

SEGURIDAD DE SISTEMAS INFORMÁTICOS

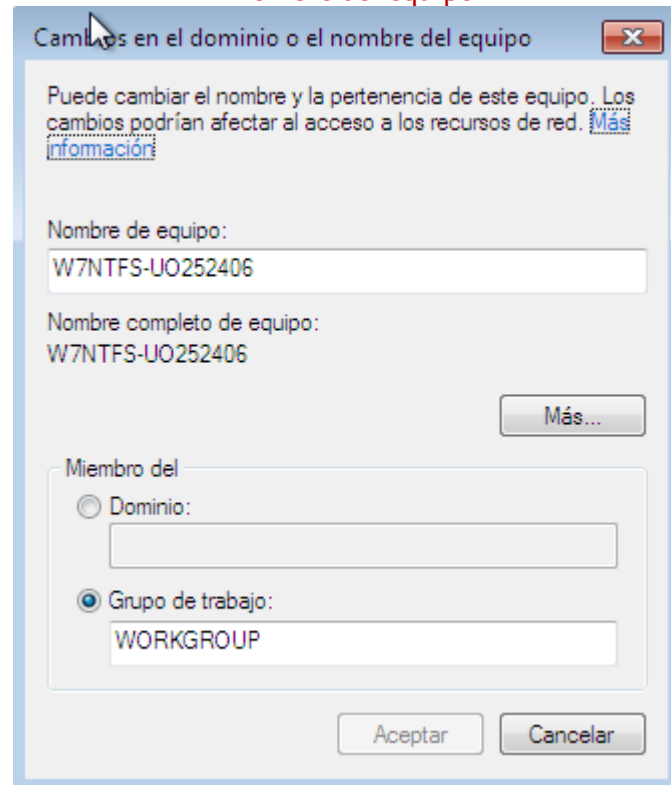
Práctica 1 – Seguridad NTFS



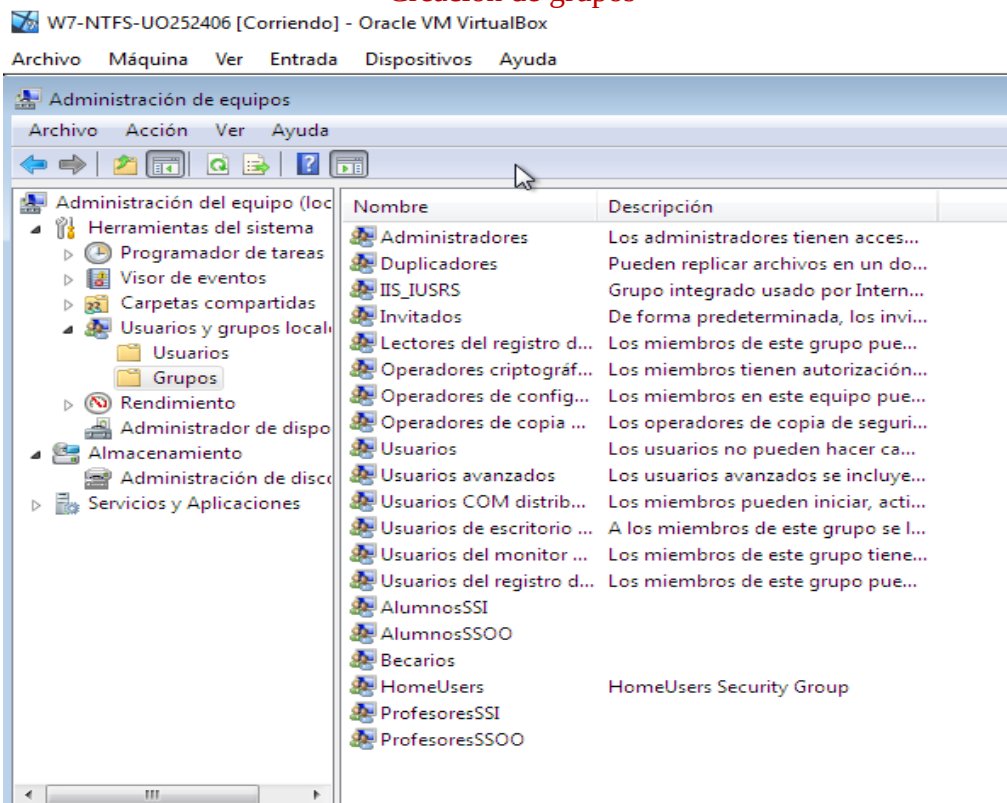
Pablo Menéndez Suárez – UO252406

Preparación del entorno

Nombre del equipo

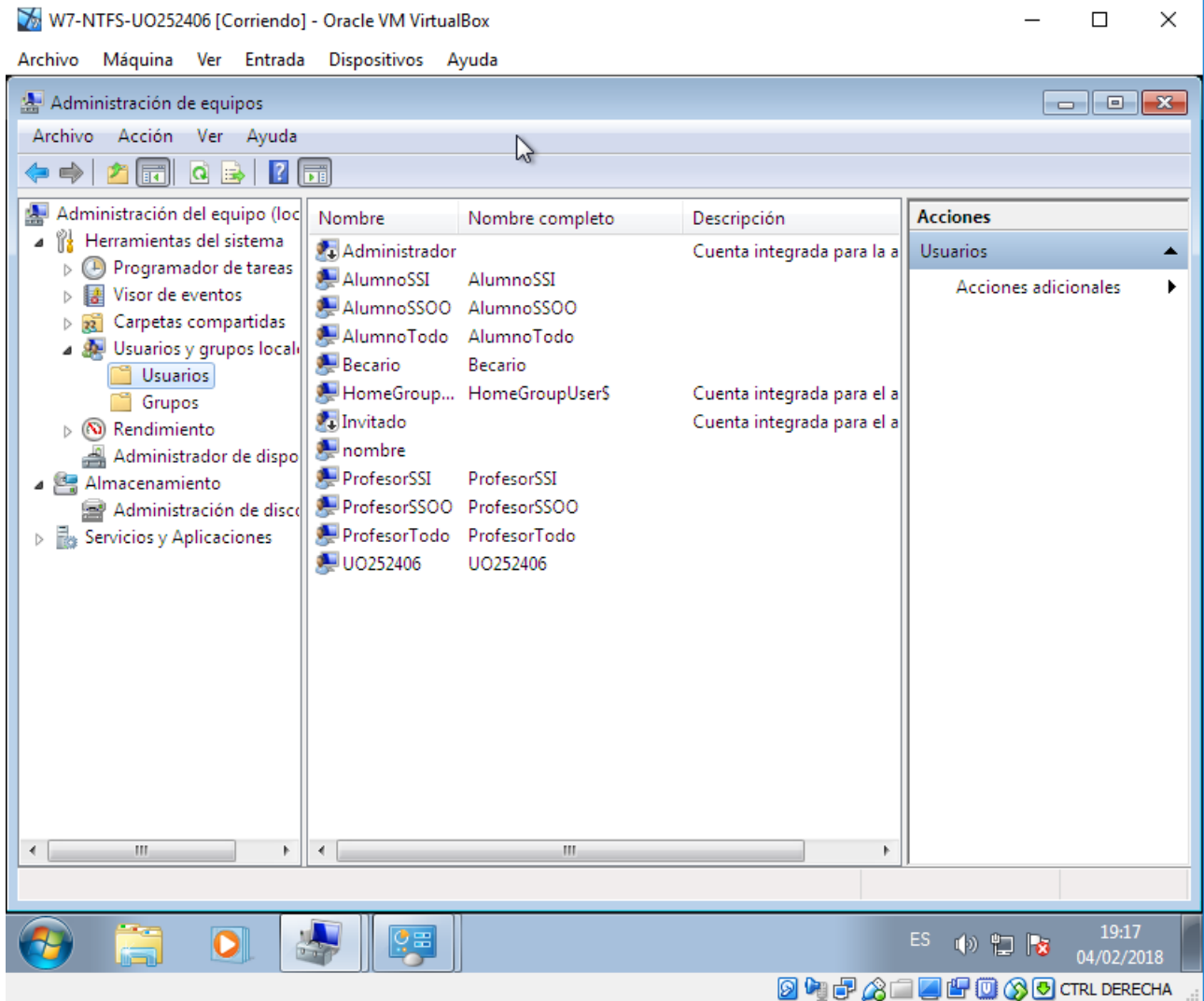


Creación de grupos



Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS

Creación de usuarios

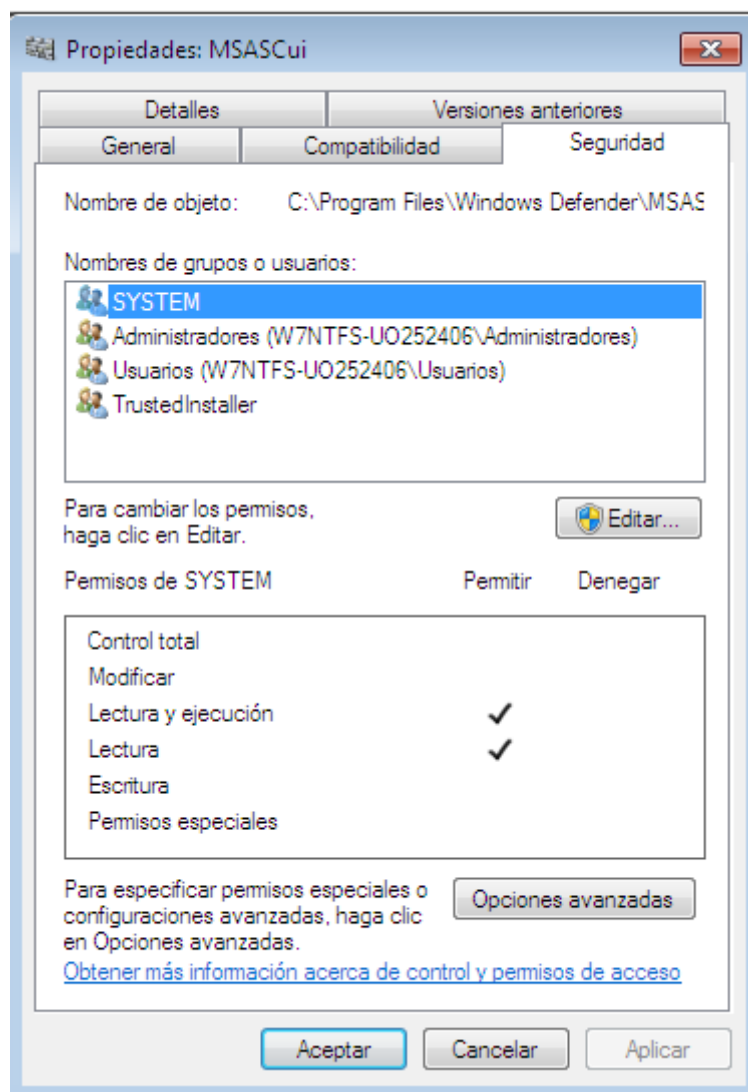


Parte 1: Exploración de permisos

Crea una carpeta para la asignatura de SSI (UOXXXX_SSI) y otra para la de SSOO (UOXXXX_SSOO). Haz que todos los alumnos puedan leer lo que se vaya a almacenar en ella, mientras que todos los profesores y becarios puedan leer, almacenar y borrar la información de dichos directorios.

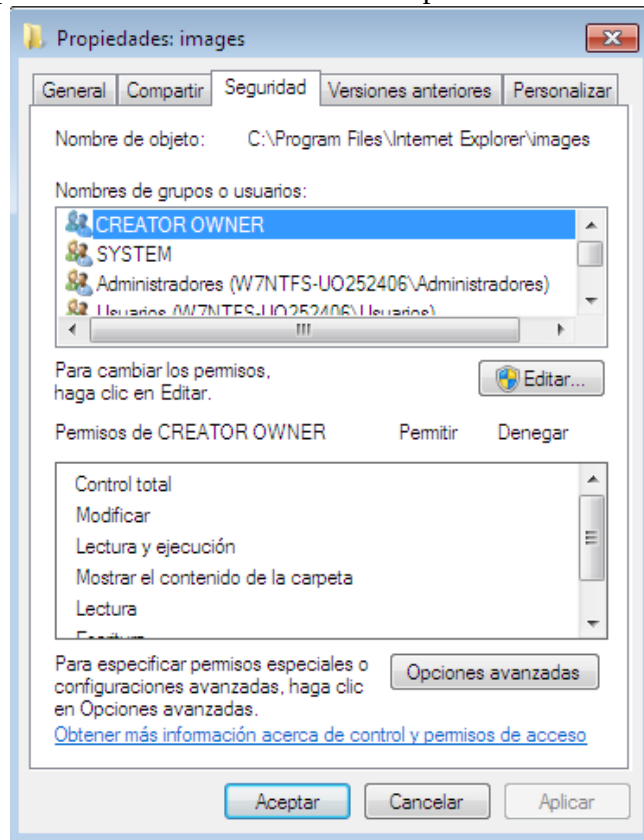
- Permisos de ficheros:**

- 1) **Lectura:** Permite leer el fichero y ver sus atributos, propietarios y permisos asociados
- 2) **Escritura:** Permite modificar el fichero, cambiar sus atributos y ver sus propietarios y permisos asociados.
- 3) **Leer y ejecutar:** Igual que Lectura, pero además permite ejecutar el fichero
- 4) **Modificación:** Permite modificar y borrar el fichero, además de todo lo permitido por todos los anteriores
- 5) **Control total:** Permite todo lo anterior, además de cambiar la propiedad del fichero
- 6) **Permisos especiales**

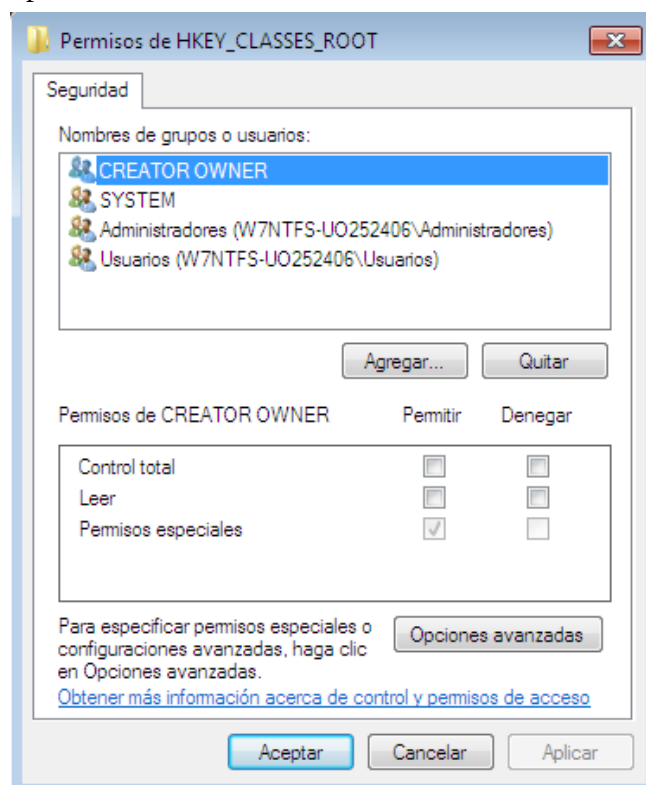


Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS

- **Permisos de carpetas:** Todos los anteriores además de mostrar el contenido de la carpeta, que permite ver el contenido de la carpeta.



