

SEGURIDAD DE SISTEMAS INFORMÁTICOS

Seguridad en Windows



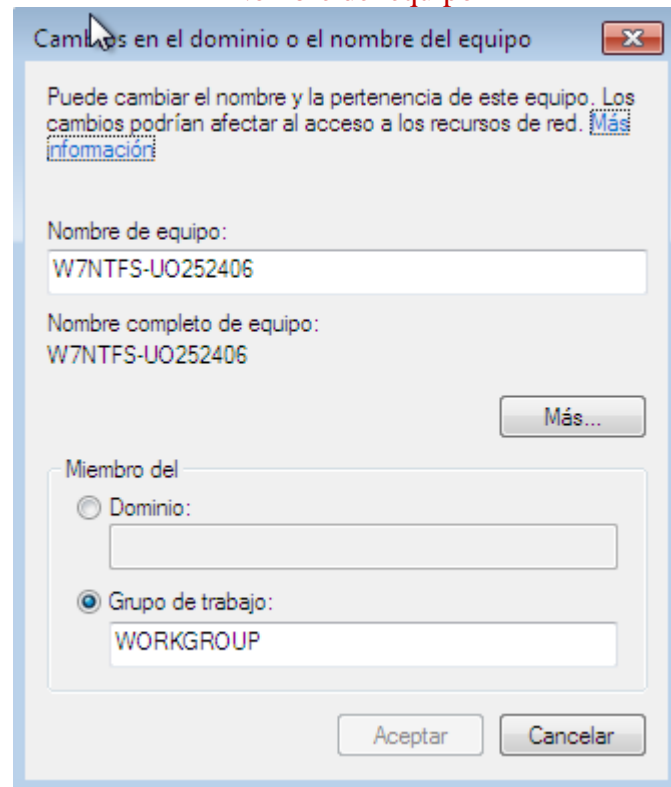
Pablo Menéndez Suárez – UO252406
71899158P

Contenido

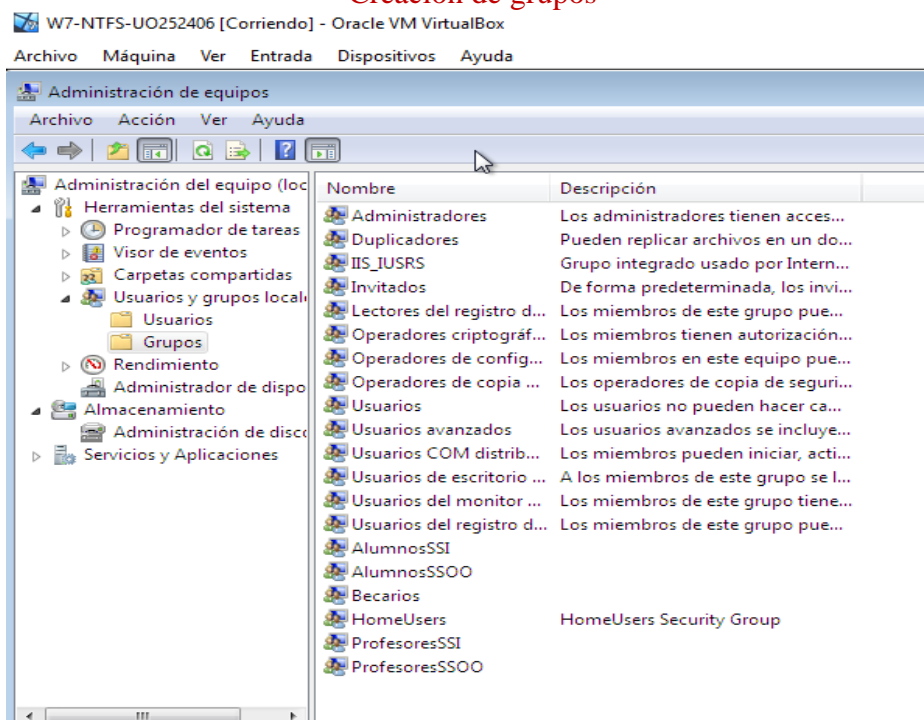
NTFS: Preparación del entorno.....	3
Parte 1: Exploración de permisos.....	5
Parte 2: Ejemplos de permisos	10
Parte 3: Trabajo con el sistema de ficheros encriptado	19
Parte 4: ¡Al ataque!	22
Parte 5: Opciones avanzadas.....	23
Directorio Activo.....	30
Parte 1: Preparación del entorno	30
Directorio Activo:	42
Parte 1: Seguridad en Active Directory.....	42
Parte 2: Políticas de Grupo.....	51

NTFS: Preparación del entorno

Nombre del equipo



Creación de grupos

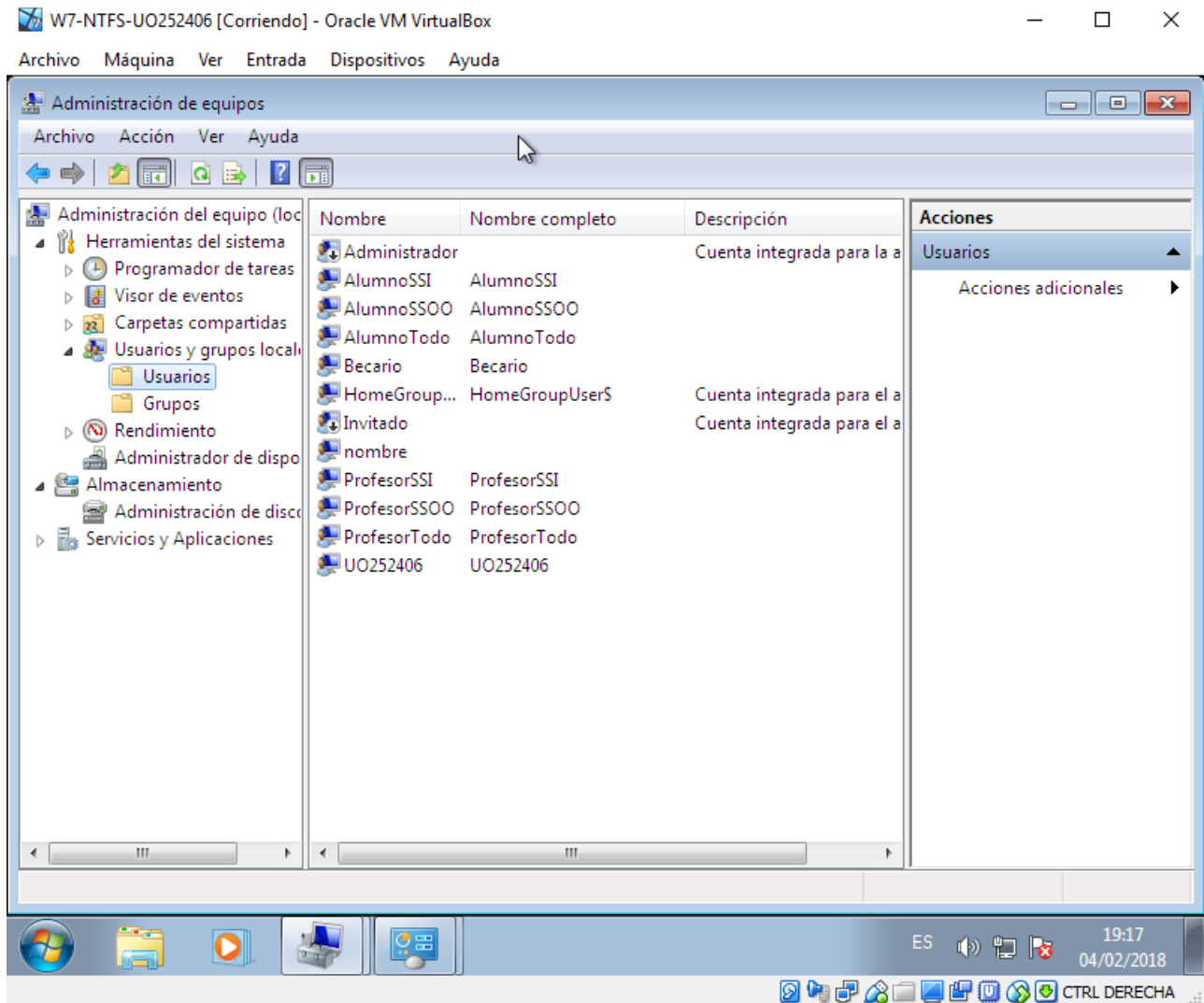


Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS

Creación de usuarios

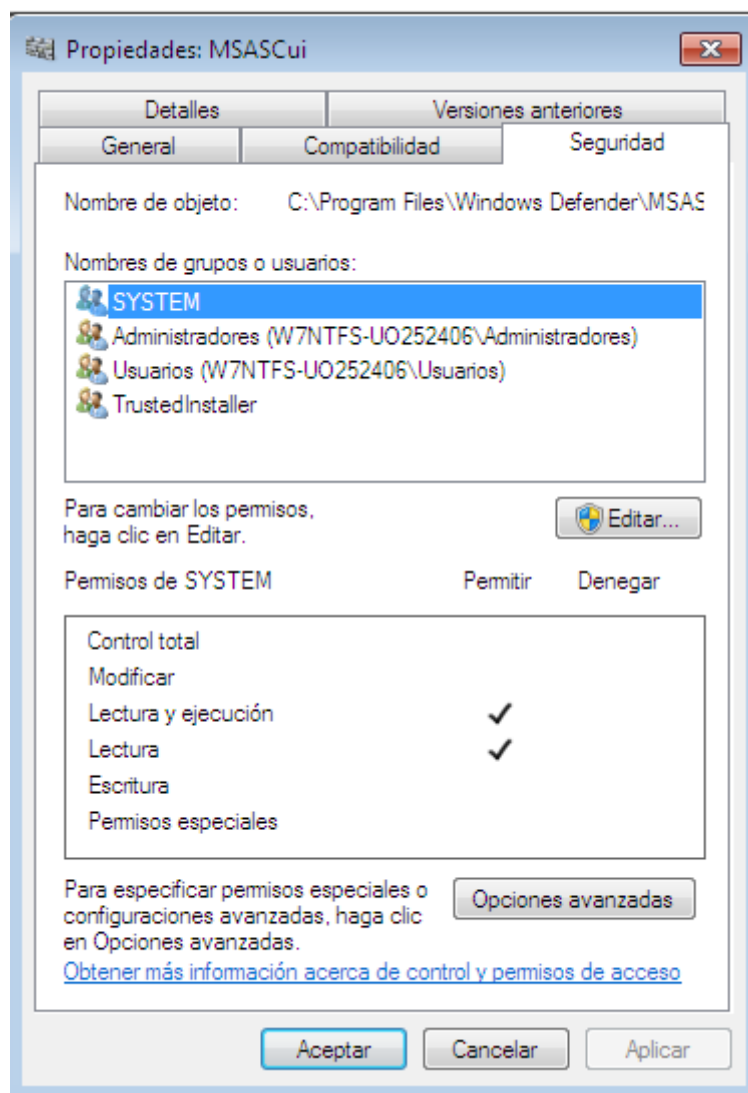


Parte 1: Exploración de permisos

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.

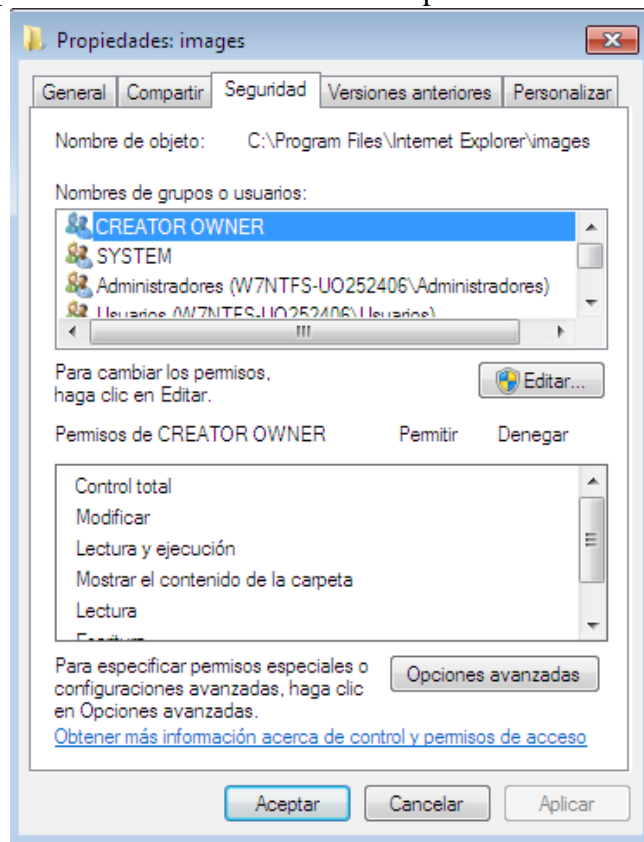
- **Permisos de ficheros:**

- 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**



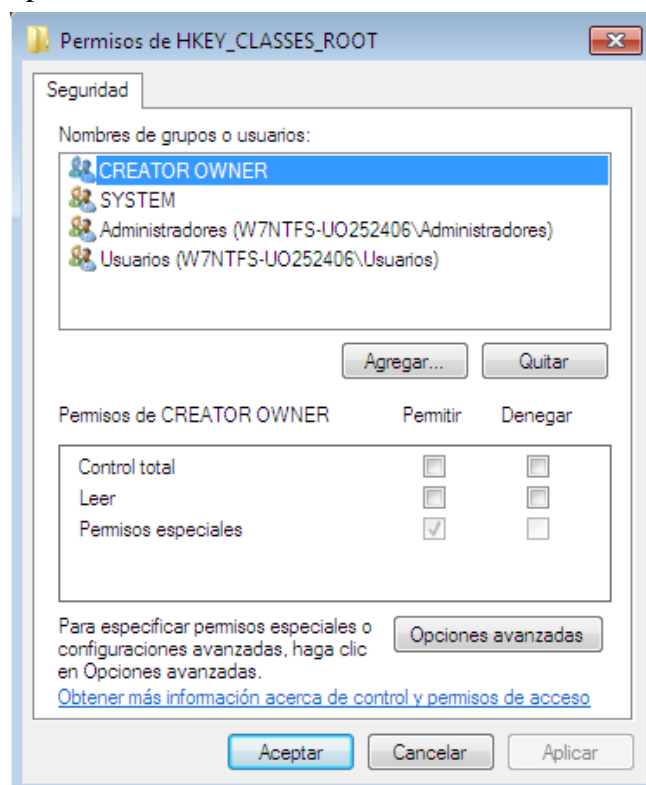
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Seguridad NTFS

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



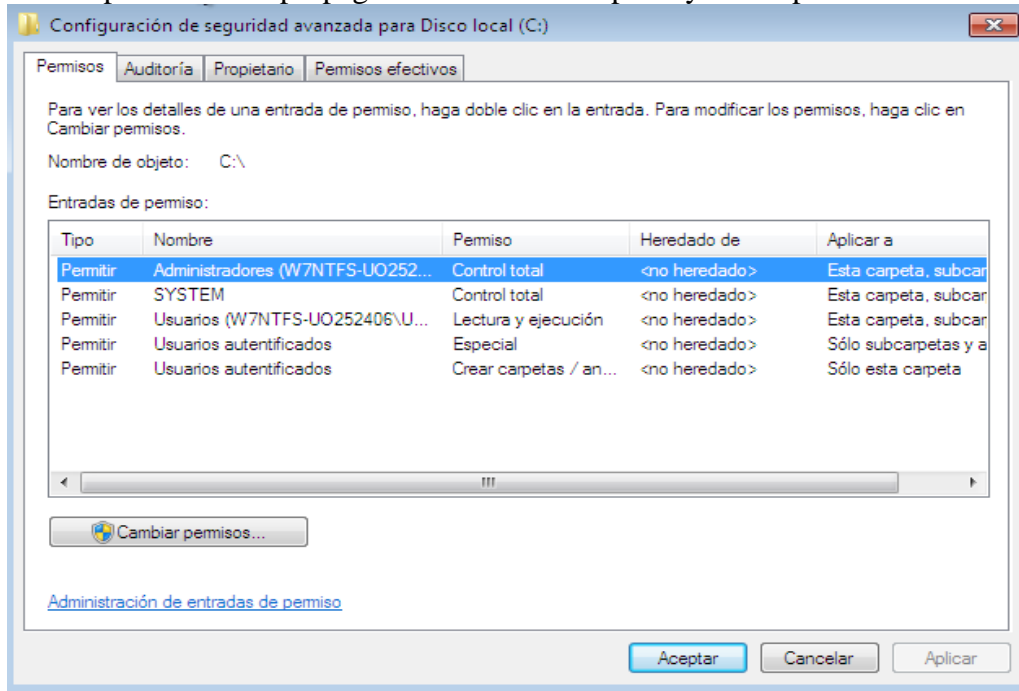
- **Permisos de elementos de registro:**

- 1) Control total
- 2) Leer
- 3) Permisos especiales

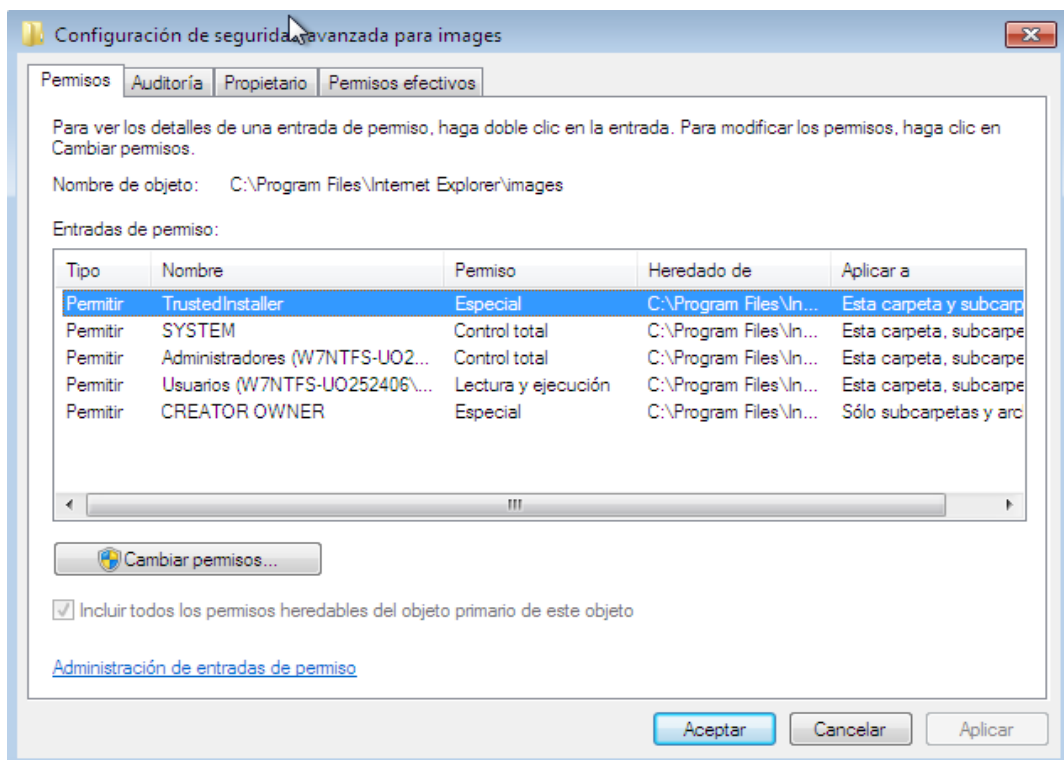


Crea una carpeta dentro de las anteriores que se llame "entregasPractica": los alumnos pueden añadir ficheros, pero no pueden ni ver el contenido ni modificar los ficheros existentes.

- **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.

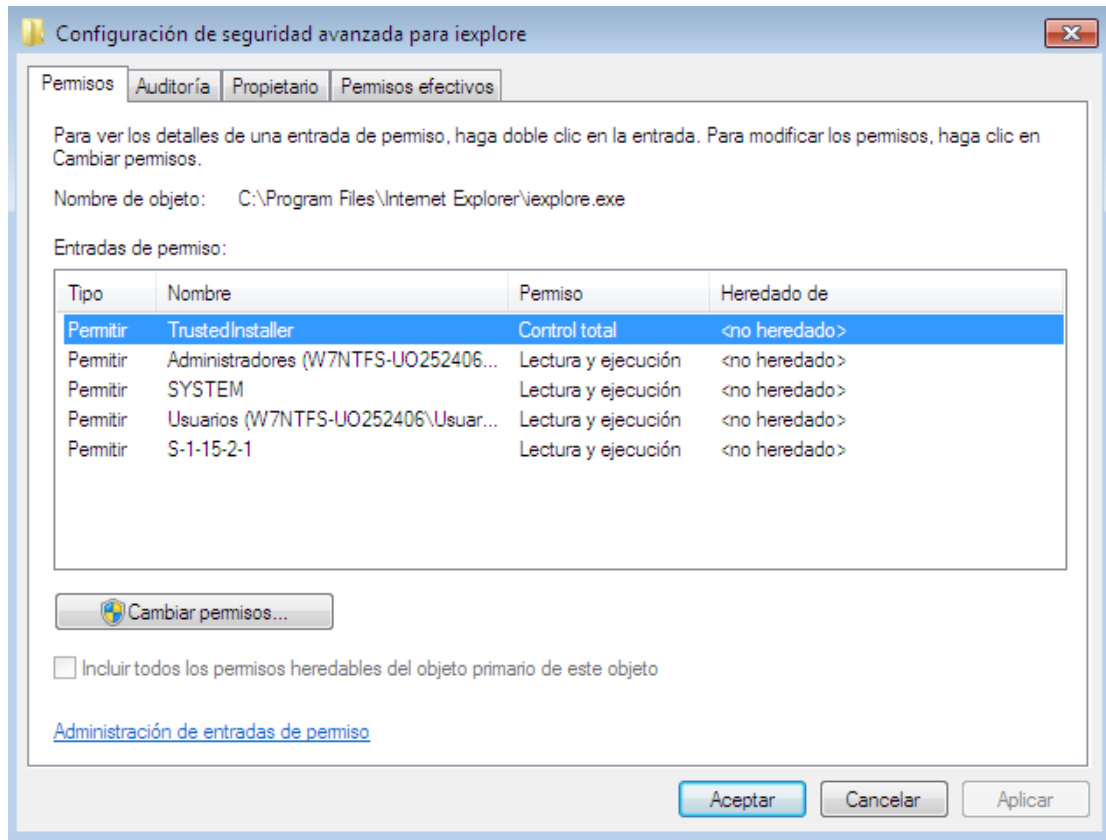


- **Directorio cualquiera** (C:\Program Files\Internet Explorer\images): Observamos que todos los permisos son heredados de la carpeta superior en la jerarquía (C:\Program Files\Internet Explorer) y además esos mismos permisos son propagados a carpetas, subcarpetas y archivos inferiores.



Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
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

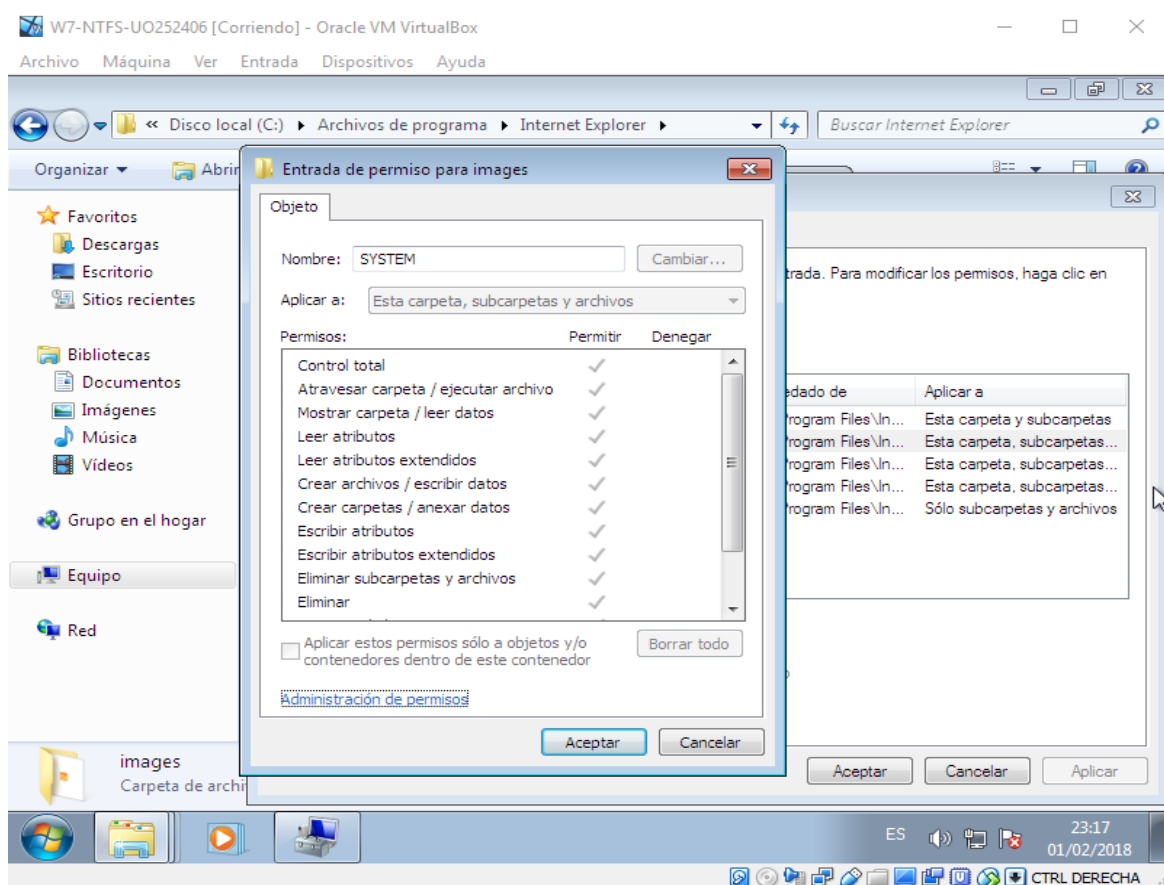
- **Atravesar carpeta/ ejecutar archivo:** Atravesar carpeta permite o deniega el movimiento por las carpetas para llegar a otros archivos o carpetas. Ejecutar archivo permite o deniega la ejecución de archivos de programa.
- **Mostrar carpeta / leer datos:** Mostrar carpeta permite o deniega ver nombres 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.

- **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.

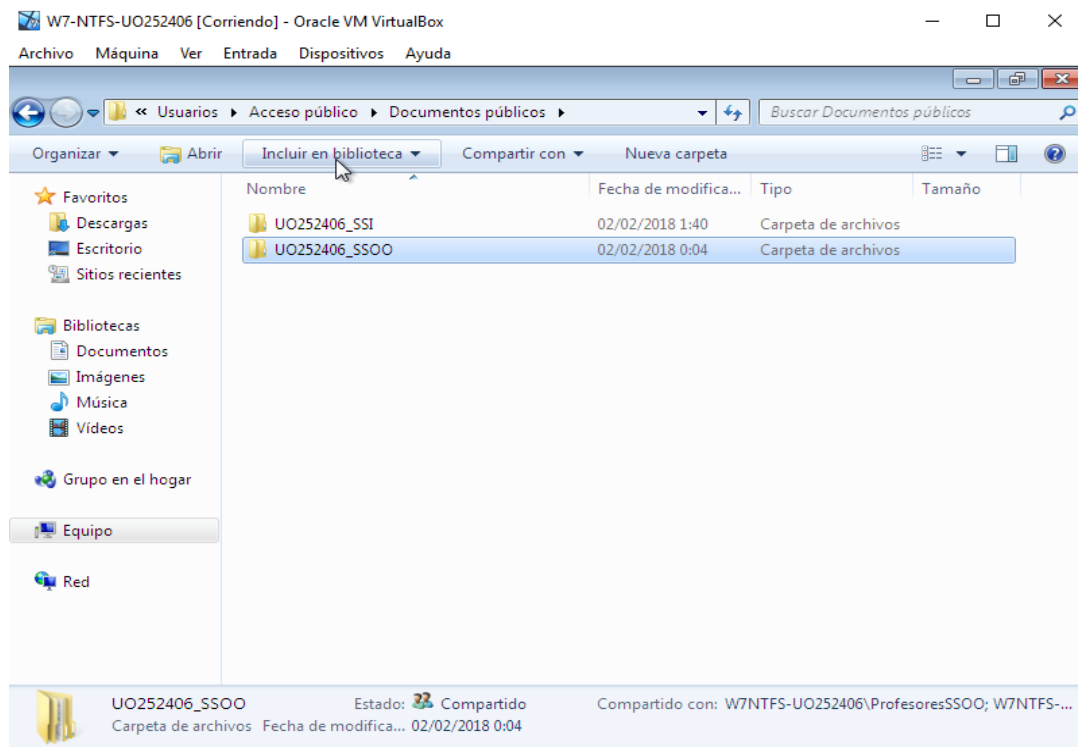
El control total en permisos normales permite todos los permisos normales mientras que el control total de permisos avanzados permite todos los permisos avanzados.

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.

