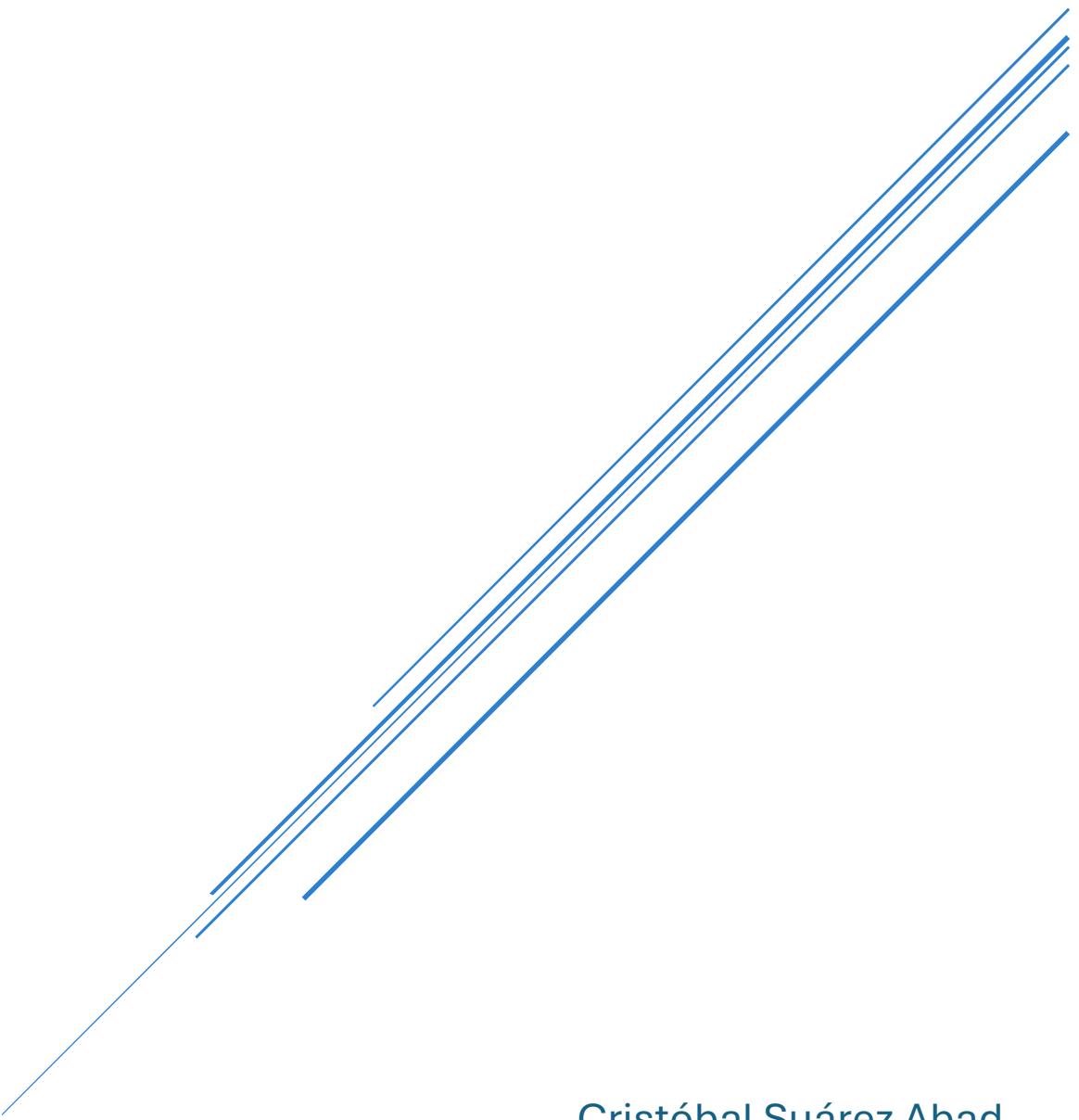


# ACTIVIDAD 1.2 ACTIVE DIRECTORY

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).**

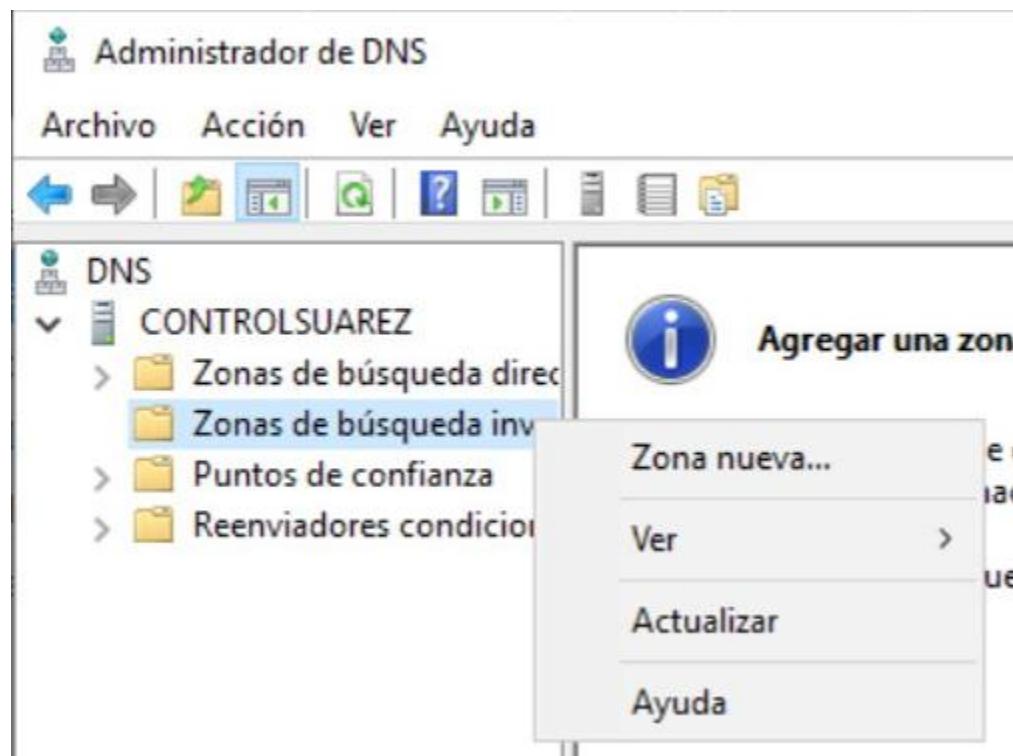
- a) Partiendo de un dominio funcional, instala un segundo servidor Windows Server y conviértelo en controlador de dominio secundario del dominio existente.**

### **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.”<sup>1</sup>*

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

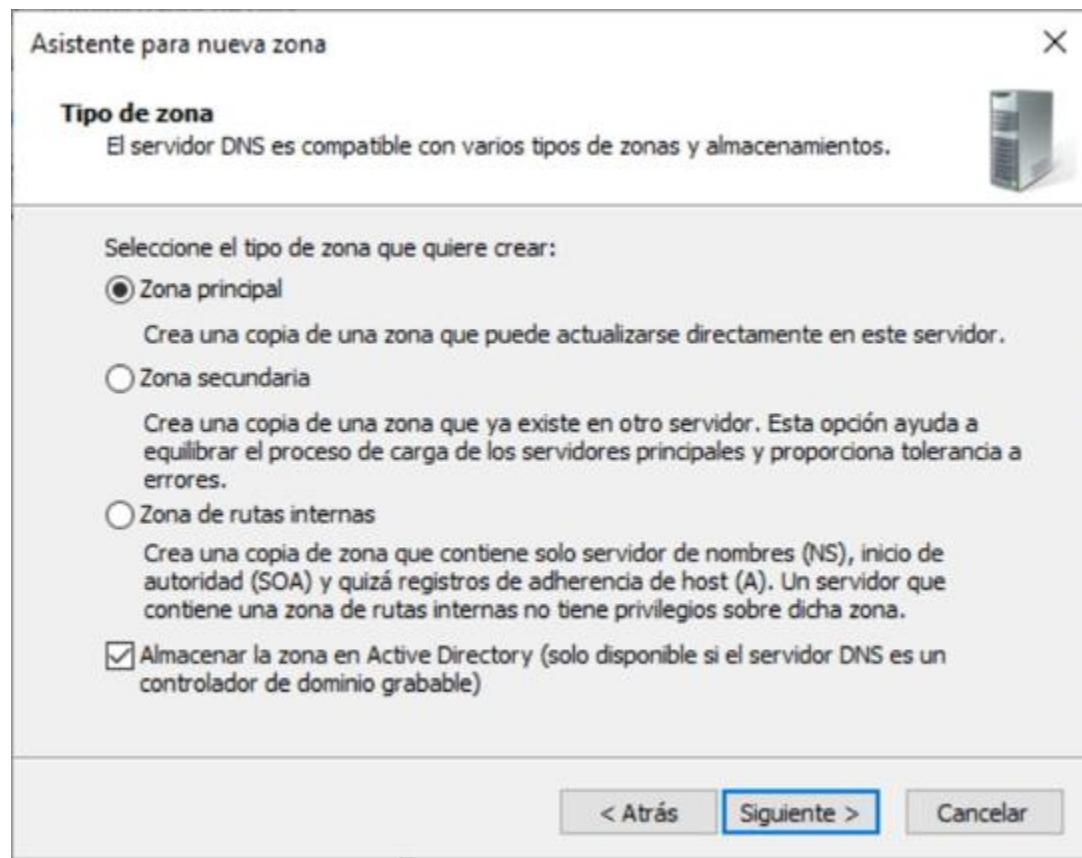
Desplegamos el nombre del Dominio y en “**Zonas de búsqueda inversa**” le damos a “**Zona nueva**”.



<sup>1</sup> <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**

Asistente para nueva zona X

**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 X

**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 X

**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:

< Atrás Siguiente > Cancelar

Configuración de actualizaciones dinámicas:

Asistente para nueva zona X

**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.

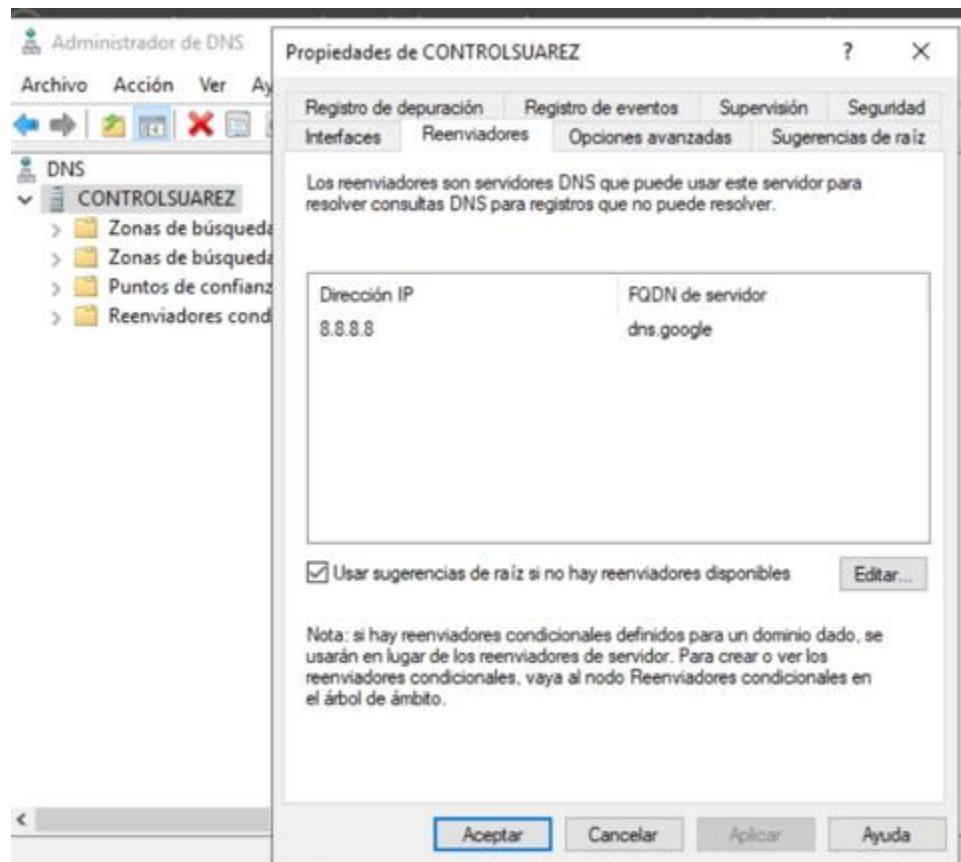


Zona de búsqueda una vez creada.

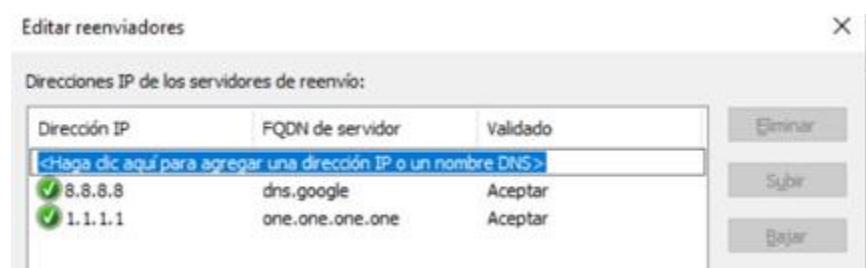
The screenshot shows the 'Administrador de DNS' (DNS Manager) interface. The left pane shows a tree view with 'DNS' expanded, showing 'CONTROLSUAREZ' and several subfolders: 'Zonas de búsqueda directa', 'Zonas de búsqueda inversa', 'Puntos de confianza', and 'Reenviadores condicionales'. The right pane displays a table of zones:

Nombre	Tipo	Estado	Estado de DNSSEC
7.2.10.in-addr.arpa	Zona primaria integrada de A...	En ejecución	Sin firma

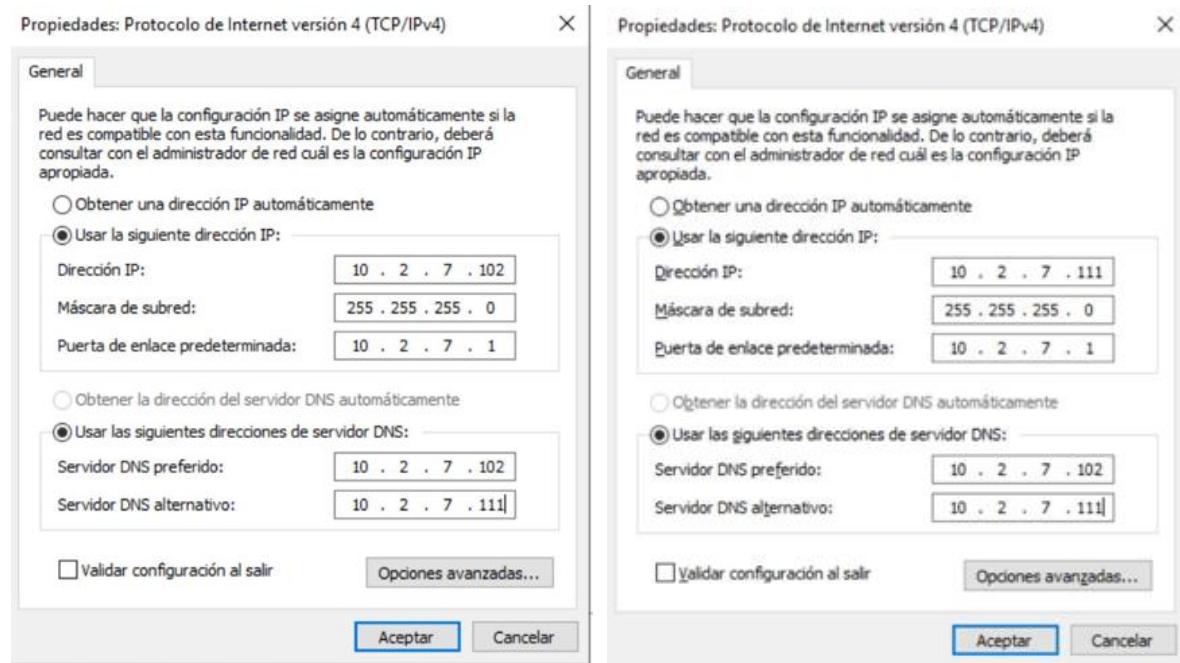
Ahora vamos a configurar los reenviadores, esto permitirá que los equipos puedan acceder a aquellos nombres que nuestro servidor DNS no pueda resolver (porque no lo conoce al no estar en nuestra red local). Para ello en DNS hacemos clic derecho en el controlador y después en Propiedades. Nos dirigimos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