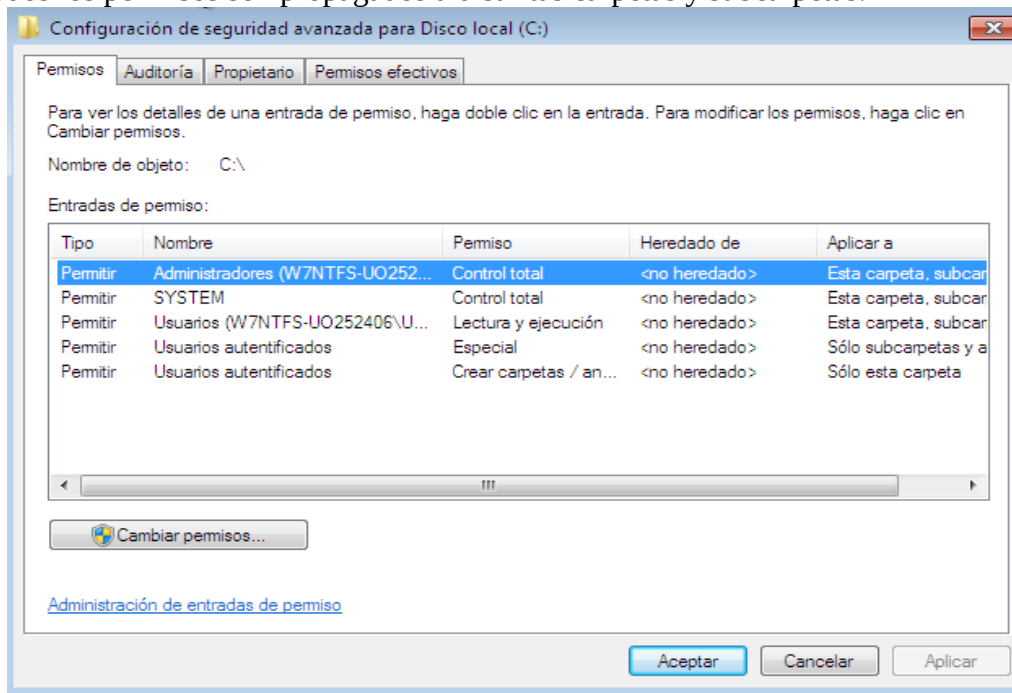
- **Permisos de elementos de registro:**
 - 1) Control total
 - 2) Leer
 - 3) Permisos especiales



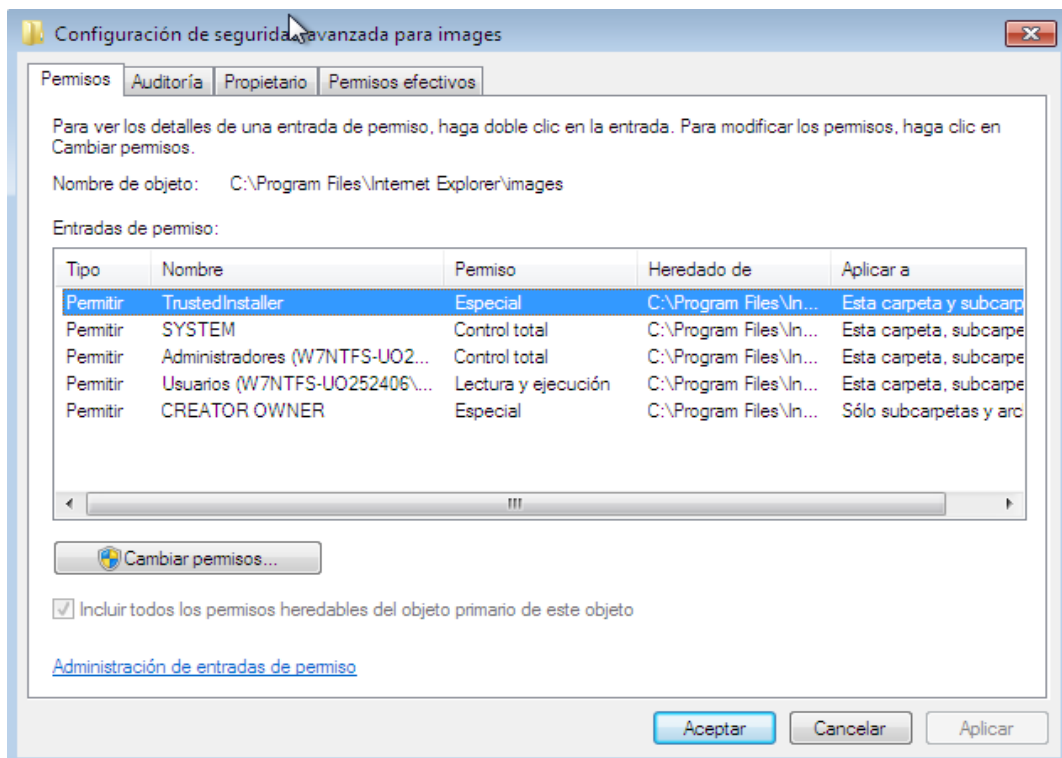
Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS

Crea una carpeta dentro de las anteriores que se llame "entregasPractica": los alumnos pueden añadir ficheros, pero no pueden ni ver el contenido ni modificar los ficheros existentes.

- **Directorio Raíz:** Podemos observar que el directorio raíz no tiene ningún permiso heredado ya que se encuentra en la parte más arriba de la jerarquía, sin embargo, sí que vemos que todos los permisos son propagados a distintas carpetas y subcarpetas.

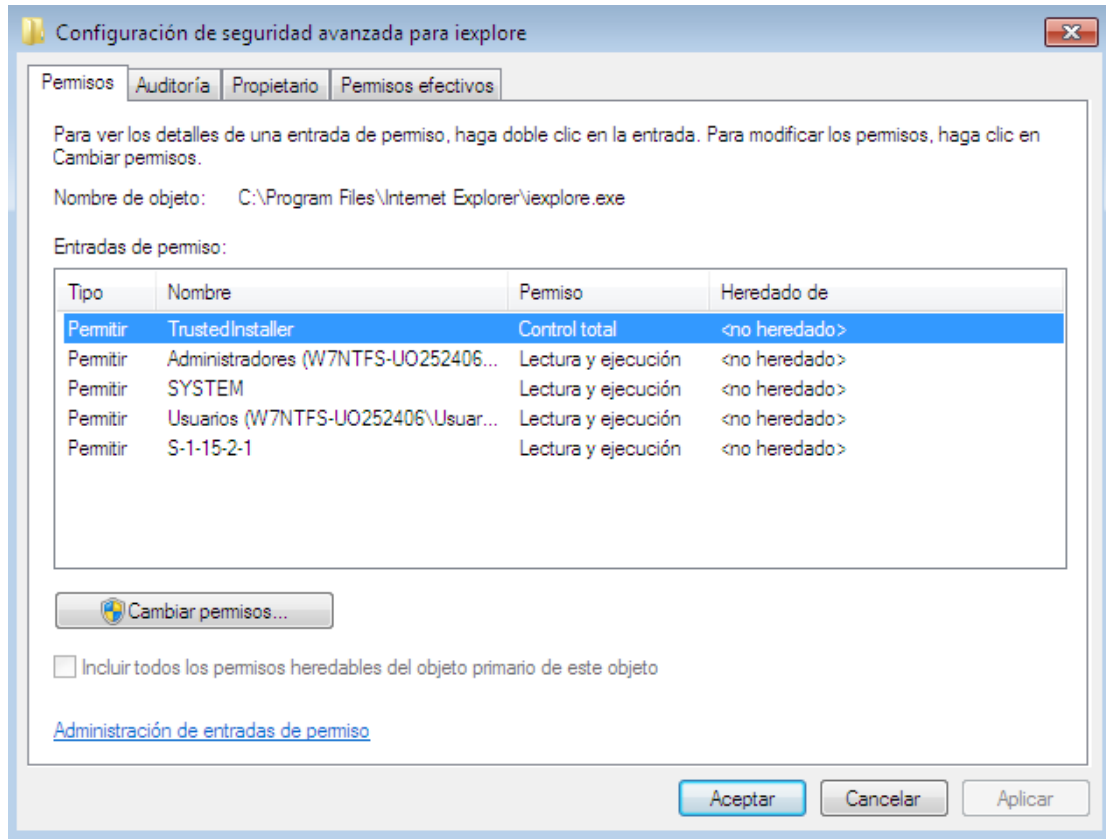


- **Directorio cualquiera (C:\Program Files\Internet Explorer\images):** Observamos que todos los permisos son heredados de la carpeta superior en la jerarquía (C:\Program Files\Internet Explorer) y además esos mismos permisos son propagados a carpetas, subcarpetas y archivos inferiores.



Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS

- **Fichero cualquiera** (C:\Program Files\Internet Explorer\iexplore): Podemos observar que este fichero no hereda ni propaga ningún tipo de permiso ya que prevalecen los permisos de ficheros sobre los de directorios.



Estudia los permisos que aparecen, tanto en la vista estándar como en la avanzada. Explica el significado de cada uno de esta última vista, y la relación que hay entre estos y los permisos normales. Estudia sobre todo el de Modificar y Control Total, viendo sus diferencias

- **Atravesar carpeta/ ejecutar archivo:** Atravesar carpeta permite o deniega el movimiento por las carpetas para llegar a otros archivos o carpetas. Ejecutar archivo permite o deniega la ejecución de archivos de programa.
- **Mostrar carpeta / leer datos:** Mostrar carpeta permite o deniega ver nombres de archivos y subcarpetas de la carpeta. Leer datos permite o deniega la vista de datos en archivos.
- **Leer atributos:** Permite o deniega la vista de los atributos de un archivo o carpeta, como sólo lectura y oculto.
- **Leer atributos extendidos:** Permite o deniega la vista de atributos extendidos de un archivo o carpeta.
- **Crear archivos / escribir datos:** Crear archivos permite o deniega la creación de archivos dentro de la carpeta. Escribir datos permite o deniega la realización de cambios en el archivo y la sobreescritura del contenido existente.
- **Crear carpetas / anexar datos:** Crear carpetas permite o deniega la creación de carpetas dentro de la carpeta. Agregar datos permite o deniega la realización de cambios al final del archivo, pero no el cambio, eliminación ni sobreescritura de los datos existentes.

