- Trabajo realizado por el equipo de la Biblioteca Digital de la Fundación Universitaria San Pablo-CEU
- Me comprometo a utilizar esta copia privada sin finalidad lucrativa, para fines de investigación y docencia, de acuerdo con el art. 37 del T.R.L.P.I. (Texto Refundido de la Ley de Propiedad Intelectual del 12 abril 1996)

Capítulo 14

CONFIGURACIÓN Y GESTIÓN

La responsabilidad de configurar y gestionar el servidor de la red corresponde al administrador.

Los pasos a seguir son:

- Instalar todo el cableado de la red.
- Instalar las tarjetas de red en los ordenadores.
- Instalar los discos duros, impresoras y otros periféricos.
- Conectar todos los equipos a la red.
- Instalar los sistemas operativos de todas las estaciones de trabajo.
- Instalar el sistema operativo de red en el servidor, identificando cada estación de trabajo y los dispositivos conectados.

Una vez instalado el sistema operativo, se ha de proceder a la configuración de la red, teniendo que realizar, entre otros, los siguientes pasos:

- Desarrollar la estructura de directorios.
- Copiar los programas de aplicaciones y los datos.
- Crear el guión de entrada del sistema y de los usuarios.
- Preparar el mapa y la asignación de unidades.
- Dar de alta a los usuarios y grupos.
- Establecer la administración de seguridad.
- Establecer la configuración de seguridad.
- Localización de problemas.
- Establecer la seguridad del servidor (ver capítulo 13).

EL DESARROLLO DE LA ESTRUCTURA DE DIRECTORIOS

Sin duda, se pueden emplear un número ilimitado de estructuras de directorios en un servidor y se debe estudiar cuidadosamente la que mejor se adapta a las necesidades de cada empresa.

Cuando se planea la disposición de los directorios, se deben considerar tres circunstancias importantes:

- La simplicidad de la estructura. No se debe hacer que la estructura de directorios sea tan complicada que los usuarios no puedan encontrar los programas ni los archivos de datos.
- La seguridad. Muchas de las previsiones de seguridad de un sistema operativo de red son relativas a los directorios y subdirectorios.
- La lógica. Los archivos deben estar agrupados lógicamente para aumentar la eficiencia de la red.

Para la utilización por los usuarios, se deberían crear varios directorios en el servidor:

- El directorio **PROGRAMA** que tendrá varios subdirectorios que contendrán los programas de aplicaciones necesarios.
- El directorio **UTILIDAD** que proporcionará un almacenamiento a los diversos programas de utilidad.
- El directorio **PRIVADO** que se utilizará para almacenar los archivos de datos individuales de cada usuario de la red local.
- El directorio **GRUPOS** que tendrá subdirectorios que se comparten por individuos del mismo grupo de trabajo.
- El directorio **PUBLICO** que almacenará cualquier archivo cuyo acceso esté permitido a todos los usuarios de la red.

Esta fórmula satisface los criterios establecidos anteriormente para la disposición de un directorio:

1. Es simple. Hay directorios específicos y sus nombres son un claro reflejo de lo que contienen.
2. La estructura de los directorios facilita una seguridad efectiva, permitiendo que los atributos de seguridad se asignen a los usuarios individualmente y a los grupos. Por ejemplo, el acceso a los archivos del directorio **GRUPOS** puede estar restringido a los usuarios individuales de la red que no pertenezcan a un grupo determinado.
3. Los archivos están agrupados lógicamente en los directorios. Los programas de aplicación están separados de los archivos de datos y los datos de cada usuario están separados.

COPIAR LOS PROGRAMAS DE APLICACIONES Y LOS DATOS

El paso siguiente es cargar en el servidor el programa o los programas de aplicaciones, y los datos que puedan ser necesarios.

En general, los procedimientos de una instalación de un programa en cualquier servidor son similares a los de una aplicación en un ordenador aislado. La única diferencia está en dónde se cargan los archivos en el disco duro.

Es conveniente asegurarse de que se está utilizando una versión del programa apropiada para funcionar en redes. No es adecuado utilizar versiones para un solo usuario (monopuesto) en una red, ya que tales versiones frecuentemente no funcionan como deben cuando varios usuarios intentan acceder a los mismos archivos.

Para cargar de forma adecuada las aplicaciones, debe seguirse cuidadosamente la documentación de instalación. De otro modo, pueden surgir problemas tales como anomalías en el programa ocasionadas por la señalización incorrecta de los archivos.

EL GUIÓN DE ENTRADA

En *NetWare*, un guión de entrada o **login script** no es más que un pequeño programa de ordenador, que contiene instrucciones que se ejecutan cuando un usuario establece contacto (**login**) con la red. El guión de entrada del sistema proporciona un conjunto uniforme de comandos para todos los usuarios de la red. Solamente el administrador de la red, o quién él autorice, puede crear o modificar los guiones de entrada del sistema.

Además, cada usuario puede tener un guión de entrada personal que se ejecuta después de haberlo hecho el guión de entrada del sistema. Ambos, el administrador y el usuario, pueden crear y modificar los guiones de entrada personales.

Cuando se escriben los guiones de entrada para una red, la mejor estrategia es definir el mayor número de comandos que sea posible en el guión del sistema. Esto hace el mantenimiento más fácil ya que se tiene que modificar un solo guión, cuando sean necesarios los cambios.

Hay cuatro tipos de guión de entrada:

- Contenedor.
- Perfil.
- Usuario.
- Defecto

El orden de ejecución de los cuatro guiones cuando se realiza la conexión es el siguiente:

- Guión de entrada del objeto contenedor.
  - Si existe, se ejecuta y continúa.
  - Si no existe, continúa.
- Guión de entrada del objeto perfil.
  - Si existe, se ejecuta y continúa.
  - Si no existe, continúa.
- Guión de entrada del objeto usuario.
  - Si existe; se ejecuta y finaliza.
  - Si no existe continúa.
- Guión de entrada por defecto.
- Se ejecuta si no hay guión de entrada del objeto usuario.

Guión de entrada del Objeto Contenedor

El guión de entrada del objeto contenedor proporciona un conjunto uniforme de comandos para todos los usuarios de la red que se conectan a dicho contenedor y sustituye al guión de entrada del sistema de versiones anteriores de *NetWare*.

Es el primero que se ejecuta al establecer la conexión y se utiliza para establecer asignaciones de unidades a todos los directorios de aplicaciones, establecer una asignación de unidad al directorio privado de cada usuario, establecer una unidad de búsqueda al directorio *PUBLIC*, enviar mensajes a todos los usuarios del contenedor y conectar a la impresora por defecto de dicho contenedor.

Solamente el administrador de la red, o quién él autorice, puede crear o modificar este tipo de guión de entrada.

Guión de entrada del objeto Perfil

También se pueden crear guiones de entrada del objeto Perfil para aquellos usuarios o grupos que necesitan entornos similares pero que no se encuentran en el mismo objeto contenedor.

Se ejecuta después del guión de entrada del objeto contenedor y se utiliza para establecer asignaciones de unidades a directorios de aplicaciones específicos, establecer unidades de búsqueda para directorios de aplicaciones, enviar mensajes a los usuarios del perfil y conectar a impresoras especiales para dicho perfil.

Solamente el administrador de la red, o quién él autorice, puede crear o modificar este tipo de guión de entrada.

Guión de entrada del objeto Usuario

Además, cada usuario puede tener un guión de entrada personal que se ejecuta después de haberlo hecho los guiones anteriores.

Se ejecuta después de los guiones de entrada anteriores y se utiliza para establecer asignaciones de unidades a directorios específicos de dicho usuario, enviar mensajes a usuarios específicos y conectar a impresoras específicas para dicho usuario.

Tanto el administrador como el usuario, pueden crear y modificar el guión de entrada del usuario.

Guión de entrada por defecto

Se ejecuta únicamente en caso de no existir el guión de entrada del objeto usuario y no puede ser editado ya que está contenido dentro del programa que realiza la conexión.

Los comandos de los guiones de entrada

NetWare reconoce varios comandos para guiones de entrada y también permite ejecutar algunos programas externos durante su ejecución.

La lista siguiente indica los comandos que se pueden emplear y sus funciones:

#	Se utiliza para ejecutar un programa externo y al finalizar devuelve el control al guión de entrada.
@	Se utiliza para ejecutar un programa externo (sólo para estaciones *Microsoft Windows*).
ATTACH	Conecta al usuario a servidores *NetWare* versiones 2.x o 3.x mientras se ejecuta el guión de entrada.
BREAK	Permite al usuario cancelar la ejecución del guión de entrada al presionar [**Ctrl**]+[**Pausa**] o [**Ctrl**]+[**C**].

CLS	Sirve para limpiar la pantalla de la estación de trabajo durante el proceso de conexión a la red (sólo para *DOS* y *OS/2*).
COMSPEC	Especifica la localización de la versión correcta del archivo *COMMAND.COM* (sólo para *DOS*).
CONTEXT	Sirve para definir el contexto actual de un usuario en el árbol del Directorio.
[F]DISPLAY	Si se especifica **DISPLAY**, se visualizan el contenido de un archivo de texto especificado. Si se especifica **FDISPLAY**, se filtran los caracteres especiales en el documento y se visualiza solamente el texto.
DOS BREAK	Permite al usuario la cancelación de cualquier programa o comando del *DOS* después del guión de entrada (sólo para *DOS*).
DOS SET	Coloca un valor específico en una variable en el entorno *DOS* (sólo para *DOS*).
DOS VERIFY	Verifica si el dato copiado en una unidad local se ha hecho sin error (sólo para *DOS* y *Windows 3.x*).
DRIVE	Especifica una unidad por defecto en lugar de la primera unidad de la red.
EXIT	Termina la ejecución del guión de entrada (también se puede utilizar para ejecutar un archivo *COM*, *EXE*, *BAT* o un comando interno del *DOS*).
FIRE PHASERS	Emite un sonido que puede utilizarse para alertar al usuario sobre algún error o cualquier otra condición.
GOTO	Ejecuta una parte del guión de entrada fuera de la secuencia normal.
IF...THEN	Permite el procesamiento condicional de los comandos del guión.
INCLUDE	Permite la inclusión de otros guiones como parte de los guiones que se están procesando.

LASTLOGINTIME	Muestra en pantalla la última vez que el usuario se conectó a la red.
MACHINE	Relaciona el nombre de la máquina de la estación de trabajo con un nombre especificado (sólo para *DOS* y *Windows 3.x*).
MAP	Utilizado en una gran variedad de parámetros para manejar y visualizar las asignaciones de unidades y unidades de búsqueda a directorios de red.
NO_DEFAULT	Permite no ejecutar el guión de entrada por defecto si no existe el guión de entrada del usuario.
NOSWAP	Impide que el guión de entrada salga de la memoria convencional al ejecutar el comando # (sólo para *DOS*).
PAUSE	Hace una pausa en la ejecución del guión de entrada.
PCCOMPATIBLE	Sirve para activar el mandato *EXIT* si el nombre de la máquina de la estación de trabajo no es un ordenador compatible *IBM*.
PROFILE	Permite ejecutar el guión de entrada del objeto Perfil indicado.
REMARK	Permite la inserción de un texto explicativo en el guión de entrada.
SCRIPT SERVER	Usado sólo en *NetWare* 2 y 3 para establecer el servidor de dónde se va a leer el guión de entrada (no tiene efecto en servidores *NetWare* 4 ó 5).
SET	Se utiliza para establecer un valor para una variable de entorno.
SET_TIME	Se utiliza para que la hora de la estación de trabajo sea la misma que la del servidor *NetWare* al que se conecta la estación en primer lugar.
SHIFT	Cambia los argumentos de un comando a la siguiente variable.

SWAP	Permite trasladar el guión de entrada fuera de la memoria convencional a una zona de memoria alta o al disco si no se cuenta con suficiente memoria en la estación de trabajo al ejecutar un comando # (sólo para *DOS*).
TERM	Se utiliza para finalizar el guión de entrada y devolver un código de error (se utiliza sólo con guiones del *Lanzador de Aplicaciones de Z.E.N. works*)
TREE	Se utiliza sólo con usuarios que han de conectarse a varios *NDS*.
WRITE	Visualiza mensajes en la pantalla durante el proceso del guión de entrada.

Las variables de los guiones de entrada

Además de los comandos descritos anteriormente, se pueden utilizar variables para personalizar los guiones de entrada.

Cuando utilice variables en comandos de los guiones de entrada ha de observar las siguientes convenciones:

- Se pueden utilizar con comandos como *IF...THEN*, *MAP* y *WRITE*. También se pueden usar con comandos donde se ha de especificar un camino de búsqueda como *COMSPEC*.
- Ha de escribir el nombre de la variable exactamente como figura en el listado y con algunos comandos debe ir precedida por el signo de porcentaje (%).
- Las variables pueden situarse junto a texto literal en un comando WRITE. Sin embargo, la variable debe estar en mayúsculas y precedida por el signo de porcentaje (%) y el texto literal entre comillas.

