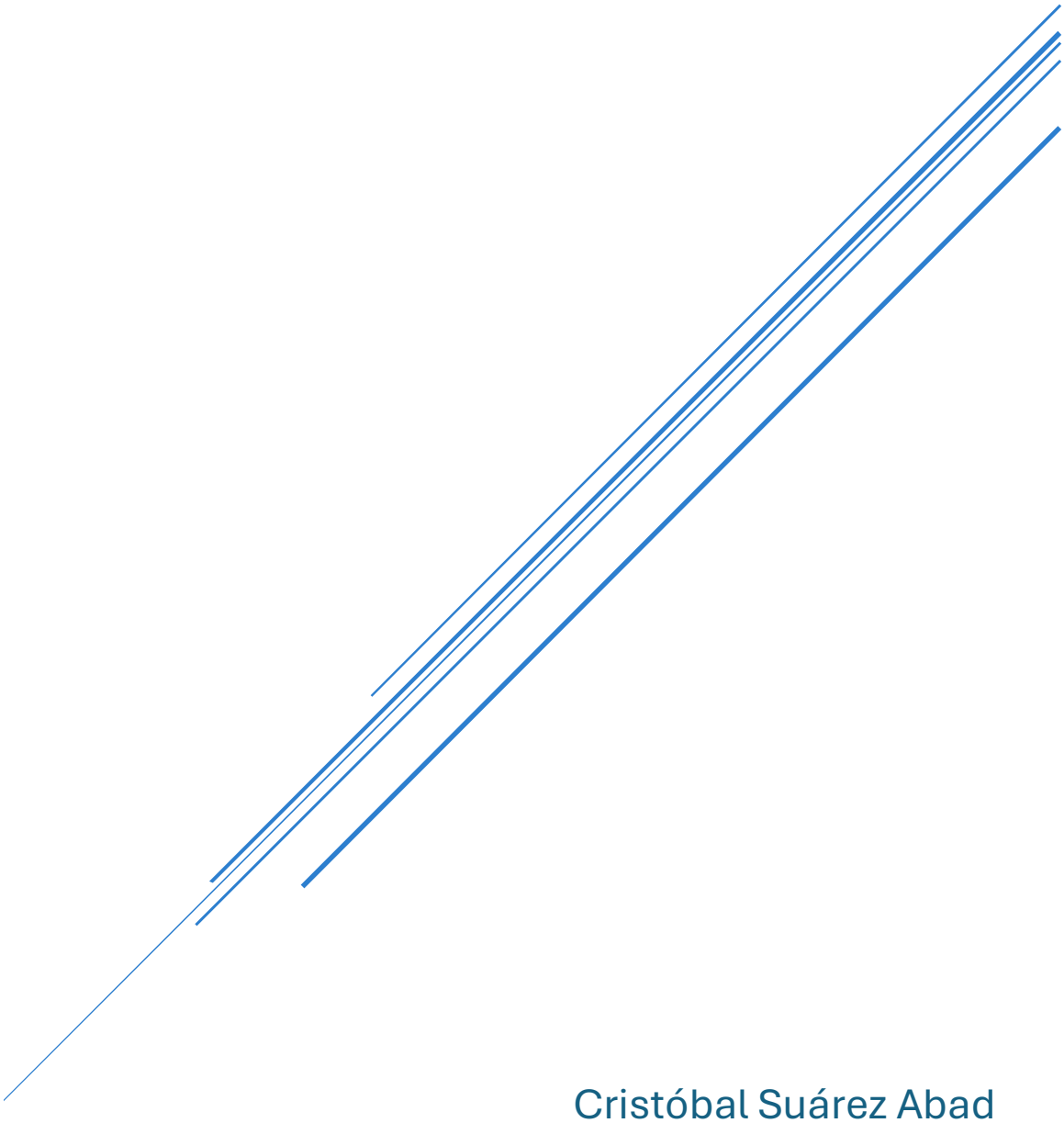
ACTIVIDAD 1.2 ACTIVE DIRECTORY

Administración de Dominios, Confianzas y Perfiles Móviles en Windows Server



Cristóbal Suárez Abad
Administración de Sistemas Operativos – 2º ASIR

Índice:

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).

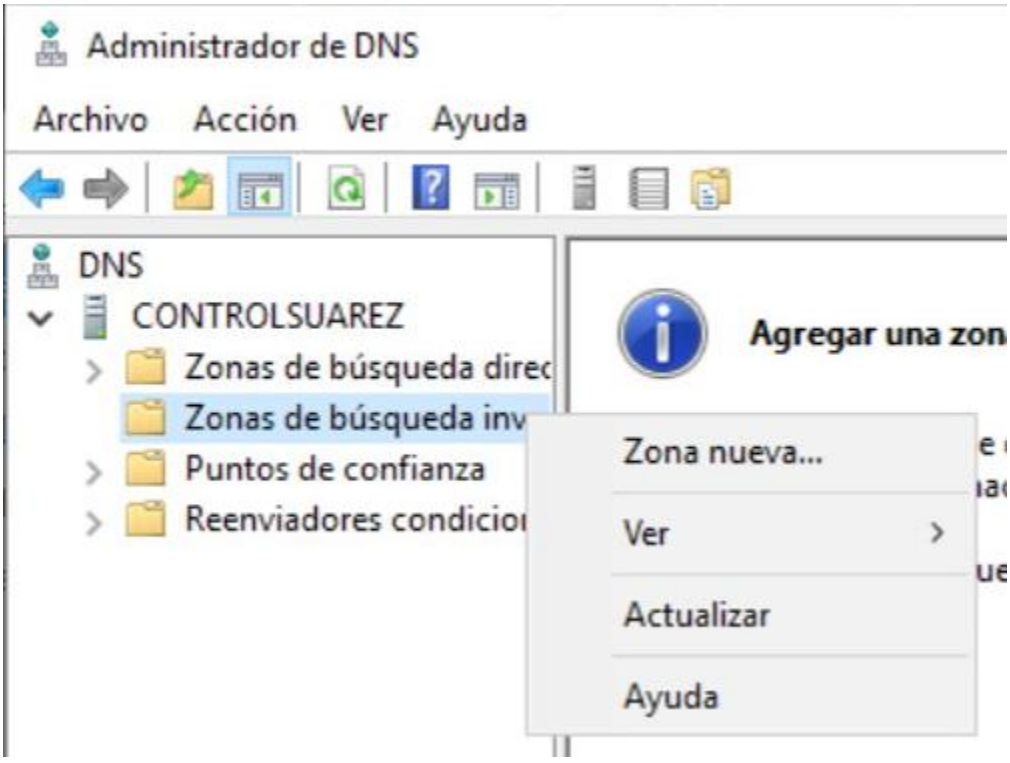
a) Partiendo de un dominio funcional, instala un segundo servidor Windows Server y conviértelo en controlador de dominio secundario del dominio existente.

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**.

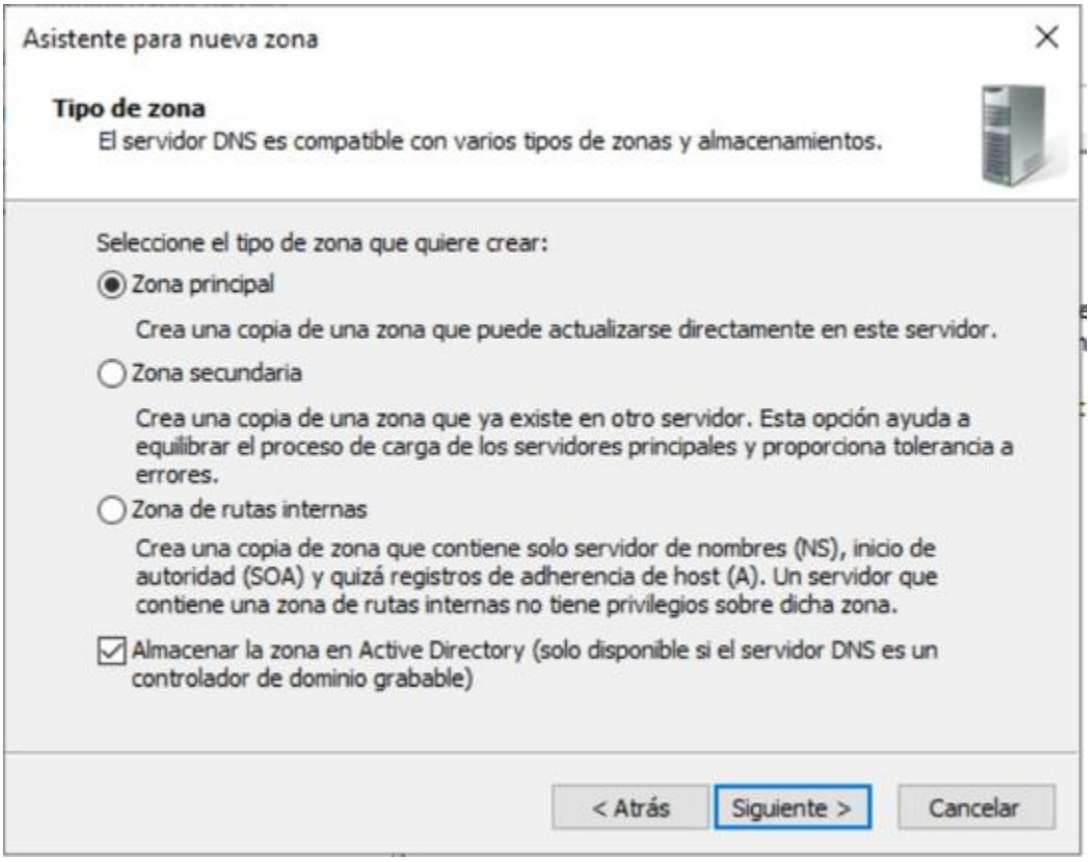
Desplegamos el nombre del Dominio y en "**Zonas de búsqueda inversa**" le damos a "**Zona nueva**".



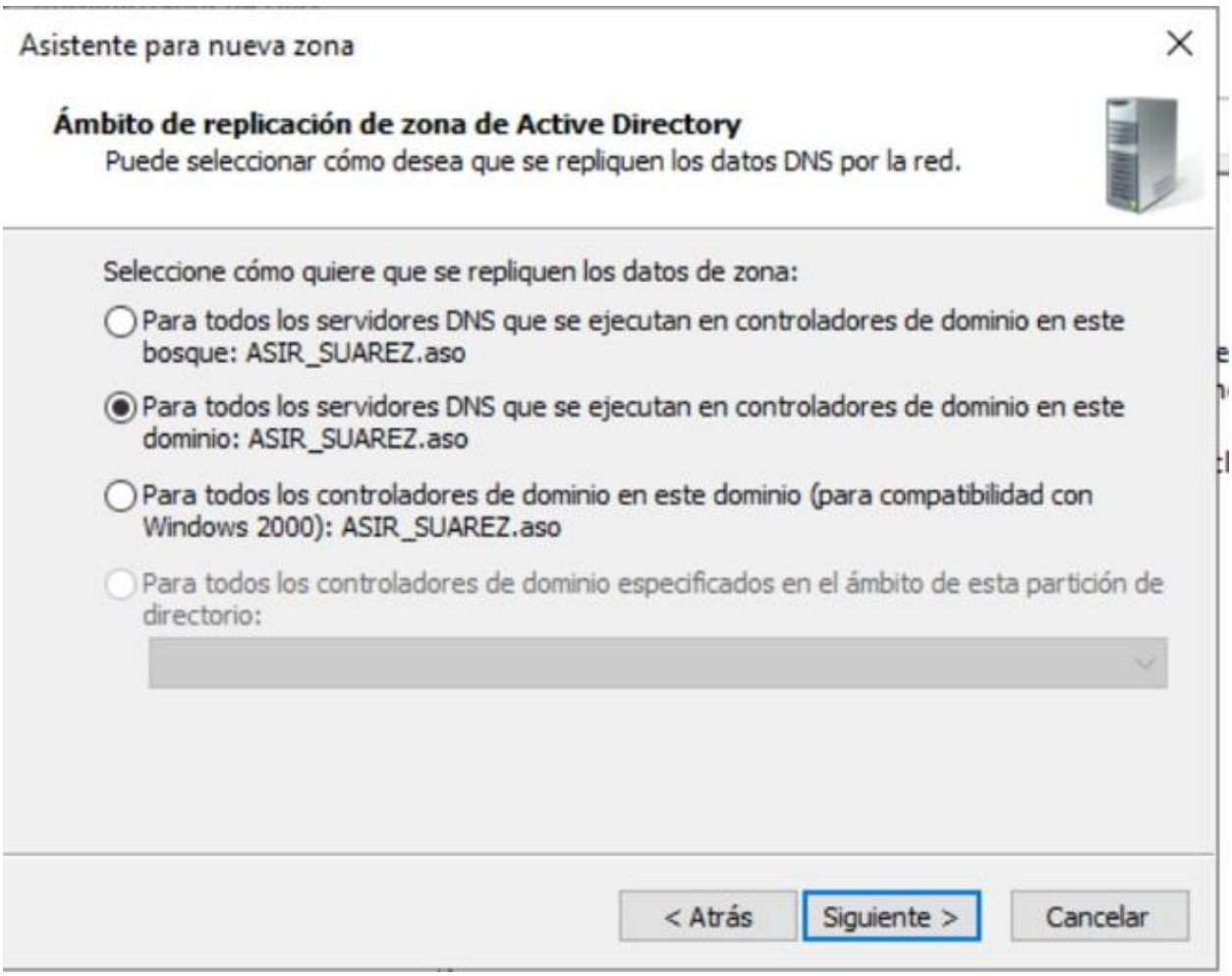
[1] https://somebooks.es/anadir-un-nuevo-controlador-de-dominio-para-un-dominio-existente-en-windows-server-2019-parte-1/

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

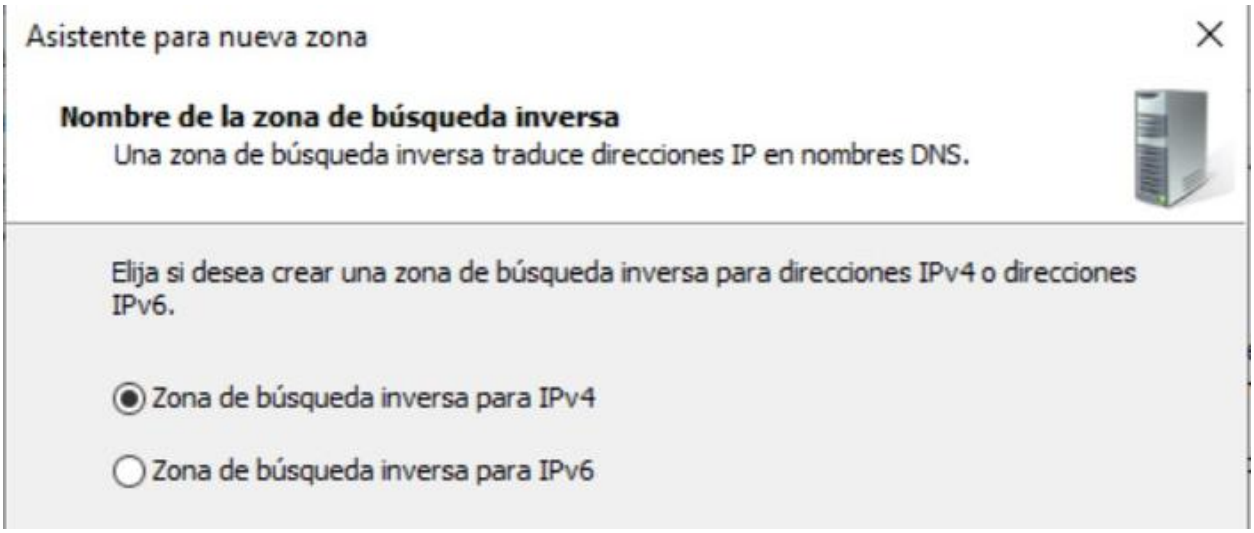
Tipo de zona: **Zona principal**.



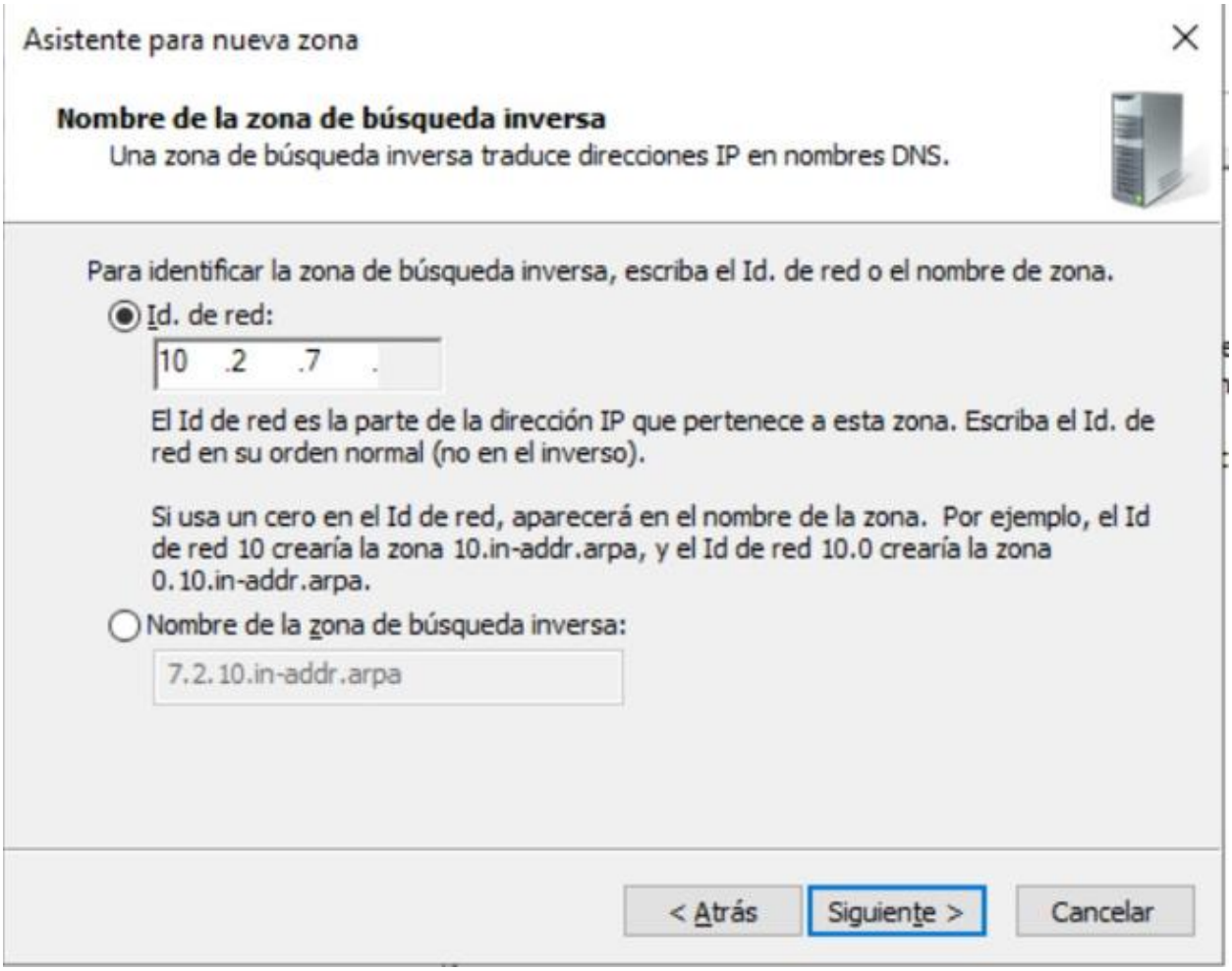
Ámbito de replicación: **Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: ASIR_SUAREZ.aso**



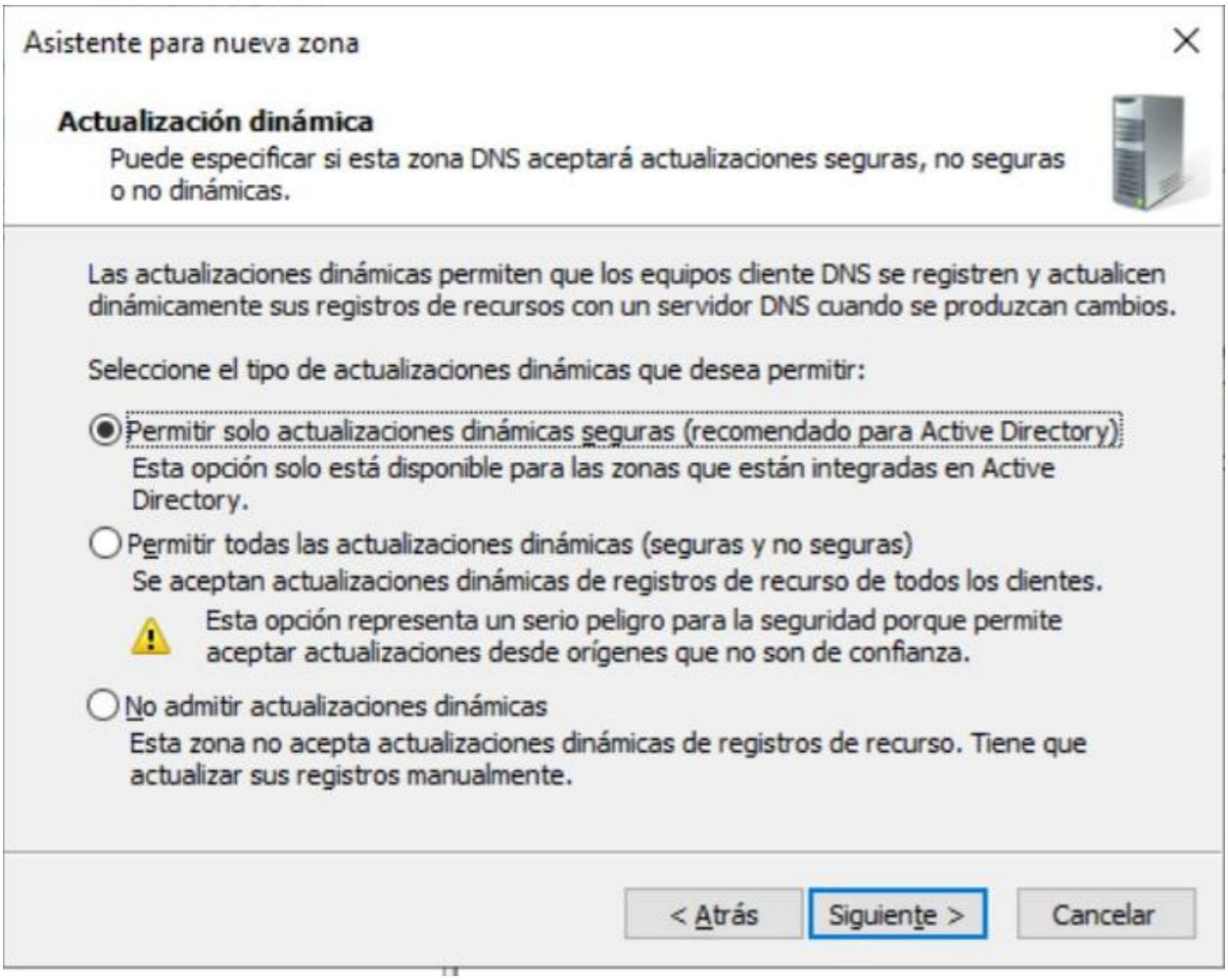
Zona búsqueda inversa: **IPv4**



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

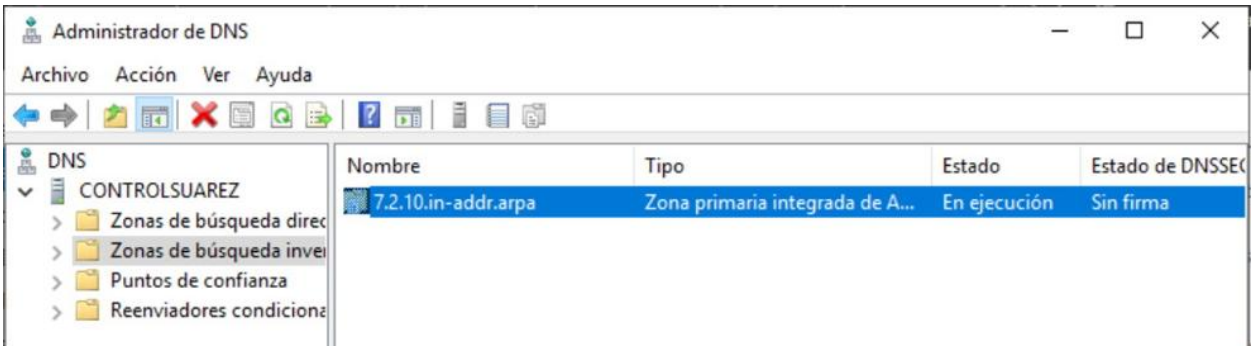


Configuración de actualizaciones dinámicas:

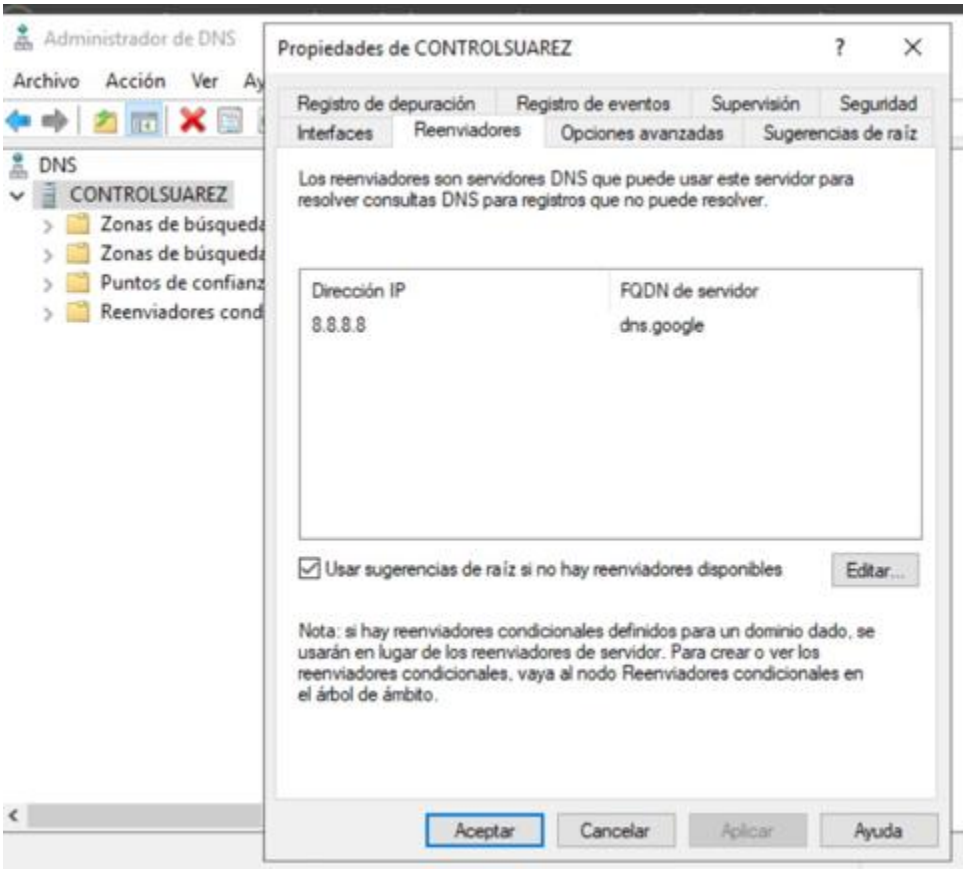


Finalización del Asistente.

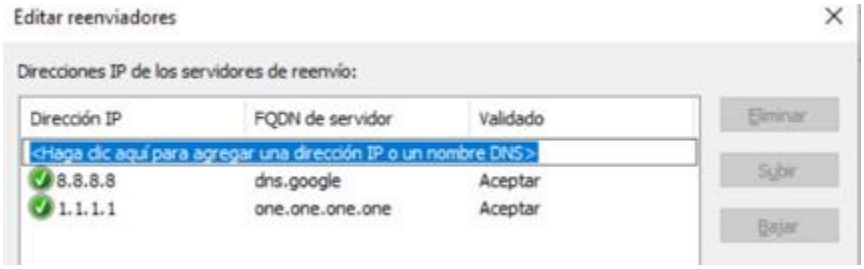
Zona de búsqueda una vez creada.



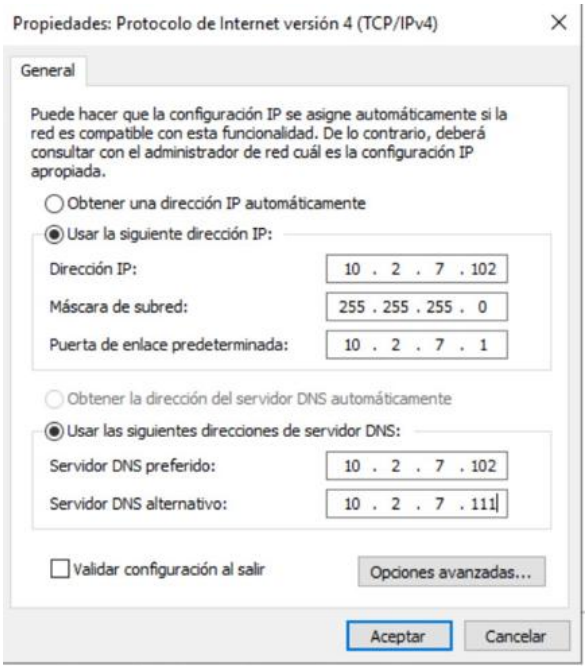
Ahora vamos a configurar los reenviadores, esto permitirá que los equipos puedan acceder a aquellos nombres que nuestro servidor DNS no pueda resolver (porque no lo conoce al no estar en nuestra red local). Para ello en DNS hacemos clic derecho en el controlador y después en Propiedades. Nos dirigimos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

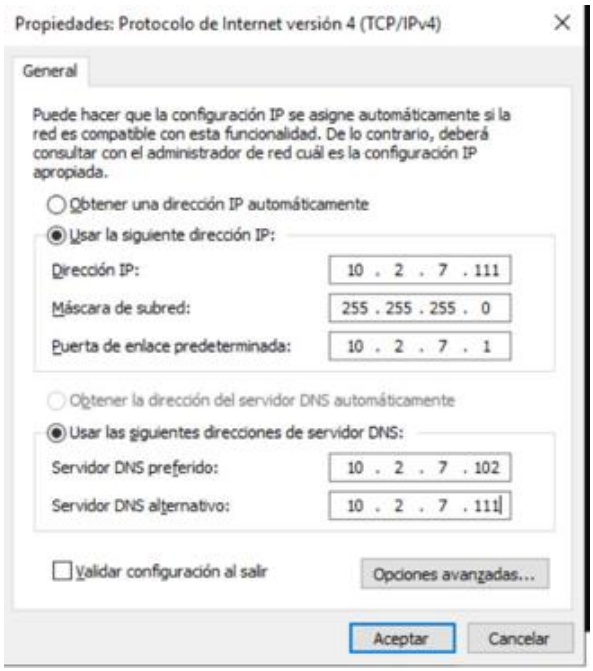


Le damos a "Editar" e introducimos la IP o nombre del servidor DNS (deben de rellenarse automáticamente los otros datos).



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.



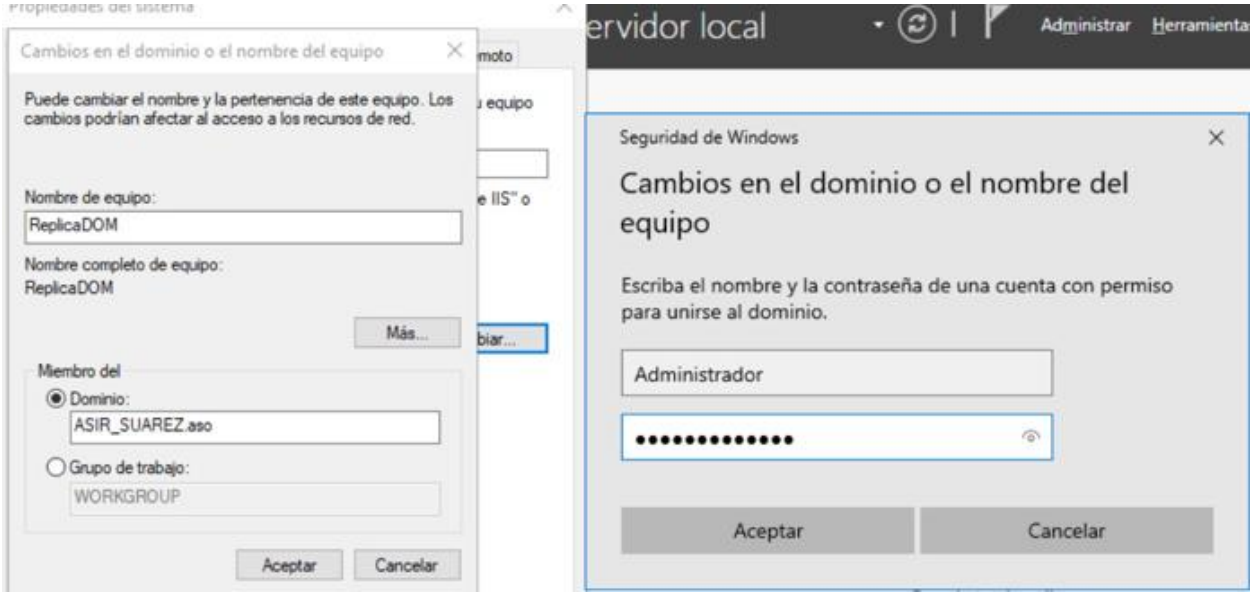


Para comprobar que funciona, podemos hacer un ping al nombre del servidor o dominio.