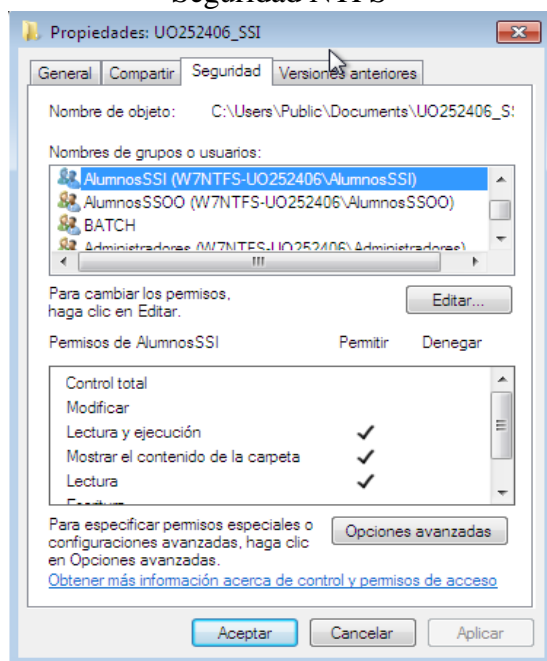


Permisos Alumnos SSI

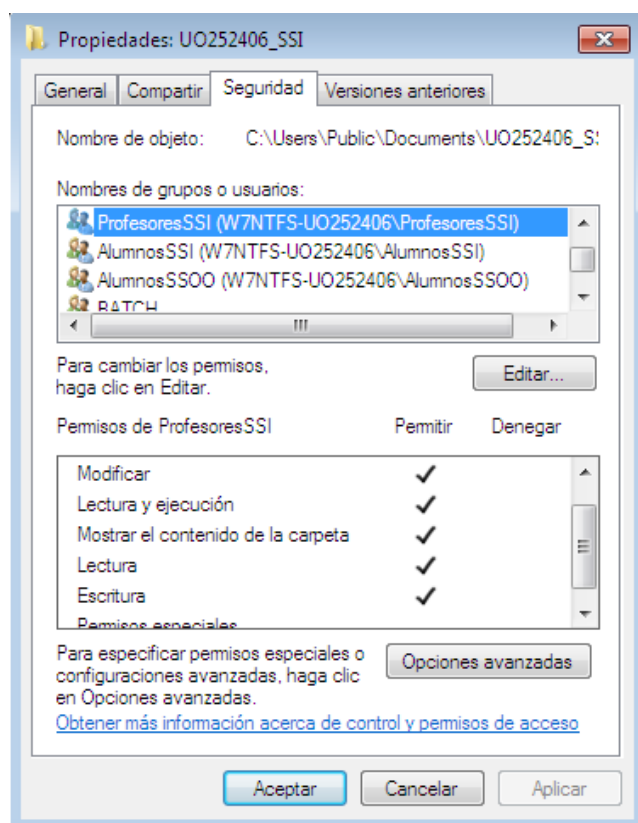
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS



Permisos Profesores SSI

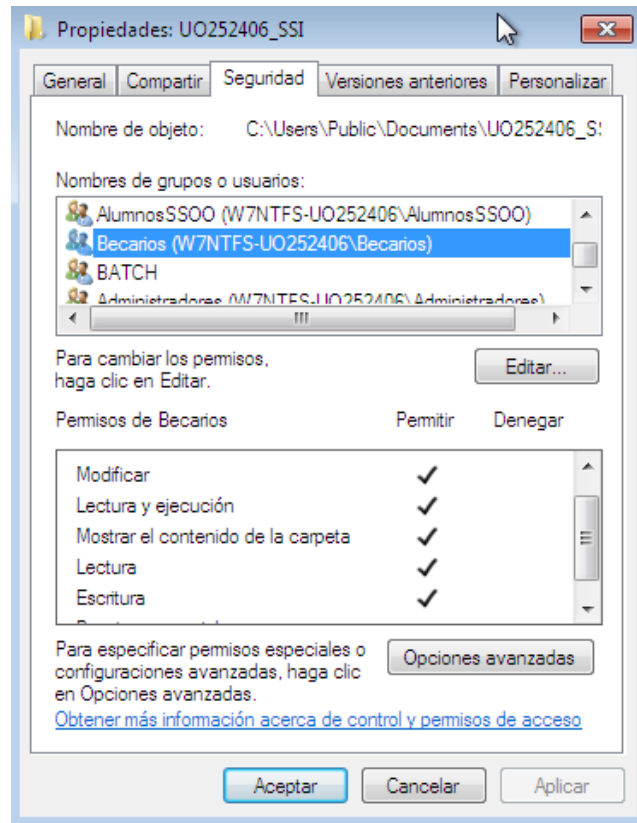


Permisos Becarios

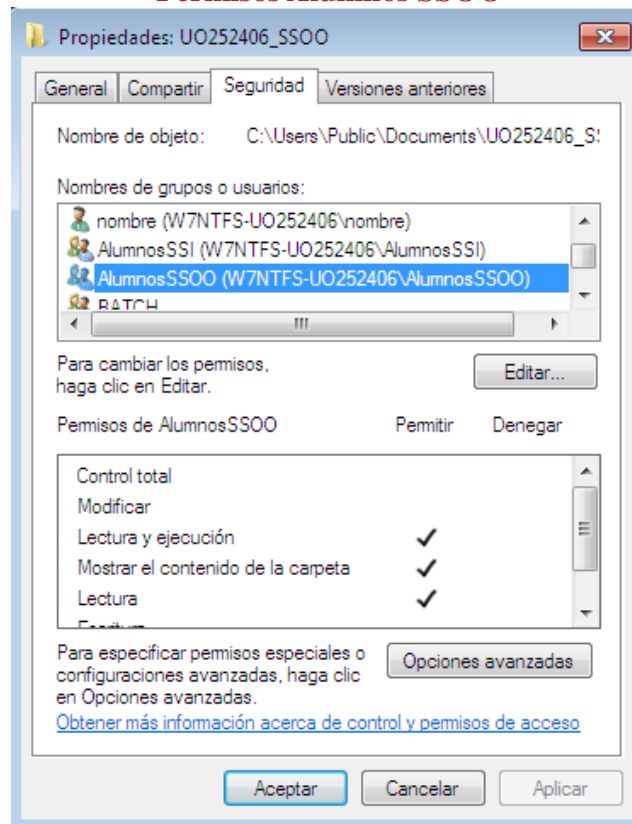
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS



Permisos Alumnos SSOO

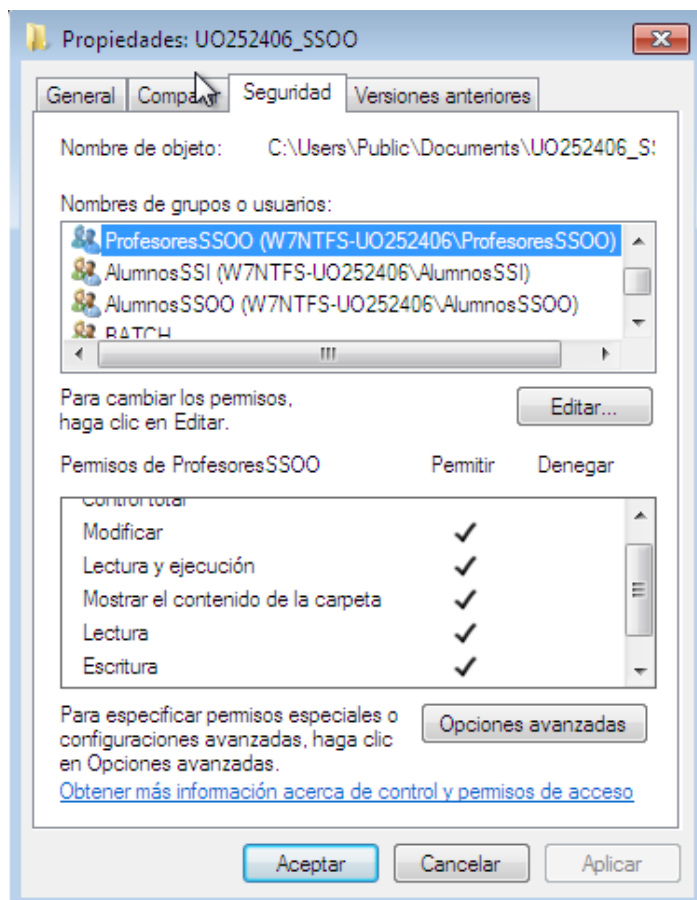


Permisos Profesores SSOO

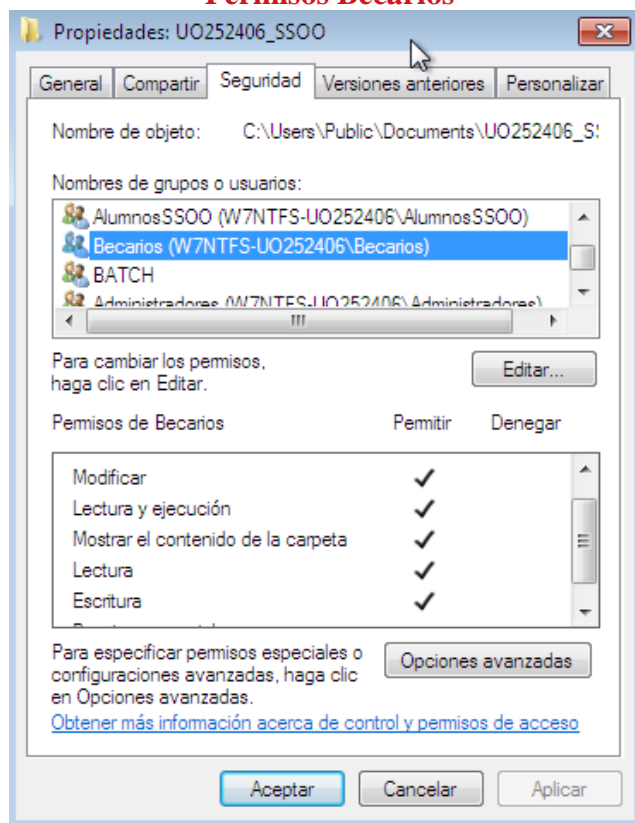
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS



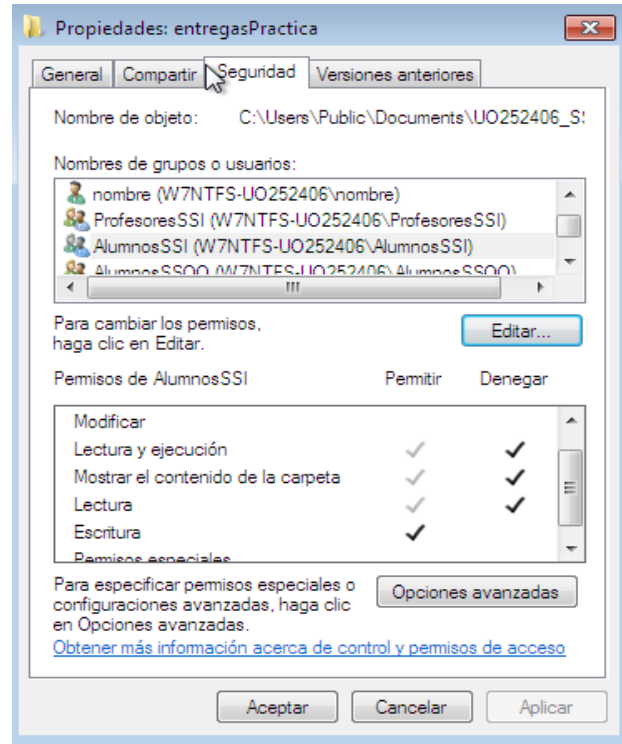
Permisos Becarios



Ingeniería Informática del Software – EII
 Seguridad de Sistemas informáticos
 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.

Permisos entregasPractica SSI

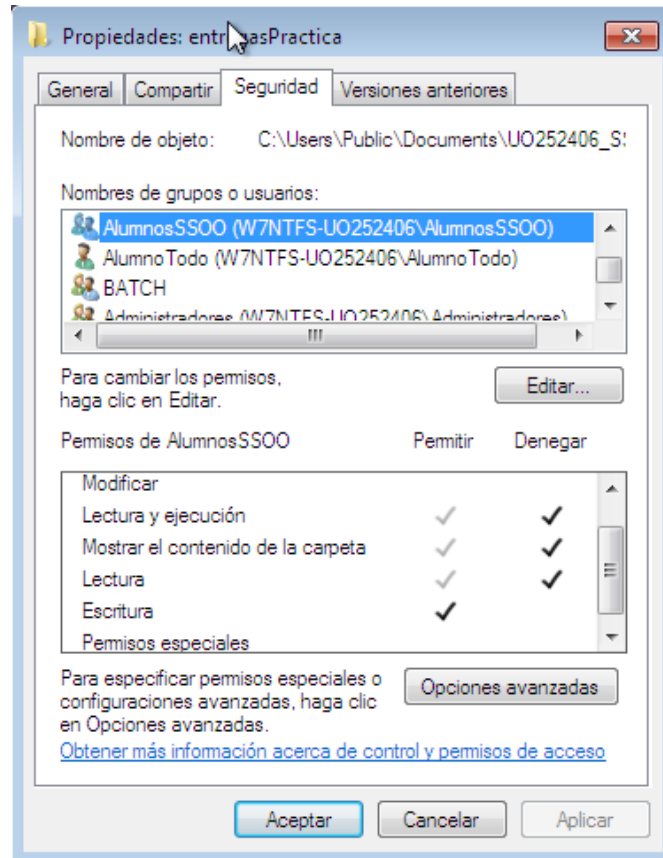


Permisos entregasPractica SSOO

Ingeniería Informática del Software – EII

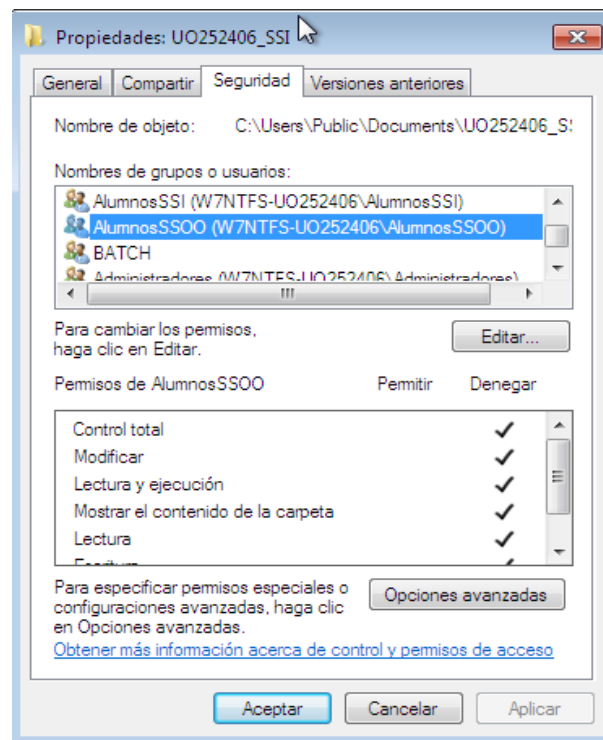
Seguridad de Sistemas informáticos

Seguridad NTFS



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

Negación de AlumnosSSOO en UO252406SSI

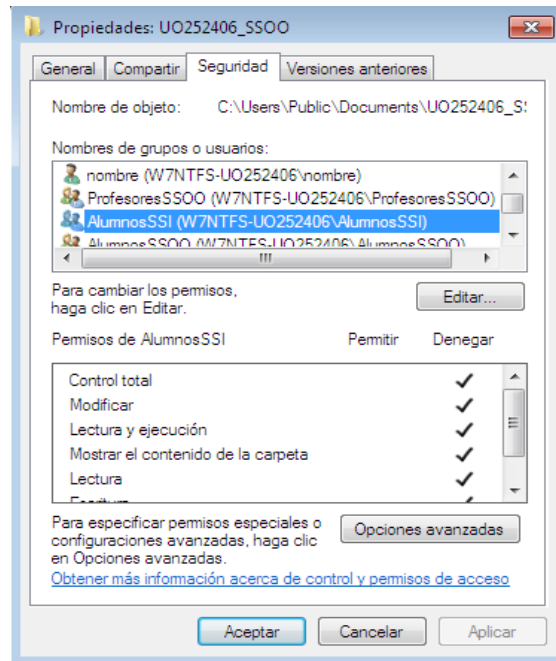


Negación de AlumnosSSI en UO252406SSOO

Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

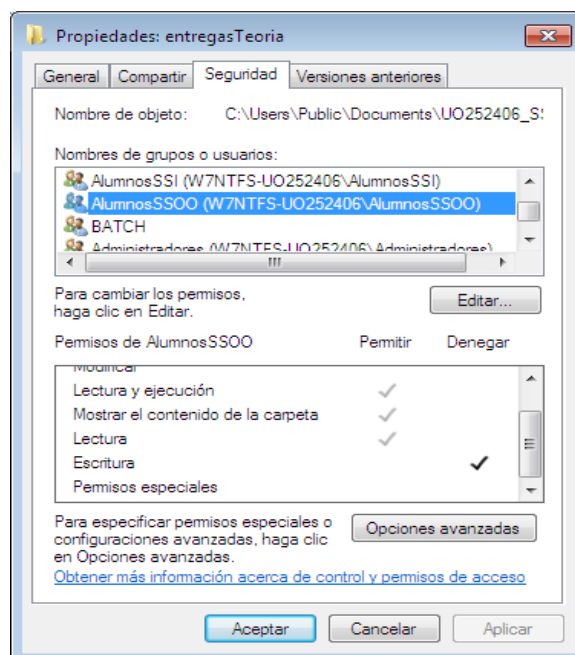
Seguridad NTFS



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

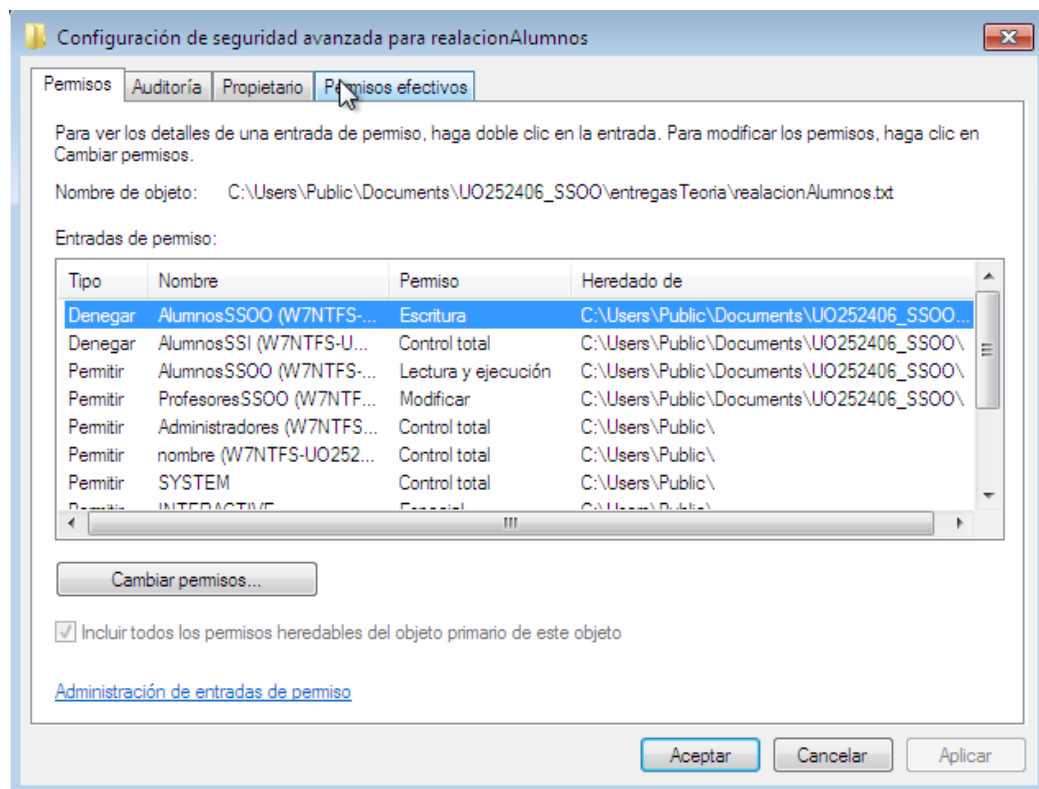


Permisos heredados

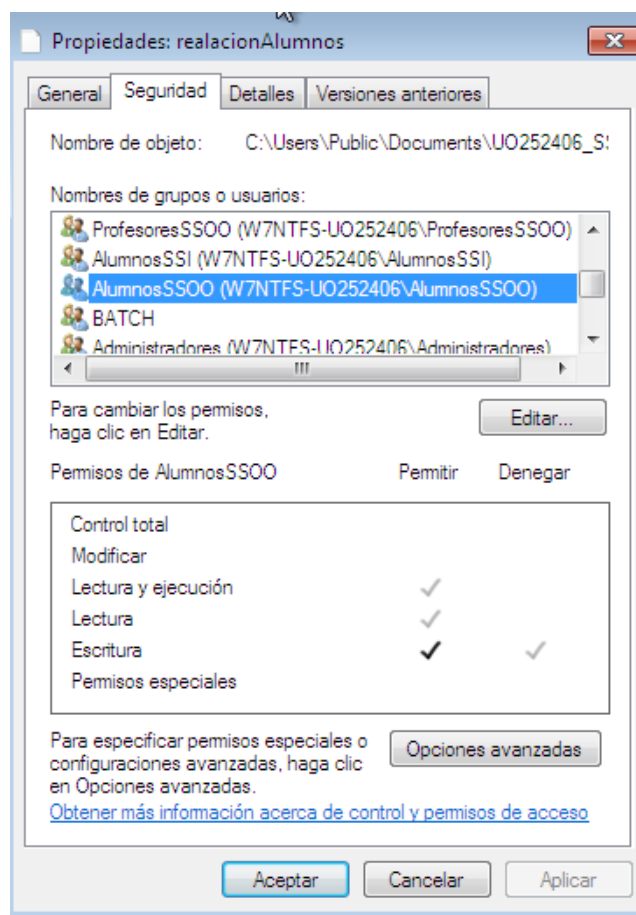
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS



Permisos AlumnosSSOO en relacionAlumnos.



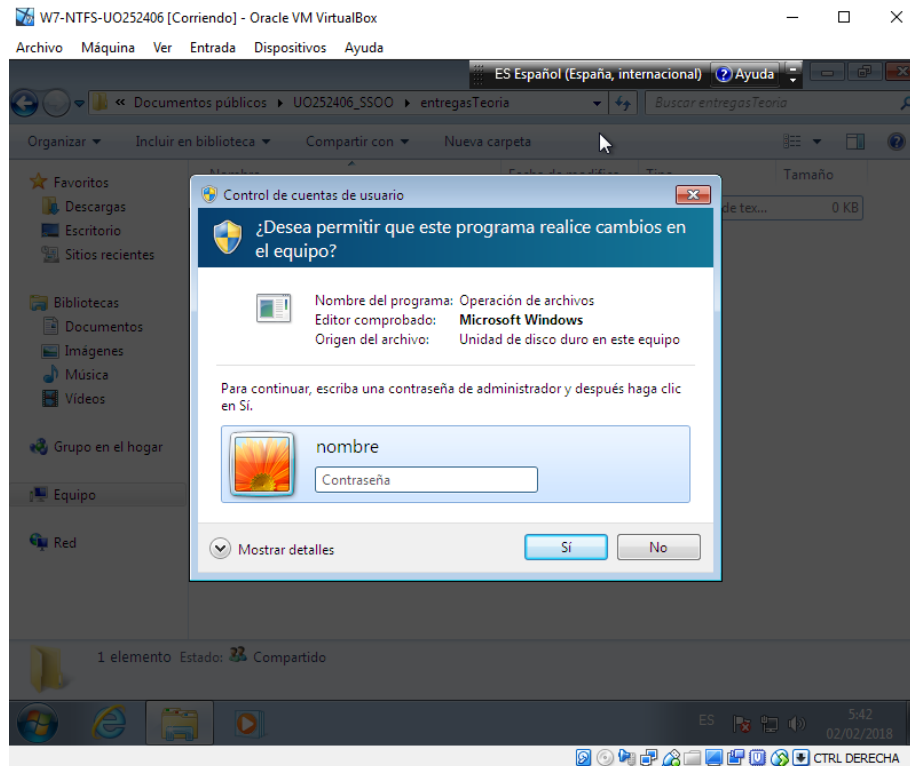
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Seguridad NTFS

- 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.

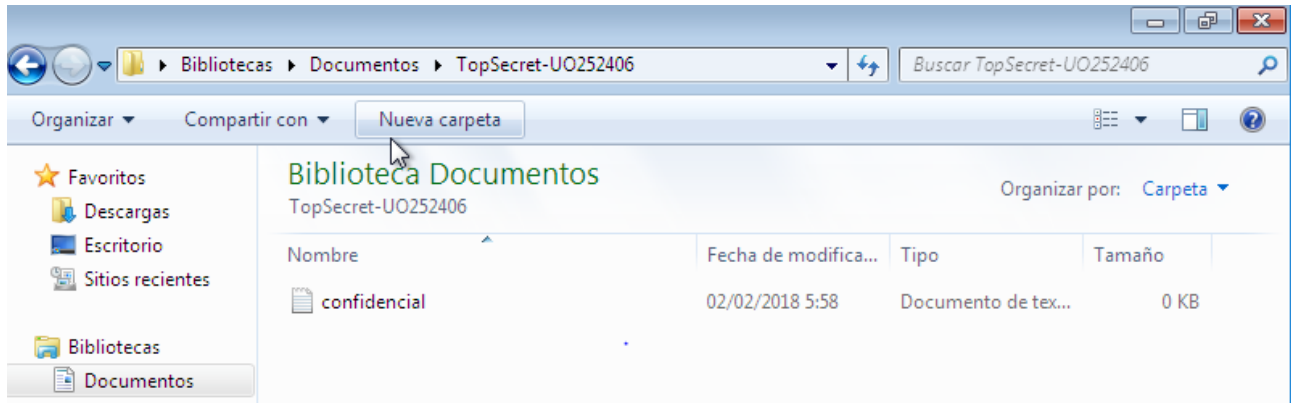
Le damos a crear nueva carpeta y nos sale el siguiente mensaje:



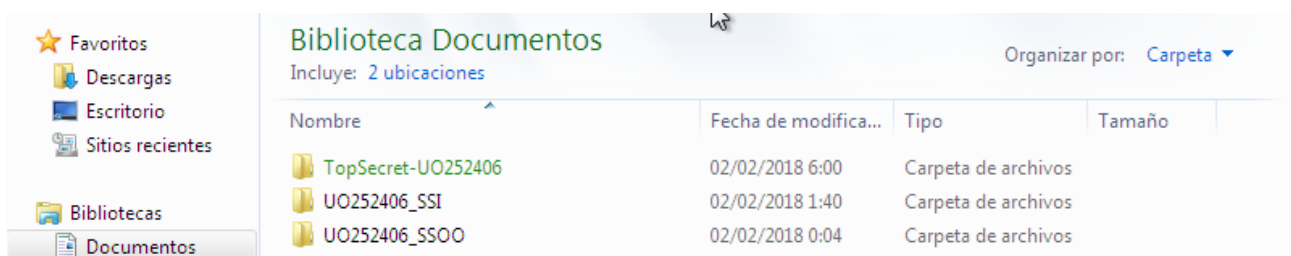
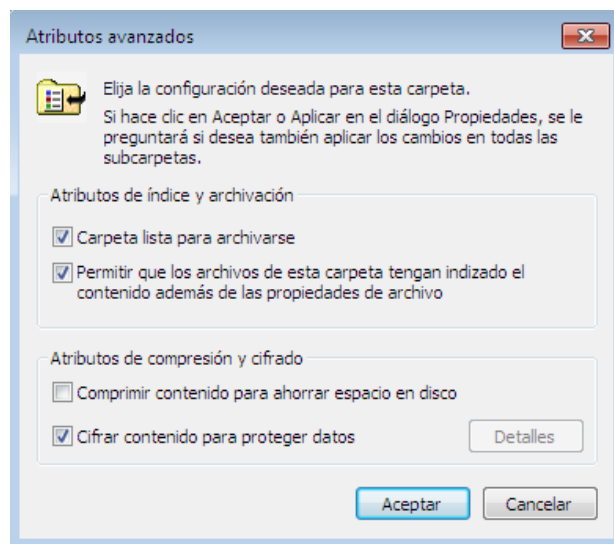
En el mensaje nos pide la contraseña de administrador, por lo que queda demostrado que los permisos son los indicados.

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.

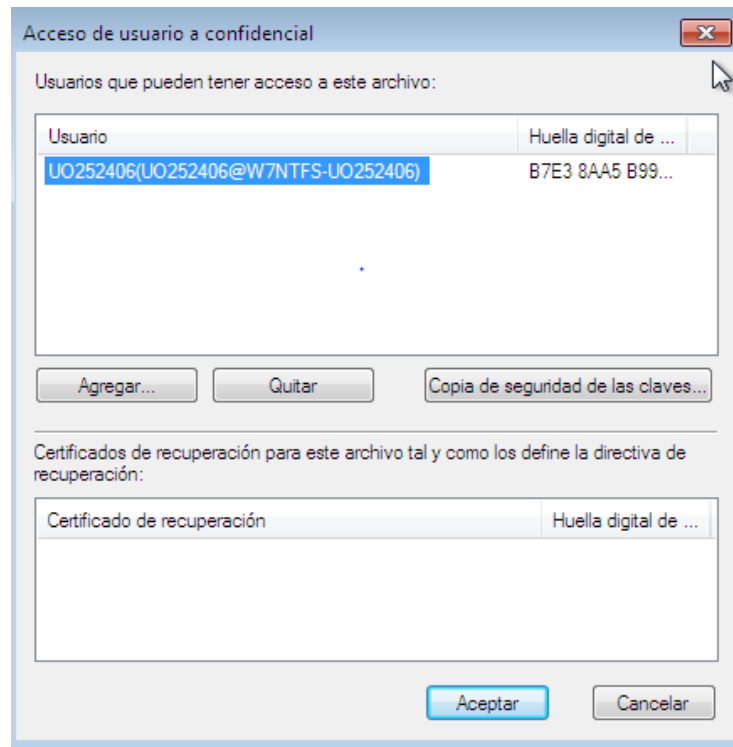


Cifra esa carpeta. (Botón derecho sobre la carpeta, Propiedades, Opciones Avanzadas, Cifrar contenido para proteger datos).

