

Materia: Sistemas Operativos  
Tema: Registro MS/Windows 2000  
Versión: Mayo 2007  
Palabras claves: Registro, Windows 2000, Regedit, Regedt32  
Autor: Nicolás Alonso. Colaborador

**Temario:**

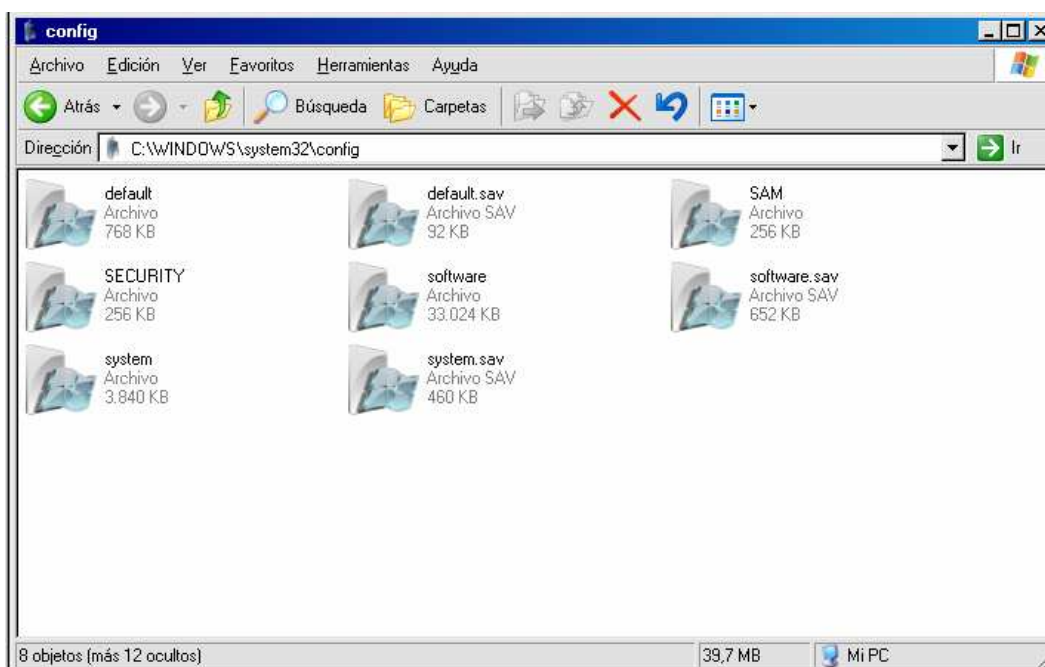
1. Registro:
  - 1.1. ¿Qué es el Registro?
  - 1.2. Orígenes del Registro
  - 1.3. Datos del Registro
  - 1.4. Estructura del registro
    - 1.4.1. Las claves predefinidas
      - 1.4.1.1. Classes
      - 1.4.1.2. Users
      - 1.4.1.3. Local Machine
      - 1.4.1.4. Current Configuration
2. Como utilizan las aplicación el registro
  - 2.1. Editores del registro
  - 2.2. Cuando utilizar las herramientas de modificación del Registro
3. Almacenamiento de datos
  - 3.1. Tipos de datos útiles
  - 3.2. Claves volátiles
  - 3.3. Claves basadas en disco
4. Como utilizar REGEDIT
  - 4.1. Búsqueda de claves y valores
  - 4.2. Edición de las entradas de valor
  - 4.3. Adición y eliminación de claves y valores
  - 4.4. Importación y exportación de información del Registro
  - 4.5. Conexión al Registro de una máquina remota
  - 4.6. Cambiar nombres de claves y valores
5. Como buscar cambios del Registro con REGEDIT
6. Cómo utilizar REGEDT32
  - 6.1. Edición de entradas de valor
  - 6.2. Adición de claves y valores
  - 6.3. Eliminación de claves y valores
  - 6.4. Carga, descarga e importación de datos del Registro
  - 6.5. Conexión al Registro de una máquina remota
  - 6.6. Administración de la seguridad en las claves del Registro
  - 6.7. Algunos trucos útiles
7. Copia de Seguridad y Recuperación del Registro
  - 7.1. Selección de un método de copia de seguridad
  - 7.2. Copia de seguridad de Windows 2000
  - 7.3. El Disco de reparación ante emergencias
  - 7.4. Copias de seguridad manuales
  - 7.5. Copia de seguridad del Registro
  - 7.6. Grabación de una copia del Registro
  - 7.7. Recuperación del Registro
8. Uso de la ultima configuración buena conocida
9. Bibliografía consultada

## 1. Registro

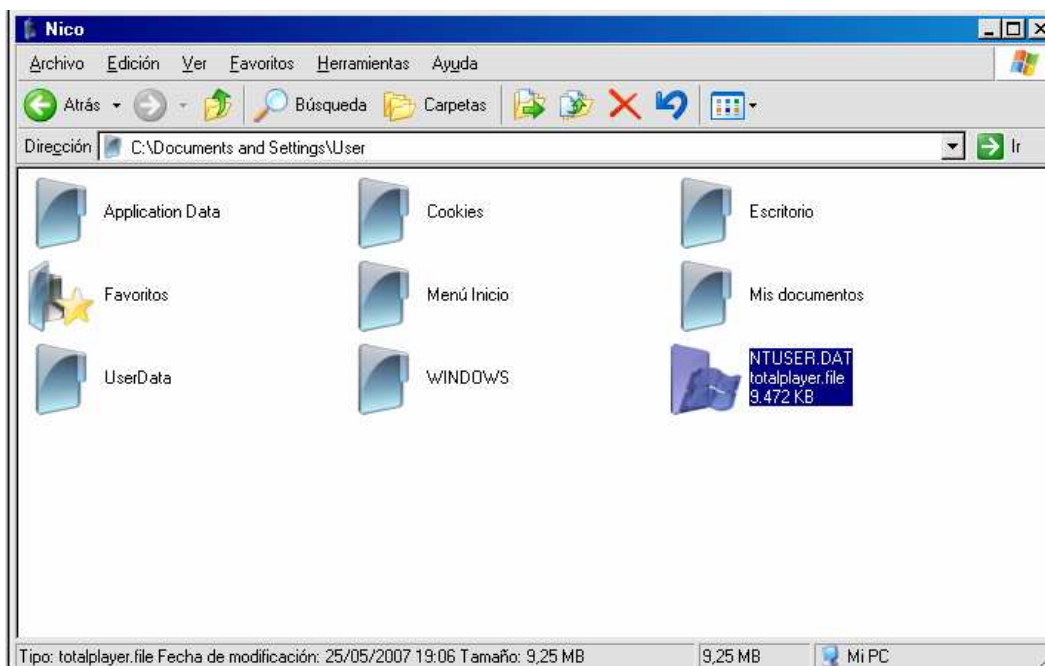
### 1.1. ¿Qué es el Registro?

El Registro es una base de datos jerárquica y centralizada, que organiza todos los parámetros de configuración del sistema. Las aplicaciones, los componentes del sistema, los controladores de dispositivos e incluso el núcleo de Microsoft Windows 2000 utilizan el Registro para almacenar sus preferencias, leerlas de nuevo y obtener información acerca de la configuración hardware del sistema, las preferencias de usuario actuales y las configuraciones predeterminadas que deben usarse cuando no existen parámetros predefinidos (como por ejemplo, cuando un usuario nuevo inicia una sesión en el sistema por primera vez).

El registro reside en un conjunto de archivos en el disco, en el directorio %SYSTEMROOT%\system32\config llamados SECURITY, SYSTEM, SOFTWARE y DEFAULT:



Así como en otro archivo en el directorio %USERPROFILE% llamado NTUSER.DAT:



El registro contiene todas las opciones de configuración que utiliza el sistema operativo y la mayor parte de las aplicaciones. El sistema operativo (SO) almacena en el Registro todo lo que diferencia la configuración de una máquina de otra como, por ejemplo, la dirección TCP/IP, el nombre del equipo, las impresoras instaladas, etc. Cualquier configuración que se pueda hacer en Windows 2000 se establece en el registro.

El registro se almacena en un formato propietario de Microsoft. No se puede editar por cualquier programa, sino con un Editor del Registro ó con una aplicación que hace las llamadas a API Win32 adecuadas. Una aplicación, puede tener acceso a cualquier clave del Registro a la que tenga acceso el usuario que ha iniciado la aplicación. Los datos del registro se almacenan en archivos binarios.

## 1.2. Orígenes del Registro

Antiguamente, en los años de Microsoft Windows 3.1, tanto las aplicaciones como el propio Windows almacenaban la información de sus configuraciones en archivos .INI. Estos archivos eran fáciles de editar, lo cual tenía sus ventajas y desventajas -los usuarios podían realizar cambios fácilmente cuando era necesario, pero también podían efectuar cambios cuando éstos no eran necesarios-. La proliferación de aplicaciones Windows supuso el esparcimiento por las computadoras de docenas de archivos .INI, cada uno de ellos con su propia combinación de parámetros (sin que la mayoría de éstos pudiera ser documentado o incluso comprendido por personas que no fueran los propios programadores de la aplicación).

Windows NT 3.1 casi eliminó por completo los archivos .INI introduciendo el predecesor de lo que hoy se conoce como Registro de Windows 2000. El Registro de Windows NT 3.1 tenía algunas características de importancia que han continuado -ó no han sufrido alteraciones- hasta Windows 2000:

- La información del Registro se organiza por categorías, de forma que los parámetros que pertenecen a un usuario concreto (como la elección del papel del tapiz) se guardan separadamente de los parámetros de otros usuarios o los propios parámetros internos del sistema. Cada parámetro se guarda como una pieza de información independiente.
- La información del Registro se almacena en archivos de base de datos binarios en disco; la única forma de visualizar o editar estos archivos es utilizando herramientas especiales destinadas a este propósito que se llaman a través de las rutinas de acceso al Registro de la Win32 API.
- Cada elemento de datos en el Registro tiene un tipo de datos, como REG\_DWORD (un entero largo) o REG\_SZ (una cadena ASCII). Los editores del Registro del sistema vigilan el cumplimiento de estos tipos de datos, por eso, no puede ponerse una cadena donde habría que poner un número.
- Al igual que cualquier objeto del sistema, cada elemento del Registro tiene un propietario, pudiendo tener su propio conjunto de listas de control de acceso (Access Control Lists, ACL) y controles de auditoria.
- Con los permisos apropiados, los administradores o programas de una computadora pueden conectarse, leer y modificar los registros de computadoras remotas.

Algunas de estas características también existen en Windows 95/98, que comparten los principios de organización del Registro de Windows NT sin sus características de seguridad y acceso remoto. Las dos familias de sistemas operativos (SO) utilizan formatos internos diferentes para sus bases de datos del Registro, a pesar de que sus registros parecen similares para las herramientas de edición del Registro; sus archivos no son intercambiables ni interoperativos.

## 1.3. Datos del Registro

La información del Registro se utiliza en seis áreas diferentes:

- La información del Registro se utiliza durante la puesta en marcha, instalación, configuración y eliminación del propio SO, de componentes del SO como los servicios de Internet Information Server (IIS) o Certificate Server, así como de dispositivos hardware. Cada vez que se ve un «Agregar/eliminar algo a otro Asistente» se utiliza la información del Registro.
- Durante el tiempo de inicio del sistema, el reconocedor de Windows 2000 (Ntdetect.com) y algún código asociado en el núcleo de Windows 2000 busca los dispositivos hardware y almacena lo que encuentra en una porción de memoria del Registro.
- El núcleo de Windows 2000 utiliza la información recogida durante el inicio del sistema para decidir qué controladores de dispositivo cargar y en qué orden; también almacena la información que necesitan dichos controladores en el Registro.
- Los controladores de dispositivo utilizan la información escrita por el reconocedor y el núcleo para autoconfigurarse en función del hardware físico que se encuentre en la máquina.
- Las herramientas del sistema y las aplicaciones, como los paneles de control y algunos complementos MMC, leen y escriben información de configuración en el Registro.
- Las aplicaciones pueden almacenar sus propios parámetros en el Registro; es más, pueden incluso leer (y posiblemente escribir) la información reunida por otro software que utiliza el Registro.

1.4. Estructura del registro

En un sistema de archivos, los objetos raíz son discos que contienen carpetas o archivos. Una carpeta concreta puede contener un número arbitrario de otras carpetas y archivos; cada carpeta o archivo tiene un nombre. Combinando los nombres de las carpetas que incluyen un archivo, se puede construir un camino capaz de nombrar sin ambigüedad un único archivo del disco, de forma que, por ejemplo, C:\Windows\Mapi32.dll y C:\Winnt\Mapi32.dll sean dos archivos completamente distintos.

Microsoft ha creado estándares sobre como se debería estructurar la información en el Registro y como almacenar datos en el Registro. El registro se asegura con los mismos permisos que utiliza Windows 2000 para asegurar archivos. Estos permisos existen incluso si la partición del sistema no admite la seguridad de archivos.

El Registro de Windows 2000 se encuentra organizado en gran parte como un "sistema de archivos". En la raíz de la estructura del Registro se encuentran las claves predefinidas (comparables con los discos en el sistema de archivos). Cada clave predefinida contiene varias subclaves (carpetas); continuando, estas subclaves contienen otras subclaves y valores (las que equivalen en el Registro a los archivos).

Al igual que pasa con los archivos, cada valor tiene un nombre que debe ser único en la subclave o carpeta que lo contiene; cada valor tiene un tipo de datos asociado que rige el tipo de datos que puede soportar.

