MÉTODOS DE CIFRADO EN WINDOWS

El cifrado de datos resulta una de las mejoras contramedidas disponibles a la hora de evitar robos de información y posibles compromisos del sistema.

Cifrar la información es uno de los recursos más eficientes contra muchos tipos de ataque, puesto que, aunque un atacante pueda eludir todo tipo de restricciones de seguridad para acceder a un fichero o dato, el hecho de que esté convenientemente cifrado lo protege además de forma segura. De este modo, la información cifrada, aunque se encuentre en poder del atacante, resultará inaccesible.

En este artículo se tratarán diferentes métodos de cifrado en Windows que permitirán al lector cifrar la información sensible de forma cómoda y segura.

I Introducción a la criptografía

La criptografía ha evolucionado vertiginosamente en la era de los ordenadores y hoy en día está al alcance de cualquiera.

En los últimos años, matemáticos y científicos han creado una serie de algoritmos que se consideran criptográficamente seguros por los especialistas, en el sentido de que no es posible aplicar ninguna técnica de criptoanálisis para romperlos. Además los han hecho públicos, convirtiéndose en estándares para que todos los sistemas que los usen puedan entenderse entre sí.

Estos algoritmos criptográficos, no sólo garantizan la confidencialidad de la comunicación o del almacenamiento de datos, sino que también aseguran la integridad, proporcionando métodos para detectar si un tercero ha manipulado los datos.

En la actualidad existen algoritmos que se consideran seguros porque los ataques contra ellos se basan en cálculos matemáticos para los que no se conocen métodos de resolución de complejidad baja. Habitualmente se basan en cálculos basados en la factorización de números primos muy elevados. Esto significa que matemáticamente es muy costoso (en tiempo y recursos) descifrarlos.

Algoritmos criptográficos

En criptografía aparecen tres elementos básicos:

- Texto en claro
- Clave o secreto
- Texto cifrado

El texto en claro es legible por cualquiera. Mediante un algoritmo criptográfico se cifra utilizando una clave. El resultado es un mensaje ininteligible: el texto cifrado. Para recuperar el texto en claro a partir del cifrado, se vuelve a utilizar el algoritmo criptográfico junto con una clave secreta.

Cabe recordar que la criptografía es tan segura como su eslabón más débil, y éste suele ser la contraseña elegida para cifrar la información. Aunque el algoritmo de cifrado sea muy seguro, si la información cifrada se genera con una contraseña débil, el cifrado no es efectivo.

La criptografía simétrica se basa en la utilización de una misma clave para cifrar y descifrar. Además, los algoritmos de este tipo son muy rápidos porque están basados en operaciones muy simples. Los más conocidos son:

- AES (*Advanced Encryption Standard*), también conocido como Rijndael
- DES, Triple DES, DESX
- IDEA. Utilizado en PGP
- RC4. Es el algoritmo utilizado en SSL en Wi-Fi
- *Blowfish*. Su autor, Bruce Schneier, lo donó al dominio público

La criptografía asimétrica o de clave pública se basa en el uso de una clave para cifrar y otra para descifrar, siendo una de ellas pública. Este modelo de cifrado es mucho más complejo. En este artículo, no se entrará a fondo en la criptografía asimétrica.

A efectos prácticos, el cifrado de datos es muy útil en situaciones comunes para el usuario medio: por ejemplo, entornos donde cierta información sensible se deba transportar en una llave USB, cinta o disco óptico; sistemas compartidos entre diferentes usuarios; o la utilización de un portátil. Para estos casos existen programas con diferentes acercamientos que permiten cifrar la información con criptografía estándar.

