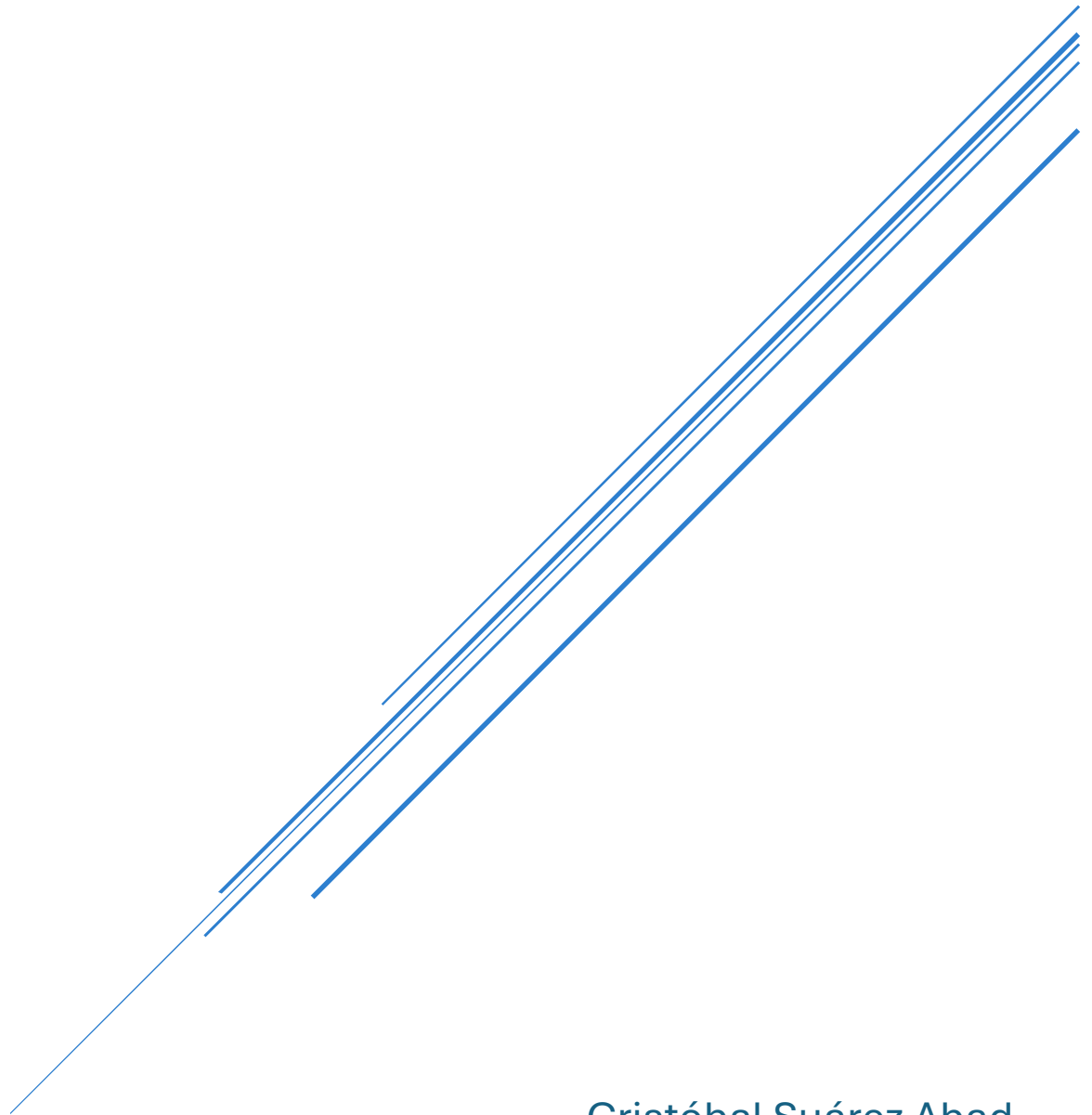


ACTIVIDAD 1.2 ACTIVE DIRECTORY

Administración de Dominios, Confianzas y Perfiles
Móviles en Windows Server



Cristóbal Suárez Abad
Administración de Sistemas Operativos – 2º ASIR

Índice:

- 1) Controlador de dominio secundario (Réplica).
 - a) Partiendo de un dominio funcional, instala un segundo servidor Windows Server y conviértelo en controlador de dominio secundario del dominio existente.
 - i) Configurar el Servidor DNS del controlador de dominio principal.
 - ii) Unión de Réplica como Cliente.
 - iii) Instalación de Active Directory en el futuro servidor Réplica.
 - b) Configura la replicación de Active Directory y comprueba su funcionamiento.
 - i) Crea un usuario en el controlador principal y verifica que aparece en el secundario.
 - ii) Simula la caída del servidor principal y valida que los usuarios siguen autenticándose.
- 2) Subdominio.
 - a) Crea un nuevo servidor y configúralo como child domain.
 - b) Configura y verifica la relación de confianza entre el dominio padre y el hijo.
 - i) Realiza pruebas de inicio de sesión con usuarios del dominio padre en equipos unidos al hijo y viceversa.
- 3) Bosque.
 - a) Configura un nuevo servidor y crea un dominio raíz de un bosque diferente.
 - b) Establece una relación de confianza bidireccional y transitiva entre ambos bosques.
 - c) Comprueba la autenticación cruzada creando usuarios en ambos bosques y validando el acceso a recursos compartidos.
 - d) Para comprobar que funciona, intenta acceder a recursos compartidos entre dominios con diferentes usuarios.
- 4) Perfiles móviles de usuario.
 - a) En el dominio principal, habilita un recurso compartido centralizado.
 - b) Modifica las propiedades de varios usuarios en Active Directory Users and Computers para que usen perfiles móviles.
 - c) Inicia sesión con los usuarios en diferentes equipos unidos al dominio y comprueba.

- 5) Escenario avanzado de pruebas.
- a) Crea un usuario en el subdominio y configura su perfil móvil en el dominio principal. Verifica si puede acceder desde equipos unidos al subdominio.
 - b) Crea un usuario en el bosque alternativo y prueba si puede usar perfiles móviles almacenados en el dominio principal mediante relaciones de confianza.
 - c) Establece políticas de grupo (GPO) para redirigir carpetas (Documentos, Escritorio) hacia carpetas de red y comprueba que funcionan junto con los perfiles móviles.

1) Controlador de dominio secundario (Réplica).

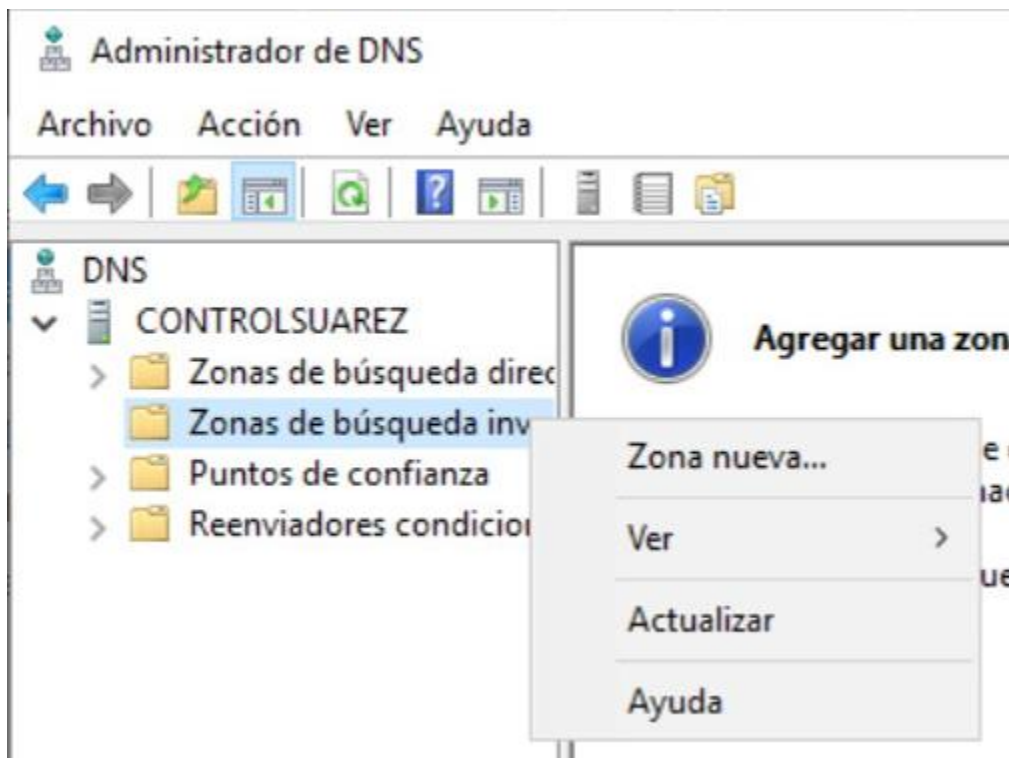
- a) Partiendo de un dominio funcional, instala un segundo servidor Windows Server y conviértelo en controlador de dominio secundario del dominio existente.

i) Configurar el Servidor DNS del controlador de dominio principal.

“El primer paso, será configurar el servidor DNS del primer controlador de dominio (el único que tenemos hasta ahora), para que atienda las solicitudes del rango de direcciones IP que forman nuestra red.”¹

Vamos a: **Administrador del Servidor → Herramientas → DNS.**

Desplegamos el nombre del Dominio y en “**Zonas de búsqueda inversa**” le damos a “**Zona nueva**”.



¹ <https://somebooks.es/anadir-un-nuevo-controlador-de-dominio-para-un-dominio-existente-en-windows-server-2019-parte-1/>

Ahora se abrirá el asistente de creación de una Zona nueva:

Tipo de zona: **Zona principal**.

Asistente para nueva zona

Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.

Seleccione el tipo de zona que quiere crear:

☒ Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.

☐ Zona secundaria
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores principales y proporciona tolerancia a errores.

☐ Zona de rutas internas
Crea una copia de zona que contiene solo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.

☒ Almacenar la zona en Active Directory (solo disponible si el servidor DNS es un controlador de dominio grabable)

< Atrás Siguiendo > Cancelar

Ámbito de replicación: **Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: ASIR_SUAREZ.aso**

Asistente para nueva zona

Ámbito de replicación de zona de Active Directory
Puede seleccionar cómo desea que se repliquen los datos DNS por la red.

Seleccione cómo quiere que se repliquen los datos de zona:

- ☐ Para todos los servidores DNS que se ejecutan en controladores de dominio en este bosque: ASIR_SUAREZ.aso
- ☒ Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: ASIR_SUAREZ.aso
- ☐ Para todos los controladores de dominio en este dominio (para compatibilidad con Windows 2000): ASIR_SUAREZ.aso
- ☐ Para todos los controladores de dominio especificados en el ámbito de esta partición de directorio:

< Atrás **Siguiente >** Cancelar

Zona búsqueda inversa: **IPv4**

Asistente para nueva zona ✕

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.

☒ Zona de búsqueda inversa para IPv4

☐ Zona de búsqueda inversa para IPv6

Identificación de la zona de búsqueda: pon los tres primeros octetos de la subred.

Asistente para nueva zona ✕

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☒ Id. de red:

El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.


☐ Nombre de la zona de búsqueda inversa:

Configuración de actualizaciones dinámicas:

Asistente para nueva zona

Actualización dinámica


Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.



Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

☒ Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción solo está disponible para las zonas que están integradas en Active Directory.

☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.

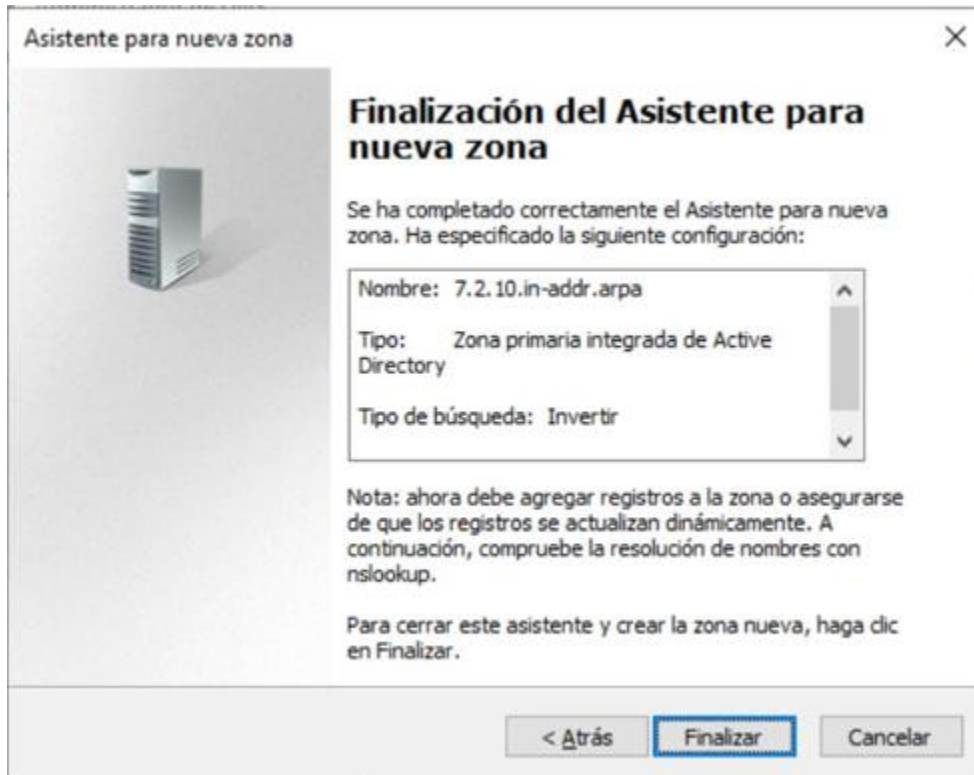
☐ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

< Atrás

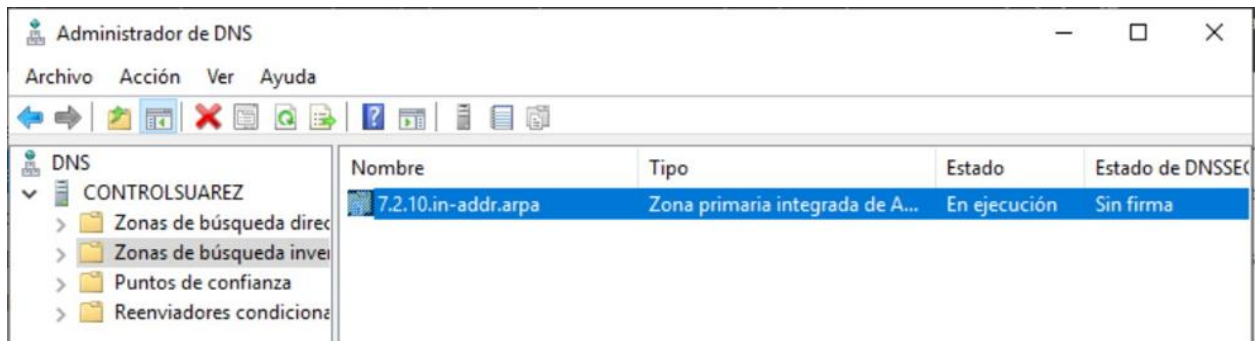
Siguiente >

Cancelar

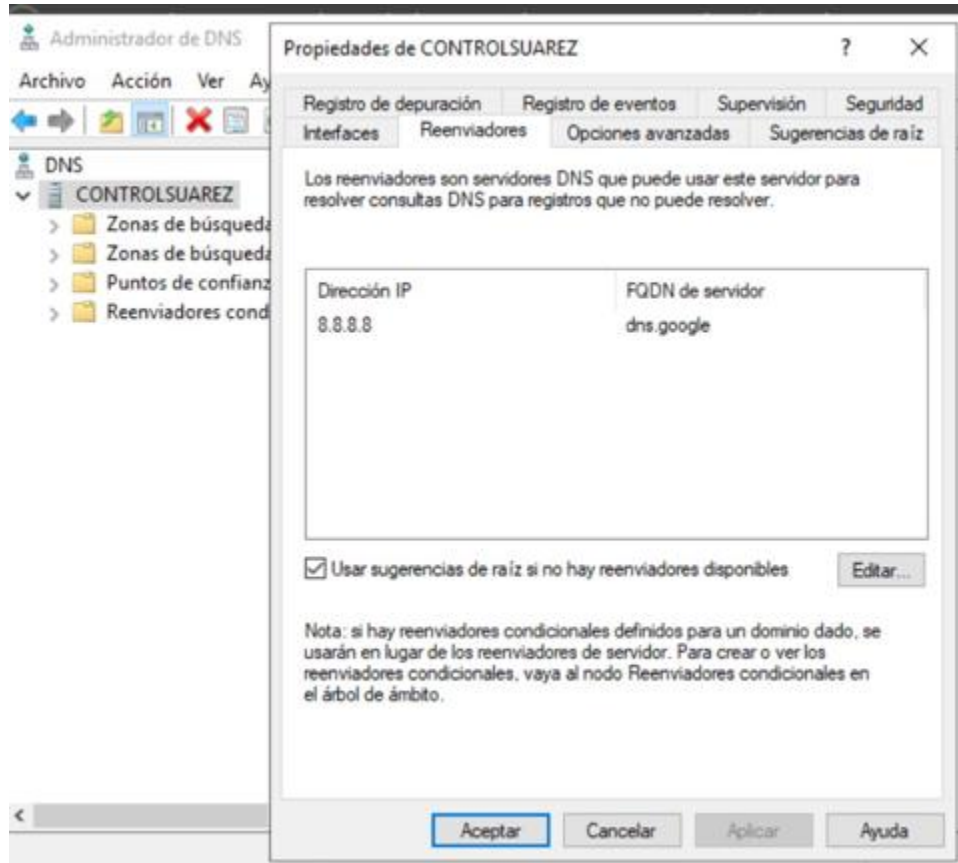
Finalización del Asistente.



Zona de búsqueda una vez creada.



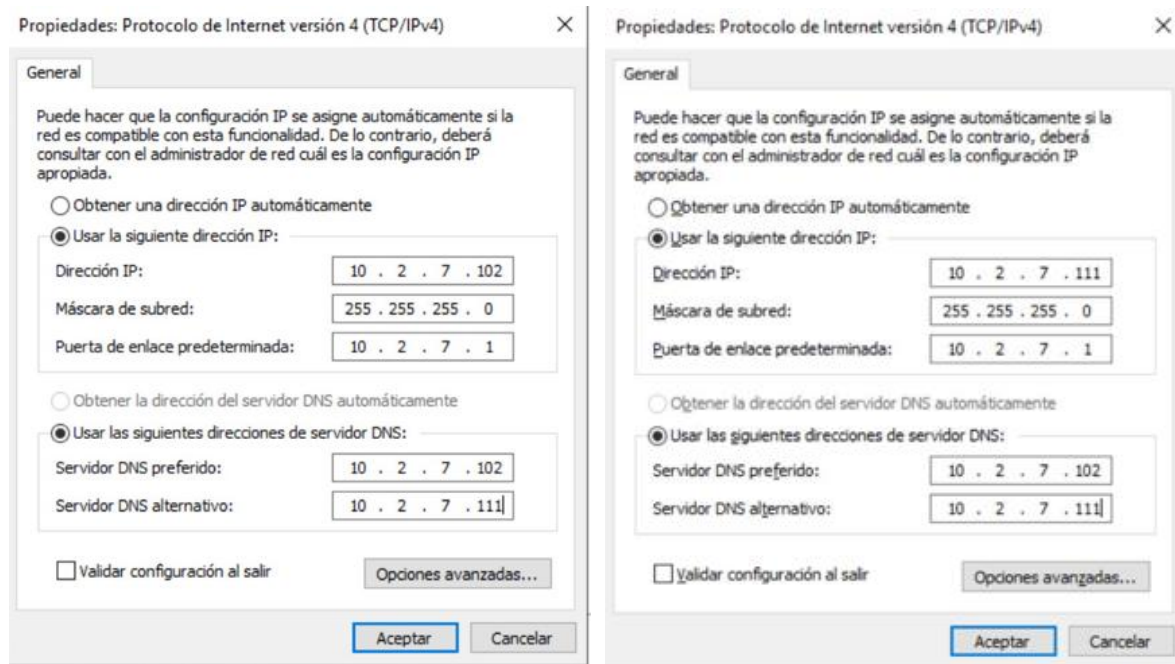
Ahora vamos a configurar los reenviadores, esto permitirá que los equipos puedan acceder a aquellos nombres que nuestro servidor DNS no pueda resolver (porque no lo conoce al no estar en nuestra red local). Para ello en DNS hacemos clic derecho en el controlador y después en Propiedades. Nos dirigimos a la pestaña “**Reenviadores**”.



Le damos a “Editar” e introducimos la IP o nombre del servidor DNS (deben de rellenarse automáticamente los otros datos).



Finalizado el paso anterior, ahora debemos configurar la tarjeta de red ambos equipos: Controlador y futura Réplica. Para ello debemos poner en ambos como servidor de DNS principal la IP del controlador y como alternativo la IP de Réplica.



Para comprobar que funciona, podemos hacer un ping al nombre del servidor o dominio.