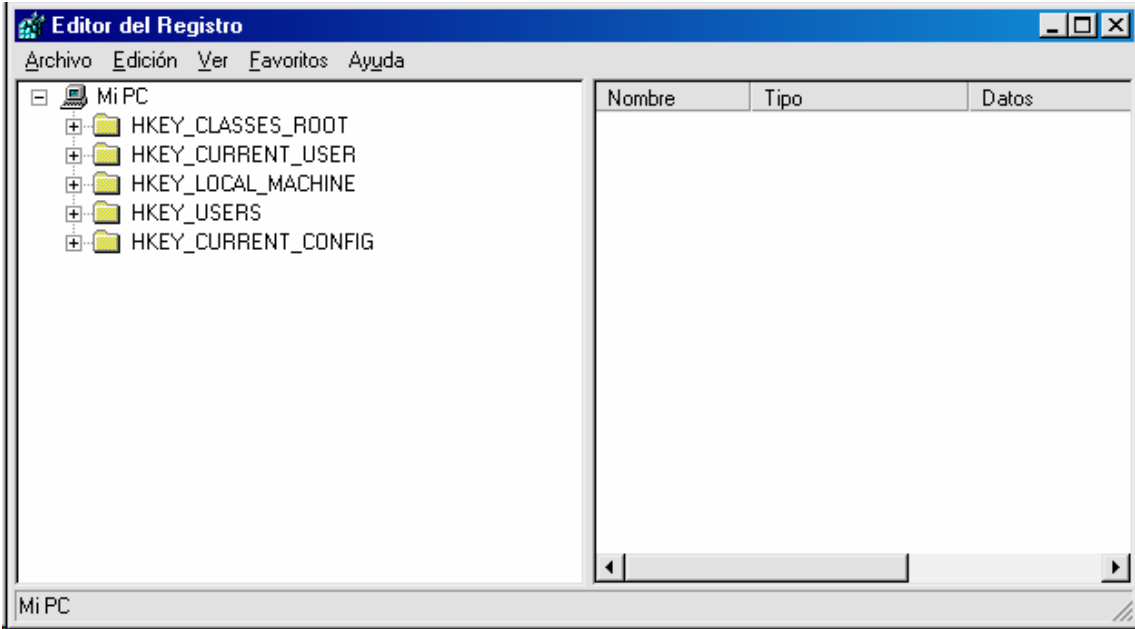
Cualquier valor del Registro puede identificarse especificando su camino completo comenzando desde la raíz. Por ejemplo, el camino:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Microsoft
\Exchange
\Security
\ObscureWireDataFormat
```

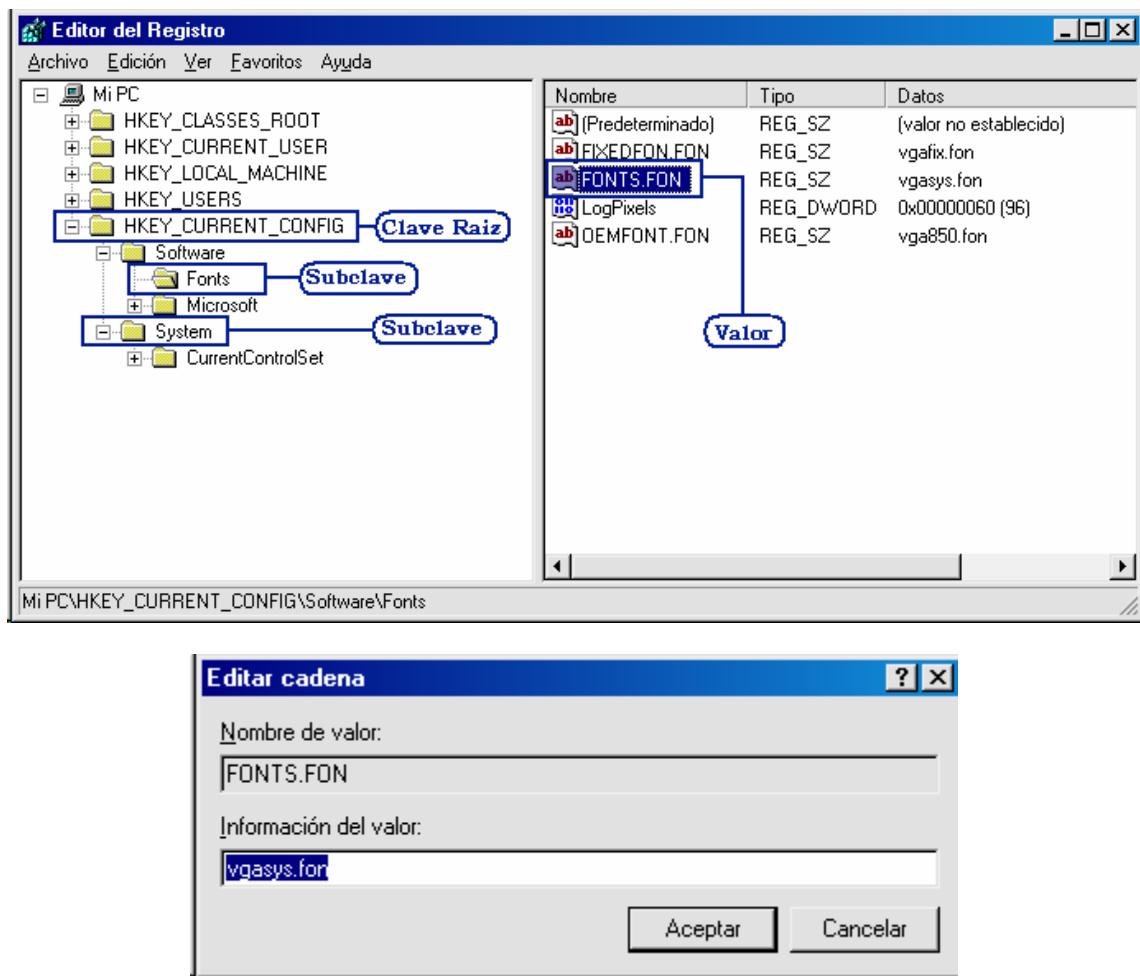
Especifica un valor concreto en la subclave de Security perteneciente a Microsoft Exchange Server.

1.4.1. Las claves predefinidas

El Registro tiene actualmente cuatro claves predefinidas diferentes, que en realidad son cuatro bases de datos llamadas "secciones". Estas secciones son Classes, Users, Local Machine y Current Configuration.



Como dijimos anteriormente, el Registro contiene dos tipos de elementos: claves y valores. Una clave es como una carpeta en el sistema de archivos, pero en lugar de contener archivos, una clave contiene valores. Cada clave tiene al menos un valor, llamado (Predeterminado) y puede contener muchos más valores.



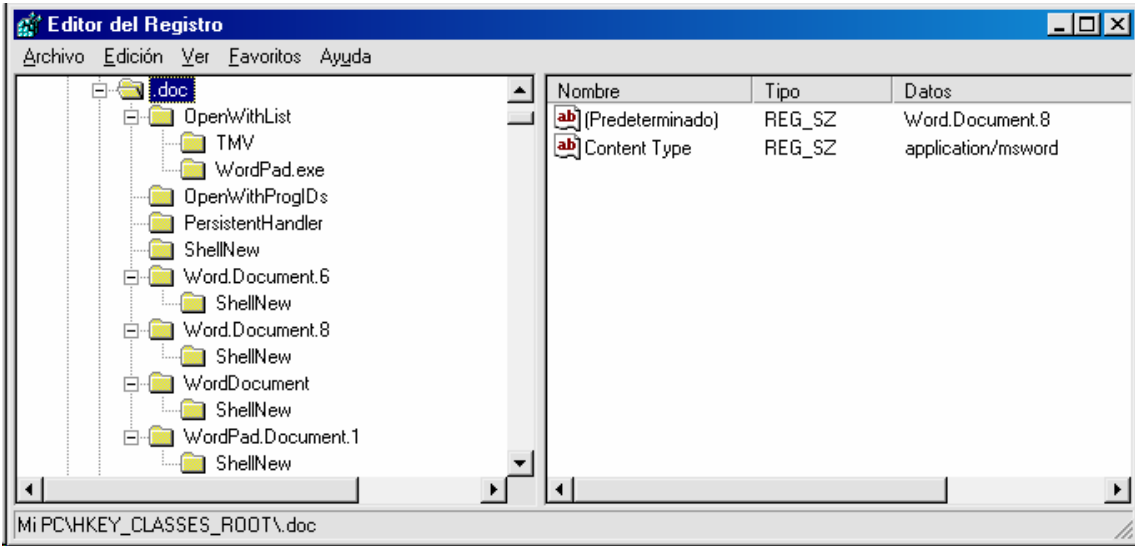
Cada jerarquía se divide de forma diferente:

- HKEY\_CLASSES\_ROOT enlaza las extensiones de archivo y los identificadores de clases OLE; realmente apunta a HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes. Los componentes del sistema como el explorador de Windows (y Microsoft Internet Explorer) utilizan estas asociaciones para determinar qué componentes o aplicaciones usar cuando se abre o se crea un tipo particular de archivo a objeto de datos. Dado que Windows 2000 se basa profundamente en el Modelo de objetos de componentes (Component Object Model, COM), quien a su vez se basa en los identificadores de objeto que se encuentran en HKEY\_CLASSES\_ROOT, esta clave y sus subclaves son más importantes de lo que pudiera parecer en un principio.
- HKEY\_CURRENT\_USER apunta al perfil del usuario que haya iniciado la sesión actual dentro de HKEY\_USERS. Microsoft requiere que las aplicaciones de Windows 2000 guarden las preferencias específicas de los usuarios en las subclaves que se encuentran por debajo de HKEY\_CURRENT\_USER; por ejemplo, HKEY\_CURRENT\_USER\SOFTWARE\Binary Research\GhostSrv\Settings almacena las preferencias de usuario personales del producto Symantec's Ghost. Otro tipo de configuración de usuario para el mismo producto se encontraría disponible en la misma clave sólo cuando el usuario se encuentre con una sesión abierta.
- HKEY\_LOCAL\_MACHINE almacena todos los parámetros pertenecientes a la máquina local. Por ejemplo, la subclave HARDWARE de HKEY\_LOCAL\_MACHINE, es donde el sistema y sus controladores de dispositivo almacenan y comparten la información de los dispositivos hardware que el sistema encuentra durante el inicio (al igual que otros dispositivos Plug-and-Play que se pueden añadir una vez que el sistema se ha iniciado). Las aplicaciones sólo deben guardar información aquí si ésta pertenece a todo el mundo que utiliza la máquina; por ejemplo, un controlador de impresora podría guardar aquí un conjunto de parámetros predeterminados de impresión y copiarlos a cada perfil de usuario nuevo cuando éste o ésta inician una sesión.
- HKEY\_USERS contiene una entrada para cada usuario que haya iniciado una sesión previamente en la computadora. Cada entrada de usuario pertenece a la cuenta del mismo usuario, y contiene los parámetros del perfil habilitado para ese usuario. Cuando se utilizan directivas de grupo, los parámetros de directiva especificados se aplican al perfil de cada usuario concreto aquí.
- HKEY\_CURRENT\_CONFIG guarda la información relativa a la configuración actual del inicio del sistema. En particular, contiene información sobre el conjunto actual de servicios del sistema, así como sobre los dispositivos presentes durante el tiempo de inicio. Esta clave predefinida es realmente un puntero a secciones dentro de HKEY\_LOCAL\_MACHINE.

Veamos en detalle cada una de ellas:

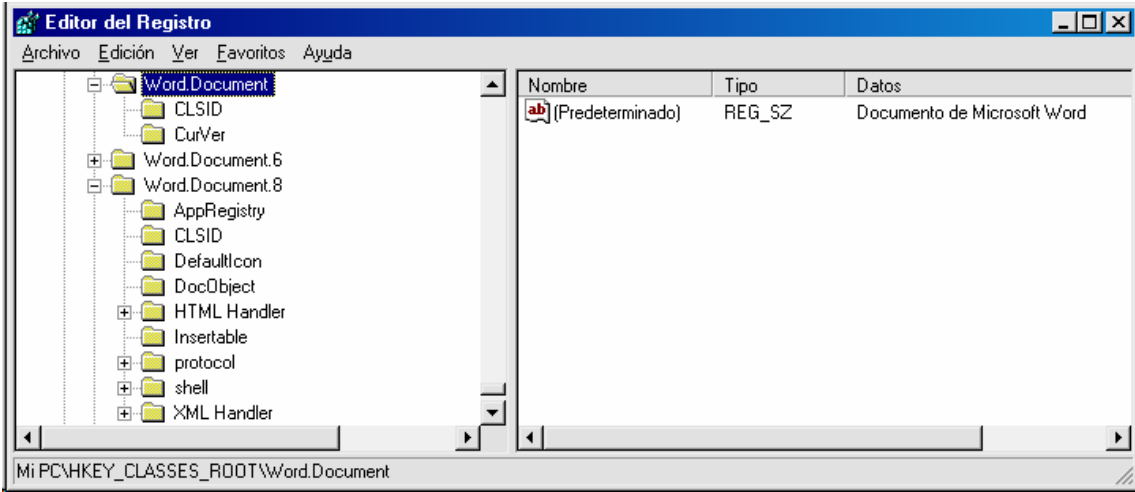
1.4.1.1 La sección Classes

La sección Classes, etiquetada, HKEY\_CLASSES\_ROOT, se almacena en el archivo SYSTEM del Registro. Esta clave almacena las opciones de configuración y registro de los componentes OLE ó ActiveX. ¿Si alguna vez te preguntaste como sabe Windows que debe iniciar Microsoft Word cuando se ejecuta un archivo con extensión .DOC? Esto es posible porque las primeras claves de esta sección determinan como ejecutar programas con diferentes extensiones.



Todas estas claves comienzan con un "." Y las secciones se enumeran siempre por orden alfabético, por lo que es fácil seleccionarl

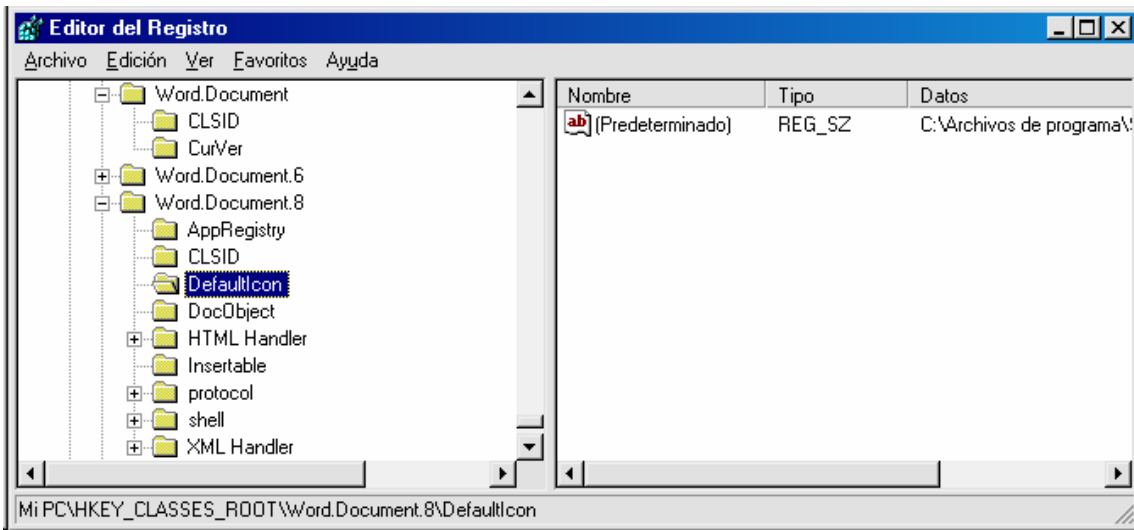
Las claves precedentes incluyen nombres de clases instaladas en la maquina y como tener acceso a las mismas. Muchas de las clases instaladas tienen dos claves diferentes. La primera es una clave de versión independiente y la segunda es una clave de versión dependiente. Por ejemplo, existe una clave Word.Document y una clave Word.Document.8. La clave Word.Document apunta a la clave Word.Document.8 que, a su vez, apunta a Microsoft Word.



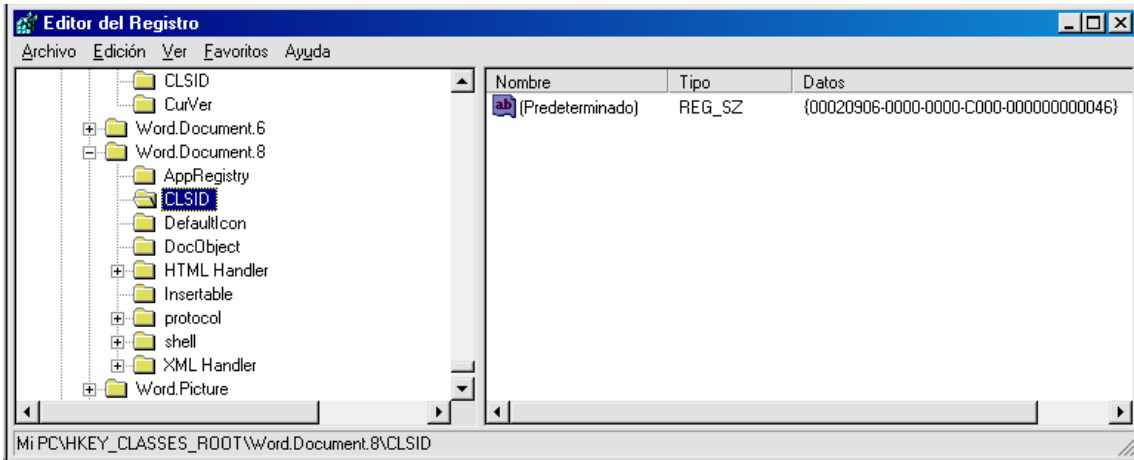
La mayoría de estas clases tienen como mínimo dos claves por debajo de ellas, una llamada CLSID y otra llamada CurVer. La clave CLSID tiene un valor predeterminado que corresponder a un identificador global único (GUID, Globally Unique Identifier) para el objeto.

El valor predeterminado de la clave CurVer suele ser el nombre de la versión de la aplicación; por lo tanto para Word.Document la clave CurVer contiene Word.Document.8. Un poco más debajo de la lista, si se examina la clave Word.Document.8, aparecerían las subclaves para la aplicación, la ubicación del icono que debe utilizar para el documento en el Explorador y una clave que explica al sistema operativo (SO) como abrir uno de estos archivos cuando se hace doble click.





La clave `Word.Document.8` también contiene el GUID para la clase, que debe parecerse a: `{00020906-0000-0000-C000-000000000046}`. Cada clase posee un identificador diferente; de esta forma es como se identifica realmente a la clase.

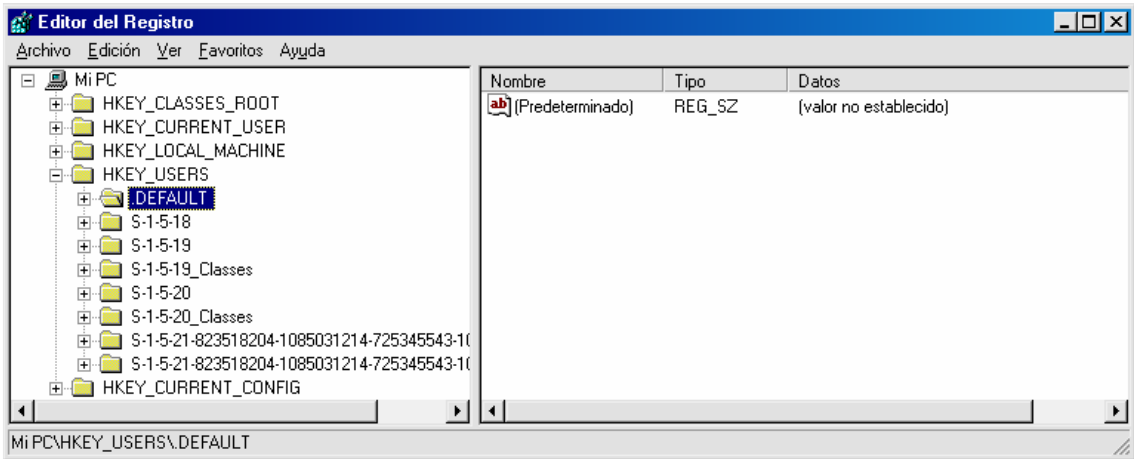


1.4.1. 2 La sección Users

La sección `Users`, que aparece como `HKEY_CURRENT_USER`, contiene las opciones definidas por el usuario para todas las aplicaciones y para el sistema operativo (SO). La sección `Users`, contiene lo que se llama “un perfil del usuario” que engloba todas las opciones de configuración, desde la imagen de fondo del escritorio hasta como colocar una ventana en la pantalla.

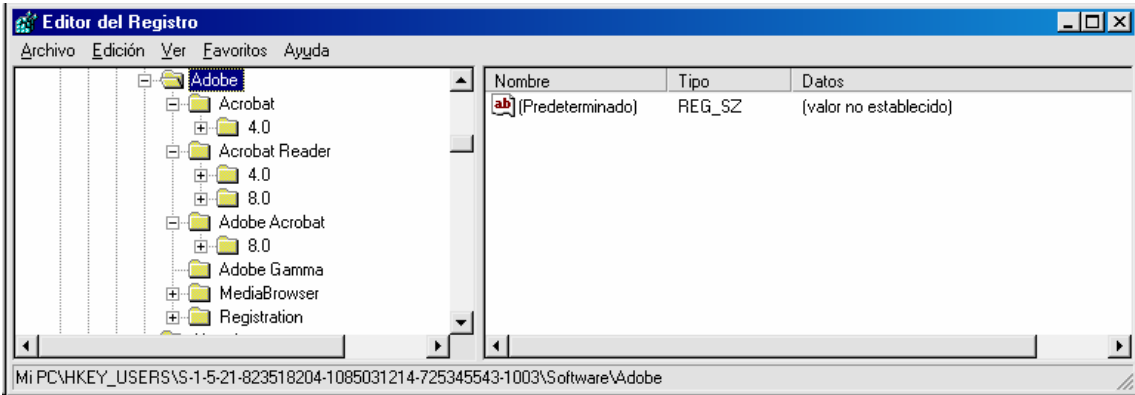
En el Registro existe también una entrada para `HKEY_CURRENT_USER`; esta entrada es realmente un vínculo con la sección `HKEY_USER` y refleja las opciones de configuración del usuario que ha iniciado actualmente una sesión.

La sección `Users` se divide en dos secciones principales: una se llama `.DEFAULT`, que contiene las opciones predeterminadas que obtendrán los usuarios nuevos que inicien una sesión por primera vez en el sistema. Las demás entradas son GUID, para todos los usuarios y contienen un perfil para cada usuario que haya iniciado una sesión en la maquina.



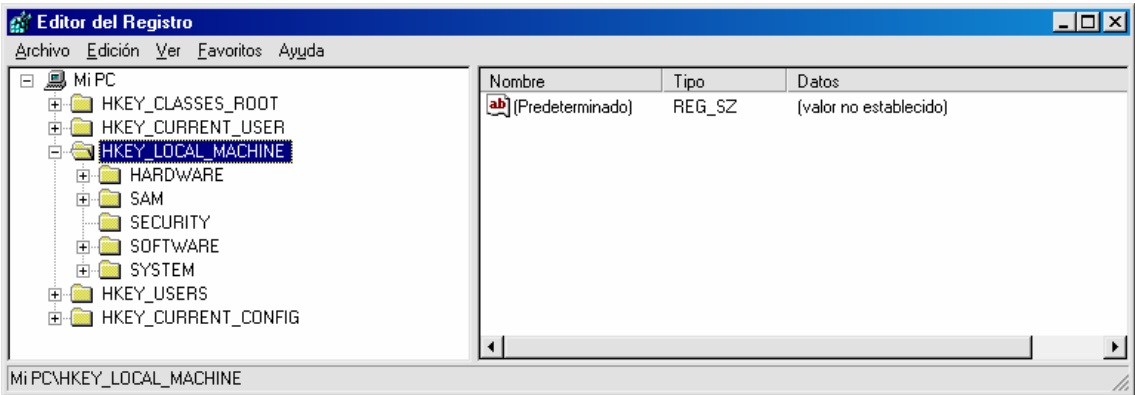
Cuando un usuario inicia una sesión, parte del proceso de inicio comprueba si el usuario ha iniciado anteriormente una sesión en esa maquina: si así es, la clave HKEY\_CURRENT\_USER se vincula a la GUID para ese usuario. Si el usuario no ha iniciado una sesión anteriormente, se crea una nueva entrada para el usuario con el GUID y, a continuación, se copia al usuario nuevo el contenido del usuario .DEFAULT. Si es necesario hacer cambios par cada usuario que inicie una sesión en la máquina, hacer cambios en el usuario .DEFAULT hará todos esos cambios para todos los nuevos inicios de sesión de la maquina, pero no hará los mismos cambios para los usuarios existentes.

Para un usuario individual, la sección contendrá muchas opciones de configuración diferentes; dependiendo de lo que este instalado en la maquina local. Una clave interesante es Software, dicha clave contiene datos para todas las aplicaciones almacenadas en la maquina, organizadas por el fabricante del software y por la aplicación. Por ejemplo, el software de Adobe Acrobat crea una clave Adobe y una subclave para Acrobat. Hay muchas claves creadas en Acrobat, pero por debajo de ese nivel la organización es responsabilidad absoluta del fabricante de software (y en última instancia del programador).



1.4.1.3. La sección Local Machine

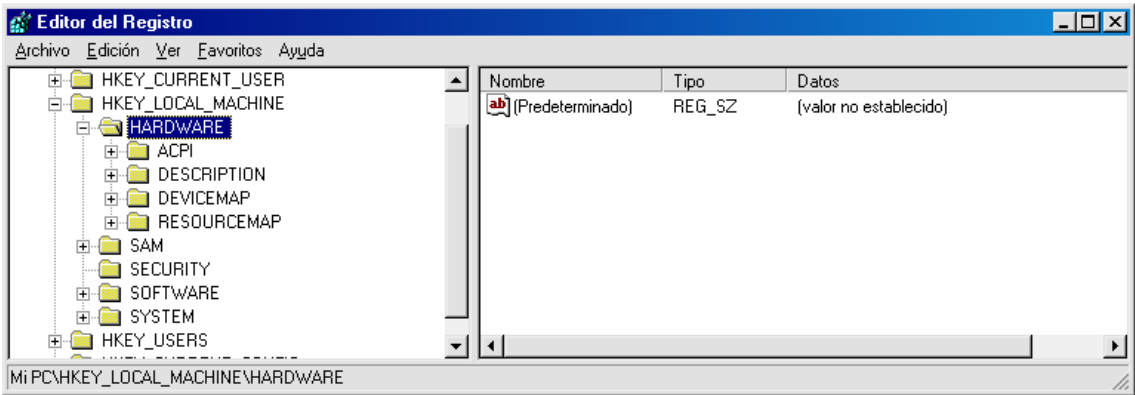
La sección Local Machine contiene la información independiente del usuario para la maquina local. Esto significa que toda la información relacionada con el inicio y las interfaces hardware, así como la información que necesita el software para ejecutarse independientemente del usuario que inicie la sesión, se almacena en la sección Local Machine del Registro.



Ahora veremos, con más detalles, cada subclave de la sección Local Machine:

