOT%\Profiles\FICTICIA. Dentro de ese directorio cambiamos la extensión del fichero **ntuser.dat** y lo llamamos **ntuser.man** (la extensión man es lo que indica que el perfil es obligatorio).
5. Ejecutamos la aplicación Sistema dentro del Panel de Control y elegimos la pestaña Perfiles de Usuario. Nos saldrán todos los perfiles que hay en el equipo y escogemos el de FICTICIA. Una vez elegido, lo copiamos en un directorio del servidor mediante el botón Copiar a.
6. Asignaremos ese perfil obligatorio a todos los usuarios que deseemos.

Este proceso se puede combinar con el empleo de plantillas para la definición de las cuentas de usuario.

Como se puede ver en el ejemplo de la Figura 16, tenemos localmente tres perfiles: el del Administrador y dos de usuarios con perfiles móviles. Para copiar cualquiera de esos perfiles en otra localización se emplea el botón *Copiar a*. Para decidir la ubicación de las copias se utiliza la ventana siguiente. En el campo *Copiar perfil a* se proporcionará una path UNC.

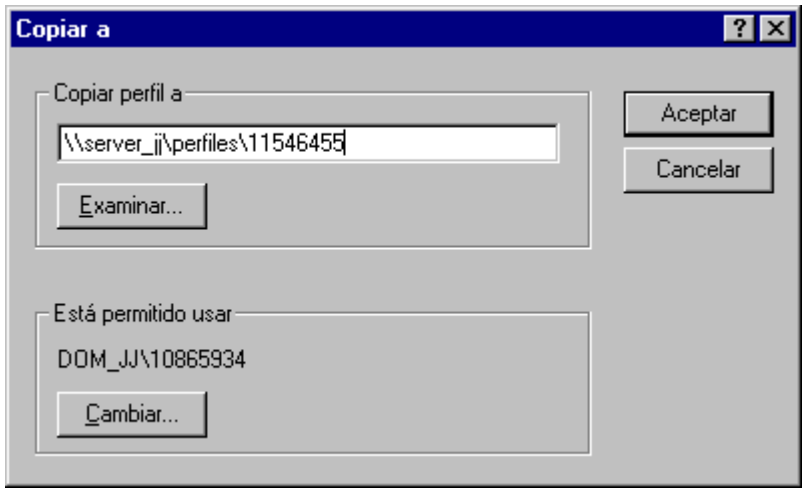


Figura 17 Copiar perfil a....

Los perfiles obligatorios se emplean cuando se desea restringir la capacidad de los usuarios para realizar ciertas tareas.

Variantes sobre perfiles obligatorios

Como se ha explicado en un párrafo anterior, la creación de perfiles obligatorios de solo lectura se realiza cambiando la extensión del fichero NTUSER.DAT y convertirlo en NTUSER.MAN. Sin embargo, también se puede cambiar la extensión del directorio donde se encuentre el perfil y asignarle la extensión MAN. Jugando con los cambios en esas dos extensiones, la del fichero y la del directorio, tenemos cuatro opciones distintas que determinan dos cosas: si el perfil es de solo lectura y/o si es obligatorio. Las variantes con las que nos podemos encontrar son las siguientes:

- **Cambiar sólo la extensión del fichero NTUSER.DAT**. Es la opción más habitual. Con este único cambio se consigue que el usuario no pueda cambiar la configuración de su entorno de trabajo. Sin embargo, a diferencia de otras de las variantes, el usuario podrá entrar en sesión aunque el perfil que se encuentra en el servidor no esté disponible, por un fallo en el servidor o por cualquier otra causa. En el caso de problemas con el servidor

se emplearán las copias locales de los perfiles. A esta variante se la debería denominar **PERFIL MÓVIL DE SOLO LECTURA**.

\\PDC\PROFILES\%USERNAME%

\\PDC\PROFILES\%USERNAME%\NTUSER.MAN

- **Cambiar sólo la extensión del directorio del perfil**. Aunque no es muy habitual emplear extensiones en directorios, si empleamos la extensión MAN en el directorio donde está el perfil daremos una funcionalidad distinta al perfil. En el caso de cambiar solamente la extensión del directorio, el usuario no podrá entrar en sesión si el perfil no se puede descargar desde el servidor. A diferencia de la opción anterior, el usuario si podrá cambiar su entorno de trabajo y recuperarlo en futuras sesiones. A esta variante habría que llamarla **PERFIL MÓVIL OBLIGATORIO**, ya que el usuario no puede entrar en sesión si no tiene su perfil, esto es, no se pueden emplear copias locales.

