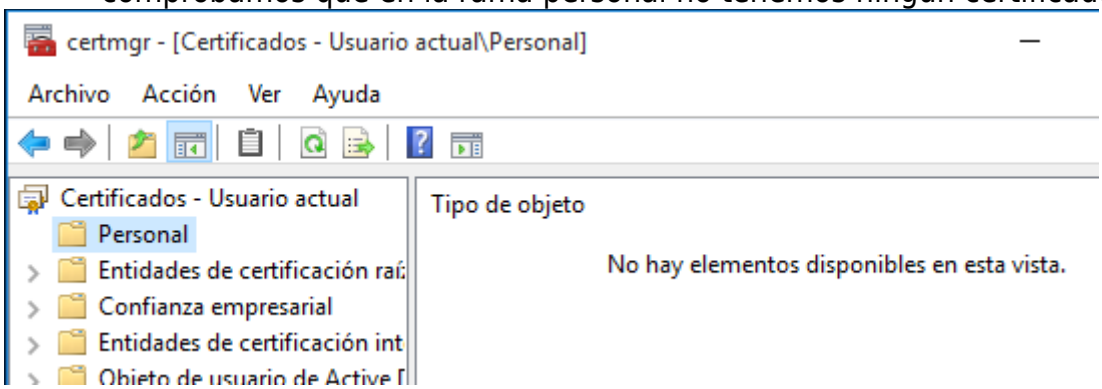
WINDOWS – HOJA DE PRÁCTICAS

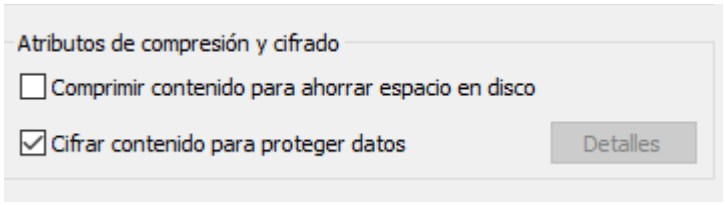
Ejercicios de Encriptación

Proceso de Encriptación

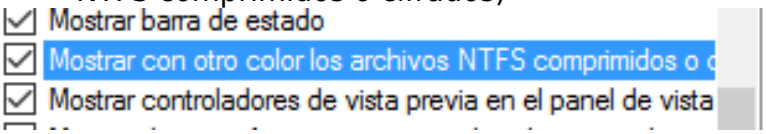
- Creamos a un usuario limitado llamado encriptador
- Iniciamos sesión con ese usuario
- Ejecutamos la consola de certificados (Inicio →certmgr.msc) y comprobamos que en la rama personal no tenemos ningún certificado.



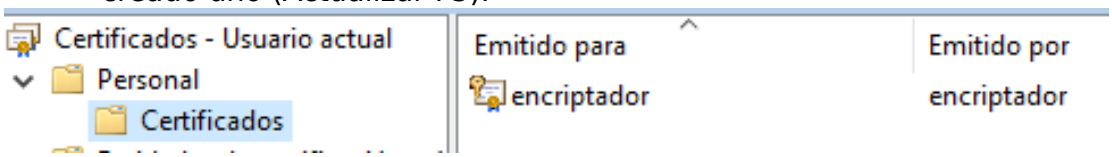
- Creamos la carpeta C:\Encriptada
- La encriptamos y le decimos que encripte su contenido.



- Resaltamos en el explorador de archivos los archivos y carpetas encriptados (Herramientas→Ver→Mostrar con otro color los archivos NTFS comprimidos o cifrados)



- Observamos nuestros certificados y comprobamos que ya se nos ha creado uno (Actualizar F5).



- En encriptada creamos un archivo de texto llamado secreto.txt y escribimos algo en el.
- Comprobamos como el acceso al contenido del archivo es transparente para nuestro usuario a pesar de estar encriptado.

WINDOWS – HOJA DE PRÁCTICAS

Comprobación de la restricción de acceso

- Le damos permiso CT a un usuario administrador
- Abrimos sesión como el usuario Administrador y comprobamos que aunque tenemos permiso para ver el contenido del archivo no podemos acceder a el.
- Como administrador, ya que tengo permiso CT, me apropio del documento e intento acceder a su contenido pero no es así.