HKEY\_LOCAL\_MACHINE\HARDWARE

La subclave HKEY\_LOCAL\_MACHINE\HARDWARE almacena la información del hardware que se encuentra en el sistema. Todos los valores que se almacenan aquí se mantienen sólo en la RAM, no en el disco, debido al ordenamiento del controlador de dispositivos mencionado anteriormente.



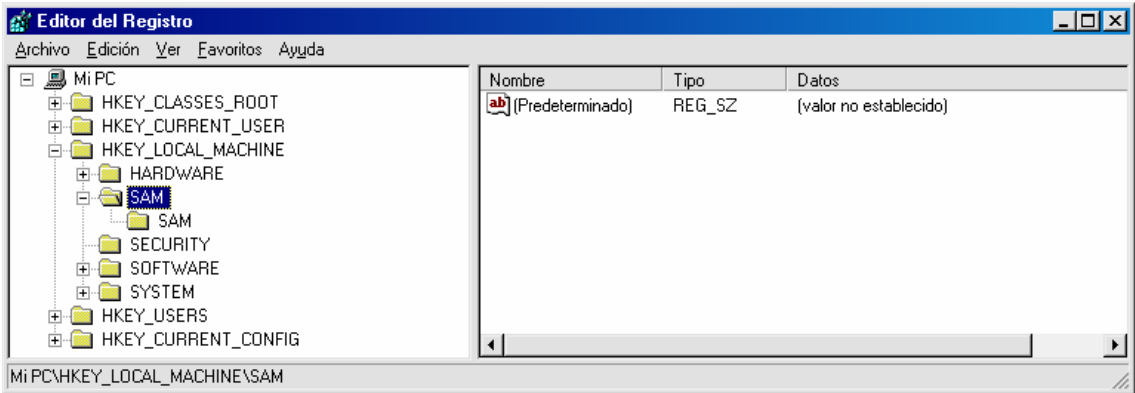


Cuando el reconecedor de hardware se ejecuta, enumera todos los dispositivos que encuentra al explorar los buses del sistema y buscar clases específicas de dispositivos, como puertos paralelos o teclados. Por debajo de HKEY\_LOCAL\_MACHINE\HARDWARE subyacen tres subclases importantes:

- La subclave DESCRIPTION contiene descripciones de las CPU, procesadores en coma flotante y dispositivos multifunción del sistema. La información almacenada aquí se ha incrementado considerablemente en comparación con lo que se encuentra disponible en Windows NT 4; por ejemplo, la subclave CentralProcessor hace un seguimiento de un cierto número de parámetros que no se encuentran disponibles en Windows NT 4. Para computadoras que usan placas base multipropósito, como la serie Intel BX, uno de los dispositivos multifunción reflejado en esta subclave refleja los controladores integrados de la placa base, con entradas separadas para los controladores de disco, teclado, puntero, paralelo y serie.
- La subclave DEVICEMAP vincula un dispositivo específico a un controlador específico. Por ejemplo, DEVICEMAP\Video contiene un valor denominado \Device\Video1 que contiene una cadena \REGISTRY\Machine\SYSTEM\ControlSet001\Services\mnmdm\Device0, que es un puntero al lugar donde el controlador para esa controladora de vídeo almacena sus parámetros.
- La subclave RESOURCEMAP existe en Windows NT 4, pero se ha reorganizado completamente en Windows 2000. Ahora contiene tres subclaves primarias: una para la capa de abstracción de hardware (Hardware Abstraction Layer, HAL) que se utiliza cuando se hace un seguimiento de los dispositivos que encuentra, otra para el administrador Plug-and-Play para registrar los dispositivos que sabe manejar y otra que refleja la cantidad de recursos del sistema (Microsoft-speak para la RAM) disponibles en la máquina.

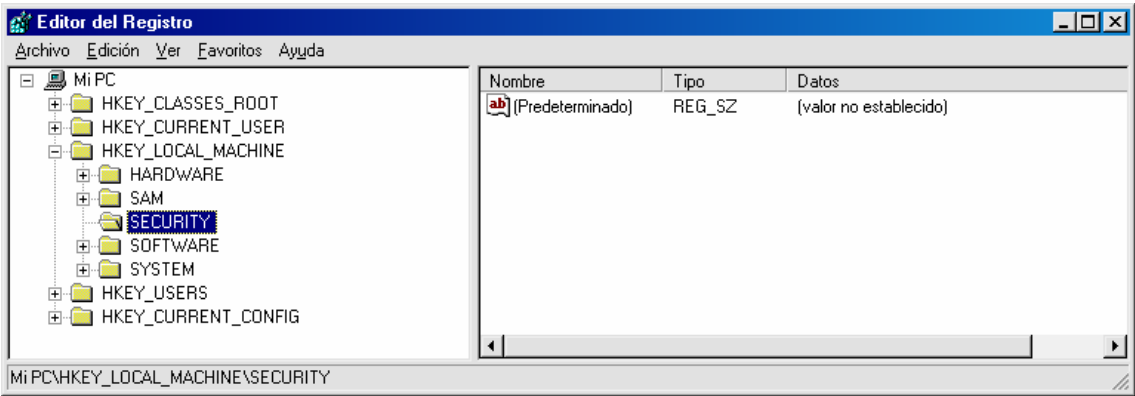
Dependiendo de la configuración de la máquina, es posible que existan otras subclaves adicionales. Por ejemplo, los sistemas que soportan Advanced Configuration Power Interface (ACPI) disponen de una subclave ACPI que contiene información sobre las subclaves ACPI concretas que la computadora soporta.

HKEY\_LOCAL\_MACHINE\SAM



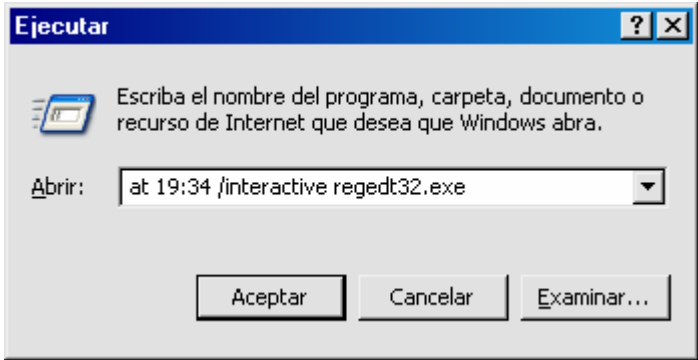
El hecho de que Windows 2000 incluya el servicio de directorio Active Directory no implica que no queden vestigios de Security Accounts Manager (SAM). Cuando se crean cuentas locales ó grupos en Windows 2000, éstos se almacenan en HKEY\_LOCAL\_MACHINE\SAM al igual que se hace en Windows NT. Sin embargo, aunque no es posible editar o visualizar la información de esta subclave, sí resulta muy útil para la compatibilidad con código de versiones antiguas de NT que da por hecho la existencia de SAM. Las rutinas de programación que acceden a la información de SAM se han reconstruido para que utilicen Active Directory cuando éste exista, o SAM si no existe un servidor Active Directory.

HKEY\_LOCAL\_MACHINE\SECURITY

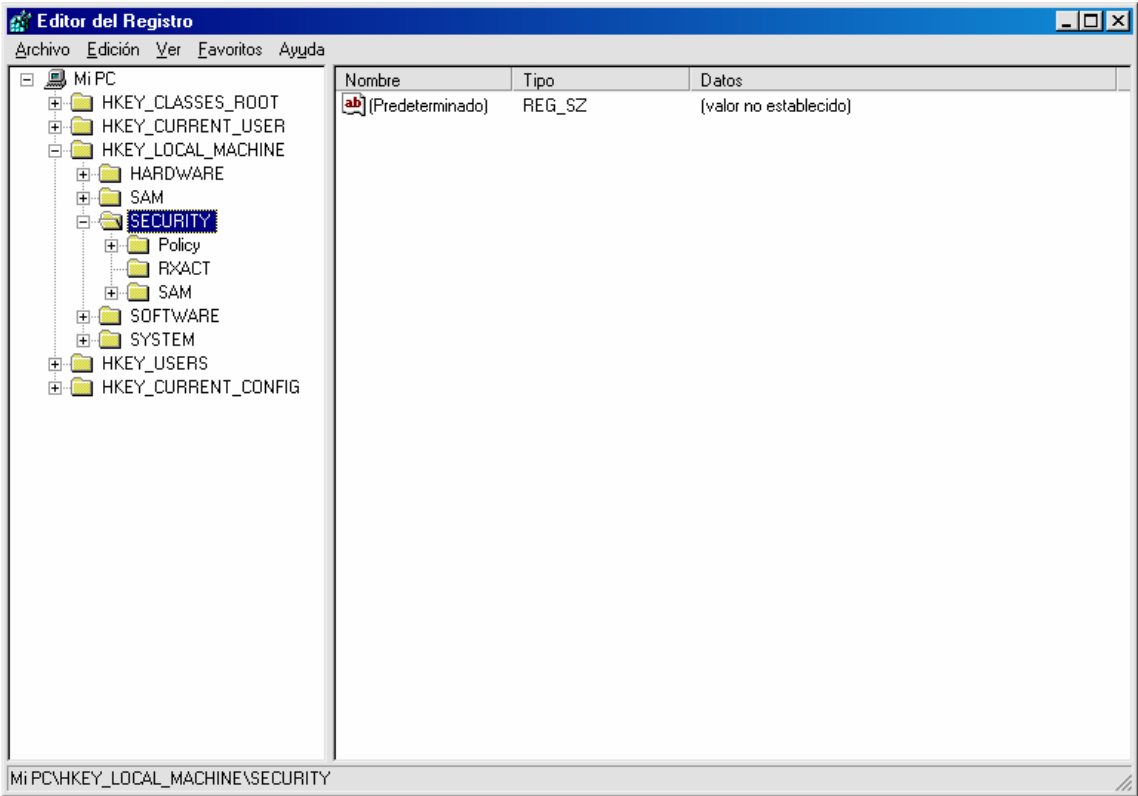


Tal y como uno espera, HKEY\_LOCAL\_MACHINE\SECURITY contiene gran cantidad de información sobre seguridad. Su formato no está documentado y no es posible realizar nada en la subclave. Sin embargo, las credenciales caché de inicio de sesión del sistema, las políticas de configuración y los secretos sobre servidores compartidos residen en esta subclave. La subclave SECURITY\SAM contiene una copia de casi toda la información de HKEY\_LOCAL\_MACHINE\SAM.

Si uno curiosidad por saber lo que hay en HKEY\_LOCAL\_MACHINE\SAM y HKEY\_LOCAL\_MACHINE\SECURITY, es posible abrir estas dos claves ejecutando Regedt32 en el contexto de seguridad LocalSystem. La forma más fácil de realizar esto es utilizando el comando "at" para programar que Regedt32 se ejecute en una sesión interactiva. Basta con programarlo para que se ejecute, aproximadamente, durante un minuto en el futuro de la siguiente forma: at 19:34 /interactive regedt32.exe

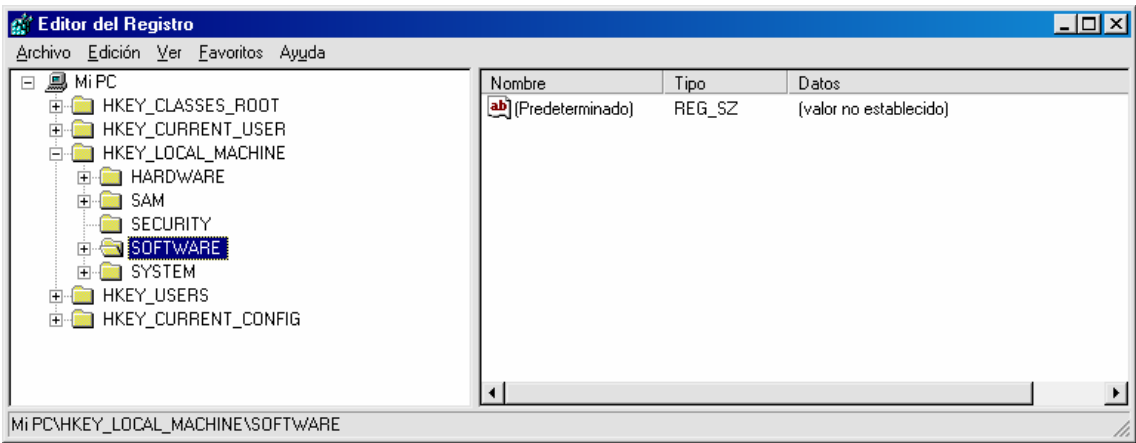


El comando advierte al sistema para que programe la ejecución de Regedt32 en un minuto a partir de ese momento (esto se escribe a las 19:33); cuando se ejecuta, el servicio de programación del sistema inicia la aplicación de forma que se ejecute en el contexto LocalSystem en lugar del contexto en el que uno tenga actualmente abierta la sesión.

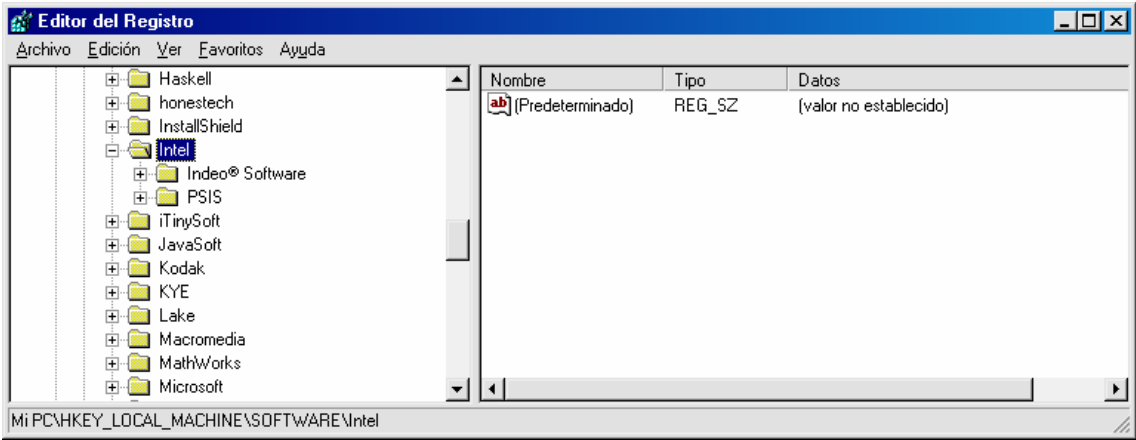


A pesar de que ésta es una forma interesante de ver lo que hay en estas subclaves, hay que estar prevenido de dos cosas. La primera es que los valores que se encuentran en estas subclaves no tendrán mucho sentido para el usuario, puesto que han sido intencionadamente ocultados. La segunda, y más importante, es que no hay que olvidar que el cambio de uno de estos valores provocará casi con toda seguridad consecuencias indeseables no intencionadas. En otras palabras, se mira, pero no se toca.

HKEY\_LOCAL\_MACHINE\SOFTWARE



La subclave HKEY\_LOCAL\_MACHINE\SOFTWARE se utiliza como ubicación raíz para el almacenamiento de las configuraciones generales de las aplicaciones y componentes del sistema. Por ejemplo, HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates contiene claves que almacenan las Listas de confianza de certificados (Certificate Trust List, CTL) y los certificados de confianza CCA de la máquina -los certificados CCA y CTL de usuarios particulares se almacenan en otro sitio-. Los programas individuales, los paneles de control y similares pueden crear sus propias subclaves bajo HKEY\_LOCAL\_MACHINE\SOFTWARE; el estándar predeterminado es que cada fabricante cree su propia clave en el nivel superior (por ejemplo, HKEY\_LOCAL\_MACHINE\SOFTWARE\Intel) para después crear subentradas por debajo de dicha clave.



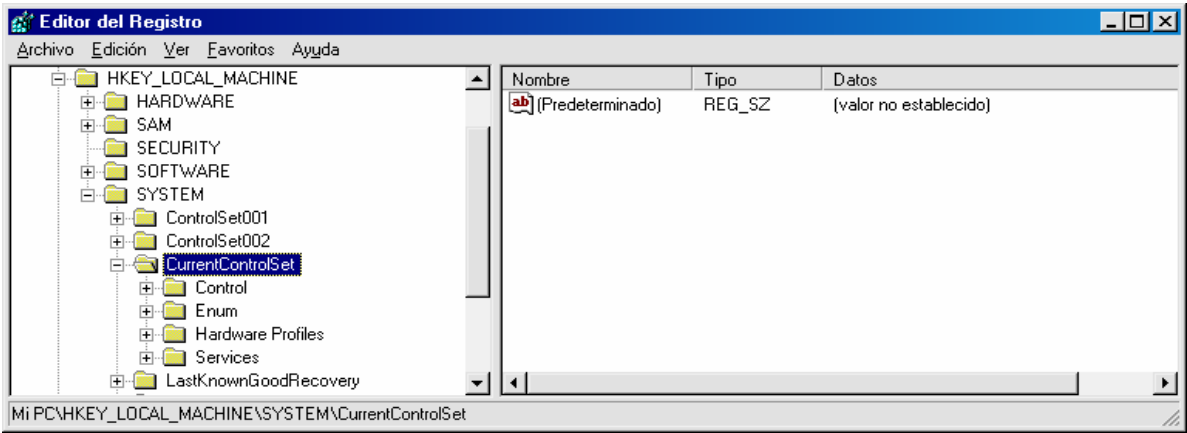
Las partes más interesantes de esta subclave son HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion (que almacena la mayor parte de la información preferente de la GUI; su nombre es el mismo que el de la correspondiente clave de Windows 95/98) y HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion. Esta última subclave se ha expandido considerablemente en Windows 2000; por ejemplo, existen nuevas claves para el manejo de la recuperación automática del servidor, el Sistema de archivos de cifrado, el Editor de configuración de seguridad, Terminal Services y otras nuevas características.

HKEY\_LOCAL\_MACHINE\SYSTEM

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet

Cuando se inicia Windows 2000, la última acción que se realiza en la fase de inicio es la actualización del Registro para que refleje el conjunto de controles y servicios que se usaron por última vez para iniciar la máquina con éxito. CurrentControlSet siempre apunta al conjunto de controles que se encuentra actualmente en uso en el sistema.

Si se mira en HKEY\_LOCAL\_MACHINE\SYSTEM, se observan principalmente claves del tipo ControlSetXXX. Cada subclave ControlSetXXX representa un conjunto de control que existió alguna vez, sin importar si se ha utilizado con éxito para iniciar la máquina. CurrentControlSet no es más que un puntero al conjunto de inicio con éxito más reciente, pero dado que no es fácil determinar qué conjunto era ése, el sistema operativo (SO) y las aplicaciones utilizan CurrentControlSet en su lugar.

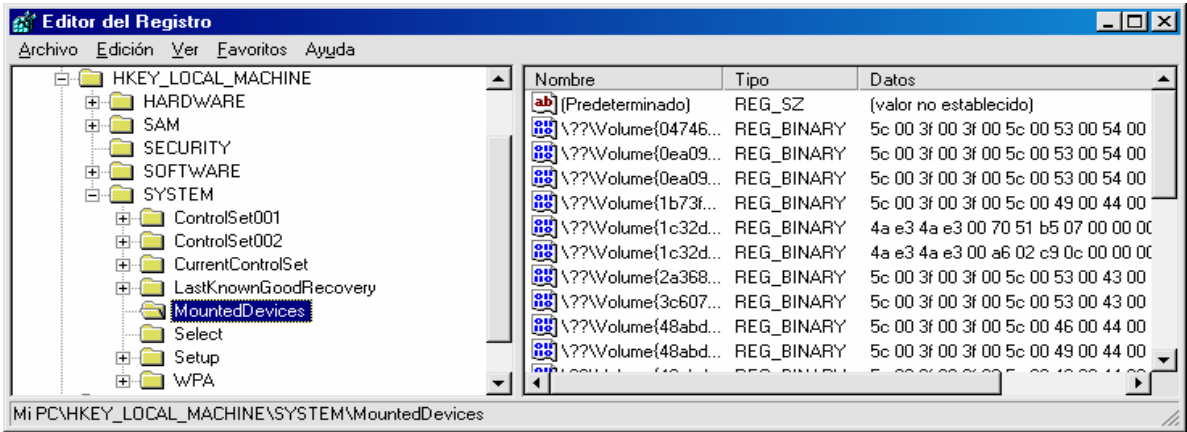


Por debajo de este conjunto existen cuatro claves que heredan sus nombres de versiones anteriores de Windows NT, si bien sus entresijos difieren bastante en comparación con Windows 2000:

- **Control:** Contiene información de control de servicios y herramientas del sistema. Por ejemplo, Control\BackupRestore\KeysNotToRestore contiene una lista de claves que la Copia de seguridad de Windows 2000 no debe restaurar (incluyendo los contenidos de la subclave Plug-and-Play) cuando recupera el Registro.
- **Enum:** Contiene una entrada para cada dispositivo o pseudodispositivo físico que detecta el sistema. Por ejemplo, Enum\USB\Vid 0461&Pid 4d03\Inst 0 contiene información sobre el ratón USB que se conecta en un portátil. Dado que se encuentra presente durante el tiempo de inicio, se incluye en la lista de enumeración.
- **Hardware Profiles:** Contiene una entrada para cada perfil hardware definido en la máquina. Al igual que HKEY\_LOCAL\_MACHINE\SYSTEM, cada perfil tiene un número de serie, comenzando siempre con 0001. HKEY\_LOCAL\_MACHINE\SYSTEM\Hardware Profiles\Current siempre apunta al perfil que se selecciona durante el tiempo de inicio.