Entre las variables que se pueden utilizar se encuentran:

ESTACIÓN DE TRABAJO

MACHINE	Devuelve el tipo de ordenador (*IBM_PC*, etc.).
NETWARE_REQUESTER	Devuelve la versión del *NetWare Requester*.

OS	Devuelve el tipo de sistema operativo de la estación de trabajo (*MSDOS*, *OS2*, etc.).
OS_VERSION	Devuelve la versión del sistema operativo de la estación de trabajo (3.30, etc.).
P_STATION	Devuelve el número de nodo de la estación de trabajo (12 dígitos hexadecimales).
PLATFORM	Devuelve a plataforma del sistema operativo de la estación de trabajo: *DOS*, *OS2*, *WIN* (*Windows 3.1*), *WNT* (*Windows NT*), *W95* (*Windows 95*) o *W98* (*Windows 98*).
SHELL_TYPE	Devuelve la versión del *shell* del DOS de la estación de trabajo (1.02, etc.).
SMACHINE	Devuelve el nombre corto del ordenador (IBM, ...).
STATION	Devuelve el número de conexión de la estación de trabajo.
WINVER	Devuelve la versión del sistema operativo *Windows* de la estación de trabajo.

FECHA

DAY	Devuelve el número del día (del 01 al 31).
DAY_OF_WEEK	Devuelve el día de la semana (lunes, martes, etc.).
MONTH	Devuelve el número del mes (del 01 al 12).
MONTH_NAME	Devuelve el nombre del mes (enero, febrero, etc.).
NDAY_OF_WEEK	Devuelve el número del día en la semana (del 1=domingo al 7=sábado).
SHORT_YEAR	Devuelve los dos últimos dígitos del año (98, 99, etc.).
YEAR	Devuelve los cuatro dígitos del año (1998, 1999, etc.).

MISCELÁNEOS

ERROR_LEVEL	Devuelve un número de error (0=no hay errores).
%n	Reemplazado por parámetros que el usuario indica desde la línea de comandos de la utilidad *LOGIN*.

PROPIEDADES DE OBJETOS

Nombre propiedad	También se pueden usar valores de propiedades de objetos *NDS* como variables (si el valor de la propiedad incluye un espacio, ha de ir encerrado entre comillas).

RED

FILE_SERVER	Devuelve el nombre del servidor *NetWare*.
NETWORK_ADDRESS	Devuelve el número de red *IPX* externo (8 dígitos hexadecimales).

TIEMPO

AM_PM	Devuelve si es am o pm.
GREETING_TIME	Devuelve la parte del día (mañana, tarde, o noche).
HOUR	Devuelve la hora (del 1 al 12).
HOUR24	Devuelve la hora (del 00 al 23; 00=medianoche).
MINUTE	Devuelve los minutos (del 00 al 59).
SECOND	Devuelve los segundos (del 00 al 59).

USUARIO

CN	Devuelve el nombre del usuario tal y como se encuentra en el *NDS*.
FULL_NAME	Devuelve el nombre completo del usuario.
LAST_NAME	Devuelve los apellidos del usuario.

LOGIN_CONTEXT	Devuelve el contexto donde se conecta el usuario.
LOGIN_NAME	Devuelve el nombre de conexión del usuario.
MEMBER OF<grupo>	Se utiliza para preguntar por el grupo al que pertenecen los usuarios (va con un comando *IF...THEN* y sin porcentaje) y ejecutar comandos para dichos ellos.
NOT MEMBER OF <grupo>	Se utiliza para preguntar por el grupo al que no pertenecen los usuarios (va con un comando *IF...THEN* y sin porcentaje) y ejecutar comandos para ellos usuarios.
PASSWORD_EXPIRES	Devuelve el número de días que faltan antes de que caduque la contraseña.
REQUESTER_CONTEXT	Devuelve el contexto donde se realiza la conexión.
USER_ID	Devuelve el número asignado a cada usuario.

LA UTILIZACIÓN DE LAS UNIDADES

En *NetWare*, las unidades proporcionan un mapa de las rutas para encontrar los archivos dentro de la estructura del directorio. Señala cualquier localización específica de la red y así permite que la información sea localizada fácilmente.

Hay tres posibilidades:

- Asignación de unidades locales.
- Asignación de unidades de red.
- Unidades de búsqueda.

La utilización de la asignación de unidades locales

La asignación de unidades locales señala a los directorios de la unidad de disquetes o del disco duro instalado en la estación de trabajo local. Por ejemplo, la dirección *A:* normalmente va asignada a una unidad de disco flexible o disquete y la dirección *C:* está generalmente asociada a un disco duro local. La asignación de unidades locales permiten acceder y guardar información en el medio de almacenamiento de la estación de trabajo, mejor que en el disco duro del servidor.

El sistema operativo en disco siempre reserva una serie de letras para los dispositivos de almacenamiento locales. Sin embargo, puede cambiarse el número de

dispositivos locales modificando la letra que aparece en el campo *1ª unidad de red* de la pestaña *Clientes* de las *Propiedades del cliente Novell* que se acceden desde el icono **N** que se encuentra en la parte derecha de la barra de tareas.

La utilización de la asignación de unidades de red

La asignación de unidades de red es similar a la asignación de unidades locales, excepto que apuntan a localizaciones del disco duro del servidor. También pueden apuntar a un subdirectorio específico. De esa forma, se podrá cambiar la dirección en curso simplemente introduciendo la letra de dirección en vez de teclear la ruta completa del directorio.

Es importante recordar que la asignación de unidades de red es una función lógica y no física. Es decir, no existe una unidad física y separada para apuntar a una localización del disco duro. Además, la asignación de unidades de red puede ser diferente según cada usuario.

La utilización de las unidades de búsqueda

Las unidades de búsqueda también asignan una letra de dirección a una localización específica de la red, similar a las asignaciones de unidades de red, pero, además, permiten al sistema operativo buscar automáticamente un archivo pedido en el mapa de directorios (son similares a los caminos del *DOS*). Cuando se ejecuta un comando, el sistema operativo busca el correspondiente archivo dentro del subdirectorio en curso. Si el sistema no puede encontrar el archivo, entonces busca en los directorios que hay señalados en las unidades de búsqueda. Éstas no sólo se aplican a los archivos ejecutables (es decir los que tienen la extensión *COM*, *EXE* o *BAT*) sino también a los archivos de datos a los que van a acceder los archivos ejecutables.

Por ejemplo, en muchas configuraciones de redes, el directorio *PUBLIC* es señalado como unidad de búsqueda. Esta distribución permite a los usuarios ejecutar los comandos *NetWare* desde cualquier lugar de la red sin tener que cambiar de directorio.

LOS PERFILES DE USUARIO

Un **perfil de usuario** es una de las herramientas más potentes de *Windows 2000* para configurar el entorno de trabajo de los usuarios de red (es el equivalente a los guiones de entrada y la asignación de unidades de *NetWare*).

Pueden especificar el aspecto del escritorio, la barra de tareas, el contenido del menú **Inicio**, etc. (incluyendo programas o aplicaciones).

Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo (aquellos usuarios que acceden a varias

estaciones pueden tener un perfil en cada una de ellas). Este perfil se denomina **perfil local** porque sólo es accesible desde la estación en que está creado.

Los usuarios que se conectan a un servidor *Windows 2000* pueden tener también perfiles en dicho servidor. De esta manera, se puede acceder al perfil independientemente de la estación en que se esté conectado. Este perfil se denomina **perfil de red** porque se puede acceder a él desde cualquier estación de la red.

Hay dos tipos de perfiles de red:

- **Perfil móvil**. Este tipo de perfil es asignado a cada usuario por los *administradores* pero puede ser modificado por el usuario y los cambios permanecen después de finalizar la conexión.

- **Perfil obligatorio.** Este tipo de perfil tiene la misma estructura que el **perfil móvil** pero asegura que los usuarios trabajen en un entorno común. Por tanto, puede ser modificado por el usuario pero los cambios realizados se pierden al finalizar la conexión. Sólo puede ser modificado (y guardados sus cambios) por los *administradores*.

Todos los perfiles locales se guardan por defecto en **\Documents and Settings\<nombre de usuario>** (únicamente en el caso de una actualización desde *Windows NT*, los archivos se guardarían en *\PROFILES\<nombre de usuario>*). En dicha ubicación se encuentran los subdirectorios de los usuarios que se crearon en el momento de la instalación (además de los que se hayan creado posteriormente) que son: **Administrador**, **All Users** y **Default User**.

- El perfil del **Administrador** es el que corresponde a dicho usuario.

- El perfil de **All Users** contiene las entradas que se incluirán en los perfiles de todos los usuarios del presente equipo e incluyen los iconos del escritorio y programas del menú **Inicio**, comunes a todos los usuarios.

- El perfil de **Default User** es el que corresponde a todo usuario que se conecta por vez primera o que no tenga asignado un perfil específico para él.

En cada uno de los perfiles puede haber las siguientes carpetas:

- **Datos de programa**. Almacena los datos específicos de los programas.

- **Cookies**. Almacena información sobre las preferencias del usuario.

- **Entorno de red**. Guarda los accesos directos a opciones de **Mis sitios de red**.

- **Escritorio**. Se guardan los iconos que aparecen en el escritorio del usuario incluyendo archivos, carpetas y accesos directos.

- **Favoritos**. Guarda los accesos directos a los programas favoritos y sus ubicaciones.
- **Configuración local**. Almacena los archivos de datos de programas, historial y archivos temporales.
- **Impresoras**. Guarda los accesos directos a los elementos de la carpeta *Impresoras*.
- **Menú Inicio**. Guarda los accesos directos que hay en el menú *Inicio*.
- **Mis documentos**. Guarda los documentos del usuario.
- **Mis imágenes**. Guarda los elementos de imagen del usuario.
- **Plantillas**. Contiene los accesos directos a plantillas del usuario.
- **Reciente**. Guarda los accesos directos usados recientemente.
- **SendTo**. Guarda los accesos directos a las utilidades de control de los documentos.

Las carpetas **Configuración local**, **Datos de programa**, **Entorno de red**, **Impresoras**, **Plantillas**, **Reciente** y **SendTo** están ocultas y no se ven a no ser que se indique expresamente, marcando **Mostrar todos los archivos y carpetas ocultos** de la ficha **Ver** de **Opciones de carpeta** del menú **Herramientas**.

Así mismo, pueden tener hasta tres archivos llamados: **NTuser.dat** (contiene los datos del **Registro** del usuario), **NTuser.dat.LOG** (que es un archivo donde se guardan los cambios anteriores, a la última modificación, por si hubiera algún problema y poder corregir los errores) y **NTuser.man** (contiene los datos del **Registro** del usuario pero es un archivo de sólo lectura y, por tanto, no se guardan los cambios).

Para asignar un perfil de usuario, un archivo de comandos para inicio de la sesión o un subdirectorio particular para la cuenta del usuario, está la ficha **Perfil** de la pantalla de *Propiedades* de cada usuario a la que se puede acceder desde el **Administrador de equipos** (si no ha instalado el *Directorio Activo*) o **Usuarios y equipos de Active Directory**.

Los Perfiles móviles

Como ya se indicó anteriormente, este tipo de perfiles son asignados a cada usuario, pueden ser modificados por ellos mismos y los cambios permanecen después de finalizar la conexión.

Para ello, se guardan los datos del **Registro** del usuario en un archivo llamado **ntuser.dat** (dentro de un subdirectorio con su nombre que se encuentra en la carpeta

\DOCUMENTS AND SETTINGS a no ser que sea una actualización de *Windows NT*). Cuando el usuario se conecta, este archivo se copia a la categoría **HKEY_CURRENT_USER** del Registro (ver apartado correspondiente). Cuando el usuario realice cambios en su perfil, éstos se guardarán en el archivo **ntuser.dat** al finalizar su conexión (de esa manera los cambios permanecerán para la próxima vez que inicie una sesión).

También, cuenta con el archivo **ntuser.dat.log** (que es un archivo donde se guardan los cambios anteriores, a la última modificación, por si hubiera algún problema y poder corregir los errores).

Los Perfiles obligatorios

Como ya se indicó anteriormente, este tipo de perfiles tienen la misma estructura que los *perfiles móviles*, pero aseguran que los usuarios trabajen en un entorno común. Por tanto, los usuarios pueden modificarlos pero los cambios realizados se pierden al finalizar la conexión (los cambios sólo se guardan cuando se realizan por los *administradores*).