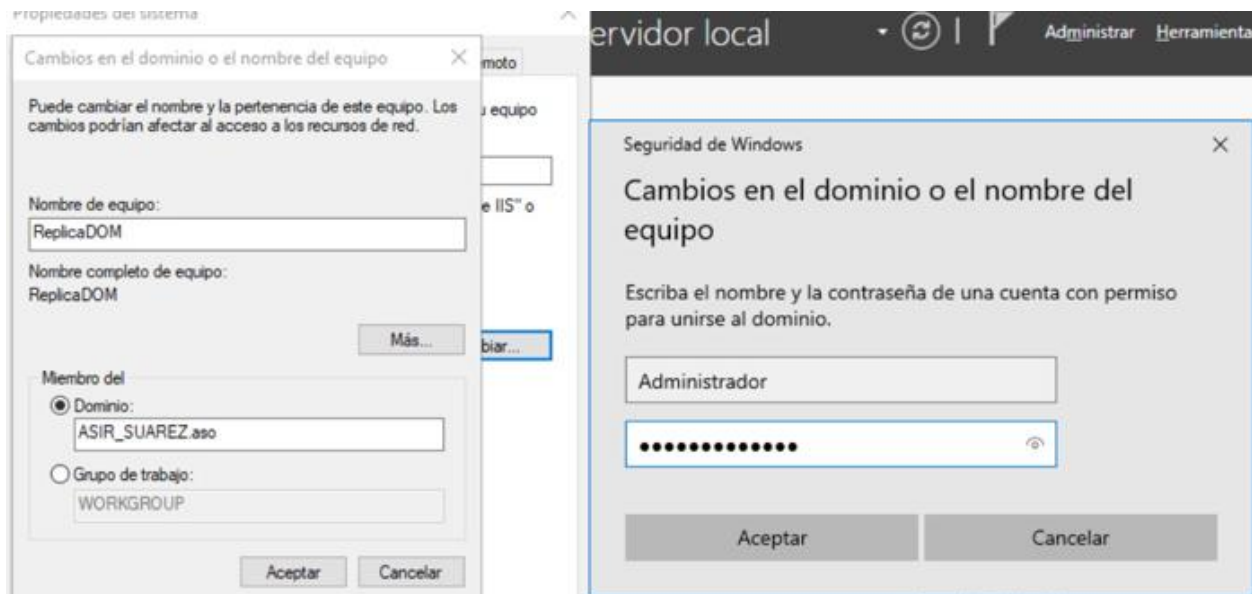
```
C:\Users\Administrador>ping CONTROLSUAREZ.ASIR_SUAREZ.aso

Haciendo ping a CONTROLSUAREZ.ASIR_SUAREZ.aso [10.2.7.102] con 32 bytes de datos:
Respuesta desde 10.2.7.102: bytes=32 tiempo=6ms TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo<1m TTL=128

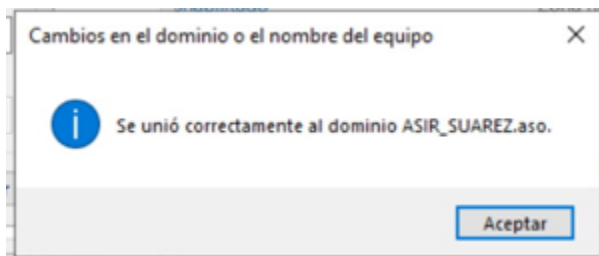
Estadísticas de ping para 10.2.7.102:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 6ms, Media = 2ms
```

ii) Unión de Réplica como Cliente.

Ahora debemos terminar la configuración de Réplica. Como hemos visto antes hemos establecido una IP estática. Y ahora debemos primero unirlo al dominio como si fuera un cliente. **Este Equipo → Propiedades → Cambiar nombre**. Indicamos el nuevo nombre (opcional) y en **Miembro del** debemos indicar el nombre del dominio.



Una vez que se ha unido correctamente, debemos reiniciar la máquina.



En el Controlador nos aparecerá el nuevo cliente en “Computers”.

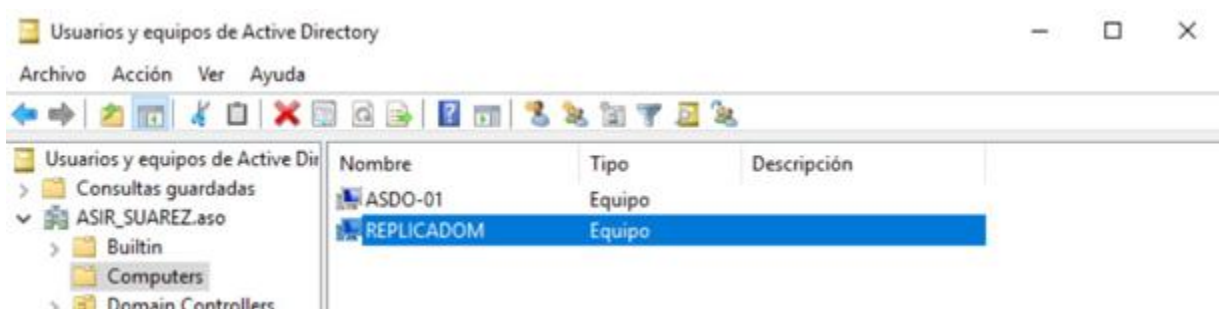
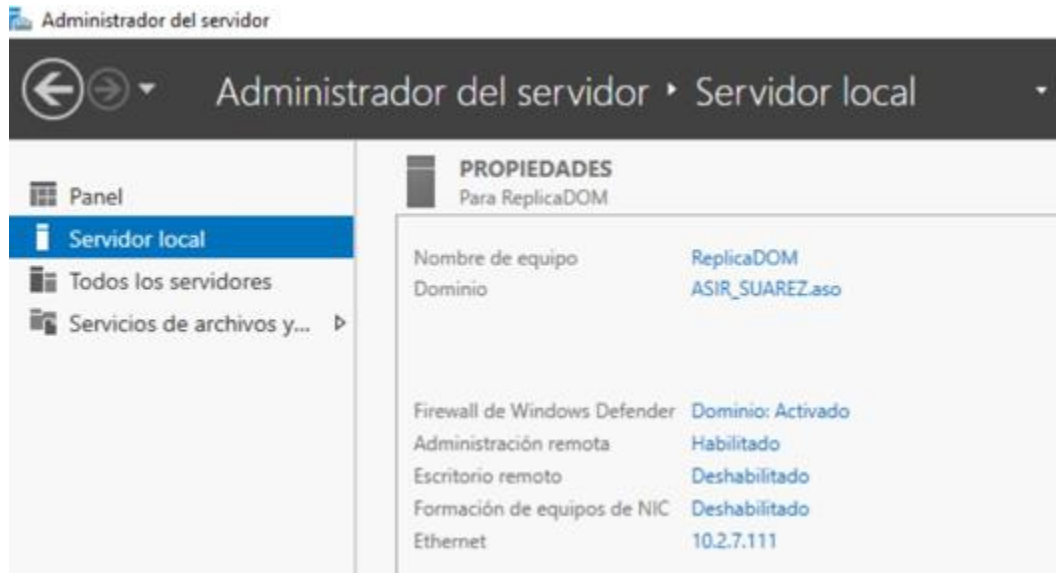
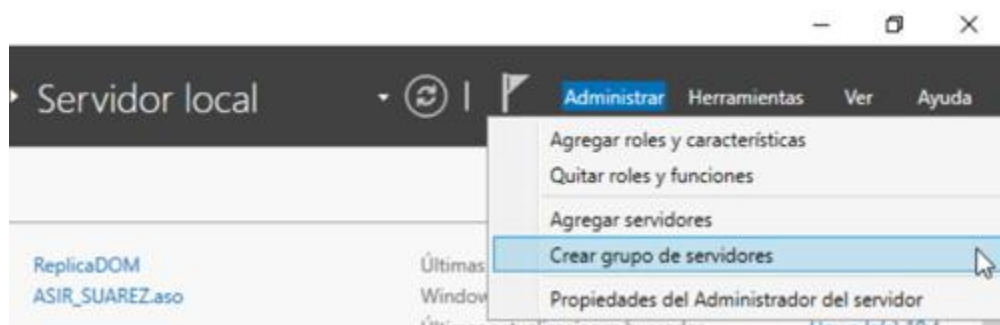


Imagen del futuro servidor Réplica después del reinicio.



iii) **Instalación de Active Directory en el futuro servidor Réplica.**

Administrador del Servidor → Servidor Local → Administrar → Agregar roles y características.



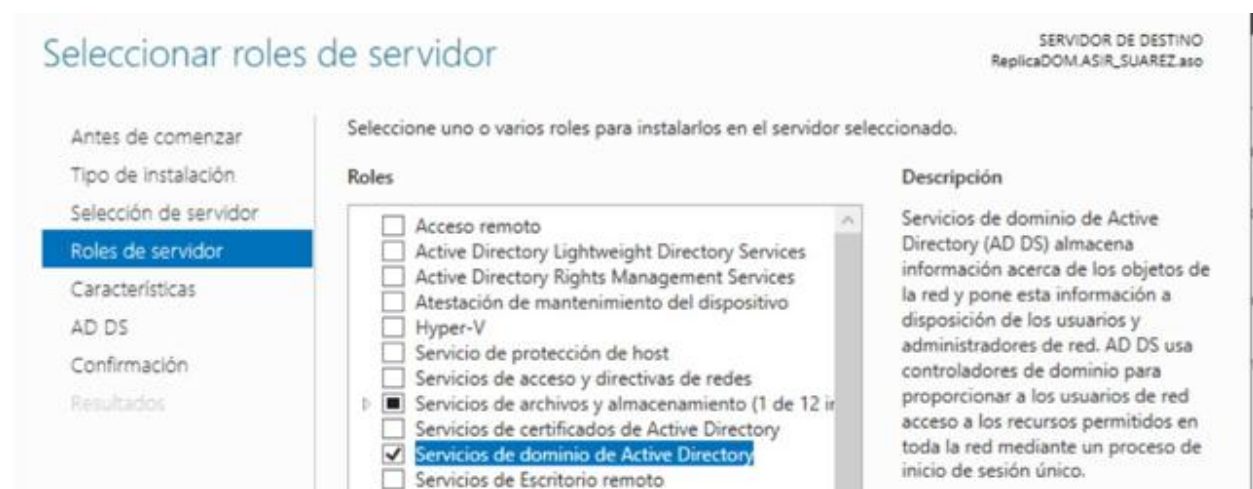
Tipo de instalación: **Instalación basada en características o en roles.**



Elegimos el Servidor: En nuestro caso solo hay uno.



Roles de Servidor: **Servicios de dominio de Active Directory.**



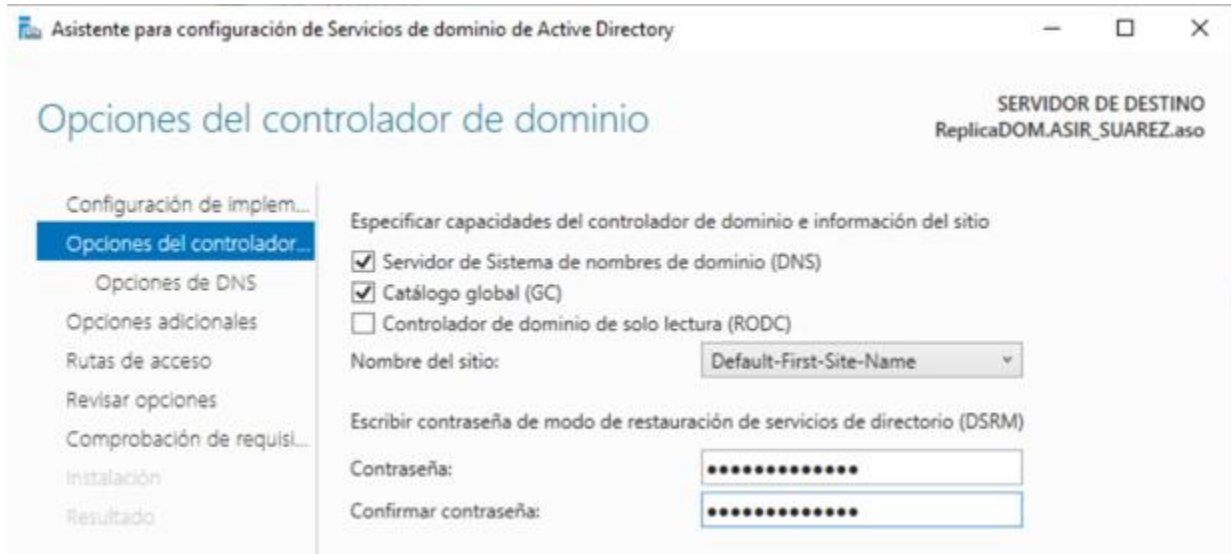
No hay que configurar nada más. Llevamos a cabo la instalación. Una vez terminada, seguimos con el proceso:



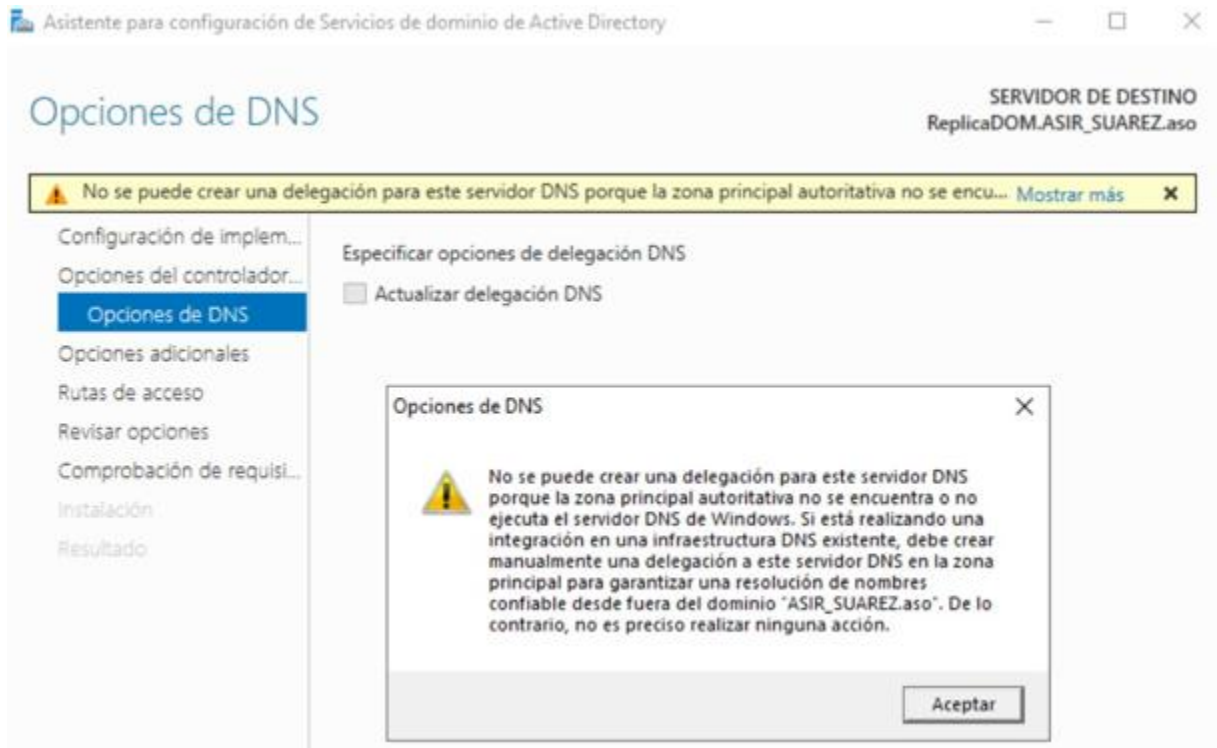
Elegimos **“Agregar un controlador de dominio a un dominio existente”**. Elegimos el dominio y ponemos las credenciales de un usuario con permisos de Administrador del Dominio.



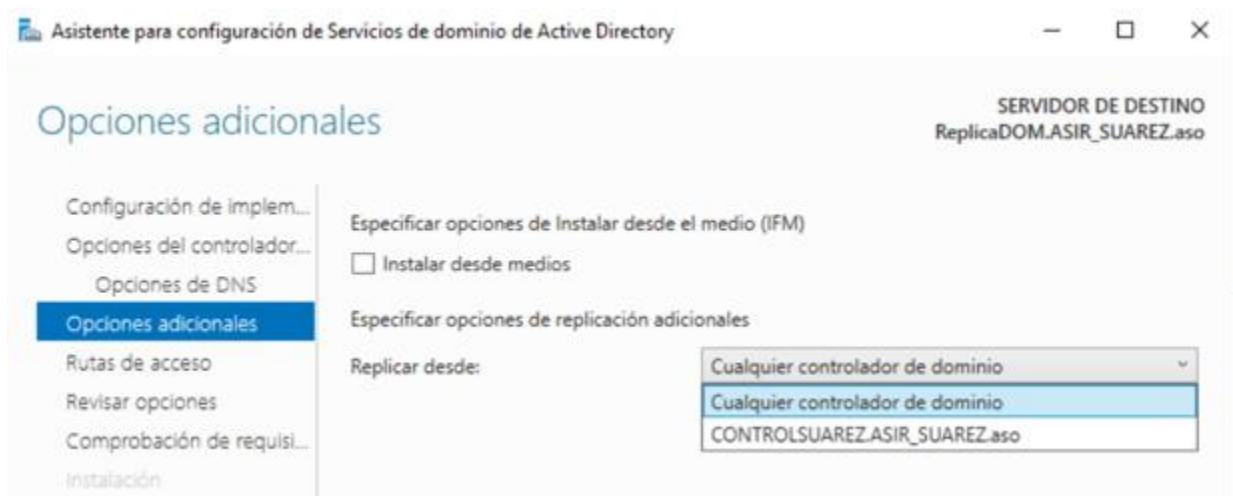
En **“Opciones del controlador de dominio”** dejamos la configuración como aparece. Solo debemos introducir una contraseña para la restauración.



En **Opciones DNS** no podemos hacer nada.



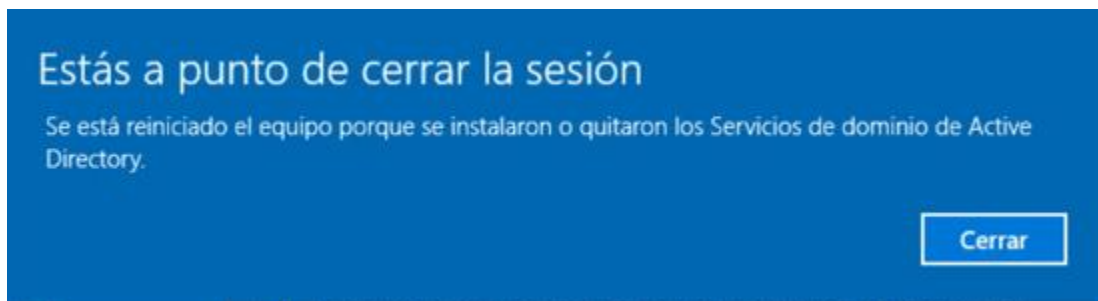
En **Opciones Adicionales** podemos especificar si queremos que se replique desde un Controlador en específico o desde cualquiera.



Rutas de acceso no se tocan.



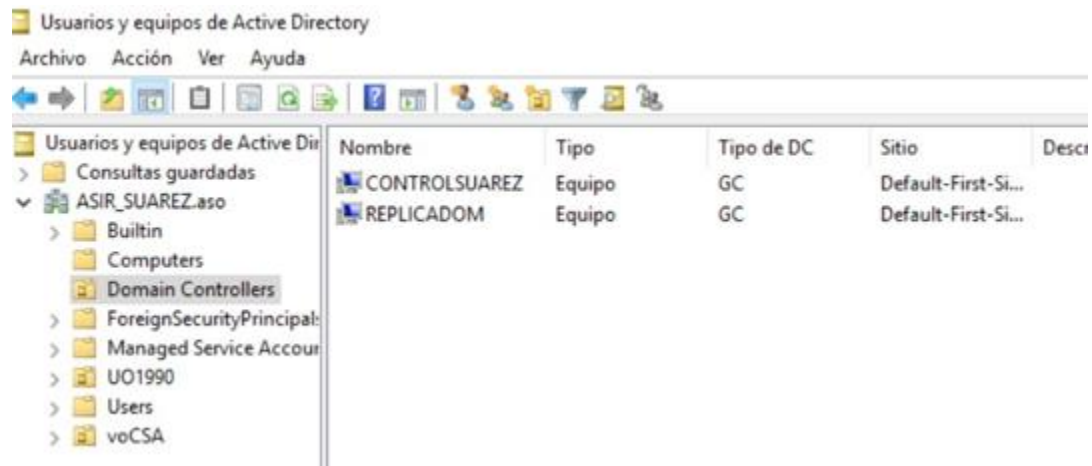
No hay que tocar nada más. Si queremos podemos guardar el Script. Una vez terminada la instalación, la máquina se reinicia.



Podemos ver en el Controlador o en Réplica como nos aparecen ambos como servidores de DNS.



