



SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

Seguridad en Windows: Sistema de archivos NTFS y Directorio Activo



4 DE MARZO DE 2019

VLADISLAV STELMAKH
UO257580 – X8226649D

Índice

Sistema de archivos NTFS	2
Software necesario	2
Preparación del entorno.....	2
Ejercicios.....	7
Parte 1: Exploración de permisos	7
Parte 2: Ejemplos de permisos.....	9
Parte 3: Trabajo con el sistema de ficheros encriptado	14
Parte 4: ¡Al ataque!.....	20
Parte 5: Opciones avanzadas	22
Parte 6: BitLocker	31
Directorio Activo	41
Preparación del entorno.....	41
Seguridad en Active Directory	63
Políticas de grupo.....	77

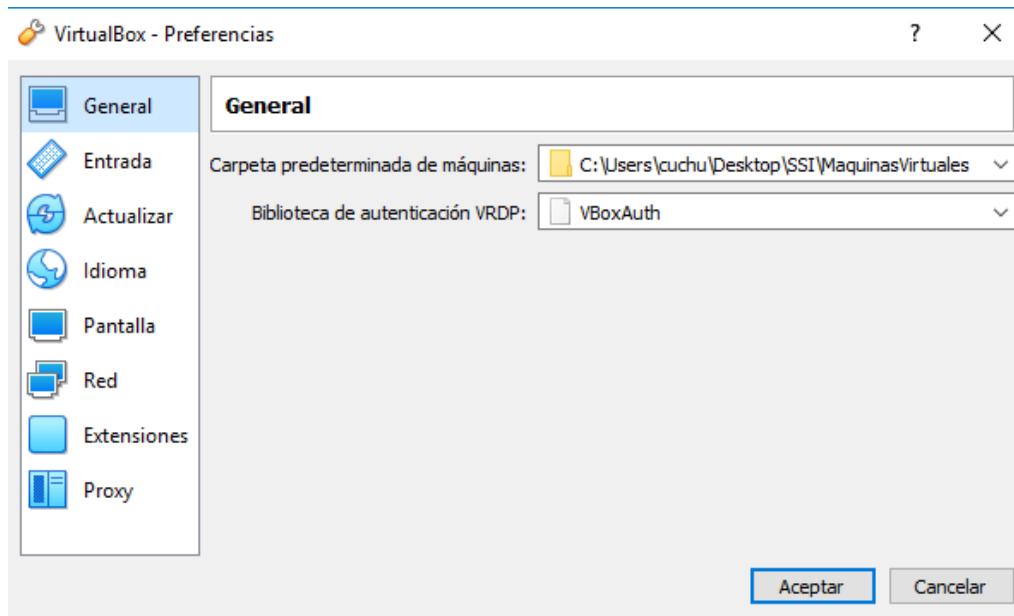
Sistema de archivos NTFS

Software necesario

- Oracle VM VirtualBox
- Máquina virtual Windows 10
- Ubuntu desktop: <http://releases.ubuntu.com/16-04/ubuntu-16.05.5-desktop-i386.iso>

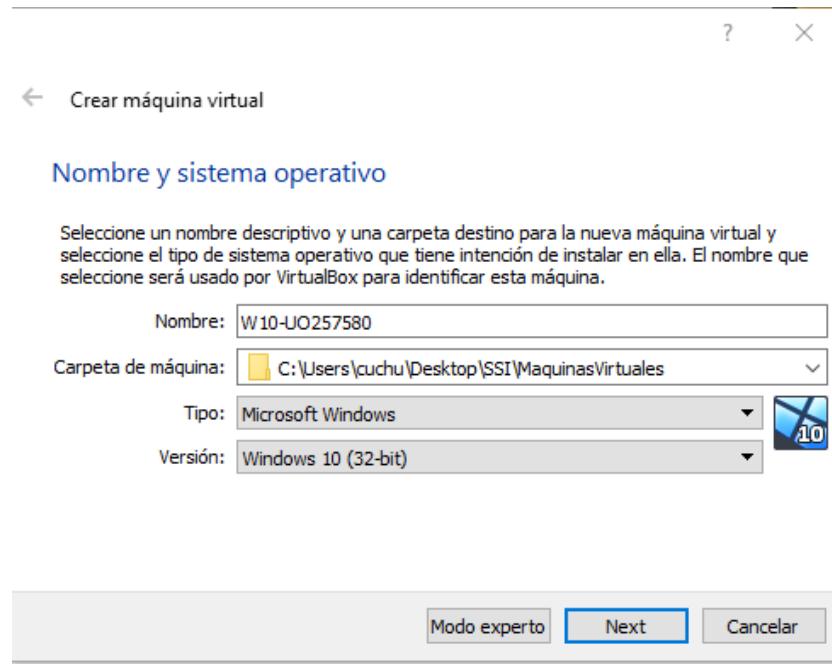
Preparación del entorno

- 1) Arrancamos el equipo en [aulasuo.uniovi.es](#) con la cuenta UO.
- 2) Descargamos la imagen del Windows 10 del campus virtual (Material auxiliar): “Windows 10”.
- 3) Creamos una carpeta que se llame “MaquinasVirtuales” en nuestro directorio: “C:\Usuarios\UOxxxxxx\MaquinasVirtuales”
- 4) Ejecutamos Oracle VM VirtualBox (debería estar en el escritorio). La instalación del VirtualBox está realizada en C: y por tanto la carpeta predeterminada para almacenar las máquinas virtuales es: “C:\ProgramFiles...”. Por cuestiones de organización y de permisos, lo más recomendable es cambiar el directorio: Archivo-General y le especificamos la carpeta “MaquinasVirtuales” creada en el paso anterior.



5) Creamos una nueva máquina virtual en modo Experto:

- a) Nombre: W10-UOxxxxx, donde xxxx es vuestro UO.
- b) Tipo: Microsoft Windows.
- c.) Versión: 32 bits.
- d) Memoria: 1GB.
- e) Disco duro: Usar uno existente y seleccionamos el archivo “W10_RSAT.vmdk” de la carpeta donde hemos descomprimido la imagen descargada del campus.



Nombre y sistema operativo

Seleccione un nombre descriptivo y una carpeta destino para la nueva máquina virtual y seleccione el tipo de sistema operativo que tiene intención de instalar en ella. El nombre que seleccione será usado por VirtualBox para identificar esta máquina.

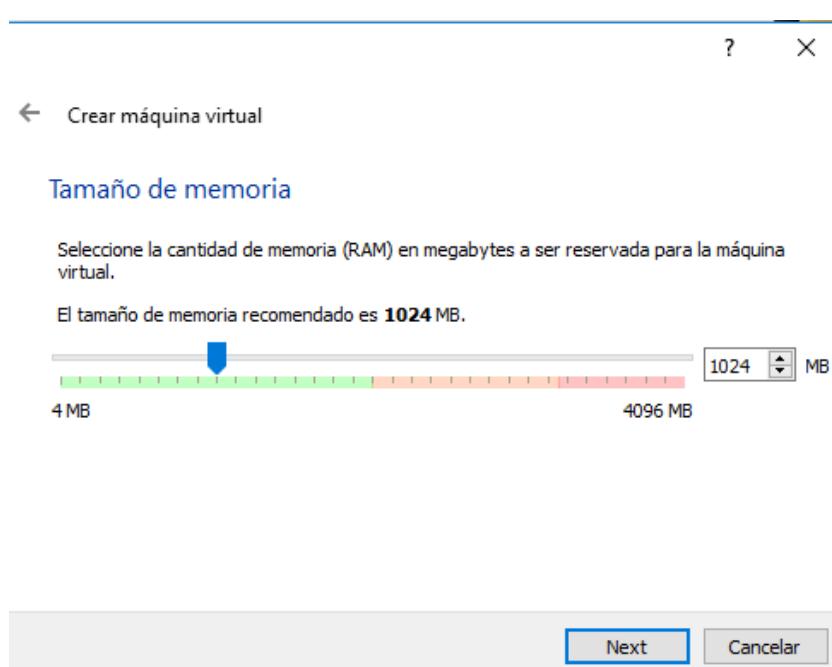
Nombre: W10-UO257580

Carpeta de máquina: C:\Users\cuchu\Desktop\SSI\Maquinas Virtuales

Tipo: Microsoft Windows

versión: Windows 10 (32-bit)

Modo experto Next Cancelar



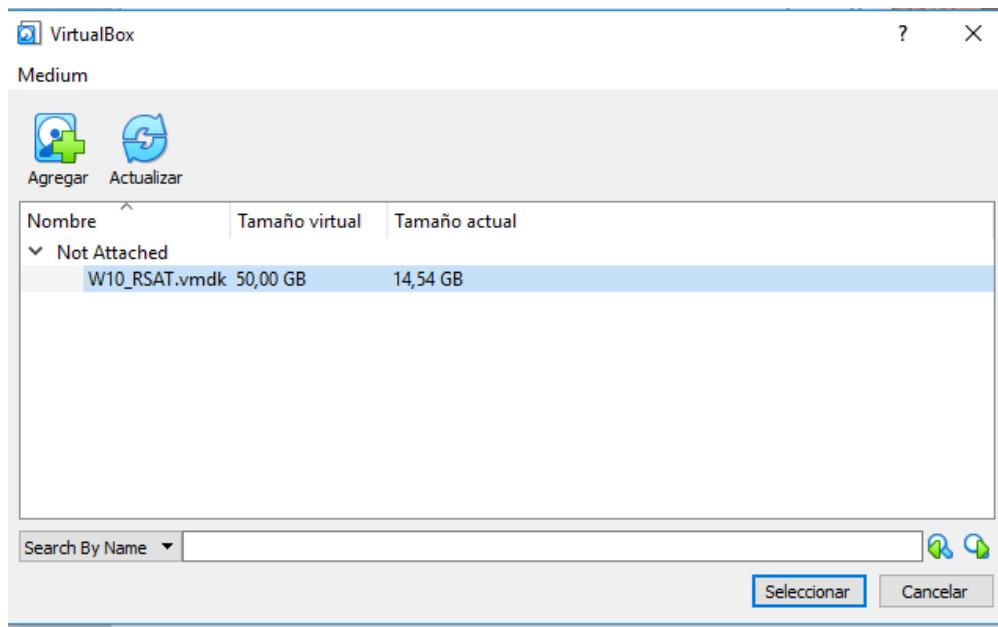
Tamaño de memoria

Seleccione la cantidad de memoria (RAM) en megabytes a ser reservada para la máquina virtual.

El tamaño de memoria recomendado es 1024 MB.

4 MB 1024 MB 4096 MB

Next Cancelar



← Crear máquina virtual

Disco duro

Si desea puede agregar un disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno de la lista o de otra ubicación usando el icono de la carpeta.

. Si necesita una configuración de almacenamiento más compleja puede omitir este paso y hacer los cambios a las preferencias de la máquina virtual una vez creada.

El tamaño recomendado del disco duro es **50,00 GB**.

- No agregar un disco duro virtual
- Crear un disco duro virtual ahora
- Usar un archivo de disco duro virtual existente

W10_RSAT.vmdk (Normal, 50,00 GB)



Crear

Cancelar

- 6) Arrancamos la máquina. Lo primero que notamos al arrancar es que entra en sesión directamente con la cuenta “ssiuniovi” que tiene privilegios de administración y no tiene contraseña, pon una contraseña que puedas recordar. Cambia el nombre del equipo a W10-UOxxxxx (vuestro UO). Reinicia el equipo.

- 7) Con objeto de homogeneizar, se trabajará con un conjunto de usuarios y grupos común a todos los alumnos. Se deben crear los siguientes grupos de usuarios (Panel de Control-Sistema y SeguridadHerramientas administrativas-Administración de equipos-Herramientas del sistema-Usuarios y grupos locales-Grupos-Acción-Grupo Nuevo):

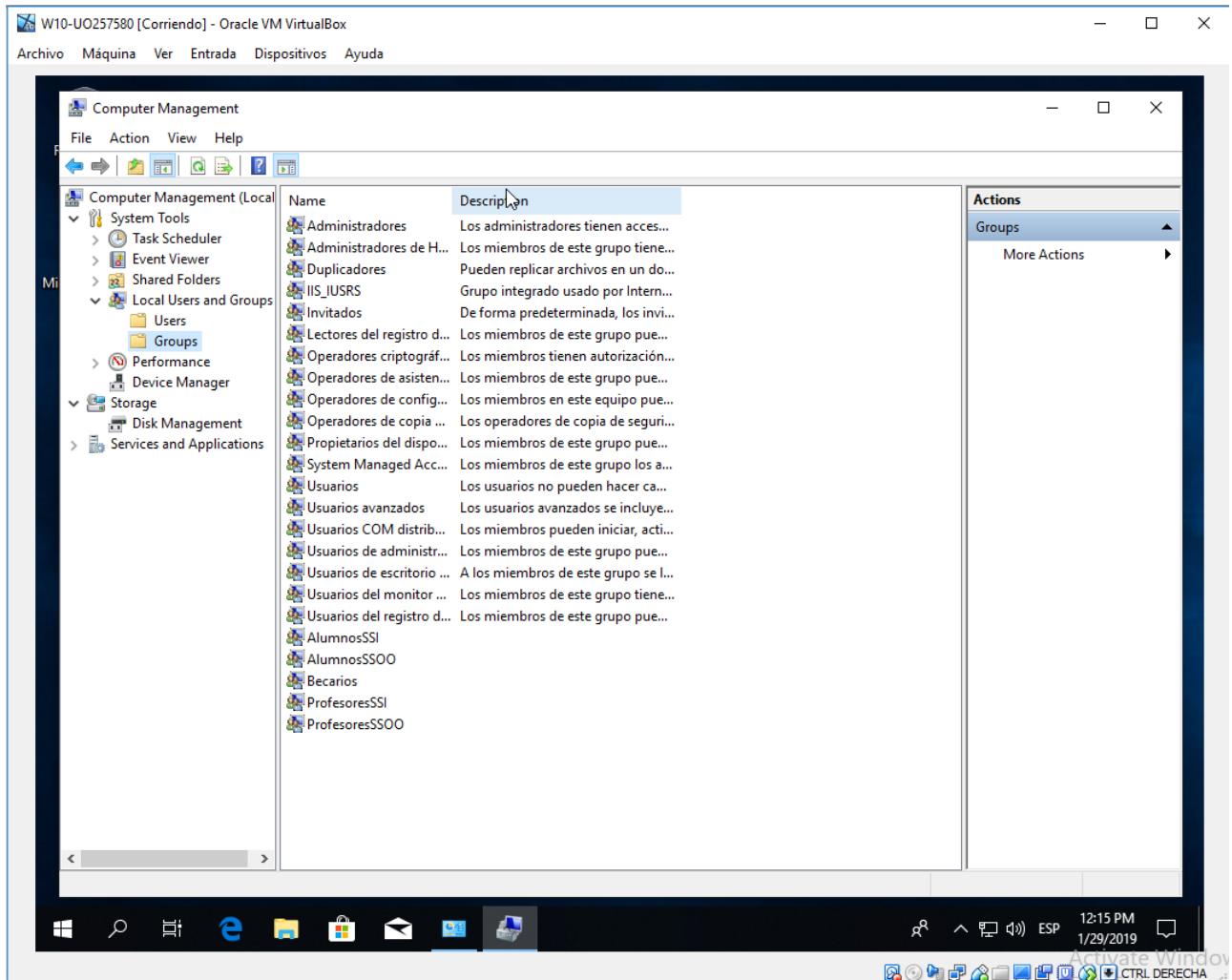
7.1) ProfesoresSSI

7.2) ProfesoresSSOO

7.3) AlumnosSSI

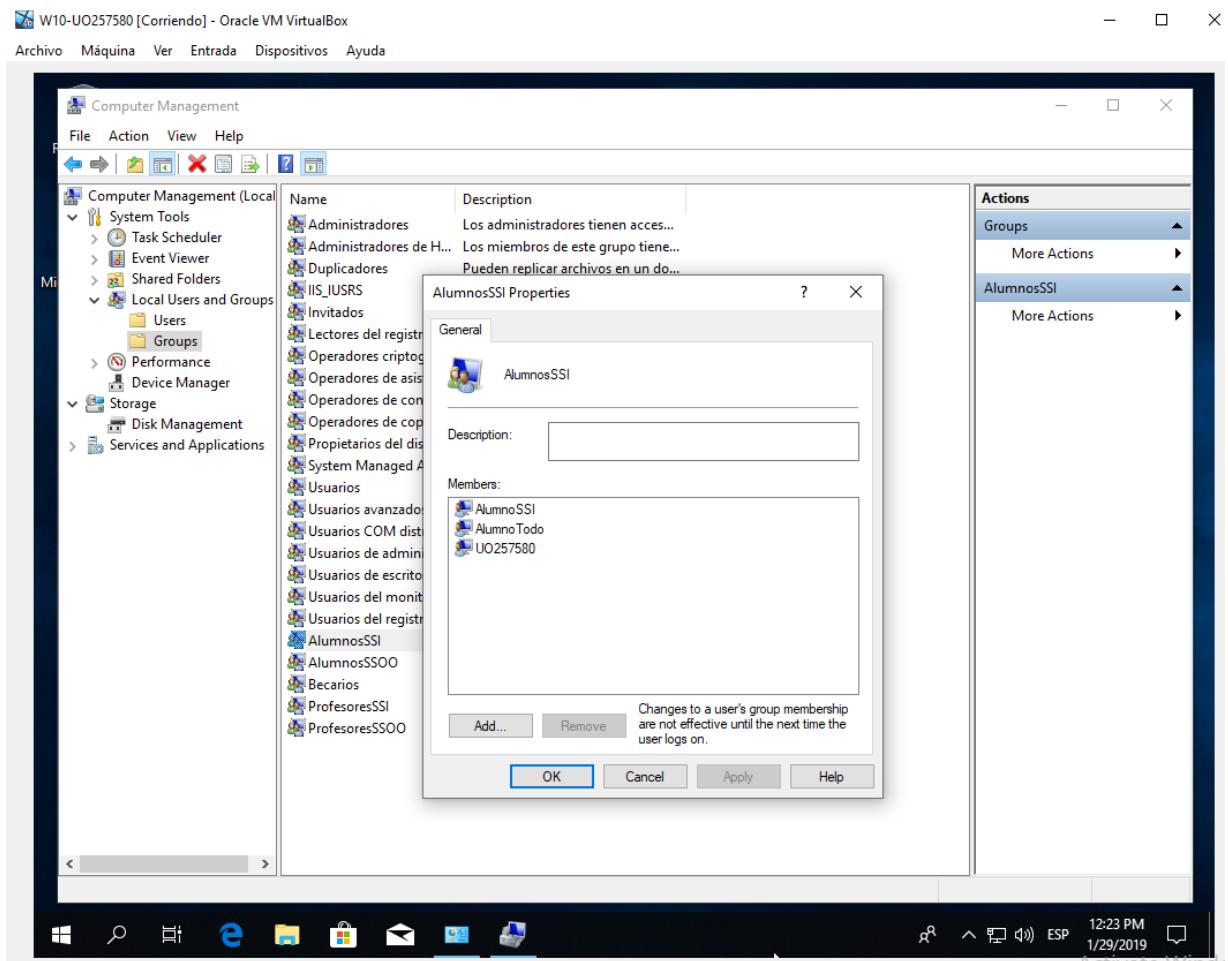
7.4) AlumnosSSI

7.5) Becarios



- 8) Se deben crear los siguientes usuarios (entre paréntesis se indican los grupos a los que pertenecen). Poned contraseñas sencillas, y que no deban cambiarla en el siguiente inicio de sesión. Crear primero los usuarios y después asociarlos a los grupos correspondientes:

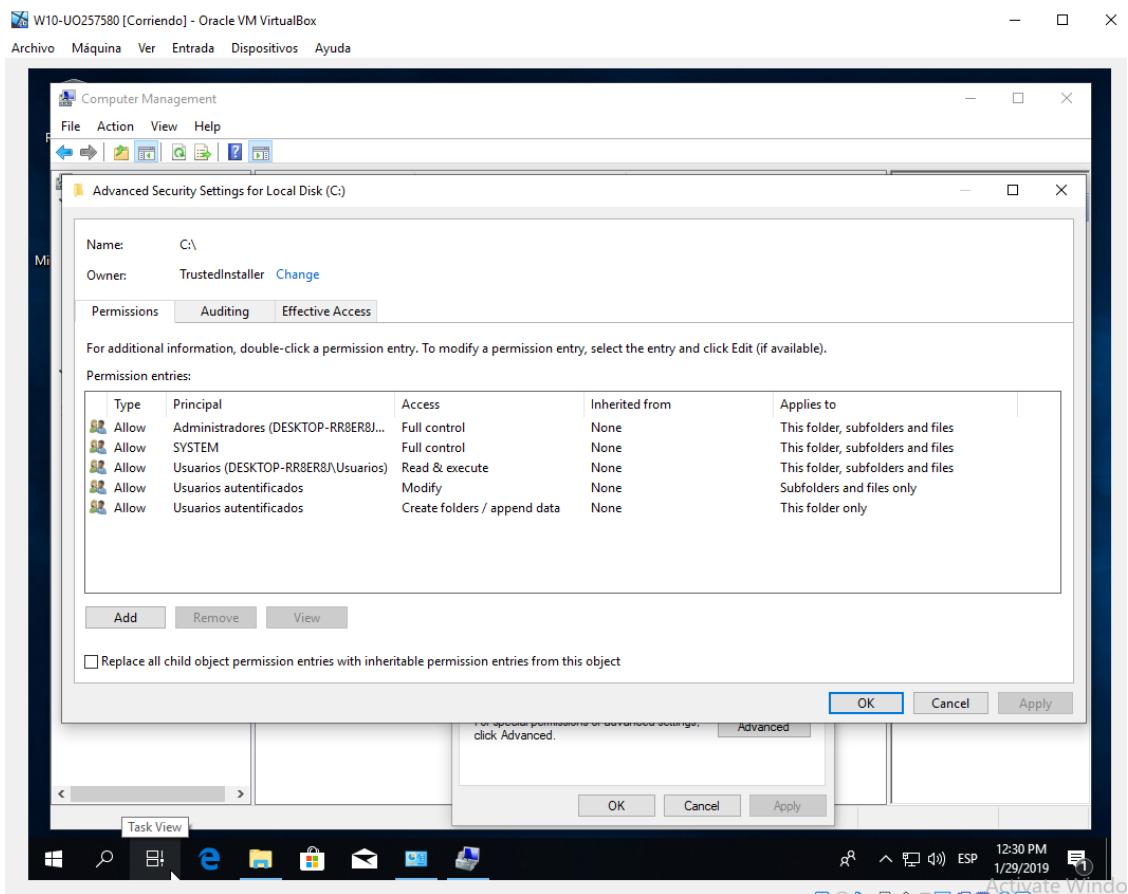
- 8.1) ProfesorSSI (ProfesoresSSI)
- 8.2) ProfesorSSOO (ProfesoresSSOO)
- 8.3) ProfesorTodo (ProfesoresSSI; ProfesoresSSOO)
- 8.4) AlumnoSSI (AlumnosSSI)
- 8.5) AlumnoSSOO (AlumnosSSOO)
- 8.6) AlumnoTodo (AlumnosSSI;AlumnosSSOO)
- 8.7) Becario (Becarios)
- 8.8) UOXXXX (AlumnosSSI), siendo UOXXXX tu UO.



Ejercicios

Parte 1: Exploración de permisos

1) Consulta los permisos asociados a ficheros y a otros objetos como los elementos del registro (se accede mediante regedit.exe), etc. ¿Qué permisos tienen? ¿Qué significan? Explica alguno.

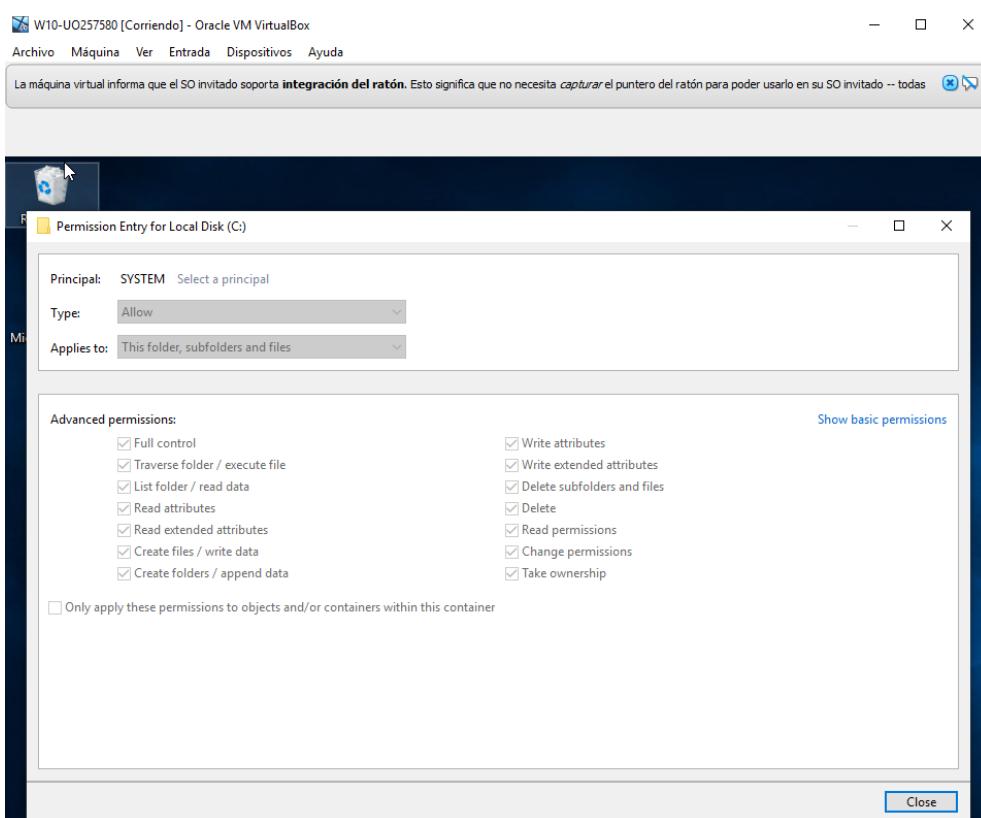
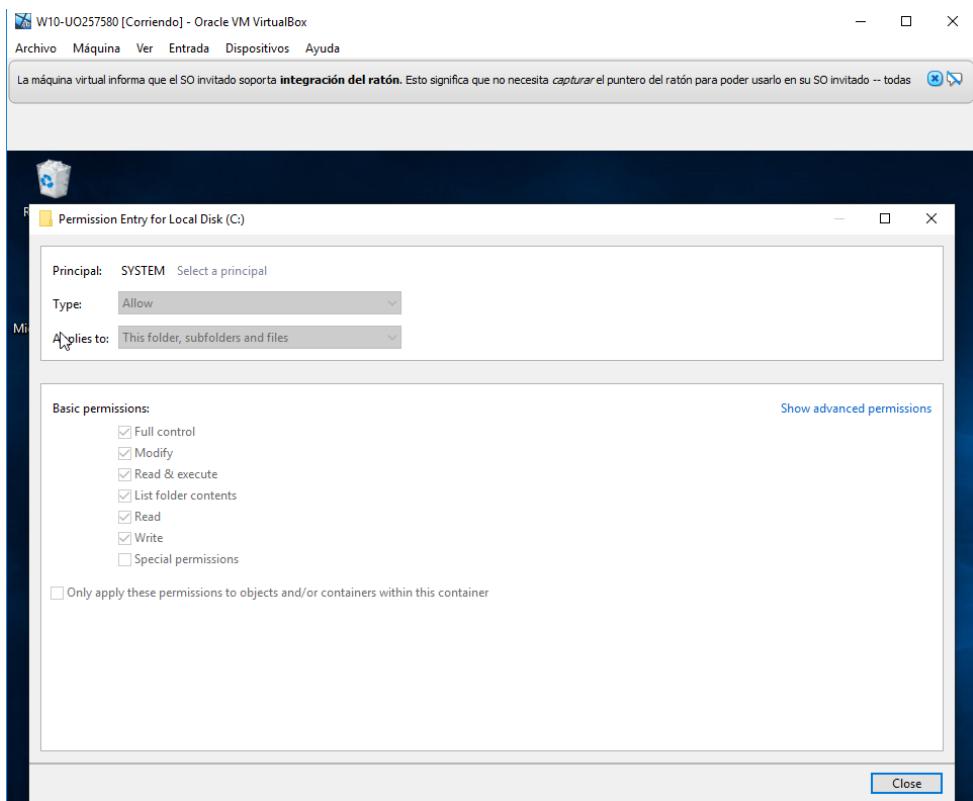


- **Full Control (Acceso Total):** Permite “lectura de ficheros”, “escritura de ficheros”, “lectura y ejecución de ficheros”, “modificación de ficheros” y “cambiar la propiedad del fichero”.
- **Read & Execute (Lectura y Ejecución):** Permite leer y ejecutar un fichero.
- **Modify (Modificar):** Permite, leer, escribir, modificar y borrar un fichero.
- **Create Folders/Append Data:** Permite crear carpetas y almacenar información.

2) Consulta las opciones de Heredar y Propagar en la ficha de avanzadas. Mira en el directorio raíz, en un directorio cualquiera y en un fichero cualquiera. ¿Qué opciones aparecen? ¿Por qué? ¿Cuáles son los propietarios?

En esta misma imagen podemos ver las propiedades “heredar” y “propagar”. En nuestro caso podemos observar que nadie hereda de nadie, pero si propagan a diferentes carpetas, subcarpetas, archivos... Dependiendo del directorio o fichero en el que nos encontramos, los diferentes usuarios tendrán o no tendrán una serie de permisos, dependiendo del grado de “privilegios” que se les conceda. Entre los usuarios que aparecen, podemos ver; el de sistema, nuestro propio usuario, administrador...

3) 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.



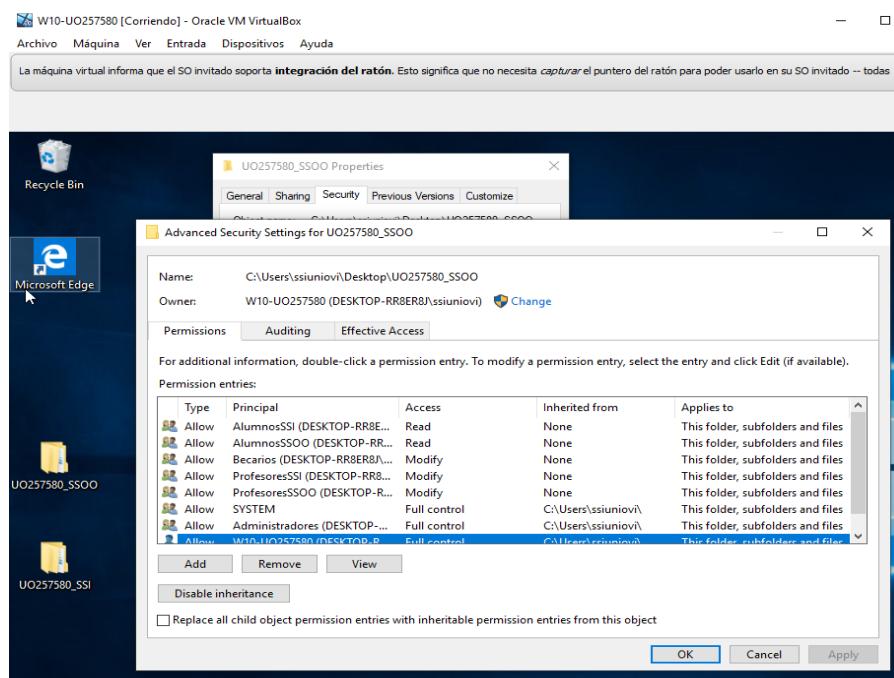
Podemos observar que en la vista avanzada disponemos de muchos más permisos que en la vista estándar. De hecho, también podemos ver como algunos permisos básicos “se transforman” en permisos “con más poder”.

- **Traverse folder/execute file:** navegar por una carpeta y ejecutar un archivo.
- **List folder/read data:** listar una carpeta y leer información.
- **Read attributes:** leer atributos.
- **Read extended attributes:** leer atributos extendidos.
- **Create files/write data:** crear archivos y escribir información.
- **Create folder/append data:** crear carpetas y almacenar información.
- **Write attributes:** escribir atributos.
- **Write extended attributes:** escribir atributos extendidos.
- **Delete subfolders and files:** borrar subcarpetas y archivos.
- **Delete:** borrar
- **Read permissions:** permisos de lectura.
- **Change permissions:** permisos de modificación.
- **Take ownership:** “tomar propiedad”.

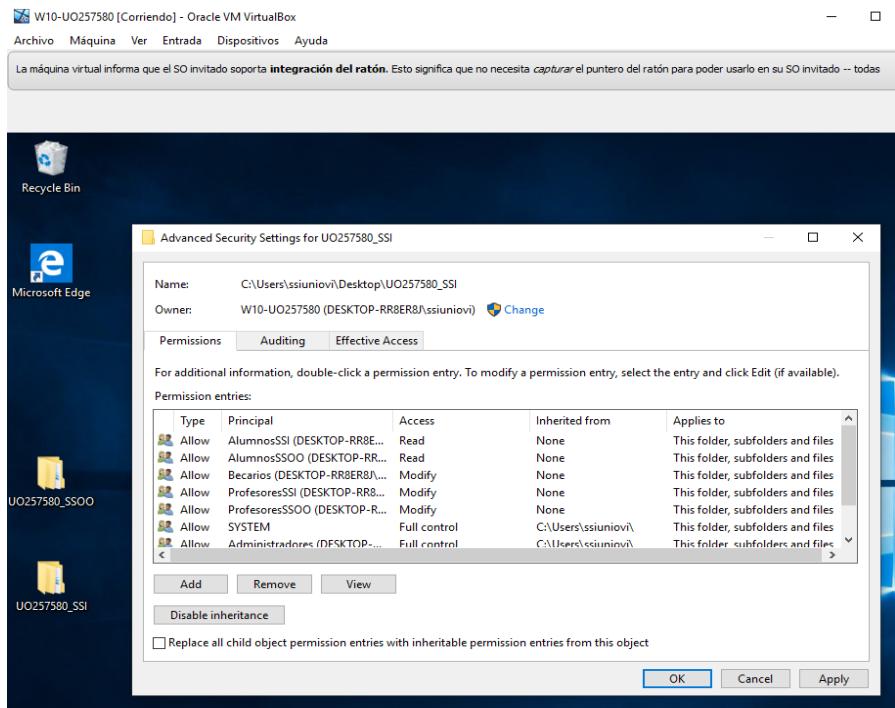
Es aquí, en la vista avanzada, dónde podemos observar como los permisos de Modificar y Control Total se “desglosan” en diversos permisos.

Parte 2: Ejemplos de permisos

- 1) Crea una carpeta para la asignatura de SSI (UO257580_SSI) y otra para la de SSOO (UO257580_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.



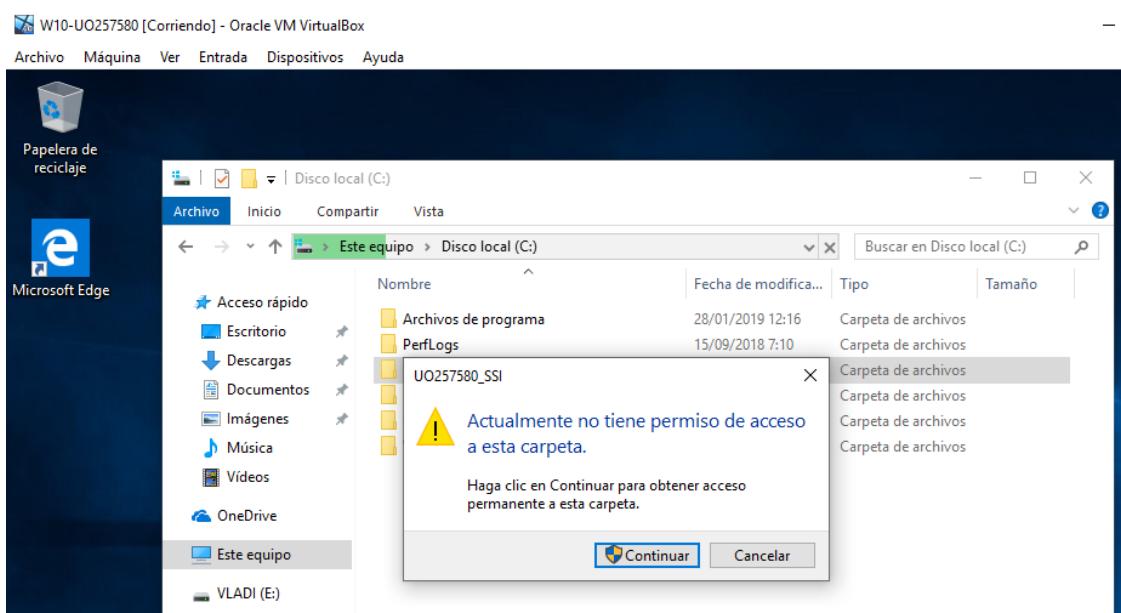
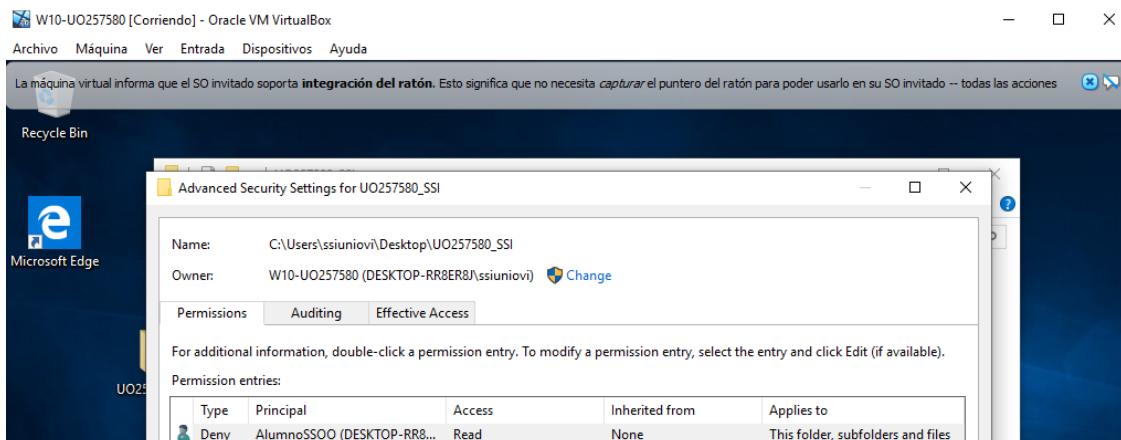
Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS



- 2) 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.

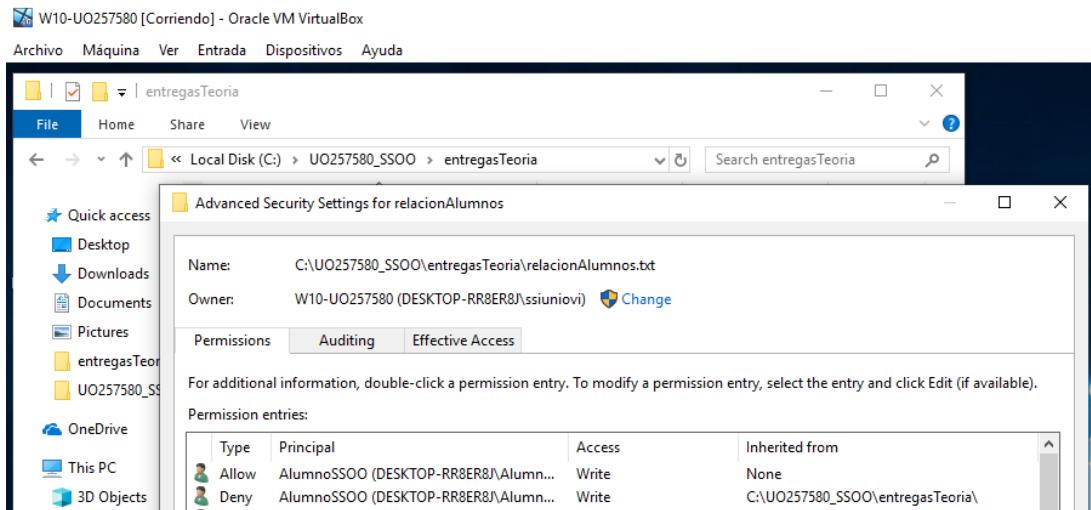
Type	Principal	Access	Inherited from	Applies to
Allow	AlumnosSSI (DESKTOP-RR8E...)	Create files / write data	None	This folder, subfolders and files
Allow	AlumnosSSOO (DESKTOP-RR...)	Create files / write data	None	This folder, subfolders and files
Allow	SYSTEM	Create files / write data	None	This folder, subfolders and files

- 3) Niega el acceso al directorio de una asignatura a los alumnos de la otra. Inicia sesión con AlumnoSSOO y explica lo que pasa.



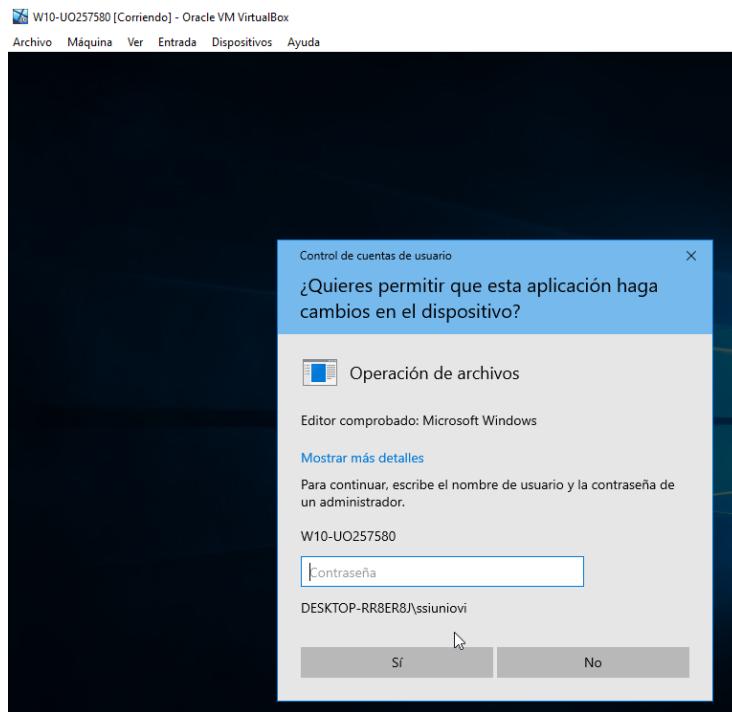
Como hemos denegado el permiso de lectura de la carpeta UO257580_SSI al AlumnoSSOO, este ahora no tiene permisos para abrirla ni leer el contenido que está dentro.

- 4) 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.



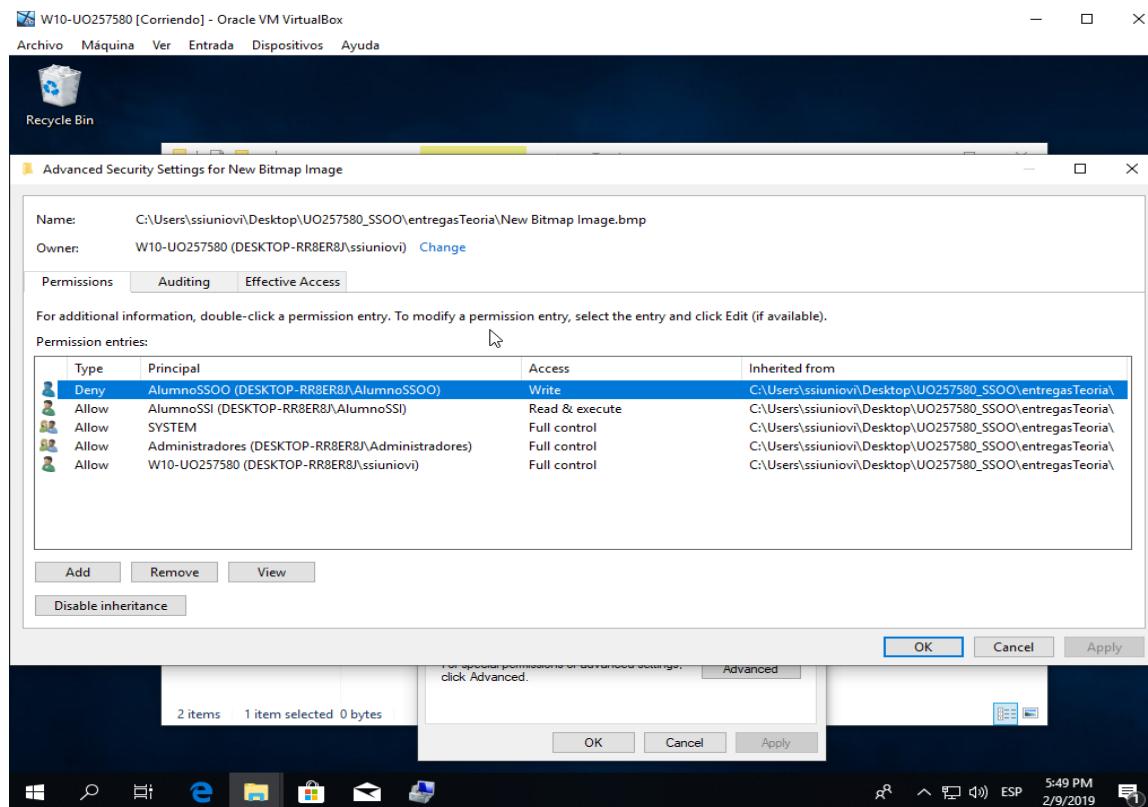
Al final, el alumno de SSOO tiene permisos de lectura y escritura (en el fichero relacionAlumnos.txt), pero no tiene permisos para crear un nuevo fichero en la carpeta.

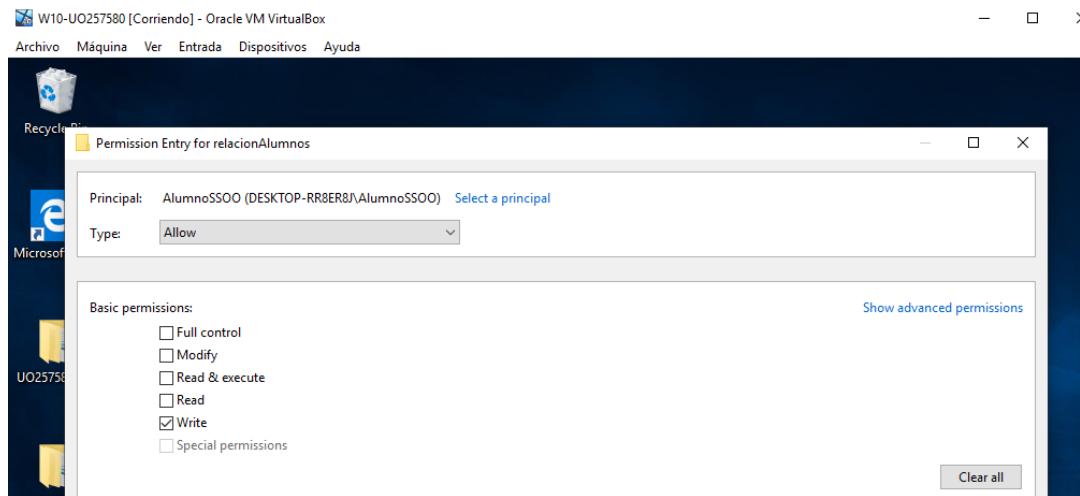




El alumno no puede crear ningún fichero en dicha carpeta ya que no tiene los permisos necesarios para ello.

La regla que se aplica es la más restrictiva (referente a un/a mism@ archivo/carpeta).

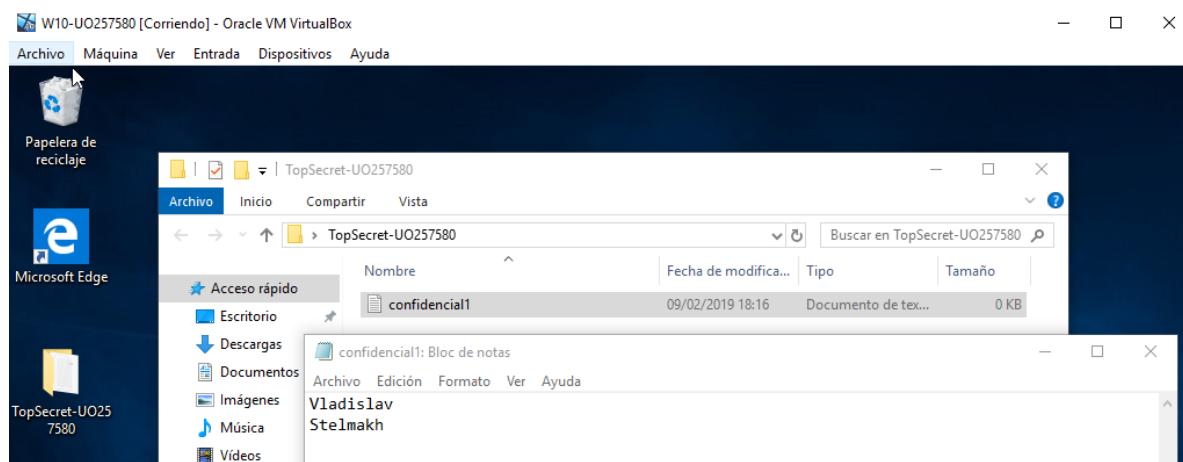
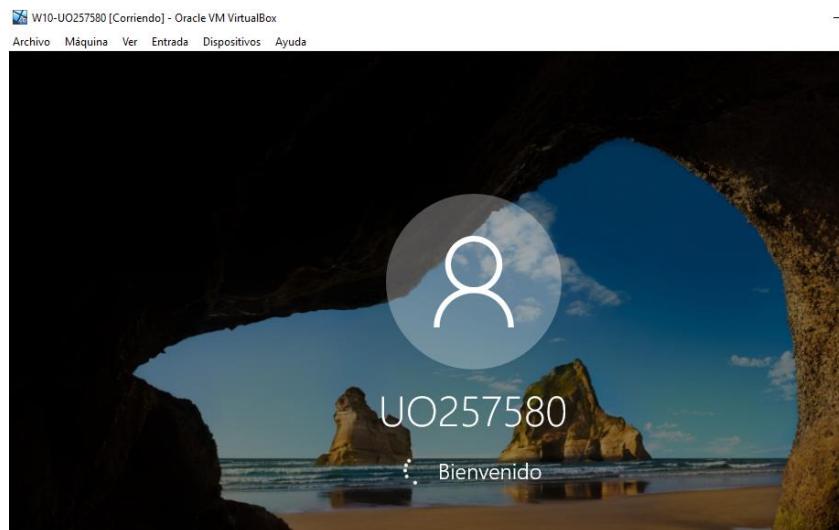




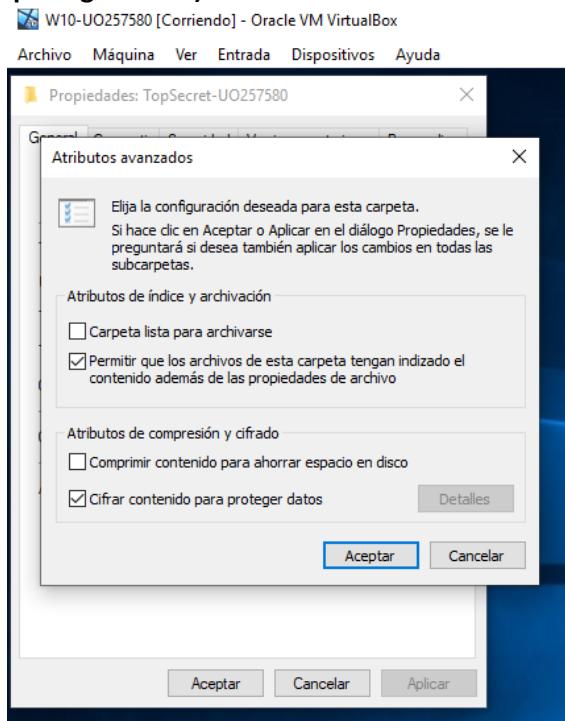
Al final, el alumno de SSOO tiene denegado el permiso de escritura, debido a que la denegación de permisos “está por encima” de la aceptación de permisos.

Parte 3: Trabajo con el sistema de ficheros encriptado

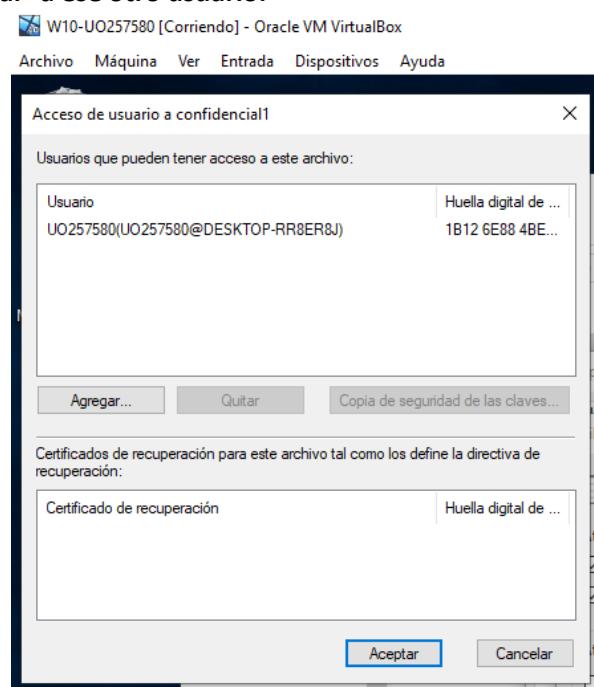
- 1) Entra en sesión con el usuario UOXXXX. Crea una carpeta dentro de ese usuario, denominada TopSecret-UOXXXX. Crea un fichero de texto denominado “confidencial” en esa carpeta y escribe tu nombre y apellidos.



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

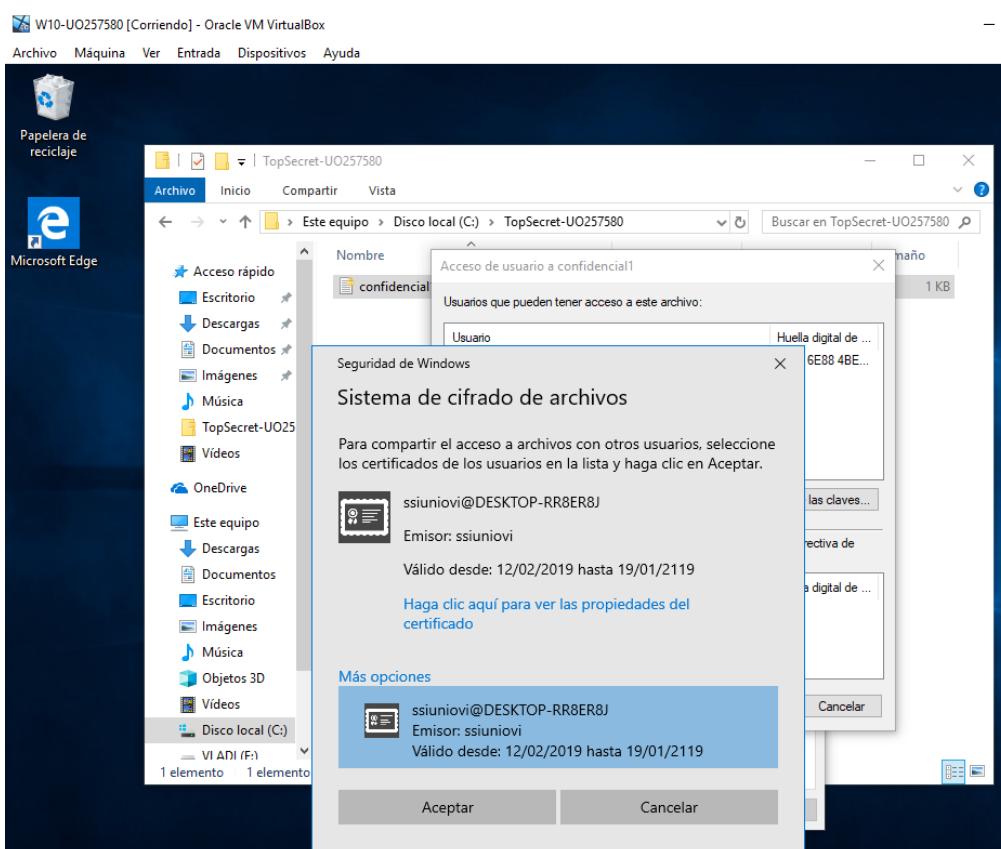
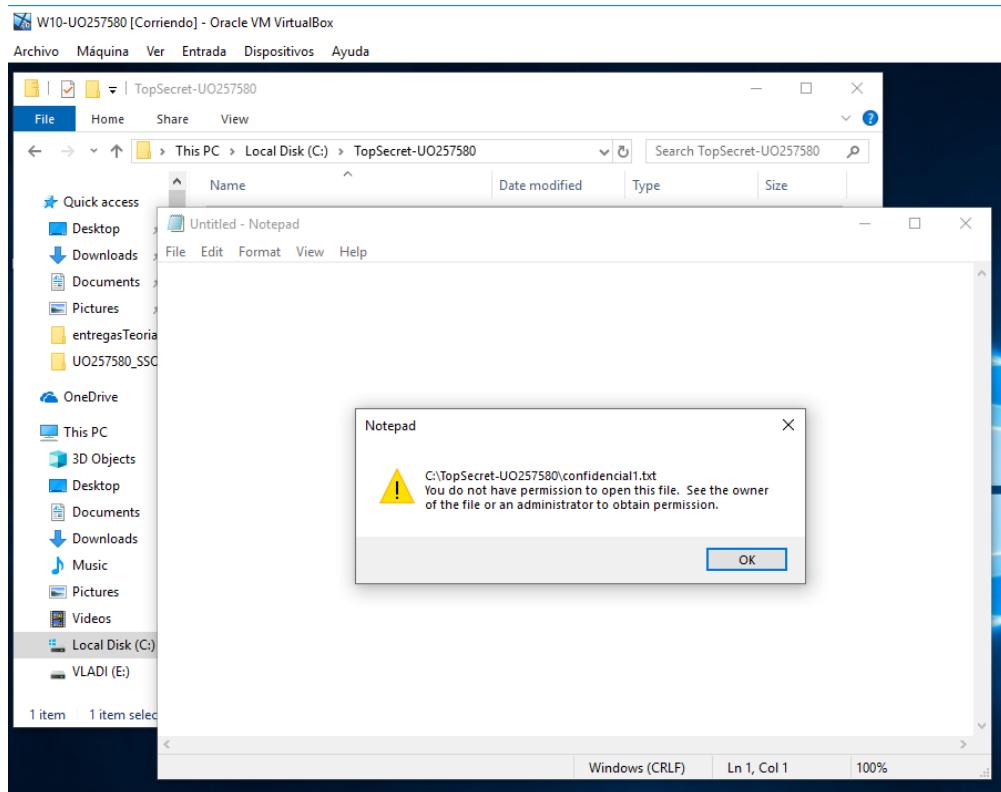


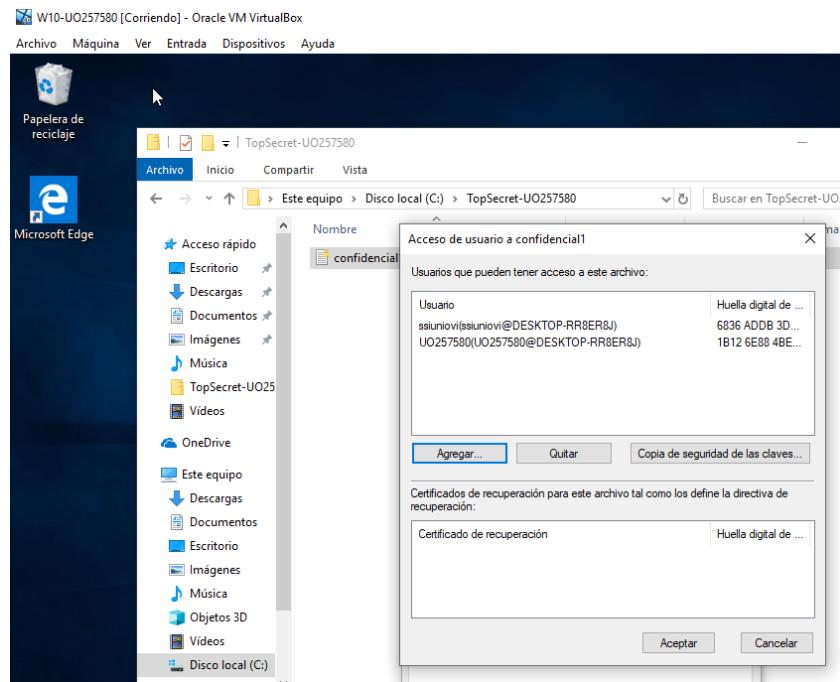
- 3) En la ventana anterior, ver los “Detalles” junto a la casilla de “Cifrar contenido para proteger datos”. Explica el contenido de esa ventana. Comprueba y documenta cómo si existe el certificado de seguridad de otro usuario se puede proporcionar acceso al archivo “confidencial” a ese otro usuario.