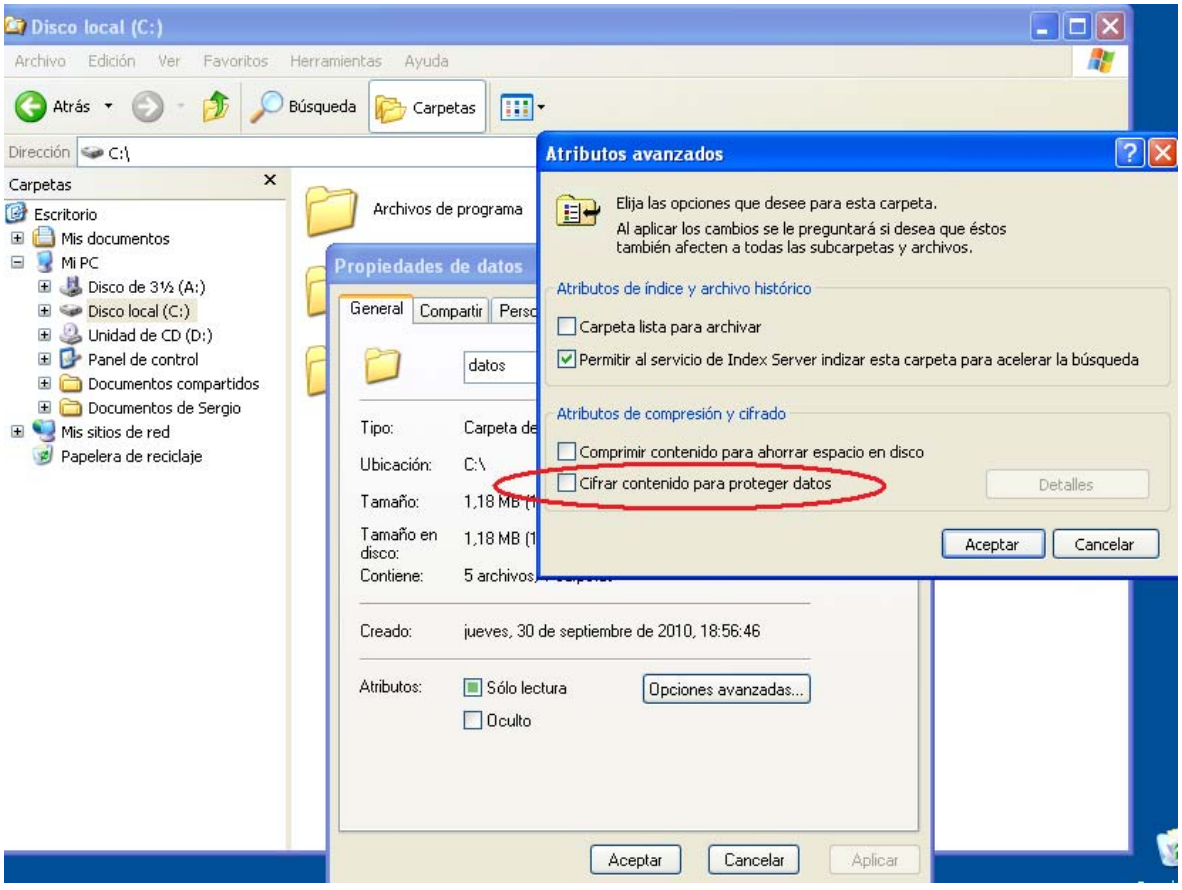
II Cifrado de datos con EFS

Windows ofrece un método de cifrado integrado, que resulta muy sencillo de utilizar, puesto que el usuario no tiene que recordar ninguna clave especial para cifrar la información.

Se llama EFS (*Encrypted File System*) y solo está presente si el disco duro está formateado con NTFS (la alternativa es FAT32, mucho más inseguro e ineficiente en general). Existe la posibilidad de, sin perder la información, convertir una partición de disco duro de FAT32 a NTFS.

Desde las propiedades de archivos o carpetas (no sirve en unidades completas), se puede acceder a un menú donde se le puede indicar al sistema que el directorio es empleado para almacenar archivos cifrados (con lo que todo lo que se almacene en él se cifrará) o que se desea cifrar un solo fichero (esta acción no se recomienda, es más útil trabajar con carpetas).

Ilustración 1: Cifrado de información EFS en Windows XP



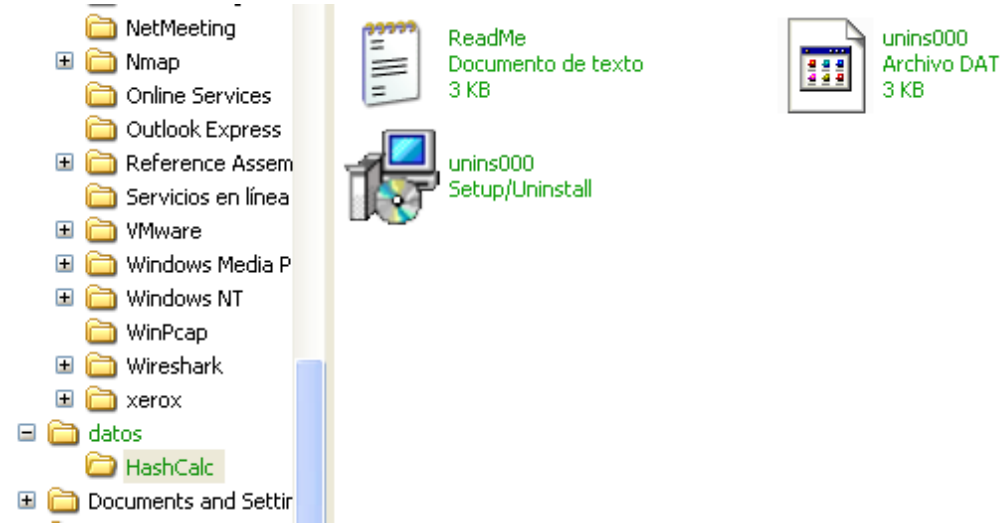
Fuente: INTECO

Una vez marcado un directorio con la opción "Cifrar contenido para proteger datos", todo lo que se almacene en él queda cifrado. Cada vez que inicie sesión, los datos se

encuentran en el directorio para poder ser manipulados, pero una vez cerrada la sesión, o si otro usuario se presenta en el sistema, los datos son inaccesibles. Incluso si el disco es explorado con otro sistema operativo desde un CD, los datos permanecen cifrados e ilegibles.

Desde el explorador de Windows, los archivos o carpetas cifrados aparecen en color verde.

Ilustración 2: Archivos cifrados EFS en Windows



Fuente: INTECO

EFS se basa en una mezcla de criptografía pública y privada. En realidad EFS utiliza una clave única por fichero para cifrarlo y descifrarlo. Esta clave (FEK o *File Encryption key*) se genera automáticamente cuando se cifra un fichero y se almacena con él. Aunque esto parezca inseguro (sería como almacenar la llave junto al candado que protege una puerta) esta FEK es a su vez cifrada con la clave pública del usuario, con lo que queda protegida.

Tanto las FEK como las claves públicas y privadas del usuario se generan de forma transparente para él la primera vez que cifra un archivo o carpeta y de forma automática. Se almacenan en forma de certificado en el repositorio de certificados del sistema operativo. El usuario no tiene por qué conocer estos datos.

La ventaja de este método es que no tiene que utilizar contraseñas adicionales cada vez que quiera acceder a los datos: todo es gestionado por el sistema operativo.

