1 Técnicas avanzadas en Windows XP. 1-2

1.1 El Registro del Sistema. 1-2

El Editor del Registro. 1-3
Claves del Editor del Registro 1-3
Editando el Registro. 1-4
Utilidad de la edición del Registro de Windows. 1-7
Modificación de un registro remoto. 1-8

1.2 Monitorizando el Sistema con el visor de Sucesos. 1-8

Auditando sucesos. 1-11

1.3 Servicios en Windows XP. 1-12

Configurando los servicios. 1-13

1 Técnicas avanzadas en Windows XP.

Windows XP es un sistema operativo altamente configurable y que cuenta con una gran cantidad de técnicas avanzadas normalmente no usadas por los usuarios genericos pero que como Administradores de Sistemas debemos conocer. Tratemos algunas de ellas.

1.1 El Registro del Sistema.

En las versiones anteriores a Windows 95, cada programa que se instalaba en el sistema (incluyendo los propios programas de Windows) contaba con una serie de ficheros donde se almacenaban las configuraciones de dichos programas. Estos ficheros solían tener la extensión .ini y se contaban por miles los que en un momento dado podían estar instalados. A partir de Windows 95, aunque no se prohibieron los ficheros .ini se ideo otra forma de trabajar. Se creó una base de datos jerárquica central donde se guardan todas las configuraciones de todos los programas, incluidas las configuraciones del sistema operativo. Esta base de datos es conocida como el Registro de Windows.

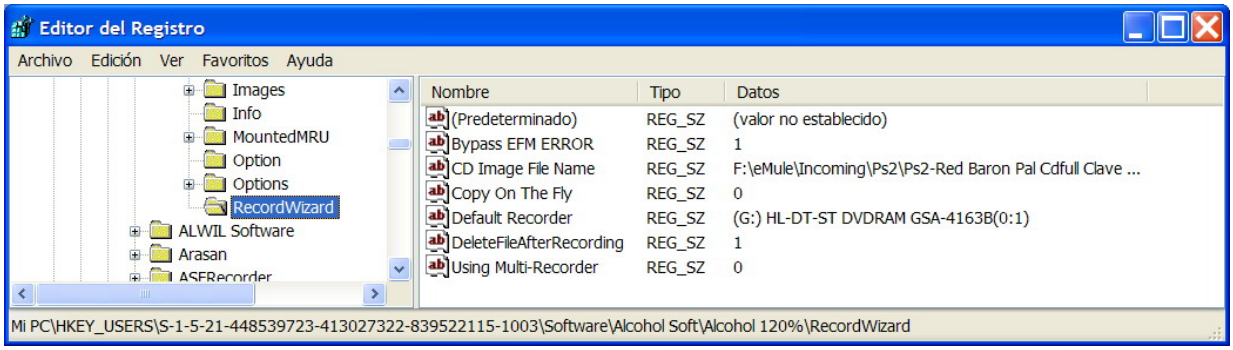
Cualquier opción que escojamos en el panel de control, en un menú de Word, una preferencia que escojamos en un juego que instalemos, cualquier directiva de grupo que activemos, etc., en realidad hace referencia a un cambio que se produce en una clave del Registro. Asimismo, existen miles de posibles configuraciones que no están a nuestro alcance usando medios normales, pero se pueden configurar desde el Registro.

Hay que tener mucho cuidado a la hora de editar el Registro. Es potencialmente posible destruir absolutamente todo nuestro sistema. Cualquier cambio que se realice, debe estar meditado con anterioridad, y nunca debe realizarse ningún cambio sin contar con una copia de seguridad actualizada del Registro. Tocar el registro viene a ser como tocar directamente las piezas del motor de un coche, nos da la máxima potencia posible a la hora de modificar el coche, pero si cometemos un error no hay marcha atrás, no hay ningún sistema que nos vigile para asegurarnos de que no metemos la pata.

El Editor del Registro.

El Editor del Registro (REGEDIT.EXE) es la herramienta que Microsoft pone a nuestra disposición en el sistema para editar el contenido del Registro. Ejecutad este programa y comprobad su aspecto, parecido al del explorador de archivos.

Las carpetas representan claves del Registro y se muestran en el área de exploración en el lado izquierdo de la ventana Editor del Registro. En el área de temas de la derecha, se muestran las entradas de una clave. Al hacer doble clic en una entrada, se abre un cuadro de diálogo de edición.



Como es obvio, esta herramienta de edición del registro sólo puede ser usada por usuarios avanzados de nuestro equipo, como todos los miembros del grupo Administradores.

Claves del Editor del Registro

El registro del sistema esta estructurado en forma arborescente (como los directorios de un volumen). En primer lugar tenemos las carpetas principales que cuelgan de la raíz del registro. Estas carpetas principales son:

Clave	Descripción
HKEY_CURRENT_USER	Información sobre el usuario actual.
HKEY_USERS	Información sobre todos los usuarios.
HKEY_LOCAL_MACHINE	Información sobre el equipo.
HKEY_CLASSES_ROOT	Información sobre las extensiones y sus asociaciones.
HKEY_CURRENT_CONFIG	Información sobre la configuración actual que se esta usando.

En cada una de estas carpetas, y en sus sucesivas subcarpetas o subdirectorios, podemos crear tanto carpetas en la parte izquierda, como entradas en la parte derecha. Estas entradas pueden ser variables de cuatro tipos distintos de datos.

Tipos de datos	Descripción
REG_BINARY	Datos binarios en formato hexadecimal.
REG_DWORD	Datos de doble palabra.

REG_EXPAND_SZ	Cadena de texto de longitud variable.
REG_MULTI_SZ	Lista o array separados por espacios.
REG_SZ	Cadena de texto de longitud fija.
REG_FULL_RESOURCE_DESCRIPTOR	Tablas anidadas.

Normalmente, cuando tengamos que crear una entrada para realizar algo, se nos indicara de qué tipo tiene que ser.

Editando el Registro.

Al editar el registro hay que tener en cuenta una serie de cuestiones

1) Cualquier cambio que se realice en el registro, se aplicará de inmediato y no existe ninguna función deshacer. Es decir, no existe ninguna forma automática de dar marcha atrás.
2) Cualquier cosa que se borre en el registro, se borra automáticamente. El registro no espera a que pulsemos Guardar (save) para guardar el registro en disco, los cambios se guardan automáticamente.