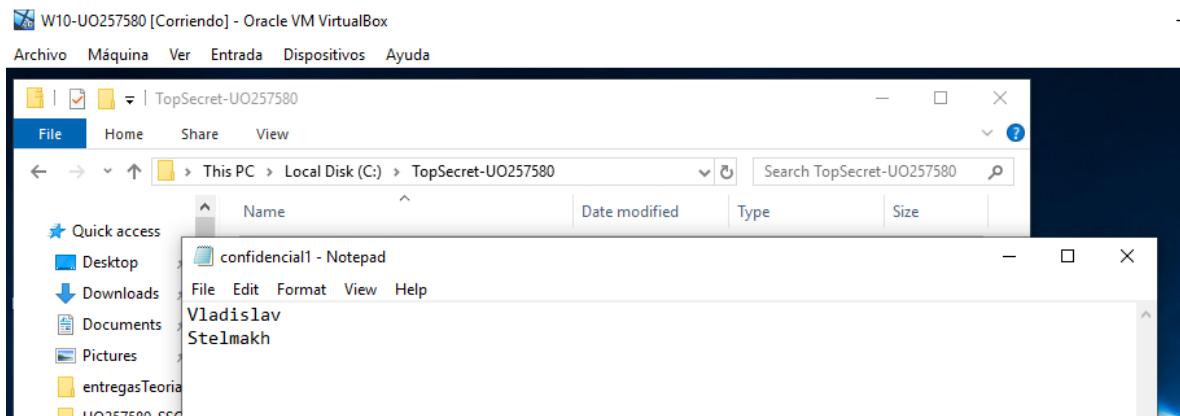
Podemos observar los usuarios que pueden tener acceso a este archivo, junto a su huella digital de certificado, y también los certificados de recuperación para el archivo tal como los define la directiva de recuperación.

Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS



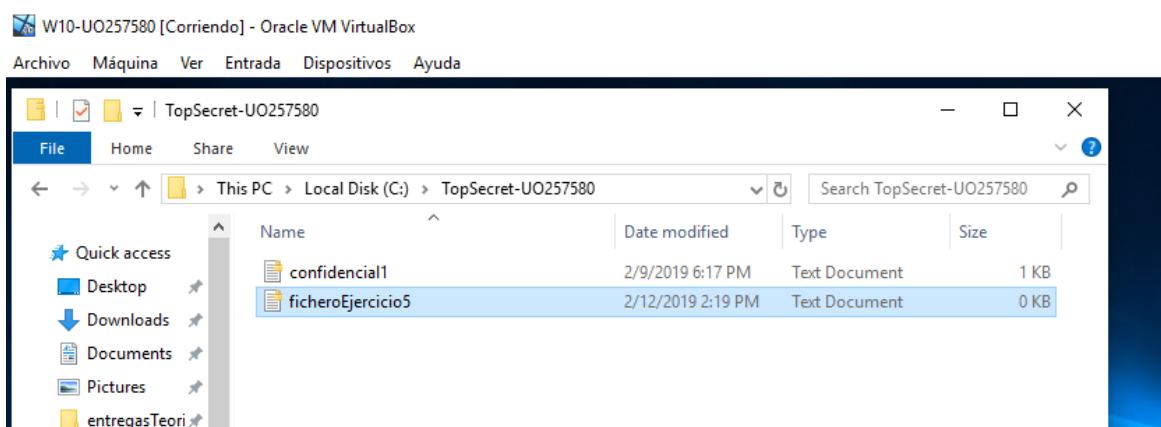


4) Entra como Administrador y accede al fichero. ¿Puedes hacerlo? ¿Por qué?

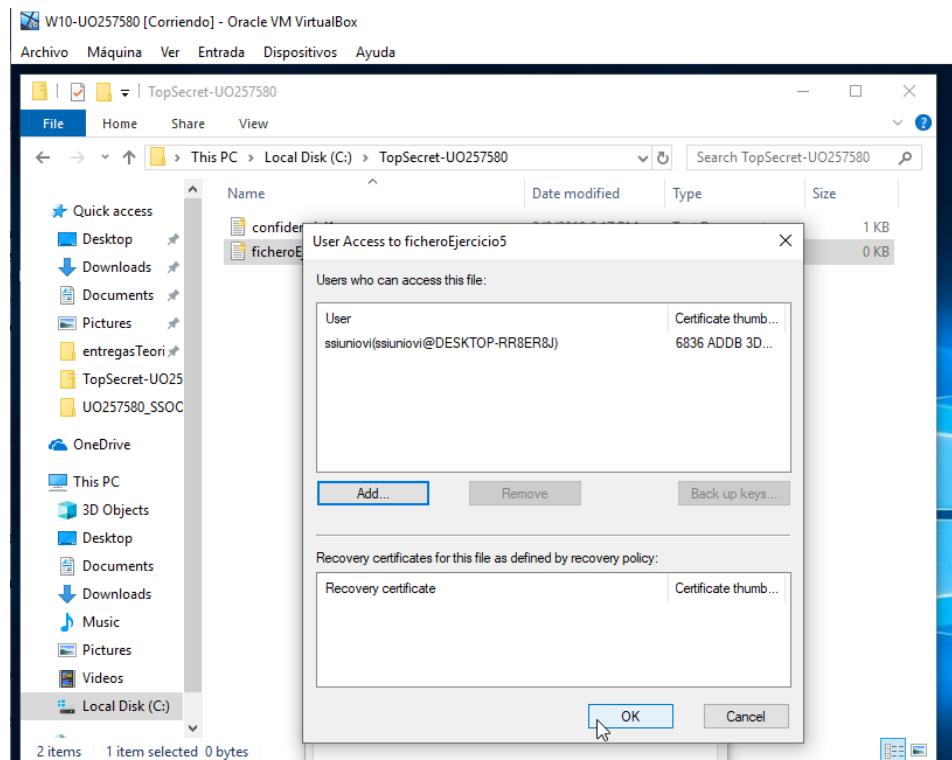


Ahora sí tengo permisos debido a que tengo acceso al archivo mediante el certificado añadido.

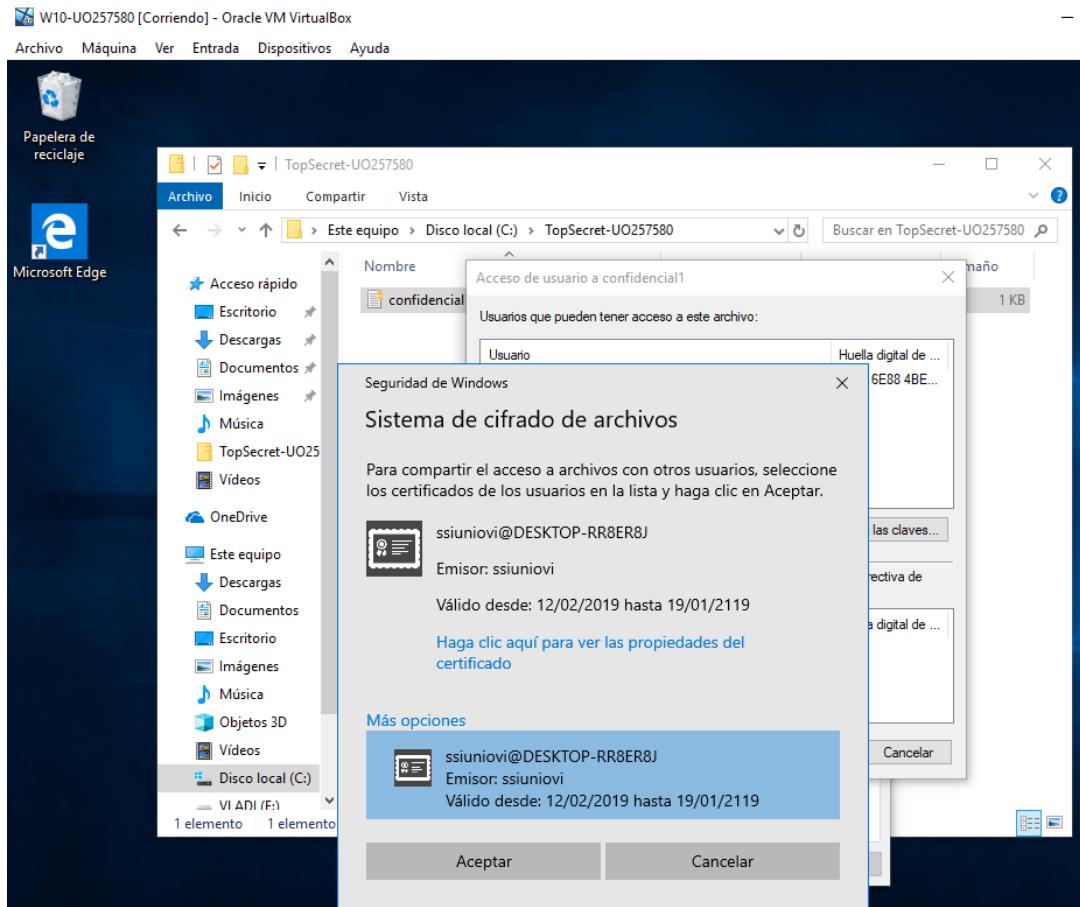
5) Como Administrador crea un nuevo fichero en esa carpeta. ¿Qué ocurre con ese fichero?.
¿Quién puede acceder a él? ¿Por qué? Agrega al usuario administrador para que pueda acceder al archivo confidencial.

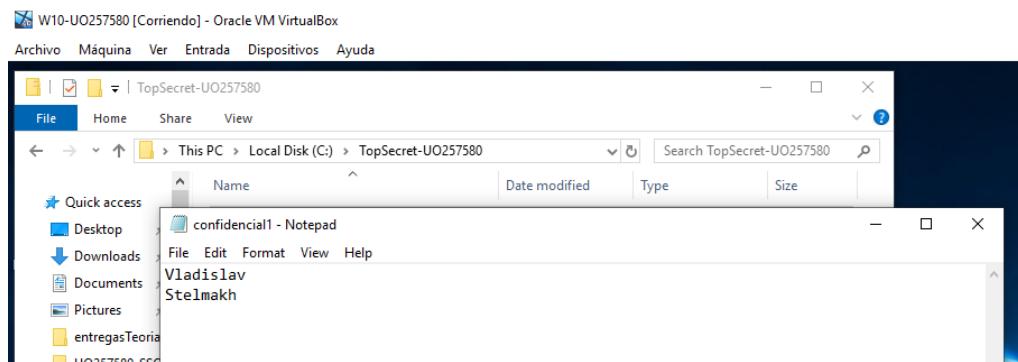
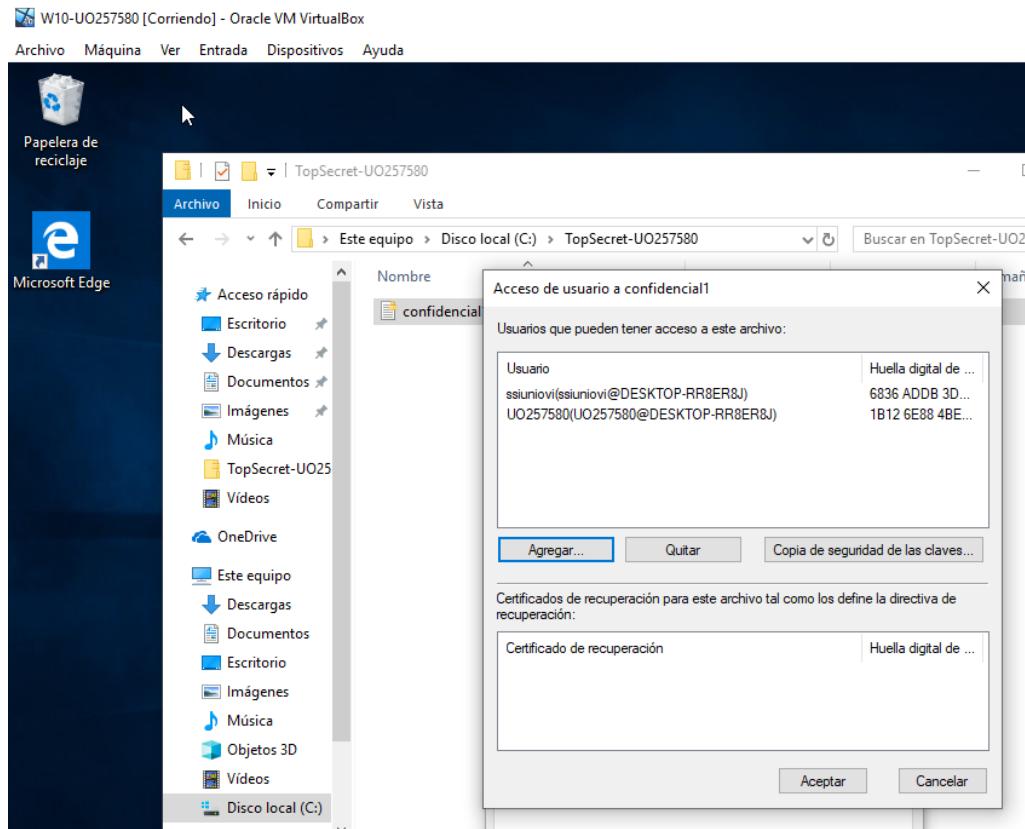


Lo que sucede nada más crear el fichero es que ese fichero queda cifrado.



Sólo él puede acceder a este fichero, ya que es quien lo creo, y es quién tiene el certificado necesario para poder acceder a él.





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

Contiene multitud de opciones destinadas a cifrar/descifrar ficheros/carpetas, así como para realizar otras acciones relacionadas.

Cifrar un archivo o carpeta: cipher /e [RUTA]

Descifrar: cipher /d [RUTA]

Borrar de forma efectiva y totalmente irrecuperable cualquier fichero o directorio, gracias al parámetro /W: cipher /w: [RUTA] ("La que más interesante me parece").

Primero debemos instalar cipher:

```
ash apt:install https://github.com/ash-shell/cipher.git
```

Cifrar archivos:

Tenemos el siguiente archivo:

```
# cat file
```

Archivo encriptado

Para encriptarlo hacemos lo siguiente:

```
ash cipher:e /root/file
```

```
<< cipher >>; Enter encryption password: *****
```

```
<< cipher >>; Confirm encryption password: *****
```

```
<< cipher >>; File encrypted at /root/file.enc
```

Finalmente obtenemos:

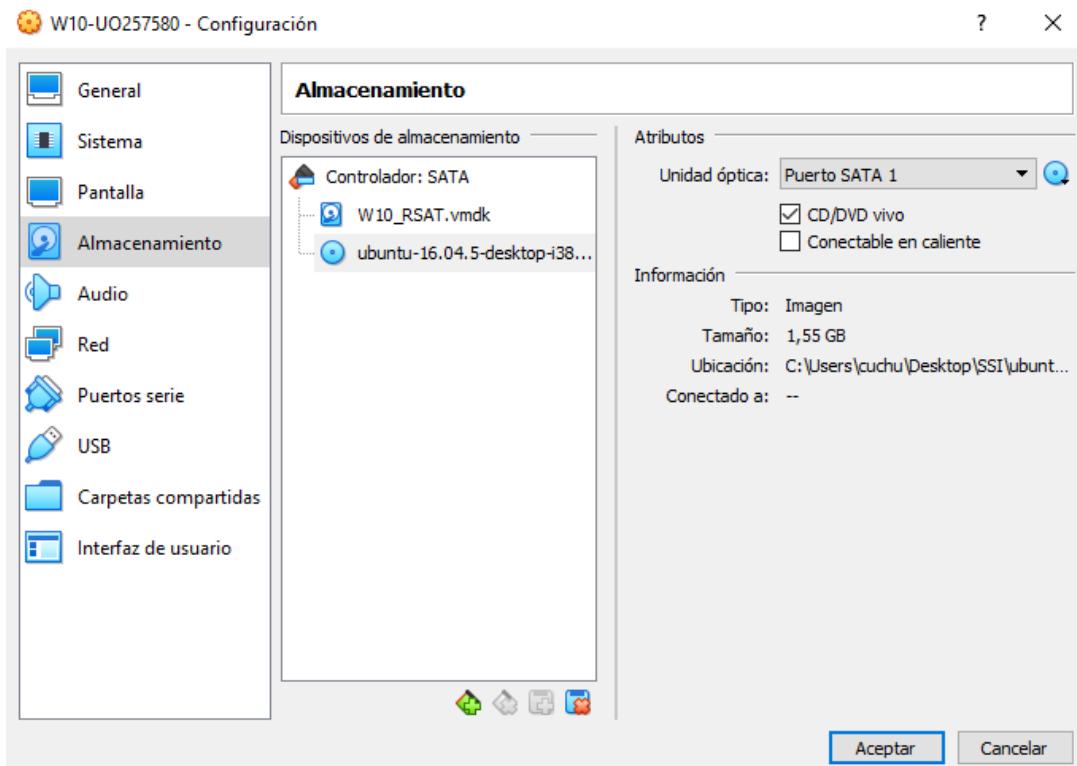
```
file.enc
```

Para cifrar carpetas el procedimiento sería prácticamente idéntico.

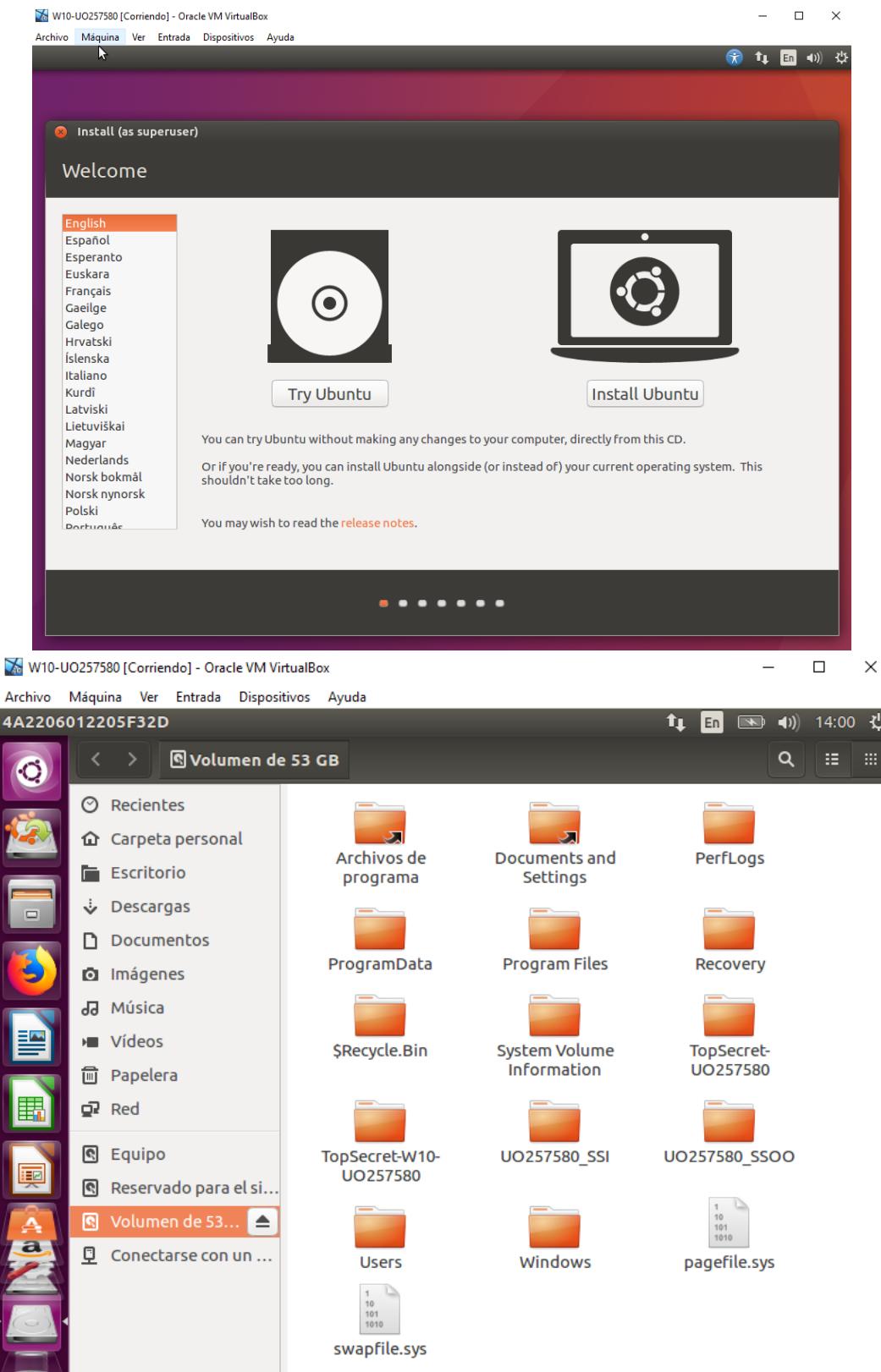
Para descifrar sería un procedimiento similar(más corto) pero con otro comando.

Parte 4: ¡Al ataque!

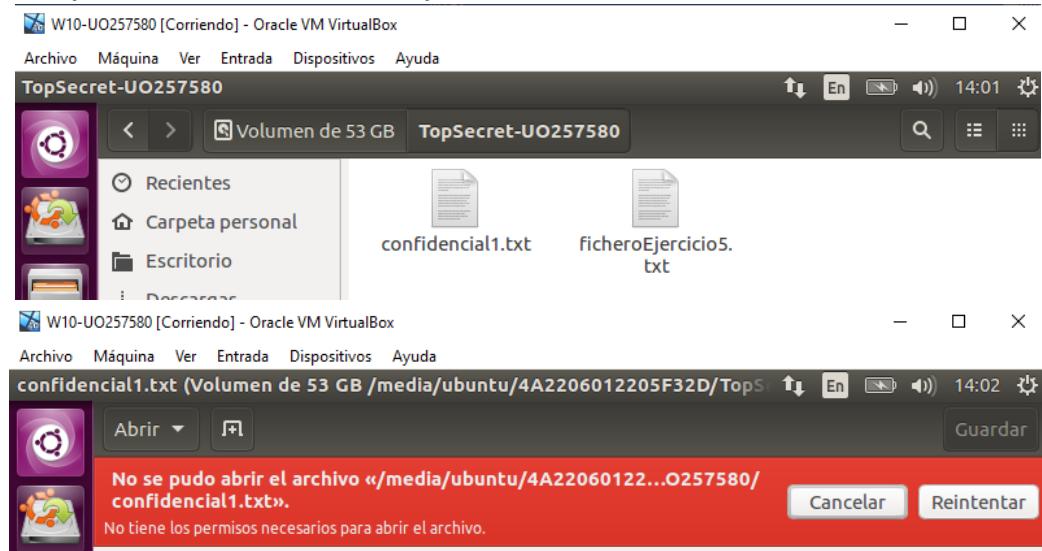
- 1) Arranca tu máquina virtual con un sistema Linux (<http://releases.ubuntu.com/16.04/ubuntu-16.04.5-desktop-i386.iso>, por ejemplo), utilizando un Live-CD. Configuración-Almacenamiento-Unidad-anfitrión-Unidad óptica, seleccionamos la imagen descargada y marcamos CD/DVD vivo.



- 2) 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?



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

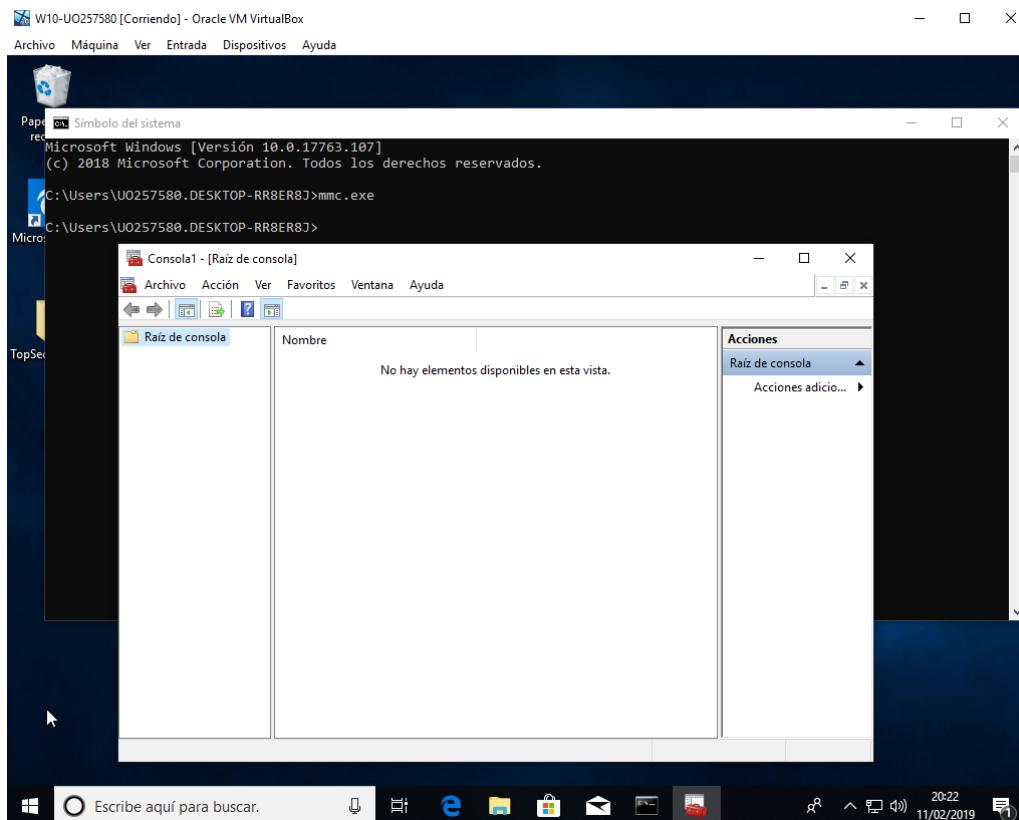


Puedo acceder a la carpeta y ver que hay un archivo .txt, pero no tengo permiso para poder visualizar/abrir dicho archivo.

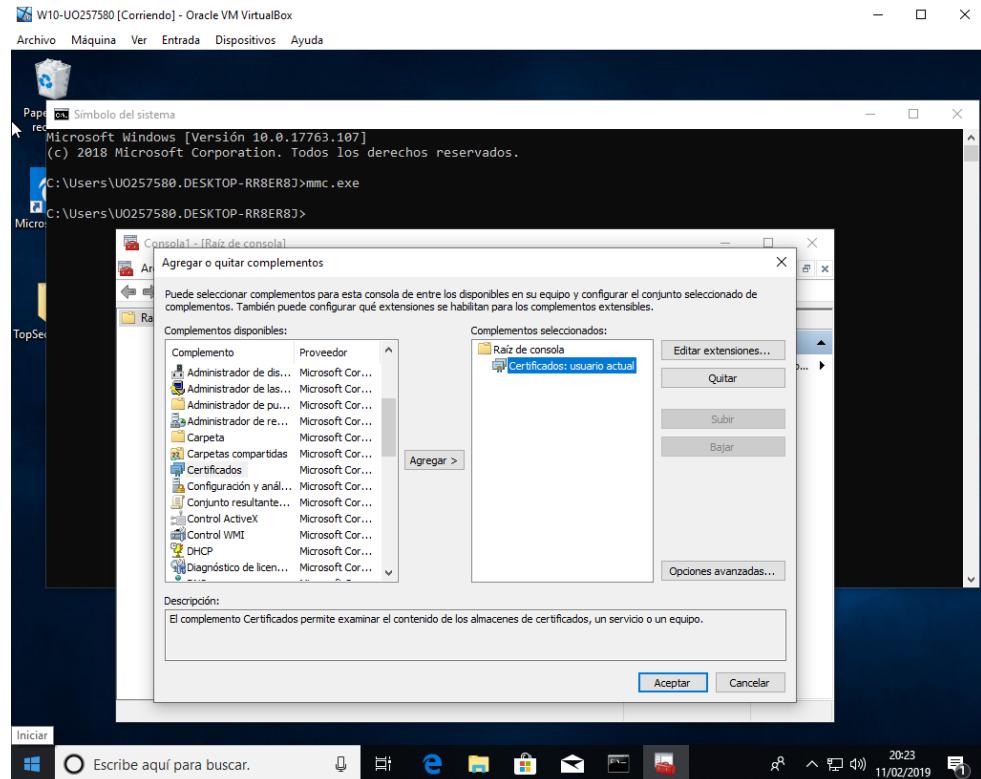
Parte 5: Opciones avanzadas

- 1) Exporta tu clave privada (usuario UO257580). Para ello:

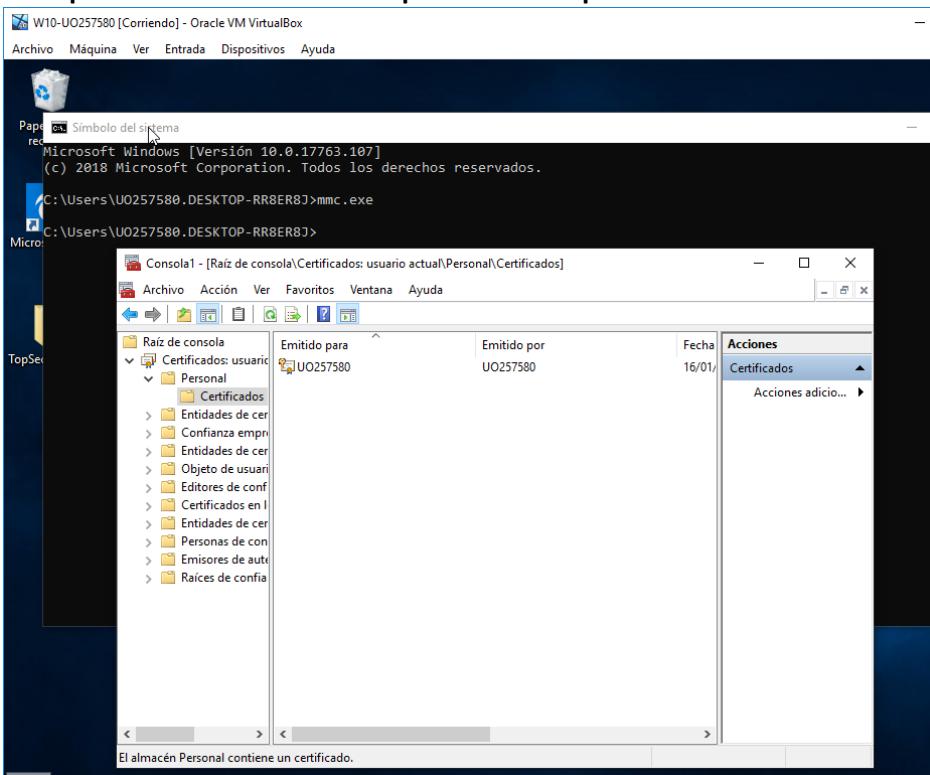
- Ejecuta mmc.exe

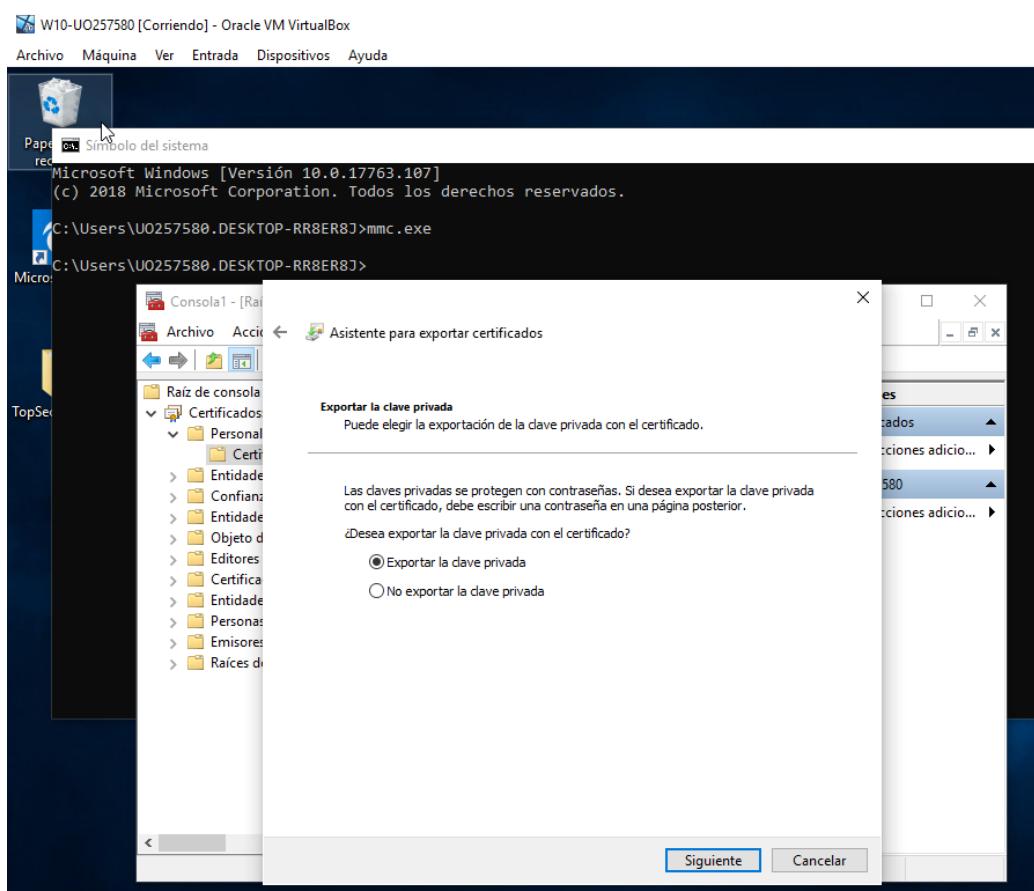
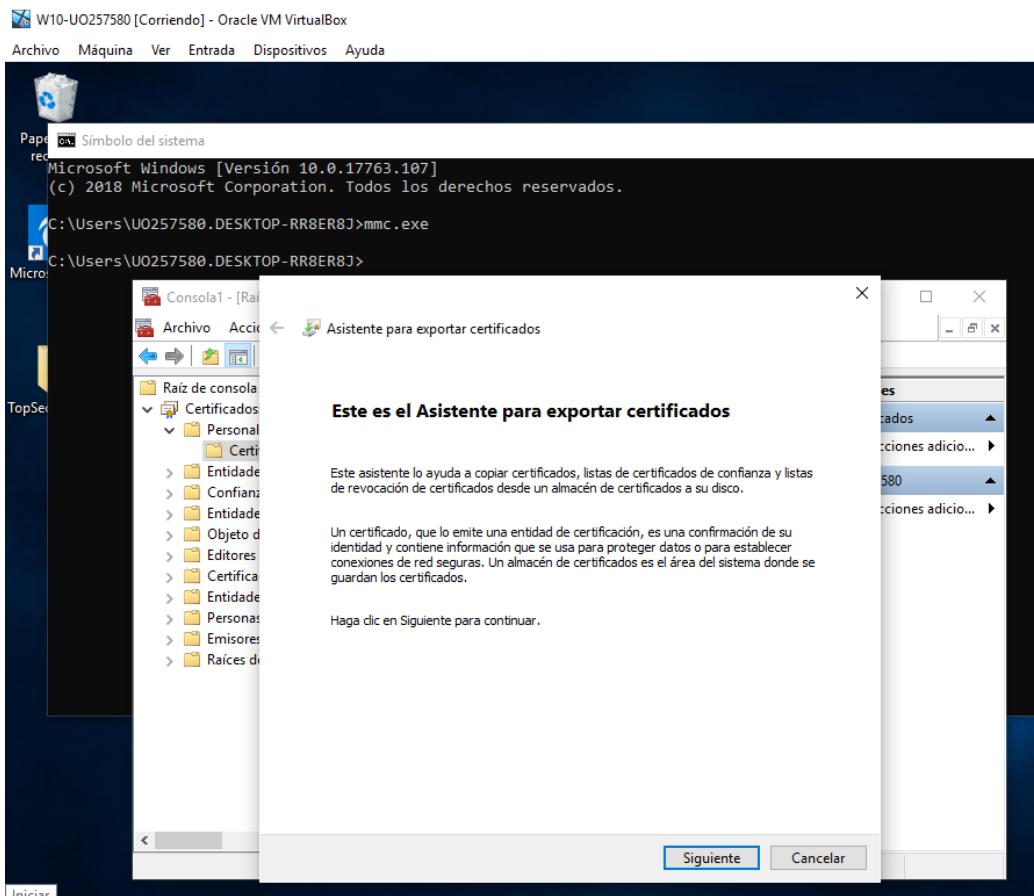


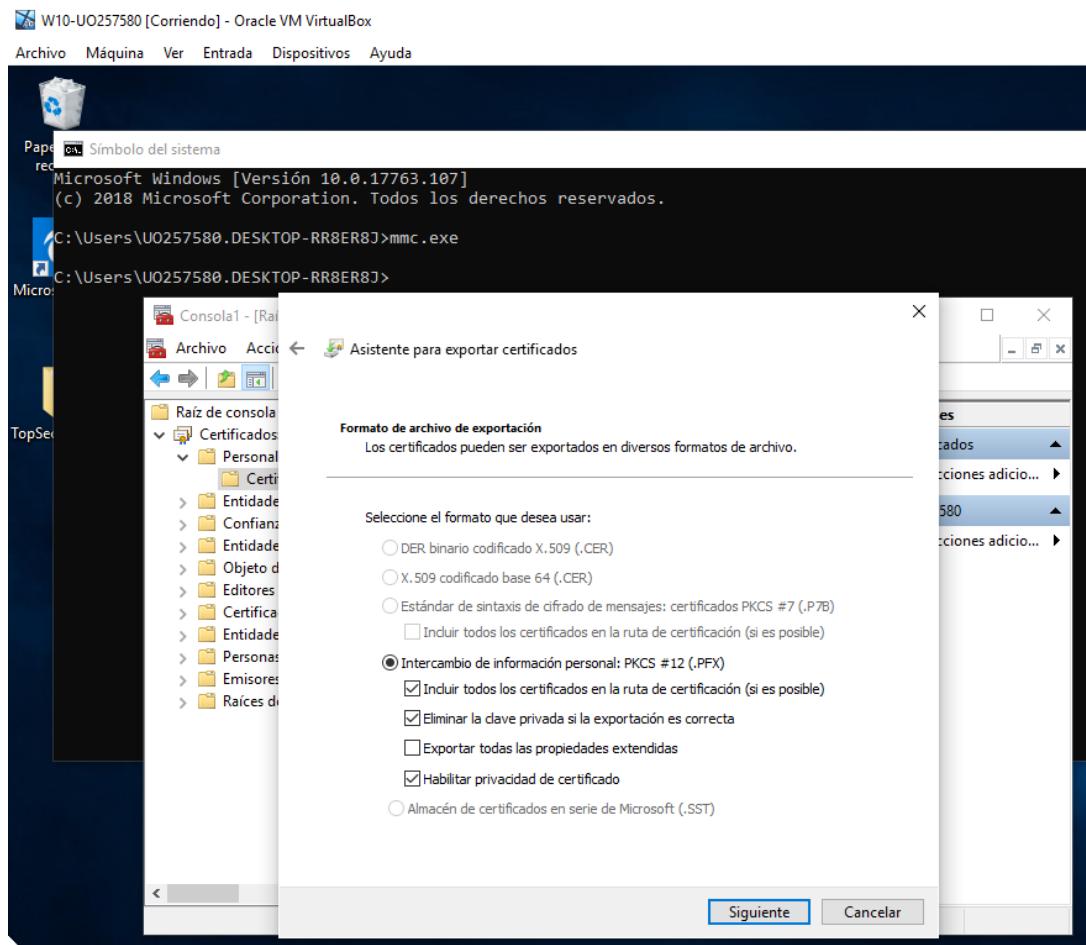
- Archivo, Añadir o quitar complemento, Agregar, Certificados, Agregar, Mi cuenta de usuario.



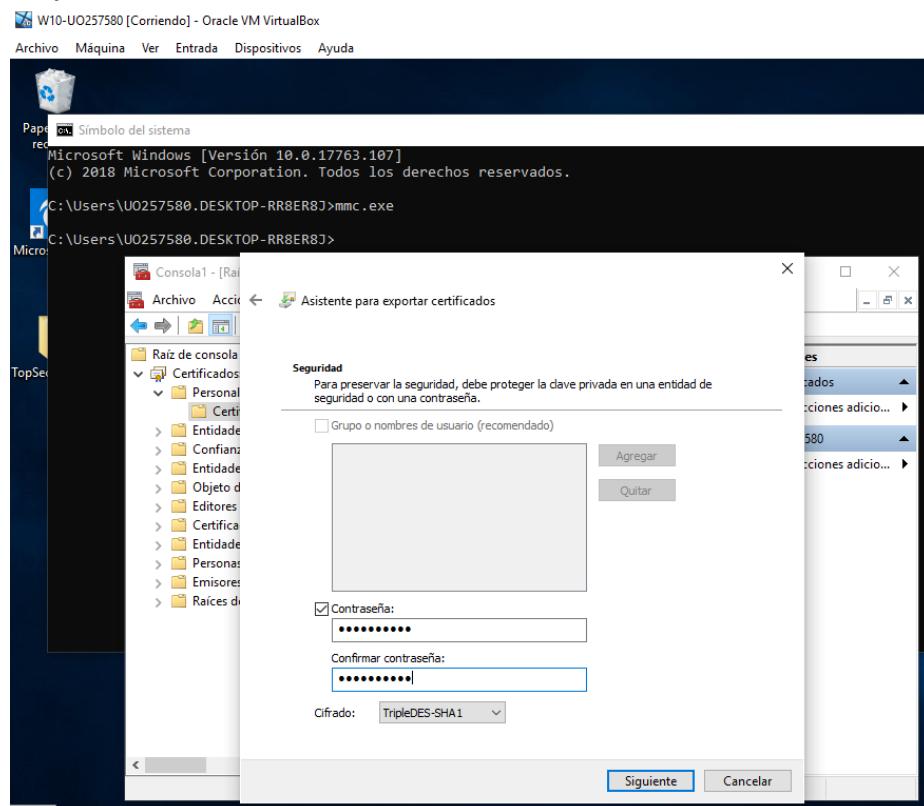
- En la carpeta que se crea “Personal-Certificados”, pulsar con el botón derecho sobre el certificado a exportar. Elegir “Todas las tareas, Exportar -> Exportar clave privada -> Eliminar la clave privada si la exportación es satisfactoria”.



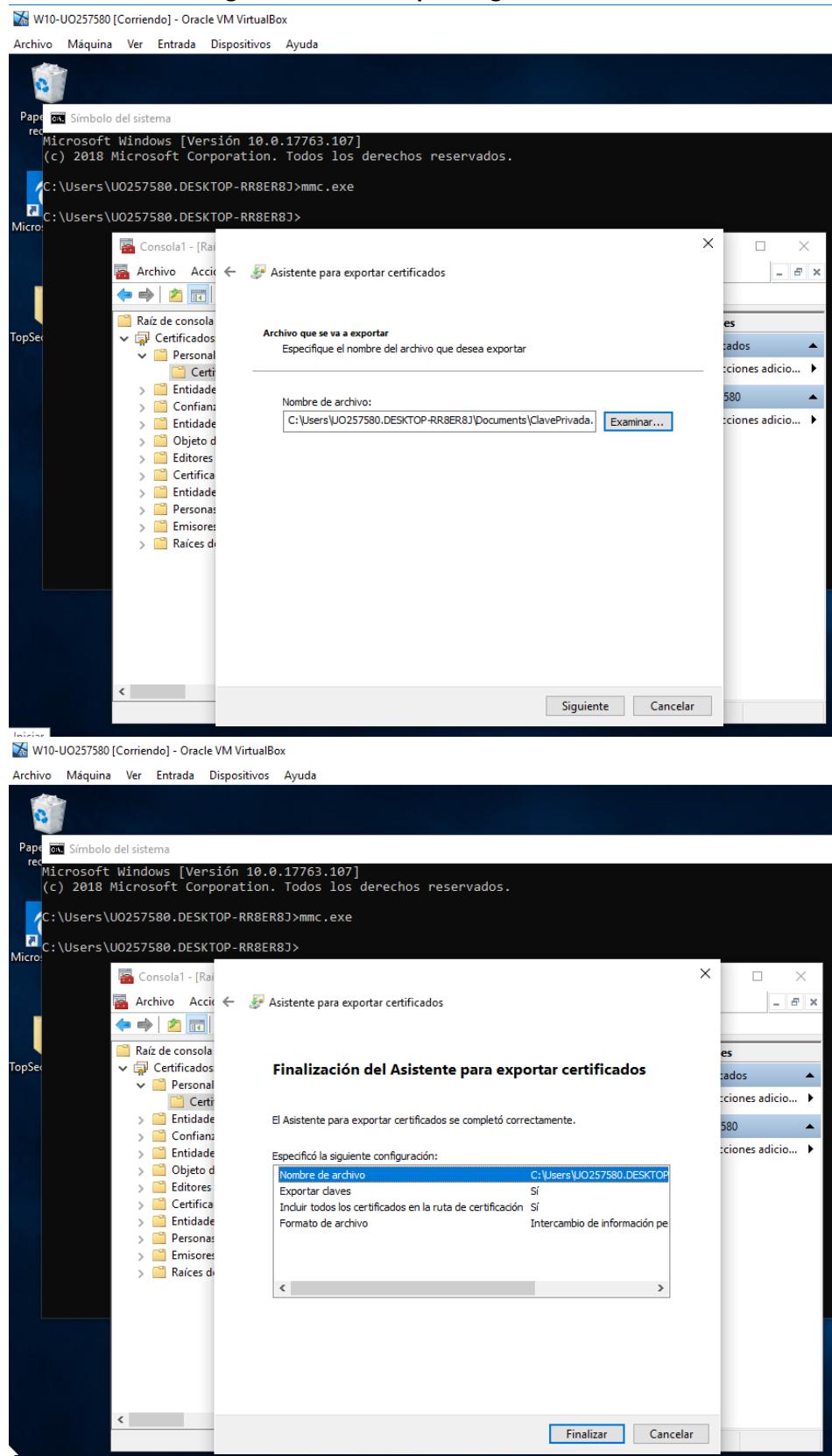




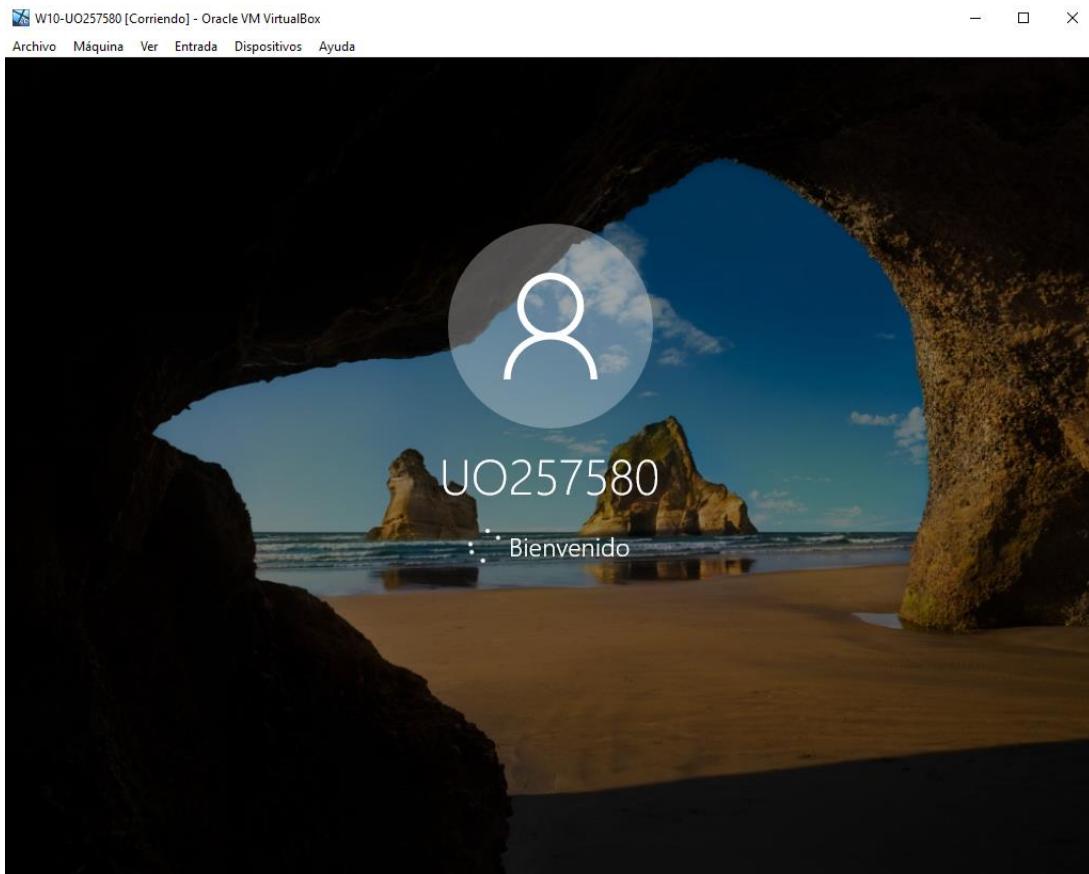
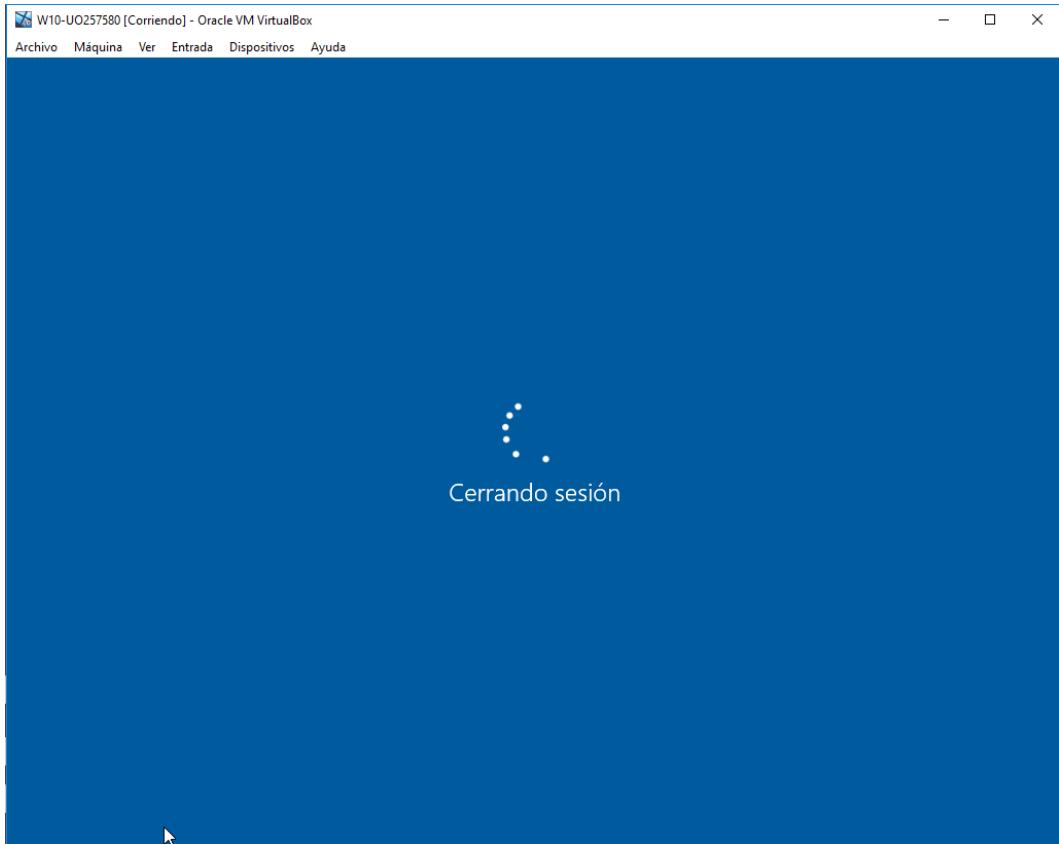
- Introduce (iiy anota en algún lado para no olvidarla!!) la clave para recuperarla.



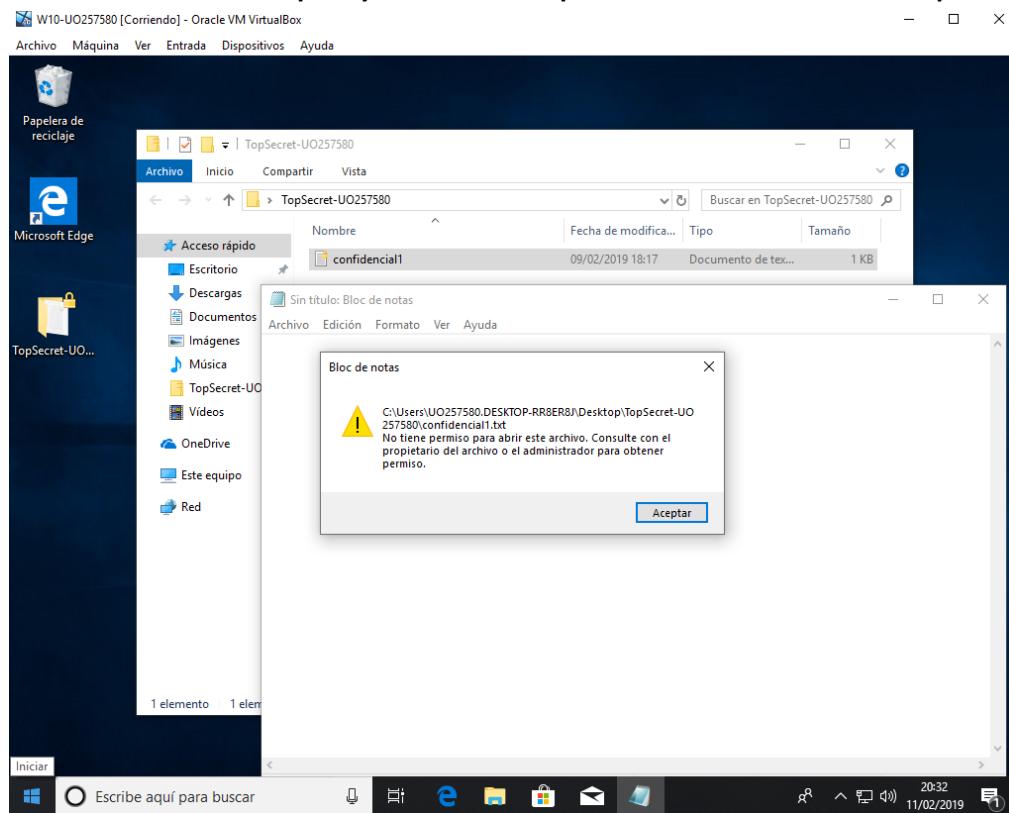
- Almacena el fichero generado en cualquier lugar.



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

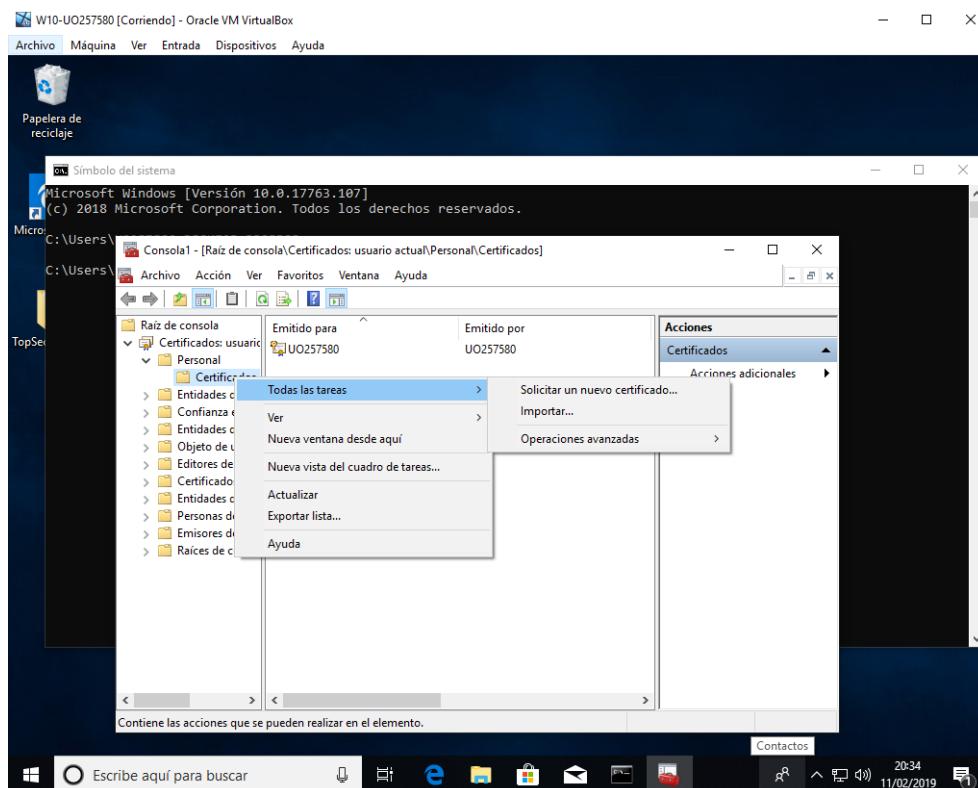


2) Prueba a acceder a la carpeta y el fichero encriptado. ¿Puedes hacerlo? ¿Por qué?

