El Registro de Windows

El Registro juega un papel clave en la configuración del sistema operativo. No es simplemente un conjunto de datos estáticos existentes en el disco duro, sino también, mediante una arquitectura compleja de información dinámica, una ventana abierta al corazón del sistema.

El Editor del Registro es una utilidad que permite visualizar y editar todas las informaciones contenidas en los archivos de subárbol. Los archivos de subárbol son los archivos que contienen los parámetros del sistema operativo y de las aplicaciones y constituyen lo que llamamos Registro.

1. Ejecutar el Registro

En el cuadro de texto **Iniciar búsqueda** situado encima del menú **Iniciar**, o desde la pantalla de inicio en Windows 8 introduzca: **`regedit`**. Para abrir varias ventanas de registro, introduzca el modificador **`-m`**: **`regedit -m`**. Puede hacerlo tantas veces como desee. Simplemente recuerde que los cambios realizados en una de las ventanas no repercutirán en la otra, a menos que seleccione una ventana y la actualice pulsando la tecla [F5].

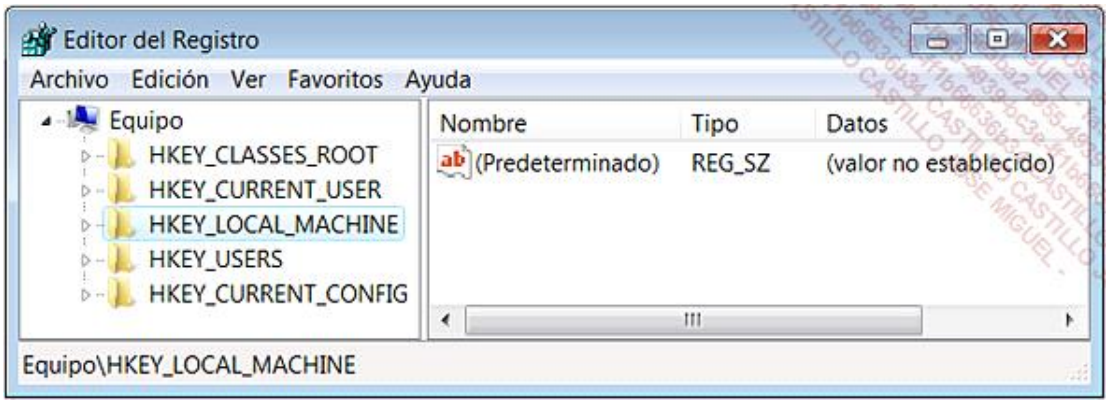
2. Actualizar el Registro

En Windows 8 y Windows 7, cuando realiza un cambio en el Registro o en el Editor de objetos de directiva de grupo, los cambios están activos de manera inmediata (salvo algunas excepciones).

3. Los valores y la información del valor

Hay cinco ramas visibles que se pueden expandir:

- Haciendo clic en la flecha pequeña de la izquierda.
- Haciendo doble clic en una de las ramas.
- Haciendo clic con el botón secundario del ratón y seleccionando la opción **Expandir**.



Verá que en el interior de cada una de las ramas hay un árbol de claves y subclaves. Las claves son una manera de organizar los datos presentes y clasificarlos por temas.

Si selecciona una de las claves, aparecerán algunos datos en la ventana de la derecha. Estos son los valores y están formados por tres informaciones:

- nombre del valor

- tipo del valor
- datos inscritos en el valor llamados "Datos del valor"

Cada una de las claves puede contener uno o más valores.

No es posible modificar las ramas principales, pero puede realizar todo tipo de operaciones en las claves, valores y datos del valor.

4. Estructura del Registro

Las claves raíz visibles son cinco.

- **HKEY_CLASSES_ROOT**: contiene principalmente la información de asociación de archivos, componentes COM y la información de registro de objetos.
- **HKEY_CURRENT_USER**: contiene los datos correspondientes al usuario que está conectado en ese momento.
- **HKEY_LOCAL_MACHINE**: contiene los datos correspondientes al sistema.
- **HKEY_USERS**: contiene los datos correspondientes al conjunto de usuarios del equipo.
- **HKEY_CURRENT_CONFIG**: contiene información del perfil físico actual.

Es habitual que algunas claves utilicen las abreviaturas siguientes:

- HKEY_CLASSES_ROOT: HKCR.
- HKEY_CURRENT_USER: HKCU.
- HKEY_LOCAL_MACHINE: HKLM.
- HKEY_USERS: HKU.
- HKEY_CURRENT_CONFIG: HKCC.

La letra H representa el identificador de Windows (Handle) de las claves (KEY).