Una forma relativamente segura de editar el registro, consiste es realizar una copia de seguridad antes de modificar nada, de forma que si deseamos volver atrás, siempre podamos cargar la copia de seguridad. En el menú Archivo del programa Regedit, tenemos la opción Exportar que nos permite grabar todo el Registro, o simplemente una porción del mismo.

Es conveniente exportar a un sitio seguro la rama del registro que vamos a modificar, de modo que siempre podamos restaurarla en caso de necesidad desde el menú Archivo con la opción Importar. Hay que tener en cuenta una cosa a la hora de importar y exportar partes del registro. Si exportamos un archivo .reg (archivo de registro) realizamos una copia parcial únicamente, de modo que si exportamos, añadimos una clave nueva al registro, y luego importamos, nuestra clave nueva seguirá existiendo. Sin embargo, un archivo de subárbol realiza una copia total, de modo que si exportamos, añadimos una clave nueva al registro, y luego importamos, veremos como nuestra nueva clave desaparece dejando el registro tal y como estaba a la hora de realizar la exportación.

Mientras que los archivos .reg se guardan en modo texto, y por lo tanto son editables, los archivos de subárbol se guardan en formato especial, y no pueden ser editados ni visualizados por métodos normales.

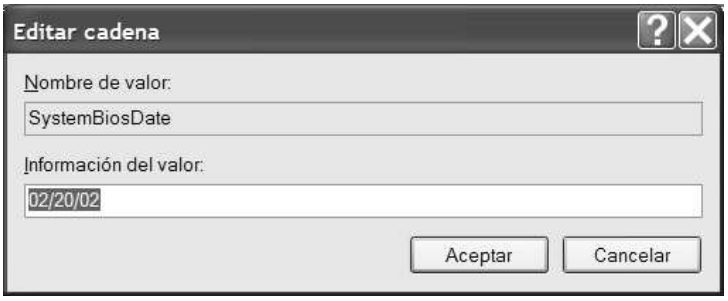
Windows XP presenta un comportamiento anómalo cuando se importan subárboles grandes, llegando a presentar problemas de memoria baja e incluso llegando a corromper partes del registro. Se recomienda no utilizar subárboles siempre que sea posible.

Para mayor seguridad, también podemos crear un punto de restauración del sistema en Windows XP, lo que nos asegura que en el peor de los casos siempre podremos volver al punto anterior a la modificación del registro, es el metodo recomendado para modificar el registro. (Creamos un punto de restauración, modificamos el registro, si algo falla restauramos).

El tamaño del Registro es considerable, por lo que el programa Regedit cuenta con una serie de comandos para facilitarnos la tarea de manejar el registro. El comando Buscar, que se encuentra en el menú Edición nos permite localizar un valor concreto dentro de registro, Buscar siguiente nos

permite ir navegando entre los distintos valores encontrados. También cuenta con una opción de Favoritos, como la de Internet Explorer para almacenar accesos a las ramas y valores a los que solemos acceder.

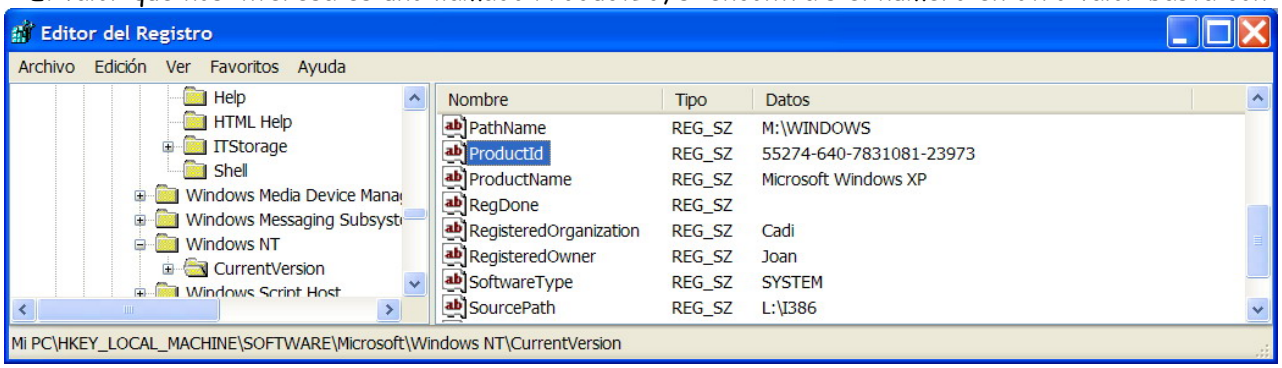
Para cambiar el valor de una clave del registro, normalmente solo tenemos que hacer doble clic sobre dicha clave (en el panel de la derecha) lo que nos mostrará un formulario donde podremos indicar el nuevo valor.



Vamos a realizar un pequeño ejercicio para comprobar como encontramos y modificamos un valor. Si vamos al formulario propiedades del sistema (botón derecho – propiedades sobre el icono de Mi PC ó bien Tecla Windows + Pause) veremos como aparece "Registrado a nombre de" y el nombre del usuario que ha registrado la copia de Windows XP. Este dato se pidió en el momento de la instalación, y no es posible cambiarlo.

Sin embargo, esta información esta almacenada como no podía ser de otra forma en el Registro. Abrid el editor de registro (Regedit.Exe) y en el menú edición escoged la opción Buscar (Control – B). Como buscar el nombre que aparece en Registrado puede ser complicado ya que puede aparecer multitud de veces, vamos a buscar el número que aparece debajo del nombre en propiedades de Mi PC. Para ello introducir el número en buscar, y marcar que busque sólo en Datos.

El valor que nos interesa es uno llamado ProductId, si encontráis el número en otro valor basta con



que indiquéis "Seguir Buscando" o pulséis la tecla F3 para que busquéis la próxima vez que aparece el valor.

En la misma carpeta (clave) en que encontramos ProductId veremos que aparecen dos valores RegisteredOwner y RegisteredOrganization. Estos son los campos donde se guardan los textos que vemos en propiedades de Mi PC. Cambiad estos valores por otros cualesquiera. Cerrad la ventana de propiedades de Mi PC si es que la tenéis abierta, y volver a abrirla. Mirad si ha cambiado algo.

Comprobareis como cualquier cambio que se hace en el registro es automáticamente ejecutado por el sistema, sin tener siquiera que cerrar el editor del registro. Esto hace que tengamos que andar con pies de plomo a la hora de modificar valores en el registro.

