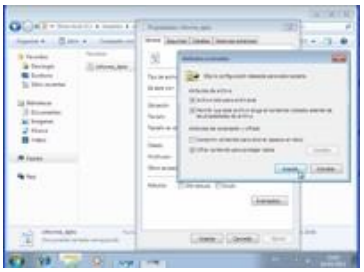
Sistema de cifrado de archivos.

El sistema de cifrado de archivos (EFS) es una característica de Windows que permite **almacenar información en el disco duro de forma cifrada**. El cifrado es la protección de mayor nivel que proporciona Windows para mantener la información a salvo.

Éstas son algunas **características** destacadas de EFS:

- ✓ El cifrado es sencillo. Se realiza activando una casilla en las propiedades del archivo o de la carpeta.
- ✓ El usuario controla quién puede leer los archivos.
- ✓ Los archivos se cifran cuando los cierra, pero cuando los abres quedan automáticamente listos para su uso.
- ✓ Si se cambia de idea con respecto al cifrado de un archivo, se puede desactivar la casilla en las propiedades del archivo.
- ✓ Sólo se pueden cifrar archivos y carpetas en los volúmenes del sistema de archivos NTFS.
- ✓ Los archivos y carpetas comprimidos también se pueden cifrar. Al cifrarlos se descomprimirán.
- ✓ Los archivos marcados con el atributo del sistema no se pueden cifrar, tampoco los archivos de la carpeta systemroot.
- ✓ EFS se instala de manera predeterminada en Windows 7.

Para **cifrar archivos o carpetas con EFS**, abre el explorador de Windows y haz click con el botón secundario en el archivo o la carpeta que quieres cifrar. Haz click en Propiedades.

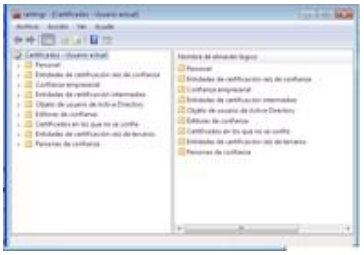


En la ficha General > Avanzadas y activamos la casilla **Cifrar contenido para proteger datos** y Aceptar. Hay disponibles opciones de cifrado adicionales.

A continuación, se solicita que se haga copia de seguridad de la clave de cifrado:

Si cifras datos en el equipo, necesitas un método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y no tienes ningún medio de recuperar los datos, éstos se perderán. También perderás datos si almacenas la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre puede tener acceso a los datos cifrados, debes hacer una copia de seguridad de la clave y del certificado de cifrado. Si hay más de una persona que usa tu equipo, o si usas una tarjeta inteligente para cifrar archivos, debes crear un certificado de recuperación de archivos.

Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.



Si quisiéramos **hacer una copia de todos los certificados EFS** del equipo:

1. Para abrir el Administrador de certificados, haz click en el botón `Inicio`, escribe `certmgr.msc` en el cuadro de búsqueda y, a continuación, presione ENTER. Si te solicita una contraseña de administrador o una confirmación, escribe la contraseña o proporciona la confirmación.
2. En el panel izquierdo, haz doble click en `Personal`.
3. Haz click en `Certificados`.
4. En el panel principal, haz click en el certificado en el que se muestra `Sistema de cifrado de archivos`, en `Propósitos planteados`. Es posible que debas desplazarte a la derecha para verlo. Debes hacer una copia de seguridad de todos los certificados EFS que haya.
5. Haz click en el menú `Acción`, apunta a `Todas las tareas` y, a continuación, haz click en `Exportar`.
6. En el Asistente para exportación de certificados, haz click en `Siguiente`, después en `Exportar la clave privada` y, a continuación, en `Siguiente`.
7. Haz click en `Personal Information Exchange` y, a continuación, en `Siguiente`.
8. Escribe la contraseña que deseas usar, confírmala y, a continuación, haz click en `Siguiente`. En el proceso de exportación, se creará un archivo para almacenar el certificado.
9. Escribe el nombre y la ubicación del archivo (incluye la ruta de acceso completa), o bien haz click en `Examinar`, desplázate hasta la ubicación, escribe el nombre del archivo y, a continuación, haz click en `Guardar`.
10. Haz click en `Siguiente` y, después, en `Finalizar`.

