[Capítulo 5]

Seguridad de los datos

Copias de seguridad

Más tarde o más temprano, todo aparato electrónico tiene tendencia a fallar. Siendo el ordenador un aparato electrónico, compuesto además de innumerables piezas electrónicas, la probabilidad de que alguna de ellas se estropee es relativamente alta. Si tenemos suerte, el fallo podrá repararse simplemente sustituyendo la pieza averiada pero, en otros casos, la reparación puede ser imposible o puede haber afectado tanto a nuestros datos que estos sean irrecuperables. Es en esos momentos cuando es más necesario tener copias de seguridad de todos nuestros datos, de forma que podamos recuperarlos rápidamente y sin problemas.

Desgraciadamente, el tener copias de seguridad no es un hecho habitual entre la mayoría de los usuarios, que solamente toman la determinación de hacer estas copias una vez han sufrido en sus propias carnes la perdida total y completa de datos importantes, momento a partir del cual realizan las copias regularmente.

Es importante tomar conciencia de la necesidad de las copias de seguridad antes de sufrir alguno de estos problemas que nos pueden hacer perder horas y horas de trabajo y que podían haber tenido fácil solución con unas pequeñas medidas de prevención.

Planeando las copias de seguridad

En un ordenador personal tenemos dos tipos de ficheros: reemplazables e irreemplazables.

Los ficheros reemplazables son aquellos de los cuales disponemos una copia. Habitualmente, estos son los ficheros del sistema operativo y de los diversos programas que hayamos ido instalando (siempre que dispongamos del original desde donde los instalamos o estos estén libremente disponibles en Internet para su descarga legal).

Los ficheros irreemplazables son aquellos de los que no disponemos de ninguna copia ni ninguna manera sencilla de recuperar su contenido en caso de borrado accidental. Normalmente estos ficheros serán los datos generados por los programas que utilicemos (documentos de texto, imágenes tomadas de nuestra cámara digital, hojas de cálculo con nuestra contabilidad,...)

Nuestro objetivo deberá ser convertir los ficheros irreemplazables en ficheros reemplazables. Para conseguirlo deberemos tener copias de seguridad de estos ficheros de forma que podamos recuperarlos en caso de pérdida.

Para tener unas buenas copias de seguridad deberemos plantearnos las siguientes preguntas:

Qué?

Cuáles son los ficheros que realmente nos interesa mantener? Hoy en dia son habituales los discos duros de 80 Gb, 120 Gb o incluso más capacidad. Es evidente que no podemos hacer una copia de todos los ficheros almacenados en ellos, así que deberemos decidir cuales son los ficheros importantes.

Cuándo?

Con que frecuencia debemos hacer copias de seguridad de los datos? Idealmente, deberíamos hacer una copia cada vez que modifiquemos el fichero. Esto es difícil, así que deberemos decidir una cierta frecuencia (dos días, una semana,...) teniendo en cuenta que si perdemos información durante ese período necesitaremos reintroducirla en el sistema.

Dónde?

En que tipo de sistema de almacenamiento vamos a guardar nuestras copias de seguridad? Para un usuario doméstico hay tres tipos de formatos disponibles: CD, DVD o disco USB. Si grabamos los datos en CD deberemos tener en cuenta que su capacidad es de tan solo unos 700 Mb, por lo que tal vez necesitaremos muchos CDs para copiar todos nuestros datos. Es un formato ideal, por ejemplo, para grabar una colección de ficheros MP3, ya que son datos que, en principio, no variarán.

Si los grabamos en DVD dispondremos de mucho más espacio para guardar los datos y, hoy en dia, el precio de una grabadora de DVD ya no es impedimento para su adquisición.

Finalmente, los discos USB habituales disponen de entre 256 Mb y 1 Gb de espacio en caso de que utilicemos los conocidos como *pendrive.* Existen también discos duros externos conectables por USB, en los cuales podemos llegar a disponer de la misma capacidad que en nuestro disco interno y a un precio asequible.