Para ello, se guardan los datos del **Registro** del usuario en un archivo llamado **ntuser.man** (dentro de un subdirectorio con su nombre que se encuentra en la carpeta *\DOCUMENTS AND SETTINGS* a no ser que sea una actualización de *Windows NT*). Cuando el usuario se conecta, este archivo se copia a la categoría **HKEY_CURRENT_USER** del Registro (ver apartado correspondiente). Cuando el usuario realice cambios en su perfil, éstos no se guardarán en el archivo al finalizar su conexión (de esa manera los cambios realizados no permanecerán para la próxima vez que inicie una sesión).

El archivo de comandos para inicio de sesión

Se entiende por archivo de comandos para inicio de sesión a un archivo de proceso por lotes que se ejecuta automáticamente cuando el usuario inicia una sesión de red. Estos archivos tienen que tener **BAT** como extensión (exceptuando cuando se trabaja desde una estación **OS/2** que tendrá como extensión **CMD**) aunque también se puede utilizar cualquier programa ejecutable.

Otra posibilidad es utilizar **Windows Script Host** que permite escribir secuencias de comandos en **Visual Basic Scripting Edition** (**VBScript**) o **JScript**. El motor de secuencias de comandos utiliza las extensiones de los archivos (*VBS* para **VBScript** y *JS* para **JScript**) para identificar el archivo de comandos.

Hay dos versiones de **Windows Script Host**: una versión que usa *Windows* (**wscript.exe**) que proporciona una hoja de propiedades basadas en *Windows* para establecer las propiedades de la secuencia de comandos y otra versión basada en el símbolo del sistema (cscript.exe) que proporciona modificadores de la línea de comandos para establecer las propiedades de las secuencias de comandos debe ejecutarlos desde el símbolo del sistema).

Todos los archivos de comandos de inicio de sesión que se van a utilizar desde la ficha **Perfil** de un usuario (y únicamente se ejecutarán para los usuarios a los que se les haya indicado expresamente) se han de guardar por defecto en *\WINNT\SYSVOL\SYSVOL\<nombre de dominio DNS>\Scripts* (exceptuando si no se ha instalado el *Directorio Activo*, que se pueden guardar en el directorio que se desee).

Ahora bien, si se desea utilizar un archivo de comandos de inicio de sesión (o de cierre de sesión) para un dominio o un sitio determinado (o para determinados usuarios) se deberá realizar desde **Directiva de grupo** y los archivos se han de guardar en otra ubicación.

Pueden contener los siguientes parámetros:

VARIABLE	*DESCRIPCIÓN*
%HOMEDRIVE%	Indica la letra que va a corresponder al directorio particular del usuario.
%HOMEPATH%	Indica la ruta de acceso del directorio particular del usuario.
%OS%	Indica el sistema operativo que está funcionando en la estación de trabajo del usuario.
%PROCESSOR_ARCHITECTURE%	Indica el tipo de procesador instalado en la estación de trabajo del usuario.
%PROCESSOR_LEVEL	Indica el nivel del procesador de la estación de trabajo del usuario
%USERDOMAIN%	Indica el nombre del dominio en el cual está definida la cuenta del usuario.
%USERNAME%	Indica el nombre del usuario.

EJEMPLO DE ARCHIVO DE COMANDOS DE INICIO DE SESIÓN

He aquí un breve archivo de inicio de sesión (que se ha creado con un editor de textos) que se llamará *ARCHIVO.BAT* (es preciso indicar que si no se ha configurado que muestre las extensiones, desactivando **Ocultar las extensiones para tipos conocidos de archivo** de la ficha **Ver** de **Opciones de carpeta** del menú **Herramientas**, al guardar el archivo le pondrá la extensión *TXT*, además de *BAT*, y como estará oculta, no se verá y no se ejecutará el archivo al iniciar la sesión el usuario):


```
@ECHO OFF
NET TIME \\PRINCIPAL /YES
NET USE F: /DELETE
NET USE F: \\PRINCIPAL\MOFFICE /YES
NET USE LPT1 /DELETE
IF %USERDOMAIN% == CONTABILIDAD NET USE LPT1 \\PRINCIPAL\HPLASERIII /YES
IF %USERDOMAIN% == PERSONAL NET USE LPT1 \\SECUNDA\HPLASERIVSI /YES
```

En él se incluyen los siguientes comandos:

La primera línea se utiliza para que no aparezcan las demás líneas al ejecutarse el archivo de comandos.

La segunda línea permite sincronizar el reloj de la estación de trabajo con el servidor **PRINCIPAL**, sin pedir confirmación.

La tercera línea elimina la conexión compartida **F:** (ya que era persistente).

La cuarta línea conecta la letra **F:** con el directorio compartido llamado **MSOFFICE**, del servidor **PRINCIPAL**, sin pedir confirmación.

La quinta línea elimina la conexión compartida **LPT1** (ya que era persistente).

La sexta línea comprueba si el dominio del usuario es **CONTABILIDAD** y entonces conecta el puerto paralelo **LPT1** a la impresora compartida denominada **HPLASERIII** del servidor **PRINCIPAL** de dicho dominio, sin pedir confirmación.

La séptima línea comprueba si el dominio del usuario es **PERSONAL** y entonces conecta el puerto paralelo **LPT1** a la impresora compartida denominada **HPLASERIVSI** del servidor **SECUNDA** de dicho dominio, sin pedir confirmación.

Puede utilizar los comandos *NET* para confeccionar un archivo de comandos de inicio de sesión.

La ruta de acceso local

Indica el directorio local privado de cada usuario, en donde puede almacenar sus archivos y programas. Así mismo, es el directorio predeterminado que se utiliza en en **Símbolo del sistema** y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Deberá crearlo antes de especificar su ruta y su utilización es incompatible con **Conectar**.

Conectar a una unidad de red

Indica una conexión con la letra deseada al subdirectorio de red privado de cada usuario, en donde puede almacenar sus archivos y programas, así mismo, es el directorio predeterminado que se utiliza en **Símbolo del sistema** y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilitan la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Al especificarlo, se crea automáticamente el subdirectorio indicado (en caso de no poder hacerlo, le mostrará un mensaje de error), si no existe.

Su utilización es incompatible con **Ruta de acceso local**.

LA DEFINICIÓN DE LOS USUARIOS DE LA RED

Usuarios en NetWare

Se pueden tener varios niveles de usuarios, entre ellos están: administradores, administradores de grupos de trabajo, responsables de un grupo de trabajo, operadores y usuarios regulares de la red.

El nivel más alto es el de administrador que tiene acceso a todas las utilidades *NetWare* (tales como el *Administrador de NetWare*, *FILER*, etc.) y a todos los directorios y subdirectorios de los discos duros de la red. *NetWare* crea automáticamente un usuario *ADMIN* cuando se instala el sistema operativo. Además, se pueden conceder equivalencias de administrador a otros usuarios de la red.

Debido a la gran autoridad concedida a los administradores, se deberá limitar el número de personas con dichos privilegios, aunque por motivos diversos siempre es recomendable que haya más de uno o que, al menos, tenga dos accesos de administrador la misma persona.

El segundo nivel es el de administradores de grupos de trabajo. Dichas personas pueden crear y borrar nuevos usuarios, grupos y colas de impresión, teniendo sobre ellos derechos de *trustee*. La diferencia entre este tipo de usuario y el administrador está en que únicamente éste puede nombrar administradores de grupos de trabajo.

El tercer nivel es el de responsable de un grupo de trabajo. Dichos usuarios tienen determinados privilegios especiales (modificar nombres de usuario, modificar contraseñas, hacer restricciones y auditorías, modificar guiones de entrada y borrar usuarios) sobre un grupo determinado.

El cuarto nivel es el de operadores. Dichas personas son usuarios regulares de la red a quienes les han sido conferidos privilegios adicionales para utilizar algunas de las utilidades *NetWare*. Por ejemplo, conceder el acceso técnico para el mantenimiento de la red, las utilidades de la consola del servidor para verificar su eficiencia, etc.

El quinto nivel es el típico usuario de la red. La mayoría de las personas que utilizan la red local estarán dentro de esta clasificación. El usuario regular de la red tiene acceso solamente a sus propios archivos y a los programas de aplicación tales como *Dbase*, *WordPerfect*, *Microsoft Office*, etc.

Para añadir usuarios a la red son precisos cuatro pasos:

1. Indicar el nombre y la identificación del nuevo usuario de la red.
2. Modificar sus restricciones según sea necesario y establecer su contraseña.
3. Indicar el nombre del grupo al que pertenece.
4. Preparar su guión de entrada.

El único usuario por defecto creado automáticamente en la instalación es *ADMIN*. El usuario *ADMIN* tiene conferido el privilegio de acceder a todos los directorios de la red. Dichos privilegios no pueden anularse ni modificarse y tampoco debe ser renombrado ni borrado.

Usuarios en Windows 2000

Las cuentas de usuario representan a una persona y se denominan **principales de seguridad** dentro del *Directorio Activo*, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de usuario permite que un usuario inicie sesiones en equipos y/o dominios con una identidad que se puede autentificar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Por tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar otros principales de seguridad.
- Auditar las acciones realizadas con la cuenta de usuario.

Los usuarios en *Windows 2000* pueden ser de dos tipos:

- **Usuarios globales**. Estas cuentas se crean en equipos *Windows 2000 Server* que sean controladores de dominio y pueden usarse para conectarse a los dominios en que están creadas y a otros dominios en los que se confía. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas** y se guardan en el *Directorio Activo*.

- **Usuarios locales**. Estas cuentas se crean en equipos con *Windows 2000 Professional* y *Server* (que no sean controladores de dominio) y, por tanto, no pueden usarse para conectarse a ningún dominio. Se crean, modifican o eliminan con la utilidad **Administración de equipos** de **Herramientas administrativas** de la opción **Programas** del menú **Inicio**.

Windows 2000 proporciona dos cuentas de usuario predefinidas que se crean en el proceso de la instalación y pueden usarse para iniciar una sesión y tener acceso a los recursos. Estas cuentas son:

La **cuenta de usuario del Administrador** que le permite administrar el equipo en el que se creó. Esta cuenta puede ser renombrada pero no puede ser borrada, deshabilitada ni quitada del **grupo local de Administradores**. Es importante renombrar y proteger esta cuenta con una contraseña especial, así como crear otras cuentas de administradores para proteger mejor la seguridad del servidor. Todos los administradores son miembros de los grupos siguientes: **grupo local de Administradores, grupo global de Administradores del dominio, grupo global de Administración de empresas, grupo global de Administradores de esquema, grupo global de Propietarios del creador de directivas de grupo** y **grupo global de Usuarios del dominio** (ver apartado siguiente para tener información de estos grupos).

La **cuenta de usuario del Invitado**. Normalmente, esta cuenta está deshabilitada (y debería permanecer de esta manera) pero puede habilitarse si se desea que alguien pueda conectarse al equipo o dominio con ella (tenga en cuenta que no precisa ninguna contraseña). Esta cuenta puede borrarse y renombrarse. Todos los invitados son miembros de los siguientes grupos: **grupo local de Invitados, grupo global de Invitados de dominio** y **grupo global de Usuarios del dominio** (ver apartado siguiente para tener información de estos grupos).

LA CREACIÓN DE GRUPOS

Los usuarios de la red pueden agruparse para permitirles compartir los datos aunque procedan de distintos lugares del árbol del directorio. Concediendo a un grupo privilegios para un subdirectorio, los miembros del grupo pueden acceder a archivos compartidos que no están accesibles a otros usuarios de la red.

Se suele definir normalmente los grupos incluyendo a todas las personas que realizan una tarea en particular.

El proceso de creación de grupos consta de tres pasos básicos:

1. Crear el grupo que se va añadir.
2. Conceder derechos de archivo y directorio al grupo.
3. Añadir los usuarios al grupo.

Las cuentas de grupo en NetWare 5

En versiones anteriores de *NetWare*, durante el proceso de instalación se crea únicamente el grupo **EVERYONE** al que pertenecen los usuarios que se crean en el proceso de instalación (en *NetWare 5* no se crea ningún grupo).

Las cuentas de grupo en Windows 2000

Las cuentas de grupo representan a un grupo y se denominan **principales de seguridad** dentro del *Directorio Activo*, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad. En *Windows 2000* se pueden dar dos tipos de grupos:

- **Los grupos de seguridad**. Este tipo de grupos se muestran en las **listas de control de acceso discrecional (DACL)** que es el lugar donde están definidos los permisos sobre los recursos y los objetos. Los grupos de seguridad se pueden utilizar también como entidades de correo electrónico de esta manera, al enviar un mensaje de correo electrónico al grupo, el mensaje se envía a todos los miembros del grupo.