Que ocurre cando copiamos un archivo encriptado

- Si lo copia el usuario encriptador
  - Si lo copia a una carpeta diferente
  - Si lo copia a una partición FAT
- Otro usuario
  - Puede copiarlo?

WINDOWS – HOJA DE PRÁCTICAS

Recuperación ante desastres

-Copia de Seguridad de Nuestro Certificado

- Iniciamos sesión como encriptador. Queremos crear una copia de seguridad de nuestro certificado. Para ello:
- Abrimos la consola de certificados (Inicio→Ejecutar→certmgr.msc). Seleccionamos nuestro certificado y le damos a exportar. Nos pide una contraseña que luego necesitaremos para reinstalar el certificado, y finalmente nos crea un archivo .pfx que es una copia de seguridad de nuestro certificado.

-Recuperación ante un borrado accidental de nuestro certificado

- Borramos nuestro certificado, reiniciamos sesión y comprobamos que no podemos acceder a nuestro documento.
- Hacemos un doble clic sobre la copia de seguridad del certificado y aparece un asistente para importar el certificado. Necesitamos la contraseña que usamos en la exportación.
- Comprobamos que ahora ya podemos acceder a nuestro documento

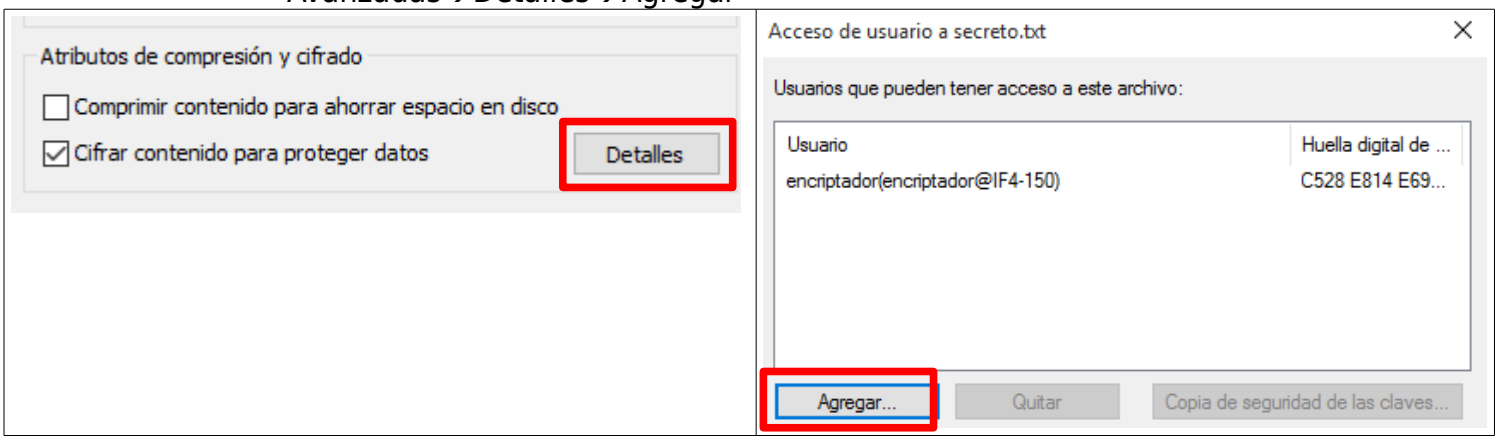
-Recuperación ante un borrado accidental de nuestro usuario

- Antes de borrar a nuestro usuario asegúrate de que tenemos almacenado en un lugar seguro nuestro certificado.
- Borra al usuario encriptador
- Creamos a otro usuario con el mismo nombre
- Intentamos acceder al contenido del archivo encriptado. ¿Por qué no podemos acceder?
- Abrimos la consola de certificados y vemos que este usuario no tiene ninguno.
- Ejecuto la copia de seguridad del certificado
- Comprobamos en la consola que ya tenemos uno para este usuario y comprobamos que ahora sí podemos acceder al contenido del documento.
- Hacemos al nuevo usuario propietario del documento.