  \\PDC\PROFILES\%USERNAME%.MAN

  \\PDC\PROFILES\%USERNAME%.MAN\NTUSER.DAT

- **Cambiar ambas extensiones**. Con esta opción se consiguen los dos efectos anteriores: el perfil es obligatorio, el usuario no puede entrar si no es con ese perfil, y además el perfil sería de solo lectura. A esta variante se la debería denominar **PERFIL MÓVIL OBLIGATORIO DE SOLO LECTURA**.

  \\PDC\PROFILES\%USERNAME%.MAN

  \\PDC\PROFILES\%USERNAME%.MAN\NTUSER.MAN

No se cambia ninguna de las extensiones. **En este caso el perfil coincide con el PERFIL MÓVIL.**

\\PDC\PROFILES\%USERNAME%

\\PDC\PROFILES\%USERNAME%\NTUSER.DAT

O dicho de forma más breve:

NTUSER.MAN Perfil de solo lectura, el usuario no pueda cambiar su configuración.

DIRECTORIO.MAN El usuario no puede entrar en sesión salvo que se descargue el perfil desde ese directorio.

¿Cómo se configura un perfil obligatorio?

Los pasos para crear un perfil obligatorio en cualquiera de sus variantes son los siguientes:

1. Crear un nuevo usuario
2. Entrar como ese usuario y configurar el entorno de trabajo.
3. Salir y entrar como Administrador.
4. Usar la aplicación Sistema y copiar el perfil recién creado en algún directorio.
5. Renombrar fichero y/o directorio según la funcionalidad que deseemos conseguir.
6. Asignar la localización del perfil en la(s) cuenta(s) de usuario que queramos que tengan ese perfil.

Usos de cada uno de los perfiles

Para elegir entre los distintos perfiles podemos considerar las siguientes circunstancias:

Perfiles locales

- en entornos variados Windows NT y Windows 95
- cuando los usuarios se conectan desde la misma estación
- dan menos trabajo pero ofrecen menos control sobre las configuraciones de los usuarios
- para ejercer ese control hay que emplear las directivas del sistema

Perfiles móviles

- cuando los usuarios entren al sistema desde distintas estaciones
- permiten un control centralizado de los perfiles
- dificultan el tráfico en la red y hacen las entradas al sistema más lentas
- se siguen manteniendo copias locales

Perfiles obligatorios

- permiten un mayor control
- se desperdicia menos espacio en disco
- se puede emplear los mismos perfiles para varios usuarios simultáneamente
- los usuarios no pueden decidir su propio entorno de trabajo

Otros perfiles

Además de las tres variedades de perfiles que maneja NT, existen otros perfiles que conviene conocer para su correcto uso.

Perfil por defecto

Cuando un usuario carece de un perfil, el usuario puede seguir accediendo al sistema gracias a los perfiles por defecto. Se utilizan en la primera conexión de los usuarios. En concreto, se emplean en las siguientes circunstancias:

- Cuando es la primera vez que el usuario entra al sistema
  - y el usuario debe emplear perfiles locales
  - o cuando el usuario utiliza un perfil móvil y no se puede acceder al path de red que tiene asignado el usuario en la definición de su cuenta y además no existe una copia local del mismo en el equipo
  - o cuando el usuario tiene un perfil de sólo lectura y tampoco tenemos acceso a él.
- Cuando un usuario se conecta con una cuenta de Invitado.

En cualquiera de esas situaciones se emplea el perfil por defecto. Cuando el usuario salga de sesión, cualquier cambio que haya efectuado no afectará al perfil por defecto y se guardará en un directorio local para el perfil de ese usuario (siempre que no entre con la cuenta de Invitado). Cuando el usuario se vuelva a conectar, NT empleará la nueva versión del perfil, no el perfil por defecto.