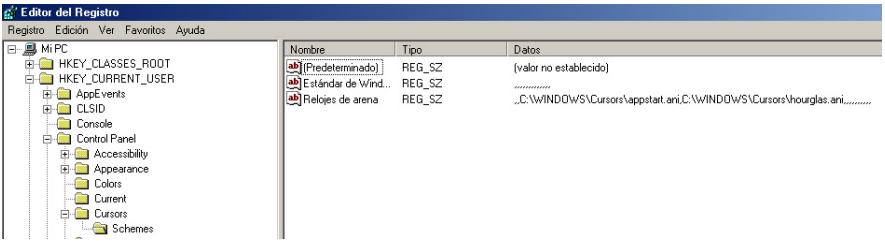
Deberemos escoger, además, donde vamos a guardar estas copias de seguridad una vez realizadas. Idealmente, estarán guardadas en una caja fuerte a prueba de fuego. Esto no suele ser posible en la mayoría de los casos, por lo que deberemos guardarlas en un sitio alejado del ordenador y protegido de posibles robos.

Es muy útil también disponer de un sistema de rotación de las copias, de forma que podamos recuperar no solo la última versión sino, también alguna de las anteriores. Para ello, no debemos sobreescribir los ficheros cada vez que realicemos la copia de seguridad sino que deberemos ir rotando entre diferentes medios según la frecuencia que nos interese. Por ejemplo, si realizamos las copias diariamente en CD regrabables podemos disponer de un CD regrabable para cada día de la semana, convenientemente etiquetado. Así, si lo necesitamos seremos capaces de recuperar datos de hasta una semana de antigüedad, lo cual puede ser útil en caso que hayamos hecho modificaciones en algún fichero y no podamos recuperar los datos originales.

El registro de Windows

Mucha de la información necesaria para el funcionamiento de Windows se guarda en el registro. El registro es una base de datos donde se centraliza la configuración del sistema, del hardware del que disponemos y de muchas aplicaciones. En las versiones antiguas de Windows esta información se guardaba en ficheros de texto (normalmente, con extensión INI) y cada aplicación los guardaba en diferentes directorios, lo que complicaba buscar el que nos interesaba para modificarlo. A partir de Windows 95 se implementó este nuevo sistema que permite editar los datos que contiene desde un único sitio.

El registro está organizado en una serie de carpetas y subcarpetas donde se almacenan las claves y el valor que tienen. Esta estructura lógica es muy parecida a un sistema de ficheros, donde las claves se corresponden a los nombres de los ficheros y los valores al contenido de ese fichero. De ese modo, podemos acceder al valor de una clave navegando hasta la subcarpeta donde está la clave y visualizando su valor.



Para poder editar el registro disponemos de dos herramientas, regedit.exe y regedt32.exe, aunque es bastante peligroso editar directamente el registro, ya que corremos el riesgo de equivocarnos, modificandolo de forma que podemos dejar el sistema en un estado

inestable o incluso inservible, llegando a tener que reinstalar el sistema operativo. Existe el riesgo, además, de que el registro quede corrupto, ya sea a causa de un programa defectuoso o de un apagado incorrecto de nuestro ordenador, de forma que no sea posible recuperarlo. Por ello, es adecuado realizar copias de nuestro registro habitualmente. Para hacerlo podemos utilizar ERUNT, que nos permite realizar una copia de todo el registro y posteriormente restaurarlo desde DOS o desde la Consola de Recuperación de Windows. Este programa nos permite planificar copias diarias del registro de forma que podemos volver a estados anteriores cuando lo necesitemos.

Del mismo autor es NTREGOPT, que permite optimizar el espacio que ocupa nuestro registro. Cuando instalamos y desinstalamos muchos programas se crean y se borran claves en el registro, pero el espacio que ocupan estas claves puede no recuperarse totalmente. NTREGOPT funciona creando un nuevo registro que contiene solo las claves existentes sin el espacio vacío que hayan podido dejar las borradas, aprovechando mejor el espacio en disco que ocupa el registro.

Otra causa de problemas en el registro son los programas que crean claves en él que después no son borradas. Esto provoca que el registro se llene de claves repetidas o innecesarias. Existen diversos programas que nos permiten la limpieza del registro, como Easy Cleaner, aunque debemos tener especial cuidado con el uso de estos programas porque podemos borrar sin querer claves que son necesarias para el buen funcionamiento de nuestro ordenador.