Algunas claves funcionan como enlaces replicados que dirigen a otros árboles:

- La clave HKEY_CURRENT_CONFIG es una réplica de esta rama: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current.
- La clave HKEY_CLASSES_ROOT es una réplica de ésta: HKEY_LOCAL_MACHINE\SOFTWARE\Classes.
- La clave HKEY_CURRENT_USER corresponde a ésta: HKEY_USERS\Usuario conectado en ese momento.

En conclusión, sólo las claves HKEY_USERS y HKEY_LOCAL_MACHINE poseen una existencia propia.

5. Los archivos de subárbol

Toda la información se extrae directamente de los archivos de subárbol que están ubicados principalmente en *\Windows\system32\config*. Presentamos aquí la lista de correspondencias:

- HKEY_LOCAL_MACHINE\BCD00000000: *\Boot\BCD*
- HKEY_LOCAL_MACHINE\COMPONENTS: *\Windows\system32\config\COMPONENTS*

- HKEY_LOCAL_MACHINE\SAM : *\windows\system32\config\SAM*
- HKEY_LOCAL_MACHINE\SECURITY: *\Windows\system32\config\SECURITY*
- HKEY_LOCAL_MACHINE\SOFTWARE: *\Windows\system32\config\SOFTWARE*
- HKEY_LOCAL_MACHINE\SYSTEM: *\Windows\system32\config\SYSTEM*
- HKEY_USERS\SID: *\Users\"Nombre_de_usuario"\ntuser.dat*
- HKEY_USERS\SID del usuario_Classes: *\Users\Juan\AppData\Local\Microsoft\Windows\UsrClass.dat*
- HKEY_USERS\.DEFAULT: *\Windows\system32\config\DEFAULT*
- HKEY_LOCAL_MACHINE\HARDWARE: subárbol volátil

Este último subárbol está ubicado exclusivamente en la memoria, así que no tiene una ruta precisa en el Explorador de Windows. Hay dos archivos de subárbol un poco particulares creados por NTDETECT.COM cada vez que el ordenador arranca:

- Servicio local: `\Windows\ServiceProfiles\LocalService\NTUSER.DAT`
- Servicio de red: `\Windows\ServiceProfiles\NetworkService\NTUSER.DAT`

Hay diferentes tipos de archivos:

- Regtrans-ms: estos archivos son diarios de transacciones que se utilizan para almacenar los cambios en bases de registro para evitar la corrupción de archivos de subárbol.
- Blf: del mismo modo, el componente Common Lof File System (CLFS) utiliza estos ficheros diarios para almacenar los cambios en bases de registro para evitar la corrupción de archivos de subárbol.
- LOG: estos archivos son archivos de registro que guardan los cambios realizados tanto en claves como en valores.

Nombre	Fecha modificación	Tipo	Tamaño
RegBack	17/06/2009 14:44	Carpeta de archivos	
systemprofile	22/04/2009 1:52	Carpeta de archivos	
TxR	10/12/2008 16:21	Carpeta de archivos	
BCD-Template	10/12/2008 23:32	Archivo	256 KB
BCD-Template.LOG	10/12/2008 23:32	Documento de texto	37 KB
BCD-Template.LOG1	02/11/2006 14:42	Archivo LOG1	0 KB
BCD-Template.LOG2	02/11/2006 14:42	Archivo LOG2	0 KB
COMPONENTS	17/06/2009 14:39	Archivo	32.000 KB
COMPONENTS.LOG	21/12/2006 23:18	Documento de texto	1 KB
COMPONENTS.LOG1	17/06/2009 14:39	Archivo LOG1	256 KB
COMPONENTS.LOG2	16/04/2009 21:38	Archivo LOG2	256 KB
COMPONENTS.SAV	02/11/2006 12:34	Archivo SAV	8 KB
DEFAULT	17/06/2009 14:39	Archivo	256 KB
DEFAULT.LOG	21/12/2006 23:18	Documento de texto	1 KB
DEFAULT.LOG1	17/06/2009 14:39	Archivo LOG1	256 KB
DEFAULT.LOG2	16/04/2009 21:38	Archivo LOG2	256 KB
DEFAULT.SAV	02/11/2006 12:34	Archivo SAV	20 KB
SAM	17/06/2009 15:34	Archivo	256 KB
SAM.LOG	21/12/2006 23:18	Documento de texto	1 KB
SAM.LOG1	17/06/2009 15:34	Archivo LOG1	256 KB
SAM.LOG2	02/11/2006 14:31	Archivo LOG2	0 KB

Las versiones de seguridad de los ficheros de subárbol se colocan en el directorio C:\Windows\System32\RegBack. En un principio, se trata de la mejor opción si quiere restaurar manualmente un archivo de subárbol de tipo Maquina y reemplazarlo por otra versión.