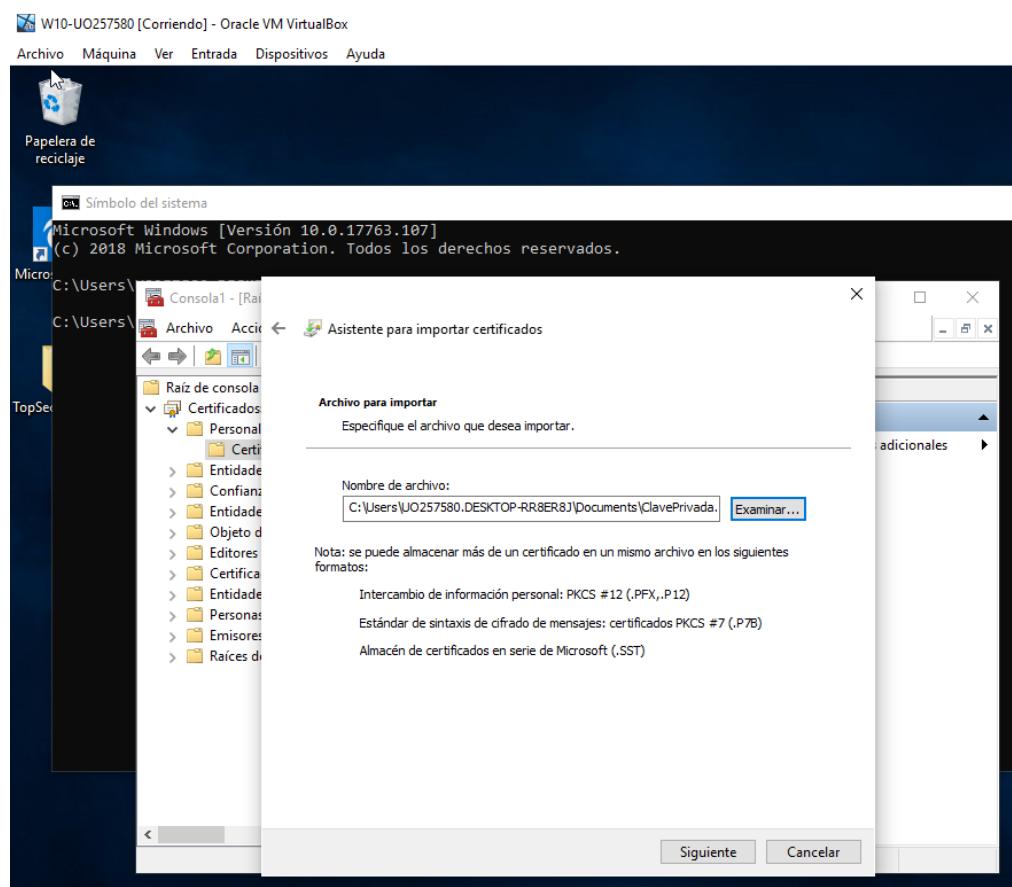
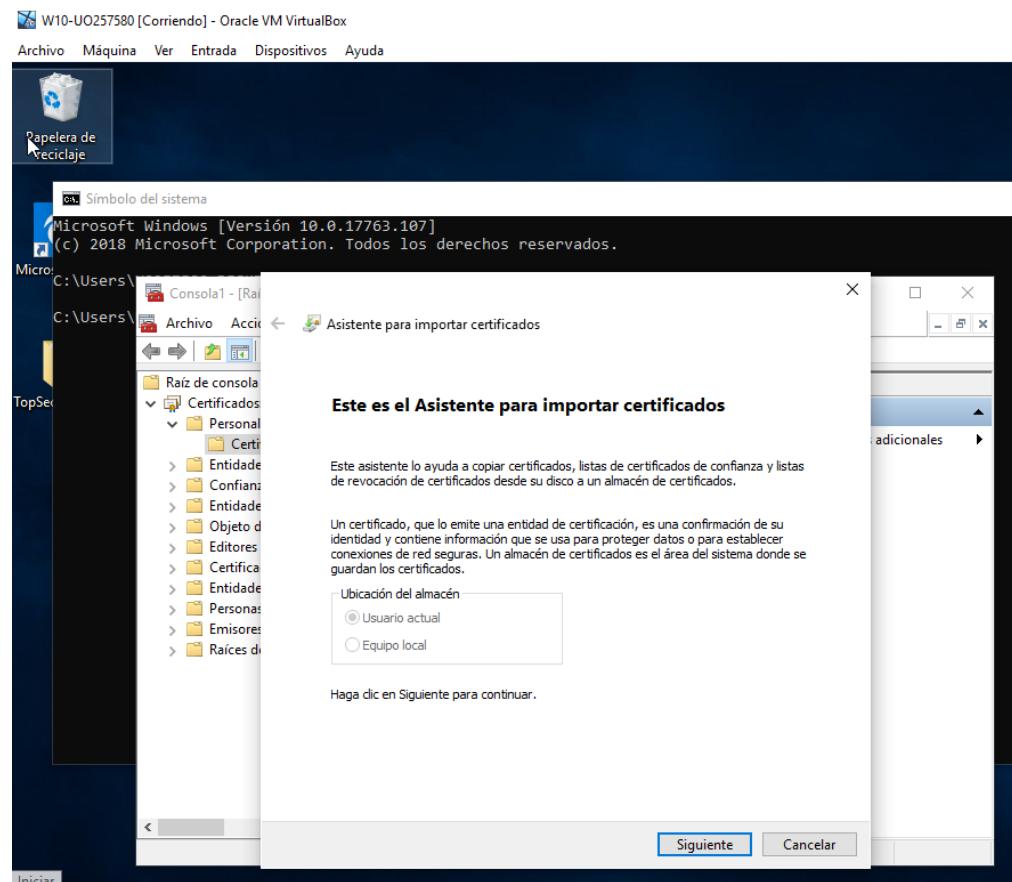


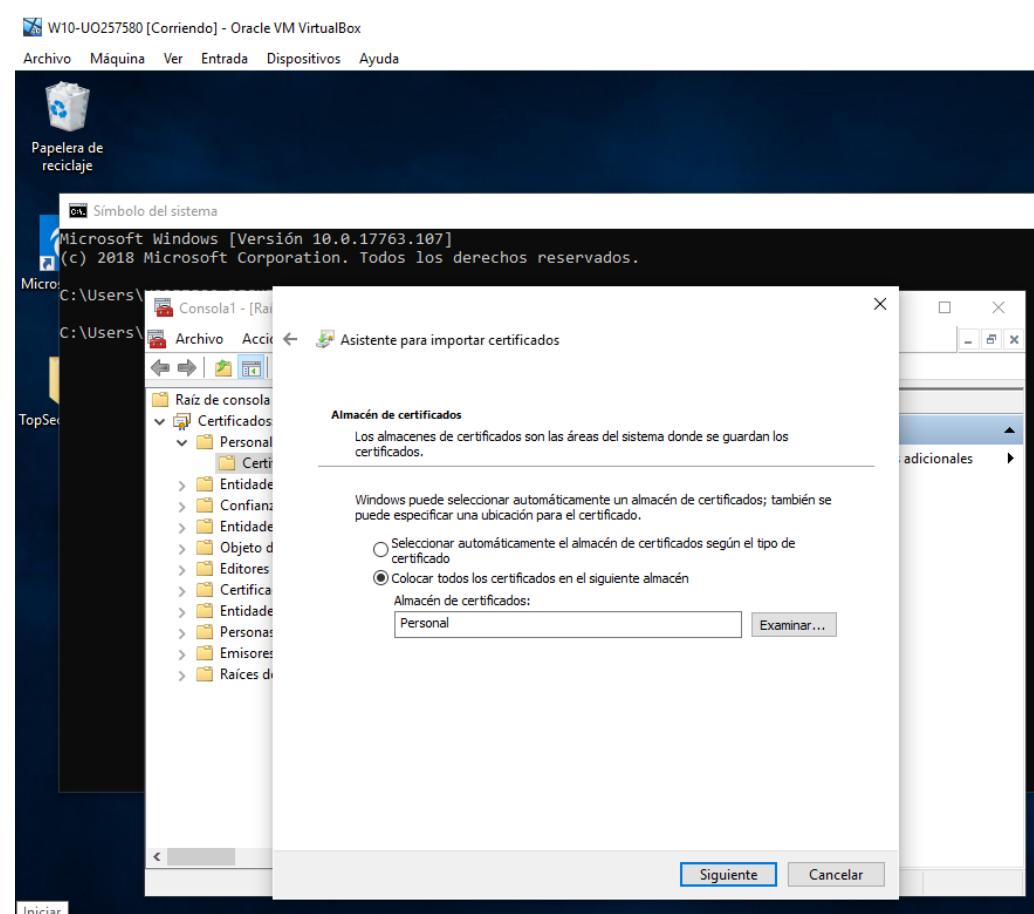
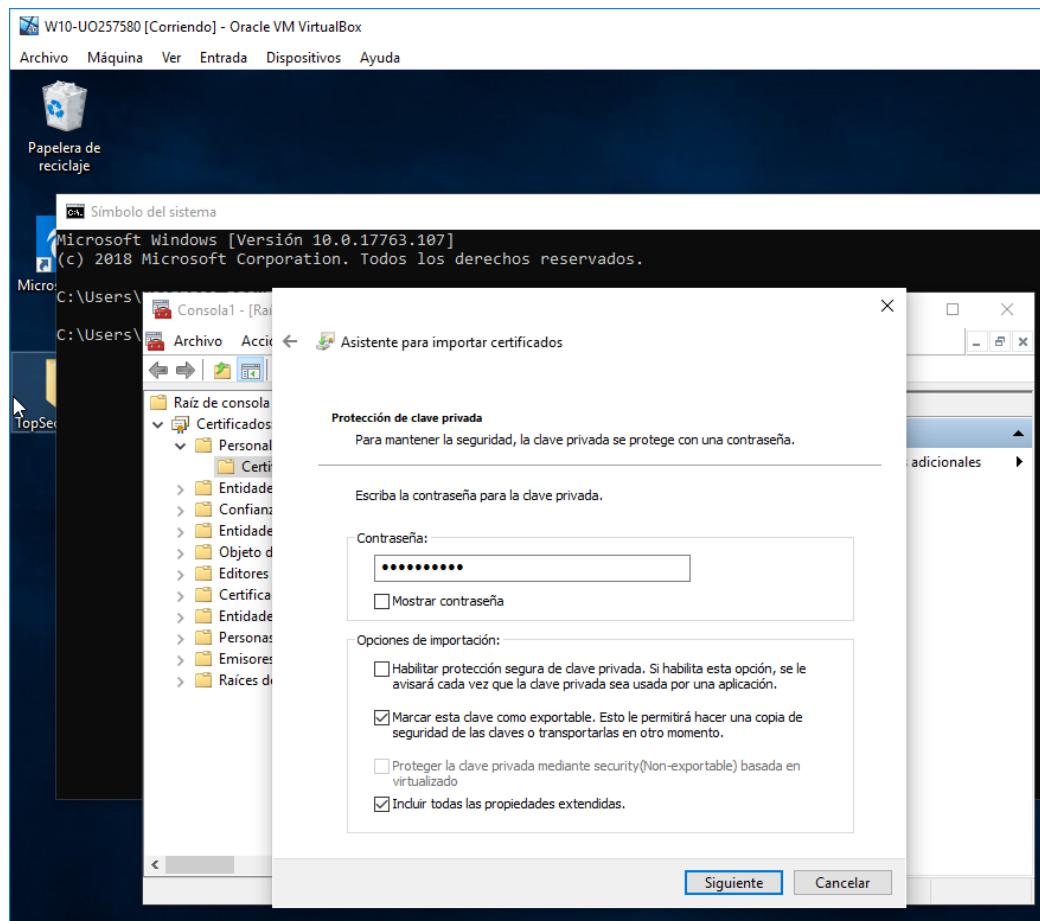
No, debido a que no tengo permiso para acceder a este archivo, no dispongo de la clave necesaria para el acceso.

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

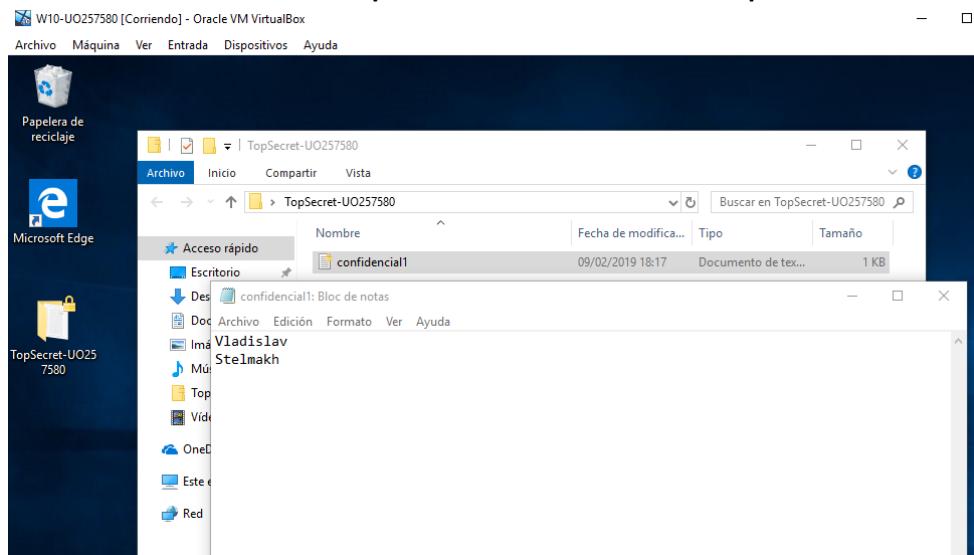


Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS





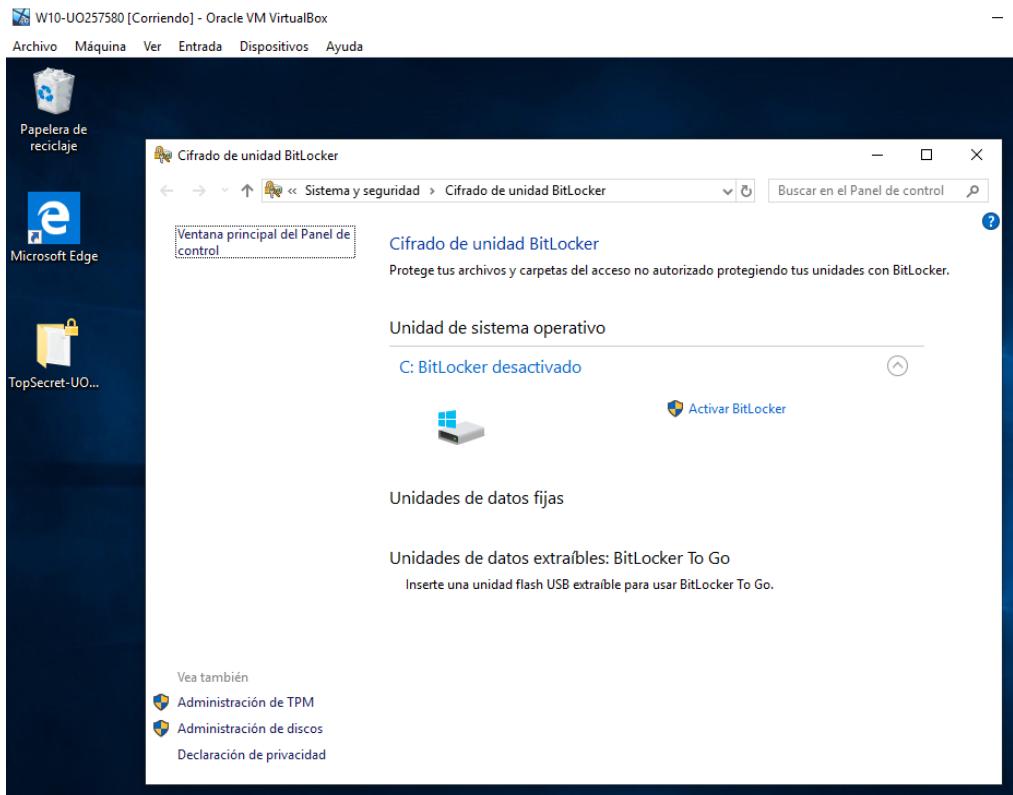
4) Prueba a acceder al fichero encriptado. ¿Puedes hacerlo? ¿Por qué?

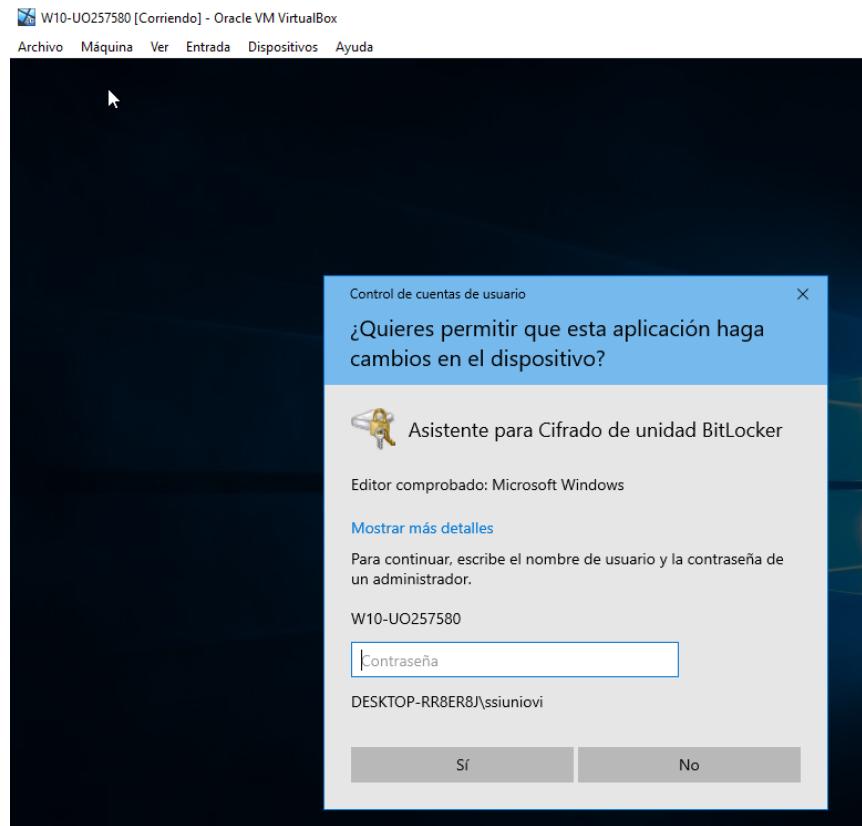


Sí, debido a que ahora poseo la clave necesaria para poder acceder a él.

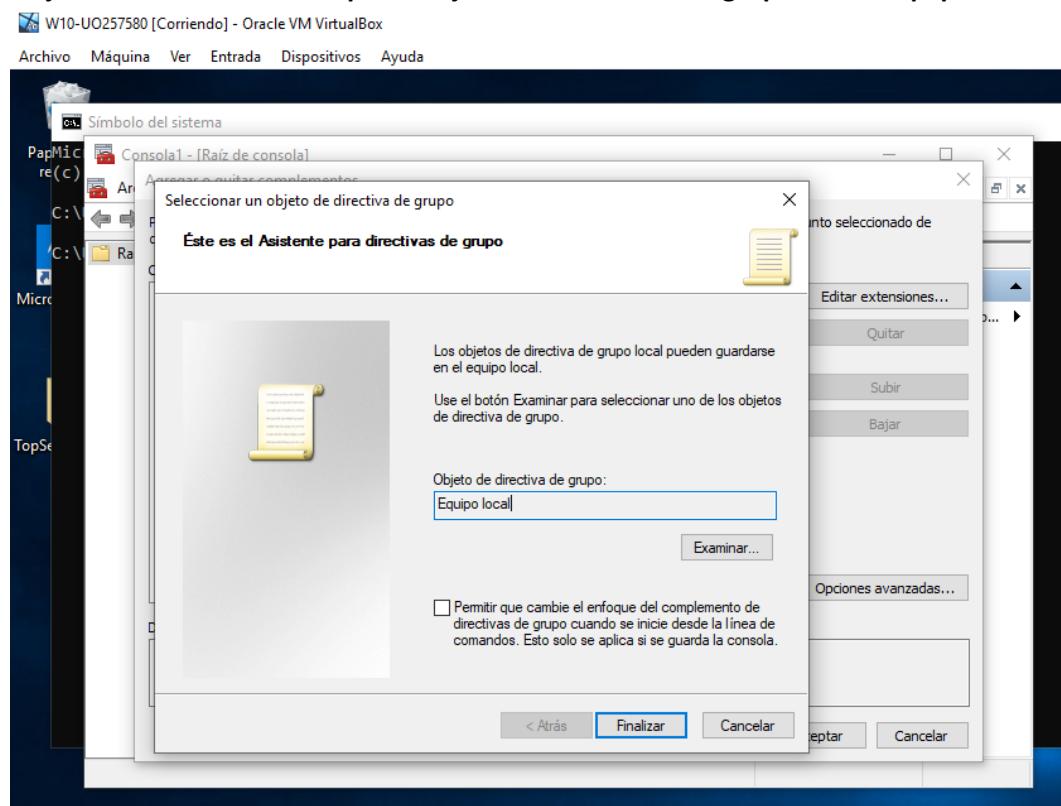
Parte 6: BitLocker

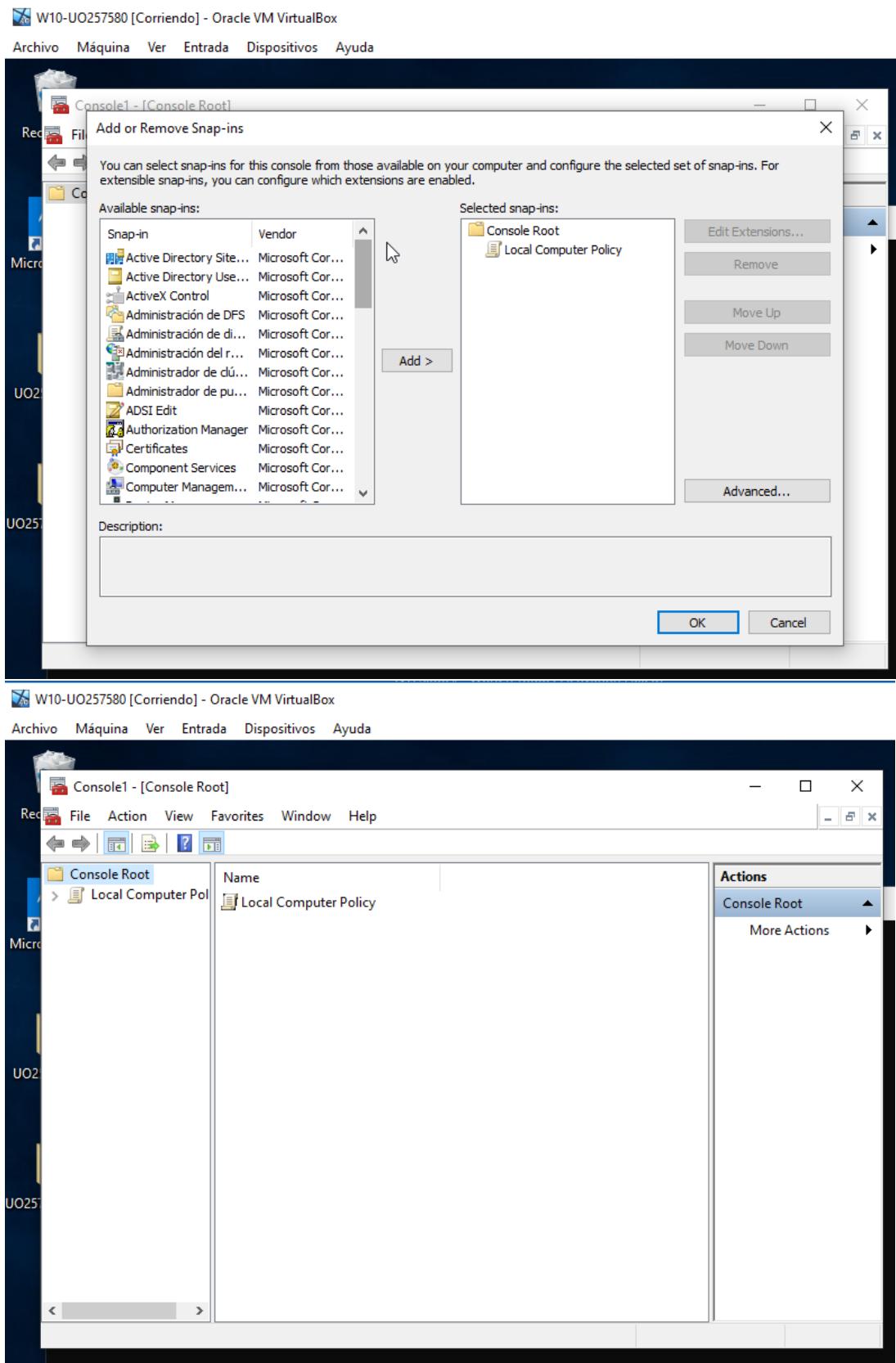
- 1) Para activar BitLocker, ejecutamos Administrar BitLocker y pinchamos en “Activar BitLocker”. Vemos que no se puede activar BitLocker porque nuestro dispositivo no tiene un TPM (Trusted Platform Module) compatible. Para usar BitLocker habrá que permitir su uso sin TPM compatible.



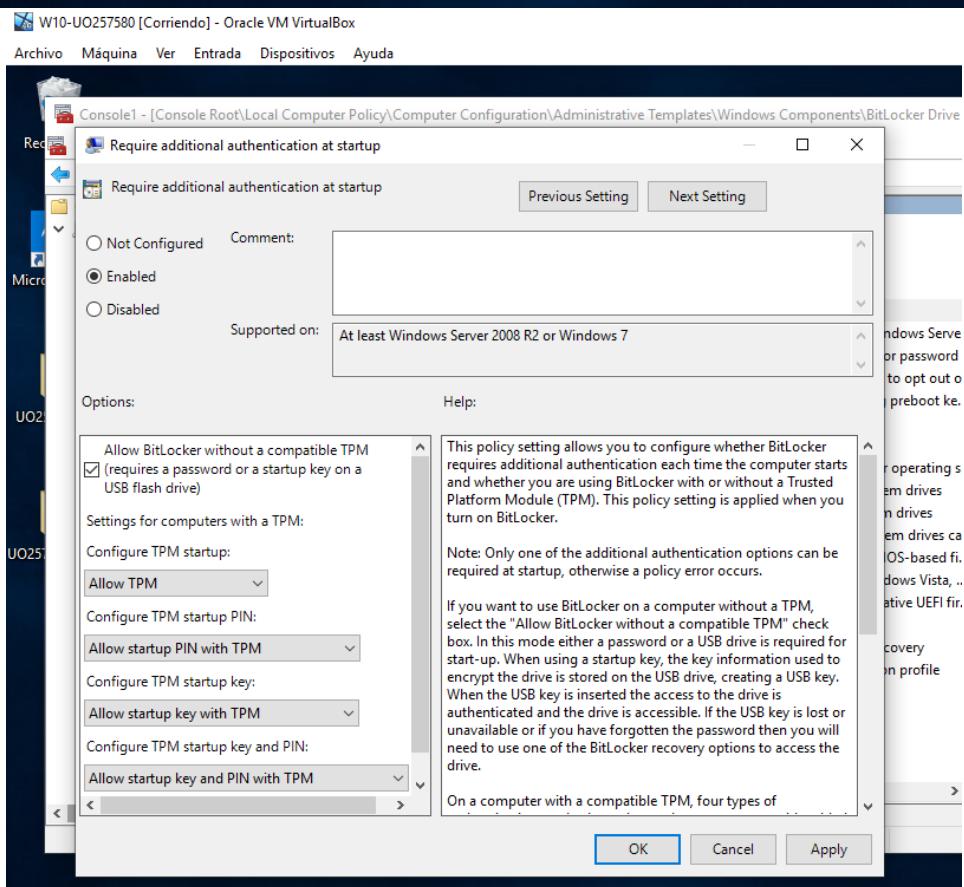
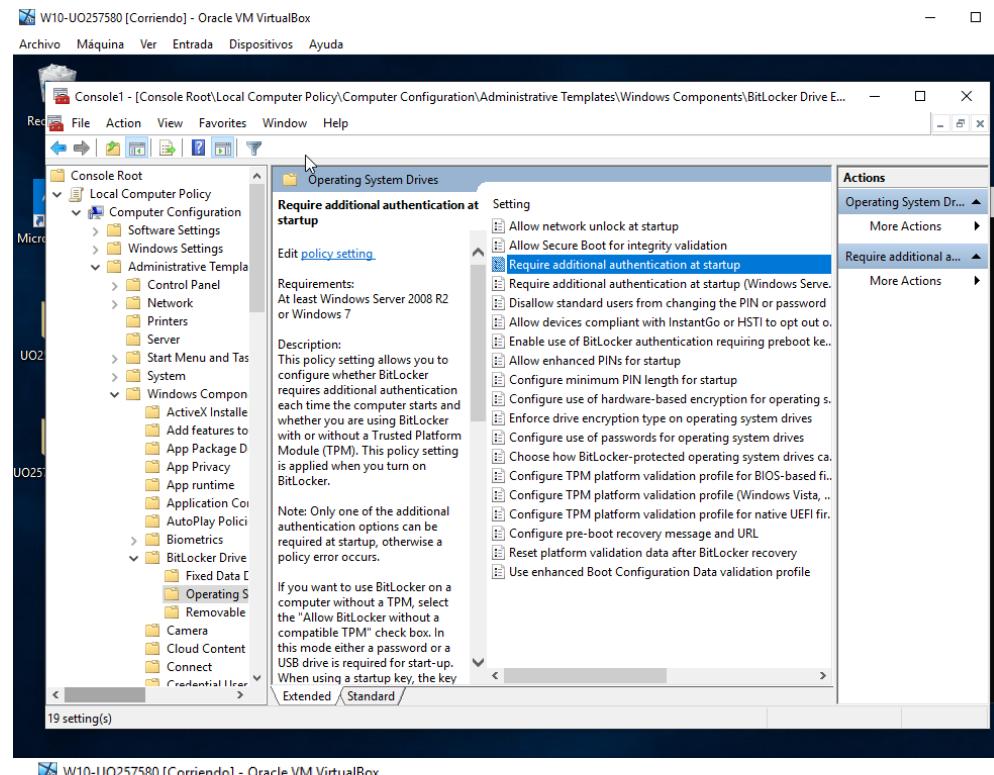


- 2) Ejecutamos mmc.exe, Archivo-Agregar o quitar complementos y añadimos Editor de Objetos de Directiva de Grupo. El objeto de la directiva de grupo será el equipo local.

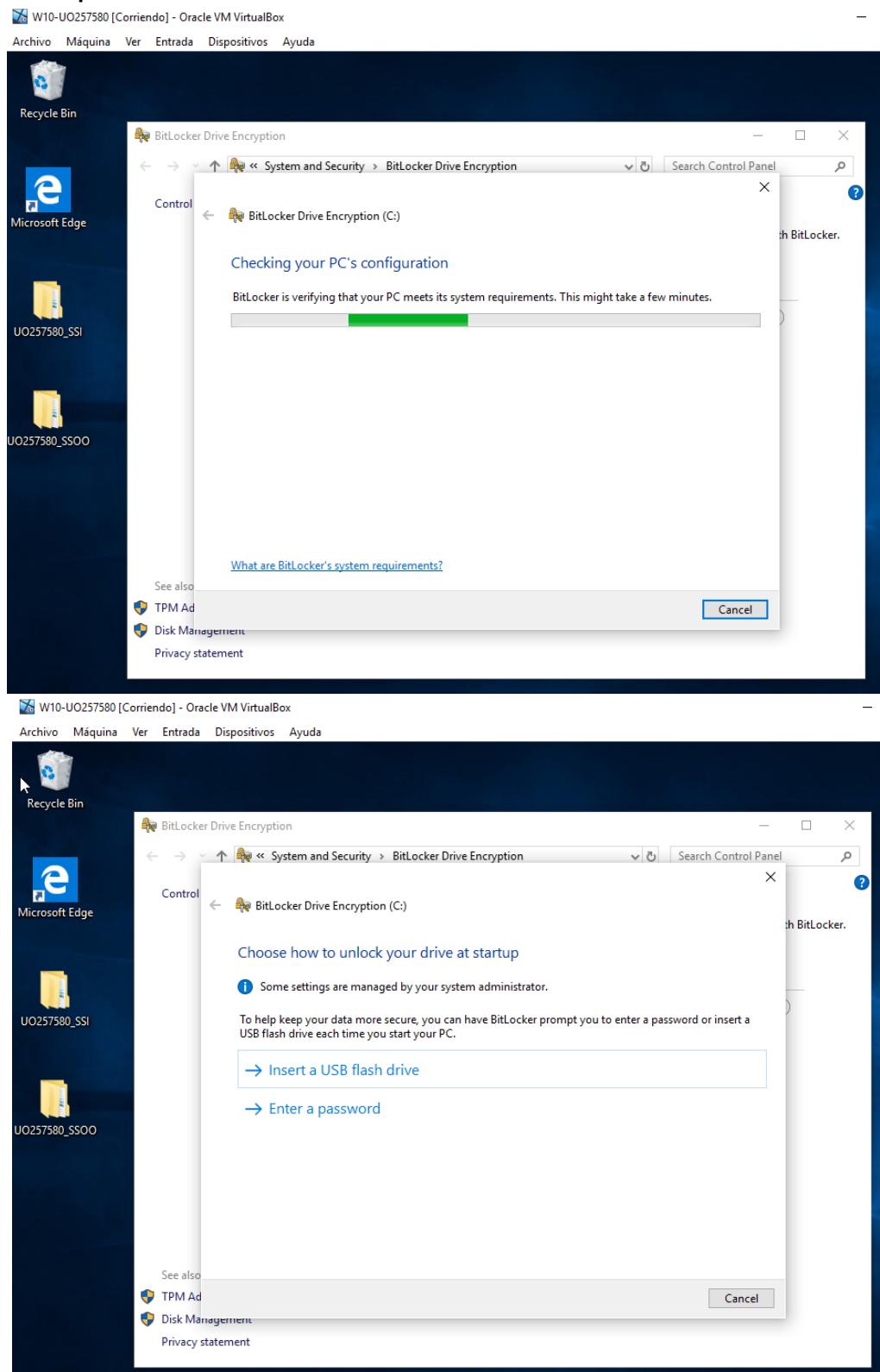


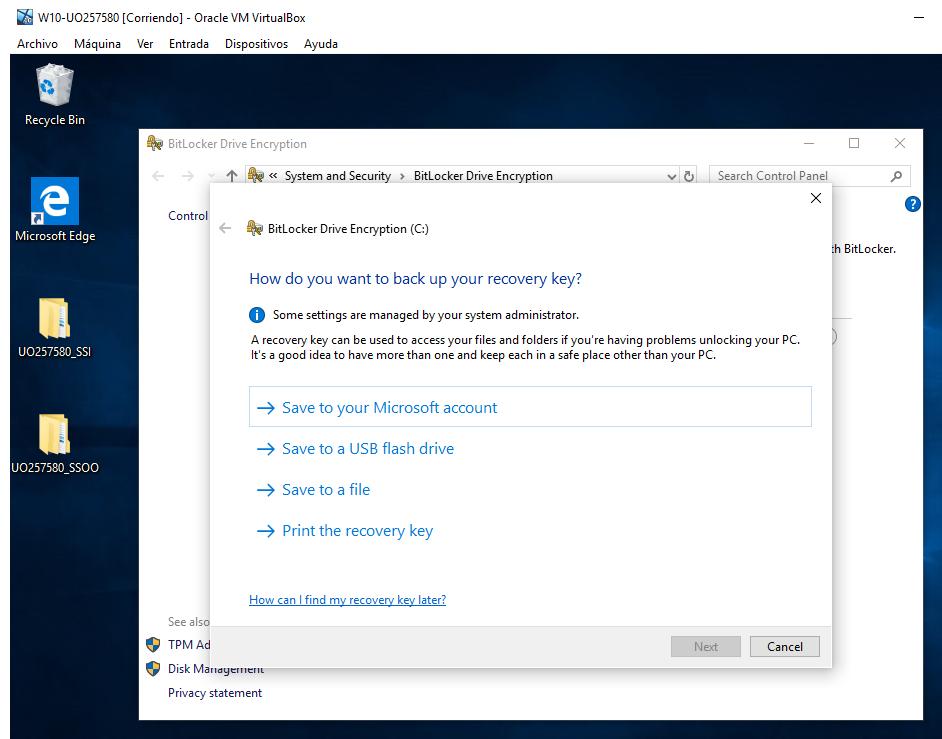


- 3) En la Directiva de Equipo Local pinchamos en Configuración del Equipo-Plantillas Administrativas-Componentes de Windows-Cifrado de unidad BitLocker-Unidades del Sistema Operativo-Requerir Autenticación al Iniciar y le damos a Habilitar. Nos aseguramos que la opción de Permitir BitLocker sin un TPM compatible este seleccionada.

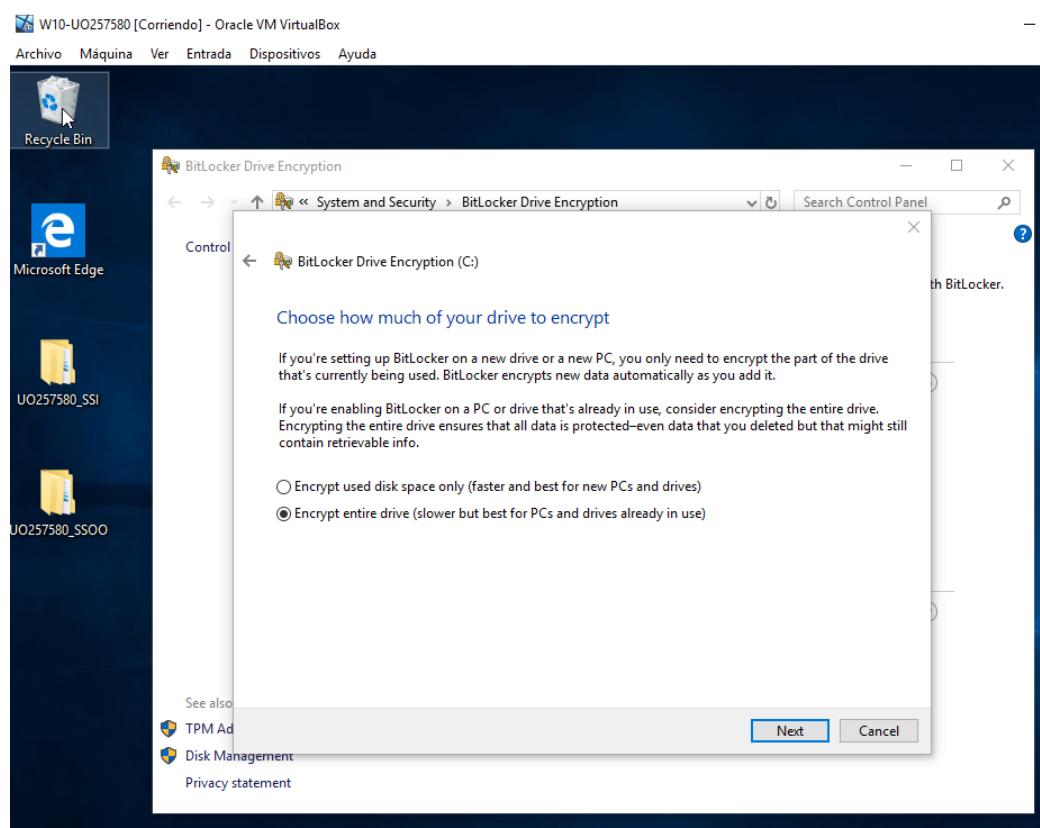


- 4) Activamos BitLocker y elegimos Escribir Contraseña como método para desbloquear la unidad en el inicio. ¡CUIDADO! Si nos olvidamos de esta contraseña no habrá forma de recuperar el acceso al S.O.

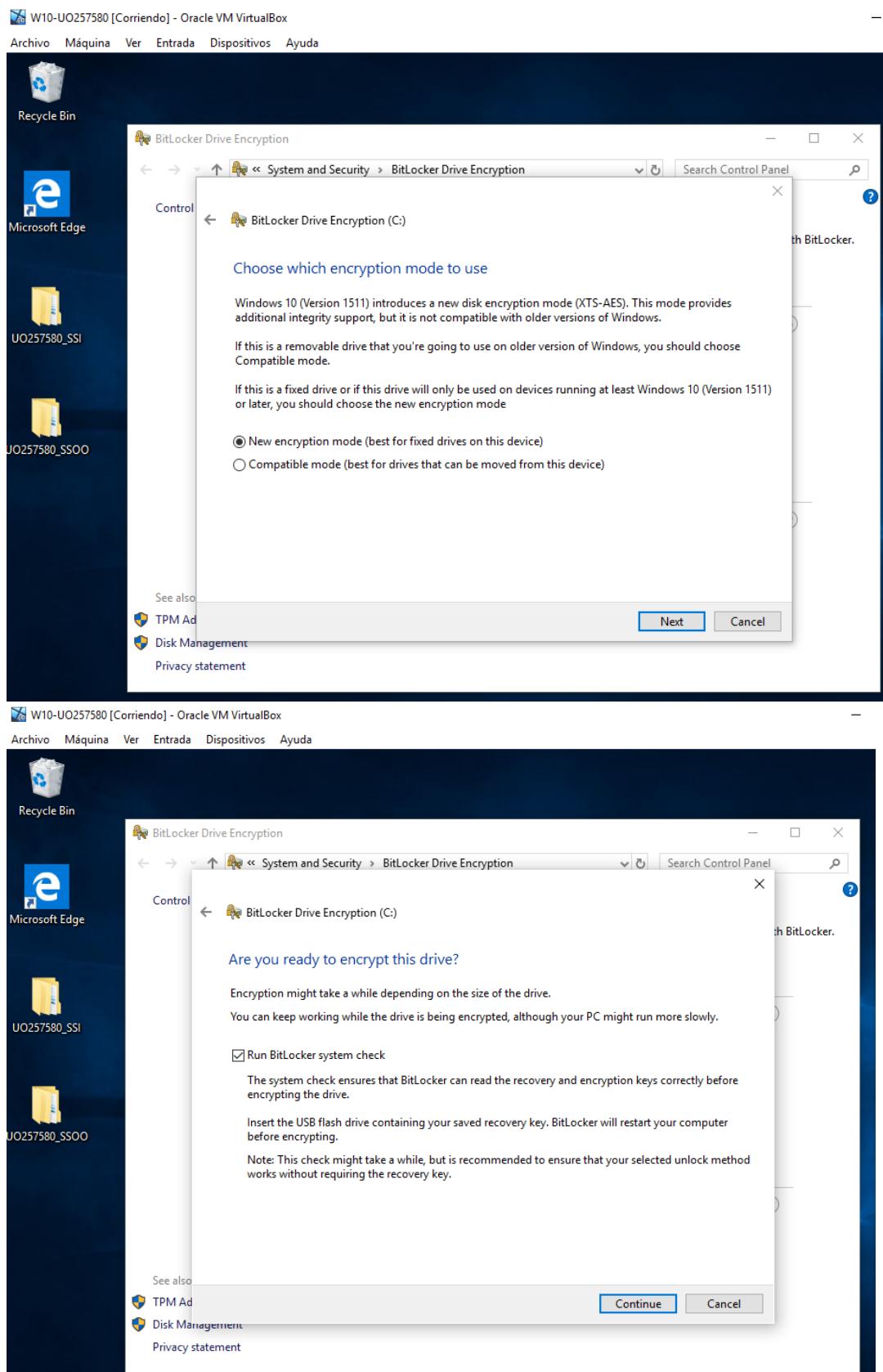


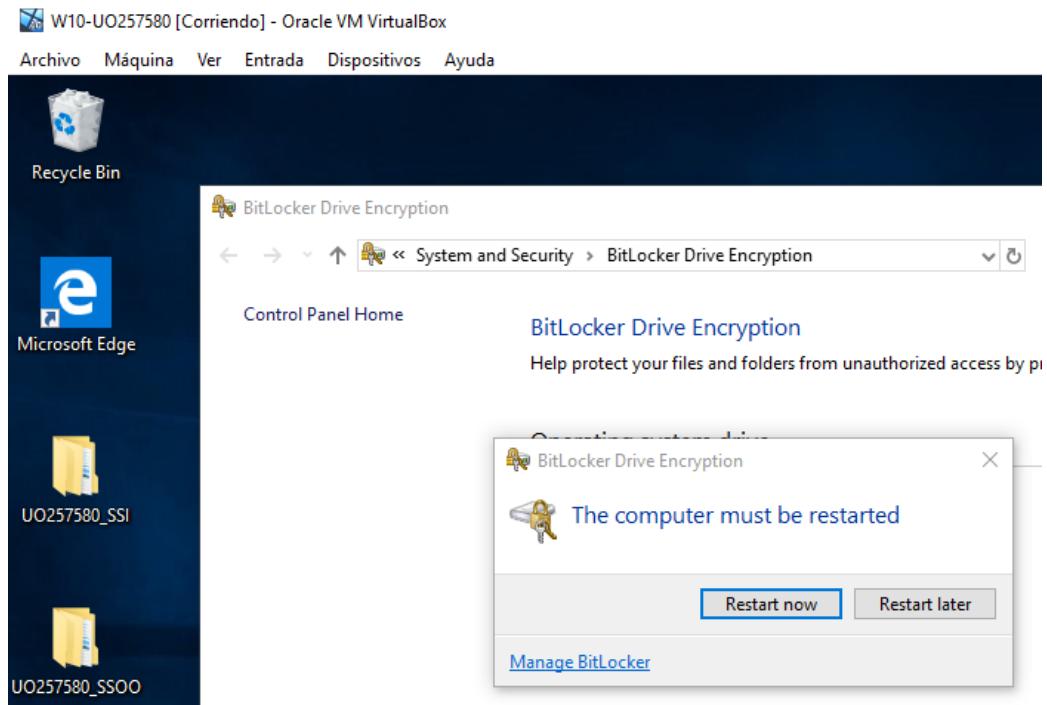


- 5) Imprimimos la clave en pdf o la guardamos en una unidad extraíble y no encriptada. Le indicamos que cifre la unidad ENTERA y que use el modo de cifrado nuevo. Nos aseguramos que este seleccionado la opción Ejecutar la comprobación del sistema de BitLocker. Nos solicita el reinicio.

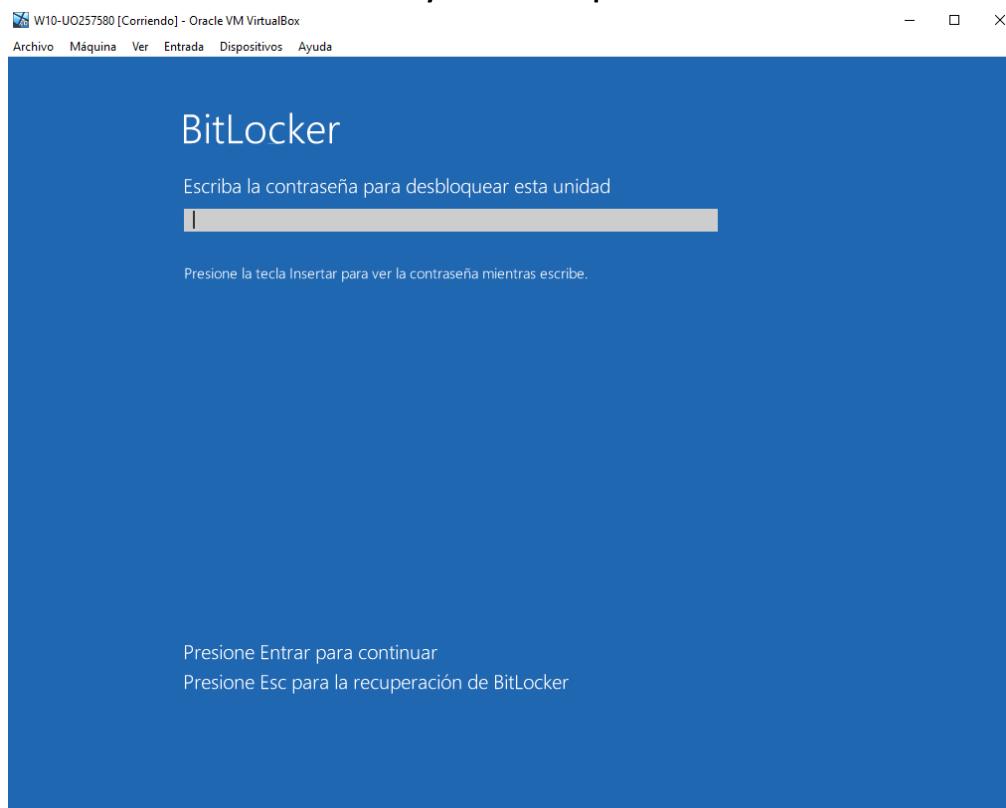


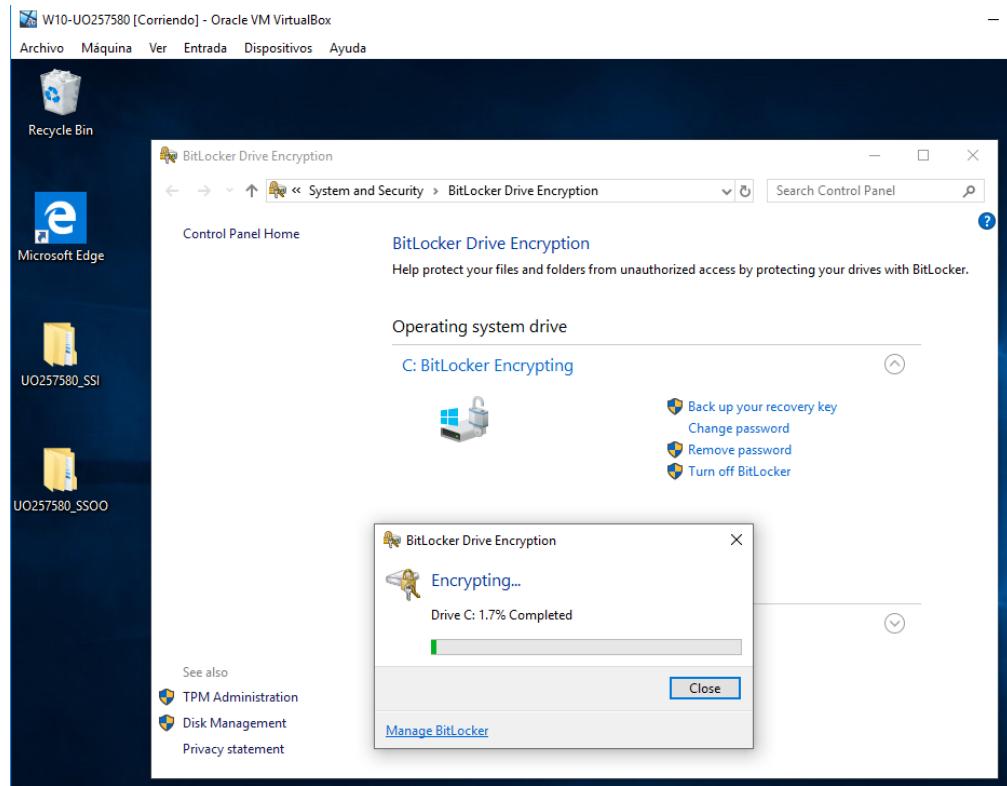
Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS



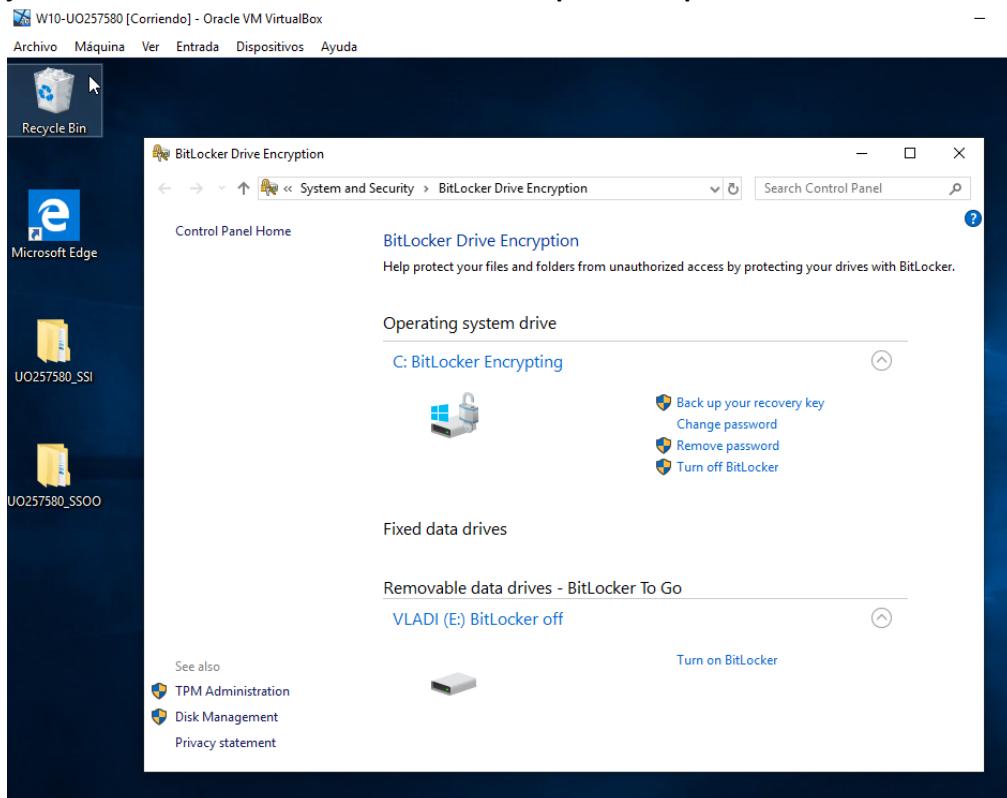


- 6) Al reiniciar nos solicitará la contraseña que introducimos anteriormente. ¡OJO! en este primer reinicio después de activar BitLocker no podemos ejecutar la recuperación de BitLocker porque todavía no hay nada cifrado. Así que, si le damos a Escape, perderemos la activación BitLocker y tendremos que volver a realizarla.

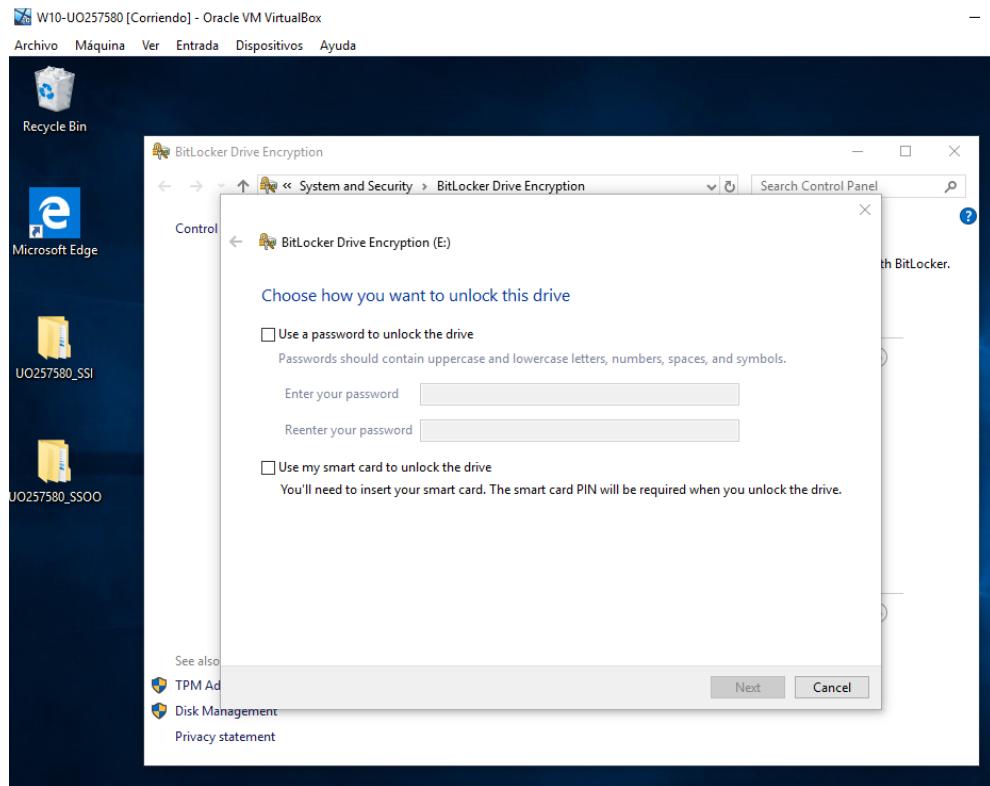




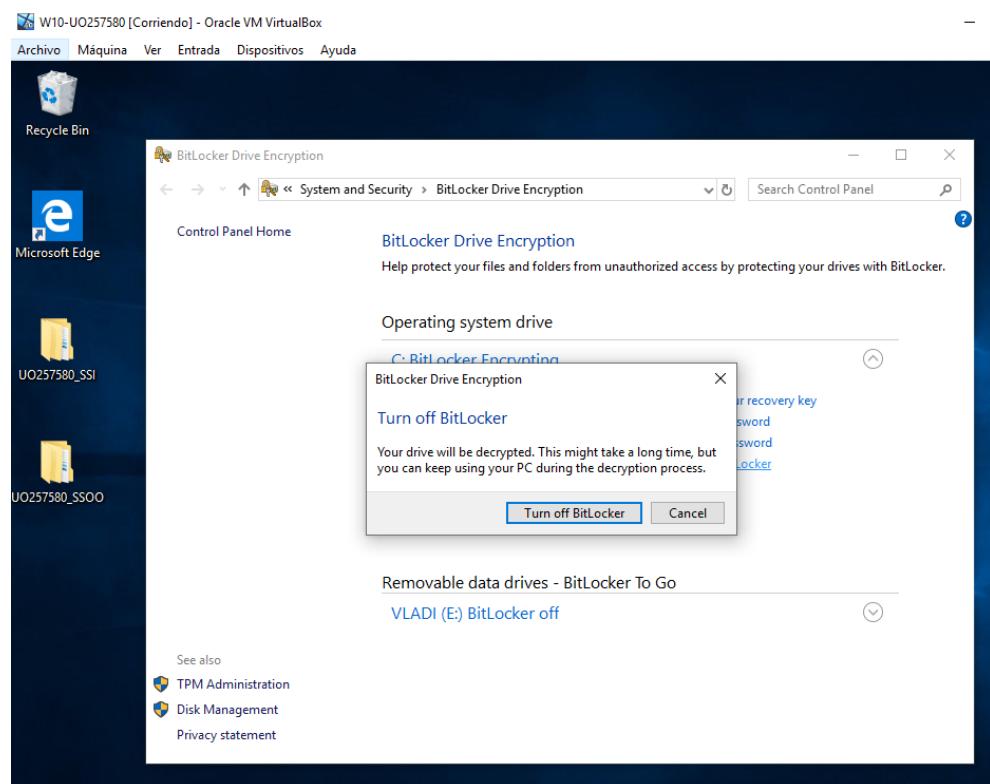
- 7) Ejecuta Administrar BitLocker y explora las opciones que nos proporciona. ¿Se podría ejecutar BitLocker con unidades extraíbles? Explora esta posibilidad.