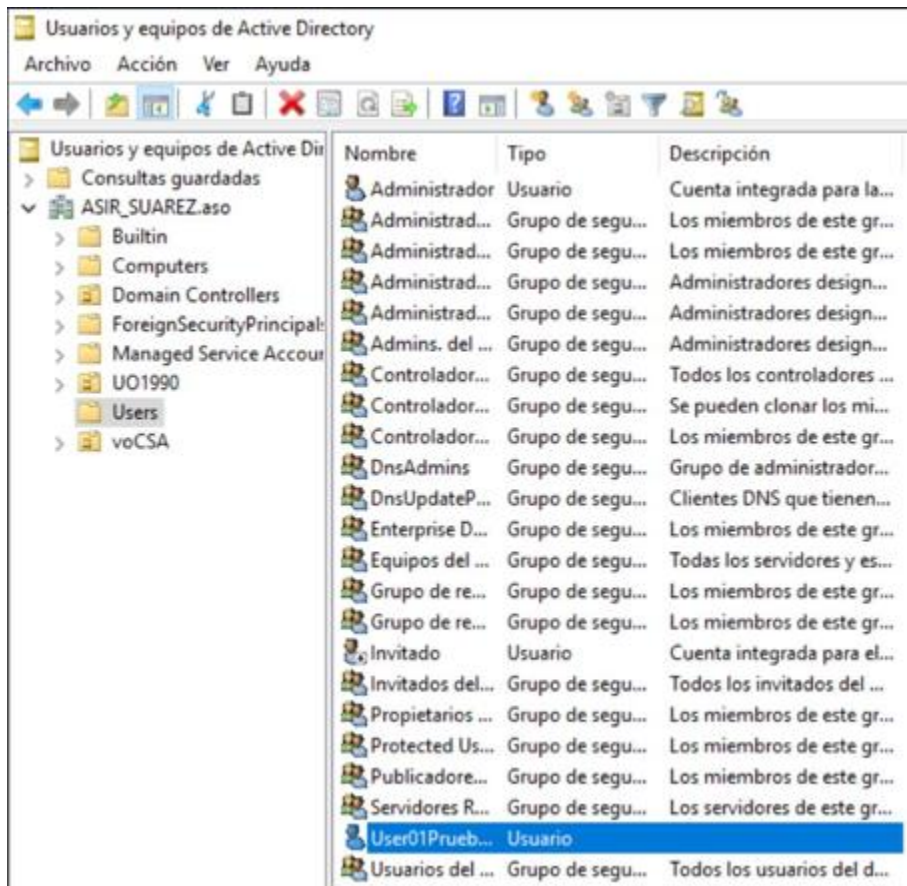
También en **Usuarios y Equipos**.



b) Configura la replicación de Active Directory y comprueba su funcionamiento.

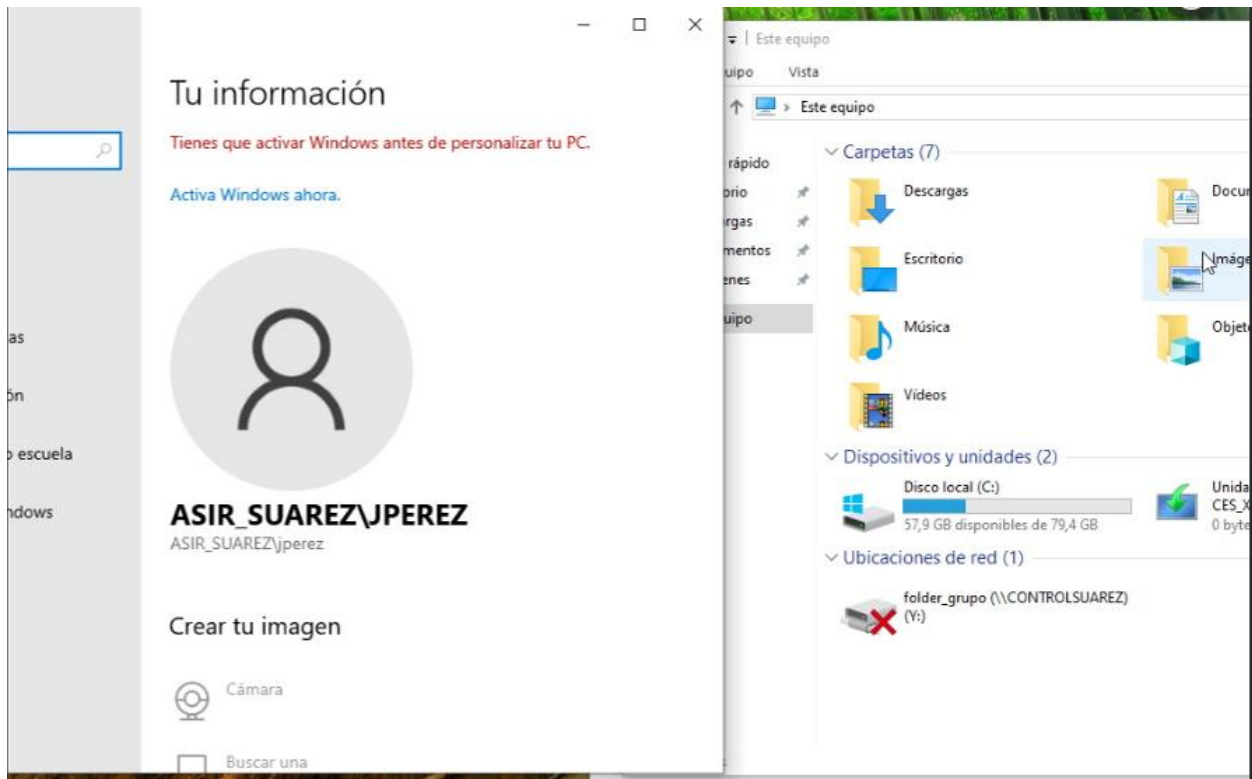
i) Crea un usuario en el controlador principal y verifica que aparece en el secundario.

Se llevó a cabo la acción y de manera automática apareció el usuario en la Réplica. Al no haber diferencias en configuración entre Controlador y Réplica, es casi imposible mostrar las diferencias entre uno y otro.



ii) **Simula la caída del servidor principal y valida que los usuarios siguen autenticándose.**

Se apaga la VM del Controlador principal y se inicia sesión con un usuario del Dominio. El usuario puede acceder perfectamente. Se nota que no puede acceder a la carpeta compartida que se había configurado en la Actividad 1, porque se encuentra dentro del Controlador.

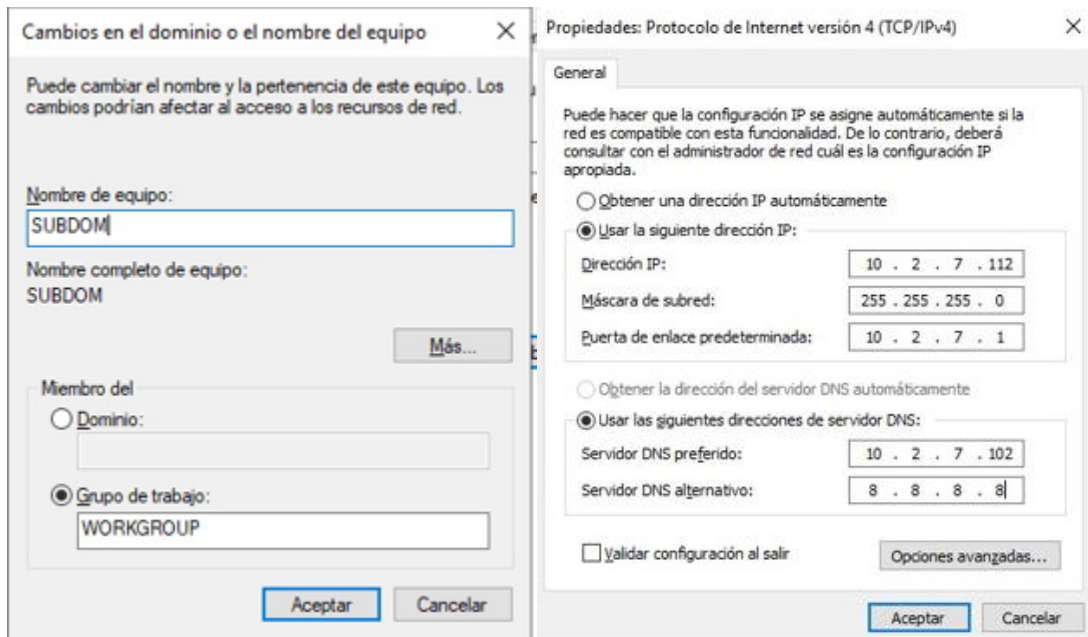


2) Subdominio.

NOTA: Una vez que se ha creado una Réplica de Controlador de Dominio, a la hora de añadir un subdominio se produce un error que indica que la Réplica debe de estar encendida durante el proceso.

a) **Crea un nuevo servidor y configúralo como child domain.**

Al nuevo servidor le cambiamos el nombre (no es completamente necesario, pero si altamente recomendable). Y establecemos IP estática y como DNS la IP del Servidor de Dominio Principal.