La lista de archivos de subárbol se puede obtener visualizando el contenido de esta clave de registro: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

6. Manipular el registro

Existen varias maneras de crear una nueva clave. Puede, por ejemplo:

- Seleccionar la clave primaria.
- Hacer clic en **Edición - Nuevo - Clave**.

Aparecerá la mención *Clave nueva #1*.

Como de manera predeterminada se encuentra en modo Edición, podrá introducir directamente el nombre de la clave. Si no es así puede cambiar de nuevo al modo Edición pulsando la tecla [F2].

También puede utilizar el menú contextual accesible desde la clave que funciona como contenedor, siempre y cuando ésta última esté seleccionada, o puede activar el menú contextual haciendo clic en la ventana de la derecha.

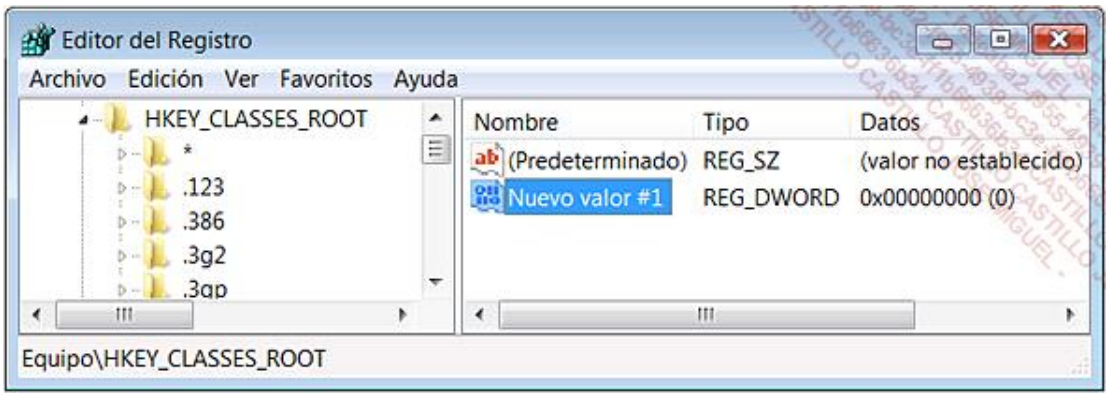
De la misma manera, también es posible eliminar ([Supr]) o renombrar una clave.

No es posible eliminar o seleccionar varias claves a la vez manteniendo presionadas las teclas [Ctrl] o [Mayús]. Sin embargo, sí puede hacerlo con los valores.

Tenga en cuenta que cada vez que cree una clave, automáticamente se creará un valor (predeterminado).

7. Modificar los valores

De la misma manera que antes, puede crear nuevos valores DWORD, de cadena, binario, etc. El nombre predeterminado será: Nuevo valor #1.



Para insertar los datos en la entrada que acaba de crear, haga doble clic en ella e introduzca la cadena de caracteres en el cuadro de texto **Información del valor**.

También puede hacer clic con el botón secundario del ratón en esa entrada y después en el comando **Modificar**. El mismo comando es accesible desde el menú **Edición**.

Existen dos opciones: **Modificar** y **Cambiar datos binarios**. Ésta última le permite visualizar los datos en su representación hexadecimal.

Puede visualizar directamente este tipo de información si selecciona un valor DWORD o binario y hace clic en **Ver - Mostrar datos binarios**.

Por otra parte, cuando introduzca la información del valor en una entrada DWORD, podrá elegir entre utilizar la base decimal o hexadecimal. En el primer caso, sólo tendrá que seleccionar la opción de botón **Decimal**. De todas maneras, la cifra o número que introduzca se mostrará en base hexadecimal.

Cuando cree un nuevo valor de cadena, los datos del valor estarán vacíos.

De manera predeterminada, al crear un valor DWORD los datos serán de valor cero y en el caso de valores binarios estos serán de longitud cero.

Cuando cree una nueva clave, el valor (predeterminado) indica que los datos no están definidos (valor no definido).

8. Buscar en el Registro

- Para realizar una búsqueda, seleccione el árbol de partida y haga clic en **Edición - Buscar** ([Ctrl]+F).
- En el cuadro de texto **Buscar**, introduzca la expresión buscada.
- En el apartado **Buscar en** indique si la búsqueda se realizará sobre las:
  - Claves

- Valores
- Datos

Puede seleccionar la casilla **Sólo cadenas completas** si prefiere encontrar los casos que corresponden exactamente a la expresión buscada (y no de manera parcial).