Sí, nos da la posibilidad de activar BitLocker en una unidad extraíble como la unidad de USB que vemos en la captura.



8) Desactiva BitLocker para tener mayor agilidad a la hora de realizar las siguientes prácticas.



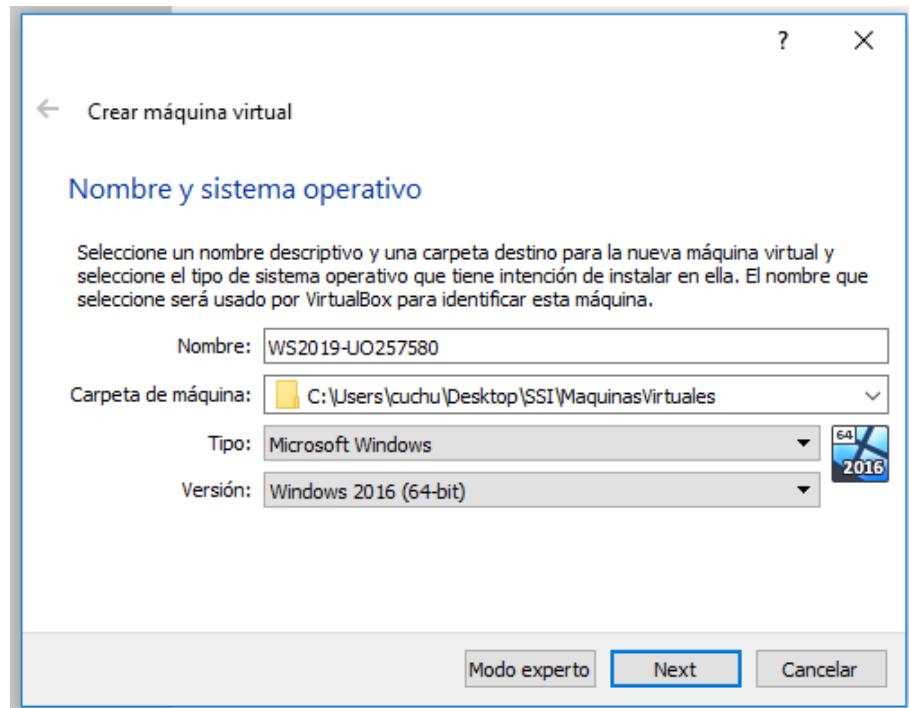
Directorio Activo

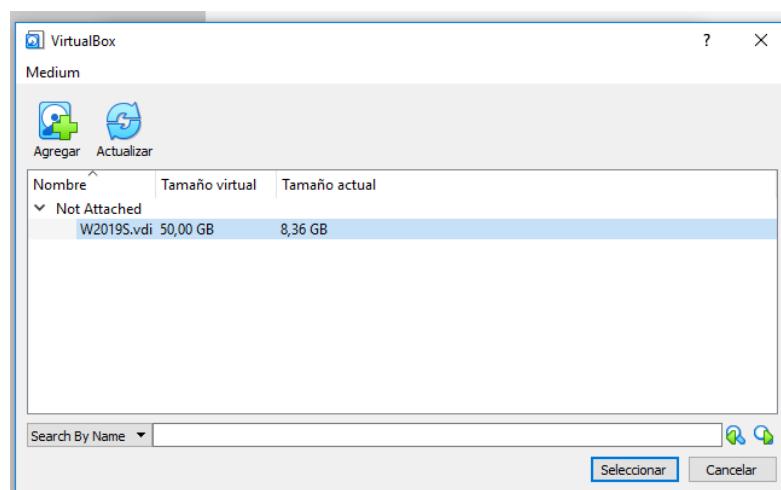
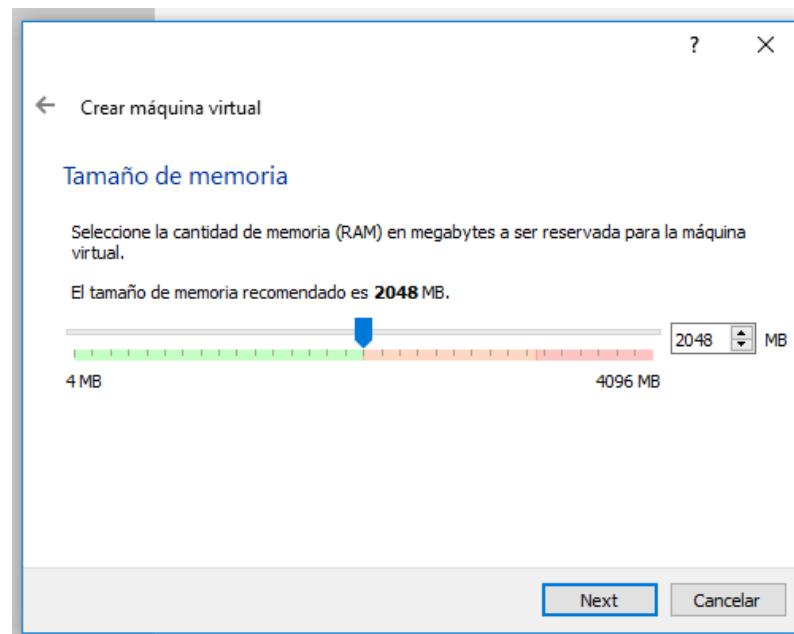
Preparación del entorno

Preparación del entorno

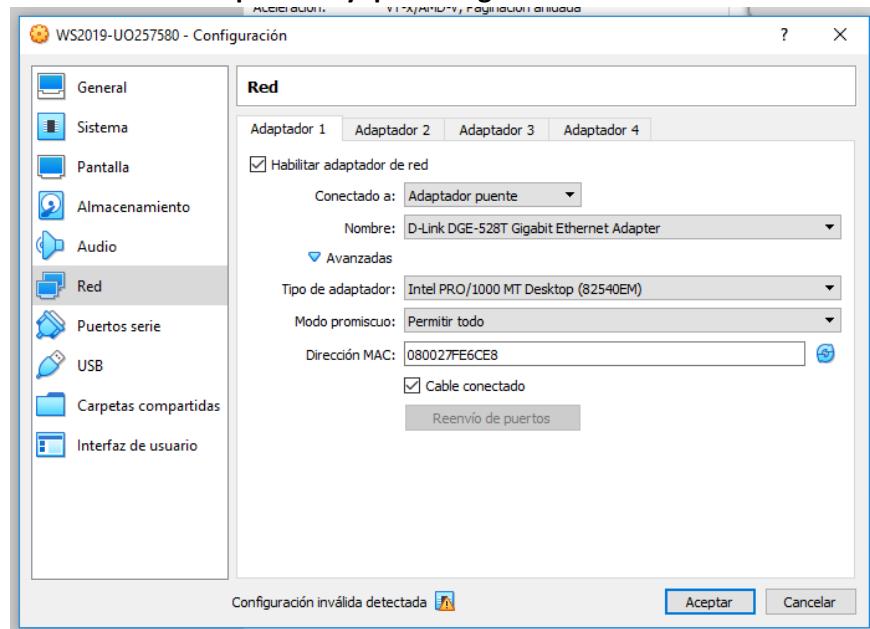
1) Se dispone de dos máquinas virtuales

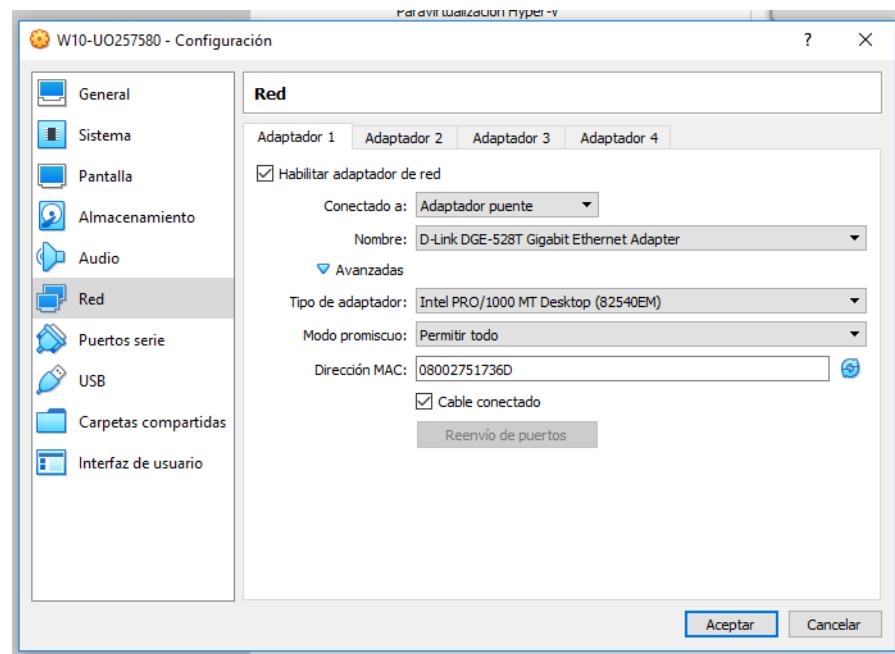
- **CLIENTE:** Windows 10, que utilizamos en la práctica anterior.
- **SERVIDOR:** Windows Server 2019, que se puede descargar del campus virtual, en Material auxiliar de clase: Windows Server 2019:
 - **Nombre:** WS2019-UOxxxxx, donde xxxx es vuestro UO.
 - **Tipo:** Microsoft Windows 2016.
 - **Versión:** 64 bits.
 - **Memoria:** 2GB.
 - Disco duro: Usar uno existente y seleccionamos el archivo “W2019S.vdi” de la carpeta donde hemos descomprimido la imagen descargada del campus Windows Server 2019.





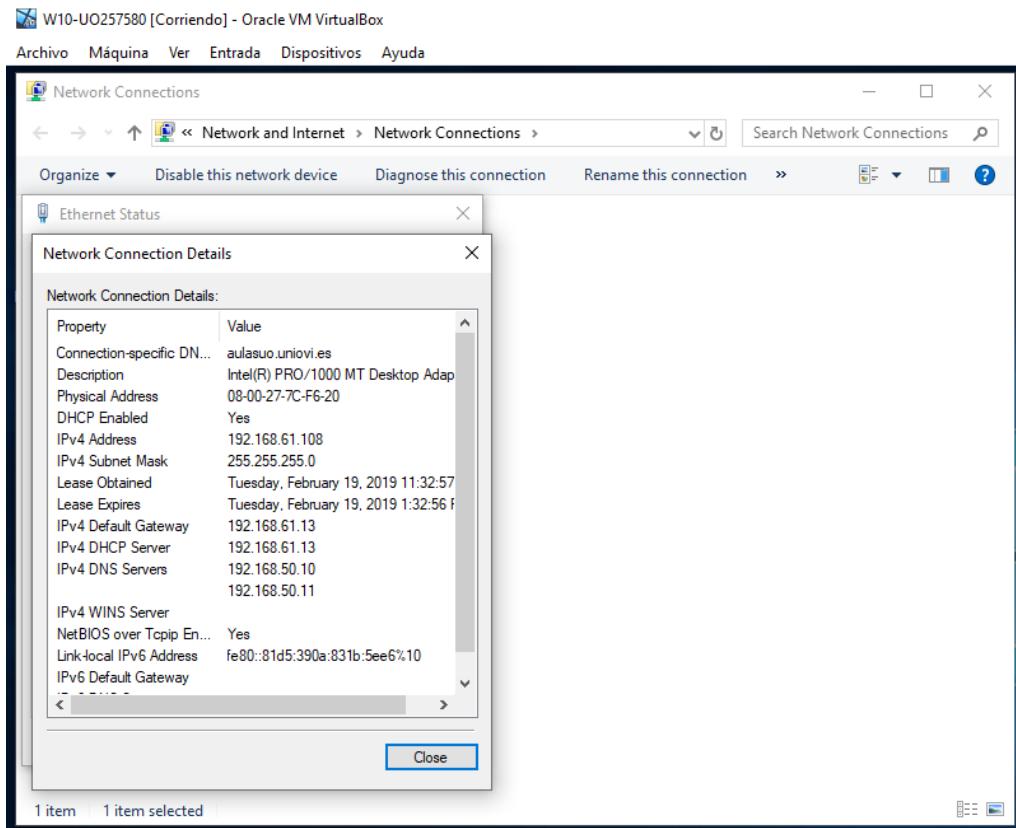
2) Antes de arrancar las máquinas hay que configurar la red:



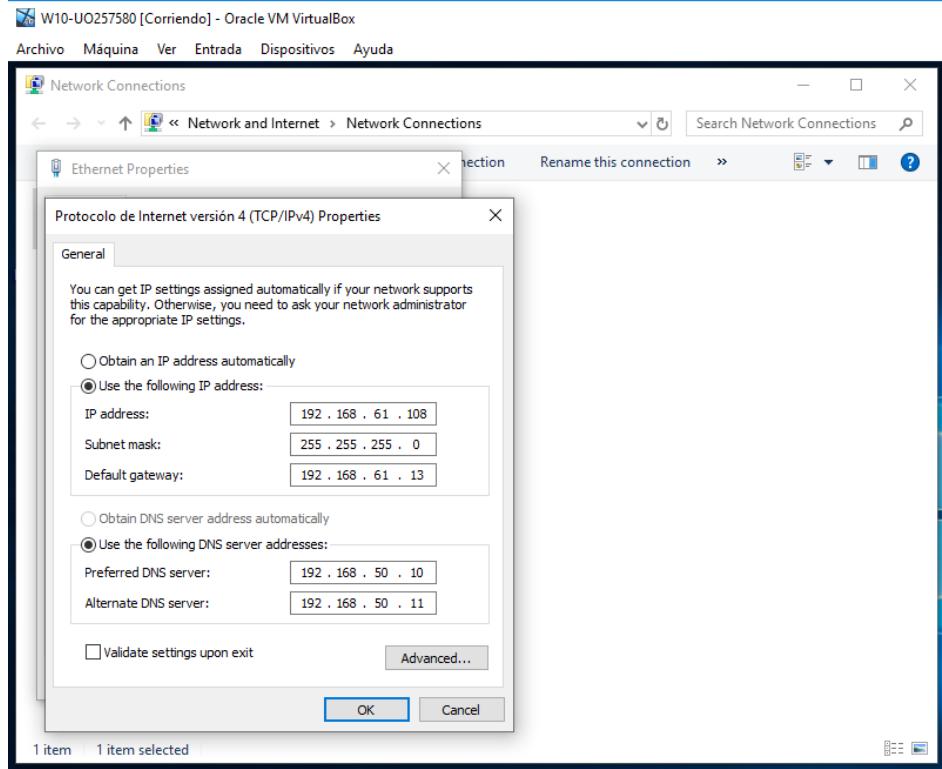


3) En primer lugar, arranca Windows 10 y toma nota de la configuración de red (IP, máscara, Gateway y DNS)

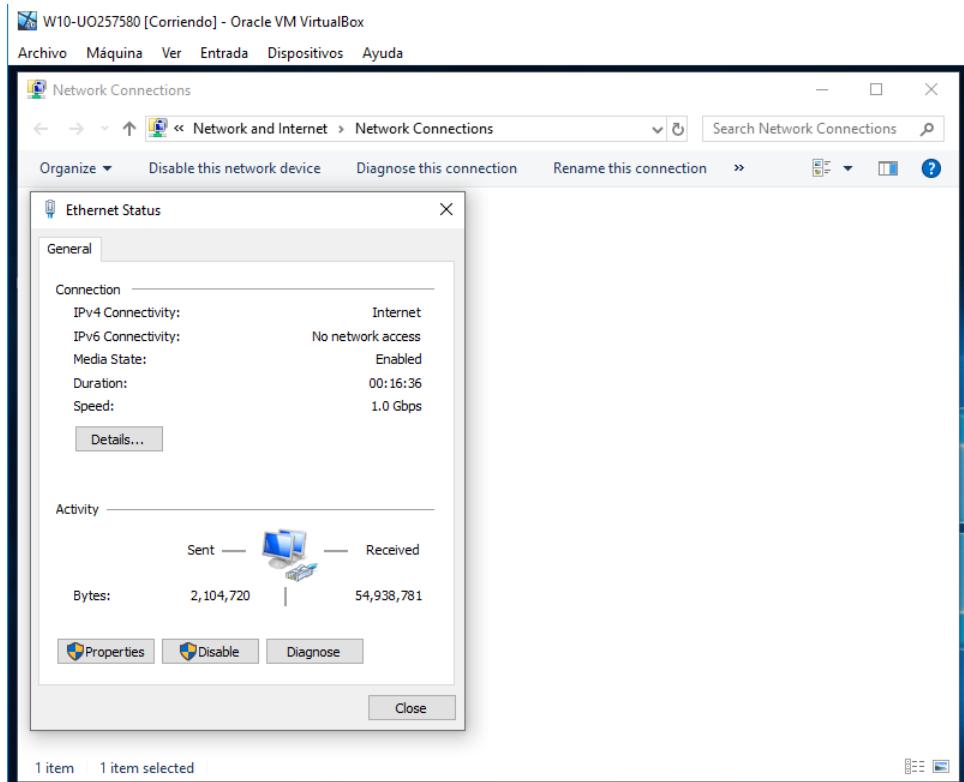
- Vete a "Menú inicio, Panel de control, Centro de Redes y Recursos Compartidos, Cambiar Configuración del Adaptador, Conexión de área local, botón derecho, estado, detalles" y toma nota de la IP, máscara de subred, la puerta de enlace y el servidor DNS.



- 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".

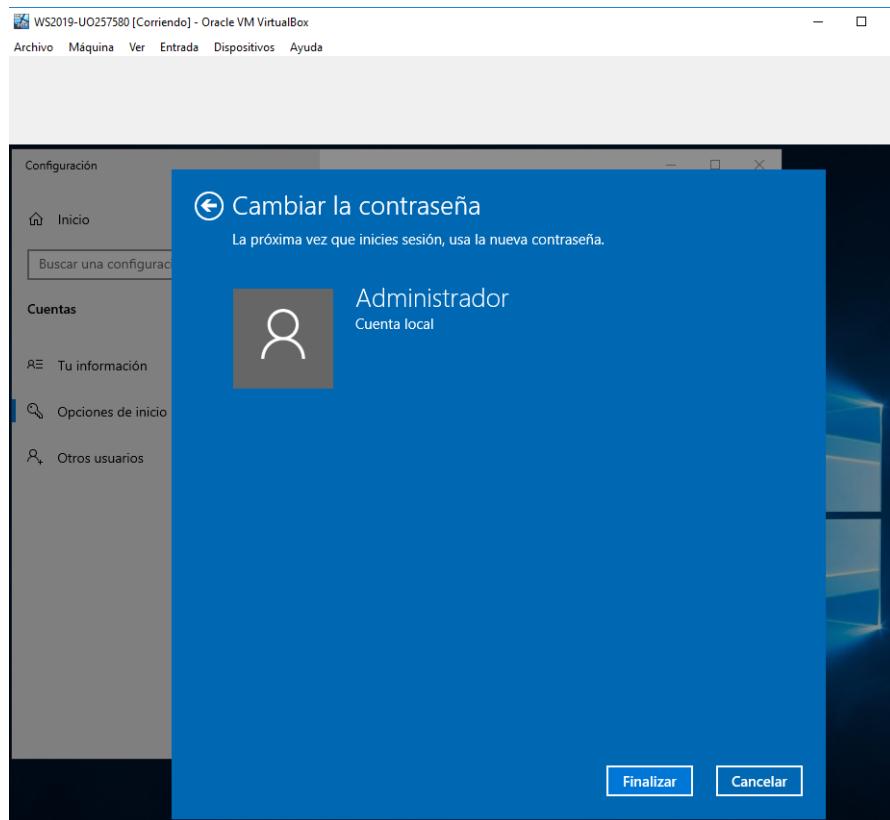
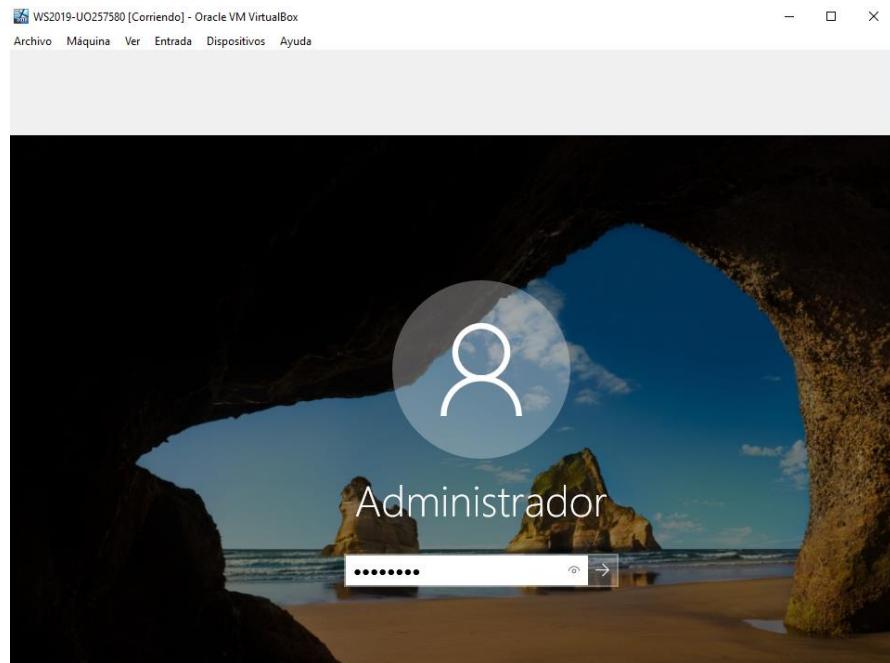


- Comprobar que tenemos conexión a internet.



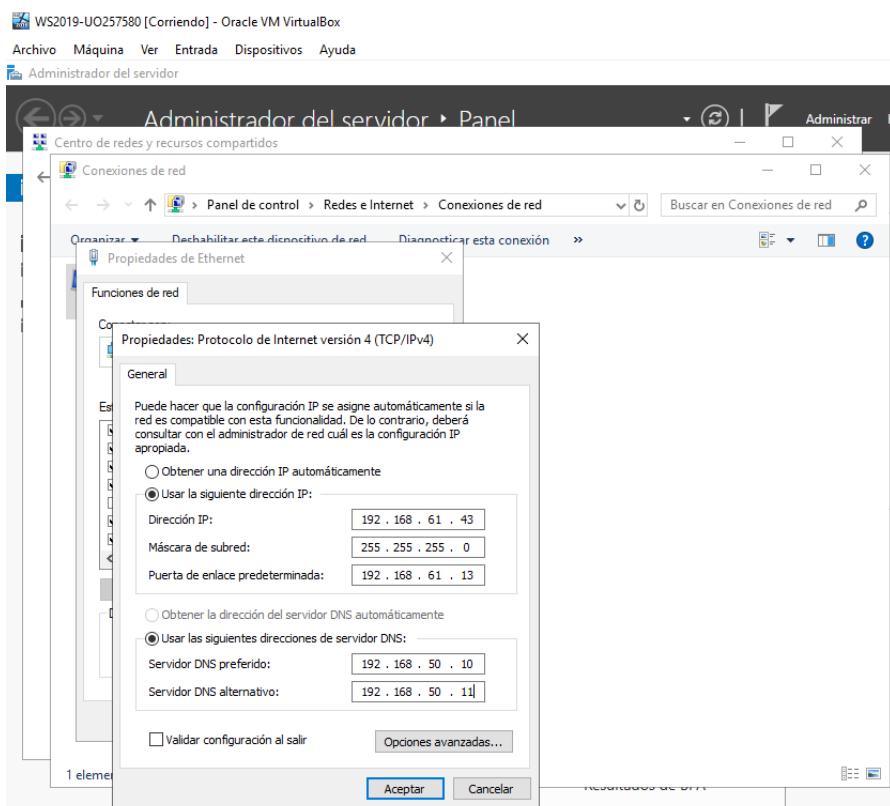
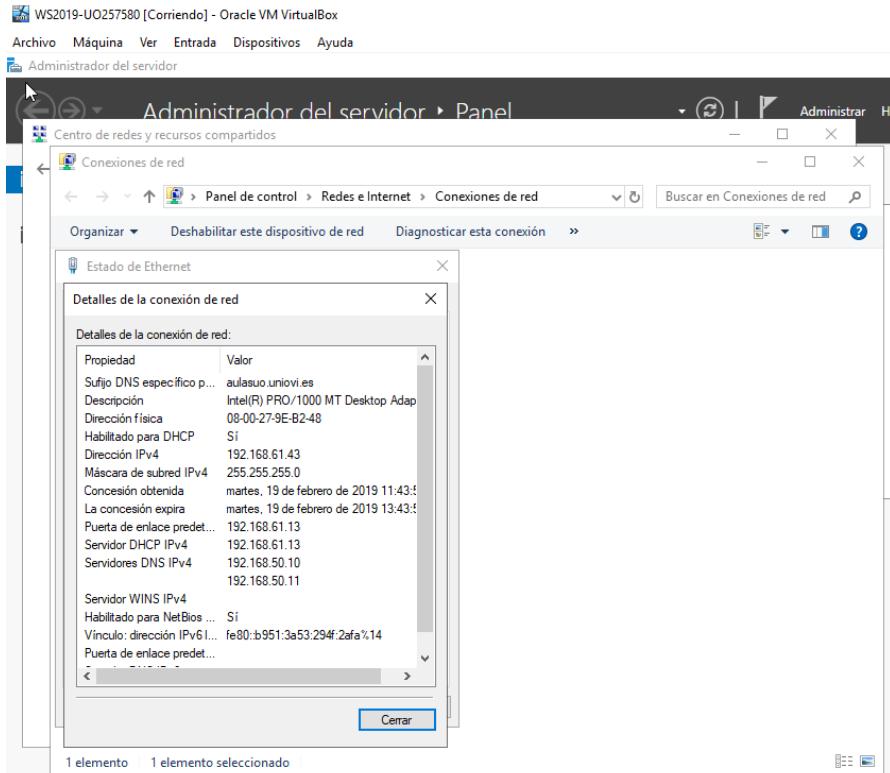
4) Configuración de Windows Server 2019.

- La máquina virtual tiene una cuenta “Administrador” con contraseña “ssi_2019”. Cambia la contraseña por una que puedas recordar. La cuenta “administrador” es la que tiene todos los permisos de administración del servidor, NO OLVIDES LA CONTRASEÑA.

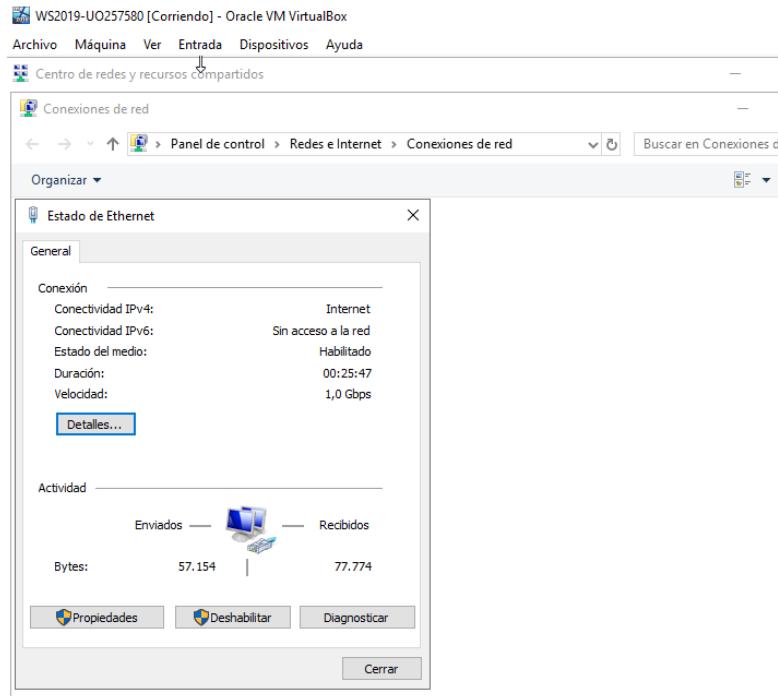


- **Configuración de red:**

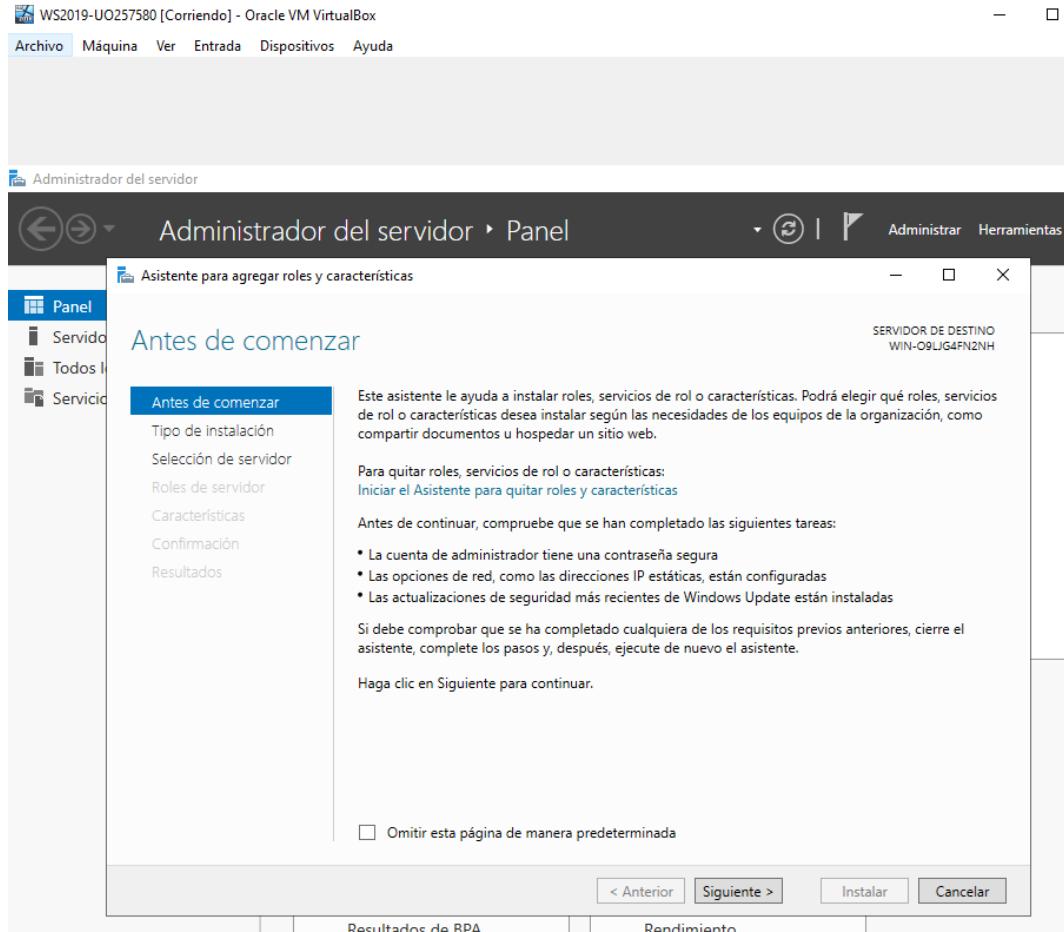
- Como hicimos con W7 anotamos los valores dinámicos de la configuración de red y asignamos esas propiedades como estáticas. Al estar en la misma red, lógicamente lo único que varía de la configuración del cliente W7 es la IP, el resto es igual.



○ Comprobar que se tiene conexión a Internet.

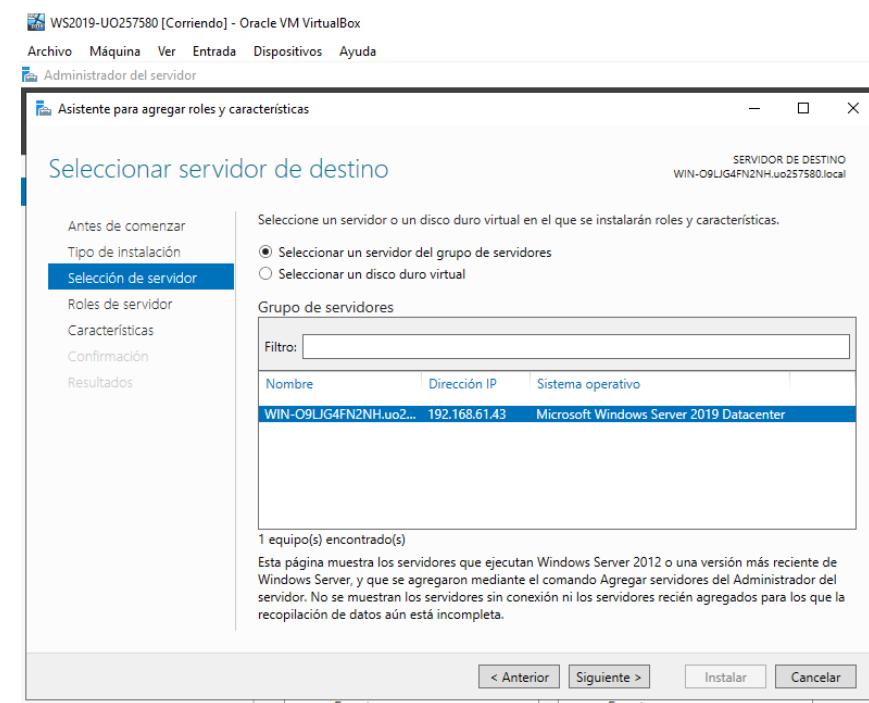
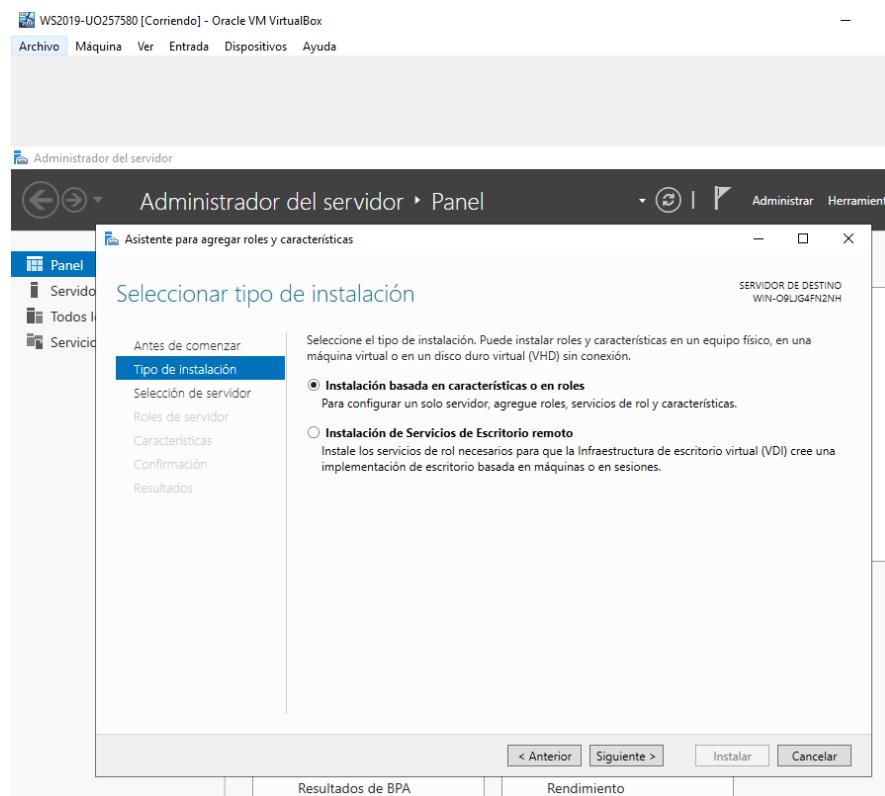


● En “Administrador del servidor” pinchar en “Aregar roles y características”

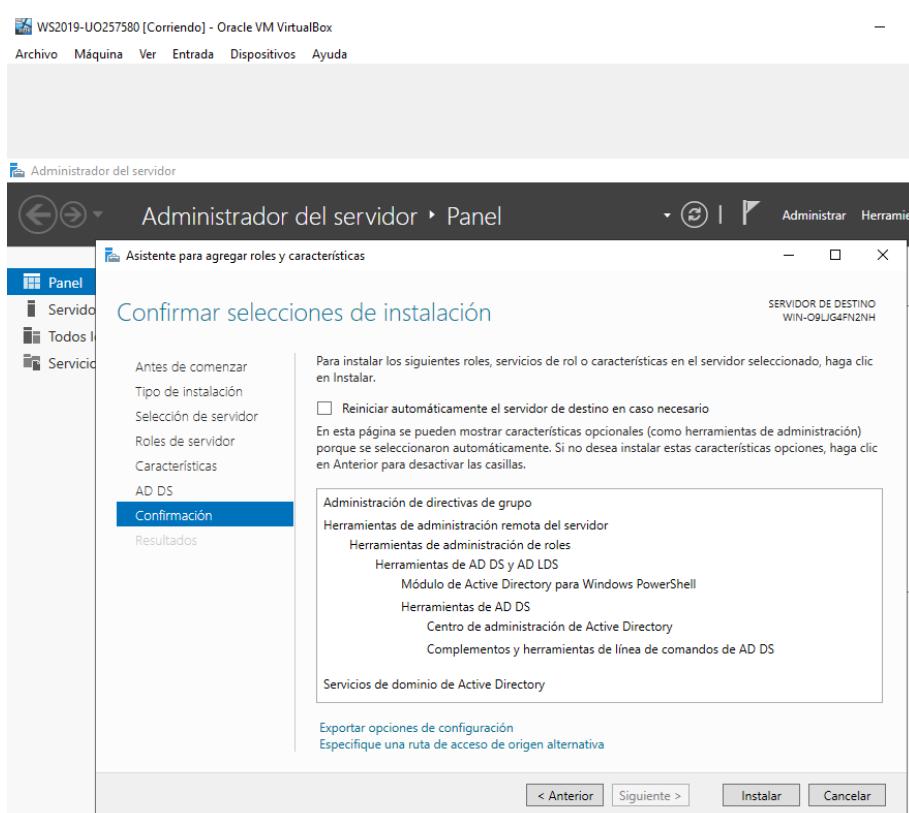
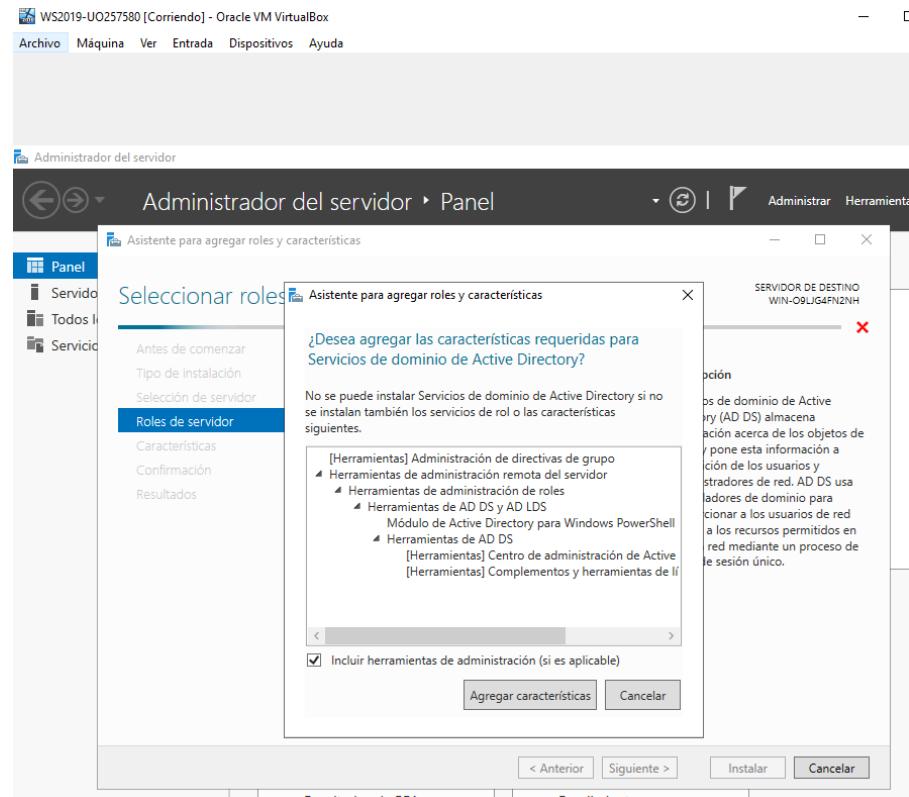


- En el asistente:

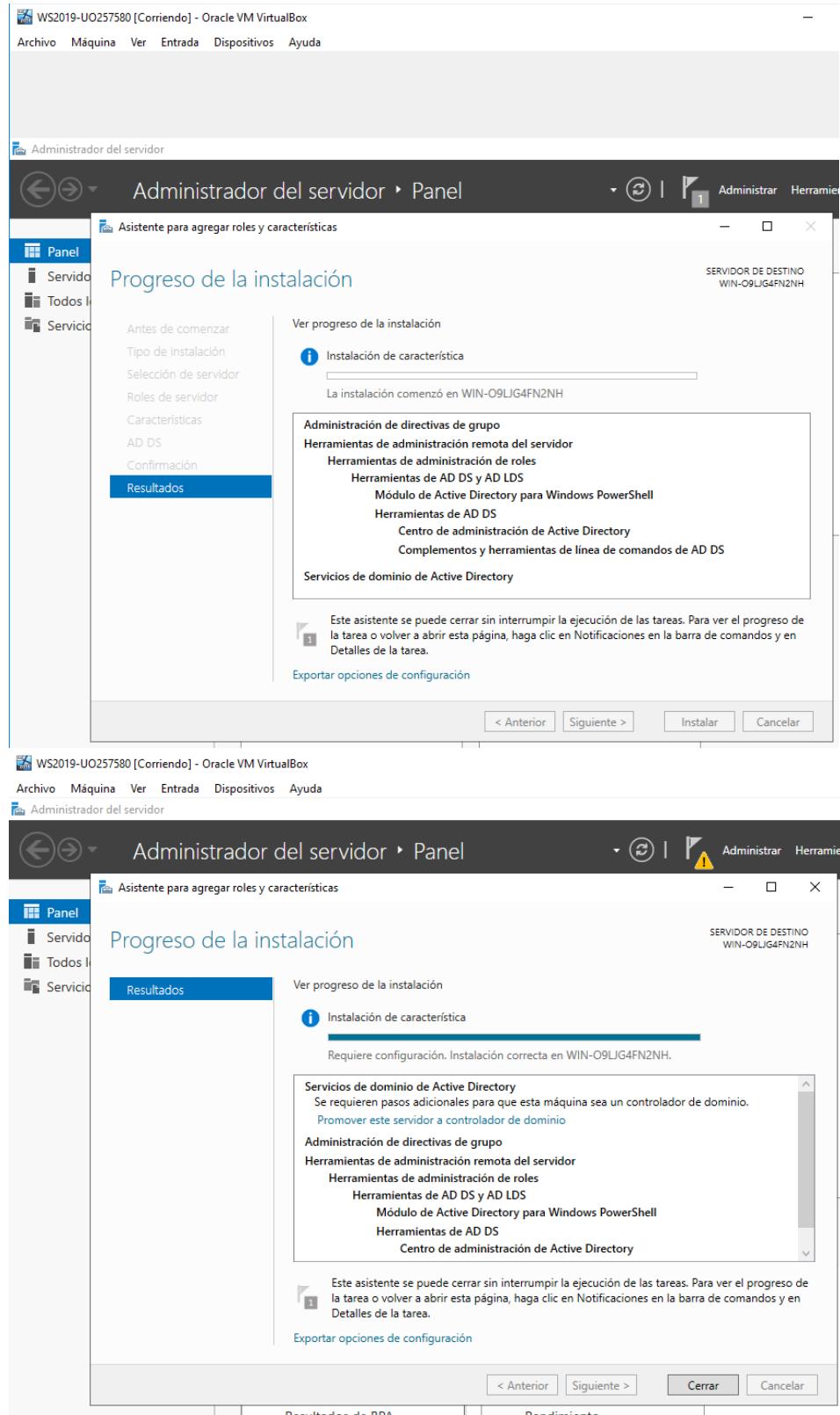
- Seleccionar “Instalación basada en características o roles”-“Siguiente” y seleccionamos nuestro servidor-“Siguiente”.



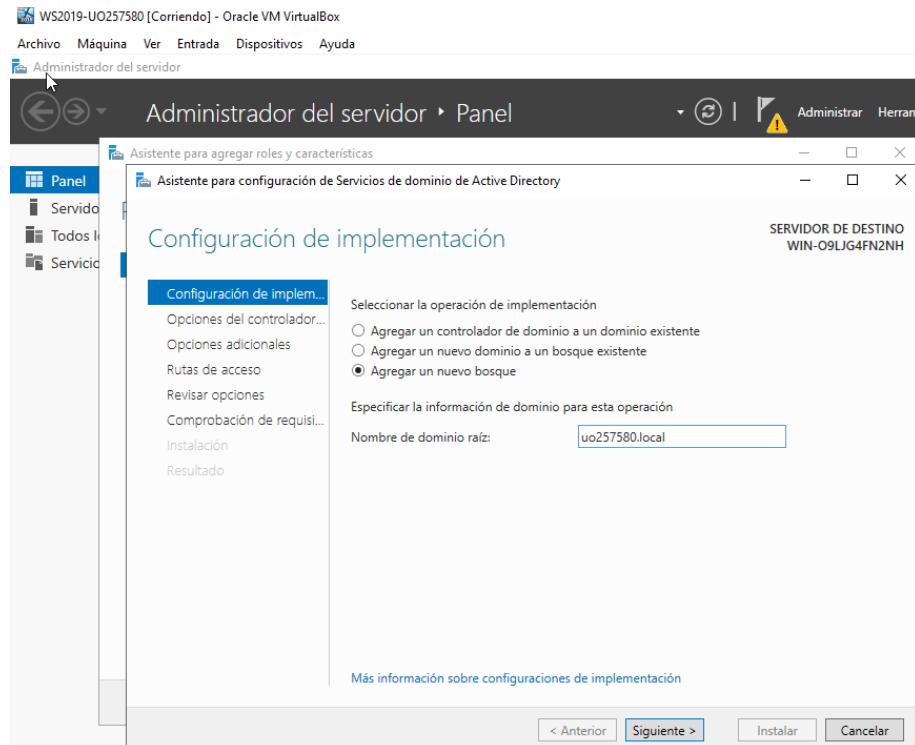
- **Seleccionar “Servicios de Dominio de Active Directory” y Agregar características. En la siguiente ventana dejamos todo lo seleccionado por defecto y le damos a “Siguiente” hasta que nos de la opción de “Instalar”. NO CERRAMOS LA VENTANA.**



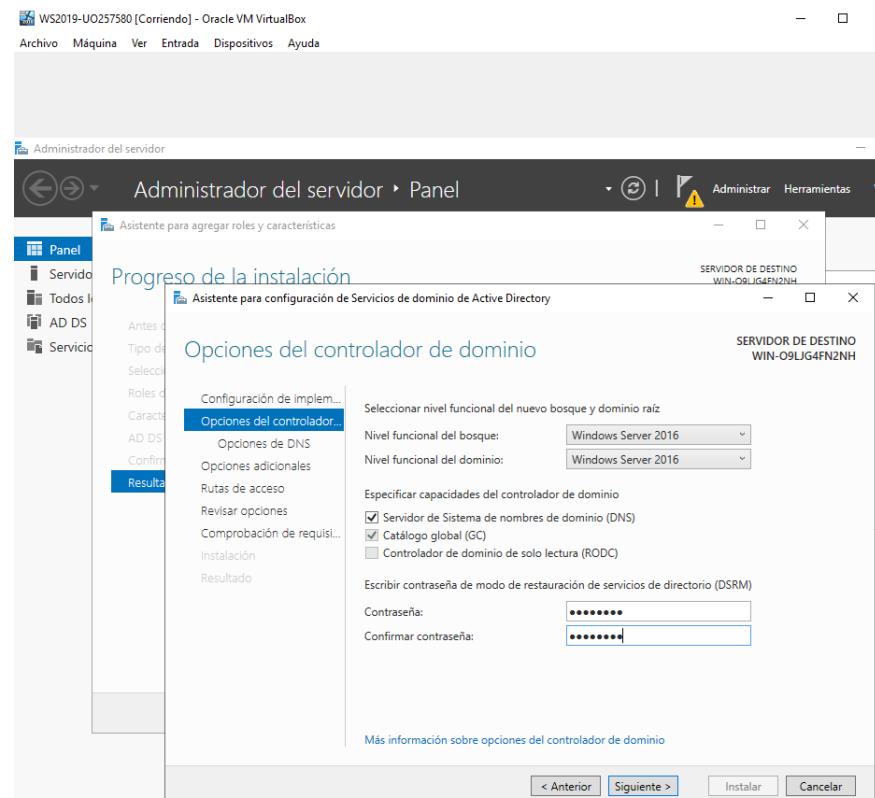
- Tras instalar una serie de componentes ahora tenemos que promover nuestro servidor a controlador de dominio. Pinchamos en el enlace que nos lo permite: “Promover este servidor a controlador de dominio”



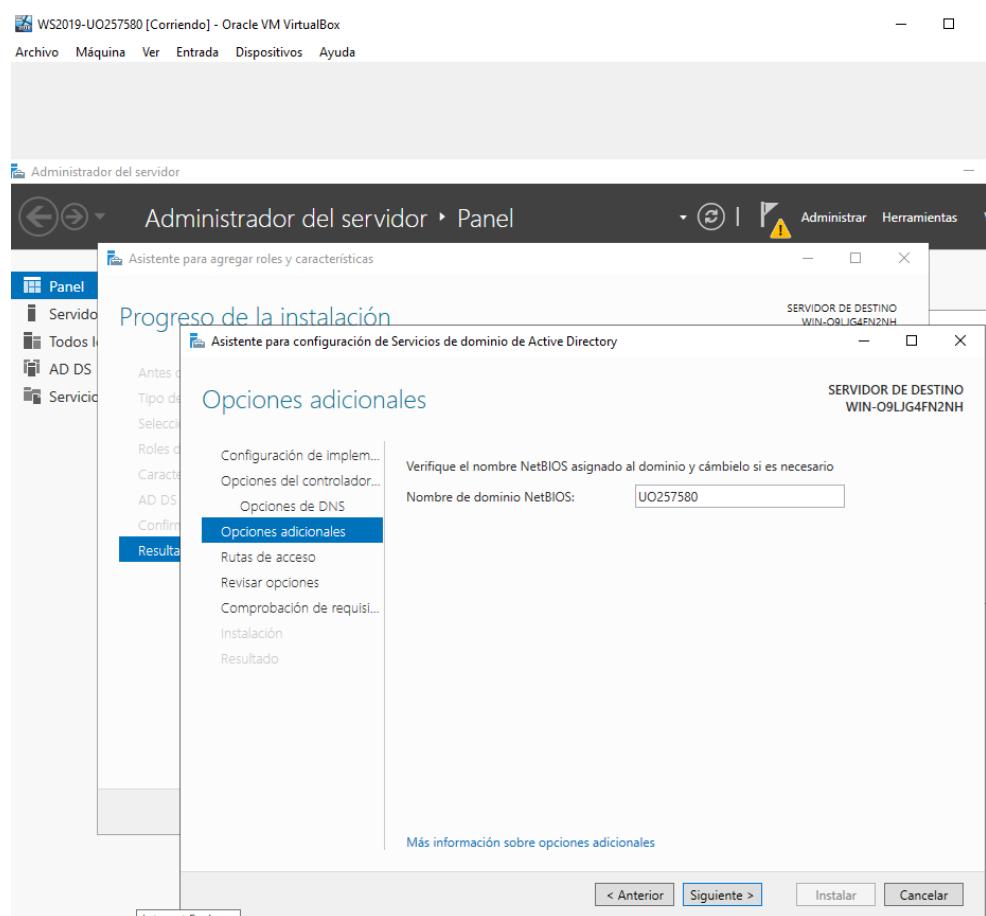
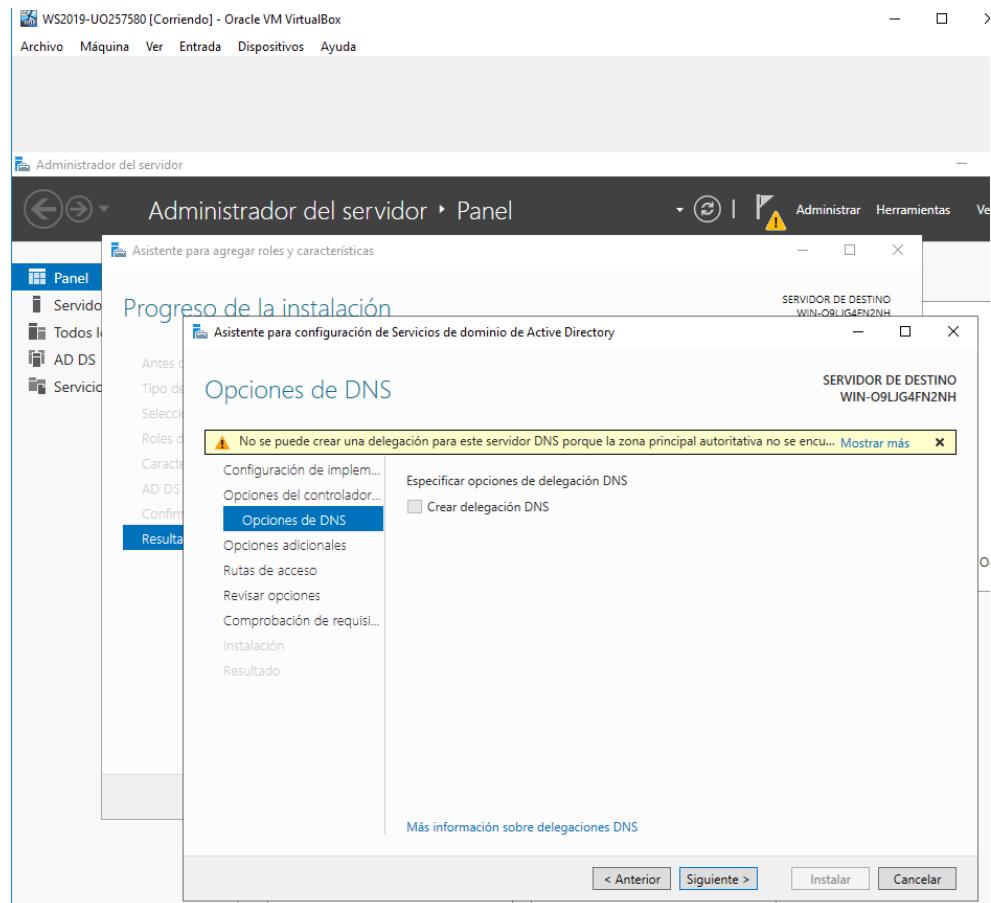
- Seleccionamos Agregar un bosque nuevo y como nombre FQDN ponemos: **uoXXXX.local.(siendo uoXXXX tu UO)**



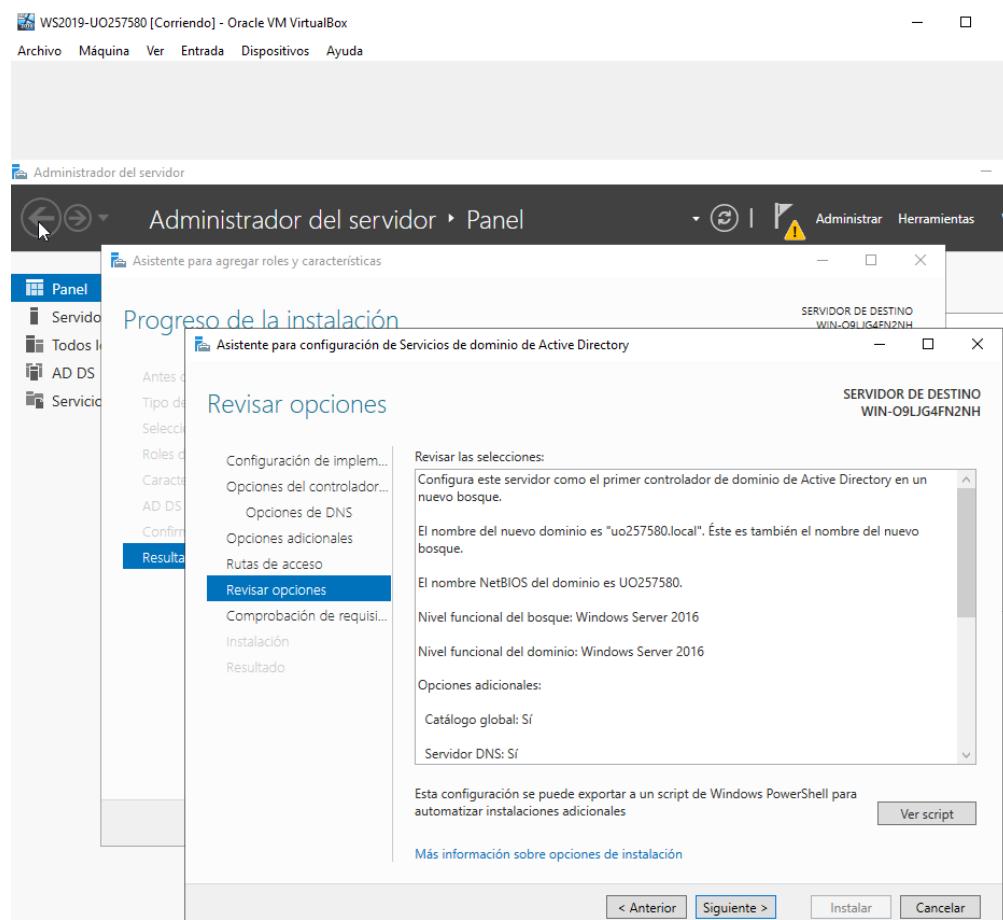
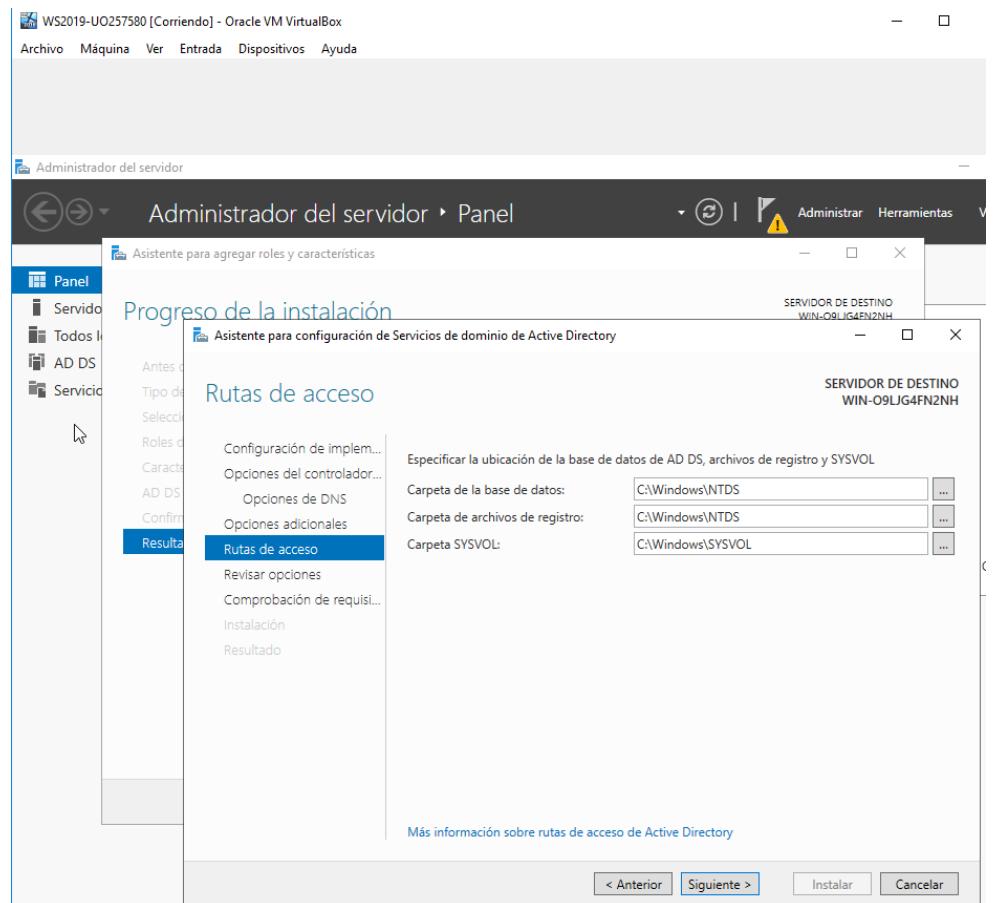
- Introducimos una contraseña que cumpla con los requisitos de complejidad (ssi_2019 por ejemplo) y vamos aceptando opciones por defecto hasta que nos de una opción de instalar (omitimos la delegación de DNS).