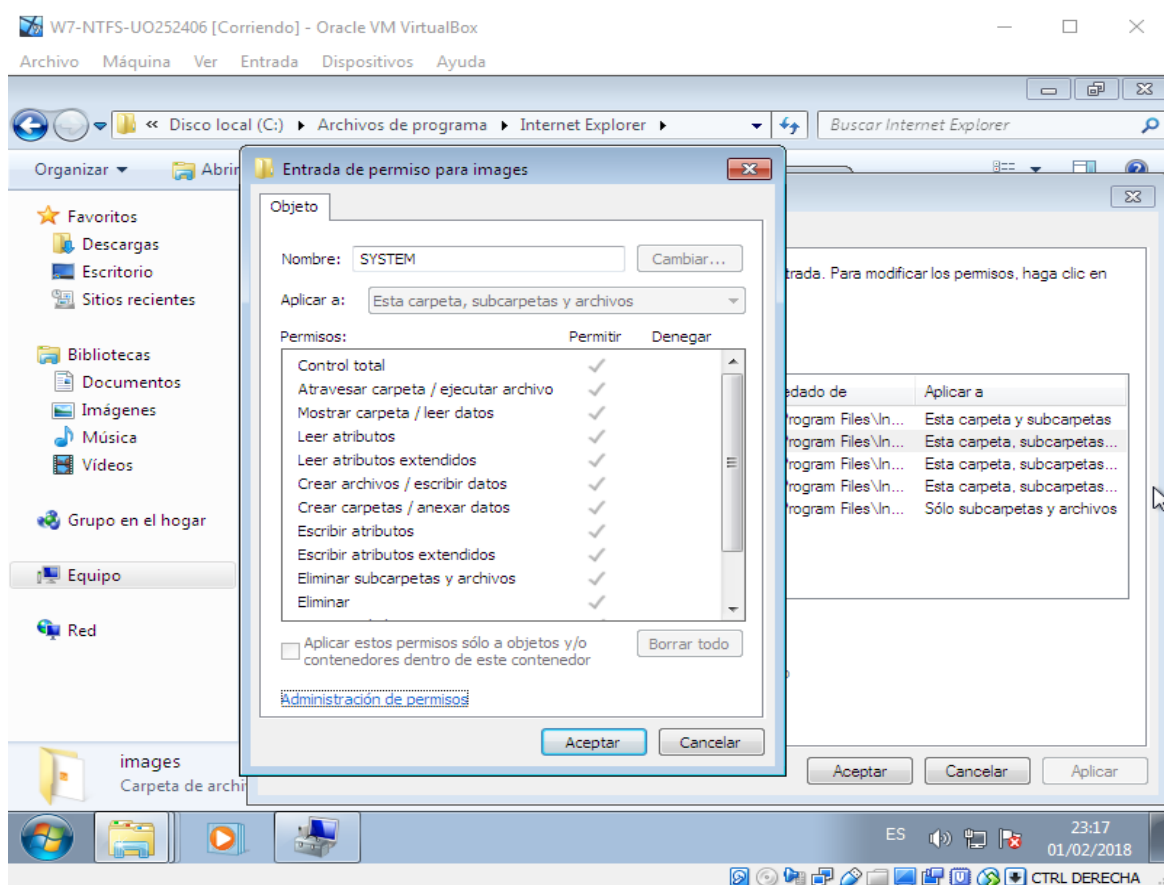
Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS

- **Escribir atributos:** Permite o deniega el cambio de los atributos de un archivo o de una carpeta.
- **Escribir atributos extendidos:** Permite o deniega el cambio de los atributos extendidos de un archivo o carpeta.
- **Eliminar subcarpetas y archivos:** Permite o deniega la eliminación de subcarpetas y archivos, incluso si no se ha otorgado el permiso Eliminar en la subcarpeta o archivo.
- **Eliminar:** Permite o deniega la eliminación del archivo o de la carpeta.
- **Permisos de lectura:** Permite o deniega la lectura de los permisos del archivo o carpeta.
- **Cambiar permisos:** Permite o deniega el cambio de los permisos del archivo o carpeta.
- **Tomar posesión:** Permite o deniega la toma de posesión del archivo o de la carpeta.

La relación que existe entre los permisos normales y los avanzados es que los normales son una combinación de los avanzados.

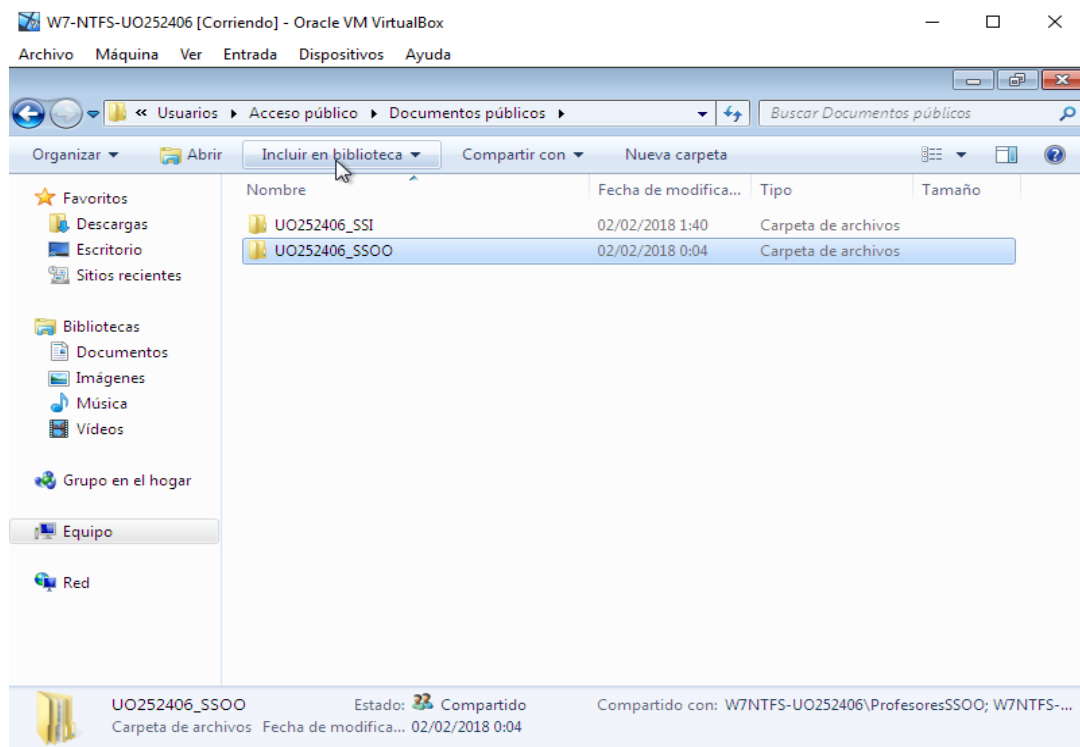
El control total en permisos normales permite todos los permisos normales mientras que el control total de permisos avanzados permite todos los permisos avanzados.

El permiso modificar en permisos normales permite todos los permisos normales de lectura y escritura mientras que el permiso modificar en permisos avanzados permite todos los permisos avanzados de lectura y escritura.

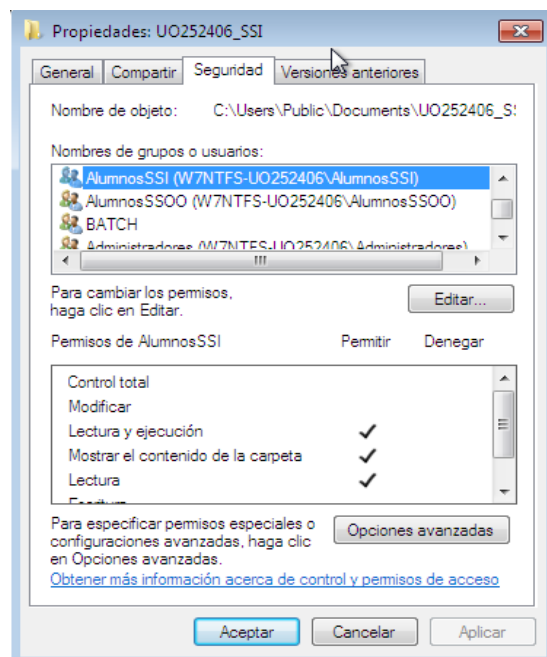


Parte 2: Ejemplos de permisos

Crea una carpeta para la asignatura de SSI (UOXXXX_SSI) y otra para la de SSOO (UOXXXX_SSOO). Haz que todos los alumnos puedan leer lo que se vaya a almacenar en ella, mientras que todos los profesores y becarios puedan leer, almacenar y borrar la información de dichos directorios.

