PRÁCTICA 1.1
CONFIDENCIALIDAD

Athos Orío Choperena

Athos Orío Choperena

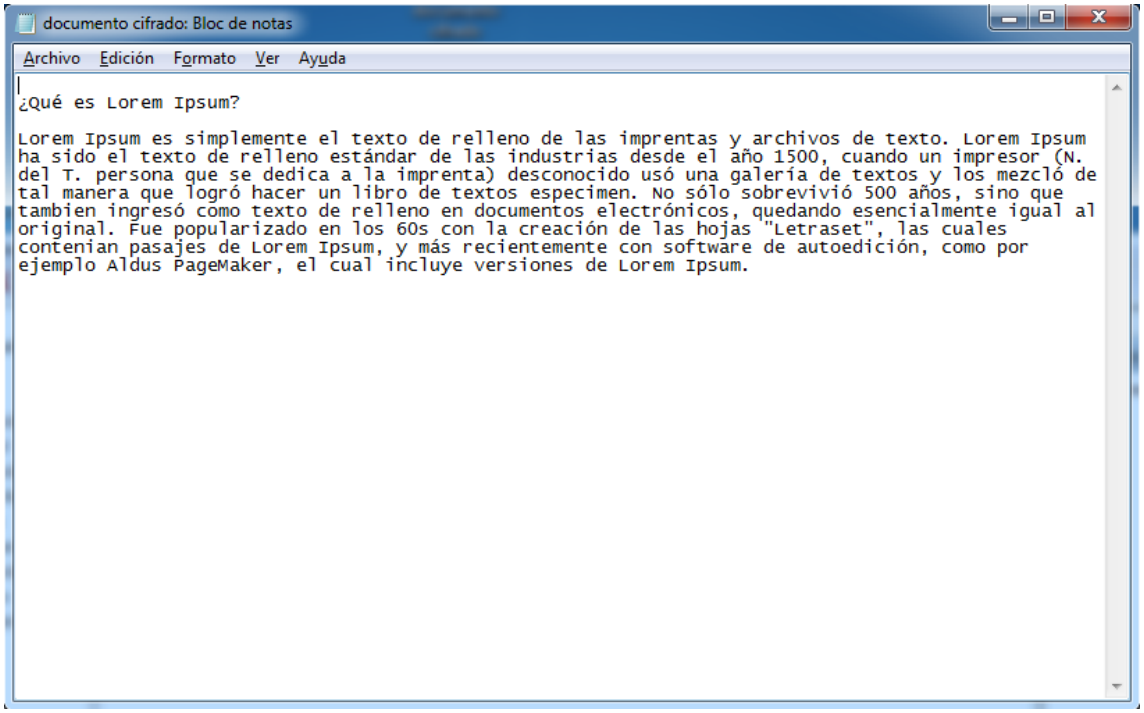
Contenido

Práctica Obligatoria 1.1: Confidencialidad

Para comprobar la confidencialidad con el sistema de encriptación de Windows vamos a crear un fichero de texto plano en el que vamos a introducir un texto, posteriormente, vamos a encriptar el archivo y vamos a realizar diferentes pruebas.

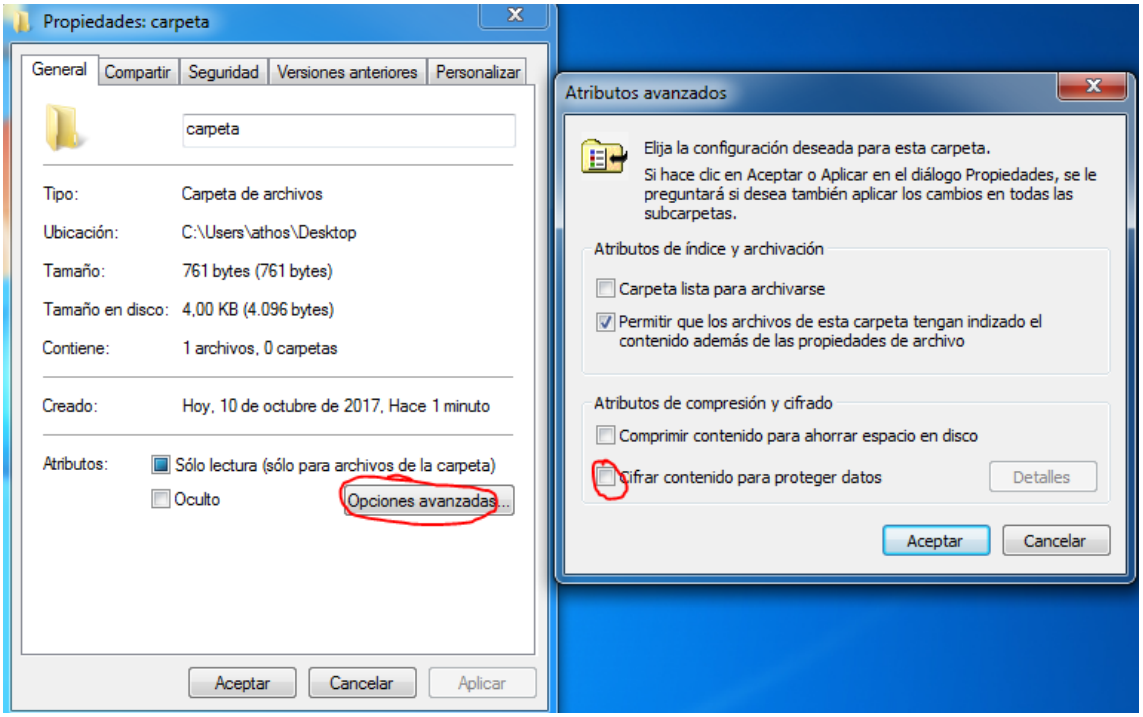
Creación de archivo de texto plano:

Creamos un archivo de texto plano con algún tipo de contenido

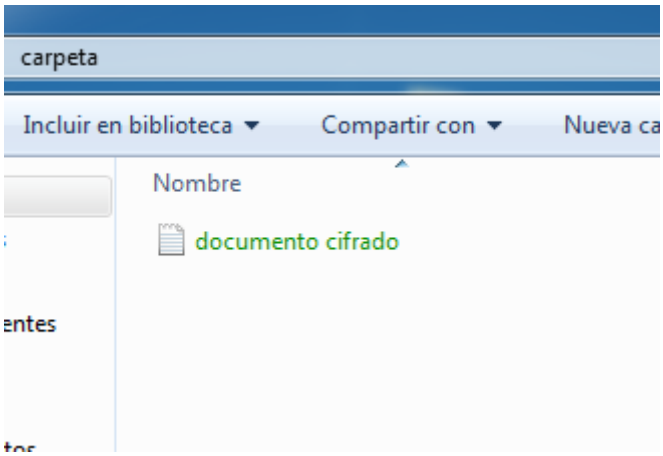


Cifrado del archivo:

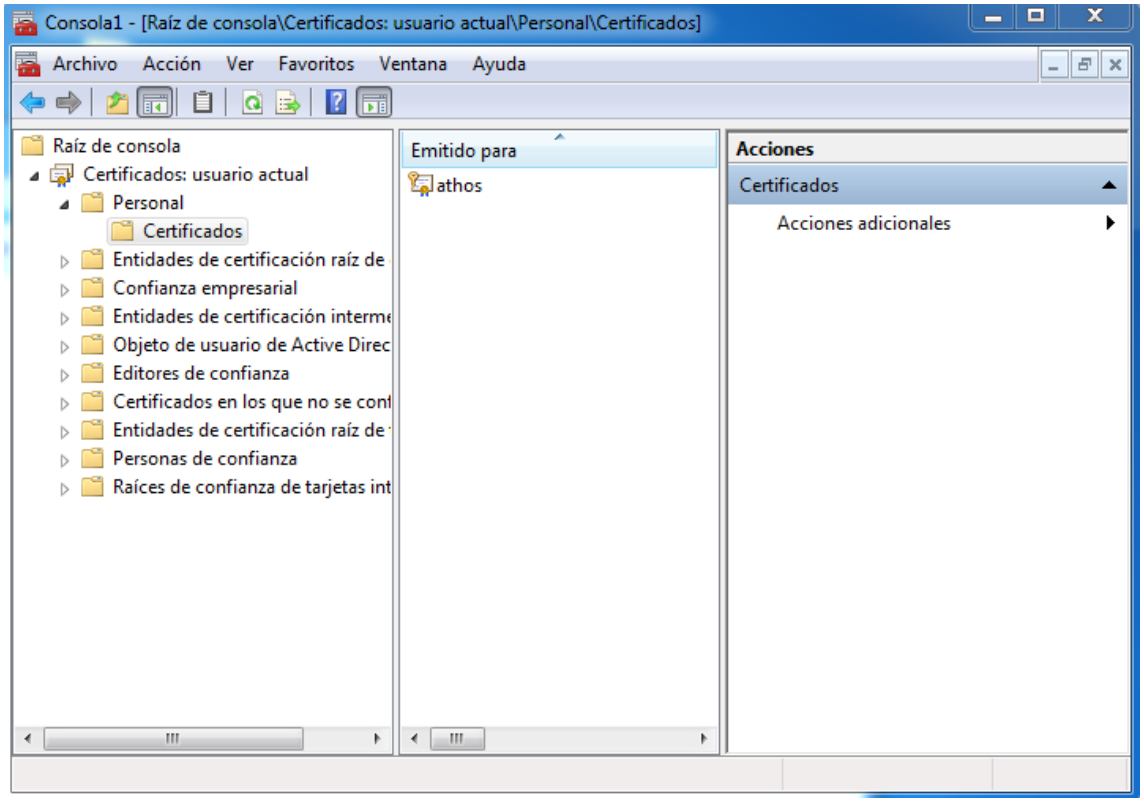
El siguiente paso es cifrar el archivo. Para ello, nos meteremos en las propiedades de la carpeta que lo contiene, y pincharemos en opciones avanzadas y luego marcaremos la casilla cifrar contenido para proteger los datos.