Si miramos en el registro ese valor que hemos modificado, el de RegisteredOwner, veremos como existe una ruta para llegar a ese valor, al igual que existe una ruta para llegar a un archivo. En concreto, la ruta completa de RegisteredOwner es:

```
Mi PC\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
```

Comprobad como al hacer click derecho sobre una entrada del registro, el sistema nos da las opciones para eliminar una entrada, y como también podemos crear entradas nuevas en el registro dentro de cualquier clave.

Bien, ahora veamos como exportar ramas. Volved a colocaros en dicha rama, sino estáis ya allí, y en el menú Archivo del editor del registro, escoged la opción Exportar. Marcad en la zona inferior del formulario de grabación Rama Seleccionada, y aseguraros de que la rama es la que hemos indicado arriba. (No importa que no comience con Mi PC). Ponerle un nombre al fichero .reg que se va a grabar y guardarlo en cualquier directorio. Abrid ahora dicho fichero .reg con el block de notas, y comprobad su contenido.

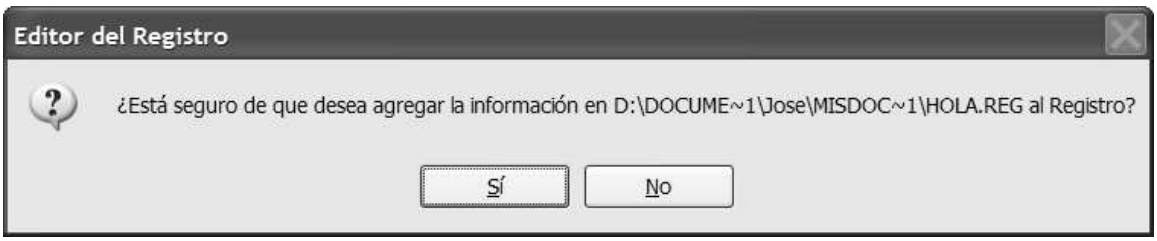
El archivo resultante es bastante grande, ya que esta rama que hemos exportado contiene mucha información, sin embargo lo que a nosotros nos interesa se encuentra al principio de dicho fichero, que será algo parecido a:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]
"CurrentBuild"="1.511.1 () (Obsolete data - do not use)"
"InstallDate"=dword:3c6674ea
"ProductName"="Microsoft Windows XP"
"RegDone"=""
"RegisteredOrganization"="Luna"
"RegisteredOwner"="Luis Enrique"
```

Vemos como es una estructura típica de un archivo de registro en Windows. Vamos a realizar nuestro propio archivo de registro. Para ello, cread con el block de notas un fichero con nombre HOLA.REG y el siguiente contenido.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]
"RegisteredOwner"="ERNESTO MATE"
```

En dicho fichero como veis, indicamos simplemente la versión que usamos (5.0) la ruta completa donde quiero trabajar y el valor que le quiero dar a la entrada. Una vez grabado dicho fichero con el contenido arriba indicado (contenido exacto), haced doble click sobre dicho fichero HOLA.REG. Veremos como Windows nos pide confirmación para insertar la información del fichero HOLA.REG en el registro.



Confirmar que se agregue HOLA.REG al registro. Ahora, pulsad Tecla Windows + Pause para ver que ha ocurrido con el usuario registrado del sistema.

Este es un método muy simple de modificar valores del registro. Basta escribir un fichero con la cabecera arriba indicada, escribir la ruta completa del valor a modificar entre corchetes, y posteriormente, y entre comillas la entrada a cambiar y el valor al que se va a cambiar.

Una ultima cosa, las claves del registro (en el panel izquierdo) tienen también permisos para usuarios, al igual que las carpetas. Dando botón derecho sobre una clave, y escogiendo la opción permisos podremos indicar que usuarios de nuestro sistema tienen derecho a modificar dicha clave (pensad en esto, si existe una clave que indica el nombre del fondo de pantalla, por ejemplo, y quitamos permisos a todos los usuarios menos al Administrador para modificar esta clave…..).

Utilidad de la edición del Registro de Windows.

Hemos visto (por encima) como se puede editar el registro y en que consiste. ¿Es esto realmente útil?

Existen infinidad de configuraciones en un entorno Windows, a muchas de ellas podremos acceder desde las directivas de grupo o desde las propias opciones de configuración que nos dan los programas, pero a muchas otras es imposible acceder desde otro sitio que no sea desde el propio registro. Un usuario avanzado de informática, debe conocer como editar el Registro, ya que tarde o temprano se verá forzado a "bajar" al nivel de registro para solucionar determinadas cosas.

Por ejemplo, podemos configurar XP para que nos muestre un mensaje cada vez que iniciamos Windows. Para ello habrá que modificar los valores de legalnoticecaption y legalnoticetext en la clave:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon]
```

Otro ejemplo, sabemos que la cuenta Administrador no aparece en la pantalla de bienvenida de usuario. Si queremos que aparezca, basta que creemos (o modifiquemos si existe) una entrada del tipo DWord con el nombre Administrador y con valor 1 en:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]
```

También es bastante interesante explorar las claves HKEY_LOCAL_MACHINE\SOFTWARE\ y HKEY_CURRENT_USER\SOFTWARE donde veremos una lista de todo el software que tenemos instalado en la maquina. Incluido el software "oculto" que no se muestra en ningún otro sitio de Windows. Un usuario avanzado debe consultar esta lista para comprobar que se ha instalado en la maquina, muchas veces sin pedir permiso (programas que se instalan junto con otros programas a modo de troyanos).

Puede ocurrir, por ejemplo, que veamos que en esta lista de software aparece una clave con el valor Cydoor (conocido troyano "legal" que espía la información que esta en nuestra maquina y la envía a Internet, incluyendo contraseñas, páginas visitadas, números de serie, etc.). En general, cualquier clave que encontremos aquí que nos parezca extraña debe ser estudiada cuidadosamente.

En Internet podéis encontrar cientos de "trucos" que pueden realizarse desde el registro. Hay que tener mucho cuidado con estos "trucos", pues muchos de ellos, amen de no servir absolutamente para nada, pueden tener efectos negativos.

Imaginemos que en un equipo instalamos un juego (podría ser cualquier otra aplicación). Este juego se instala en un directorio de nuestro disco duro, y como no necesita el cd para funcionar, perdemos dicho cd. ¿Es posible en estas circunstancias copiar el juego a otro ordenador?. En la mayoría de las ocasiones, esto es imposible puesto que al instalar el juego en realidad estamos instalando dos cosas

en el sistema: El juego en si en un directorio (que podemos copiar a otro ordenador), y una serie de líneas, valores y claves en el registro, que no podremos copiar directamente. Pero ahora que sabemos como exportar e importar ramas del registro, no tendríamos problemas en realizar esta copia.