- **Services:** Contiene una subclave para cada servicio instalado. De hecho, estas subclaves guardan toda la información de configuración que un servicio necesita. El conjunto exacto de claves de dos máquinas será diferente si éstas tienen diferentes servicios cargados.

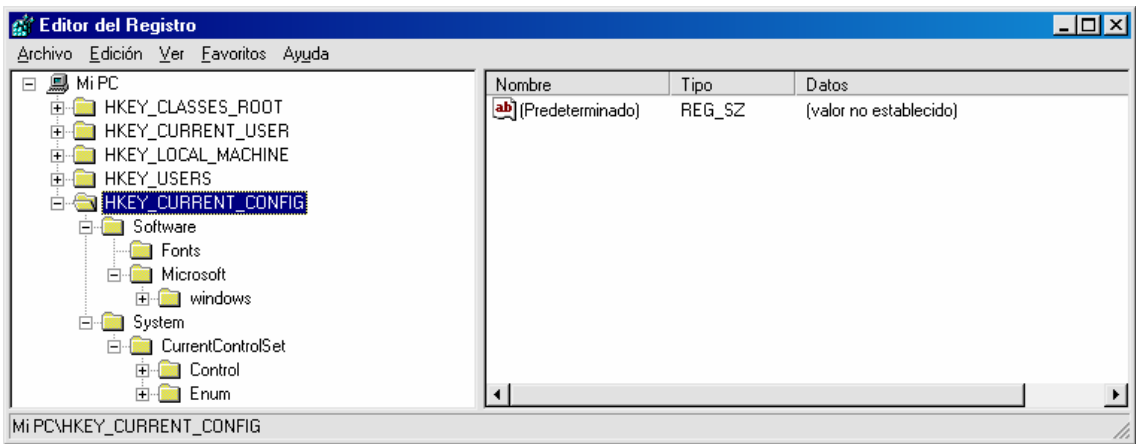
HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices

Los volúmenes de discos dinámicos de Windows 2000 son un gran logro técnico y un regalo para los administradores, pero su funcionamiento se basa en tener una configuración actual de los volúmenes lógicos en disco. Las aplicaciones (y complementos, como el complemento de Administración de archivos) toman esta información del servicio de Administración de volúmenes lógicos; de hecho, este servicio almacena su lista de dispositivos montados y disponibles en la subclave MountedDevices.



1.4.1.4. La sección Current Configuration

La sección Current Configuration, que aparece como HKEY\_CURRENT\_CONFIG se utiliza para contener información fugaz acerca de la configuración de la maquina local. Esto incluye información de la configuración PCI, información de la configuración PCMIA, las opciones acerca de la resolución de video actual, etc. Esta información se descarta cuando se cierra el sistema y cambiara conforme se ejecuten distintas aplicaciones.



2. Como utilizan las aplicación el registro

Microsoft ha puesto el Registro a disposición de las aplicaciones para que esas aplicaciones puedan guardar las opciones de configuración genéricas de la maquina y las que establecen los usuario de forma independiente unos de otros. De este modo, los distintos usuarios pueden modificar las opciones de configuración del sistema operativo (SO), como por ejemplo, los esquemas de fondo y color, sin que afecte a los demás usuarios. Así, al usuario que le guste que su pantalla este en azul sobre blanco, no le afectara la configuración de otro usuario que piensa que lo mejor es el tradicional negro sobre blanco. Los colores de pantalla pueden parecer algo trivial, pero hay que pensar que pasa con, los usuarios que cambian el aspecto de las aplicaciones, configuran macros especificas para ciertas claves, etc. Estos tipos de cambios mejoran la productividad y pueden ser muy importantes.

Cuando una aplicación se instala, hará cambios en distintas partes del Registro que inicializa la aplicación. La mayor parte de las aplicaciones instalan sus extensiones en HKEY\_CLASSES, y a continuación, configuran las opciones de usuario básicas y la información de ubicación de ventana en HKEY\_CURRENT\_USER.

Para los servicios, como, por ejemplo Microsoft SQL Server la información se guarda en todo el Registro. Las herramientas de cliente registran sus extensiones, y los componentes de servidor, crearan entradas en HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Services para controlar el inicio del servicio y HKEY\_LOCAL\_MACHINES/SOFTWARE/Microsoft/MSSQLServer para el propio software. Una vez que se inicia el servicio con la información que contiene la clave Services, la aplicación lee la información desde la clave Software para completar su inicio. Esto es bastante típico del software de servicio.

Algunas aplicaciones utilizan todavía los archivos INI para almacenar opciones de configuración. Un archivo INI es un archivo almacenado en el disco en formato de solo texto; normalmente en el directorio WINNT. Cada archivo contiene las opciones de configuración de una aplicación y el formato y uso del archivo INI queda totalmente a elección del programador.

Cuando un usuario inicia una sesión en un sistema Windows 2000, puede tener programas que se inician automáticamente. Existen distintas formas de iniciar las aplicaciones durante el inicio de sesión; una de ellas es escribir las rutas de acceso ejecutables de las aplicaciones dentro de un valor en HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Run (ó RunOnce). El usuario también puede colocar aplicaciones dentro del grupo Inicio en el menú inicio. El método mas insidioso, y el que utilizan mas a menudo los virus que necesitan iniciarse automáticamente, es poner una entrada en WIN.INI llamada RUN. Esto ejecutará el programa y puede ser muy difícil deshacerlo. Para averiguarlo, simplemente abra el archivo WIN.INI con el bloc de notas. Lo puede encontrar en el directorio del sistema, normalmente en C:\WINNT.

2.1. Editores del registro

Cuando se necesite cambiar algún valor en el Registro, habrá que utilizar algún tipo de editor del Registro. Muchos de los parámetros que se cambian en los paneles de control, objetos de Políticas de grupo o complementos MMC se guardan realmente en el Registro, por eso estas utilidades pueden verse como un tipo de editor del Registro. Otro tipo es un script, escrito a medida que se utiliza para hacer un cambio específico, quizás como una parte del script de inicio ó un archivo que se distribuye a los usuarios. Sin embargo, la mayor parte de las veces que se quiera realizar un cambio directamente en el Registro, se utilizará una de las dos herramientas que Microsoft incluye con Windows 2000: Regedt32.exe o Regedit.exe.

Si se preguntan ¿por qué hay dos editores del Registro en Windows 2000? Es debido a Windows NT 4. Las distribuciones de Windows NT 3.1, 3.5 y 3.51 incluían un editor del Registro denominado Regedt32. Esta herramienta se construyó para manipular las claves y valores del Registro de Windows NT y refleja los estándares para el diseño de interfaces de Microsoft de la época en la que fueron escritos (aproximadamente en el año 1992).

Cuando se desarrollaba Windows 95, Microsoft se percató de que Regedt32 no era una apuesta acertada para la interfaz de Windows 95 o para las diferencias estructurales subyacentes entre los registros de los dos sistemas. Dado que Windows 95 necesitaba un editor del Registro también, Microsoft desarrolló una herramienta de acompañamiento, Regedit, y la distribuyó con Windows 95.

Microsoft tomó la decisión de incluir ambos editores (Regedt32 y Regedit) en Windows NT 4. A pesar de que esto pudiera parecer innecesariamente redundante, es realmente una ventaja, dado que los dos programas poseen habilidades distintas que se complementan. Microsoft continuó distribuyendo ambas herramientas como parte de Windows 2000; exceptuando algunos pequeños detalles -relacionados con la interface, y el arreglo de algunos fallos- las versiones de Windows 2000 son idénticas a sus predecesoras.

### Regedit y Regedt32

Con dos editores donde poder elegir, ¿cómo saber cuál utilizar en una determinada circunstancia? Ambas herramientas poseen las mismas capacidades fundamentales. Ellos permiten:

- Explorar una estructura gráfica que representa la jerarquía del Registro.
- Visualizar y modificar claves, subclaves, valores y entradas, dependiendo siempre de los privilegios de seguridad que se tengan.
- Conectarse a una computadora remota para la que se tienen privilegios a inspeccionar, o incluso cambiar, las entradas de su Registro.

Sin embargo, sí hay algunas diferencias significativas que se enmarcan en la existencia de ciertas funcionalidades en un editor pero no en el otro. Comencemos con Regedt32; dado que se diseñó específicamente para Windows NT, presenta algunas funcionalidades muy útiles que se han extendido a Windows 2000:

- Permite la visualización y el cambio de ACL de seguridad en las claves del Registro.
- Permite activar la auditoria en las claves de tal forma que uno pueda averiguar quién ha intentado -o ha conseguido- eliminar, añadir o editar las claves o sus entradas.
- Soporta todos los tipos de datos de registro descritos anteriormente en el capítulo; es más, permite editar el valor de un tipo utilizando otro editor de tipos (muy útil cuando se editan valores REG\_BINARY).
- Posee un modo de sólo lectura que permite inspeccionar el Registro sin realizar cambios.
- Puede cargar o guardar archivos de sección o claves individuales.
- Utiliza el paradigma de la interfaz de documentos múltiples (Multiple Document Interface, MDI), en el que cada clave raíz tiene su propia ventana.

En cambio, está Regedit, que fue diseñado para hacer uso de la interfaz del estilo Windows 95, por lo que se diferencia un poco de Regedt32. También posee una funcionalidad diferente:

- Para una cadena específica, busca claves, nombres de valores y entradas. Esta funcionalidad no tiene precio y es la primera razón para utilizar Regedit.
- Utiliza el familiar interfaz de dos paneles del Explorador de Windows, facilitando la comparación de las ubicaciones de dos claves o valores. También incluye otras características típicas del Explorador de Windows, como menús contextuales, edición in situ y el también familiar control en árbol.
- Importa y exporta claves seleccionadas (y sus elementos subordinados) en un archivo de texto legible para los humanos, en lugar de importar y exportar las claves del Registro en un formato binario.
- Incluye un menú de favoritos (en la versión de Windows 2000), al que se pueden añadir las claves que se editen repetidamente.