- **Los grupos de distribución**. En este tipo de grupos no es posible habilitar la seguridad ya que no aparecen en las **listas de control de acceso discrecional (DACL)**. Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como *Microsoft Exchange*) para enviar correo electrónico a los grupos de usuarios.

Un *grupo de seguridad* puede convertirse en *grupo de distribución* (y viceversa) en cualquier momento si todos los controladores del dominio se han actualizado a *Windows Server Server* y el administrador ha habilitado el funcionamiento en **modo nativo** (si esto no es así, estarán en modo mixto y no se podrá realizar esta conversión).

Cada grupo de seguridad o de distribución tiene un ámbito que identifica el alcance de aplicación del grupo. Existen cuatro tipos de grupos en función de su ámbito de aplicación:

- **Grupos de ámbito universal**. Este tipo de grupos (que únicamente puede crearse en equipos con *Windows 2000 Server* que tenga instalado el *Directorio Activo)* puede tener como miembros a otros grupos universales, grupos globales y cuentas de cualquier dominio de *Windows 2000*, y se le puede conceder permisos en cualquier dominio. También se les denomina **grupos universales**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas** y se guardan en el *Directorio Activo*.

- **Grupos de ámbito global**. Este tipo de grupos (que únicamente puede crearse en equipos con *Windows 2000 Server* que tenga instalado el *Directorio Activo)* puede tener como miembros a grupos globales y cuentas únicamente del dominio en el que se ha definido el grupo, y se le puede conceder permisos en cualquier dominio. Tambien se les denomina **grupos globales**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas** y se guardan en el *Directorio Activo*.

- **Grupos de ámbito local de dominio**. Este tipo de grupos (que únicamente puede crearse en equipos con *Windows 2000 Server* que tenga instalado el *Directorio Activo)* puede tener como miembros a grupos universales, grupos globales, grupos locales de dominio de su propio dominio y cuentas de cualquier dominio de *Windows 2000* o *Windows NT*, y sólo se pueden utilizar para conceder permisos en el dominio que contiene el grupo. También se les denomina **grupos de dominio local**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas** y se guardan en el *Directorio Activo*.

- **Grupos locales**. Este tipo de grupo únicamente puede crearse en equipos que ejecutan *Windows 2000 Professional* o que sean servidores miembros (equipos con *Windows 2000 Server* que no tienen instalado el *Directorio Activo*). Puede tener como miembros a cuentas locales del equipo en el que se crean y, si el equipo forma parte de un dominio, podrá tener también cuentas y grupos globales del propio dominio y de los dominios de confianza, y se puede utilizar para conceder permisos en el equipo en el que se crea el grupo. Se crean, modifican o eliminan con la utilidad **Administración de equipos** de **Herramientas administrativas** de la opción **Programas** del menú **Inicio**.

Al crear un nuevo grupo, éste se configura de forma predeterminada como grupo de seguridad de ámbito global, independientemente del modo del dominio actual, pero se pueden realizar las siguientes conversiones en los dominios que están en modo nativo (no se puede realizar un cambio de ámbito de un dominio si se está en modo mixto):

- **De ámbito global a universal**. Esta conversión sólo se permite si el grupo global que se desea convertir no es miembro de otro grupo de ámbito global.

- **De ámbito local de dominio a universal**. Esta conversión sólo se permite si el grupo local de dominio que se va a convertir no tiene como miembro a otro grupo local de dominio.

CUENTAS DE GRUPO CREADAS EN LA INSTALACIÓN

Los grupos se utilizan para agregar a los usuarios (o equipos) de forma que se puedan asignar, más fácilmente, privilegios a dichos usuarios (o equipos) y hacer más sencilla su administración. Por tanto, se puede incorporar un usuario (o equipo) a uno o a varios grupos teniendo, en cada uno de ellos, unos permisos determinados que le permitirán realizar distintas funciones.

Cuando se procedió a la instalación se crearon distintos grupos que estaban en función del tipo de instalación realizada (básicamente si se instala o no el *Directorio Activo*). Estos grupos son los siguientes:

- **Si no se instala el Directorio Activo**. En este caso, los grupos que se crean durante el proceso de instalación son únicamente **grupos locales**, se denominan **grupos integrados** y son los siguientes:

  - **Grupo local de Administradores**. Los miembros de este grupo tienen control total sobre el equipo y se les conceden automáticamente todos los derechos y capacidades integradas del sistema.
  - **Grupo local de Duplicadores**. La función de este grupo es la de realizar la duplicación de archivos en el dominio y el único miembro que tendrá es una cuenta de usuario de dominio que se utilizará para iniciar los servicios correspondientes (no se deben agregar a este grupo las cuentas de los usuarios reales).
  - **Grupo local de Invitados**. Este grupo permite a los usuarios ocasionales iniciar una sesión en el equipo utilizando la cuenta de *Invitado* y se le conceden menos capacidades que al **grupo local de Usuarios**.
  - **Grupo local de Operadores de copia**. Los miembros de este grupo pueden realizar copias de seguridad y restaurar los archivos en el equipo, independientemente de los permisos que protejan dichos archivos. También pueden iniciar una sesión en el equipo y cerrarlo, pero no pueden cambiar la configuración de seguridad.
  - **Grupo local de Usuarios**. Los miembros de este grupo pueden realizar, entre otras, las siguientes tareas: ejecutar aplicaciones, utilizar impresoras locales y de red, cerrar y bloquear la estación de trabajo pero no pueden compartir directorios ni crear impresoras locales. Pueden crear grupos locales nuevos pero únicamente pueden modificar los grupos locales que ellos hayan creado.
  - **Grupo local de Usuarios avanzados**. Los miembros de este grupo pueden crear cuentas de usuario y grupos locales pero únicamente pueden modificar y eliminar las cuentas que ellos hayan creado. También pueden quitar usuarios de los grupos locales de *Usuarios avanzados*, *Usuarios* e *Invitados* pero no pueden modificar los grupos locales de *Administradores* u *Operadores de copia*, ni pueden tomar posesión de archivos, copiar o restaurar directorios, cargar o descargar controladores de dispositivo ni administrar los registros de auditoría y seguridad.

- **Si se instala el Directorio Activo**. En este caso, los grupos que se crean durante el proceso de instalación son **locales de dominio** y **globales**.

Algunos **grupos locales de dominio** se crean en la carpeta **Builtin**, se denominan **grupos integrados** y son los siguientes:

- **Grupo local de dominio de Acceso compatible con Pre-Windows 2000**. Este grupo permite únicamente el acceso de lectura a todos los usuarios y grupos en el dominio y son miembros de este grupo todos los usuarios del dominio.
- **Grupo local de dominio de Administradores**. Los miembros de este grupo tienen control total sobre el equipo y el dominio y se les conceden automáticamente todos los derechos y capacidades integradas del sistema.
- **Grupo local de dominio de Duplicadores**. La función de este grupo es la de realizar la duplicación de archivos en el dominio y el único miembro que tendrá es una cuenta de usuario de dominio que se utilizará para iniciar los servicios correspondientes (no se deben agregar a este grupo las cuentas de los usuarios reales).
- **Grupo local de dominio de Invitados**. Este grupo permite a los usuarios ocasionales iniciar una sesión en el equipo utilizando la cuenta de *Invitado* y se le conceden menos capacidades que al **grupo local de dominio de Usuarios**.
- **Grupo local de dominio de Operadores de copia**. Los miembros de este grupo pueden realizar copias de seguridad y restaurar los archivos en el equipo, independientemente de los permisos que protejan dichos archivos. También pueden iniciar una sesión en el equipo y cerrarlo, pero no pueden cambiar la configuración de seguridad.
- **Grupo local de dominio de Operadores de cuentas**. Los miembros de este grupo pueden crear cuentas de usuario y grupos de dominio, modificar y eliminar las cuentas que ellos hayan creado, así como, modificar y borrar las cuentas de algunos otros grupos pero no pueden modificar los grupos de *Administradores*, *Administradores del dominio*, *Operadores de copia*, *Operadores de cuentas*, *Operadores de impresión* y *Operadores de servidores* ni administrar las directivas de seguridad pero pueden añadir equipos al dominio, conectarse y parar los servidores.
- **Grupo local de dominio de Operadores de impresión**. Los miembros de este grupo pueden crear, administrar y borrar impresoras compartidas, así como conectarse y parar los servidores.
- **Grupo local de dominio de Operadores de servidores**. Los miembros de este grupo pueden administrar los servidores del dominio. De esta forma pueden realizar las siguientes acciones en los servidores: crear, administrar y borrar impresoras y recursos compartidos, hacer copia de seguridad y su restauración, formatear los discos duros, bloquearlos y desbloquearlos, desbloquear archivos, cambiar la fecha y hora del sistema, así como conectarse y pararlos.
- **Grupo local de dominio de Usuarios**. Los miembros de este grupo pueden realizar, entre otras, las siguientes tareas: ejecutar aplicaciones, utilizar impresoras locales y de red, cerrar y bloquear la estación de trabajo pero no pueden compartir directorios ni crear impresoras locales. Pueden crear grupos locales de dominio nuevos pero únicamente pueden modificar los grupos locales de dominio que ellos hayan creado.

Otros **grupos locales de dominio** y los **grupos globales** se crean en la carpeta **Users**, se denominan **grupos predefinidos** y son los siguientes:

- **Grupo global de Administración de empresas**. A este grupo forman parte todos los administradores que tienen asignada la administración de los equipos de la empresa.
- **Grupo global de Administradores de esquema**. A este grupo forman parte todos los administradores que tienen asignada la administración del esquema.
- **Grupo local de dominio de Administradores DHCP**. A este grupo forman parte todos los administradores que tienen asignada la administración del servicio *DHCP*.
- **Grupo global de Administradores del dominio**. A este grupo forman parte todos los administradores que tienen asignada la administración del dominio.
- **Grupo global de Controladores del dominio**. A este grupo forman parte todos los equipos que son controladores de dominio del dominio.
- **Grupo local de dominio de DnsAdmins**. A este grupo forman parte todos los administradores que tienen asignada la administración *DNS*.
- **Grupo global de DnsUpdateProxy.** A este grupo forman parte los clientes *DNS* que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes.
- **Grupo global de Equipos del dominio.** A este grupo forman parte todos los servidores (que no sean controladores de dominio) y estaciones del dominio.
- **Grupo global de Invitados de dominio.** A este grupo forman parte todos los inivitados del dominio.
- **Grupo local de dominio de <nombre equipo> Administradores**. A este grupo forman parte todos los usuarios que pueden crear y administrar servidores *Webs* en el equipo indicado.
- **Grupo local de dominio de <nombre equipo> Autores**. A este grupo forman parte todos los usuarios que pueden crear y modificar carpetas y archivos *Webs* en el equipo indicado.
- **Grupo local de dominio de <nombre equipo> Visitantes**. A este grupo forman parte todos los usuarios que pueden leer las páginas *Webs* en el equipo indicado.
- **Grupo global de Propietarios del creador de directivas de grupo**. A este grupo forman parte todos los usuarios que pueden modificar la directiva de grupo del dominio.
- **Grupo global de Publicadores de certificados**. A este grupo forman parte todos los publicadores de certificados de empresa y agentes de revocación.

- **Grupo local de dominio de Servidores RAS e IAS**. A este grupo forman parte todos los servidores que pueden obtener propiedades de acceso remoto de los usuarios.
- **Grupo global de Usuarios del dominio**. A este grupo forman parte todos los usuarios del dominio.
- **Grupo local de dominio de Usuarios DHCP.** A este grupo forman parte todos los miembros que tienen acceso al servicio *DHCP*.
- **Grupo local de dominio de Usuarios WINS**. A este grupo forman parte todos los miembros que tienen acceso al servidor *WINS*.

ESTABLECER LA ADMINISTRACIÓN DE SEGURIDAD

La administración de seguridad se usa para asignar derechos a los usuarios y grupos para trabajar dentro de los directorios y archivos, o derechos para administrar objetos y propiedades.

La administración de seguridad en NetWare

Es importante hacer una breve explicación del concepto de **síndico** (**trustee**). Se entiende por **síndico** (**trustee**) a todo usuario o grupo al que se le han asignado derechos para trabajar con un directorio, archivo u objeto. Hay una clase especial de **trustee** llamada [**Público**] que permite que todos los derechos otorgados a él son aplicables a cualquier objeto del Directorio que no posea otros derechos vigentes.