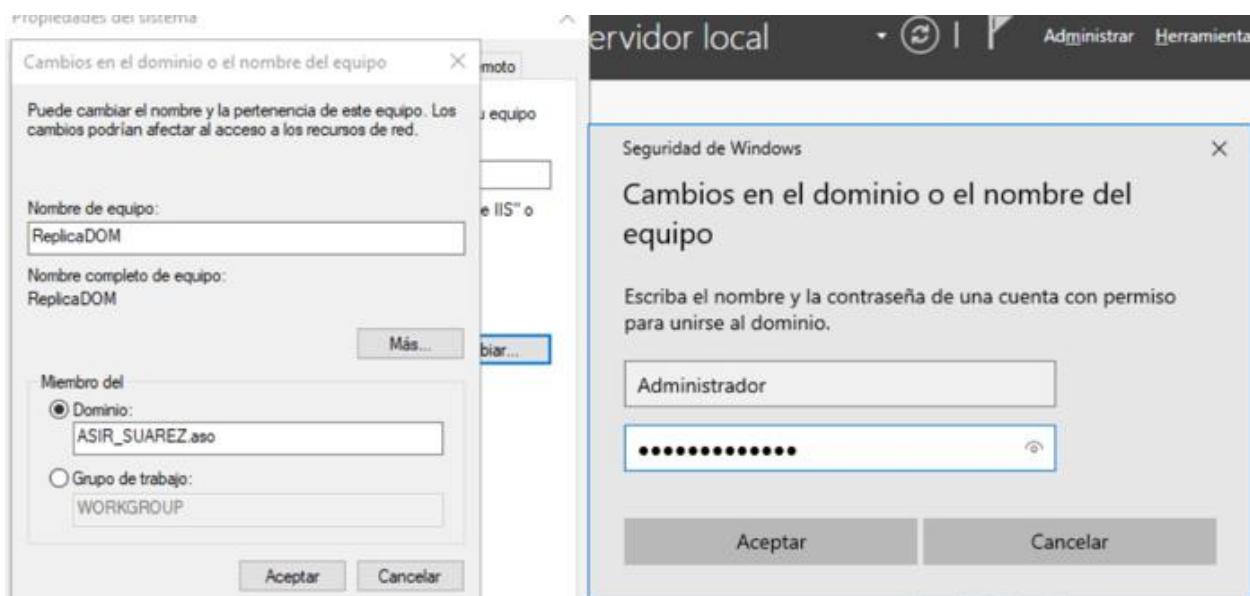
```
C:\Users\Administrador>ping CONTROLSUAREZ.ASIR_SUAREZ.aso

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<1ms TTL=128

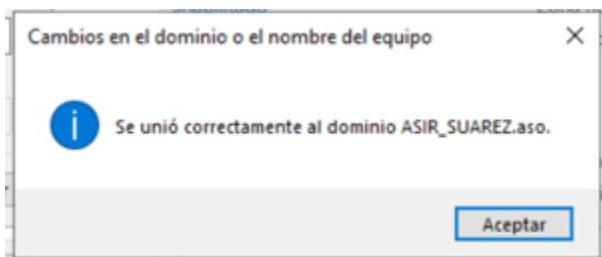
Estadísticas de ping para 10.2.7.102:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 6ms, Media = 2ms
```

## 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.

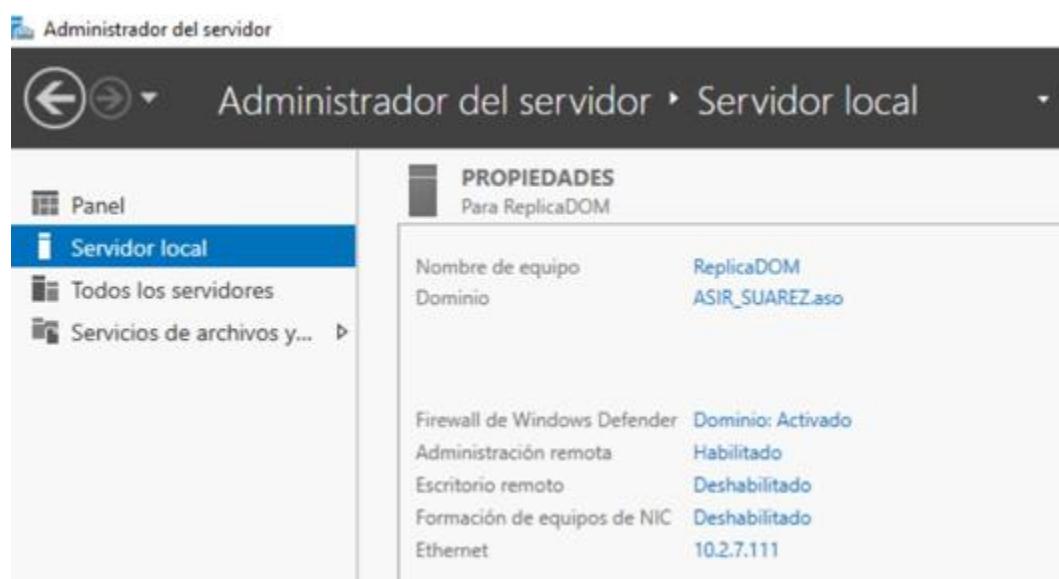


En el Controlador nos aparecerá el nuevo cliente en “Computers”.

The image shows the 'Usuarios y equipos de Active Directory' (Active Directory Users and Computers) snap-in. The left pane shows the organizational structure with 'Computers' selected under 'ASIR\_SUAREZ.aso'. The right pane displays a table of computer objects:

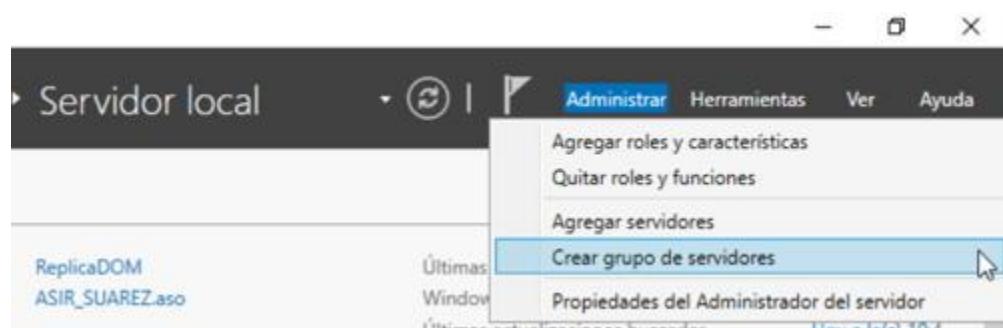
Nombre	Tipo	Descripción
ASDO-01	Equipo	
REPLICADOM	Equipo	

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.**

The screenshot shows the 'Seleccionar tipo de instalación' (Select Installation Type) wizard. The 'Tipo de instalación' (Installation Type) section is selected and highlighted in blue. The other options in this section are 'Selección de servidor', 'Roles de servidor', 'Características', 'Confirmación', and 'Reasignar'. The main content area provides instructions for selecting the type of installation (roles and features vs. roles and services) and describes each option.

**Antes de comenzar**

**Tipo de instalación** (selected)

**Selección de servidor**

**Roles de servidor**

**Características**

**Confirmación**

**Reasignar**

**Seleccionar tipo de instalación**

SERVIDOR DE DESTINO  
ReplicaDOM.ASIR\_SUAREZ.adso

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

**Instalación basada en características o en roles**  
Para configurar un solo servidor, agregue roles, servicios de rol y características.

**Instalación de Servicios de Escritorio remoto**  
Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

Elegimos el Servidor: En nuestro caso solo hay uno.

Seleccionar servidor de destino

SERVIDOR DE DESTINO  
ReplicaDOM.ASIR\_SUAREZ.aso

Antes de comenzar	Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.		
Tipo de instalación	<input checked="" type="radio"/> Seleccionar un servidor del grupo de servidores <input type="radio"/> Seleccionar un disco duro virtual		
Selección de servidor	<b>Grupo de servidores</b>		
Roles de servidor			
Características			
Confirmación			
Resultados			

Filtro:

Nombre	Dirección IP	Sistema operativo
ReplicaDOM.ASIR_SUAR...	10.2.7.111	Microsoft Windows Server 2019 Standard

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

Seleccionar roles de servidor

SERVIDOR DE DESTINO  
ReplicaDOM.ASIR\_SUAREZ.aso

Antes de comenzar	Seleccione uno o varios roles para instalarlos en el servidor seleccionado.	
Tipo de instalación		
Selección de servidor		
Roles de servidor	<b>Roles</b>	
Características		
AD DS		
Confirmación		
Resultados		

Acceso remoto  
Active Directory Lightweight Directory Services  
Active Directory Rights Management Services  
Atestación de mantenimiento del dispositivo  
Hyper-V  
Servicio de protección de host  
Servicios de acceso y directivas de redes  
Servicios de archivos y almacenamiento (1 de 12 ir)  
Servicios de certificados de Active Directory  
 **Servicios de dominio de Active Directory**  
Servicios de Escritorio remoto

Descripción

Servicios de dominio de Active Directory (AD DS) almacena información acerca de los objetos de la red y pone esta información a disposición de los usuarios y administradores de red. AD DS usa controladores de dominio para proporcionar a los usuarios de red acceso a los recursos permitidos en toda la red mediante un proceso de inicio de sesión único.

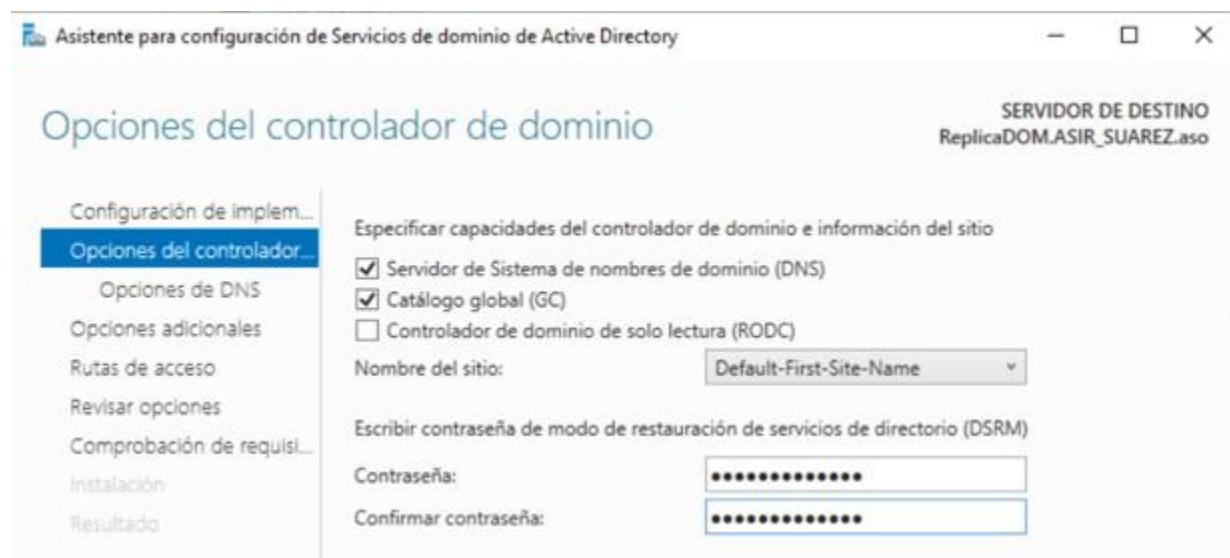
No hay que configurar nada más. Llevamos a cabo la instalación. Una vez terminada, seguimos con el proceso:



Elegimos “Aregar 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.

The screenshot shows the 'Opciones de DNS' (DNS Options) step of the Active Directory Domain Services Wizard. The title bar reads 'Asistente para configuración de Servicios de dominio de Active Directory' and 'SERVIDOR DE DESTINO ReplicaDOM.ASIR\_SUAREZ.aso'. The main pane displays a warning message: 'No se puede crear una delegación para este servidor DNS porque la zona principal autoritativa no se encuentra o no ejecuta el servidor DNS de Windows. Si está realizando una integración en una infraestructura DNS existente, debe crear manualmente una delegación a este servidor DNS en la zona principal para garantizar una resolución de nombres confiable desde fuera del dominio 'ASIR\_SUAREZ.aso''. Below the message is a button labeled 'Aceptar' (Accept). The left sidebar lists navigation options: Configuración de implementación, Opciones del controlador, **Opciones de DNS**, Opciones adicionales, Rutas de acceso, Revisar opciones, Comprobación de requisitos, Instalación, and Resultado.

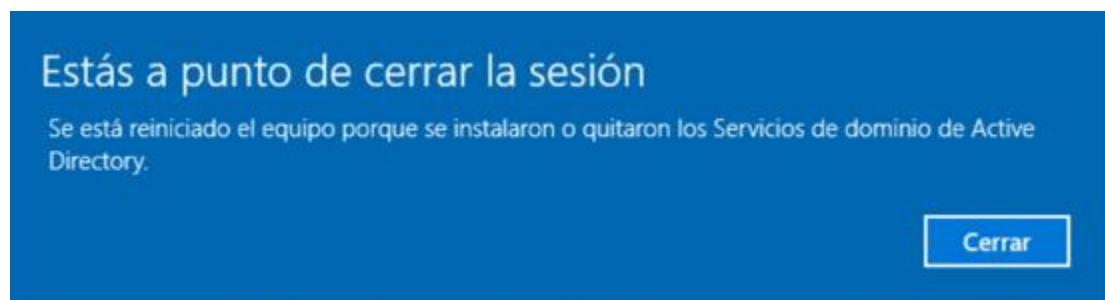
En **Opciones Adicionales** podemos especificar si queremos que se replique desde un Controlador en específico o desde cualquiera.

The screenshot shows the 'Opciones adicionales' (Additional Options) step of the Active Directory Domain Services Wizard. The title bar reads 'Asistente para configuración de Servicios de dominio de Active Directory' and 'SERVIDOR DE DESTINO ReplicaDOM.ASIR\_SUAREZ.aso'. The main pane has two sections: 'Especificar opciones de Instalar desde el medio (IFM)' with an unchecked checkbox for 'Instalar desde medios', and 'Especificar opciones de replicación adicionales' with a dropdown menu titled 'Replicar desde:' containing three items: 'Cualquier controlador de dominio', 'Cualquier controlador de dominio' (which is highlighted in blue), and 'CONTROLSUAREZ.ASIR\_SUAREZ.aso'. The left sidebar lists navigation options: Configuración de implementación, Opciones del controlador, Opciones de DNS, **Opciones adicionales**, Rutas de acceso, Revisar opciones, Comprobación de requisitos, and Instalación.

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.

Nombre	Tipo	Datos	Marca de tiempo
_msdc			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(igual que la carpeta princip... Inicio de autoridad (SOA)	Servidor de nombres (NS)	[45], controlsuarez.asir_suarez.aso., hostmaster.asir_suarez.aso.	static
(igual que la carpeta princip... Servidor de nombres (NS)	replicadom.asir_suarez.aso.		static
(igual que la carpeta princip... Servidor de nombres (NS)	controlsuarez.asir_suarez.aso.		static
(igual que la carpeta princip... Host (A)	10.2.7.102		20/09/2025 11:00:00

También en **Usuarios y Equipos**.

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

NOMBRE TIPO TIPO DE DC SITIO DESCRIPCION

NOMBRE	TIPO	TIPO DE DC	SITIO	DESCRIPCION
ASIR_SUAREZ.aso				
Builtin				
Computers				
Domain Controllers				
ForeignSecurityPrincipal				
Managed Service Account				
UO1990				
Users				
voCSA				
REPLICADOM	Equipo	GC	Default-First-Site	
CONTROLSUAREZ	Equipo	GC	Default-First-Site	

Consultas guardadas

ASIR\_SUAREZ.aso

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipal

Managed Service Account

UO1990

Users

voCSA

REPLICADOM

CONTROLSUAREZ

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

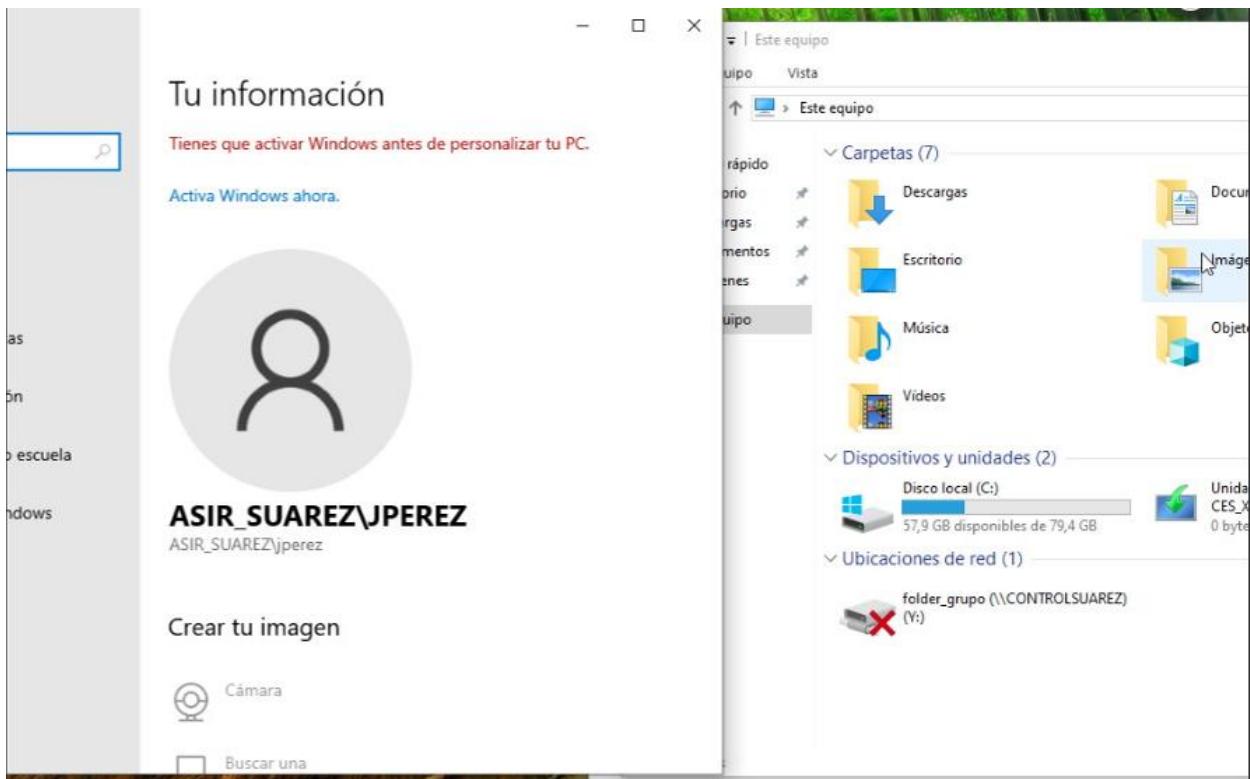
**i) Crea un usuario en el controlador principal y verifica que aparece en el secundario.**

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.