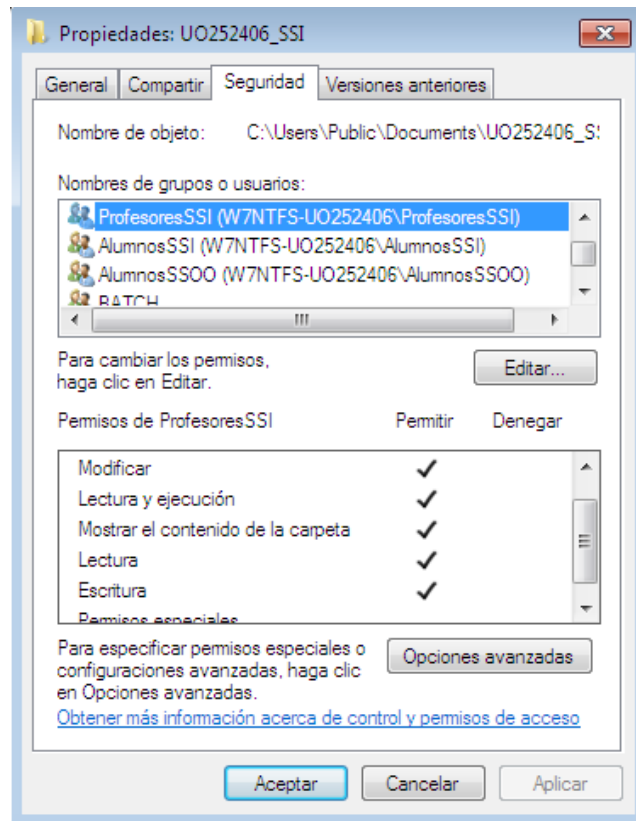


Permisos Alumnos SSI

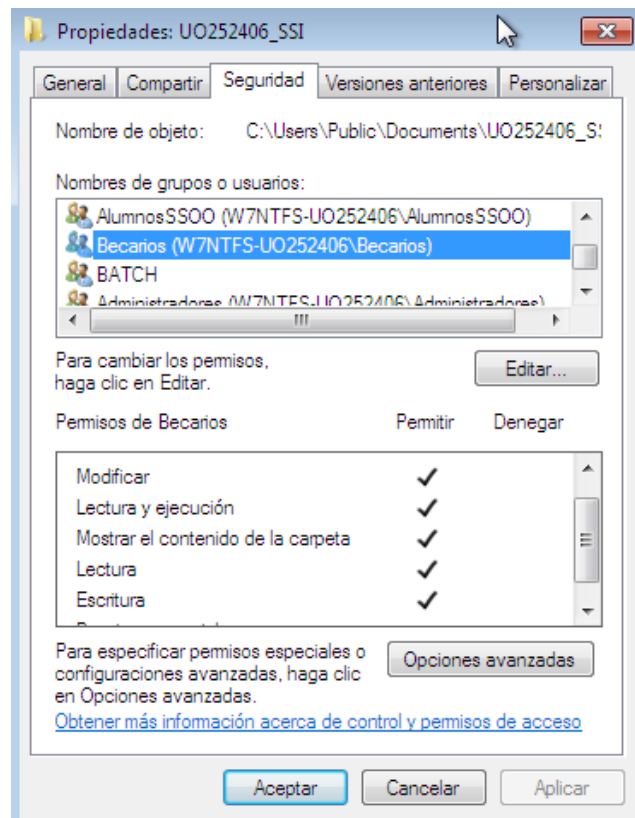


Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

Permisos Profesores SSI

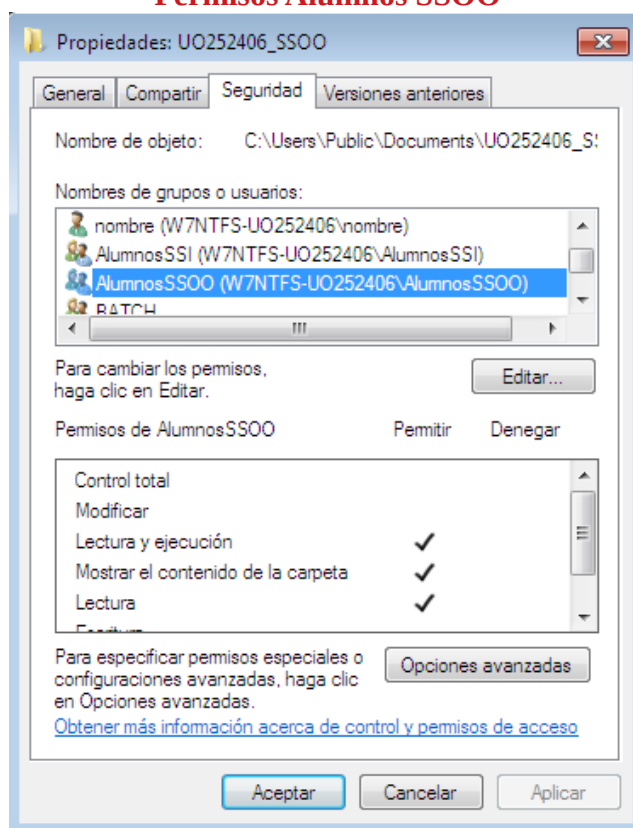


Permisos Becarios

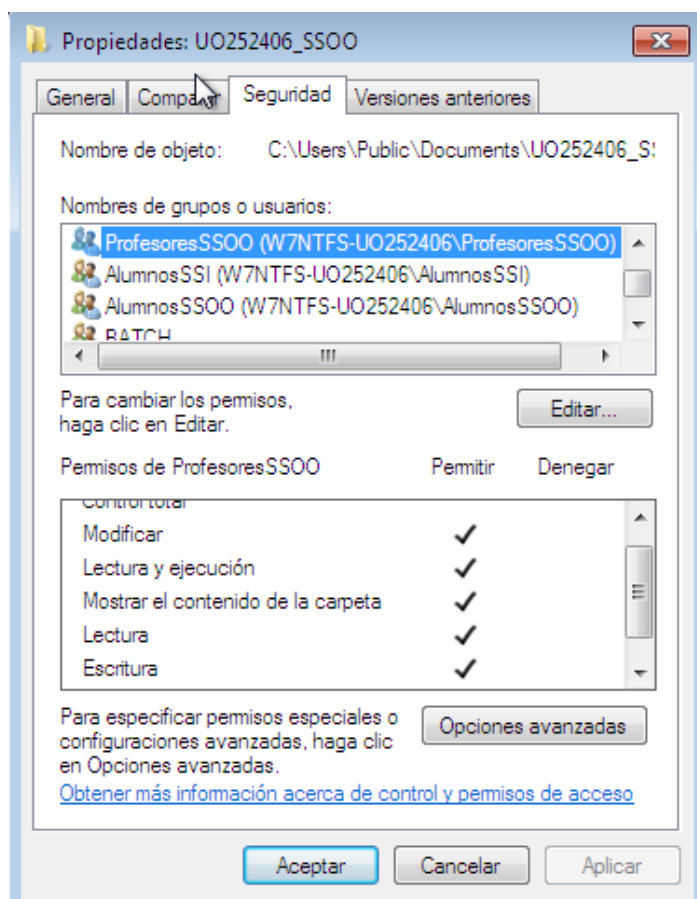


Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

Permisos Alumnos SSOO

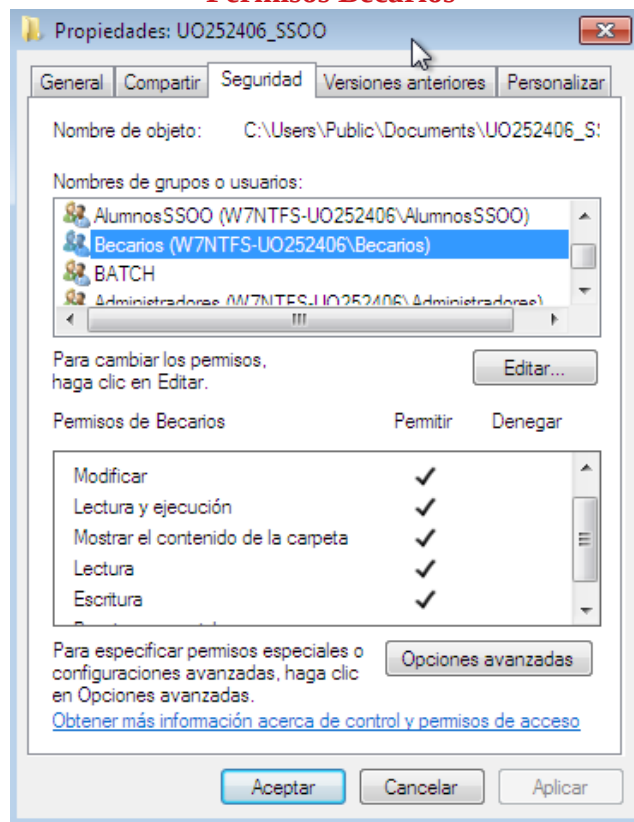


Permisos Profesores SSOO



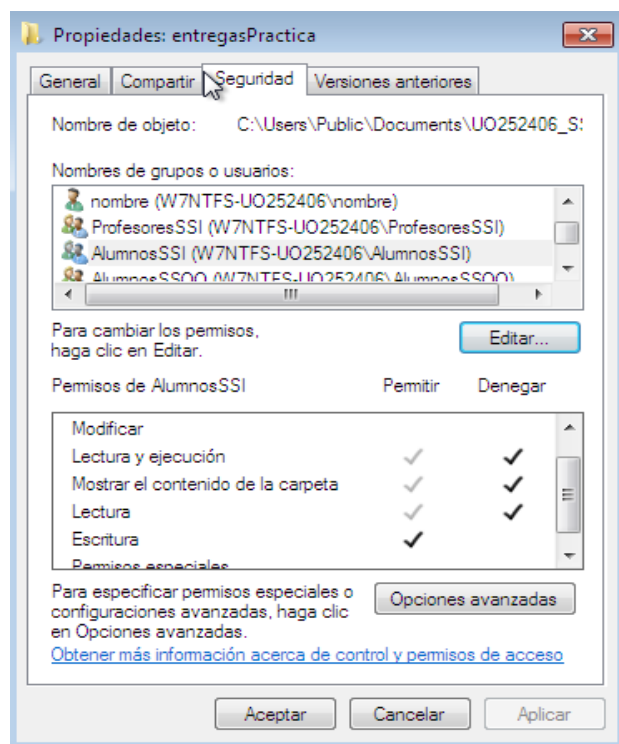
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

Permisos Becarios



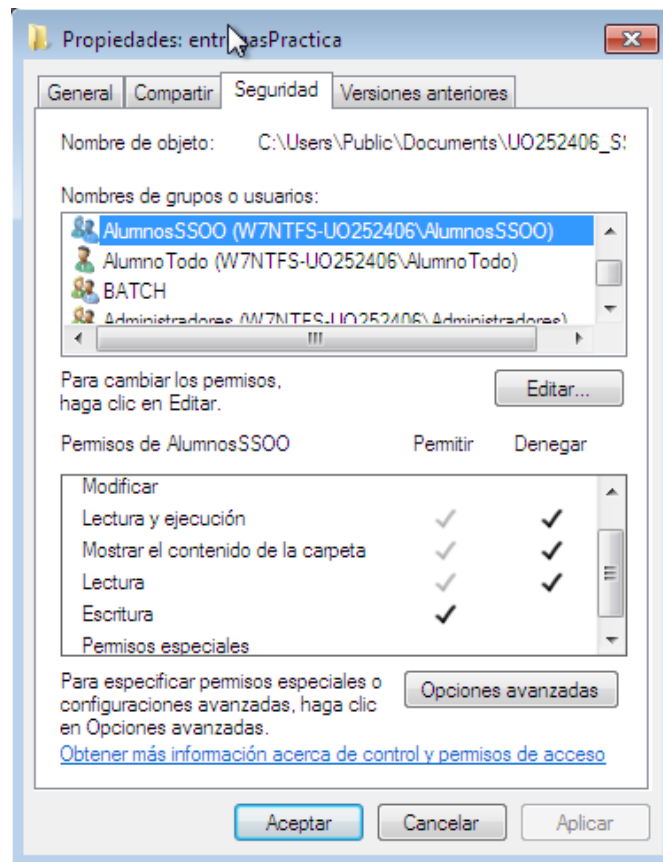
Crea una carpeta dentro de las anteriores que se llame "entregasPractica": los alumnos pueden añadir ficheros, pero no pueden ni ver el contenido ni modificar los ficheros existentes.

Permisos entregasPractica SSI



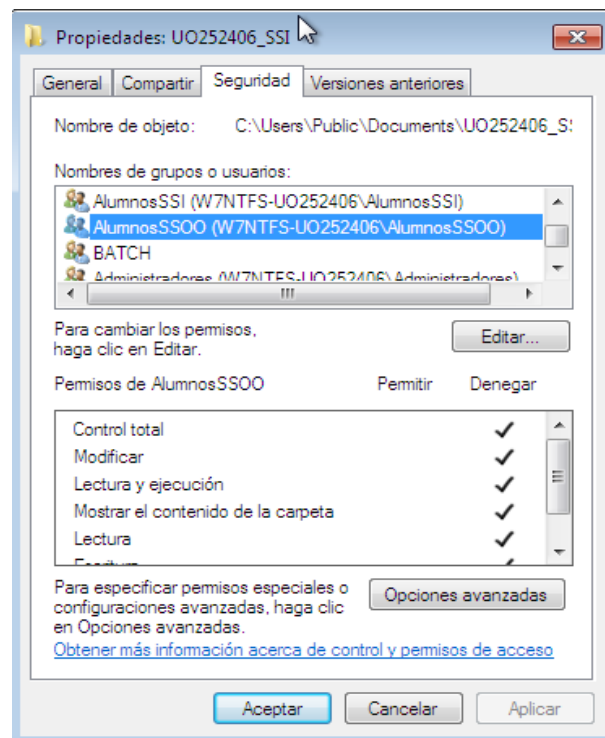
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

Permisos entregasPractica SSOO



Niega el acceso al directorio de una asignatura a los alumnos de la otra. ¿Qué pasa con AlumnoSSOO?

Negación de AlumnosSSOO en UO252406SSI

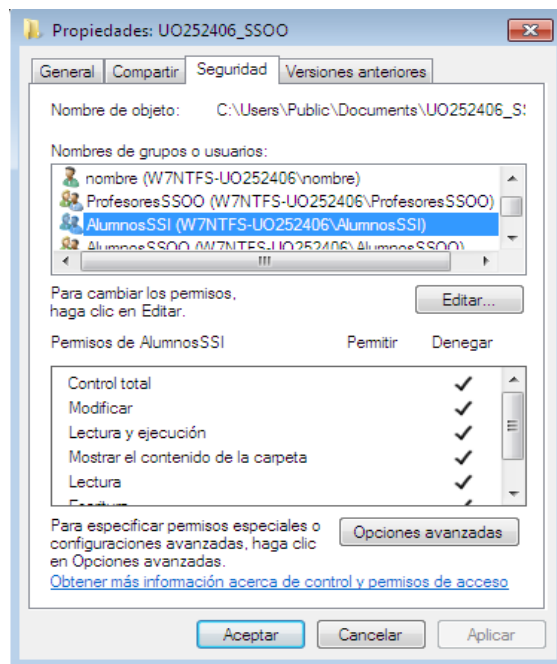


Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Práctica 1 – Seguridad NTFS

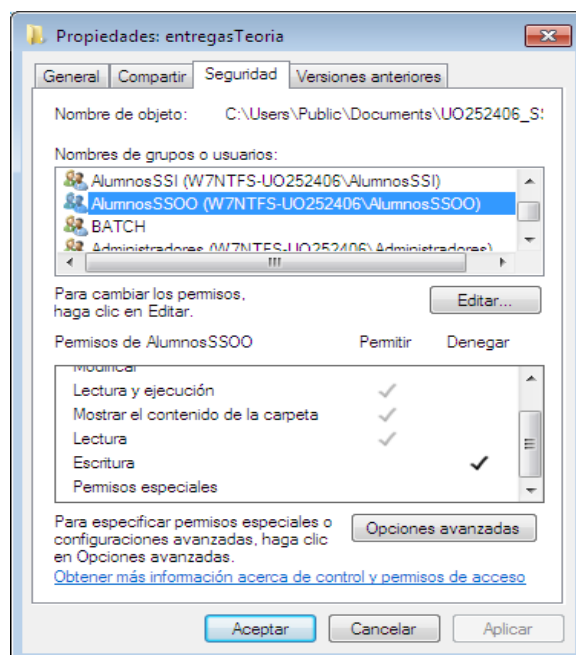
Negación de AlumnosSSI en UO252406SSOO



Al negarle el acceso a la carpeta UO252406_SSI, el AlumnoSSOO podrá visualizar tanto la carpeta UO252406_SSI como la carpeta UO252406_SSOO, pero solo podrá acceder a UO252406_SSI

Crea otra carpeta “entregasTeoria”, dentro de UOXXXX_SSOO. Deniega el permiso de escritura a los alumnos de SSOO. Crea dentro de esta carpeta un fichero relacionAlumnos, que herede los permisos de la carpeta. En relacionAlumnos, añade los permisos de escritura para los alumnos de SSOO. ¿Qué permisos tiene finalmente un alumno de SSOO? ¿Por qué? Comprueba si realmente un alumno de SSOO puede leer/escribir el fichero. ¿Puede crear un nuevo fichero en la misma carpeta? Explícalo. Prueba distintas combinaciones de "Permitir/Denegar/No especificar", e intenta describir las reglas que se aplican en caso de conflicto