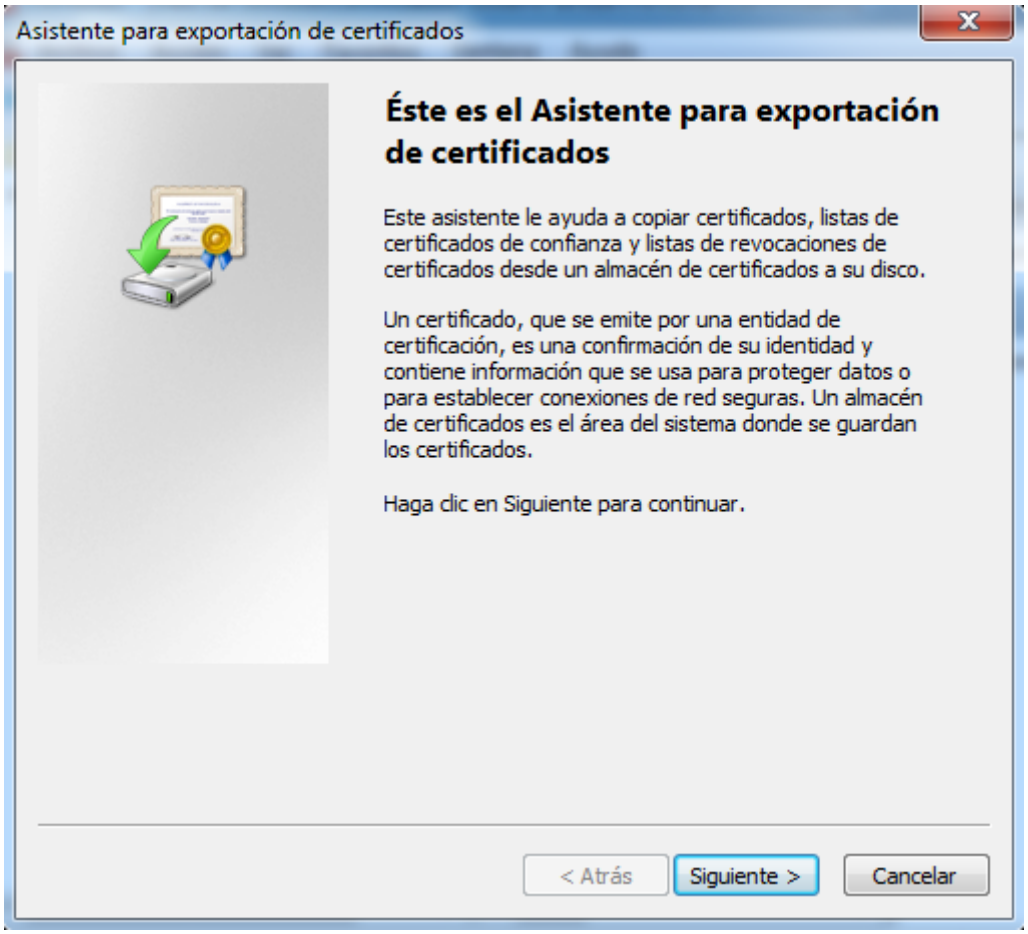
Después de aceptar, vemos que el color del archivo ha cambiado a verde, esto quiere decir que está cifrado



Si vamos a la consola de certificados (mmc) podemos comprobar cómo nos ha generado un certificado.



Podemos exportarlo con el botón derecho pinchando en exportar



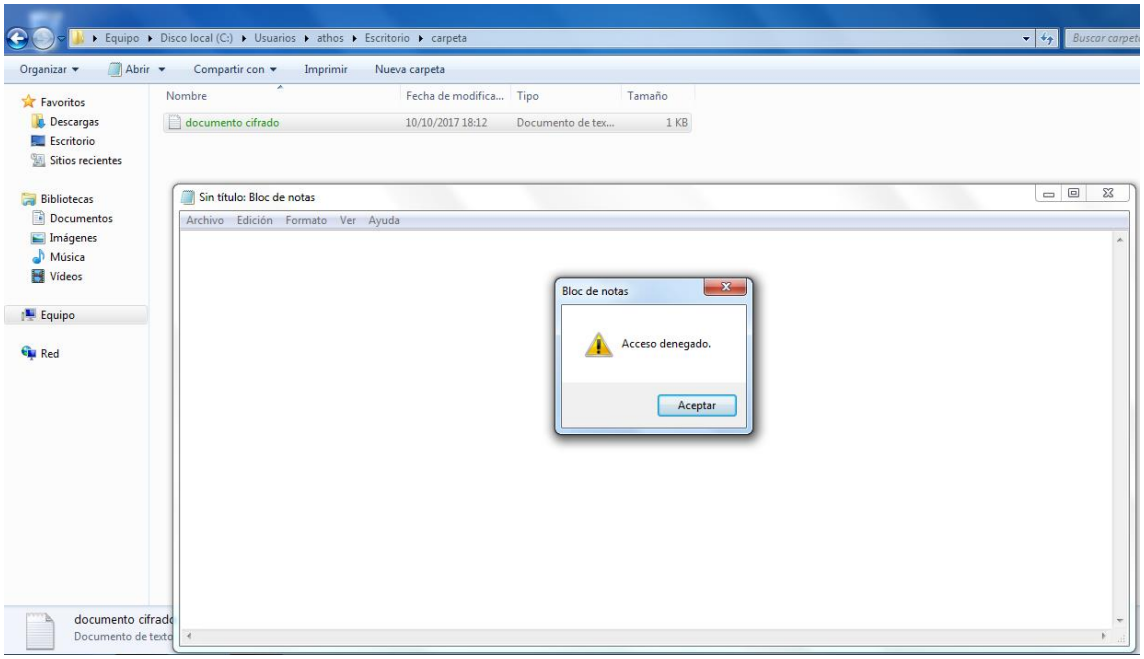
Tras completar el asistente, veremos que se nos genera un certificado, que luego podremos usar para des encriptar los archivos.