Como ejercicio: en el registro existen varias ramas desde donde se puede indicar que se ejecuten programas en el inicio de Windows XP. Buscar desde que posiciones del registro se puede hacer esto. (Anteriormente vimos algunas utilidades que nos permitían ver que aplicaciones se ejecutaban en el inicio). Una vez encontradas dichas ramas, introducir una nueva entrada para ejecutar un programa cualquiera en el inicio de Windows XP.

Modificación de un registro remoto.

Podemos modificar el registro de otro ordenador, por ejemplo, para repararlo o hacerle algún tipo de mantenimiento. Es parecido a la administración remota de otra equipo que hacemos desde Administración de equipos, aunque podemos perfilar algo más la administración directamente desde el registro.

Para ello, veremos que en el programa Regedit.exe tenemos una opción en el menú para conectar a un registro de red. Solo podemos modificar las ramas HKEY_USERS y HKEY_LOCAL_MACHINE remotamente, que suelen ser las más interesantes.

Imaginemos que queremos cambiar el fondo de pantalla que esta usando un usuario, su combinación de colores, el salvapantallas que usa o cualquier otro aspecto que no podemos modificar directamente desde Administración de Equipos. Esto lo podemos modificar tocando la rama de HKEY_USERS que se refiere al usuario al que deseamos modificar. (Para que esta rama exista realmente, el usuario debe tener abierta sesión en el equipo a controlar remotamente). Estos cambios no se producirán automáticamente, y solo serán llevados a cabo cuando el usuario del equipo remoto cierre la sesión actual y abra una nueva.

1.2 Monitorizando el Sistema con el visor de Sucesos.

Un suceso es cualquier incidencia que se produce en un sistema, que puede ser potencialmente interesante para un administrador.

Windows XP permite llevar un registro de los sucesos que se producen en el sistema. Estos registros son almacenados automáticamente en tres ficheros:

- Seguridad (Secevent.evt),
- Aplicación (Appevent.evt)
- Sistema (Sysevent.evt).

El visor de sucesos, es un añadido de consola que se instala conjuntamente con el Windows XP y que nos permite visualizar estos tres archivos.

Los sucesos se dividen en categorías o tipos, y estos pueden ser:

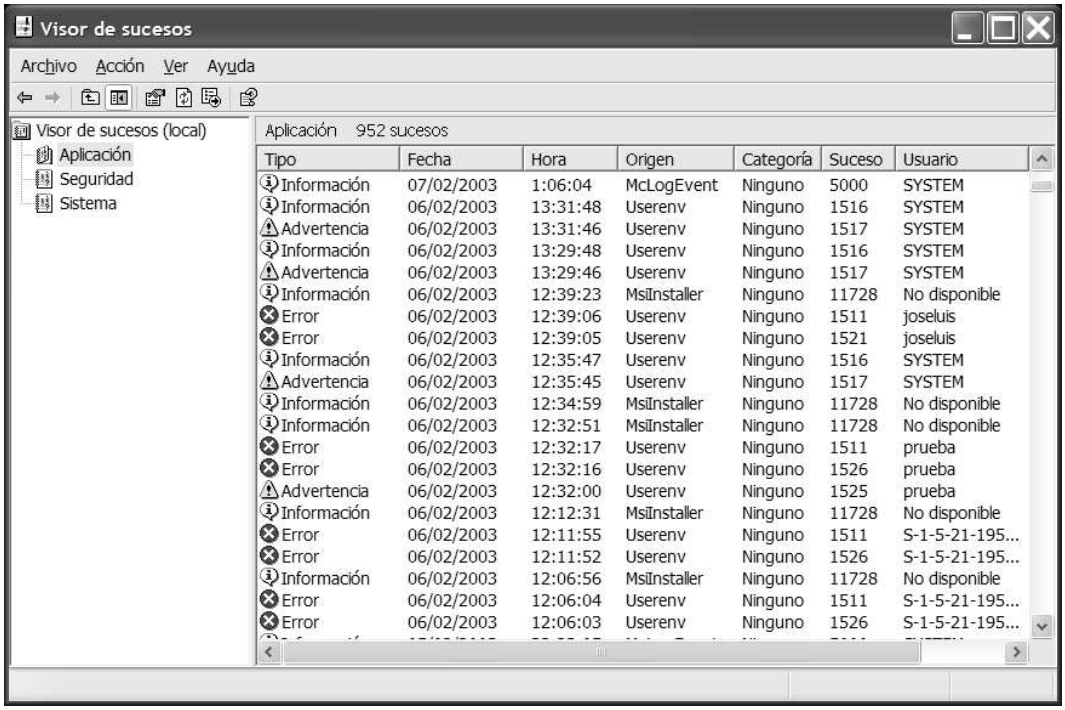
- Error.- Representan posibles perdidas de datos o rendimiento.
- Advertencia.- Posibilidad de que se produzca un error en un futuro.

- Información.- Informan de un tipo de actividad, y pueden ser configurables

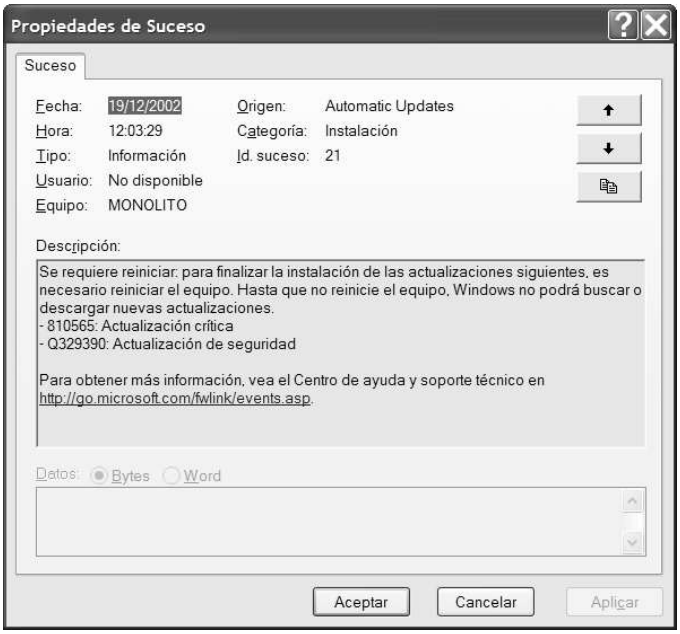
Para ejecutar el Visor de Sucesos, podemos ir Herramientas Administrativas – Visor de Sucesos o directamente ejecutar la consola mediante la orden eventvwr.msc.