Cuando se instala un objeto *Servidor NetWare* nuevo en el árbol *NDS*, se crean las siguientes asignaciones de **Trustees**:

Trustees por defecto	Derechos por defecto
Admin (primer servidor *NDS* del árbol)	Derecho de objeto *Supervisor* para el objeto [*Root*]
[*Public*] (primer servidor *NDS* del árbol)	Derecho del objeto *Examinar* para el objeto [*Root*]
Servidor *NetWare*	*Admin* tiene el derecho del objeto *Supervisor* para el objeto *Servidor NetWare*, lo que significa que *Admin* también tiene el derecho de *Supervisión* para el directorio raíz del sistema de archivos de cualquiera de los volúmenes *NetWare* del servidor.
Volúmenes (si se crean)	[*Root*] tiene el derecho de propiedad de *Lectura* para las propiedades *Nombre de servidor host* y *Recurso de host* en todos los objetos *Volumen*. Esto otorga a todos los objetos, acceso al nombre del volumen físico y al nombre del servidor físico.

Trustees por defecto	Derechos por defecto
Volúmenes (si se crean)	*Admin* tiene el derecho de *Supervisión* para el directorio raíz de los sistemas de archivo del volumen. Para el volumen *SYS*, el objeto contenedor tiene los derechos de *Lectura* y de *Exploración* de archivos para el directorio *PUBLIC* del volumen. Esto permite que los objetos *Usuario* del contenedor tengan acceso a las utilidades *NetWare* que se hallan en *PUBLIC*.
Usuario	Si los directorios personales de los usuarios se crean automáticamente, los usuarios tienen el derecho de *Supervisión* para dichos directorios.

Referente a archivos y directorios, se pueden conceder a los usuarios o grupos varios derechos:

DERECHOS	FUNCIÓN
Borrado	Permite el borrado de directorios, subdirectorios o archivos.
Control de Acceso	Permite cambiar las asignaciones de *Trustee* y el filtro de derechos heredados de un directorio o archivo.
Creación	Permite crear nuevos archivos y subdirectorios en el directorio y, también, recuperar un archivo después de su supresión.
Escritura	Permite abrir un directorio y escribir en los archivos.
Exploración de archivo	Permite ver un listado con los nombres de los archivos y directorios con los comandos *DIR* o *NDIR*.
Lectura	Permite abrir y leer los archivos.
Modificación	Permite cambiar los atributos y el nombre del directorio o archivo.
Supervisión	Permite disponer de todos los derechos y otorgarlos a otro.

Los derechos referentes a objetos controlan lo que un *trustee* puede realizar con sus objetos y son los siguientes:

Creación	Permite crear objetos nuevos en el árbol del directorio.
Examinar	Permite ver objetos en el árbol del directorio.
Heredado	Permite que los objetos y contenedores situados bajo el objeto que tiene este derecho, heredan la asignación de *trustee*.
Renombrado	Permite cambiar el nombre de un objeto.
Supervisor	Otorga todos los derechos a un objeto (incluyendo sus propiedades).
Suprimir	Permite suprimir un objeto del árbol del directorio.

Los derechos referentes a propiedades de los objetos permiten ver la información almacenada en las propiedades de los objetos y son los siguientes:

Autoadición	Permite añadirse o suprimirse a sí mismo como valor de una propiedad (este derecho sólo se utiliza para propiedades que contienen nombres de objetos como valores).
Comparación	Permite comparar el valor de una propiedad con otro valor para ver si son iguales (la comparación devuelve verdadero o falso y no el valor real de la propiedad).
Escritura	Otorga el derecho de añadir, cambiar o eliminar los valores de una propiedad (este derecho implica el derecho de *Autoadición*).
Lectura	Otorga el derecho de leer y comparar los valores de una propiedad (este derecho implica el derecho de *Comparación*).
Supervisor	Otorga todos los derechos sobre todas las propiedades o sobre una propiedad específica.
Todas las propiedades	Otorga derechos de acceso a todas las propiedades de un objeto (una asignación de derechos a una propiedad específica anula una asignación de derechos a todas las propiedades pero únicamente para dicha propiedad).

Cuando se agrega un nuevo usuario a la red, automáticamente se le concede los siguientes derechos: *lectura* y *exploración de archivo* para los directorios *LOGIN* y *PUBLIC* y *creación* para el directorio *MAIL*. Disponen de los mismos derechos para los volúmenes *SYS* de los contenedores padres, pero no para los volúmenes *SYS* de los contenedores subordinados.

Además, si se crea un directorio personal durante la creación del usuario, dispondrá de todos los derechos de sistema de archivos para su directorio personal, sea cual sea su situación en el árbol.

Los derechos a todos los demás directorios deben ser asignados por el administrador de la red.

Los derechos se pueden conceder tanto a los usuarios individuales como a los usuarios pertenecientes a un grupo. Además, se pueden asignar derechos, directa o indirectamente, a través de las equivalencias de seguridad. La función de equivalencia de seguridad permite al administrador conceder a un usuario o a un grupo los mismos derechos que tiene otro usuario o grupo.

Cuando un usuario tiene derechos sobre un directorio, tiene también los mismos derechos sobre cualquier subdirectorio de nivel inferior, a menos que estén explícitamente restringidos.

EL FILTRO DE DERECHOS HEREDADOS

El filtro de derechos heredados, creado automáticamente con cada directorio, controla qué derechos reales puedan ejercitarse cuando se trabaja con un objeto y con sus subordinados y cuáles no.

Tiene las siguientes restricciones:

- Únicamente pueden filtrarse derechos heredados. Los derechos otorgados en el nivel actual, ya sea por asignación explícita o por equivalencia de seguridad, no pueden bloquearse.
- El derecho de *Supervisión* puede bloquearse para un objeto, pero no para un archivo ni para un directorio.
- Los derechos de objeto y los de propiedades se heredan y se filtran por separado; por lo tanto, los derechos de objeto y los de propiedades pueden bloquearse individualmente sin que el bloqueo de unos afecte a los otros.
- Si se otorgan derechos de forma explícita sobre un directorio se anula el filtro de derechos heredados.

ESTABLECER ATRIBUTOS A ARCHIVOS Y DIRECTORIOS

Cuando se crean nuevos archivos en *NetWare*, los atributos del archivo que por defecto se establecen son los de *Respaldo necesario* (su actuación es cambiar un valor en la información del archivo cuando se produce una modificación en él. Sirve para indicar a los programas de copia de seguridad que hay que copiarlo y después se pone a cero) y *Lectura/Escritura* (está indicado al no estar marcado el atributo de *Sólo lectura*).

Estos atributos sólo permiten al usuario acceder y manipular el archivo (siempre que el usuario tenga los derechos efectivos adecuados).

Se pueden asignar, además, los siguientes atributos a los archivos:

ATRIBUTO	FUNCIÓN
Compartible	Permite que más de un usuario utilice el archivo al mismo tiempo.
Compresión inmediata	Indica que el archivo se comprime tan pronto como se pueda.
Inhibir renombrado	Indica que no se puede renombrar, aunque se tengan los derechos.
Inhibir supresión	Indica que no se puede borrar, aunque se tengan los derechos.
Limpiar inmediatamente	Permite que el archivo se limpie en cuanto se borre.
No comprimir	Impide que el archivo se comprima incluso aunque se supere el umbral definido por el servidor.
No migrar	Indica que el archivo no se migrará a un sistema de respaldo secundario, independientemente del valor por omisión del volumen.
No subasignar	Impide que un archivo se pueda almacenar en porciones de bloques de disco no utilizados aunque el sistema tenga habilitada la subasignación.
Ocultar	Impide que se visualice al listar y, por tanto, no se puede copiar ni suprimir.

ATRIBUTO	FUNCIÓN
Respaldo necesario	Indica que el archivo se ha modificado desde la última copia de seguridad.
Sistema	Indica lo mismo que *Ocultar*, pero reservado para archivos de operaciones de la red.
Sólo ejecución	Indica que no es posible copiar el archivo ni sobreescribirlo, ni eliminarlo (este atributo sólo puede aplicarse a archivos *EXE* y *COM*).
Sólo lectura	Indica que el archivo no se puede modificar, ni borrar, ni suprimirlo (al poner este atributo automáticamente se ponen *Inhibir renombrado* e *Inhibir supresión*).
Transaccional	Asegura que se guardan todas las modificaciones o no se guarda ninguna, así se previene la corrupción de los datos.

También es posible asignar atributos a los directorios. Entre aquellos que se pueden otorgar, se encuentran los siguientes:

ATRIBUTO	FUNCIÓN
Compresión inmediata	Indica que el directorio se comprime tan pronto como se pueda.
Inhibir renombrado	Indica que no se puede renombrar, aunque se tengan los derechos.
Inhibir supresión	Indica que no se puede borrar, aunque se tengan los derechos
Limpiar	Permite que el directorio se limpie en cuanto se borre.
No comprimir	Impide que el directorio se comprima incluso aunque se supere el umbral definido por el servidor.
No migrar	Indica que el directorio no se migrará a un sistema de respaldo secundario, independientemente del valor por omisión del volumen.

ATRIBUTO	FUNCIÓN
Ocultar	Impide que se visualice al listar y, por tanto, no se puede copiar ni suprimir.
Sistema	Indica lo mismo que *Ocultar*, pero reservado para archivos de operaciones de la red.

La administración de seguridad en Windows 2000

Hay que distinguir entre permisos estándar y permisos de acceso especial tanto a nivel de directorios como de archivos.

LOS PERMISOS ESTÁNDAR DE DIRECTORIO

Cuando se establecen permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos.

Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él, tanto los que se creen posteriormente como los que ya existían previamente (este hecho se denomina **herencia**). Si no desea que se hereden, deberá indicarse expresamente cuando se indiquen los permisos.

Hay tres modos de realizar cambios en los permisos heredados:

- Realizar los cambios en el carpeta principal y la carpeta secundaria heredará estos permisos.
- Seleccione el permiso contrario (**Permitir** o **Denegar**) para sustituir el permiso heredado.
- Desactivar la casilla de verificación **Hacer posible que los permisos heredables del principal se propaguen a este objeto** (de esta manera, podrá realizar cambios en los permisos, ya que la carpeta no heredará los permisos de la carpeta principal).

Sólo es posible establecer permisos para directorios de unidades formateadas con el sistema **NTFS**.

Los permisos estándar para directorios que se pueden conceder o denegar son:

- **Control total**. Es el máximo nivel y comprende todas las acciones tanto al nivel de archivos como de directorios.

- **Modificar**. Comprende todos los permisos menos eliminar los archivos y directorios, cambiar los permisos y tomar posesión.
- **Lectura y ejecución**. Comprende ver los nombres de los archivos y directorios, los datos de los archivos, los atributos y permisos, y ejecutar programas.
- **Listar el contenido de la carpeta**. Comprende los mismos permisos que **lectura y ejecución** pero aplicables sólo a las carpetas.
- **Leer**. Comprende ver los nombres de los archivos y directorios, los atributos, los datos de los archivos y los permisos.
- **Escribir**. Comprende crear archivos y directorios, escribir los atributos, añadir datos a los archivos y leer los permisos.

Estos permisos son acumulables pero denegar el permiso **Control total** elimina todos los demás.

Para establecer permisos estándar de directorio se utiliza el **Explorador de Windows**.

LOS PERMISOS ESTÁNDAR DE ARCHIVO

Cuando se establecen permisos sobre un archivo, se define el acceso de un usuario o de un grupo a dicho archivo. Los archivos que se crean en un directorio adoptan por defecto los permisos del directorio del que forman parte.

Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Sólo es posible establecer permisos para archivos de unidades formateadas para ser usadas por el sistema **NTFS**.

Los permisos estándar para archivos que se pueden conceder o denegar son:

- **Control total**. Es el máximo nivel y comprende todas las acciones al nivel del archivo.
- **Modificar**. Comprende todos los permisos menos eliminar el archivo, cambiar los permisos y tomar posesión.
- **Lectura y ejecución**. Comprende ver el nombre del archivo, sus datos, sus atributos y permisos y ejecutarlo.
- **Leer**. Comprende ver el nombre del archivo, sus datos, los atributos y permisos.

- **Escribir**. Comprende añadir datos al archivo, escribir sus atributos y ver sus permisos.

Estos permisos son acumulables, pero denegar el permiso **Control total** elimina todos los demás.

Para establecer permisos estándar de archivo se utiliza el **Explorador de Windows**.

LOS PERMISOS ESPECIALES

Generalmente, todo lo que necesitará para proteger los directorios y los archivos son los permisos estándar que se han descrito anteriormente.

Sin embargo, si desea crear un sistema personalizado de permisos, puede utilizar los permisos especiales.

Puede establecer permisos especiales para directorios, para todos los archivos de los directorios seleccionados o para los archivos seleccionados (los no seleccionados mantendrán sus actuales permisos).

Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Sólo es posible establecer permisos para archivos de unidades formateadas para ser usadas por el sistema **NTFS**.