Permisos entregasTeoria AlumnosSSOO

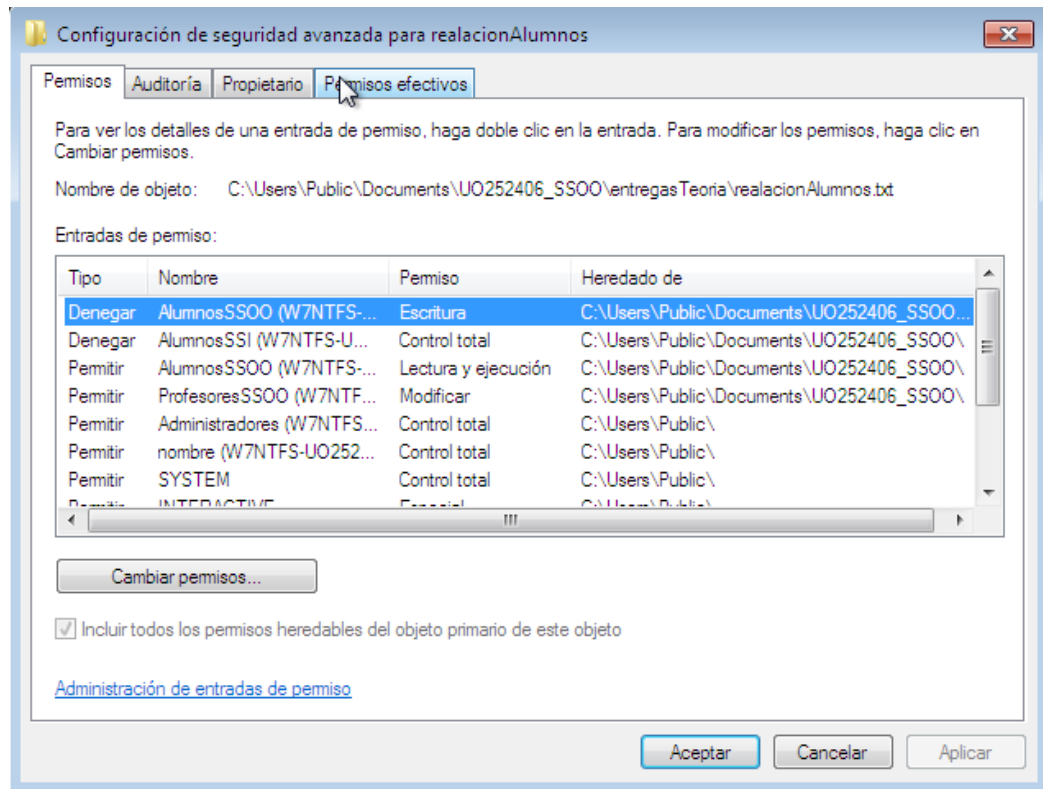


Ingeniería Informática del Software – EII

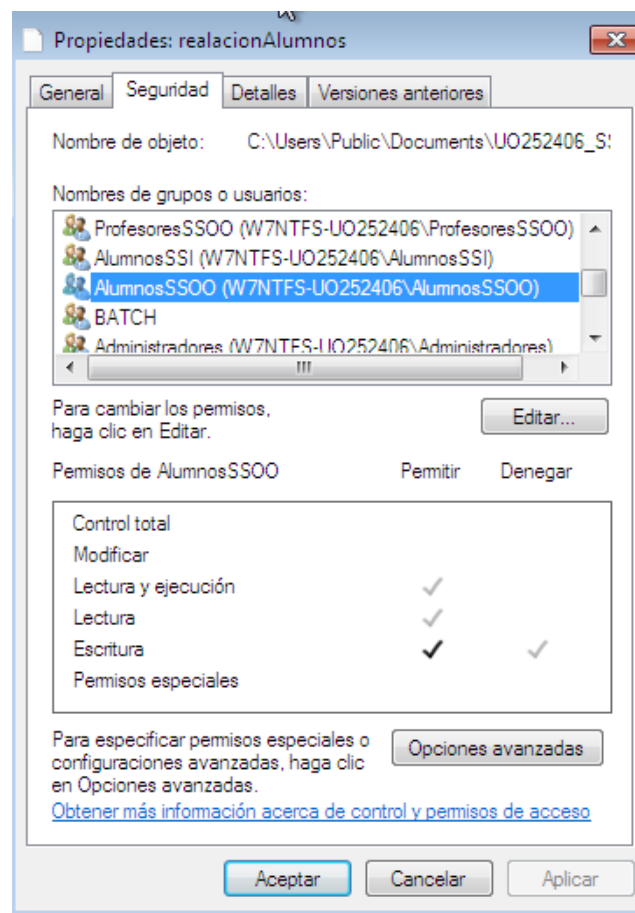
Seguridad de Sistemas informáticos

Práctica 1 – Seguridad NTFS

Permisos heredados



Permisos AlumnosSSOO en relacionAlumnos.



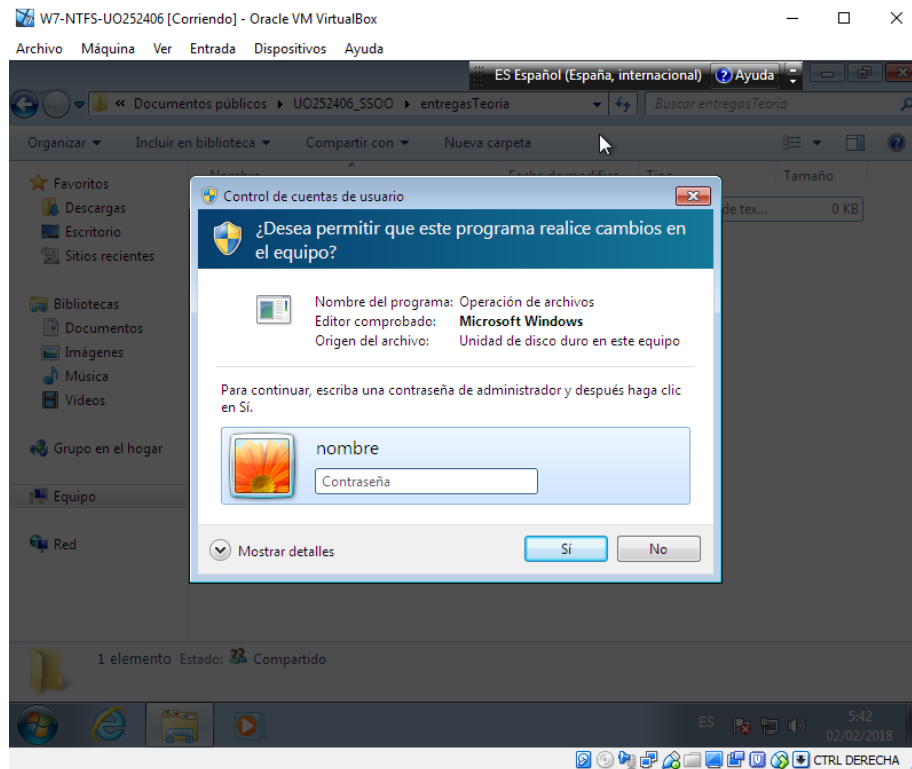
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

- Los permisos finales para un AlumnoSSOO sobre relacionAlumnos son de lectura, ejecución y escritura, ya que los dos primeros son heredados y el permiso de escritura, aunque se hereda la denegación prevalece el permiso del propio fichero.
- Un AlumnoSSOO no puede crear una carpeta dentro del directorio entregasTeoria ya que le hemos denegado los permisos de escritura.

Demostración:

Accedemos a el directorio entregasTeoria como un AlumnoSSOO.

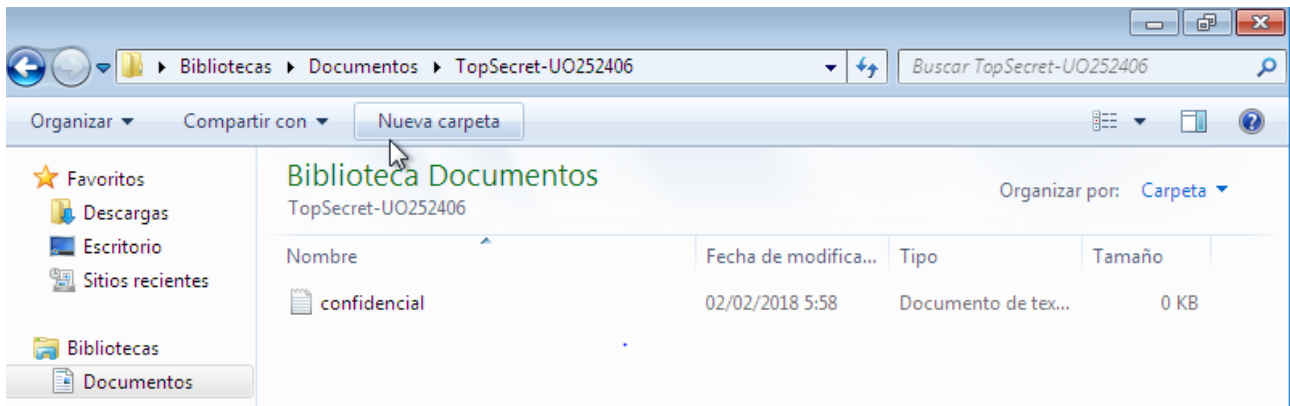
Le damos a crear nueva carpeta y nos sale el siguiente mensaje:



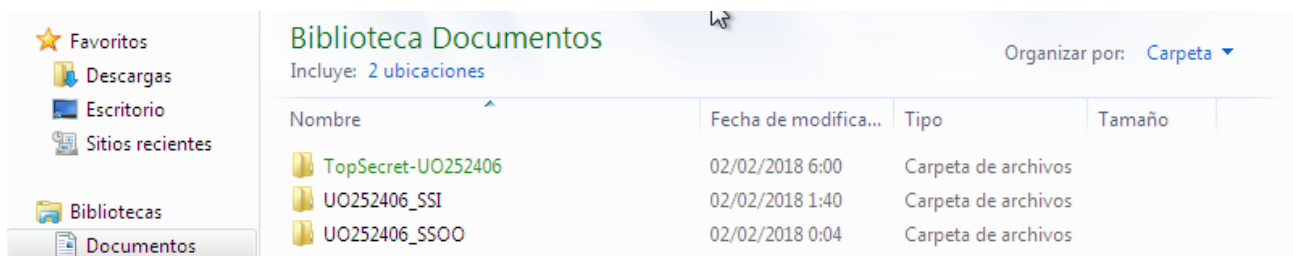
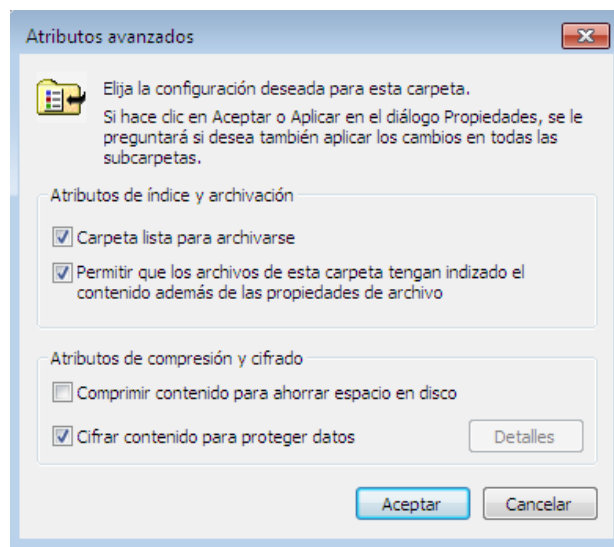
En el mensaje nos pide la contraseña de administrador, por lo que queda demostrado que los permisos son los indicados.

Parte 3: Trabajo con el sistema de ficheros encriptado

Entra en sesión con el usuario UOXXXX. Crea una carpeta dentro de ese usuario, denominada TopSecret-UOXXXX. Crea un fichero de texto denominado “confidencial” en esa carpeta y escribe tu nombre y apellidos.

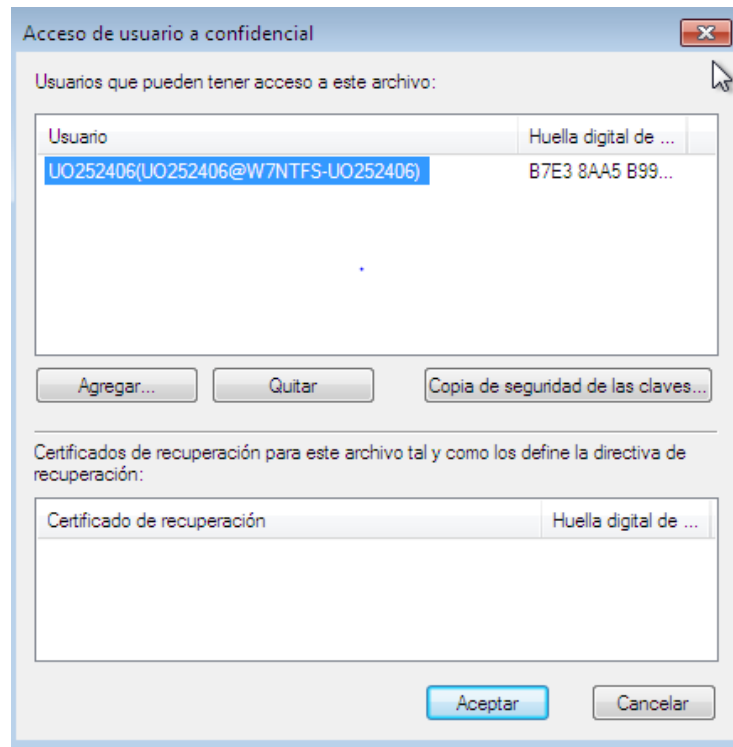


Cifra esa carpeta. (Botón derecho sobre la carpeta, Propiedades, Opciones Avanzadas, Cifrar contenido para proteger datos).

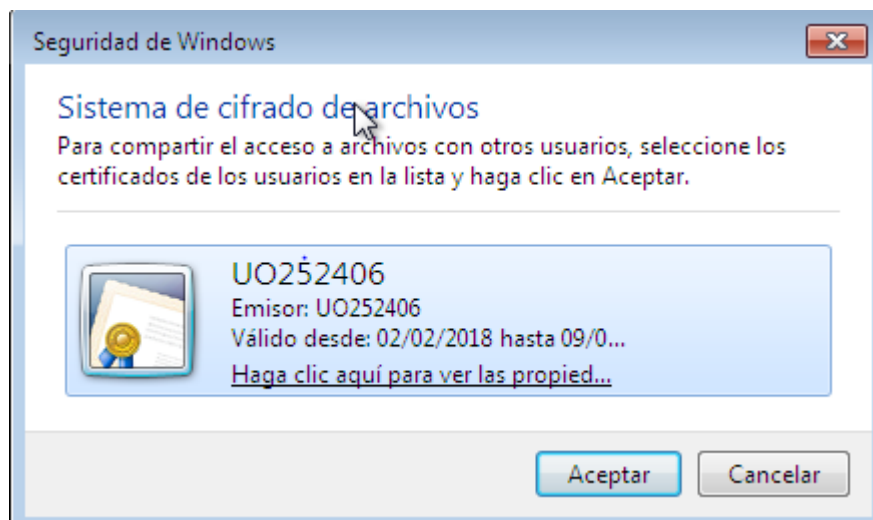


En la ventana anterior, ver los “Detalles” junto a la casilla de “Cifrar contenido para proteger datos”. Explica el contenido de esa ventana. Comprueba y documenta cómo si existe el certificado de seguridad de otro usuario se puede proporcionar acceso al archivo “confidencial” a ese otro usuario

Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS



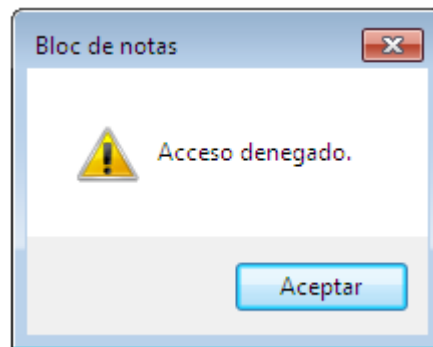
- En esta ventana podemos observar los usuarios que pueden tener acceso a el archivo y los certificados de recuperación del mismo, que en este caso no hay ninguno.
- Para proporcionar acceso a otro usuario iríamos a la ventana anterior y le daríamos a agregar. Nos aparecería la siguiente imagen:



- Si el usuario dispone de certificado de seguridad nos aparecería debajo del nuestro y tendríamos que seleccionarlo.