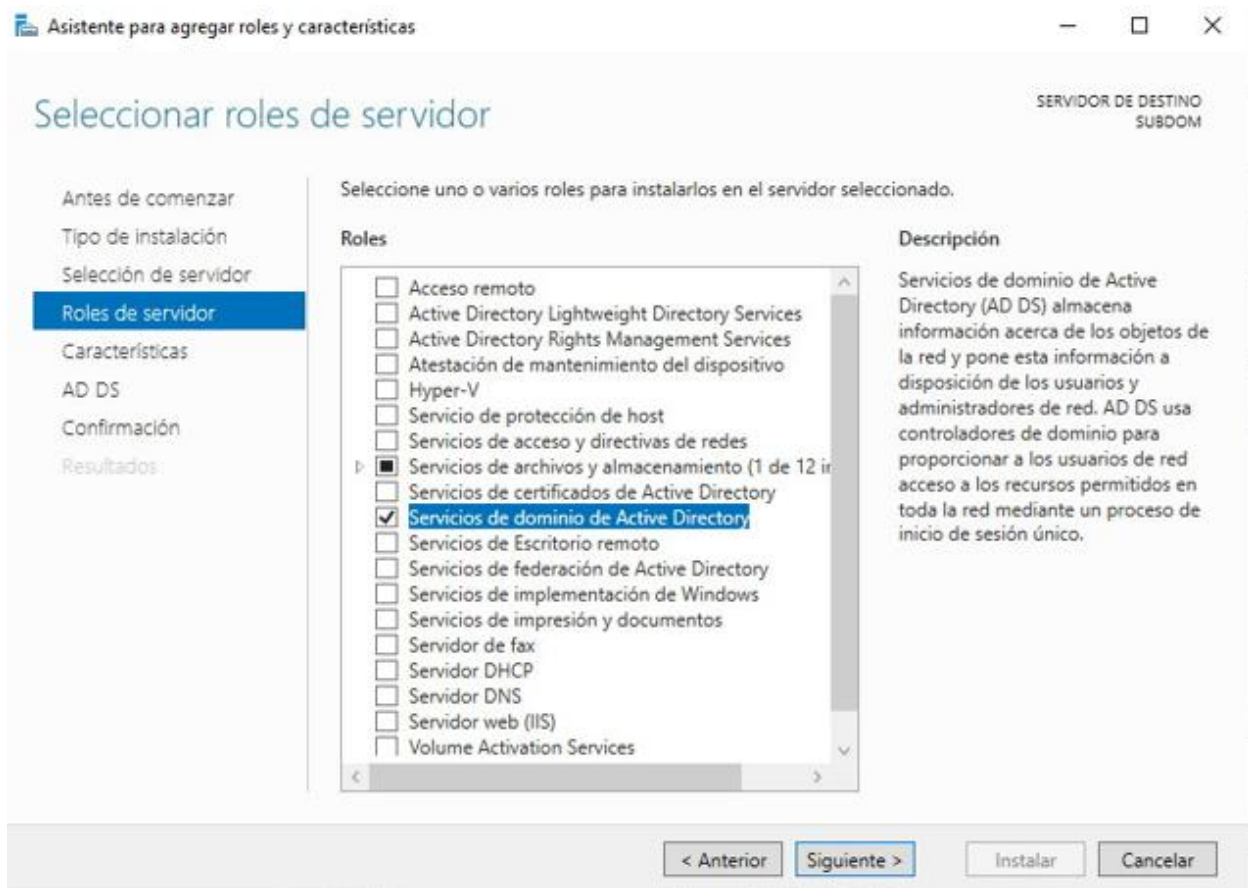
Comprobamos la conexión.

```
C:\Users\Administrador>ping ASIR_SUAREZ.aso

Haciendo ping a ASIR_SUAREZ.aso [10.2.7.102] con 32 bytes de datos:
Respuesta desde 10.2.7.102: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.2.7.102: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.2.7.102:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Una vez configurada, instalamos el rol de “**Servicios de Dominio de Active Directory**”.



Una vez terminada la instalación, seguiremos con el siguiente asistente. Elegimos **“Agregar un nuevo dominio a un bosque existente”**. Ponemos el nombre del Dominio principal y la del Subdominio. Y las credenciales de un administrador del Dominio principal.

Asistente para configuración de Servicios de dominio de Active Directory

Configuración de implementación

SERVIDOR DE DESTINO SUBDOM

Configuración de imple...

Opciones del controlador...

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Seleccionar la operación de implementación

☐ Agregar un controlador de dominio a un dominio existente

☒ Agregar un nuevo dominio a un bosque existente

☐ Agregar un nuevo bosque

Especificar la información de dominio para esta operación

Seleccionar tipo de dominio: Dominio secundario

Nombre de dominio principal: ASIR_SUAREZ.aso Seleccionar...

Nuevo nombre de dominio: hijo09

Proporcionar las credenciales para realizar esta operación

ASIR_SUAREZ\Administrador Cambiar...

Más información sobre configuraciones de implementación

< Anterior Siguiente > Instalar Cancelar

El resto de las configuraciones es muy parecida, excepto en la de **Opciones DNS**, donde ya nos viene marcada la opción de **“Crear delegación DNS”**.

Asistente para configuración de Servicios de dominio de Active Directory

Opciones de DNS

SERVIDOR DE DESTINO SUBDOM

Configuración de imple...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Especificar opciones de delegación DNS

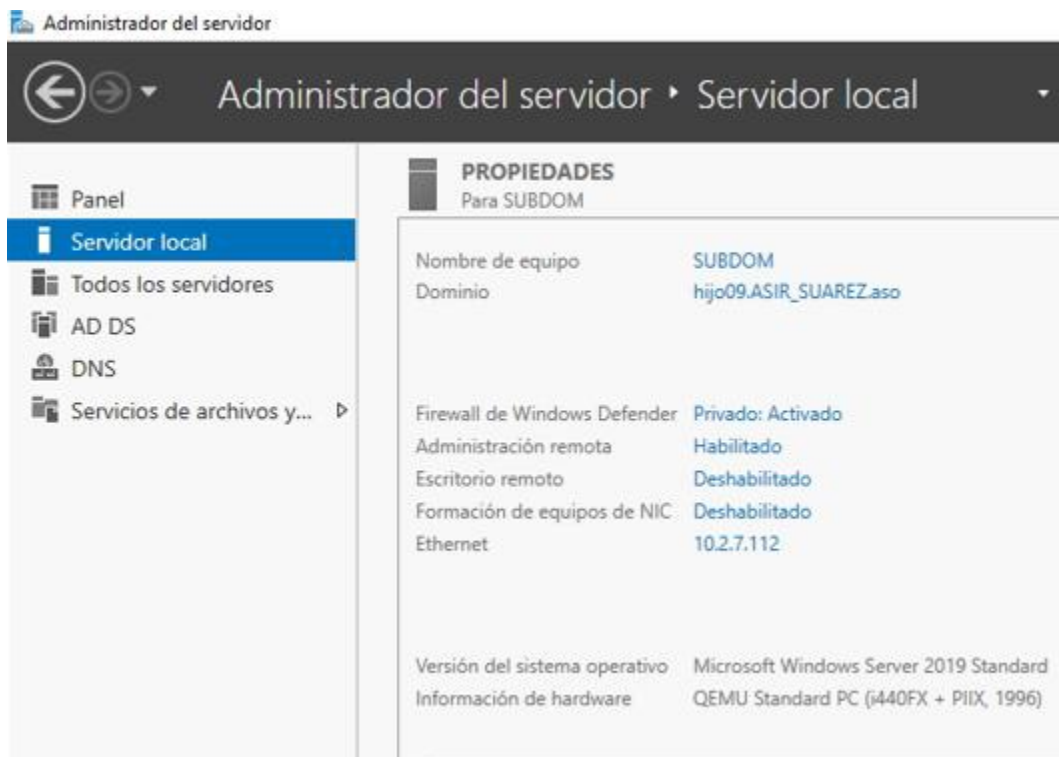
☒ Crear delegación DNS

Credenciales para crear delegaciones

ASIR_SUAREZ\Administrador Cambiar...

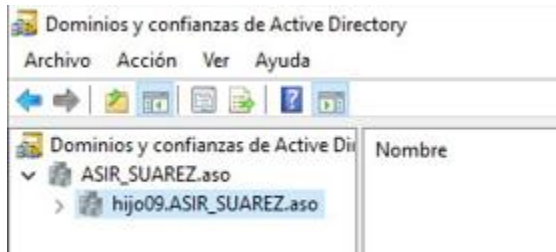
< Anterior Siguiente > Instalar Cancelar

Una vez terminada la instalación se reiniciará la máquina.



b) Configura y verifica la relación de confianza entre el dominio padre y el hijo.

En el Controlador en **Dominios y Confianzas de Active Directory**, podemos ver la relación de confianza.



Cuando se crea un subdominio, la relación con el dominio principal siempre es bidireccional y transitiva.

10.4. Añadir un subdominio a un dominio existente

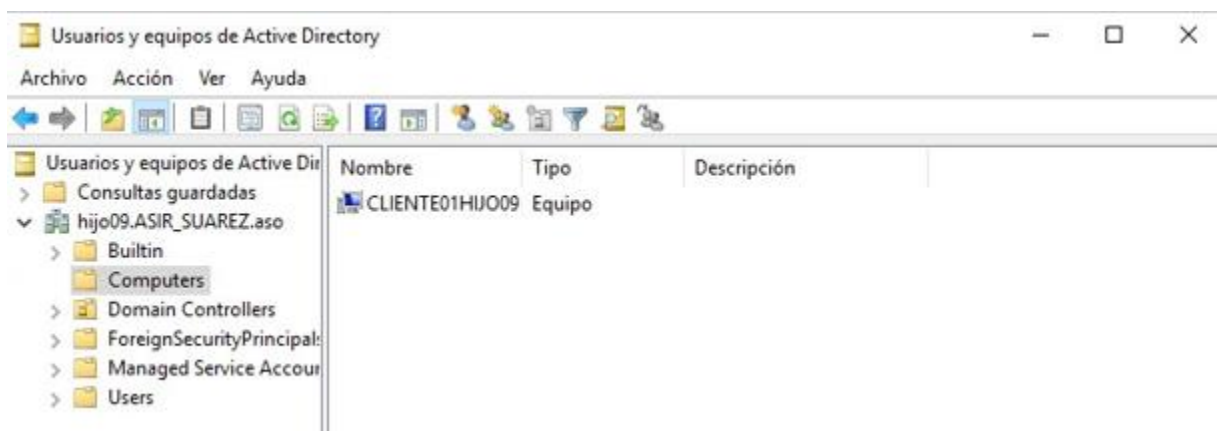
Como dijimos más arriba, cuando creamos un nuevo subdominio, de un dominio ya existente, se establece de manera implícita y automática una relación de confianza bidireccional y transitiva entre el nuevo dominio y su dominio padre.

2

i) Realiza pruebas de inicio de sesión con usuarios del dominio padre en equipos unidos al hijo y viceversa.

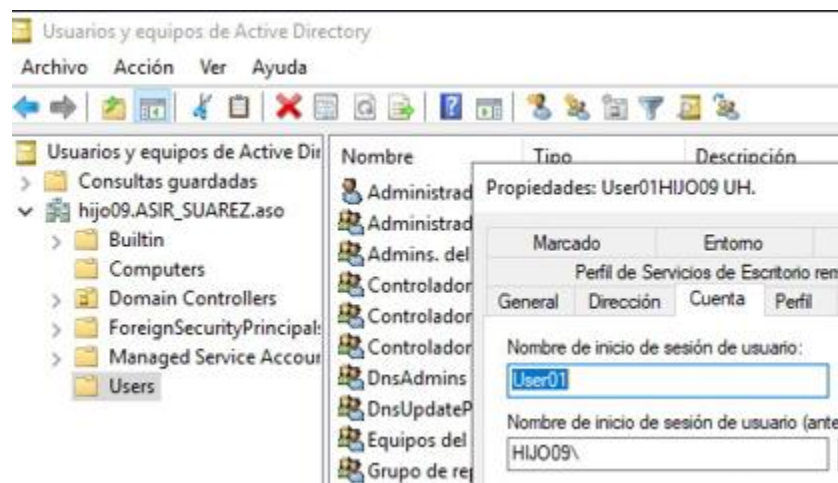
Para esto vamos a crear un Cliente y Usuarios en el Subdominio.

Cliente unido.

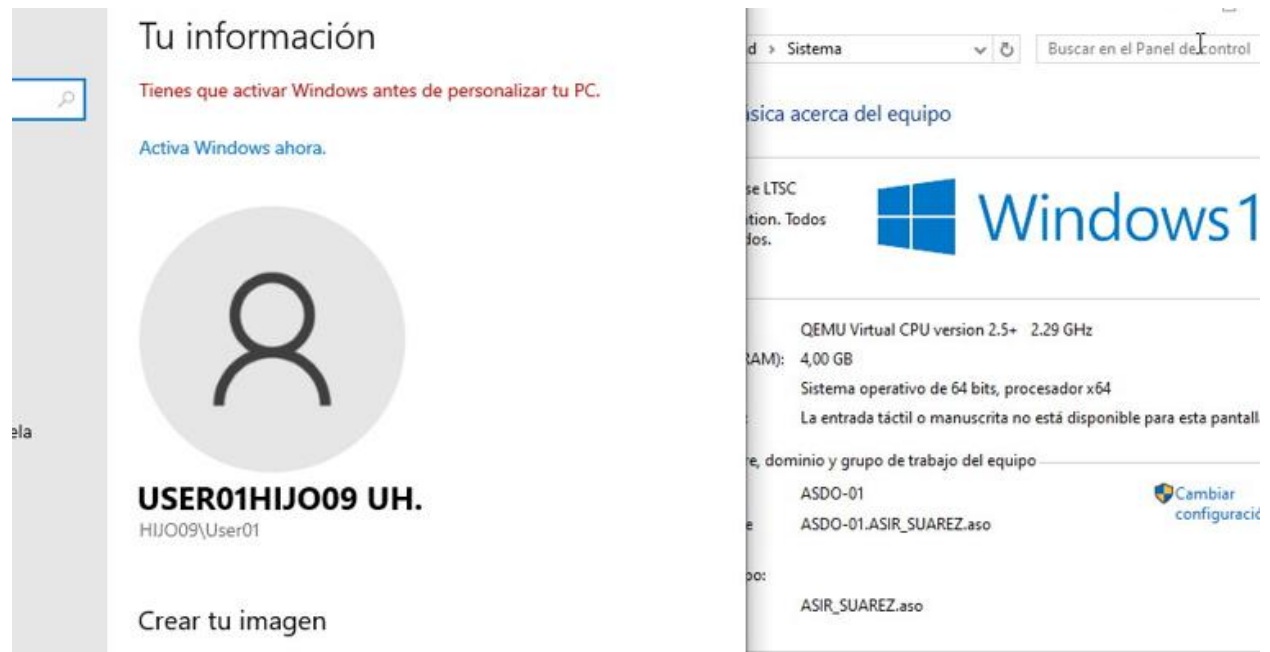


² <https://somebooks.es/capitulo-7-relaciones-entre-dominios/4/>

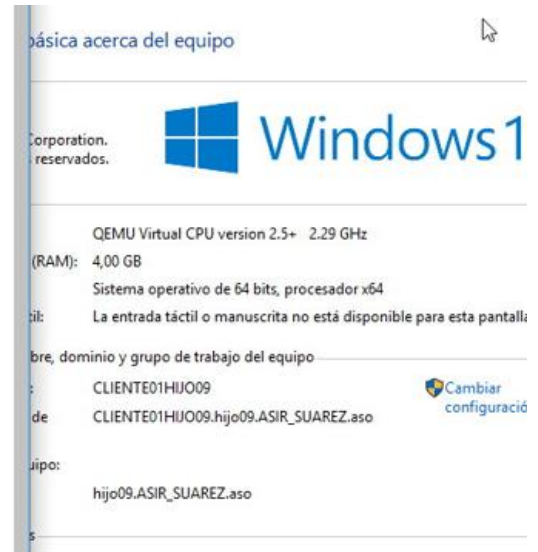
Usuario creado.



Entramos con el usuario del subdominio en un equipo cliente del dominio principal.



Y ahora con un usuario del Dominio principal, en un equipo cliente del subdominio.

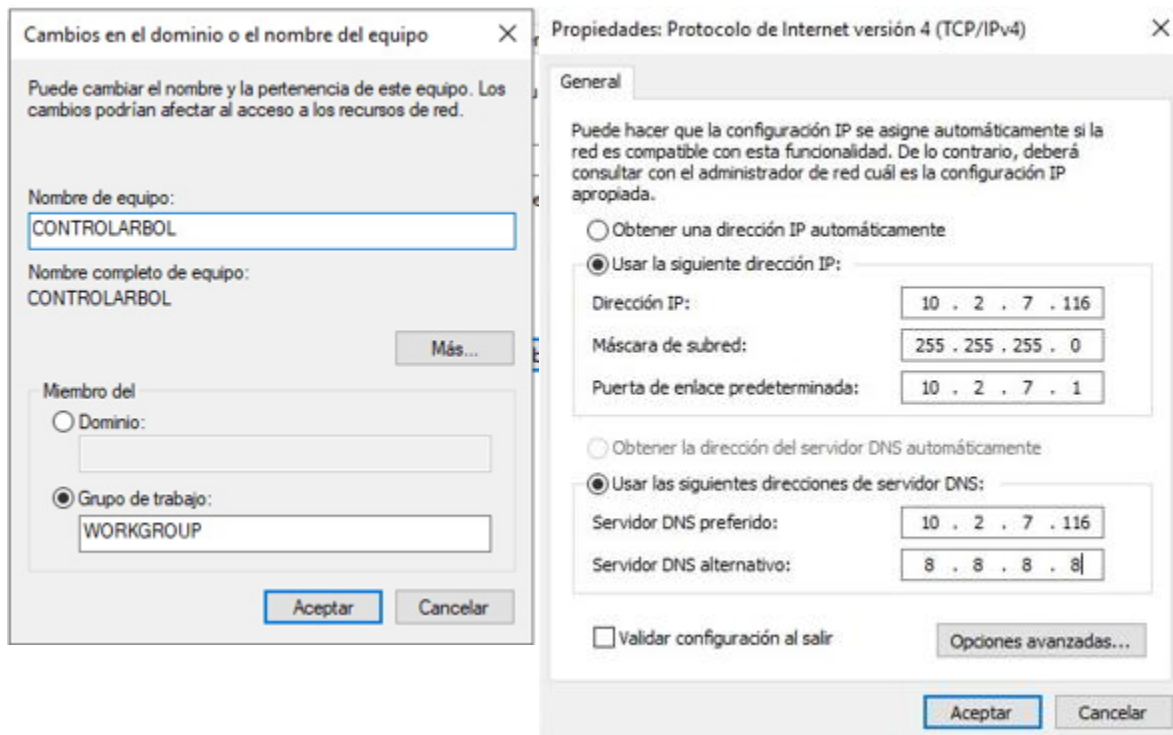


3) **Bosque.**

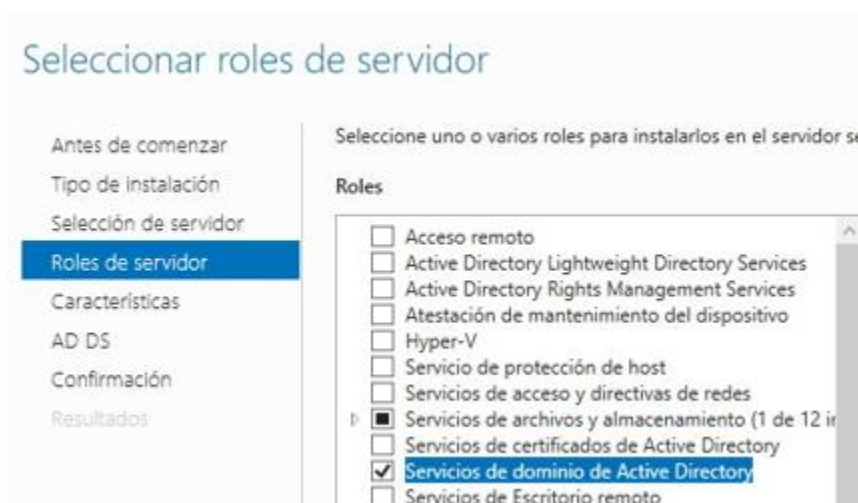
NOTA: Si se usa una VM clonada de la misma fuente que el otro dominio, pueden producirse problemas. Se debe realizar “sysprep”.

a) **Configura un nuevo servidor y crea un dominio raíz de un bosque diferente.**

Configuramos el servidor.



Instalamos “Servicios de Dominio”.



En el siguiente asistente elegimos la opción **“Agregar un nuevo bosque”**. Establecemos el nombre del Dominio raíz del nuevo bosque.

Configuración de implementación

SEVIDOR
COI

Configuración de implem...

Opciones del controlador...

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Selección de la operación de implementación

☐ Agregar un controlador de dominio a un dominio existente

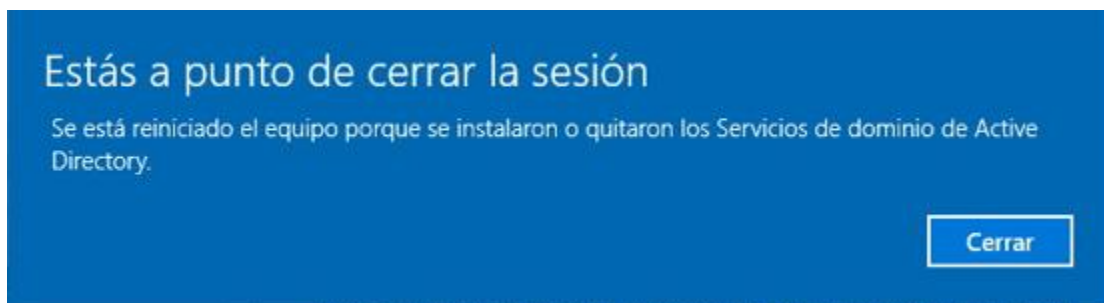
☐ Agregar un nuevo dominio a un bosque existente

☒ Agregar un nuevo bosque

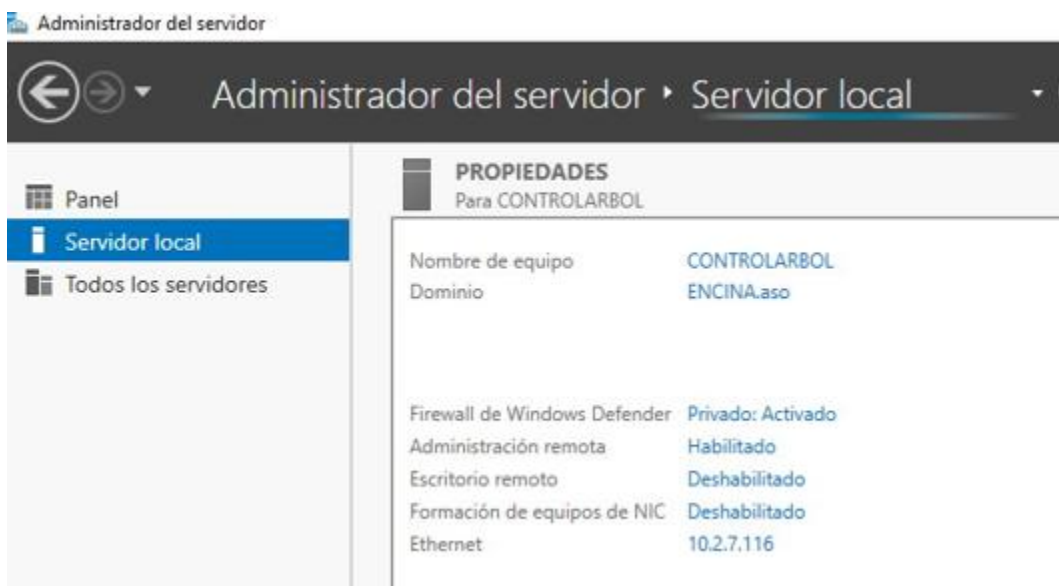
Especificar la información de dominio para esta operación

Nombre de dominio raíz:

El resto de la configuración es idéntica a lo que hemos visto antes.



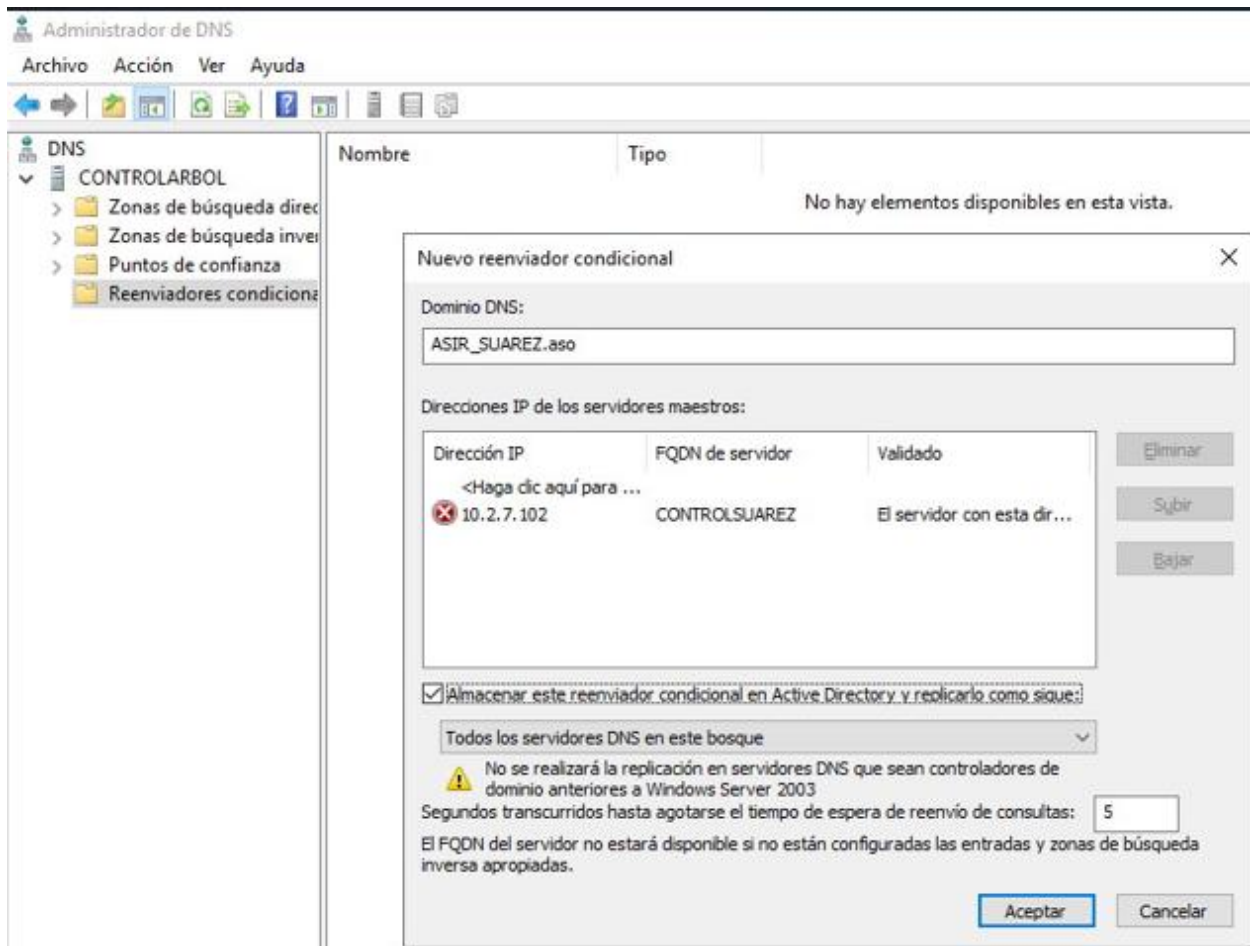
Una vez reiniciada la máquina, podemos ver que se ha creado el dominio.



b) Establece una relación de confianza bidireccional y transitiva entre ambos bosques.

El primer paso es establecer **Reenviadores condicionales** en ambos Servidores, para que puedan verse el uno al otro.

DNS → Reenviadores condicionales: Nuevo. E introducimos la IP del otro servidor. **Se debe hacer en ambos, poniendo la IP del otro.**

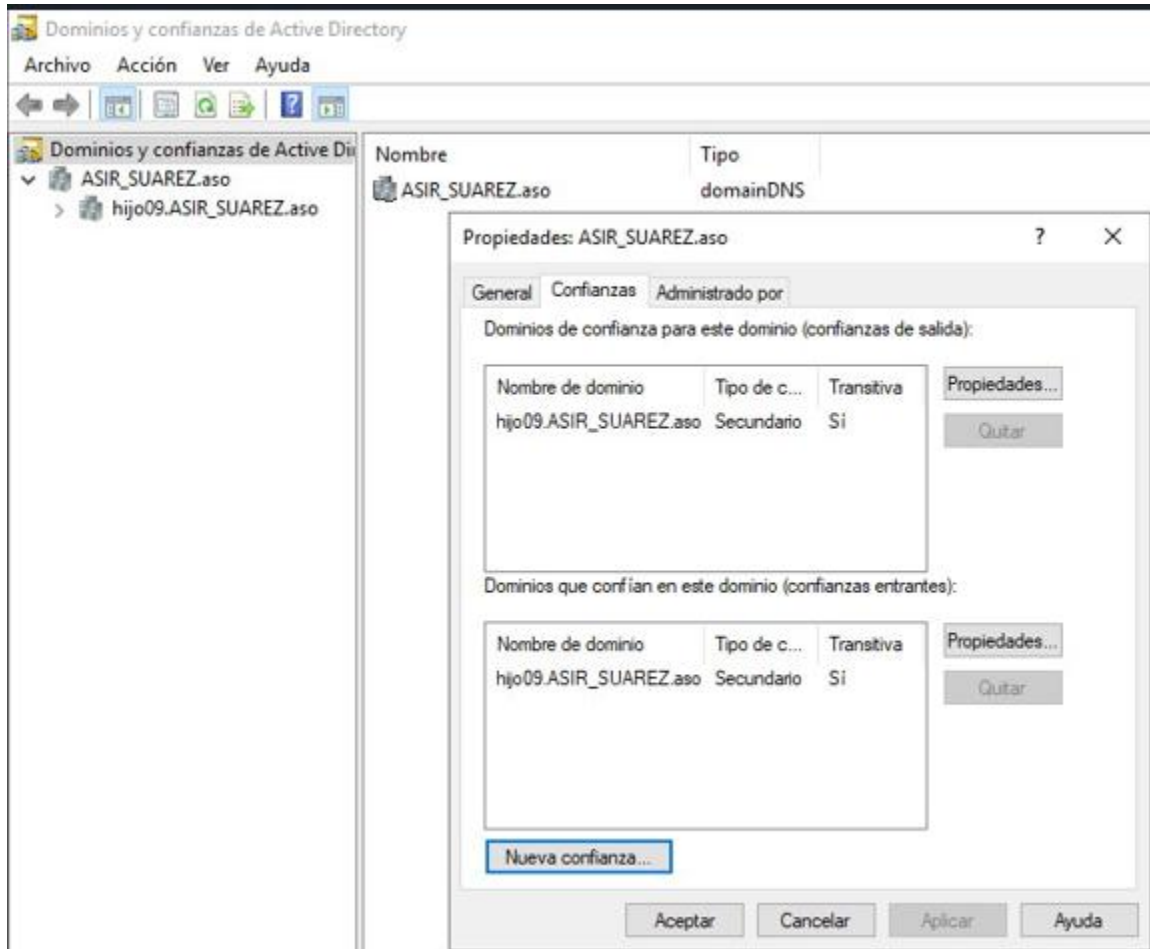


Para comprobar que funciona se hace ping:

```
C:\Users\Administrador>ping ENCINA.aso

Haciendo ping a ENCINA.aso [10.2.7.116] con 32 bytes de datos:
Respuesta desde 10.2.7.116: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.2.7.116: bytes=32 tiempo<1m TTL=128
```

El siguiente paso es establecer la **relación de confianza**. Para ello: **Herramientas → Dominios y confianzas de Active Directory**. Y vamos a propiedades del dominio y luego a la pestaña **Confianzas** y ahí en **Nueva Confianza**. Hay que tener en cuenta que solo hace falta establecerlo en uno de los dominios de la relación.



El nombre del dominio con el que queremos establecer la relación.

Asistente para nueva confianza

Nombre de confianza
Puede crear una relación de confianza mediante un nombre NetBIOS o DNS.

Escriba el nombre de dominio, bosque o dominio kerberos para esta confianza. Si escribe el nombre de un bosque, debe escribir un nombre DNS.

Ejemplo de nombre NetBIOS: proveedor01-int
Ejemplo de nombre DNS: proveedor01-interno.microsoft.com

Nombre:

< Atrás **Siguiente >** Cancelar

Tipo de Confianza: de Bosque.

Asistente para nueva confianza

Tipo de confianza
Este dominio es un dominio raíz de bosque. Si el dominio especificado está cualificado, puede crear una confianza de bosque.

Seleccione el tipo de confianza que desea crear.

☐ Confianza externa
Una confianza externa es una confianza no transitiva entre un dominio y otro dominio de fuera del bosque. Una confianza no transitiva está limitada por los dominios de la relación.

☒ Confianza de bosque
Una confianza de bosque es una confianza transitiva entre dos bosques que permite que los usuarios de cualquiera de los dominios de uno de los bosques sean autenticados en cualquiera de los dominios del otro bosque.

< Atrás **Siguiente >** Cancelar

Dirección de confianza: Bidireccional.

Asistente para nueva confianza

Dirección de confianza

Puede crear confianzas unidireccionales o bidireccionales.

Seleccione la dirección de esta confianza.

☒ Bidireccional
Los usuarios de este dominio pueden ser autenticados en el dominio, dominio kerberos o bosque especificado y los usuarios del dominio, dominio kerberos o bosque especificado pueden ser autenticados en este dominio.

☐ Unidireccional de entrada
Los usuarios de este dominio pueden ser autenticados en el dominio, dominio kerberos o bosque especificado.

☐ Unidireccional de salida
Los usuarios del dominio, dominio kerberos o bosque especificado pueden ser autenticados en este dominio.

< Atrás **Siguiente >** Cancelar

Partes de la relación de confianza: Ambos.

Asistente para nueva confianza

Partes de la relación de confianza

Si dispone de los permisos apropiados en ambos dominios, puede crear ambas partes de la relación de confianza.

Para empezar a utilizar una confianza es necesario crear ambas partes de la relación. Por ejemplo, si crea una confianza entrante unidireccional en el dominio local, también debe crear una confianza saliente unidireccional en el dominio especificado para que el tráfico de autenticación empiece a fluir a través de la relación de confianza.

Crear la relación de confianza para los dominios siguientes:

☐ Solo este dominio
Esta opción crea la relación de confianza en el dominio local.

☒ Ambos, este dominio y el dominio especificado
Esta opción crea relaciones de confianza en el dominio local y en el dominio especificado. Debe tener privilegios de creación de relaciones de confianza en el dominio especificado.