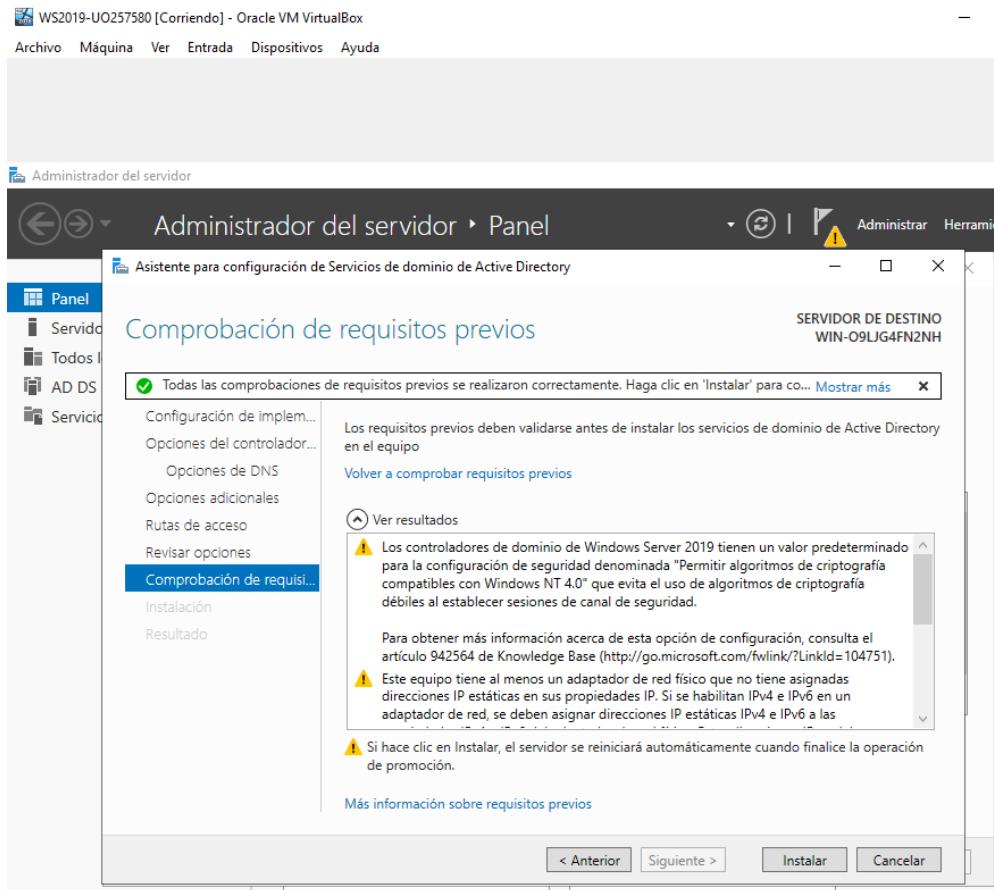


Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

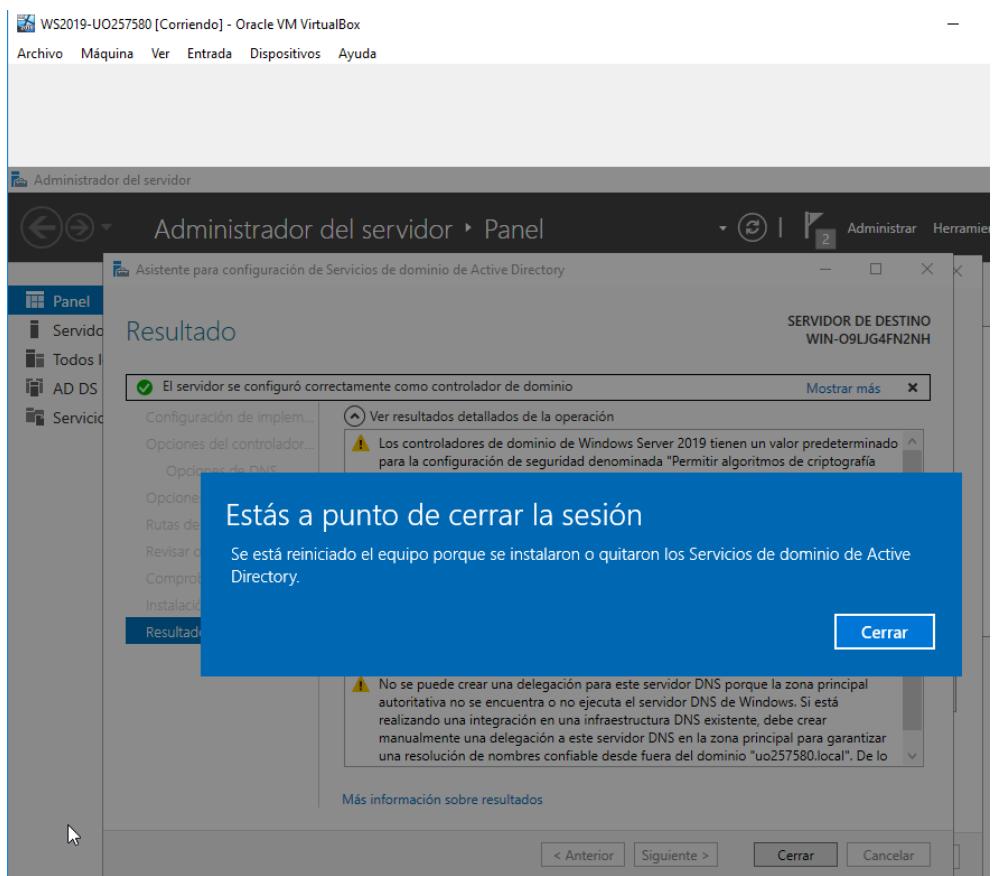


Vladislav Stelmakh – UO257580 / X8226649D
SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS



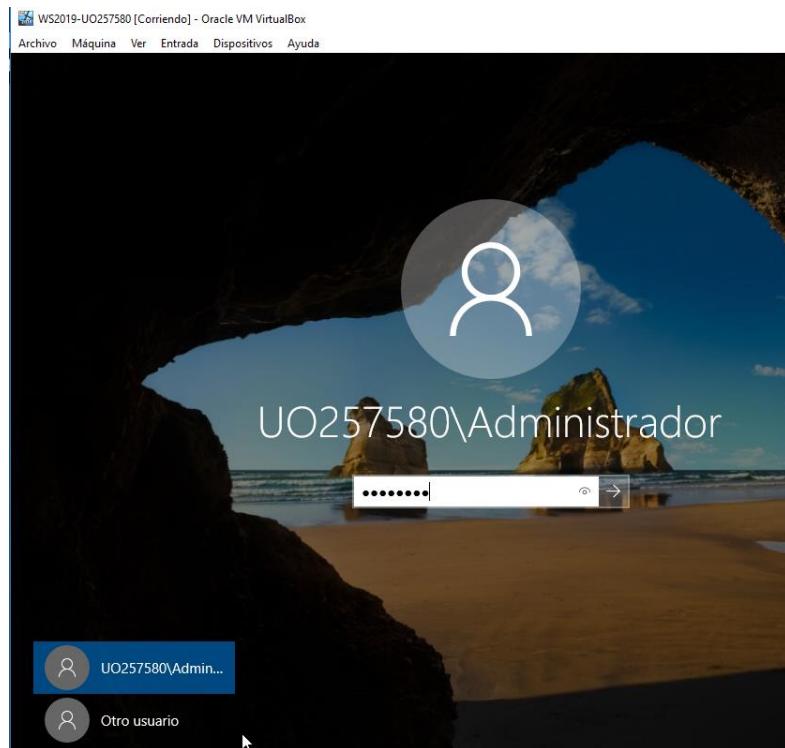


○ Al finalizar pide que reiniciemos y lo hacemos.

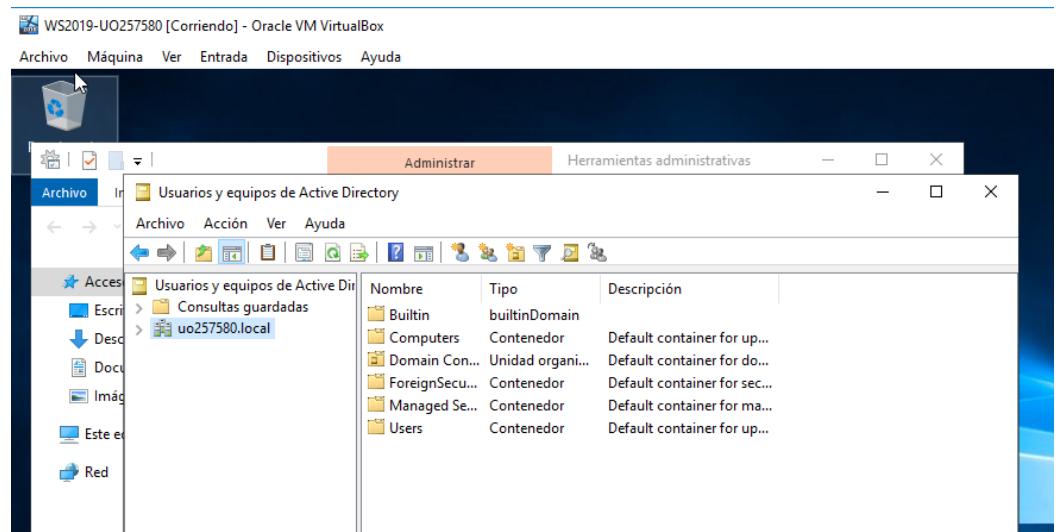


- Una vez reiniciado, nuestro servidor se habrá convertido en Controlador de Dominio:

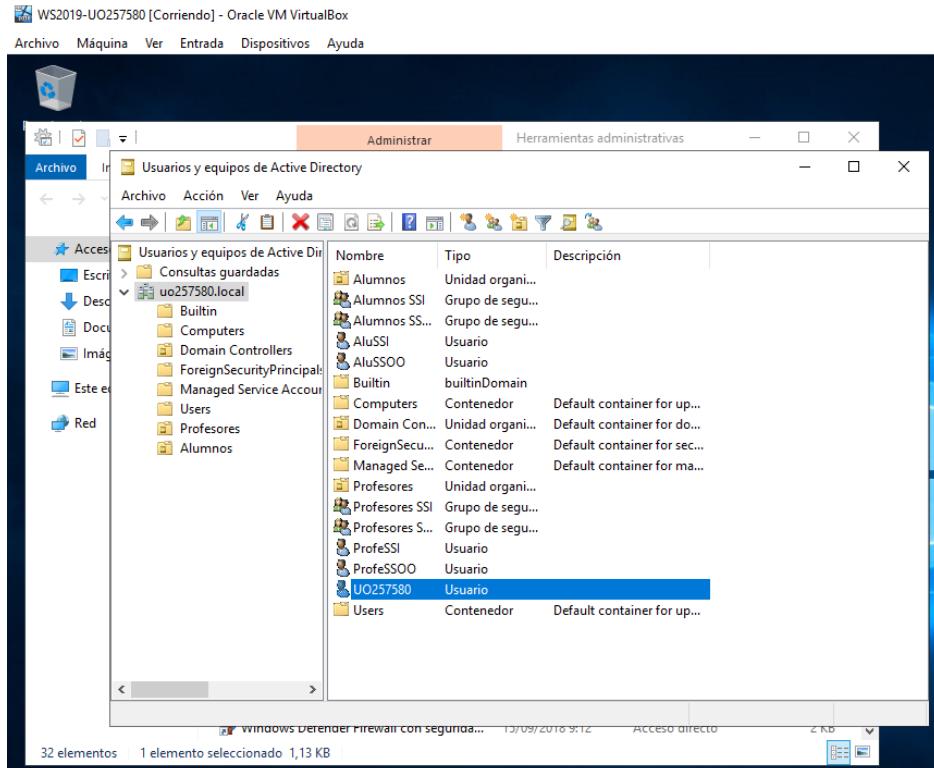
- Iniciar sesión con la cuenta Administrador.



- En "Menú inicio, Herramientas administrativas, Usuarios y equipos de AD, UOXXXX.local (botón derecho)".

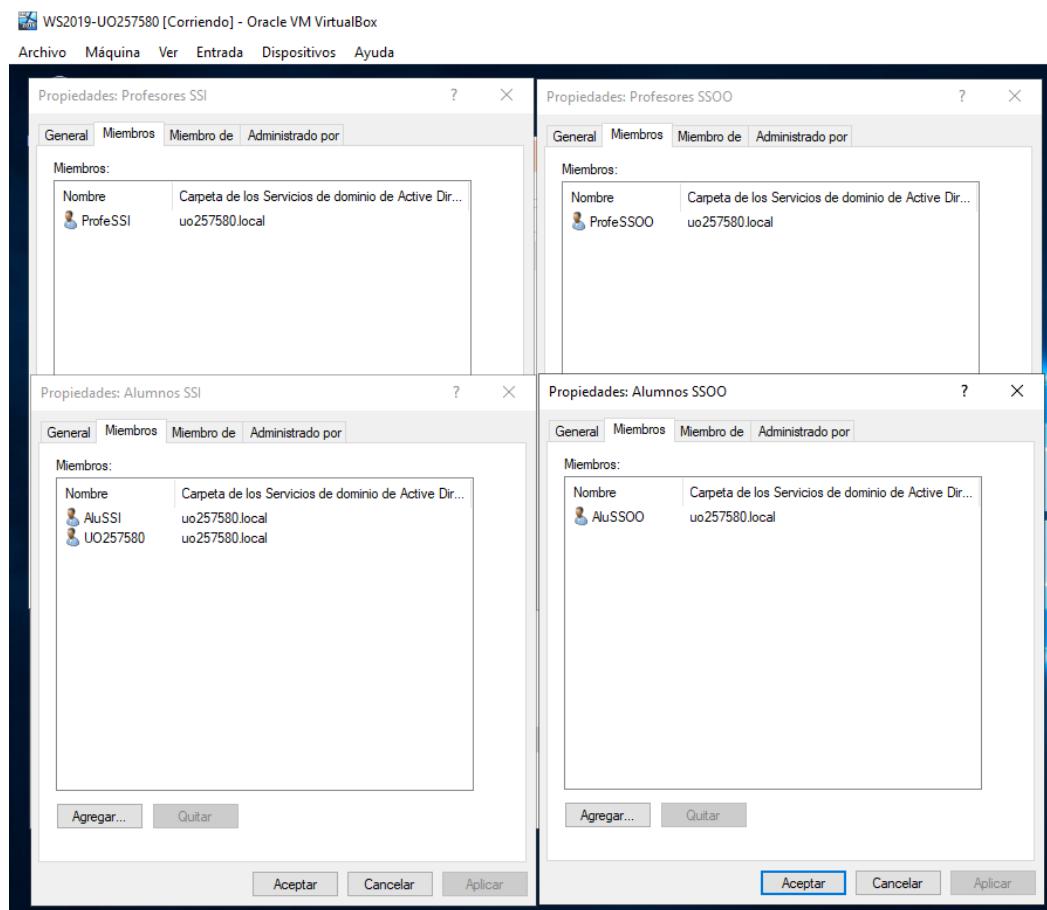


- **Crear las Unidades Organizativas (UO), grupos y usuarios siguientes:**
 - **Unidades Organizativas:**
 - Profesores.
 - Alumnos.



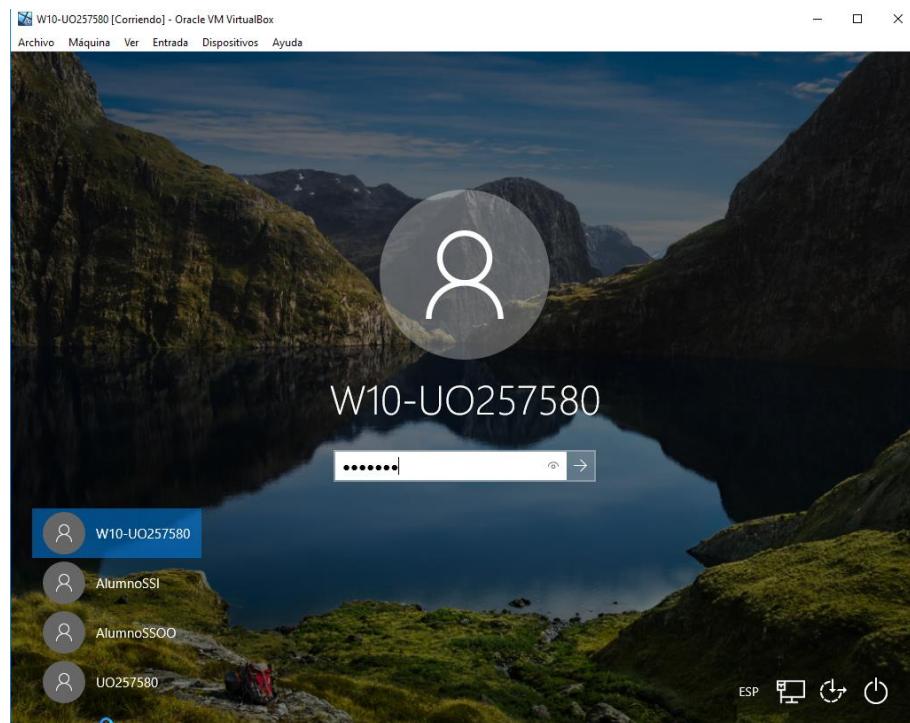
CORREGIDO MÁS ADELANTE EL PROBLEMA DE METER A ALUMNOS SSI/SSOO EN ALUMNOS Y PROFESORES SSI/SSOO EN PROFESORES.

- **Grupos de seguridad globales (en las respectivas UO):**
 - Profesores SSI
 - Profesores SSOO
 - Alumnos SSI
 - Alumnos SSOO
- **Usuarios (en las respectivas UO):**
 - ProfeSSI (miembro de grupo Profesores SSI).
 - ProfeSSOO (miembro de grupo Profesores SSOO).
 - AluSSI (miembro de grupo Alumnos SSI).
 - UOXXXXSSI (miembro de grupo Alumnos SSI).
 - AluSSOO (miembro de grupo Alumnos SSOO).
 - Poner a todos ellos contraseñas fáciles de recordar (por ejemplo "ssi_2019"), que nunca caducan y que no cambie al inicio de sesión.

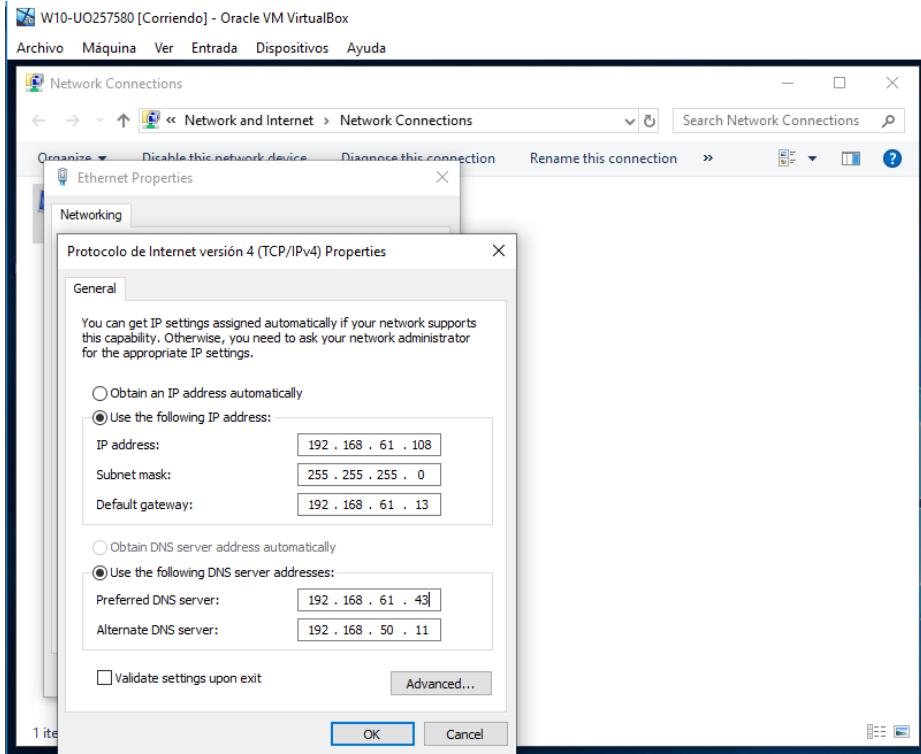


5) Configuración de Windows 10.

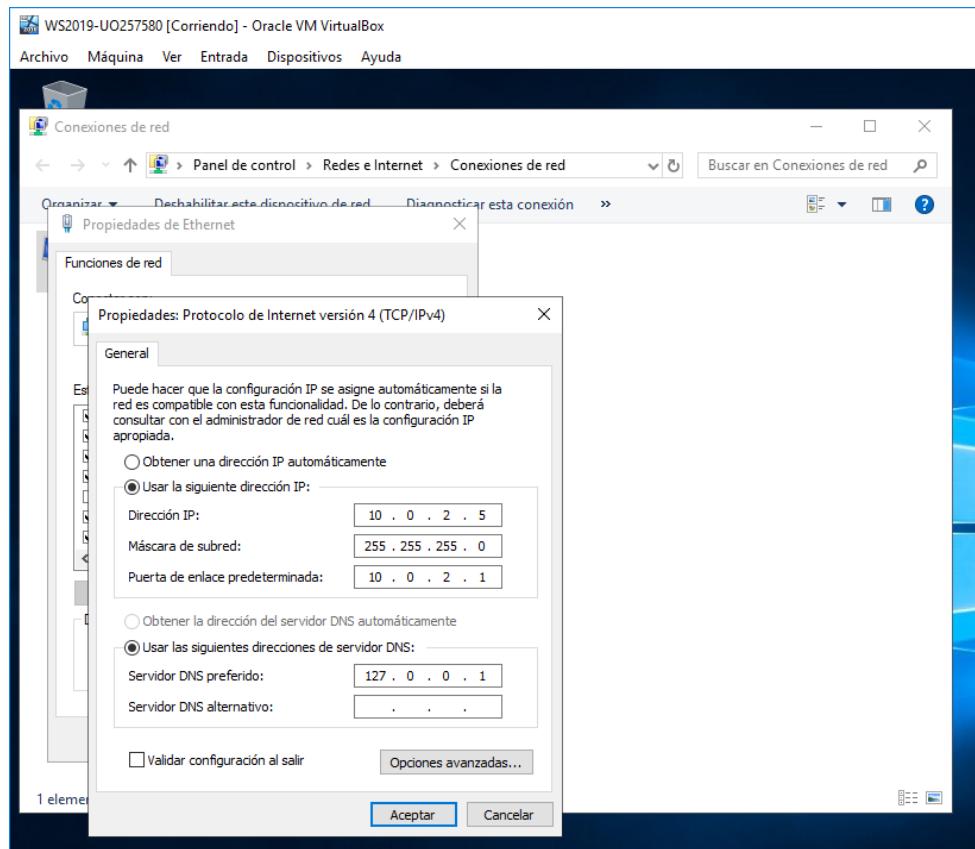
- Iniciar sesión como administrador.



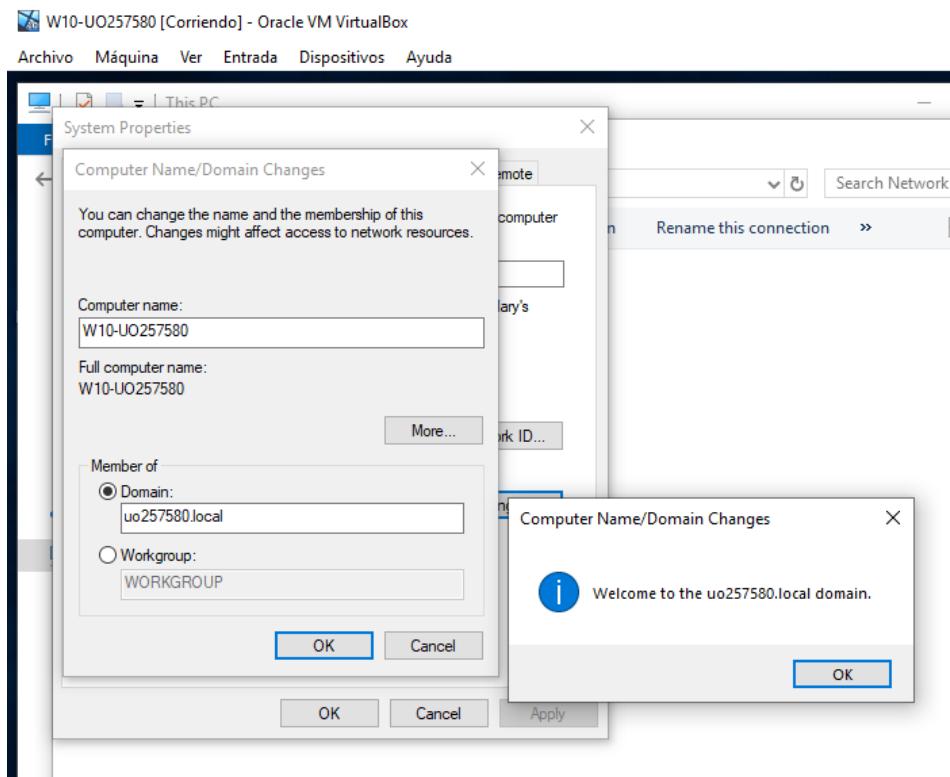
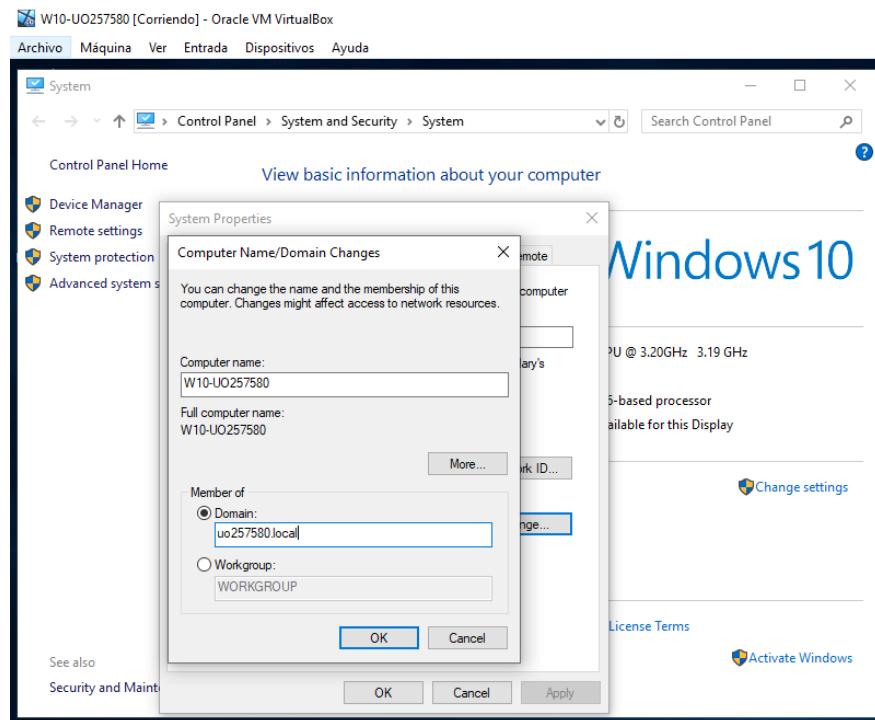
- Añadir en el W10 la IP del equipo W2019 como DNS. ("Menú inicio, Panel de control, Centro de Redes y Recursos Compartidos, Cambiar Configuración del Adaptador, Conexión de área local, botón derecho, propiedades, protocolo internet (TCP/IP), propiedades").



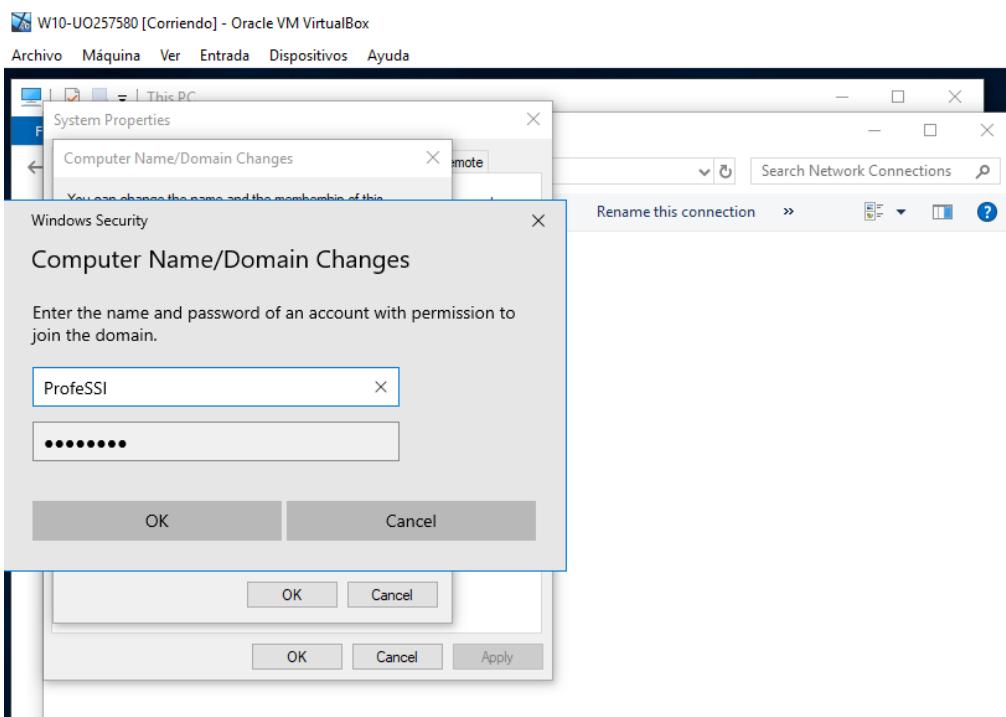
¡¡¡CORREGIDO MÁS ADELANTE!!!



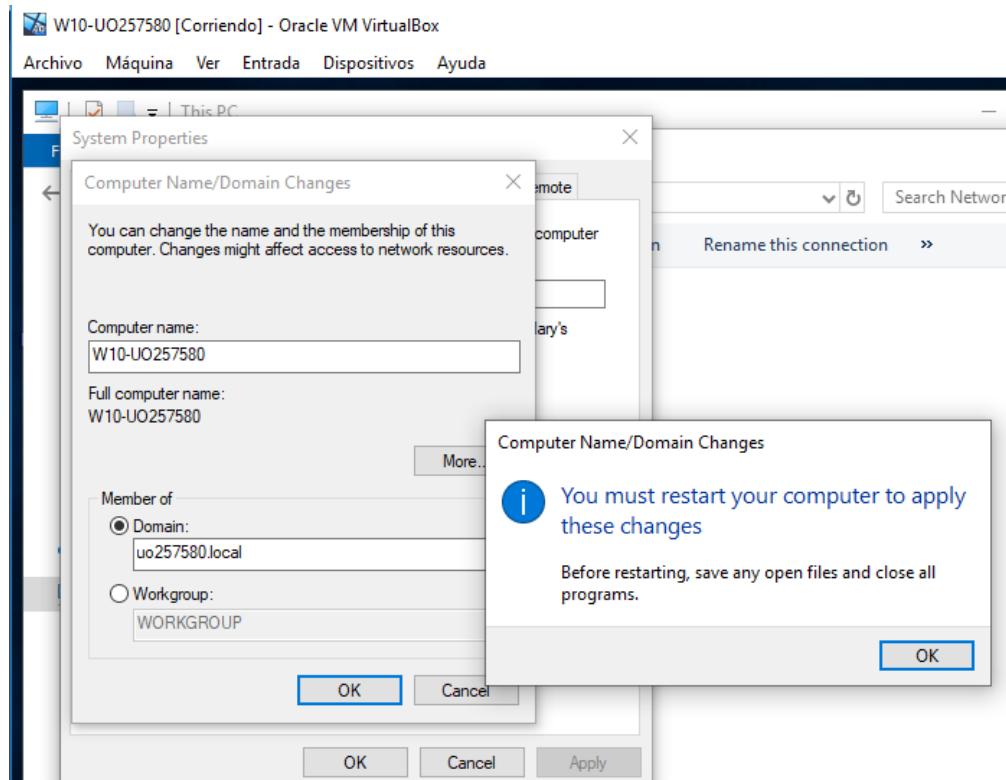
- Incluye esta máquina en el dominio **uoXXXX.local**:
 - "Inicio, Equipo, Propiedades, Nombre de equipo, Cambiar configuración":
 - **Nombre de equipo: W10-UOxxxxxx**
 - **Dominio: uoXXXX.local**



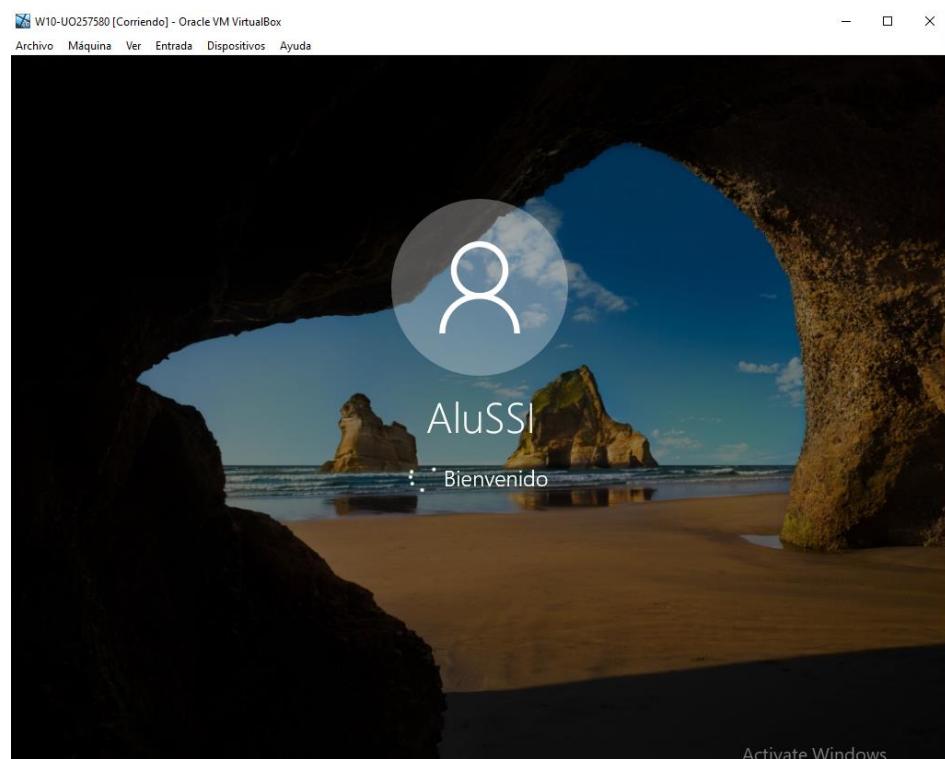
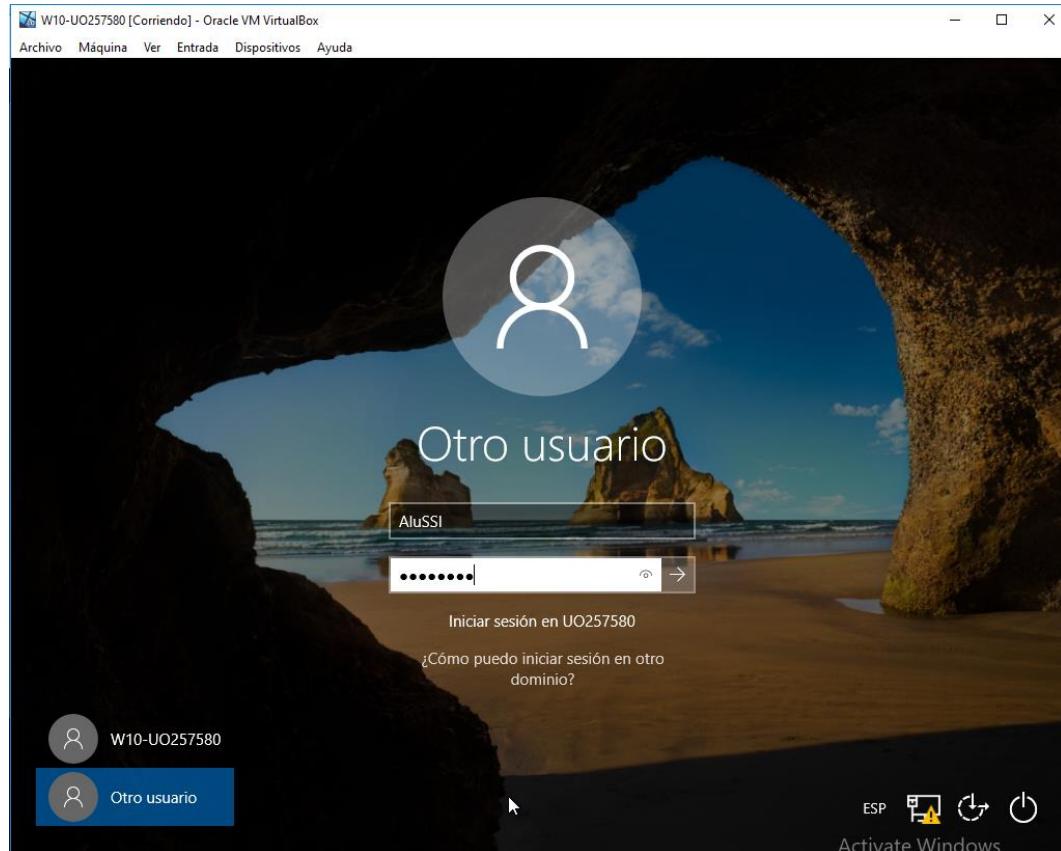
- Se pedirán credenciales de una cuenta del dominio para poder añadirlo.



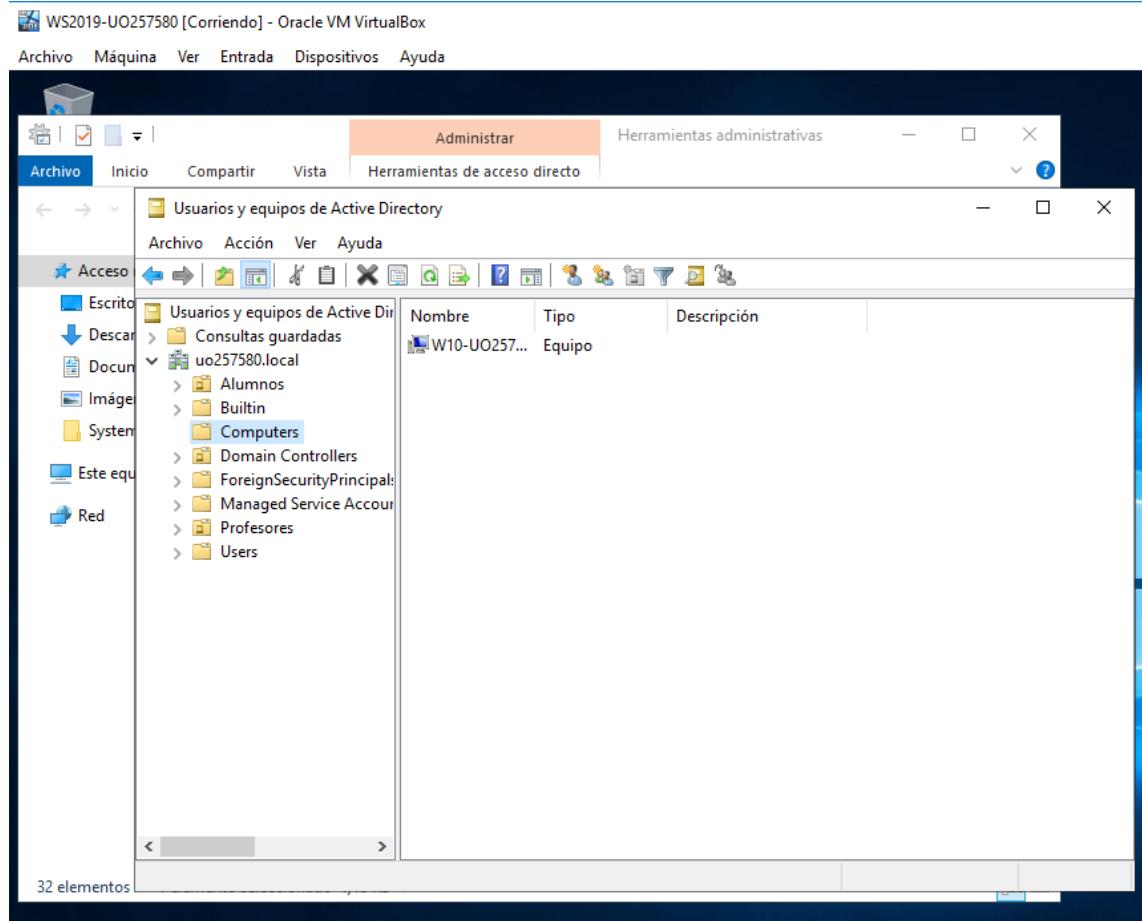
- Una vez añadido el equipo se reiniciará.



- Comprueba que puedes entrar en Windows 10 con los usuarios del dominio UOXXXXXX.



- Comprueba que puedes ver el equipo en el servidor W2019
 - Menu inicio, Herramientas administrativas, Usuarios y equipos de AD, UOXXXX.local, computers

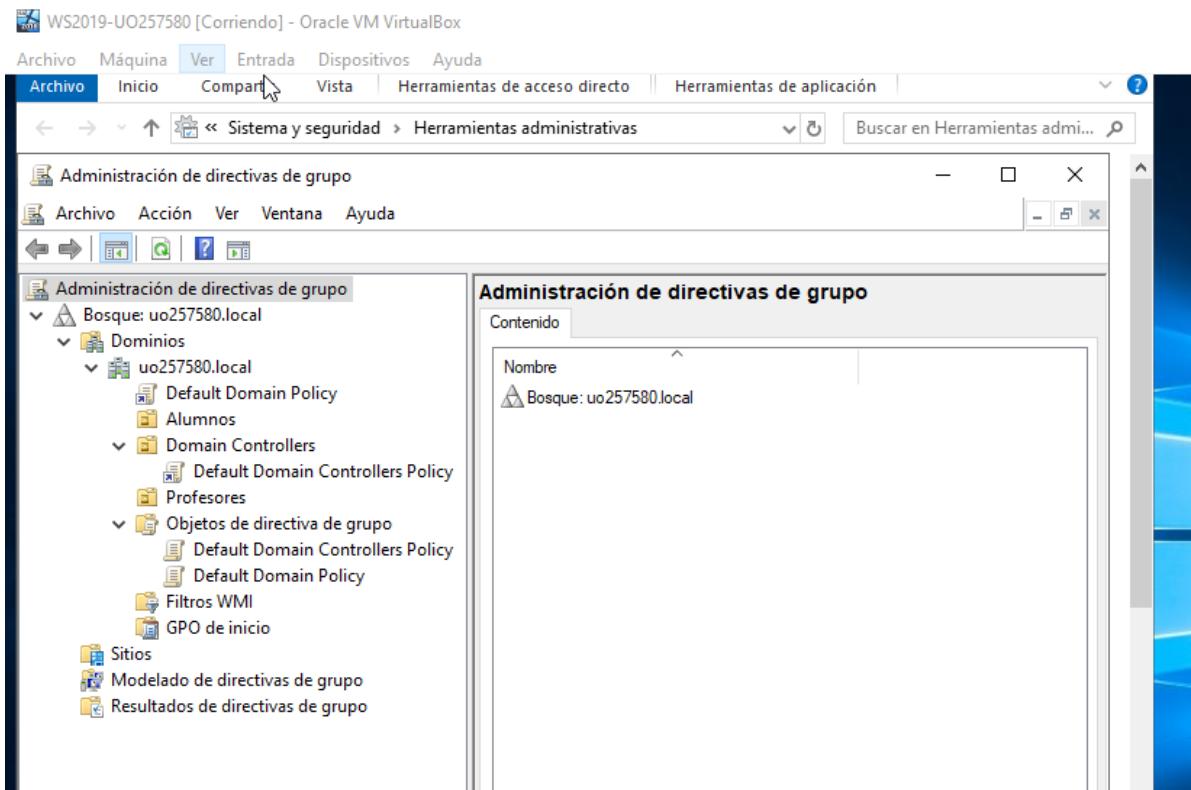


Directorio Activo

Políticas de grupo

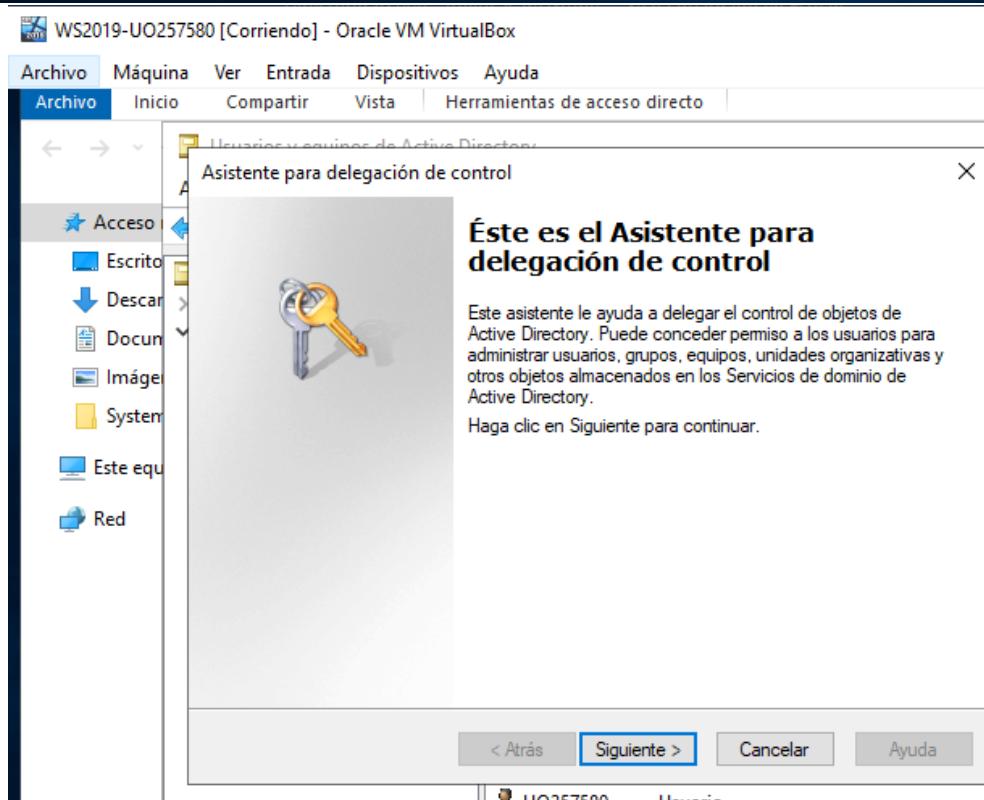
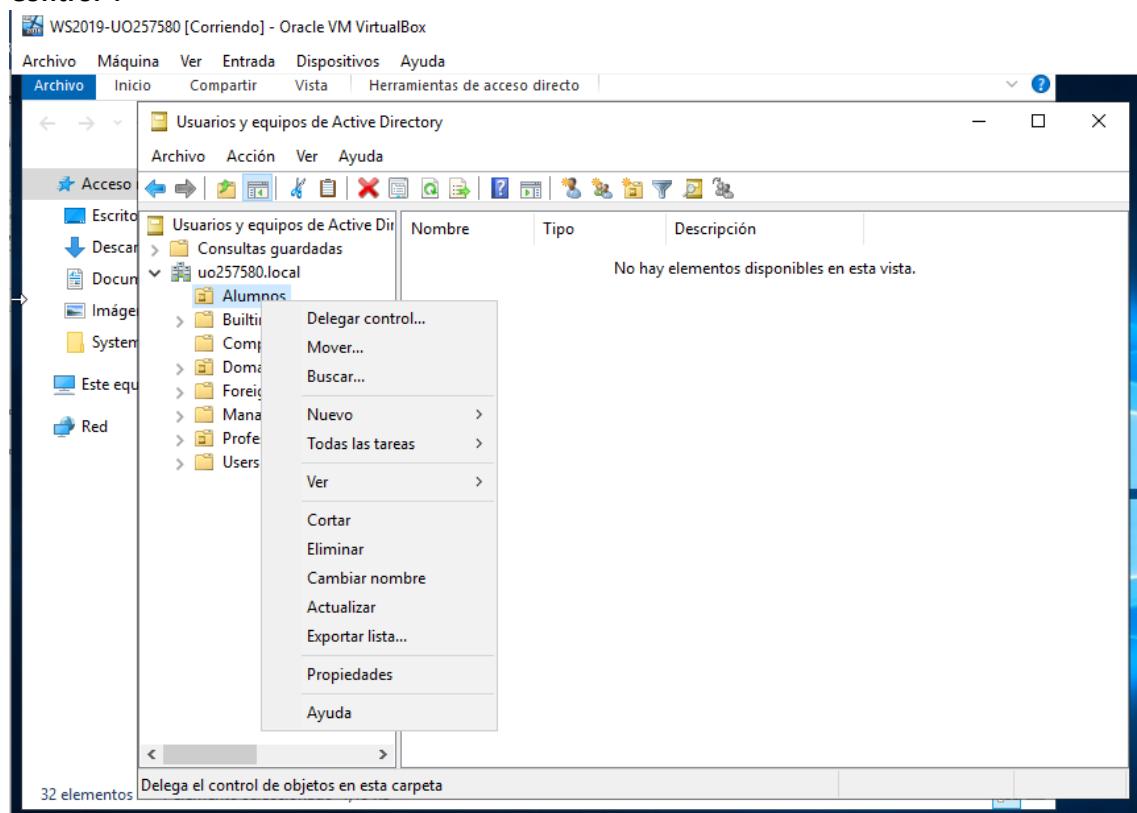
Seguridad en Active Directory

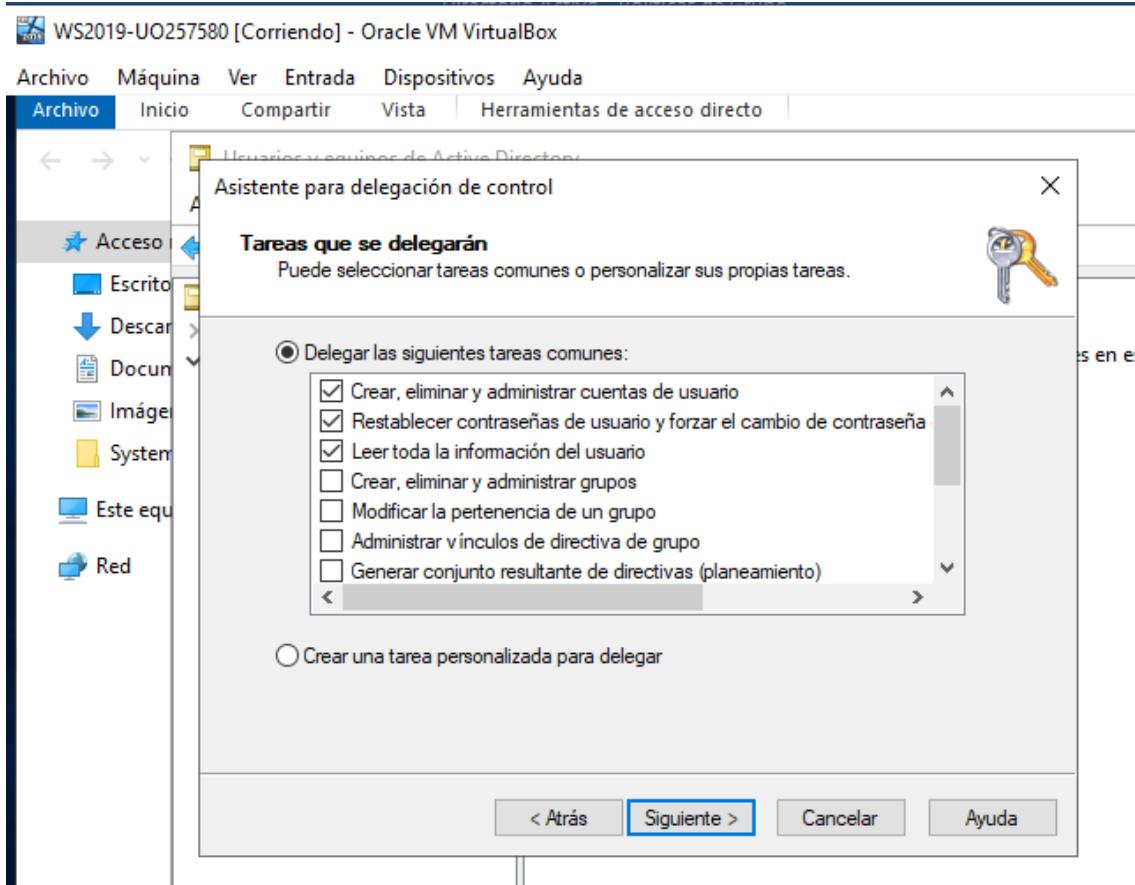
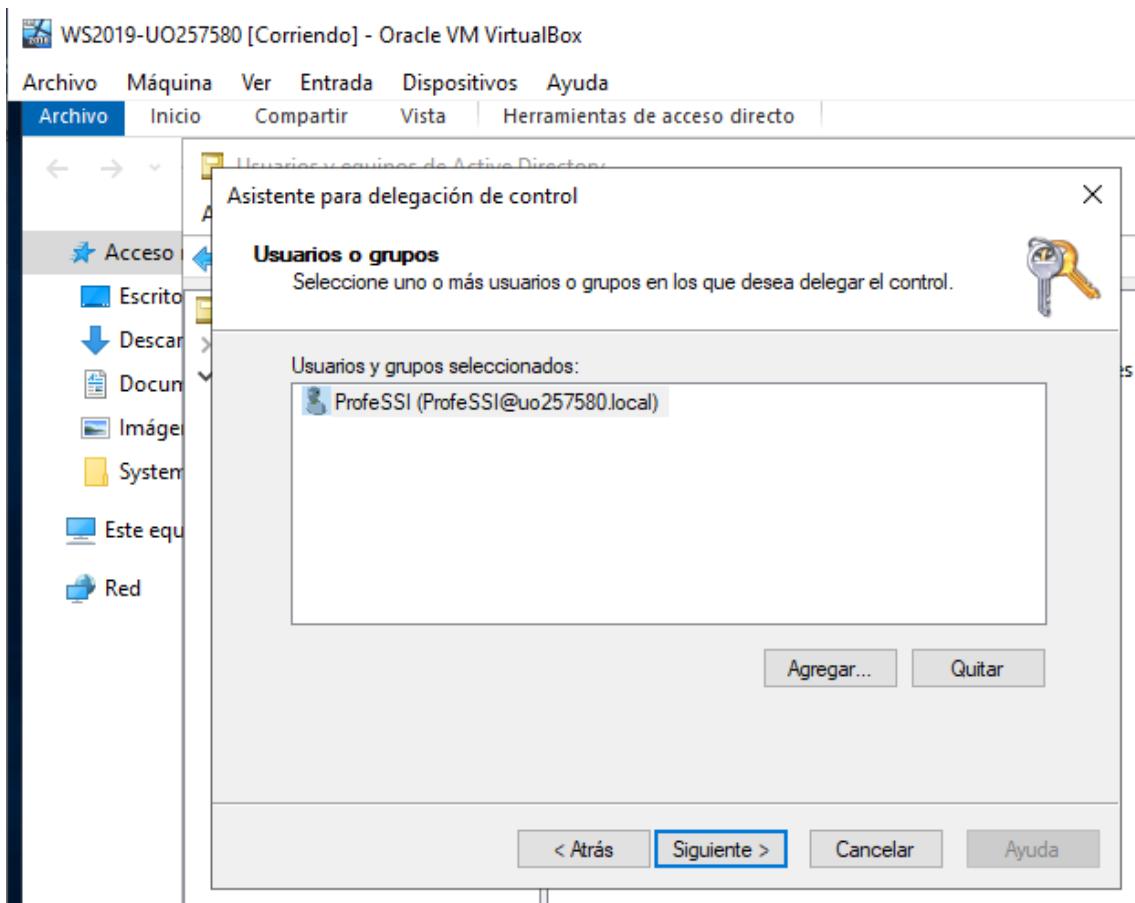
- 1) Desde el servidor, explora las opciones de Configuración de Seguridad del Dominio.