Las 8 columnas que podemos ver por cada suceso son:

- Tipo. Indica si es Información, Advertencia o Error.
- Fecha. Indica la fecha en que se produjo el suceso.
- Hora. Indica la hora en que se produjo el suceso.
- Origen. La aplicación o componente del sistema que genero dicho suceso.
- Categoría. Algunos sucesos pertenecen a alguna categoría especial. La mayoría de los sucesos no pertenecen a ninguna categoría especial.
- Suceso. Todos los sucesos son identificados mediante un valor numérico. Este valor corresponde a la descripción del suceso.
- Usuario. La cuenta de usuario asociada con cada suceso. No todos los sucesos están asociados con una cuenta de usuario particular. Muchos sucesos, especialmente los de sistema, no son generados por ningún usuario. Estos sucesos muestran en esta columna No disponible.
- Equipo. El equipo donde ocurrió el suceso.



Al hacer doble clic sobre un suceso, veremos una información detallada del mismo. También podemos acceder a esta información pulsando la tecla Enter o desde el menú del visor de sucesos.



Podemos gestionar algunas configuraciones sobre estos tres archivos de sucesos, como el tamaño máximo que queremos que tengan, o establecer un tiempo de caducidad. Para ello, hay que dar botón derecho sobre Aplicación, Seguridad o Sistema en el panel de la izquierda y escoger la opción Propiedades del menú contextual que aparecerá. Desde aquí, también podemos realizar otras opciones como filtrar los sucesos o borrar los archivos.

Desde estas propiedades también indicaremos al sistema la forma en la que queremos que se comporte cuando los registros lleguen a su tamaño máximo permitido. Hay que tener mucho cuidado con esta opción, ya que si estos archivos llegan a su tamaño máximo y le indicamos al sistema que no puede borrarlos, el sistema no permitirá que inicie sesión ningún usuario en nuestro sistema, a excepción del Administrador.

Auditando sucesos.

Hemos visto anteriormente como podemos ver los sucesos que se producen en el sistema, pero la principal utilidad del visor de sucesos es la de auditar nuestros propios sucesos. Existe la posibilidad de añadir a esas listas de auditoria, una serie de sucesos que nosotros establezcamos. Esto se conoce como establecer auditorias sobre dispositivos.

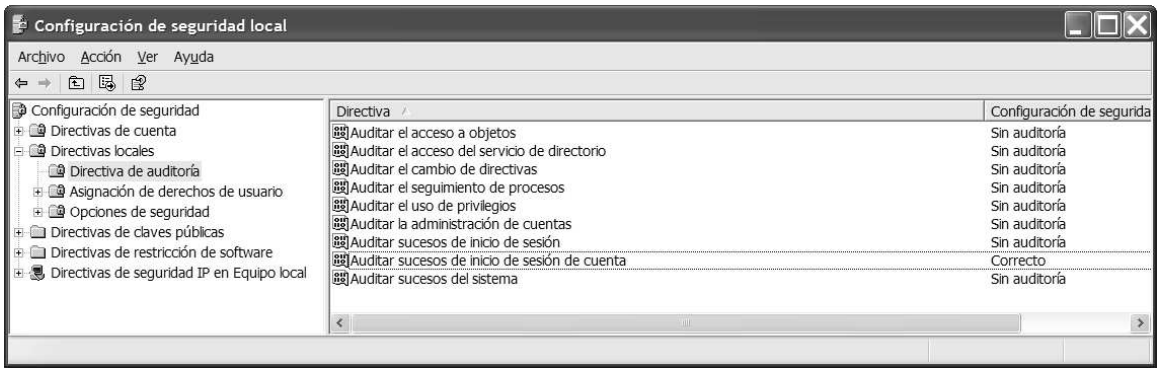
Habremos comprobado anteriormente, que el archivo de sucesos seguridad no tiene ninguna entrada. Este archivo se reserva para las auditorias que nosotros establezcamos. Para comenzar a utilizar estas auditorias de seguridad:

Nos vamos a Herramientas Administrativas – Directivas de seguridad local. (SECPOL.MSC).

Nos vamos a Directivas Locales – Directivas de Auditoria.

Aquí veremos los posibles sucesos que podemos auditar. Por cada suceso, podemos habilitar que se auditen tanto los intentos correctos como los erróneos.

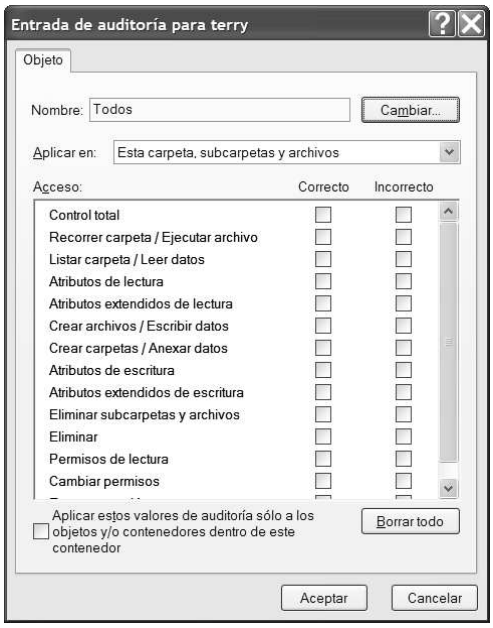
Por ejemplo, para que nuestro sistema audite los inicios de sesión basta que activemos desde SECPOL.MSC – Directivas locales – Directivas de Auditorias – Auditar sucesos de inicio de sesión de cuenta – Correctos. De este modo, cada vez que un usuario inicie sesión en nuestro sistema se crearán varios sucesos en el registro de seguridad de sucesos. (Si marcamos ambos sucesos, los erróneos y los correctos, es normal que se nos produzcan en muchas ocasiones ambos).



La opción que nos aparece en la configuración de seguridad local sobre el acceso a objetos, nos va a permitir auditar el acceso a cualquier objeto del sistema que deseemos. Para comprobarlo, activar dicha opción (Auditar el acceso a objetos – Correcto) en la configuración de seguridad local.