Existen dos tipos de perfiles por defecto:

- **Local**. NT crea un directorio DEFAULT USER dentro de %SYSTEMROOT%\Profiles que contiene el perfil por defecto local. Si queremos adaptar y crear nuestro propio perfil por defecto, habrá que copiar el perfil que deseemos en ese subdirectorio.
- **Del dominio**. Si creamos una carpeta DEFAULT USER en el recurso compartido NETLOGON del controlador primario tendremos un perfil por defecto que podrá ser empleado desde todos los equipos del dominio, con la ventaja de no tener que configurar localmente cada perfil por defecto local.

Lo mejor para crear un perfil por defecto, ya sea local o del dominio es crear una cuenta ficticia[8], configurar su entorno, es decir, su perfil, y copiarlo en el directorio apropiado. Si lo hacemos en el Default User del directorio Profiles habremos creado un perfil por defecto local. Si por el contrario lo hacemos en el Default User de NETLOGON del controlador primario estableceremos un perfil por defecto para todo el sistema.

(GRÁFICO COMO SE CREA EL PRIMER PERFIL)

[8] No se debe crear una cuenta Default User esperando que el sistema guarde el perfil en ese directorio. Si se creará esa cuenta el sistema utilizaría el directorio Default User.000. Cuando dentro de Profiles aparecen directorio con una extensión numérica, indica que ese usuario ha empleado el equipo para conectarse con distintos dominios

Cuando un usuario se conecta por primera vez a un dominio, primero se chequea el recurso compartido NETLOGON (%SYSTEMROOT%\SYSTEM32\REPL\IMPROT\SCRIPTS) para ver si existe un directorio Default User. Si existe se asigna el perfil por defecto del dominio al usuario, perfil que durante la sesión podrá cambiar el propio usuario. Si no existe, se empleará el perfil contenido en el Default User local.

Perfil del sistema

Es el perfil que se emplea cuando no hay ningún usuario conectado al sistema. Es decir, es el perfil que está activo cuando se muestra la pantalla de Inicio de Sesión en la que el usuario debe pulsar Ctrl+Alt+Del para iniciar una sesión. A través de este perfil se puede controlar el protector de pantalla o la imagen del escritorio que se verá cuando no hay usuarios conectados.

Las opciones de configuración de este perfil se puede ver y fijar a través del registro de NT. Dentro del árbol HKEY_USERS hay una clave .DEFAULT donde se encuentra la configuración del perfil del sistema. A pesar de que el nombre puede llevar a engaño, este perfil **NO es ninguno de los perfiles por defecto**.

Este perfil se guarda en %SYSTEMROOT%\SYSTEM32\CONFIG\.DEFAULT

Consejos sobre perfiles

Unos breves consejos para acabar con el tema de los perfiles:

- Si empleamos cualquier tipo de perfil móvil, se deben borrar periódicamente las copias locales. En entornos de ese tipo, como pasa en el dominio de INFORMATICA, las estaciones acaban manteniendo muchas copias locales no demasiado útiles. Para borrarlas se puede emplear la aplicación Sistema o utilizar el Editor de Directivas y configurarlo para que borre las copias locales después de un cierto número de días.
- No se debería emplear perfiles móviles cuando estamos en una red WAN. La carga de los perfiles es un proceso lento y más aún si nos movemos en una red donde las distancias son grandes. En ese tipo de redes es mejor utilizar perfiles locales.
- Tampoco se deben usar perfiles móviles cuando los usuarios se conectan a través del servicio remoto (RAS). Estas conexiones suelen ser lentas y no es lógico emplearlos, es mucho mejor utilizar perfiles locales.
- Hay que tener especial cuidado con algunas configuraciones hardware y sobre todo con aquellas relacionadas con las tarjetas de vídeo y los monitores. Dado que los perfiles guardan la configuración del escritorio, lo que incluye resolución y número de colores, si no tenemos cuidado podríamos asignar a los perfiles por defecto, o al perfil de un usuario, una configuración inadecuada para el hardware de algunos equipos. Esta misma consideración hay que tenerla en cuenta cuando se emplea un perfil obligatorio para un conjunto de usuarios. En ese caso hay que asegurarse de que la configuración común sea compatible con los equipos que ese grupo de usuarios emplearán.