Nombre	Tipo	Descripción
Administrator	Usuario	Cuenta integrada para la...
Administrad...	Grupo de segu...	Los miembros de este gr...
Administrad...	Grupo de segu...	Los miembros de este gr...
Administrad...	Grupo de segu...	Administradores design...
Administrad...	Grupo de segu...	Administradores design...
Admins. del ...	Grupo de segu...	Administradores design...
Controlador...	Grupo de segu...	Todos los controladores ...
Controlador...	Grupo de segu...	Se pueden clonar los mi...
Controlador...	Grupo de segu...	Los miembros de este gr...
DnsAdmins	Grupo de segu...	Grupo de administrador...
DnsUpdateP...	Grupo de segu...	Clientes DNS que tienen...
Enterprise D...	Grupo de segu...	Los miembros de este gr...
Equipos del ...	Grupo de segu...	Todas los servidores y es...
Grupo de re...	Grupo de segu...	Los miembros de este gr...
Grupo de re...	Grupo de segu...	Los miembros de este gr...
Invitado	Usuario	Cuenta integrada para el...
Invitados del...	Grupo de segu...	Todos los invitados del ...
Propietarios ...	Grupo de segu...	Los miembros de este gr...
Protected Us...	Grupo de segu...	Los miembros de este gr...
Publicadore...	Grupo de segu...	Los miembros de este gr...
Servidores R...	Grupo de segu...	Los servidores de este gr...
User01Prueb...	Usuario	
Usuarios del ...	Grupo de segu...	Todos los usuarios del d...

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.

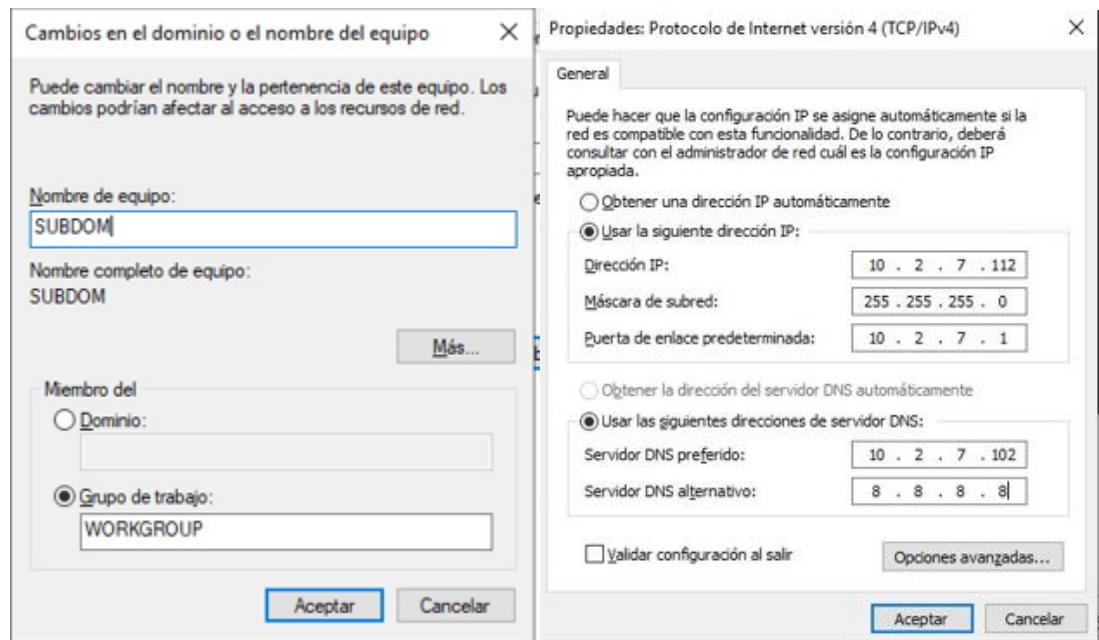


## 2) Subdominio.

**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.

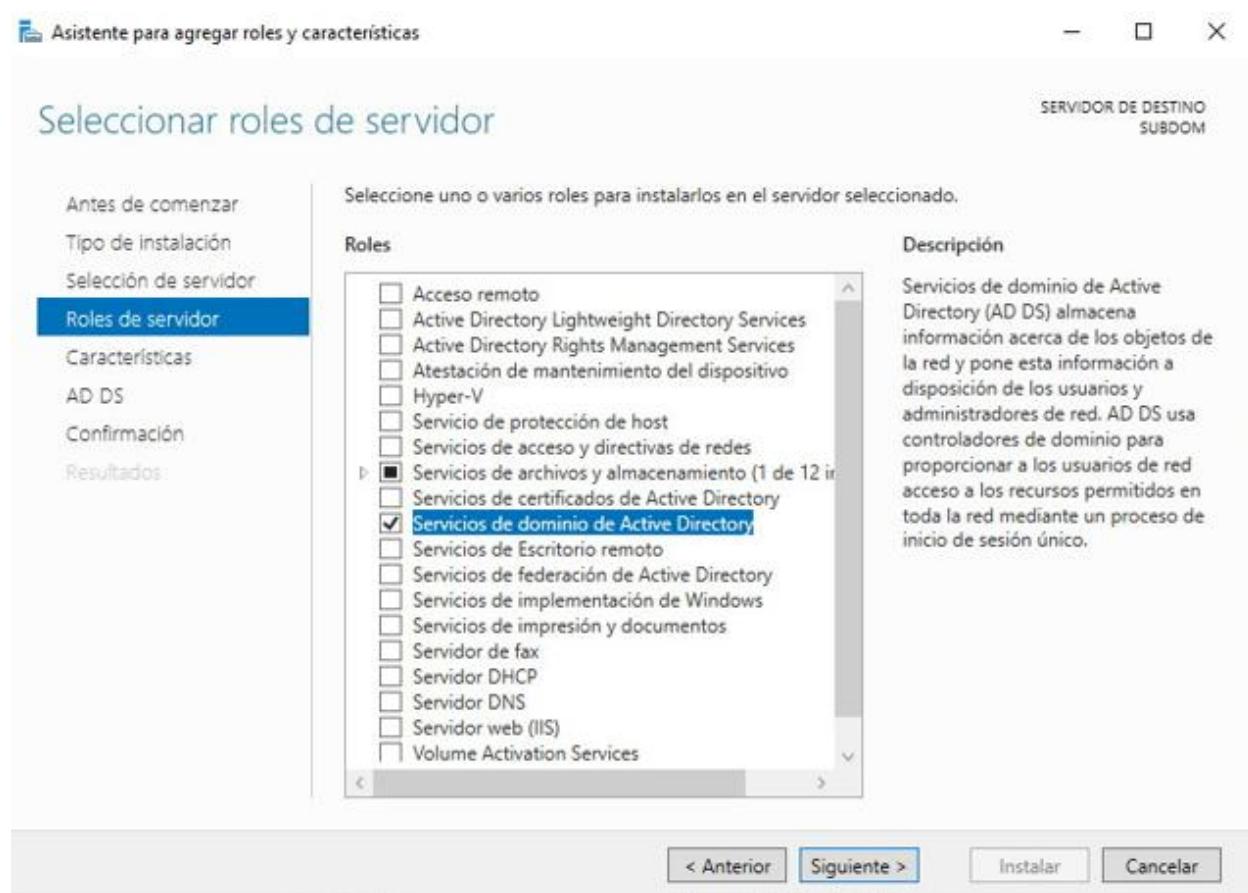


Comprobamos la conexión.

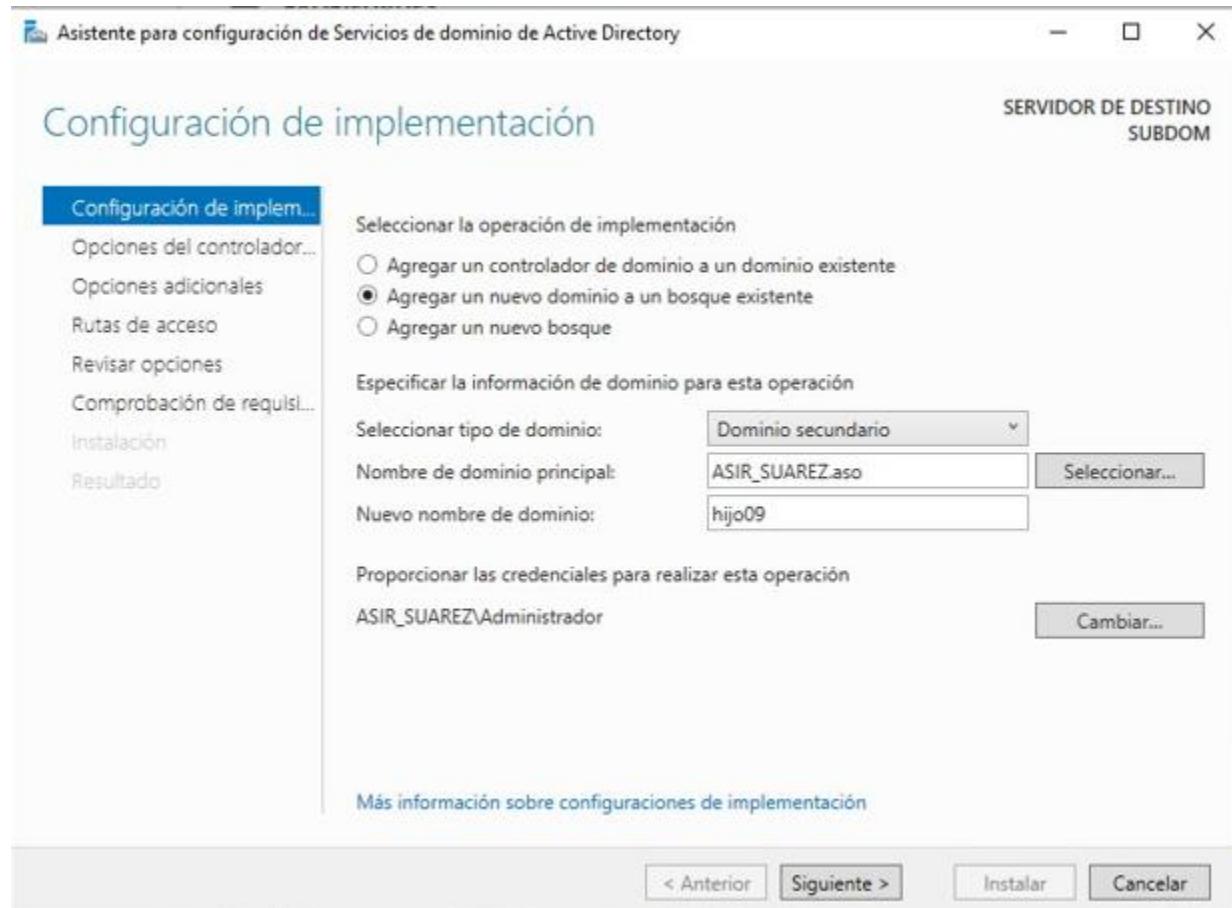
```
C:\Users\Administrador>ping ASIR_SUAREZ.aso
Haciendo ping a ASIR_SUAREZ.aso [10.2.7.102] con 32 bytes de datos:
Respuesta desde 10.2.7.102: bytes=32 tiempo<1ms TTL=128

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
```

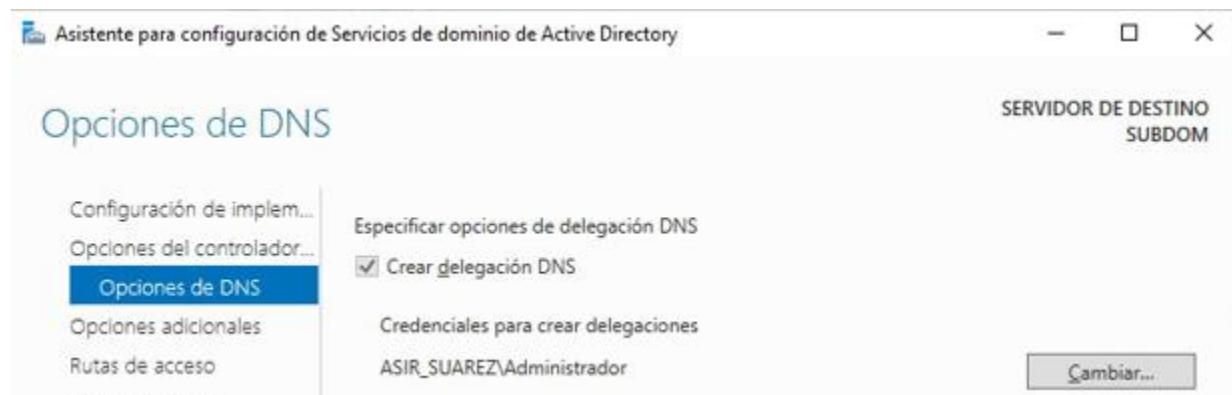
Una vez configurada, instalamos el rol de “**Servicios de Dominio de Active Directory**”.



Una vez terminada la instalación, seguiremos con el siguiente asistente. Elegimos “Aregar 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.

Administrador del servidor

Administrador del servidor • Servidor local

Panel

**Servidor local**

- Todos los servidores
- AD DS
- DNS
- Servicios de archivos y...

PROPIEDADES  
Para SUBDOM

Nombre de equipo	SUBDOM
Dominio	hijo09.ASIR_SUAREZ.aso
Firewall de Windows Defender	Privado: Activado
Administración remota	Habilitado
Escritorio remoto	Deshabilitado
Formación de equipos de NIC	Deshabilitado
Ethernet	10.2.7.112
Versión del sistema operativo	Microsoft Windows Server 2019 Standard
Información de hardware	QEMU Standard PC (i440FX + PIIX, 1996)

**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

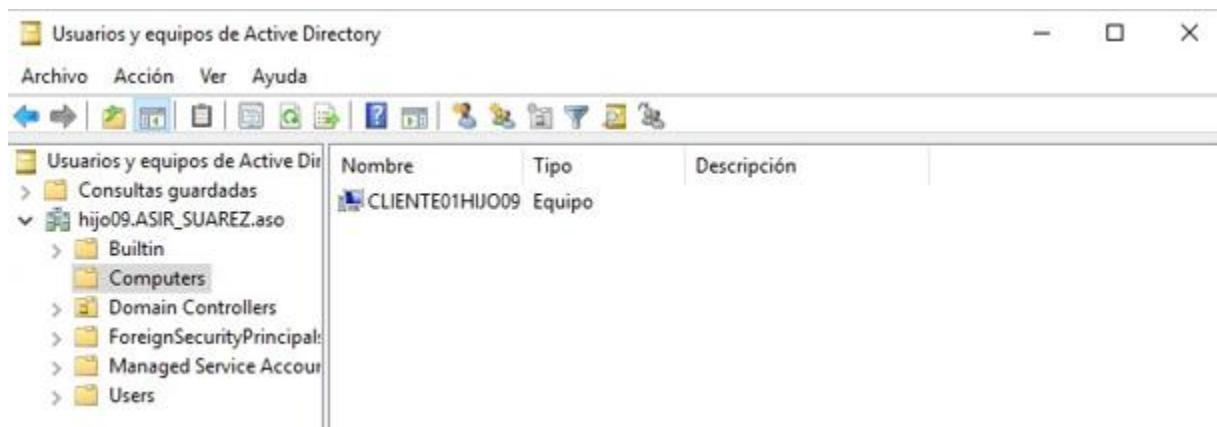
Como dijimos más arriba, cuando creamos un nuevo subdominio, de un dominio ya existente, se establece de manera implícita y automática una relación de confianza bidireccional y transitiva entre el nuevo dominio y su dominio padre.

<sup>2</sup>

**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.



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

## Usuario creado.

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory

Consultas guardadas

hijo09.ASIR\_SUAREZ.aso

Builtin Computers Domain Controllers ForeignSecurityPrincipal Managed Service Account Users

Nombre: User01HIJO09 UH.