Ahora, creamos una carpeta con nombre VIGILAR por ejemplo, en el systemdrive. Si accedemos a las propiedades de dicha carpeta, pestaña Seguridad – Opciones Avanzadas, (el mismo sitio desde donde cambiábamos la herencia de los objetos) veremos que también tenemos aquí una pestaña Auditoria. En dicha opción de auditoria, podemos indicar si queremos auditar el acceso a este recurso u objeto, e incluso indicar a que usuarios queremos auditar. Para nuestro ejemplo, vamos a insertar en la lista de usuarios de la Auditoria de la carpeta VIGILAR al meta grupo TODOS. (Con lo que auditaremos los accesos a dicha carpeta para todos los usuarios de nuestro sistema).

Cuando hagamos esto, veremos que nos aparece un nuevo formulario, en el que podemos indicar que tipo de acceso queremos auditar para el usuario TODOS en la carpeta VIGILAR.



De este modo, podemos auditar sobre un objeto, los intentos de cambiar sus permisos, de tomar posesión de la misma, de crear carpetas dentro, etc.

Para nuestro ejemplo, vamos a auditar los intentos (tanto correctos como incorrectos) de recorrer carpeta y listar carpeta.

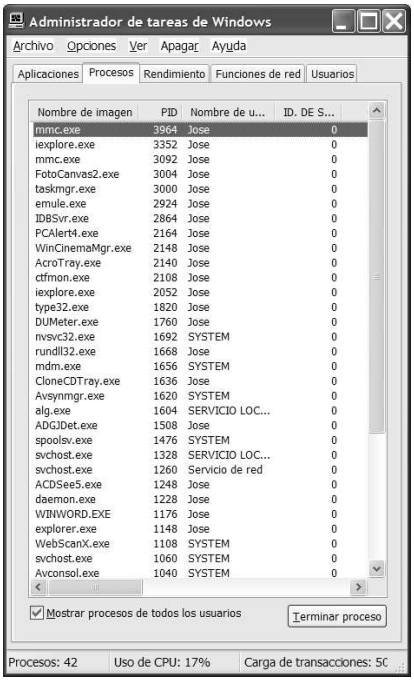
Si ahora nos vamos a el visor de sucesos y miramos en su apartado seguridad, veremos como aparecen varios accesos a la carpeta VIGILAR, indicando que nosotros mismos estamos accediendo a dicha carpeta. Si dejamos la carpeta abierta en una ventana del explorador, veremos además como estamos generando sucesos continuos, pues el explorador relee la carpeta cada pocos segundos.

Esto nos indica que tenemos que tener mucho cuidado a la hora de auditar sucesos, pues es muy fácil que acabemos con una cantidad tal de sucesos auditados que sea casi imposible buscar el que realmente queremos ver. Por suerte, tenemos en el visor de sucesos, en sus menús, la opción de buscar un suceso determinado por varios campos.

Vamos a perfilar la auditoria de esta carpeta VIGILAR. Cambiar su auditoria, de tal modo que audite sólo los intentos de acceso de un usuario de vuestro sistema. Abrid sesión como dicho usuario, intentad acceded a la carpeta, y comprobar como se crea el registro de sucesos adecuado.

1.3 Servicios en Windows XP.

Un servicio es un programa especializado que normalmente desarrolla una función de soporte para otros programas y que corre en segundo plano o Background. Muchos servicios operan a niveles muy bajos (interactuando directamente con el hardware, por ejemplo); por esta razón, suelen ejecutarse directamente por la cuenta de Sistema (una cuenta automática que usa nuestro sistema para ejecutar aplicaciones con privilegios totales), en lugar de ejecutarse desde la cuenta de un usuario particular. Existen muchos servicios que se ejecutan en Windows XP, veamos como podemos verlos, iniciarlos, pararlos, añadir servicios y en general, configurarlos.

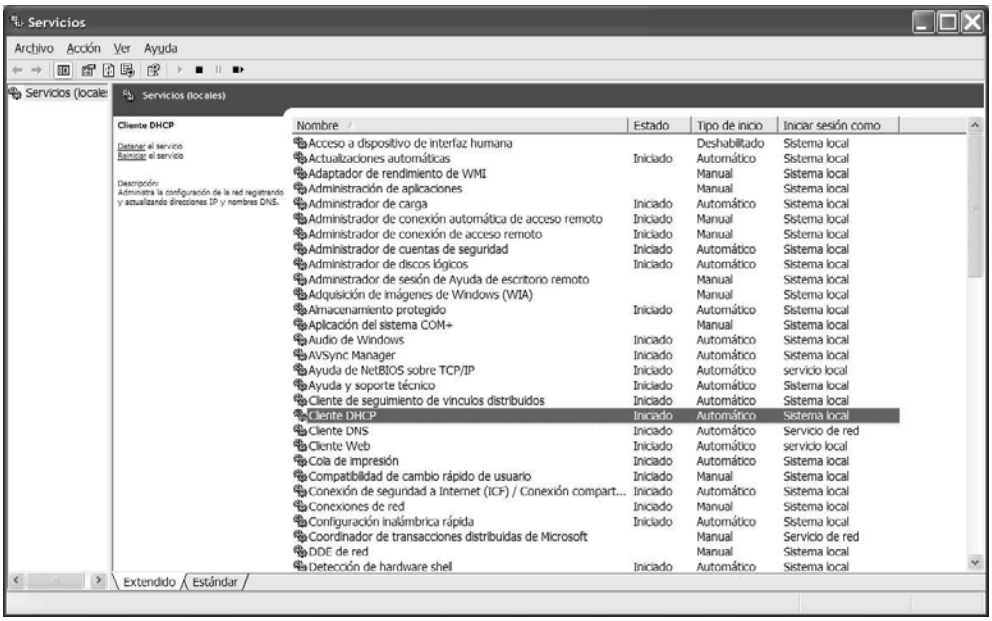


De momento, si pulsamos Control – Alt. – Suprimir (para acceder al Administrador de Tareas) y accedemos a los procesos que actualmente están corriendo en nuestro sistema, veremos como se están ejecutando gran cantidad de ellos. La mayoría de dichos procesos son servicios, que XP pone en marcha al iniciar el sistema y solo detiene cuando vayamos a apagar el sistema.

Para gestionar los servicios, usamos la consola services.msc (como siempre, podemos ejecutar directamente la consola, o llegar a ella desde Herramientas Administrativas – Servicios.

Esta consola de servicios, ofrece mucha información sobre cada uno de los servicios que actualmente se están usando. Desde esta consola podemos parar, iniciar, detener y reiniciar cualquier servicio. Para ello, basta con dar botón derecho sobre un servicio y escoger la opción deseada desde el menú contextual que aparece.