Los permisos especiales para directorios y archivos son:

- **Recorrer carpeta/Ejecutar archivo**. El permiso **Recorrer carpeta** (sólo afecta a los directorios) comprende el desplazamiento por las carpetas para llegar a otros archivos o carpetas, incluso si el usuario no tiene permisos para las carpetas recorridas (sólo entra en vigor cuando el grupo o usuario no tiene otorgado el derecho de usuario **Saltarse la comprobación de recorrido** en la **Directiva de grupo**). El permiso **Ejecutar archivo** comprende la ejecución de archivos de programa (sólo afecta a los archivos) y al configurar el permiso **Recorrer carpeta** en un directorio no se define de manera automática el permiso **Ejecutar archivo** en todos sus archivos.

- **Listar carpeta/Leer datos**. El permiso **Listar carpeta** (sólo afecta a los directorios) comprende ver los nombres de los archivos y subdirectorios de la carpeta. El permiso **Leer datos** comprende ver los datos de los archivos (sólo afecta a los archivos).

- **Atributos de lectura**. Comprende ver los atributos normales de un archivo o directorio.

- **Atributos extendidos de lectura**. Comprende ver los atributos extendidos de un archivo o directorio (estos atributos se definen mediante programas y pueden variar según el programa).

- **Crear archivos/Escribir datos**. El permiso **Crear archivos** (sólo afecta a los directorios) comprende la creación de archivos dentro de la carpeta. El permiso **Escribir datos** (sólo afecta a los archivos) comprende los cambios en los archivos y la sobrescritura de su contenido.

- **Crear carpetas/Anexar datos**. El permiso **Crear carpetas** (sólo afecta a los directorios) comprende la creación de subdirectorios dentro de la carpeta. El permiso **Anexar datos** (sólo afecta a los archivos) comprende el añadido de contenido del archivo pero no el cambio, eliminación ni sobrescritura de los datos existentes.

- **Atributos de escritura**. Comprende el cambio de los atributos normales de un archivo o directorio.

- **Atributos extendidos de escritura**. Comprende el cambio de los atributos extendidos de un archivo o directorio (estos atributos se definen mediante programas y pueden variar según el programa).

- **Eliminar subcarpetas y archivos**. Comprende la eliminación de subdirectorios y archivos.

- **Eliminar**. Comprende la supresión del archivo o directorio.

- **Permisos de lectura**. Comprende ver los permisos del archivo o directorio.

- **Cambiar permisos**. Comprende el cambio de los permisos del archivo o directorio.

- **Tomar posesión**. Comprende la toma de posesión del archivo o directorio. El propietario de un archivo o carpeta siempre puede cambiar los permisos en la misma, independientemente de los permisos existentes que protejan al archivo o carpeta.

Para establecer permisos especiales se utiliza el **Explorador de Windows**.

LA CONFIGURACIÓN DE SEGURIDAD

Una sistema operativo de red cuenta con distintas opciones para realizar restricciones en las cuentas de cada usuario que permitirán un mayor control sobre lo que está ocurriendo en cada momento en la red.

Para proteger la red ante accesos no deseados, un sistema operativo de red cuenta con las opciones siguientes:

- Detección y cierre de la red ante intrusos (*NetWare 5*).
- Restricción horaria de acceso a la red (*NetWare 5*).
- Limitación de conexiones concurrentes (*NetWare 5*).
- Limitación de las estaciones desde las que conectarse (*NetWare 5*).
- Las configuración de seguridad (*Windows 2000*).

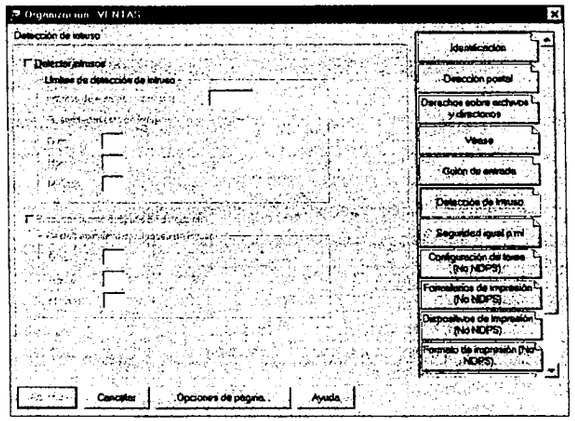
Detección y cierre de la red ante intrusos

Los usuarios de la red han de estar identificados ante el sistema. Éste permitirá acceder a los datos a aquellos que cuenten con autorización. Para ello, se proporciona al usuario un nombre que el sistema reconoce y una contraseña (*password*).

Si se desconoce cualquiera de las dos el sistema no deja acceder a ninguno de los datos. Pero puede haber usuarios que, para intentar acceder a la red, hagan pruebas de introducción de nombres y/o de contraseñas.

Para incrementar la seguridad de la red, puede hacer que la red controle el número de intentos incorrectos al introducir la contraseña de acceso.

Después de especificar el número de intentos fallidos, puede hacer que la red cierre la entrada al usuario durante un tiempo determinado. Esta estrategia detiene a los intrusos que conectando con el nombre de un usuario (por ejemplo, el supervisor) intentan introducir varias contraseñas con la esperanza de conseguir la correcta.



Para ello, se dispone de las siguientes opciones:

- **Detectar intrusos**. Al marcar en este campo, se establece la detección de intrusos.

- En el bloque **Límites de detección de intruso** se encuentran los siguientes apartados:

- **Intentos de entrada incorrectos**. Indica el número de intentos de entrada fallidos que se permite a los usuarios (por defecto es 7).

- **Restablecimiento de intrusión**. Indica el período de tiempo durante el cual se están contando los intentos de conexión erróneos para que se contabilicen (por defecto es 30 minutos).

- Si marca en **Bloquear cuenta después de detección** está indicando que una vez se hayan dado el número de intentos de entrada fallidos en el período de tiempo indicado, se debe bloquear la cuenta durante el tiempo indicado en **Restablecimiento de bloqueo de intrusos** (por defecto es 15 minutos) durante el cual no se permitirá la entrada a ese usuario.

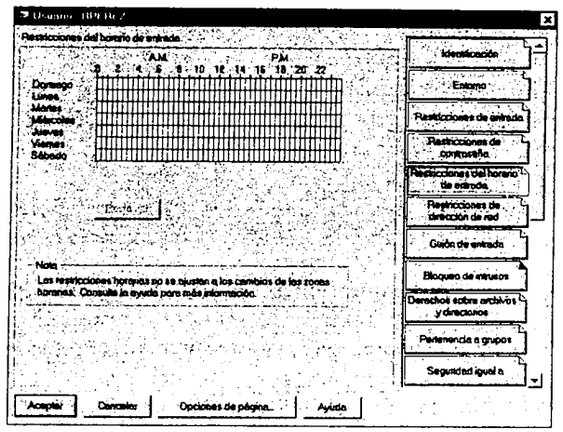
El bloqueo de intrusos sólo se ha activado para los usuarios cuyo contexto es el objeto contenedor indicado, el resto no tiene ningún tipo de bloqueo de intrusión.

Restricción horaria de acceso a la red

También, se puede limitar las horas del día en que un usuario puede acceder a la red. El restringir el acceso a la red durante determinados períodos de tiempo puede ser necesario por motivos de mantenimiento. Por ejemplo, se podría desear eliminar toda actividad en la red y cerrar todos los accesos durante el tiempo necesario para hacer las copias de seguridad del disco duro del servidor.

Normalmente se permite a todos los usuarios el acceso a la red las 24 horas del día durante los siete días de la semana.

La pantalla siguiente (correspondiente a *NetWare 5*) contiene una matriz con los días de la semana en el eje vertical y las horas (con un incremento de media hora) a lo largo del eje horizontal. Un cuadrado de color oscuro en la intersección del día y la hora indica que el usuario no puede acceder a la red en dicho período. Puede moverse por la matriz, con las teclas de flechas o con el ratón.



Para eliminar períodos de tiempo, sitúese en un lugar en el que esté autorizada la entrada (estará de color claro) y pulse el botón izquierdo del ratón (también puede pulsar dicho botón izquierdo y, sin soltarlo, desplazarse sobre la cuadrícula clara. Cuando lo suelte, la zona marcada se pondrá de color oscuro).

Para autorizar períodos de tiempo, sitúese en un lugar en el que no esté autorizada la entrada (estará de color oscuro) y pulse el botón izquierdo del ratón (también puede pulsar dicho botón izquierdo y, sin soltarlo, desplazarse sobre la cuadrícula oscura. Cuando lo suelte, la zona marcada se pondrá de color claro).

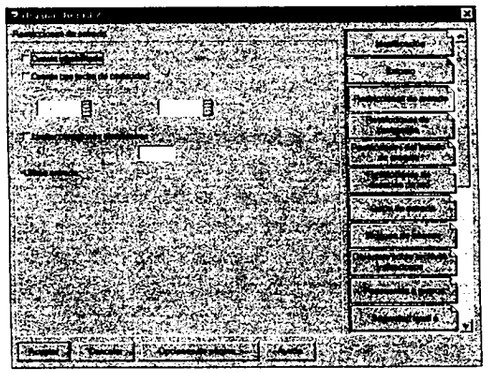
Si marca en **Restaurar** dejará la página tal y como estaba cuando entró en ella.

Limitación de conexiones simultáneas

Normalmente no se establece por defecto ninguna limitación de conexiones simultáneas.

Sin embargo, el permitir a los usuarios conectar con la red simultáneamente desde diversas estaciones de trabajo puede ser utilizado por otro usuario distinto al del nombre y contraseña utilizada, para ver o sacar información para la cual no cuenta con la debida autorización.

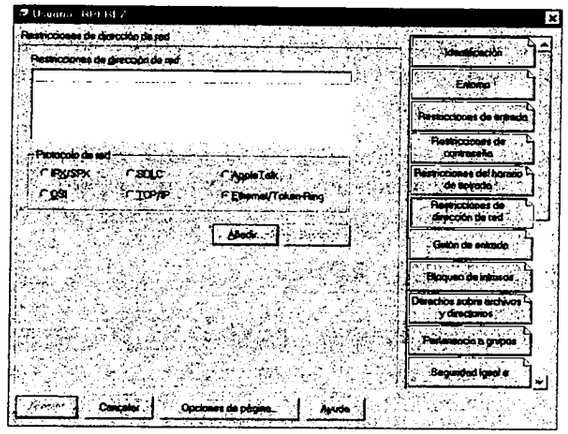
Por ello, es conveniente limitar como máximo a dos, el número de conexiones concurrentes que puede realizar un usuario. Desde ese momento, si un usuario al que ha limitado, intenta conectarse desde más de dos estaciones de trabajo al mismo tiempo, aparecerá un mensaje de error indicando que se ha alcanzado el número máximo de conexiones concurrentes y que el acceso ha sido denegado.



- **Limitar conexiones simultáneas**. Al marcar en este campo está indicando que el usuario tiene limitado el número de sesiones que puede tener abiertas al mismo tiempo (en caso de intentar sobrepasarlas, aparecerá un mensaje de error indicando que se ha alcanzado el número máximo de conexiones simultáneas y que el acceso ha sido denegado).

Limitación de estaciones desde las que conectarse

Un sistema operativo de red, por defecto, permite iniciar una sesión desde todas las estaciones de trabajo pero, también, se puede limitar las estaciones desde las que puede conectarse un usuario.



Así, será más fácil controlar los accesos de los usuarios ya que, cada uno de ellos, únicamente podrán hacerlo desde determinados ordenadores.

La configuración de seguridad en Windows 2000

Se puede modificar la configuración de la seguridad de una de las formas siguientes (depende de la función que realice el servidor):

Si el servidor *Windows 2000* es un controlador de dominio y desea modificar la configuración de seguridad para todos los miembros del dominio: **Utilizar la Directiva de seguridad de dominio**.

Si el servidor *Windows 2000* es un controlador de dominio y desea modificar la configuración de seguridad sólo para los controladores del dominio: **Utilizar la Directiva de seguridad del controlador de dominio**.

Si el servidor *Windows 2000* ejerce cualquier otra actuación: **Utilizar la Directiva de seguridad local**.

NOTA: Si se modifican las opciones de configuración de las directivas de seguridad de un dominio, la nueva configuración de seguridad aparecerá en las cuentas de los miembros del dominio, la próxima vez que se actualice la configuración de la **Directiva de grupo**.

También, se puede establecer la configuración de seguridad utilizando las siguientes herramientas:

- Para definir y modificar las plantillas de seguridad personalizadas, se utiliza el **complemento Plantillas de seguridad** de la *Consola de Administración de Microsoft*.
- Para configurar el equipo y analizar su seguridad de forma local, se utiliza el **complemento Configuración y análisis de seguridad** de la *Consola de Administración de Microsoft*.
- Para configurar la seguridad de forma centralizada en el *Directorio Activo*, se utiliza el **complemento Directiva de grupo** de la *Consola de Administración de Microsoft* o la directiva de seguridad correspondiente.