Recuperación de certificados EFS:
Si por cualquier motivo tuvieras que **recuperar la clave privada** realizarías el proceso contrario, **importarías el certificado** al equipo en cuestión.

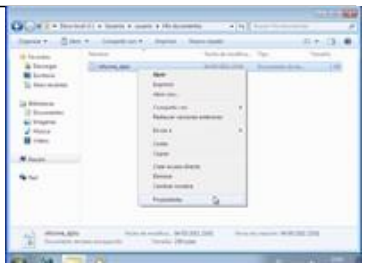
Conoce con más detalle el proceso de cifrado de datos, la exportación e importación de certificados EFS:

Procesos de cifrado, exportación e importación de certificados EFS.

Proceso de cifrado de datos

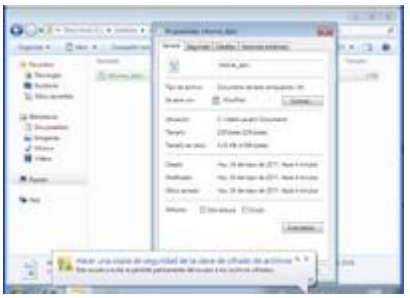
El sistema de cifrado de archivos (EFS) es una característica de Windows que permite **almacenar información en el disco duro de forma cifrada**. El cifrado es la protección de mayor nivel que proporciona Windows para mantener la información a salvo.

Para cifrar archivos o carpetas con EFS, abre el explorador de Windows y haz clic con el `botón secundario` en el archivo o la carpeta que quieres cifrar. Haz clic en `Propiedades`.



En la ficha `General` > `Avanzadas` y activamos la casilla `Cifrar contenido para proteger datos` y `Aceptar`.

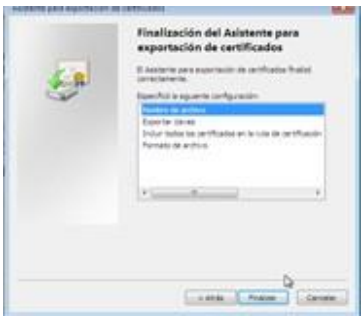
Hay disponibles opciones de cifrado adicionales.



Exportación de certificados EFS (copia de seguridad)

Después de realizar el cifrado de datos, se solicita que se haga copia de seguridad de la clave de cifrado:

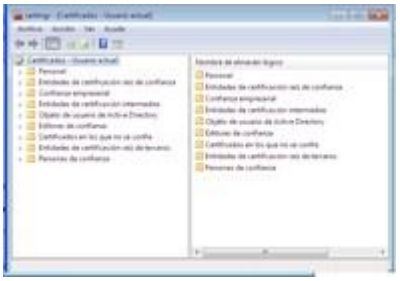
Si cifras datos en el equipo, necesitas un método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y no tienes ningún medio de recuperar los datos, éstos se perderán. También perderás datos si almacenas la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre puede tener acceso a los datos cifrados, debe hacer una copia de seguridad de la clave y del certificado de cifrado. Si hay más de una persona que usa tu equipo, o si usas una tarjeta inteligente para cifrar archivos, debes crear un certificado de recuperación de archivos.



Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.

Existe la posibilidad de hacer una copia de seguridad de todos o algunos de los certificados EFS almacenados en nuestro sistema en otro momento posterior al cifrado de la información.