La mayoría de los servicios son iniciados automáticamente cuando iniciamos el sistema (aunque ningún usuario haya iniciado sesión), y son parados cuando le indicamos al sistema que se cierre. Sin embargo, algunas veces nos podemos ver forzados a parar o iniciar manualmente algún servicio. No todos los servicios permiten que los iniciemos o paremos manualmente, esto suele ser debido a que existen servicios que dependen de otros servicios.



Otra manera de iniciar o detener un servicio, es utilizar los comandos NET START y NET STOP desde el símbolo de sistema. El modo de usar estos comandos es NET START/STOP nombre del servicio.

Configurando los servicios.

Para revisar o modificar la forma en que un servicio se inicia, o que sucede cuando no funciona correctamente, podemos acceder a las propiedades de dicho servicio. (Doble clic sobre el servicio en la consola de servicios).

Desde este formulario, podemos modificar una gran variedad de aspectos sobre dichos servicio. En la pestaña general del formulario, podemos especificar las opciones de inicio del servicio. La más interesante es la que se refiere al tipo de inicio. Las opciones son:

- Automático. El servicio se inicia conjuntamente con el sistema.
- Manual. El servicio no se inicia hasta que nosotros (usuario) se lo indiquemos.
- Deshabilitado. El servicio nunca será iniciado.

Desde la pestaña Iniciar sesión, podemos indicar que el servicio se inicie desde una cuenta de usuario y no desde la cuenta del sistema. En caso de usar esta opción, debemos asegurarnos de que el usuario indicado tiene derecho para iniciar dicho servicio.

Desde la pestaña recuperación, podemos indicar que queremos que se realice si dicho servicio deja de funcionar. (Que re reinicie automáticamente el servicio, que se reinicie todo el sistema, que lo deshabilite, que se ejecute un programa determinado, etc.).

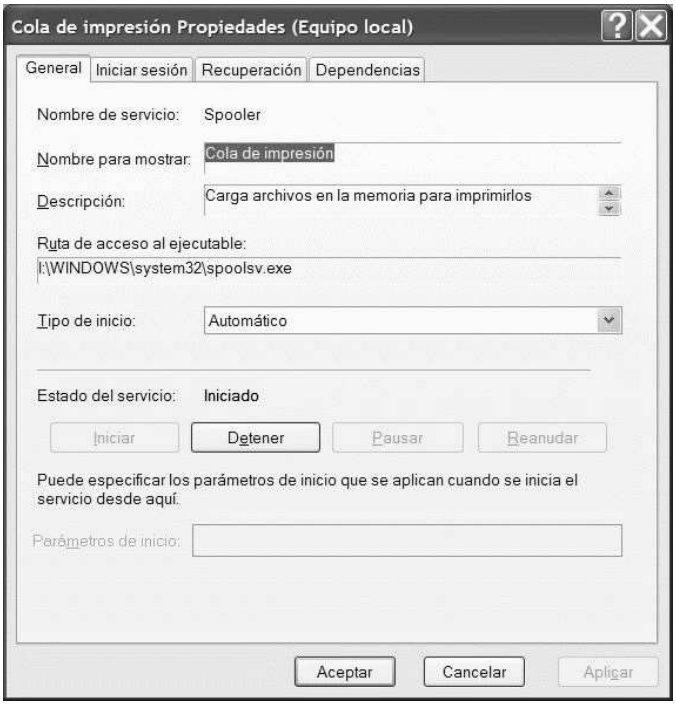
La ultima pestaña, de Dependencias, nos indica si este servicio depende de otro, de modo que podamos ver la jerarquía de servicios, y sepamos que ocurrirá si paramos dicho servicio.

Hay que tener en cuenta, que los nombres de servicios que vemos desde esta consola, no se corresponden normalmente con los nombres de los servicios que vemos desde el administrador de tareas de Windows (pulsando Control – Alt. – Suprimir). Así, veremos en el administrador de tareas que existe un Proceso en funcionamiento denominado SVCHOST.EXE. Este proceso en realidad es el servicio de alerta, como podemos comprobar si hacemos clic sobre dicho servicio y vemos la ruta de ejecución del mismo, que hace referencia al programa SVCHOST.EXE. (Veremos en varios servicios, como todos ellos utilizan el servicio SVCHOST.EXE como servidor (host) para ejecutarse).

También podemos gestionar los servicios desde el símbolo del sistema, mediante las órdenes NET START, NET STOP, NET PAUSE y NET CONTINUE.

Como ejemplo, para que la orden NET SEND mensaje funcione, debemos tener activo el servicio MENSAJERO. Podemos activar dicho servicio desde la consola de servicios o directamente con la orden NET START MENSAJERO. De igual modo, podemos pararlo desde la consola o con NET STOP MENSAJERO. (Probad como funciona dicho NET SEND) ;-)

Hay que tener en cuenta que si dicho servicio lo dejamos en manual, tendremos que iniciarlo siempre cada vez que iniciemos sesión en la maquina. Sin embargo, si lo dejamos en automático, el servicio siempre estará activo, aunque no haya ningún usuario usando nuestra maquina mediante una sesión abierta.



Existen determinados programas, como puede el ICS (Conexión compartida a Internet) que corren como servicios automáticos. Esto permite, que baste con encender nuestro equipo para que dichos programas funcionen, sin que sea necesario que abramos ninguna sesión en la maquina. Esto es una ventaja de Windows 2000 sobre otros sistemas como Windows 98, donde no se ejecuta ningún programa hasta que no comencemos a utilizar directamente el sistema.

Hay que tener mucho cuidado al parar servicios, ya que muchos de ellos son imprescindibles para el funcionamiento del sistema. Sin embargo, en muchos casos es conveniente parar sistemas que sepamos que no son imprescindibles, bien para ganar rendimiento o para solucionar problemas.

Por ejemplo, si tenemos una cola de impresión que se niega a vaciarse, podemos parar un momento el servicio de cola de impresión, para iniciarlo posteriormente, con lo que vaciaremos toda la cola de impresión.

Como hemos visto en este tema, un servicio presenta muchas ventajas sobre un programa normal.

- Se inicia automáticamente en cuanto que se enciende el sistema, sin necesidad de iniciar sesión con ninguna cuenta.
- Podemos indicar que se ponga en marcha de nuevo si surge algún problema y se para, recuperando dicho servicio.
- Siempre se va a ejecutar si lo ponemos en Automático.

De este modo, podría ser ventajoso poder transformar un programa normal y corriente en un servicio. Ahora bien, podemos comprender fácilmente que solo determinado tipo de programas puede ser convertido en un servicio; aquellos que no necesitan interactividad con el operario, puesto que un servicio se va a ejecutar en segundo plano, y no puede emitir formularios por pantalla.