< Atrás **Siguiente >** Cancelar

Acreditación de usuario administrador del otro Dominio.

Asistente para nueva confianza

Nombre de usuario y contraseña

Para crear esta relación de confianza, debe tener privilegios administrativos para el dominio especificado.

Dominio especificado: ENCINA.aso

Escriba el nombre de usuario y la contraseña de una cuenta que tiene privilegios de administrador en el dominio especificado.

Usuario:

Contraseña:

< Atrás **Siguiente >** Cancelar

Nivel de autenticación de confianza saliente – Bosque local: **Autenticación en todo el bosque.**

Asistente para nueva confianza

Nivel de autenticación de confianza saliente – Bosque local

Es posible autenticar a los usuarios del bosque especificado para utilizar todos los recursos del bosque local o solo aquellos recursos que especifique.

Seleccione el ámbito de autenticación de usuarios del bosque ENCINA.aso.

☒ Autenticación en todo el bosque
Windows autenticará automáticamente a los usuarios del bosque especificado para todos los recursos del bosque local. Se recomienda esta opción cuando ambos bosques pertenezcan a la misma organización.

☐ Autenticación selectiva
Windows no autenticará automáticamente a los usuarios del bosque especificado para ninguno de los recursos en el bosque local. Luego de cerrar este asistente, conceda acceso individual a cada dominio y servidor que desee estén disponibles para los usuarios en el bosque especificado. Se recomienda esta opción cuando los bosques pertenezcan a organizaciones diferentes.

< Atrás **Siguiente >** Cancelar

Nivel de autenticación de confianza saliente – Bosque especificado: **Autenticación en todo el bosque.**

Asistente para nueva confianza

Nivel de autenticación de confianza saliente – Bosque especificado

Es posible autenticar a los usuarios del bosque local para utilizar todos los recursos del bosque especificados o solo aquellos recursos que especifique.

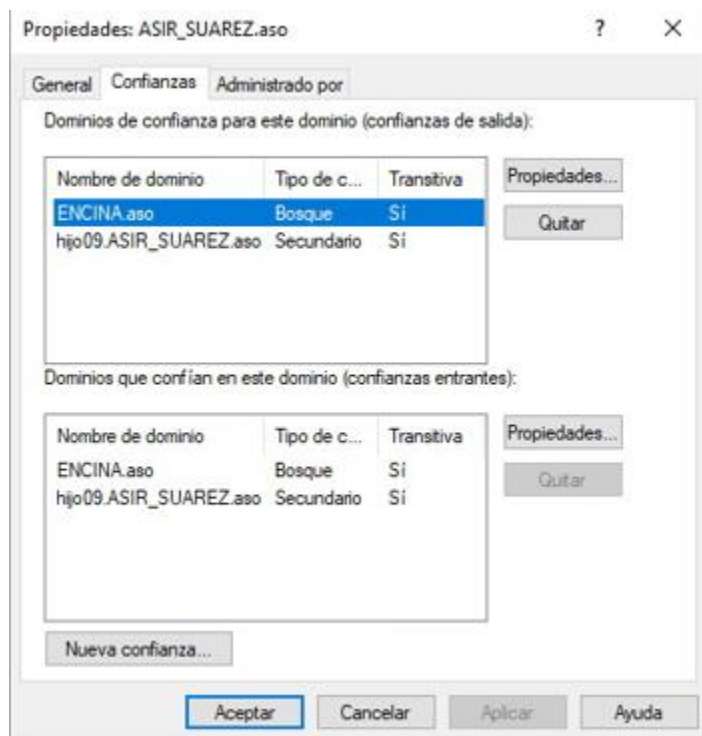
Seleccione el ámbito de autenticación de usuarios del bosque local.

☒ Autenticación en todo el bosque
Windows autenticará automáticamente a los usuarios del bosque local para todos los recursos del bosque ENCINA.aso. Se recomienda esta opción cuando ambos bosques pertenezcan a la misma organización.

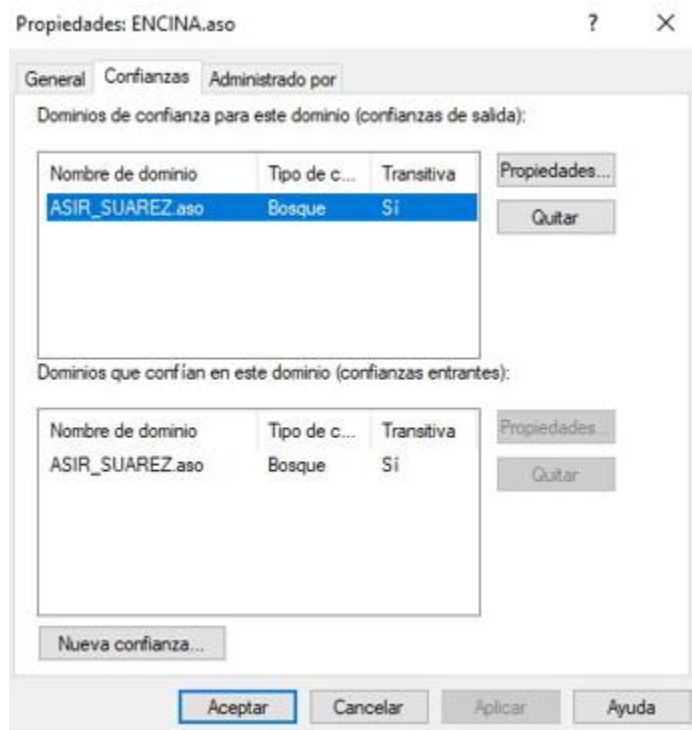
☐ Autenticación selectiva
Windows no autenticará automáticamente a los usuarios del bosque local para ninguno de los recursos en el bosque ENCINA.aso. Luego de cerrar este asistente, conceda acceso individual a cada dominio que desee esté disponible para los usuarios en el bosque local. Se recomienda esta opción cuando los bosques pertenezcan a organizaciones diferentes.

< Atrás **Siguiente >** Cancelar

Una vez terminado el asistente, nos aparece la relación de confianza:

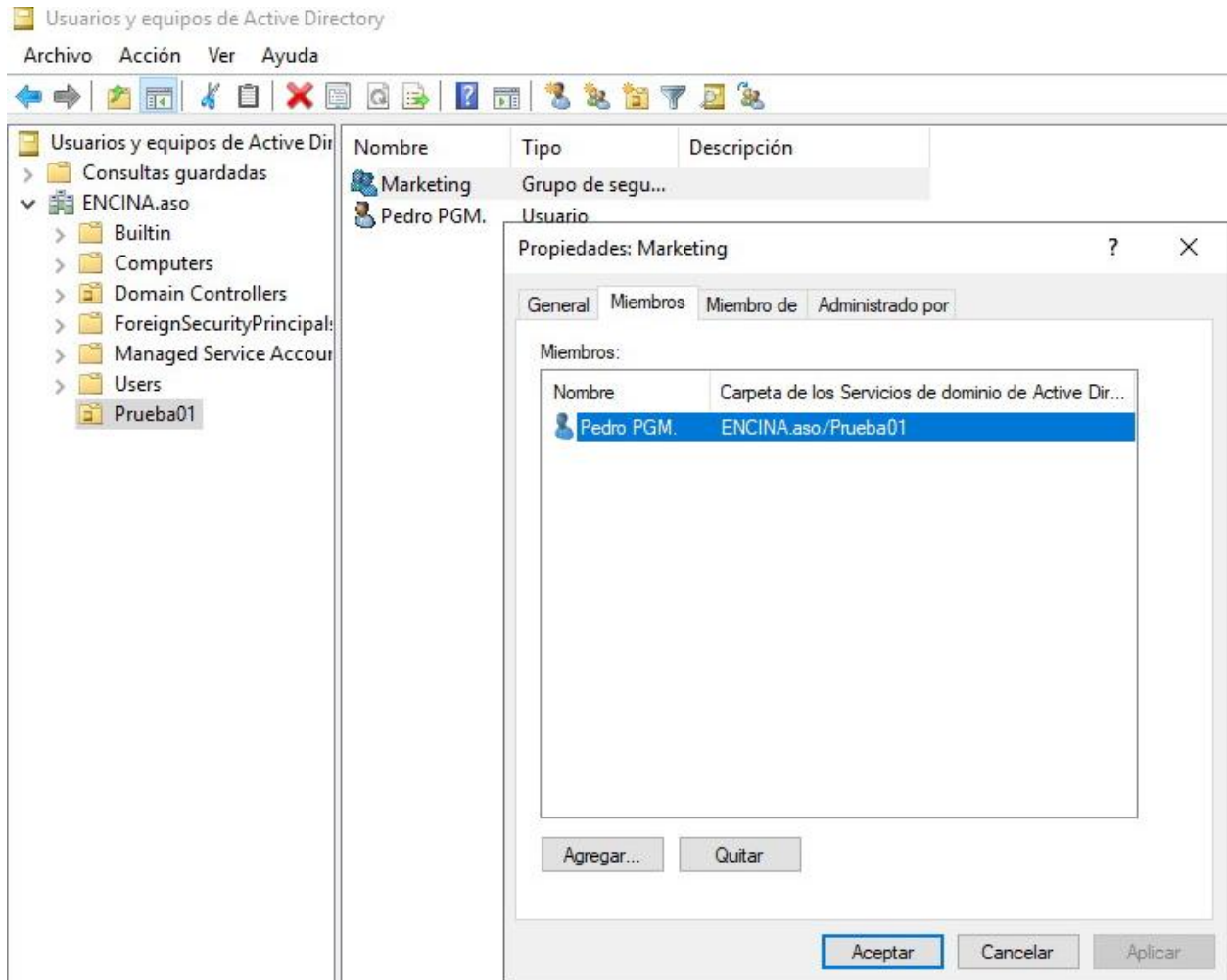


En el otro dominio se crea automáticamente.

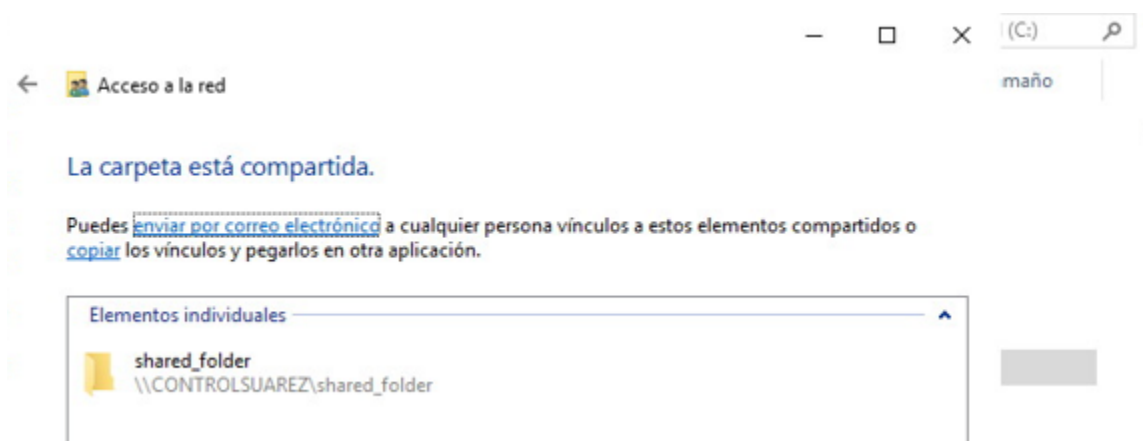
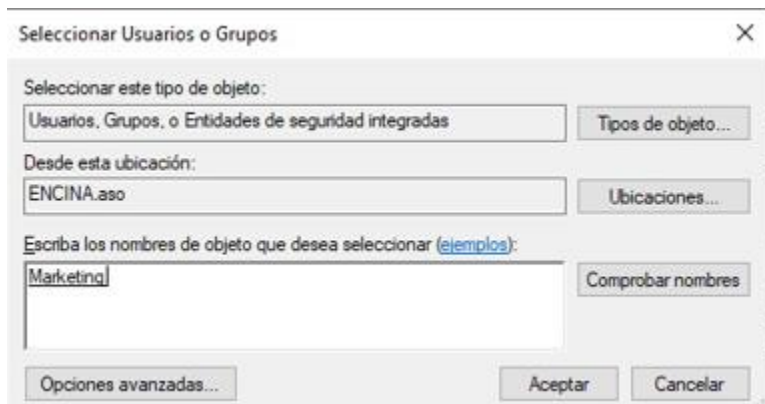
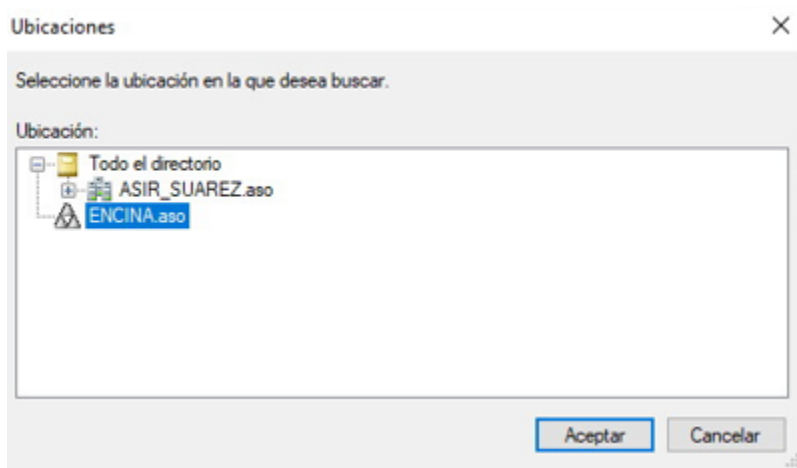


- c) Comprueba la autenticación cruzada creando usuarios en ambos bosques y validando el acceso a recursos compartidos.

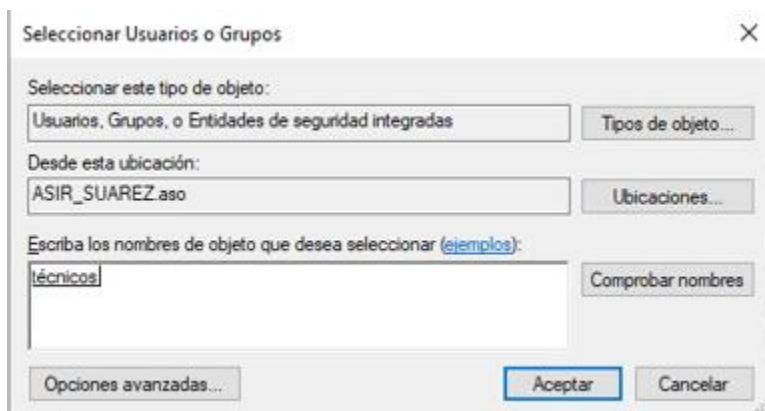
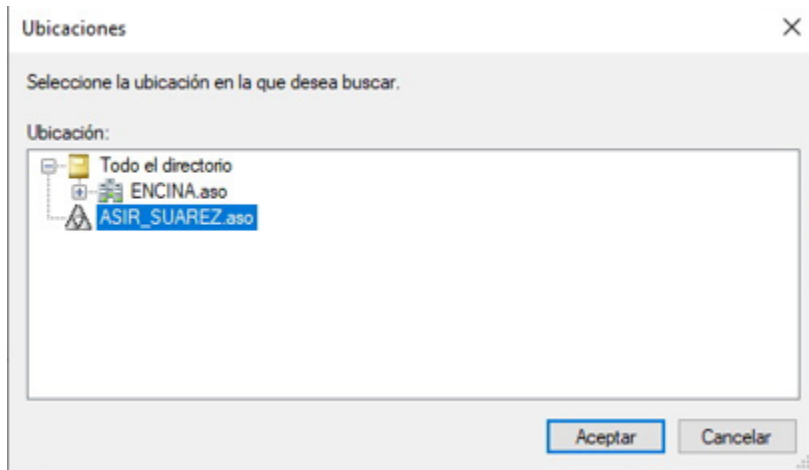
En **Encina.aso** hemos creado un usuario que pertenece al grupo **Marketing**.