Es imprescindible destacar que sólo el usuario con el que se ha cifrado la información (y sólo ese mismo usuario) puede acceder a los datos. Esto significa que en el caso de que el usuario del sistema operativo se pierda, los datos quedan inaccesibles

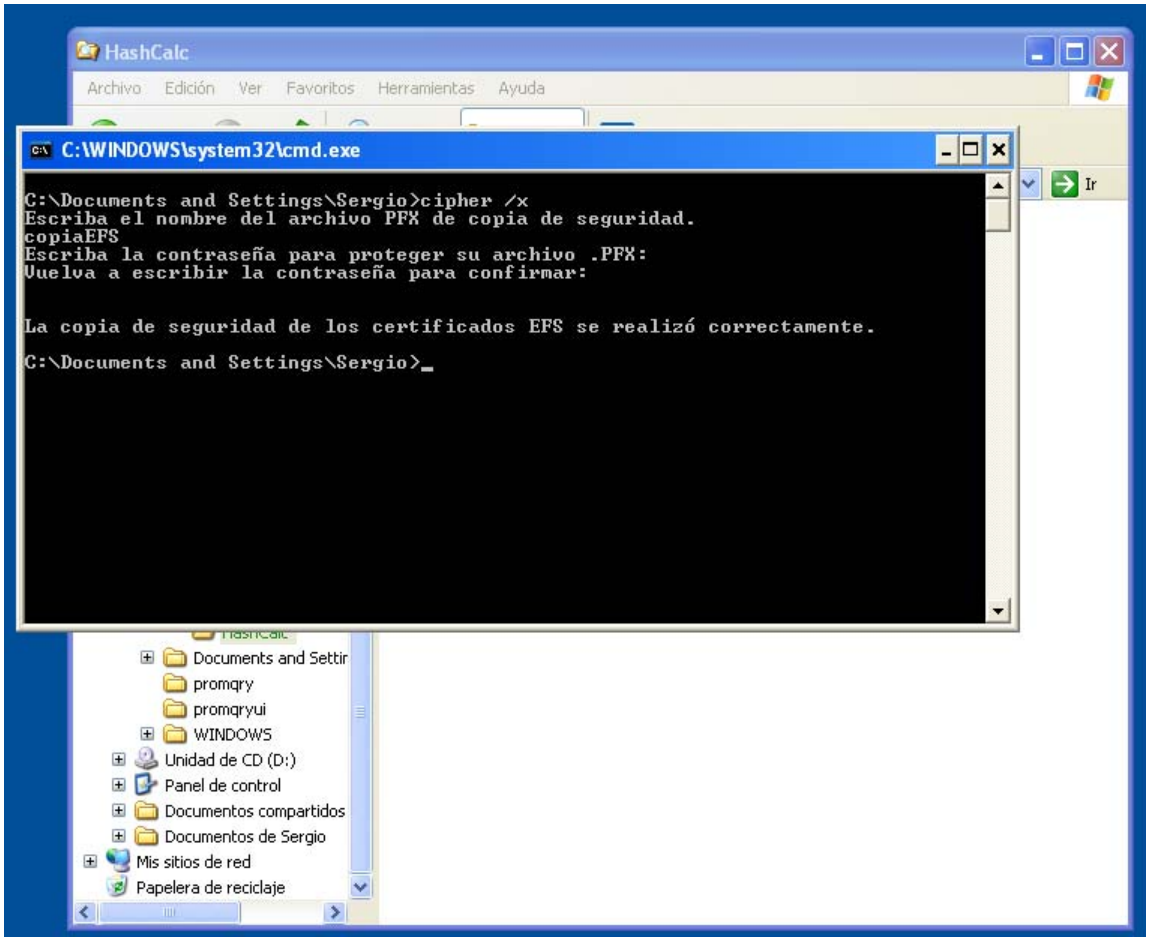
irremediablemente, incluso si se crea un nuevo usuario con el mismo nombre y características.

La única forma de recuperar los datos, en caso de que el usuario se pierda o se traslade a un sistema operativo diferente, es crear una copia de seguridad del certificado y almacenarla en un lugar seguro para utilizarla en caso de necesidad. Para ello, una vez cifrados los directorios o archivos, se debe abrir una consola de sistema (tecleando cmd.exe en el cuadro de Ejecutar) y teclear el siguiente comando:

Cipher /x

Tal y como se indica en la figura.

Ilustración 3: Realizar copia de seguridad del certificado EFS



Fuente: INTECO

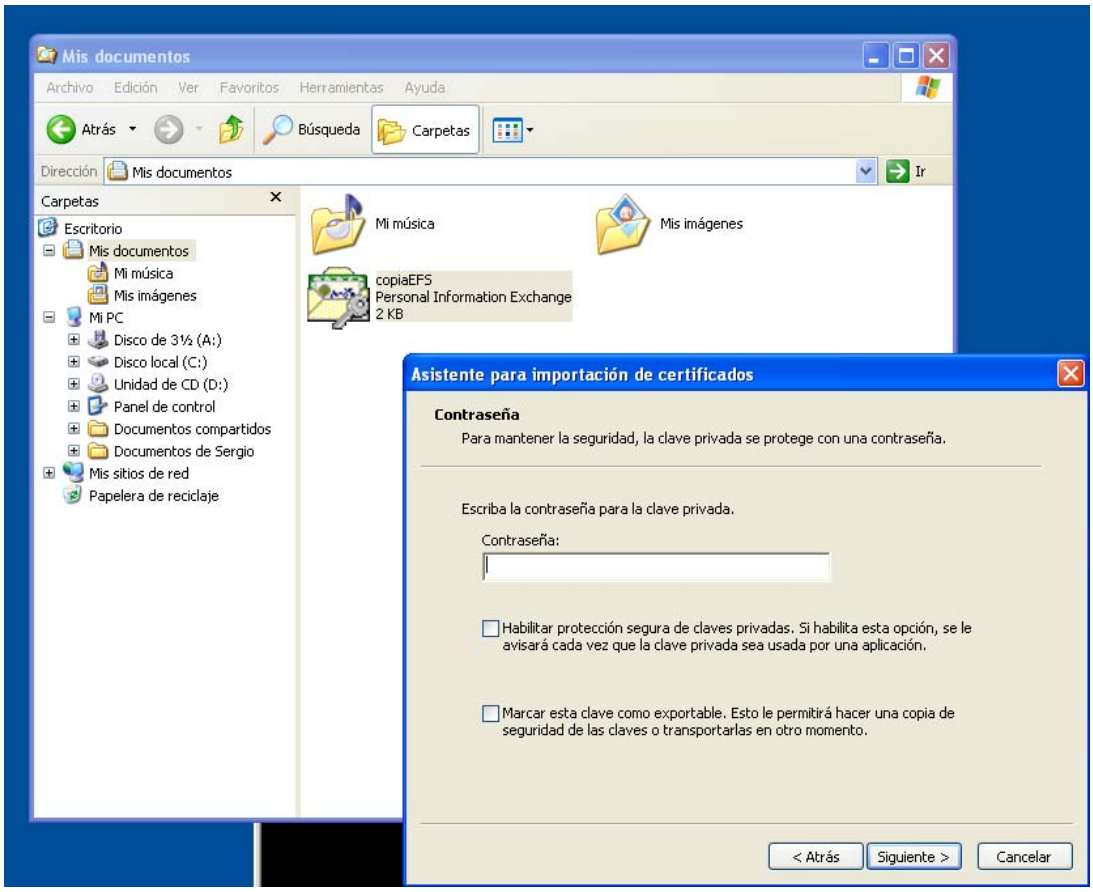
Esto crea un archivo (con extensión PFX) que es necesario guardar en un lugar seguro, puesto que es el único método para recuperar la información en caso de desastre. Por supuesto, también es necesario recordar la contraseña utilizada para proteger este