¿Cómo saber qué herramienta utilizar? La mayor parte de las veces las preferencias personales de cada uno dictarán la elección. A algunas personas les gusta la forma en que trabaja Regedit, mientras que otras prefieren la interfaz de la vieja escuela de Regedt32.

Por ejemplo, si se busca la clave que contiene un determinado valor, es mejor utilizar Regedit; por otra parte, si lo que se pretende es asignar permisos de seguridad a una clave, se tendrá que utilizar Regedt32.



## 2.2. Cuando utilizar las herramientas de modificación del Registro

Para modificar el Registro, Microsoft recomienda seguir únicamente los pasos indicados en su propia documentación. Si es posible, utilice la interfaz de usuario de Windows en vez de modificar el Registro directamente. También advierte constantemente de que la edición del Registro es peligrosa. Dado que el Registro se utiliza por casi cualquier parte de Windows 2000, y dado también que los programadores no suelen tomar todos los recaudos necesarios —a la hora de escribir código que compruebe los valores que provienen del Registro— cualquier cambio inadecuado o poco contrastado que se haga al Registro, puede provocar un gran daño a la máquina. Dicho esto, sin embargo, si se tiene cuidado y se presta atención, no hay razón alguna para temer al Registro.

Algunas reglas simples que nos ayudan a evitar problemas:

- No editar ninguna parte del Registro por diversión. Si no se sabe cómo puede afectar al sistema un cambio puntual, es mejor no hacerlo a menos que uno sepa cargar con las consecuencias.
- Hay que ser cuidadoso a la hora de añadir nuevos valores o claves. El software sólo prestará atención a las claves que contengan nombres que pueda comprender. La excepción a esta regla es que Microsoft utiliza a menudo código capaz de reconocer claves ocultas (o al menos poco documentadas) y cambiar su comportamiento apropiadamente.
- Mantener una copia de seguridad actual del estado del sistema.

## 3. Almacenamiento de datos

A pesar de que los programas y servicios que utilizan el Registro no tienen por qué comprender cómo se almacena la información del Registro, los administradores sí deben saberlo —de esta forma es posible saber dónde se almacenan los datos, cómo utiliza el Registro los diferentes tipos de datos, así como qué archivos deben ser salvaguardados como parte de las copias de seguridad—. No es necesario conocer los formatos internos que utilizan las herramientas del Registro, pero sí los tipos de datos básicos y las ubicaciones de almacenamiento. Cada valor del Registro tiene tres partes: un nombre, un tipo de datos y un valor actual.

### 3.1. Tipos de datos útiles

Para almacenar datos en el Registro, es posible utilizar siete tipos de datos. Aunque realmente sólo se suelen utilizar dos tipos para almacenar la mayor parte de la información del Registro: REG\_DWORD y REG\_SZ; los siete tipos son:

- REG\_BINARY almacena datos binarios arbitrarios en un formato no procesado, sin ningún tipo de reformato o análisis. Es posible ver los datos binarios en formato binario o hexadecimal utilizando uno de los editores del Registro de Windows 2000.
- REG\_DWORD guarda un valor de entero largo de 8 bits (o palabra doble). Este tipo se utiliza normalmente cuando una entrada indica una cuenta o intervalo, aunque también es común ver indicadores REG\_DWORD (0 significa que el indicador está desactivado y 1 que está activado).
- REG\_SZ es una cadena ordinaria de tipo Unicode. Estas cadenas pueden tener cualquier longitud; este tipo se utiliza normalmente para guardar caminos, mensajes legibles para los humanos, nombres de dispositivos, etc.
- REG\_EXPAND\_SZ es un REG\_SZ con una variación —las aplicaciones pueden contener caracteres especiales en la cadena y después traducir esos caracteres cuando se lee el valor desde el Registro—. Por ejemplo, "Algo" es un REG\_EXPAND\_SZ cuyo valor normal es %SystemRoot%\System32\Algo. Cuando Windows 2000 lee la cadena, expande %SystemRoot% al camino completo donde está instalado el sistema operativo.
- REG\_MULTI\_SZ es una colección de un número arbitrario de valores REG\_SZ. Por ejemplo, la lista de servidores DNS especificados en el cuadro de diálogo Propiedades TCP/IP se almacena en un valor REG\_MULTI\_SZ. Las aplicaciones deben saber cómo dividir un único REG\_MULTI\_SZ en sus partes correspondientes.
- REG\_FULL\_RESOURCE\_DESCRIPTOR es un tipo raro; se utiliza para codificar información sobre los recursos de sistema requeridos por un dispositivo concreto. Nunca lo hemos visto aparecer fuera de las subclaves de HKEY\_LOCAL\_MACHINE\HARDWARE.
- REG\_NONE es sólo un contenedor. Se utiliza para indicar la existencia de un valor de registro que actualmente no contenga ninguna información. Algunos componentes comprueban la presencia o ausencia de una clave o valor específico para controlar su funcionamiento en tiempo de ejecución; es normal que estos componentes busquen un elemento de tipo REG\_NONE; dado que este tipo no contiene ninguna información, es posible que los usuarios jueguen con estos valores.

En la administración rutinaria, bastará con saber la diferencia existente entre los valores REG\_DWORD y REG\_SZ. Un valor REG\_DWORD cuyo contenido sea 0 (el valor numérico 0) es distinto de un valor REG\_SZ cuyo contenido sea «0» (el carácter "0"). Si es necesario añadir un nuevo valor de Registro, habrá que asegurarse de utilizar el tipo correcto si no se quiere tener problemas con los componentes que utilicen dicho valor.

3.2. Claves volátiles

Algunas claves y valores de registro son volátiles en el sentido original de la palabra, es decir, no son persistentes. Como ejemplo, ninguna de la información en HKEY\_LOCAL\_MACHINE\HARDWARE existe en ninguna parte del disco; la subclave completa y todos sus contenidos residen completamente en memoria. Cada vez que se inicia una máquina con Windows 2000 se crea una nueva subclave, y cuando se cierra el sistema sus contenidos desaparecen.

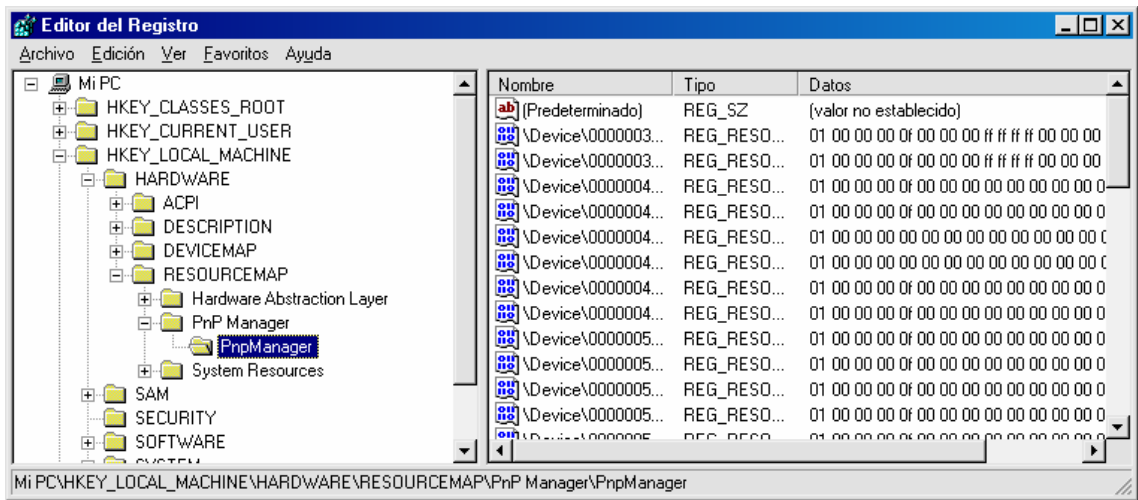
3.3. Claves basadas en disco

Las claves volátiles son útiles para guardar la información que no necesita permanecer entre los distintos reinicios de la máquina, pero la mayor parte de los datos almacenados en el Registro no servirían de mucho si no fueran persistentes. Basta con imaginarse el tener que reconfigurar todas las preferencias y configuraciones siempre que se reinicia la máquina, lo que la haría caducar pronto. La mayor parte de las claves de registro están basadas en disco, lo cual significa que sus contenidos se guardan en las estructuras del disco. Siempre que se actualiza el contenido de alguna clave, la versión de disco hace lo propio.

A pesar de que las claves basadas en disco se guardan eventualmente en el disco, Windows 2000 las hace corresponder con un conjunto de memoria paginado (un área de la memoria cuyos contenidos pueden escribirse al archivo de página cuando éste no se esté usando) para conseguir un acceso más eficiente. El límite de tamaño del Registro, regula la cantidad de información que puede almacenarse en el conjunto paginado.

4. Como utilizar REGEDIT

El programa REGEDIT.EXE, es el programa de modificación del Registro de Windows. Tiene una interfaz de usuario muy amigable (similar a la del Explorador de Windows).



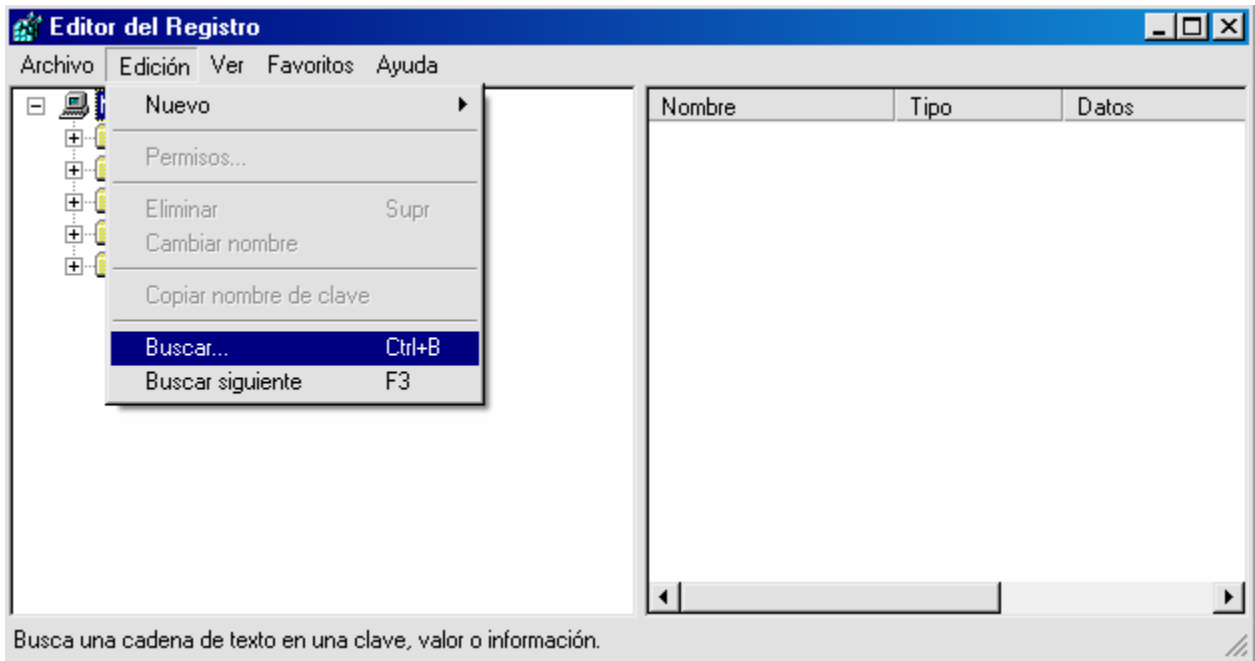
Las partes importantes de la interfaz son claramente fáciles de entender. Resaltaremos las siguientes características:

- El árbol en el panel izquierdo de la ventana Editor del Registro muestra todas las claves y subclaves raíz; lo que aquí se visualiza depende de las claves y subclaves que se hayan expandido.
- El panel derecho muestra los valores asociados a la clave seleccionada en el panel izquierdo. Cada valor se muestra con tres elementos: el nombre del valor (el nombre -Predeterminado- se usa para el valor predeterminado sin nombrar qué tiene cada clave), el tipo del valor y las entradas o información del valor.
- La barra de estado en la parte inferior de la ventana muestra el camino completo de la clave que se encuentre actualmente seleccionada (Regedit puede también copiar el camino de la clave al portapapeles utilizando el comando Copiar nombre de clave en el menú Edición).

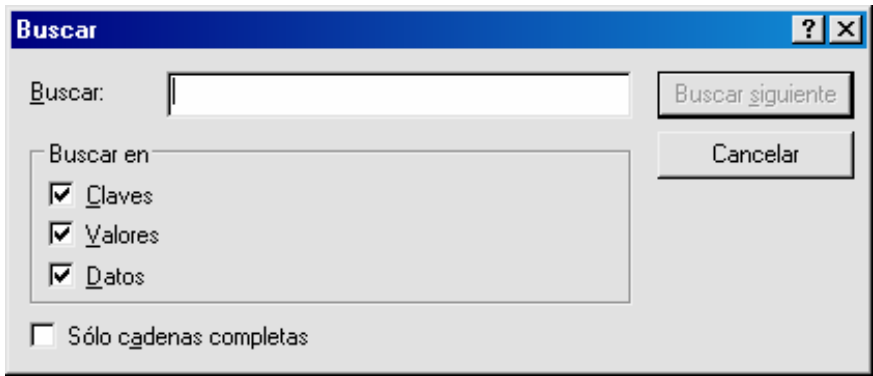
Dado que estas características de interfaz están escritas con los controles estándar de Windows, toda la navegación con el teclado y la combinación de teclas de control que uno está acostumbrado a utilizar en el Explorador de Windows funcionan aquí también. Por ejemplo, es posible saltar a una clave particular pulsando en algún sitio del panel izquierdo y escribiendo las primeras letras del nombre de la clave. Y también se pueden utilizar los cursores para moverse por cualquier panel de la ventana Regedit.

4.1. Búsqueda de claves y valores