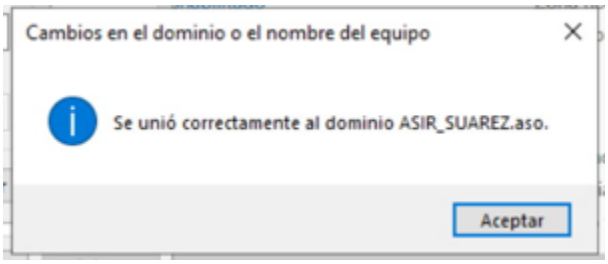
```
C:\Users\Administrador>ping CONTROLSUAREZ.ASIR_SUAREZ.aso

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**".

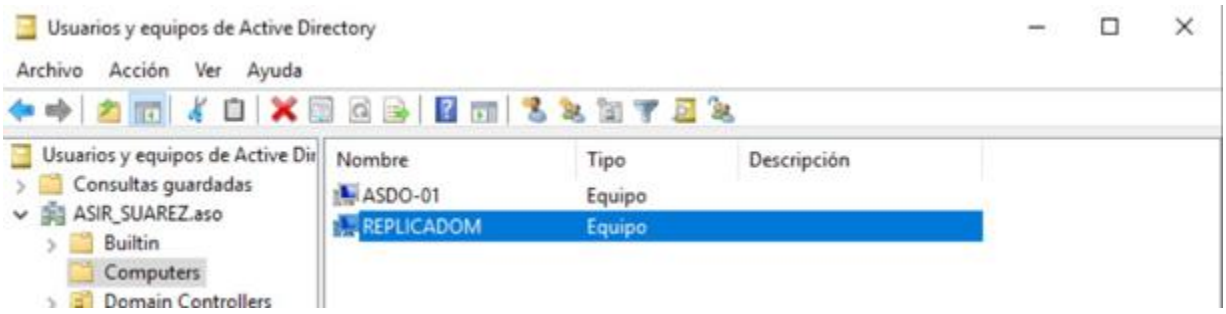
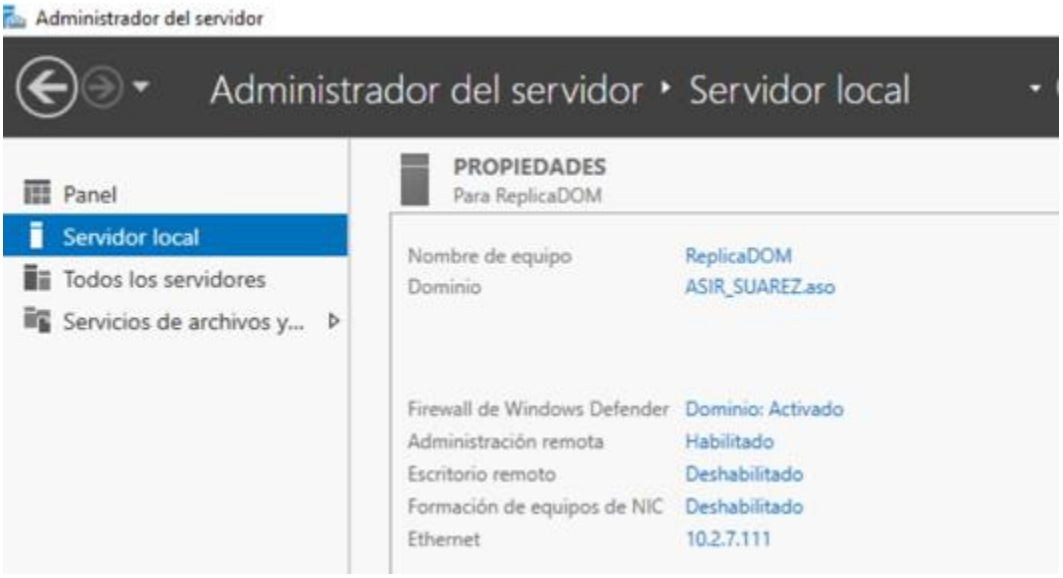
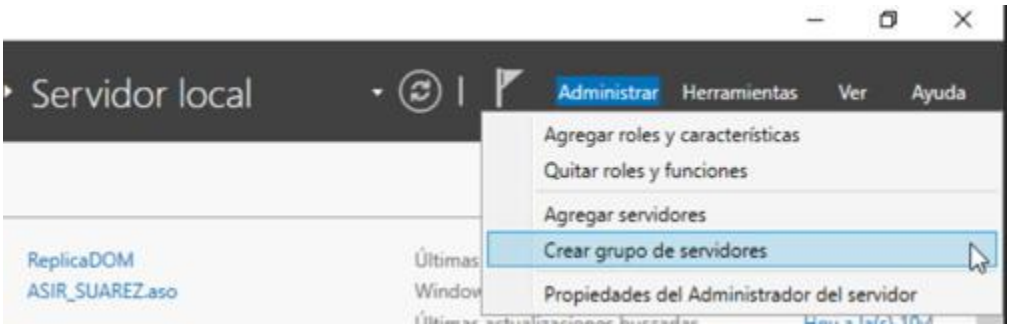


Imagen del futuro servidor Réplica después del reinicio.

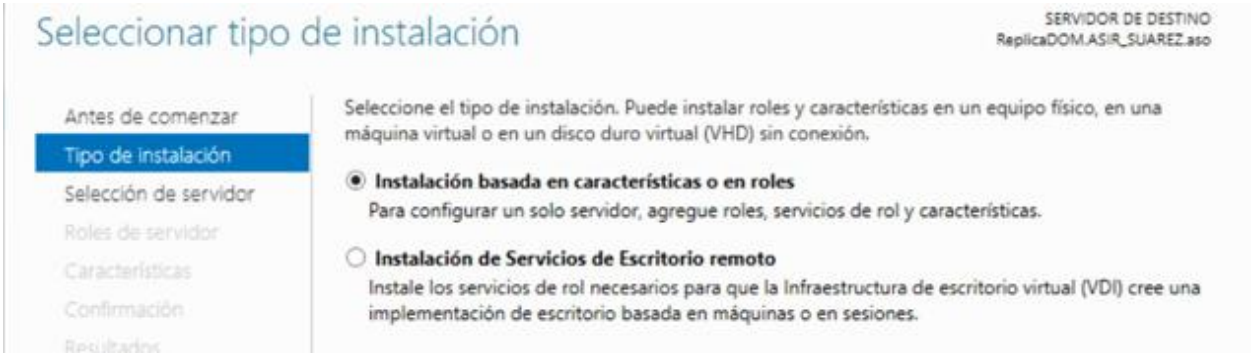


iii) **<u>Instalación de Active Directory en el futuro servidor Réplica.</u>**

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



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



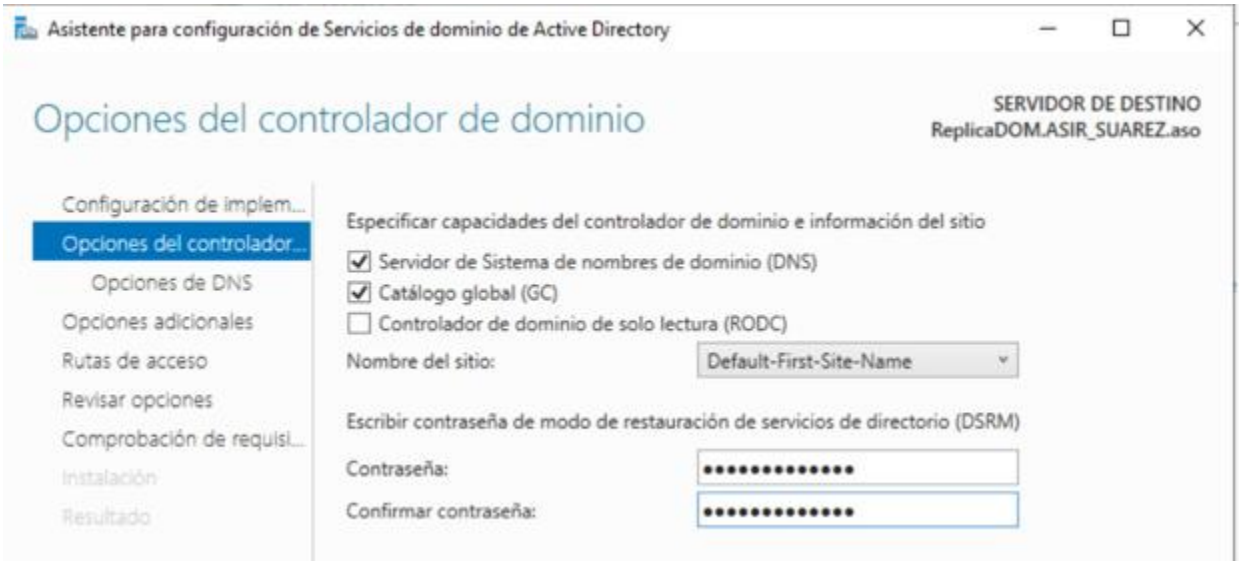
Elegimos el Servidor: En nuestro caso solo hay uno.

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:

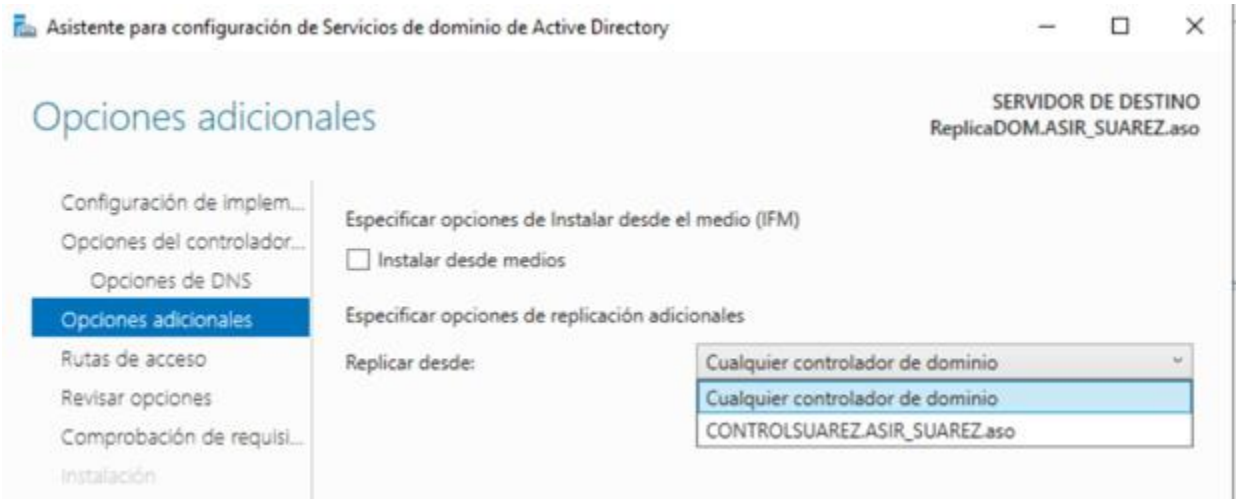
Elegimos “**Agregar un controlador de dominio a un dominio existente**”. Elegimos el dominio y ponemos las credenciales de un usuario con permisos de Administrador del Dominio.

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



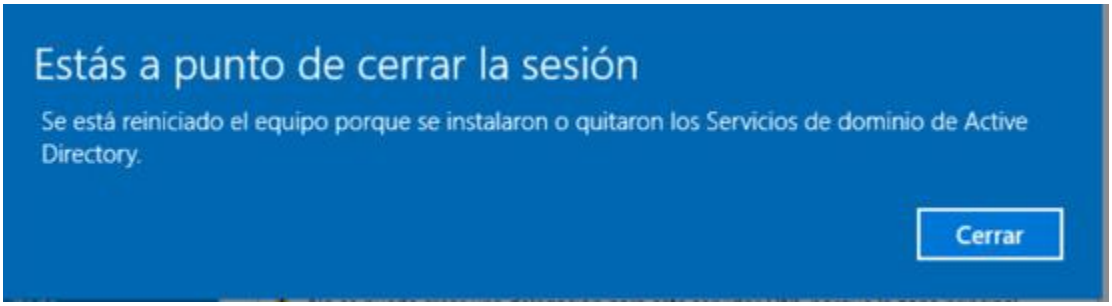
En **Opciones DNS** no podemos hacer nada.

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

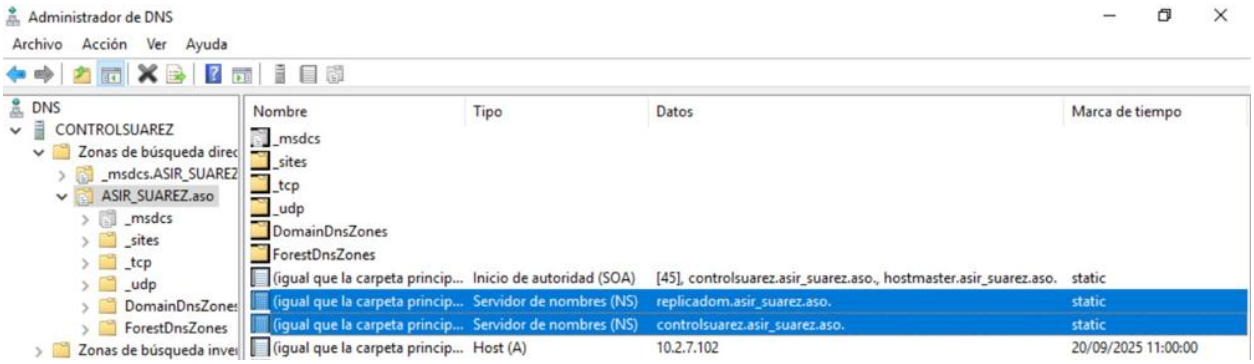


Rutas de acceso no se tocan.

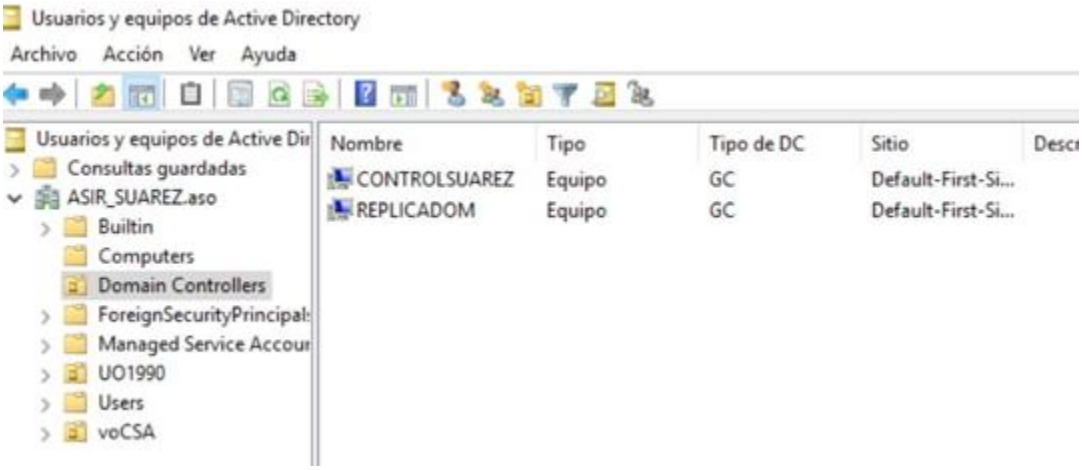
No hay que tocar nada más. Si queremos podemos guardar el Script. Una vez terminada la instalación, la máquina se reinicia.



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



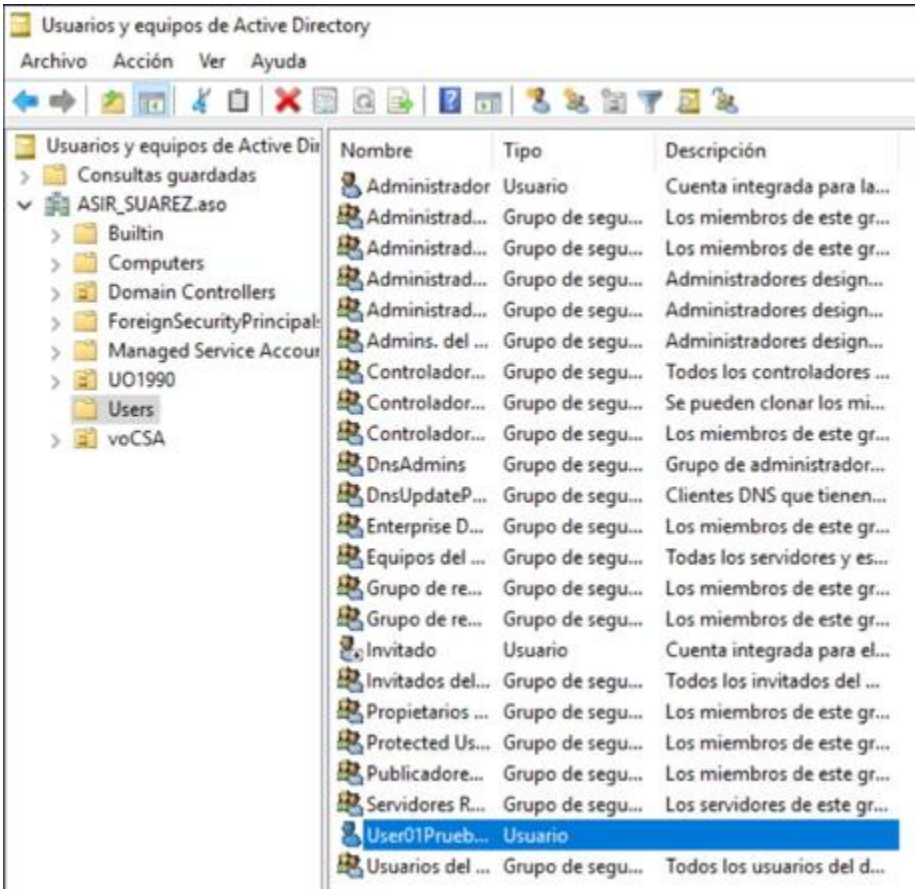
También en **Usuarios y Equipos.**



b) <u>Configura la replicación de Active Directory y comprueba su funcionamiento.</u>

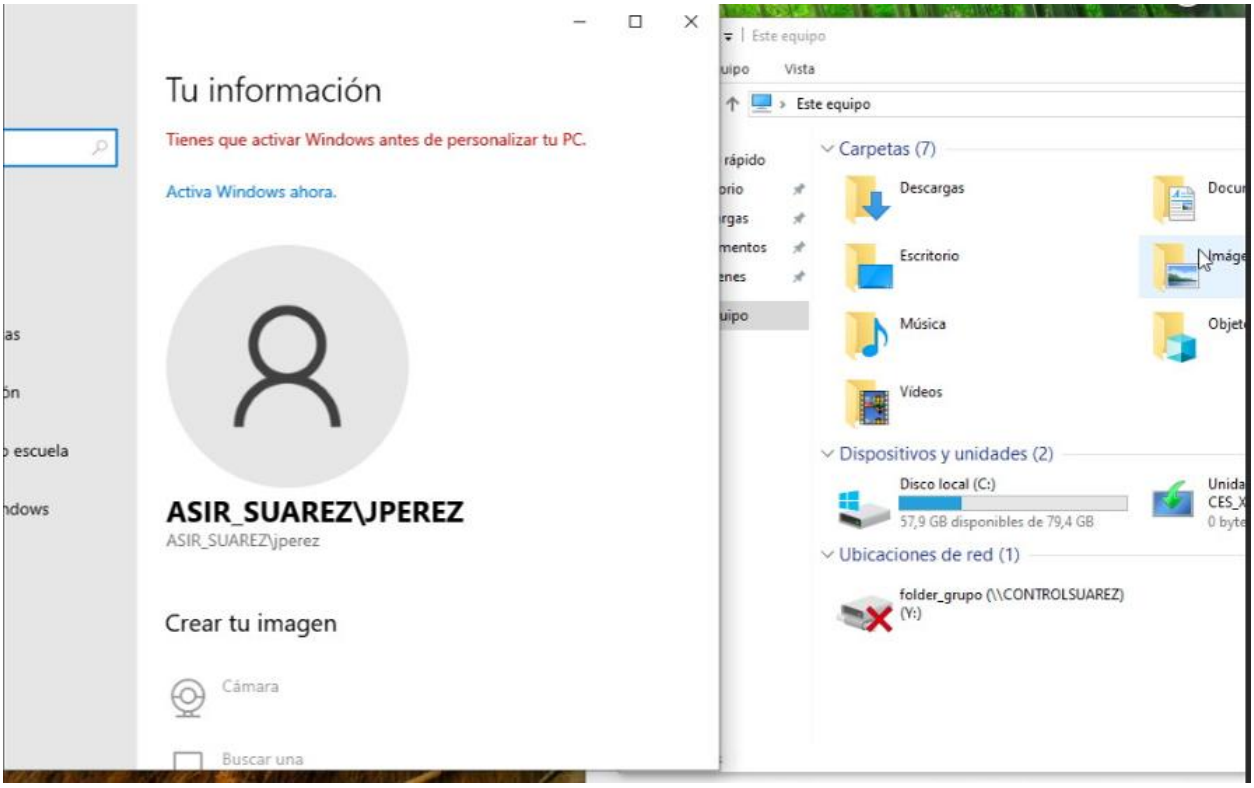
i) <u>Crea un usuario en el controlador principal y verifica que aparece en el secundario.</u>

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.