certificado. La contraseña previene el uso del certificado si alguien tiene acceso a él. Puede dejarse en blanco, pero no se recomienda.

Si se pierde el usuario o se cambia de sistema operativo, solo es necesario exportar el certificado para poder tener de nuevo acceso a los archivos. Esto se consigue ejecutando directamente el archivo PFX y siguiendo las instrucciones.

El hecho de realizar copia de seguridad del certificado necesario para recuperar los datos, no significa que no sea igualmente necesario realizar una copia de los datos en sí. El certificado no contiene los datos, solo permite el acceso a ellos en otro sistema o a otro usuario diferente al que inicialmente cifró la información.

Ilustración 4: Recuperación del certificado



Fuente: INTECO

Ventajas e inconvenientes de EFS

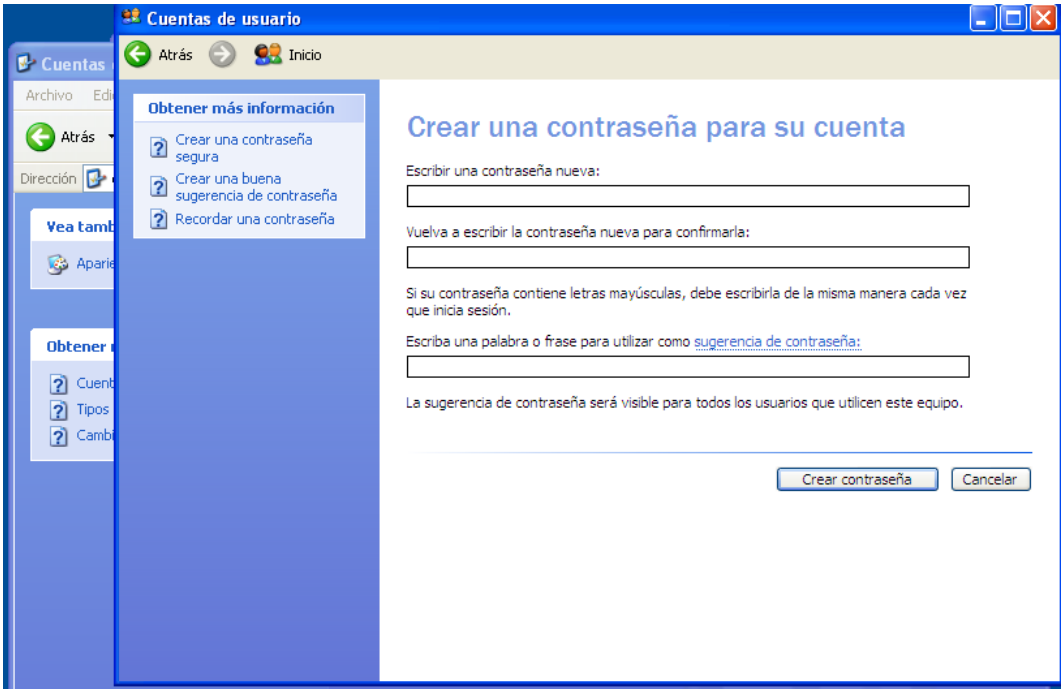
EFS es un sistema que utiliza tecnología estándar y, por tanto, es seguro. Su mayor ventaja es la facilidad de uso. Cada vez que el usuario inicie sesión, los datos están ahí para poder ser manipulados, pero una vez cerrada la sesión, o si otro usuario utiliza el sistema, los datos aparecen inaccesibles.

Sin embargo, uno de los inconvenientes que pueden surgir es que está totalmente ligado a Windows y NTFS. Esto quiere decir que si el archivo es copiado a una unidad en red que no sea NTFS (muchas unidades USB no están formateadas así, y muchos sistemas operativos tampoco soportan NTFS), el archivo se copia sin contenido (un archivo de 0 bytes de tamaño). Por el contrario, si se copia de una unidad NTFS a otra unidad NTFS, permanece perfectamente cifrado y con todo su contenido.

Esto hace que cifrar con NTFS no sea muy adecuado para transportar estos ficheros. Sin embargo, lo hace útil para utilizar en portátiles, por ejemplo, puesto que pueden llegar a ser sustraídos o extraviados con mayor facilidad. En estos casos, la información en el disco duro cifrada no puede ser obtenida por alguien que tenga acceso al mismo. También es útil en sistemas compartidos (un mismo ordenador con varios usuarios diferentes) para mantener ciertos datos accesibles por un solo usuario.