LAS DIRECTIVAS DE SEGURIDAD

Como se indicó anteriormente, puede haber tres tipos de directivas de seguridad:

- **Directiva de seguridad de dominio**. Es la que se debe utilizar si el servidor *Windows 2000* es un controlador de dominio y se desea modificar la configuración de seguridad para todos los miembros del dominio.
- **Directiva de seguridad del controlador de dominio**. Es la que se debe utilizar si el servidor *Windows 2000* es un controlador de dominio y se desea modificar la configuración de seguridad para todos los controladores de dominio.
- **Directiva de seguridad local**. Es la que se debe utilizar si el servidor *Windows 2000* actúa como servidor independiente o servidor miembro y se desea modificar su configuración de seguridad (cuenta con menos nodos de configuración que las dos anteriores).

LAS PLANTILLAS DE SEGURIDAD

Una **Plantilla de seguridad** es un archivo donde se almacena un grupo de configuraciones de seguridad (*Windows 2000* incluye una serie de plantillas de seguridad, basadas en la función de un equipo que van desde configuraciones de seguridad para los clientes de un dominio de baja seguridad hasta controladores de dominio de alta seguridad. Estas plantillas se pueden utilizar tal como se proporcionan y, también, se pueden modificar o servir como base para crear plantillas de seguridad personalizadas).

Están compuestas por:

- **Directivas de cuentas.**
- **Directivas locales.**

- **Registro de sucesos.**
- **Grupos restringidos.**
- **Registro.**
- **Servicios del sistema.**
- **Registro.**
- **Sistema de archivos.**

NOTA: Fíjese que, con la excepción de las *directivas de seguridad IP en Active Directory* y las *directivas de claves públicas*, los atributos de seguridad de una *Directiva de grupo* pueden estar contenidos en una plantilla de seguridad.

Cada plantilla se guarda como un archivo de texto (con extensión *INF*) en el directorio *\WINNT\SECURITY\TEMPLATES*. De esta forma, se pueden copiar, pegar, importar o exportar todos (o algunos de) los atributos de la plantilla.

Las plantillas se pueden aplicar a la directiva del equipo local e/o importar a un objeto de **Directiva de grupo** (de esta manera, cualquier cuenta de usuario o de equipo del sitio, dominio o unidad de organización a la que se aplica dicho objeto de *Directiva de grupo* recibirá la configuración de la plantilla de seguridad), utilizar para realizar un análisis de la seguridad o asignar automáticamente mediante el comando **Secedit**.

La plantilla inicial aplicada a un equipo se denomina **Directiva de seguridad local** y se puede exportar a un archivo de plantillas de seguridad para conservar la configuración de seguridad del sistema inicial (de esta forma, se podrá restaurar la plantilla de seguridad inicial en el futuro).

El complemento Plantillas de seguridad

El **complemento Plantillas de seguridad** de la *Consola de Administración de Microsoft* (*MMC*) permite definir y modificar plantillas de seguridad personalizadas (son las creadas por los usuarios autorizados) tomando como base una plantilla vacía o una de las plantillas predefinidas (son las que incorpora *Windows 2000*).

Para poder trabajar con dicho complemento, primero debe agregarlo a una consola *MMC* (para hacerlo consulte el apartado *Cómo crear un archivo de consola*). Una vez agregado, siga los pasos siguientes:

1. Abra la consola donde se encuentre este complemento y, en el panel izquierdo, pulse en el signo + que hay a la izquierda de **Plantillas de seguridad**.
2. Pulse en el signo + que hay a la izquierda del directorio *\WINNT\SECURITY\TEMPLATES* y le mostrará la lista de plantillas de seguridad predefinidas que hay disponibles (si se hubiera definido alguna plantilla personalizada, también se mostrará).

3. Pulse en el signo + que hay a la izquierda de la plantilla predefinida que desee y se desplegará su contenido. Realice las modificaciones que considere oportunas y, cuando haya finalizado, sitúese sobre el nombre de la plantilla que acaba de modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Guardar como**, indique el nombre que desea dar a la plantilla personalizada, marque en *Guardar* y aparecerá en el panel izquierdo junto a las plantillas anteriores (si se realizan cambios en una plantilla predefinida o personalizada y se desean guardar en dicha plantilla, se ha de seleccionar *Guardar*).

4. Si se desea crear una plantilla vacía para establecer toda la configuración de seguridad completa, sitúese sobre el directorio donde se guardan las plantillas de seguridad (*\WINNT\SECURITY\TEMPLATES*) que se encuentra en el panel izquierdo, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Nueva plantilla**, indique el nombre y la descripción que desea darle, marque en *Aceptar* y aparecerá en el panel izquierdo junto a las plantillas que anteriormente. Ahora podrá establecer la configuración de seguridad y guardarla posteriormente.

5. Cuando haya finalizado, cierre la consola y guarde su configuración (si así se lo indica).

El complemento Configuración y análisis de seguridad

El **complemento Configuración y análisis de seguridad** de la *Consola de Administración de Microsoft* (*MMC*) permite configurar el equipo y analizar su seguridad de forma local.

Para poder trabajar con dicho complemento, primero debe agregarlo a una consola *MMC*. Una vez agregado, siga los pasos siguientes:

1. Abra la consola donde se encuentre este complemento y, en el panel izquierdo, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Abrir base de datos**, indique el nombre que desea darle, marque en *Abrir*, indique la plantilla de seguridad que desea configurar y/o analizar (si desea que la plantilla que va a importar elimine cualquier otra plantilla que hubiera en la base de datos, active la casilla **Limpiar esta base de datos antes de importarla**. En caso contrario, ambas se combinarán), marque en *Abrir* y en el panel derecho le indicará los procesos que se pueden realizar.

2. Para configurar el equipo, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Configurar el equipo ahora**, indique el nombre que desea dar al archivo donde se va a guardar el registro de errores de la configuración, marque en *Aceptar* y procederá a configurar el sistema en función de la plantilla importada (le irá mostrando el proceso que está realizando). Para ver el archivo de registro con los errores encontrados en la configuración, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Ver el archivo de registro** y compruebe los errores.

   Si se han producido errores, pulse en el signo + que hay a la izquierda de **Configuración y análisis de seguridad** para que despliegue los nodos de la plantilla de seguridad que ha importado. Haga las modificaciones necesarias para corregir los errores, vuelva a configurar el equipo y compruebe de nuevo si se han producido errores.

3. Para analizar el equipo, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Analizar el equipo ahora**, indique el nombre que desea dar al archivo donde se va a guardar el registro de errores del análisis, marque en *Aceptar* y procederá a analizar el sistema en función de la plantilla importada (le irá mostrando el proceso que está realizando). Para ver el archivo de registro con los errores encontrados en el análisis, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Ver el archivo de registro** y compruebe los errores.

   Si se han producido errores, pulse en el signo + que hay a la izquierda de **Configuración y análisis de seguridad** para que despliegue los nodos de la plantilla de seguridad que ha importado. Haga las modificaciones necesarias para corregir los errores, vuelva a configurar el equipo y a analizarlo, y compruebe de nuevo si se han producido errores.

4. Si se han realizado cambios en la plantilla importada y se ha configurado y analizado el sistema sin errores, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual y seleccione **Guardar**.

5. Si desea importar otra plantilla para que se combine con una previa, active la casilla **Limpiar esta base de datos antes de importarla** cuando vaya a indicar el nombre de la plantilla y se creará una plantilla compuesta). Una vez configurado el equipo y analizado sin errores, pulse con el botón derecho del ratón sobre **Configuración y análisis de seguridad** para que muestre su menú contextual, seleccione **Exportar plantilla**, indique el nombre que desea dar a la nueva plantilla de seguridad personalizada y marque en *Guardar*.

6. Cuando haya finalizado, cierre la consola y guarde su configuración (si así se lo indica).

El complemento Directiva de grupo

El **complemento Directiva de grupo** de la *Consola de Administración de Microsoft* (*MMC*) permite configurar la seguridad de forma centralizada en el

Directorio Activo (es equivalente a la utilización de la **Directiva de grupo** que se explicará posteriormente).

Para poder trabajar con dicho complemento, primero debe agregarlo a una consola *MMC* e indique, cuando se le pregunte, el objeto *Directiva de grupo* que desee agregar. Una vez realizada la operación, siga los pasos siguientes:

1. Abra la consola donde se encuentre este complemento y, en el panel izquierdo, pulse en el signo + que hay a la izquierda de la directiva que ha agregado (en el ejemplo, **Directiva Equipo local**) y mostrará en el panel izquierdo las posibles opciones de configuración de esta directiva.

2. Si pulsa el botón izquierdo del ratón sobre el signo + que hay en cada uno de los nodos, se desplegará su contenido.

3. Las posibles opciones disponibles se explican en el apartado siguiente **Las Directivas de grupo**.

4. Cuando haya finalizado, cierre la consola y guarde su configuración (si así se lo indica).

LAS DIRECTIVAS DE GRUPO

Las **Directivas de grupo** definen los distintos componentes del entorno de escritorio del usuario que tiene que configurar un administrador del sistema (por ejemplo, los programas que tiene disponibles, los que aparecen en su escritorio y las opciones del menú **Inicio**). Influye en las cuentas de usuario y de equipo, y se puede aplicar a sitios, dominios o unidades organizativas (utilizando una unidad organizativa en la que se haya creado un único usuario o un número limitado de usuarios, se puede aplicar una **directiva de grupo** a quién se considere conveniente).

Los usuarios y los equipos son los únicos tipos de objetos del *Directorio Activo* que pueden recibir directivas (de forma específica, a los grupos de seguridad no se les aplica directivas. En lugar de ello y por motivos de rendimiento, los grupos de seguridad se utilizan para filtrar la directiva por medio del permiso **Aplicar directiva de grupos** dentro de la ficha **Seguridad** de la directiva correspondiente).

Las **Directivas de grupo** se aplican en el orden siguiente:

1. La Directiva de grupo local único (se ha de configurar utilizando el **complemento Directiva de grupo** tal y como se indicó anteriormente).

2. La Directiva de grupo del sitio (en el orden indicado).

3. La Directiva de grupo del dominio (en el orden indicado).

4. La Directiva de grupo de unidad organizativa (de mayor a menor) y, dentro de cada una de ellas, en el orden indicado.

Las **Directivas de grupo** son similares al **Editor de Directivas** del sistema que estaban incluidas en *Windows NT 4 Server*.

Una **directiva de grupo** incluye los siguientes apartados:

- **Configuración del equipo** que se aplica cuando se inicia el equipo independientemente del usuario que lo haga. Normalmente, está formada por:

  - **Configuración de software**. Corresponde a la configuración de *software* que se aplica a todos los usuarios que inician una sesión en el equipo. De este nodo cuelga **Instalación de software** (le ayuda a indicar la forma de instalar y mantener aplicaciones en la organización) y otros posibles subnodos situados allí por proveedores de *software* independientes.

  - **Configuración de Windows**. Corresponde a la configuración de las ventanas que se aplica a todos los usuarios que inician una sesión en el equipo. De este nodo cuelgan los subnodos:

    - **Archivos de comandos**. Le permite indicar la secuencia de comandos que se va a ejecutar cuando se inicie o apague el equipo.

    - **Configuración de seguridad**. Corresponde a la configuración de

- **Configuración de seguridad**. Corresponde a la configuración de seguridad que se aplica a todos los usuarios que inician una sesión en el equipo. De este nodo cuelgan varios subnodos:

  - **Directivas de cuenta** que están formadas por:

    - **Directiva de contraseñas**. Permite definir las directivas por la que se regirán las contraseñas. Entre ellas se encuentran los siguientes subnodos: **Longitud mínima de la contraseña**, **Vigencia máxima de la contraseña**, **Vigencia mínima de la contraseña**, etc.

    - **Directiva de bloqueo de cuentas**. Permite definir la directivas a seguir para el bloqueo de cuentas cuando se ha intentado iniciar una sesión y no se ha introducido correctamente la contraseña. Cuenta con los siguientes subnodos: **Duración del bloqueo de cuenta**, **Restablecer la cuenta de bloqueos Umbral de bloqueos de la cuenta**.

    - **Directiva Kerberos**. Permite definir las directivas por las que se regirá este protocolo de autentificación. Entre ellas se encuentran los siguientes subnodos: **Edad máxima de renovación de tíquets**, **Vigencia máxima del tíquet de servicio**, **Vigencia máxima del tíquet de usuario**, etc.