Tipo: Propiedades: User01HIJO09 UH.

Descripción:

Marcado Entorno

Perfil de Servicios de Escritorio remoto

General Dirección Cuenta Perfil

Nombre de inicio de sesión de usuario: User01

Nombre de inicio de sesión de usuario (ante): HIJO09\

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

Tu información

Tienes que activar Windows antes de personalizar tu PC.

Activa Windows ahora.

USER01HIJO09 UH.

HIJO09\User01

Crear tu imagen

Sistema

Buscar en el Panel de control

Windows 1

es LTSC

ction. Todos

se

QEMU Virtual CPU version 2.5+ 2.29 GHz

RAM): 4,00 GB

Sistema operativo de 64 bits, procesador x64

La entrada táctil o manuscrita no está disponible para esta pantalla

re, dominio y grupo de trabajo del equipo

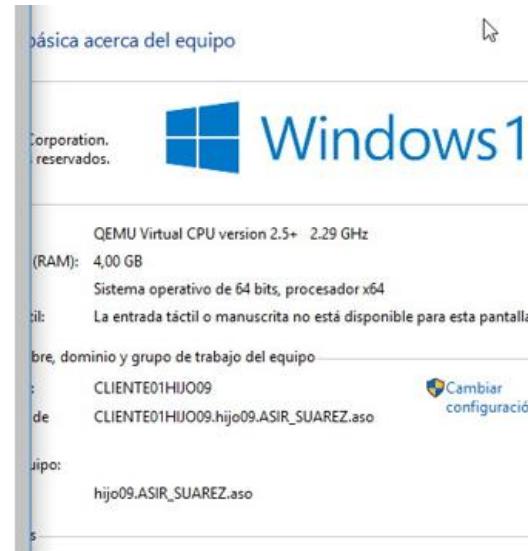
ASDO-01

ASDO-01.ASIR\_SUAREZ.aso

Cambiar configuración

ASIR\_SUAREZ.aso

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

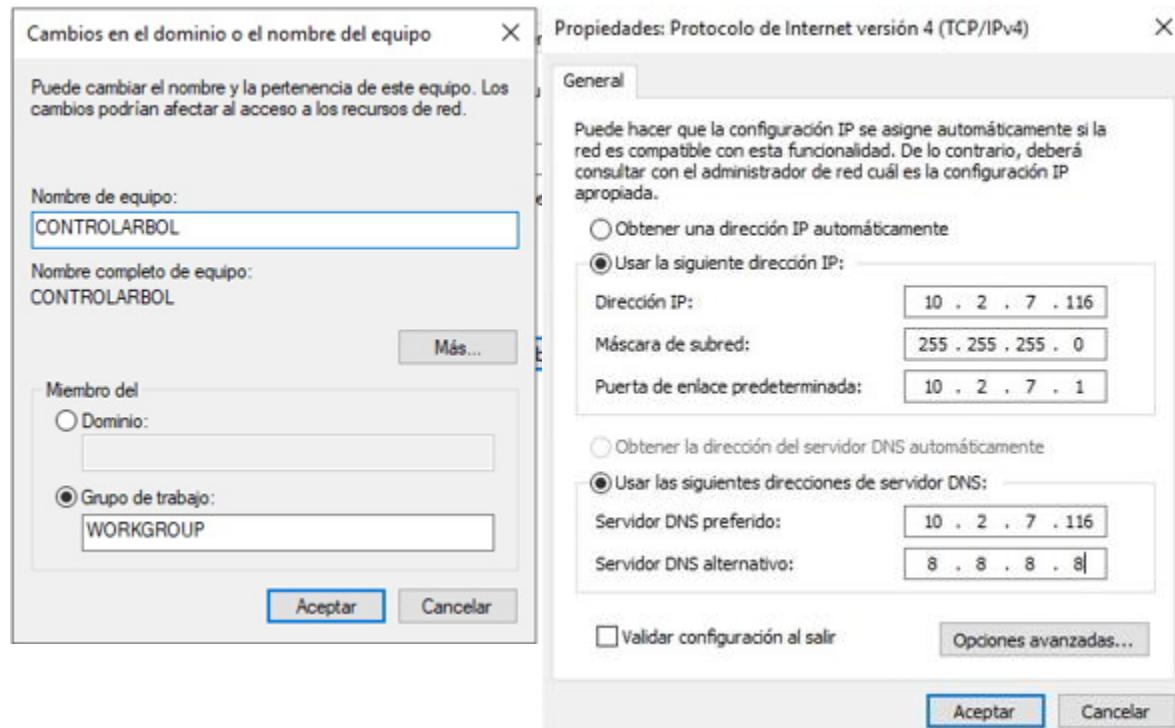


### 3) Bosque.

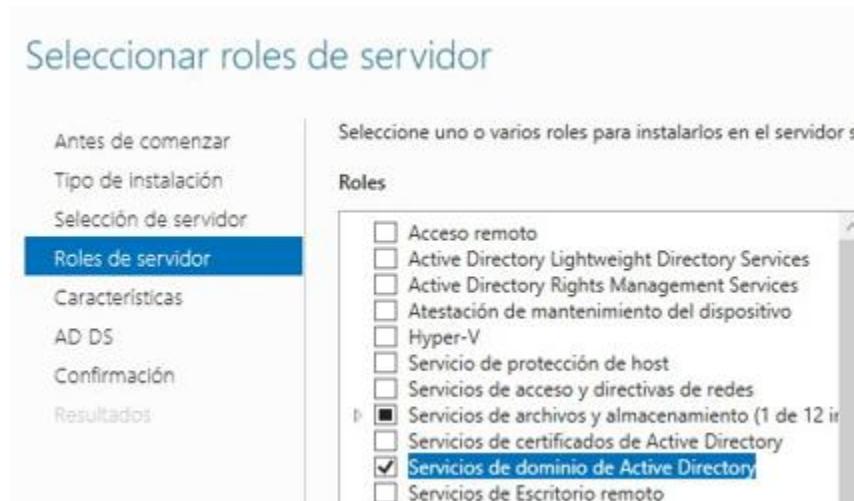
NOTA: Si se usa una VM clonada de la misma fuente que el otro dominio, pueden producirse problemas. Se debe realizar “sysprep”.

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

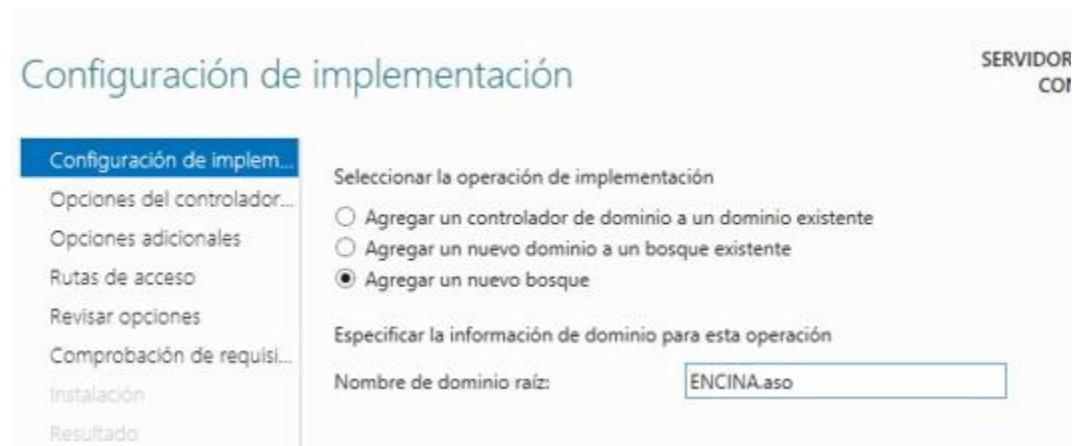
Configuramos el servidor.



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.



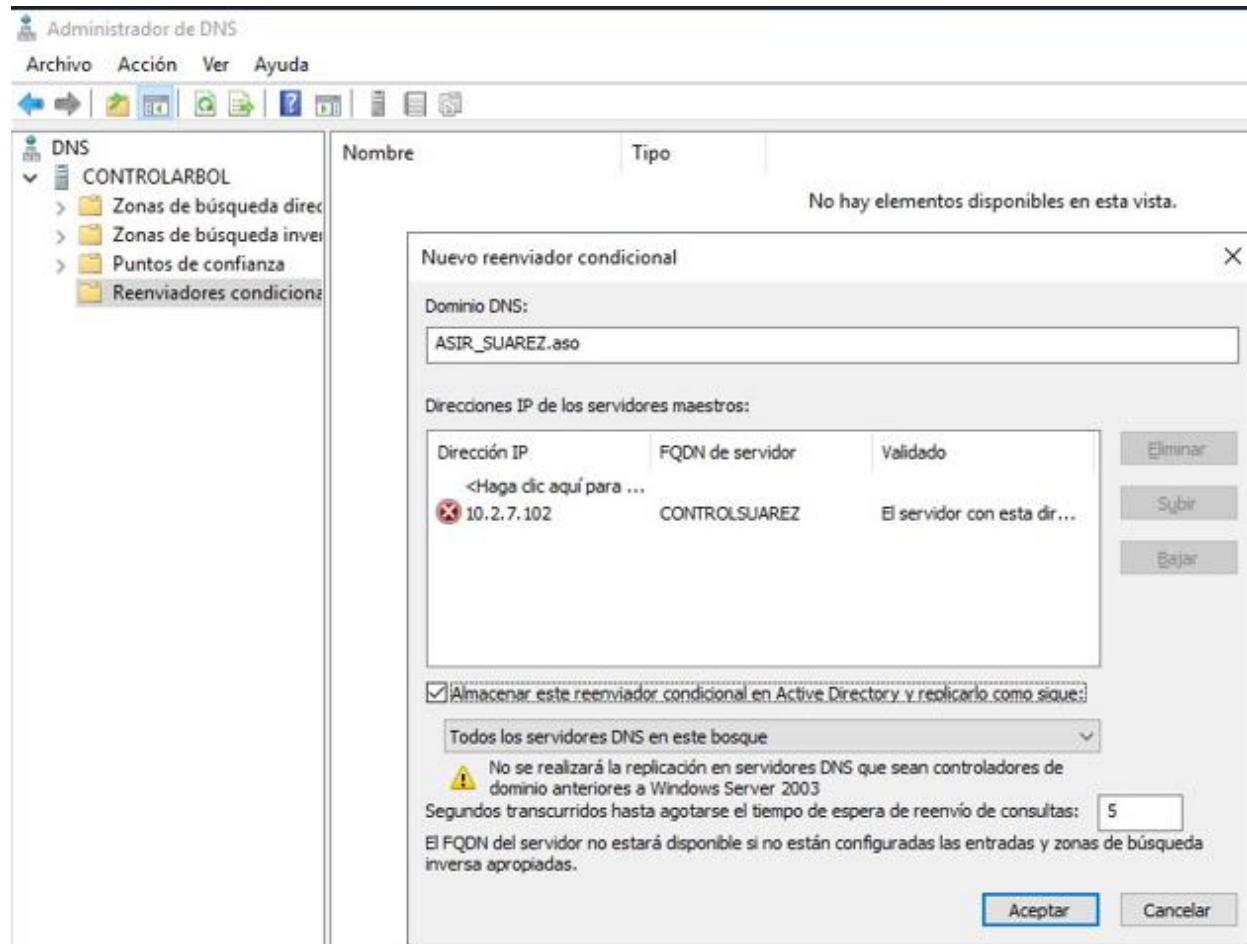
Una vez reiniciada la máquina, podemos ver que se ha creado el dominio.

Nombre de equipo	CONTROLARBOL
Dominio	ENCINA.aso
Firewall de Windows Defender	Privado: Activado
Administración remota	Habilitado
Escritorio remoto	Deshabilitado
Formación de equipos de NIC	Deshabilitado
Ethernet	10.2.7.116

- 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.**

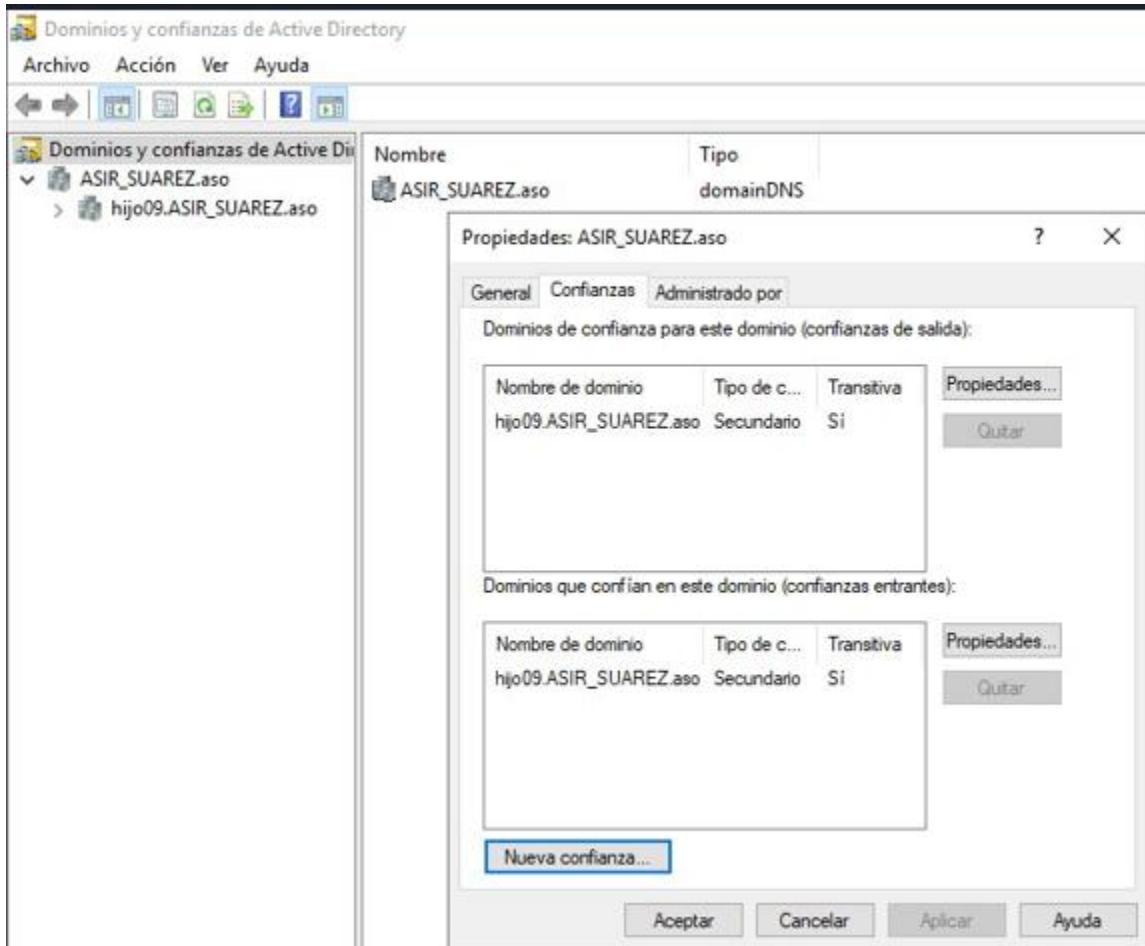


Para comprobar que funciona se hace ping:

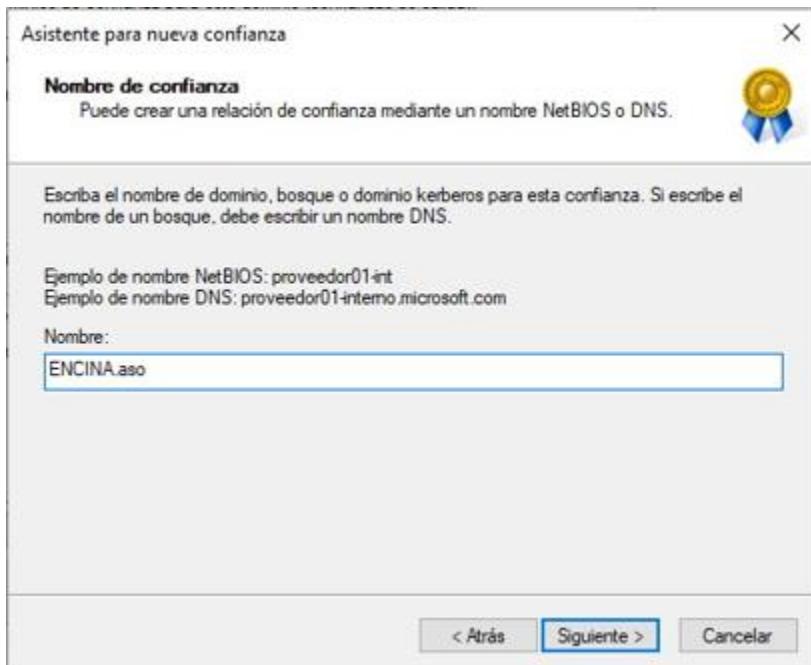
```
C:\Users\Administrador>ping ENCINA.aso

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
```