Otro inconveniente a tener en cuenta es que toda la seguridad se concentra en su eslabón más débil, y en este caso es la contraseña de usuario de Windows. La contraseña es la que permite descifrar el certificado que es utilizado a su vez para descifrar la contraseña con la que se cifra cada archivo. Por tanto, es imprescindible proteger la cuenta de usuario con una contraseña mayor de catorce caracteres, que mezcle letras, números y símbolos. Para asignar una clave al usuario, se debe ir al panel de control, "cuentas de usuario" y "crear una contraseña" en el usuario elegido.

Ilustración 5: Asignación de contraseña a un usuario



Fuente: INTECO

Otra desventaja es que no está permitido cifrar archivos de sistema, como la carpeta Windows, por ejemplo.

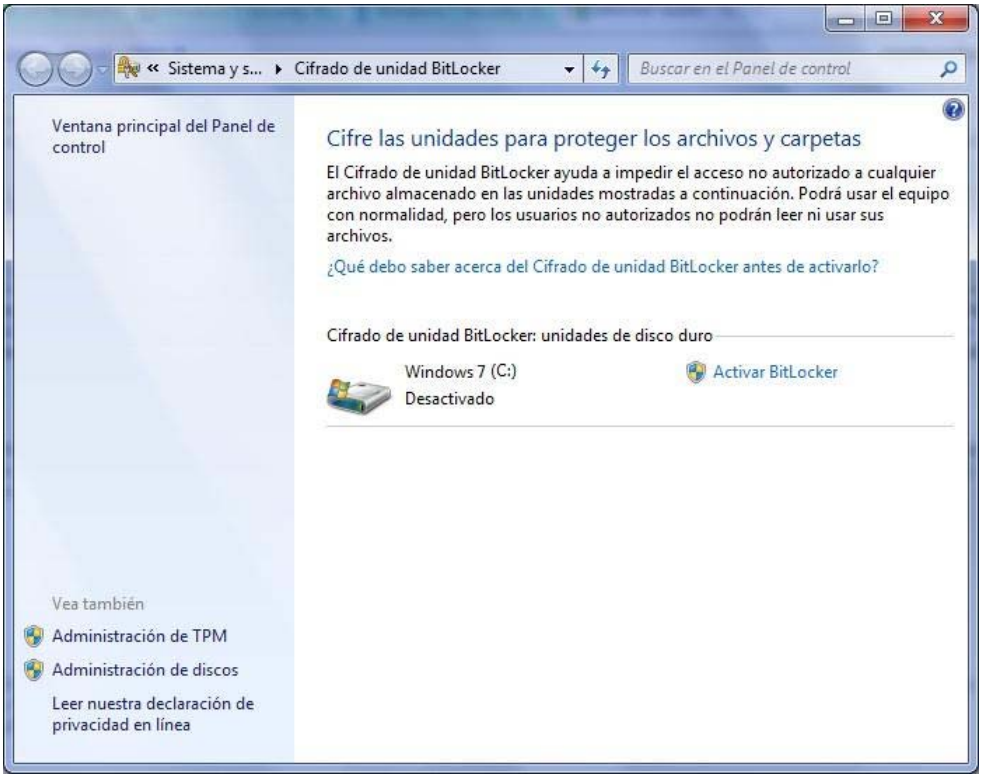
III Cifrado de datos con *BitLocker*

BitLocker es una tecnología introducida por Microsoft exclusivamente en las versiones más avanzadas de Windows Vista y 7. Permite aprovechar una característica de cierto hardware, llamada TPM (*Trusted Platform Module*) que lo hace muy robusto. El TPM interactúa con *BitLocker* para proporcionar una protección mejorada incluso durante el inicio de sistema.

BitLocker es mucho más potente que EFS y ha sido introducido para complementarlo. Permite cifrar todo un disco duro, incluido el sistema operativo. Esto evita una debilidad en EFS ya mencionada: toda la seguridad recae sobre la contraseña del usuario de Windows y el problema es que ésta se mantiene almacenada en el disco duro (lógicamente cifrada por Windows independientemente del EFS). Aunque, si es suficientemente compleja, no supone mayor problema.

BitLocker también permite el cifrado de unidades del sistema que se pueden dedicar exclusivamente a datos e incluso unidades extraíbles gracias a su función "*BitLocker To Go".*

Ilustración 6: Cifrado *BitLocker*



Fuente: INTECO

Al igual que EFS, está pensado para la comodidad del usuario, sin embargo, el hecho de que esté disponible exclusivamente para versiones más caras de Windows, lo ha hecho menos popular.

BitLocker no sustituye a EFS, sino que lo complementa. Por ejemplo, con *BitLocker* no es posible en un sistema multiusuario, que cada usuario proteja sus propios archivos, aunque es posible combinar ambas tecnologías y obtener mejores resultados (EFS sigue presente en todas las versiones de Windows y ambos métodos son compatibles).

Tabla 1: Comparativa tecnologías de cifrado Windows

BitLocker	EFS
Permite cifrar todo: datos, unidades de disco extraíbles, unidad de sistema...	Solo permite cifrar archivos o carpetas, excluyendo las de sistema.
No depende de los usuarios. Está activo o inactivo.	Permite que múltiples usuarios cifren independientemente sus datos en un sistema multiusuario.
Se debe ser administrador de sistema para usarlo.	Cualquier usuario de sistema, independientemente de sus permisos, puede utilizarlo.
Sólo disponible en las versionas más completas de Windows 7, Vista y 2008.	Disponible desde Windows 2000, en todas las versiones.
Utiliza TPM (*Trusted Platform Module*).	Es independiente del hardware.