Perfiles Windows 95

Windows 95 también puede emplear perfiles, aunque no se establecen por defecto cuando se instala el sistema, hay que habilitarlos explícitamente. Funcionan de forma similar a como lo hacen los de NT, sin embargo existen pequeñas diferencias que hay que considerar si deseamos emplearlos:

- Difieren en el nombre de los archivos. (User.dat, User.da0y User.man)
- Los perfiles de Windows 95 no guardan todos los elementos del escritorio, solamente los accesos directos (.lnk) y los ficheros de información de programas (.pif).
- Los clientes Windows 95 no usan el path del perfil para cargar un perfil móvil; los perfiles móviles se cargan desde el directorio particular del usuario. Es decir, hay que almacenar el perfil de los usuarios dentro de sus directorios particulares.
- Los perfiles obligatorios se pueden emplear, pero tienen que crearse para cada usuario. Dado que los perfiles no-locales deben estar en el directorio particular, el Administrador

deberá crear el perfil obligatorio y copiarlo en los directorios personales de todos los usuarios a los que desee asignárselo.

- No soportan la información sobre los grupos de programas comunes.
- No soporta perfiles por defecto del sistema.

Los perfiles de Windows 95 no se pueden intercambiar con los de NT ya que las claves que emplean en el registro difieren en ambas versiones. Son idénticas salvo en el directorios Datos de Programas ya que Windows 95 no lo soporta. Cuando un usuario se conecta desde una estación95, se cheque en el registro la siguiente entrada

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Profile List,

para ver si existe una entrada para ese usuario. Si existe, el sistema trata de buscar la copia local del perfil para ese usuario y además chequea el directorio particular del usuario para ver si tiene una copia móvil. Si existen las dos, emplea la más reciente. Los cambios que realice el usuario durante la sesión se reflejarán en cualquier caso localmente y si el usuario tiene un perfil móvil, también se guardará en el servidor.

Directivas del Sistema

Como se ha explicado durante toda el apartado previo, el look & feel, la configuración del entorno de trabajo de los usuarios se guarda en el perfil. Como Administrador, se pueden controlar esas configuraciones de dos maneras: mediante la utilización de perfiles obligatorios o con el Editor de Directivas del Sistema.

Figura 18 Editor de Directivas del Sistema

El Editor de Directivas del Sistema permite establecer las políticas del sistema, pudiendo crearse opciones para todos los equipos y todos los usuarios o establecer configuraciones especiales para ciertos usuarios, grupos o incluso para ciertos equipos dentro de nuestro dominio.

Nos permite controlar lo que los usuarios pueden hacer desde su entorno de trabajo, pero no llegan a dar el control absoluto que nos proporcionan los perfiles obligatorios. Sin embargo, te permite controlar algunos aspectos del entorno de los usuarios, impidiéndoles el acceso a zonas que no deseas que cambien. Por ejemplo, tal vez te gustaría que el protector de pantalla salga tras dos minutos de inactividad y que tenga contraseña. Este tipo de cosas se establecen en sistemas donde la seguridad es importante y pueden implementarse con el Editor de Directivas. Además te permite controlar los procesos de conexión al sistema y el acceso a través de la red. Por ejemplo, puedes decidir si el botón de Cerrar el Sistema va a estar habilitado en la ventana de Inicio de Sesión.

Plantillas

NT incluyen una serie de plantillas de políticas de sistemas para facilitar tu labor proporcionando un punto de partida para la edición de opciones del registro en los equipos

con Windows NT Server, Workstation y Windows 95. Dentro del subdirectorio %SYSTEMROOT%\inf se encuentra tres plantillas:

- **WINDOWS.ADM.** Plantilla para Windows 95.
- **WINNT.ADM.** Plantilla para Windows NT.
- **COMMON.ADM.** Contiene las opciones comunes de las dos plantillas anteriores para Windows NT y 95.

Crear una nueva directiva por defecto para el Sistema

Se puede crear una directiva de forma que afecte a todos los equipos del dominio o todos los usuarios. **La nueva directiva debe guardarse en un fichero de nombre NTCONFIG.POL dentro del recurso compartido NETLOGON**. De esta forma nos garantizamos que la directiva afecte a todo el sistema. Para crearla hay que ejecutar el Editor de Directivas (Figura 18) y ejecutar el comando *Nueva Directiva*. Tendremos en la ventana dos iconos:

- uno que representa las directivas para todos los equipos del dominio y
- otro que contiene las directivas para los usuarios.