Finalmente, existen toda una serie de "trucos" que podemos aplicar a nuestro ordenador para cambiar alguna de sus funcionalidades a través de modificaciones en el registro. Hay una lista bastante completa de estas modificaciones en Winguides.

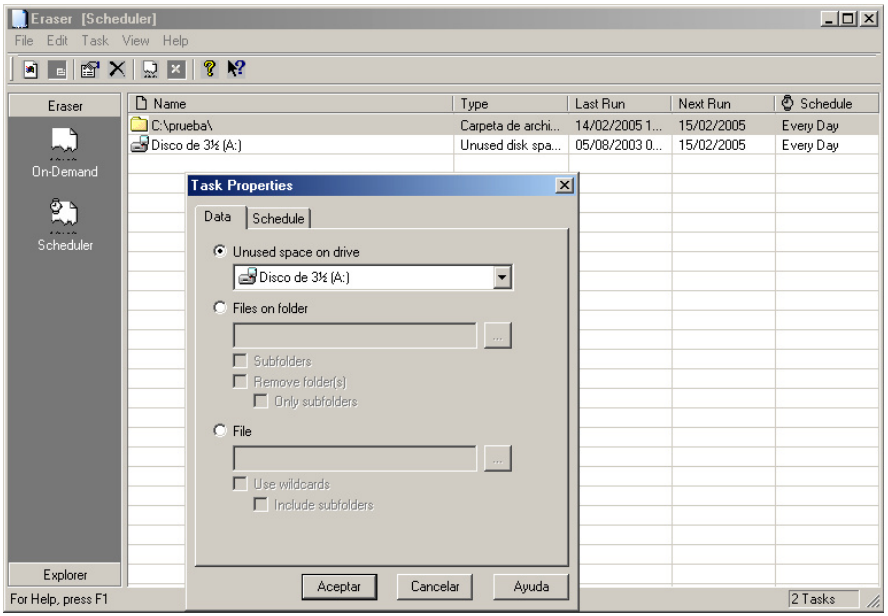
Borrado seguro de datos

Muchas veces no nos planteamos la cantidad de información que podemos estar proporcionando en cualquier momento. Por ejemplo, en el momento de vender nuestro ordenador, un disco duro o de lanzar un disquete o un CD a la basura nos estamos arriesgando a que nuestros datos estén a disposición de quien quiera (y pueda) leerlos. Según un estudio hecho por dos estudiantes del MIT, la mayoría de discos duros que se venden a través de eBay contienen información privada del vendedor. De los 158 discos que compraron, 69 contenían ficheros recuperables y 49 contenían ficheros con información personal (cartas de amor, números de tarjetas de crédito, pornografía.)

Podemos pensar que un simple formateo del disco duro impedirá que los datos almacenados en este puedan ser recuperados, pero resulta bastante sencillo recuperar archivos que hayan sido borrados de un disco y algunos programas permiten deshacer el formateo de una determinada unidad.

Existen incluso métodos para recuperar los datos de los discos aunque estos hayan sido sobreescritos. Aunque las técnicas para conseguir extraer esa información no están al alcance de cualquiera, podemos localizar diversas empresas especializadas en recuperación de datos a través de Internet que disponen de las herramientas para ello. Esto nos puede ser útil en el caso que se estropee alguno de nuestros discos o hayamos borrado alguna información y no tengamos copia de seguridad de los datos. Hay que tener en cuenta que la tarifa que cobran por estos servicios es considerablemente elevada por lo que solo será una opción a tener en cuenta si los datos son realmente importantes y necesarios.

Si queremos asegurarnos de no estar distribuyendo información privada debemos sobreescribir los datos de forma que no sea posible recuperarlos de ningún modo. Para ello, es necesario realizar diversas pasadas de escritura sobre cada uno de los sectores donde se almacena la información, algunas con datos aleatorios y otras con datos fijos.
Para simplificar la tarea lo más sencillo es utilizar algún programa como Eraser o un disco de arranque como DBAN, que nos permitirán eliminar la información de forma sencilla.