Fuente: INTECO

IV TrueCrypt

TrueCrypt es un programa libre, gratuito y de código abierto ajeno a Microsoft y más potente (aunque algo más complejo de utilizar) que las dos tecnologías descritas. Por ejemplo, entre otras muchas funcionalidades, *TrueCrypt* puede ser configurado para aumentar el factor de autenticación, de modo que sólo pueda recuperarse la información si además de una contraseña se dispone de un archivo especial que actúa como "llave".

TrueCrypt permite dos modos básicos de funcionamiento: cifrado de unidades enteras de información o creación de volúmenes cifrados.

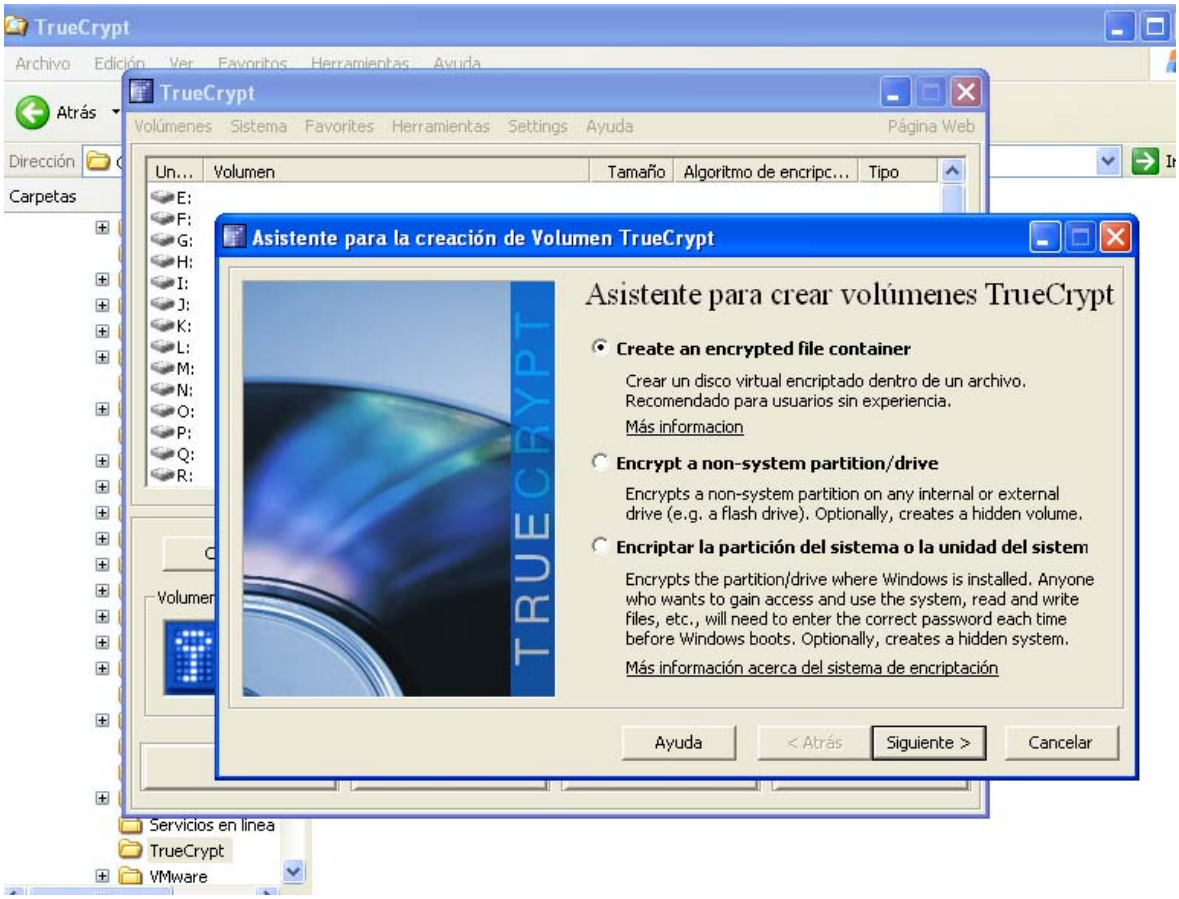
Un volumen cifrado es en realidad un archivo de un cierto tamaño, un "contenedor" en el que existen a su vez archivos, una vez sea "montado". "Montar" el archivo significa hacerlo accesible como una unidad más para el sistema operativo. La gran ventaja de esto es que permite crear volúmenes (que no son más que archivos) que pueden ser transportados y montados en cualquier sistema operativo en el que se instale *TrueCrypt*, y la información permanece cifrada mientras el volumen no sea montado.

Esto permite compartir el archivo cifrado, transportarlo en un dispositivo USB, enviarlo por correo, etc. de forma segura. *TrueCrypt* tiene la ventaja de que es multiplataforma (funciona en Windows, Mac, Linux...), gratuito, y que no depende de ningún sistema de ficheros.

El otro método de funcionamiento permite cifrar toda una unidad por completo, que es "montada" en cada inicio de sesión bien automáticamente o bien de forma manual. En sus últimas versiones, además, permite cifrar incluso la partición del sistema operativo por completo.

Veamos un ejemplo de cómo crear un volumen con *TrueCrypt*. El asistente del programa permite crear un contenedor (un volumen) de forma muy sencilla.