Entra como Administrador y accede al fichero. ¿Puedes hacerlo? ¿Por qué?

No podemos acceder ya que está cifrado y necesitaríamos el certificado de seguridad del usuario que la creo. En este caso UO252406. La ventana que aparece al intentar acceder es la siguiente:



Como Administrador crea un nuevo fichero en esa carpeta. ¿Qué ocurre con ese fichero? ¿Quién puede acceder a él? ¿Por qué? Agrega al usuario administrador para que pueda acceder al archivo confidencial.

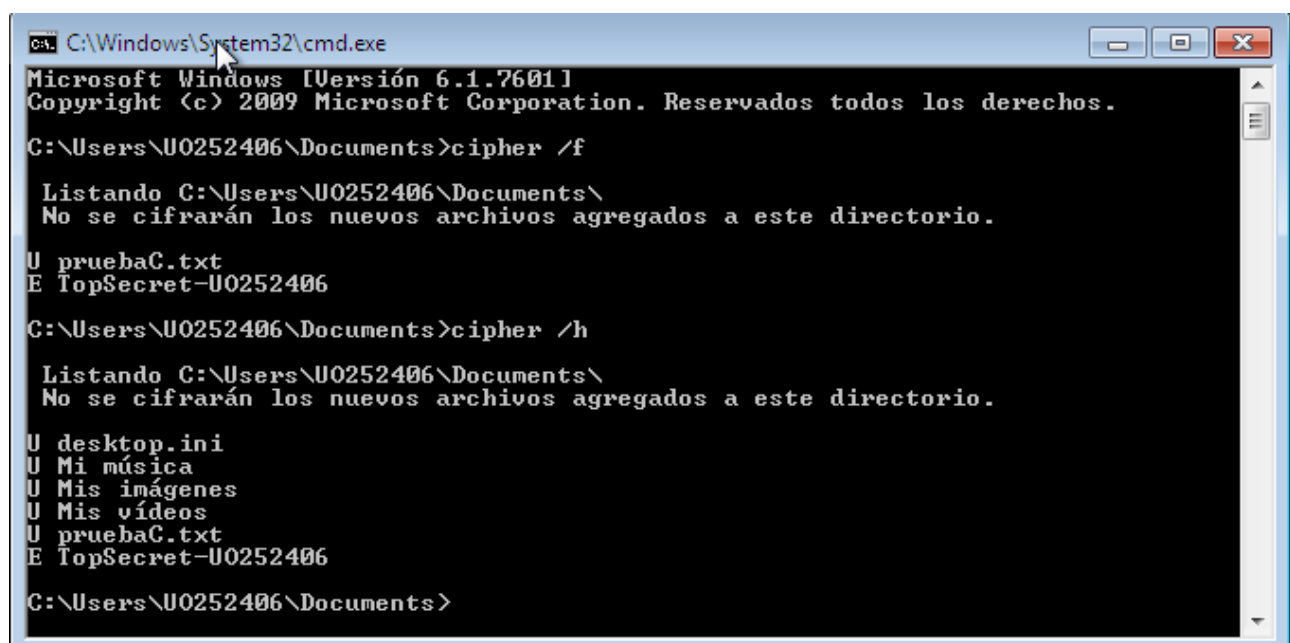
El fichero queda cifrado y solo podrá acceder a él el propio administrador ya que fue el que lo creó. Si intentamos acceder desde otro usuario como por ejemplo UO252406 se nos deniega el acceso y el mensaje que aparece es igual que el anterior.

Obtén información de la orden cipher. Prueba y explica las opciones que más te llamen la atención.

Muestra o cambia el cifrado de directorios y archivos en volúmenes NTFS. Si se utiliza sin parámetros, cipher muestra el estado de cifrado del directorio actual y los archivos que contiene.

/f: Fuerza el cifrado o descifrado de todos los objetos especificados.

/h: muestra archivos con atributos ocultos o del sistema



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\UO252406\Documents>cipher /f

Listando C:\Users\UO252406\Documents\
No se cifrarán los nuevos archivos agregados a este directorio.
U pruebaC.txt
E TopSecret-UO252406

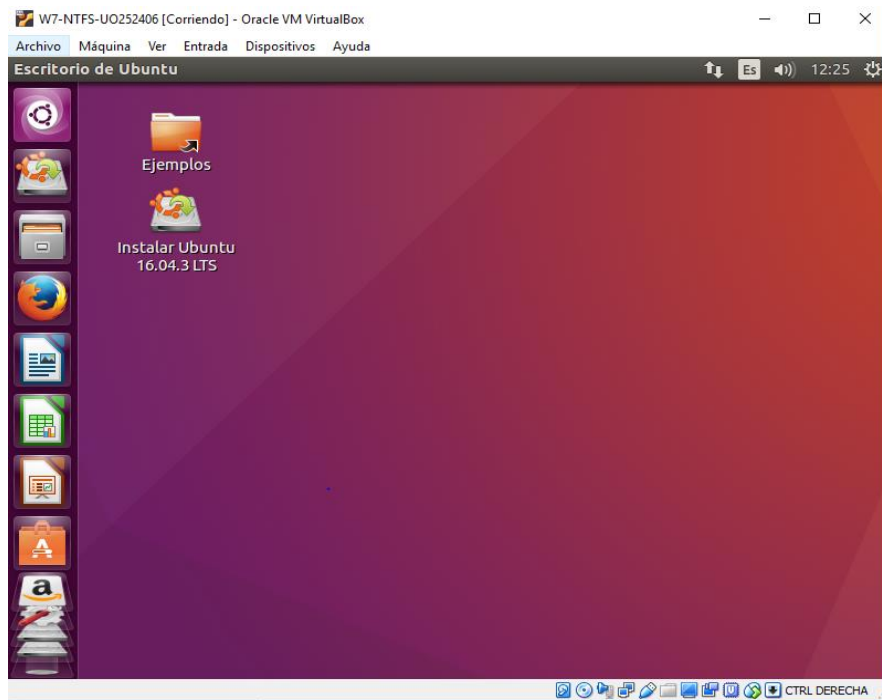
C:\Users\UO252406\Documents>cipher /h

Listando C:\Users\UO252406\Documents\
No se cifrarán los nuevos archivos agregados a este directorio.
U desktop.ini
U Mi música
U Mis imágenes
U Mis vídeos
U pruebaC.txt
E TopSecret-UO252406