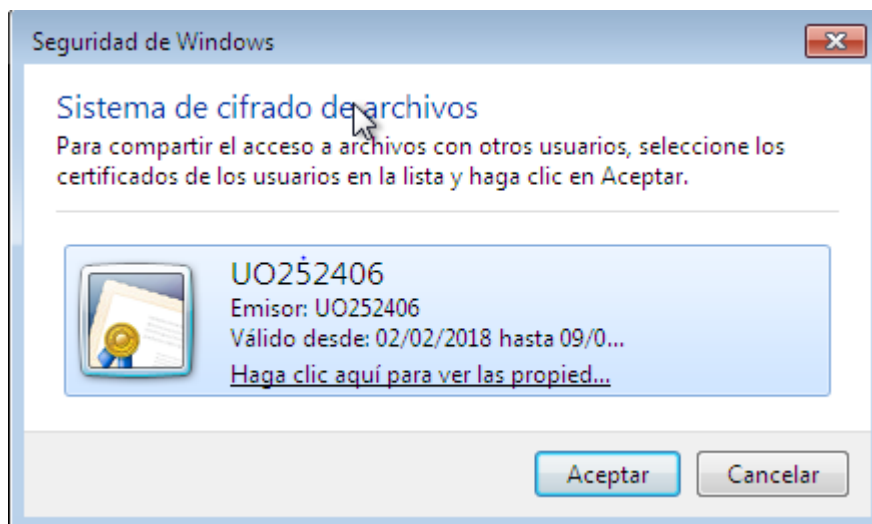


En la ventana anterior, ver los “Detalles” junto a la casilla de “Cifrar contenido para proteger datos”. Explica el contenido de esa ventana. Comprueba y documenta cómo si existe el certificado de seguridad de otro usuario se puede proporcionar acceso al archivo “confidencial” a ese otro usuario

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



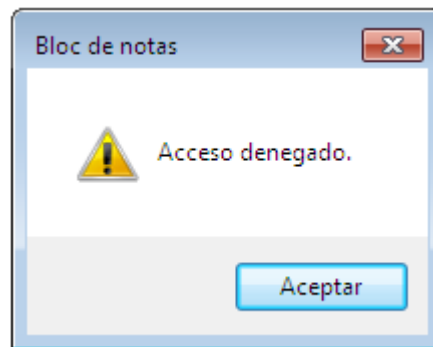
- En esta ventana podemos observar los usuarios que pueden tener acceso a el archivo y los certificados de recuperación del mismo, que en este caso no hay ninguno.
- Para proporcionar acceso a otro usuario iríamos a la ventana anterior y le daríamos a agregar. Nos aparecería la siguiente imagen:



- 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.

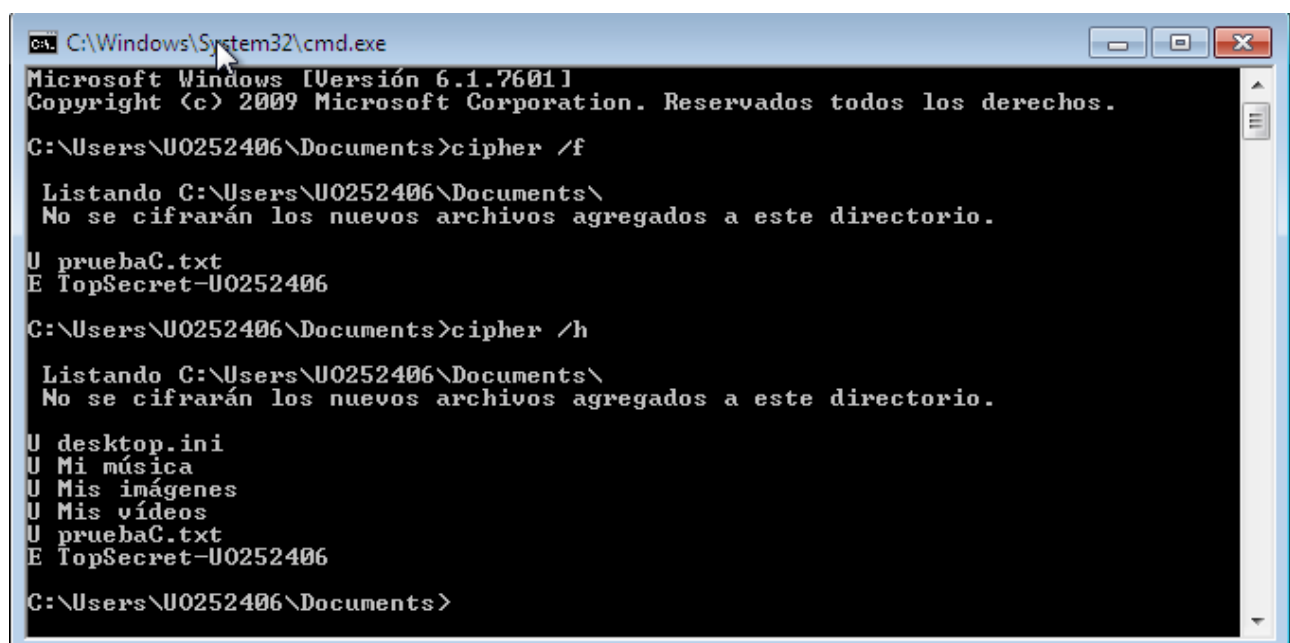
El fichero queda cifrado y solo podrá acceder a él el propio administrador ya que fue el que lo creó. Si intentamos acceder desde otro usuario como por ejemplo UO252406 se nos deniega el acceso y el mensaje que aparece es igual que el anterior.

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

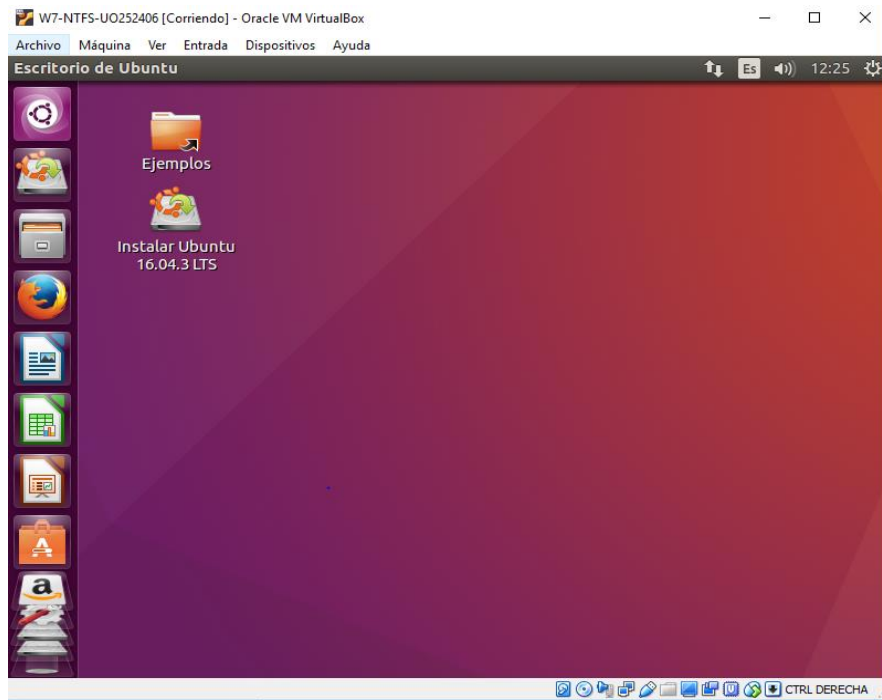
Listando C:\Users\UO252406\Documents\
No se cifrarán los nuevos archivos agregados a este directorio.

U desktop.ini
U Mi música
U Mis imágenes
U Mis vídeos
U pruebaC.txt
E TopSecret-UO252406