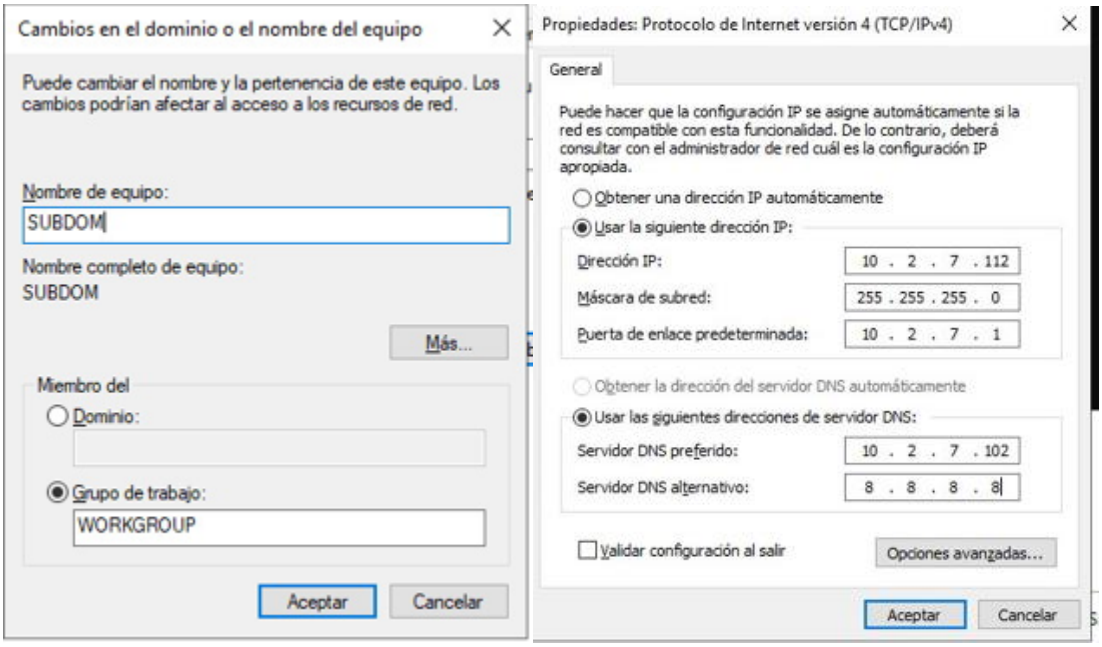


2) Subdominio.

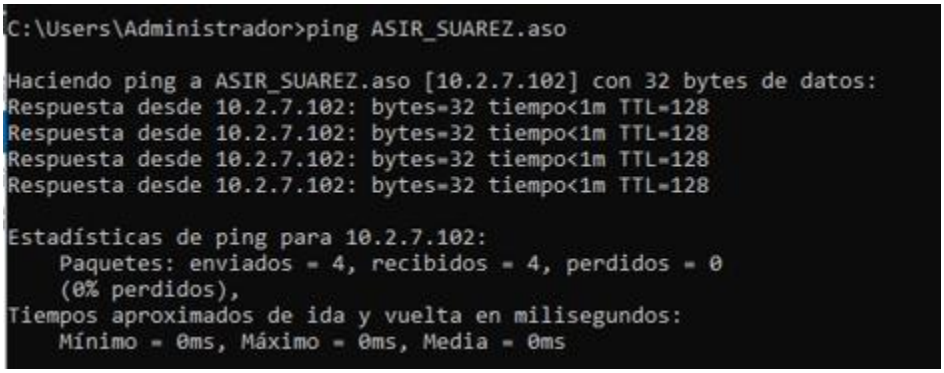
NOTA: Una vez que se ha creado una Réplica de Controlador de Dominio, a la hora de añadir un subdominio se produce un error que indica que la Réplica debe de estar encendida durante el proceso.

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

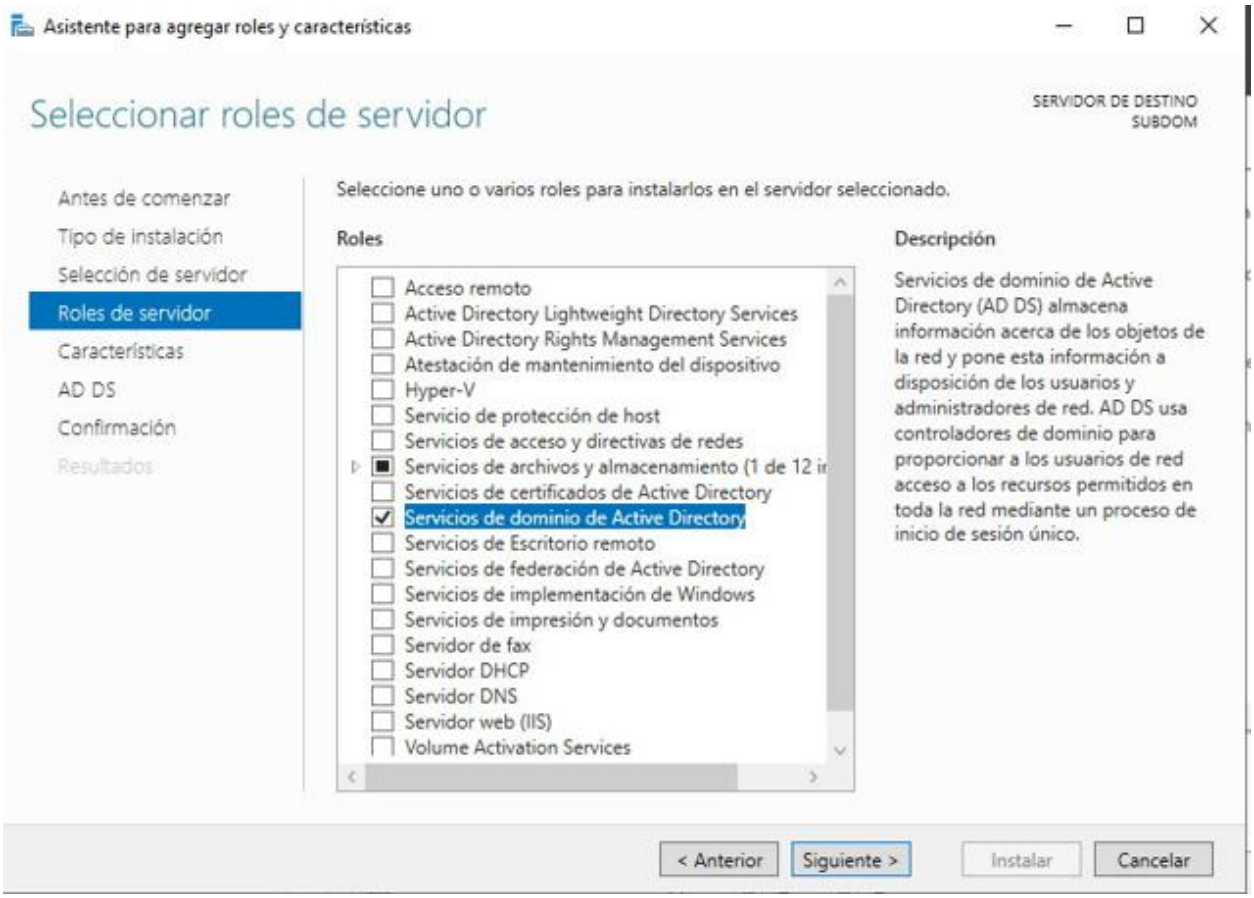
Al nuevo servidor le cambiamos el nombre (no es completamente necesario, pero si altamente recomendable). Y establecemos IP estática y como DNS la IP del Servidor de Dominio Principal.



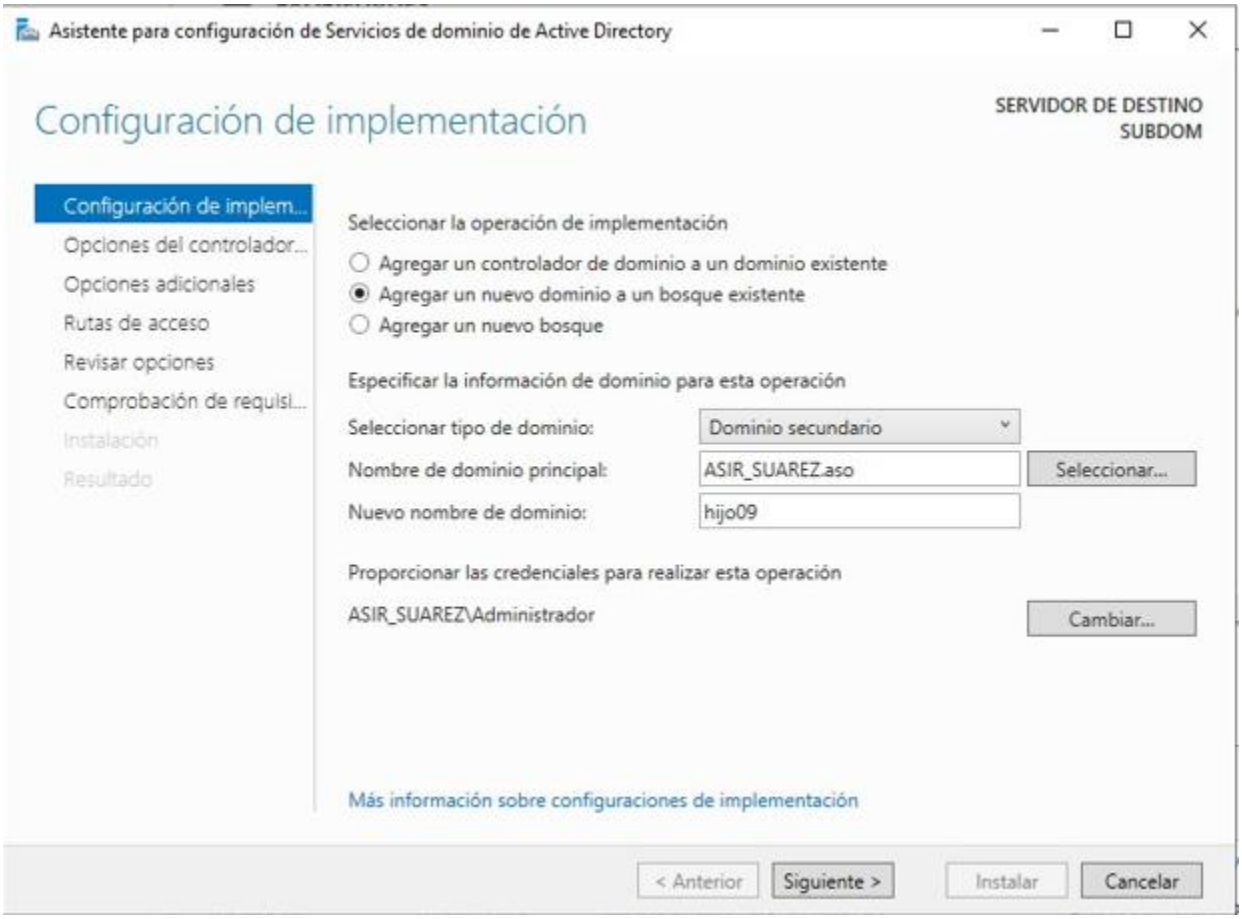
Comprobamos la conexión.



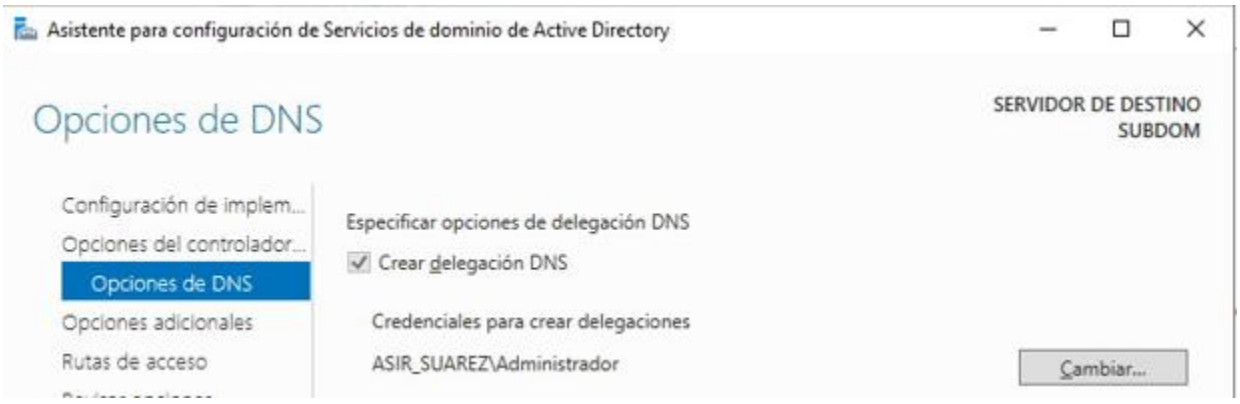
Una vez configurada, instalamos el rol de “**Servicios de Dominio de Active Directory**”.



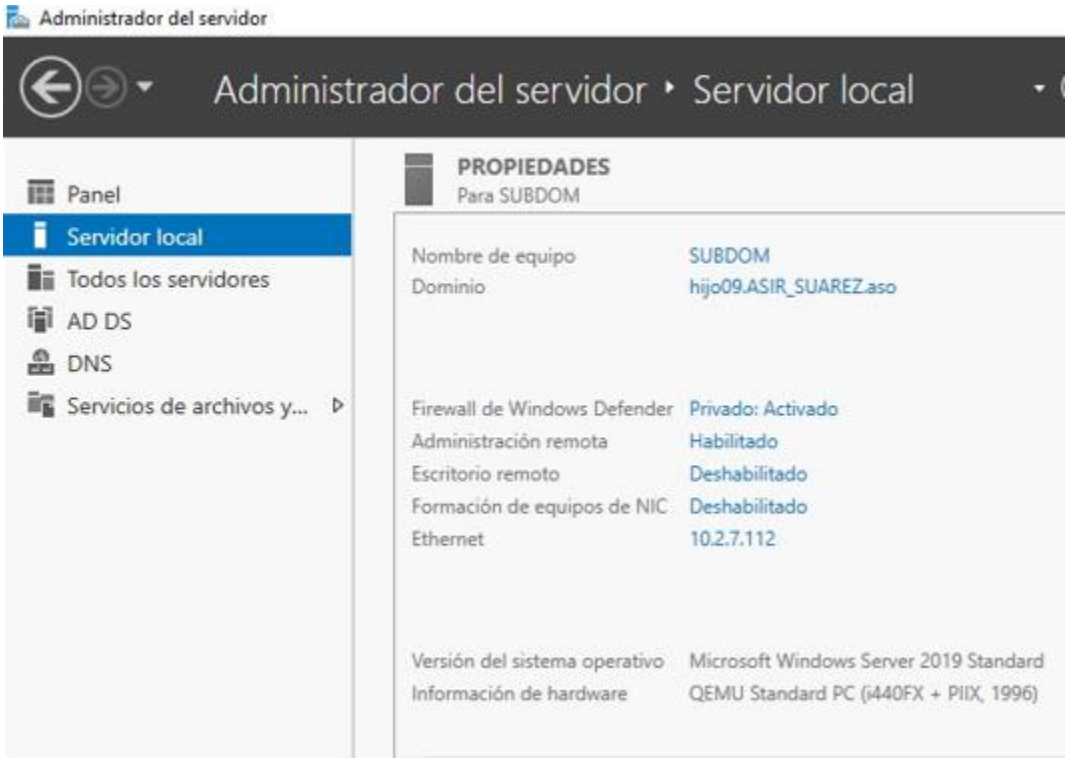
Una vez terminada la instalación, seguiremos con el siguiente asistente. Elegimos "**Agregar un nuevo dominio a un bosque existente**". Ponemos el nombre del Dominio principal y la del Subdominio. Y las credenciales de un administrador del Dominio principal.



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**".

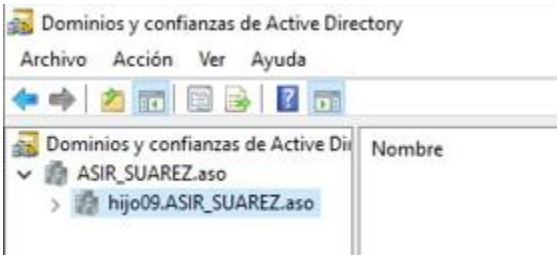


Una vez terminada la instalación se reiniciará la máquina.



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

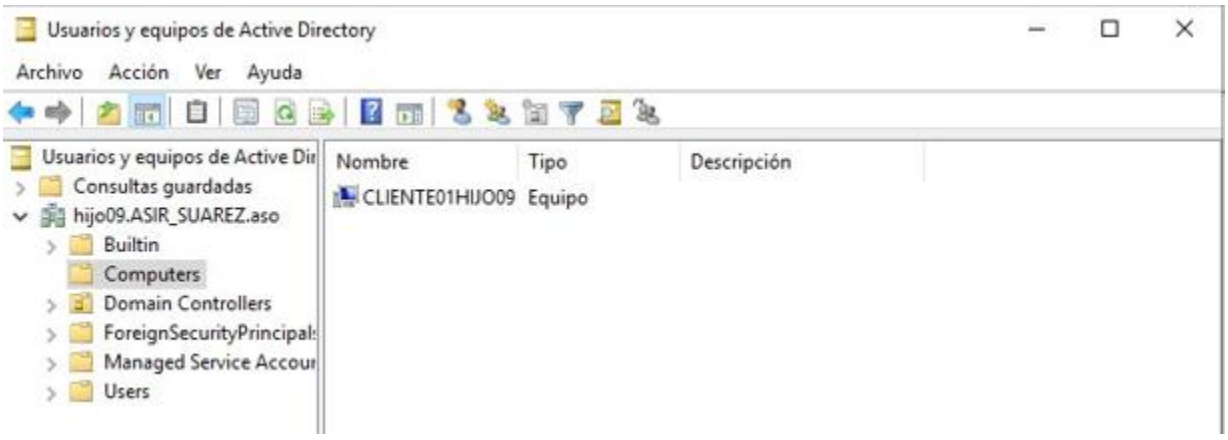
Como dijimos más arriba, cuando creamos un nuevo subdominio, de un dominio ya existente, se establece de manera implícita y automática una relación de confianza bidireccional y transitiva entre el nuevo dominio y su dominio padre.

[2]

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

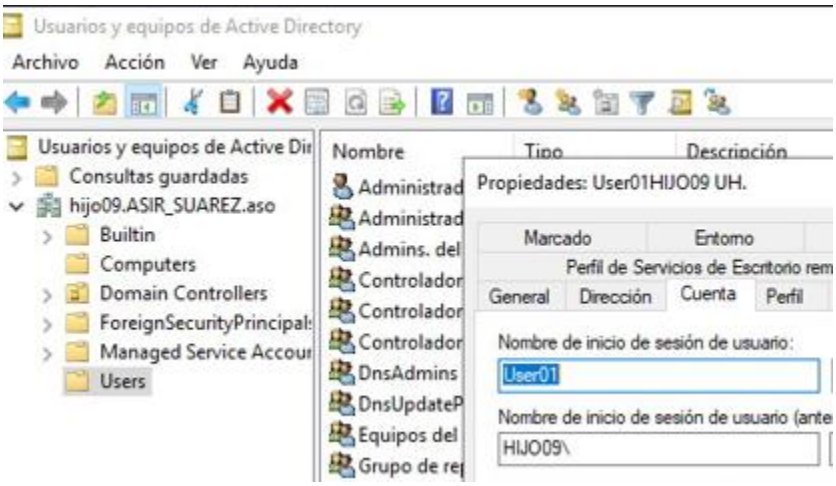
Para esto vamos a crear un Cliente y Usuarios en el Subdominio.

Cliente unido.

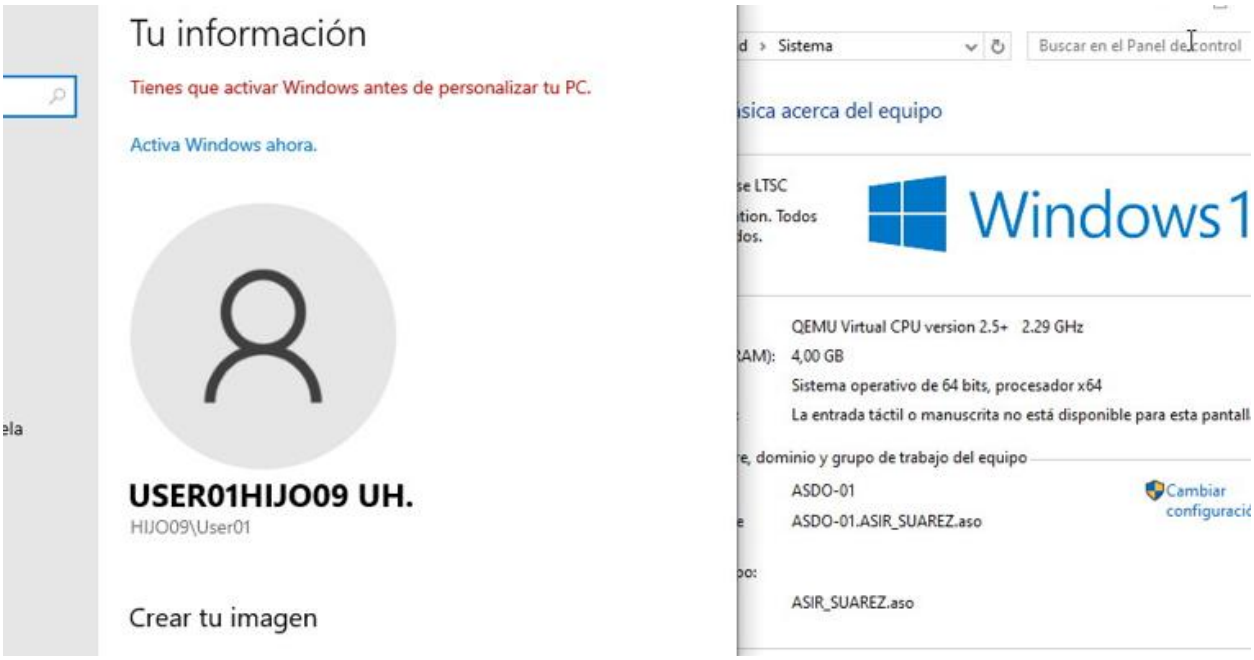