El comando Buscar, en el menú Edición en Regedit, se utiliza cuando se necesita buscar qué clave o valor tiene un nombre o entrada específica. La interfaz de esta función es muy sencilla; a pesar de esto, esta herramienta es extremadamente útil, dado a que permite buscar un valor determinado por todo el Registro. La forma de conseguir lo que uno busca a través del cuadro de diálogo Buscar es la siguiente:



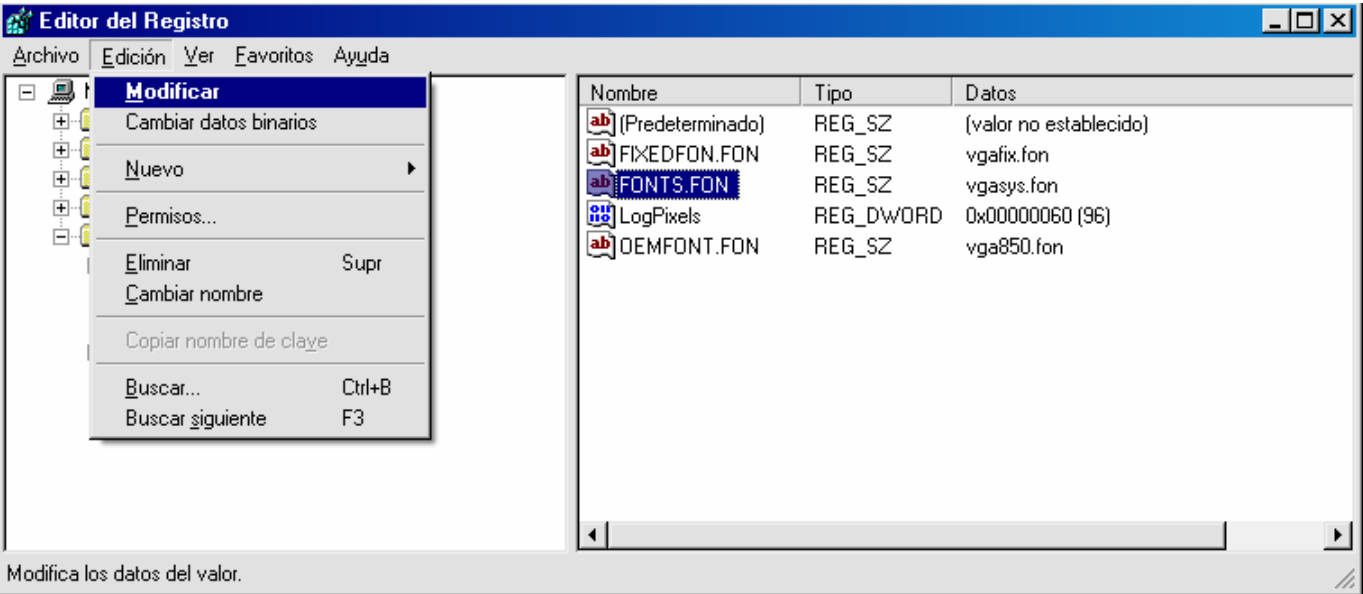
- Escribir el patrón de lo que se quiere buscar en el cuadro Buscar. Sólo se puede buscar texto ASCII sin formato -los comodines no están permitidos-. Si lo que se busca son valores, Regedit examina sólo los valores de cadena (REG\_SZ, REG\_EXPAND\_SZ y REG\_MULTI\_SZ) para buscar el patrón deseado.
- Utilizar las opciones del cuadro Buscar en para controlar los sitios en los que Regedit busca el valor especificado. De manera predeterminada se busca en los nombres de las claves (casilla Claves), los nombres de valor (casilla Valores) y las entradas de valor (casilla Datos), pero esto se puede configurar.
- La casilla de Sólo cadenas completas indica a Regedit que encuentre la cadena de búsqueda completa, no sólo una porción de ella. Por ejemplo, si se hace una búsqueda de «Windows» con esta casilla seleccionada, en la búsqueda se ignorará HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT.



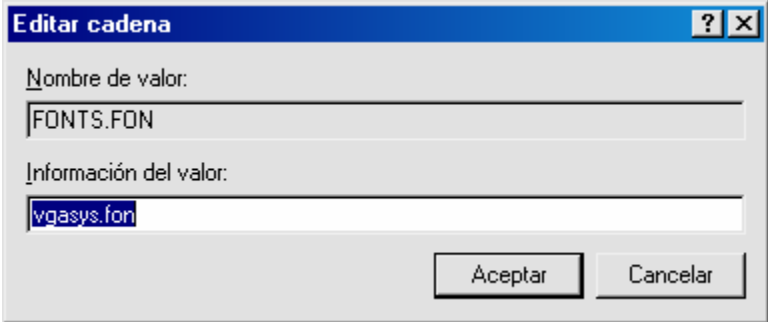
Cuando se hayan realizado las selecciones en el cuadro de diálogo Buscar, hay que presionar Buscar siguiente para que Regedit comience la búsqueda. Eventualmente ocurrirá alguna de estas dos cosas: o bien Regedit alcanzará el final del Registro (en cuyo caso comunicará que no se encontró ninguna coincidencia), o bien encontrará una coincidencia. En el último caso, se resaltará dicha coincidencia; si la coincidencia no es exactamente lo que se andaba buscando, el comando Buscar siguiente en el menú Edición (ó la tecla F3) continuará la búsqueda.

Cada vez que se realiza una búsqueda, Regedit comienza al principio de HKEY\_CLASSES\_ROOT y se abre camino hasta el final de HKEY\_CURRENT\_CONFIG. No es posible cambiar este orden de búsqueda, por lo que es mejor acostumbrarse a él.

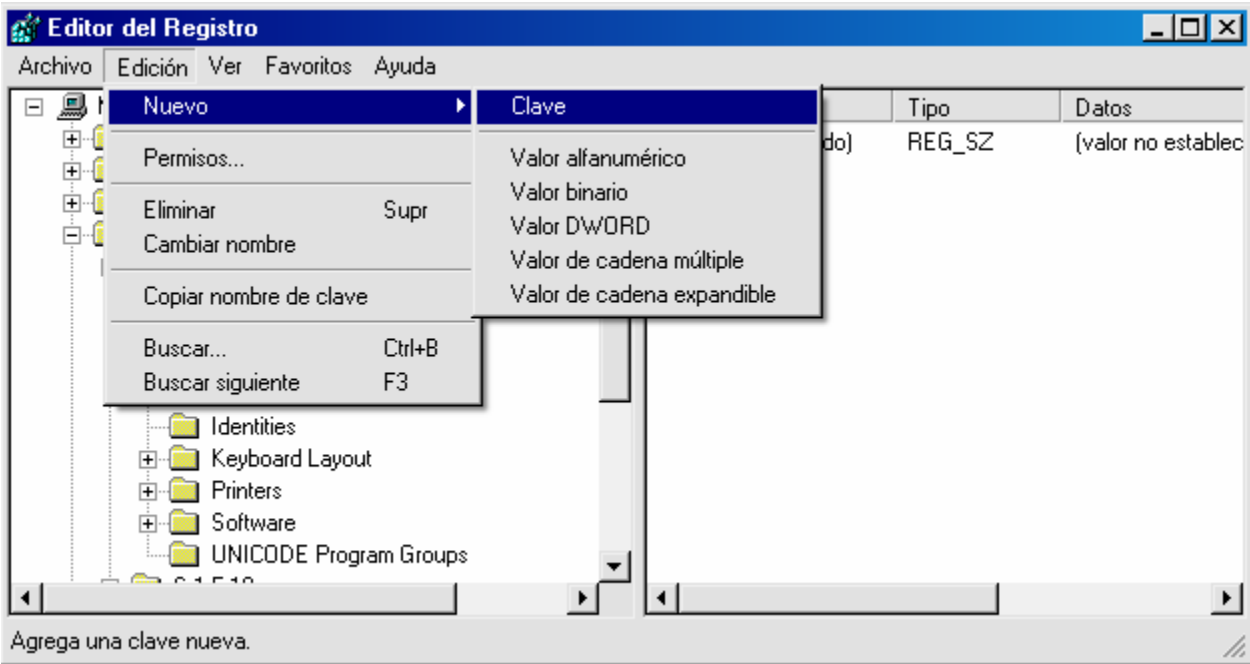
4.2. Edición de las entradas de valor



El comando Modificar del menú Edición permite cambiar los contenidos de la entrada de valor seleccionada (también es posible editar un valor seleccionándolo y presionando INTRO –ENTER–). Lo que se ve después depende del tipo de valor que se esté editando; existen cuadros de diálogo de edición diferentes para los valores de cadena, los valores DWORD y los valores binarios. Regedit permite la edición de tipos de datos que no soporta, como por ejemplo, REG\_FULL\_RESOURCE\_DESCRIPTOR o REG\_MULTI\_SZ; para estos tipos, Regedit abre el cuadro de diálogo del editor binario. Los cuadros de diálogo de edición son directos, esto es, cada uno presenta el valor actual y permite su edición. Las combinaciones de teclas para los comandos Cortar, Copiar y Pegar también funcionan en los cuadros de diálogo de edición.

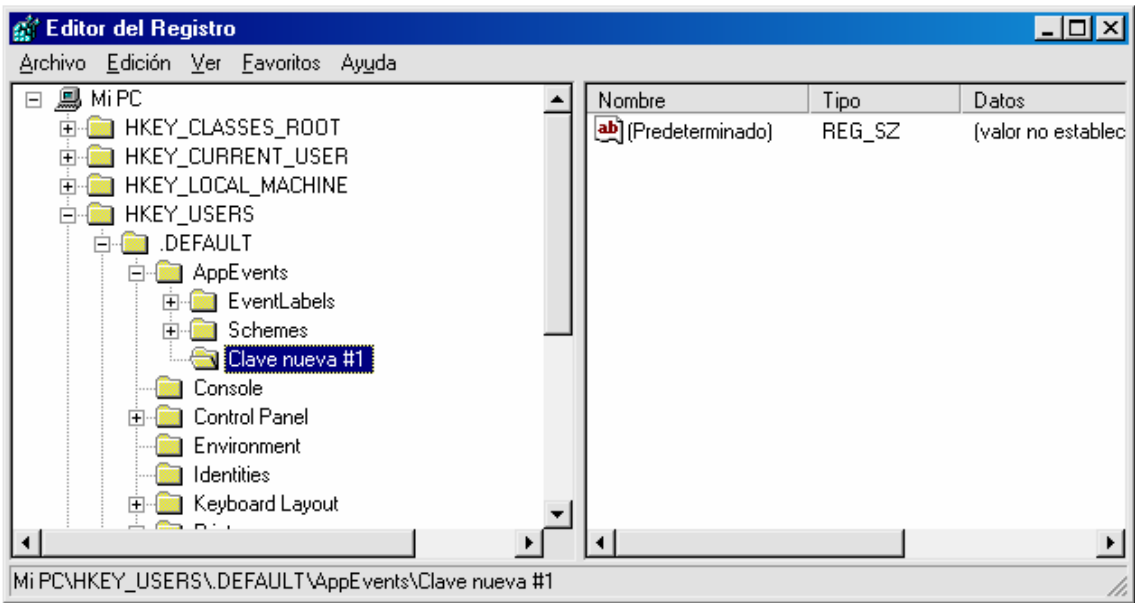


4.3. Adición y eliminación de claves y valores

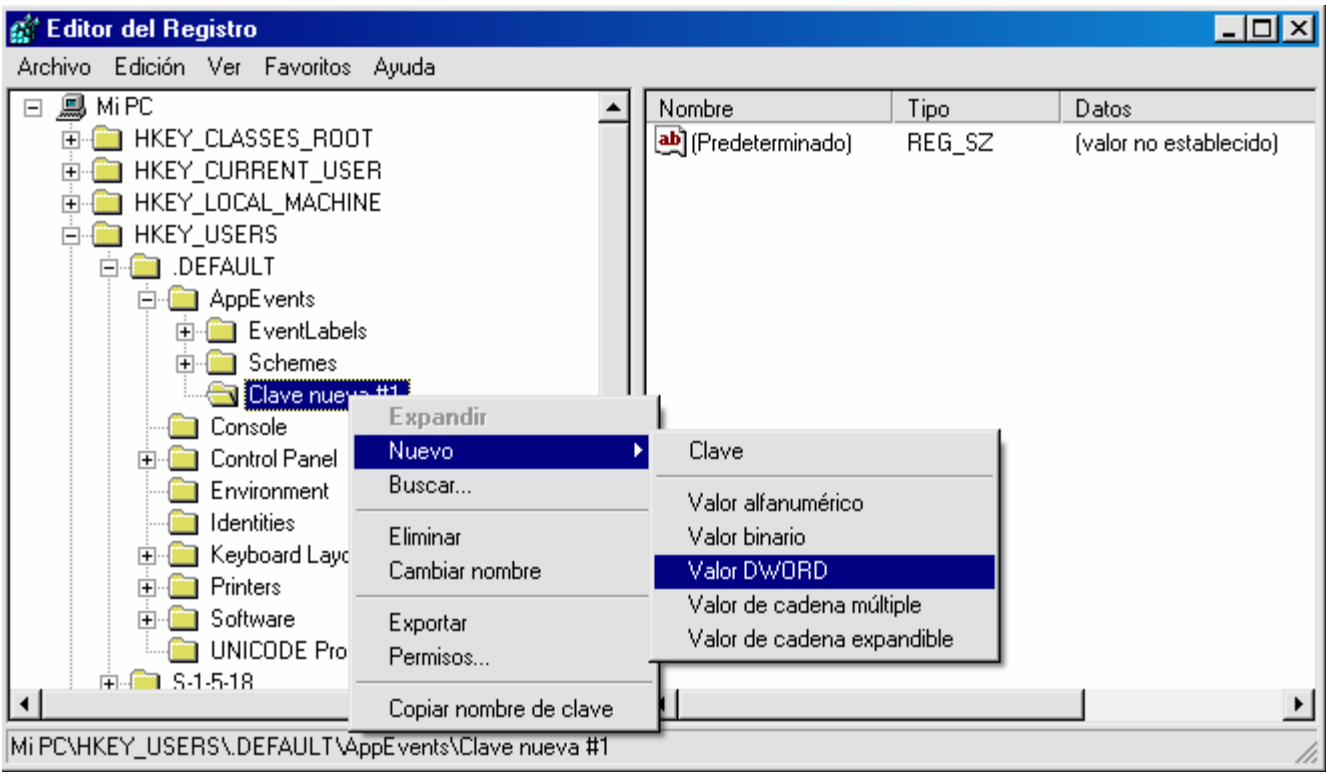


Regedit permite también la adición y eliminación de claves, subclaves y valores individuales. Ahora es un buen momento para reiterar el frecuente aviso de Microsoft: “La realización de cambios innecesarios en el Registro puede dañar de manera considerable el sistema operativo de la computadora”. Hay que ser cuidadoso a la hora de añadir información y doblemente cuidadoso a la hora de eliminarla.

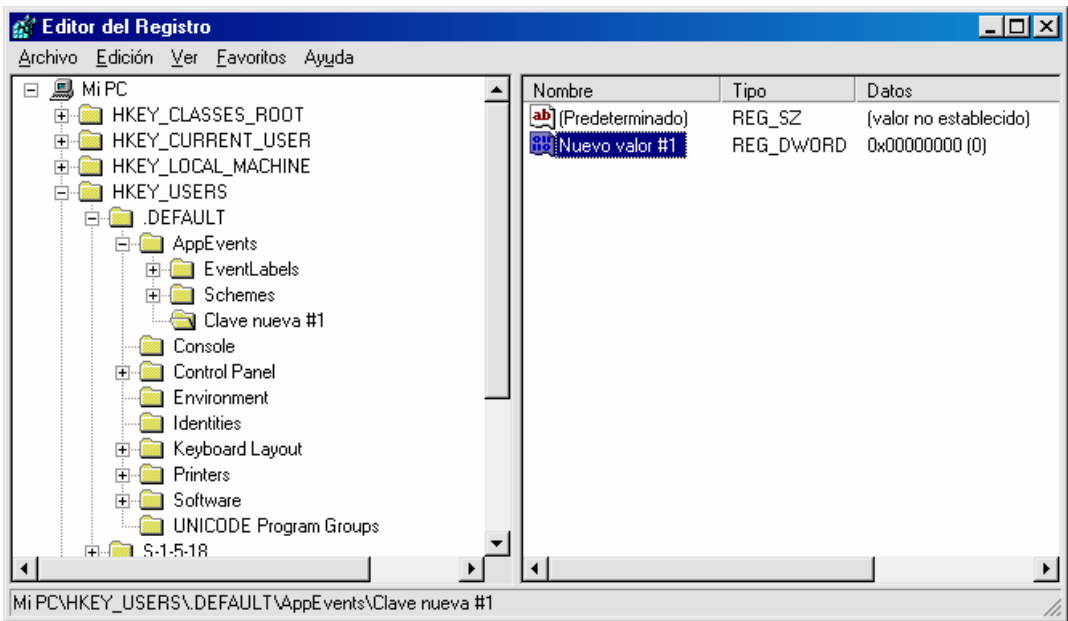
Para agregar una nueva clave como hijo de una clave seleccionada, hay que abrir el menú Edición, apuntar a Nuevo y elegir Clave. Regedit creará una nueva clave y seleccionará su nombre para que se pueda configurar correctamente (el valor predeterminado es Clave nueva #1).



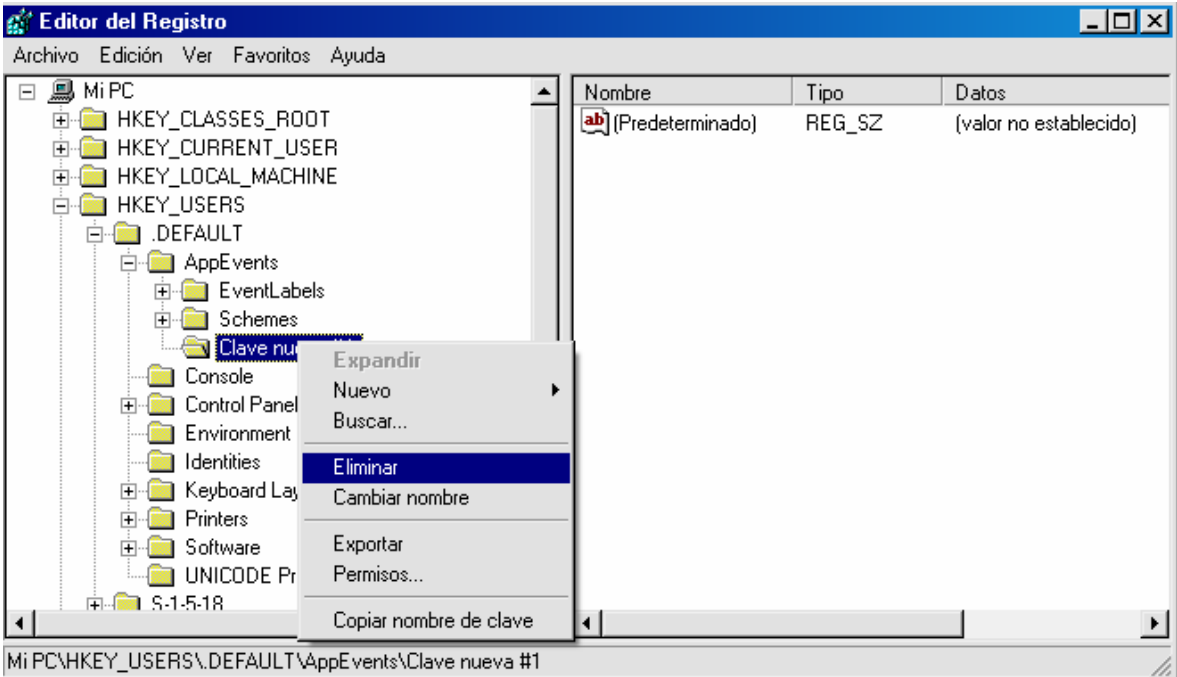
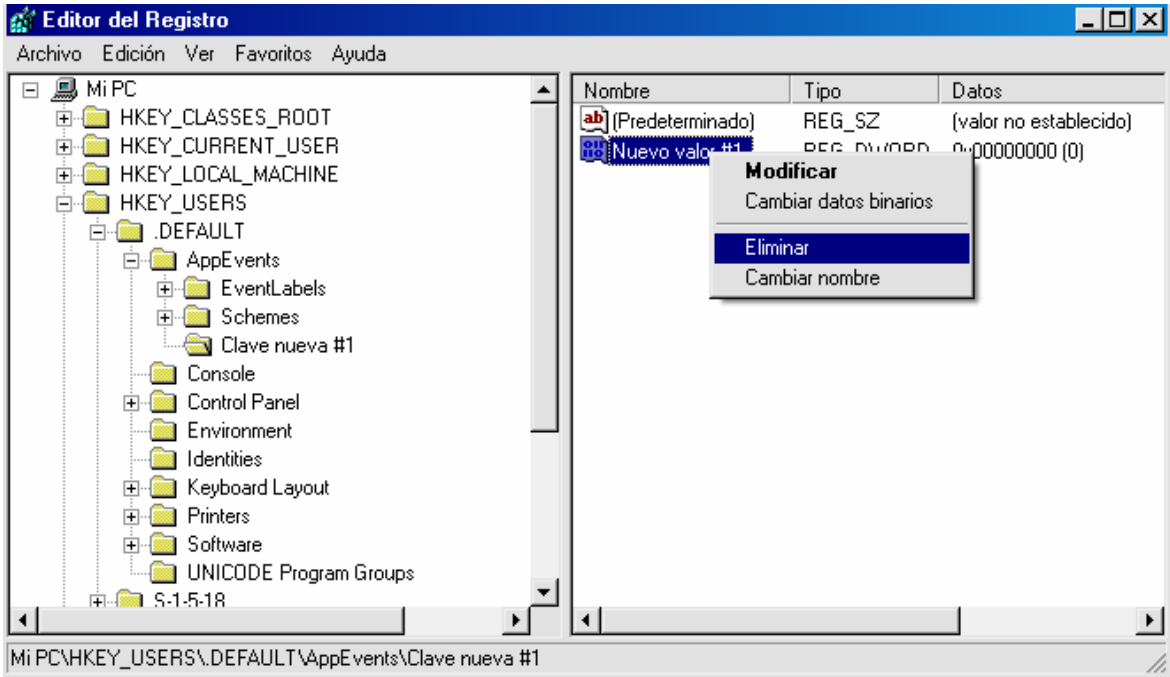
La nueva clave tendrá automáticamente un valor asociado no establecido. Es posible añadir nuevos valores utilizando alguno de los tres comandos restantes en el submenú Nuevo: valor alfanumérico, valor binario y valor DWORD. No hay que olvidar que Regedit no puede crear ningún otro tipo de datos, y si se crea un valor binario, los componentes lo interpretarán como un dato no procesado de tipo REG\_BINARY.



Cuando se crea un nuevo valor, éste se añade como un hijo de la clave seleccionada y se le asigna un nombre predeterminado (Valor nuevo #1, Valor nuevo #2, etc.), el cual puede ser inmediatamente cambiado. Una vez que se ha terminado de añadir y nombrar los nuevos valores, se pueden utilizar los cuadros de diálogo de edición estándar para cambiar sus contenidos por los valores apropiados.

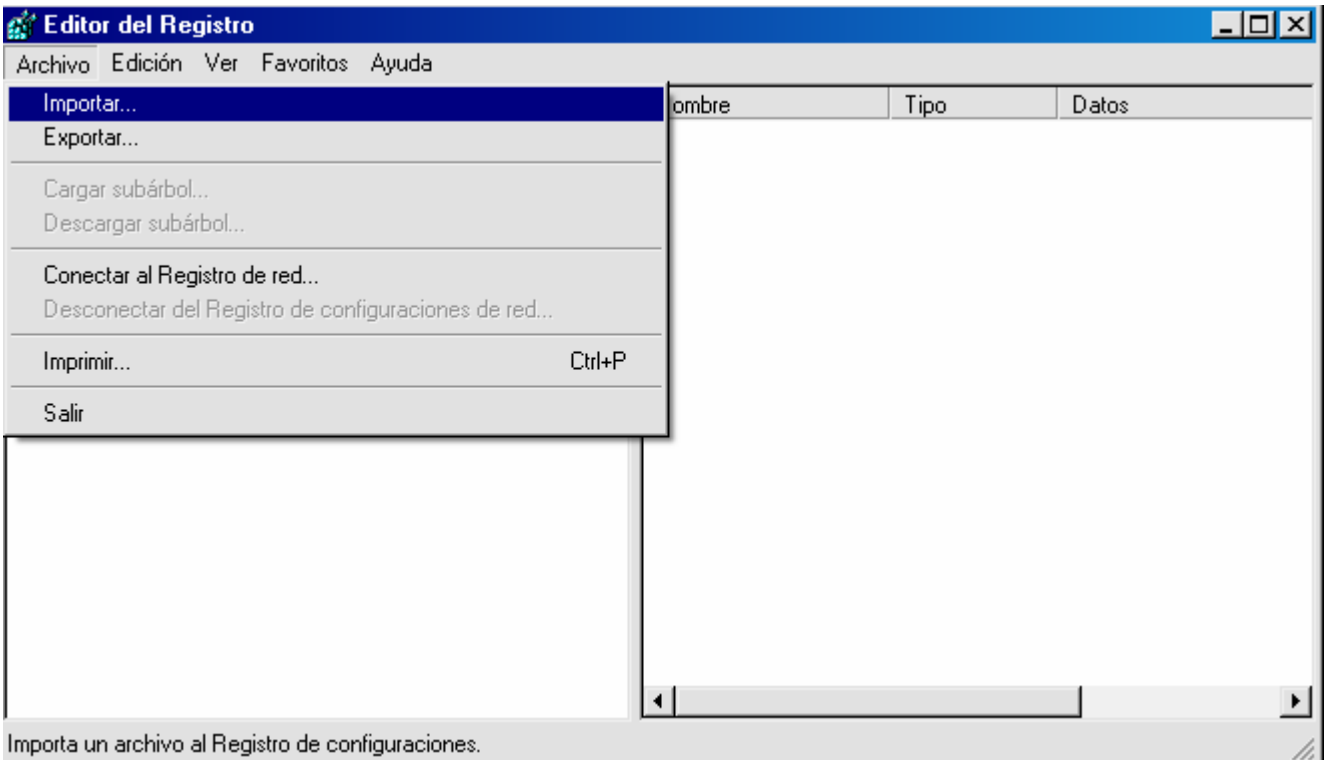


La eliminación de valores y claves es sencilla. Basta con seleccionar el objeto que se desea eliminar y seleccionar Eliminar en el menú Edición o simplemente pulsar la tecla SUPR. Regedit pedirá entonces una confirmación para ejecutar el comando; una vez confirmada, la clave o valor se eliminará inmediatamente.



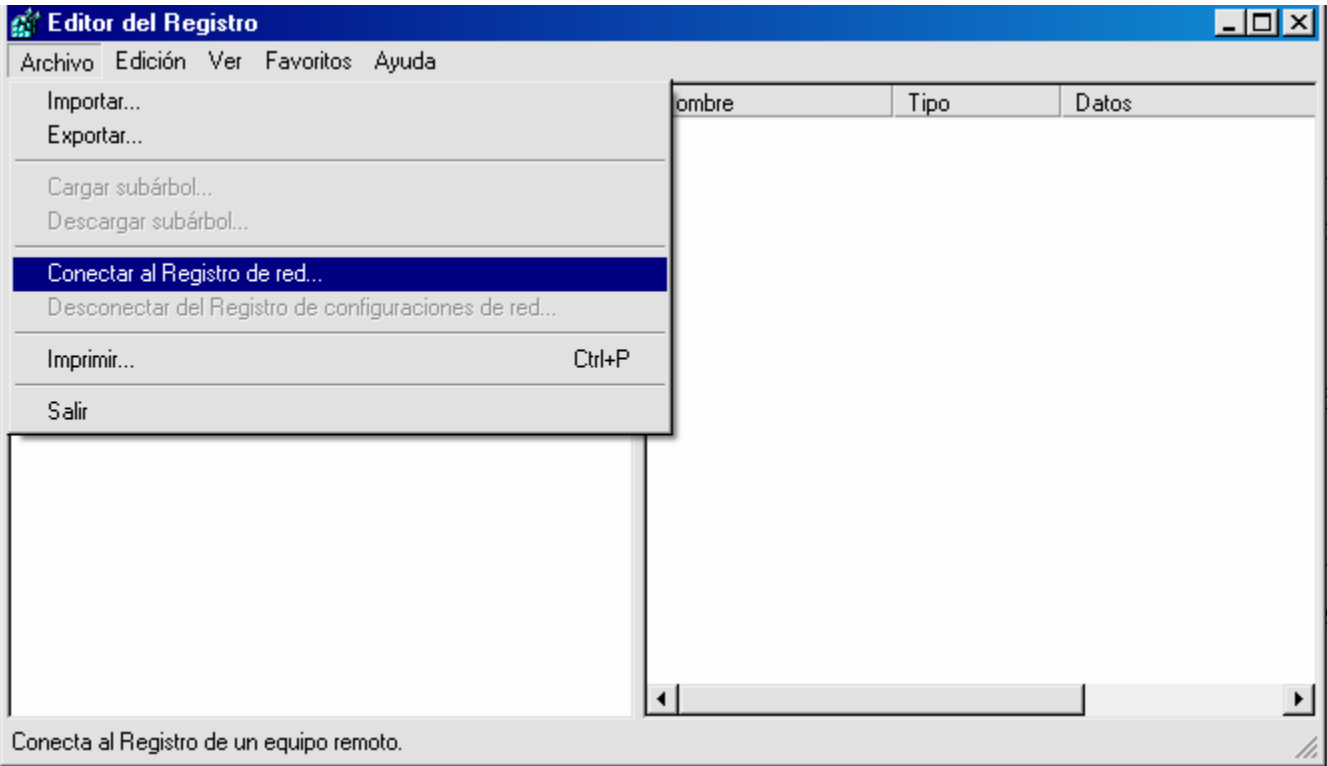


4.4. Importación y exportación de información del Registro



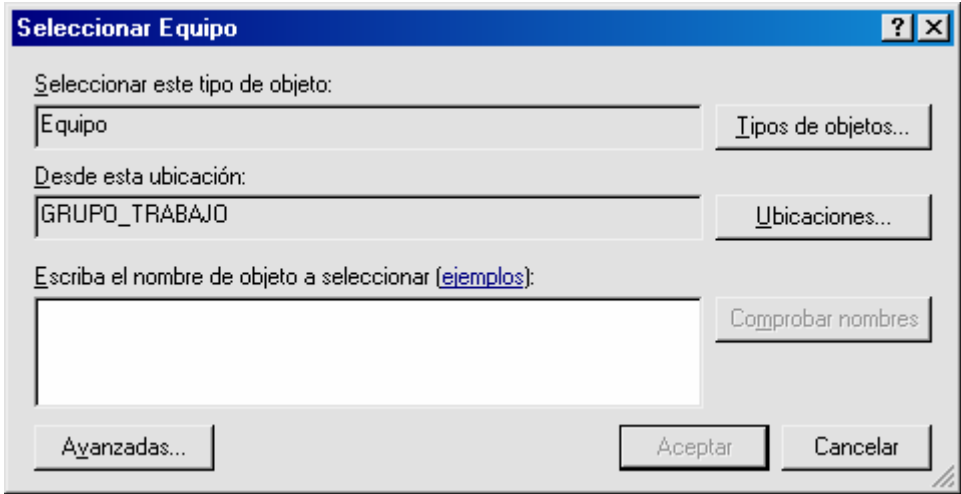
Es posible importar y exportar información del Registro desde Regedit. Los archivos de texto resultantes son fáciles de leer, y es posible moverlos de manera segura de una máquina a otra. De hecho, la asociación predeterminada para los archivos .REG inicia automáticamente Regedit y carga el contenido del archivo cuando se pulsa dos veces sobre éste. El comando Exportar archivo del Registro en el menú Registro permite guardar la clave seleccionada en un archivo, y el comando Importar archivo del Registro hace lo inverso. La importación de archivos del Registro desde Regedit sucede inmediatamente, es decir, aparece un cuadro de diálogo de confirmación para indicar si la importación ha culminado con éxito o no, pero no es posible pararla. Sin embargo, si se inicia un archivo .REG pulsando sobre él, sí se muestra un cuadro de diálogo de confirmación.

4.5. Conexión al Registro de una máquina remota



Si se ha iniciado una sesión con los permisos adecuados, se puede utilizar Regedit para conectarse al Registro de otra computadora para inspeccionarlo o editarlo. Para conseguirlo es necesario disponer de privilegios de administración en ambas máquinas, la máquina donde se ha iniciado una sesión y la otra máquina cuyo Registro se quiere inspeccionar/editar. Es más, la Directiva de grupos puede impedir este acceso.

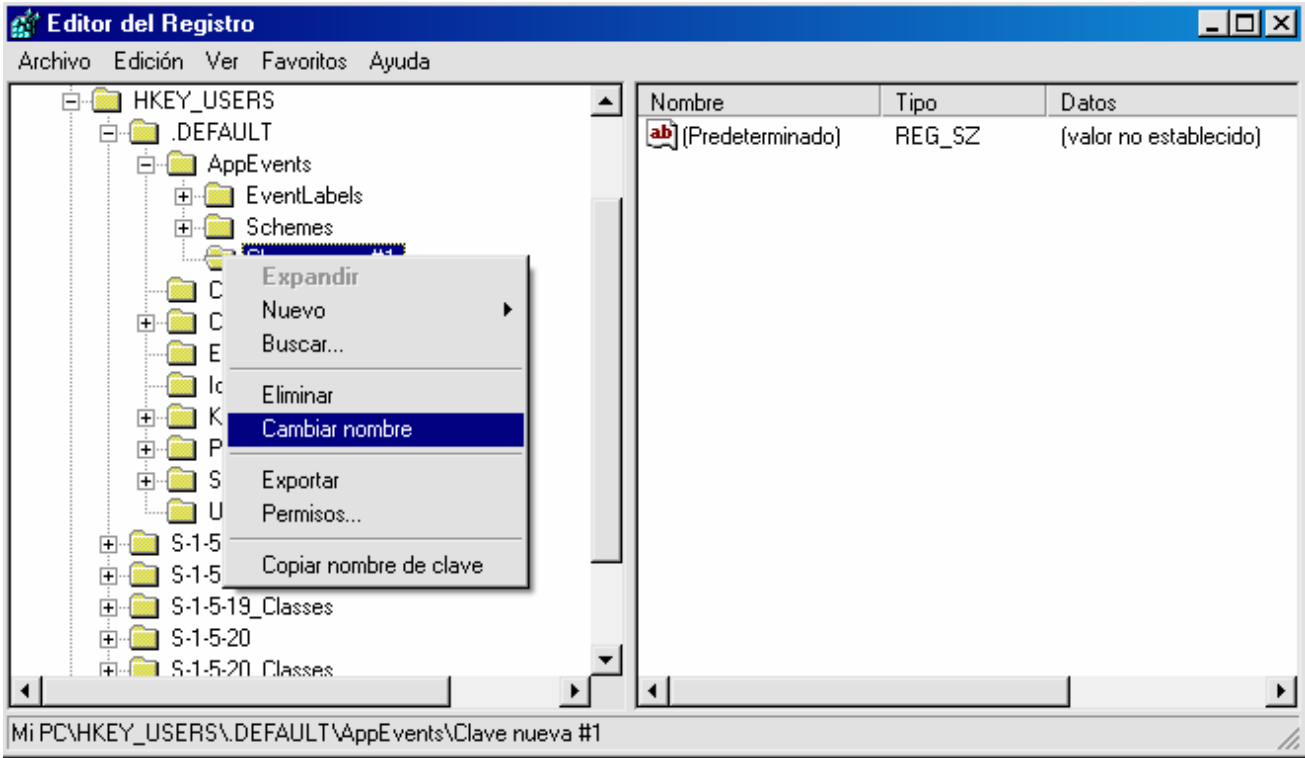
Asumiendo que las credenciales se encuentran en orden, la conexión a la máquina remota se realiza realmente seleccionando Conectarse al Registro de red en el menú Registro.



Este comando permite explorar la red para encontrar la máquina a la que desea conectarse; una vez que se haya realizado la conexión con éxito, aparece el nombre de la computadora en el panel izquierdo al mismo nivel que Mi PC. A partir de aquí es posible expandir su clave raíz, fisgar en las subclaves, buscar y modificar los datos. Cuando se termine, hay que elegir Desconectar del Registro de configuraciones de red en el menú Registro para seleccionar la computadora de la que quiere desconectarse.

4.6. Cambiar nombres de claves y valores

Es posible cambiar el nombre de una clave o valor seleccionando Cambiar nombre en el menú Edición. En la mayoría de los casos, no se querrá ni se necesitará hacer esto. Dado que el software busca valores de nombre específicos, cambiar el nombre de uno de ellos no es una buena idea. Sin embargo, cuando se añaden claves o valores, es posible que se deletree mal el nombre, y el comando Cambiar nombre se convierte entonces en la única alternativa posible para borrar y reproducir la clave.



5. Como buscar cambios del Registro con REGEDIT

Una de las tareas más pesadas del Registro, es hacer un seguimiento de las modificaciones realizadas en el mismo durante la instalación de software nuevo. Para distribuir correctamente el software en una gran empresa, se debe crear normalmente programas de instalación personalizada que controlen, la colocación de archivos, creen los accesos directos en el menú inicio, y a continuación, importen los cambios en el registro.

El programa REGEDIT ofrece algunas funciones para facilitar estas modificaciones. Antes de instalar la aplicación, realice una exportación del Registro para las secciones completas HKEY\_LOCAL\_MACHINE y HKEY\_CURRENT\_USER, y a continuación, ejecute el programa de instalación.

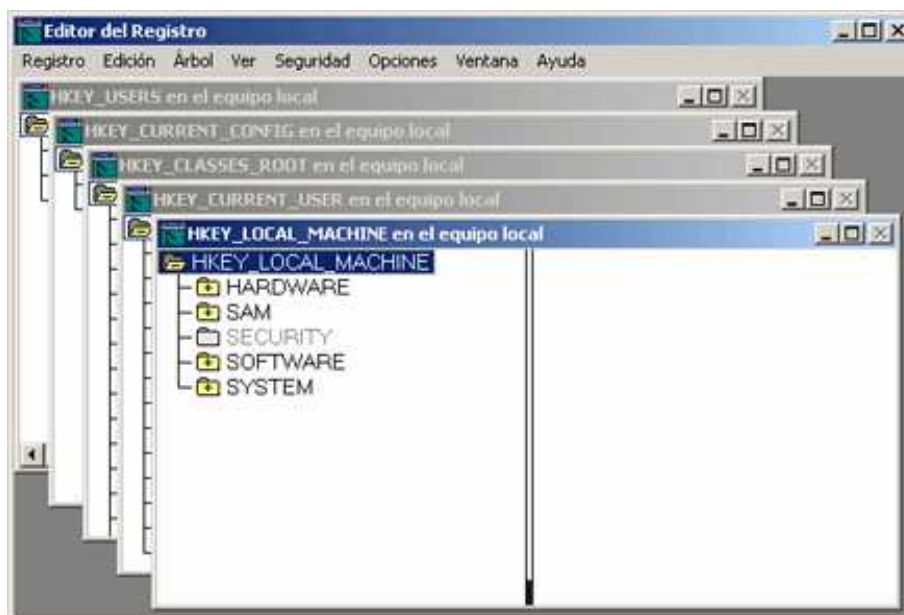
Una vez finalizada la instalación, vuelva a iniciar la maquina si es necesario, y a continuación, exporte de nuevo las mismas secciones del Registro. Al utilizar la línea de comandos de Windows 2000, se ejecuta el programa "FC" para llevar a cabo una comparación de archivos:

```
FC ArchivoAntesDeInstalar.reg ArchivoDespuesDeInstalar.reg > diferencias.txt
```

Este comando mostrara las diferencias entre los dos archivos del Registro en un archivo llamado "diferencias.txt"; Este archivo contendrá las opciones de configuración del Registro que hayan cambiado. Muchas de estas opciones de configuración, sin embargo, puede que no sean importantes en la instalación, por lo que debe examinar con cuidado el archivo de salida para determinar las opciones que se aplican.

## 6. Cómo utilizar REGEDT32

La diferencia con REGEDIT, en cuanto a interfaz, es que REGEDT abre una ventana independiente para cada sección; por lo tanto, se abren cinco ventanas cuando se inicia REGEDT32.



### 6.1. Edición de entradas de valor

Para editar un valor, basta con pulsar sobre él dos veces. Esto hace que el cuadro de diálogo del editor apropiado se abra. Esto es bastante fácil y los editores son fáciles de comprender -exceptuando el editor de REG\_FULL\_RESOURCE\_DESCRIPTOR-. Pero no importa, ya que no se deben editar elementos en HKEY\_LOCAL\_MACHINE\HARDWARE de todas formas, especialmente dado que las modificaciones no se guardan.

Regedt32 también permite editar un elemento como si fuera de un tipo diferente. Por ejemplo, es posible editar un REG\_SZ como información binaria o un REG\_DWORD como una cadena. La mayor parte de las veces esto no resultará de gran utilidad, pero quizás algún día se pueda aprovechar esta funcionalidad para hacer algo, como editar una máscara de bits guardada como un REG\_DWORD. Para editar se deben usar los cuatro comandos del menú Edición: hay uno por cada tipo de dato (Binario, Cadena, DWORD y Cadena múltiple).

Cuando se utilicen estos editores de tipos de datos, no conviene olvidar que:

- En el Editor binario se pueden visualizar los elementos en binario o hexadecimal. El editor marca los desplazamientos en la información mostrando una acotación del desplazamiento de 32 bytes en la izquierda y una escala de 0 a 31 en la parte superior. Esto facilita la localización de bytes con un desplazamiento específico si es necesario.
- El Editor de cadenas múltiples permite introducir una cadena por línea utilizando las teclas RETORNO DE CARRO a INTRO para saltar a la siguiente línea.
- El Editor de DWORD permite la entrada de valores en binario, hexadecimal y decimal. El cuadro de diálogo de este editor ignora las pulsaciones de teclas ilegales (como la del 2 cuando se edita un valor binario)

Al igual que ocurre con Regedit, Regedt32 no comprueba la legalidad de los valores que se introducen; por eso el usuario debe asegurarse de que éstos son correctos.

## 6.2. Adición de claves y valores

Para añadir una clave, se selecciona la clave por debajo de la cual se quiere que aparezca. Por ejemplo, para añadir una subclave a HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ESENT, se tendría que seleccionar la clave y después elegir Agregar clave en el menú Edición. Esto abre un cuadro de diálogo donde se puede introducir el nombre de la nueva clave. Una vez que ésta haya sido nombrada, la nueva clave aparece inmediatamente.

Al contrario que Regedit, Regedt32 no añade automáticamente un valor sin nombrar a la nueva clave, por lo que si se necesita el valor predeterminado por alguna razón, se tendrá que añadir manualmente. Para añadir un valor, se utiliza el comando Agregar valor en el menú Edición. Para añadir un valor, hay que realizar los siguientes pasos:

1. Seleccionar la clave a la que se quiere agregar el valor y después utilizar el comando Agregar valor. Esto hace que se muestre el cuadro de diálogo Agregar valor.
2. Introducir el nombre del nuevo valor en el cuadro de texto Nombre de valor. (Dejarlo en blanco si se quiere añadir el valor predeterminado <No Name>.)
3. Utilizar el cuadro de lista Tipo de datos para seleccionar el tipo del nuevo valor. Presionar el botón Aceptar. El cuadro de diálogo del editor de tipos apropiado aparece; el tipo de editor que se muestre depende del tipo especificado en el campo Nombre de valor.
4. Introducir el dato que se quiera almacenar en el valor y a continuación presionar Aceptar para guardar el nuevo valor, o Cancelar para dejar el Registro intacto.

## 6.3. Eliminación de claves y valores

Regedt32 permite eliminar claves (y todos sus elementos subordinados) o un simple valor -basta con seleccionar el elemento a eliminar y a continuación presionar la tecla SUPR (o seleccionar Eliminar en el menú Edición)-. Regedt32 pide una confirmación de lo que se está realizando de manera predeterminada; si se prefiere, es posible ahorrarse este paso deshabilitando el comando Confirmar eliminación en el menú Opciones (aunque se recomienda -por seguridad- que se deje habilitado).

## 6.4. Carga, descarga e importación de datos del Registro

Regedt32 ofrece dos formas de intercambiar información entre el Registro y un archivo de disco externo. La primera es cargando y guardando conjuntos individuales de claves con los comandos del Registro Guardar clave y Restaurar, y la segunda es cargando y descargando archivos de sección enteros con los comandos Cargar sección y Descargar sección (en el menú Registro).

¿Cuál es la diferencia? Hay que recordar que los archivos de sección son entidades autónomas que contienen un conjunto particular de claves. Cuando se guarda una clave con el comando Guardar clave, realmente se está creando un nuevo archivo de sección que coexiste con las secciones predefinidas al mismo nivel expuestas anteriormente en el capítulo. Posteriormente, la sección puede recomponerse de dos formas: creando una nueva clave dentro de la sección existente (esto es lo que hace el comando Cargar sección) o sobrescribir una clave con los contenidos de la sección guardada tal y como hace Restaurar.

Crear una nueva sección con un conjunto de claves guardadas es fácil: basta con seleccionar la clave que se quiera guardar y a continuación elegir el comando Guardar clave en el menú Registro. Cuando se indique, se introduce el nombre del nuevo archivo de sección y Regedt32 se encarga de guardarlo. La sección no podrá guardarse si no se dispone de los permisos adecuados para todas las subclaves de la clave seleccionada; por ejemplo, incluso cuando se inicia una sesión como administrador, no es posible guardar HKEY\_LOCAL\_MACHINE\HARDWARE a una sección.

Una vez que se ha guardado el archivo de sección, es posible cargarlo dentro de una nueva clave o por encima de una clave que ya existe. Para cargar el archivo de sección en una nueva clave, hay que seleccionar la clave raíz HKEY\_LOCAL\_MACHINE o HKEY\_USERS y a continuación elegir Cargar sección en el menú Registro. (El resto del tiempo esta opción se encuentra deshabilitada.) Cuando se indica, se escoge el archivo de sección que se quiere cargar y el nombre de la nueva clave donde éste se va a cargar.

Para cargar un archivo de sección por encima de una clave existente, hay que seleccionar la clave que se quiera sobrescribir y a continuación elegir Restaurar en el menú Registro; una vez que se haya elegido el archivo y se haya confirmado que se está preparado para eliminar la clave seleccionada, Regedt32 cargará la sección y reemplazará todos los contenidos que existen en las claves con los contenidos de la sección (siempre, naturalmente, que se disponga de los permisos para poder realizar esto).

Por ejemplo, pongamos que se guardan los contenidos de HKEY\_LOCAL\_MACHINE\SOFTWARE\AOL en un archivo de sección. Si se selecciona HKEY\_LOCAL\_MACHINE y se utiliza el comando Cargar sección, se puede crear una nueva clave (denominada, quizás, AOL) donde se guardan los contenidos originales. Si se selecciona la copia existente de HKEY\_LOCAL\_MACHINE\SOFTWARE\AOL y se utiliza el comando Restaurar, entonces todo lo que haya en la clave antes de restaurar el archivo se pierde.

6.5. Conexión al Registro de una máquina remota

Para conectarse a una máquina remota utilizando Regedt32, hay que elegir Seleccionar equipo en el menú Registro. El cuadro de diálogo Seleccionar equipo se abre para que se pueda seleccionar el dominio o grupo de trabajo deseado y el Registro de la máquina que se quiera administrar. Una vez hecho esto, si se dispone de acceso administrativo a la máquina, se estará conectado; es posible que se visualice un cuadro de diálogo en el que se advierte de que las claves del Registro de la máquina remota no se cambiarán automáticamente. Cuando se cierra este mensaje de confirmación, aparecen otras dos ventanas MDI: una para HKEY\_LOCAL\_MACHINE y otra para HKEY\_USERS. Cada título de cada ventana, incluye el nombre de la máquina remota para que se pueda identificar qué tipo de información se encuentra en cada una de ellas.

Una vez que se hayan abierto estas ventanas, se puede navegar y editar de la misma forma que en la máquina local (condicionado, naturalmente, a que se disponga de los permisos de edición de las claves). Cuando se establece una conexión con una máquina remota, se está efectuando realmente una conexión de tipo llamada a un procedimiento remoto (Remote Procedure Call, RPC), que se mantiene abierta hasta que se utiliza el comando Cerrar para cerrar la última ventana que muestra información de ese servidor.

6.6. Administración de la seguridad en las claves del Registro

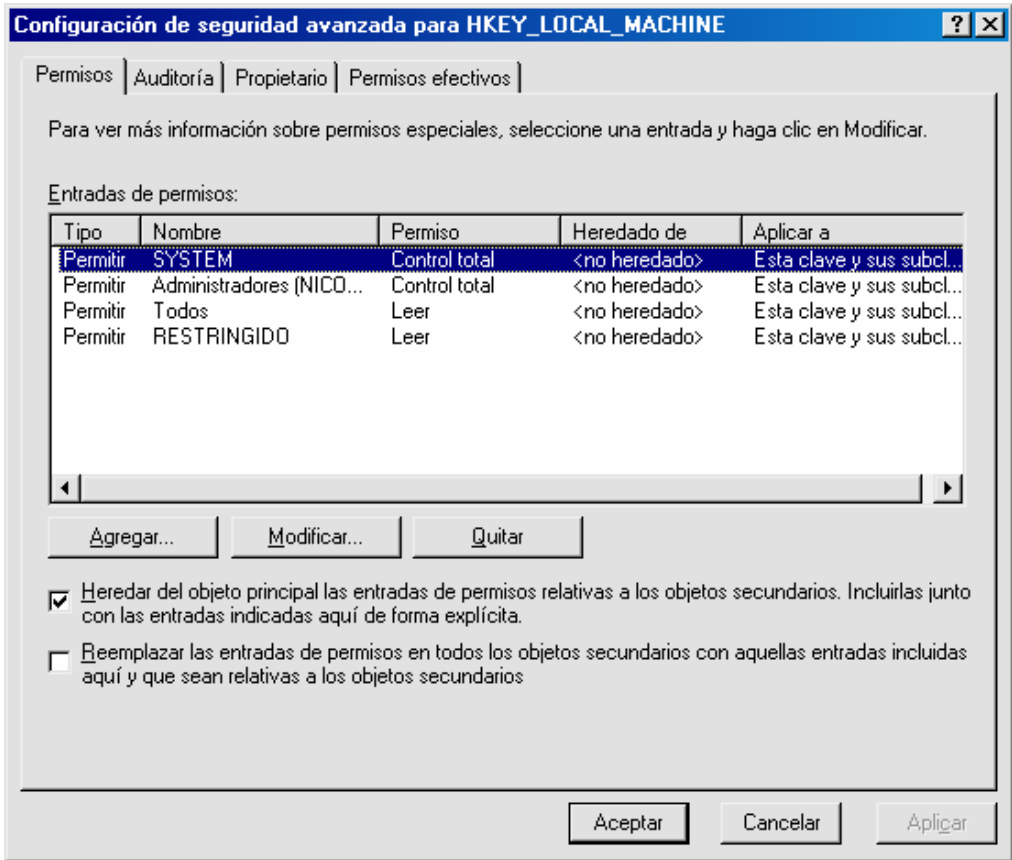
Regedt32 permite fijar la seguridad de las claves del Registro seleccionando una clave y eligiendo el comando Permisos del menú Seguridad. Todo lo aprendido sobre configuración de permisos de archivos es válido aquí también, y las operaciones básicas funcionan del mismo modo: se selecciona un objeto y a continuación se conceden o deniegan privilegios específicos a usuarios y grupos concretos. En el cuadro de diálogo Permisos, se muestran cinco principios de seguridad: Administradores, Usuarios, CREATOR OWNER, Usuarios avanzados y SYSTEM. Los contenidos exactos que se visualizan en la computadora varían dependiendo de la plantilla de seguridad que se haya aplicado; las plantillas más restrictivas podrían cambiar estos permisos significativamente.

El cuadro de diálogo Permisos permite conceder y denegar permisos de Lectura y Control total a las claves. Sin embargo, en general, no deberá hacerse uso de esto en las claves que sean propiedad del sistema; es por ello que Windows incluye las plantillas de seguridad. Resulta sumamente sencillo configurar un permiso accidentalmente de forma tan restrictiva que se consiga que el software que necesita acceso al Registro no pueda tenerlo, y al contrario, es posible que se configuren permisos que son innecesariamente relajados.

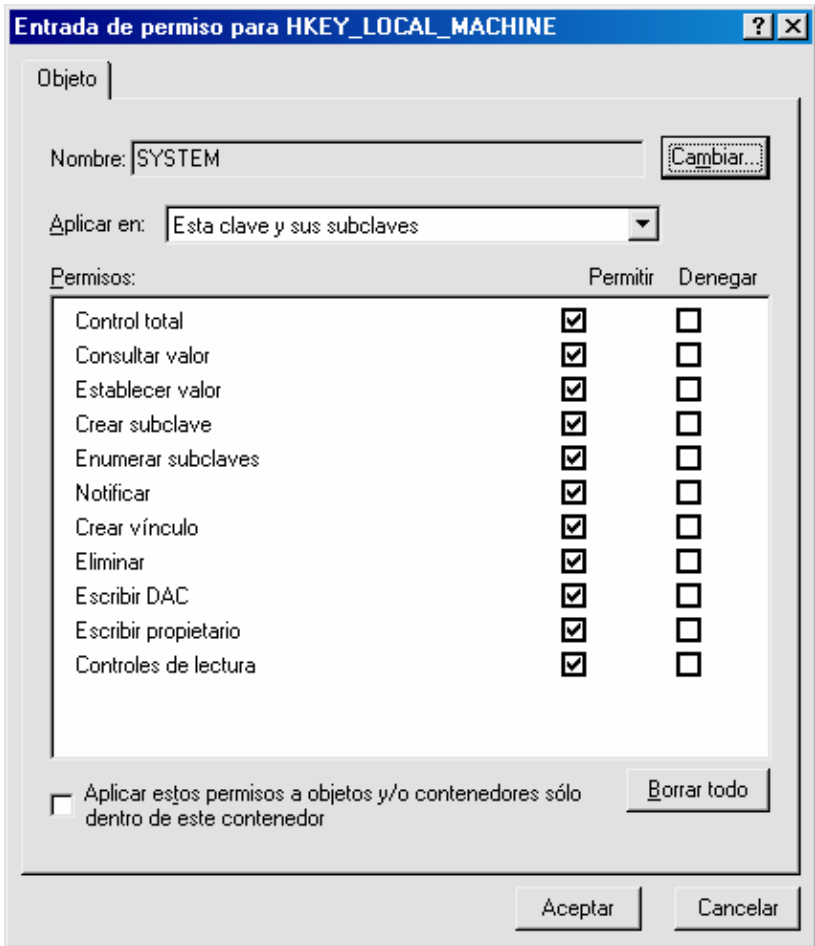
Cuando se configuran los permisos utilizando el cuadro de diálogo Permisos, hay que fijarse en si se habilita o no la opción de Hacer posible que los permisos heredables de un objeto primario se propaguen a este objeto. Esta opción se encuentra habilitada de manera predeterminada, de forma que cuando se aplican nuevos permisos, se propagan automáticamente a todas las subclaves de la clave seleccionada. Dependiendo del nivel en el que se apliquen estos permisos, la herencia puede tener consecuencias no deseadas -si se “relajan” los permisos de una clave, podrían relajarse accidentalmente los permisos de una subclave que deba mantenerse segura-. Antes de cambiar los permisos de cualquier clave, hay que asegurarse de hacer una copia de seguridad correcta del Registro, así como de anotar los cambios que se han realizado para poder deshacerlos más tarde.



Las configuraciones pertenecientes a las aplicaciones son, naturalmente, otra historia. En Windows NT 4 la única forma para determinar los permisos adecuados de la mayoría de las claves de las aplicaciones es expandirlas todo lo posible para a partir de ahí comenzar a relajar los controles gradualmente de abajo arriba hasta que la aplicación funcione correctamente. Desafortunadamente, este enfoque se requiere también en Windows 2000.

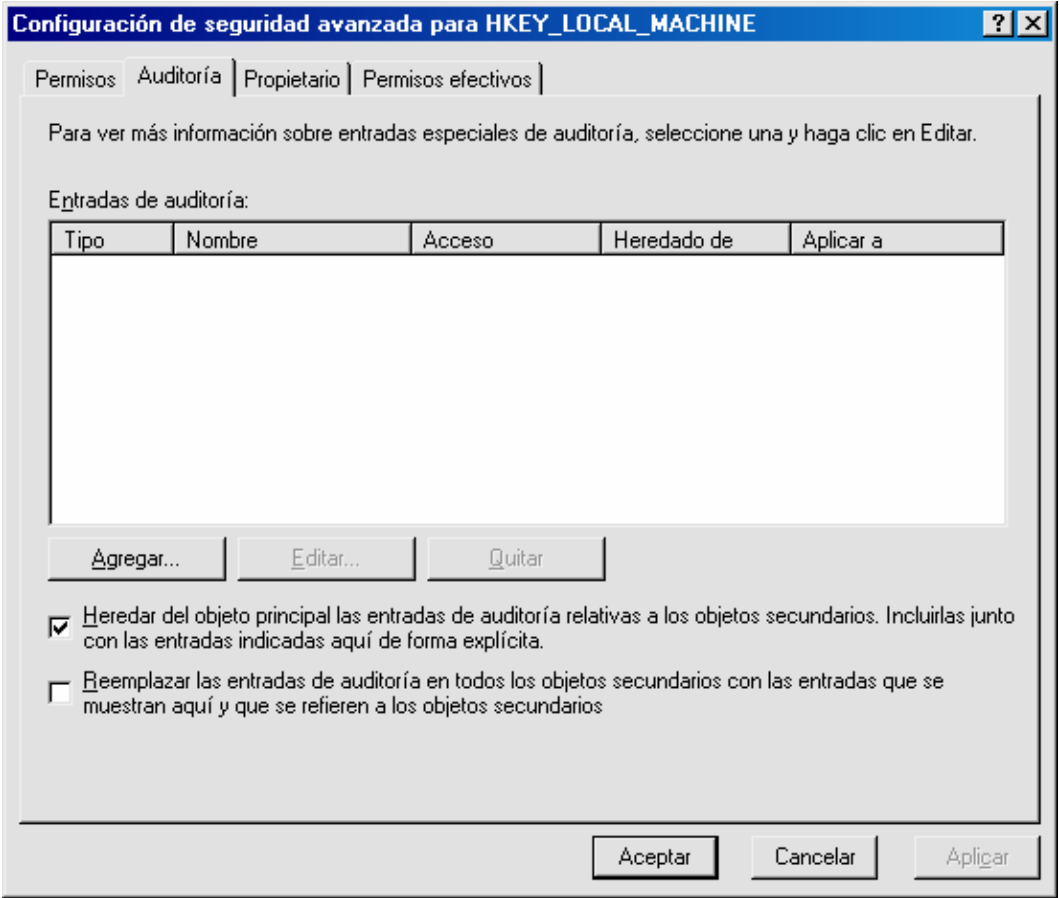


Cuando se pulsa sobre el botón Avanzada del cuadro de diálogo Permisos, se muestra el cuadro de diálogo Configuración de control de acceso que aglutina a tres fichas. Cada ficha tiene un significado especial para las claves del Registro:

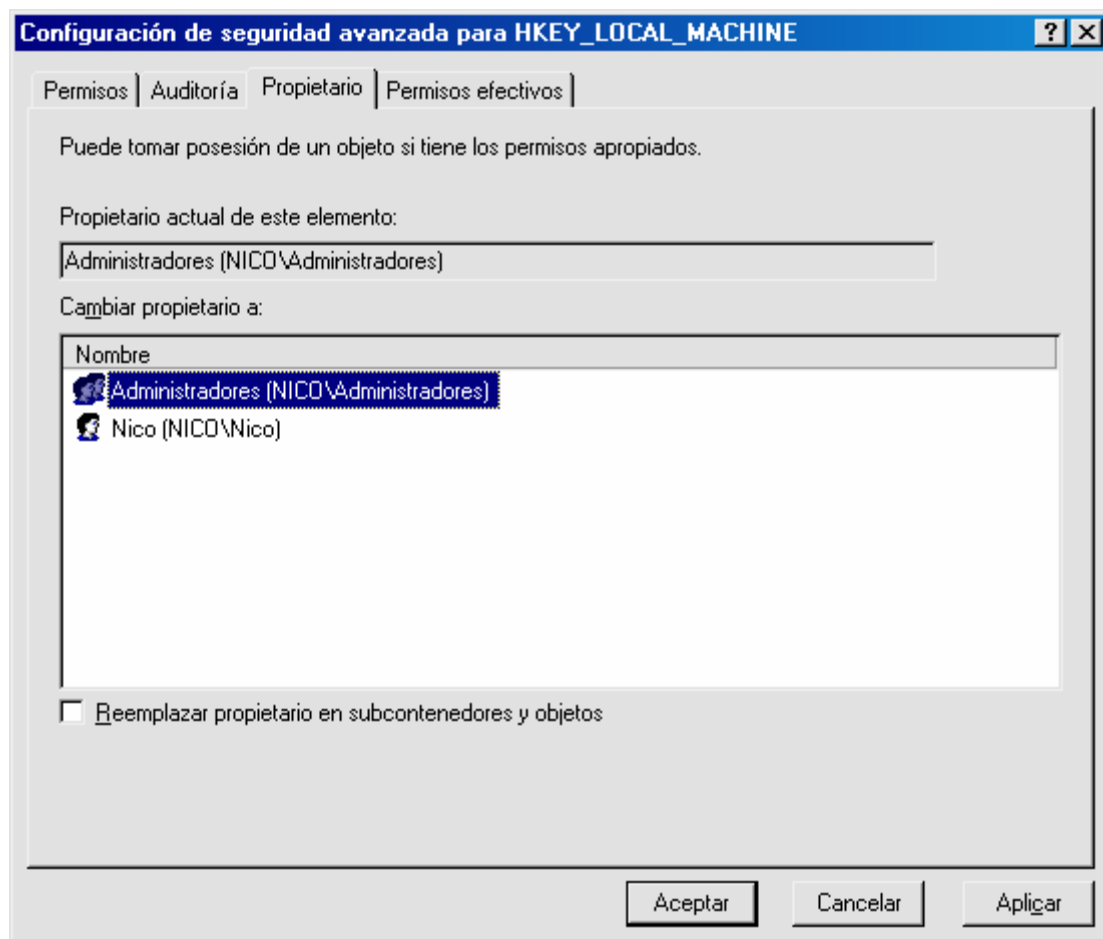