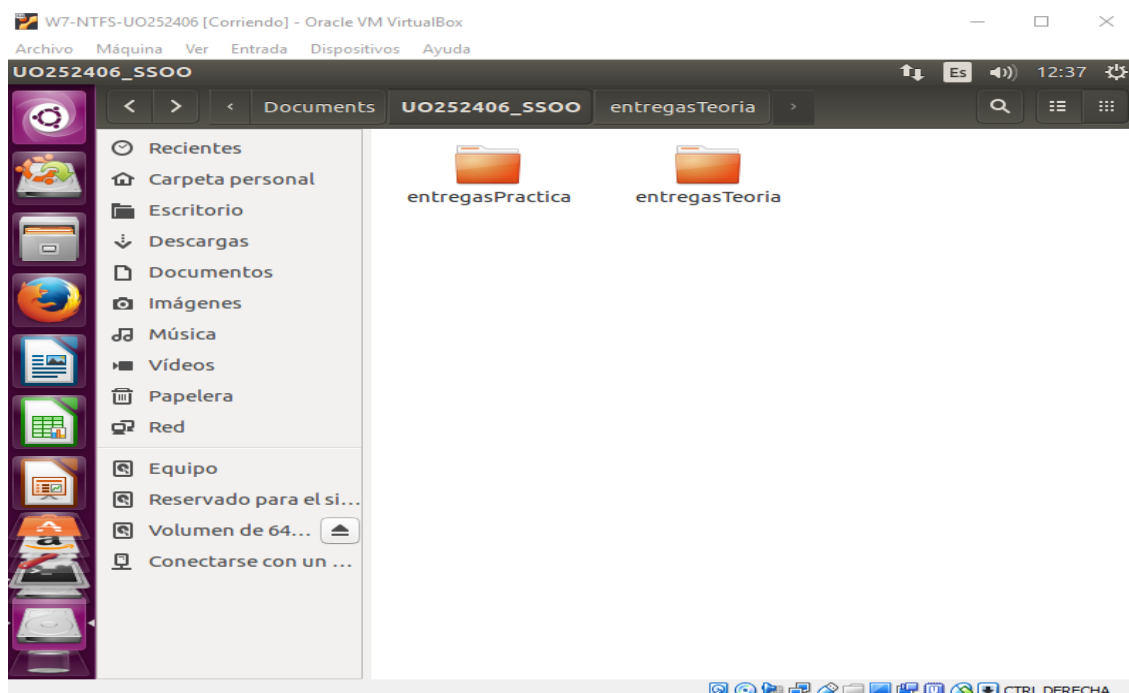
C:\Users\UO252406\Documents>
```

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?

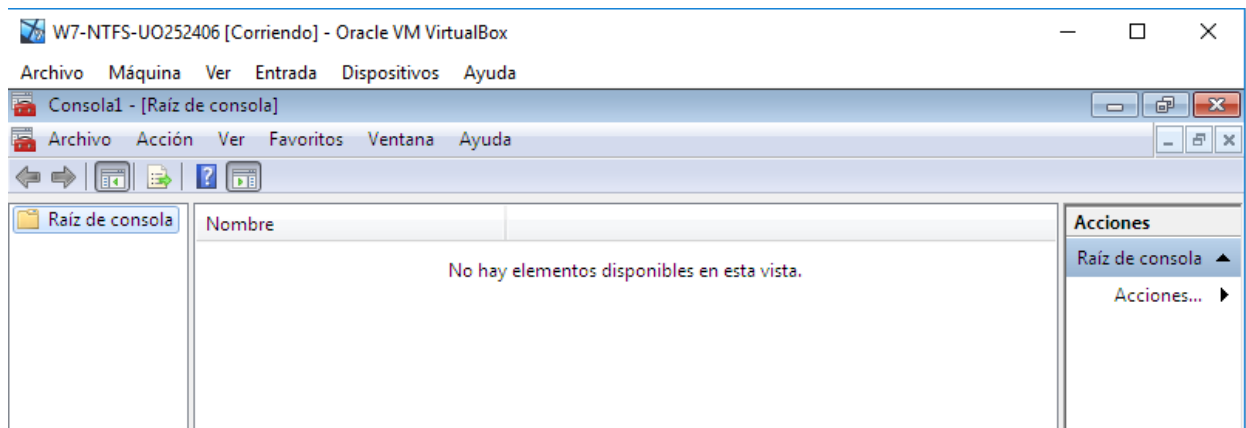
Podemos visualizar el contenido de la carpeta, sin embargo, no tenemos los permisos necesarios para acceder al fichero confidencial ya que está encriptado y nos salta el siguiente mensaje:



Parte 5: Opciones avanzadas

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

- **Ejecuta mmc.exe**

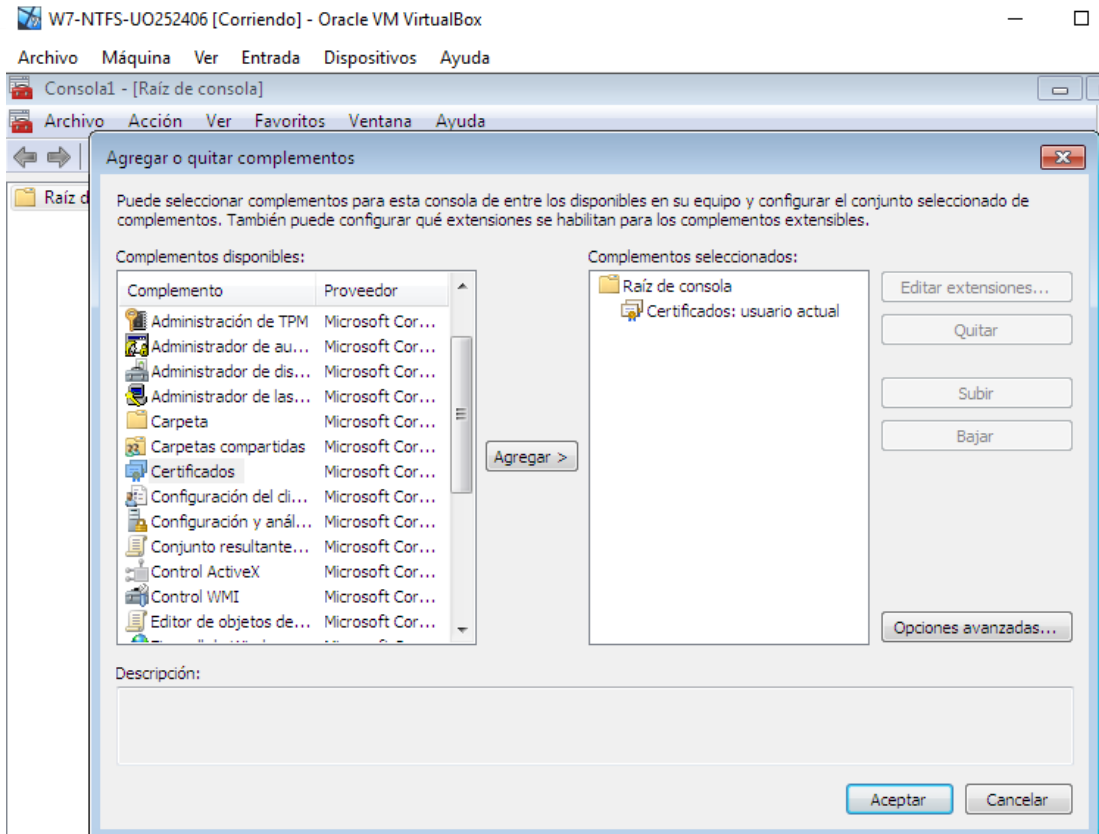


- **Archivo, Añadir o quitar complemento, Agregar, Certificados, Agregar, Mi cuenta de usuario.**

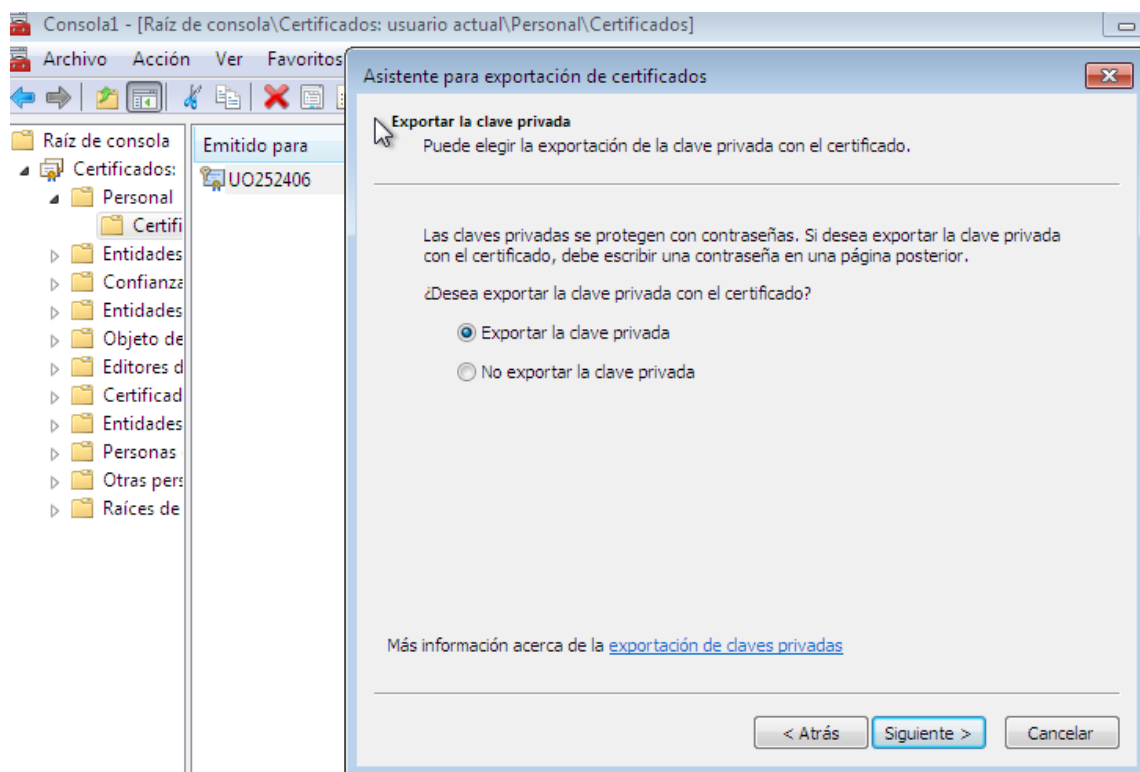
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS

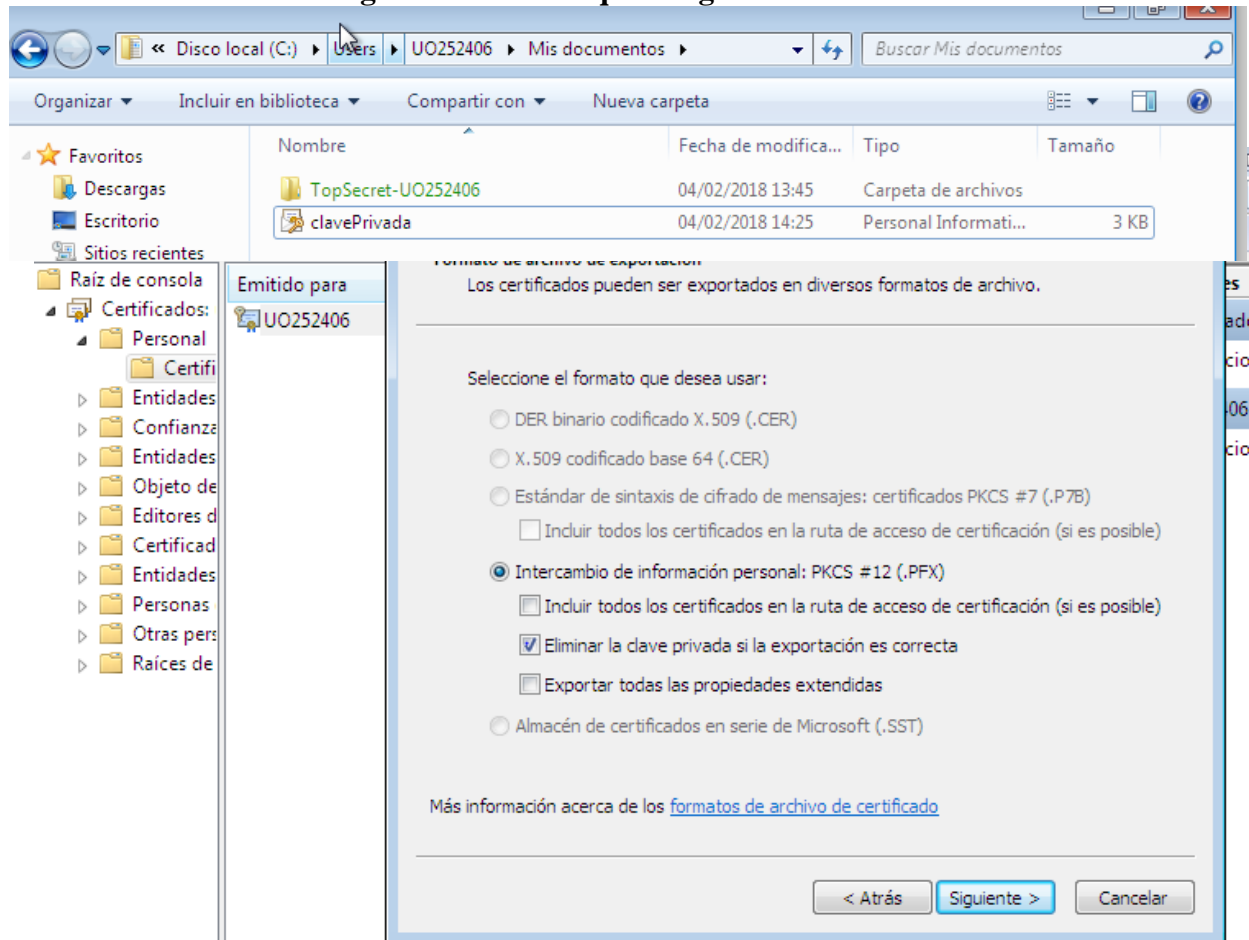


- En la carpeta que se crea “Personal-Certificados”, pulsar con el botón derecho sobre el certificado a exportar. Elegir “Todas las tareas, Exportar -> Exportar clave privada -> Eliminar la clave privada si la exportación es satisfactoria”



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

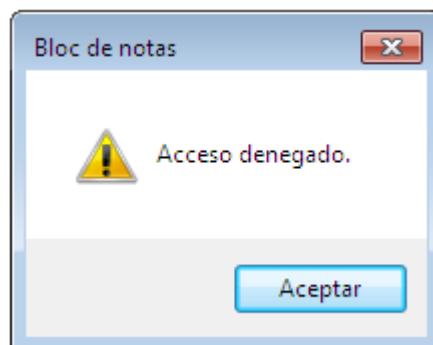
- **Almacena el fichero generado en cualquier lugar.**



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

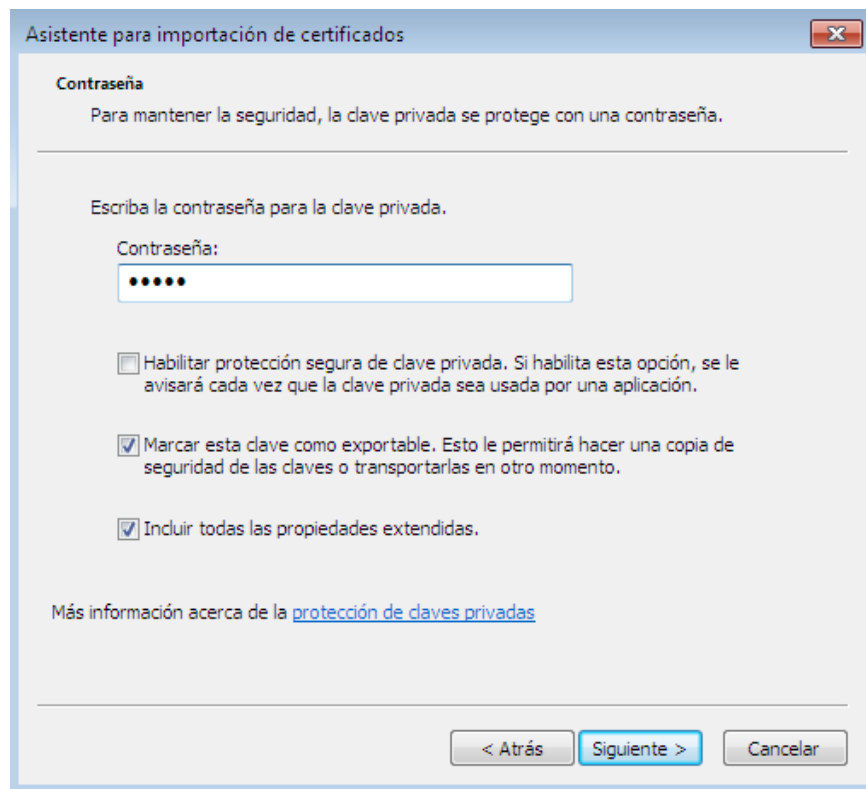
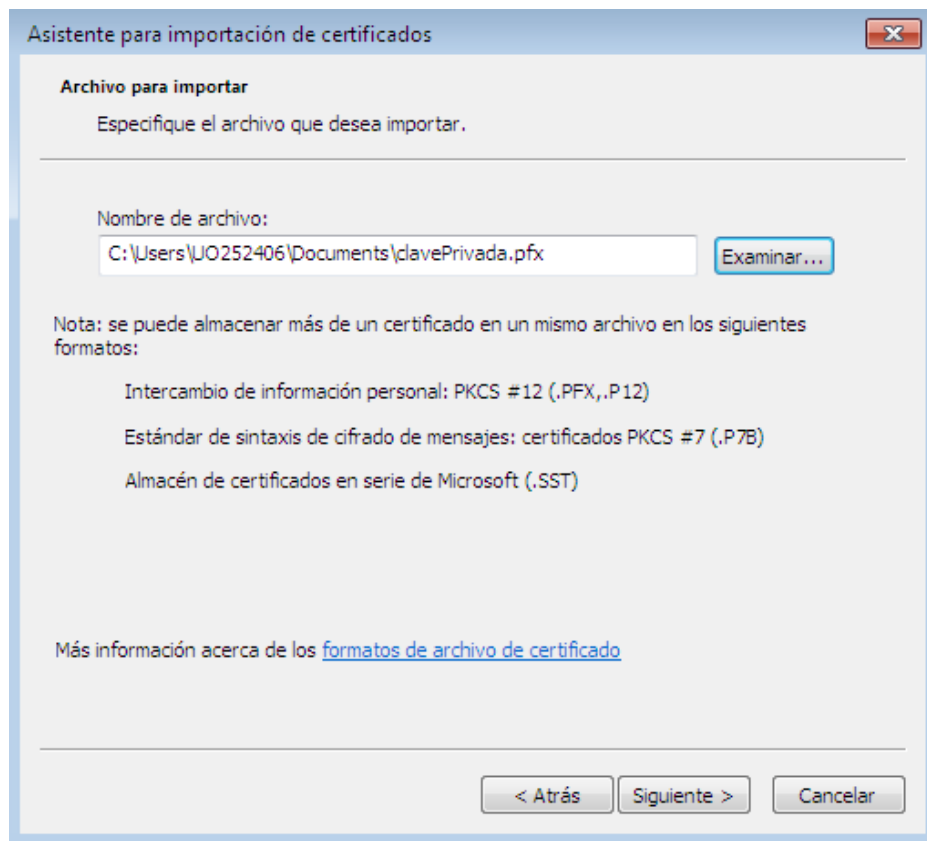
Prueba a acceder a la carpeta encriptada. ¿Puedes hacerlo? ¿Por qué?

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



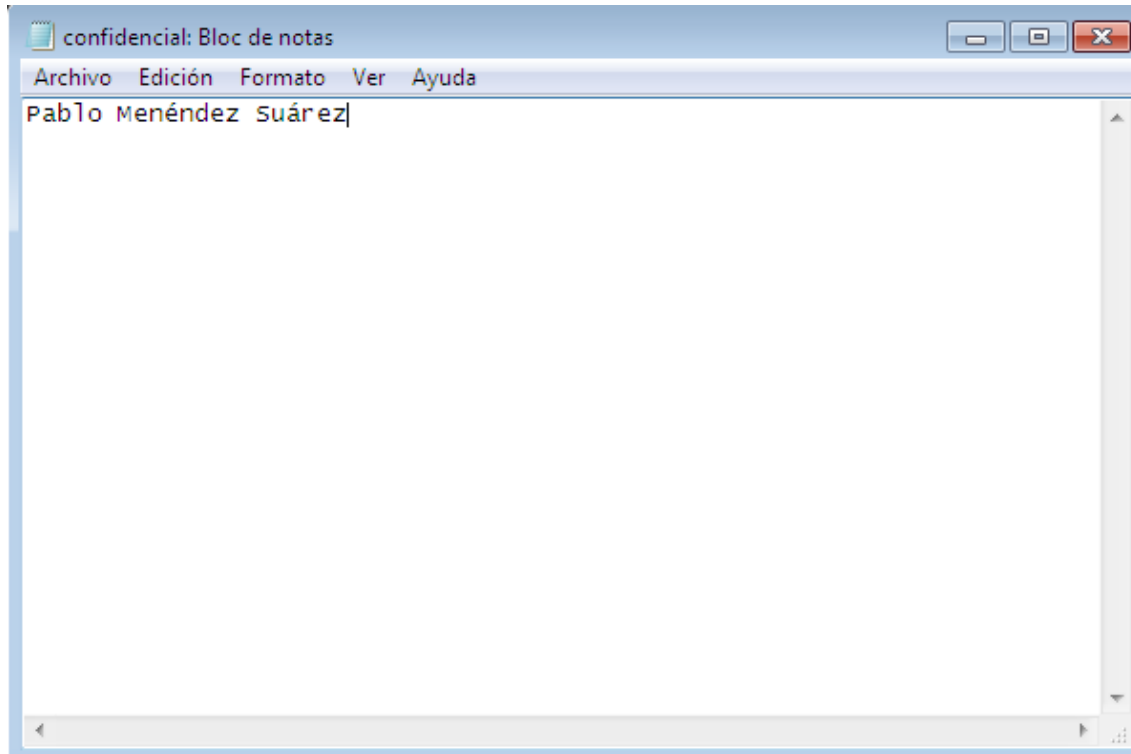
Importa el certificado (mmc.exe, ... Todas las tareas, Importar). Recuerda al importar hacer la clave exportable para que se pueda volver a retirar.

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



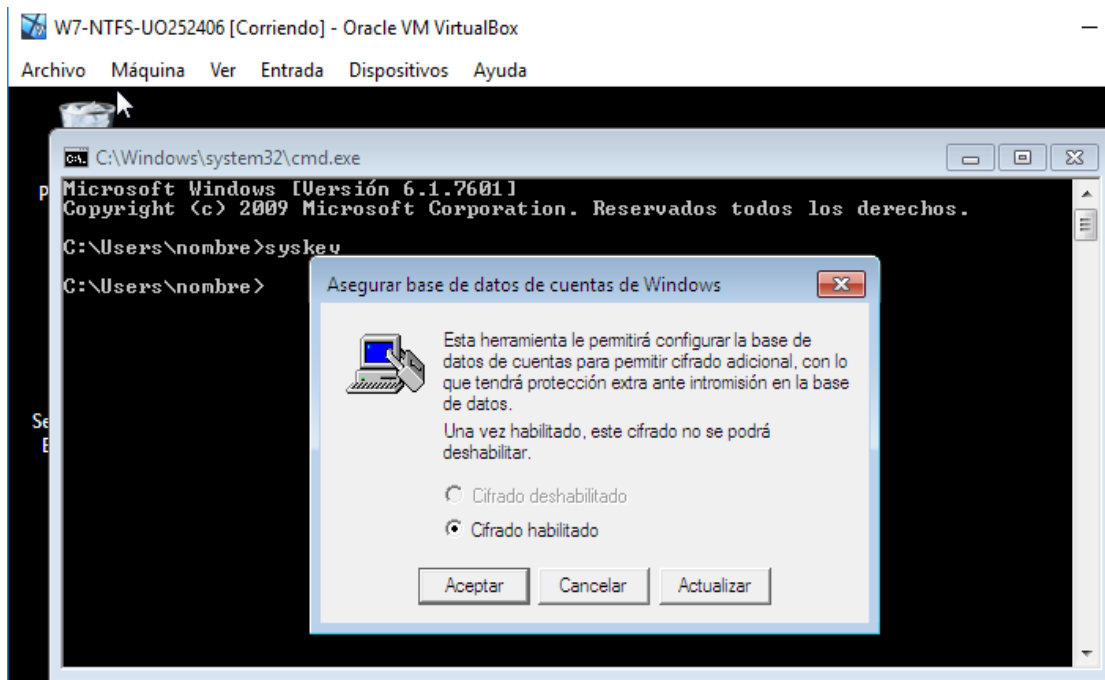
Prueba a acceder a la carpeta encriptada. ¿Puedes hacerlo? ¿Por qué?

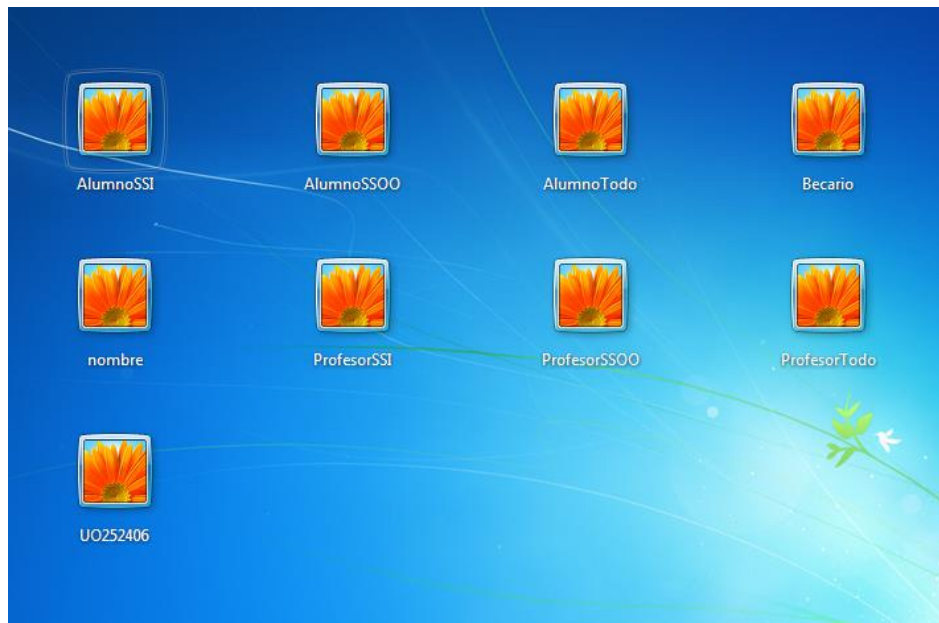
Si, tanto a la carpeta como al fichero ya que hemos importado el certificado de seguridad.



Parte 6: Otras órdenes

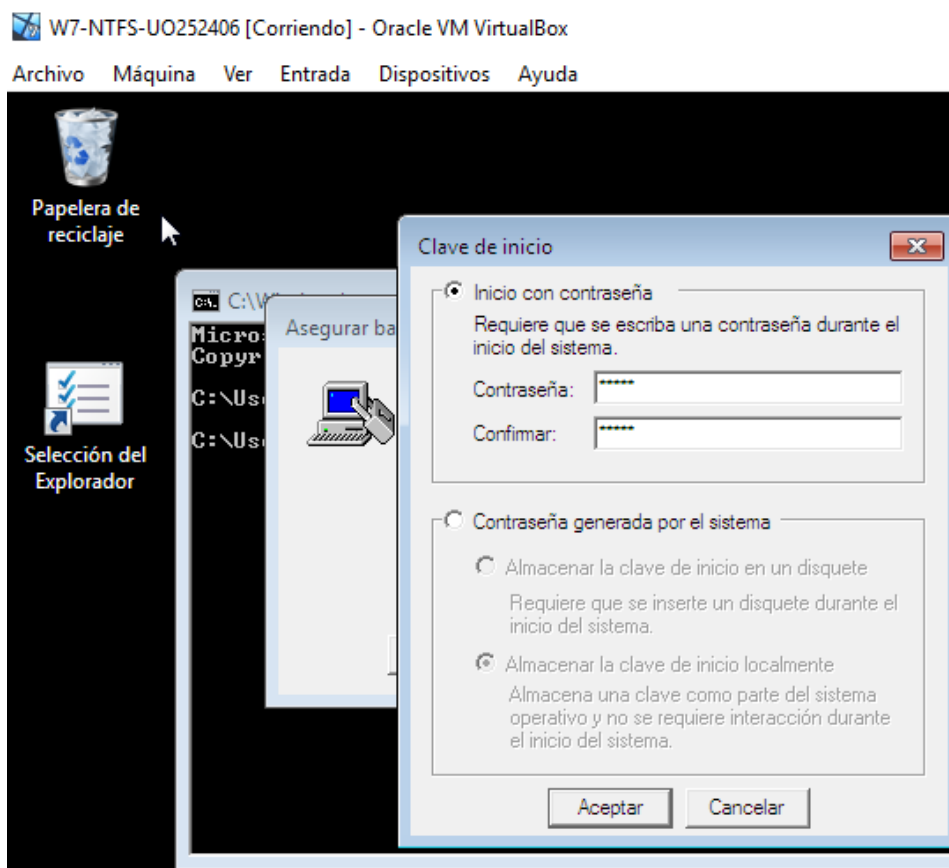
Utiliza la orden syskey para encriptar la base de datos de cuentas, utilizando la contraseña generada por el sistema. Reinicia el sistema. ¿Hay algún cambio en el comportamiento del mismo? ¿Por qué?



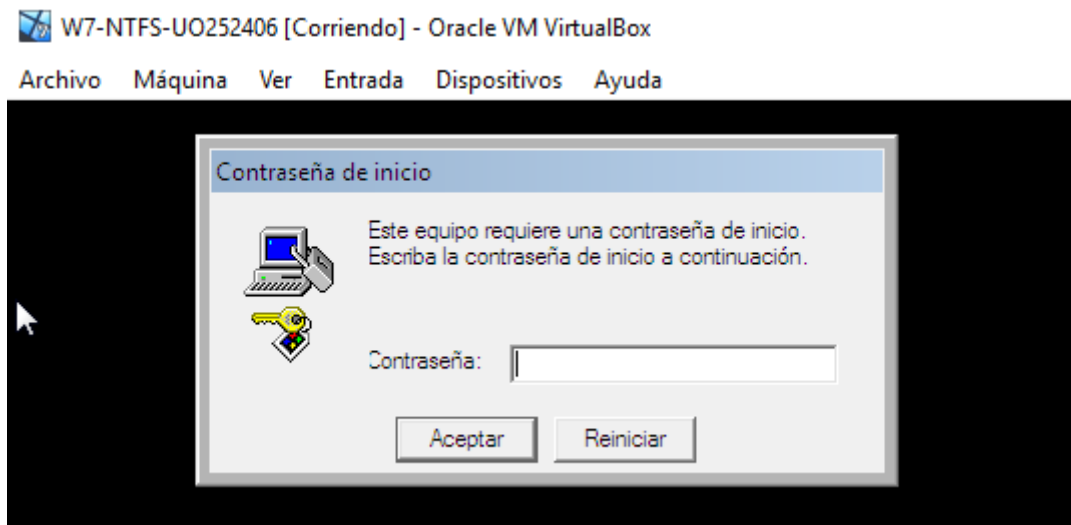


No existe ningún cambio aparente en el comportamiento del sistema, ya que el propio sistema fue el que generó la contraseña y no es necesario introducirla debido a que ya la conoce, sin embargo, la base de datos estará cifrada.

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?



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.

Directorio Activo

Parte 1: Preparación del entorno

1. Se dispone de dos máquinas virtuales

CLIENTE: Windows 7 – AD

← Crear máquina virtual

Nombre y sistema operativo

Nombre: W7-AD-UO252406

Tipo: Microsoft Windows

Versión: Windows 7 (32-bit)

Tamaño de memoria

4 MB 2048 MB 16384 MB

Disco duro

☐ No agregar un disco duro virtual

☐ Crear un disco duro virtual ahora

☒ Usar un archivo de disco duro virtual existente

Windows 7.vmdk (Normal, 60,00 GB)

Modo guiado Crear Cancelar

SERVIDOR: Windows Server 2008

← Crear máquina virtual

Nombre y sistema operativo

Nombre: WS8-AD-UO252406

Tipo: Microsoft Windows

Versión: Windows 2008 (64-bit)

Tamaño de memoria

4 MB 2048 MB 16384 MB

Disco duro

☐ No agregar un disco duro virtual

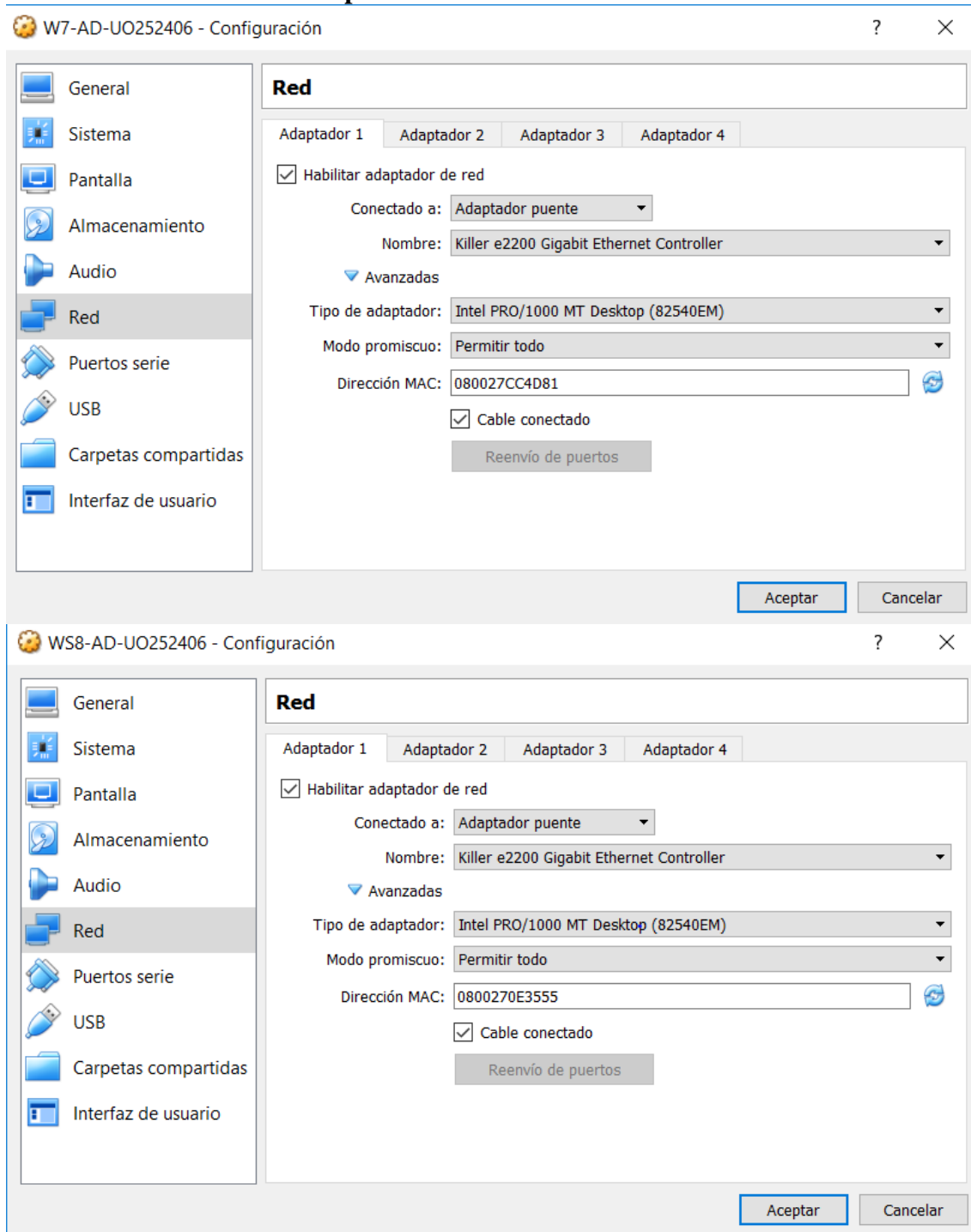
☐ Crear un disco duro virtual ahora

☒ Usar un archivo de disco duro virtual existente


Windows Server 2008.vmdk (Normal, 60,00 GB)

Modo guiado Crear Cancelar

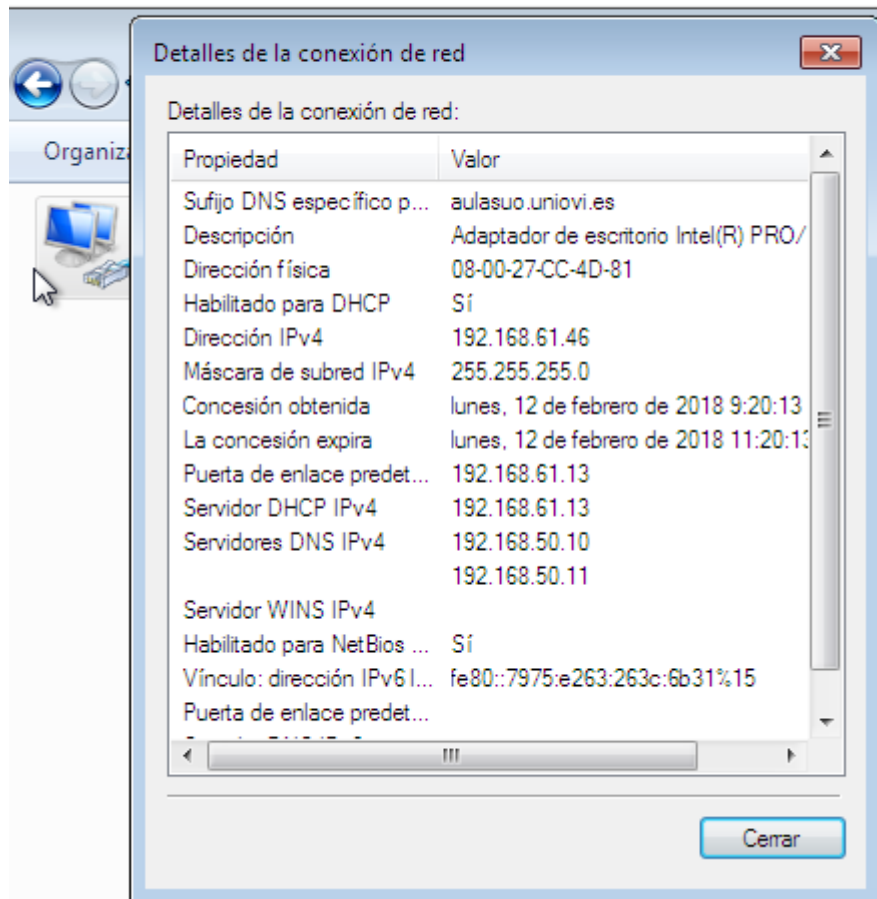
Para que ambas máquinas puedan comunicarse entre sí, hay que especificar en cada una de ellas que usen el modo “Adaptador puente”. Clic derecho en la máquina virtual-Red y en el Adaptador 1 elegimos conectado a “Adaptador puente”. En Avanzadas elegimos Modo promiscuo-Permitir todo.