[2] https://somebooks.es/capitulo-7-relaciones-entre-dominios/4/

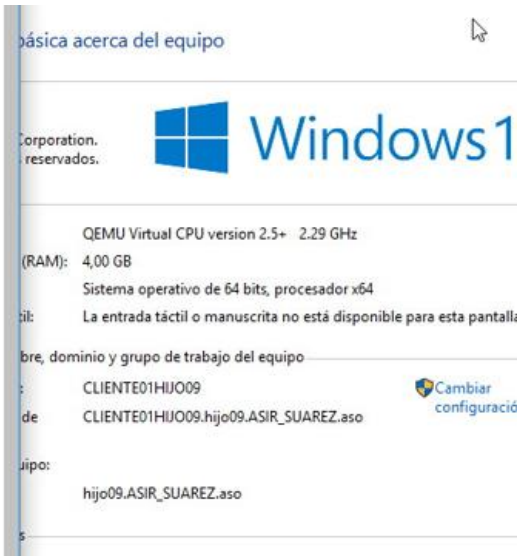
Usuario creado.



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.

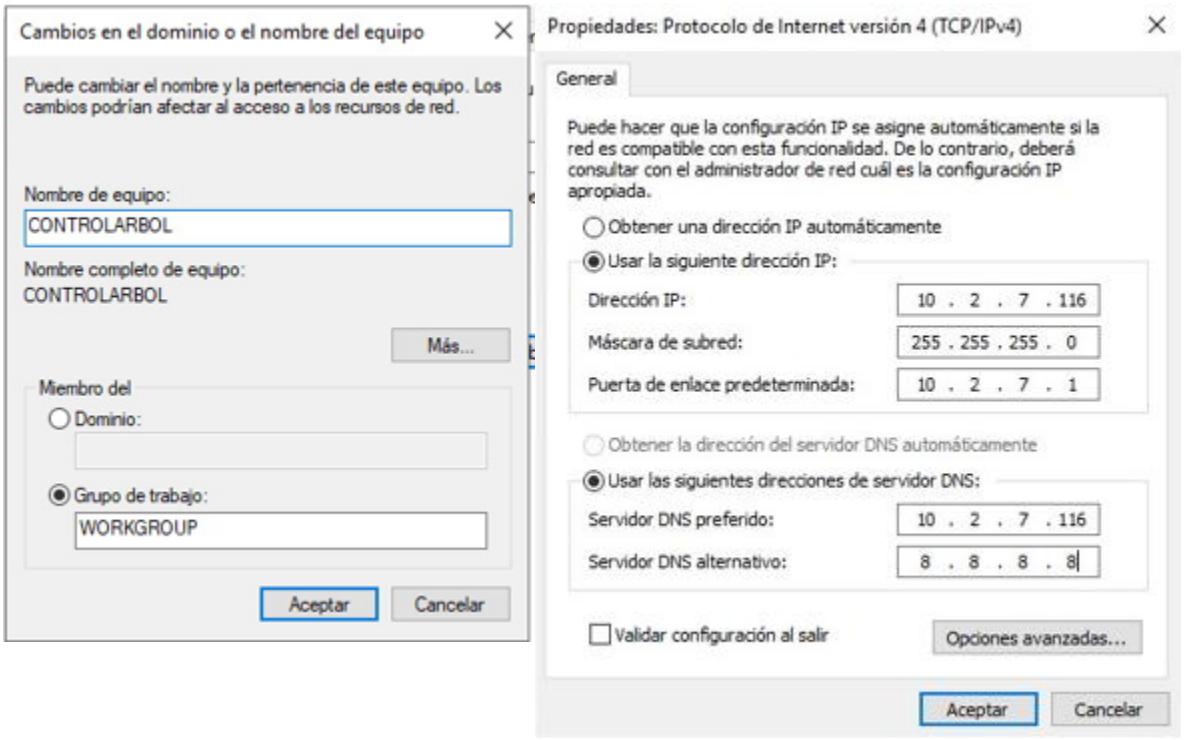


3) Bosque.

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.

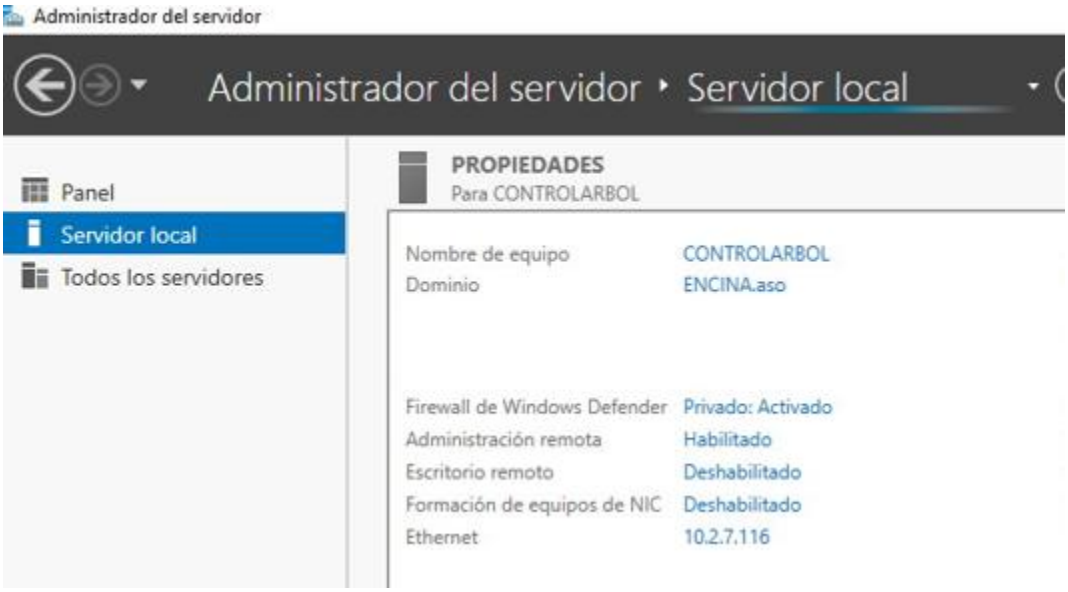


Instalamos “Servicios de Dominio”.

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

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

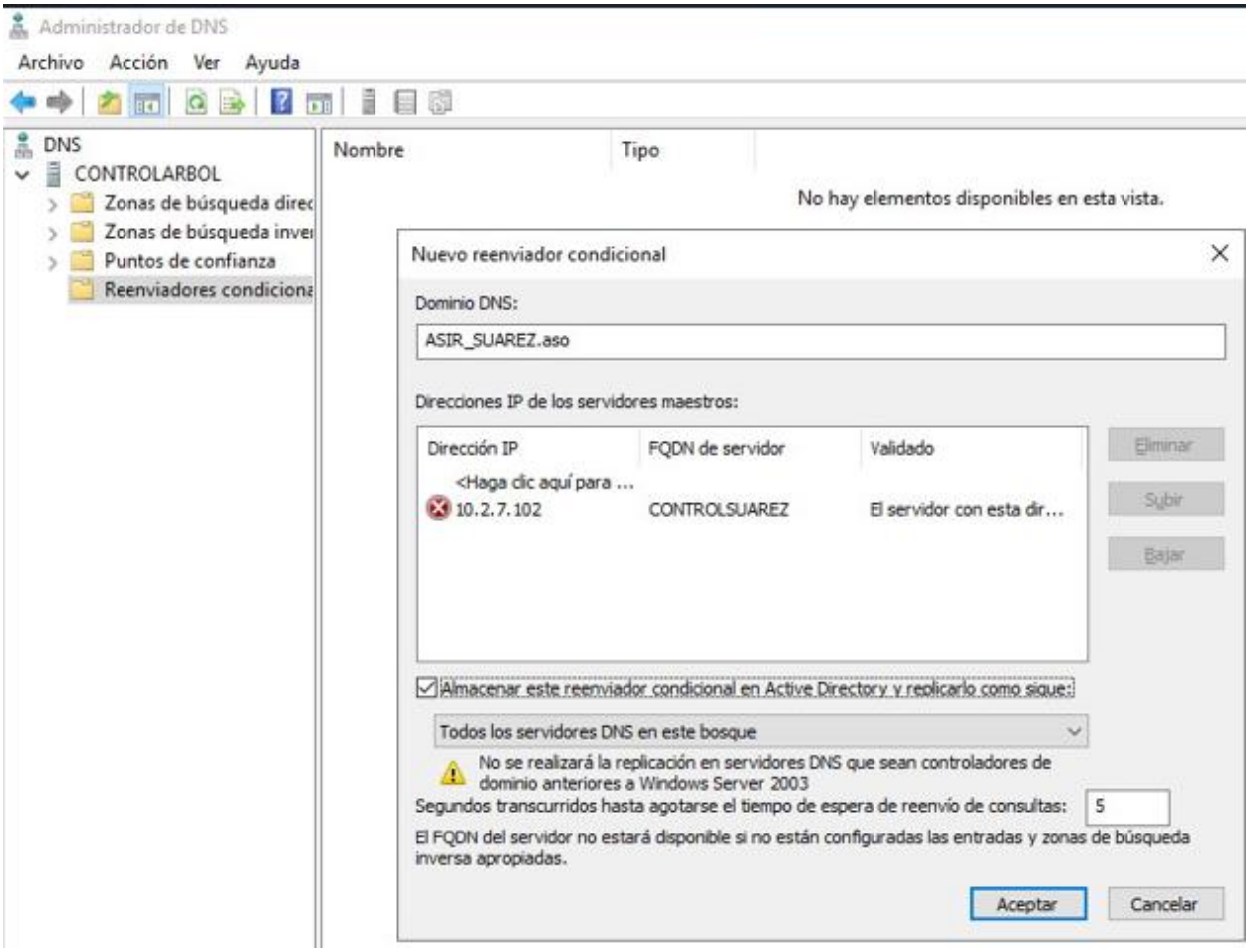
Una vez reiniciada la máquina, podemos ver que se ha creado el dominio.



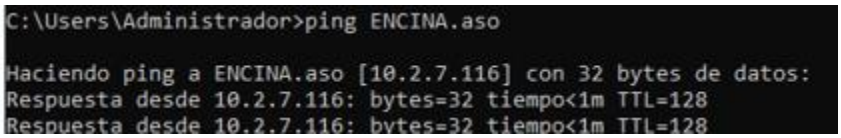
b) Establece una relación de confianza bidireccional y transitiva entre ambos bosques.

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

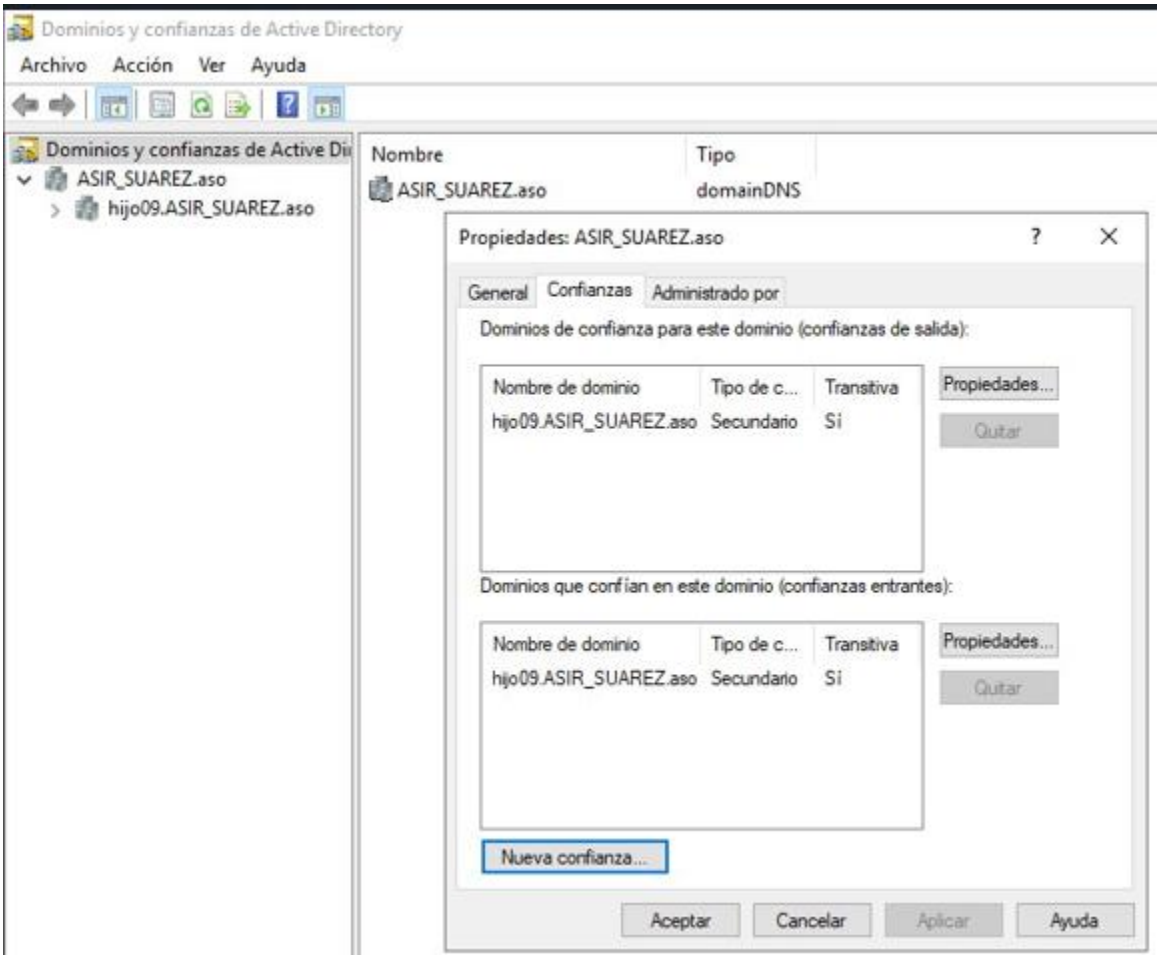
DNS → Reenviadores condicionales: Nuevo. E introducimos la IP del otro servidor. **Se debe hacer en ambos, poniendo la IP del otro.**



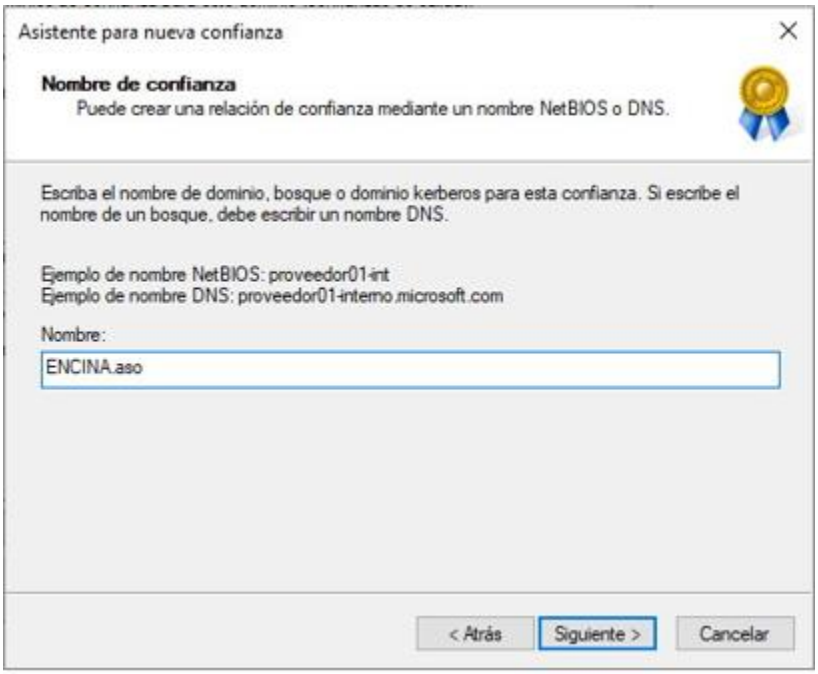
Para comprobar que funciona se hace ping:



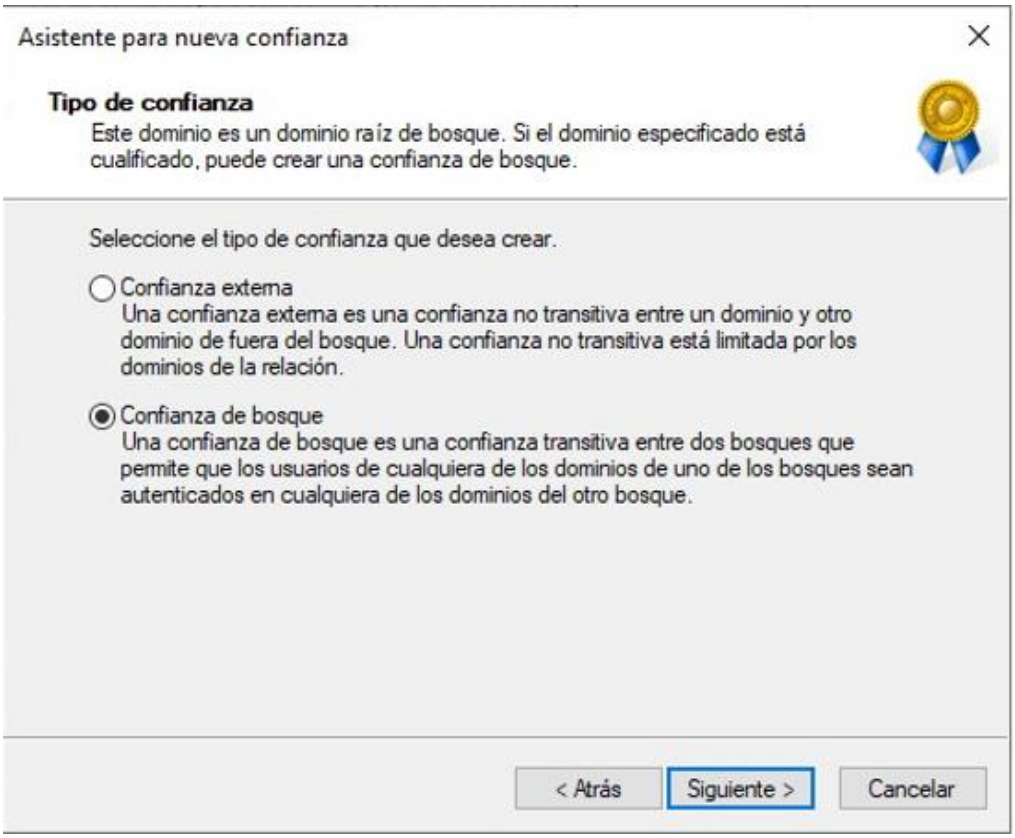
El siguiente paso es establecer la **relación de confianza**. Para ello: **Herramientas → Dominios y confianzas de Active Directory**. Y vamos a propiedades del dominio y luego a la pestaña **Confianzas** y ahí en **Nueva Confianza**. Hay que tener en cuenta que solo hace falta establecerlo en uno de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



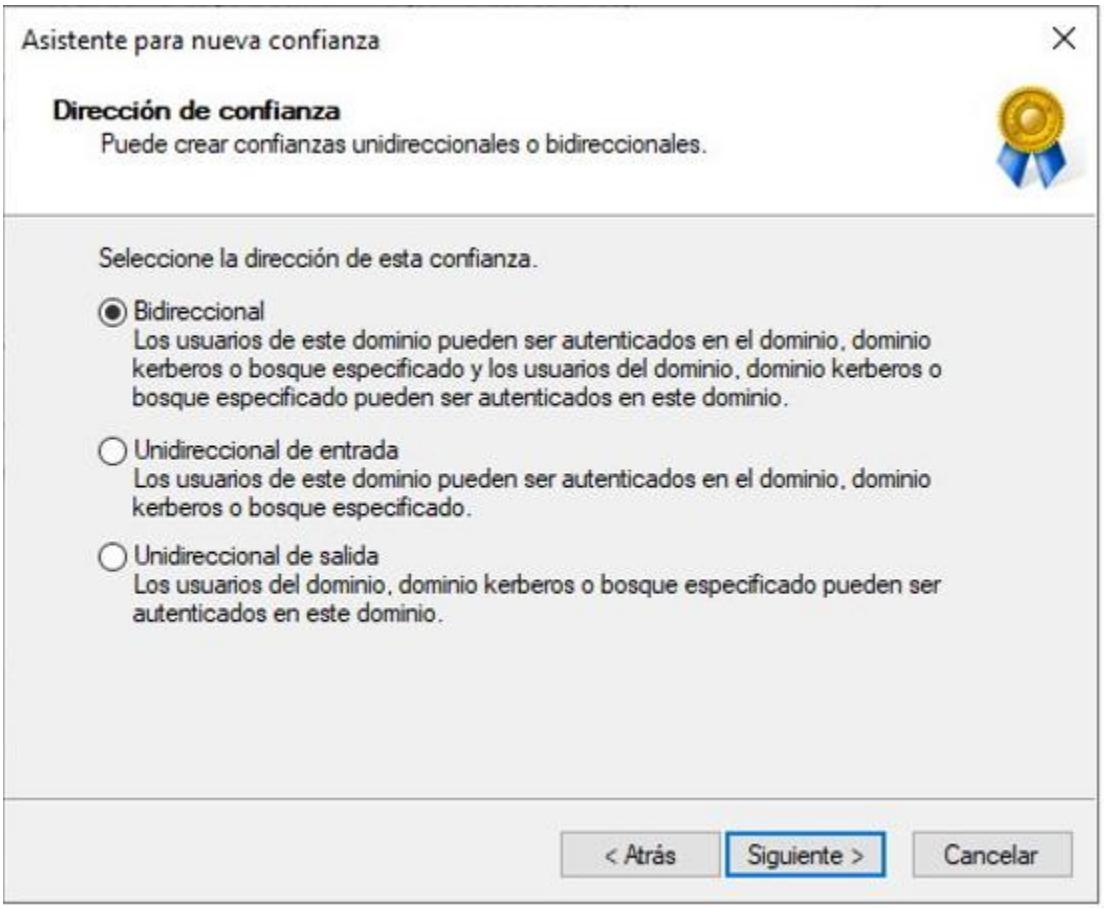
El nombre del dominio con el que queremos establecer la relación.



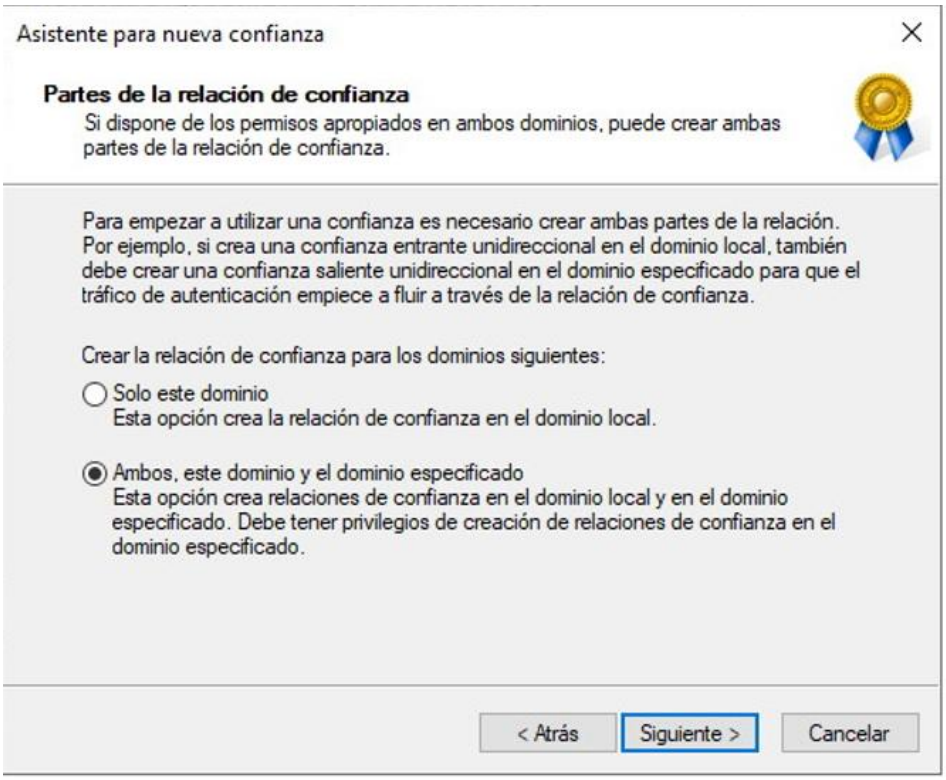
Tipo de Confianza: de Bosque.



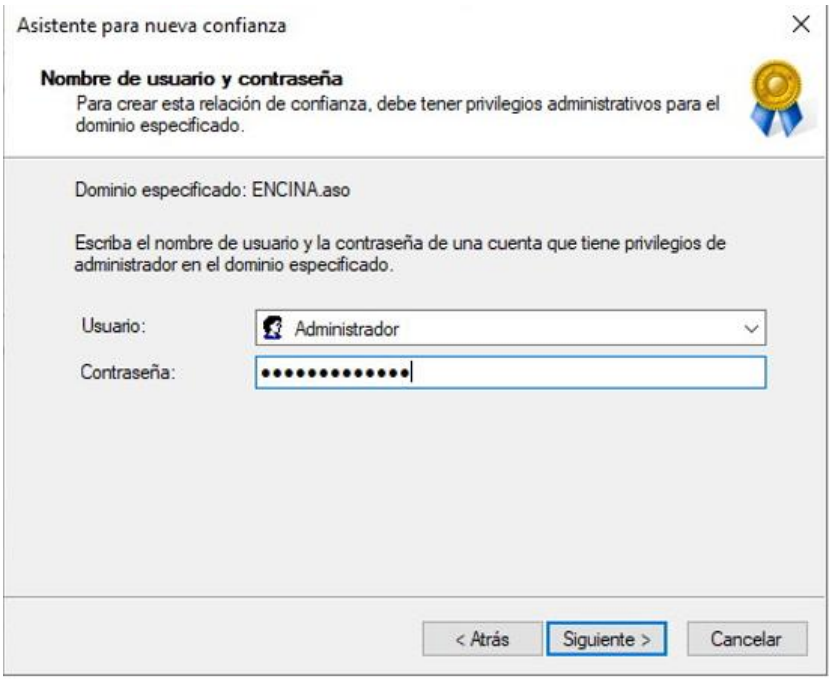
Dirección de confianza: Bidireccional.



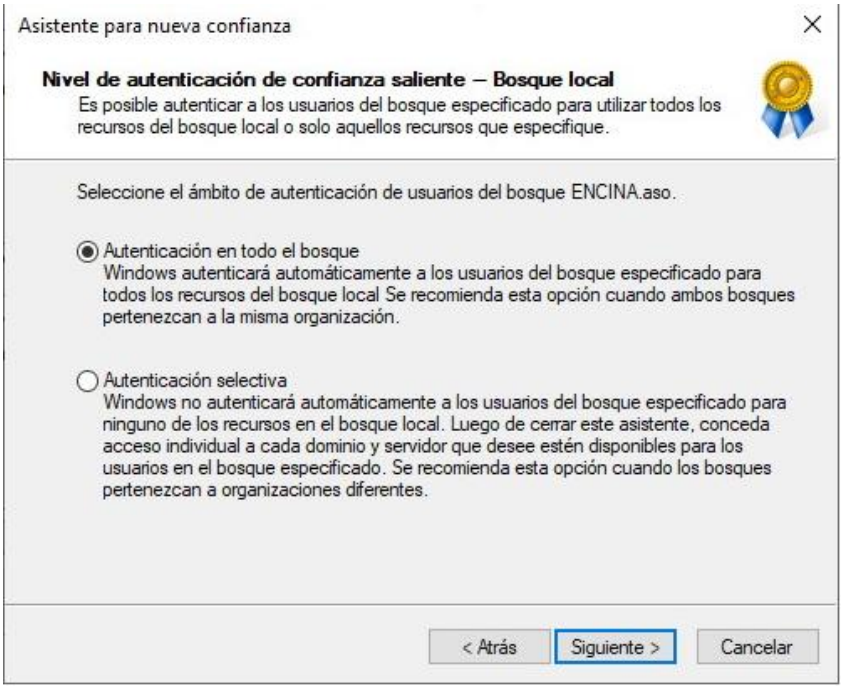
Partes de la relación de confianza: Ambos.



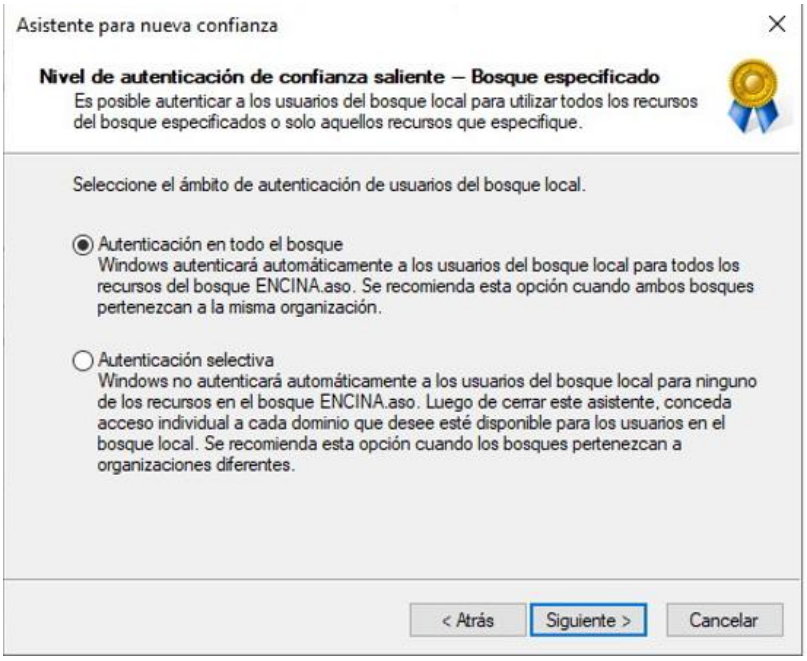