Haciendo doble click en cualquiera de ellos estableceremos las opciones que deseemos incluir en nuestra directiva. Las opciones se agrupan bajo un icono que representa un libro. Dentro de esos 'libritos' están cada una de las opciones que se pueden configurar. Al lado de cada opción tenemos un check box con tres posibilidades:

- **Vacío.** Aparece el cuadrito en blanco. Eso indica que la directiva está deshabilitada y no se emplea.
- **Marcado.** Aparece el cuadro con una cruz. Esto habilita la directiva. En alguna de ellas hará falta configurar algunos parámetros.
- **Sombreado.** Aparece el cuadro sombreado en gris. Eso indica que la directiva no se cambia y permanece en el estado en que se encuentre.

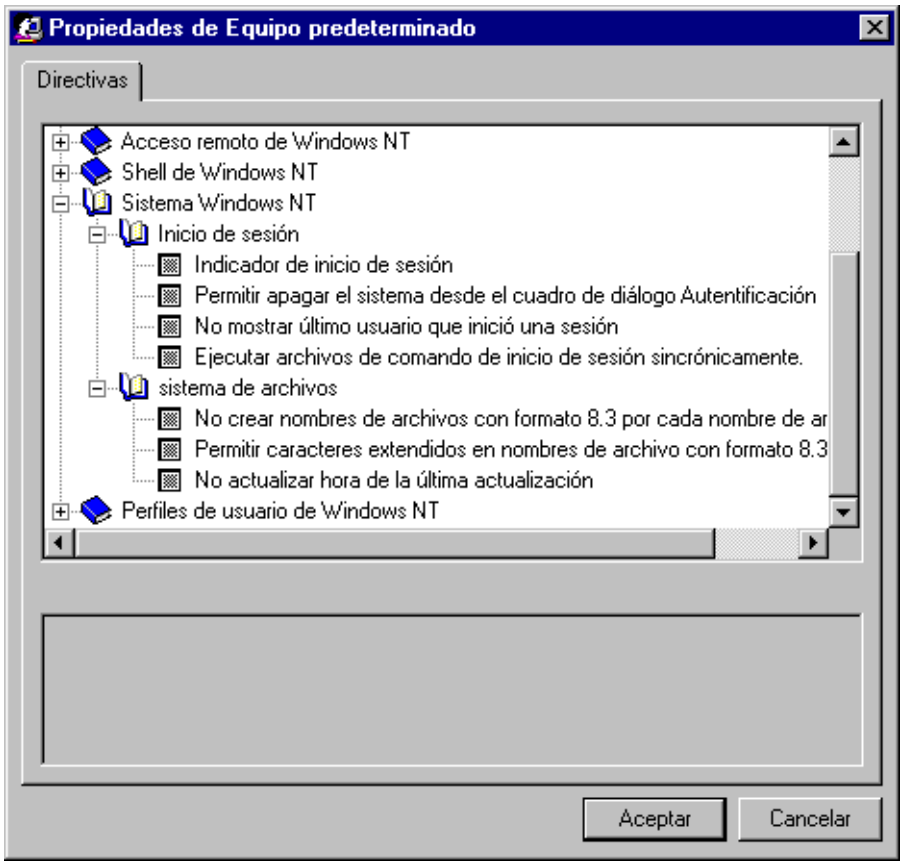


Figura 19 Directivas para el equipo por defecto

Equipo predeterminado

Dentro de Equipo Predeterminado se pueden configurar detalles que afectarán a cualquier equipo del dominio. Por ejemplo, en la Figura 19, se puede ver las cosas que se pueden configurar sobre el inicio de sesión: si en la ventana se muestra o no el botón para apagar el sistema, o si en el campo reservado al nombre de usuario se muestra el del último usuario que inicio una sesión en el equipo. Como se puede ver, son detalles independientes del usuario y que afectan a todo el equipo.

Usuario predeterminado

A través del icono de Usuario predeterminado podremos configurar aspectos que tienen más relación con el entorno de trabajo de los usuarios y, sobre todo, aquellas cosas que el usuario puede y no puede hacer. Como se puede observar en la ventana de la , se pueden restringir aspectos de la pantalla, o del escritorio (tapiz y la combinación de colores) o también impedir que los usuarios ejecuten el editor del Registro de NT.