Pruebas de descifrado:

Vamos a realizar diferentes pruebas de descifrado:

Intentando acceder al archivo desde otra cuenta de usuario:

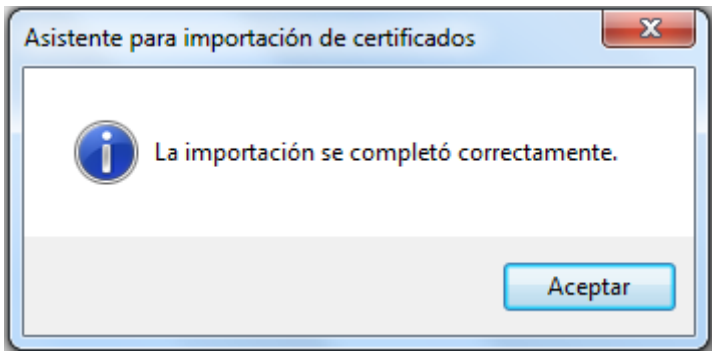
Vamos a crear otra cuenta de usuario en el mismo pc, y vamos a intentar acceder al archivo para ver su contenido.



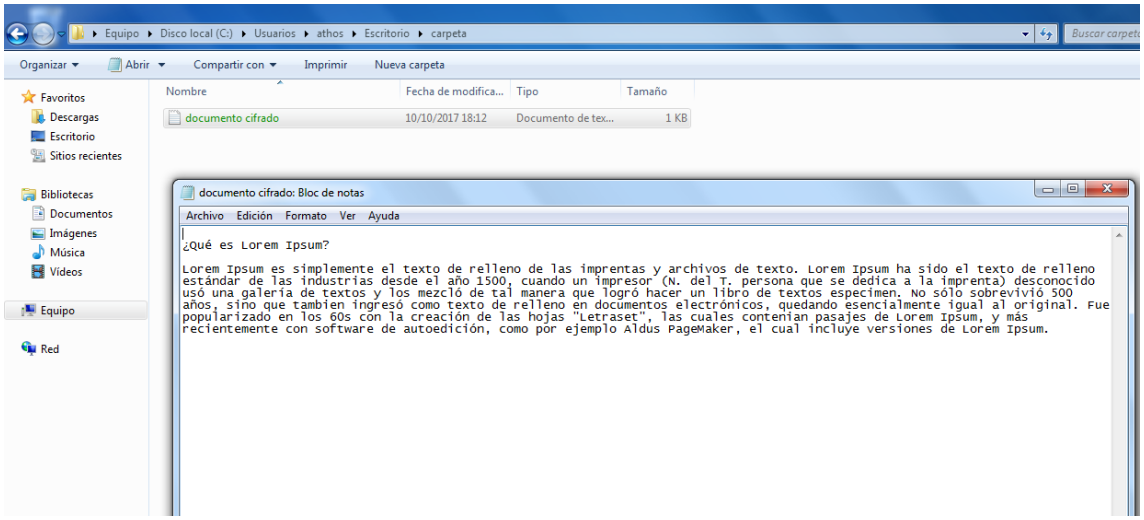
Como podemos ver, no nos deja acceder al archivo, ahora lo que haremos, es intentar importar el certificado (el que exportamos anteriormente). En este caso, cuando exportamos el certificado, pusimos una contraseña.

Al intentar importar el certificado, nos pide la contraseña, pero… ¿qué hubiese pasado si no le hubiésemos puesto contraseña? Vamos a continuar el proceso de importación…

Si el certificado no hubiese tenido contraseña (o si la supiésemos) nos hubiese dejado importarlo correctamente.