Eraser nos permite borrar ficheros individuales, carpetas completas y/o el espacio sin usar de cualquier unidad de disco. Además, también permite programar la tarea para que se realice con una determinada frecuencia, con lo que no tendremos que preocuparnos de tener información comprometida en algún lugar de nuestro ordenador.

De todas formas, si la información que contiene nuestro disco es muy importante y queremos asegurarnos de que nadie pueda acceder a ella, lo mejor es destruir fisicamente ese disco. Para ello, deberemos abrir el disco duro y asegurarnos de destruir los platos que contiene de forma que no puedan ser leídos, por ejemplo, sumergiéndolos en ácido o destruyéndolos en una fundición. Esta es la mejor solución hoy en día; teniendo en cuenta el precio de un disco duro, si este contiene datos realmente confidenciales no merece la pena arriesgarse por el poco dinero que podemos obtener en su venta.

También deberíamos asegurarnos de que los disquetes o los CDs que lanzamos a la basura no puedan ser leídos por nadie si contienen datos confidenciales. Para los disquetes podemos seguir el mismo método que con el disco duro o simplemente abrir la carcasa de plástico, extraer el disco magnético de su interior y cortarlo en trozos lo más pequeños posible. Para destruir los CDs podemos envolverlos con un trapo o un papel y romperlos en trozos pequeños. Si hacemos estos, debemos procurar no tirar todos los trozos en la misma basura para dificultar aun más su posible recuperación.

Protección ante la copia de datos en discos USB

En un domicilio particular será un poco extraño, pero en un empresa es habitual que haya un ordenador que contenga datos confidenciales y que no deben salir de ese ordenador (nóminas, facturación, planos, diseños industriales...) Si estos datos son importantes es de suponer que se habrán tomado medidas para que nadie pueda copiarlos, como por ejemplo, no conectar ese ordenador a la red, desactivar la disquetera, no dar permiso a los usuarios para utilizar la grabadora de CDs (de alguna manera habrá que hacer copias de los datos, pero nunca deberá hacerlas un simple usuario).

Pero no debemos pasar por alto un detalle, la aparición de discos duros que se conectan a través del puerto USB. Estos discos tienen una gran capacidad de almacenamiento (128, 256, 512 Megabytes e incluso superiores) y no tenemos ningún mecanismo para evitar que alguien pueda conectarlos a ese ordenador y utilizarlos (aparte de desactivar fisicamente los puertos USB, cosa que no es posible en muchas placas base).

Si disponemos de Windows 2000 o Windows XP existen un par de soluciones sencillas, la primera en caso de que no se haya instalado aun ningún disco de este tipo y la segunda en caso de que ya se haya instalado alguna vez.

Si no se ha instalado ningún disco USB

Debemos quitar todos los permisos a los ficheros:

```
c:\windows\Inf\Usbstor.pnf
c:\windows\Inf\Usbstor.inf
```

Para ello iremos a las propiedades del fichero y en la pestaña *Seguridad* denegamos todos los permisos para todos los usuarios.

Si ya se ha instalado algún disco USB

Debemos editar el registro de Windows y buscar la siguiente carpeta:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
```

y editar la clave Start para ponerle el valor 4.

En caso de que queramos una solución más general existe un programa llamado DeviceLock que nos permitirá controlar que usuarios pueden acceder a cada tipo de dispositivo y no permitirá el uso de dispositivos externos (tanto USB como Firewire u otros).

Referencias

Artículo sobre la información encontrada en discos duros usados
http://news.bbc.co.uk/1/hi/technology/2676461.stm

Diferencias entre regedit y regedt32
http://support.microsoft.com/default.aspx?kbid=141377

Dirección de descarga de ERUNT y NTREGOPT
http://home.t-online.de/home/lars.hederer/erunt/index.htm

Dirección de descarga de EasyCleaner
http://personal.inet.fi/business/toniarts/ecleane.htm

Modificaciones del registro de Windows
http://www.winguides.com/registry/

Dirección de descarga de Eraser
http://www.heidi.ie/eraser/default.php

Dirección de descarga de DBAN
http://dban.sourceforge.net/

Dirección de descarga de DeviceLock
http://www.protect-me.com/dl/

Cómo desactivar el uso de discos USB
http://support.microsoft.com/default.aspx?scid=kb;en-us;823732