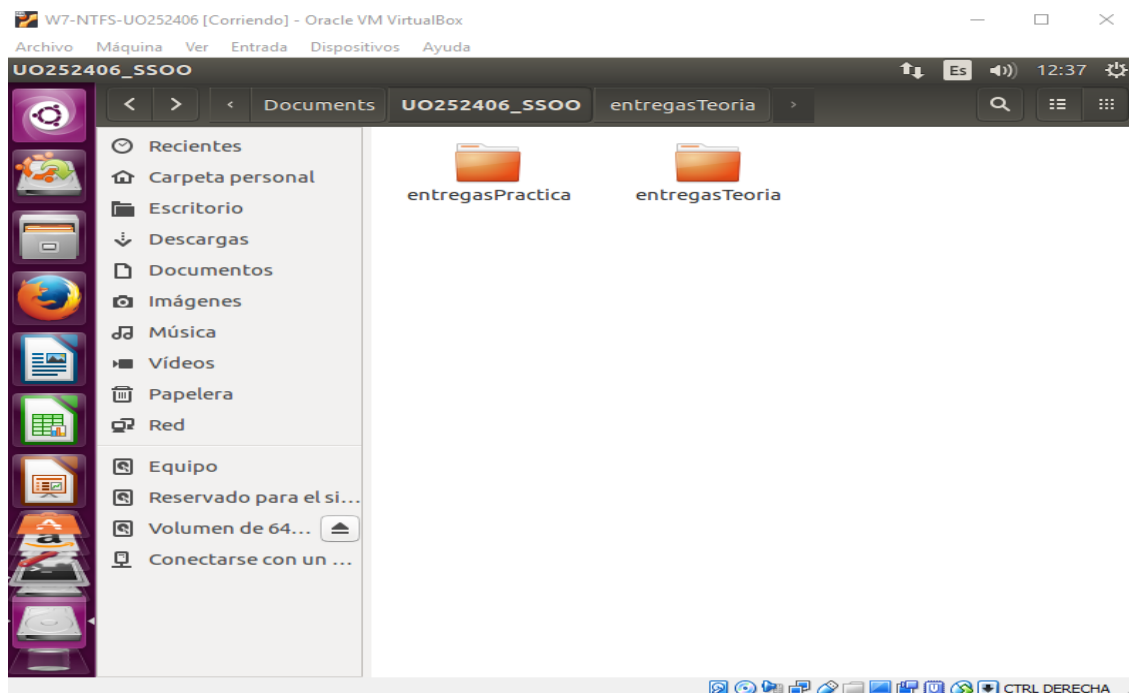
C:\Users\UO252406\Documents>
```

Parte 4: ¡Al ataque!

Arranca tu máquina virtual con un sistema Linux (Ubuntu desktop, por ejemplo), utilizando un LiveCD. Configuración-Almacenamiento-Unidad anfitrión-Unidad óptica, seleccionamos la imagen descargada y marcamos CD/DVD vivo.



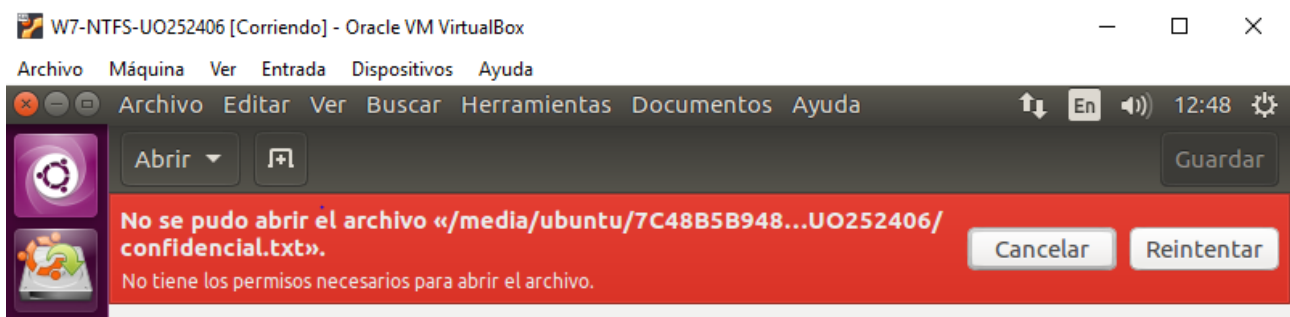
Accede al disco duro (con sistema de ficheros NTFS). Navega por el disco, buscando las carpetas y ficheros que protegiste usando NTFS en ejercicios anteriores. ¿Puedes acceder a ellos? ¿Por qué?



Tenemos control total sobre los ficheros ya que somos administradores y tenemos todos los permisos.

En la misma situación anterior, accede a la carpeta TopSecret-UOXXXX. ¿Puedes acceder a la carpeta o a su contenido? ¿Por qué?

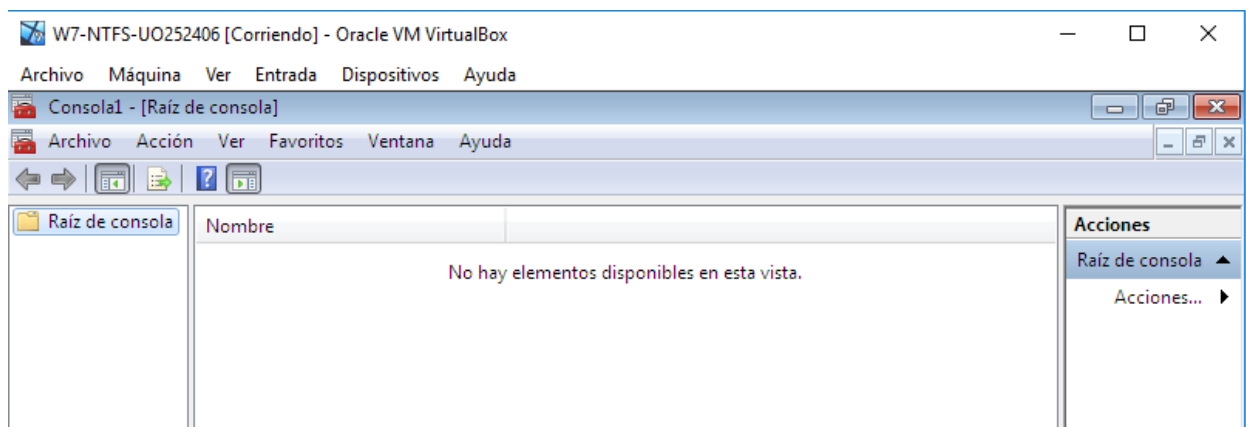
Podemos visualizar el contenido de la carpeta, sin embargo, no tenemos los permisos necesarios para acceder al fichero confidencial ya que está encriptado y nos salta el siguiente mensaje:



Parte 5: Opciones avanzadas

Exporta tu clave privada (usuario UOXXXX). Para ello:

- Ejecuta mmc.exe

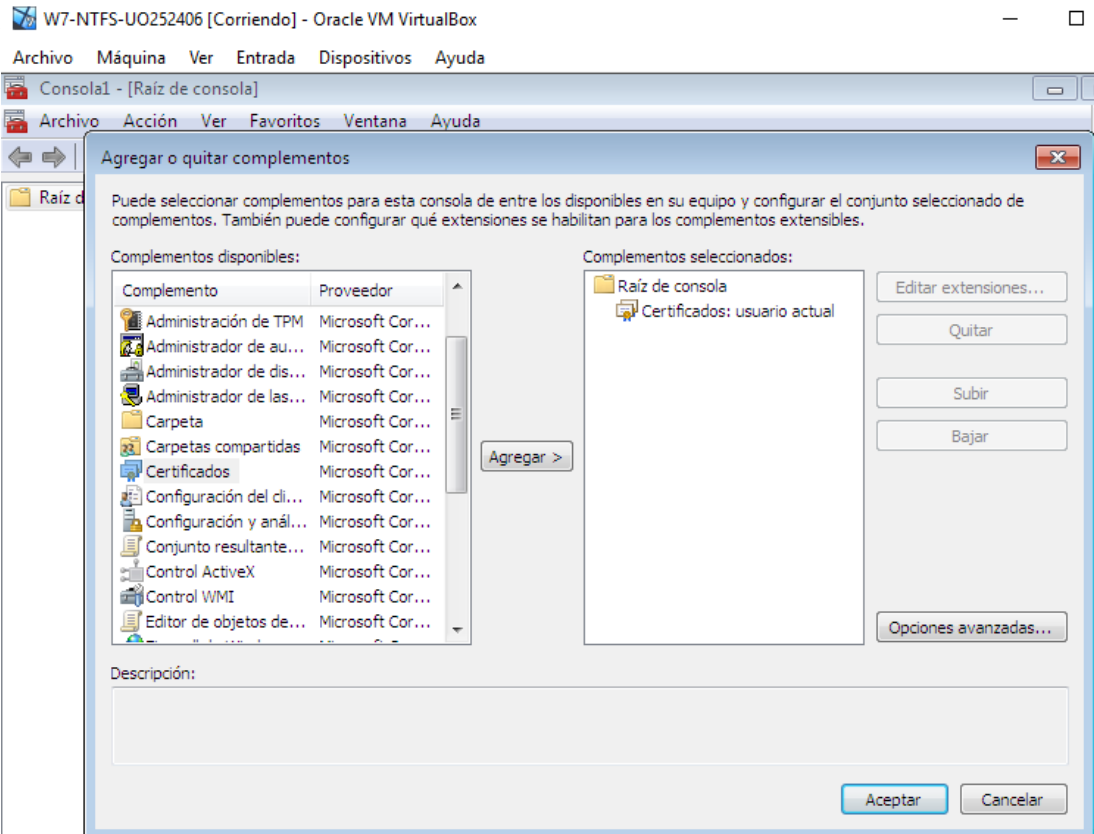


- Archivo, Añadir o quitar complemento, Agregar, Certificados, Agregar, Mi cuenta de usuario.

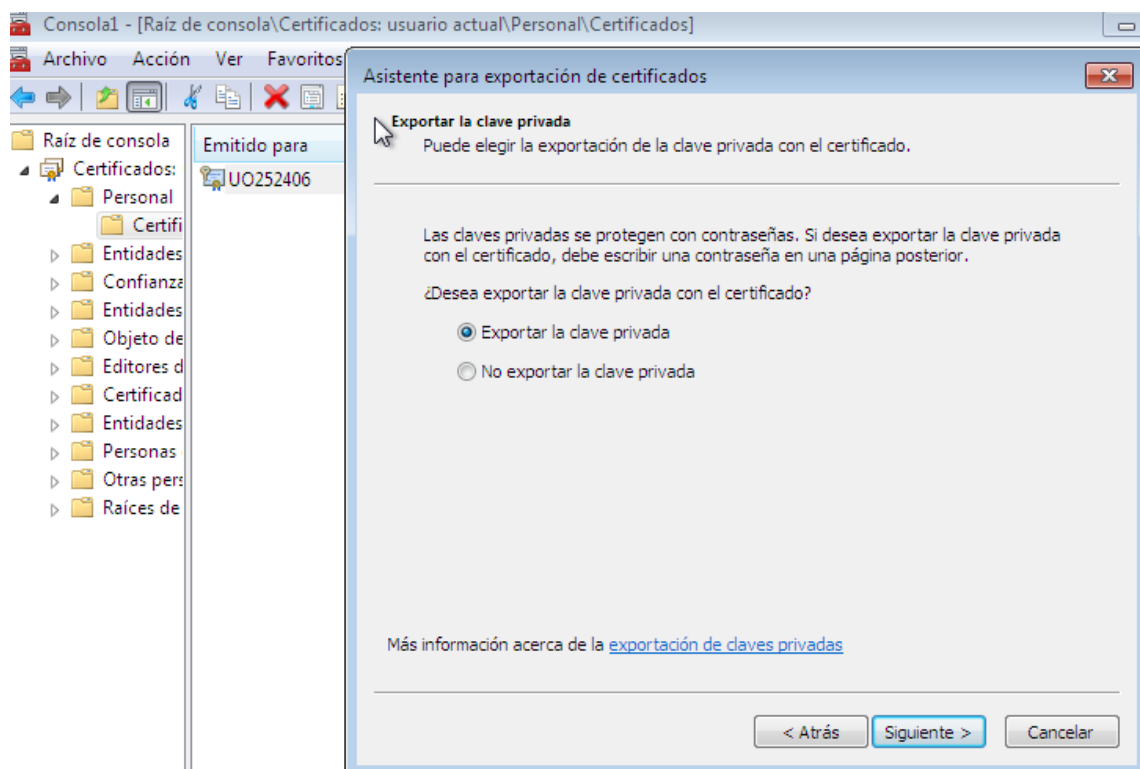
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Práctica 1 – Seguridad NTFS



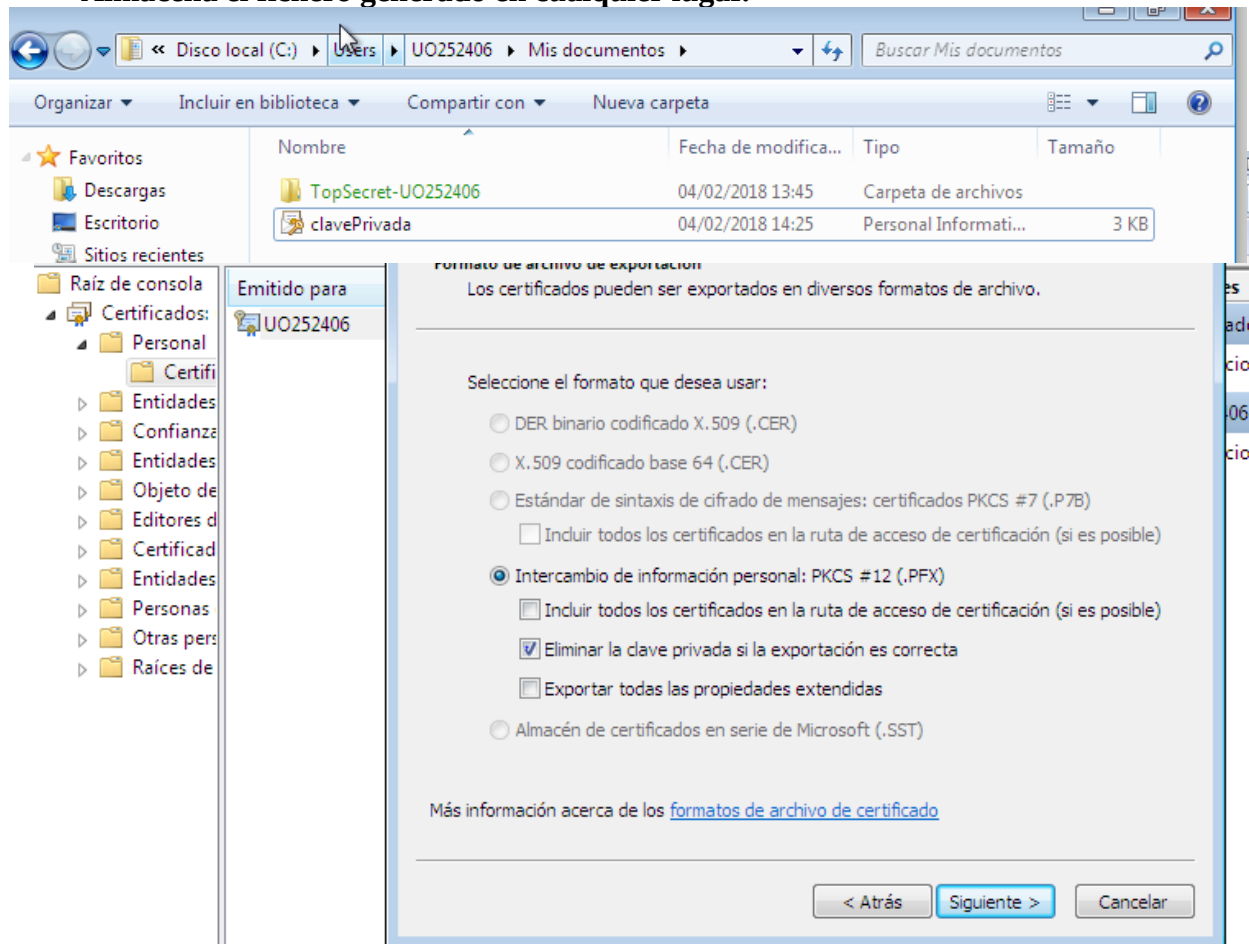
- En la carpeta que se crea “Personal-Certificados”, pulsar con el botón derecho sobre el certificado a exportar. Elegir “Todas las tareas, Exportar -> Exportar clave privada -> Eliminar la clave privada si la exportación es satisfactoria”



- Introduce (¡¡y anota en algún lado para no olvidarla!!) la clave para recuperarla.

Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

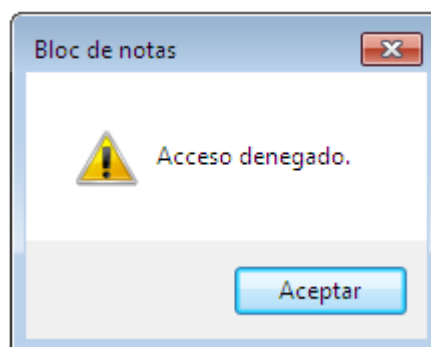
- **Almacena el fichero generado en cualquier lugar.**



- **Sal de sesión y vuelve a entrar, para que deje de usarse la clave privada.**

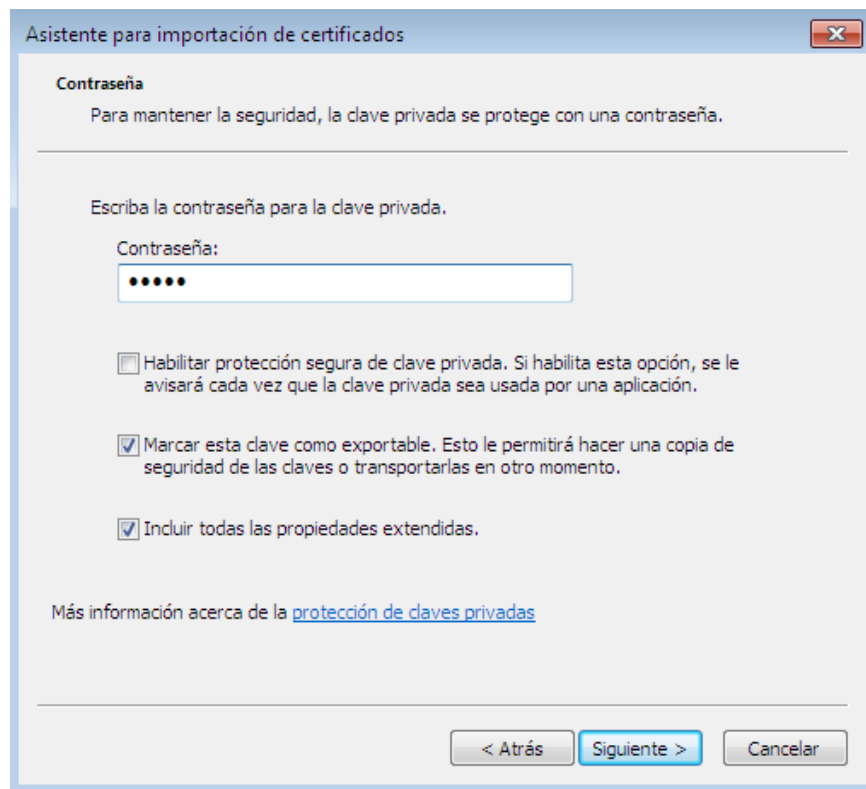
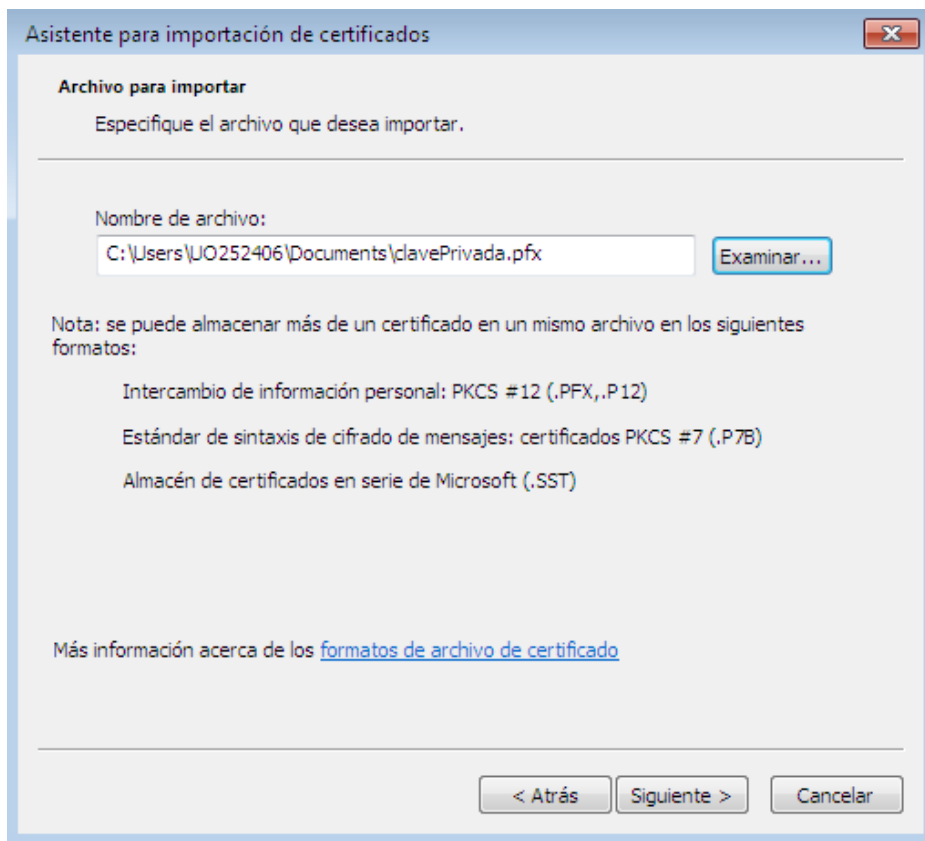