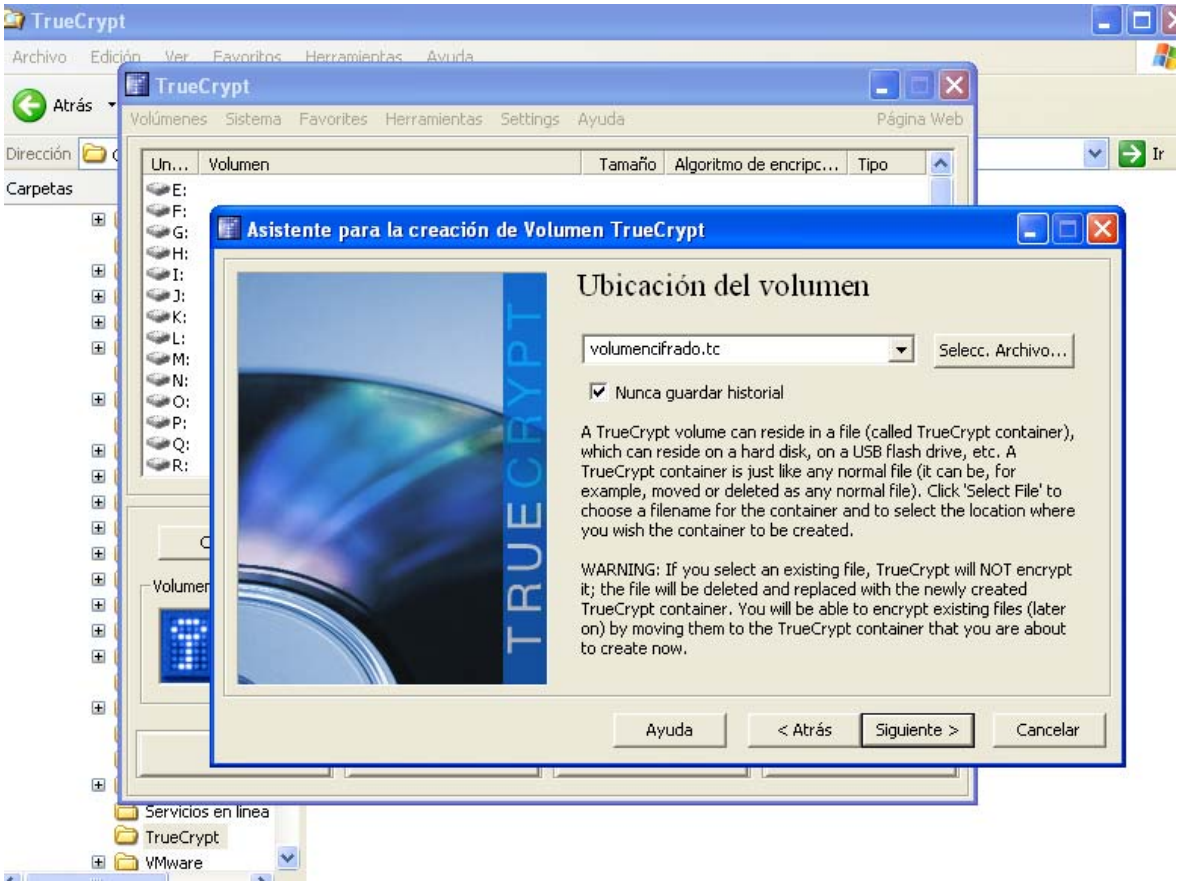
Ilustración 7: Crear un volumen de cifrado con TrueCrypt



Fuente: INTECO

Los contenedores o volúmenes son archivos del tamaño que el usuario elija y se alojarán donde el usuario quiera. Es preferible que los contenedores tengan la extensión ".tc" puesto que así el sistema los asocia a *TrueCrypt* y pueden ser montados de forma más sencilla (con un doble click). En la Ilustración 8, se crea un volumen llamado volumencifrado.tc y más tarde se monta como la unidad "S:".