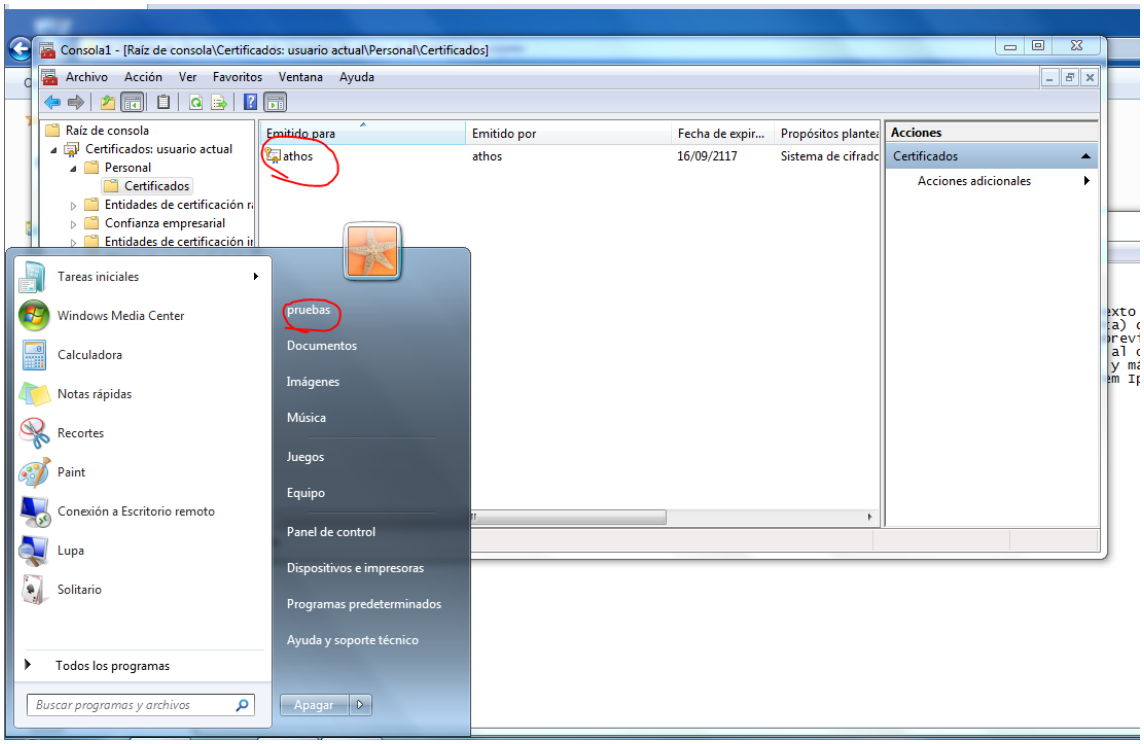
Ahora vamos a ver, si después de importar el certificado nos deja abrir el archivo cifrado…



Como podemos ver, sí que nos deja ver el contenido. De aquí sacamos una conclusión, cifrar carpetas de Windows, y dejar el certificado sin clave accesible, no sirve de nada.

¿Y si no estuviese exportado el certificado? ¿Podría un usuario administrador exportar un certificado de otro usuario? Vamos a probar…

Abrimos mmc y comprobamos si podemos exportar el certificado.

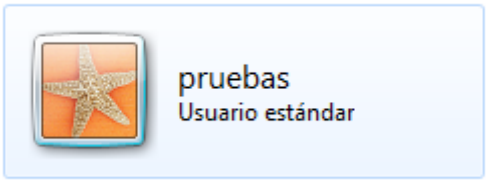


De momento el certificado lo podemos ver… a ver si lo podemos exportar…

Un usuario administrador, por lo que se ve, puede exportar cualquier certificado que esté instalado (siempre y cuando este tenga la clave privada instalada).

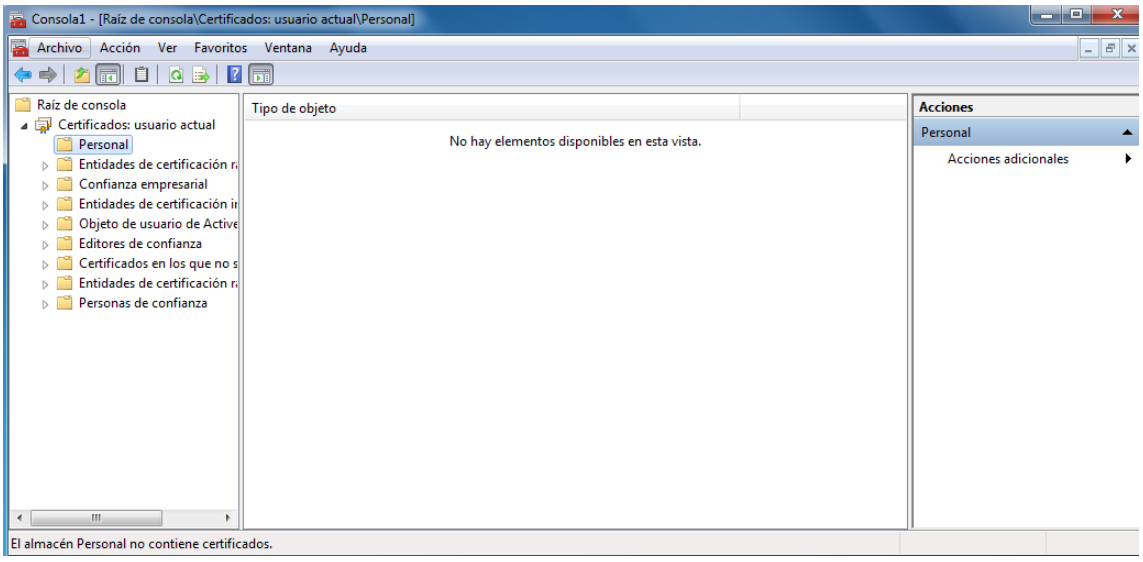
Ahora vamos a probar si el usuario fuese un usuario sin privilegios de administrador, ¿nos dejaría exportarlo?