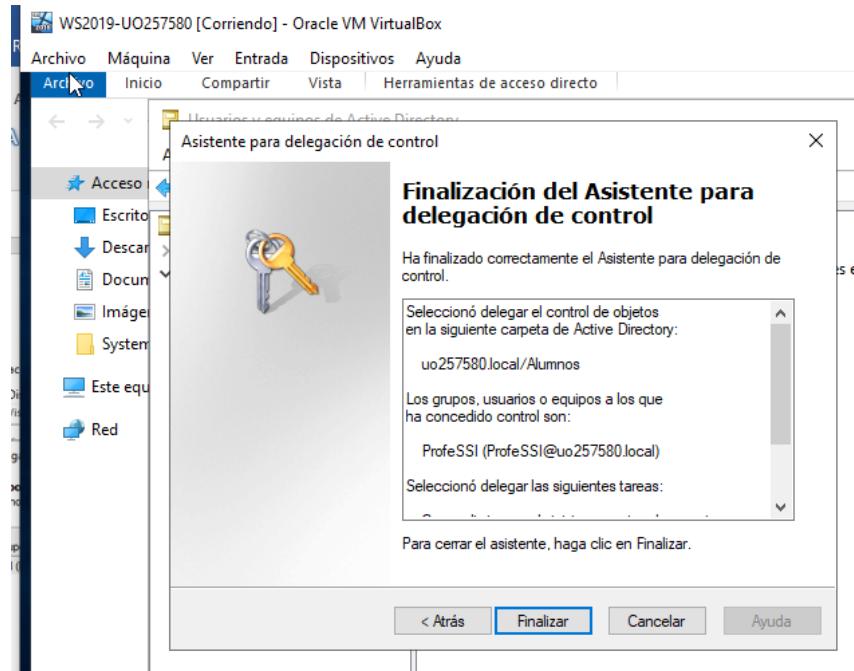


- 2) Desde el servidor, delega el control de la UO "Alumnos" a profeSSI (para crear, eliminar y administrar cuentas de usuario y restablecer contraseñas y forzar el cambio de contraseña y leer toda la información del usuario) "Herramientas"

Administrativas/Usuarios y Equipos de Active Directory, botón derecho en la UO, delegar Control".

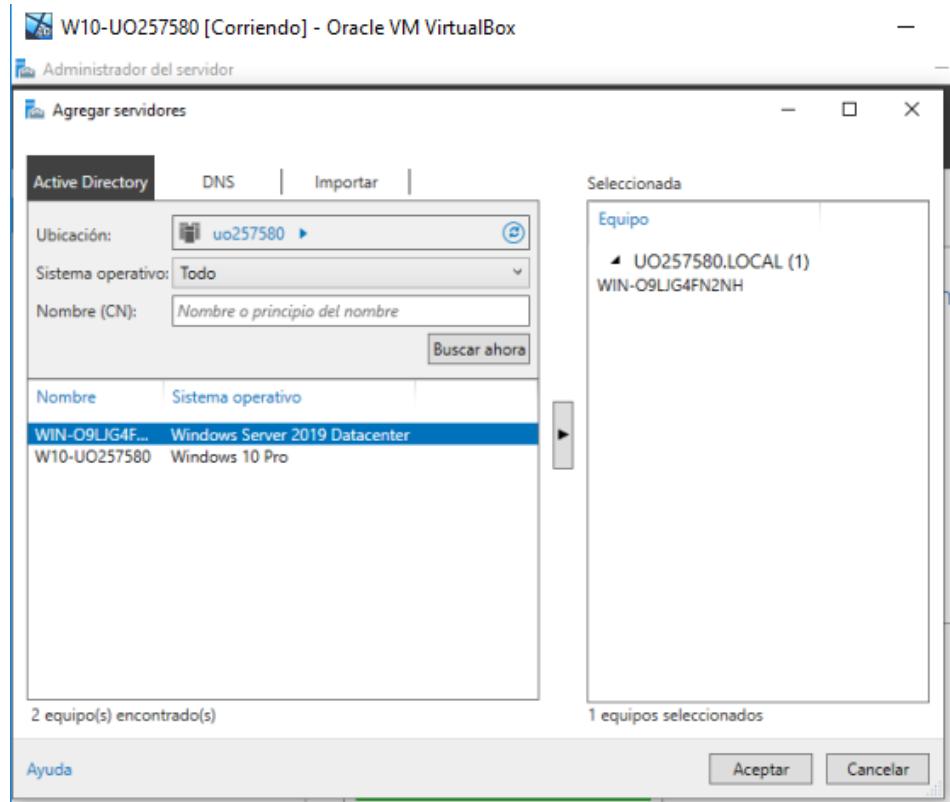




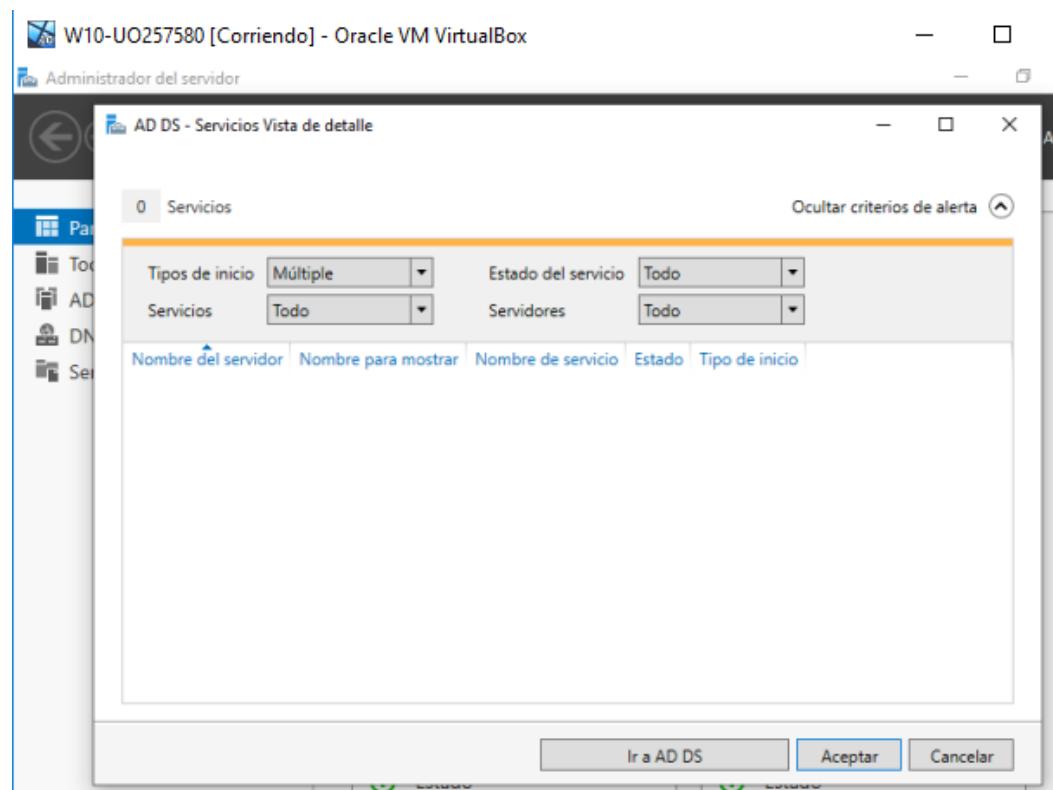
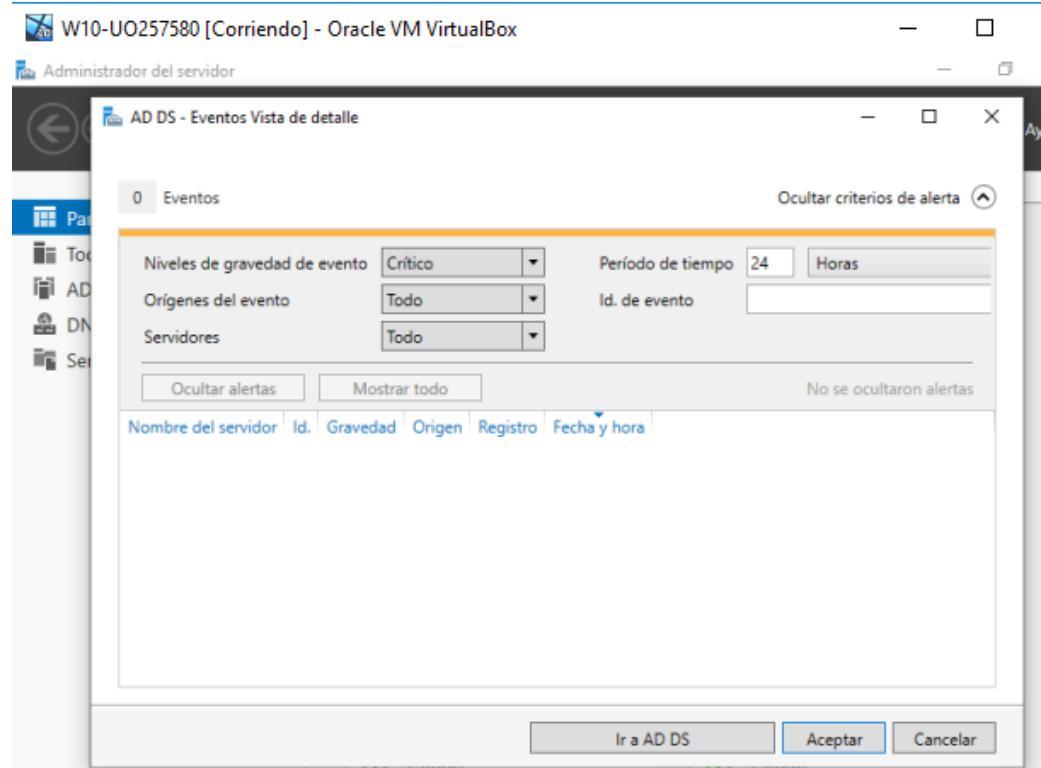


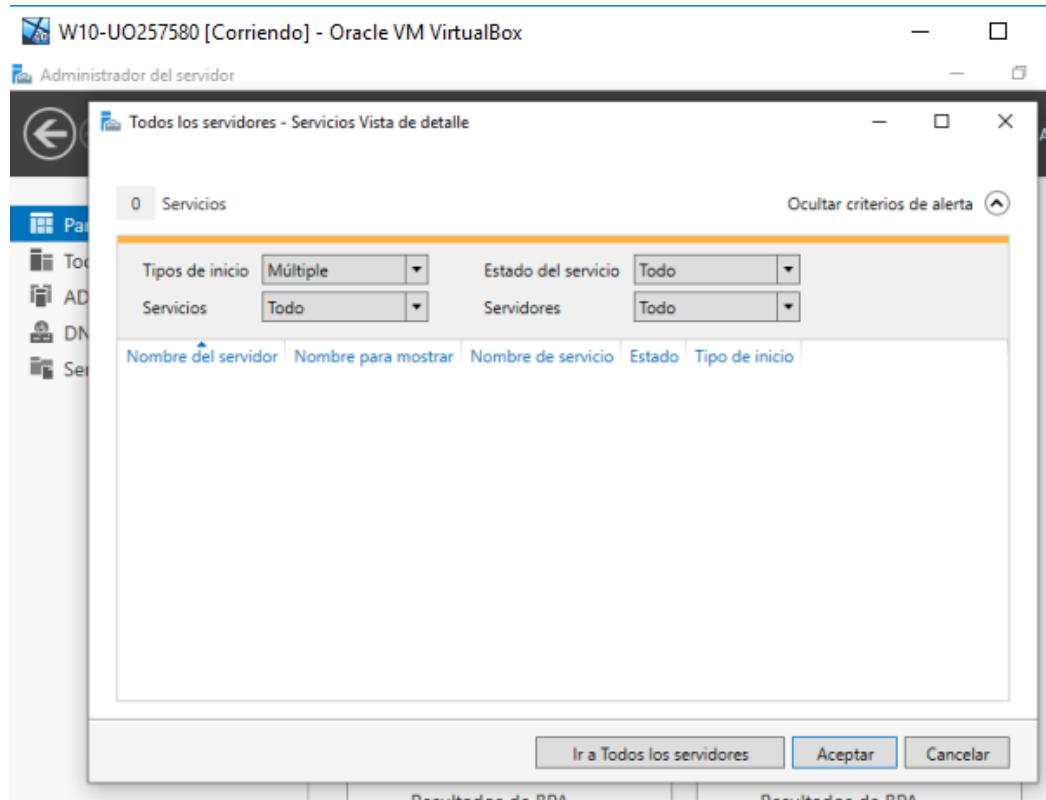
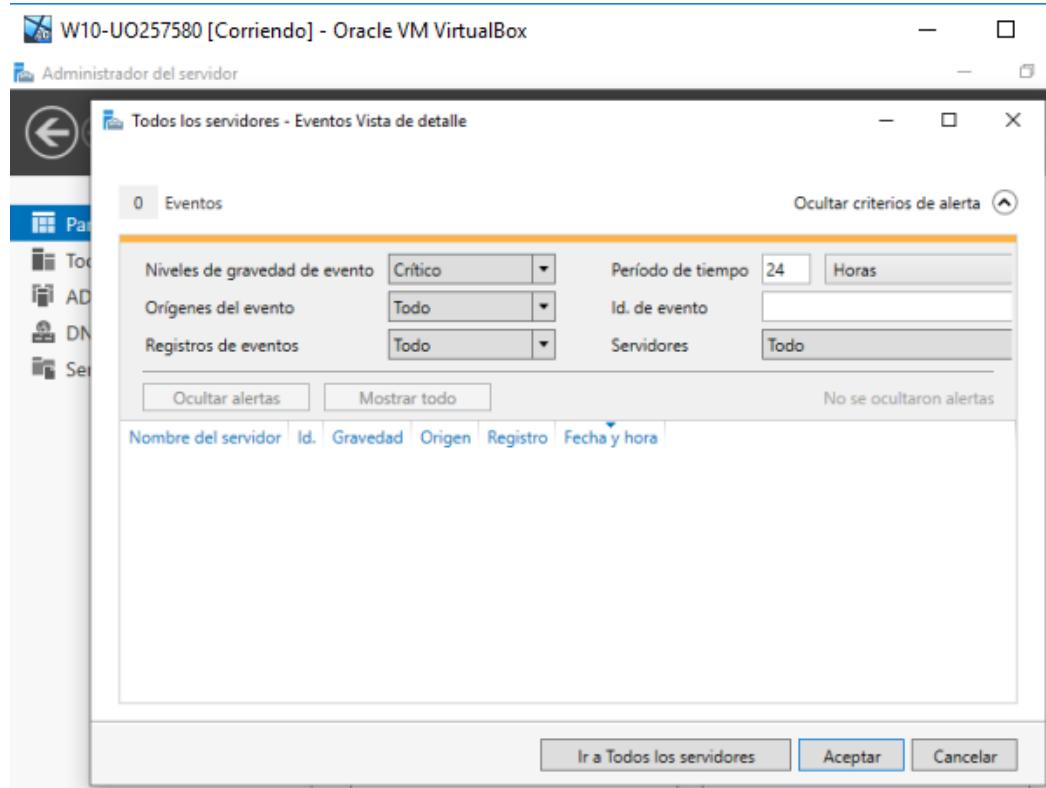
- 3) Inicia sesión con la cuenta administrador del dominio en el cliente (administrador@uo12345678.local) y a través de “Administración del servidor” añade nuestro servidor para poder administrarlo de forma remota.

- Administrador del Servidor-Agregar otros servidores para administrar-Active Directory. Asegurate que la ubicación es el dominio uoxxxxx, pincha en buscar y añade el Windows Server 2019.



- Explora toda la información disponible de tanto el rol de Directorio Activo como el de Servidor de Dominio de nuestro servidor: Eventos, Servicios...

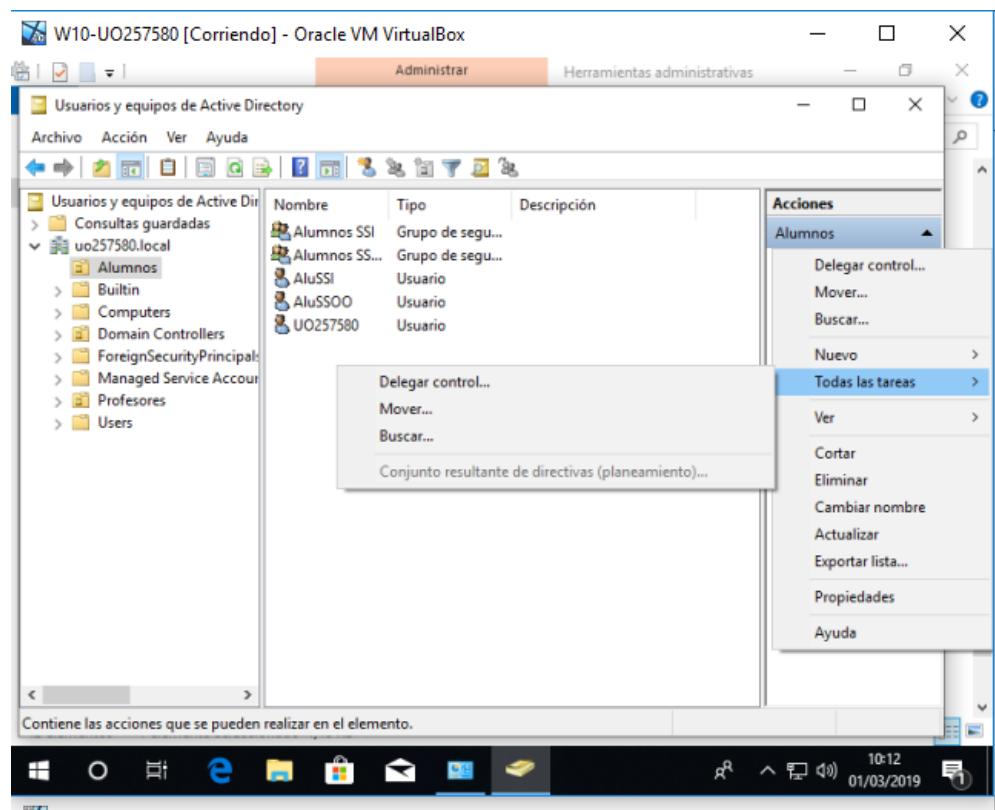




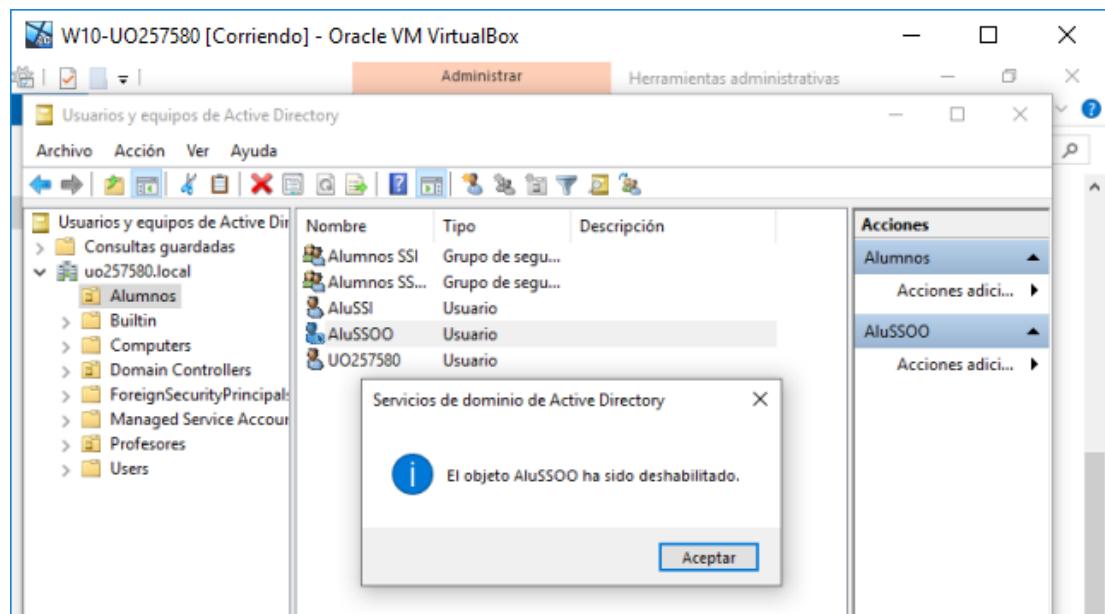
4) Sal de sesión y entra como profeSSI.



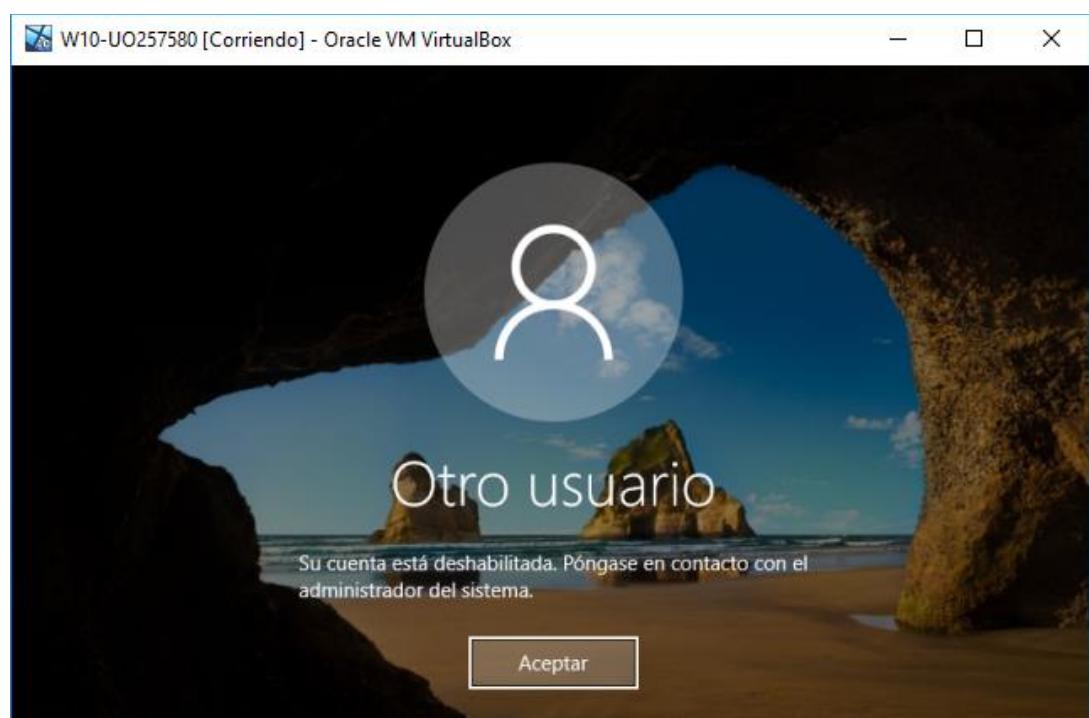
- En "Herramientas administrativas - Usuarios y Equipos de Active Directory" mira las opciones de administración que tiene profeSSI con los miembros de la UO Alumnos.



○ Deshabilita la cuenta de aluSSO.

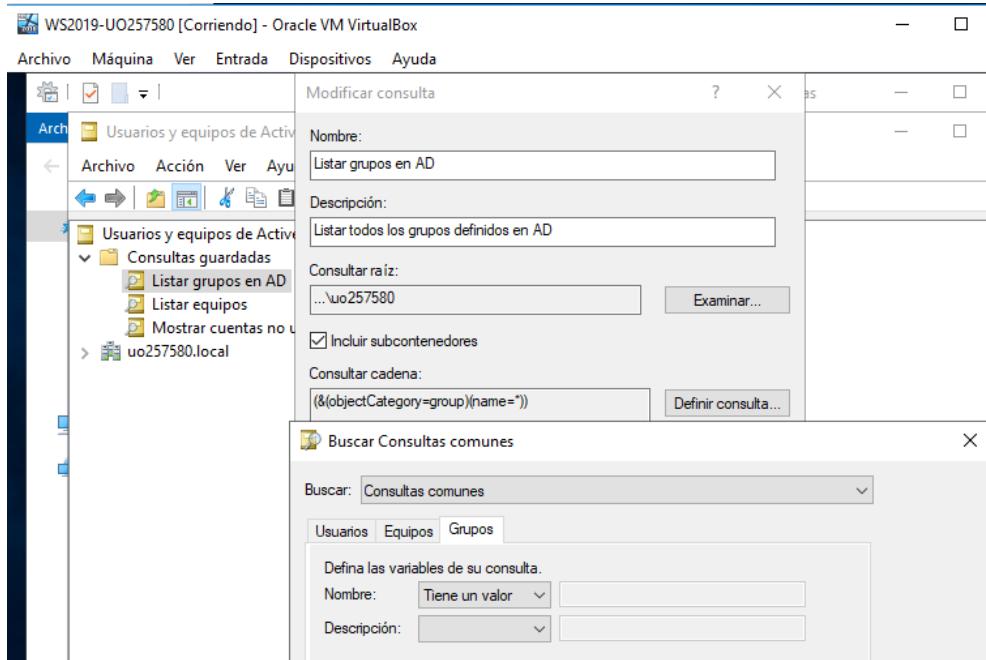


○ Intenta iniciar sesión como aluSSO.



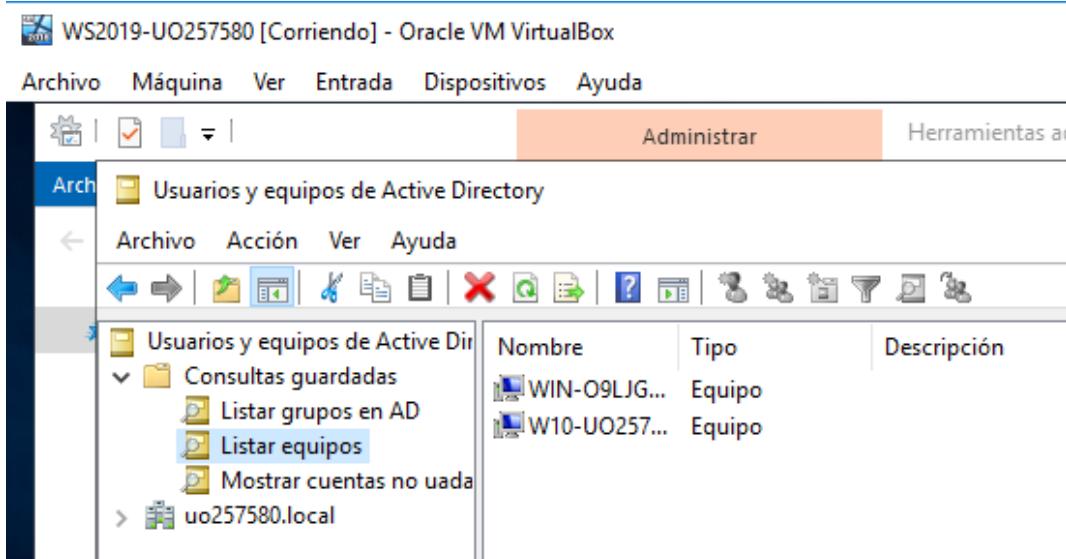
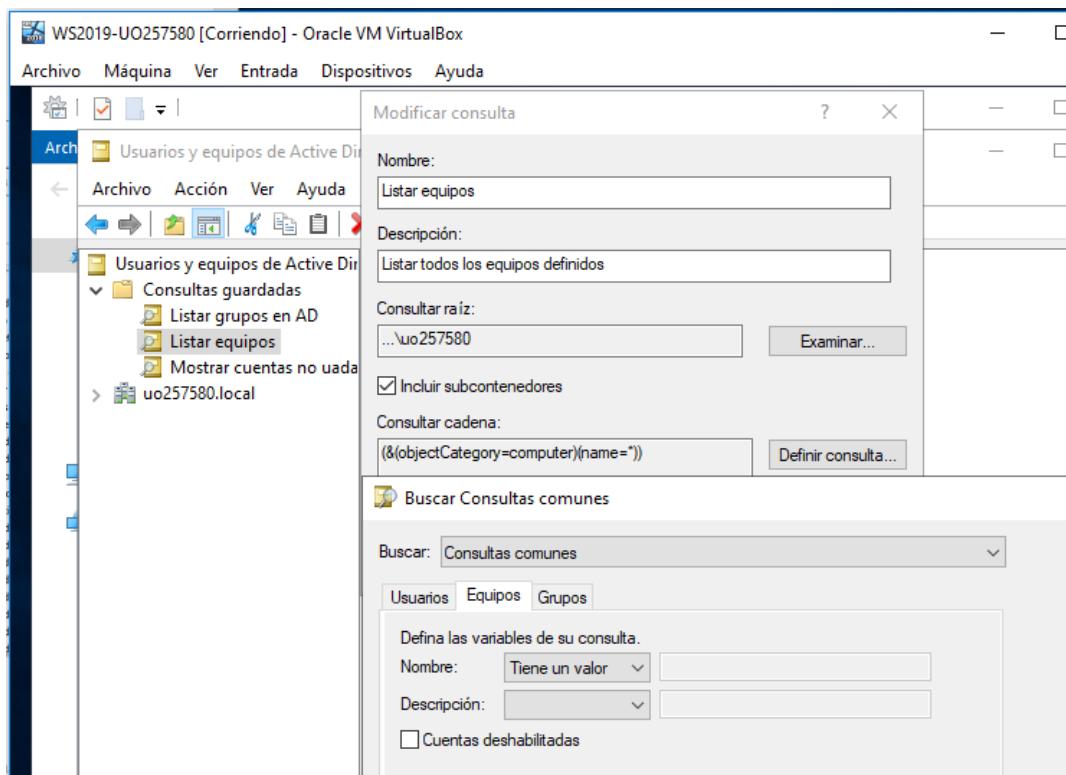
- 5) En "Usuarios y Equipos de Active Directory - Consultas guardadas - Nuevo - Consulta"
 crea consultas (y ejecutarlas).

- Listar todos los grupos definidos en AD.

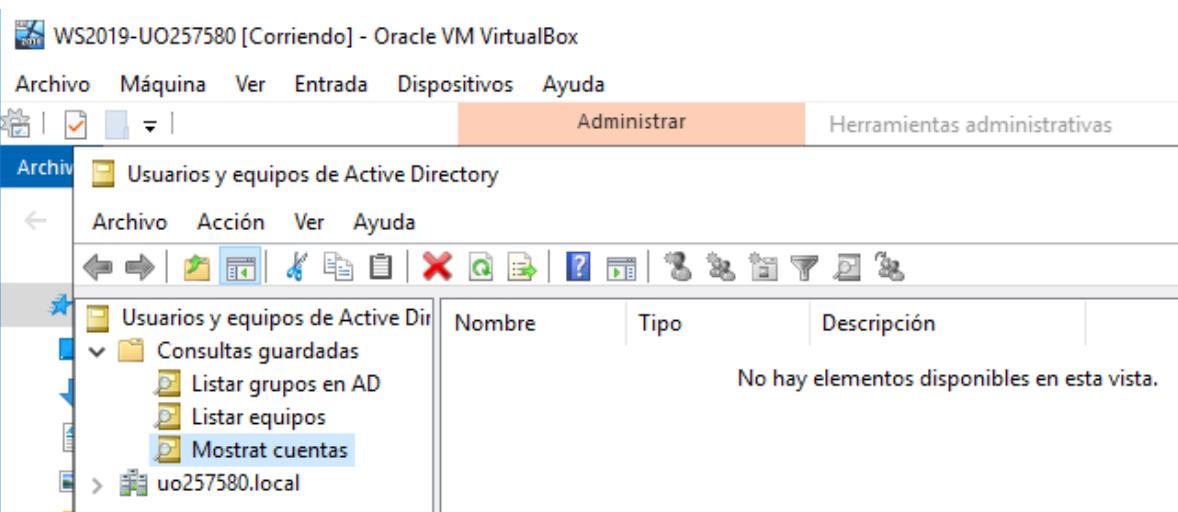
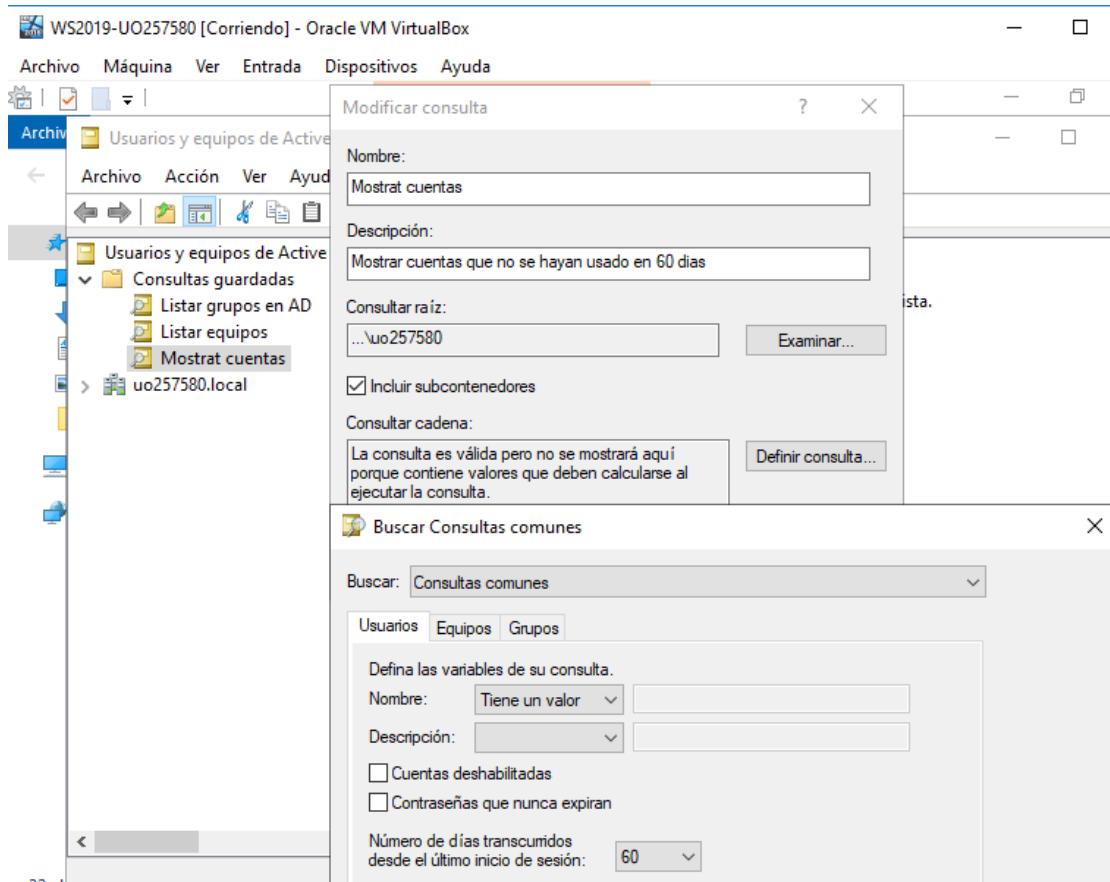


Nombre	Tipo	Descripción
Administrad...	Grupo de segu...	Los administradores tien...
Usuarios	Grupo de segu...	Los usuarios no pueden ...
Invitados	Grupo de segu...	De forma predetermina...
Oper. de im...	Grupo de segu...	Los miembros pueden a...
Operadores ...	Grupo de segu...	Los operadores de copia...
Duplicadores	Grupo de segu...	Pueden replicar archivos...
Usuarios de ...	Grupo de segu...	A los miembros de este ...
Operadores ...	Grupo de segu...	Los miembros en este e...
Usuarios del ...	Grupo de segu...	Los miembros de este gr...
Usuarios del ...	Grupo de segu...	Los miembros de este gr...
Usuarios CO...	Grupo de segu...	Los miembros pueden i...
IIS_IUSRS	Grupo de segu...	Grupo integrado usado ...
Operadores ...	Grupo de segu...	Los miembros tienen au...
Lectores del ...	Grupo de segu...	Los miembros de este gr...
Acceso DCO...	Grupo de segu...	Los miembros de este gr...
Servidores d...	Grupo de segu...	Los servidores de este gr...
Servidores d...	Grupo de segu...	Los servidores de este gr...
Servidores d...	Grupo de segu...	Los servidores de este gr...
Administrad...	Grupo de segu...	Los miembros de este gr...
Operadores ...	Grupo de segu...	Los miembros de este gr...
Usuarios de ...	Grupo de segu...	Los miembros de este qr...

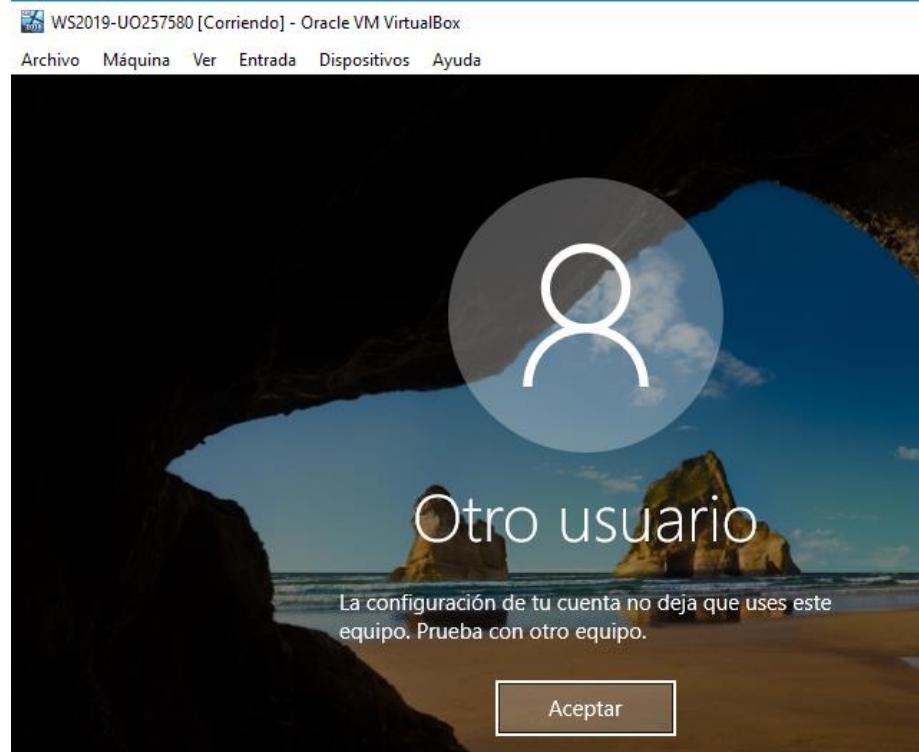
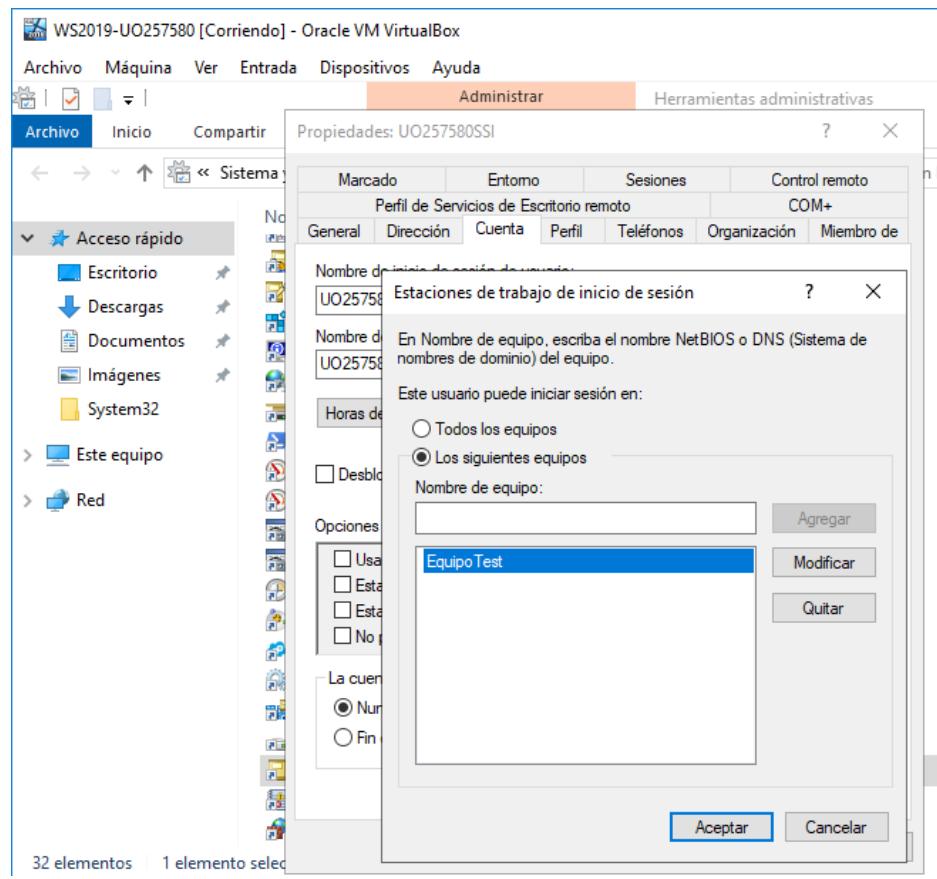
- Listar todos los equipos definidos.



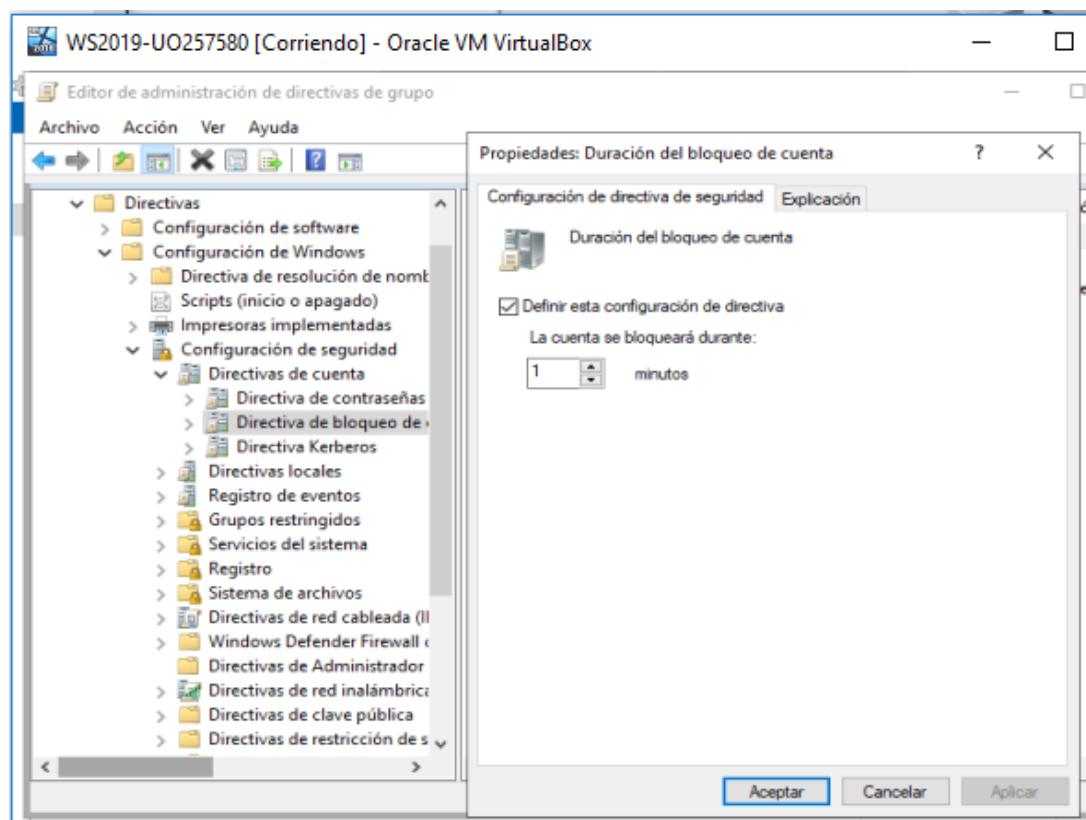
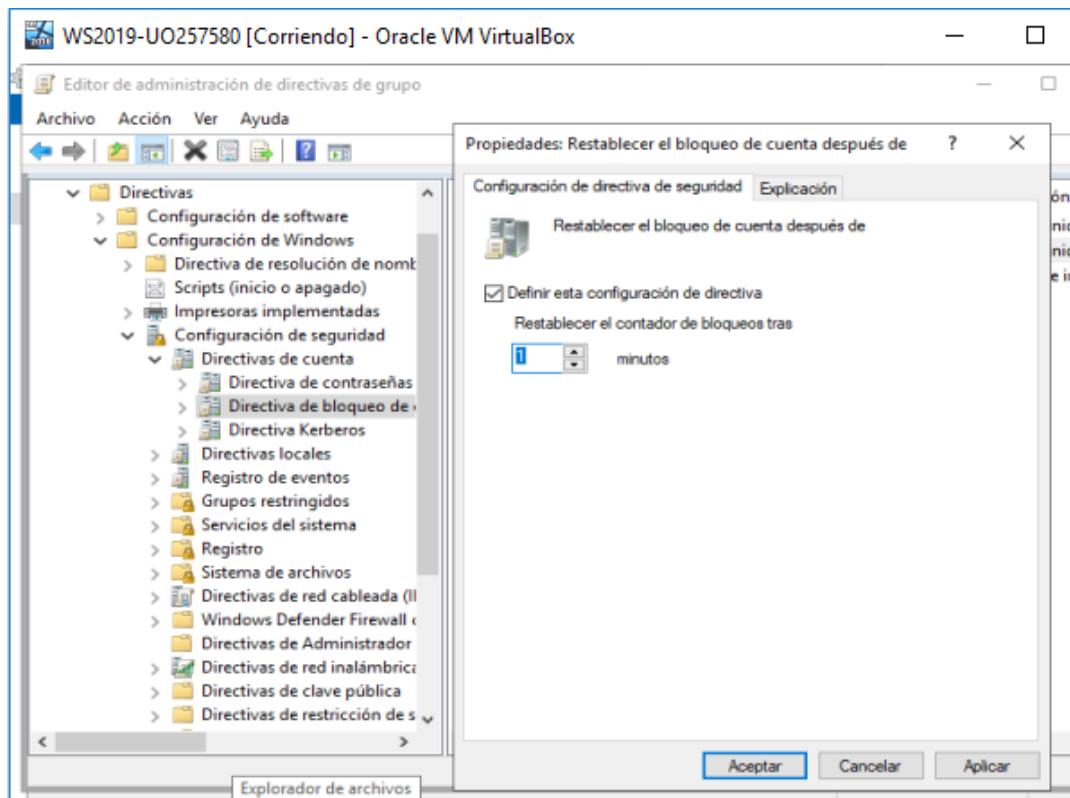
- Mostrar cuentas que no se hayan usado en 60 días.

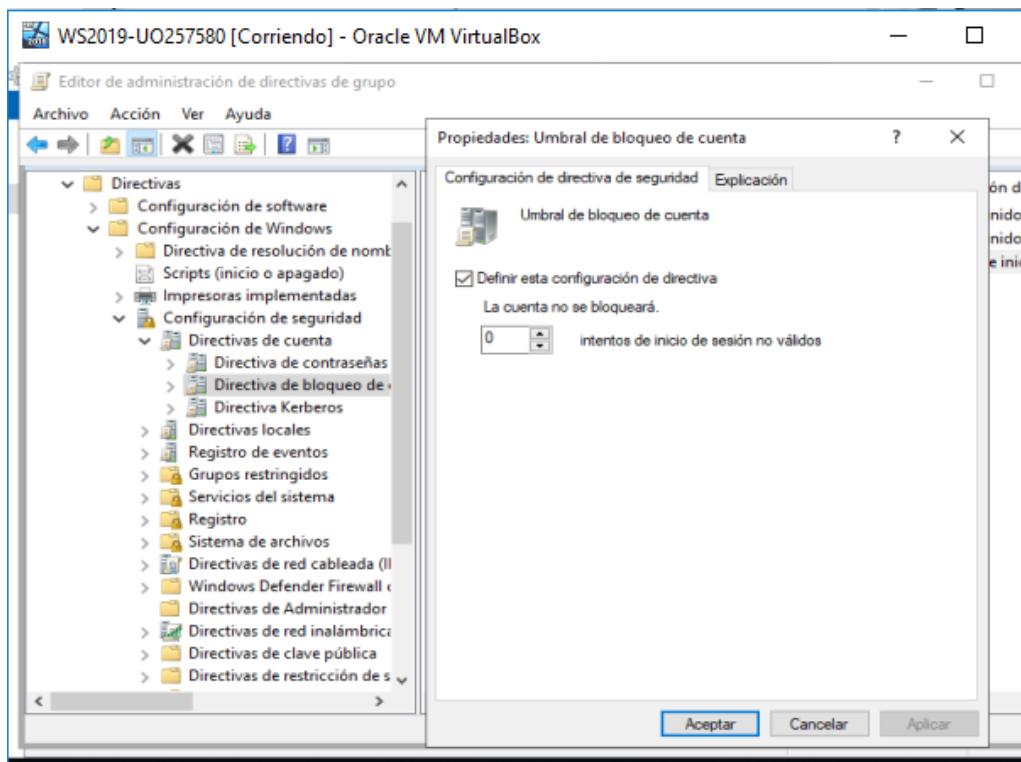


- 6) Impide que UOXXXXSSI pueda iniciar sesión en el equipo Servidor (Usuarios y Equipos de Active Directory - Users -UOXXXXSSI - Propiedades, Cuenta). Compruébalo.

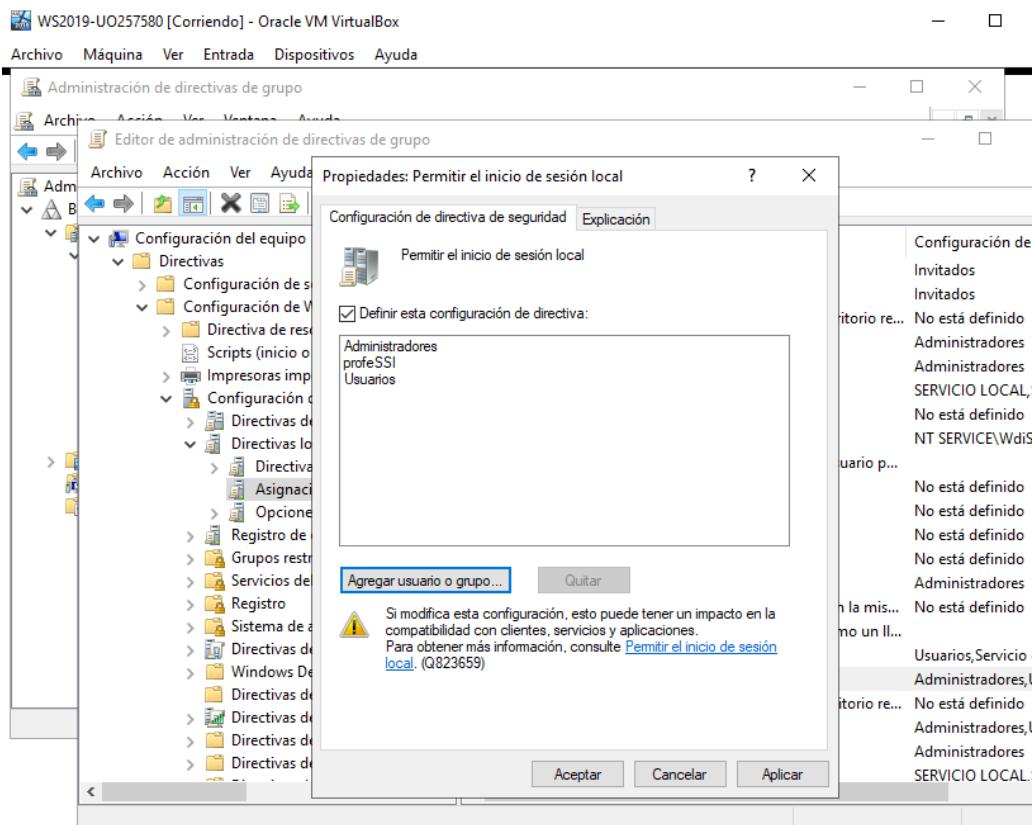


- 7) Desde el servidor, define la directiva de bloqueo de cuentas de manera que se frustre un ataque de fuerza bruta, causando la menor perturbación posible al usuario "olvidadizo" (Configuración de Seguridad del Dominio):





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



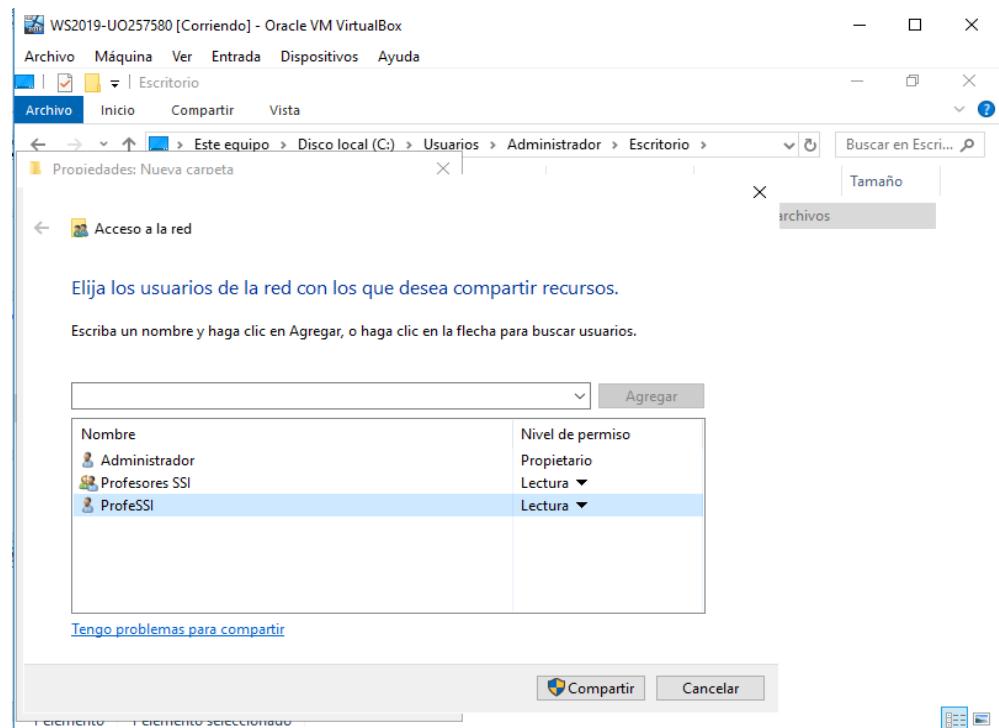
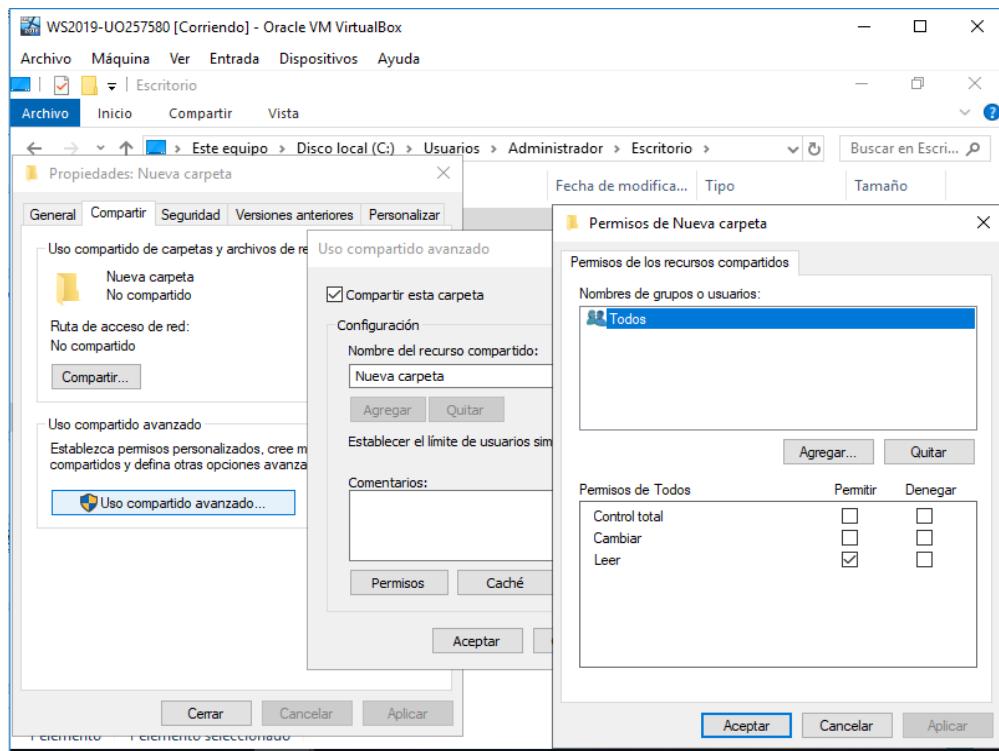
- Comprueba que el usuario puede iniciar sesión localmente. (Recuerda que se tarda tiempo en actualizar).