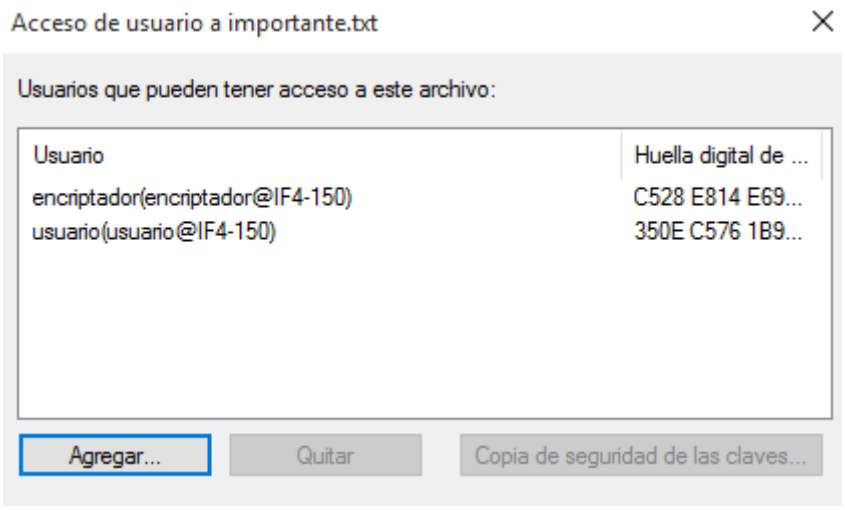
WINDOWS – HOJA DE PRÁCTICAS

-Conceder acceso a otro usuario a nuestros archivos encriptados

- Creamos otro usuario limitado llamado usuario
- Necesitamos que tenga un certificado, así que abrimos sesión con el y encriptamos cualquier archivo
- Comprobamos que usuario no puede ver el contenido de secreto.txt
- Abrimos sesión como encriptador
- Seleccionamos el archivo secreto.txt. Propiedades→Opciones Avanzadas→Detalles→Agregar



- Sólo podemos agregar los usuarios que tienen un certificado.
- Agregamos a usuario



- Comprobamos que amigo ya puede acceder a su contenido

-Creando un agente de recuperación

Un agente de recuperación es otro usuario, normalmente un Administrador, que puede usar nuestros archivos encriptados. Esto permite la recuperación de nuestro fichero encriptado si algo pasase con nuestra clave privada. Eso si, el agente de recuperación solo podrá acceder a los archivos encriptados después de convertirse en agente de recuperación.

- Abrimos sesión como el usuario Administrador
- En una consola ejecutamos `cipher /r:nombrefichero`. Esto nos crea un fichero .pfx y un fichero .cer con el nombre de fichero que hemos especificado anteriormente que serán el certificado del agente de recuperación. Nos pedirá una contraseña igual que cuando exportamos un certificado.

Con estos certificados podemos convertir a cualquier usuario en agente de recuperación, para convertir al usuario actual.

- Conectarnos con la cuenta del usuario que queremos designar como agente de recuperación.
- En la consola de certificados, Usuario Actual\Personal.
- En el menú Acción→Todas las tareas→ Importar, lanzará el asistente de recuperación.
- Escogemos el certificado de encriptación (el fichero .pfx).
- Escribimos la contraseña para este certificado (la tecleada anteriormente cuando ejecutamos el comando cipher) y seleccionamos "marcar esta clave como exportable". Pulsamos siguiente.
- Seleccionamos: automáticamente seleccionar el certificado basado en el tipo de certificado y pulsamos siguiente. A continuación pulsamos finalizar.
- En Local Security Settings (ejecutando: secpol.msc) vamos a Security Settings→Public Key Policies→Encrypting File System
- Menu Acción → Añadir un agente de recuperación. Pulsamos siguiente.
- En la página de seleccionar agente de recuperación, pulsamos el botón de Ver y navegamos a la carpeta que contiene el .cer que hemos creado. Seleccionamos el fichero y le damos "Abrir". Ahora nos mostrará el nuevo agente como USER_UNKNOWN. Esto es normal debido a que el nombre no está almacenado en el fichero.