Vete a "Menú inicio, Panel de control, Centro de Redes y Recursos Compartidos, Cambiar Configuración del Adaptador, Conexión de área local, botón derecho, estado, detalles" y toma nota de la IP, máscara de subred, la puerta de enlace y el servidor DNS

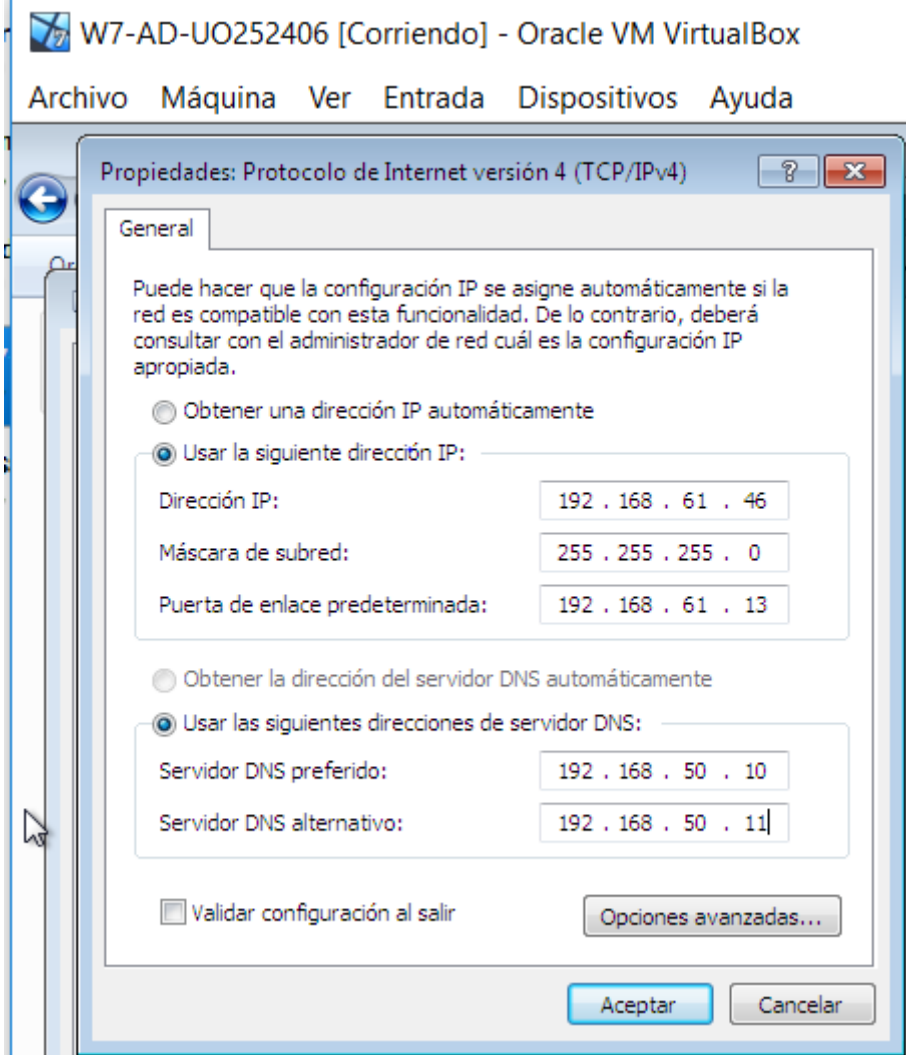
 W7-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

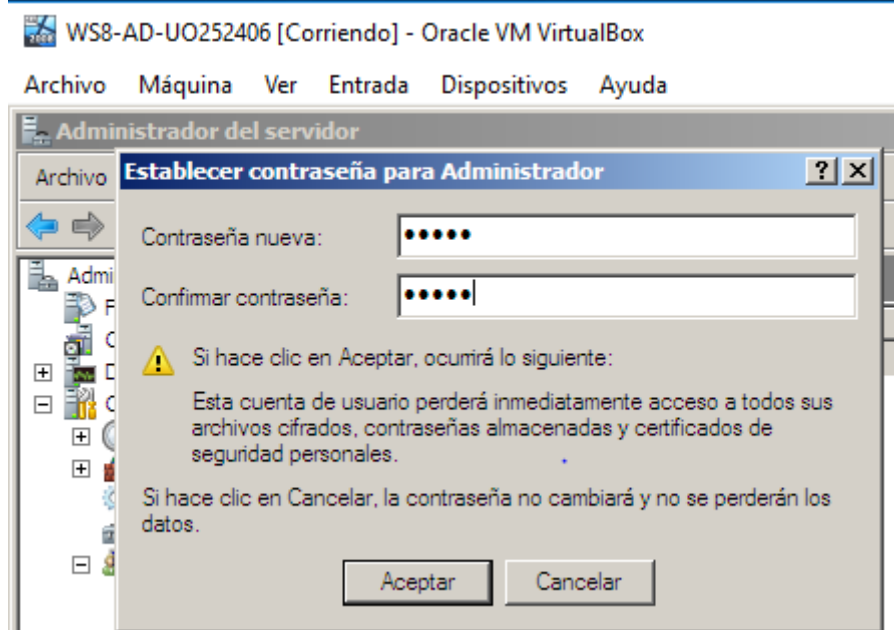


- **Dirección IPv4:** 192.168.61.46
- **Mascara de subred:** 255.255.255.0
- **Puerta de enlace:** 192.168.61.13
- **Servidor DNS preferido:** 192.168.50.10
- **Servidor DNS alternativo:** 192.168.50.11

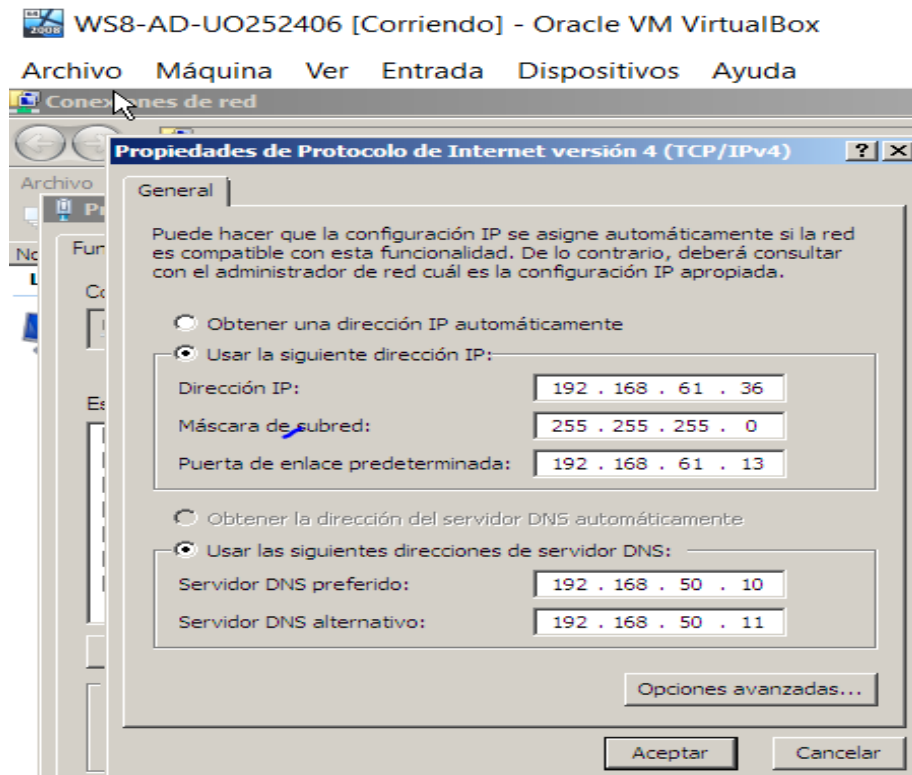
Asigna esas propiedades como valores estáticos. "Menú inicio, Panel de control, Centro de Redes y Recursos Compartidos, Cambiar Configuración del Adaptador, Conexión de área local, botón derecho, propiedades, protocolo internet (TCP/IP), propiedades"



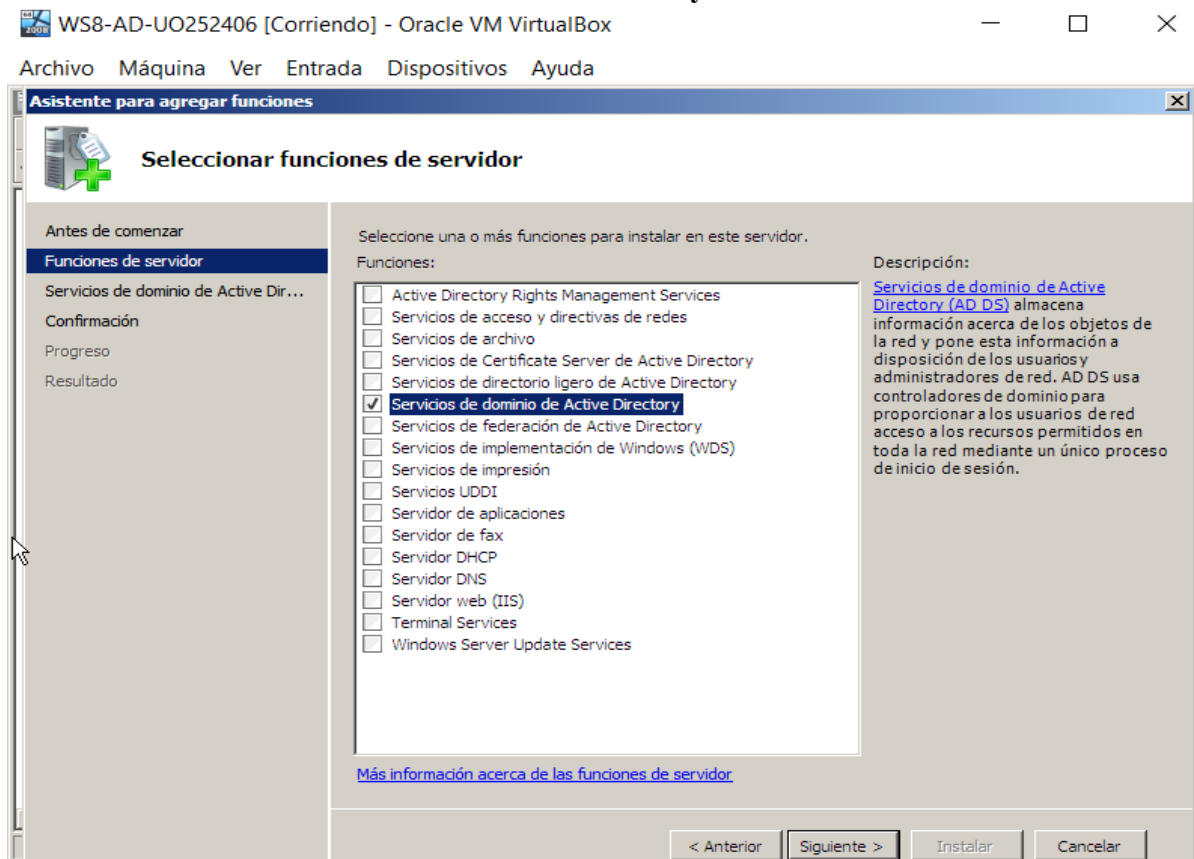
La máquina virtual tiene dos cuentas: “nombre” y “administrador” e inicialmente no tienen contraseña ninguna de ellas. Añade una contraseña que puedas recordar a la cuenta a cada una de ellas. La cuenta “administrador” es la que tiene todos los permisos de administración del servidor.



Asignar una IP estática del mismo rango que la máquina W7. Inicio, Red, (botón derecho) Propiedades, Administrar Conexiones de Red, Conexión de Área Local, (botón derecho) Propiedades, protocolo internet (TCP/IP), propiedades

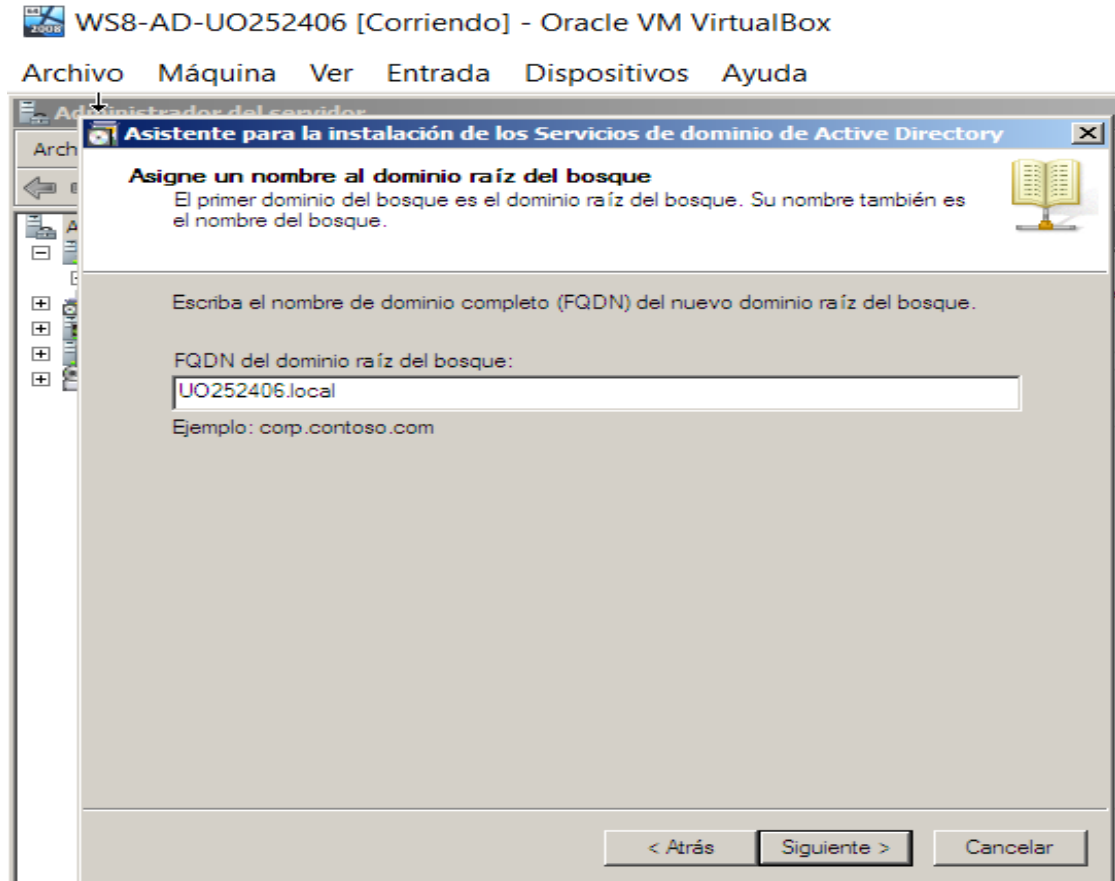


Pinchar en “Agregar funciones” • En el asistente: • Seleccionar “Servicios de Dominio de Active Directory”



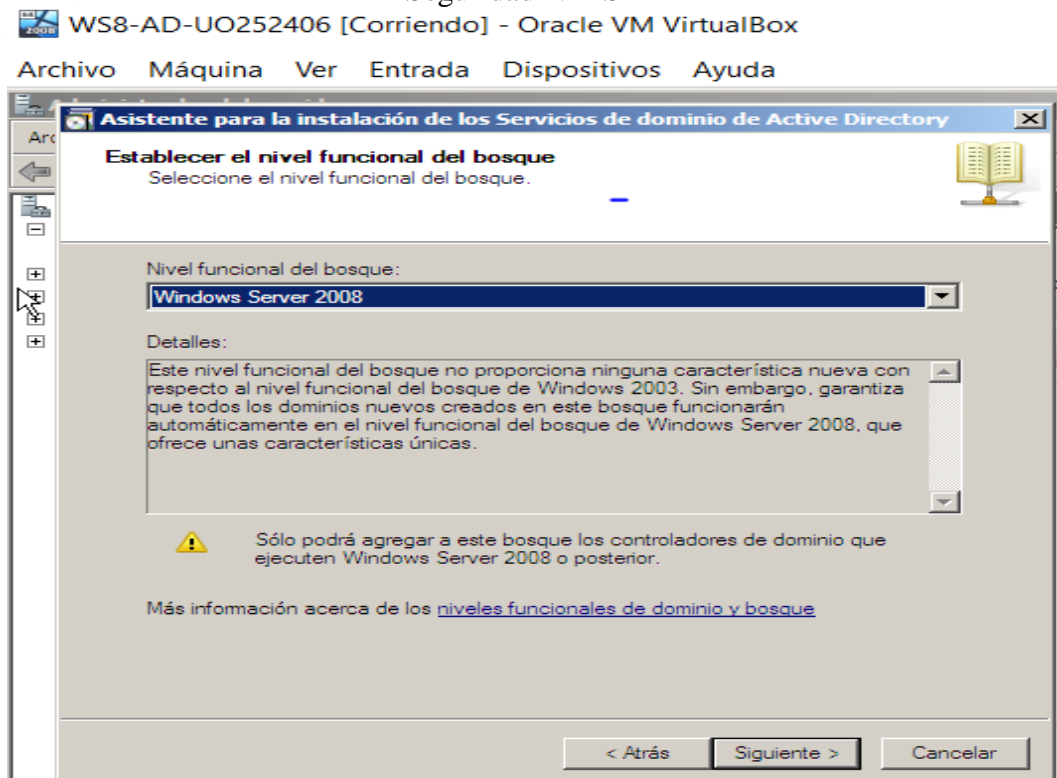
Tras instalar una serie de componentes llegaremos a una pantalla donde nos pide que iniciemos el asistente, lo hacemos. Si nos equivocamos podemos ejecutar el asistente mediante dcpromo.exe

Seleccionamos crear un bosque nuevo • Como nombre FQDN": UOXXXX.local.(siendo UOXXXX tu UO)

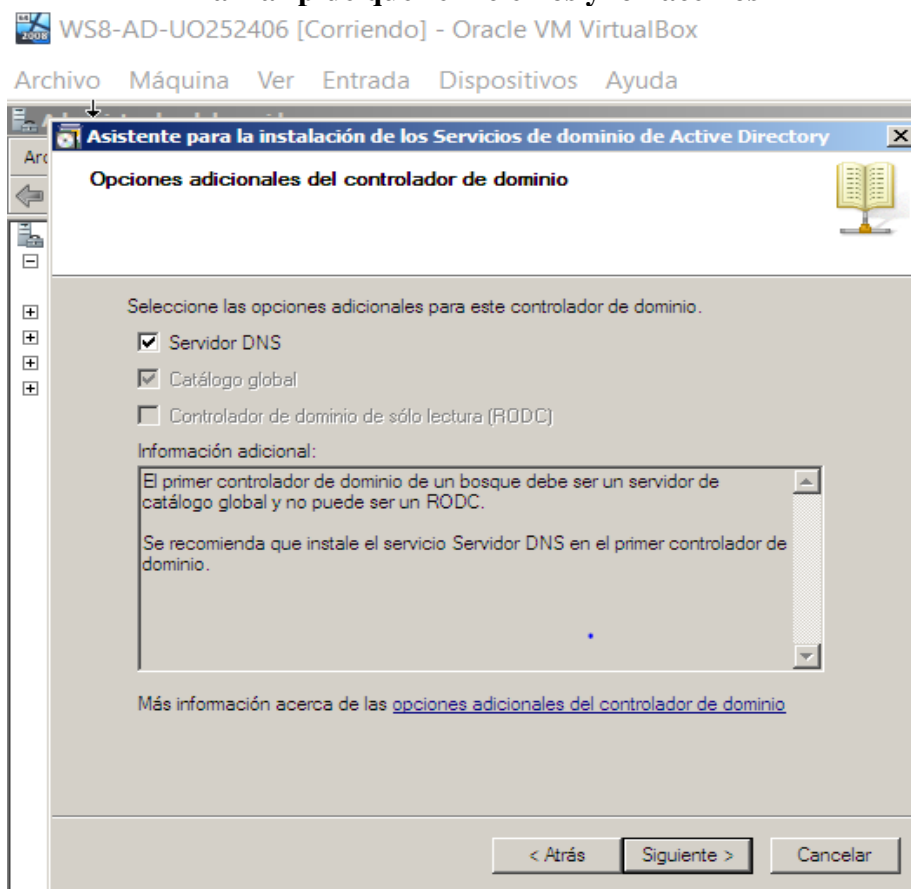


• Vamos aceptando opciones por defecto. • Cuando nos pregunta por el “nivel Funcional del Bosque” seleccionamos 2003 si queremos que el cliente sea un XP, si tenemos como cliente W7 podemos usar 2008.

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

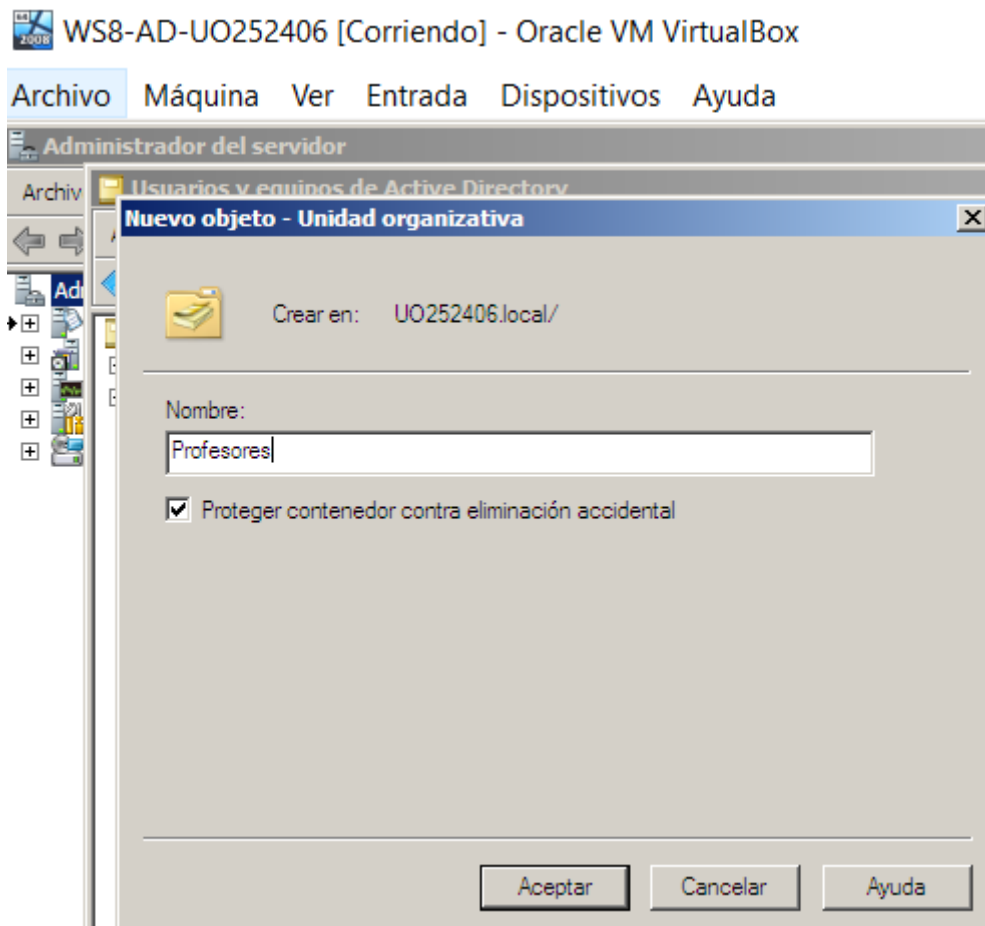


Cuando nos pregunta por la opción de crear un DNS aceptamos todo por defecto. • Al finalizar pide que reiniciemos y lo hacemos

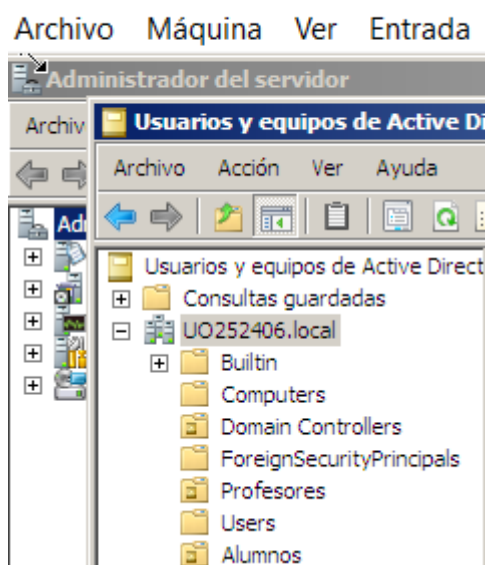


Una vez reiniciado: • Iniciar sesión como administrador. • En "Menu inicio, Herramientas administrativas, Usuarios y equipos de AD, UOXXXX.local (botón derecho)": • Crear las Unidades Organizativas (UO), grupos y usuarios siguientes:

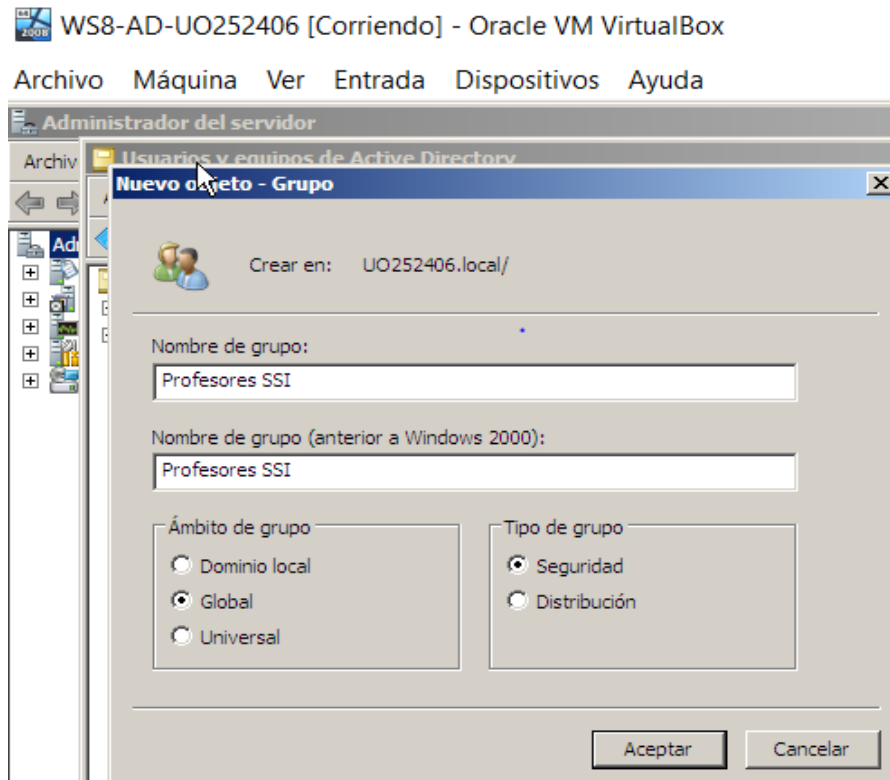
Unidades Organizativas: • Profesores. • Alumnos.



WS8-AD-UO252406 [Corriendo]

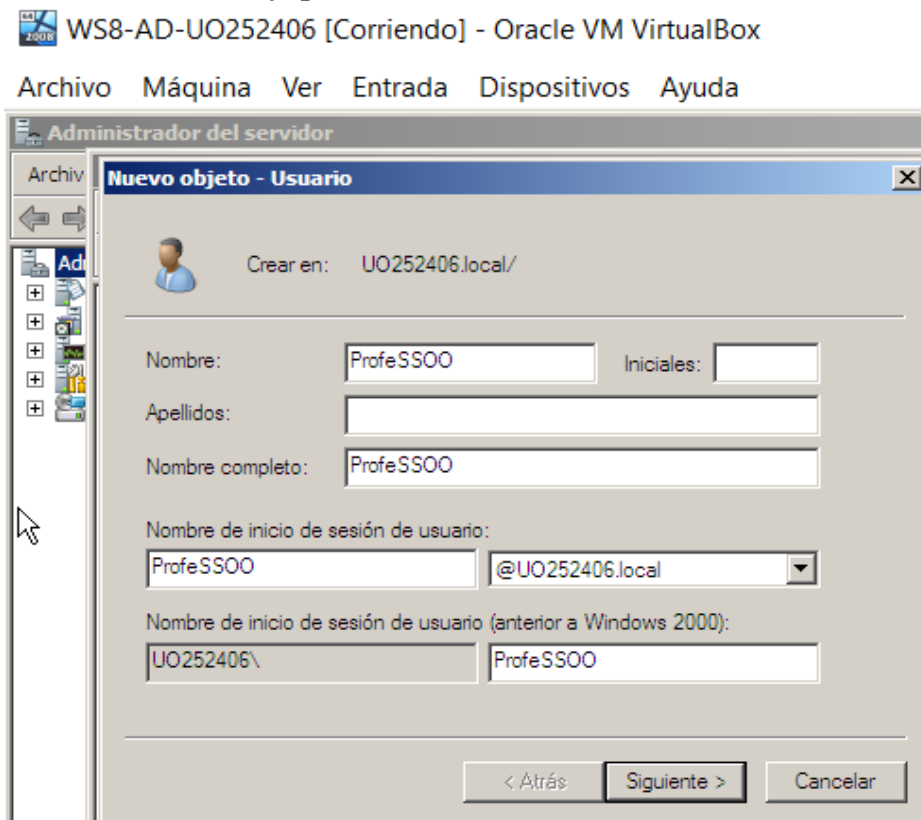


Grupos de seguridad globales (en las respectivas UO): • Profesores SSI • Profesores SSOO
 • Alumnos SSI • Alumnos SSOO



Usuarios (en las respectivas UO):

Poner a todos ellos contraseñas fáciles de recordar (por ejemplo “ssi_2018”), que nunca caducan y que no cambie al inicio de sesión.



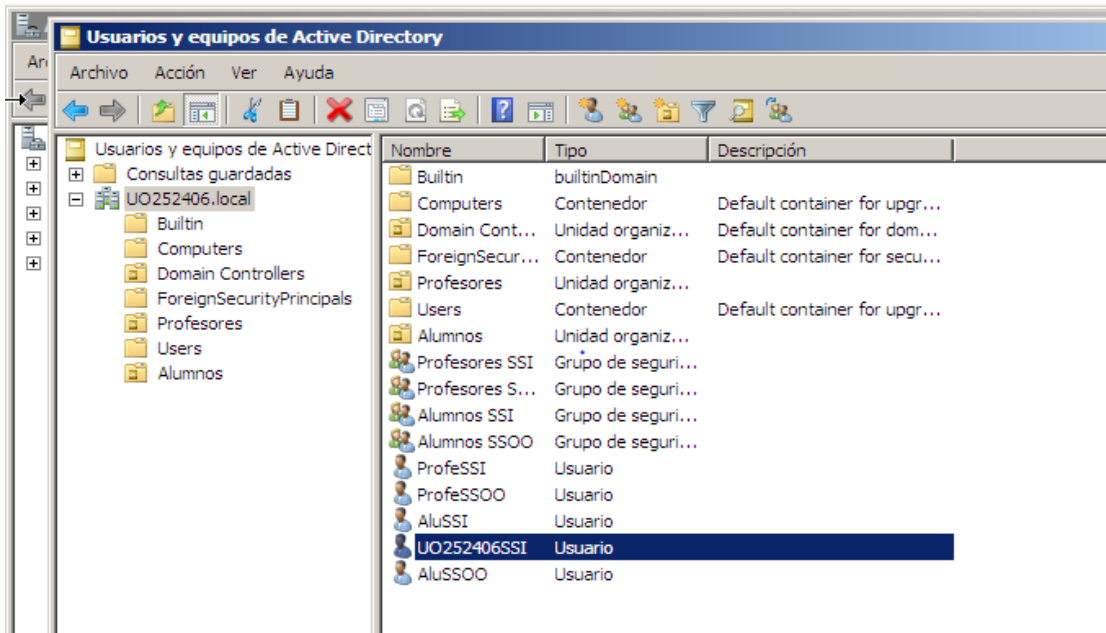
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS

WS8-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

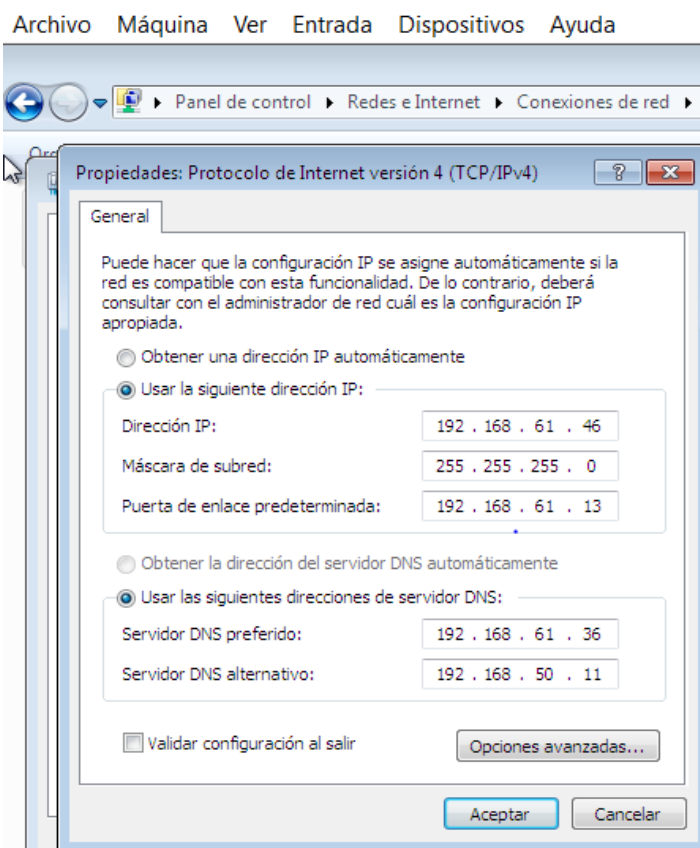
Archivo Máquina Ver Entrada Dispositivos Ayuda



5. Configuración de Windows 7:

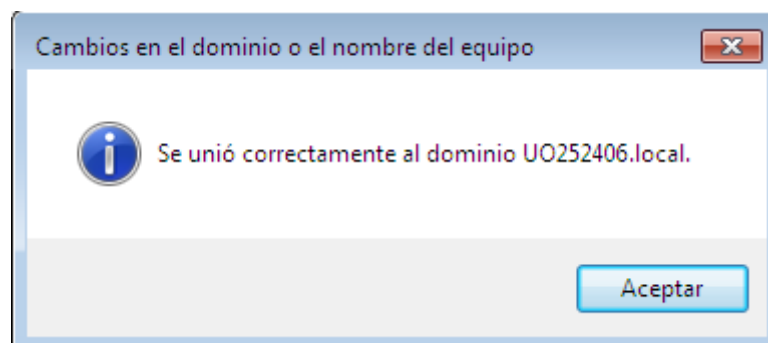
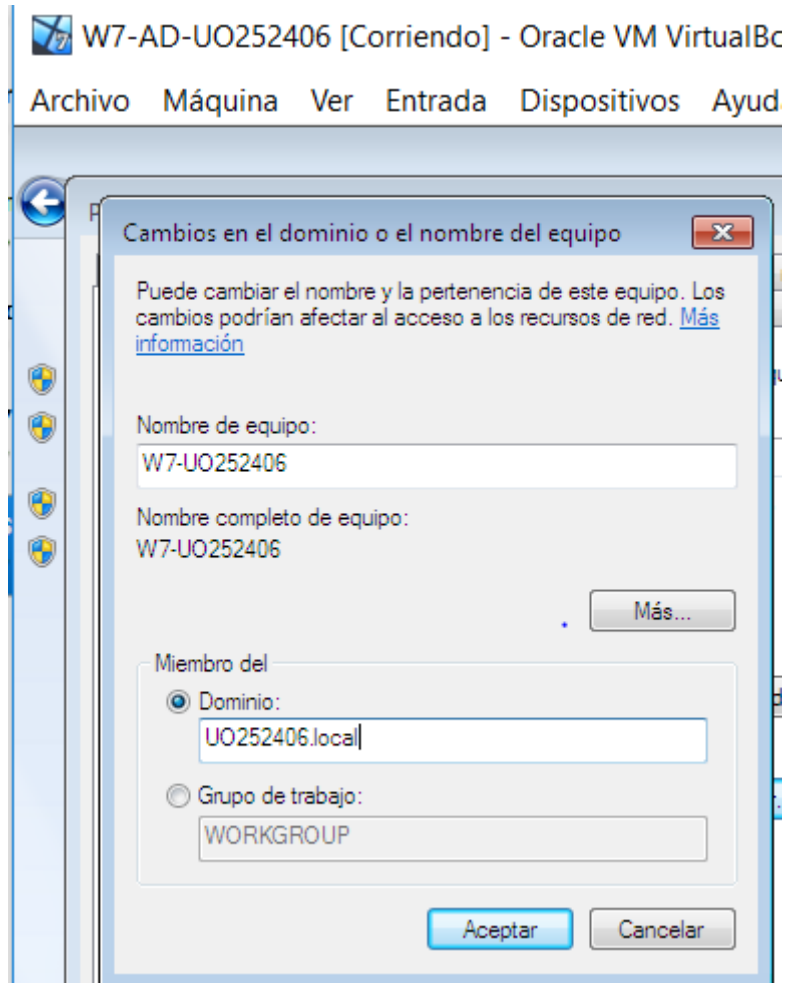