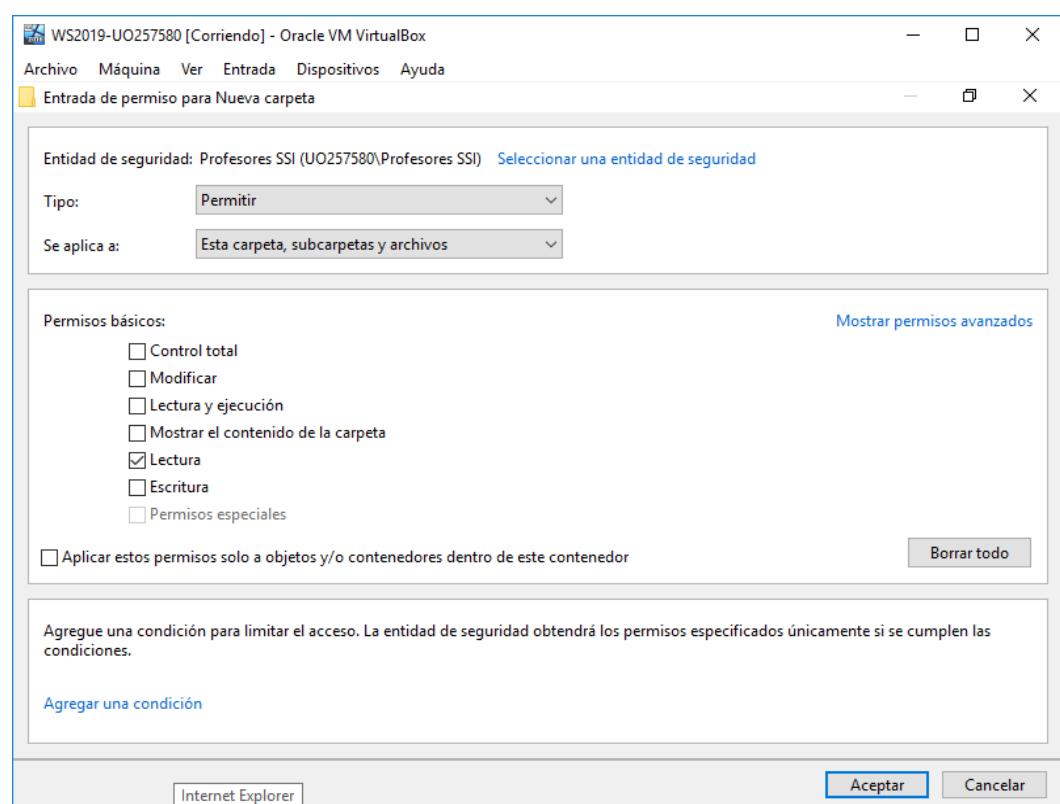
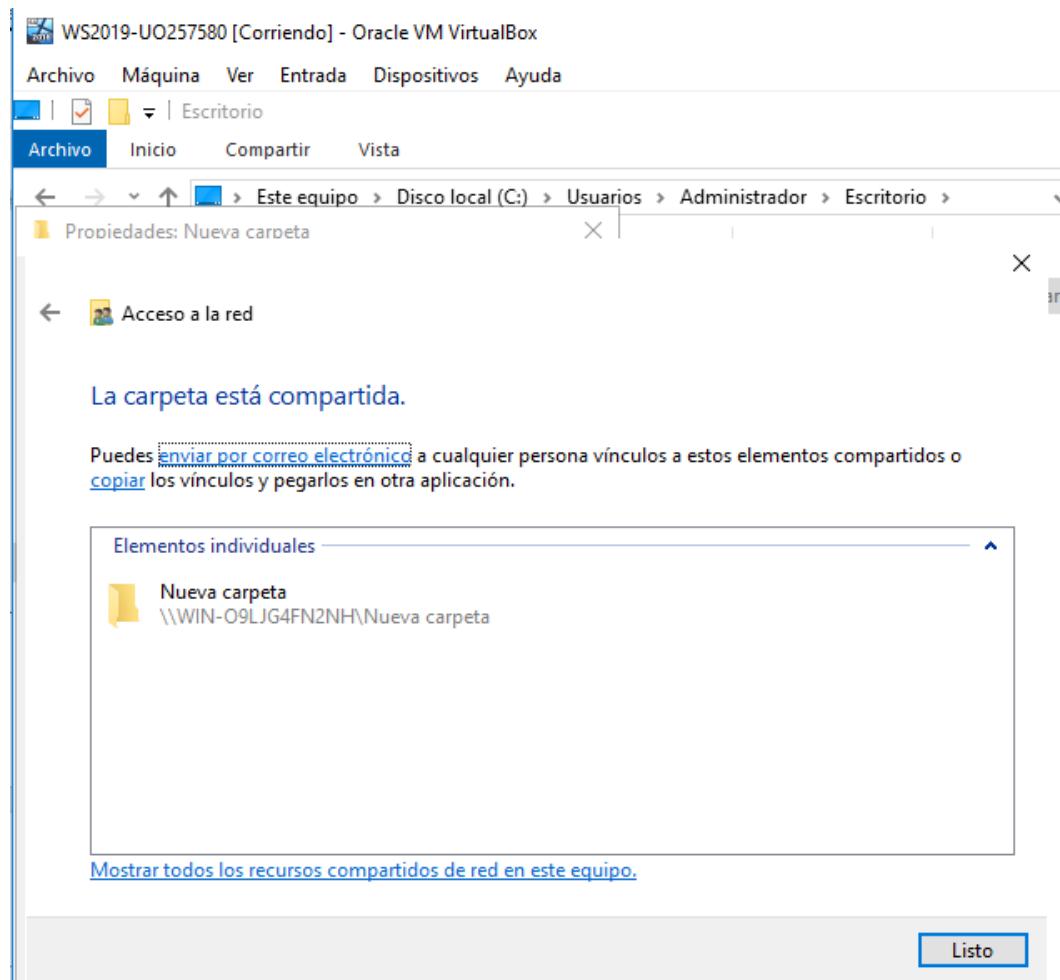


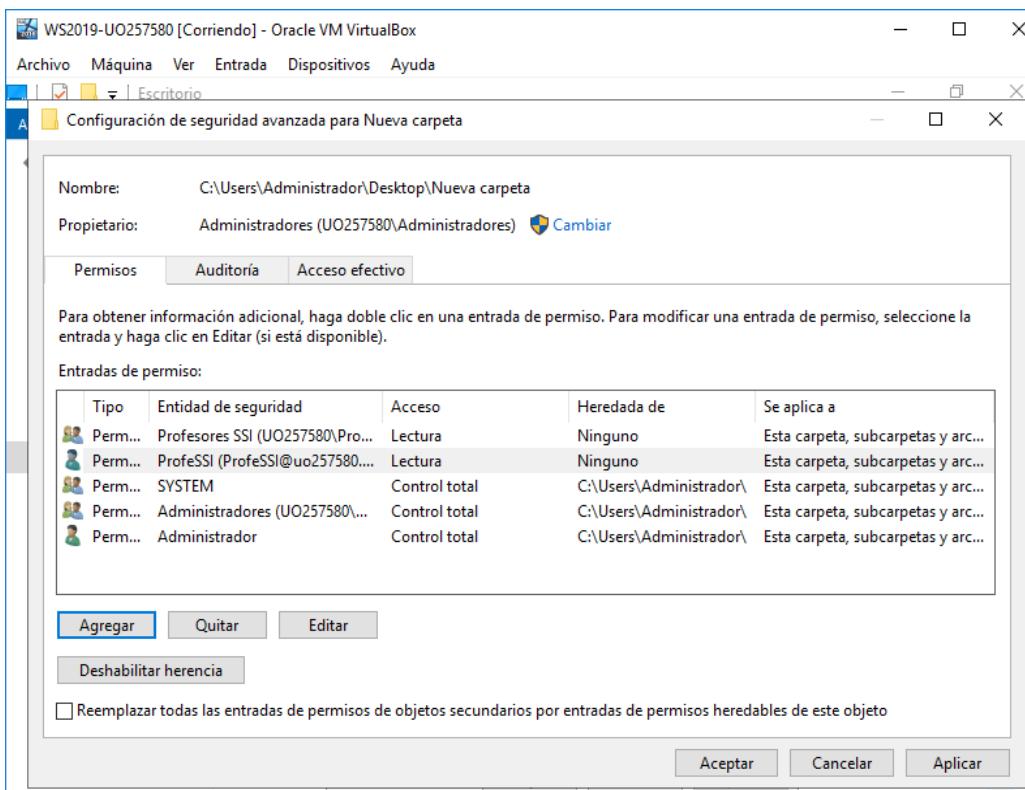
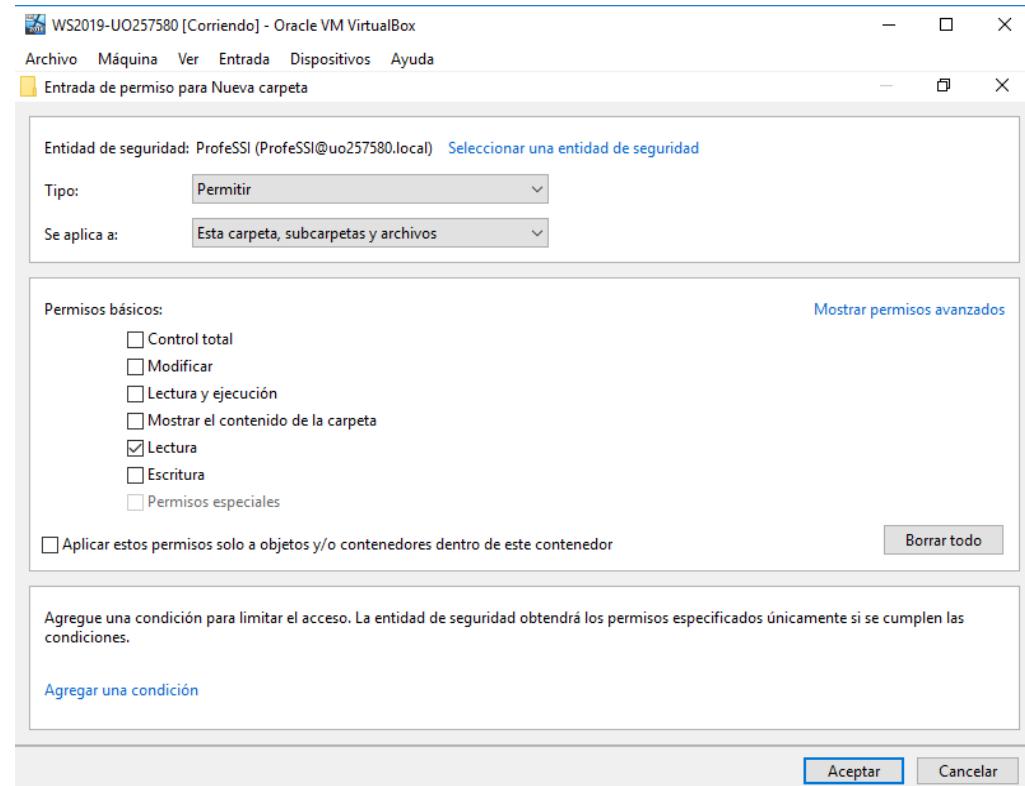
Políticas de grupo

- 1) Crea una carpeta compartida en el escritorio del Administrador en el Windows Server 2019.
 - Con permiso de lectura para los miembros del grupo "Profesores de SSI"

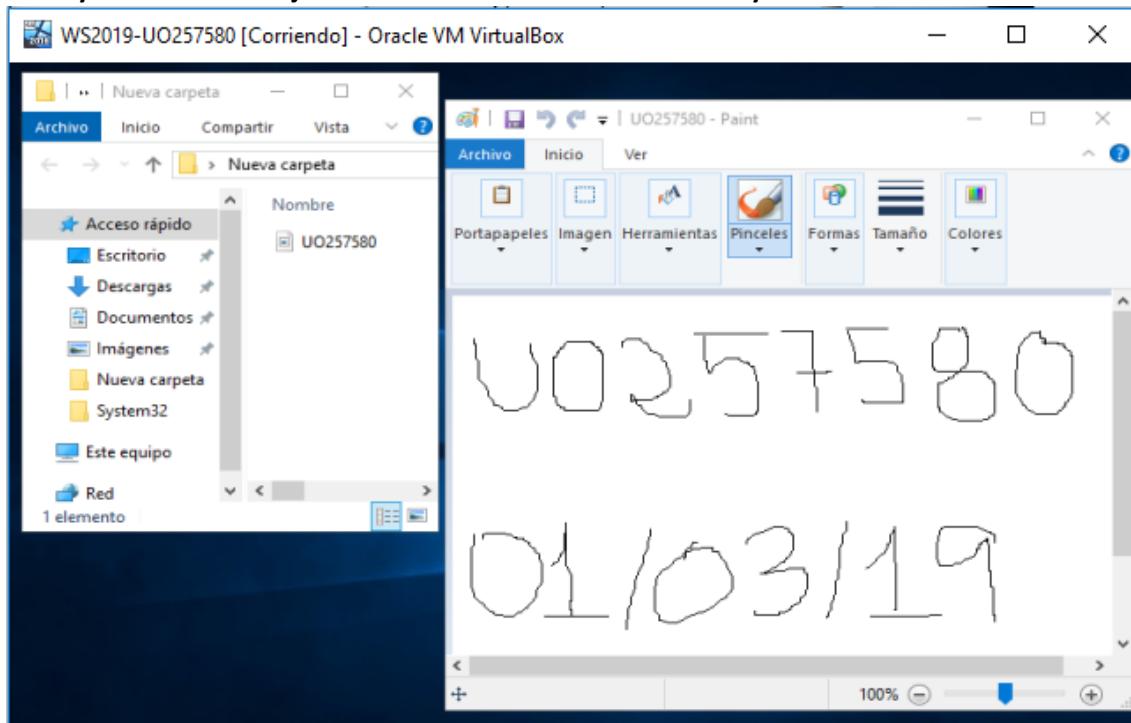




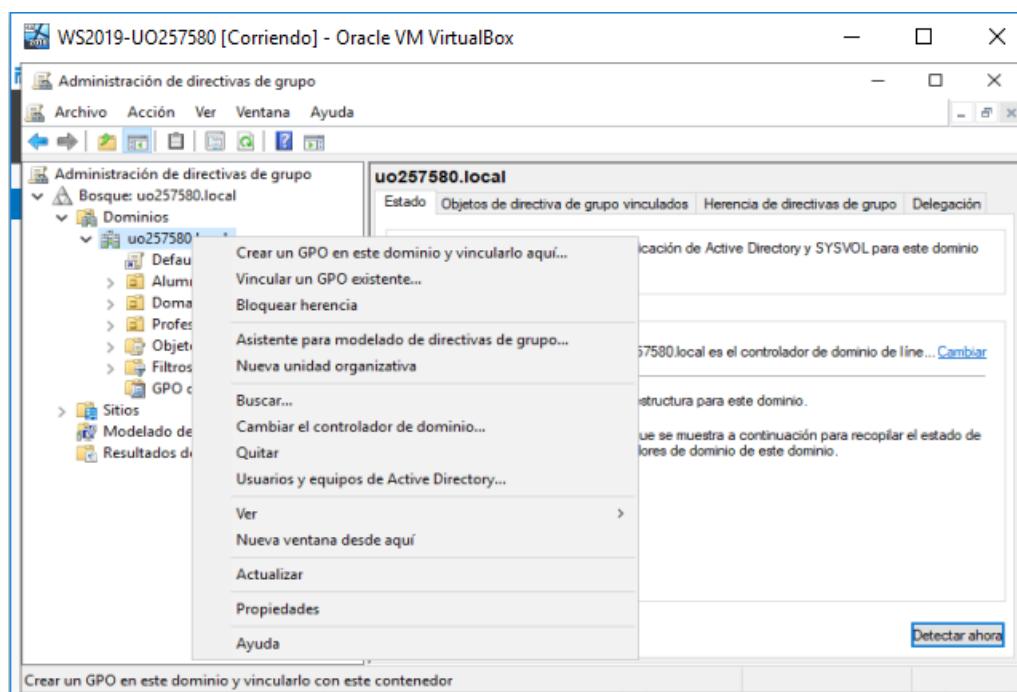


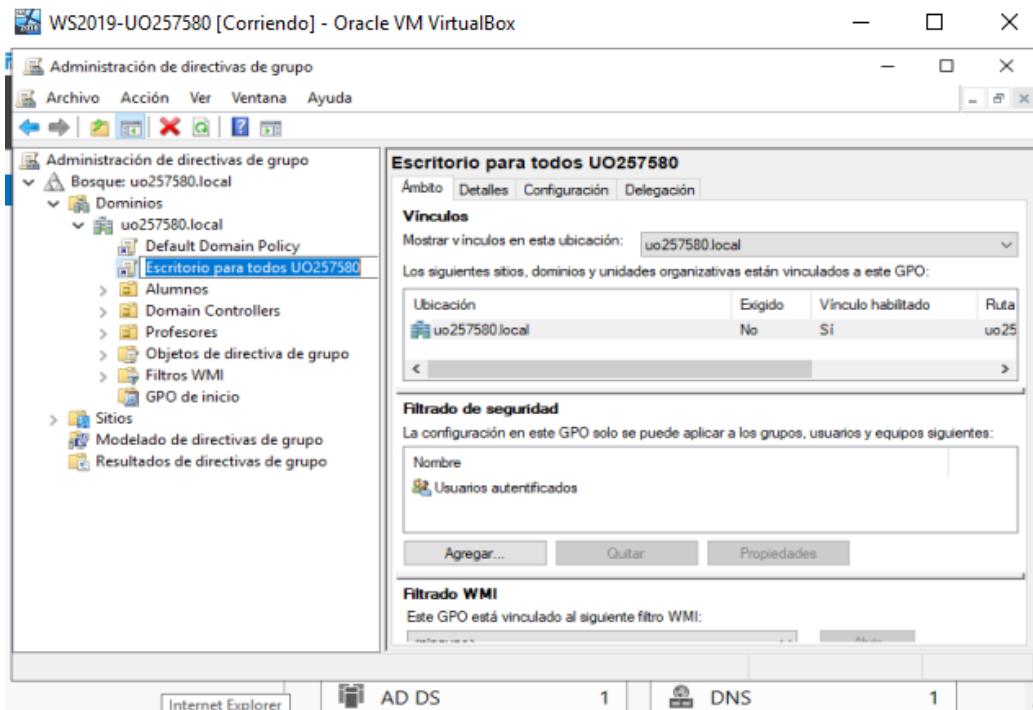


- 2) Coloca en dicha carpeta un fichero JPG que se utilizará como fondo de escritorio para los miembros del grupo "Profesores de SSI". Esa imagen JPG tiene que ser realizada con el Paint y debe tener dibujado a "mano alzada" tu UOXXXXXX y la fecha.

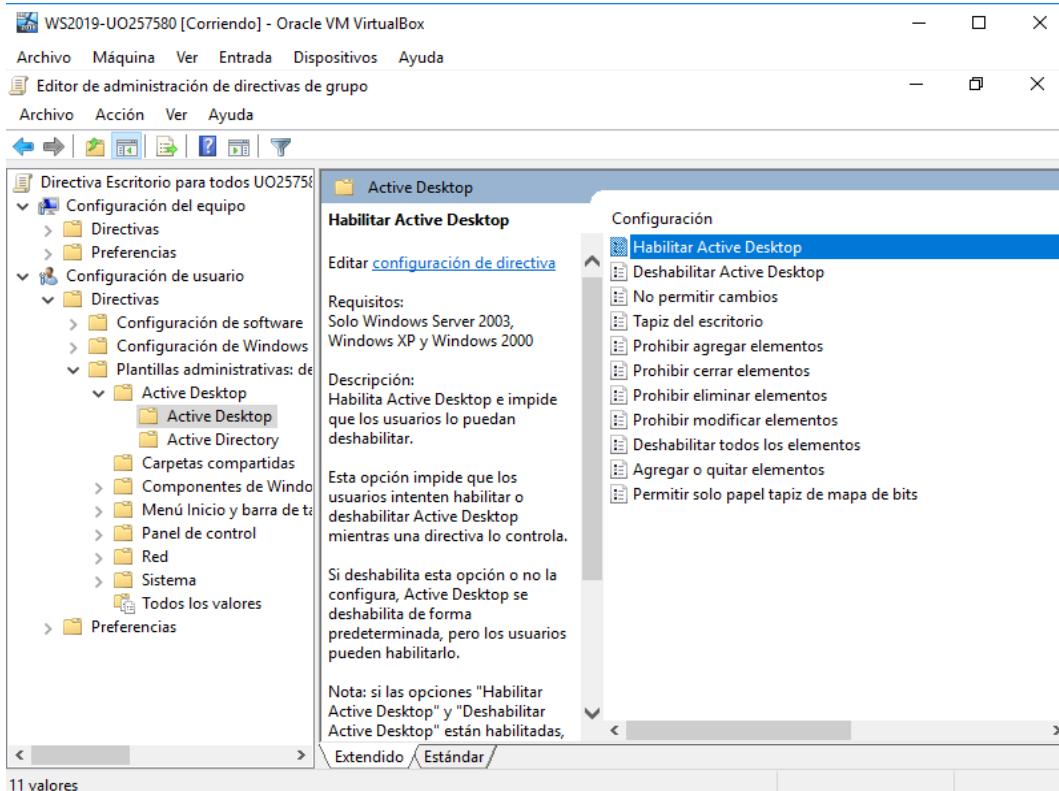


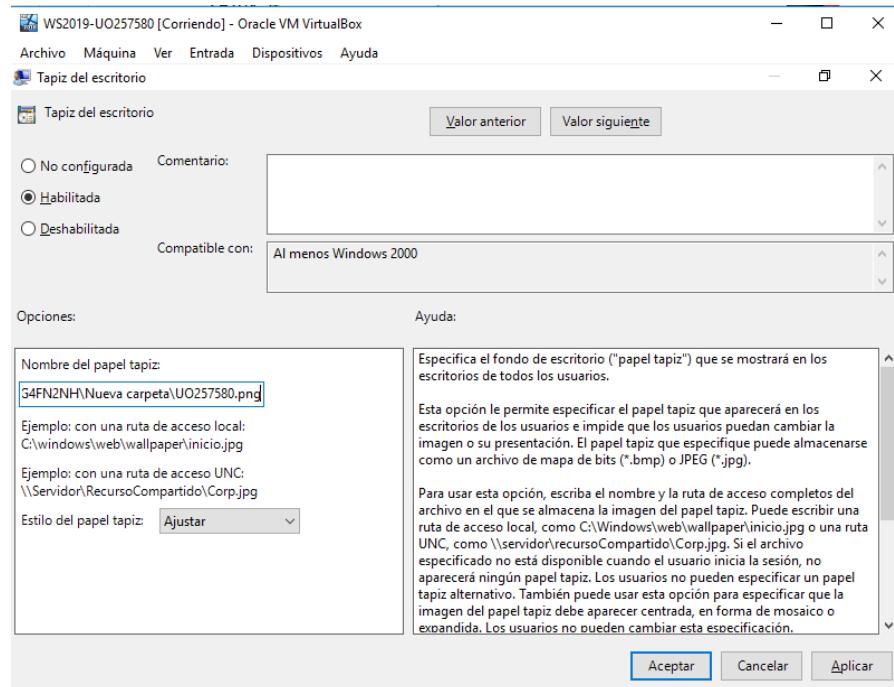
- 3) Crea una nueva GPO para todo el dominio denominada "Escritorio para todos UOXXX" y edítala de la manera siguiente:



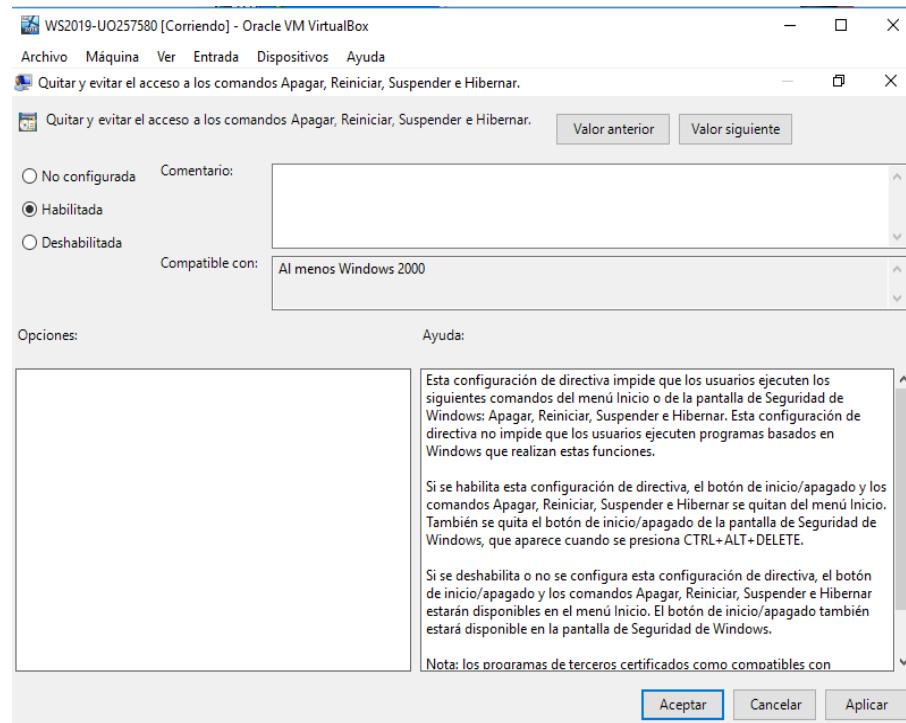


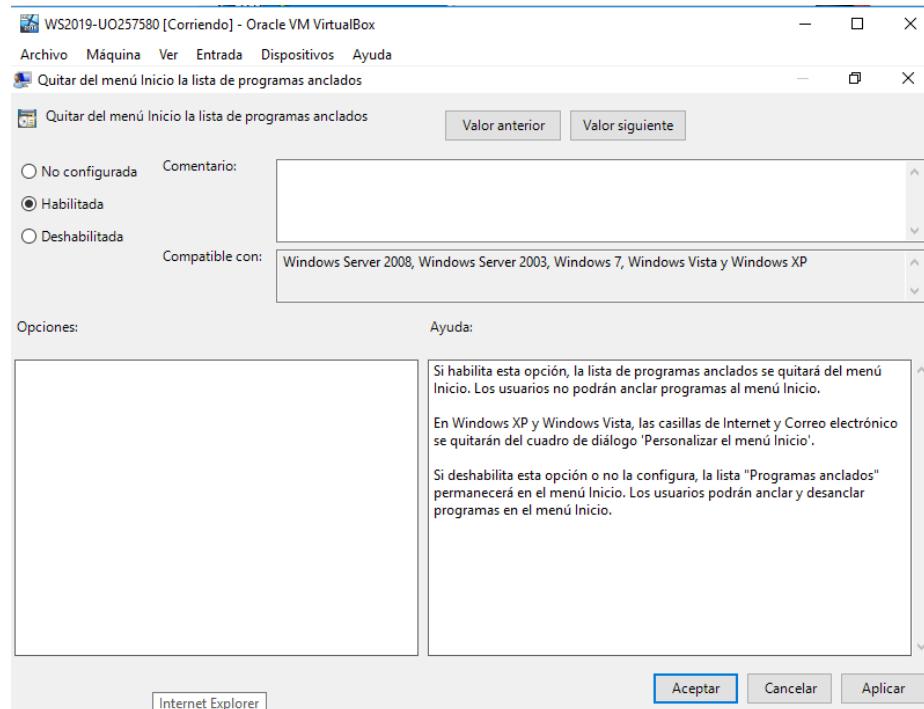
- Habilita el Active Desktop.
 - Además, definir como papel tapiz de Active Desktop utilizando el fichero JPG anterior en estilo "mosaico" (utilizando para ello una ruta UNC).





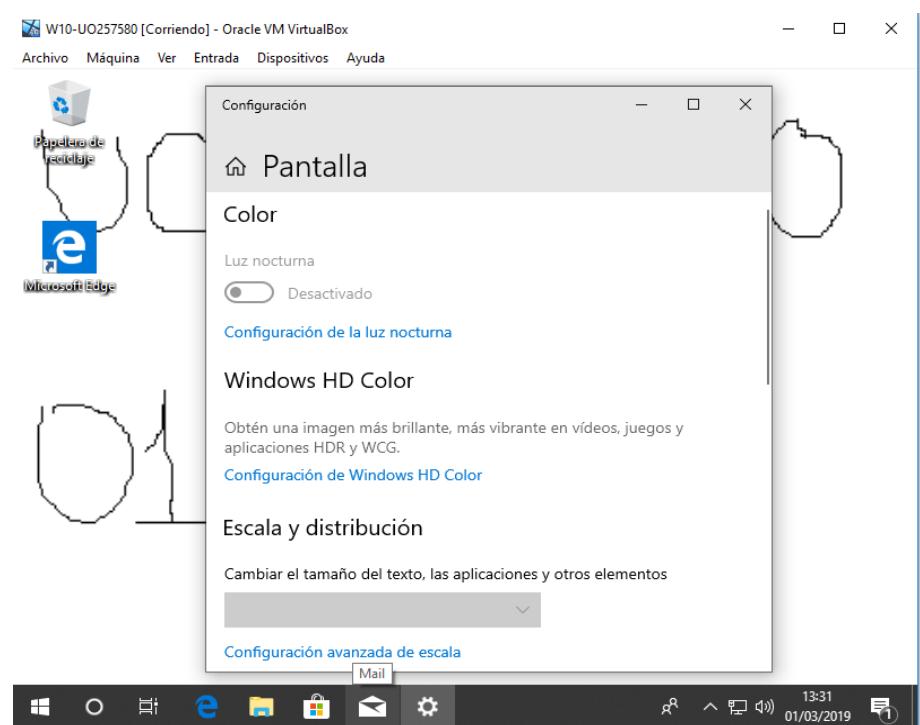
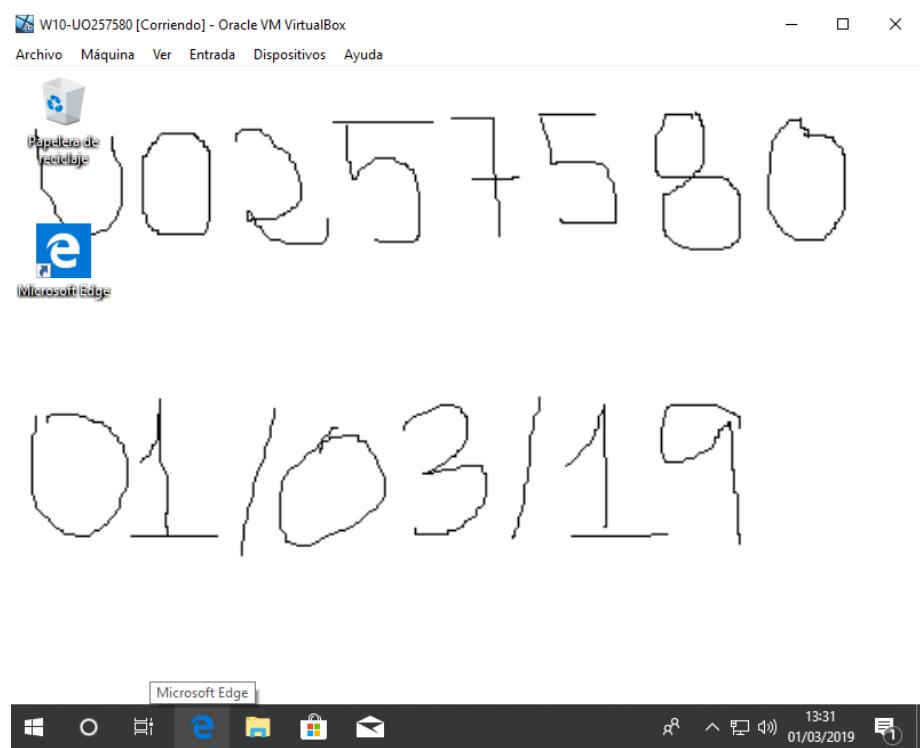
- **Quita también del menú inicio:**
 - "Quitar acceso a los comandos Apagar, reiniciar..., quitar los programas anclados a la barra de tareas."

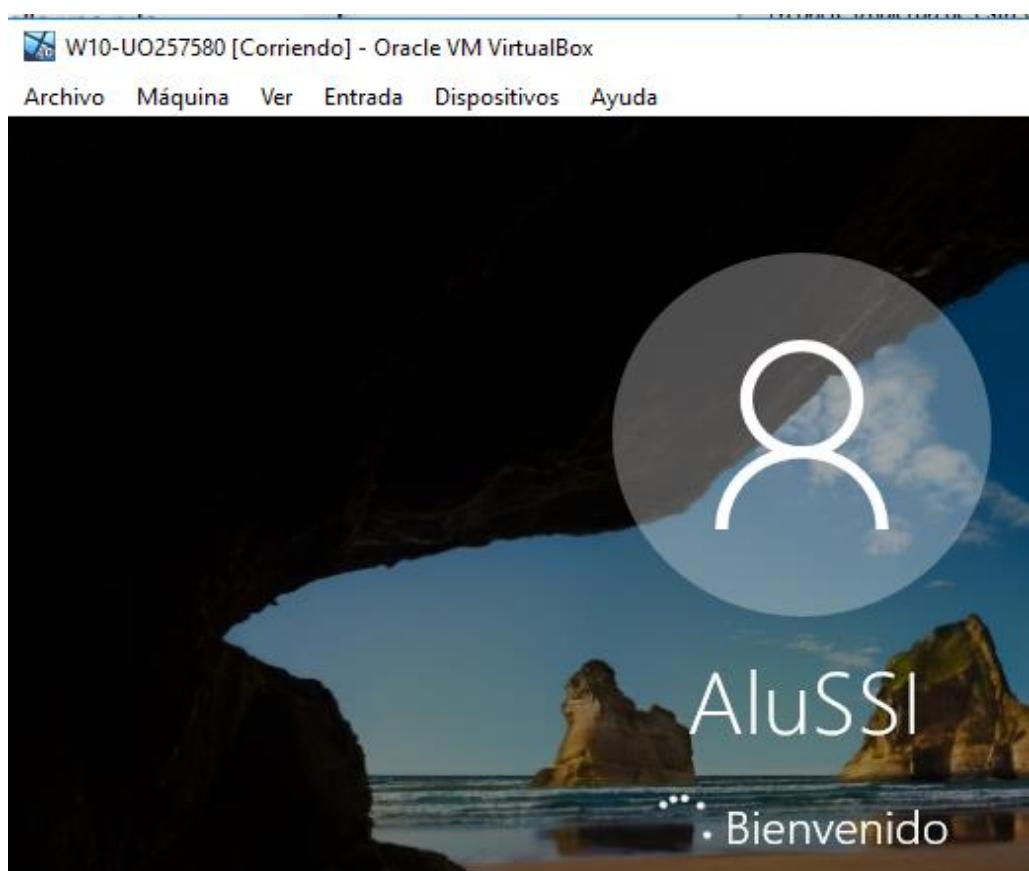
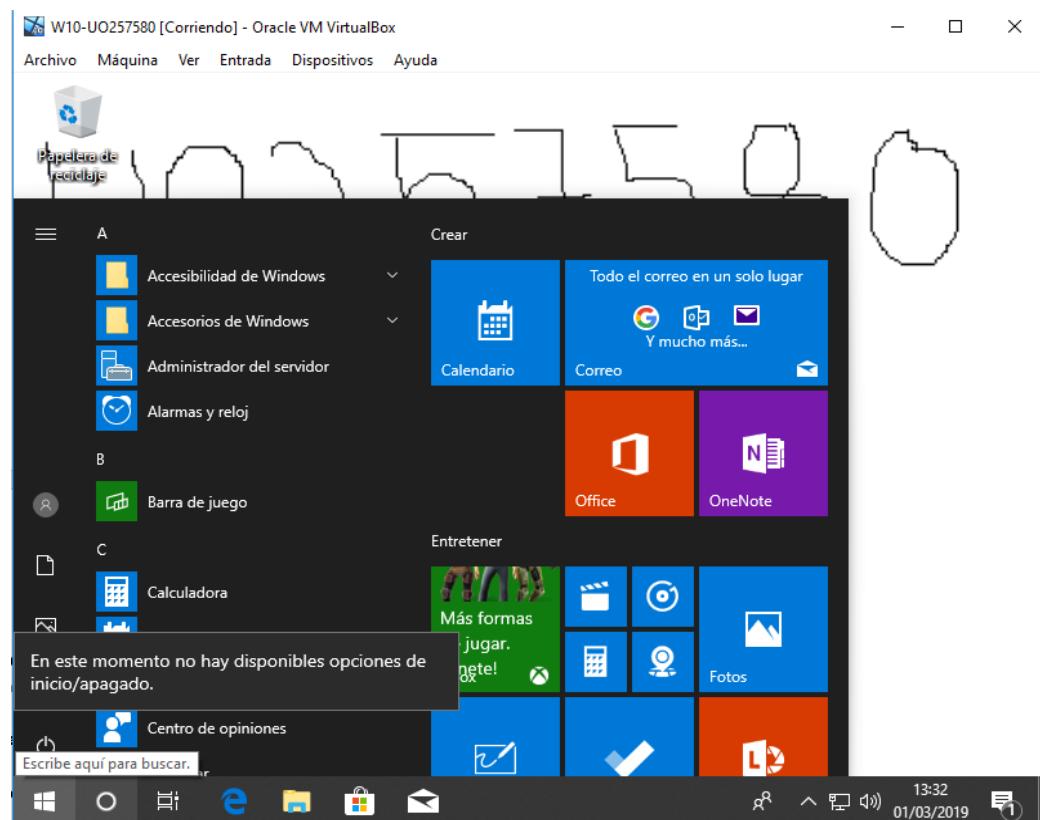


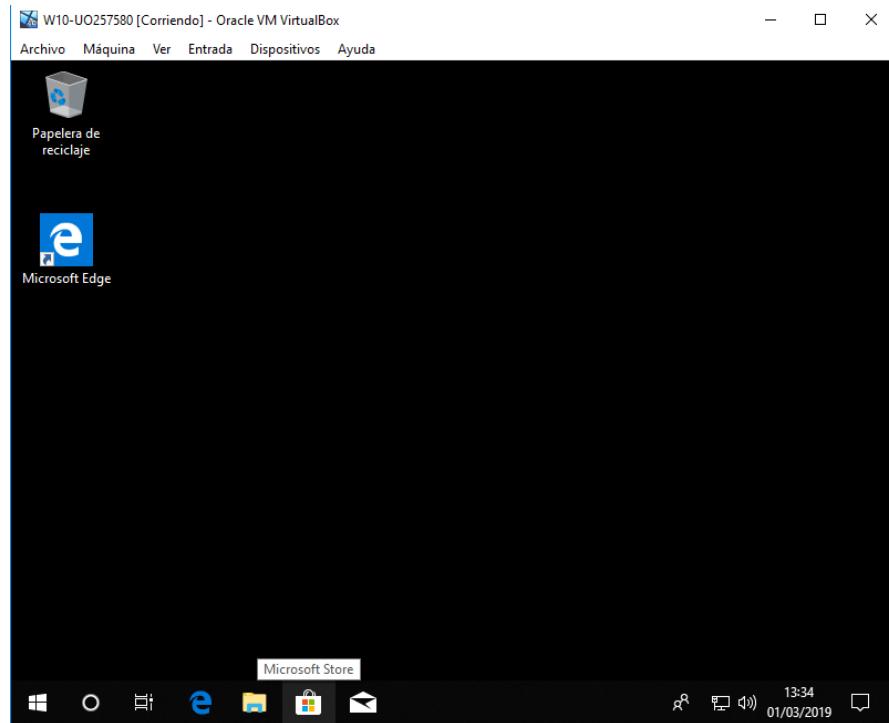


- 4) Inicia sesión en el cliente como profeSSI y estudia los cambios producidos en el escritorio (mira también sus propiedades) y menú inicio (quizá sea necesario reiniciar). Entra con otro usuario que no tenga permiso sobre la carpeta compartida (p.ej AluSSO) y comenta qué ocurre.

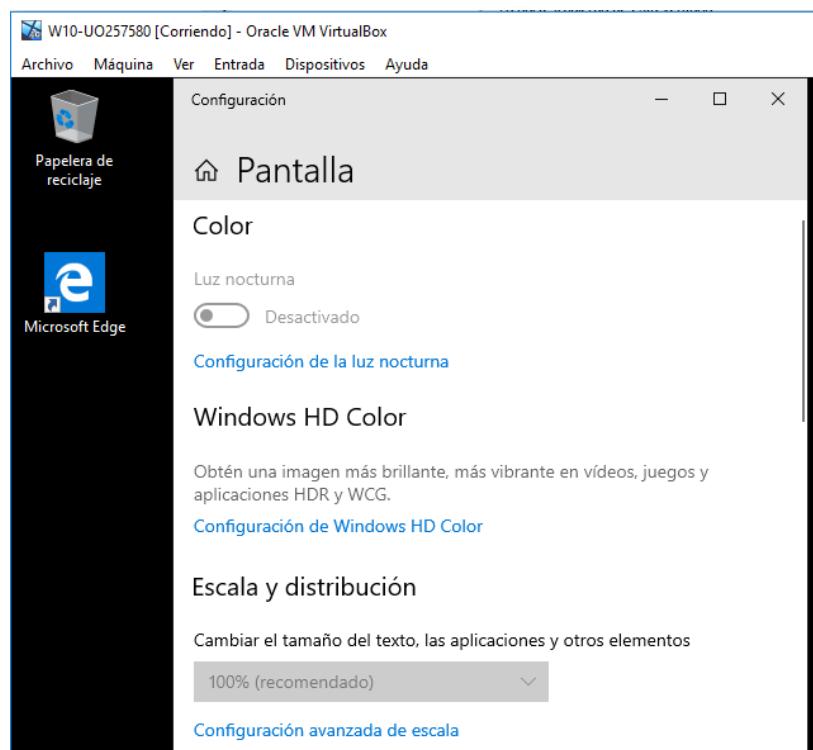


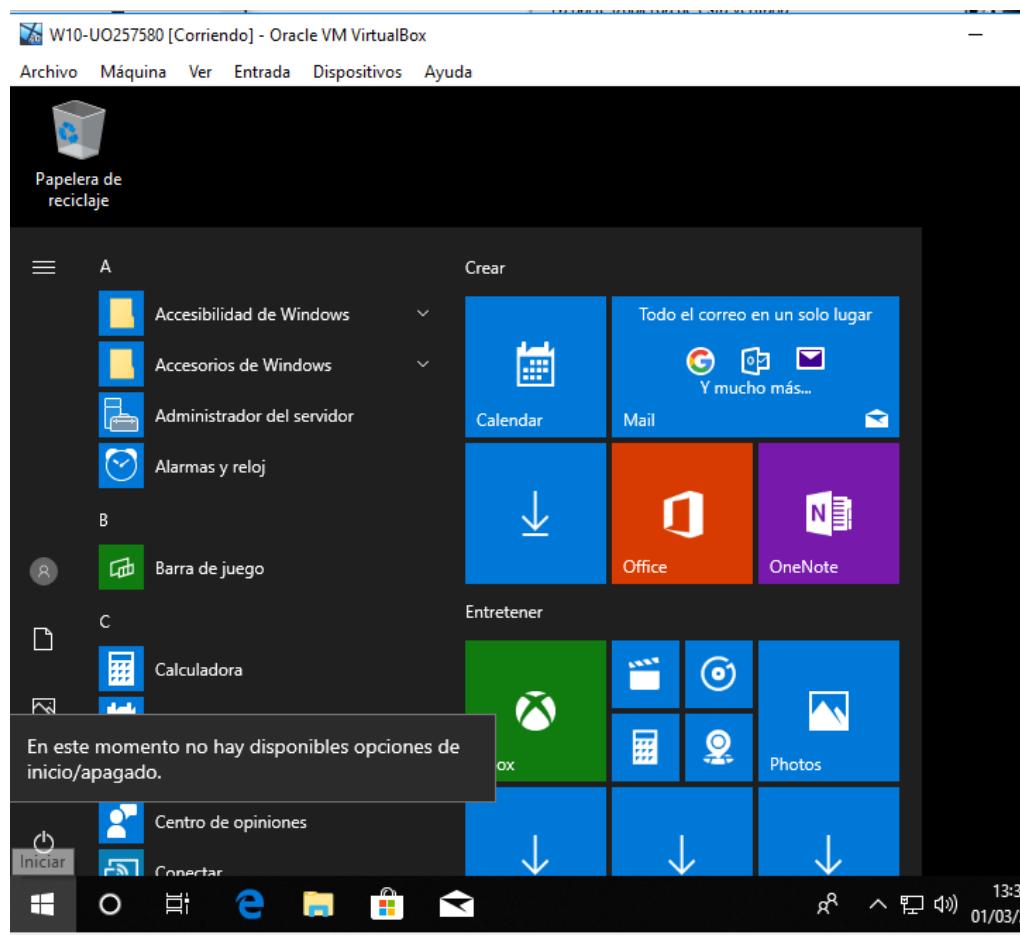






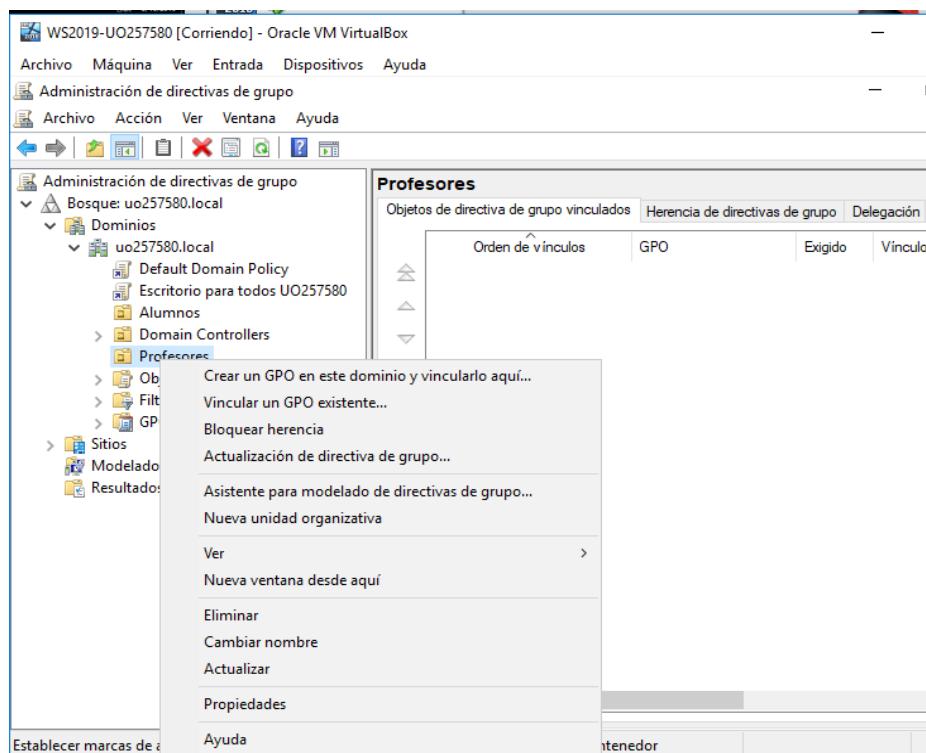
Al no tener ningún permiso sobre la carpeta del Administrador y que esa carpeta no sea compartida con él (AluSSI), no tenemos acceso a la foto, por lo que no podemos visualizarla como fondo de pantalla, por lo que tenemos un fondo de pantalla de color negro.

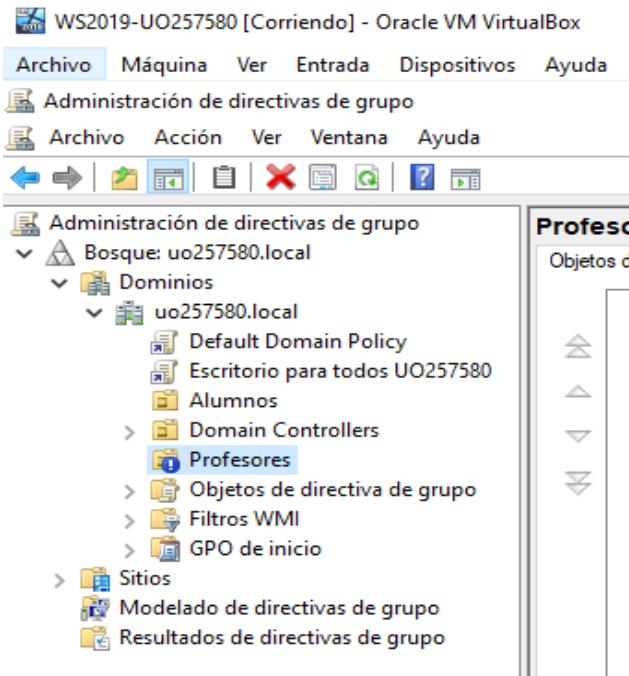




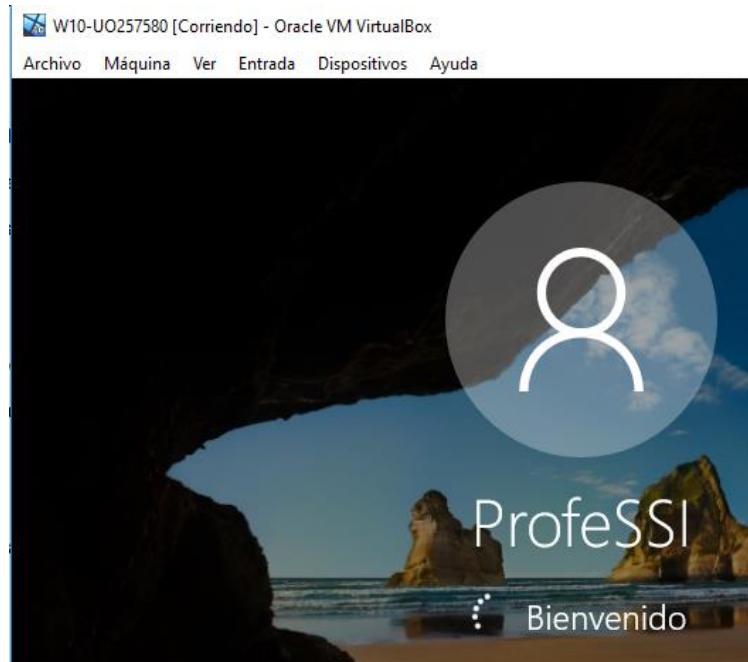
Y tampoco podemos apagar o reiniciar el ordenador.

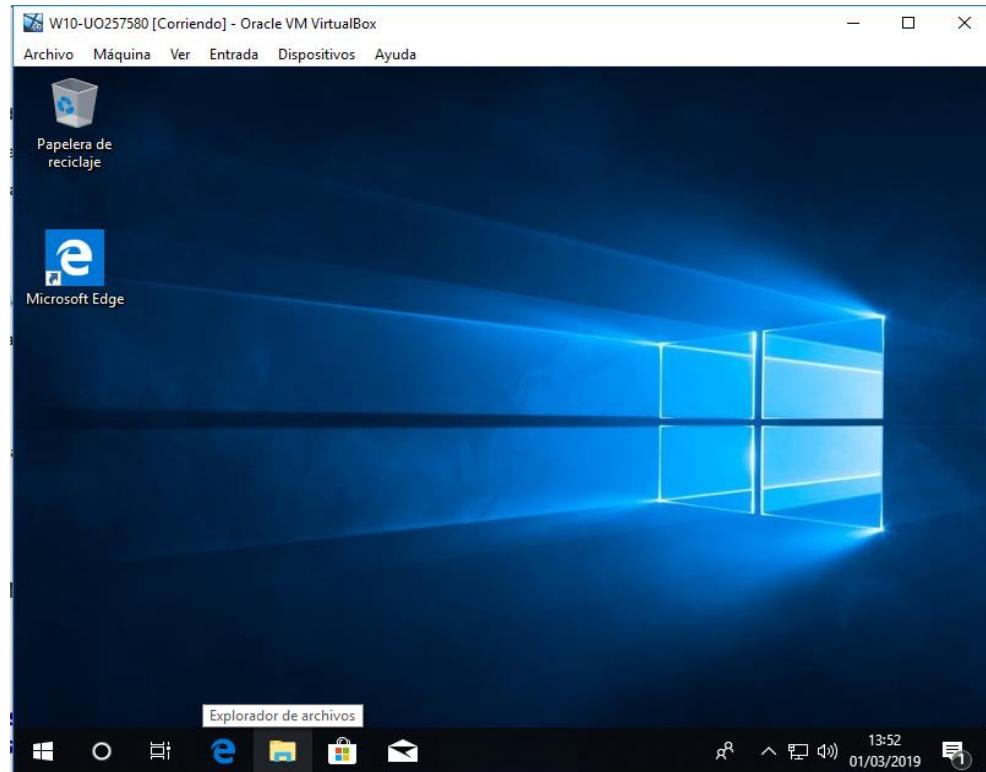
5) Prueba a bloquear la herencia de directivas para la UO "Profesores".



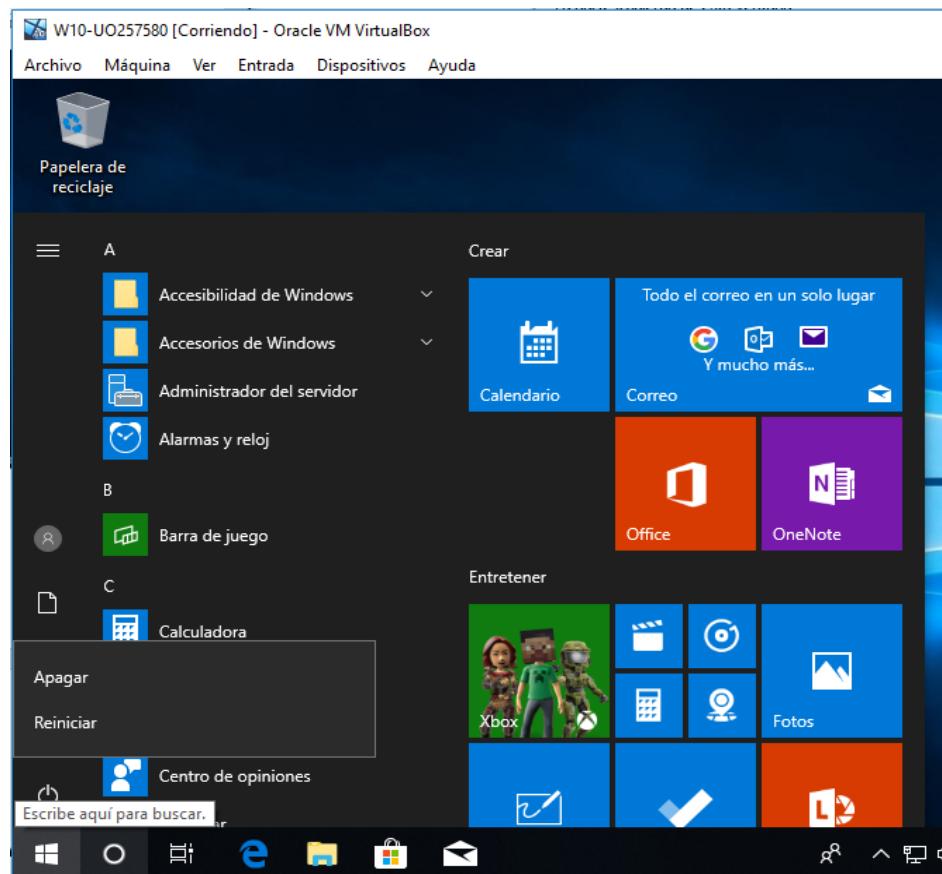


- Inicia de nuevo sesión en W7 como profeSSI y estudia de nuevo los cambios producidos en el escritorio (mira también sus propiedades) y menú inicio (quizá sea necesario reiniciar).



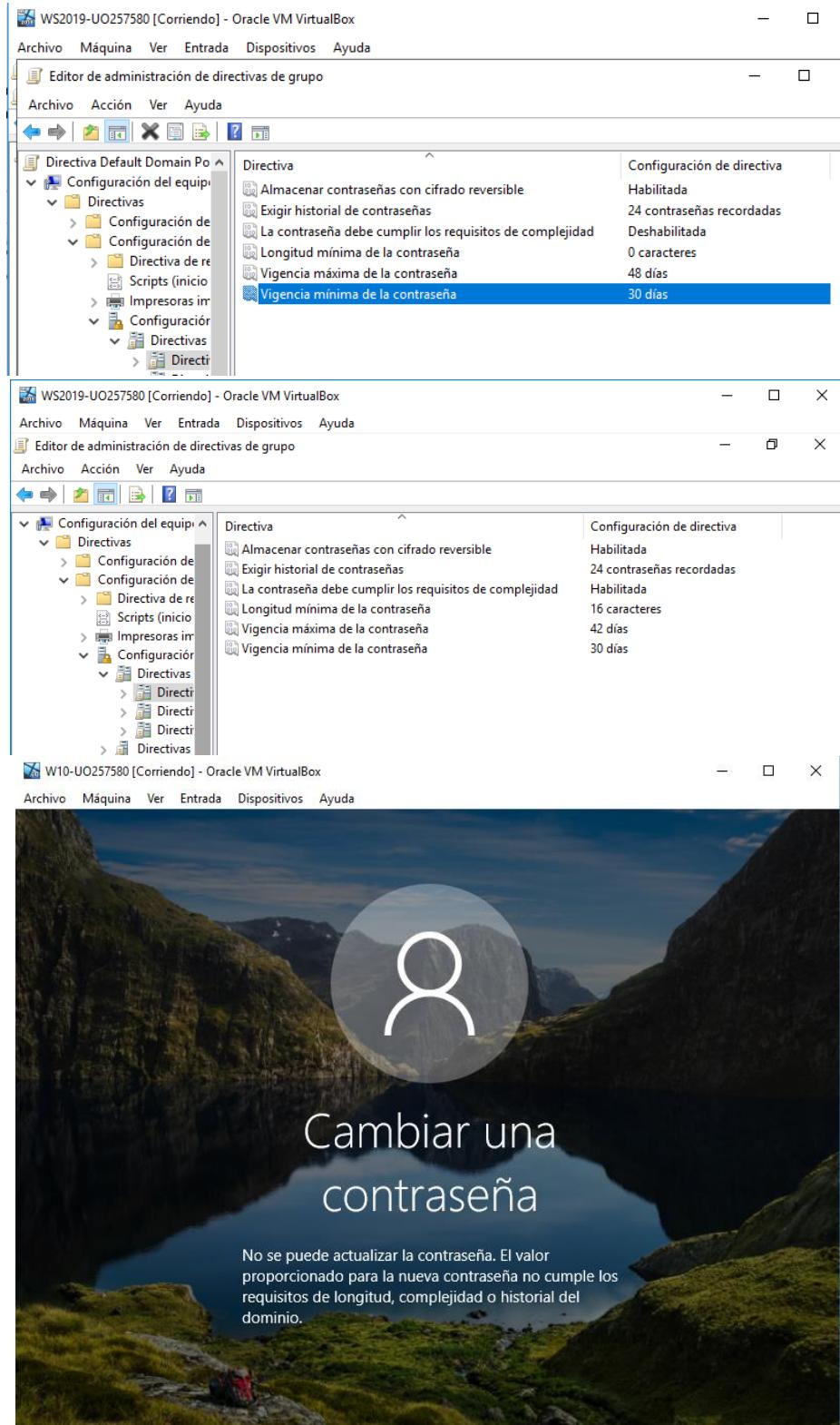


Ahora ya podemos ver el escritorio normal como siempre.