Prueba a acceder a la carpeta encriptada. ¿Puedes hacerlo? ¿Por qué?

Ya no podemos acceder ya que necesitamos el certificado de seguridad que hemos exportado. El mensaje de error es el siguiente.



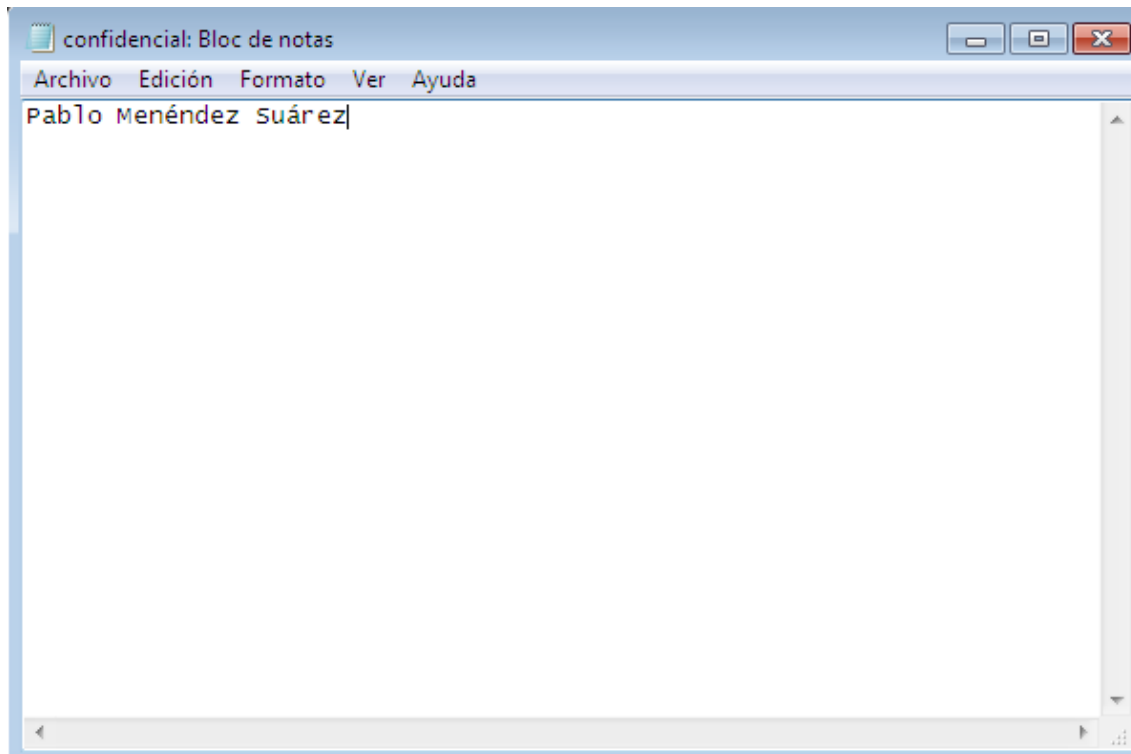
Importa el certificado (mmc.exe, ... Todas las tareas, Importar). Recuerda al importar hacer la clave exportable para que se pueda volver a retirar.

Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS



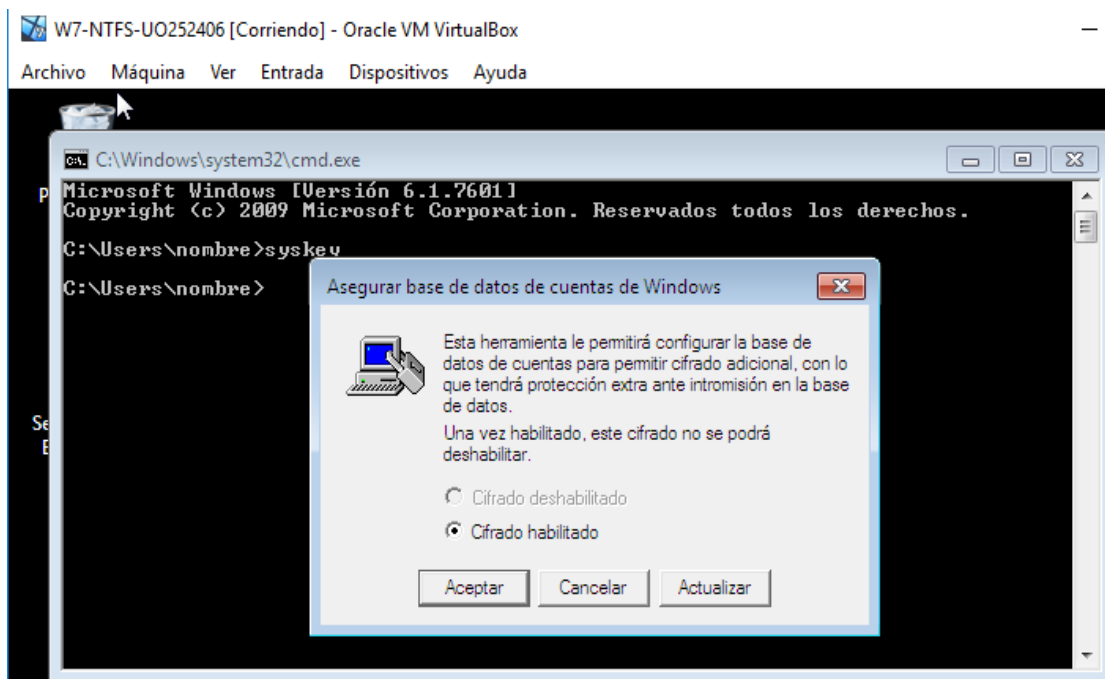
Prueba a acceder a la carpeta encriptada. ¿Puedes hacerlo? ¿Por qué?

Si, tanto a la carpeta como al fichero ya que hemos importado el certificado de seguridad.



Parte 6: Otras órdenes

Utiliza la orden syskey para encriptar la base de datos de cuentas, utilizando la contraseña generada por el sistema. Reinicia el sistema. ¿Hay algún cambio en el comportamiento del mismo? ¿Por qué?

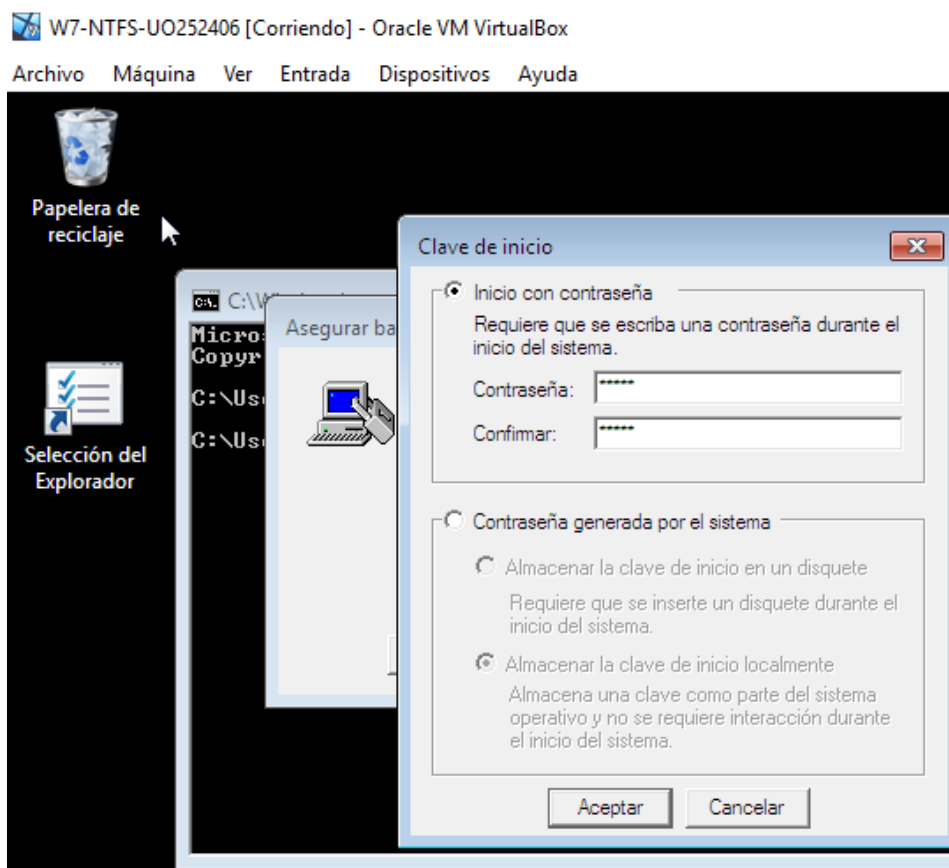


Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 Práctica 1 – Seguridad NTFS



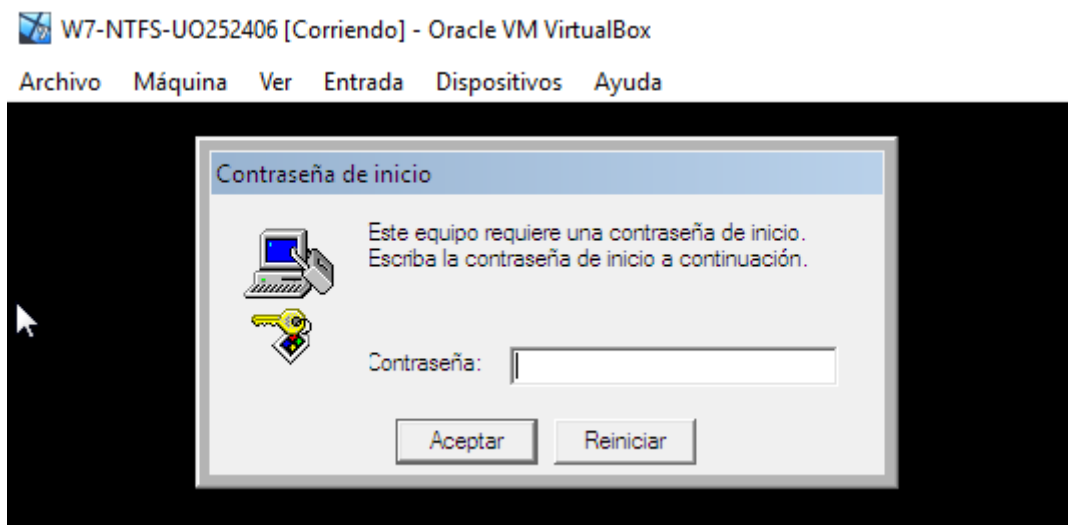
No existe ningún cambio aparente en el comportamiento del sistema, ya que el propio sistema fue el que generó la contraseña y no es necesario introducirla debido a que ya la conoce, sin embargo, la base de datos estará cifrada.

Utiliza la orden syskey para encriptar la base de datos de cuentas, utilizando una contraseña de usuario (importante no olvidarla). Reinicia el sistema. ¿Hay algún cambio en el comportamiento del mismo? ¿Por qué? ¿Qué puedes hacer para evitar tener que introducir esa información en el arranque del sistema?



Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Práctica 1 – Seguridad NTFS

Reiniciamos el sistema y nos aparece lo siguiente:



Apreciamos cambios en el comportamiento del mismo, ya que para poder iniciar sesión con cualquiera de los usuarios se nos pide la clave de inicio que hemos indicado anteriormente en el cifrado de la base de datos de cuentas. Una alternativa para no tener que introducir dicha contraseña sería dejar que sea el propio sistema el que cifre la base de datos de cuentas.