Añadir en el W7 el equipo W2008 como DNS. ("Menú inicio, Panel de control, Centro de Redes y Recursos Compartidos, Cambiar Configuración del Adaptador, Conexión de área local, botón derecho, propiedades, protocolo internet (TCP/IP), propiedades")

W7-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

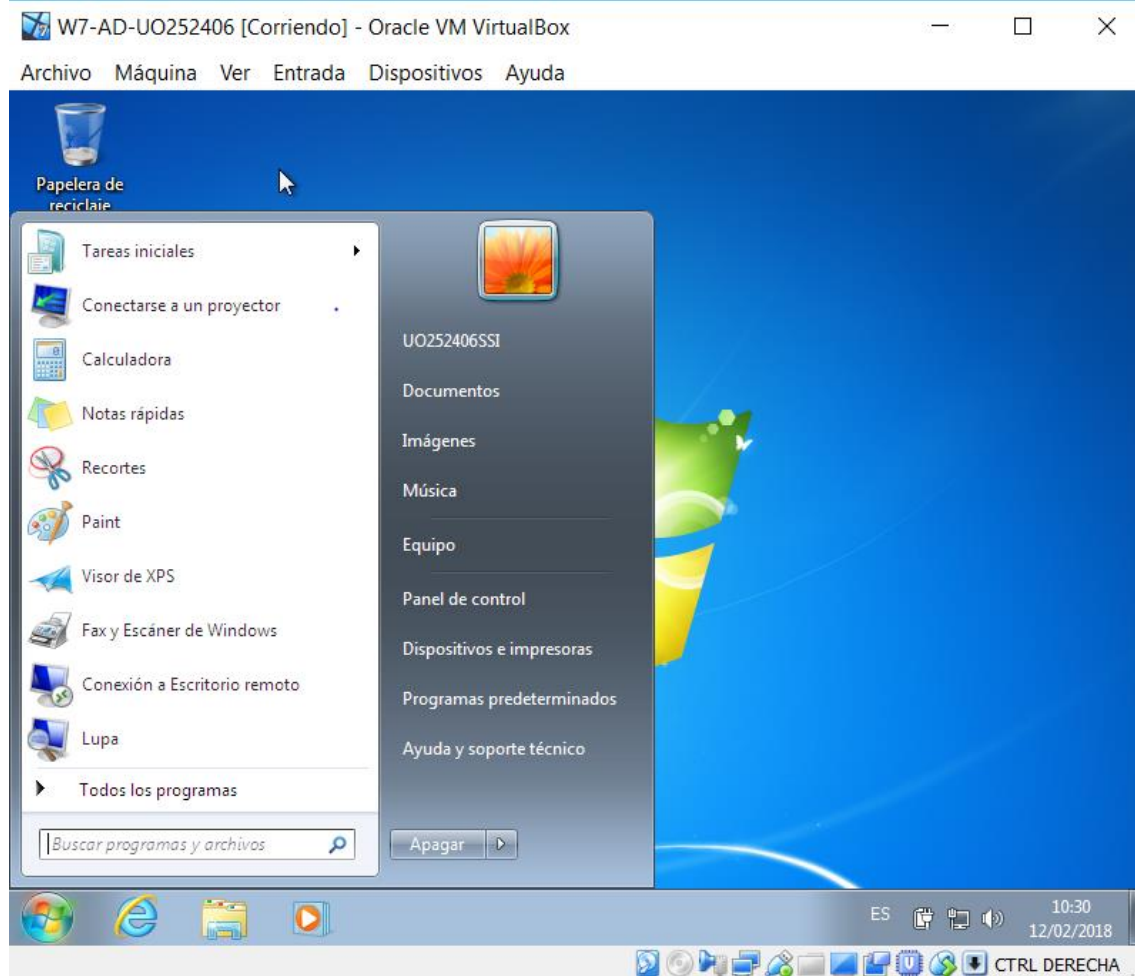


Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Seguridad NTFS

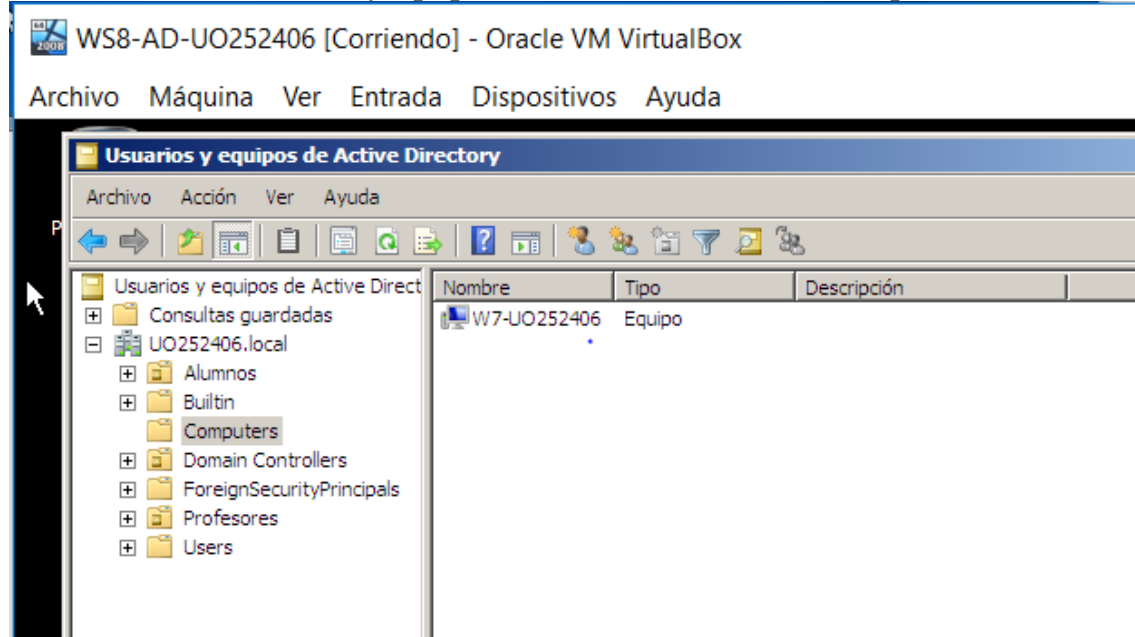
Incluye esta máquina en el dominio UOXXXX.local:



Comprueba que puedes entrar en Windows 7 con los usuarios del dominio UOXXXXXX.



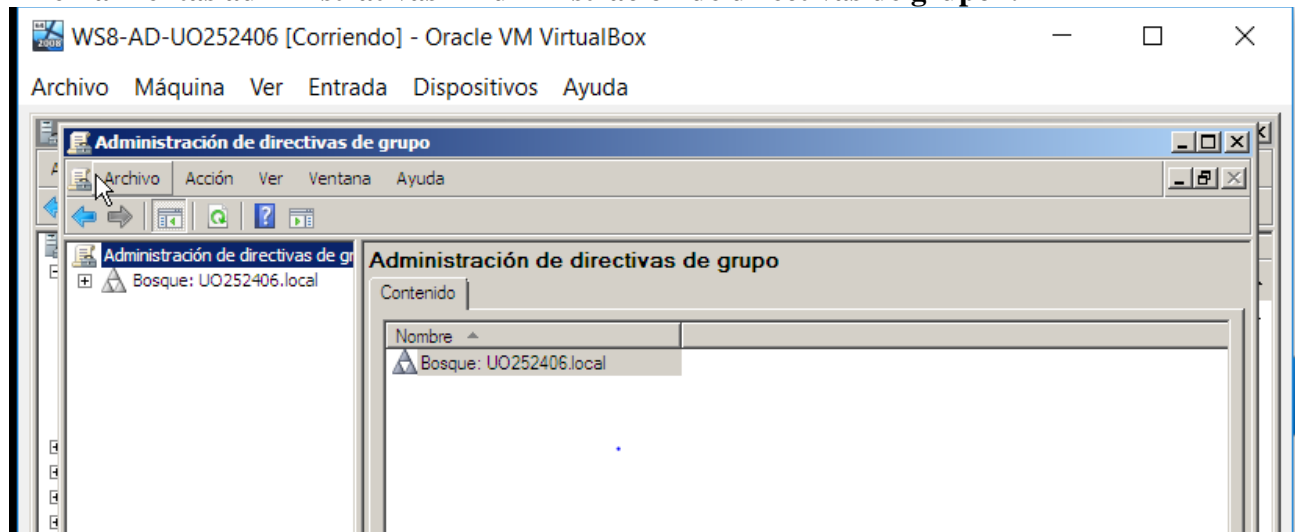
Comprueba que puedes ver el equipo en el servidor 2008 • Menu inicio, Herramientas administrativas, Usuarios y equipos de AD, UOXXXX.local, computers



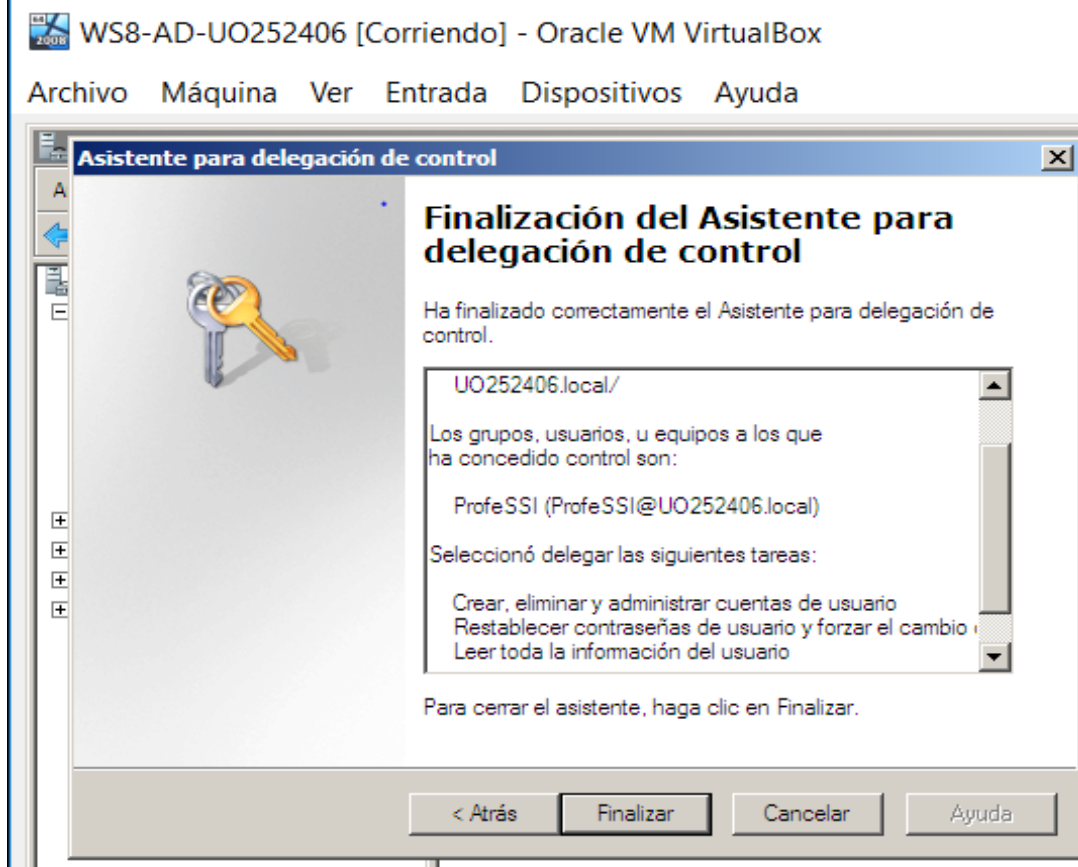
Directorio Activo:

Parte 1: Seguridad en Active Directory

1. Desde el servidor, explora las opciones de Configuración de Seguridad del Dominio. o "Herramientas administrativas – Administración de directivas de grupo".



2. Desde el servidor, delega el control de la UO "Alumnos" a profeSSI (para crear, eliminar y administrar cuentas de usuario y restablecer contraseñas y forzar el cambio de contraseña y leer toda la información del usuario) "Herramientas Administrativas/Usuarios y Equipos de Active Directory, botón derecho en la UO, delegar Control"



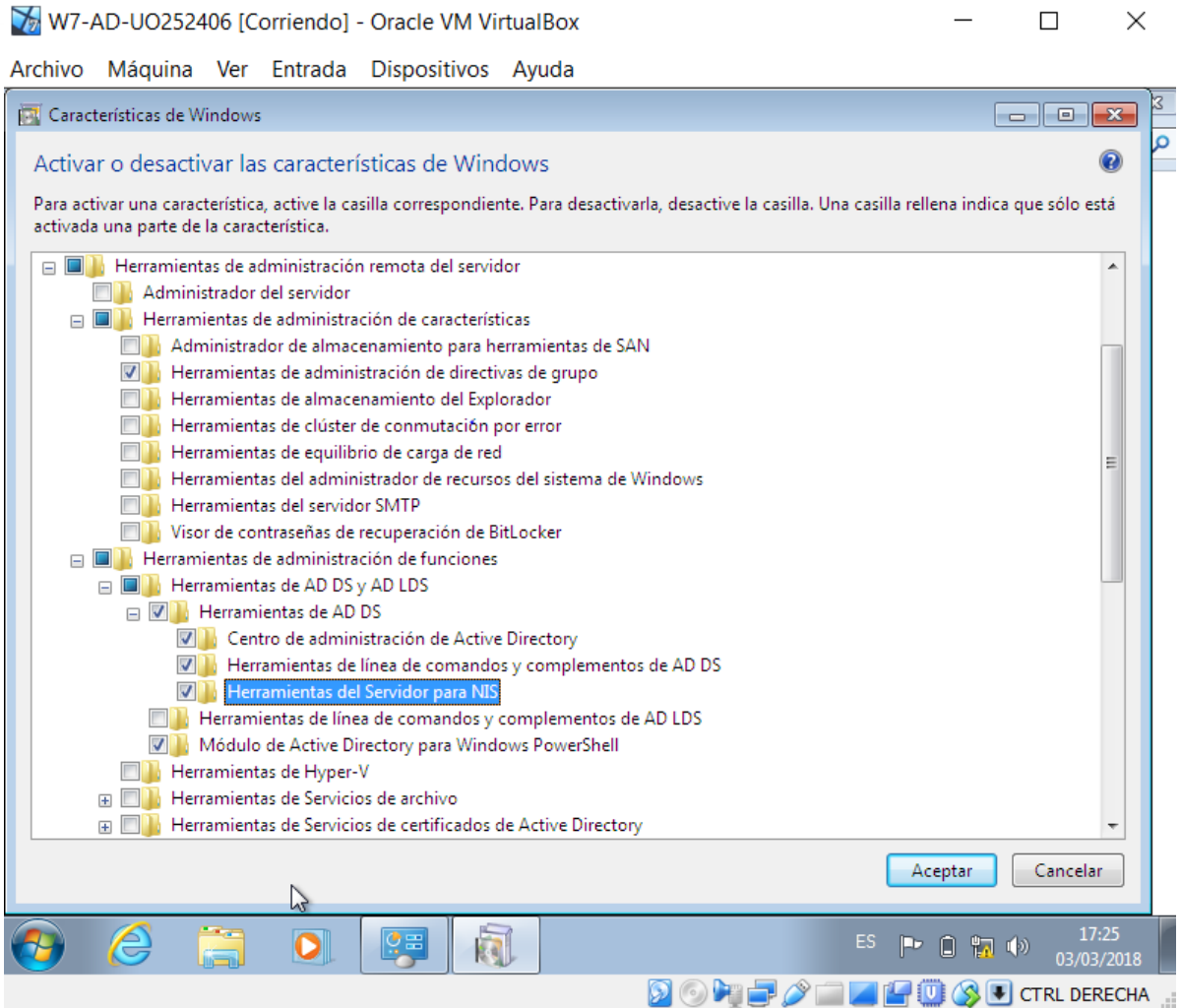
3. Inicia sesión como administrador en Windows 7 y active las herramientas de administración remota del servidor:

- Haga clic en Inicio, Panel de control y, a continuación, en Programas. En la sección Programas y características, haga clic en Activar o desactivar las características de Windows. Si el Control de cuentas de usuario le pide que permita que se abra el cuadro de diálogo de las características de Windows, haga clic en Continuar. En el cuadro de diálogo Características de Windows, expanda las Herramientas de administración remota del servidor.
- Los paquetes a instalar son los de AD. Se encuentran dentro de Herramientas de administración remota del servidor, y dentro de ella Herramientas de administración de características/Herramientas de administración de directivas de grupo. Y también el Centro de Administración de Active Directory, dentro de Herramientas de administración de funciones/Herramientas de AD DS y AD LDS / Herramientas de AD DS, marcar todas las opciones AD DS.

Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS

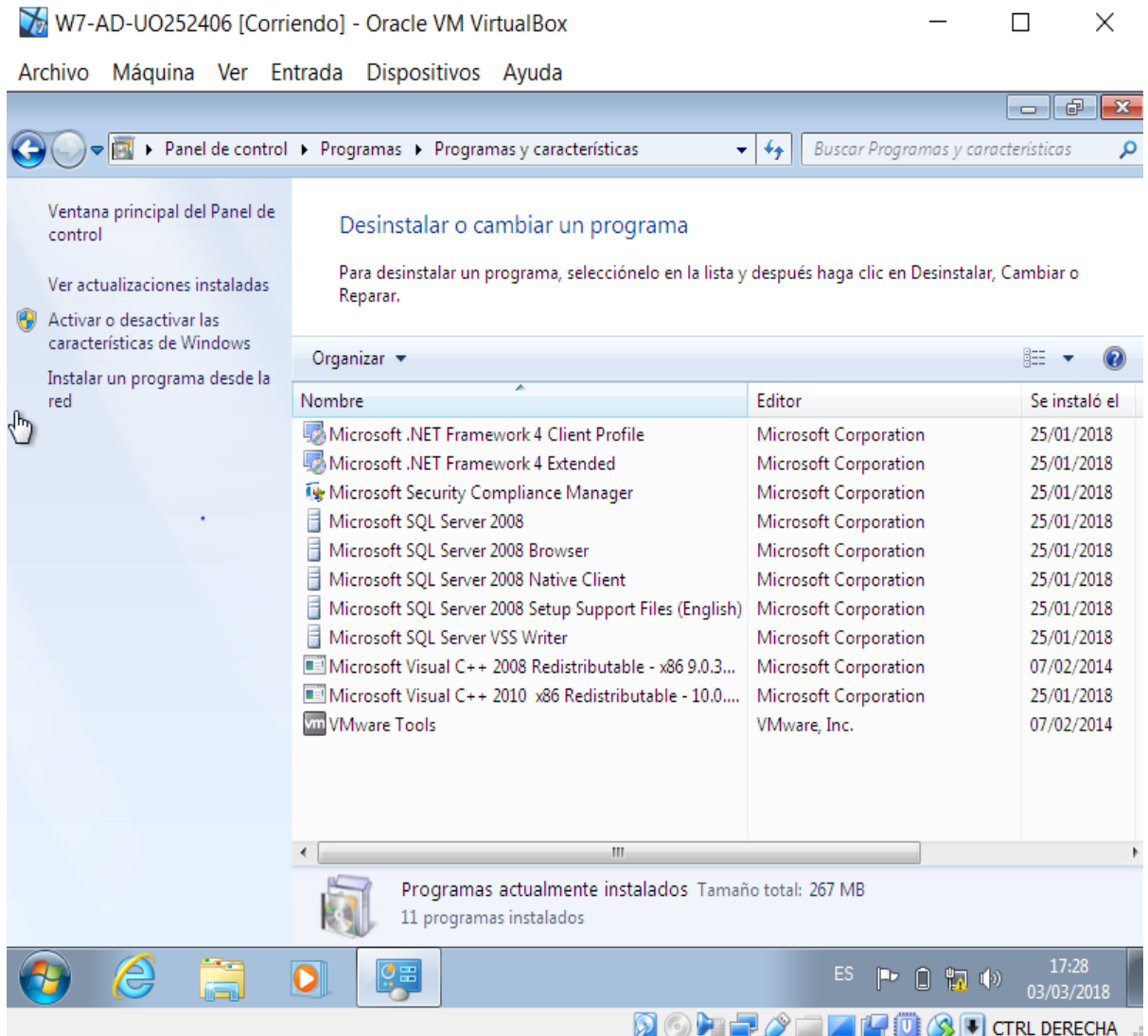


- **Explora las nuevas herramientas instaladas**

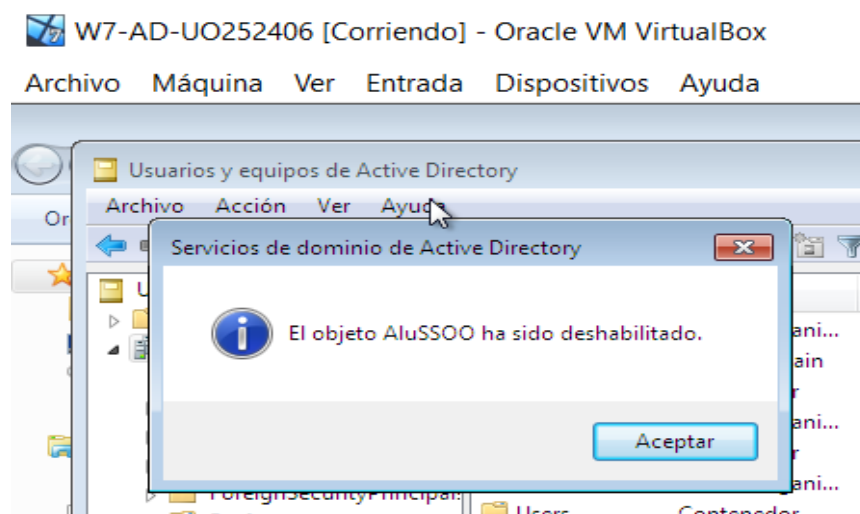
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS



- Sal de sesión y entra como profeSSI.
- En "Panel de control - Herramientas administrativas - Usuarios y Equipos de Active Directory" mira las opciones de administración que tiene profeSSI con los miembros de la UO Alumnos.
 - Deshabilita la cuenta de aluSSO.

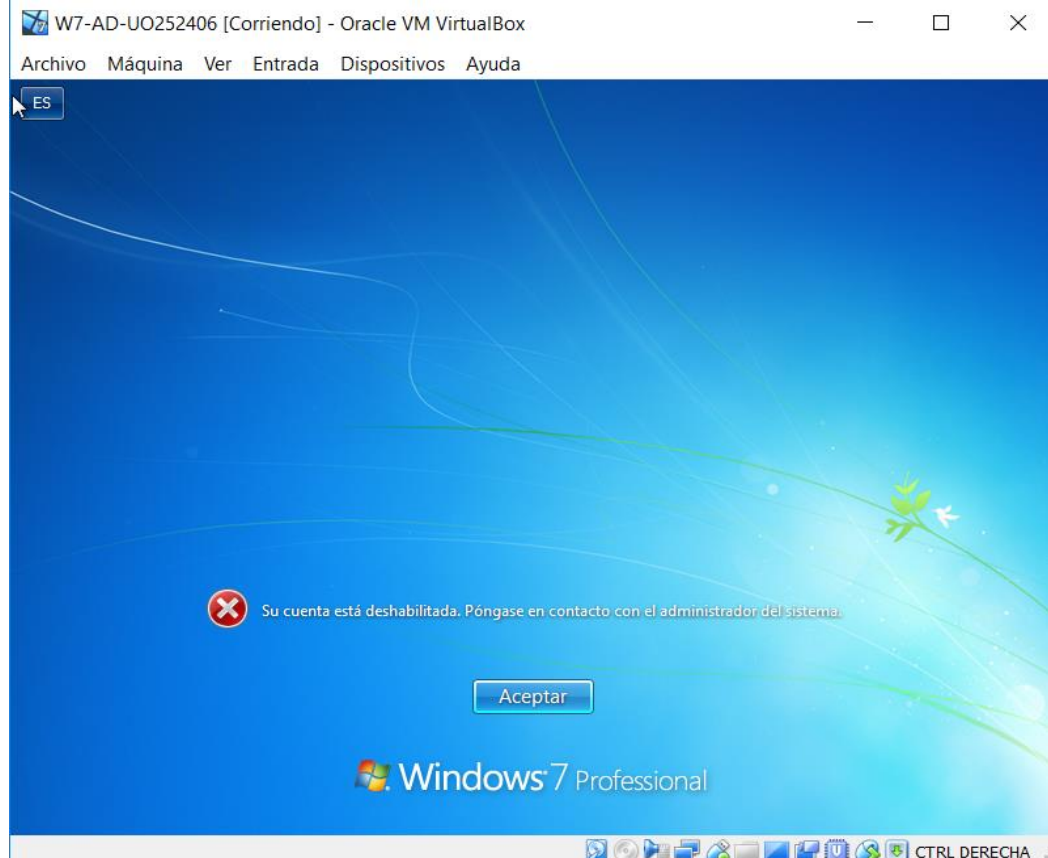


- Intenta iniciar sesión como aluSSO.

Ingeniería Informática del Software – EII

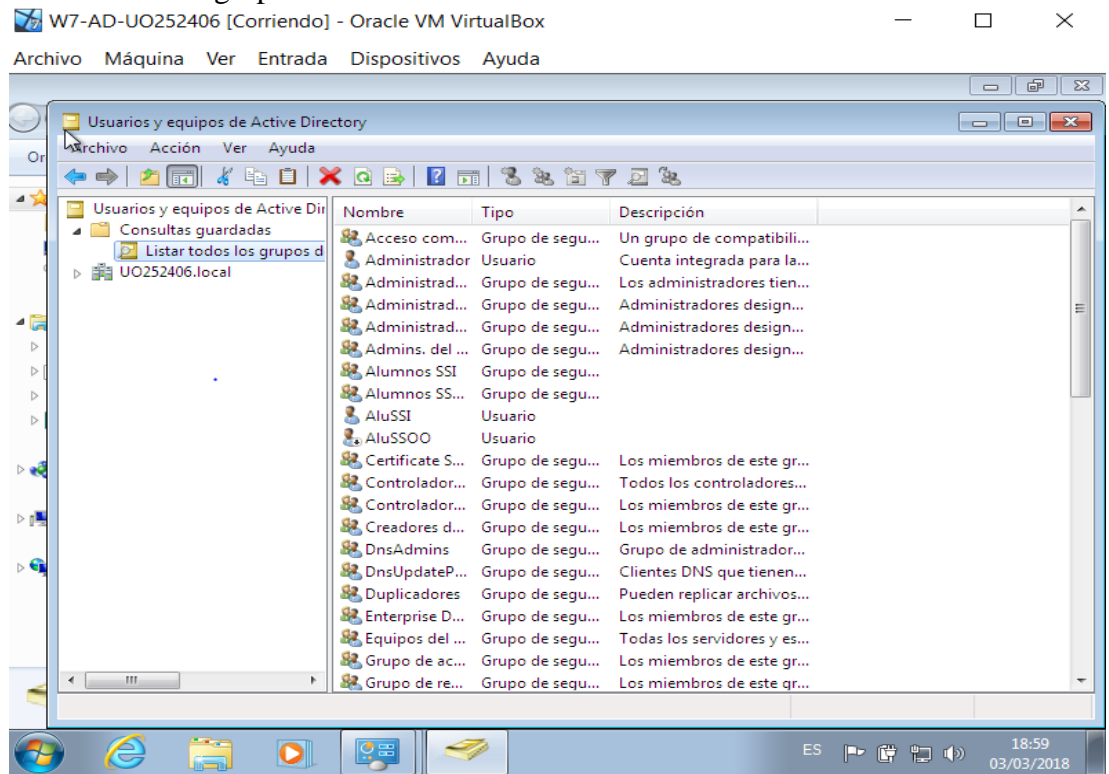
Seguridad de Sistemas informáticos

Seguridad NTFS



4. En "Usuarios y Equipos de Active Directory - Consultas guardadas - Nuevo - Consulta" crea consultas (y ejecutarlas) para:

- Listar todos los grupos definidos en AD.

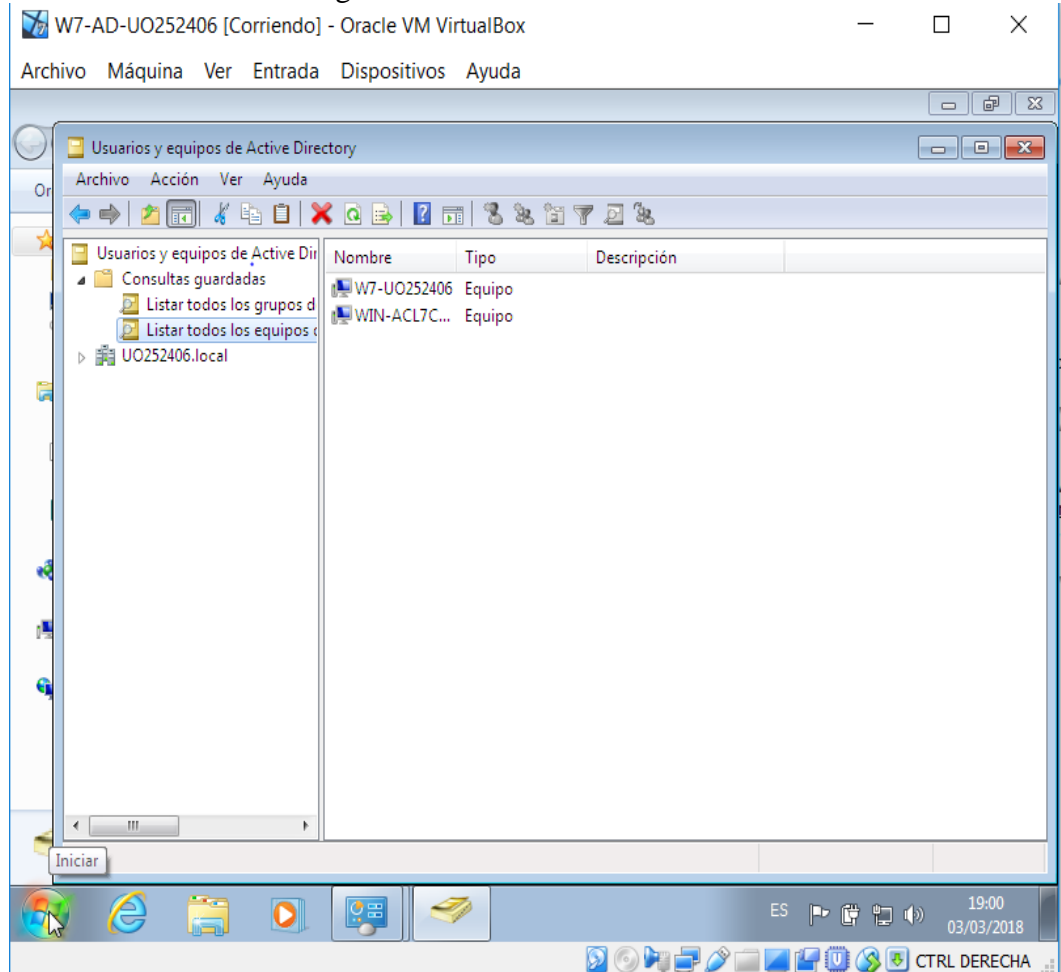


- Listar todos los equipos definidos

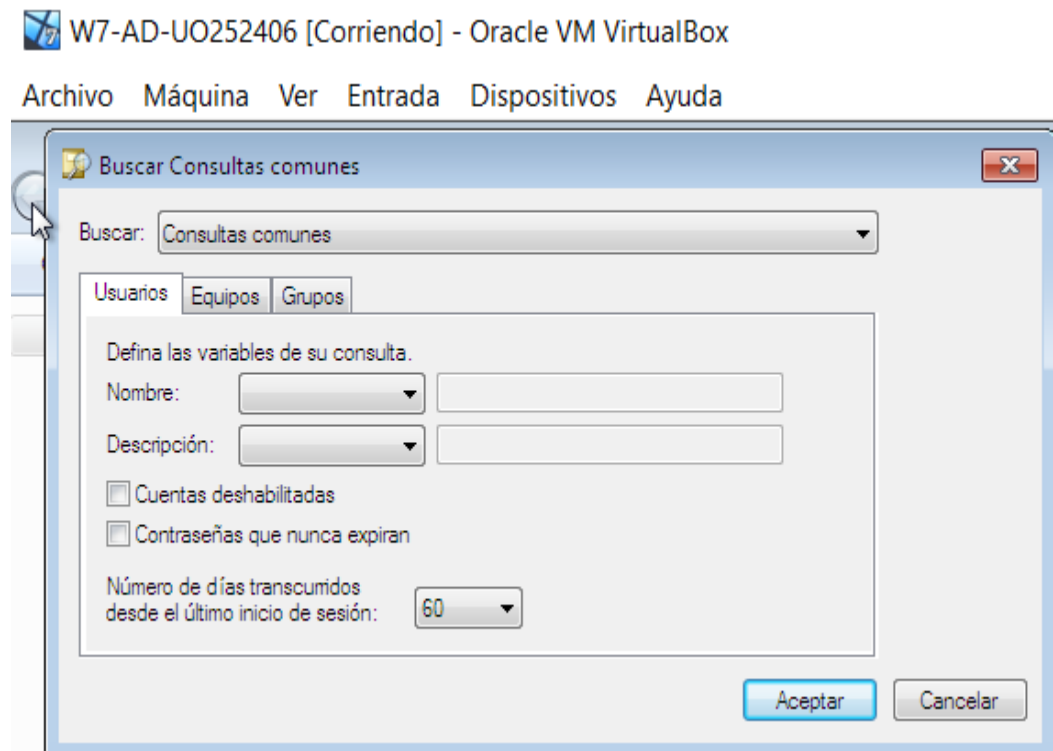
Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

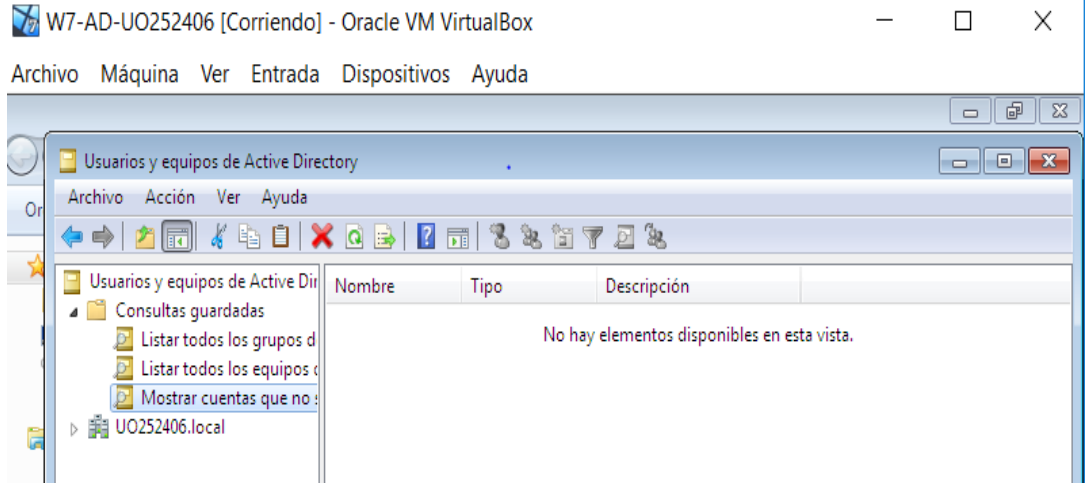
Seguridad NTFS



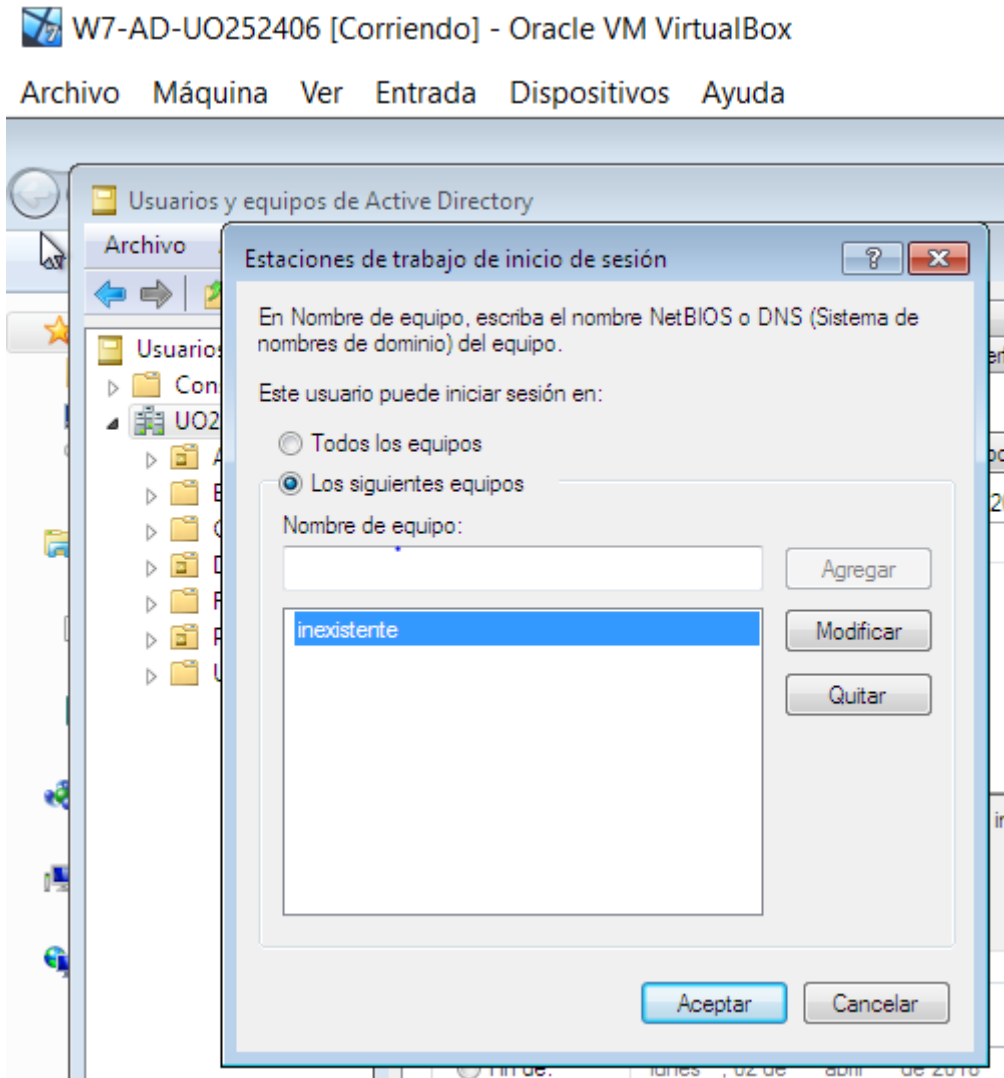
- Mostrar cuentas que no se hayan usado en 60 días



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

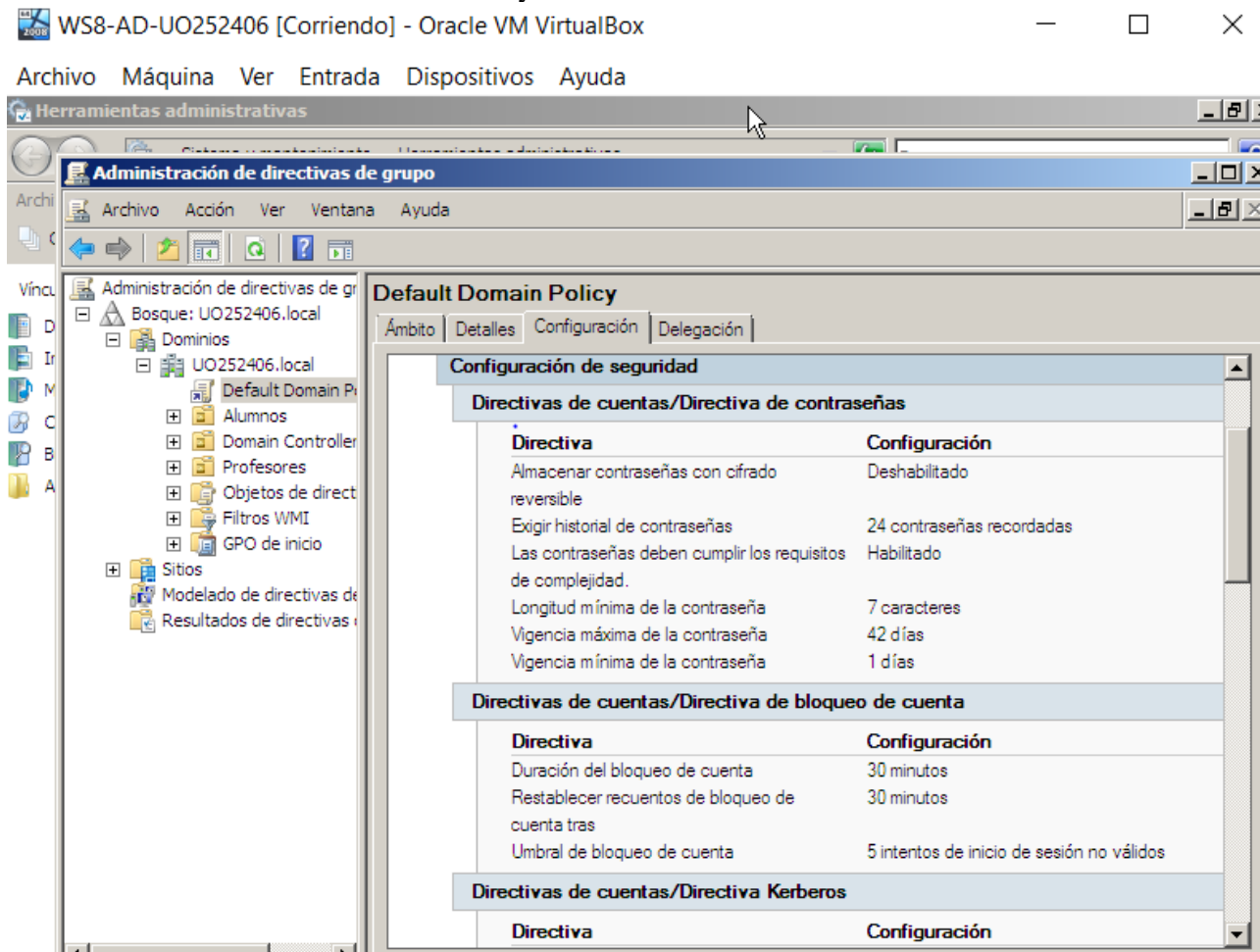