Si quisiéramos hacer una copia de todos los certificados EFS del equipo:



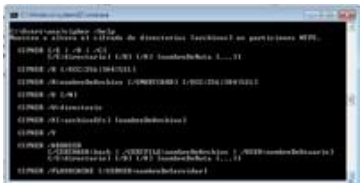
1. Para abrir el Administrador de certificados, haz clic en el botón `Inicio`, escribe `certmgr.msc` en el cuadro de búsqueda y, a continuación, presiona `ENTER`. Si se te solicita una contraseña de administrador o una confirmación, escribe la contraseña o proporciona la confirmación.
2. En el panel izquierdo, haz doble clic en `Personal`.
3. Haz clic en `Certificados`.
4. En el panel principal, haz clic en el certificado en el que se muestra `Sistema de cifrado de archivos`, en Propósitos planteados. Es posible que debas desplazarte a la derecha para verlo.
   Consejo: **Hacer una copia de seguridad de todos los certificados EFS** que haya.
5. Haz clic en el menú `Acción`, apunta a `Todas las tareas` y, a continuación, haz clic en `Exportar`.
6. En el Asistente para exportación de certificados, haz clic en `Siguiente`, después en `Exportar la clave privada` y, a continuación, en `Siguiente`.
7. Haz clic en `Personal Information Exchange` y, a continuación, en `Siguiente`.
8. Escribe la clave o contraseña que deseas usar, confírmala y, a continuación, haz clic en `Siguiente`. En el proceso de exportación, se creará un archivo para almacenar el certificado.
9. Escribe el nombre y la ubicación del archivo (incluye la ruta de acceso completa), o bien haz clic en `Examinar`, desplázate hasta la ubicación, escribe el nombre del archivo y, a continuación, haz clic en `Guardar`.
10. Haz clic en `Siguiente` y, después, en `Finalizar`.

Recuperación de certificados EFS:

Si por cualquier motivo tuvieras que **recuperar la clave privada** realizarías el proceso contrario, **importarías el certificado** al equipo en cuestión.

Importante, en la importación activar las siguientes opciones:

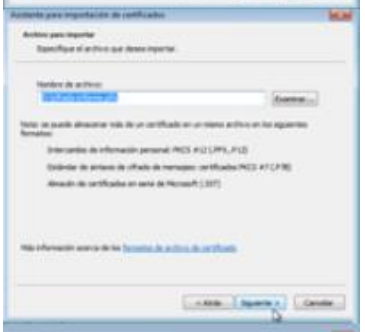
También se puede usar la **herramienta de la línea de comandos cipher** para mostrar o cambiar el cifrado de carpetas y archivos en las particiones NTFS.



Importación de certificados EFS (restaurar la copia de seguridad)

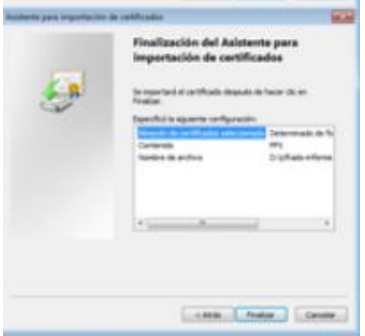
Podemos restaurar la copia de un certificado directamente haciendo doble clic sobre el fichero del certificado. En ese momento se iniciará un asistente que te guiará durante el proceso.

Indicamos donde está el archivo del certificado:

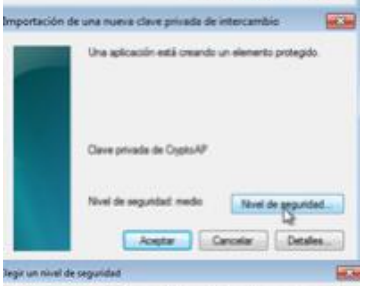


Importante: En la siguiente pantalla debemos introducir la clave privada y marcar las dos opciones que aparecen deseleccionadas:

La primera opción, "Habilitar protección segura de clave privada" va a conseguir que cada vez que un programa haga uso del certificado por seguridad pida que introduzcamos la clave privada. La segunda opción, "Marcar esta clave como exportable", consigue que en el futuro cuando se haga una nueva copia de seguridad (exportación del certificado), éste se exporte completo, incluyendo sus claves.



Ahora llega el momento de establecer el nivel de seguridad con el que se va a utilizar el certificado. Es fundamental establecer un **nivel Alto**, en el cual nos va a pedir la clave cada vez que hagamos uso del certificado.



Tras este paso, continuaremos con el asistente hasta la finalización del proceso.