Para lanzar una búsqueda, haga clic en **Edición - Buscar siguiente** o pulse la tecla [F3].

En cada ocasión, la entrada o clave correspondientes se señalarán con un resaltado.

Tenga en cuenta que si la búsqueda se realiza en todo el conjunto del Registro no deberá seleccionar la rama primaria Equipo, sino la primera clave: HKEY_CLASSES_ROOT. En caso contrario, la búsqueda no dará ningún resultado.

Por otra parte, una búsqueda se inicia siempre desde la clave seleccionada. Para alcanzar rápidamente el punto de partida de la búsqueda pulse la tecla [Inicio]. La rama Equipo se resaltará automáticamente. Una vez realizado esto, sólo tendrá que seleccionar la clave HKEY_CLASSES_ROOT.

9. Importar o exportar una clave

Esta operación permite copiar el conjunto de valores incluidos en una clave, así como la propia clave. Esto le permitirá exportar una parte del Registro procedente de un ordenador "sano" e importarlo al sistema "dañado". Es una manera rápida y segura de reparar un problema debido a entradas defectuosas en el registro.

- Seleccione una de las claves del registro.
- Haga clic en **Archivo - Exportar**.

También puede utilizar la opción **Exportar** que aparece en el menú contextual de la clave.

- En la lista desplegable **Guardar en**, seleccione el directorio de destino.
- En el cuadro de texto **Nombre**, introduzca un nombre para el archivo.

Le recordamos que el nombre que elija no tiene importancia.

- En la lista desplegable **Tipo**, seleccione el formato que tendrá el archivo de rescate.

Puede elegir entre:

- **Archivo de Registro (*.reg)**: el archivo tendrá una extensión en REG que contendrá como encabezado lo siguiente: Windows Registry Editor Version 5.00. Este formato es compatible con las versiones Windows XP y posteriores.
- **Archivo de subárbol de Registro**: este archivo no tendrá ninguna extensión visible. Más adelante veremos su utilidad práctica.
- **Archivos de texto (*.txt)**: el archivo tendrá una extensión TXT. Muestra el nombre de la clase así como la hora de la última escritura para cada clave o valor de la lista.
- **Archivos de Registro de Win9x/NT4 (REGEDIT4) (*.reg)**: este formato de registro es compatible con las versiones antiguas de Regedit que podemos encontrar en Windows 9X, ME y Windows NT. El encabezado del archivo será: REGEDIT4. También puede utilizar el formato de registro en los sistemas más recientes de Windows.
- **Todos los archivos**: esta posibilidad permite cambiar de manera sencilla la extensión del fichero de registro.

Esta opción necesita algunas aclaraciones: no es necesario que un archivo de registro tenga una extensión REG, ya que también funciona con archivos sin extensión que lleven una extensión que usted ha creado.

Con el fin de editar un archivo de registro REG en formato de texto, haga clic con el botón derecho en el archivo y seleccione la opción **Modificar**.

El archivo de registro se abrirá en el Bloc de notas de Windows.

También puede seleccionar abrirlo con otro programa haciendo clic en el submenú **Abrir con**.

En lo que respecta a los archivos de subárbol, describimos aquí los pasos que se deben seguir:

- Haga clic con el botón secundario del ratón en el archivo y seleccione la opción **Abrir**.
- En el apartado **Elija el programa que desea usar** para abrir el archivo seleccionado, utilice, por ejemplo, el Bloc de notas de Windows.

Como podrá comprobar es ilegible.