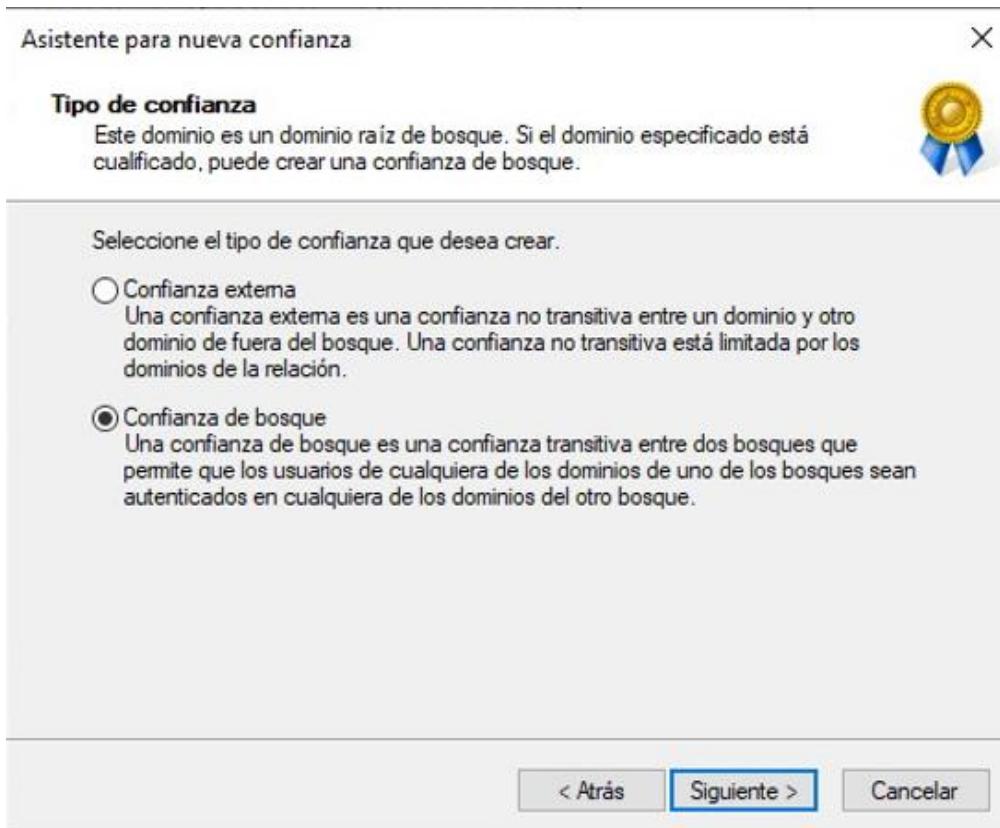
El siguiente paso es establecer la **relación de confianza**. Para ello: **Herramientas → Dominios y confianzas de Active Directory**. Y vamos a propiedades del dominio y luego a la pestaña **Confianzas** y ahí en **Nueva Confianza**. Hay que tener en cuenta que solo hace falta establecerlo en uno de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



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



Tipo de Confianza: de Bosque.



Dirección de confianza: Bidireccional.

Asistente para nueva confianza X

**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 X

**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 X

**Nombre de usuario y contraseña**

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



Dominio especificado: ENCINA.aso

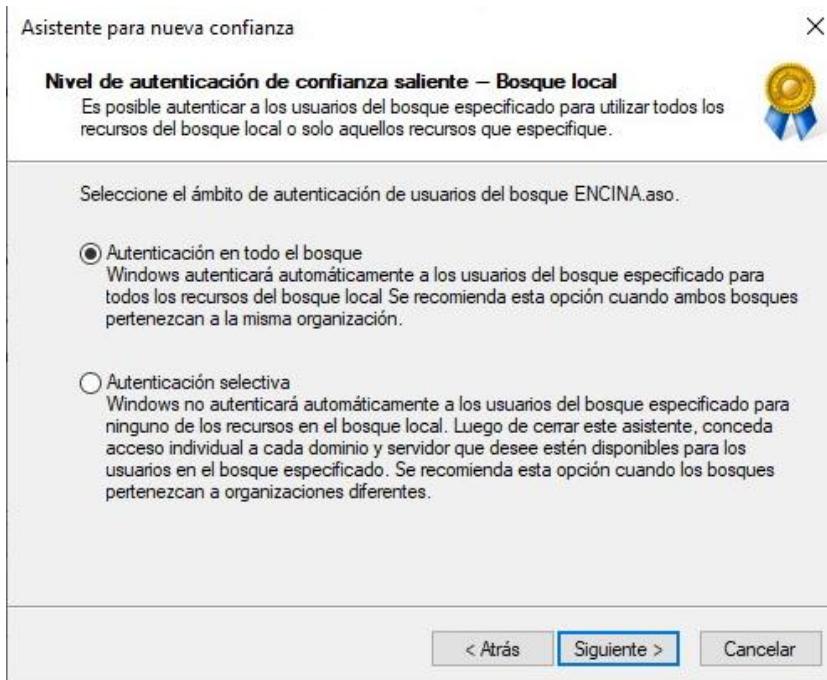
Escriba el nombre de usuario y la contraseña de una cuenta que tiene privilegios de administrador en el dominio especificado.

Usuario:  ▼

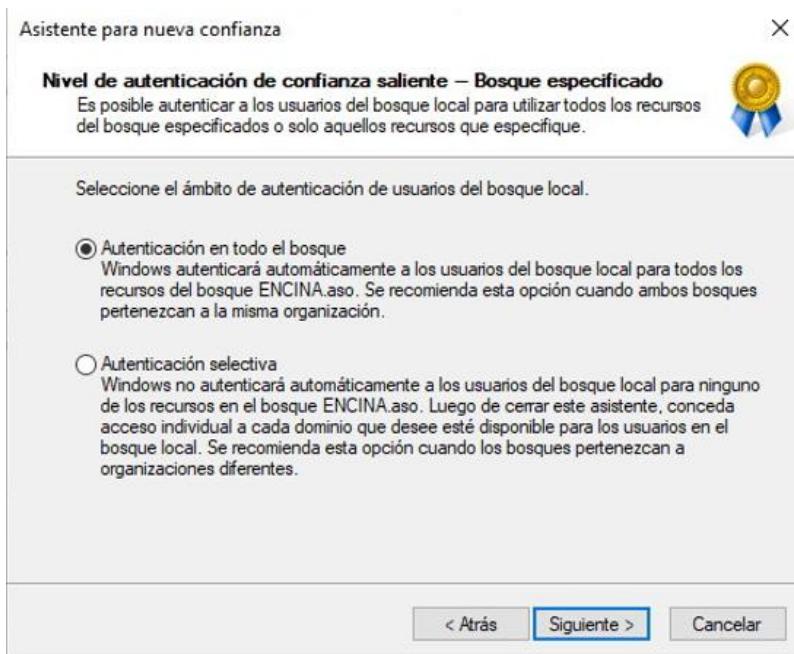
Contraseña:

[< Atrás](#) Siguiente > [Cancelar](#)

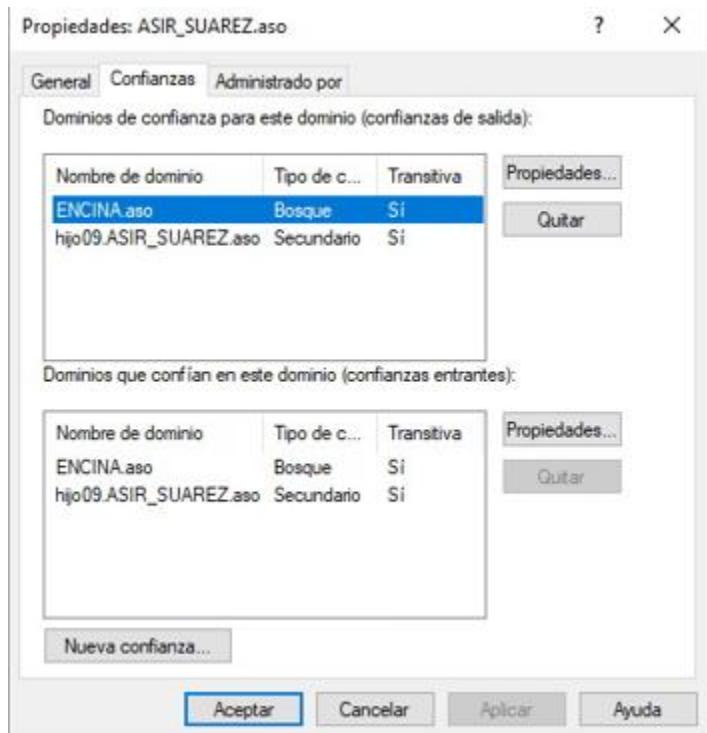
## Nivel de autenticación de confianza saliente – Bosque local: **Autenticación en todo el bosque.**



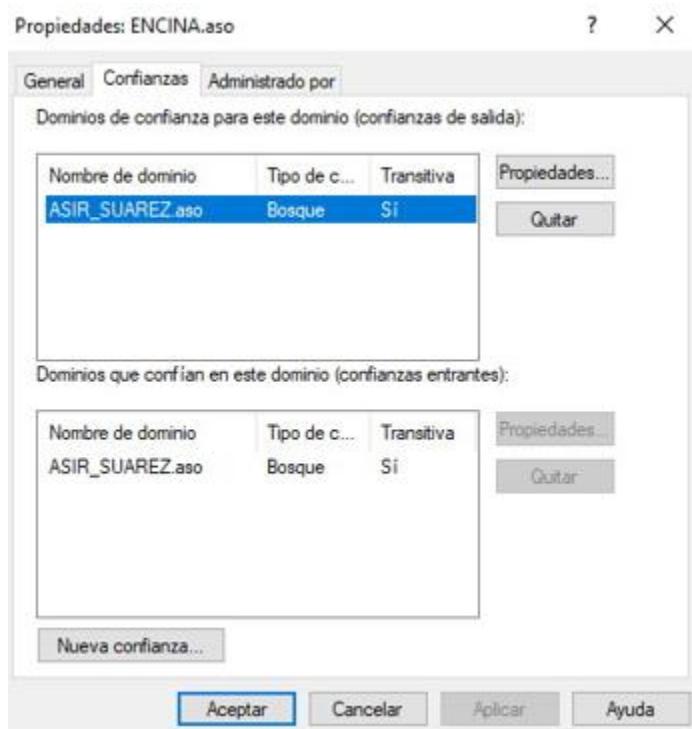
## Nivel de autenticación de confianza saliente – Bosque especificado: **Autenticación en todo el bosque.**



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



En el otro dominio se crea automáticamente.

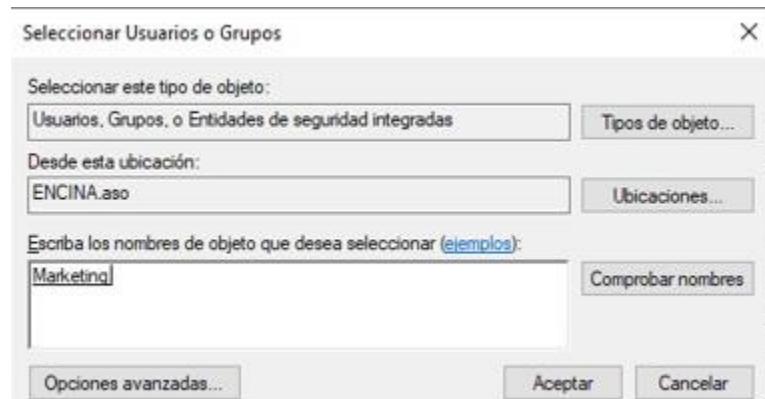
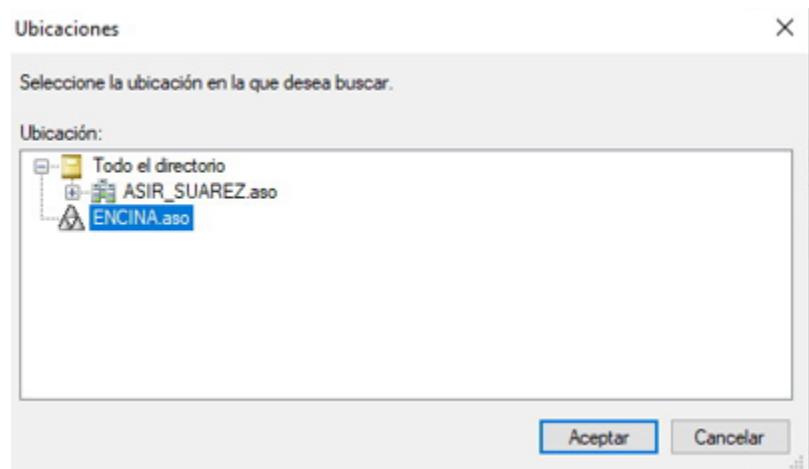


- c) Comprueba la autenticación cruzada creando usuarios en ambos bosques y validando el acceso a recursos compartidos.

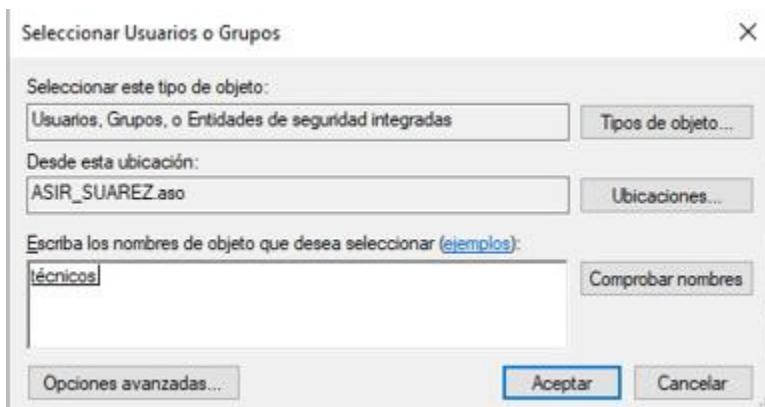
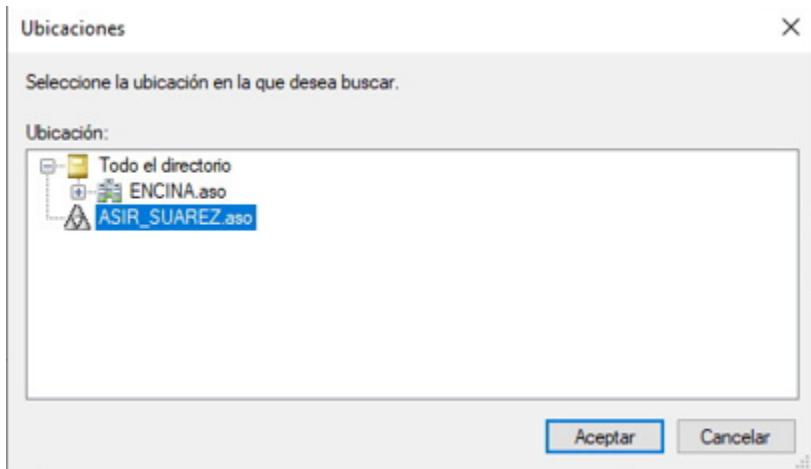
En **Encina.aso** hemos creado un usuario que pertenece al grupo **Marketing**.

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the tree structure of the domain, including 'ENCINA.aso' which is expanded to show 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Users', and 'Prueba01'. In the center, a table lists two objects: 'Marketing' (Type: Grupo de seguimiento) and 'Pedro PGM.' (Type: Usuario). A context menu is open over the 'Marketing' object, and a sub-menu window titled 'Propiedades: Marketing' is displayed. This window has tabs for 'General', 'Miembros', 'Miembro de', and 'Administrado por'. The 'Miembros' tab is selected, showing a list of members with one entry: 'Pedro PGM.' under 'ENCINA.aso/Prueba01'. At the bottom of the window are buttons for 'Agregar...', 'Quitar', 'Aceptar', 'Cancelar', and 'Aplicar'. The 'Aceptar' button is highlighted with a blue border.