Desgraciadamente, Microsoft no incluye en su sistema operativo directamente ninguna utilidad que nos permita realizar esta conversión, sin embargo, la propia Microsoft si incluye dicha utilidad (srvany) "Kit de recursos de Windows 2000". También necesitamos para este fin la utilidad instsrv que nos permite instalar un servicio mediante srvany.

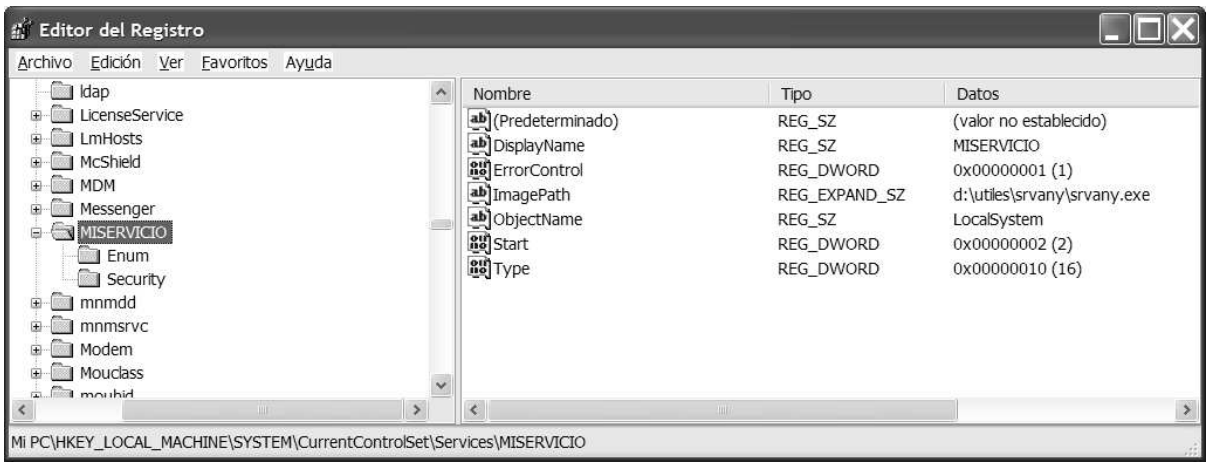
Para ello, copiamos en un directorio (por ejemplo C:\SERV) los archivos necesarios, que podemos bajarnos directamente de Internet realizando una búsqueda sobre srvany download. Estos archivos son: srvany.exe, srvany.wri e instsrv.exe.

Desde un símbolo de comandos, nos vamos al directorio anterior (C:\SERV) y escribimos la orden

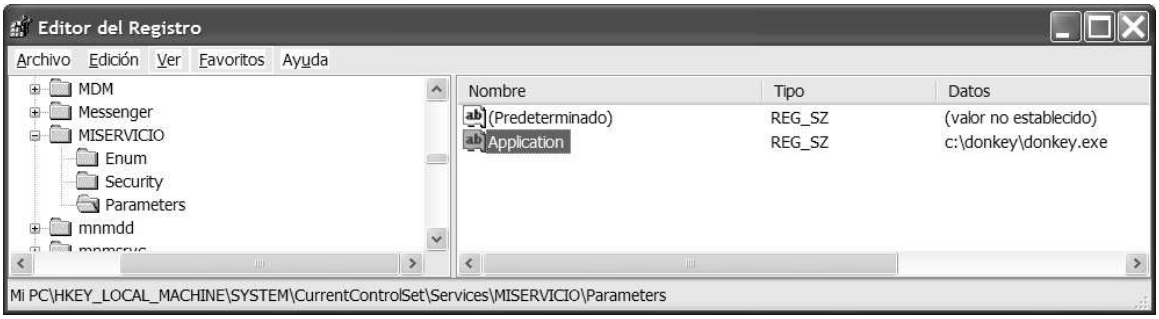
```
INSTSRV MISERVICIO  C:\SERV\SRVANY.EXE
```

Con esto, hemos creado un nuevo servicio, con el nombre que le hayamos indicado (MISERVICIO en este ejemplo, pero puede ser cualquiera) para comprobarlo, ejecutamos la consola services.msc y veremos como efectivamente se ha creado un servicio con el nombre que le hayamos dado. Desde aquí, podemos indicar el tipo de inicio que deseamos para nuestro servicio, la cuenta a la que vamos a asociarlo, etc.

Bien, ahora tenemos que indicar a dicho servicio que es programa es el que queremos que se ejecute como servicio. Para ello, nos vamos al editor del registro del sistema (Regedit) y nos vamos a la ruta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services y veremos como se ha creado una carpeta con el nombre que le hayamos dado al servicio.



Bajo esta carpeta MISERVICIO, tenemos que crear una clave con nombres Parameters, y en dicha clave tenemos que crear un nuevo valor alfanumérico con nombre Application. El valor de Application debe ser el nombre del programa que queremos ejecutar como un servicio, utilizando la RUTA COMPLETA del ejecutable.



Podemos crear también aparte del valor Application, los valores AppParameters y AppDirectory para indicar los parámetros que va a usar el programa y el directorio donde se va a ejecutar el programa. Ambos valores también son alfanuméricos.

Una vez realizado esto, ya tenemos nuestro programa funcionando continuamente en la maquina como servicio. Si queremos poner en marcha o parar el servicio, podemos usar bien la consola que vimos anteriormente (services.msc) o podemos usar las ordenes del símbolo de comandos NET START MISERVICIO y NET STOP MISERVICIO.

Si queremos desinstalar un servicio que hayamos instalado con instsrv podemos utilizar el formato:

INSTSRV MISERVICIO remove

Podemos instalar tantas instancias de srvany como queramos, siempre que utilicemos un nuevo nombre para cada servicio distinto que instalemos.

Normalmente este procedimiento se suele utilizar para transformar en servicios programas que actúan de servidor de algún tipo, ya sea de FTP, Web, News, P2P, etc.

Si el programa que transformamos en servicio no funciona, o no puede ser ejecutado como servicio (cosa que ocurre con algunos programas, por la forma en la que están programados) el servicio podrá ser iniciado, pero se detendrá automáticamente. Asi por ejemplo, un programa tipo emule es casi imposible de correr como servicio (aunque se puede conseguir con mucho esfuerzo) dado que es un programa que cuenta con una pesada interfaz grafica y no esta diseñada para trabajar en segundo plano, sin acceso a la pantalla.