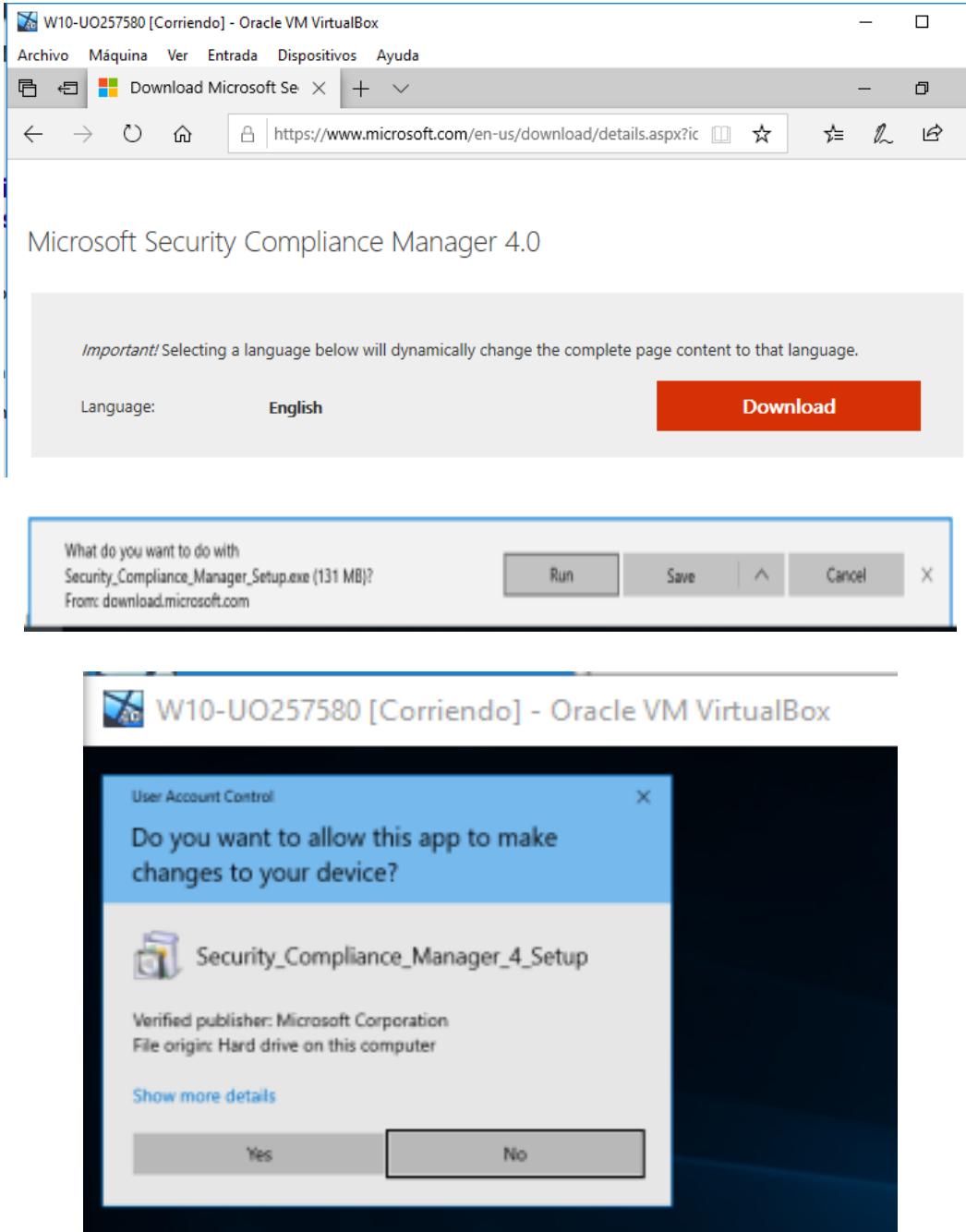
Y podemos tanto apagar como reiniciar el ordenador.

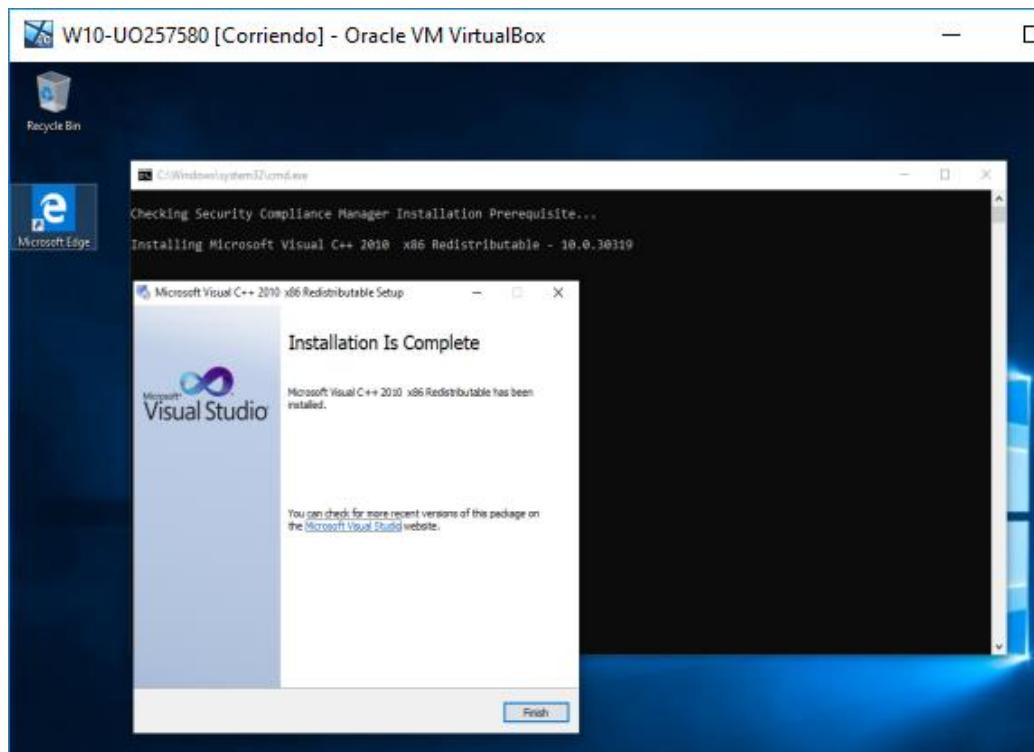
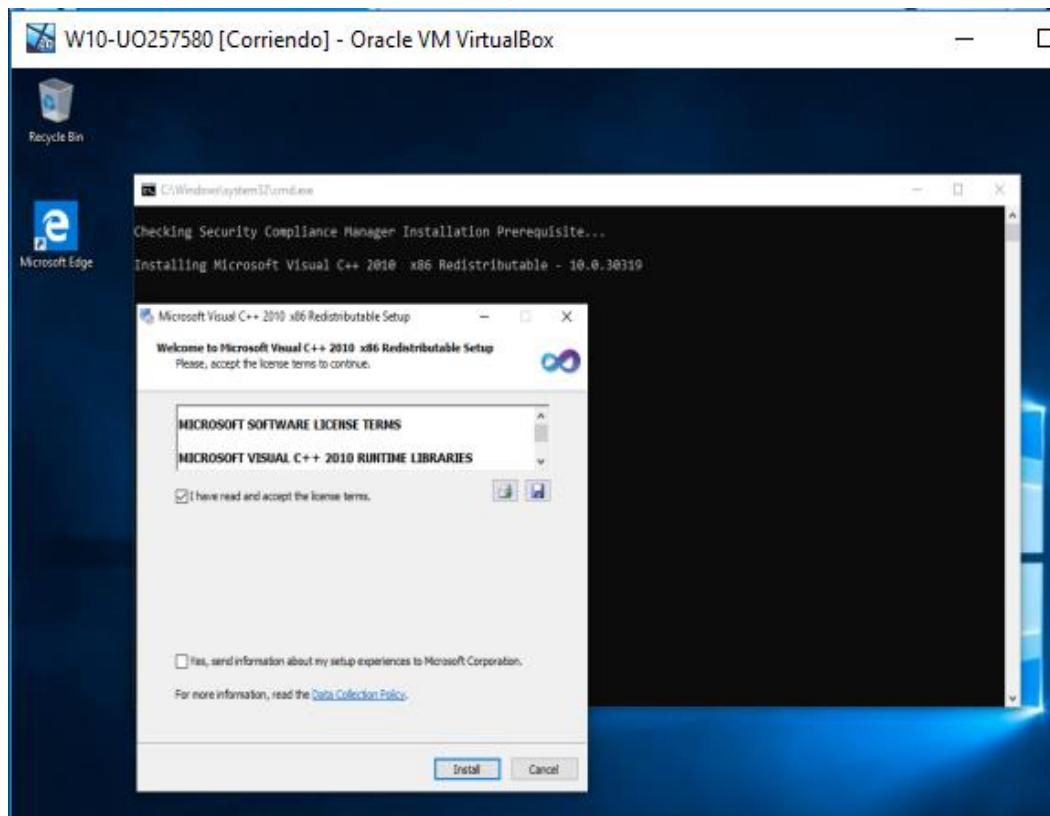
- 6) Cambia la política de contraseñas. Cámbiala a nivel de dominio (sin cumplir requisitos de seguridad) y a nivel de una de las UO que tengas definidas (haciendo que los cumplan). Prueba a cambiar la contraseña de un usuario de esa UO, poniendo una sencilla. ¿Te deja? ¿Por qué?

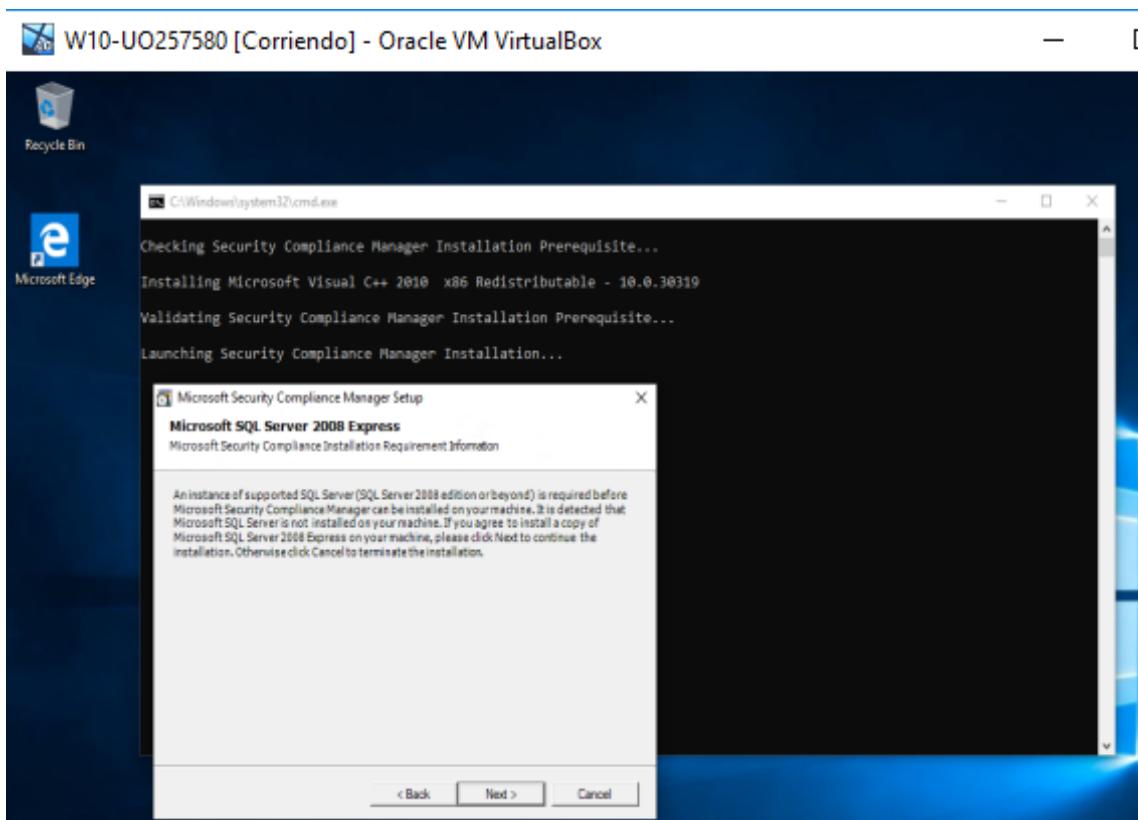
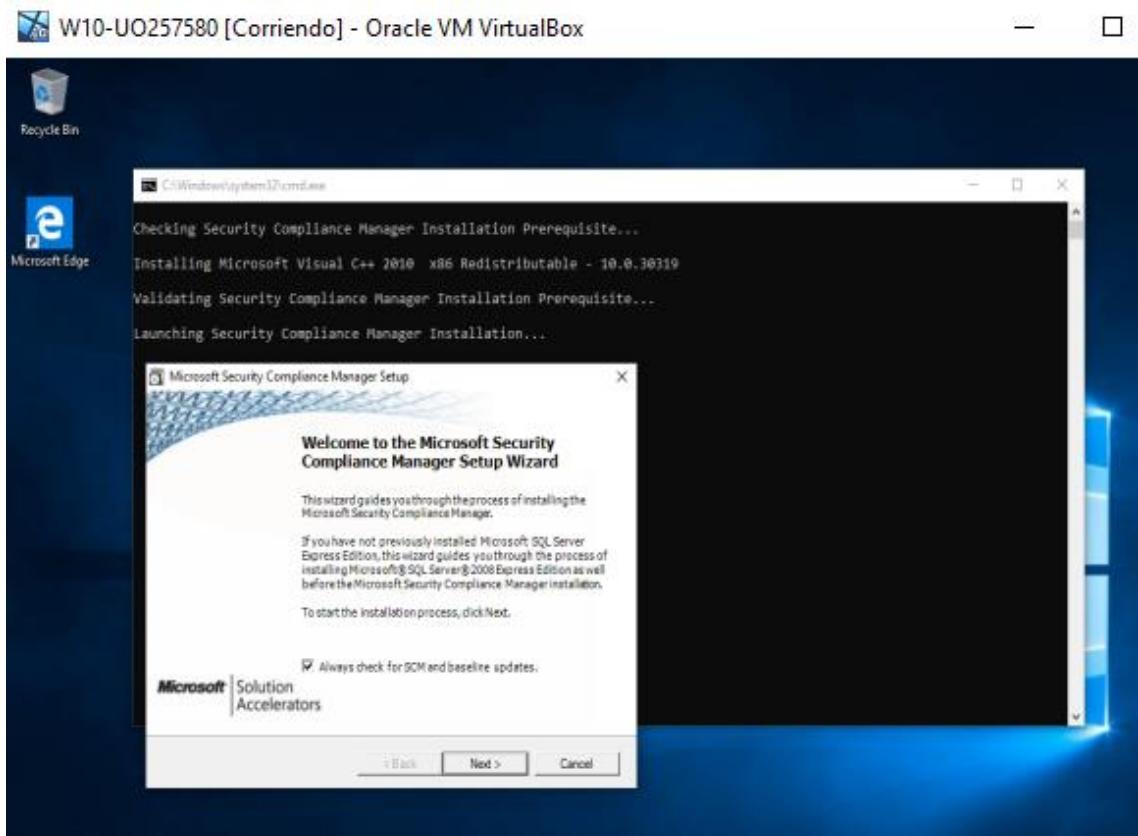


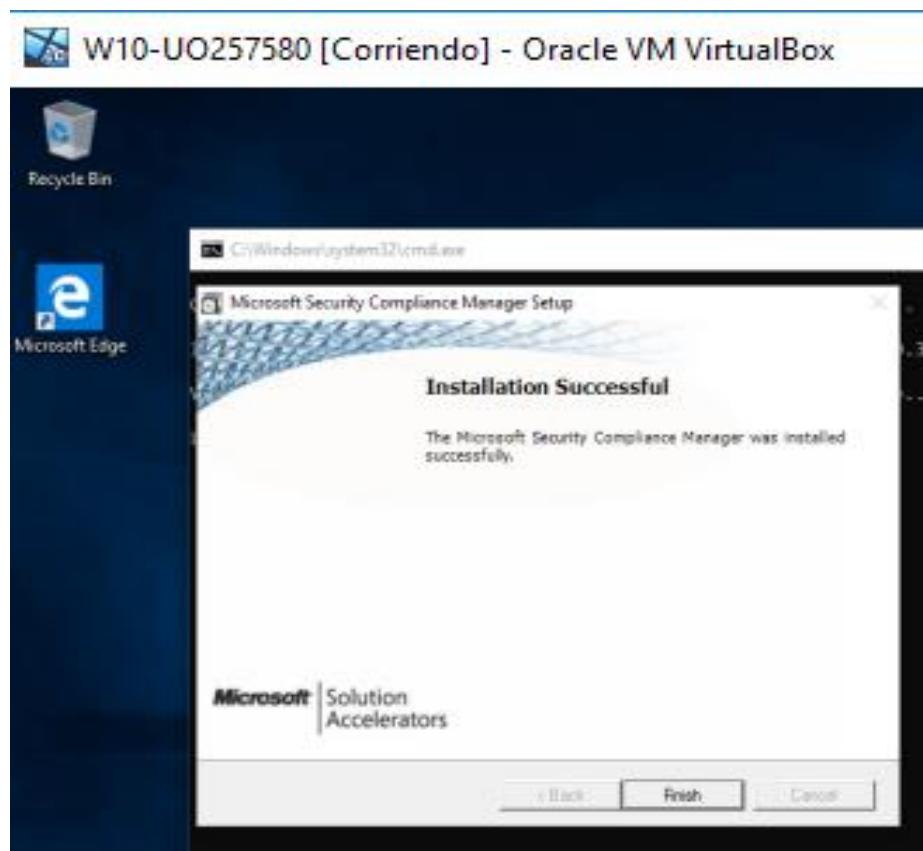
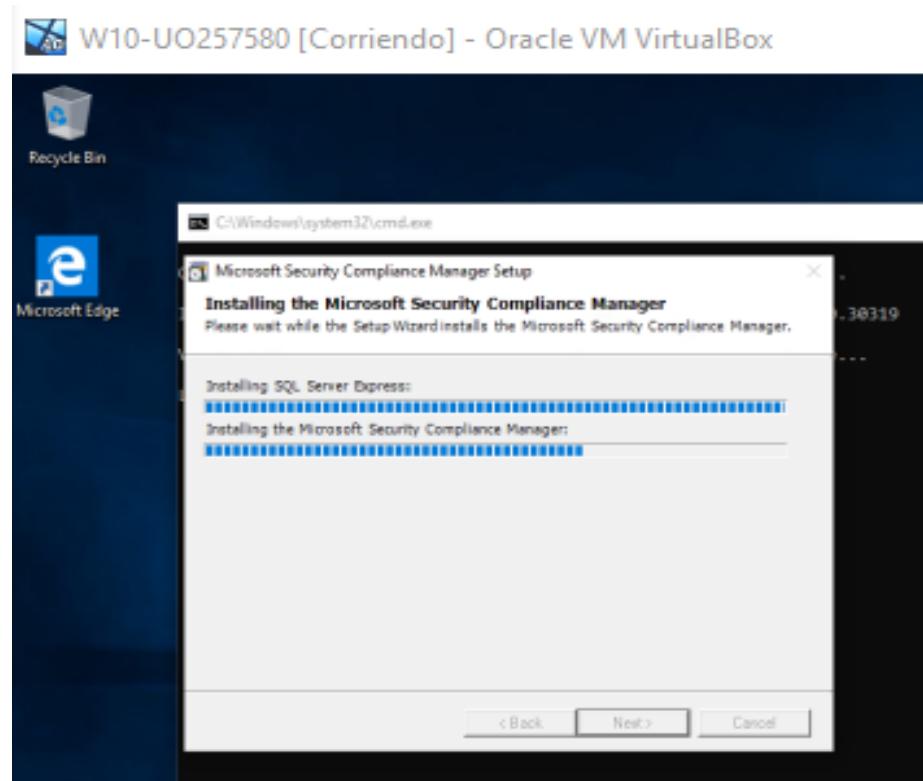
No, no puedo, debido a que no cumple con los requisitos necesarios, debido a que AluSSI pertenece a la UO, que es donde establecí los requisitos de contraseña (los más restrictivos).

- 7) Desde el cliente inicia sesión con la cuenta administrador del dominio e instala el Microsoft Security Compliance Manager (SCM) de la siguiente dirección: <https://www.microsoft.com/en-us/download/details.aspx?id=53353> Si os pide que instaléis el framework .Net, hacedlo. ¡OJO! Al instalar el framework, se leéis bien es necesario volver a ejecutar el instalador SCM.

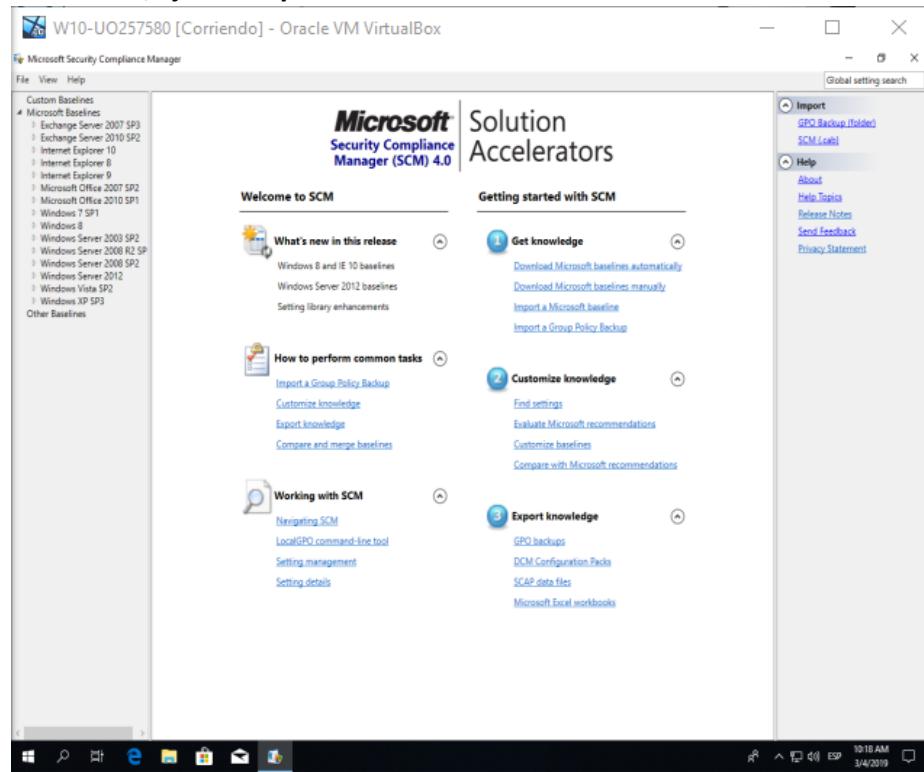




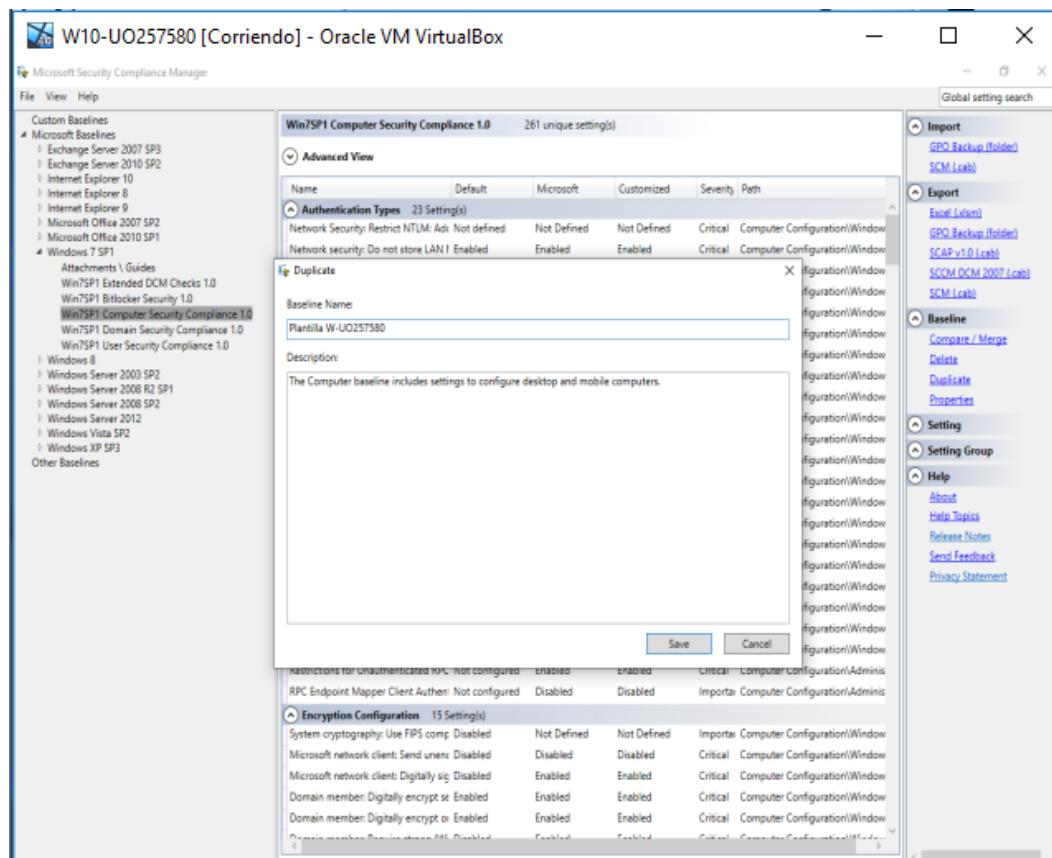




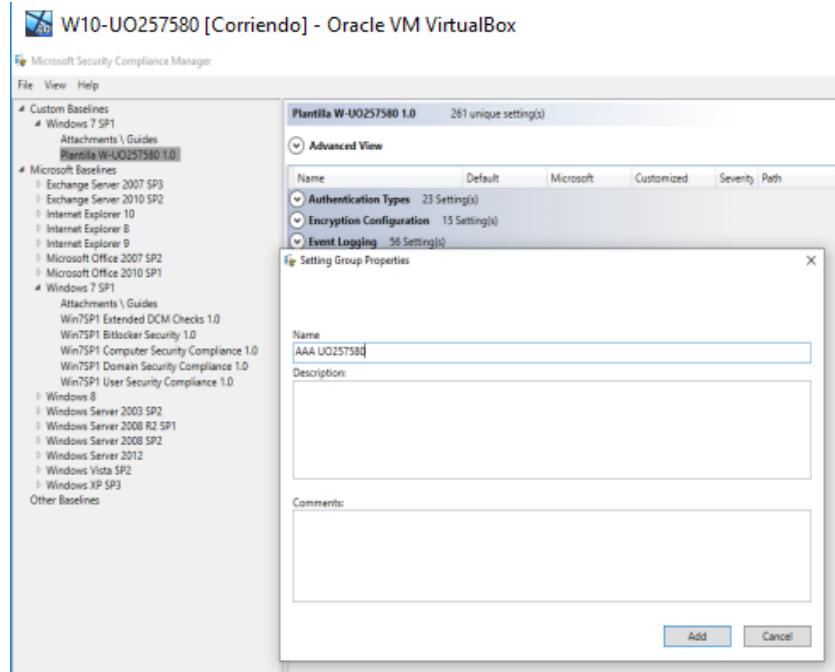
8) Una vez instalado, ejecútalo y:



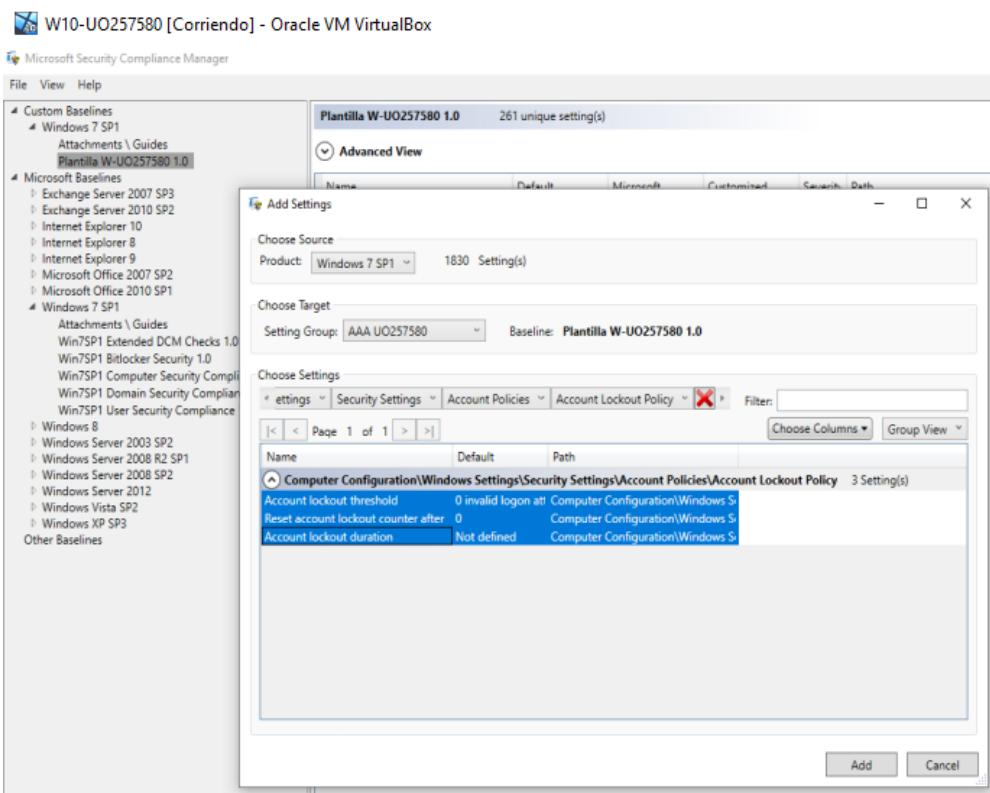
- Duplica la plantilla Win7SP1 Computer Security Compliance 1.0, y llámala Plantilla W-UOXXX (usa tu UO).



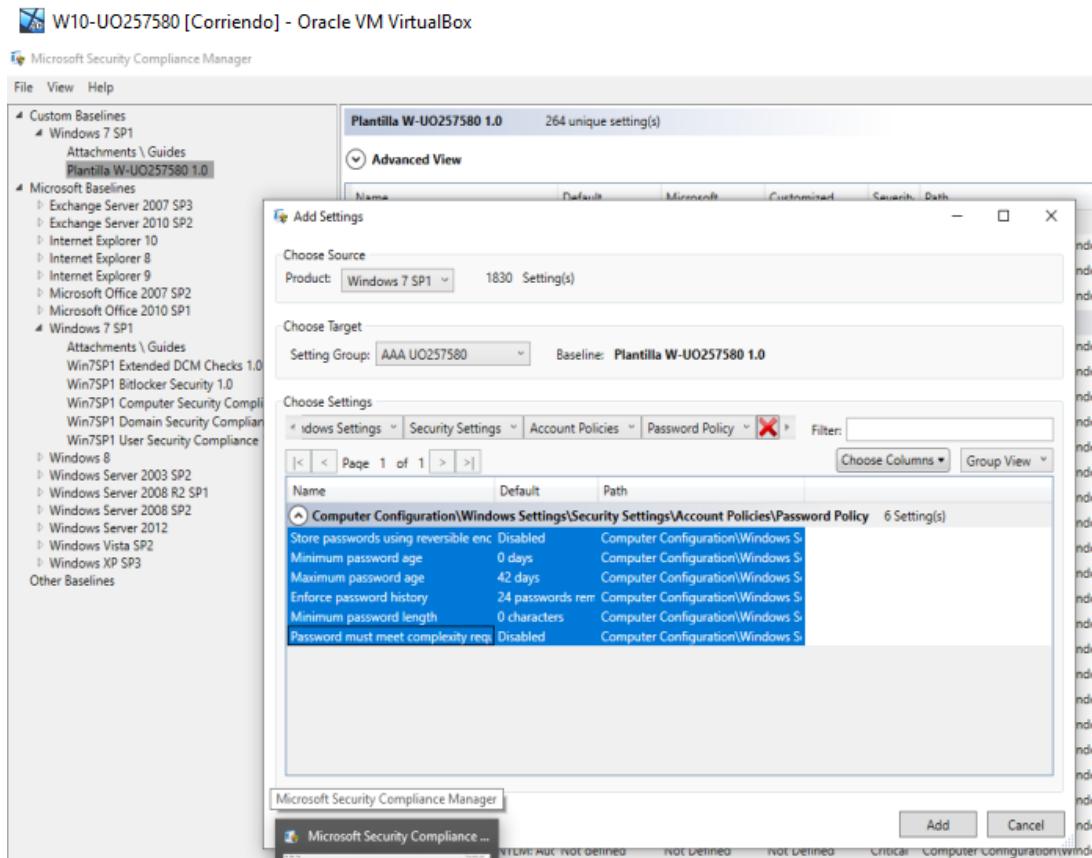
- Edita la plantilla para añadir un Group (Setting Group – Add). Llámalo AAA UOXXX.



- 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:
 - 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.



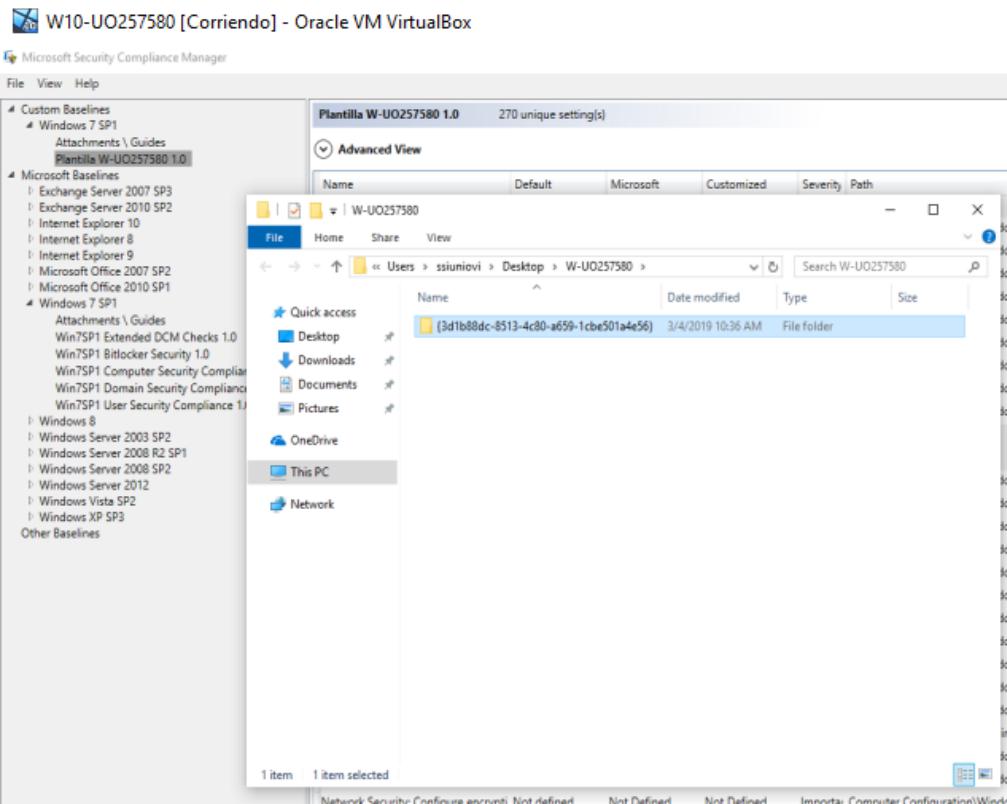
- Edita las propiedades para que:
 - La cuenta se bloquee tras 17 intentos fallidos.
 - La cuenta de accesos fallidos se resetee a cero tras 15 minutos.
 - El bloqueo de cuenta dure 19 minutos.
 - No te deje cambiar contraseñas de menos de 3 días.
 - Hay que cambiar la contraseña cada 30 días.
 - Recuerde 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).

The screenshot shows the Microsoft Security Compliance Manager interface. On the left, there's a navigation pane with sections like 'Custom Baselines' and 'Microsoft Baselines'. Under 'Custom Baselines', 'Windows 7 SP1' is expanded, showing various guides and a specific baseline named 'Plantilla W-UO257580 1.0'. The main pane displays the details of this baseline under 'Advanced View'. It lists 270 unique settings, including account lockout thresholds, password policies, and various security configurations. The table columns include Name, Default, Microsoft, Customized, Severity, and Path.

Name	Default	Microsoft	Customized	Severity	Path
AAA UO257580 9 Setting(s)					
Account lockout threshold	0 invalid logon at	17	Critical	Computer Configuration\Window	
Reset account lockout counter after	0	15	Critical	Computer Configuration\Window	
Account lockout duration	Not defined	19	Critical	Computer Configuration\Window	
Store passwords using reversible enc	Disabled	Not Defined	Critical	Computer Configuration\Window	
Minimum password age	0 days	3	Critical	Computer Configuration\Window	
Maximum password age	42 days	30	Critical	Computer Configuration\Window	
Enforce password history	24 passwords rem	15	Critical	Computer Configuration\Window	
Minimum password length	0 characters	10	Critical	Computer Configuration\Window	
Password must meet complexity requi	Disabled	Enabled	Critical	Computer Configuration\Window	

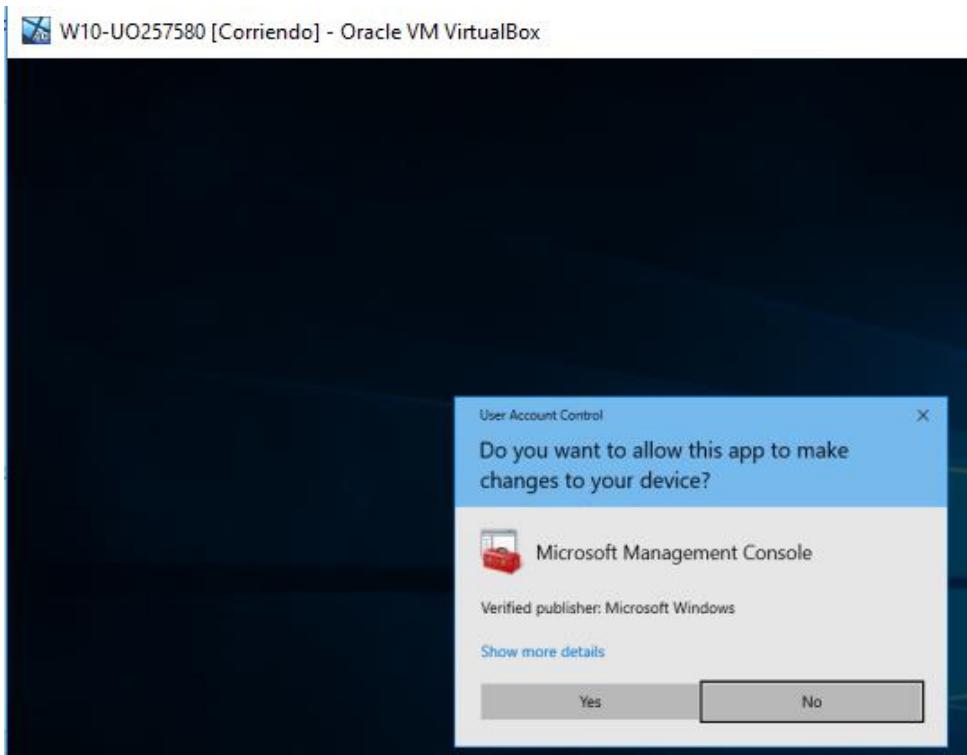
- **Exporta la plantilla como una GPO. Crea para ello una carpeta (por ejemplo, en el escritorio) que se llame como la plantilla y exporta allí.**

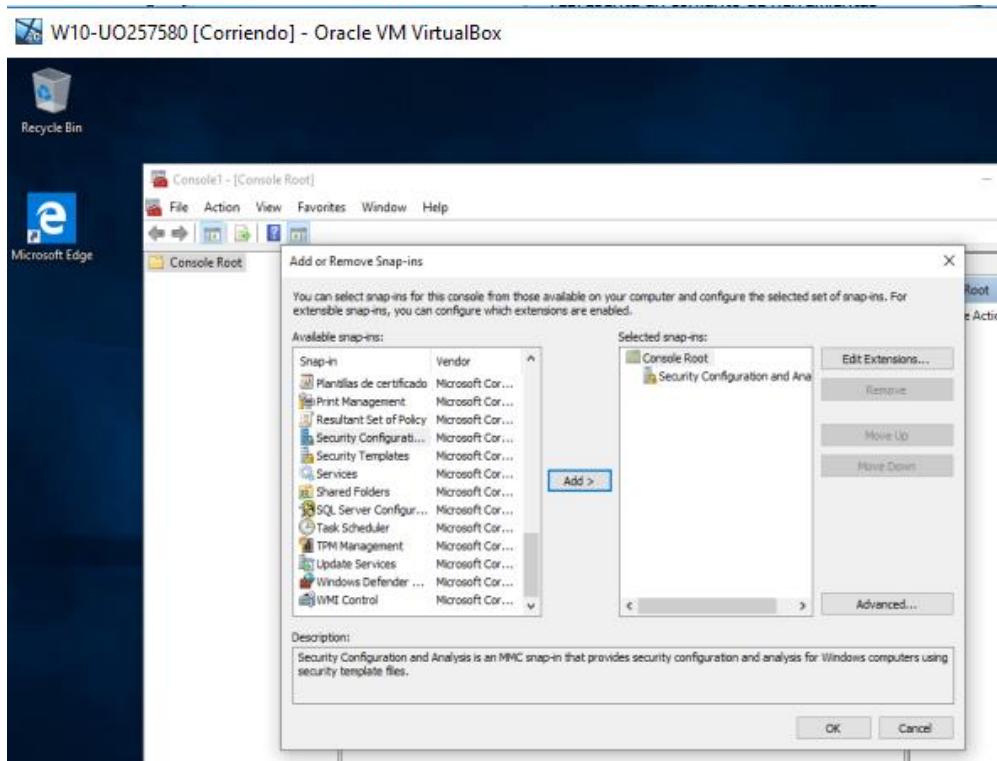
This screenshot shows the 'Browse For Folder' dialog box overlaid on the Microsoft Security Compliance Manager interface. The dialog is titled 'Export GPO Backup (folder)' and shows a tree view of a local drive. The path 'W-UO257580' is selected under 'Desktop'. The main interface on the left shows the same 'Advanced View' of the 'Plantilla W-UO257580 1.0' baseline with its 270 settings listed.



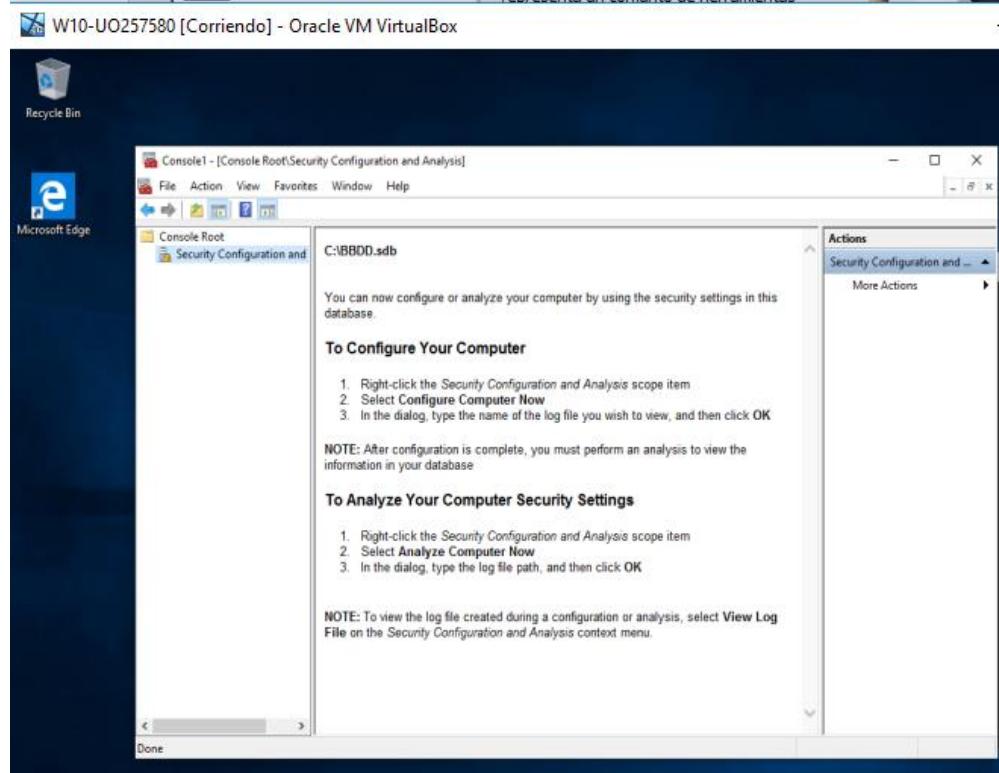
9) Utilizar la plantilla de seguridad creada anteriormente en el equipo local.

- En la máquina W10 (como Administrador) ejecutar mmc; agrega el complemento Configuración y análisis de seguridad.

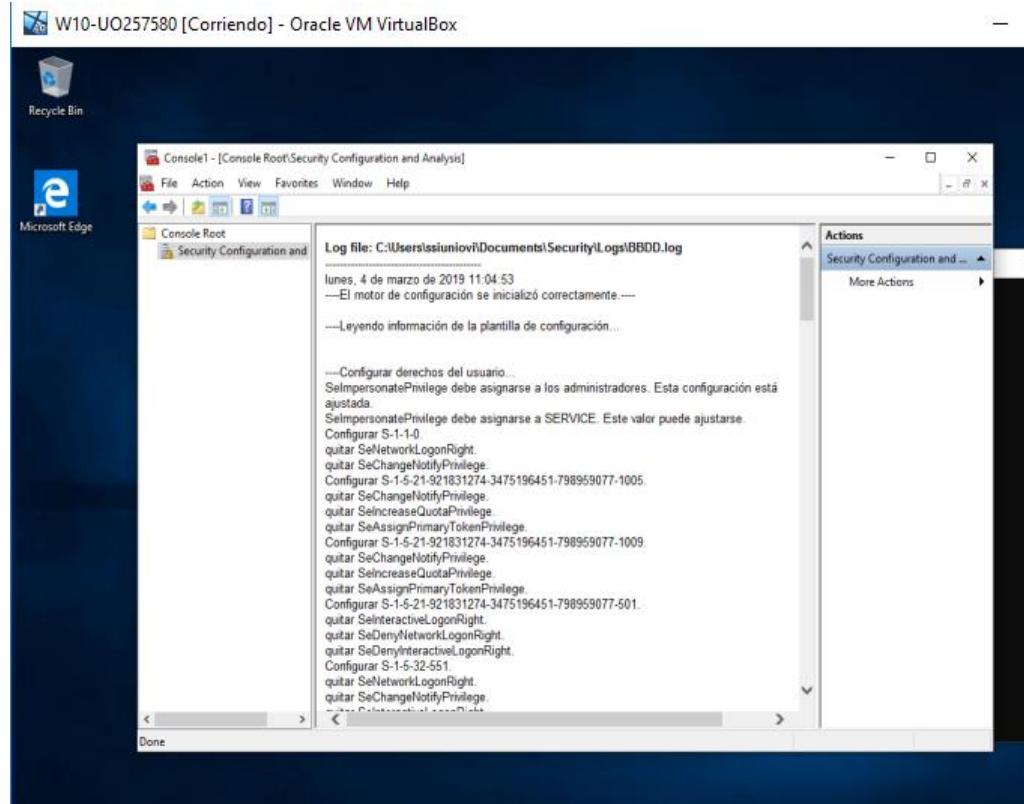




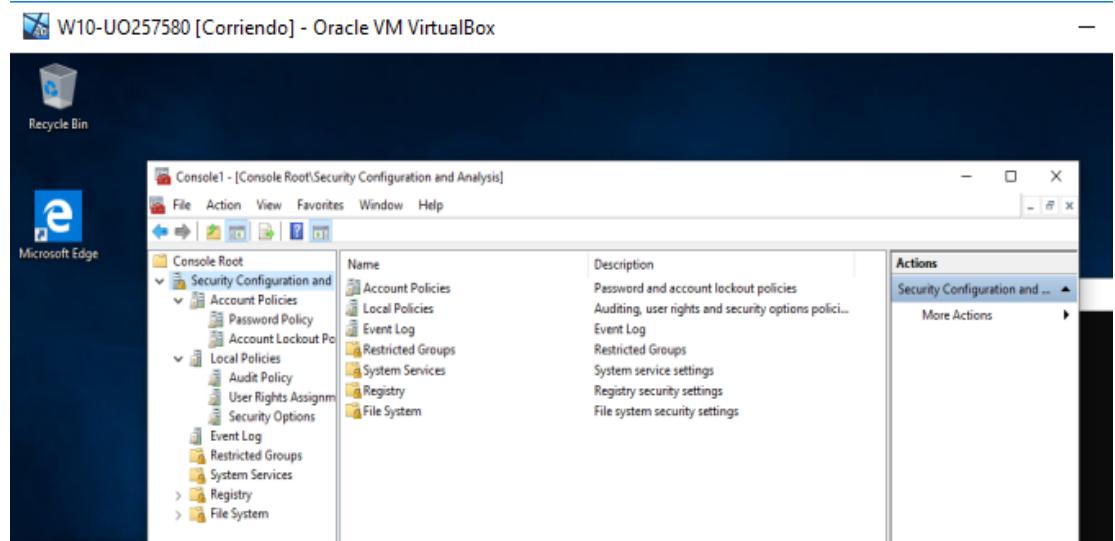
- Abrir base de datos (dar un nombre para una base de datos nueva) e importar la plantilla creada anteriormente.

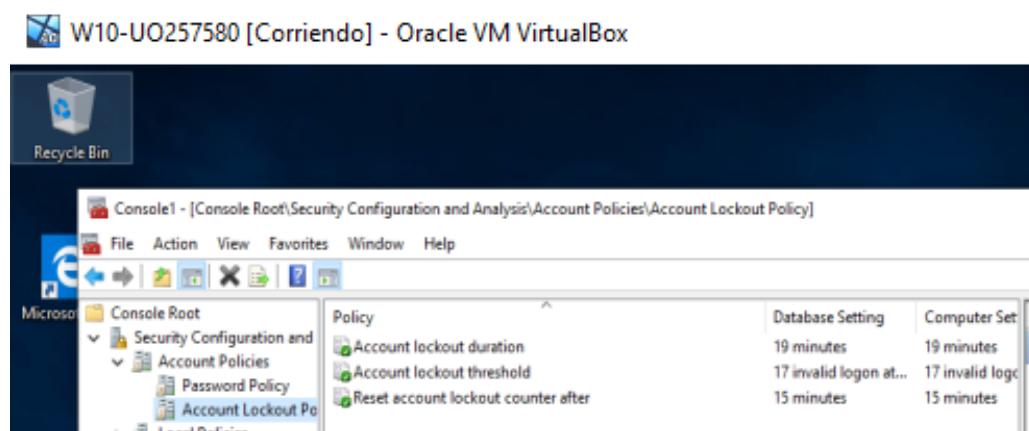
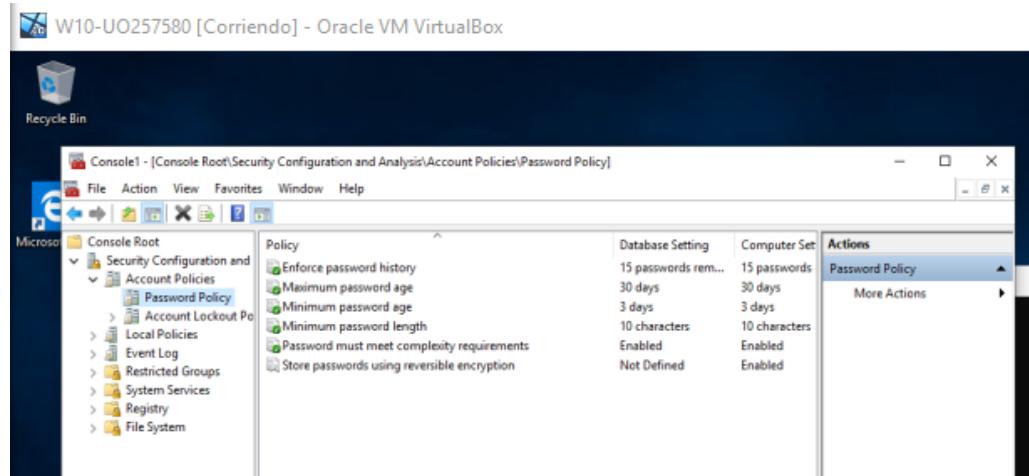


- Comprobar que se ha importado correctamente (las propiedades que se han definido anteriormente deben reflejarse). Analizar el equipo y mostrar mediante una captura que se ha analizado el equipo.



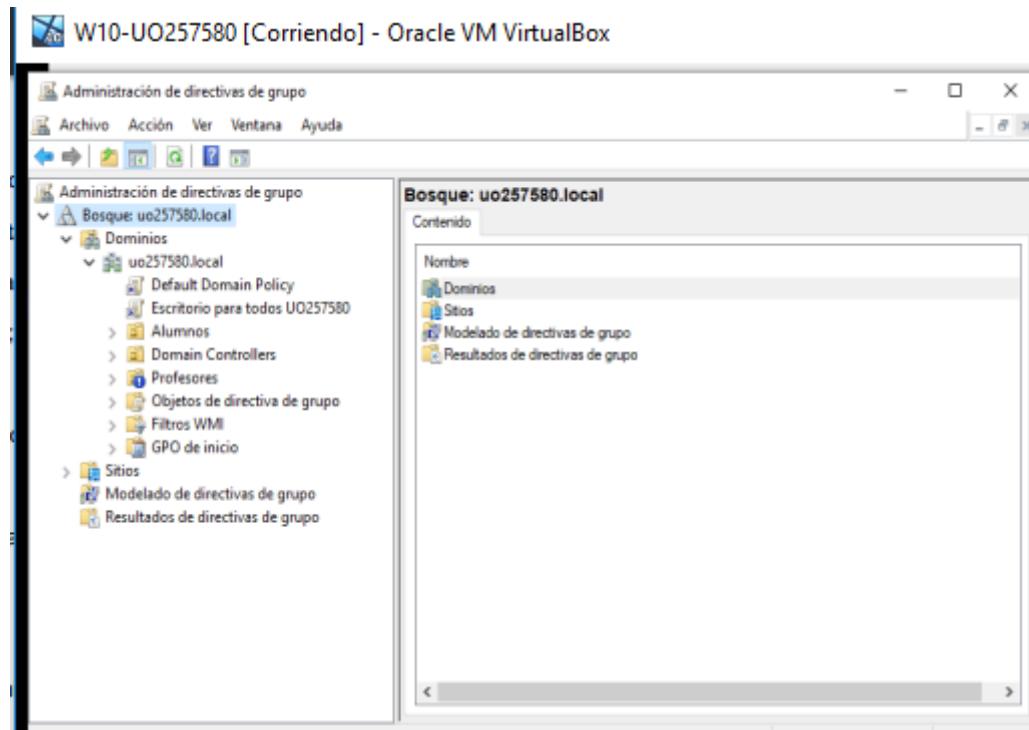
- Configurar equipo, analizar equipo y mostrar mediante una captura que se ha analizado el equipo y ahora sí que coinciden las configuraciones del equipo y la plantilla.



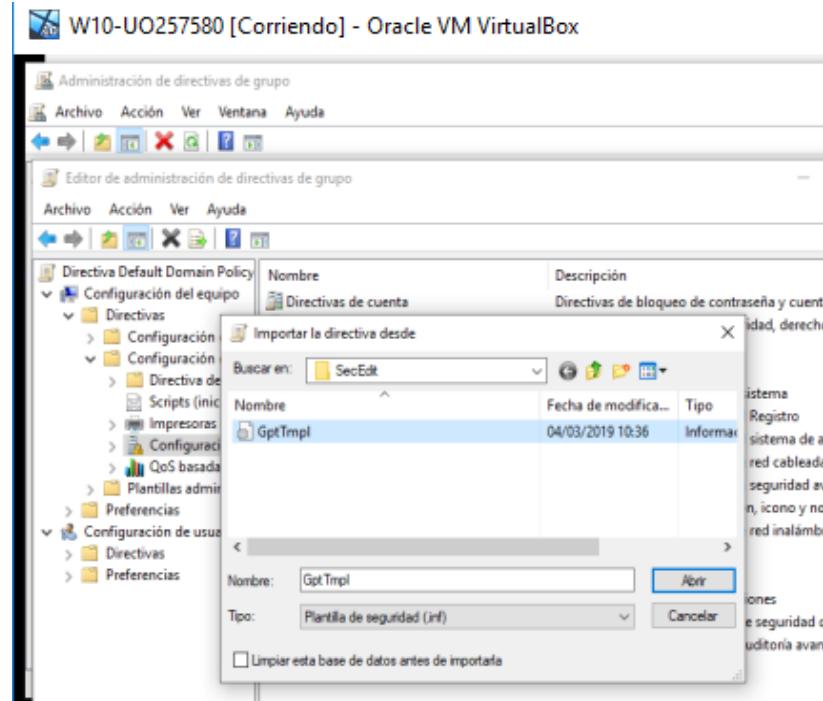


10) Utilizar la plantilla de seguridad creada anteriormente en el dominio.

- En el Cliente 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.