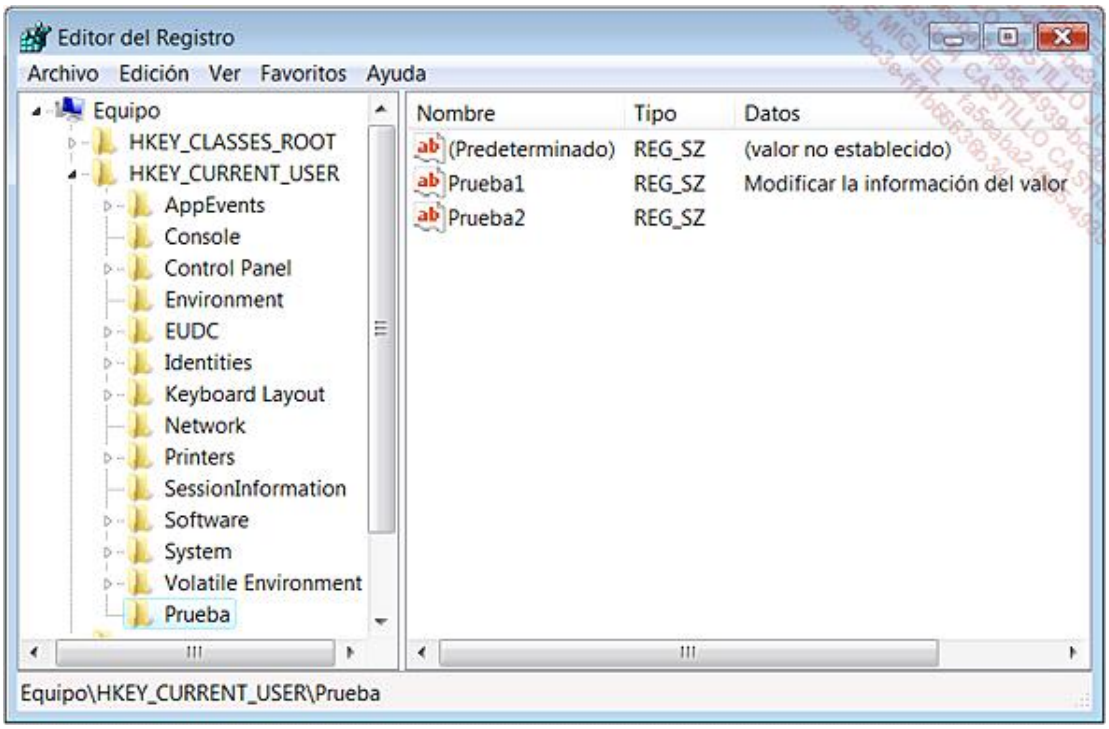
- En el apartado **Intervalo de exportación**, indique si desea exportar el registro completo o simplemente el árbol que ha seleccionado. Esta última posibilidad es mucho más razonable.
- Haga clic en **Guardar**.

Veamos ahora las ventajas e inconvenientes de estos dos métodos:

Un archivo de subárbol ocupa el doble que un archivo REG. Se trata de una imagen en formato binario del árbol que ha guardado. No puede exportar este archivo mediante el comando Regedit ni haciendo doble clic en el archivo de subárbol. Deberá hacer clic en **Archivo - Importar** y seleccionar el archivo de subárbol. Al contrario que un archivo *.reg*, se sobrescribirá el árbol existente y todo el contenido remplazará al archivo *.hiv*. En el caso de tratarse

de un archivo REG, se conservarán los valores antiguos. Si dos valores tienen el mismo nombre, sólo los datos del valor serán modificados si es preciso. Veamos un ejemplo práctico:

- En el Registro, abra esta rama: HKEY_CURRENT_USER.
- Cree una nueva clave llamada **Prueba**.
- Seleccione esta última clave y cree un valor de cadena llamado **prueba1**.
- Edite este valor e introduzca un texto cualquiera. Sólo es una prueba.
- Exporte la clave **Prueba** como un archivo de subárbol en el formato REG.
- Edite el nuevo valor **prueba1** y modifique su contenido.
- Cree ahora un segundo valor de cadena llamado **prueba2**.



- Abra el Explorador de Windows en la ubicación en la que haya guardado los archivos REG y de subárbol.
- Haga clic con el botón secundario del ratón en el archivo REG y en la opción **Combinar**.
- Confirme la combinación de los datos con los del Registro de Windows.

Después de actualizar la visualización del Registro pulsando la tecla [F5], podrá comprobar que:

- Los datos del valor prueba1 se han modificado correctamente.
- El valor test2 todavía está presente.