Acreditación de usuario administrador del otro Dominio.



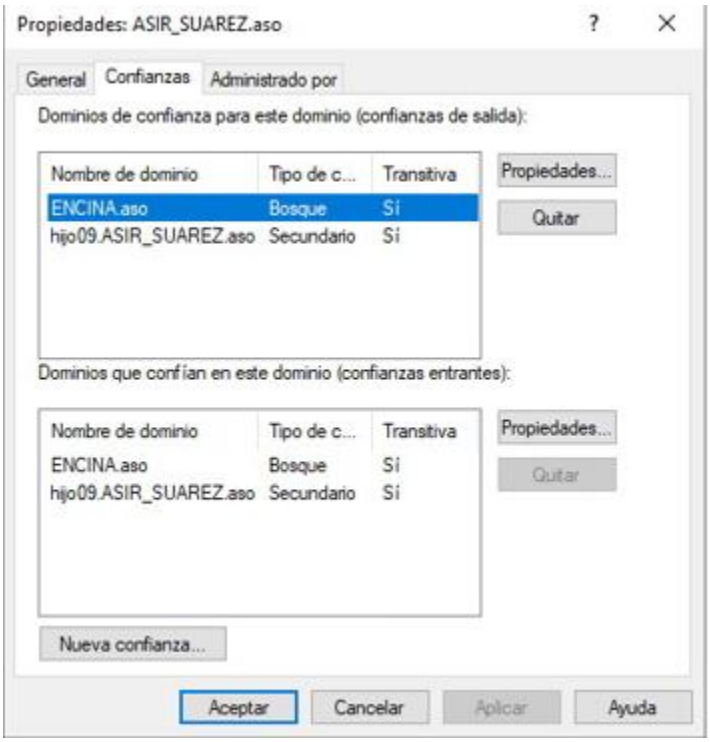
Nivel de autenticación de confianza saliente – Bosque local: **Autenticación en todo el bosque.**



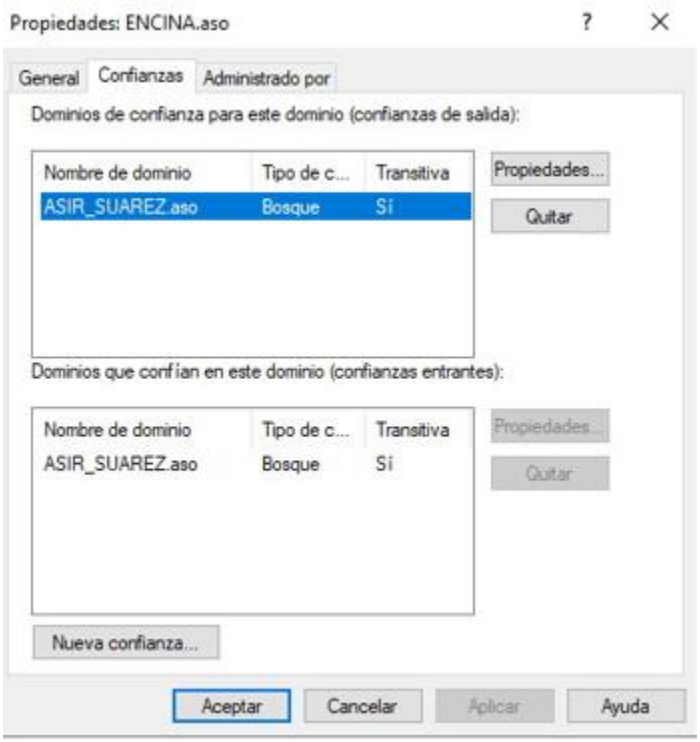
Nivel de autenticación de confianza saliente – Bosque especificado: **Autenticación en todo el bosque**.



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

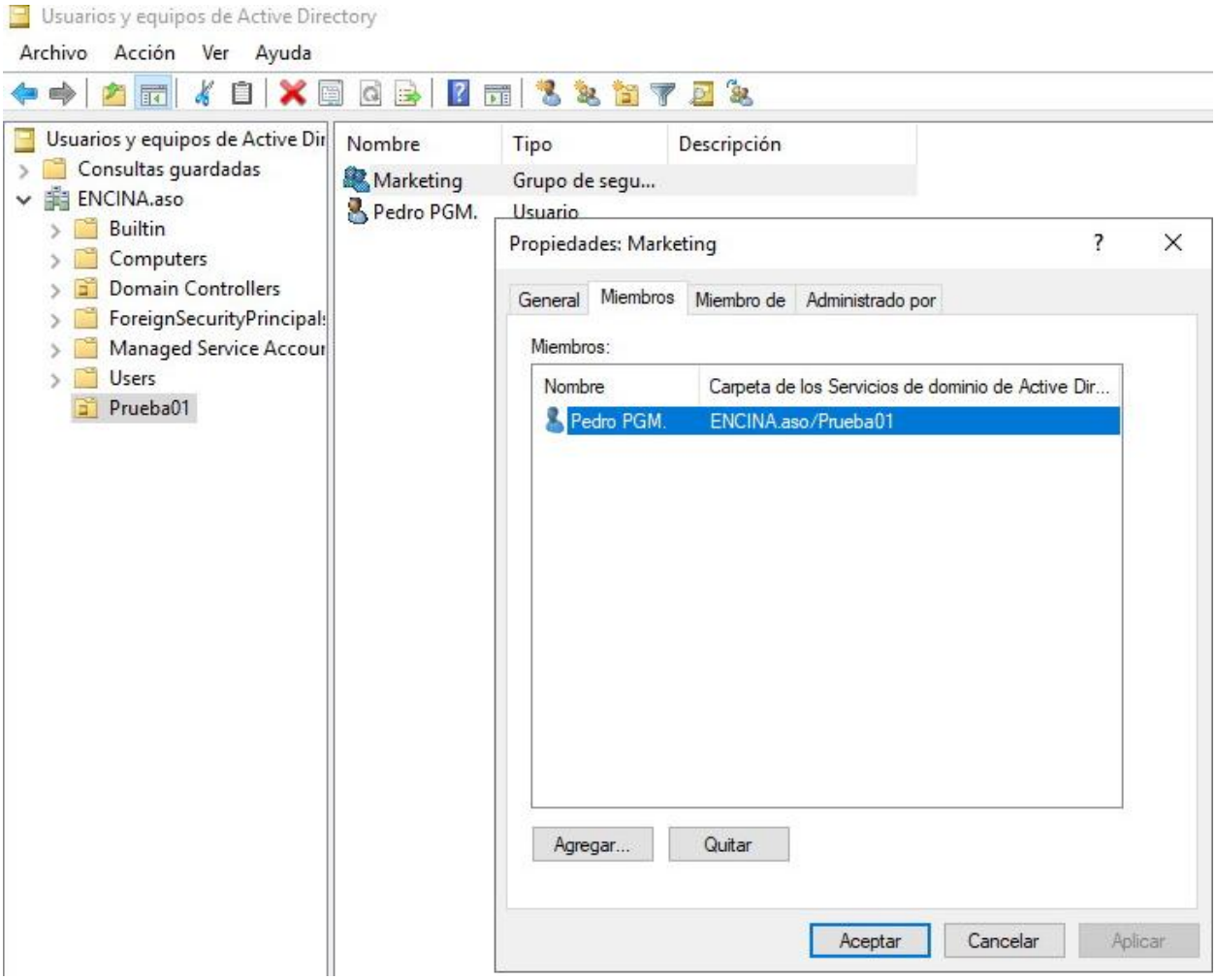


En el otro dominio se crea automáticamente.

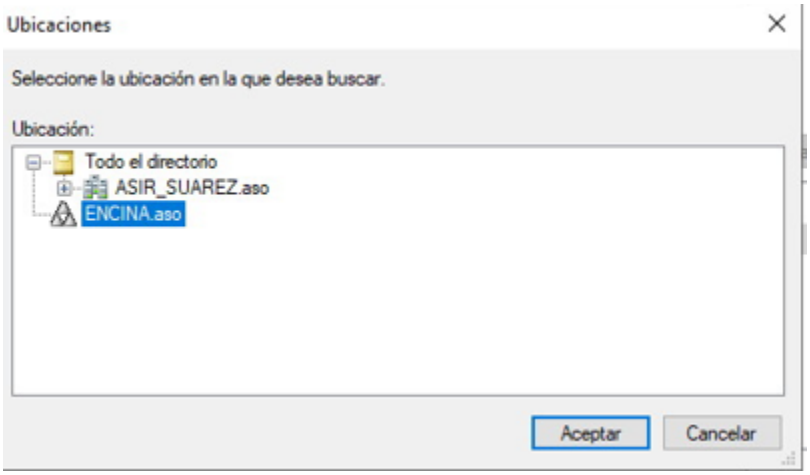


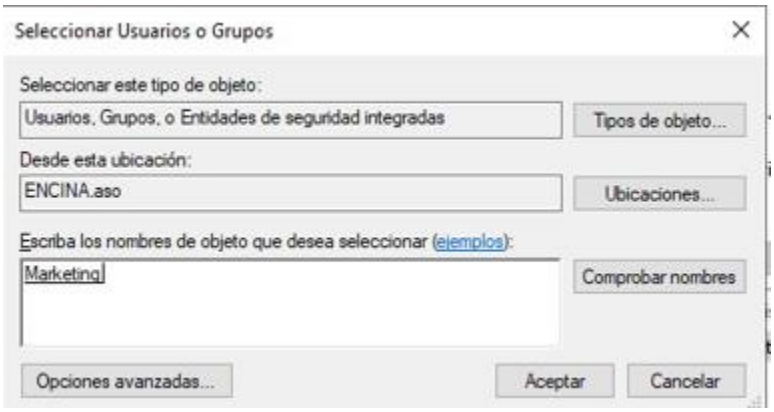
c) Comprueba la autenticación cruzada creando usuarios en ambos bosques y validando el acceso a recursos compartidos.

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

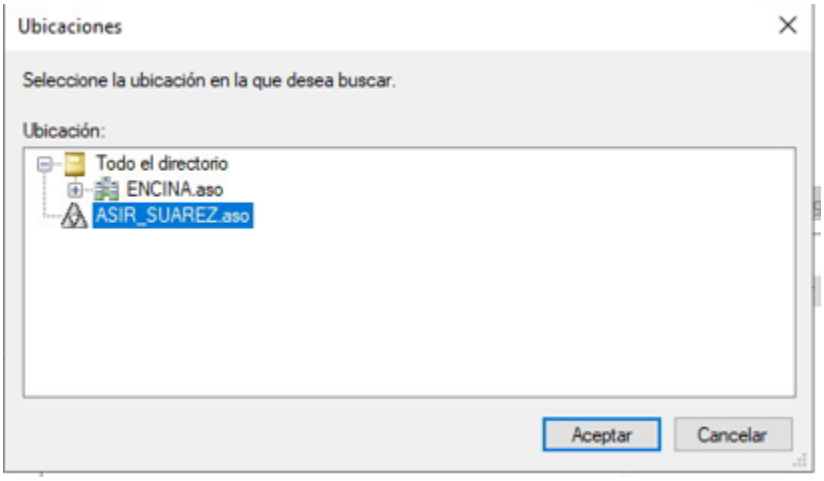


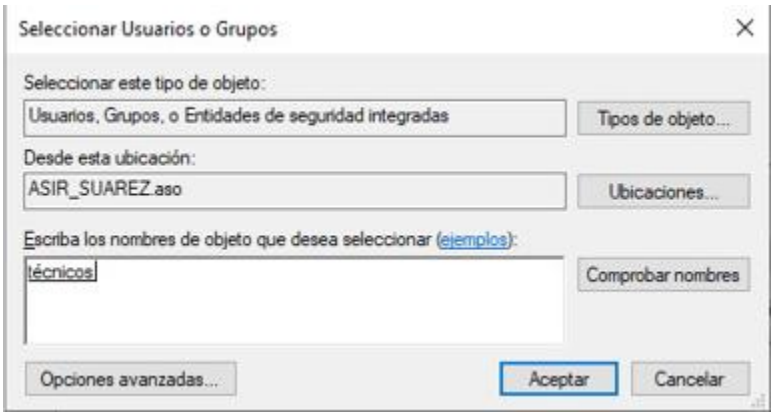
Luego en **ASIR_SUAREZ.aso** hemos creado una carpeta compartida para el grupo **Marketing**, perteneciente al dominio **ENCINA.aso**

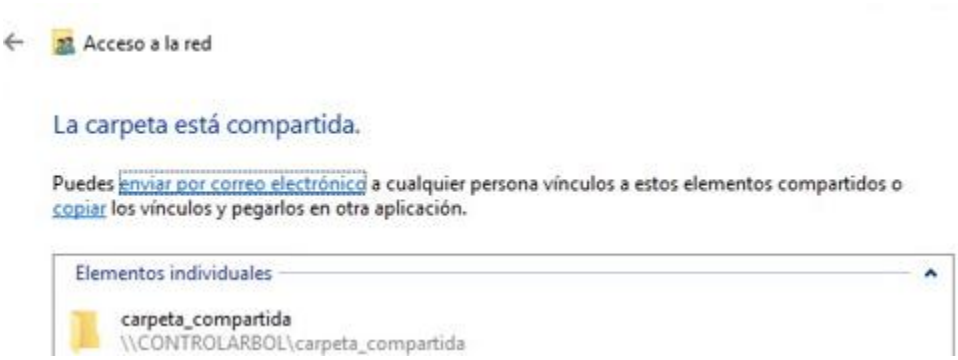




Luego hicimos lo mismo en el Controlador de **Encina.aso** para el grupo **técnicos** de **ASIR_SUAREZ.aso**

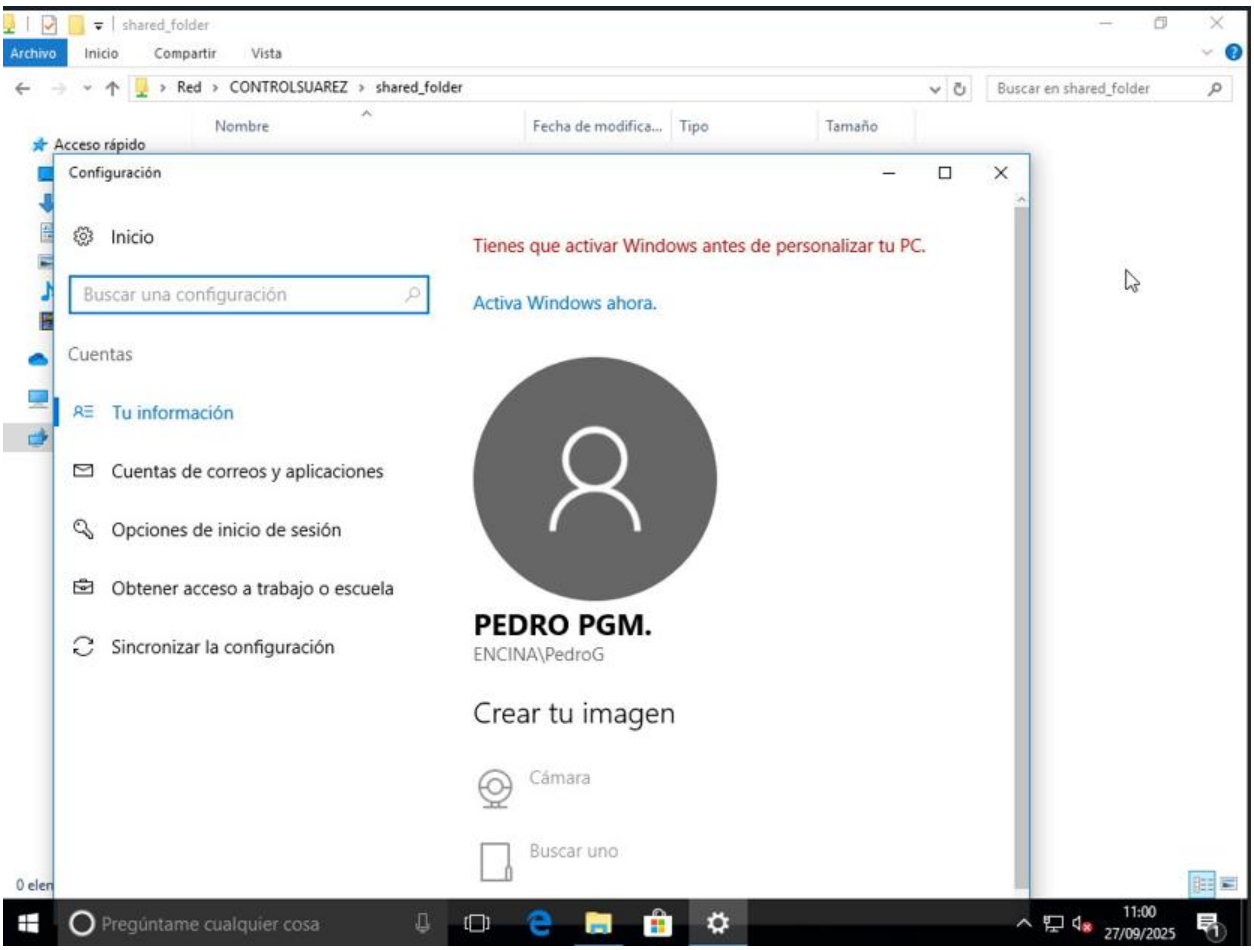




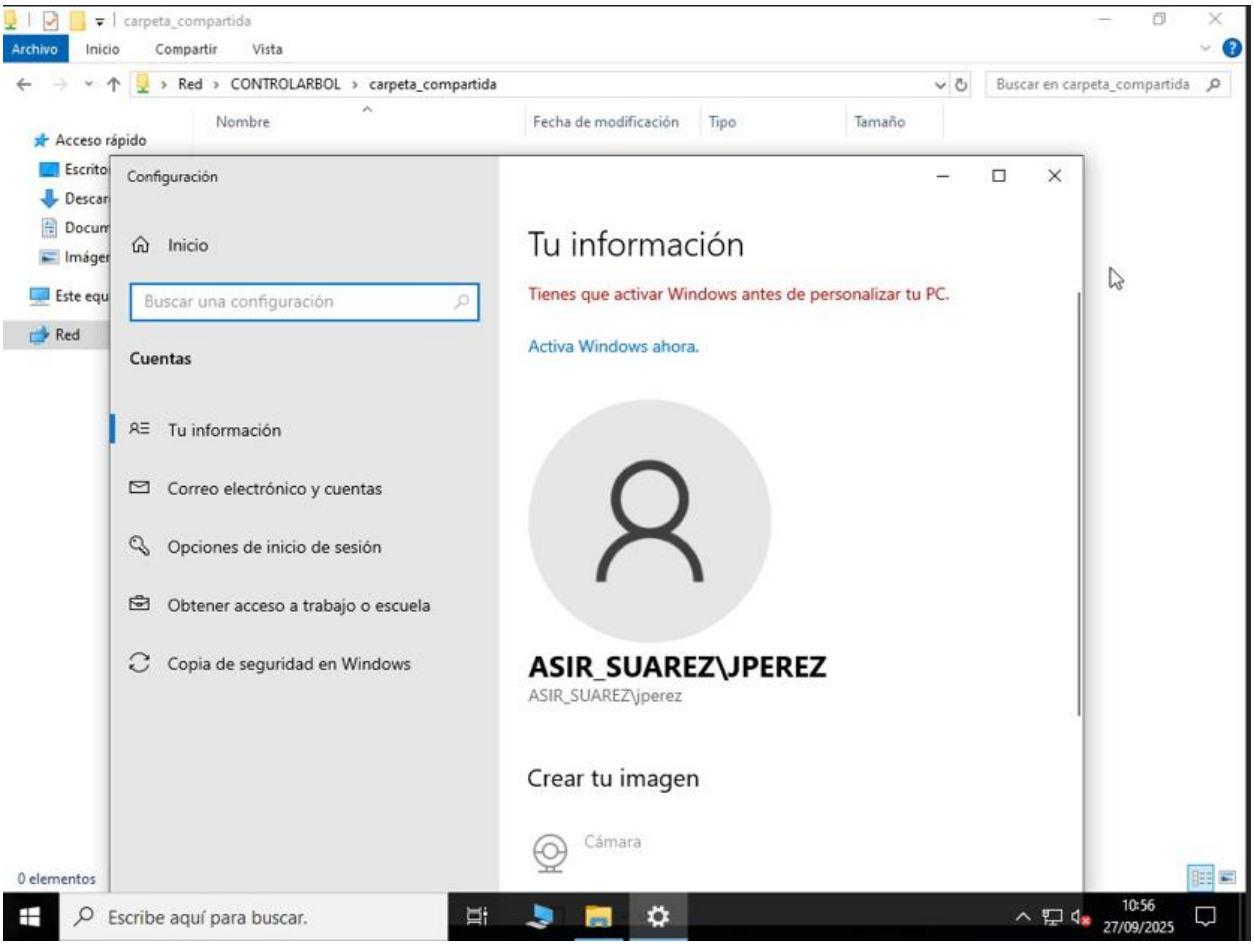


d) Para comprobar que funciona, intenta acceder a recursos compartidos entre dominios con diferentes usuarios.

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



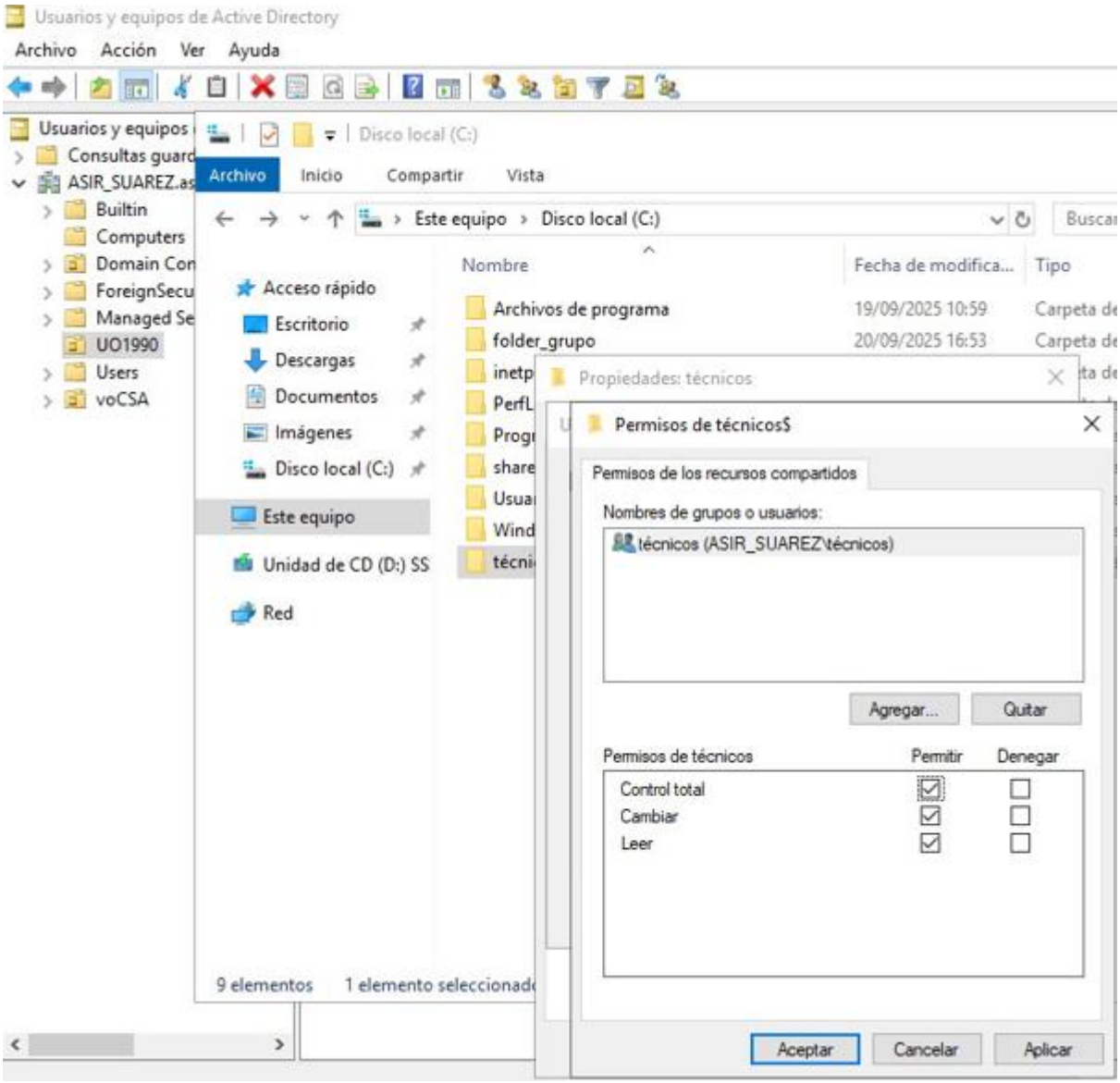
Y al usuario **jperez** de **ASIR_SUAREZ.aso** acceder al que está en **ENCINA.aso**



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 pertenece a un grupo que tenga control total en la carpeta donde se van a establecer los perfiles móviles).

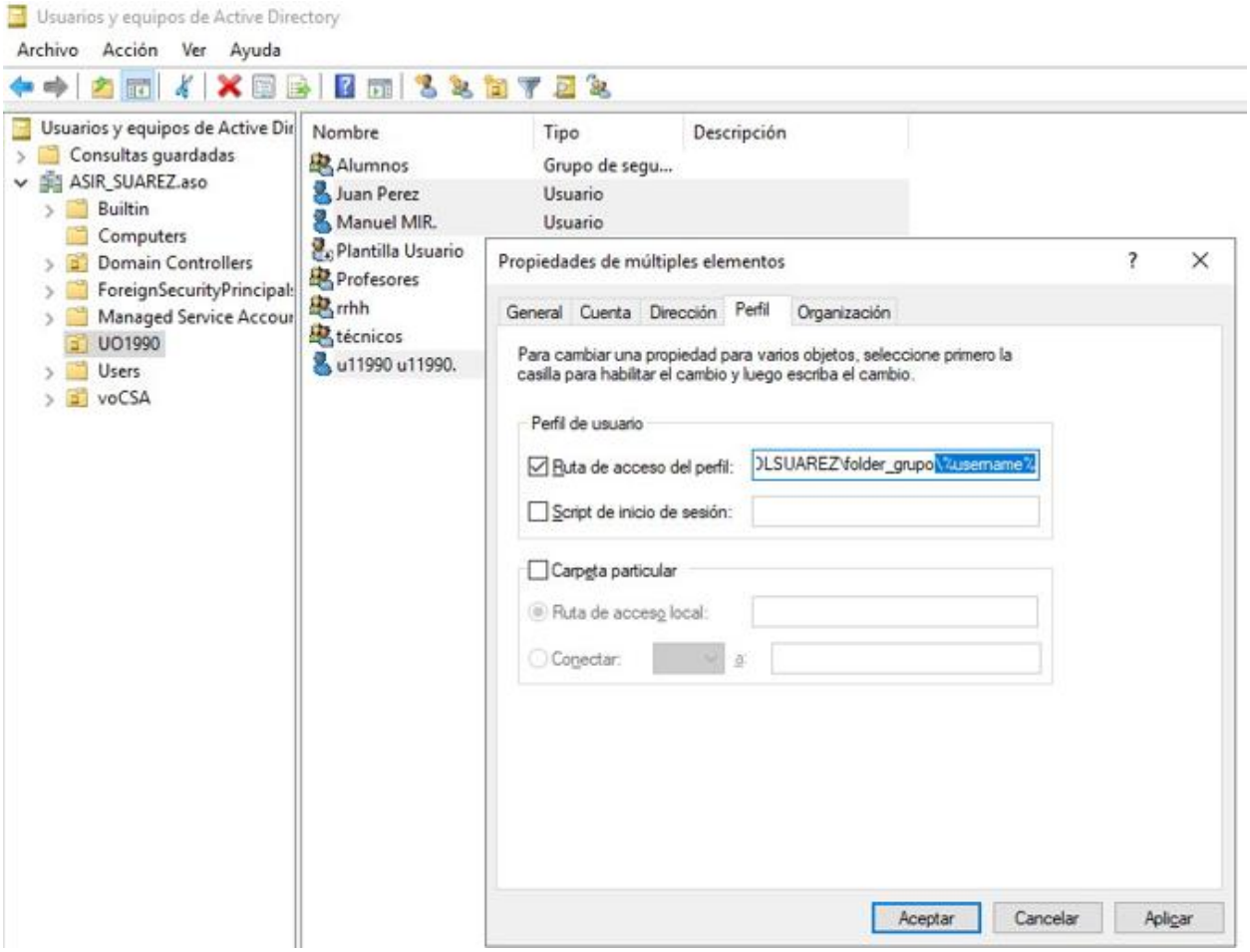


b) Modifica las propiedades de varios usuarios en Active Directory Users and Computers para que usen perfiles móviles.