5. Impide que UOXXXXSSI pueda iniciar sesión en el equipo W7-UOxxxx (Usuarios y Equipos de Active Directory - Users -UOXXXXSSI - Propiedades, Cuenta).



6. Desde el servidor, define la directiva de bloqueo de cuentas de manera que se frustre un ataque de fuerza bruta, causando la menor perturbación posible al usuario "olvidadizo" (Configuración de Seguridad del Dominio):

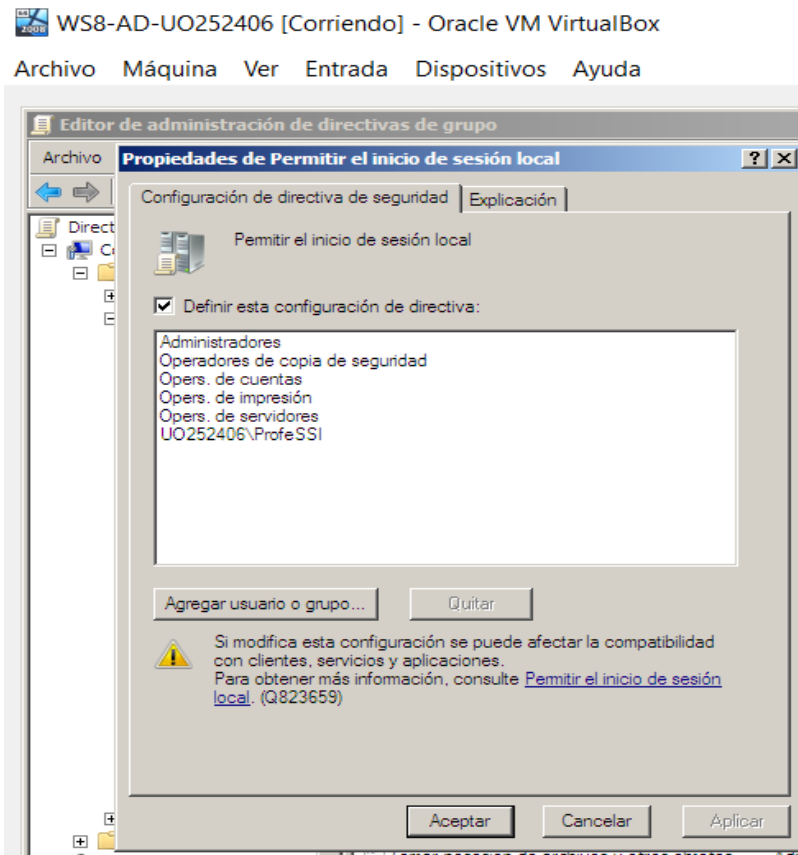
- "Herramientas administrativas – Administración de directivas de grupos – Default Domain Policy".



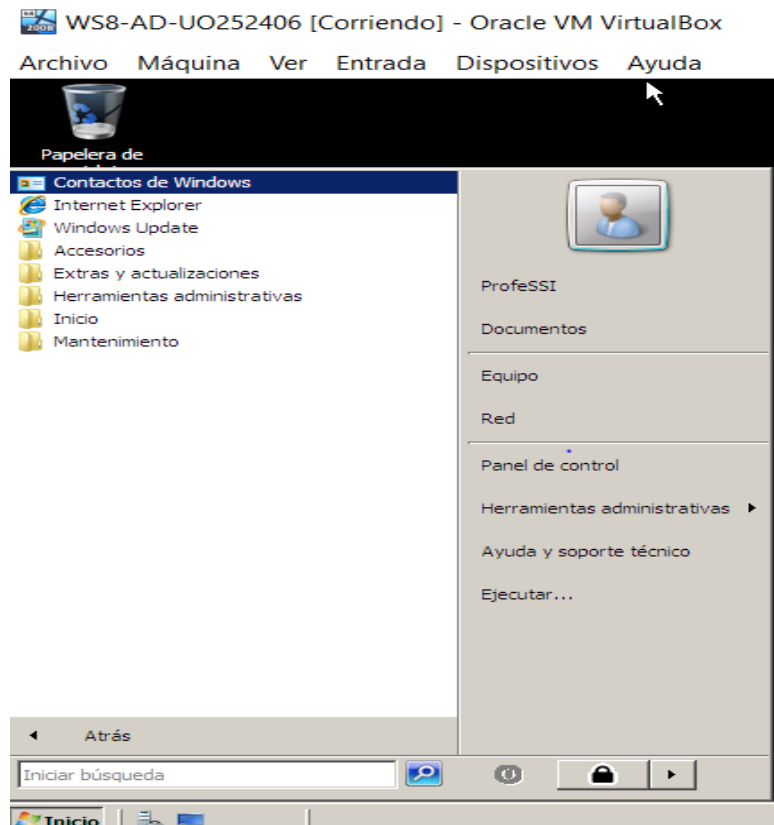
7. Desde el servidor, añade el usuario profeSSI a la lista de usuarios que pueden entrar localmente en el servidor.

- "Herramientas administrativas - Administración de directivas de grupos – Domain Controllers Default Policy - Configuración de seguridad - Directivas locales - Asignación de derechos de usuario".

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

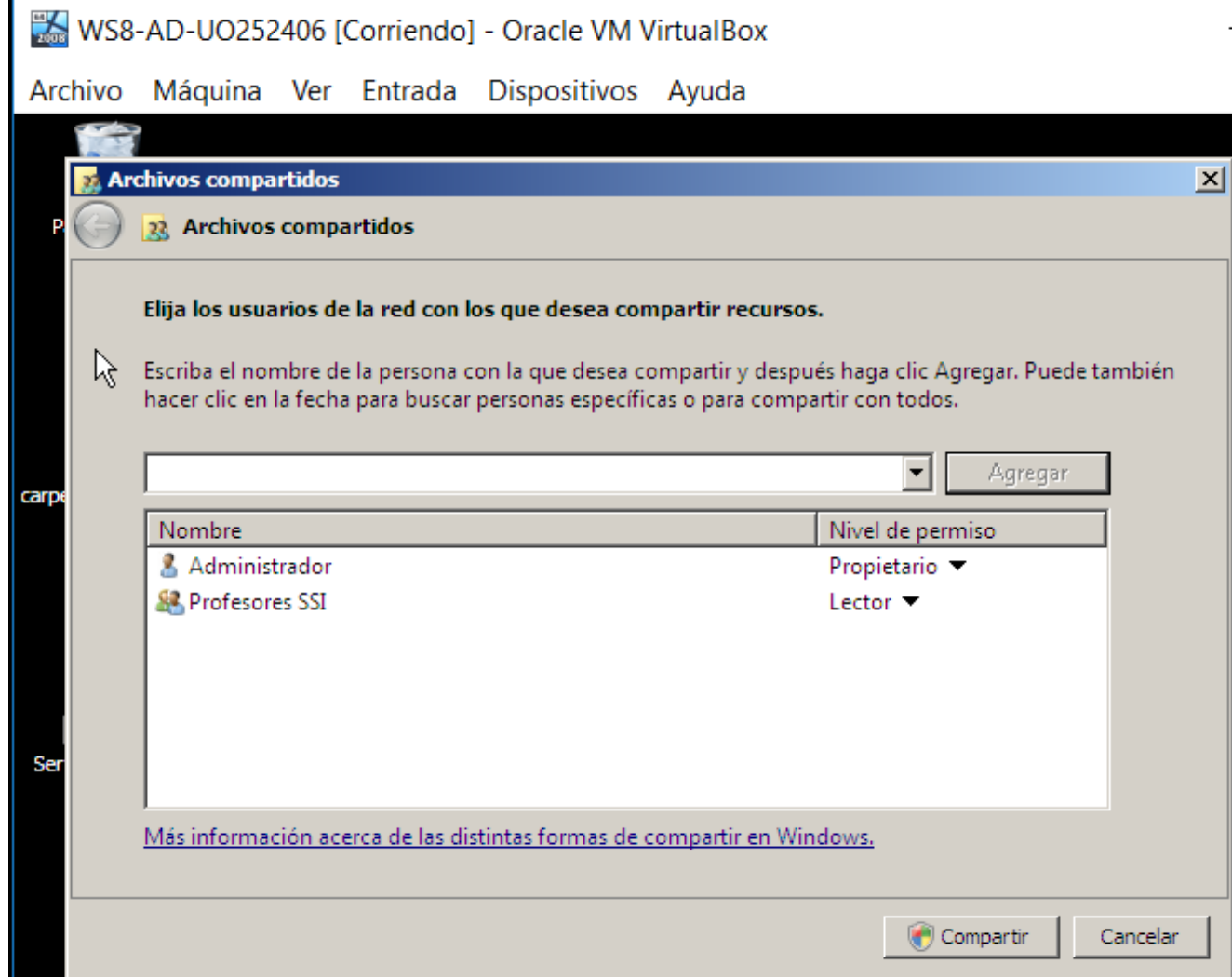


- **Comprueba que el usuario puede iniciar sesión localmente. (Recuerda que se tarda tiempo en actualizar).**



Parte 2: Políticas de Grupo

1. Crea una carpeta compartida en el escritorio del Administrador en el Windows Server 2008. o Con permiso de lectura para los miembros del grupo "Profesores de SSI"

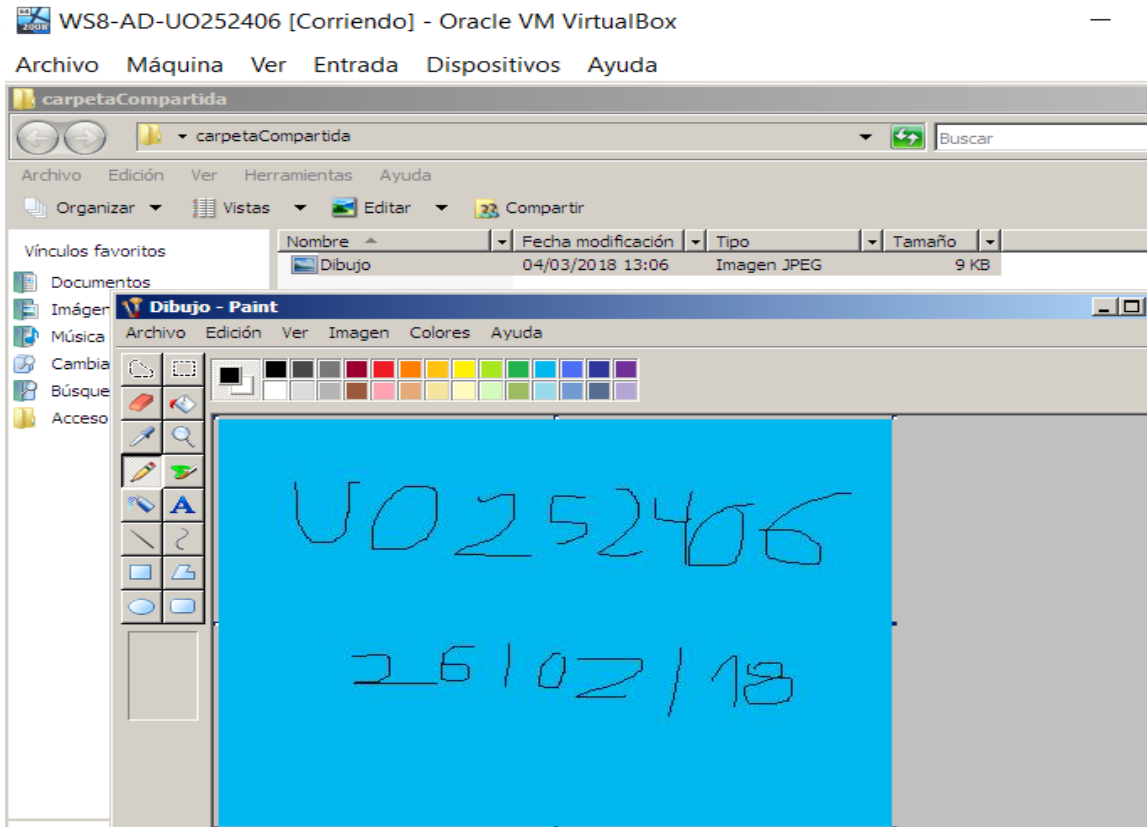


2. Coloca en dicha carpeta un fichero JPG que se utilizará como fondo de escritorio para los miembros del grupo "Profesores de SSI". Esa imagen JPG tiene que ser realizada con el Paint y debe tener dibujado a "mano alzada" tu UOXXXXXXX y la fecha.

Ingeniería Informática del Software – EII

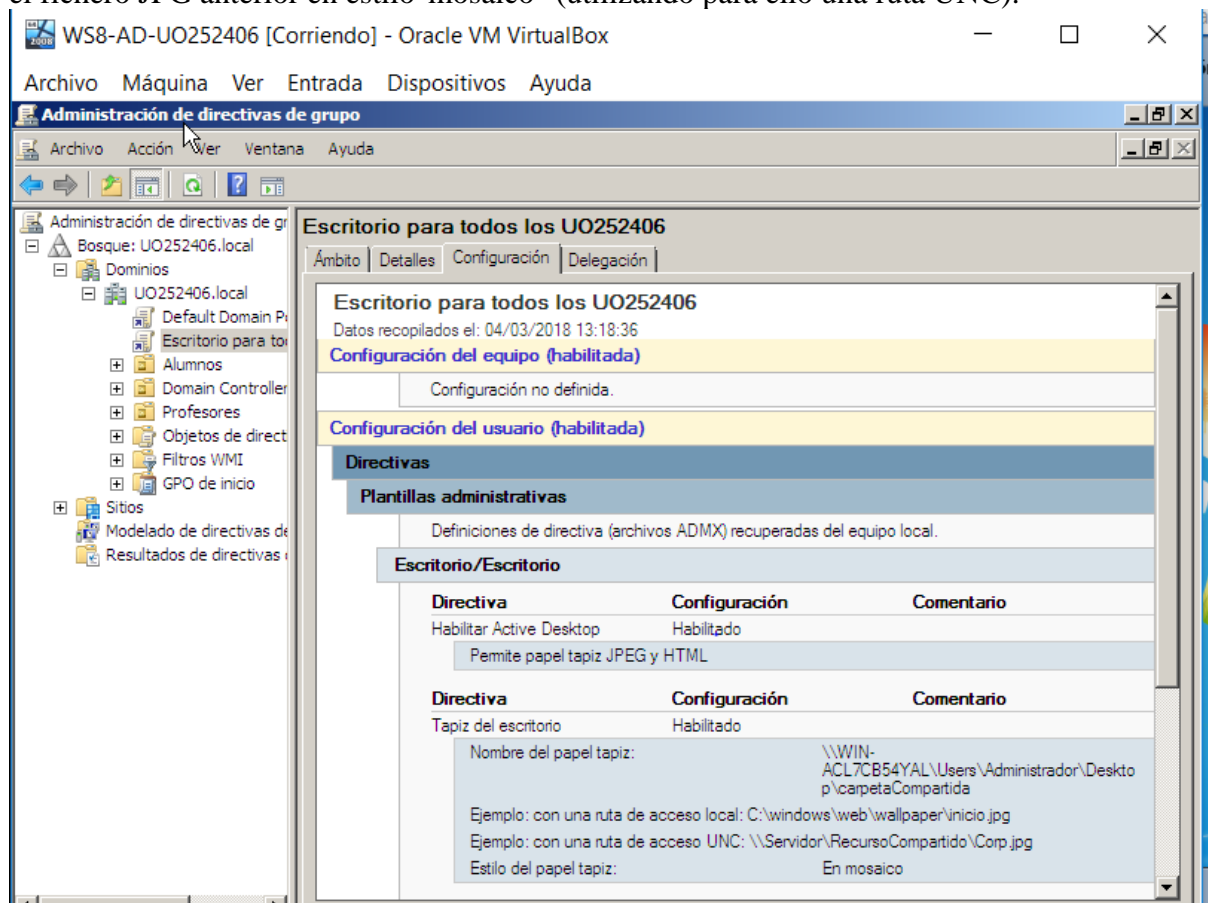
Seguridad de Sistemas informáticos

Seguridad NTFS

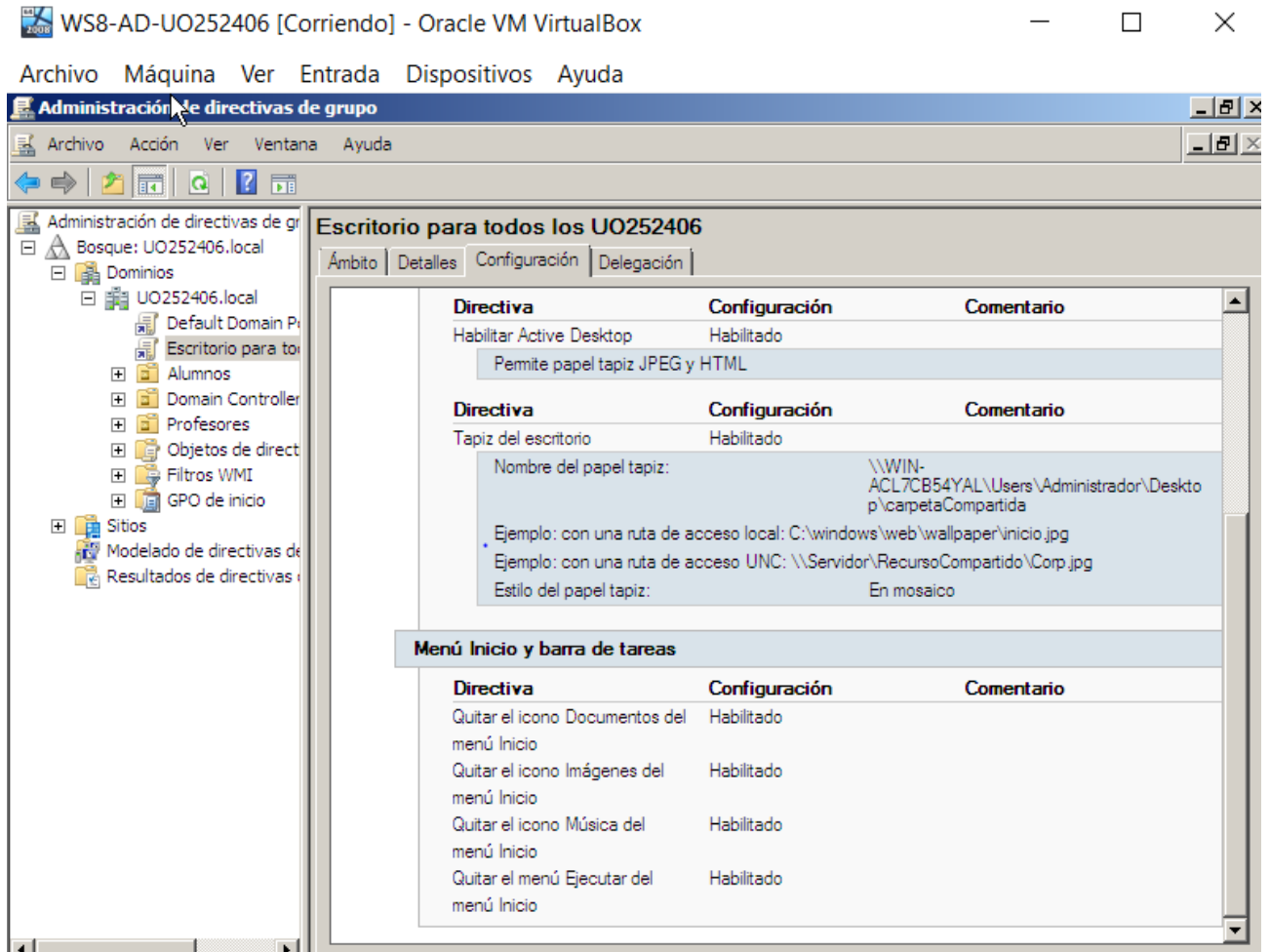


3. Crea una nueva GPO para todo el dominio denominada "Escritorio para todos UOXXX" y edítala de la manera siguiente:

- Habilita el Active Desktop. Además, definir como papel tapiz de Active Desktop utilizando el fichero JPG anterior en estilo "mosaico" (utilizando para ello una ruta UNC).



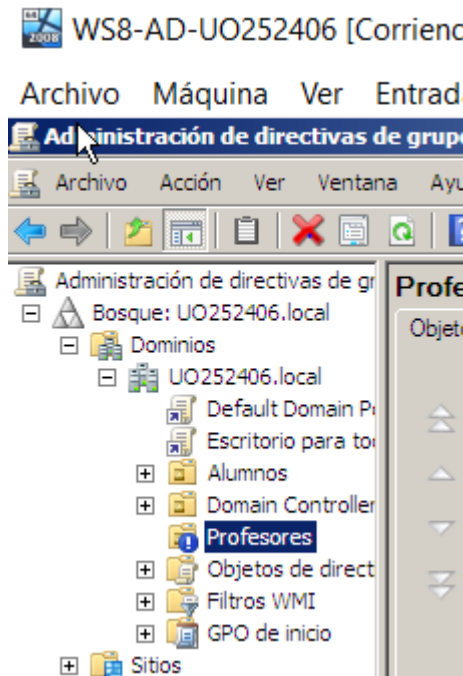
- Quita también del menú inicio:



4. Inicia sesión en W7 como profeSSI y estudia los cambios producidos en el escritorio (mira también sus propiedades) y menú inicio (quizá sea necesario reiniciar). Entra con otro usuario que no tenga permiso sobre la carpeta compartida (p.ej AluSSO) y comenta qué ocurre.

Entrando como profeSSI el escritorio se ve en mosaico con el fondo que hemos creado anteriormente con el paint. En cambio, con AluSSO se ve el de por defecto.

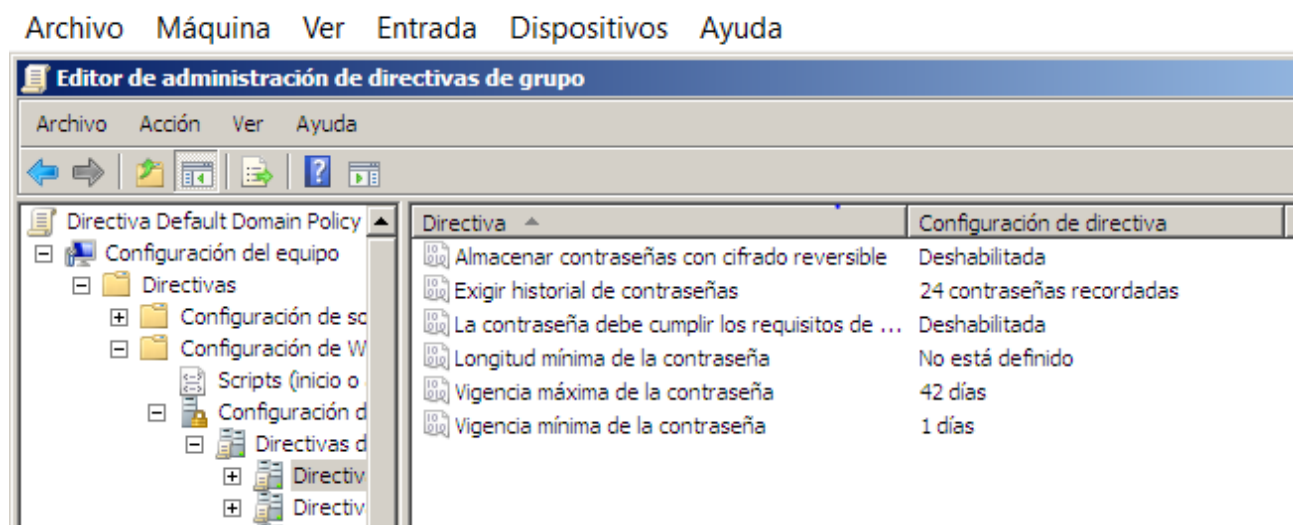
5. Prueba a bloquear la herencia de directivas para la UO "Profesores"



- Inicia de nuevo sesión en W7 como profeSSI y estudia de nuevo los cambios producidos en el escritorio (mira también sus propiedades) y menú inicio (quizá sea necesario reiniciar). El escritorio pasa a estar como estaba ya que los cambios de directivas no se aplican a los profesores.

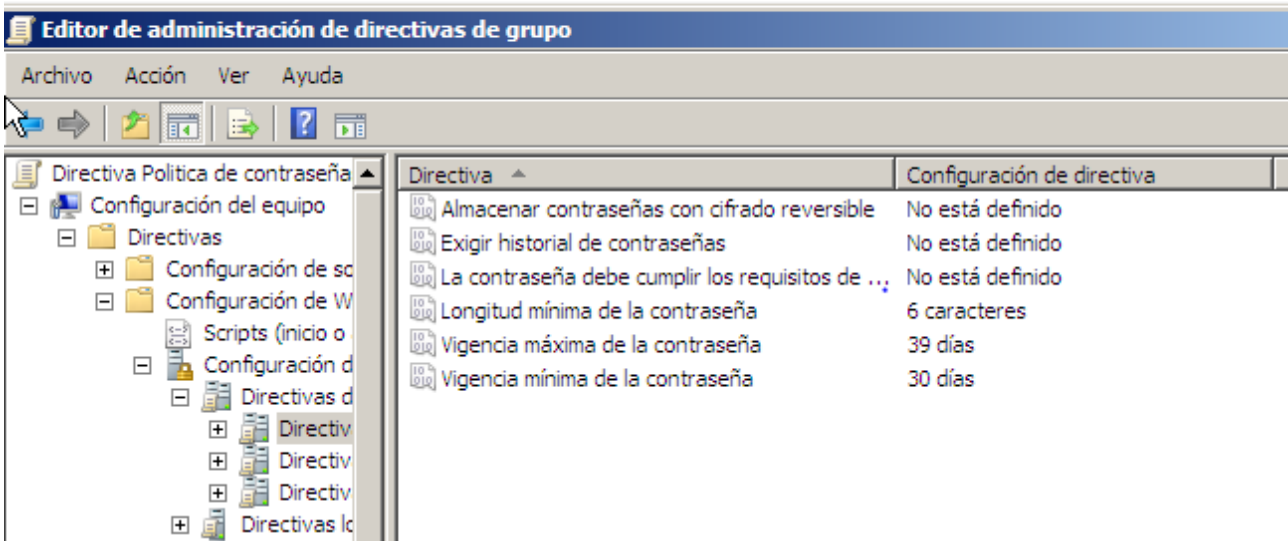
6. Cambia la política de contraseñas. Cámbiala a nivel de dominio (sin cumplir requisitos de seguridad) y a nivel de una de las UO que tengas definidas (haciendo que los cumplan). Prueba a cambiar la contraseña de un usuario de esa UO, poniendo una sencilla. ¿Te deja? ¿Por qué?

WS8-AD-UO252406 [Corriendo] - Oracle VM VirtualBox



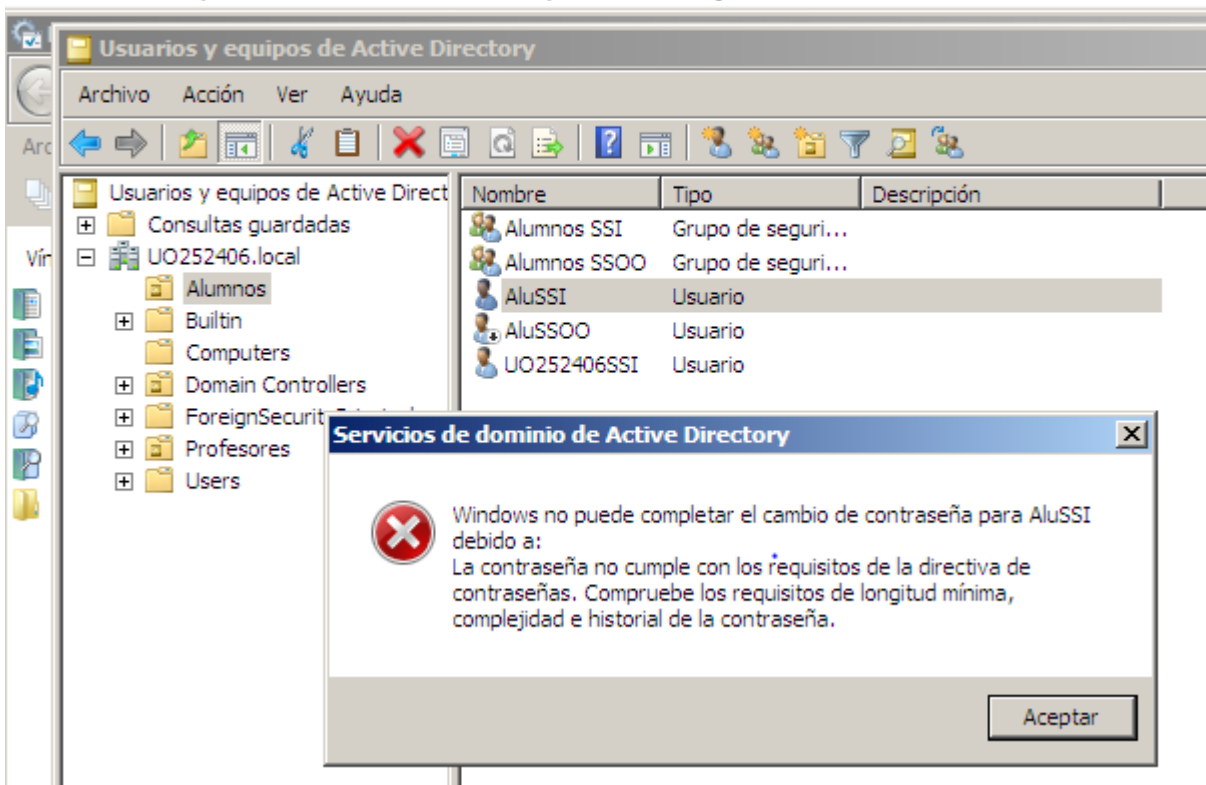
WS8-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda



WS8-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

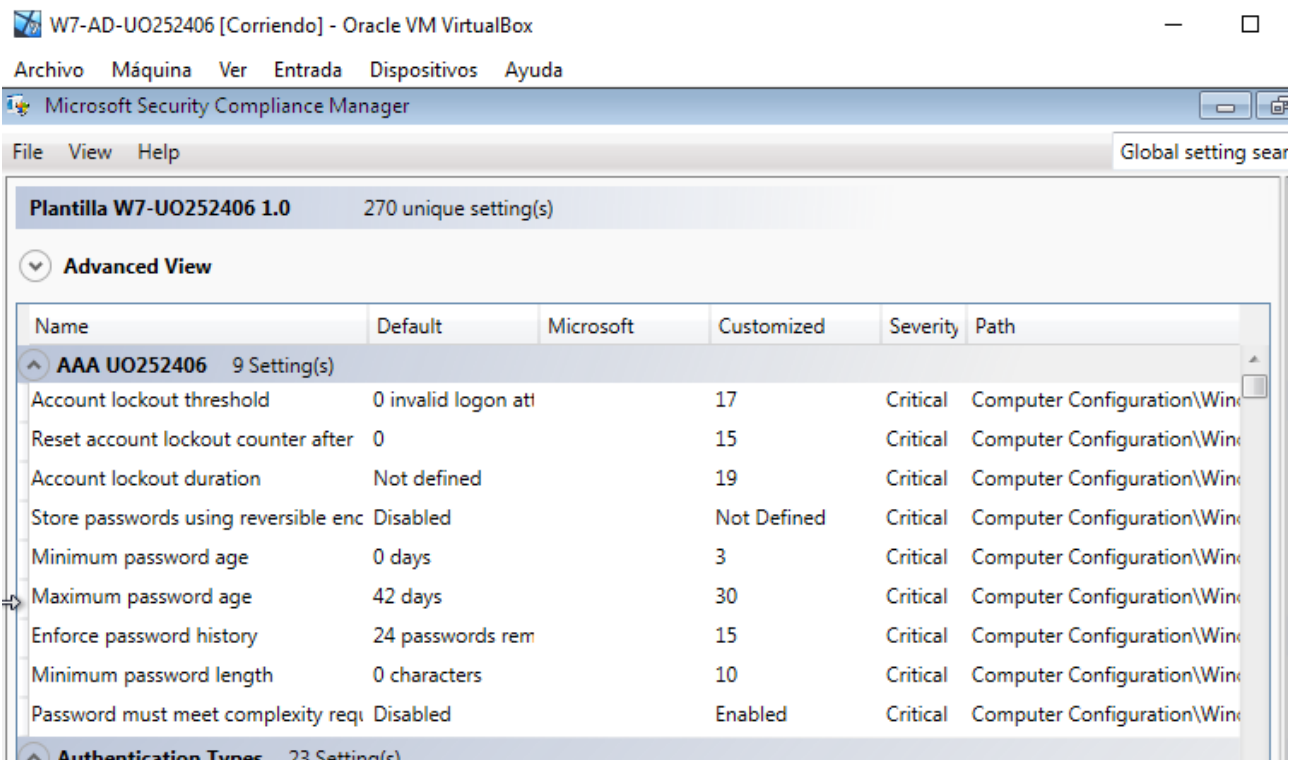


7. Entra en el Microsoft Security Compliance Manager SCM:

- Duplica la plantilla Win7SP1 Computer Security Compliance 1.0, y llámala Plantilla W7-UOXXX (usa tu UO)