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

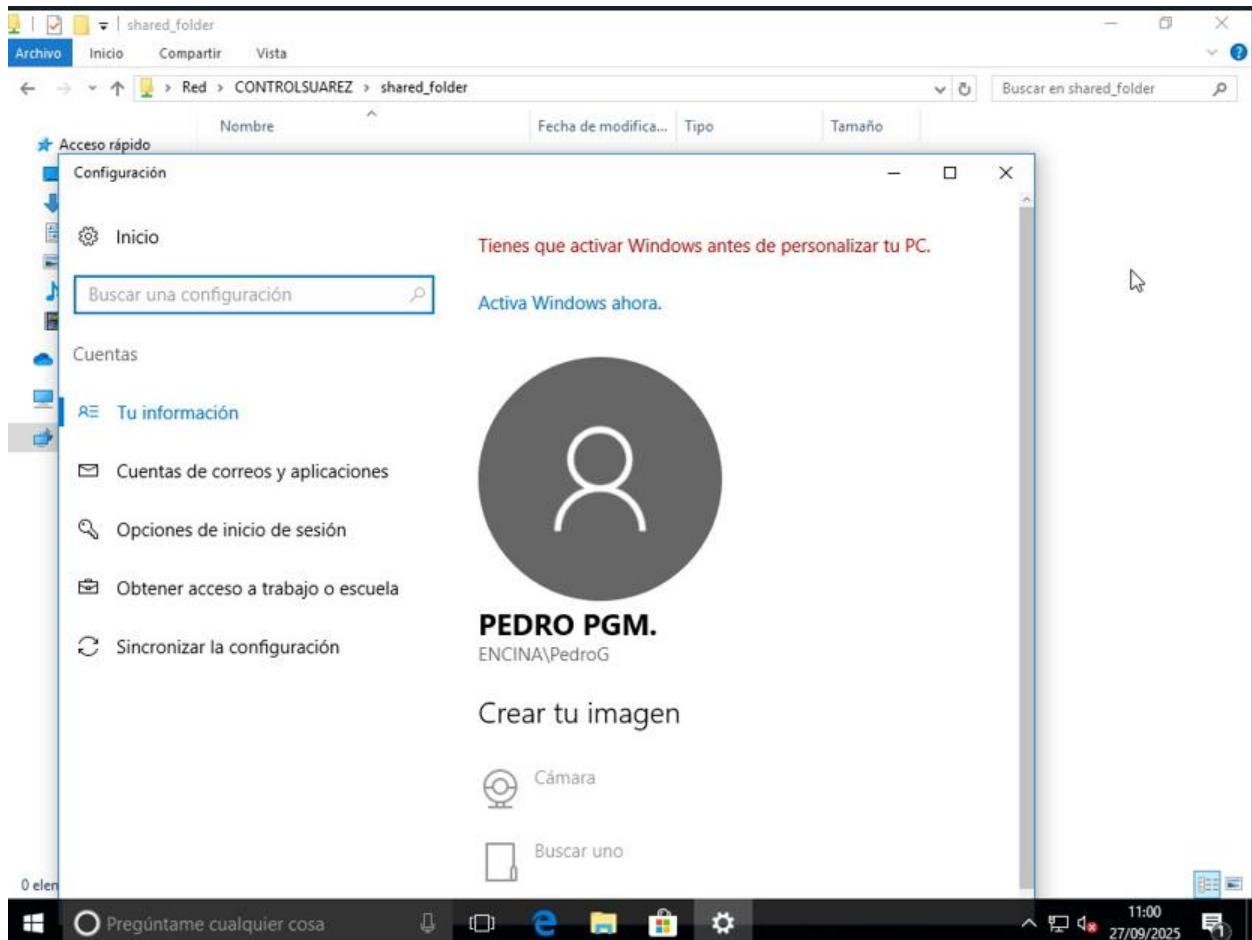
La carpeta está compartida.

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

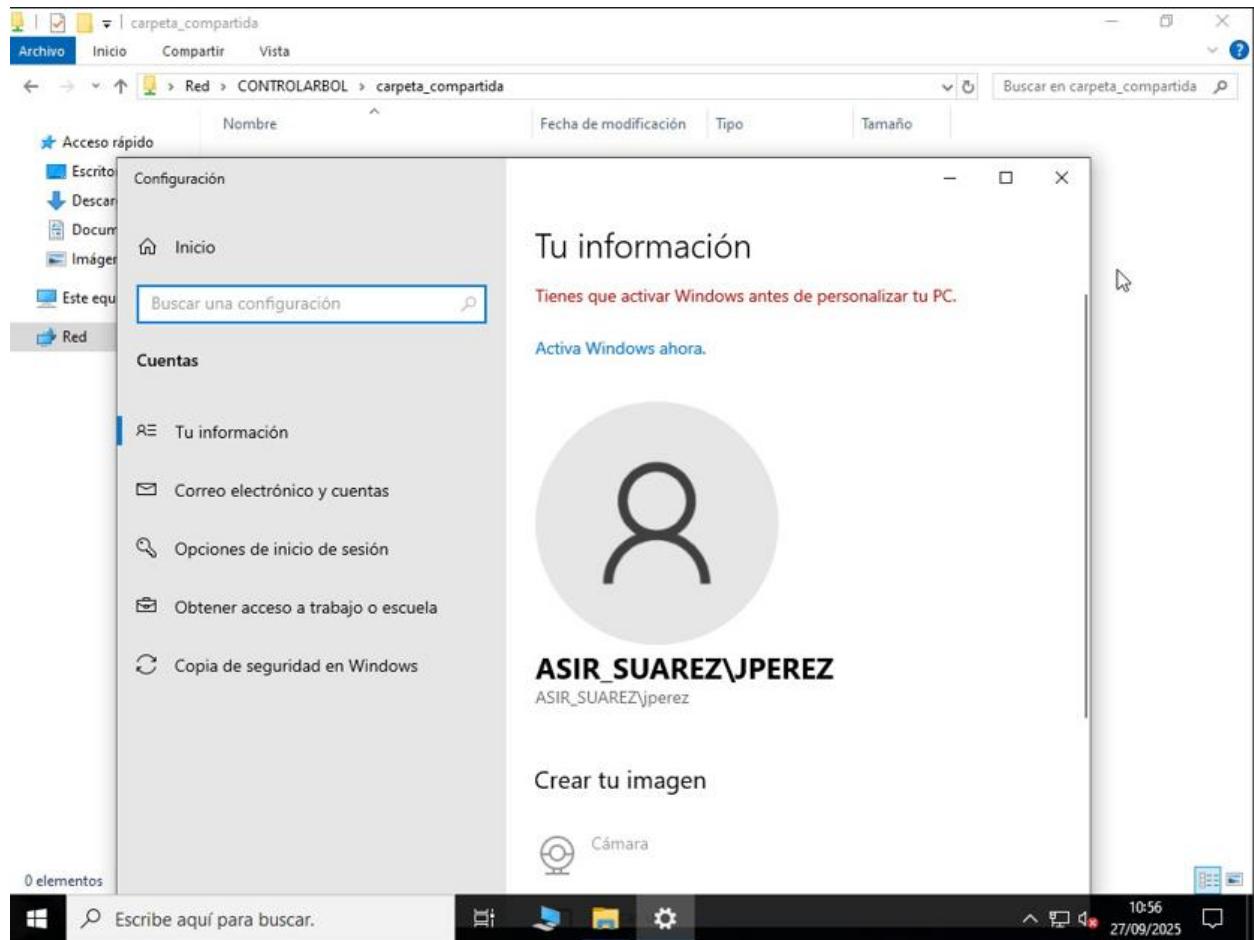


- d) Para comprobar que funciona, intenta acceder a recursos compartidos entre dominios con diferentes usuarios.

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



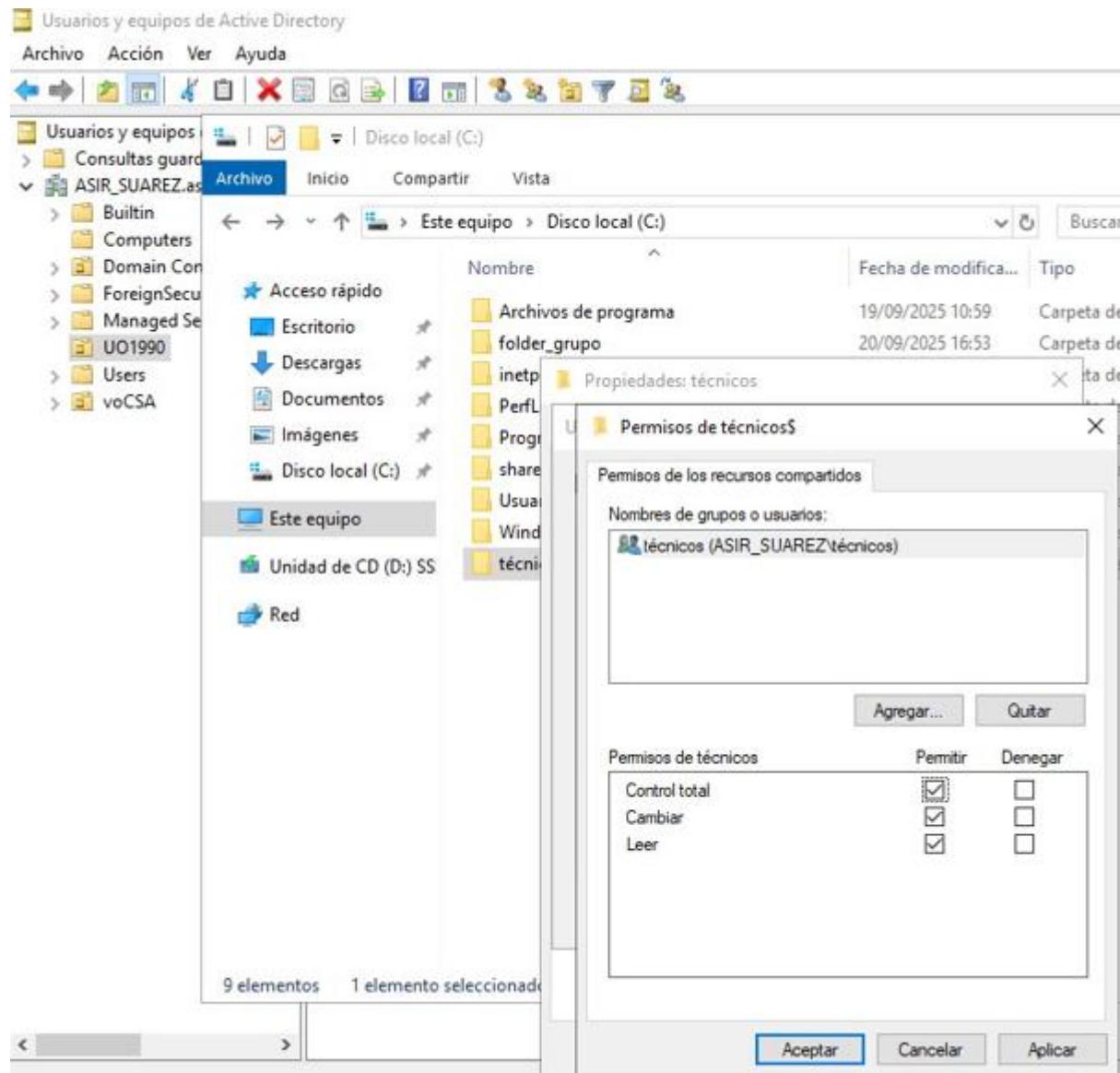
Y al usuario **jperez** de **ASIR\_SUAREZ.aso** acceder al que está en **ENCINA.aso**



## 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).

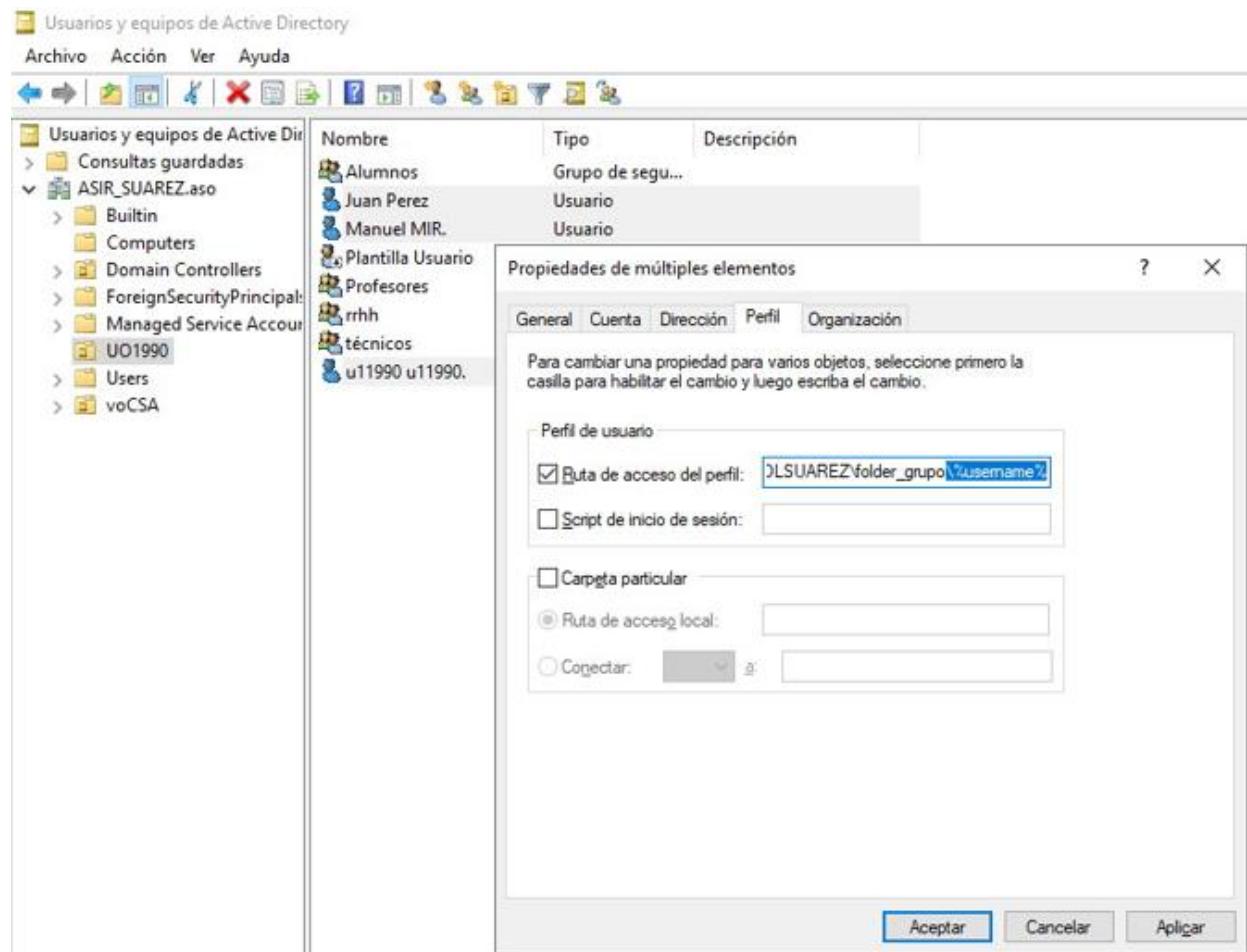


**b) Modifica las propiedades de varios usuarios en Active Directory Users and Computers para que usen perfiles móviles.**

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:

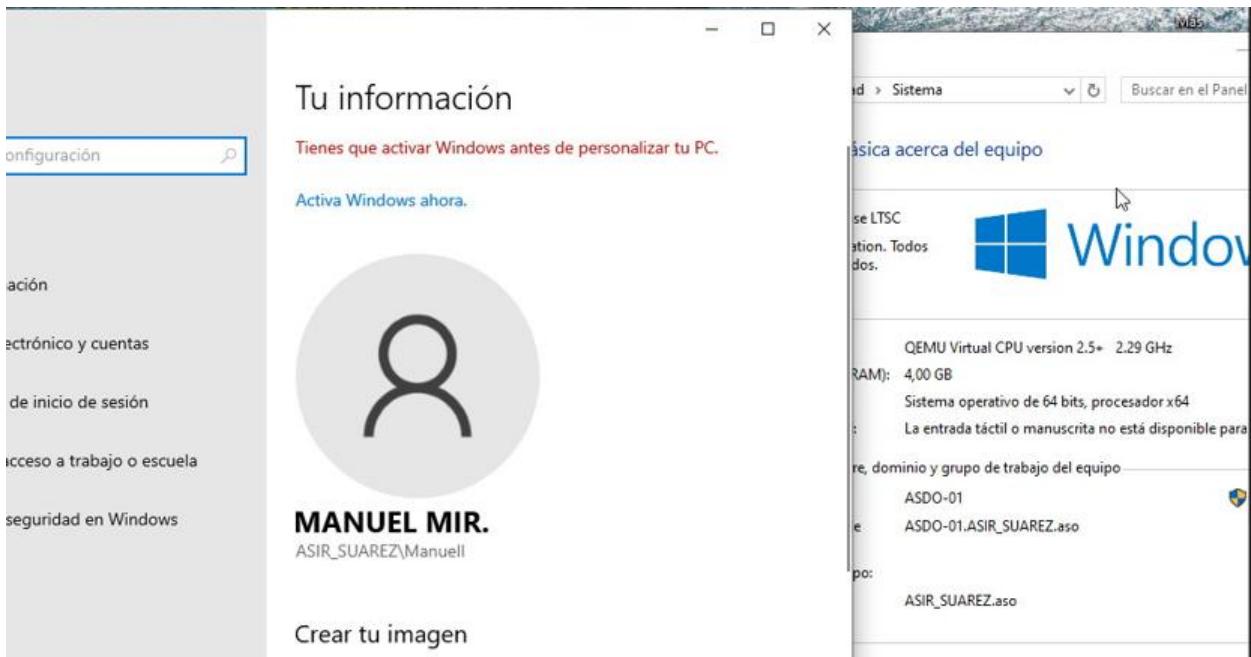
[\\Nombre\\_del\\_servidor\ruta\%username%](\\Nombre_del_servidor\ruta\%username%)

Esto generará una carpeta para cada usuario cuando inicien sesión.