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:

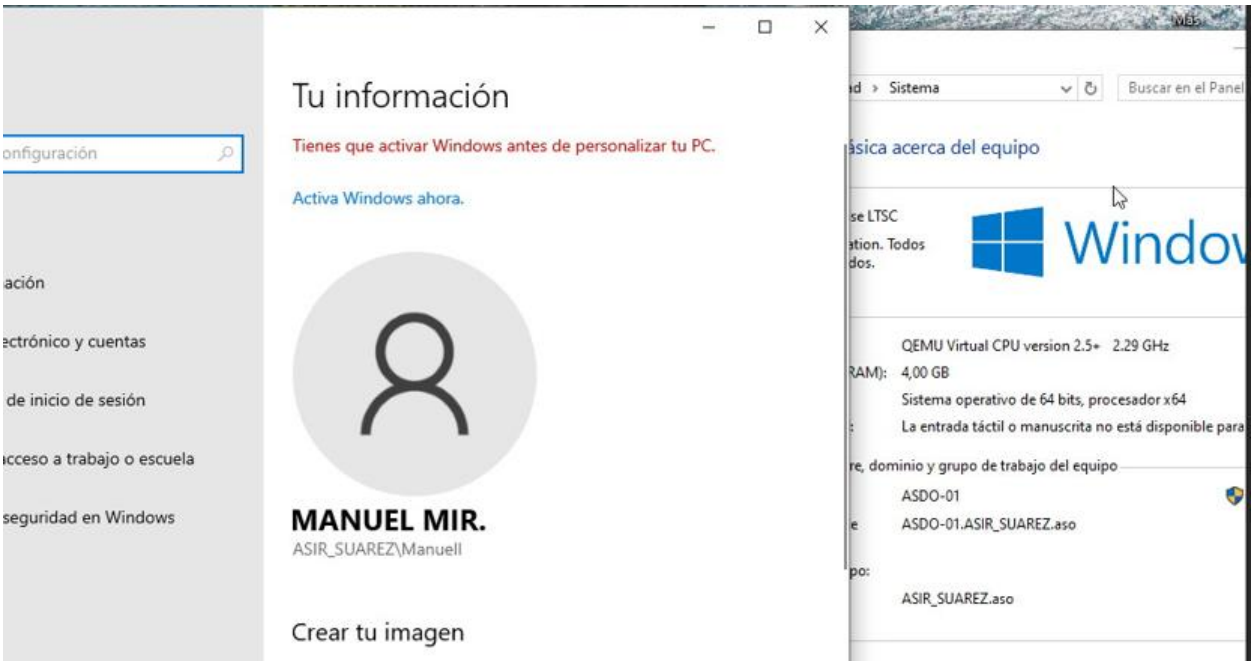
\\Nombre_del_servidor\ruta\%username%

Esto generará una carpeta para cada usuario cuando inicien sesión.

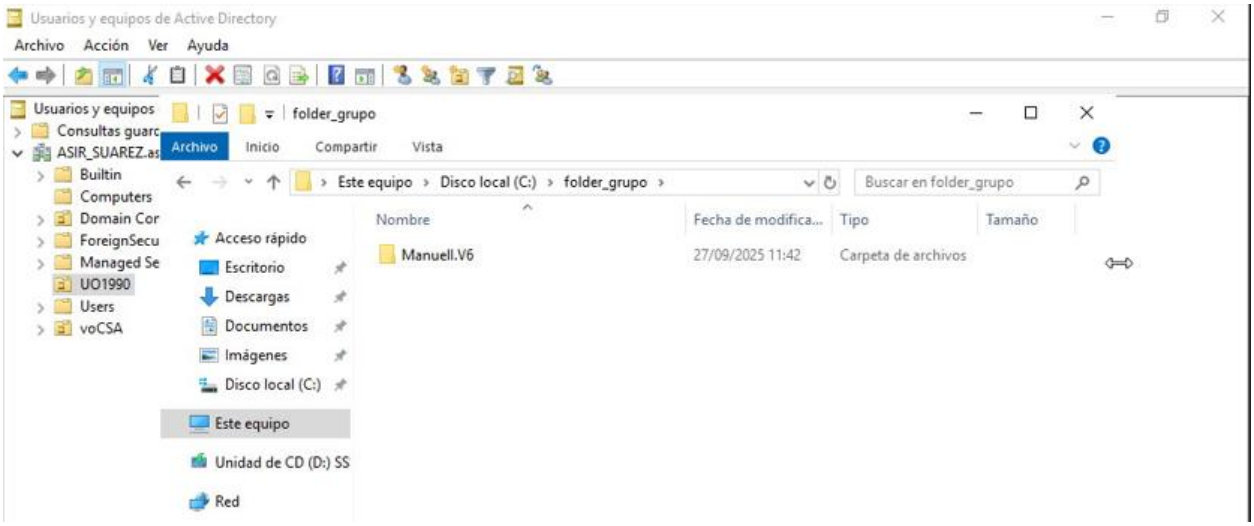


c) Inicia sesión con los usuarios en diferentes equipos unidos al dominio y comprueba.

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

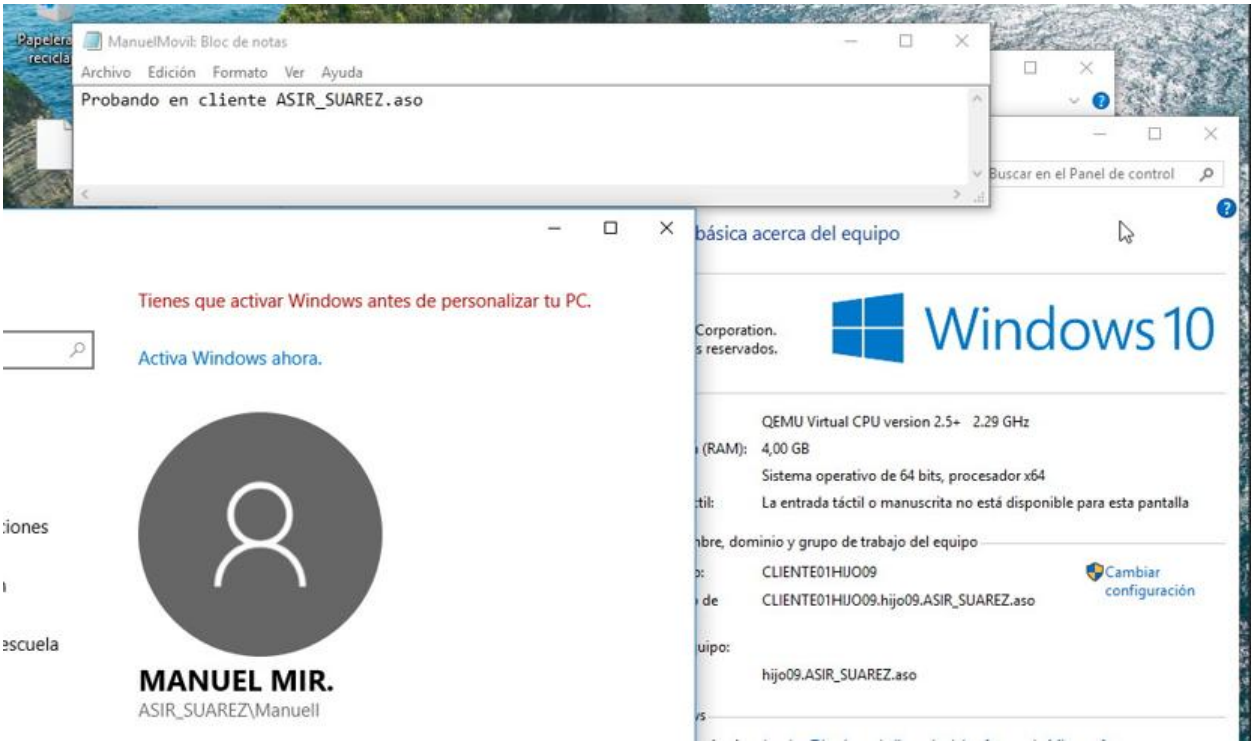


Al instante se crea la carpeta que contiene el perfil móvil.



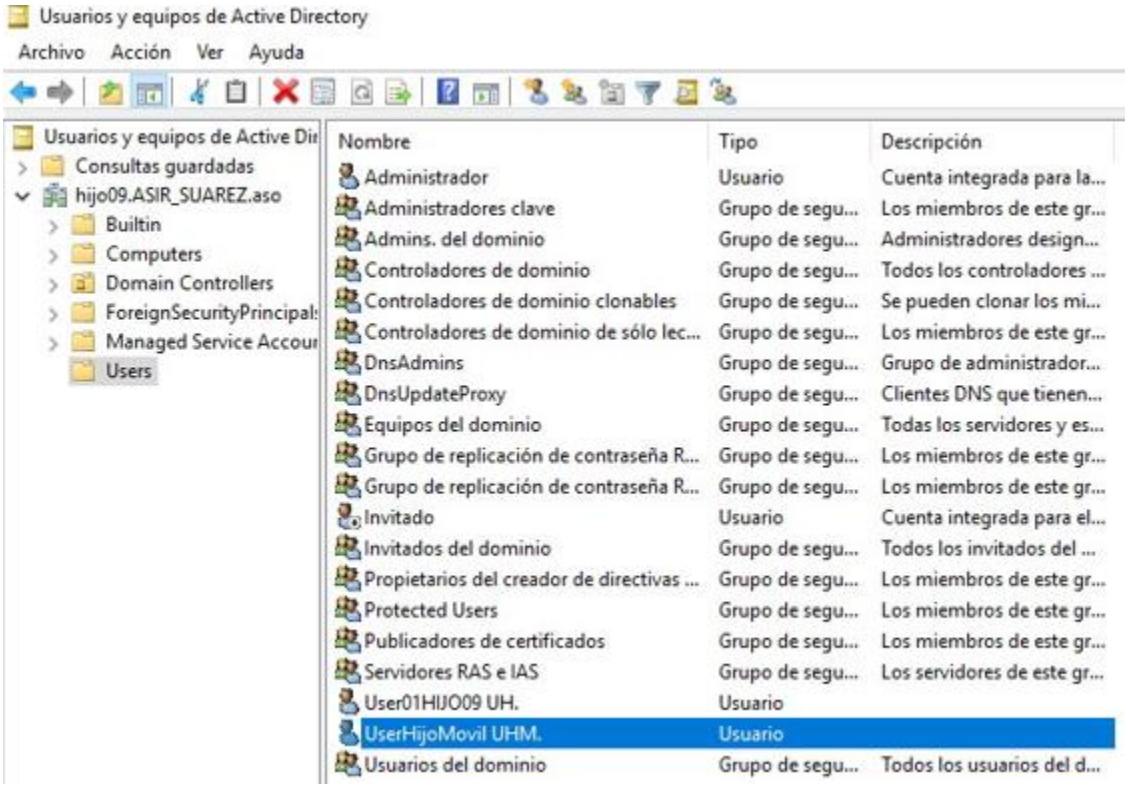
Creamos un documento de texto en el Escritorio del Cliente del Dominio **ASIR_SUAREZ.aso** con el usuario **ManuelI**

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.

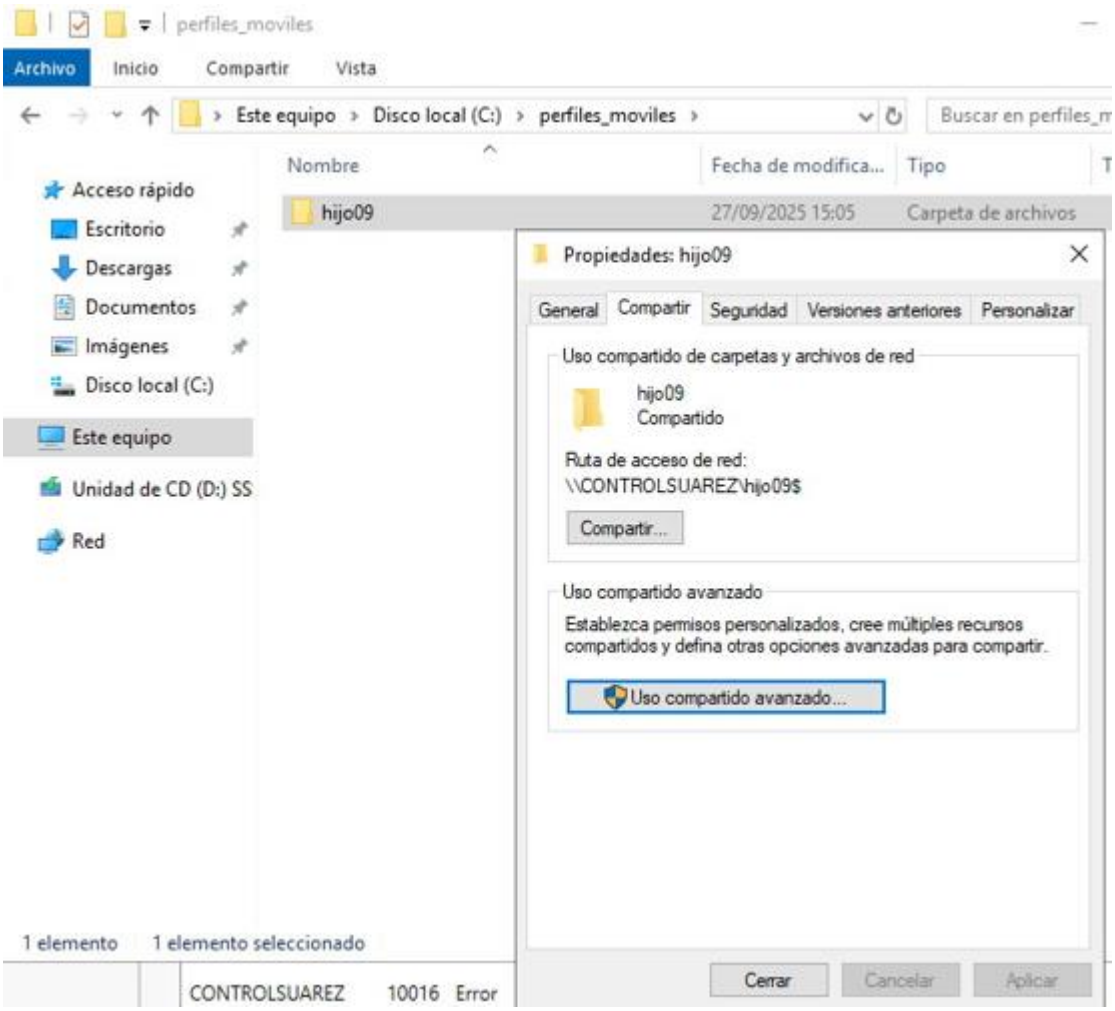


5) Escenario avanzado de pruebas.

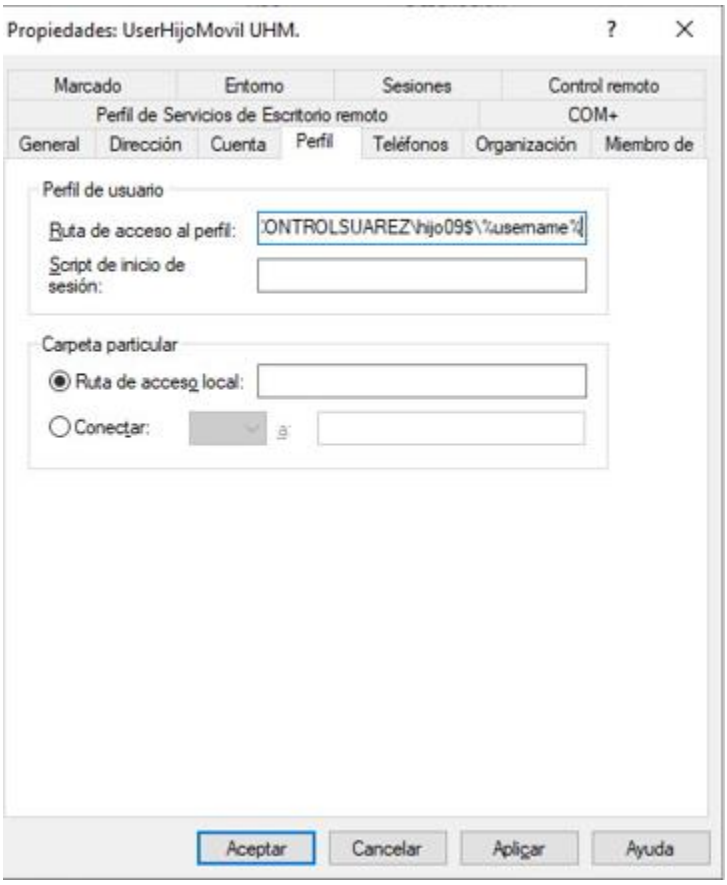
a) Crea un usuario en el subdominio y configura su perfil móvil en el dominio principal. Verifica si puede acceder desde equipos unidos al subdominio.



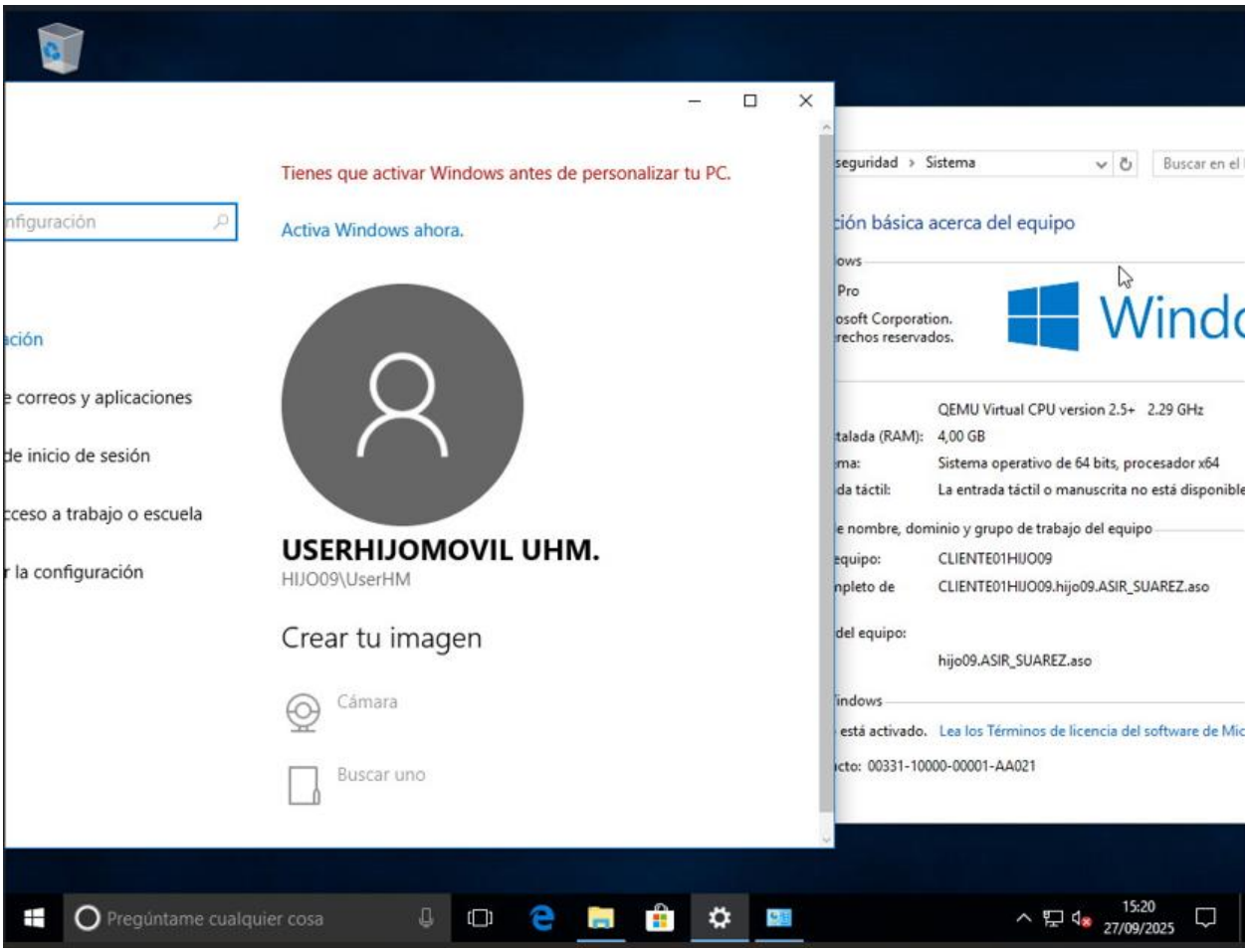
Creamos una carpeta compartida en el Controlador del Dominio Principal donde se almacenarán las carpetas de los perfiles.



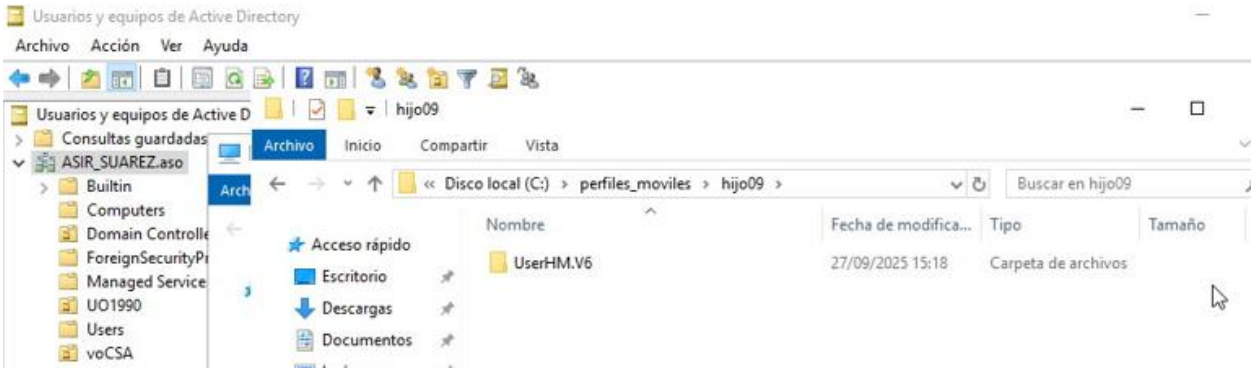
Establecemos la **Ruta del Perfil** en la cuenta de usuario:



Iniciamos sesión con el usuario en un cliente del Subdominio.

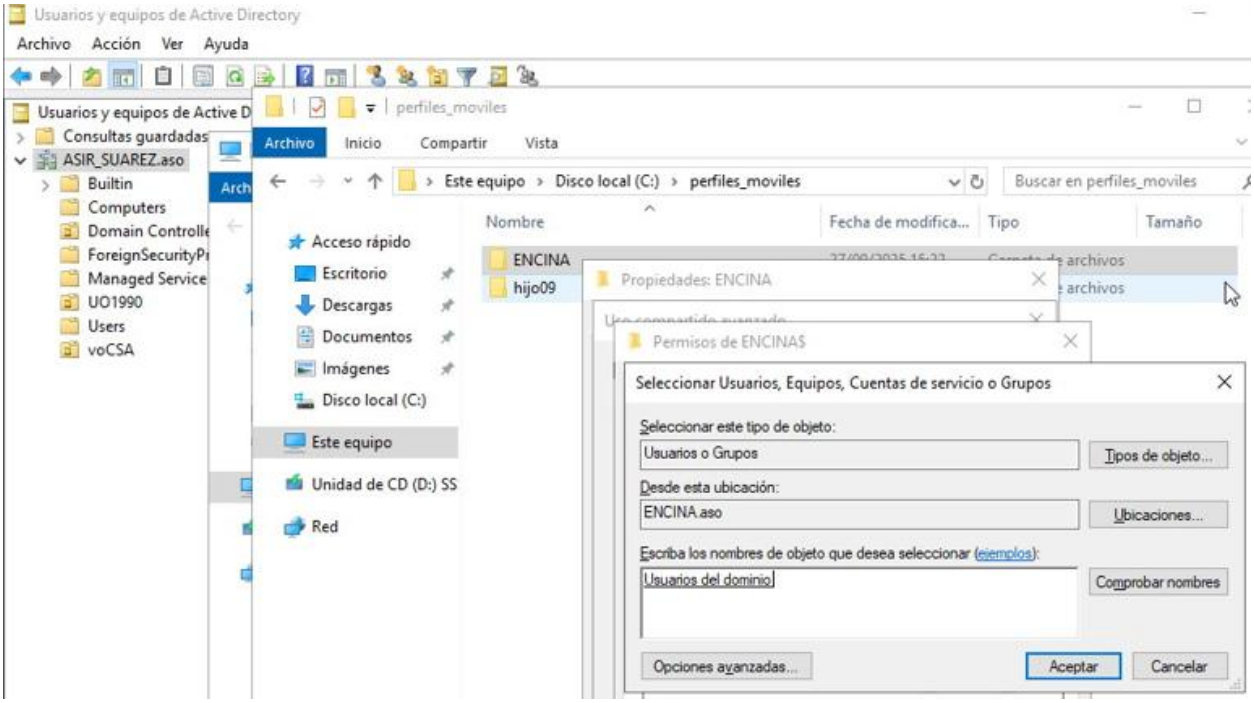


La carpeta se crea en el Controlador.

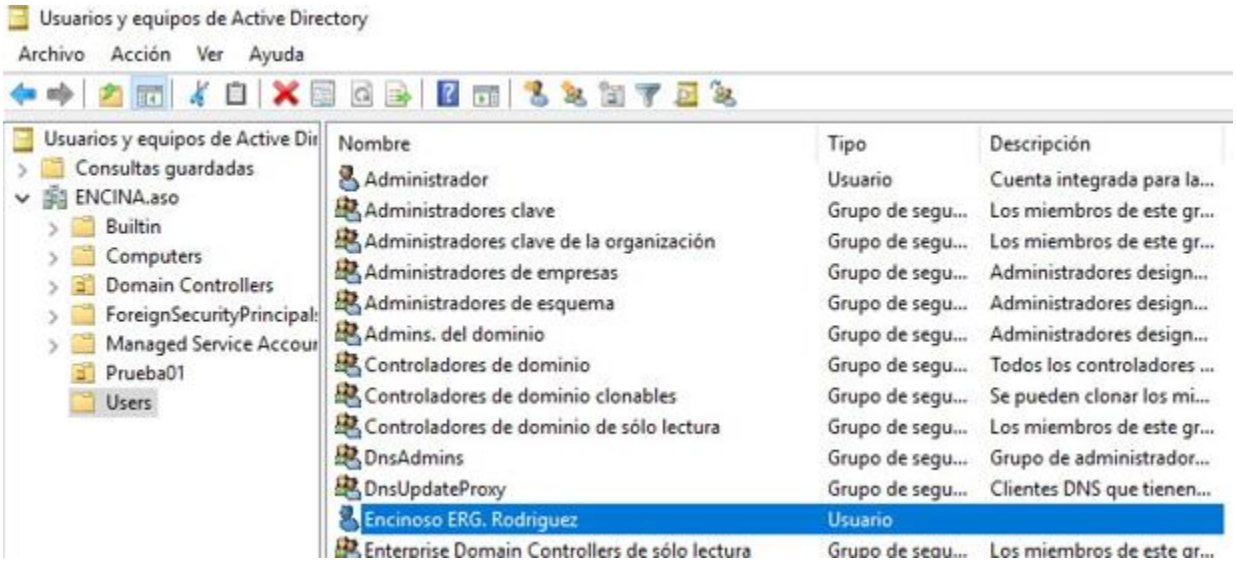


b) Crea un usuario en el bosque alternativo y prueba si puede usar perfiles móviles almacenados en el dominio principal mediante relaciones de confianza.

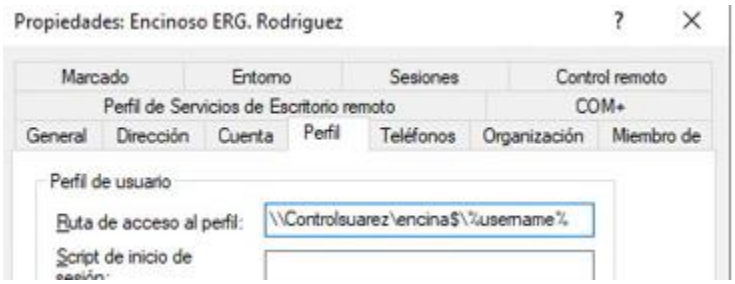
En el Controlador del Dominio Principal creamos una carpeta para los **Usuarios del dominio** de **Encina.aso**



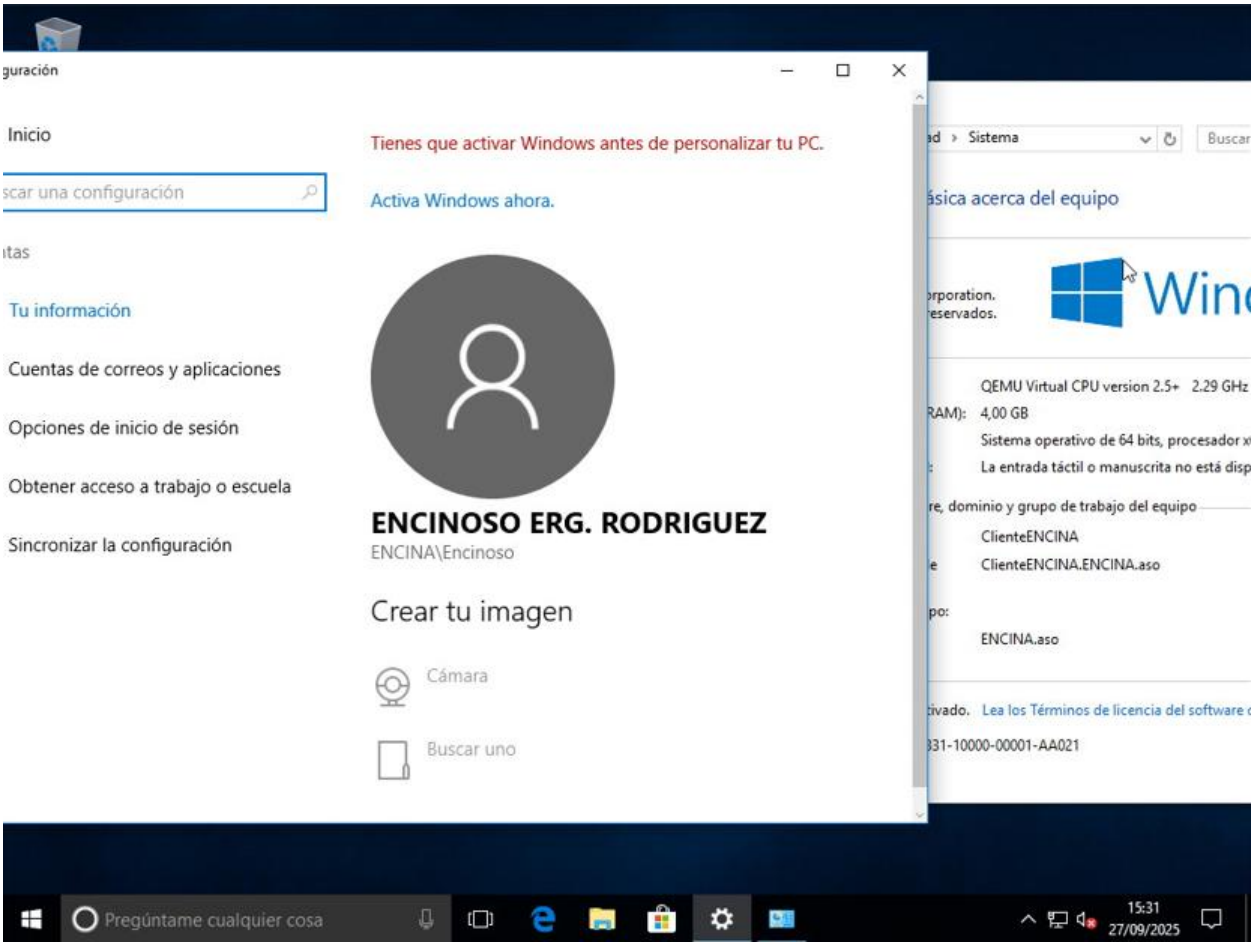