- Edita la plantilla para añadir un Group (Setting Group – Add). Llámalo AAA UOXXX
- Edita la plantilla para añadir dentro de ese grupo que has creado settings a nivel de bloqueo de cuenta y política de contraseñas. Setting – Add En el Setting Group selecciona el que has creado. En Choose Settings selecciona

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

- Computer Configuration – Windows Settings – Security Settings – Account Policies – Account Lockout Policy y selecciona los tres y pulsa el botón Add.
- Computer Configuration – Windows Settings – Security Settings – Account Policies – Password Policy y selecciona los seis y pulsa el botón Add.
- Edita las propiedades para que
 - La cuenta se bloquee tras 17 intentos fallidos
 - La cuenta de accesos fallidos se resetee a cero tras 15 minutos
 - El bloqueo de cuenta dure 19 minutos
 - No te deje cambiar contraseñas de menos de 3 días
 - Hay que cambiar la contraseña cada 30 días
 - Recuerde las últimas 15 contraseñas
 - La contraseña debe tener una longitud mínima de 10
 - La contraseña debe cumplir con los requerimientos de complejidad
- Captura pantalla en la que se vea la plantilla, el grupo y las propiedades editadas (es la única pantalla que necesito en este punto)
- Exporta la plantilla como una GPO. Crea para ello una carpeta (por ejemplo, en el escritorio) que se llame como la plantilla y exporta allí.



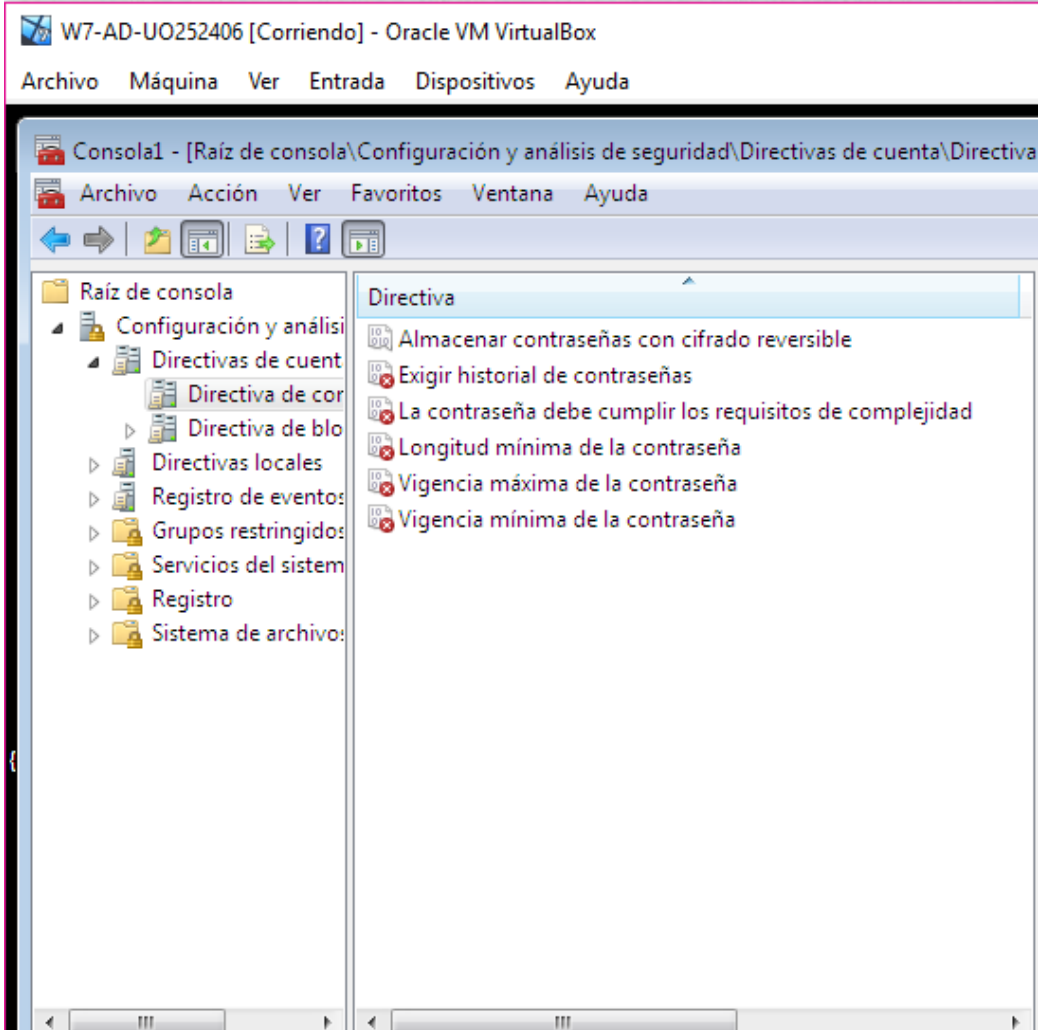
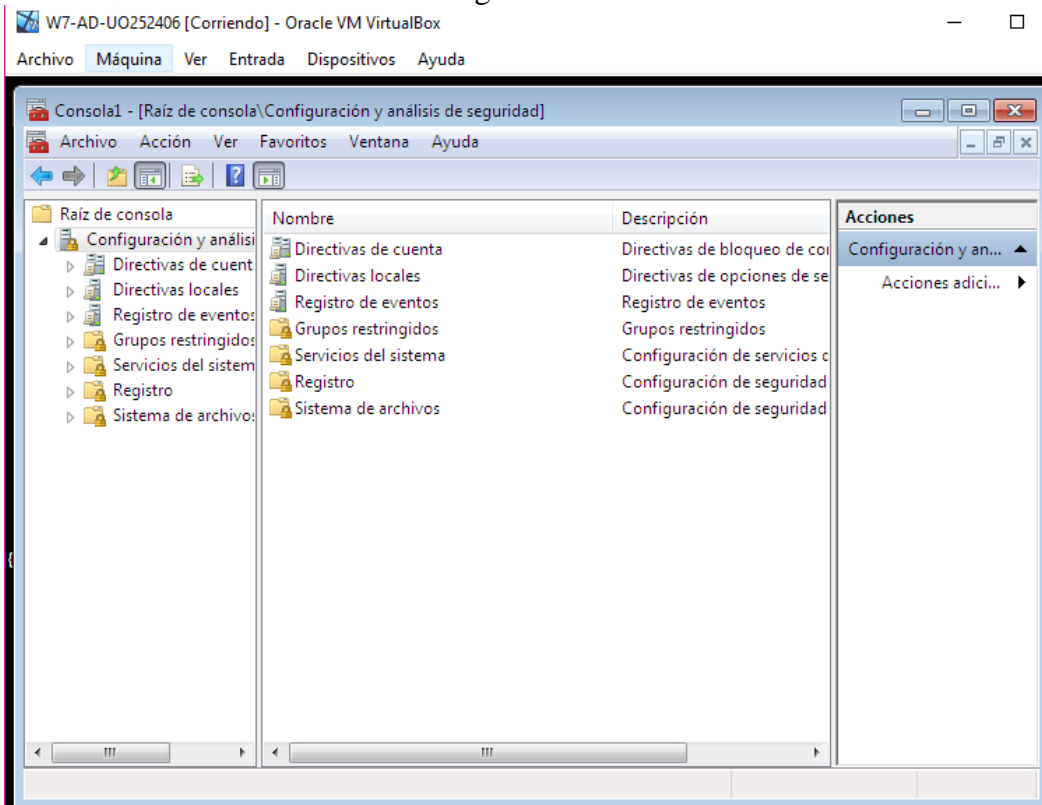
8. Utilizar la plantilla de seguridad creada anteriormente en el equipo local:

- En la máquina W7 (como Administrador) ejecutar mmc; agrega el complemento Configuración y análisis de seguridad.
- Abrir base de datos (dar un nombre para una base de datos nueva) e importar la plantilla creada anteriormente
- Comprobar que se ha importado correctamente (las propiedades que se han definido anteriormente deben reflejarse)
- Analizar el equipo.
- Mostrar mediante una captura que se ha analizado el equipo y habrá directivas de contraseñas o de bloqueo de cuenta que no coincidirán entre la configuración real del equipo y la que tenemos en la plantilla

Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

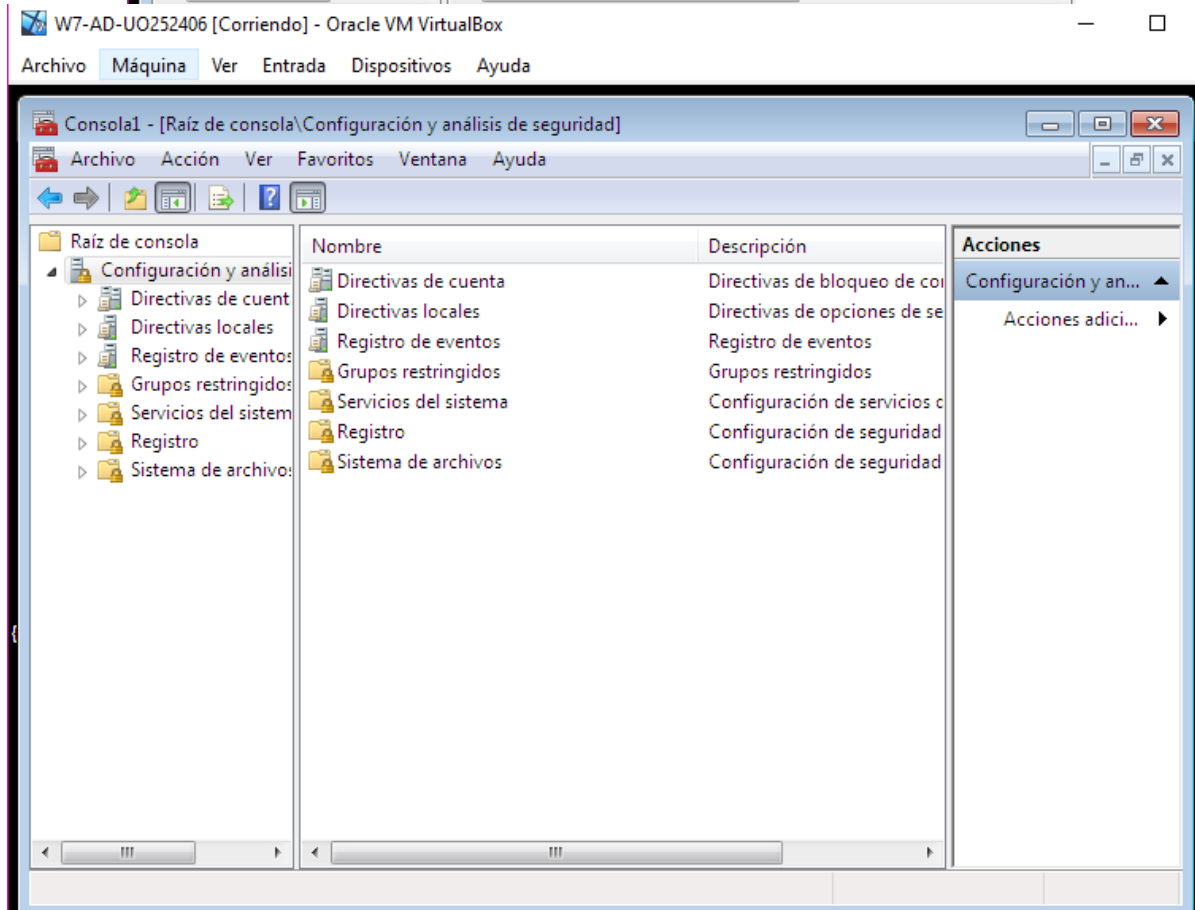
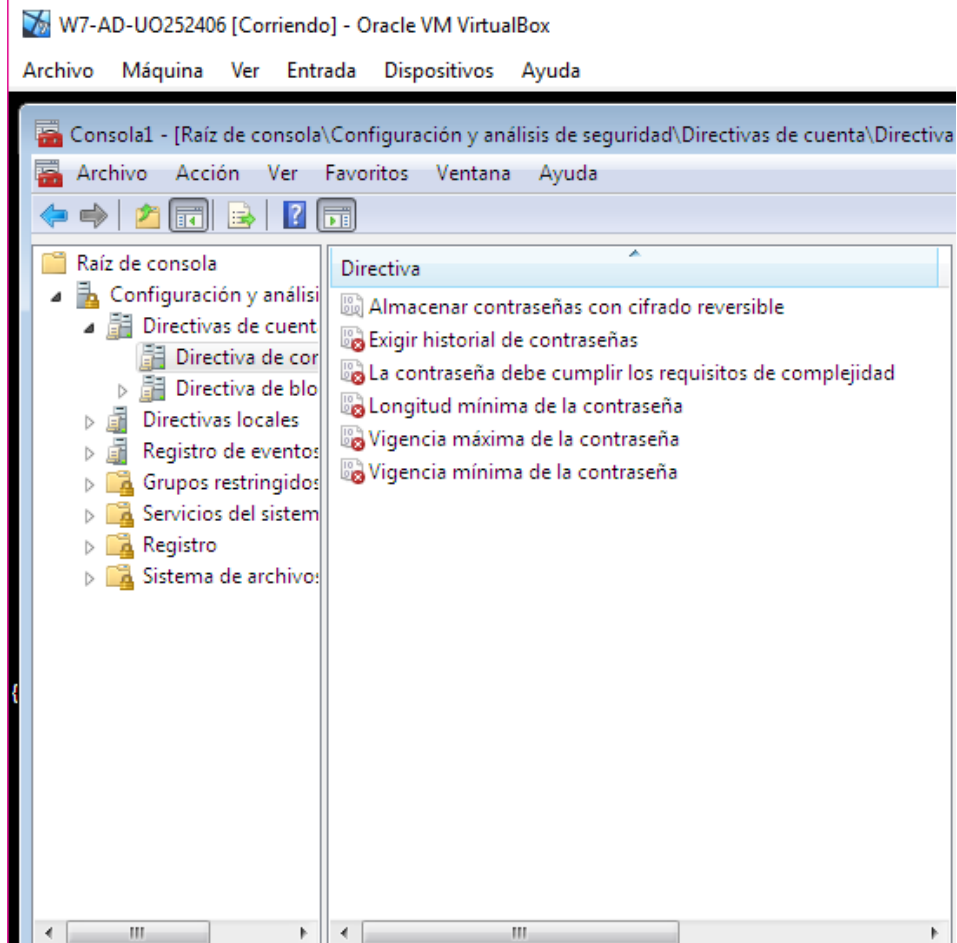
Seguridad NTFS



Ingeniería Informática del Software – EII

Seguridad de Sistemas informáticos

Seguridad NTFS

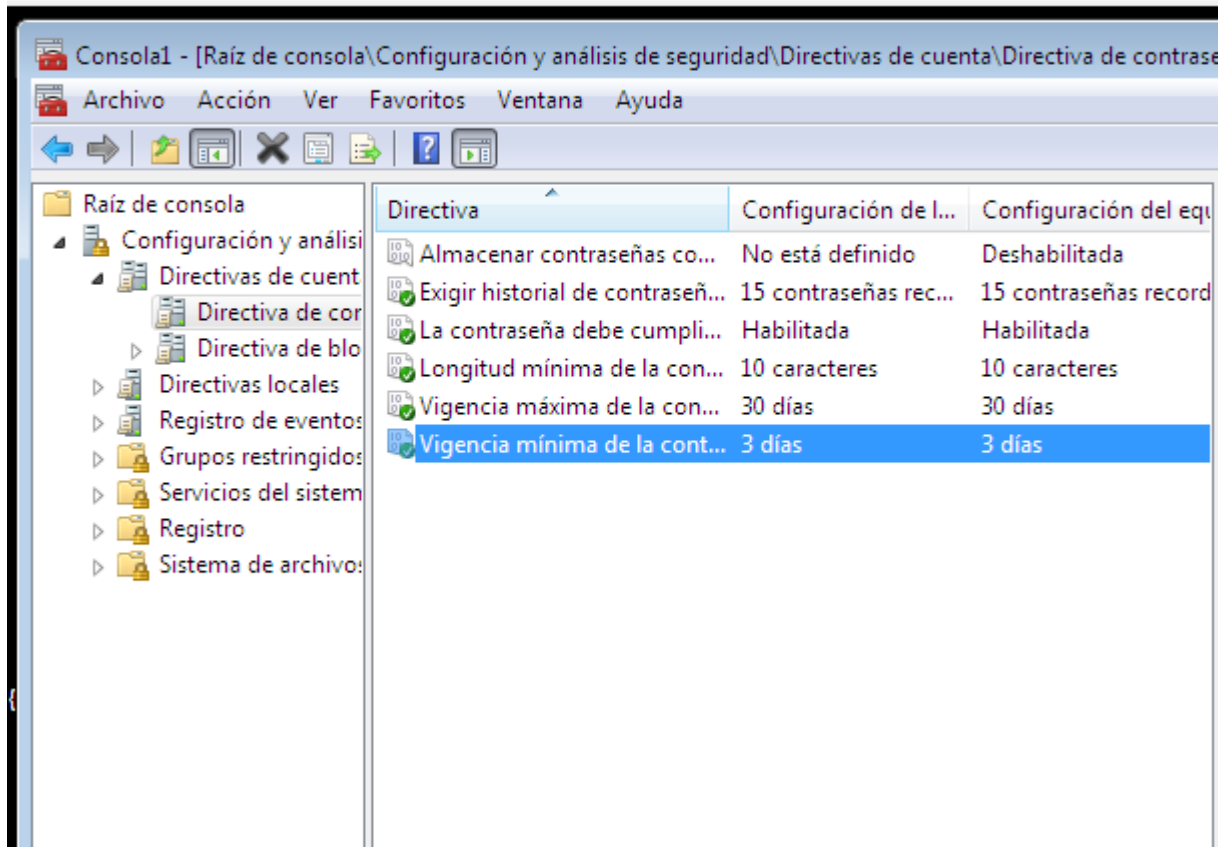


Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Seguridad NTFS

- Configurar equipo (las directivas de la plantilla se aplican al equipo).
- Analizar equipo (para comprobar que las directivas de la plantilla se han aplicado).
- Mostrar mediante una captura que se ha analizado el equipo y ahora sí que coinciden las configuraciones del equipo y la plantilla.

W7-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda



9. Utilizar la plantilla de seguridad creada anteriormente en el dominio:

- En el W7 o en el 2008. Entra en Administración de directivas de grupo.
- Sobre el GPO Default Domain Policy, botón derecho, editar. Configuración de Equipo, Directivas, Configuración de Windows, Configuración de Seguridad, botón derecho, importar directiva: elige la que exportaste anteriormente.
- Comprueba que en directivas de cuentas – Directiva de contraseña y Directiva de bloqueo de cuentas están los valores anteriormente fijados en SCM.

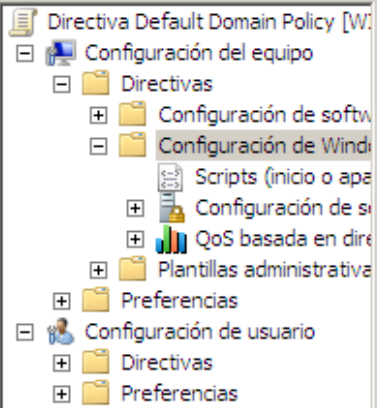
Ingeniería Informática del Software – EII
Seguridad de Sistemas informáticos
Seguridad NTFS

WS8-AD-UO252406 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Editor de administración de directivas de grupo

Archivo Acción Ver Ayuda



Configuración de Windows

Configuración de seguridad