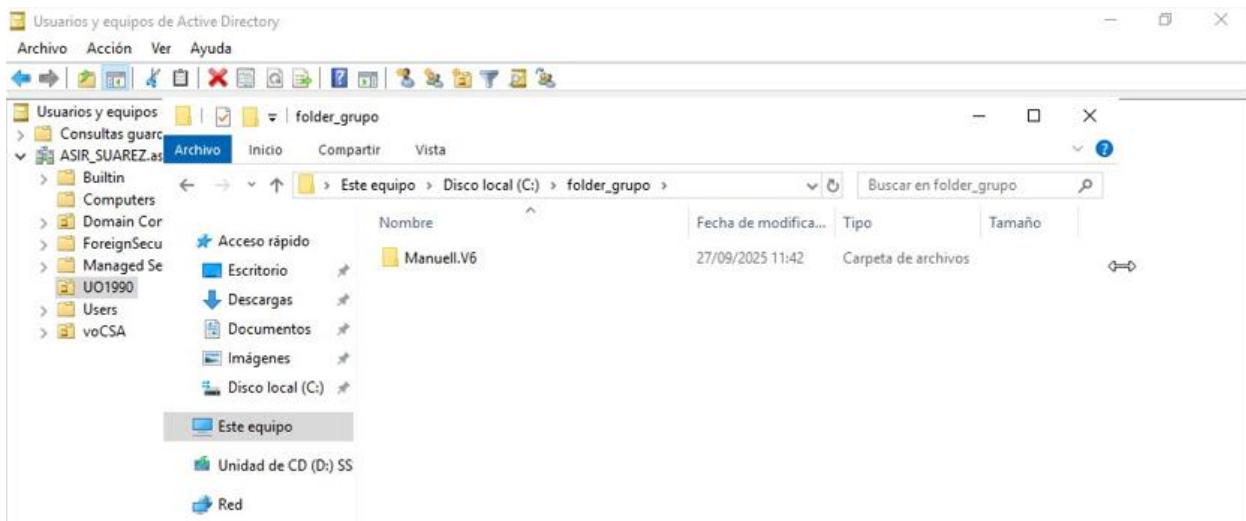


**c) Inicia sesión con los usuarios en diferentes equipos unidos al dominio y comprueba.**

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



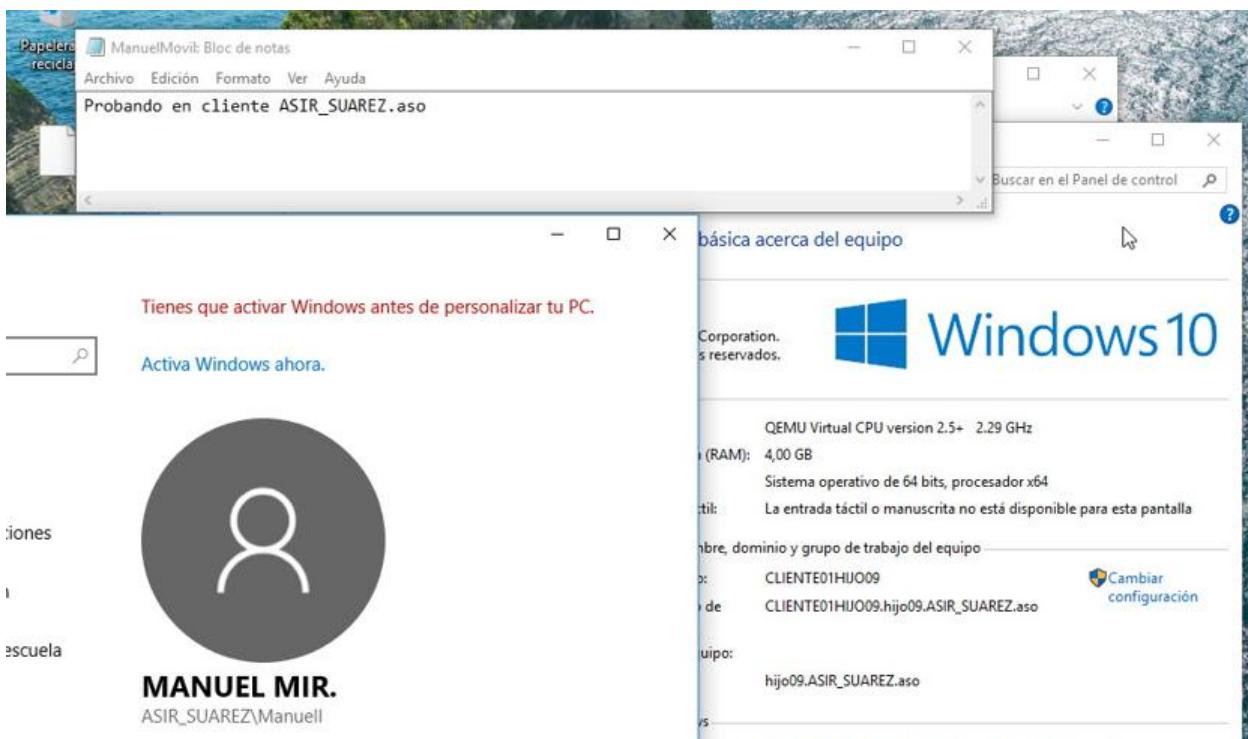
Al instante se crea la carpeta que contiene el perfil móvil.



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.

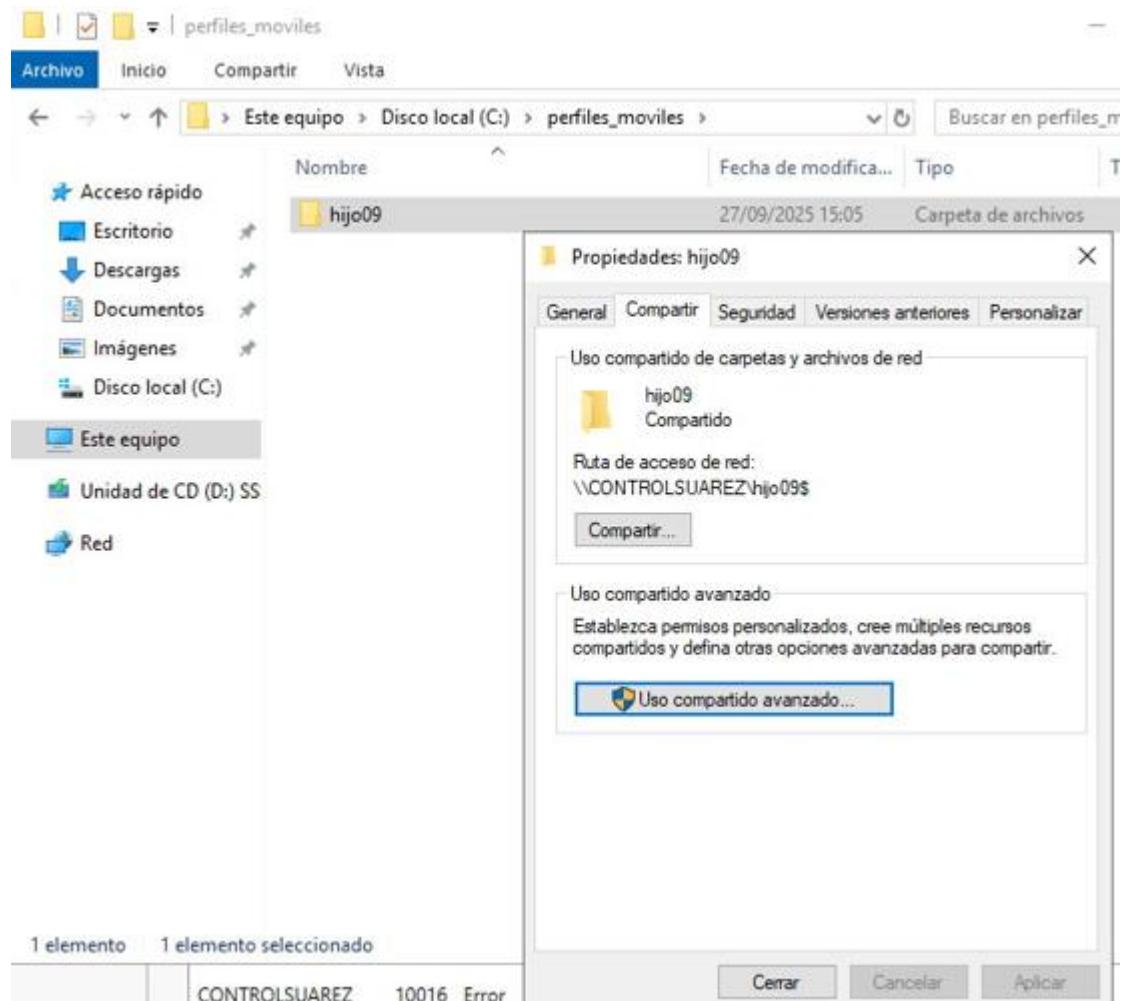


## **5) Escenario avanzado de pruebas.**

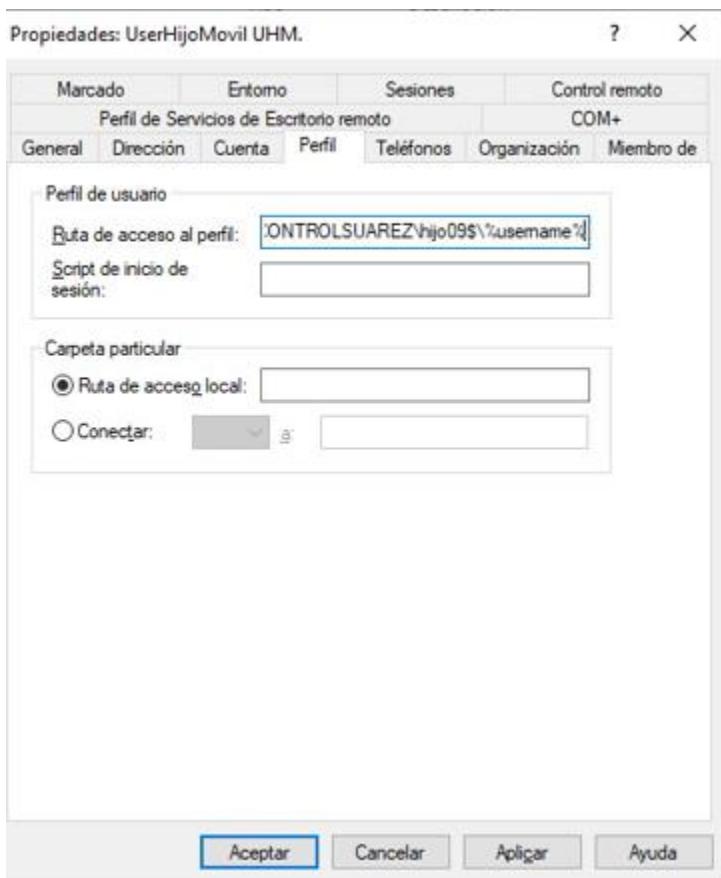
- a) Crea un usuario en el subdominio y configura su perfil móvil en el dominio principal. Verifica si puede acceder desde equipos unidos al subdominio.

Usuarios y equipos de Active Directory			
	Nombre	Tipo	Descripción
Usuarios y equipos de Active Dir	Administrador	Usuario	Cuenta integrada para la...
> Consultas guardadas	Administradores clave	Grupo de segu...	Los miembros de este gr...
hijo09.ASIR_SUAREZ.aso	Admins. del dominio	Grupo de segu...	Administradores design...
> Builtin	Controladores de dominio	Grupo de segu...	Todos los controladores ...
> Computers	Controladores de dominio clonables	Grupo de segu...	Se pueden clonar los mi...
> Domain Controllers	Controladores de dominio de sólo lec...	Grupo de segu...	Los miembros de este gr...
> ForeignSecurityPrincipal	DnsAdmins	Grupo de segu...	Grupo de administrador...
> Managed Service Accou	DnsUpdateProxy	Grupo de segu...	Clientes DNS que tienen...
Users	Equipos del dominio	Grupo de segu...	Todas los servidores y es...
	Grupo de replicación de contraseña R...	Grupo de segu...	Los miembros de este gr...
	Grupo de replicación de contraseña R...	Grupo de segu...	Los miembros de este gr...
	Invitado	Usuario	Cuenta integrada para el...
	Invitados del dominio	Grupo de segu...	Todos los invitados del ...
	Propietarios del creador de directivas ...	Grupo de segu...	Los miembros de este gr...
	Protected Users	Grupo de segu...	Los miembros de este gr...
	Publicadores de certificados	Grupo de segu...	Los miembros de este gr...
	Servidores RAS e IAS	Grupo de segu...	Los servidores de este gr...
	User01HIJO09 UH.	Usuario	
	UserHijoMovil UHM.	Usuario	
	Usuarios del dominio	Grupo de segu...	Todos los usuarios del d...

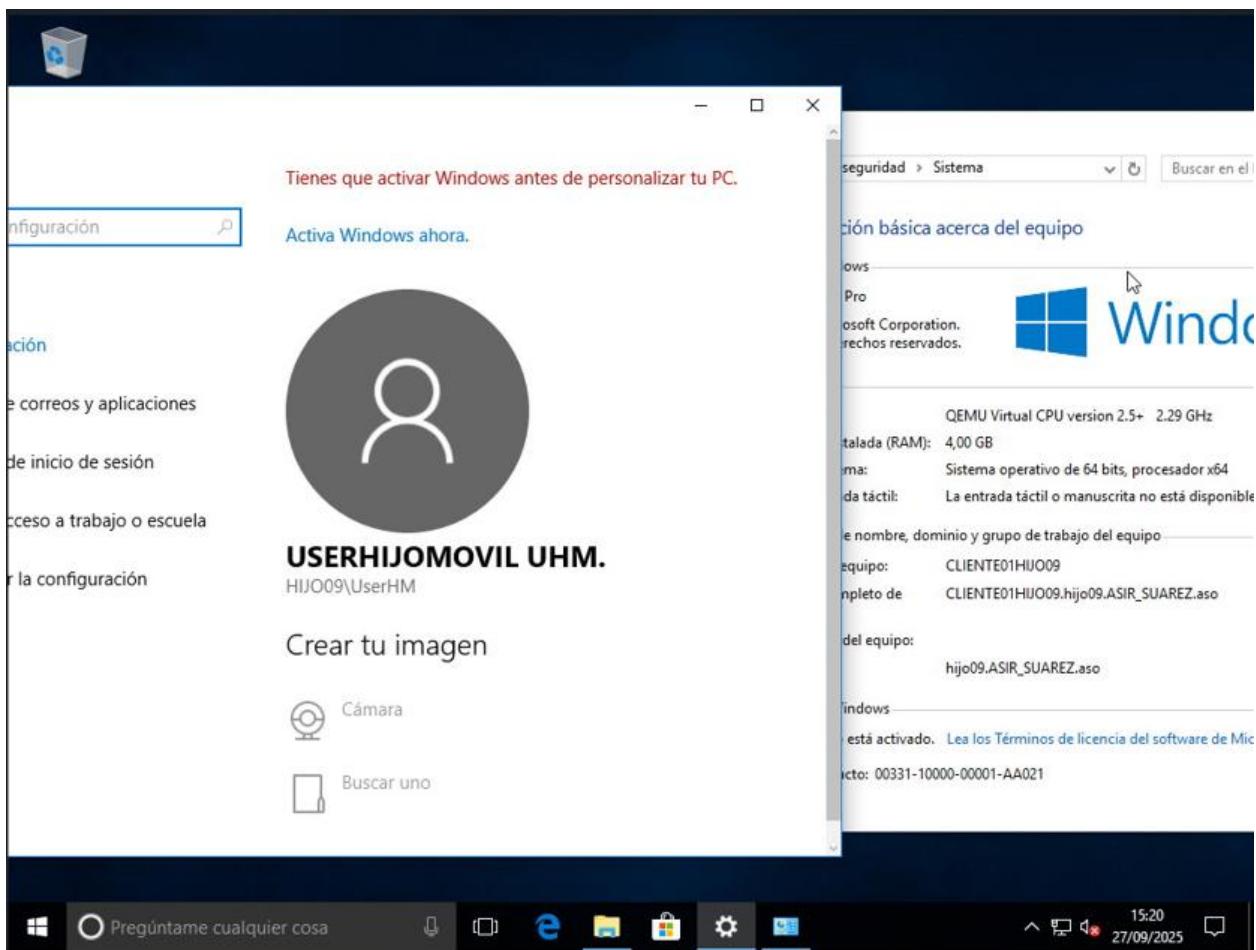
Creamos una carpeta compartida en el Controlador del Dominio Principal donde se almacenarán las carpetas de los perfiles.