Luego en **Encina.aso** creamos al usuario **Encinoso**.



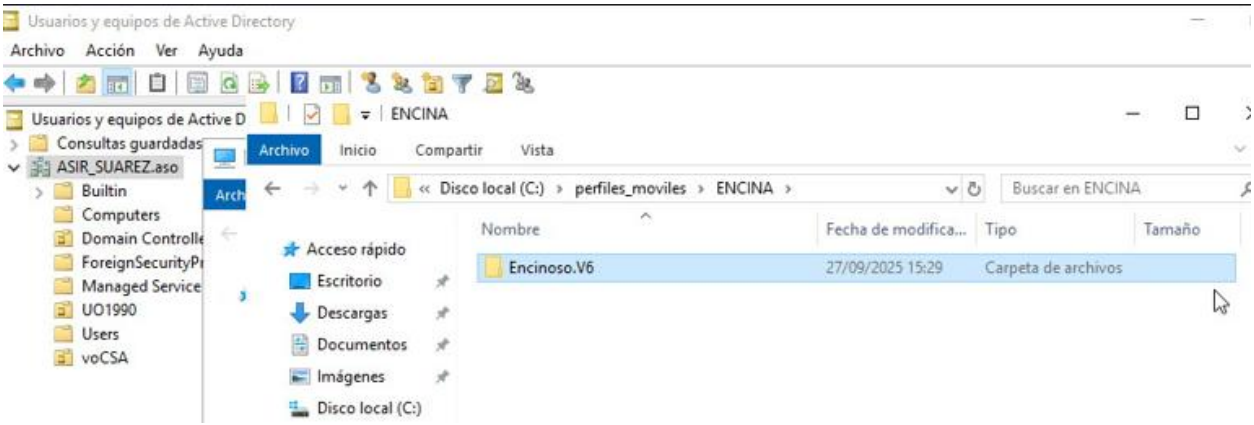
Establecemos su ruta de Perfil Movil.



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

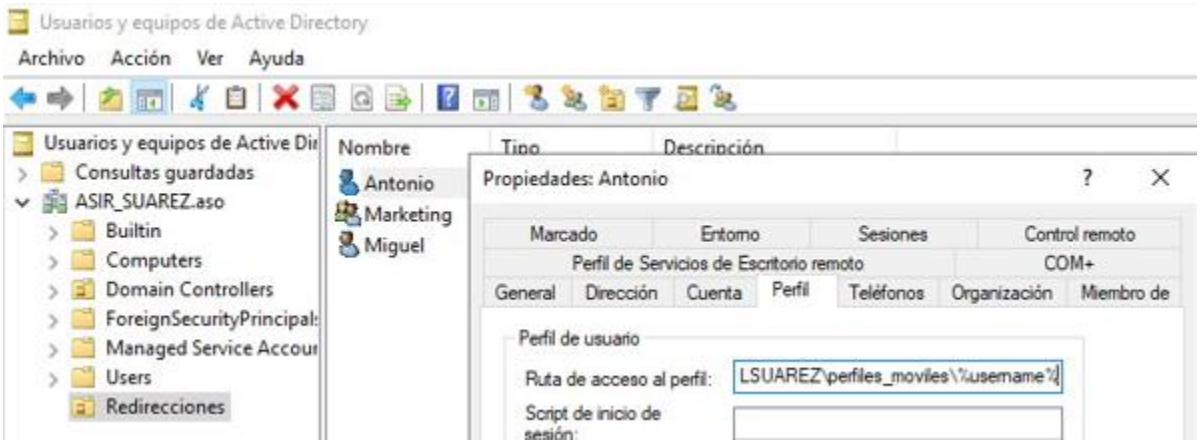


Vemos como se ha creado la carpeta del perfil móvil en el Controlador de **ASIR_SUAREZ.aso**

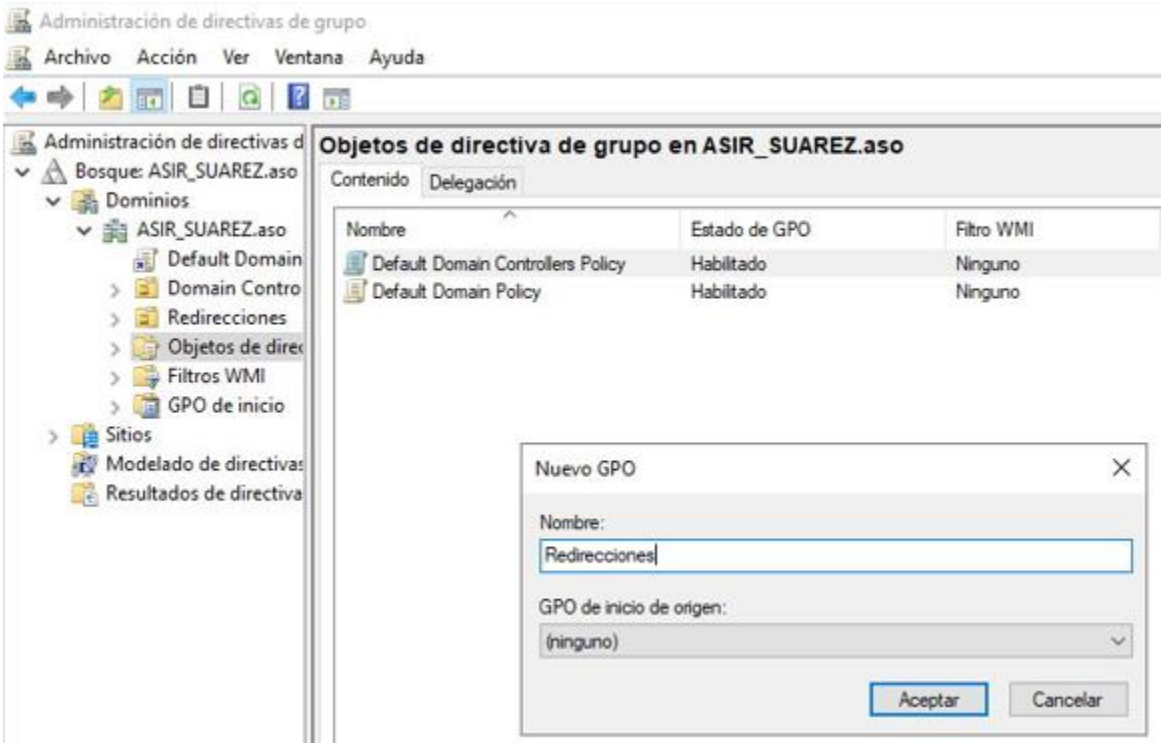


c) **Establece políticas de grupo (GPO) para redirigir carpetas (Documentos, Escritorio) hacia carpetas de red y comprueba que funcionan junto con los perfiles móviles.**

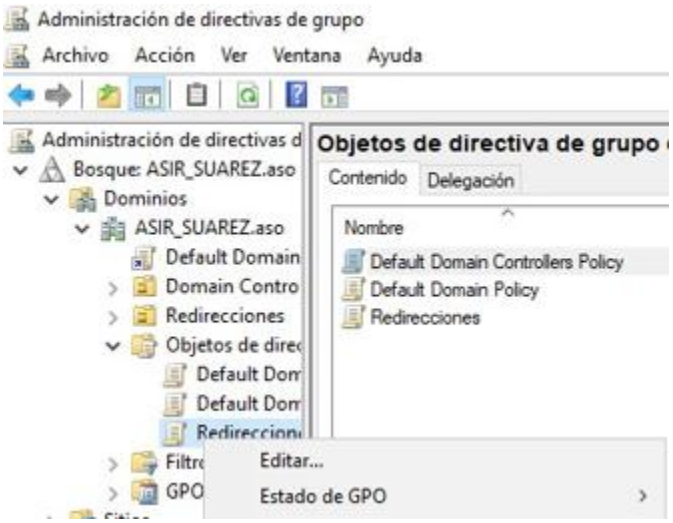
Para este ejercicio, creamos vamos a crear una Unidad Organizativa específica: **Redirecciones**. Donde vamos a colocar al grupo **Marketing** y a dos de sus usuarios. Como hemos hecho en actividades anteriores, debemos configurar la carpeta **perfiles_moviles** como un recurso compartido al cual los 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**.

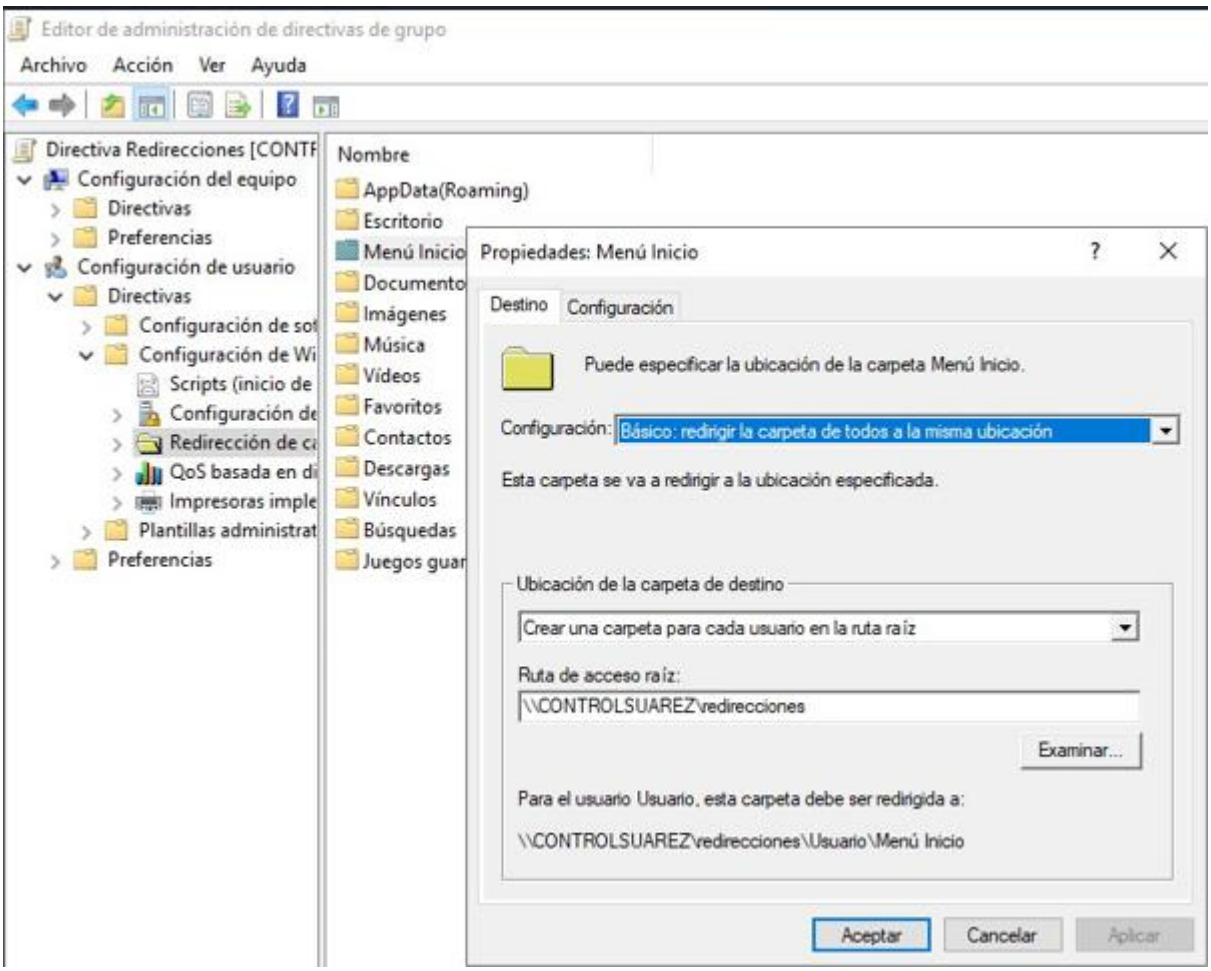


Una vez creada, la buscamos dentro de **Objetos de directiva de grupo** y le damos a **Editar...**

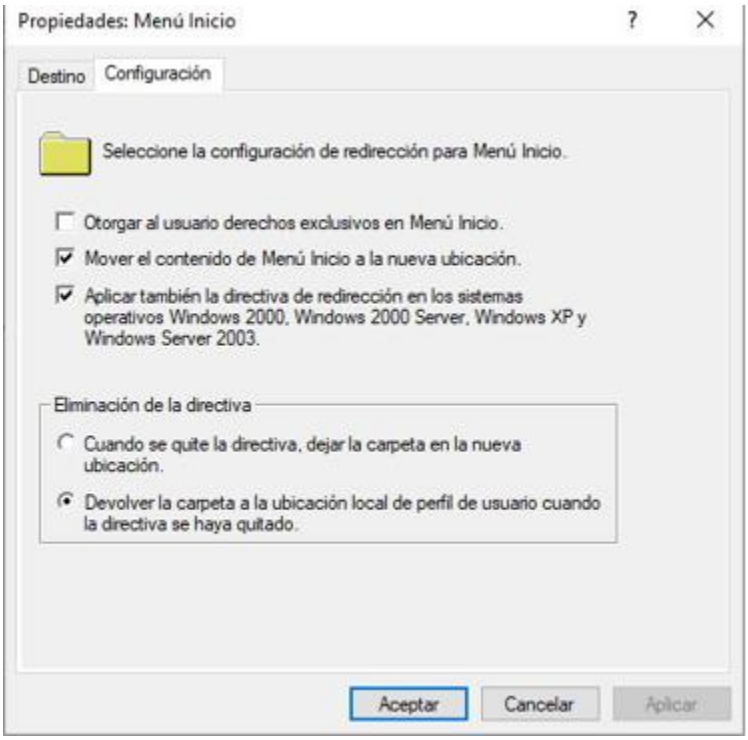


Navegamos: **Configuración de usuario → Directivas → Configuración de Windows → Redirección de carpetas**. Aquí tenemos una selección de carpetas predefinidas del usuario que podemos redirigir. En este caso vamos a usar “Menú inicio” y “Documentos”. La configuración para ambas es la misma.

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)

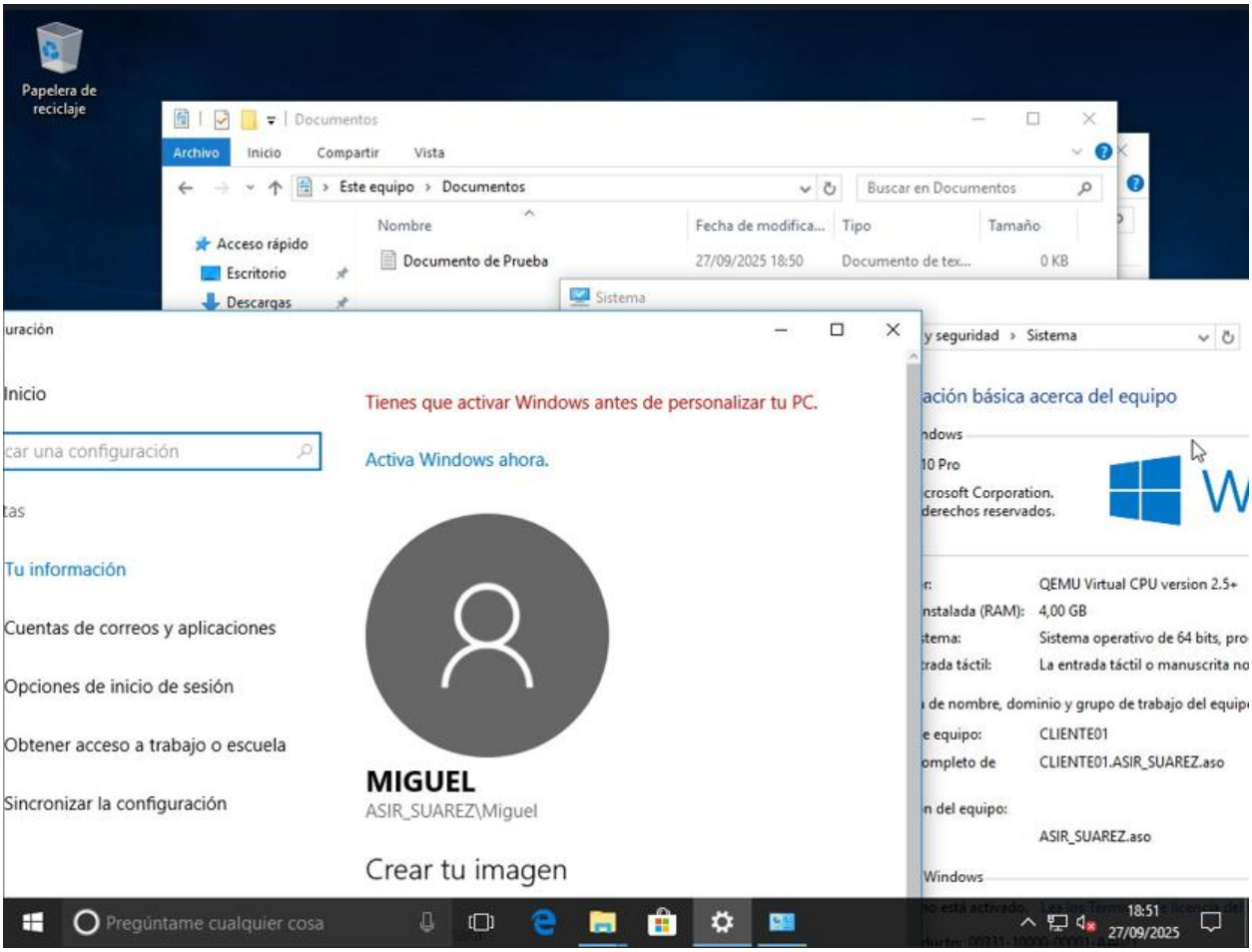


Pestaña **Configuración.**

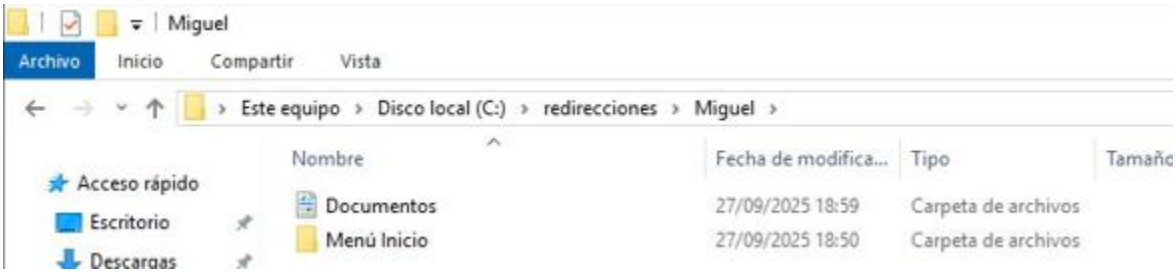


Una vez configurada la GPO, debemos vincularla con la Unidad Organizativa. Para ello seleccionamos la UO y le damos a **Vincular un GPO existente…**

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**.