- **Directivas locales** que están formadas por:
  - **Directiva de auditoría**. Permite definir la directivas a seguir para el establecimiento de las auditorías. Entre ellas se encuentran los siguientes subnodos: **Auditar el acceso a objetos**, **Auditar sucesos de inicio de sesión**, **Auditar el cambio de directivas**, etc.
  - **Asignación de derechos de usuario**. Permite asignar derechos a los usuarios. Entre ellos se encuentran los siguientes: **Hacer copia de seguridad de archivos y directorios**, **Restaurar la copia de seguridad de archivos y directorios**, **Inicio de sesión local**, **Añadir estaciones al dominio**, **Denegar el acceso a la red desde este equipo**, **Tirar abajo el sistema**, etc.
  - **Opciones de seguridad**. Permite definir actuaciones a seguir referentes a la seguridad del sistema. Entre ellas se encuentran las siguientes: **Impedir que los usuarios instalen controladores**, **No mostrar el último nombre de usuario al iniciar la sesión**, **Permitir apagar el sistema sin tener que iniciar una sesión**, **Restringir el acceso al CD-ROM**, **Restringir el acceso a la unidad de disquete**, **Tiempo de inactividad requerido antes de desconectar la sesión**, etc.
- **Registro de sucesos** que define la directivas a seguir para los registros de sucesos. Entre ellas se encuentran las siguientes: **Apagar el equipo cuando se llena el registro**, **Tamaño máximo de los distintos registros**, **Conservar los distintos registros**, etc.
- **Grupos restringidos** que permite la administración de miembros de grupos locales.
- **Servicios del sistema** que define los permisos y modo de inicio para los distintos servicios locales.
- **Registro** que permite agregar claves a las categorías del *Registro* local.
- **Sistema de archivos** que define la seguridad para el sistema de archivos local.
- **Directivas de claves públicas** que están formadas por los agentes de recuperación de datos cifrados, la configuración de petición de certificados automática, la entidad emisora raíz de confianza y la confianza de empresa.

- **Directivas de seguridad IP en Active Directory** que definen las reglas de seguridad *IP* para establecer la comunicación entre equipos.

- **Plantillas administrativas**. Permiten administrar la configuración que figura en el *Registro* referente al equipo (categoría *HKEY_LOCAL_MACHINE*). Para ello, se utilizan unos archivos de texto con extensión *ADM* en los que se especifican los valores, las claves y las categorías del *Registro* asociadas. *Windows 2000* incorpora varios de ellos (*conf.adm*, *system.adm*, *inetres.adm*, *winnt.adm*, *windows.adm*, *commom.adm*, etc) pero se pueden generar otros nuevos personalizados. De este nodo cuelgan varios subnodos:
  - **Componentes de Windows**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:
    - **NetMeeting**.
    - **Internet Explorer**.
    - **Programador de tareas**.
    - **Instalador de Windows**.
  - **Sistema**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:
    - **Inicio de sesión**.
    - **Cuotas de disco**.
    - **Cliente DNS**.
    - **Directiva de grupo**.
    - **Protección de archivos de Windows**.
  - **Red**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:
    - **Archivos sin conexión**.
    - **Conexiones de red y de acceso telefónico**.
  - **Impresoras**. Incorpora directivas para su habilitación y configuración.
- **Configuración de usuario** que se aplica cuando un usuario inicia una sesión independientemente del equipo en donde lo haga. Normalmente, está formada por:
  - **Configuración de software**. Corresponde a la configuración de *software* que se aplica a los usuarios, independientemente del equipo en el que inicien una sesión. De este nodo cuelga **Instalación de software** (le ayuda a indicar la forma de instalar y mantener aplicaciones en la

organización) y otros posibles subnodos situados allí por proveedores de *software* independientes.

- **Configuración de Windows**. Corresponde a la configuración de las ventanas que se aplica a los usuarios, independientemente del equipo en el que inicien una sesión. De este nodo cuelgan varios subnodos:

  - **Mantenimiento de Internet Explorer**. Cuenta con los siguientes subnodos que incorporan distintas opciones para su configuración:

    - **Interfaz de usuario del explorador**.
    - **Conexión**.
    - **Direcciones URL**.
    - **Seguridad**.
    - **Programas**.

  - **Archivos de comandos**. Le permite indicar la secuencia de comandos que se va a ejecutar cuando un usuario inicie o finalice una sesión.

  - **Configuración de seguridad** que está formada por la confianza de empresa dentro de las directivas de claves públicas.

  - **Servicios de instalación remota**. Permiten establecer las opciones disponibles para los usuarios durante el *Asistente para la instalación de clientes*.

  - **Redireccionamiento de carpetas**. Permite redirigir algunas carpetas especiales de *Windows 2000* (que se encuentran en *Documents and Settings*) a ubicaciones de red. De este nodo cuelgan varios subnodos que corresponden a distintas carpetas:

    - **Datos de programa**.
    - **Escritorio**.
    - **Mis documentos**.
    - **Menú Inicio**.

- **Plantillas administrativas**. Permiten administrar la configuración que figura en el *Registro* referente al usuario (categoría *HKEY_CURRENT_USER*). Para ello, se utilizan unos archivos de texto con extensión *ADM* en los que se especifican los valores, las claves y las categorías del *Registro* asociadas. *Windows 2000* incorpora varios de ellos (*conf.adm*, *system.adm*, *inetres.adm*, *winnt.adm*, *windows.adm*, *commom.adm*, etc) pero se pueden generar otros nuevos personalizados. De este nodo cuelgan varios subnodos:

  - **Componentes de Windows**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:

    - **NetMeeting**.
    - **Internet Explorer**.
    - **Explorador de Windows**.
    - **Microsoft Management Console**.
    - **Programador de tareas**.
    - **Instalador de Windows**.

  - **Menú Inicio y barra de tareas**. Incorpora directivas para su habilitación y configuración.

  - **Escritorio**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:

    - **Active Desktop**.
    - **Active Directory.**

  - **Panel de control**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:

    - **Agregar o quitar programas**.
    - **Pantalla**.
    - **Impresoras**.
    - **Opciones regionales**.

  - **Red**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:

    - **Archivos sin conexión**.
    - **Conexiones de red y de acceso telefónico.**

  - **Sistema**. Cuenta con los siguientes subnodos que incorporan directivas para su habilitación y configuración:

    - **Inicio/cierre de sesión**.
    - **Directiva de grupo**.

El redireccionamiento de carpetas de los usuarios proporciona ventajas para ellos, pero es especialmente importante la redirección de la carpeta **Mis documentos**, ya proporciona las siguientes ventajas:

- Si un usuario inicia una sesión en varios equipos de la red, los documentos siempre estarán disponibles.

- Cuando se utilizan perfiles de usuario móviles, únicamente será necesario indicar la ruta de acceso de red de la carpeta **Mis documentos** (en lugar de la propia carpeta).

- Se puede realizar una copia de seguridad de los datos almacenados en un servidor de red compartido como parte de la administración habitual del sistema (es más seguro, ya que no se requiere ninguna acción por parte del usuario).

- El administrador del sistema puede utilizar la *Directiva de grupo* para establecer cuotas de disco, con lo que limita la cantidad de espacio que ocupan las carpetas especiales de los usuarios.

- Los datos específicos de un usuario pueden redirigirse a otro disco duro del equipo local del usuario desde el disco duro en el que se encuentran los archivos del sistema operativo (de esta forma, los datos del usuario estarán más seguros si tiene que volverse a instalar el sistema operativo).

LOCALIZACIÓN Y RESOLUCIÓN DE PROBLEMAS

Es necesario controlar el rendimiento del sistema revisando ciertos factores como, por ejemplo, el tiempo que tarda el sistema en recuperar los programas del disco duro del servidor, en clasificar una base de datos, en ejecutar un programa, en guardar un archivo, etc.

Los cambios en el rendimiento ocurren normalmente de forma gradual, aunque no lo note hasta que sucede algo anormal en la red.

Normalmente, debido a la forma de trabajo del sistema operativo de la red, el rendimiento de un disco duro de la red es superior al obtenido con otro tipo de unidades.

Controle de forma periódica el rendimiento del sistema y compare los resultados sucesivos. Será capaz de distinguir las variaciones en el rendimiento cuando la red esté ocupada y, al mismo tiempo, los resultados que produzcan podrán ser la primera pista cuando el rendimiento del sistema empiece a funcionar peor.

Los problemas de funcionamiento de la red que se podrán encontrar pueden depender del *software* o del *hardware*.

Localización y resolución de problemas de software

Generalmente, los problemas de *software* se originan al no ser instalados de forma adecuada o al utilizar programas monousuario en la red. Normalmente, estos problemas afectan solamente a algún programa y pueden ocurrirle a uno o a todos los usuarios de dicho programa.

Si sospecha que el fallo de funcionamiento es debido a un problema de *software*, lo primero que deberá hacer es comprobar los derechos de todos los usuarios que están teniendo problemas.

Un error muy común es instalar y probar el *software* como administrador y, como tiene todos los derechos en todos los directorios, puede ocurrir que después se genere algún error al no contar los usuarios con tantos derechos como él.

Si los derechos de seguridad no son la causa del problema, compruebe la configuración del *software*. Muchos de los programas contienen archivos ejecutables y archivos de configuración, así que deben están localizados en directorios compartidos.

Si aún sigue dando problemas, vuelva a reinstalar el *software* en un nuevo subdirectorio y siga al pie de la letra el manual sin saltarse ningún paso de la instalación.

Si no se soluciona el problema, consulte con el distribuidor del programa.

Localización y resolución de problemas de hardware

La localización y reparación de los problemas de *hardware* empiezan en la estación de trabajo que produce el error de funcionamiento.

Cuando ocurra un problema de *hardware*, primero ha de inspeccionar la tarjeta adaptadora de red instalada en la estación de trabajo, así como los cables de la red y las conexiones con la tarjeta.

COMPROBACIÓN DE LAS TARJETAS ADAPTADORAS DE RED

Si una estación de trabajo falla al colocarse por primera vez en la red, asegúrese de que la tarjeta está colocada de forma adecuada en el ordenador.

Si la estación sigue fallando, compruebe las especificaciones de la tarjeta adaptadora de red.

Todas las tarjetas adaptadoras de red requieren el uso de interrupciones (*IRQ*), acceso de memoria dinámica (*DMA*) y puertos de entrada/salida (*I/O Ports*).

Las **interrupciones** son señales que se envían desde un dispositivo al procesador del sistema para su control. Van numeradas desde el número cero al quince.

El **acceso de memoria dinámica** es un método rápido de transferencia de información desde un dispositivo de almacenamiento a la memoria sin control del procesador.

Los **puertos de entrada/salida** describen la transferencia de datos entre el ordenador y los dispositivos periféricos.

Otras tarjetas, como la del ratón, las tarjetas de puerto serie, controladoras, etc., usan también interrupciones. Compruebe que la tarjeta adaptadora de red no

utiliza la misma interrupción y la misma dirección de memoria que las otras tarjetas que estaban instaladas anteriormente.

La mayoría de las veces no podrá saber las direcciones de las otras tarjetas que haya. En tal caso, la mejor solución es quitar las tarjetas que no sean esenciales. Después, coloque la tarjeta adaptadora de red en el ordenador e intente conectarse. Si puede hacerlo, empiece a colocar las otras tarjetas, una a una y probando la conexión cada vez, hasta encontrar la que origina el fallo de la estación de trabajo.

COMPROBACIÓN DE LOS CABLES

Los problemas de los cables son muy difíciles de diagnosticar. Si sospecha de un problema con un cable, primero compruebe que está conectado de forma adecuada con la tarjeta adaptadora de red.

Después, compruebe si el cable está partido. Un cable partido, interrumpirá el acceso de la estación de trabajo a la red. Un cable dañado puede permitir a la estación de trabajo seguir funcionando, pero de forma deficiente.

También es posible que fallen las conexiones. Es fácil que no hagan buen contacto con el cable y no permitan el correcto funcionamiento.

COMPROBACIÓN DEL RESTO DEL HARDWARE

El *hardware* específico de la red, las tarjetas y los cables, no son siempre los únicos responsables de los problemas de *hardware*. A veces el problema está en el servidor o en una estación de trabajo.

Los tres componentes con más posibilidades de fallo del servidor son la tarjeta controladora del disco, el disco duro y la memoria *RAM*.

La tarjeta controladora y el disco duro del servidor están constantemente en uso y pueden fallar en cualquier momento. Cuando la tarjeta controladora funciona mal, el servidor puede enviar un mensaje de error (normalmente no). Cuando falla el disco duro, casi siempre aparece un mensaje de error en el momento de arrancar el servidor.

Los problemas con la memoria pueden generar algún mensaje. Algunas veces aparecerá un mensaje de error que informa de un problema en la memoria que produce una paralización del servidor, pero puede que no se repita en un período de tiempo, con lo que es difícil la reparación por parte del servicio técnico.