Ilustración 8: Crear un volumen de cifrado con *TrueCrypt*

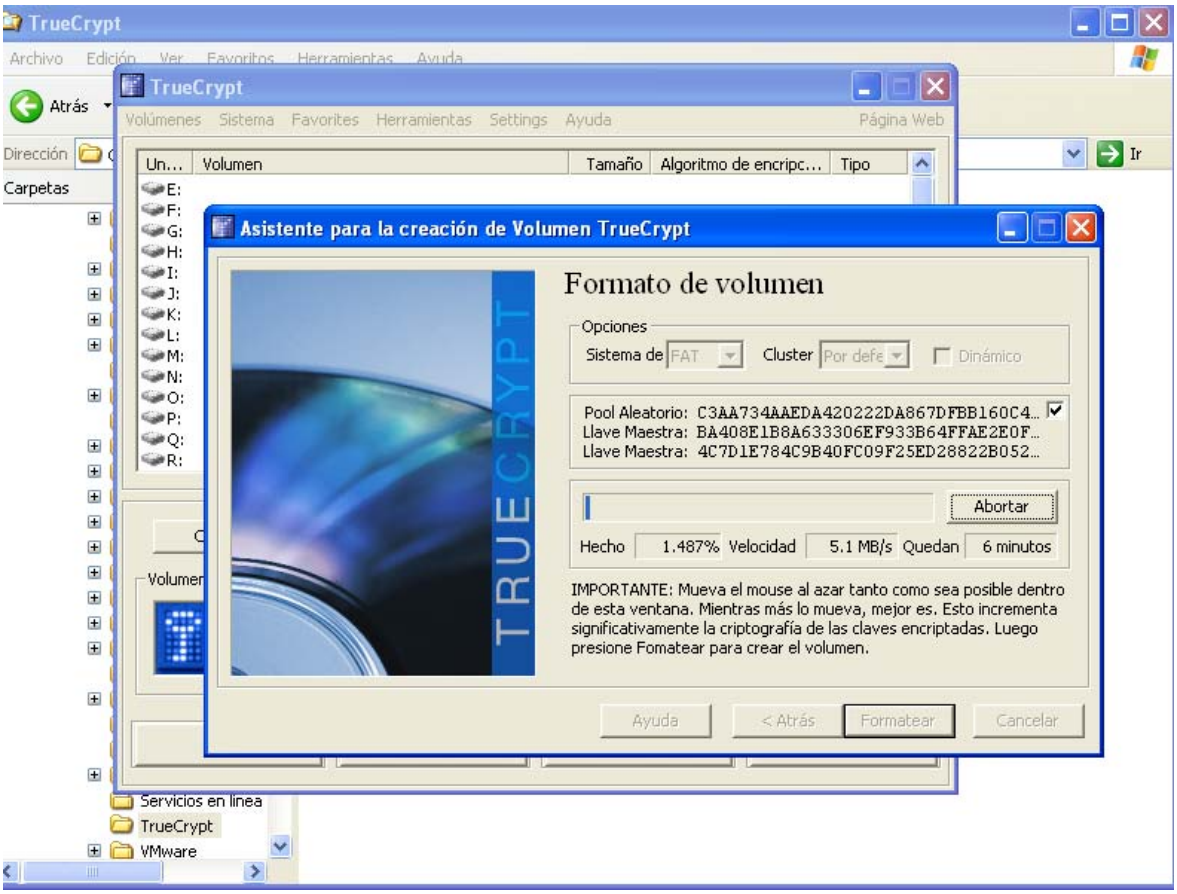


Fuente: INTECO

Una vez elegido el nombre y el tamaño (puede ser desde un megabyte hasta varios gigas) *TrueCrypt* se encarga de crear el volumen (el archivo) con una serie de datos cifrados y aleatorios según la contraseña introducida.

Este proceso se llama "formateo" del contenedor, y no es más que preparar el gran archivo para alojar los ficheros que se mantienen cifrados dentro. Aunque contenga desde el principio datos cifrados (llamados "ruido") el volumen todavía está "vacío" si es montado.

Ilustración 9: Formateo de un contenedor cifrado de *TrueCrypt*

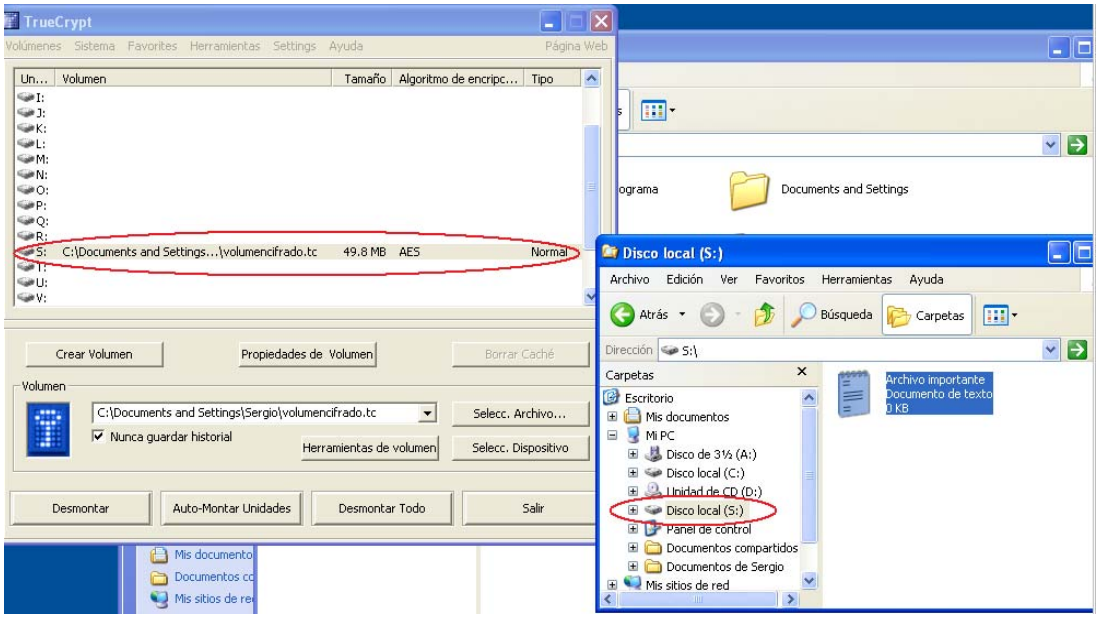


Fuente: INTECO

Una vez formateado, para el sistema operativo el volumen es un archivo con el tamaño deseado por el usuario. Para montarlo, se puede simplemente realizar doble click sobre él, y *TrueCrypt* pide la contraseña.

Es necesario elegir la unidad (la letra) donde es montado. Este proceso puede automatizarse, de forma que el programa arranque con Windows y pida la contraseña automáticamente cada vez que se inicie.

Ilustración 10: Unidad montada en *TryeCrypt* que aparece como unidad en el sistema



Fuente: INTECO

Si es montado con éxito, aparece como una unidad más para el sistema operativo. Todo lo que se copie a esa unidad queda cifrado cuando se desmonte la unidad, y está accesible mientras permanezca montada.

Ventajas e inconvenientes de *TrueCrypt*

TrueCrypt es gratuito y se encuentra, desde hace años, en continua mejora y evolución. Se basa en estándares y su código es abierto. Esto garantiza que no existe un método por el que los fabricantes puedan acceder a los datos cifrados sin conocer la contraseña.

Otra de sus grandes ventajas es que permite el cifrado de todas las particiones, incluida la de sistema. Esto, para proteger ordenadores portátiles, resulta muy cómodo y seguro. El hecho de que exista para otros sistemas operativos también es una gran ventaja que lo vuelve muy versátil.

Como inconveniente, requiere un mínimo conocimiento por parte del usuario, puesto que posee múltiples funcionalidades muy avanzadas, aunque su funcionamiento básico es sencillo. Otra desventaja es que para poder acceder a los datos creados en los contenedores desde cualquier sistema, se debe utilizar el propio *TrueCrypt* para montar las unidades, por tanto, o bien está instalado en el sistema destino, o bien es necesario transportarlo junto con los datos cifrados. Para estos casos existe una versión "portable", muy ligera (de pocos megabytes) que se puede descargar desde la propia página de los creadores.

Puede ser descargado desde www.truecrypt.org.