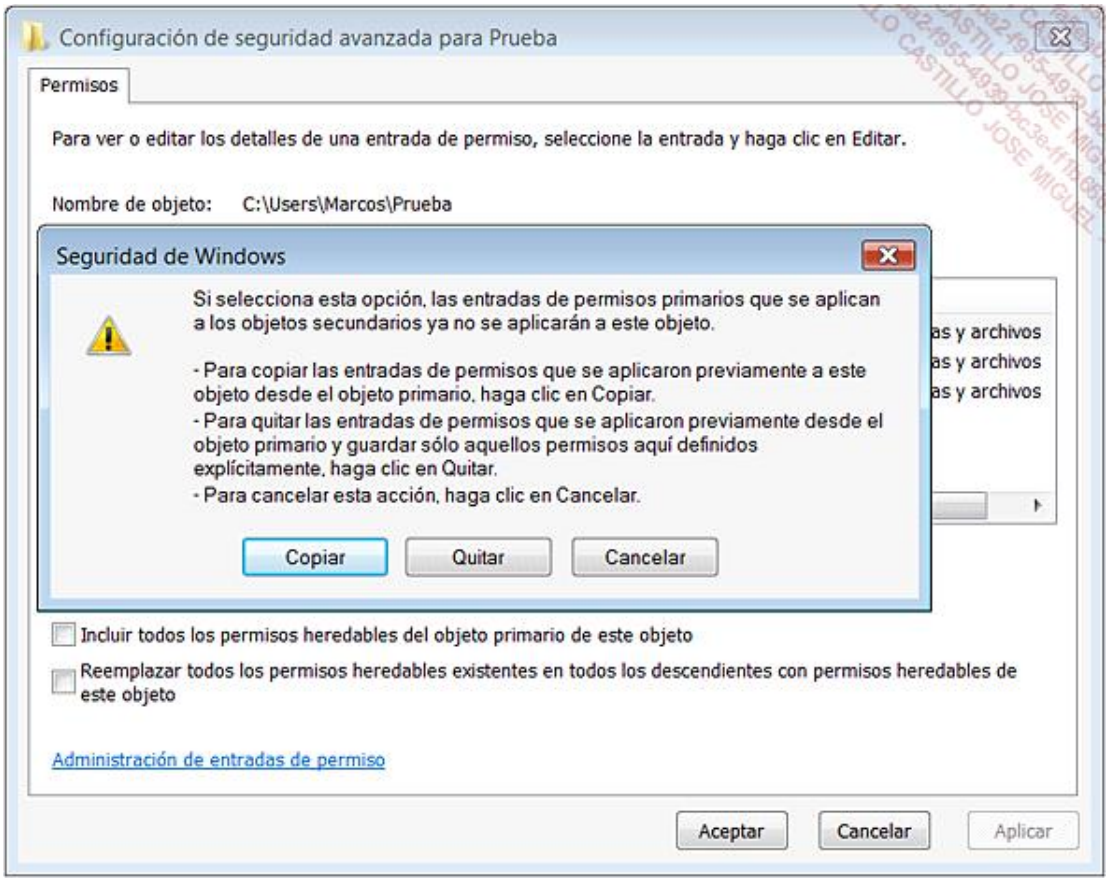
- En el Registro, haga clic en **Archivo - Importar** y seleccione el archivo de subárbol.
- En la lista desplegable situada en la parte inferior de la ventana, seleccione la opción **Archivos de subárbol de Registro (*.*)** y seleccione el archivo de subárbol.
- Haga clic en el botón **Abrir**.
- Confirme la sustitución de la clave.

El registro de Windows se actualizará inmediatamente y la clave prueba2 se eliminará correctamente.

Todo esto para decirle que si debe guardar claves de Registro antes de hacer una operación que le parece peligrosa, es preferible exportarlas en formato de subárbol y no en formato REG.

Hay una pregunta que nos viene a la mente (aunque es un poco pronto en este capítulo): si realizamos una modificación en los permisos de una clave de Registro, ¿es posible restaurar el conjunto de permisos NTFS? En estos casos llevaremos a cabo el mismo tipo de modificación:

- Haga clic con el botón secundario del ratón en la clave llamada **Prueba** y seleccione el submenú **Permisos**.
- Haga clic en el botón **Opciones avanzadas** y desmarque la casilla **Incluir todos los permisos heredables del objeto primario de este objeto**.
- Haga clic en los botones **Copiar** y **Aceptar**.



- En Windows 8, haga clic en el botón **Desactivar la herencia** y a continuación seleccione el vínculo **Convertir las autorizaciones heredadas en autorizaciones explícitas de este objeto**.
- Seleccione el nombre de usuario que aparece en la sección **Nombres de grupos o usuarios** y haga clic en los botones **Quitar** y **Aceptar**.

De esta manera, habremos:

- Desactivado el mecanismo de herencia de los permisos NTFS.
- Eliminado su cuenta de usuario de la lista de usuarios para los que se estableció una ACE.

- Con el botón secundario del ratón haga clic en el archivo de registro y, a continuación, en la opción **Combinar**.

Tenga en cuenta que también puede hacer doble clic en el archivo de registro.

Si accede otra vez al conjunto de permisos NTFS de la clave Prueba verá que la situación sigue siendo la misma.