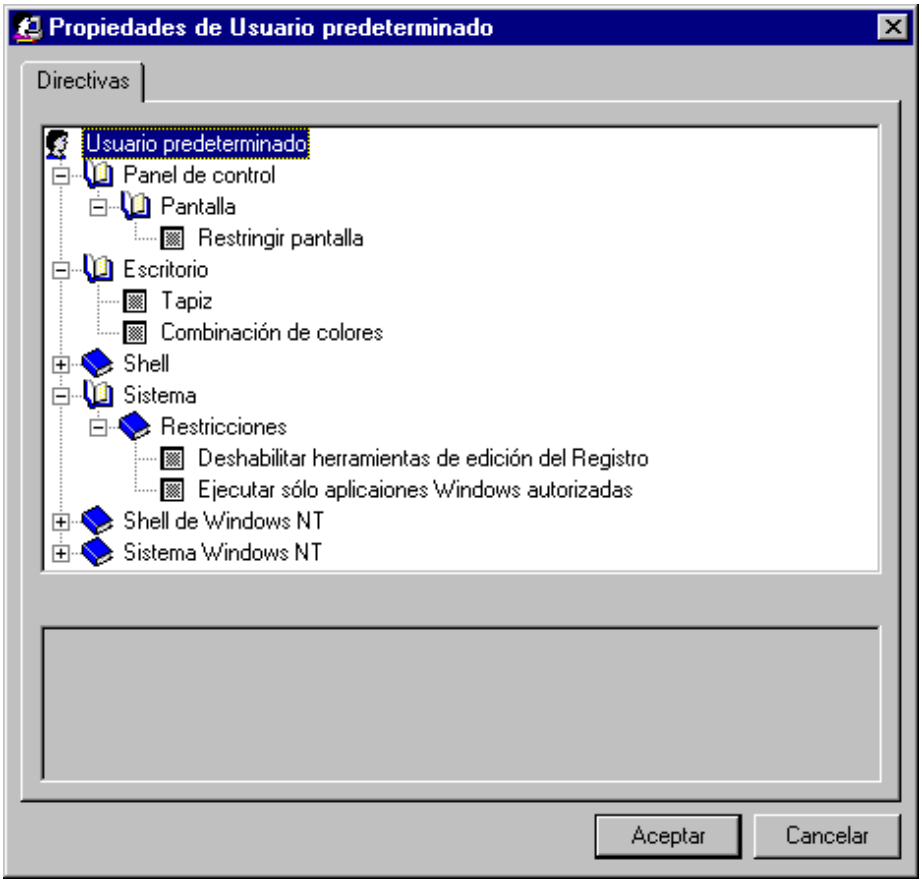


Figura 20 Directivas para el usuario por defecto

Figura 21 Directivas con restricciones para un equipo, un grupo y un usuario

Directivas específicas para equipos, usuarios y grupos

Además de configurar directivas por defecto para los equipos y usuarios del dominio, también podemos establecer directivas específicas tanto para equipos como para usuarios y grupos globales de usuarios. Para ello habrá que emplear los comandos *Agregar ...* dentro del menú *Edición*.

En la Figura 21, se aprecia una directiva, donde además de las configuraciones por defecto, incluye restricciones para el equipo Server_jj, para el grupo global Alumnos de ASO y para el usuario 10865934. Obviamente las directivas tienen su orden de prioridad. Por ejemplo, para el usuario 10865934 las directivas impuestas específicamente para él prevalecen sobre las del usuario por defecto. Es importante tener en cuenta que cada opción tiene tres posibles valores, y uno de ellos es dejarlo como esté.

Las opciones que se pueden configurar para usuarios y grupos son las mismas que se configuran para el usuario predeterminado. Lo mismo pasa con las opciones del equipo predeterminado y las del equipo Server_jj, son iguales.

Después de establecer las opciones que queramos hay que salvar todo ello dentro de un fichero que debe llamarse NTCONFIG.POL (POL de Policy) y que debe ubicarse en NETLOGON.

Las directivas y el Registro de NT

Cada opción que se configura con esta herramienta corresponde a una entrada en el Registro de NT (véase apartado Registro de NT). Es decir, al final lo que se establece con el Editor de Directivas es hacer que el Registro contenga unos valores determinados cuando el usuario entre en sesión en un equipo. Esos valores suelen representar restricciones o configuraciones para la sesión y son una forma elegante de modificar valores del Registro. De hecho, el Editor de Directivas tienen un comando que permite la modificación de Registros de otros equipos.