- El botón Ver o modificar de la ficha Permisos permite asignar a usuarios particulares más permisos granulares. Por ejemplo, es posible ajustar quién puede crear nuevos valores en una clave modificando el parámetro de permiso Establecer valor. Es posible que no se puedan realizar cambios aquí sin deshabilitar la herencia, dado que la mayor parte de los registros obtiene sus permisos de esta forma.
  - Consultar valor: Permite al usuario consultar el Registro para un valor específico dando el camino completo a ese valor.
  - Establecer valor: Permite al usuario crear nuevos valores por debajo de una clave o sobrescribir un valor existente.
  - Crear subclave: Permite al usuario crear una nueva subclave por debajo de la clave especificada.
  - Enumerar subclaves: Permite al usuario obtener una lista de todas las subclaves de una clave particular; similar a un recorrido de directorios de un volumen NTFS.
  - Notificar: Permite al usuario registrar una función de respuesta que se dispara cuando el valor seleccionado cambia.
  - Crear vínculo: Permite al usuario crear un vínculo a una clave específica (de la misma forma que HKEY\_CLASSES\_ROOT se vincula a HKEY\_LOCAL\_MACHINE\Classes).
  - Eliminar: Permite al usuario eliminar una clave o valor individual.
  - Escribir DAC Permite al usuario rescribir los controles de acceso de una clave específica.
  - Escribir propietario: Permite al usuario convertirse en el propietario de la clave seleccionada.
  - Controles de lectura: Permite al usuario leer la lista de control de acceso discrecional (Discretionary Access Control List, DACL) para un valor específico.
- La ficha auditoria permite establecer permisos de auditoria para la clave seleccionada. Primero, se especifican los usuarios y grupos cuyas acciones se pretende auditar; entonces se especifica qué acciones particulares se quieren guardar. Es posible auditar los intentos fallidos y exitosos del ejercicio de estos permisos.



- La ficha Propietario permite reasignar al propietario de la clave seleccionada, con o sin propagar los cambios a todos los subelementos por debajo de ella. Un cambio de propietario puede desencadenar la generación de una huella de auditoría dependiendo de los parámetros de configuración de seguridad.



## 6.7. Algunos trucos útiles

Existen cuatro comandos muy útiles de Regedt32 que no se ajustan a ningún punto de esta exposición:

- Regedt32 no puede buscar valores, pero sí buscar una clave con un nombre especificado. El comando Buscar clave en el menú Ver permite buscar en el Registro el nombre de una clave en particular (comenzando con la clave seleccionada y procediendo hacia arriba o abajo). Las búsquedas pueden distinguir entre mayúsculas y minúsculas o no, y se puede elegir entre buscar el texto suministrado completo o como parte de otro nombre.
- Ya hemos trabajado tímidamente con el comando Confirmar eliminación del menú Opciones. Cuando se selecciona (tal y como está de manera predeterminada), Regedt32 pide que se confirme la intención de eliminar una clave.
- El comando Sólo lectura del menú Opciones conmuta Regedt32 entre el modo de sólo lectura y el normal. El modo de sólo lectura es una gran bendición, ya que evita que se causen daños al Registro cuando se encuentra habilitado. Posibilita que se pueda aprender explorando sin que se corran riesgos de causar daños accidentales.
- El comando Actualización automática del menú Opciones controla la posibilidad de que Regedt32 actualice automáticamente las ventanas de las claves raíces periódicamente. Esta opción se encuentra habilitada de manera predeterminada, por lo que Regedt32 actualiza por sí mismo las ventanas locales. En las máquinas donde se produzcan muchos cambios en los registros, podría considerarse la posibilidad de deshabilitar las actualizaciones automáticas y utilizar los comandos Actualizar todo y Actualizar la activa del menú Ver para disparar las actualizaciones sólo cuando se necesiten.

## 7. Copia de Seguridad y Recuperación del Registro

La copia de seguridad de Windows 2000, para copiar y restaurar el estado general del sistema, difiere un poco de Windows NT, donde se puede hacer fácilmente una copia de seguridad del Registro creando un disco de reparaciones ante emergencias (Emergency Repair Disk, ERD) o ejecutando Ntbackup y habilitando la opción de Incluir Registro local.

Estas diferencias se deben al Active Directory. En Windows NT, una copia de seguridad del Registro contiene una copia de la base de datos SAM de la máquina local (al igual que una copia del dominio SAM cuando se realiza una copia de seguridad del controlador de dominios). En una red que utilice Active Directory, el directorio contiene la mayor parte de la información existente formalmente en el SAM, que es la razón por la que para los controladores de dominio se tenga que realizar un proceso de recuperación en dos fases.

### 7.1. Selección de un método de copia de seguridad

Dado que el Registro es algo más que un archivo ordinario, tiene sentido otorgar a los procedimientos de copia de seguridad y restauración una dedicación en tiempo superior a la normal. Es posible hacer copias de seguridad y restauración del Registro de otras formas aparte de haciendo copias de seguridad completas del estado del sistema entero. Naturalmente, esto no excluye el seguir haciendo copias de seguridad regulares de los datos personales, así como de los estados del sistema de cada computadora que se administre. La copia de seguridad del Registro por sí sola es muy útil, dado que es en éste donde la mayor parte de las aplicaciones y los componentes del sistema guardan sus preferencias y parámetros de configuración.

### 7.2. Copia de seguridad de Windows 2000

Cuando se utiliza la Copia de seguridad de Windows 2000 para hacer una copia del estado del sistema, ésta incluye una copia completa del Registro de la máquina. También incluye copias del volumen del sistema (en controladores de dominio), datos de certificación, información de Registro de las clases COM+, así como otra información ajena a lo que es el Registro. Por otro lado, la Copia de seguridad de Windows 2000 automatiza el proceso de realizar una copia de seguridad del Registro, de forma que sea fácil de utilizar y comprender. Además, el guardar la información del Registro con el resto de la información del servidor permite restaurar todo sin tener que recurrir a CD de otros fabricantes, controladores y otras cosas relativas.

### 7.3. El Disco de reparación ante emergencias

El Disco de reparación ante emergencias (Emergency Repair Disk, ERD) de la Copia de seguridad de Windows 2000 permite también hacer una copia de seguridad del Registro; la mayoría de los administradores de Windows NT utilizan esto como primera línea de defensa contra los fallos, dado que las herramientas de reparación incluidas en Windows NT 4 pueden restaurar la información del Registro desde un ERD. Windows 2000 utiliza los ERD también, pero no incluyen la información del Registro. Cuando se utiliza la Copia de seguridad de Windows 2000 para crear un ERD, debe especificarse que se desea hacer una copia de seguridad del Registro y esta información no se almacena directamente en el disco del ERD (hace falta guardar manualmente una copia y entonces reemplazar durante la restauración los archivos de Registro copiándolos empleando la consola de recuperación).

### 7.4. Copias de seguridad manuales

Dado que Regedt32 permite cargar y descargar archivos de sección y claves, es posible aproximarse a lo que hace la Copia de seguridad de Windows 2000 guardando manualmente en un archivo de sección las claves en las que se está más interesado, copiando los archivos resultado en algún lugar seguro y cargándolos de nuevo si se necesitan. Esta aproximación es correcta, pero requiere mucho trabajo dado que al no ser posible informar a Regedt32 de las claves que se quieren guardar, no hay forma de automatizar el proceso.

### 7.5. Copia de seguridad del Registro

El proceso de copia de seguridad de Windows 2000 es sencillo (es una gran mejora respecto a Windows NT 4).

Pasos recomendados:

1. Ejecutar la aplicación de Copia de seguridad de Windows 2000; cuando aparezca, pulsar la pestaña de Copia de seguridad.
2. Especificar el dispositivo de copia de seguridad o la ubicación que se quiera emplear con las opciones de Destino de la copia de seguridad o Hacer copia de seguridad del medio o del archivo.
3. Si es necesario, expandir el icono de Mi PC.
4. Seleccionar la opción de Estado del sistema (hay que recordar que los elementos del estado del sistema están relacionados entre sí y no pueden copiarse por separado).
5. Pulsar el botón Iniciar. Cuando el sistema copia la información del estado del sistema, se incluyen los archivos del Registro permitiendo su recuperación posterior.

### 7.6. Grabación de una copia del Registro

Cuando se crea un ERD, la Copia de seguridad de Windows 2000 ofrece la posibilidad de copiar el Registro. Cuando se selecciona esta opción, una copia extra de los archivos de sección del Registro se almacena en la carpeta %SystemRoot%\Repair\REGBACK. Además de los archivos de sección estándar (SECURITY, SAM, SYSTEM, SOFTWARE, DEFAULT, Ntuser.dat y Usrclass.dat), se pueden observar los archivos representativos de las secciones que se hayan cargado manualmente en el Registro.

Cuando la Copia de seguridad de Windows 2000 termina de copiar estos archivos, éstos quedan a disposición del usuario -el usuario puede moverlos, copiarlos, hacer una copia de seguridad de ellos o cualquier otra cosa que se quiera-. En particular, se pueden comprimir y guardar en un disquete, así como mover a cualquier medio extraíble que se tenga a mano.

### 7.7. Recuperación del Registro

Si se dispone de una copia de seguridad en la carpeta %SystemRoot%\Repair\REGBACK, la Consola de recuperación puede utilizarse para restaurar la copia de seguridad del Registro. Cuando se ejecuta la Consola de recuperación, se pueden copiar los archivos de Registro necesarios para restaurarlos en su ubicación normal en disco y a continuación reiniciar la máquina. No hay que olvidar que al hacer esto se eliminan todos los cambios que se hayan realizado desde el momento en que se creó la copia de seguridad.

## 8. Uso de la última configuración buena conocida

A pesar de las advertencias, algunos usuarios modifican el Registro de forma que será imposible volver a iniciar Windows 2000 de manera correcta. Afortunadamente, en Windows 2000, existe una característica llamada "la última configuración buena conocida".

Durante el proceso de inicio, Windows 2000, lee información que necesita ejecutar desde dentro de la parte CurrentControlSet del Registro. Cuando Windows 2000 se inicia correctamente -al mismo tiempo que muestra en pantalla el mensaje "Presione Ctrl+Alt+Supr para iniciar"- vuelve a vincular ControlSet001 con ControlSet002 y, a continuación, copia las opciones actuales a ControlSet001. Si el sistema no puede iniciar hasta el punto donde vuelve a escribir los conjuntos de control, el usuario puede volver a iniciar la máquina desde la última configuración buena conocida, que leerá las opciones de ControlSet001 en lugar de CurrentControlSet, omitiendo de este modo, las entradas erróneas del Registro.

Para tener acceso a la última configuración buena conocida, tenemos que volver a iniciar la máquina, y en el menú de selección del sistema operativo (SO), presionamos F8. Y esto va a permitir seleccionar la opción "la última configuración buena conocida"; la misma es (valga la redundancia) la última configuración que funcionaba antes de, la última vez que se volvió a iniciar. En otras palabras, si la máquina no se ha vuelto a iniciar desde hace mucho tiempo, las opciones de configuración pueden que estén desfasadas, y quizás, muchas opciones sean antiguas; no solo la que impidió que la máquina se iniciara normalmente. Por lo tanto, sería mejor que volviéramos a iniciar el sistema antes de realizar cambios a la máquina local, como por ejemplo, instalar software nuevo, ó modificar el Registro.

## 9. Bibliografía consultada

<http://support.microsoft.com/kb/256986>

[http://fmc.axarnet.es/win2000srv/tema-21/tema\\_21\\_m.htm](http://fmc.axarnet.es/win2000srv/tema-21/tema_21_m.htm)

[http://www.svetlian.com/windows/temas\\_registro.htm](http://www.svetlian.com/windows/temas_registro.htm)

<http://www.qsl.net/ea3dlv/Info/registry.htm>

Entorno del sistema operativo Windows 2000 [Capítulo 7 – El Registro]