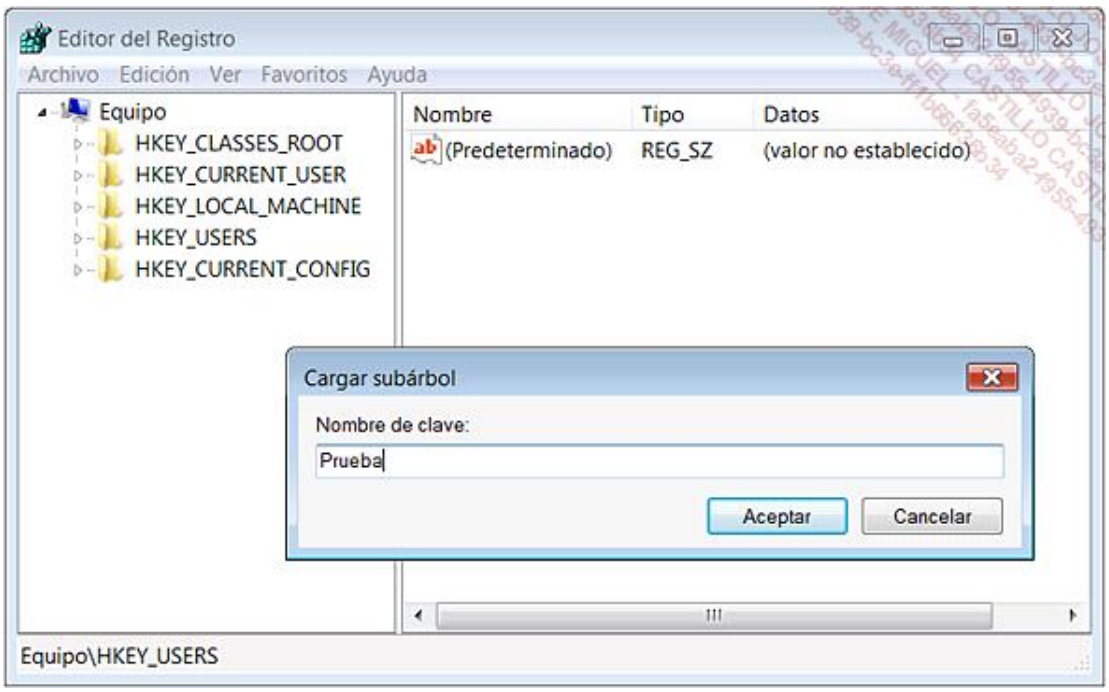
- Realice la misma modificación pero, esta vez, importe el archivo de subárbol.
- Abra otra vez la ventana de permisos de la clave **Prueba**. Esta vez, el mecanismo de herencia y el conjunto de permisos han sido restaurados.

La conclusión es irrefutable: si debe realizar modificaciones en el conjunto de permisos de una clave, elija como copia de seguridad un archivo de subárbol.

10. Editar el Registro Windows XP desde Windows 7

Si utiliza Dual-Boot, aquí le presentamos una manera sencilla de reparar el Registro del sistema operativo de Windows XP; tan sólo abra el Editor del Registro de Windows 7. También puede editar un Registro de XP desde el mismo tipo de sistema operativo instalado en otra partición. Lo mismo pasaría si tuviera varios sistemas de Windows 7.

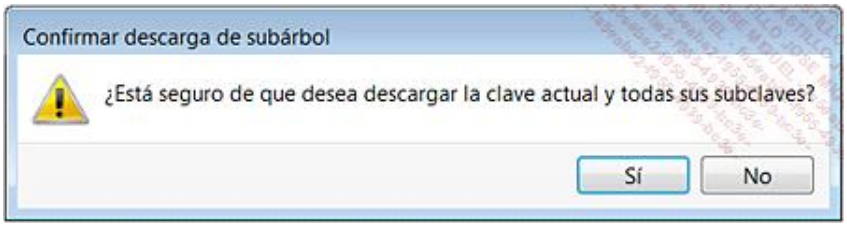
- Primero, active la visualización de los archivos y carpetas ocultas en el Explorador de Windows.
- Abra el Editor del Registro.
- Seleccione la clave HKEY_USERS.
- Haga clic en **Archivo - Cargar subárbol...**.
- Abra el directorio: \WINDOWS\system32\config.
- Seleccione el archivo de subárbol deseado, por ejemplo, *Software*. Estos archivos no tienen una extensión visible.
- En el cuadro de texto **Nombre de clave**, introduzca un nombre temporal para el archivo de subárbol. En nuestro ejemplo, **Prueba**.



- Abra HKEY_USERS\prueba.