Cambiamos al usuario pruebas a usuario estándar (antes estaba como administrador)



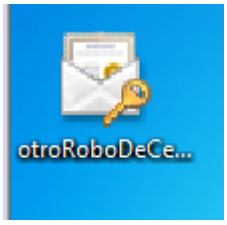
Realizamos el proceso de exportación con un usuario estándar y también nos deja

Ahora vamos a activar la cuenta invitado y probaremos también



En este caso, no nos aparece el certificado… menos mal….

Todas estas pruebas, han sido hechas, sabiendo que el usuario con el que se creó el archivo cifrado, y el certificado, no tenía contraseña para el inicio de sesión de Windows, vamos a probar a poner una contraseña al usuario athos, y probaremos otra vez si un usuario estándar podría exportar el certificado.



Si hemos podido exportar el certificado, esto quiere decir, que cualquier usuario valido, administrador o usuario estándar es capaz de exportar los certificados de otros usuarios, lo que es un problema de seguridad.

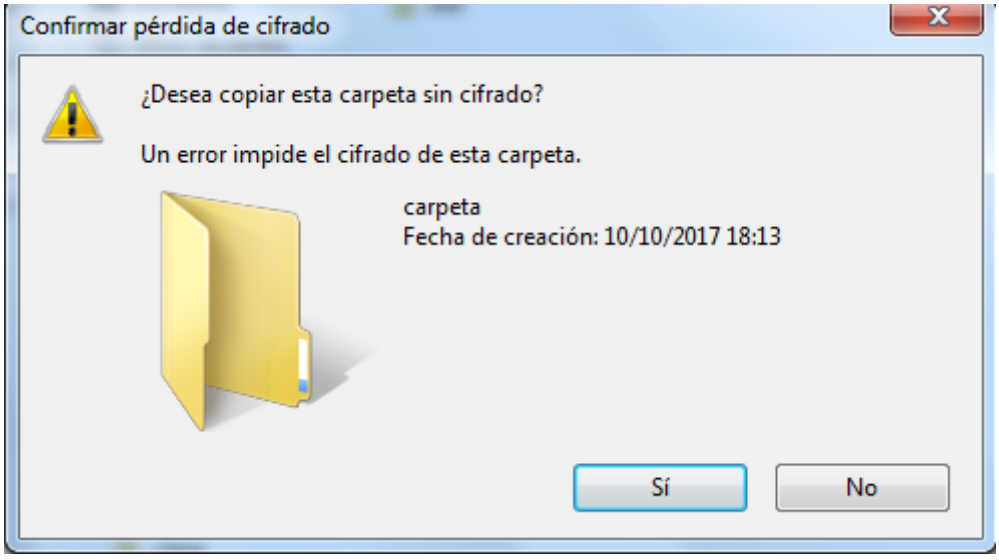
Intento de llevar el archivo a otro pc

Otra prueba de concepto que vamos a realizar es intentar llevarnos el archivo a otro pc, he intentar abrirlo en el otro equipo.

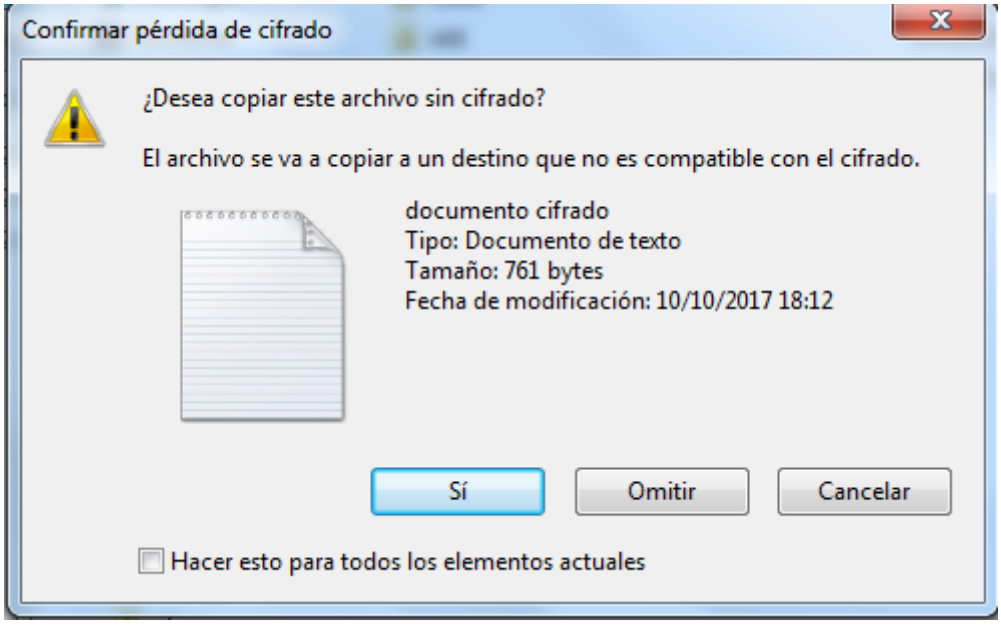
Lo vamos a realizar de dos formas:

La primera con el certificado instalado

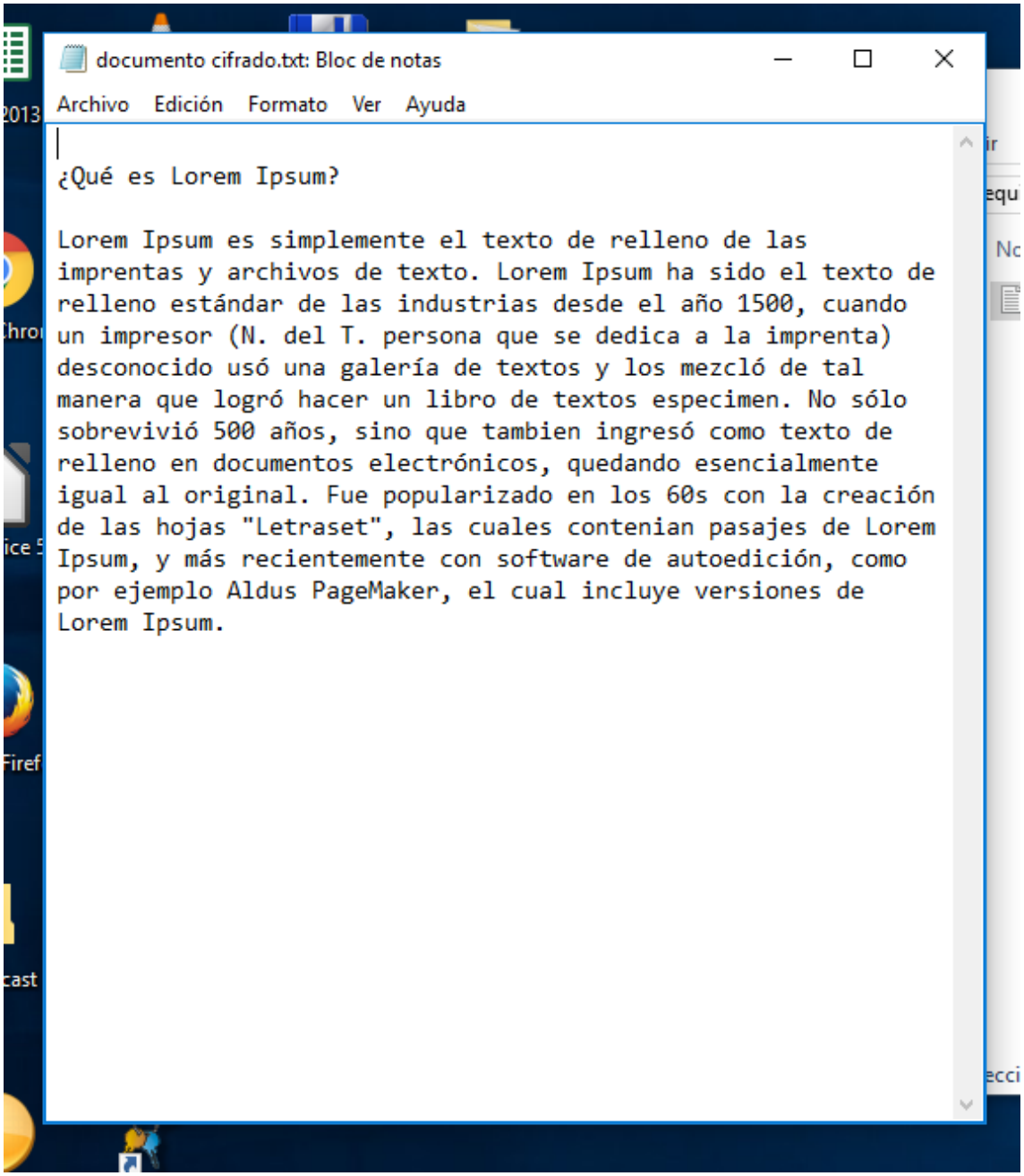
Entrando en el escritorio del usuario que encripto el archivo, pero siendo otro usuario, si intento copiar la carpeta en un pendrive obtenemos este mensaje



Vamos a darle a si, a ver qué pasa….



Y poniendo luego el pendrive en otro equipo podemos ver el contenido

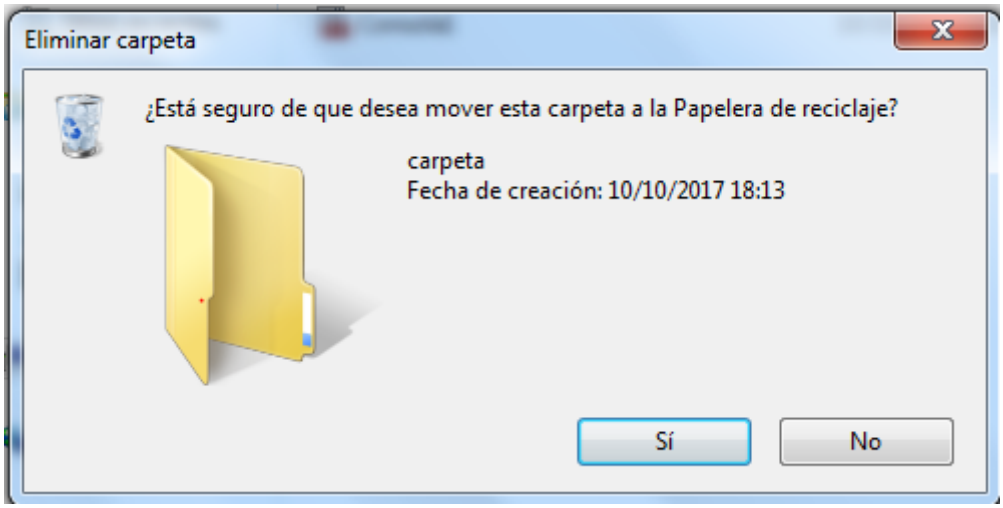


Esto quiere decir, que la única forma de que los datos estén un poco seguros es que desinstales el certificado, y no lo dejes en el sistema para instalarlo