Luego en **ASIR_SUAREZ.aso** hemos creado una carpeta compartida para el grupo **Marketing**, perteneciente al dominio **ENCINA.aso**



Luego hicimos lo mismo en el Controlador de **Encina.aso** para el grupo **técnicos** de **ASIR_SUAREZ.aso**



← Acceso a la red

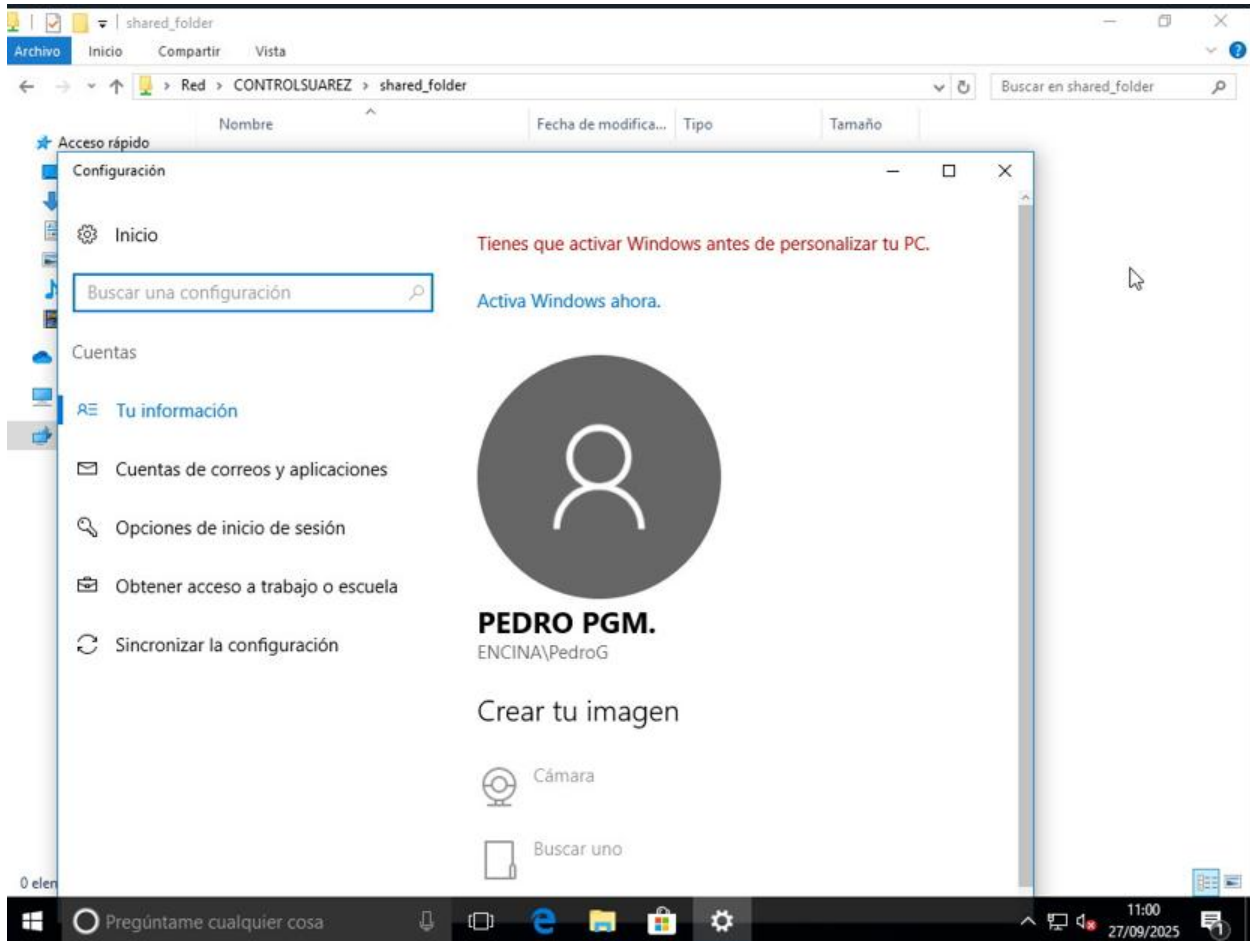
La carpeta está compartida.

Puedes [enviar por correo electrónico](#) a cualquier persona vínculos a estos elementos compartidos o [copiar](#) los vínculos y pegarlos en otra aplicación.

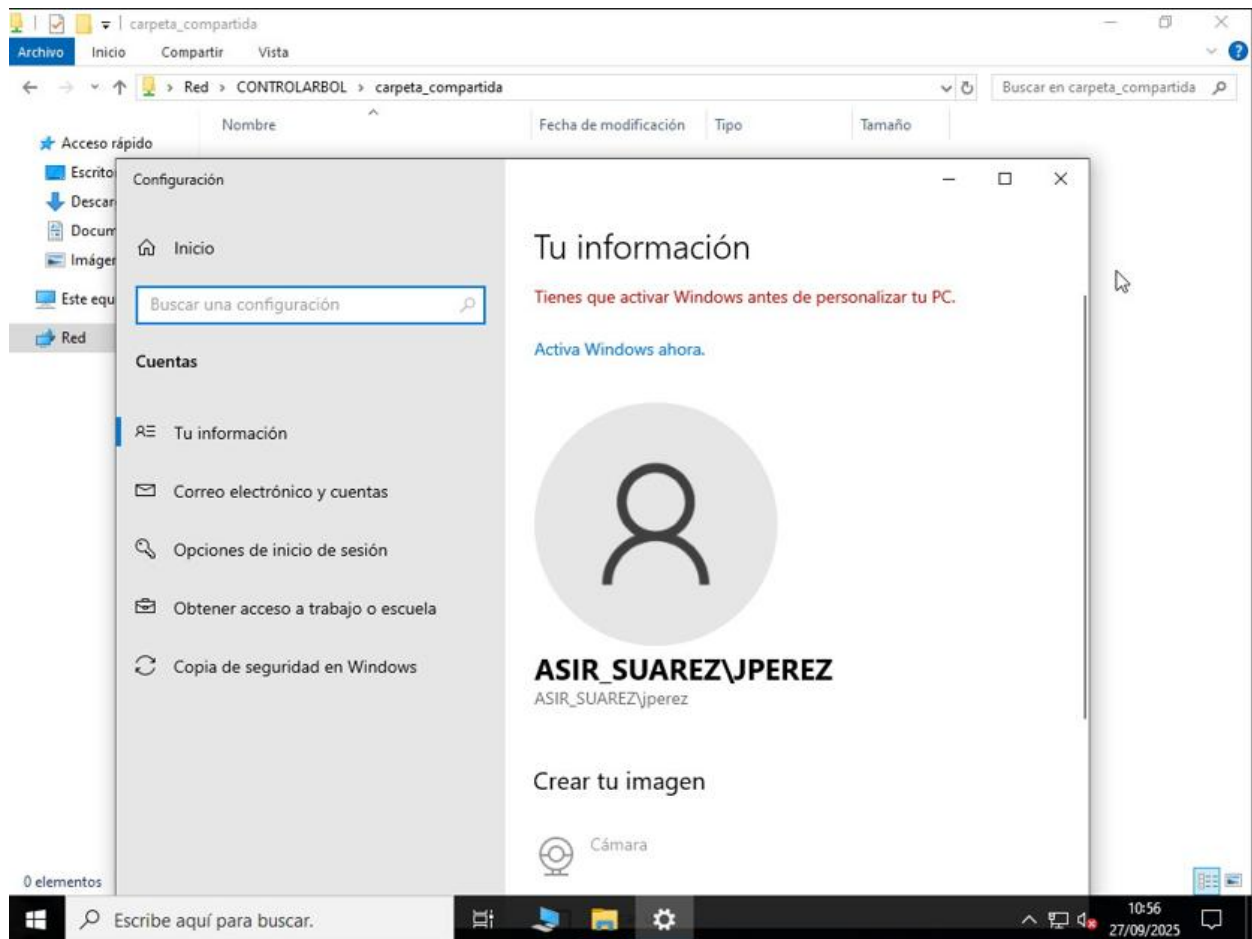


d) Para comprobar que funciona, intenta acceder a recursos compartidos entre dominios con diferentes usuarios.

Ahora podemos ver como el usuario **Pedro** de **Encina.aso** accede al recurso compartido que está configurado en el Controlador de **ASIR_SUAREZ.aso**



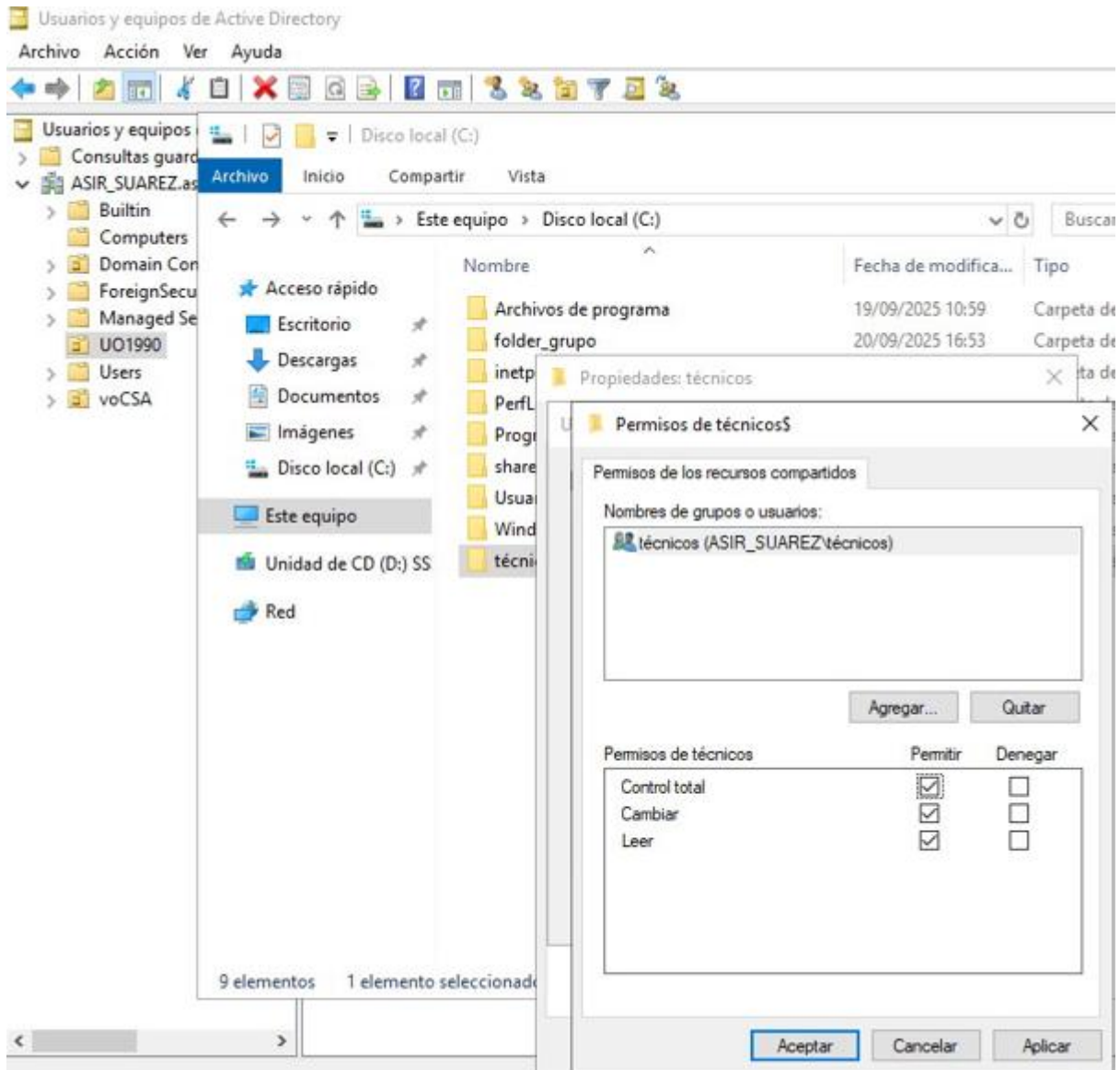
Y al usuario **jperez** de **ASIR_SUAREZ.aso** acceder al que está en **ENCINA.aso**



4) Perfiles móviles de usuario.

a) En el dominio principal, habilita un recurso compartido centralizado.

Vamos a aprovechar la carpeta compartida que creamos en la Actividad 1 y vamos a colocar allí los perfiles móviles (los usuarios deben pertenecer a un grupo que tenga control total en la carpeta donde se van a establecer los perfiles móviles).

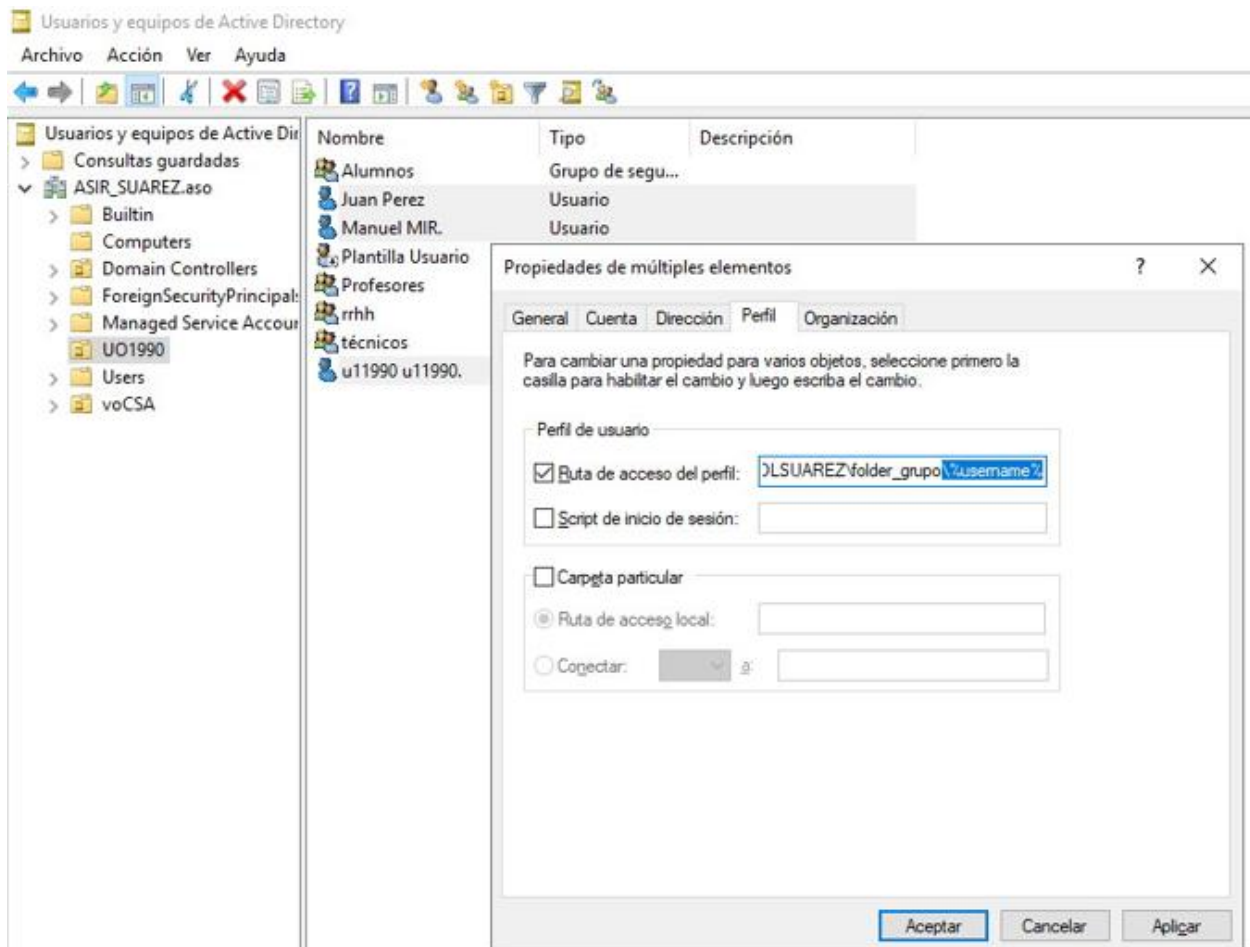


b) Modifica las propiedades de varios usuarios en Active Directory Users and Computers para que usen perfiles móviles.

Ahora solo debemos ir a **Usuarios y equipos de Active Directory**, seleccionar los usuarios del grupo (esta configuración no se puede llevar a cabo en el objeto del grupo), abrimos **Propiedades**, pestaña **Perfil** y marcamos **Ruta de acceso del perfil**, poniendo:

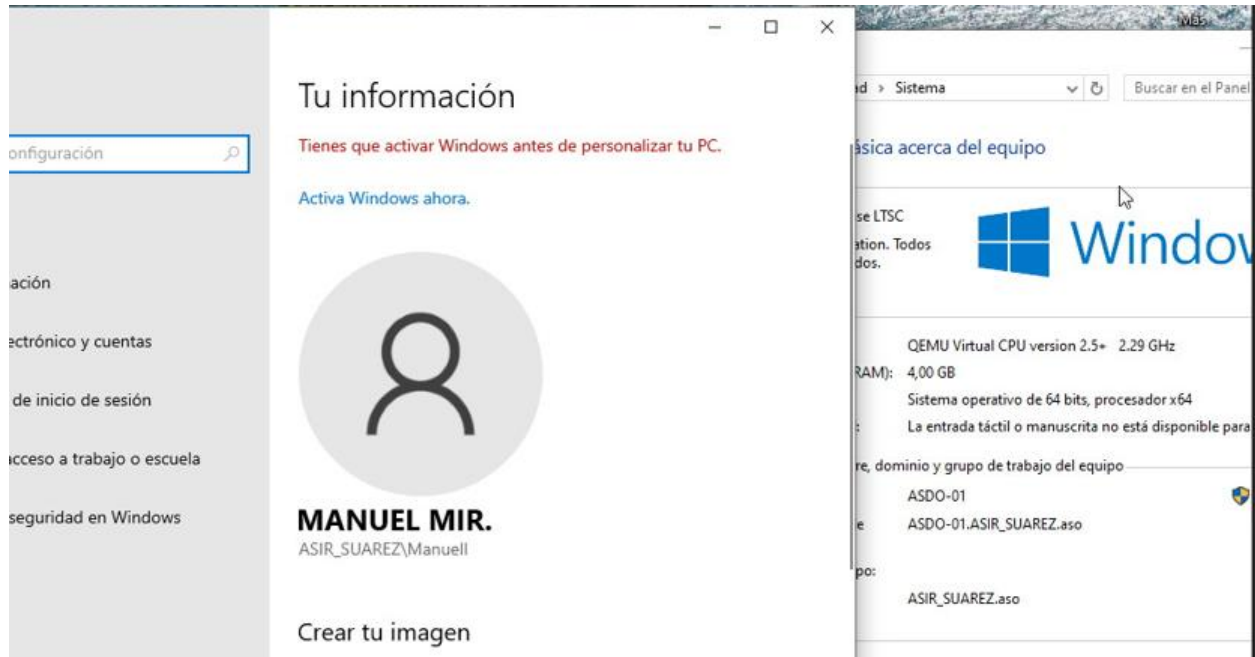
[\\Nombre_del_servidor\ruta\%username%](#)

Esto generará una carpeta para cada usuario cuando inicien sesión.

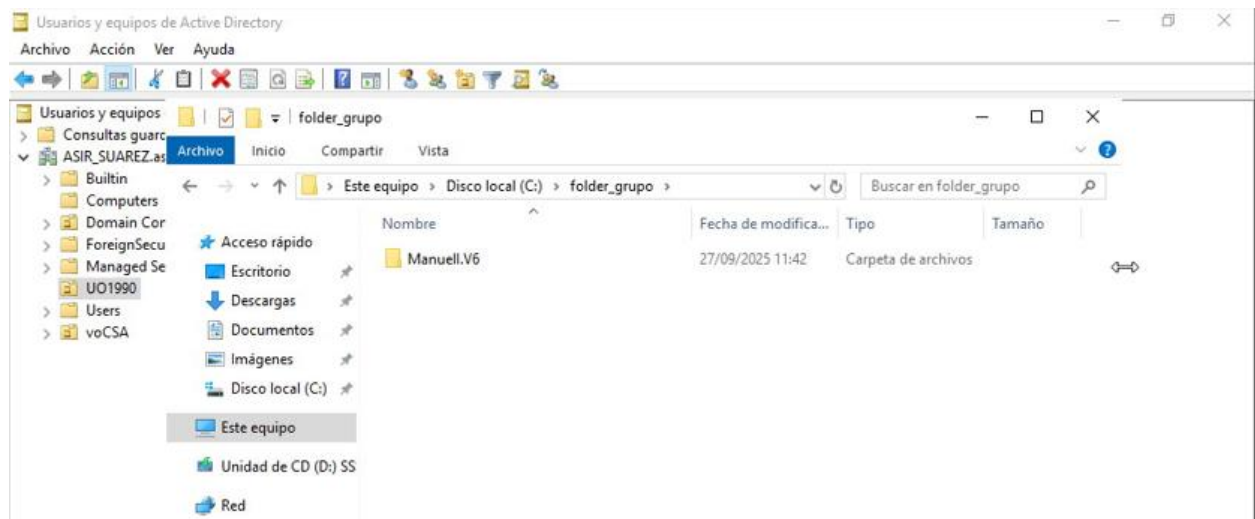


c) Inicia sesión con los usuarios en diferentes equipos unidos al dominio y comprueba.

Iniciamos sesión con el usuario **Manuell** en un cliente perteneciente al dominio.

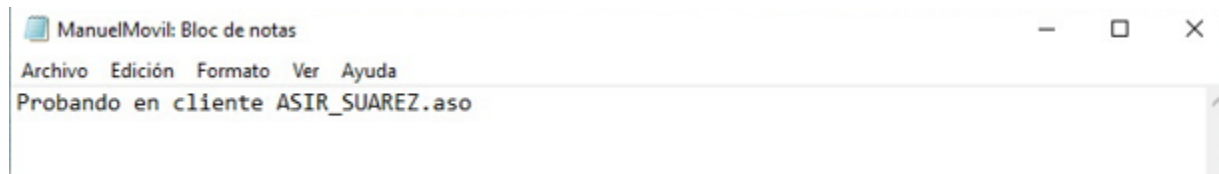


Al instante se crea la carpeta que contiene el perfil móvil.

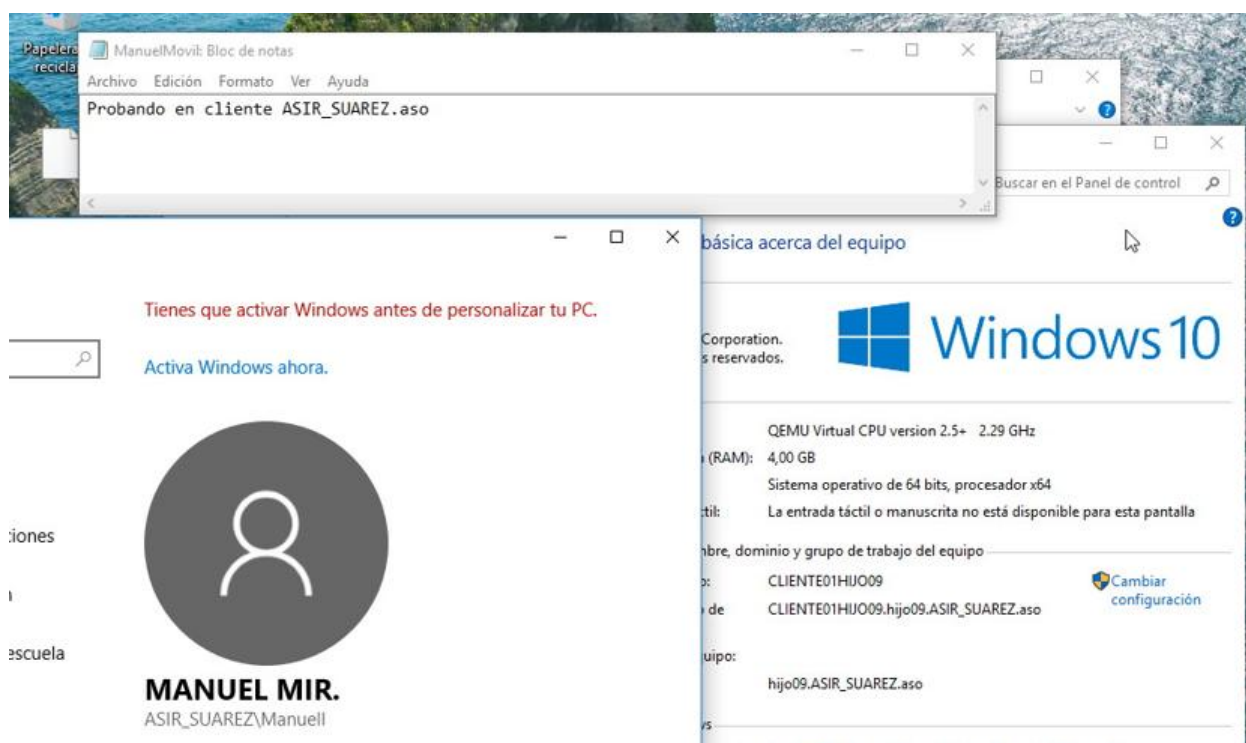


Creamos un documento de texto en el Escritorio del Cliente del Dominio

ASIR_SUAREZ.aso con el usuario **Manuell**

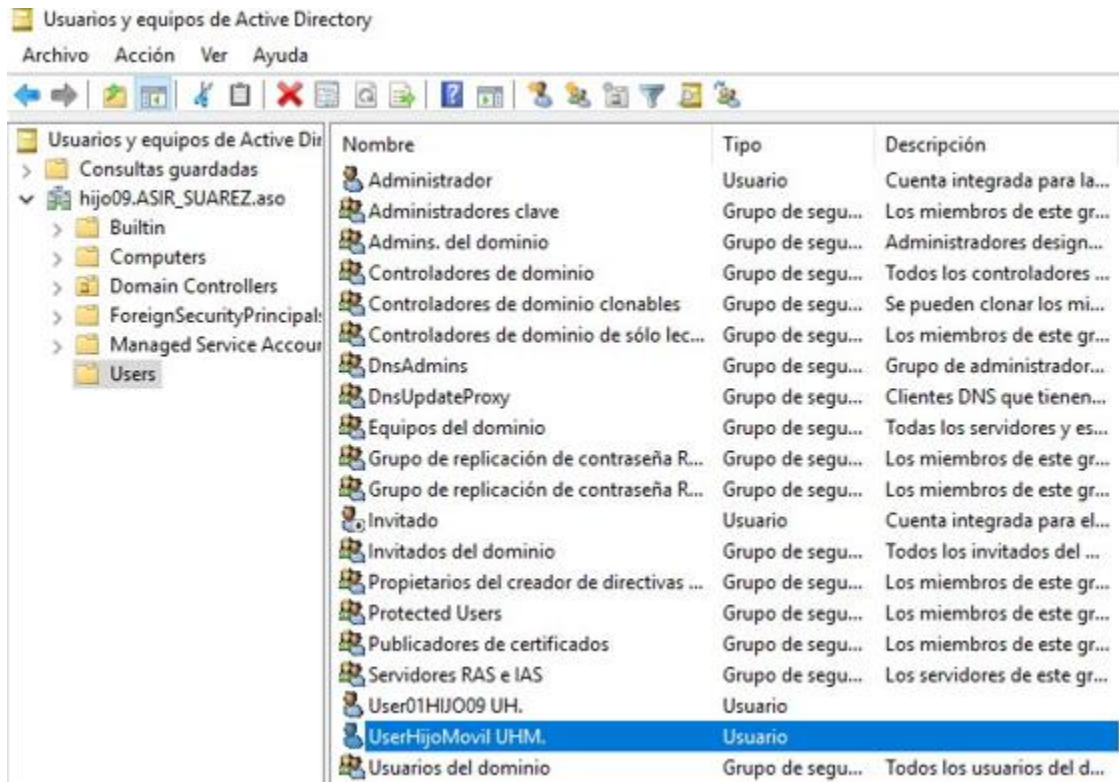


Después con el mismo usuario, iniciamos sesión en un cliente del subdominio. El archivo se encontraba en el Escritorio, de igual manera que en el otro cliente.

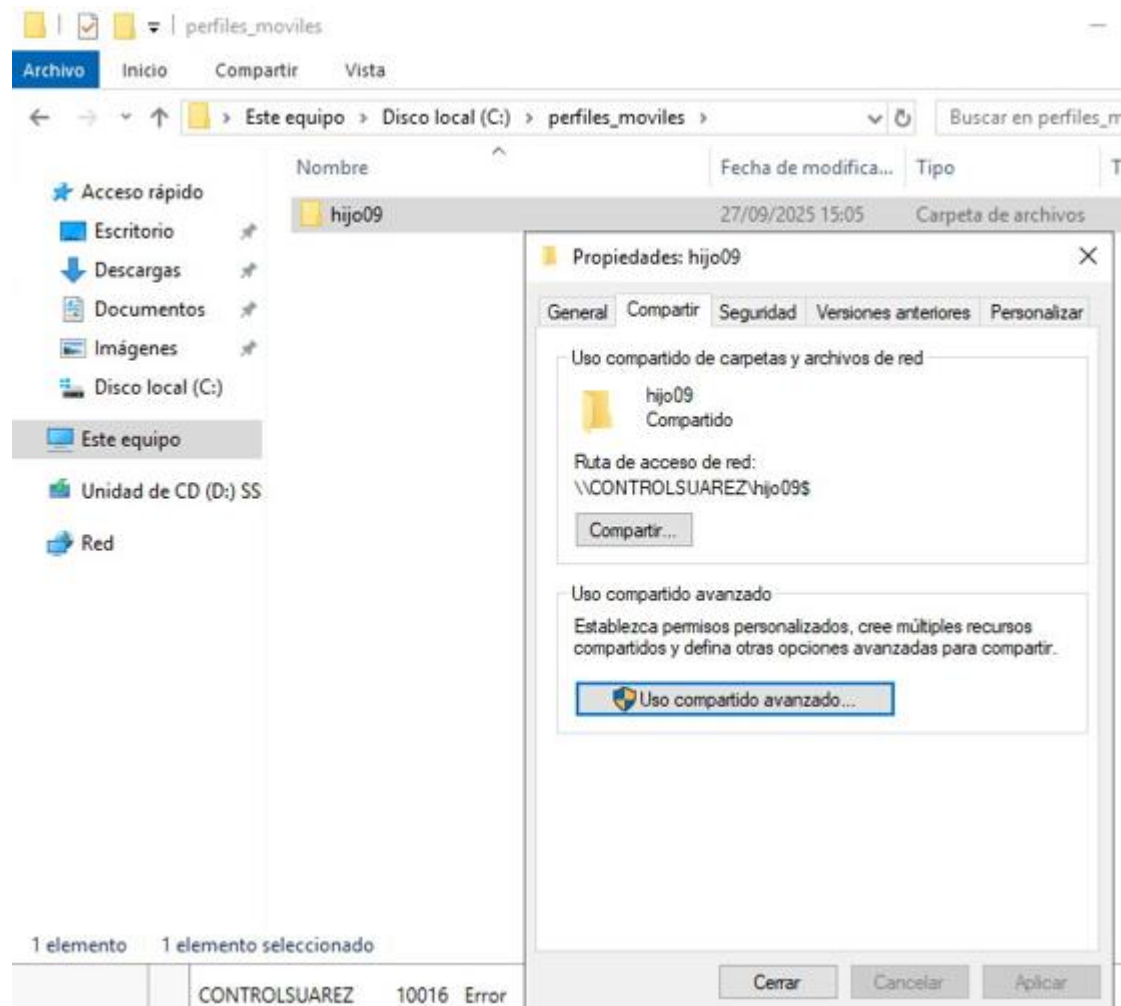


5) Escenario avanzado de pruebas.

- a) Crea un usuario en el subdominio y configura su perfil móvil en el dominio principal. Verifica si puede acceder desde equipos unidos al subdominio.



Creamos una carpeta compartida en el Controlador del Dominio Principal donde se almacenarán las carpetas de los perfiles.



Establecemos la **Ruta del Perfil** en la cuenta de usuario:

Propiedades: UserHijoMovil UHM. ? X

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto		COM+	
General	Dirección	Cuenta	Perfil
Teléfonos		Organización	Miembro de

Perfil de usuario

Ruta de acceso al perfil:

Script de inicio de sesión:

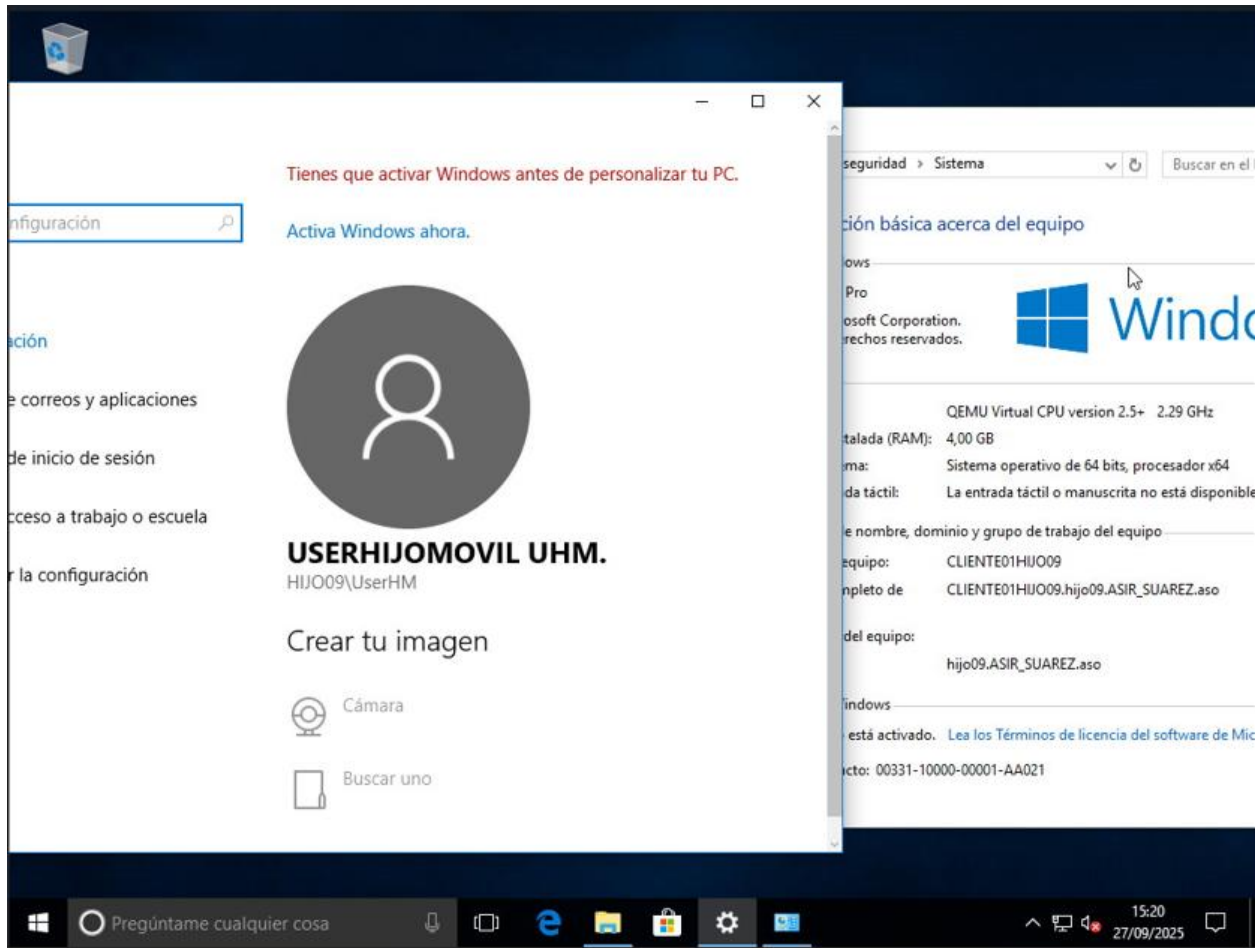
Carpeta particular

☒ Ruta de acceso local:

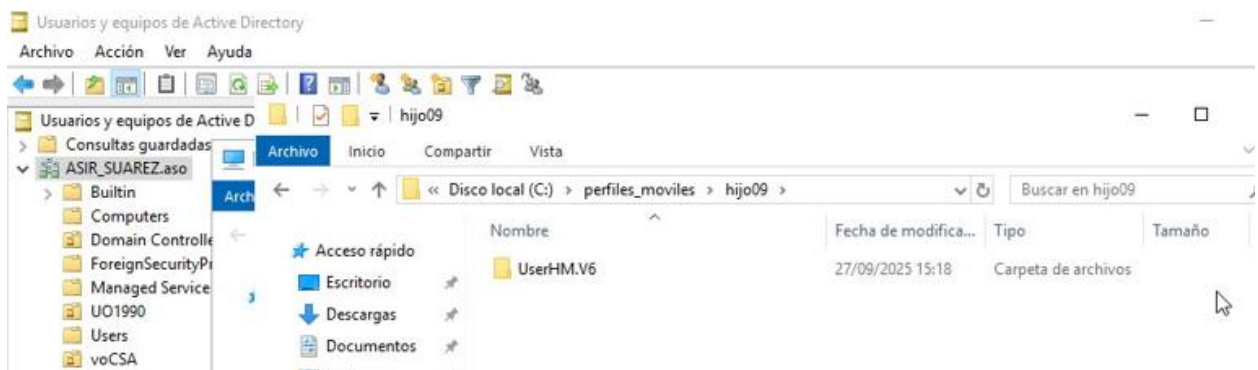
☐ Conectar: a:

Aceptar Cancelar Aplicar Ayuda

Iniciamos sesión con el usuario en un cliente del Subdominio.

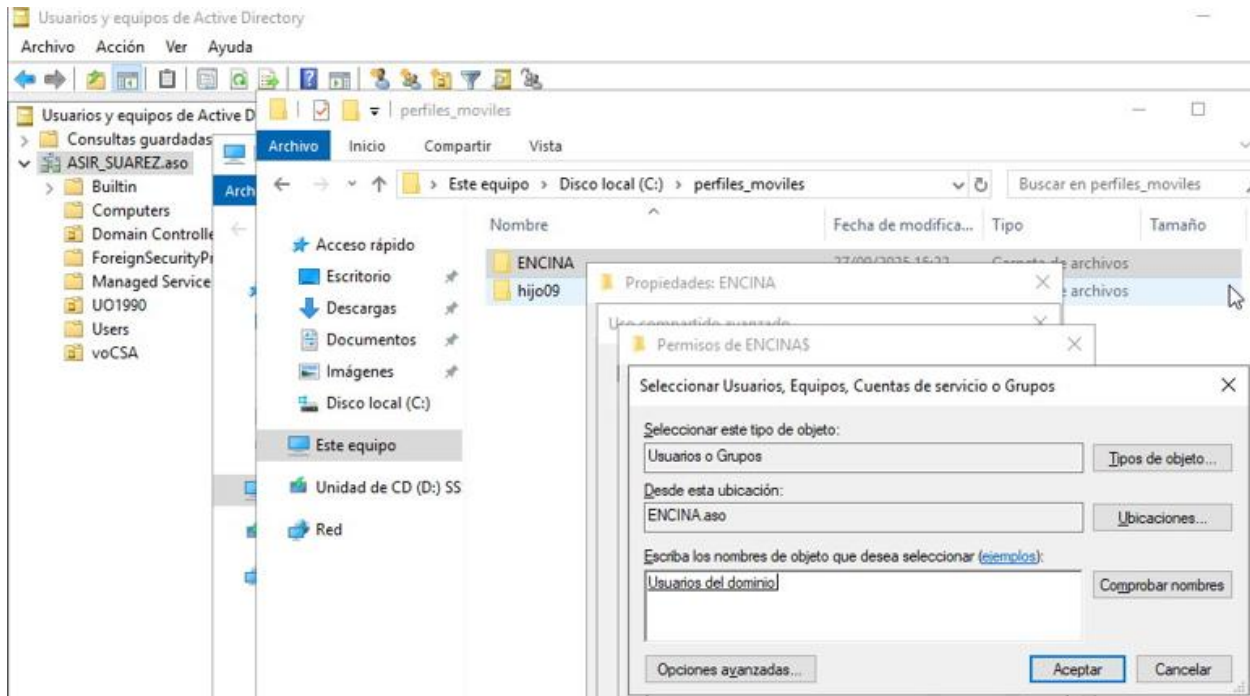


La carpeta se crea en el Controlador.

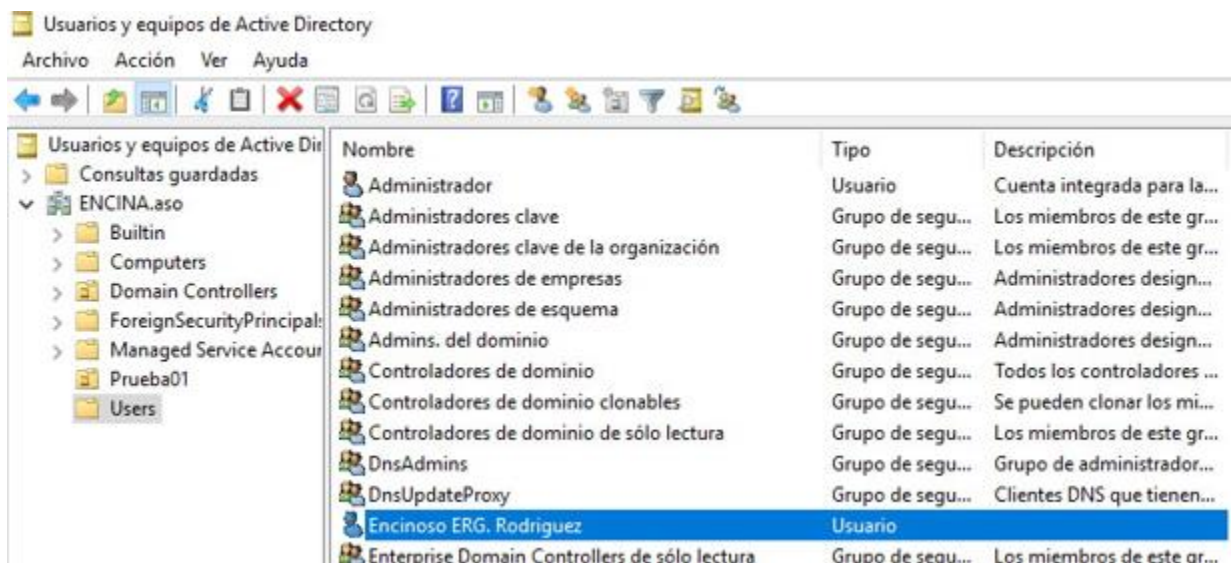


- b) Crea un usuario en el bosque alternativo y prueba si puede usar perfiles móviles almacenados en el dominio principal mediante relaciones de confianza.

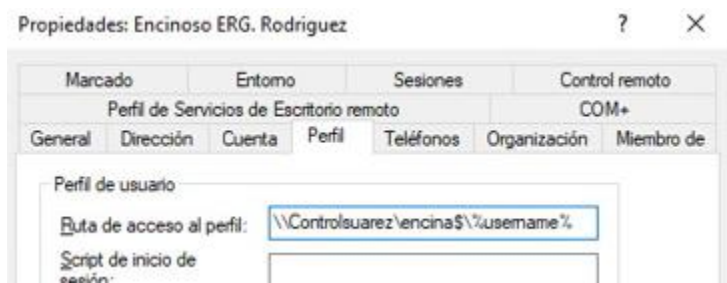
En el Controlador del Dominio Principal creamos una carpeta para los **Usuarios del dominio de Encina.aso**



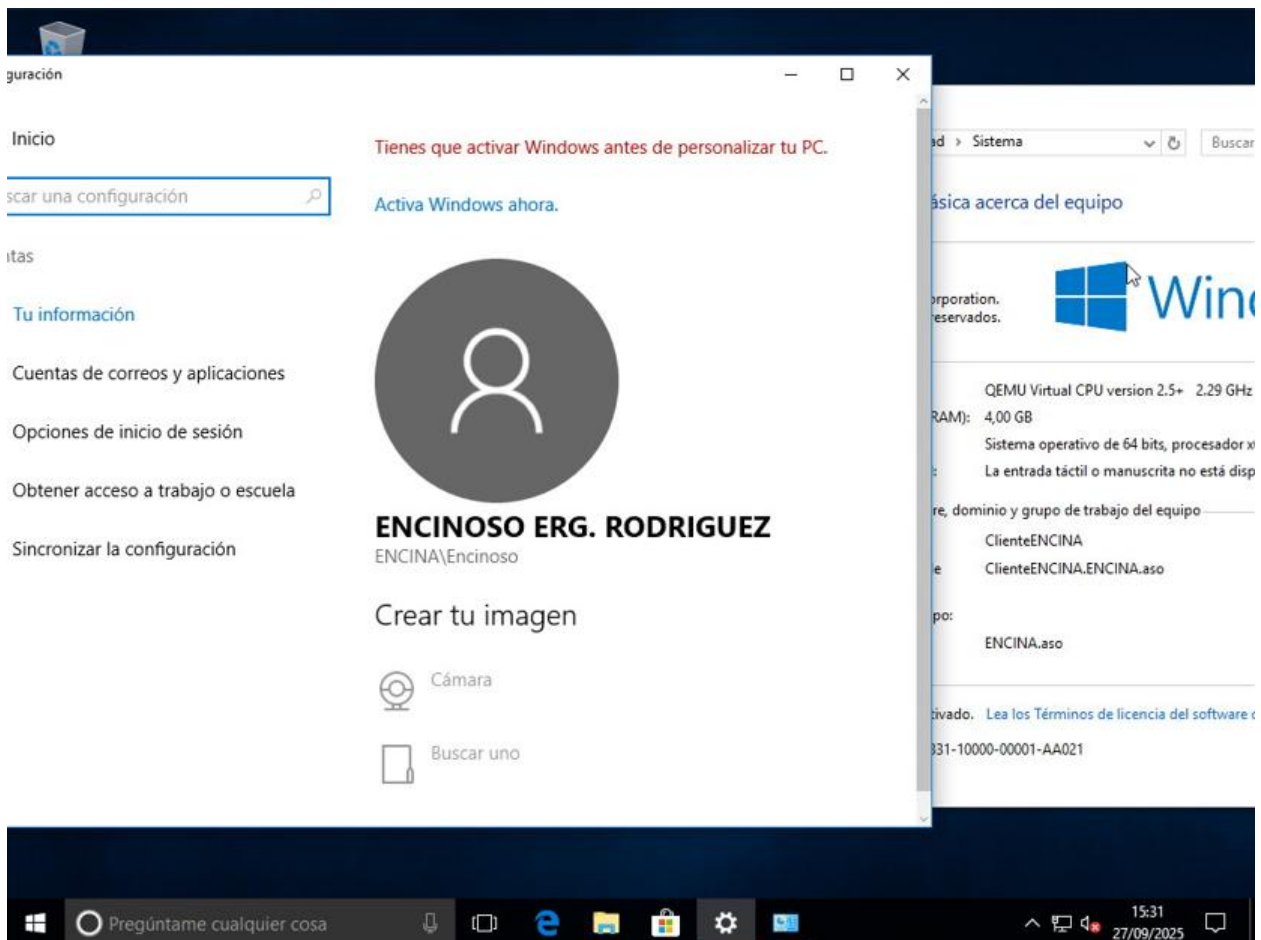
Luego en **Encina.aso** creamos al usuario **Encinoso**.



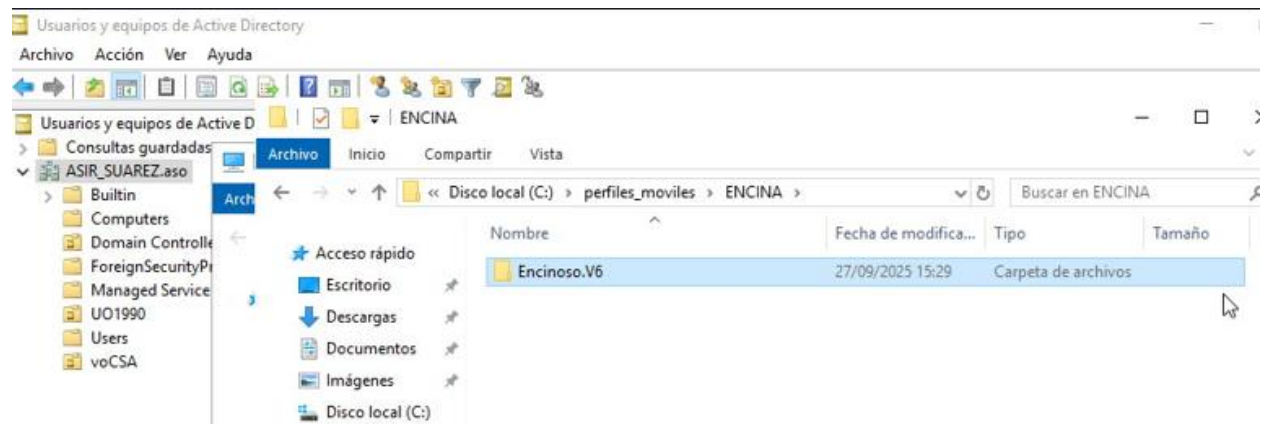
Establecemos su ruta de Perfil Movil.



Iniciamos sesión en un cliente de **Encina.aso**



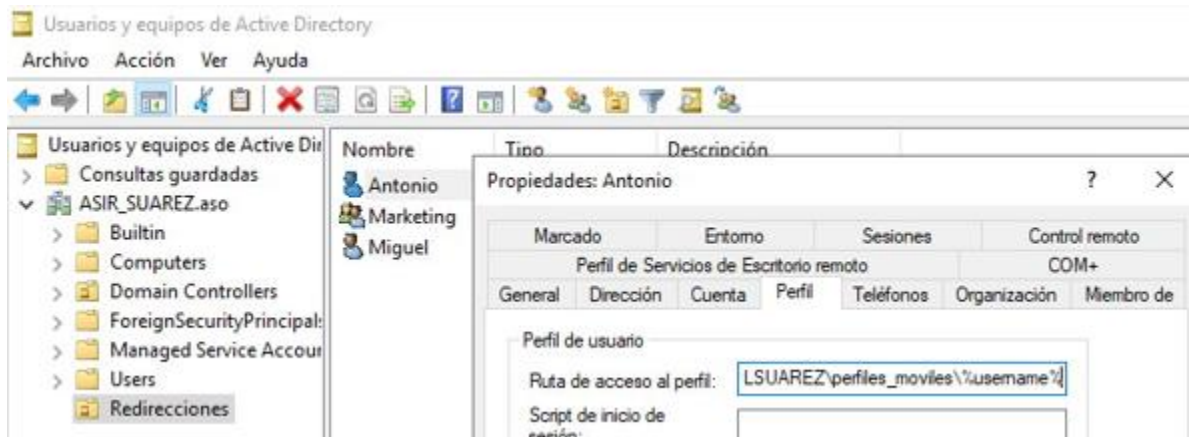
Vemos como se ha creado la carpeta del perfil móvil en el Controlador de **ASIR_SUAREZ.aso**



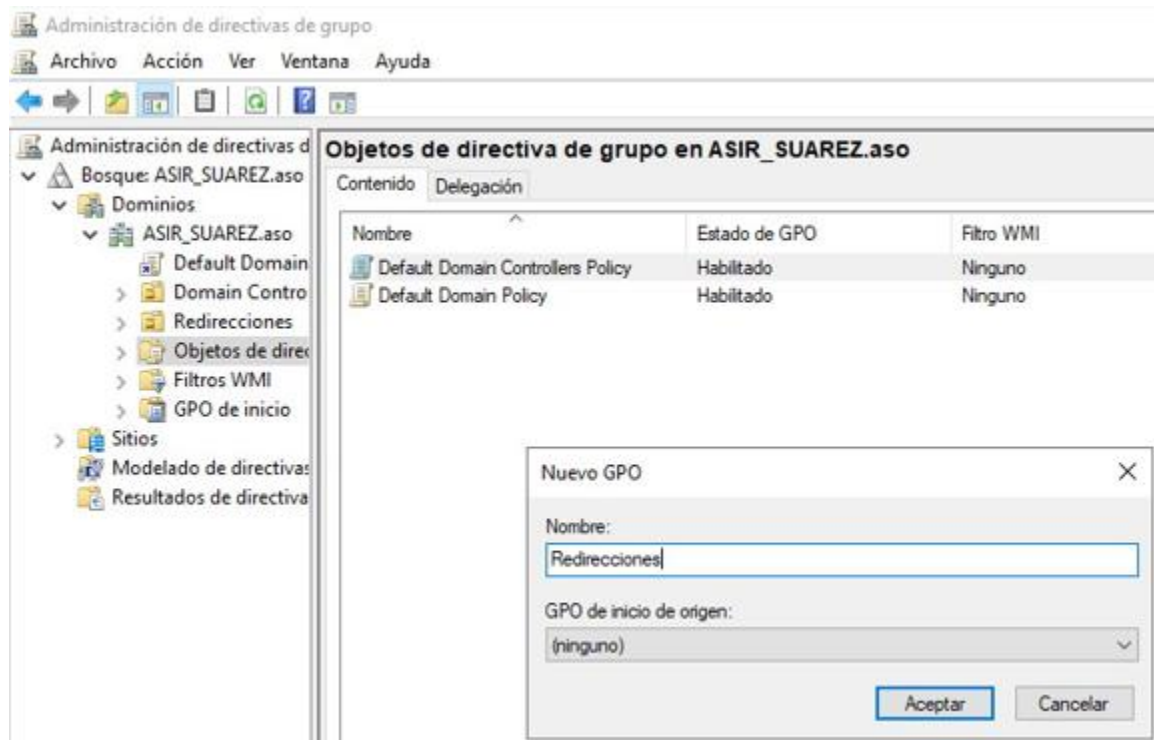
- c) Establece políticas de grupo (GPO) para redirigir carpetas (Documentos, Escritorio) hacia carpetas de red y comprueba que funcionan junto con los perfiles móviles.

Para este ejercicio, creamos vamos a crear una Unidad Organizativa específica:

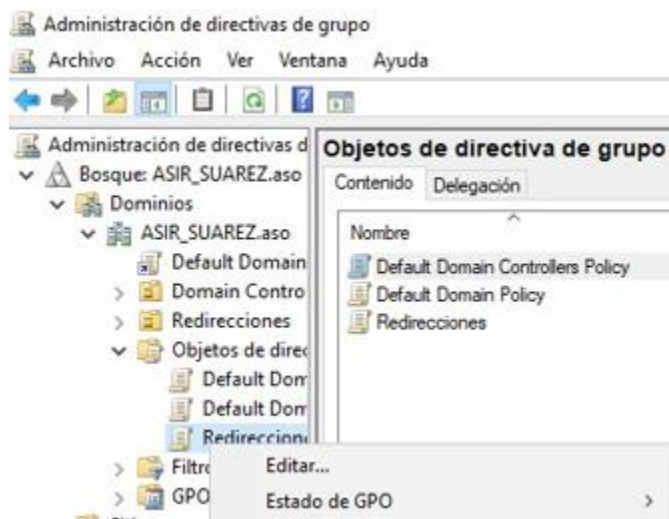
Redirecciones. Donde vamos a colocar al grupo **Marketing** y a dos de sus usuarios. Como hemos hecho en actividades anteriores, debemos configurar la carpeta **perfiles_moviles** como un recurso compartido al cual los usuarios puedan tener acceso (ya sea por grupos específicos o con “Usuarios del dominio”).



Ahora vamos a crear la GPO: **Herramientas → Administración de directivas de grupo**. Desplegamos hasta el dominio y luego en **Objetos de directiva de grupo** le damos a **Nuevo GPO**. Ponemos el nombre y en este caso no hay que marcar **GPO de inicio de origen**.

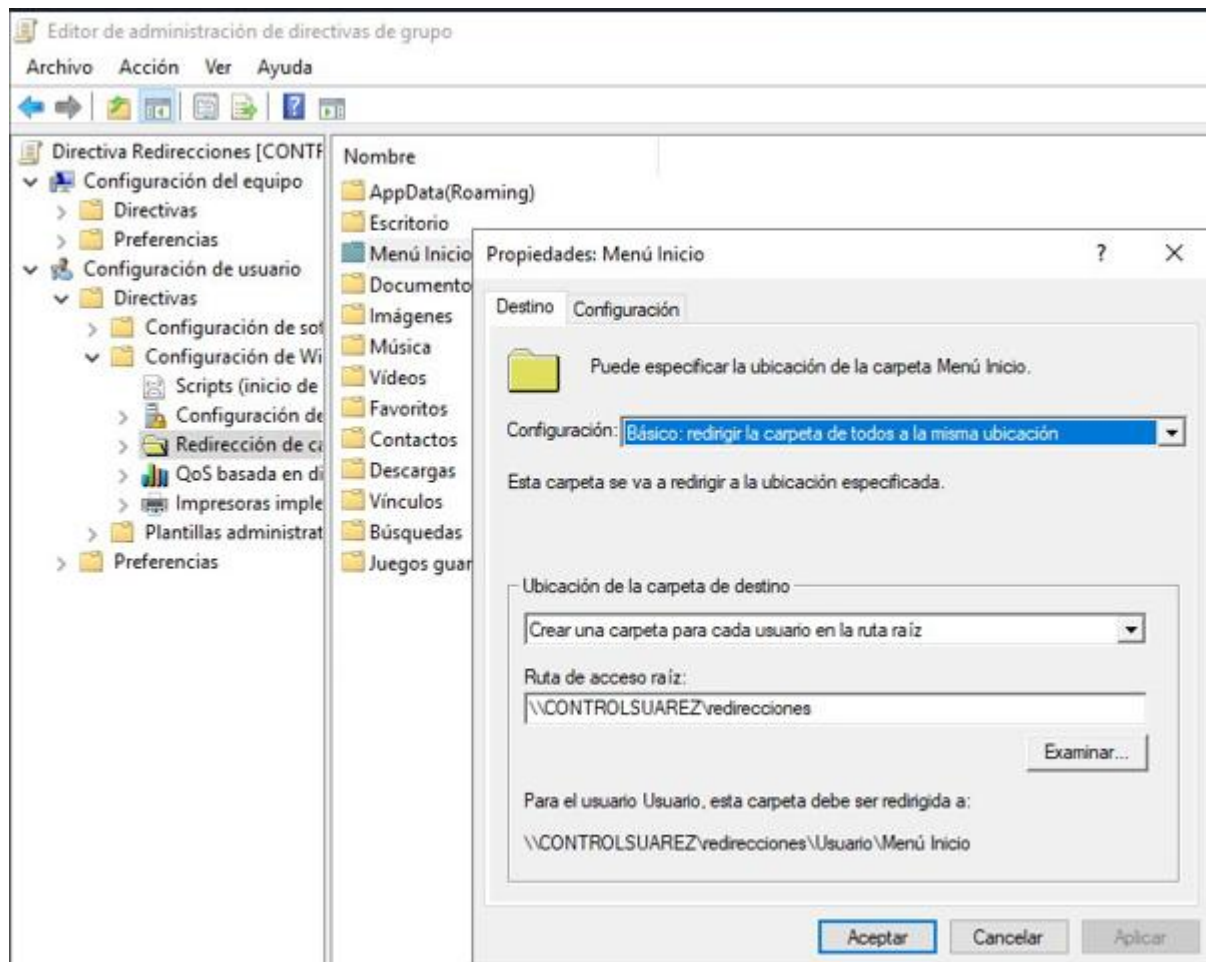


Una vez creada, la buscamos dentro de **Objetos de directiva de grupo** y le damos a **Editar...**

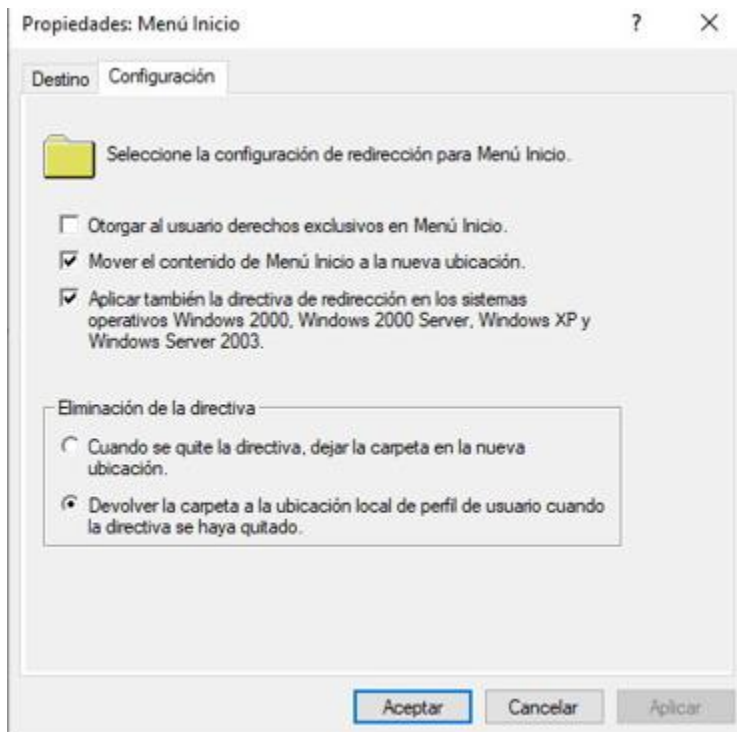


Navegamos: **Configuración de usuario → Directivas → Configuración de Windows → Redirección de carpetas**. Aquí tenemos una selección de carpetas predefinidas del usuario que podemos redirigir. En este caso vamos a usar “Menú inicio” y “Documentos”. La configuración para ambas es la misma.

Elegimos **Básico: redirigir la carpeta de todos a la misma ubicación**. Luego **Crear una carpeta para cada usuario en la ruta raíz**. Y más adelante establecemos la dirección del servidor donde estará la carpeta. Recuerda que la carpeta debe tener permisos para poder compartirla con los usuarios que van a usar los perfiles móviles (si no pueden acceder a ella no se pueden crear los perfiles de manera automática)



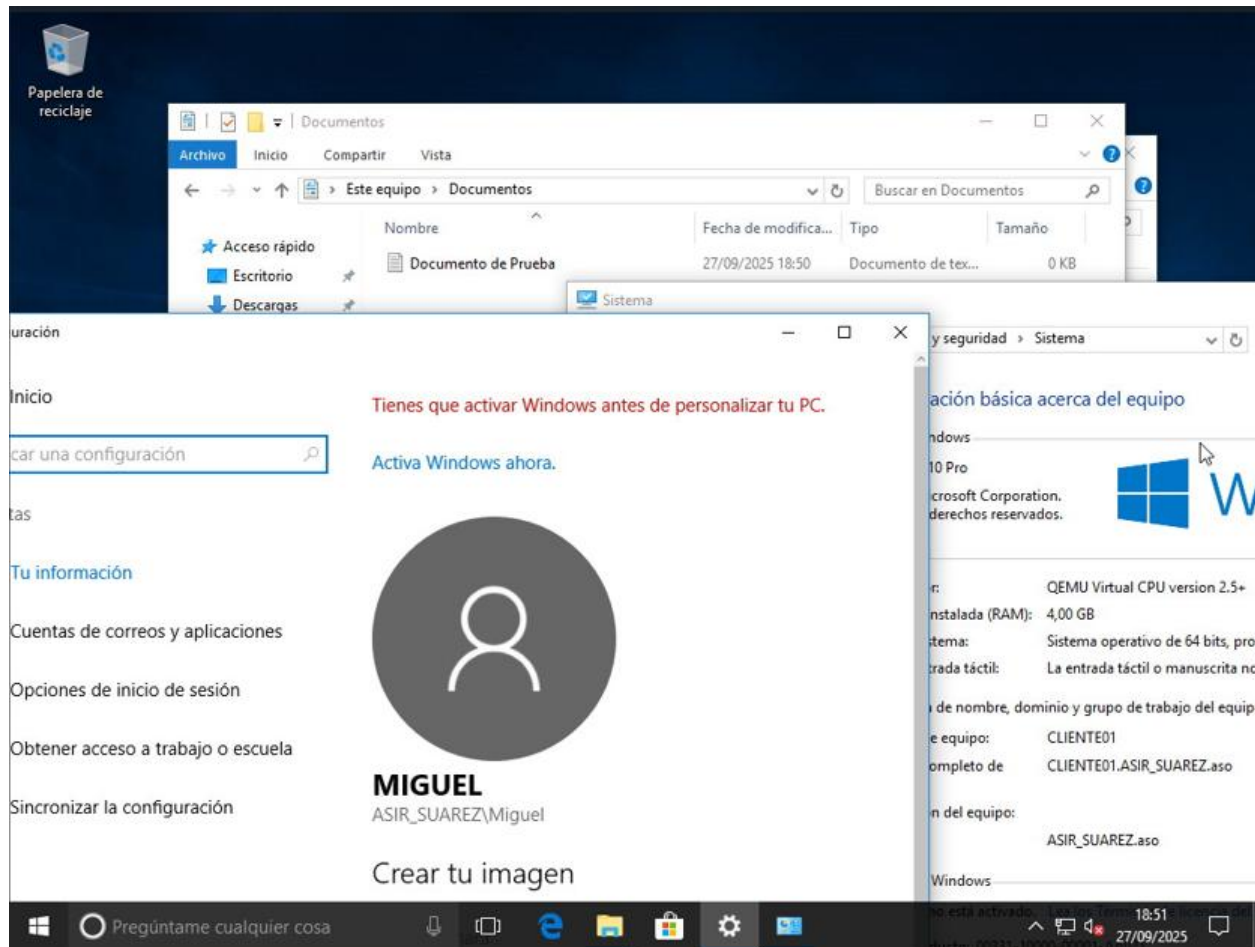
Pestaña **Configuración**.



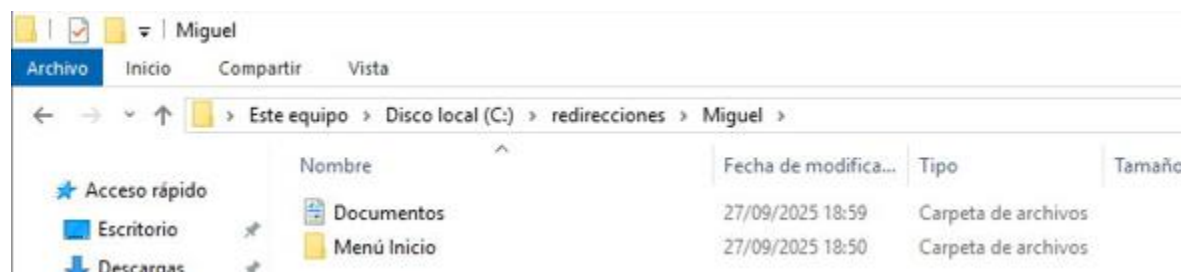
Una vez configurada la GPO, debemos vincularla con la Unidad Organizativa. Para ello seleccionamos la UO y le damos a **Vincular un GPO existente...**



Ahora solo queda comprobar: iniciamos sesión con un usuario y creamos un archivo en **Documentos**.



En la carpeta **redirecciones** del Controlador, se creará una carpeta llamada **Manuel** donde se encontrarán las carpetas **Menú de Inicio** y **Documentos** de dicho usuario.



También podremos ver que se replica el archivo de prueba que creamos en la carpeta **Documentos**.