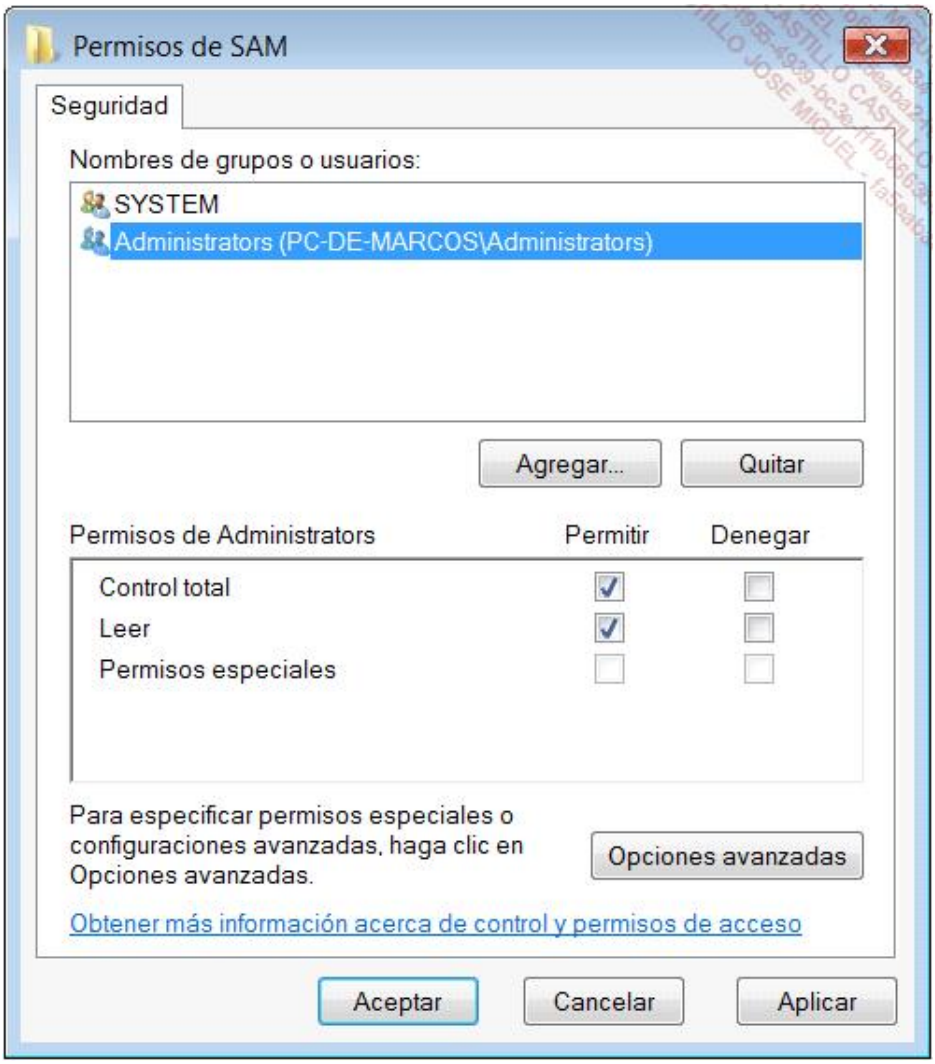
Continúe y despliegue, por ejemplo, este árbol: \Microsoft\Windows\CurrentVersion\policies\system.

- Realice las modificaciones deseadas.
- A continuación, seleccione la clave HKEY_USERS\prueba.
- Haga clic en **Archivo - Descargar subárbol**.
- Confirme la descarga del subárbol.



- Inicie en Windows XP para comprobar que los cambios se han realizado correctamente.

Si, por ejemplo, usted carga el archivo de subárbol SAM, bastará con que otorgue temporalmente el permiso Control total al grupo de administradores para tener un acceso completo a los subárboles de clave SAM.



No siempre es necesario, pero tenga cuidado de no olvidar copiar las autorizaciones especiales que posee el grupo

de administradores de esta clave.

¡Está claro que al contrario también es posible! Es evidente que la copia exacta de permiso resulta útil si un problema le impidiera acceder al Escritorio de Windows XP (o al revés).

11. Reparar un servicio utilizando las herramientas WinRE

Vamos a utilizar el mismo truco para editar el Registro de Windows 7. Esto supone que la opción **Última configuración válida conocida** no ha funcionado y no ha podido restaurar el ordenador a un estado anterior.

- Abra una ventana de Símbolo del sistema.
- Introduzca estos dos comandos y acepte después de cada uno con la tecla [Intro]:
  - **`\windows\inf\`**
  - **`notepad setupapi.app.log`**

Cada servicio y controlador de dispositivos se clasifica por fecha.

- Así pues, identifique el último controlador o servicio que haya instalado.
- A continuación, introduzca el siguiente comando: **`regedit`**.
- Cargue el subárbol SYSTEM que está accesible en esta ubicación: \Windows\System32\Config.
- Dele un nombre temporal y abra este árbol: Current\ControlSetxxx_Services.
- Acto seguido, localice la clave que el servicio o controlador han instalado.
- Edite un valor DWORD llamado **Start** e introduzca como información del valor la cifra 4.

Haga lo siguiente para desactivarlo:

- Libere el subárbol temporal y reinicie el ordenador.