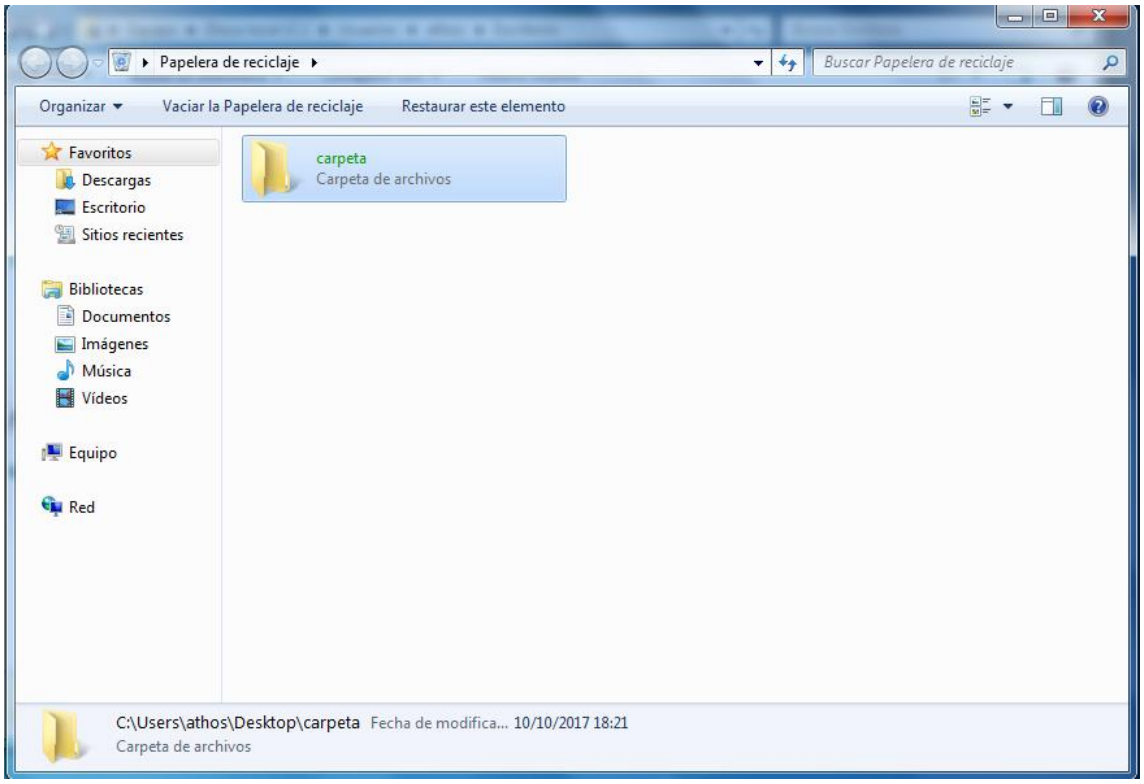
La segunda sin el certificado instalado

Intento de borrado de archivos encriptados:

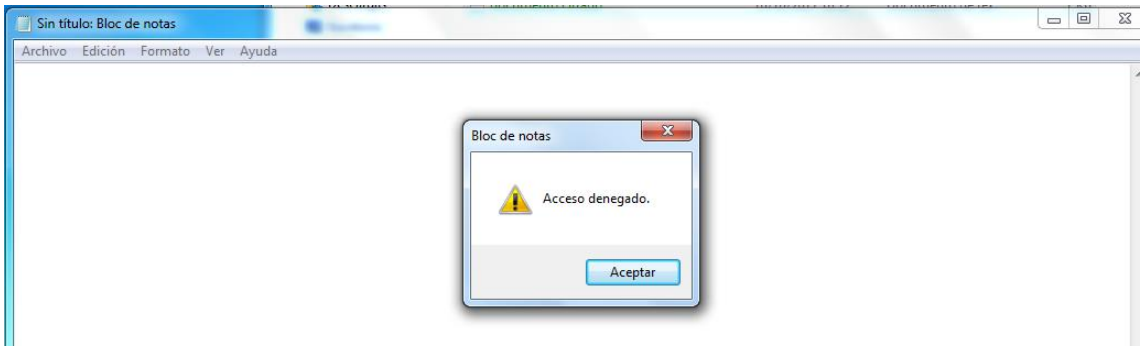
La última prueba que vamos a realizar es la eliminación de los archivos encriptados.



Y como podemos ver, en la papelera tenemos los documentos.



Ahora vamos a intentar restaurarlos, a ver si por un casual, nos deja ver el contenido.



Pero por suerte no nos deja verlos.