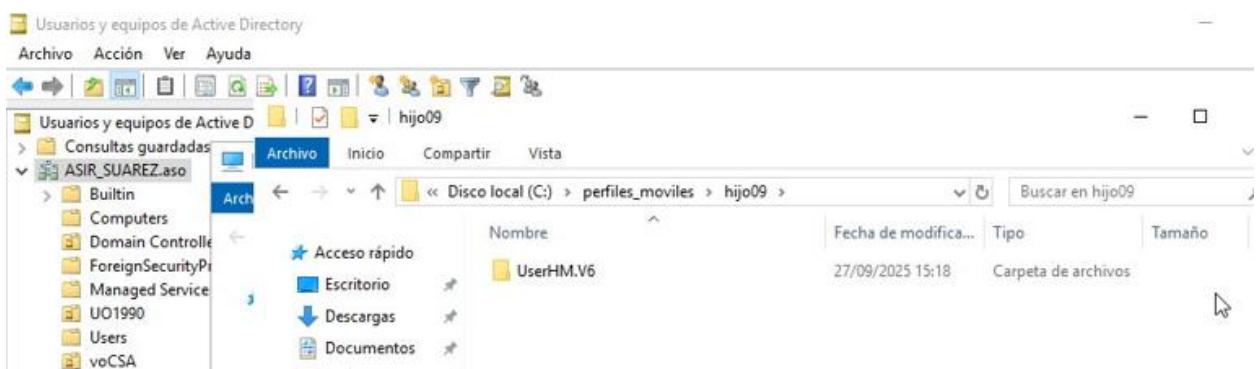
Establecemos la **Ruta del Perfil** en la cuenta de usuario:



Iniciamos sesión con el usuario en un cliente del Subdominio.

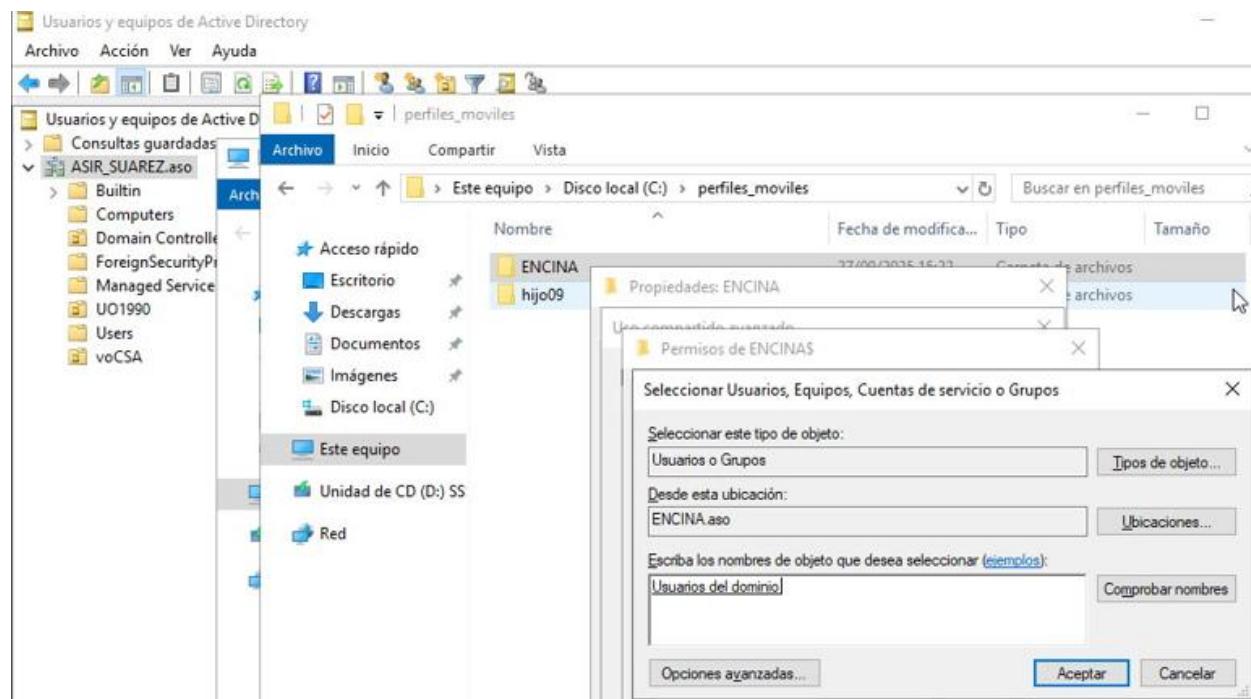


La carpeta se crea en el Controlador.



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

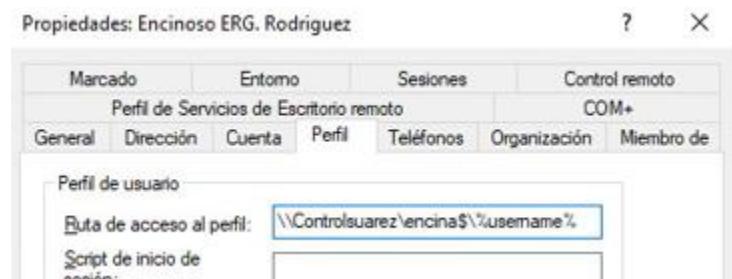
En el Controlador del Dominio Principal creamos una carpeta para los **Usuarios del dominio de Encina.aso**



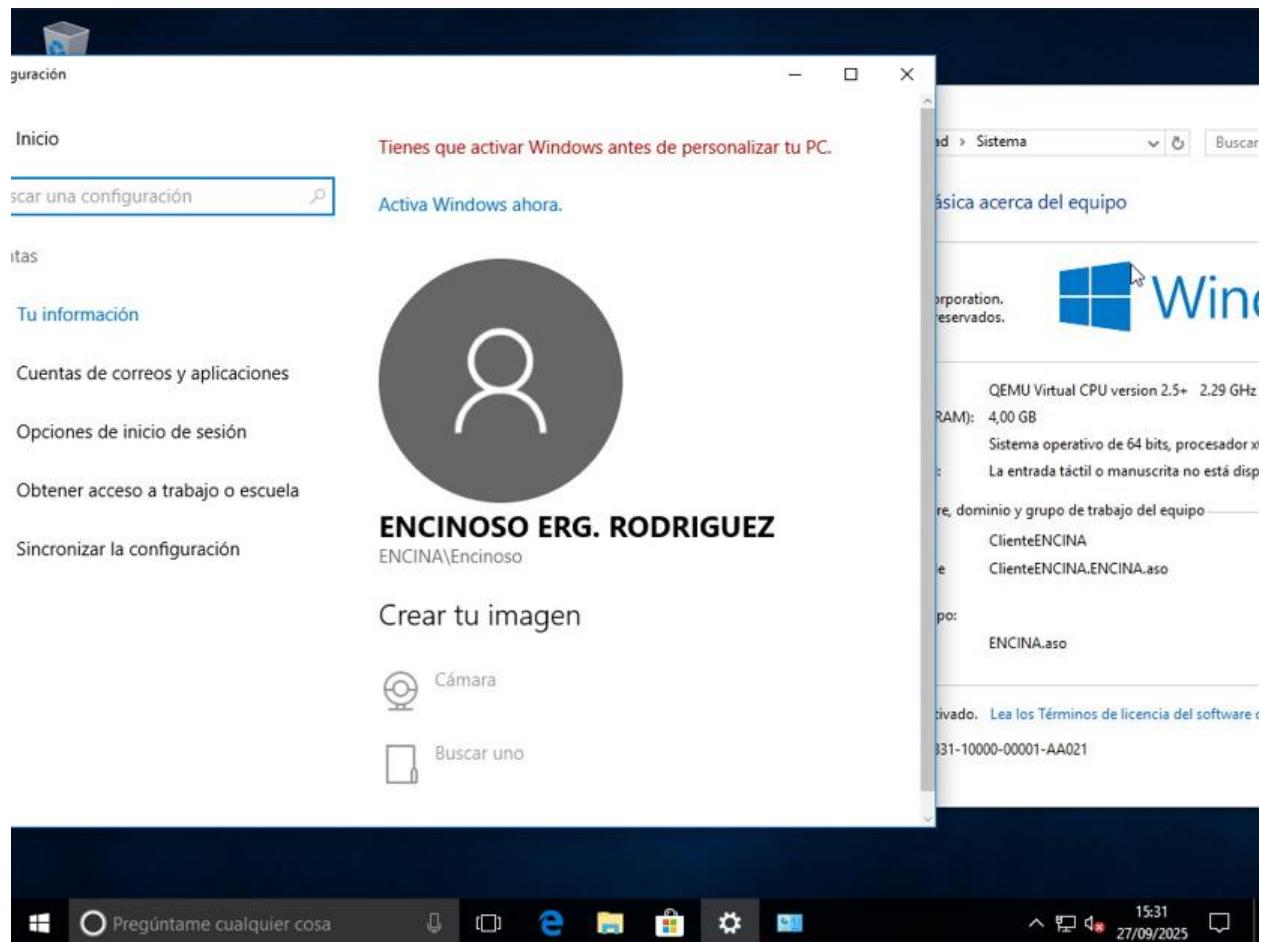
Luego en **Encina.aso** creamos al usuario **Encinoso**.

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la...
Administradores clave	Grupo de segu...	Los miembros de este gr...
Administradores clave de la organización	Grupo de segu...	Los miembros de este gr...
Administradores de empresas	Grupo de segu...	Administradores design...
Administradores de esquema	Grupo de segu...	Administradores design...
Admins. del dominio	Grupo de segu...	Administradores design...
Controladores de dominio	Grupo de segu...	Todos los controladores ...
Controladores de dominio clonables	Grupo de segu...	Se pueden clonar los mi...
Controladores de dominio de sólo lectura	Grupo de segu...	Los miembros de este gr...
DnsAdmins	Grupo de segu...	Grupo de administrador...
DnsUpdateProxy	Grupo de segu...	Clientes DNS que tienen...
Encinoso ERG. Rodriguez	Usuario	
Enterprise Domain Controllers de sólo lectura	Grupo de segu...	Los miembros de este ar...

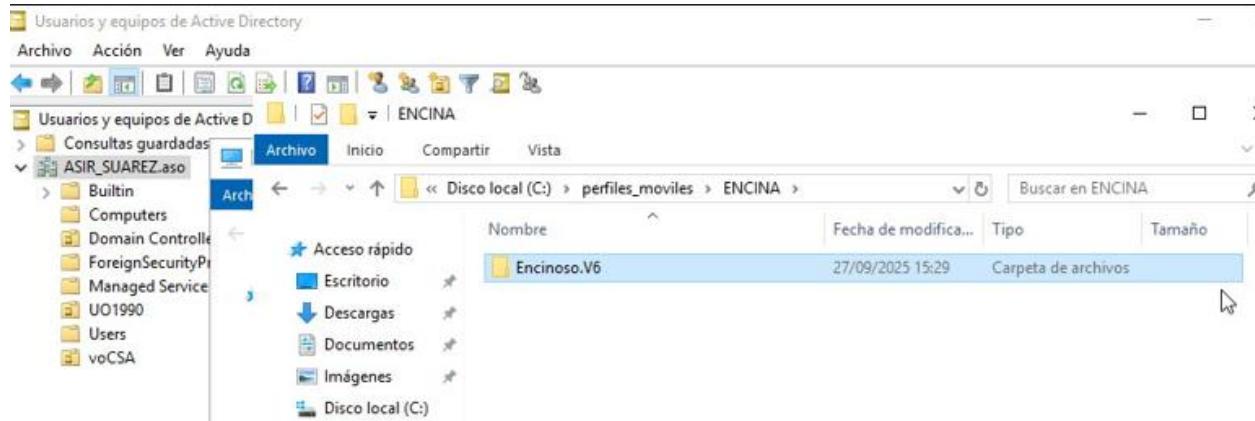
Establecemos su ruta de Perfil Móvil.



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



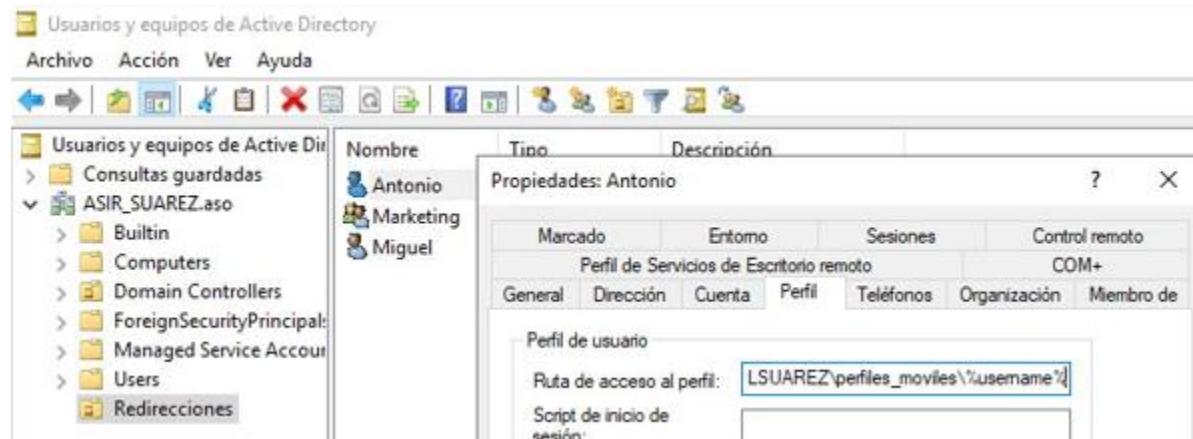
Vemos como se ha creado la carpeta del perfil móvil en el Controlador de ASIR\_SUAREZ.aso



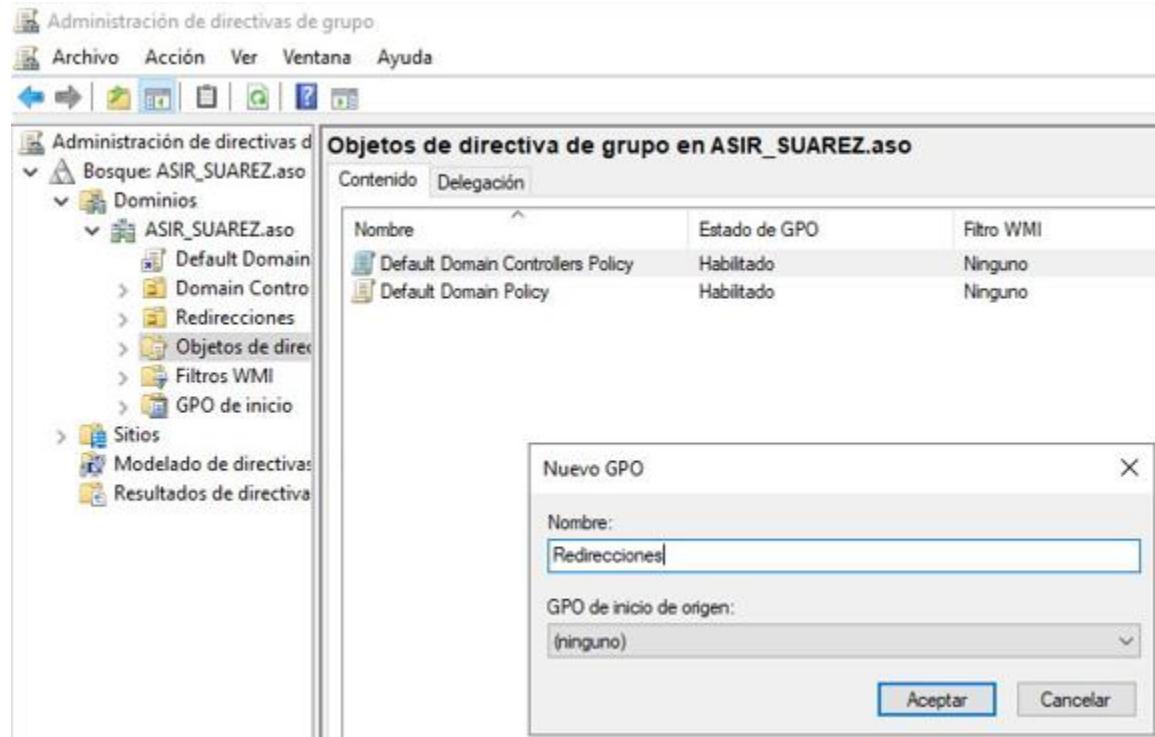
- c) Establece políticas de grupo (GPO) para redirigir carpetas (Documentos, Escritorio) hacia carpetas de red y comprueba que funcionan junto con los perfiles móviles.

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

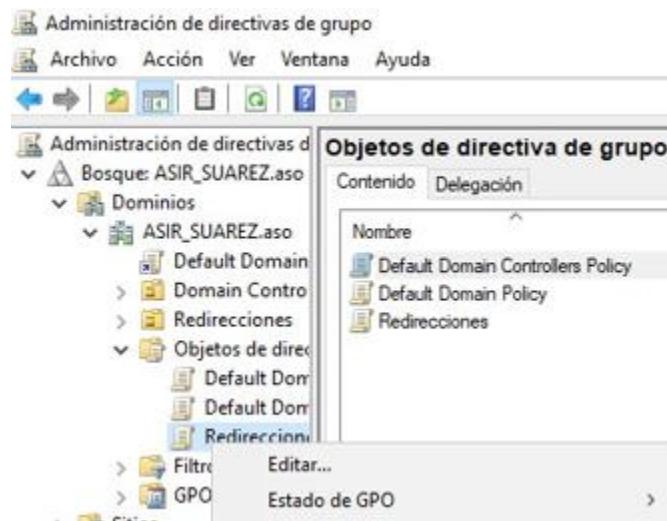
**Redirecciones**. Donde vamos a colocar al grupo **Marketing** y a dos de sus usuarios. Como hemos hecho en actividades anteriores, debemos configurar la carpeta **profiles\_móviles** como un recurso compartido al cual los usuarios puedan tener acceso (ya sea por grupos específicos o con “Usuarios del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

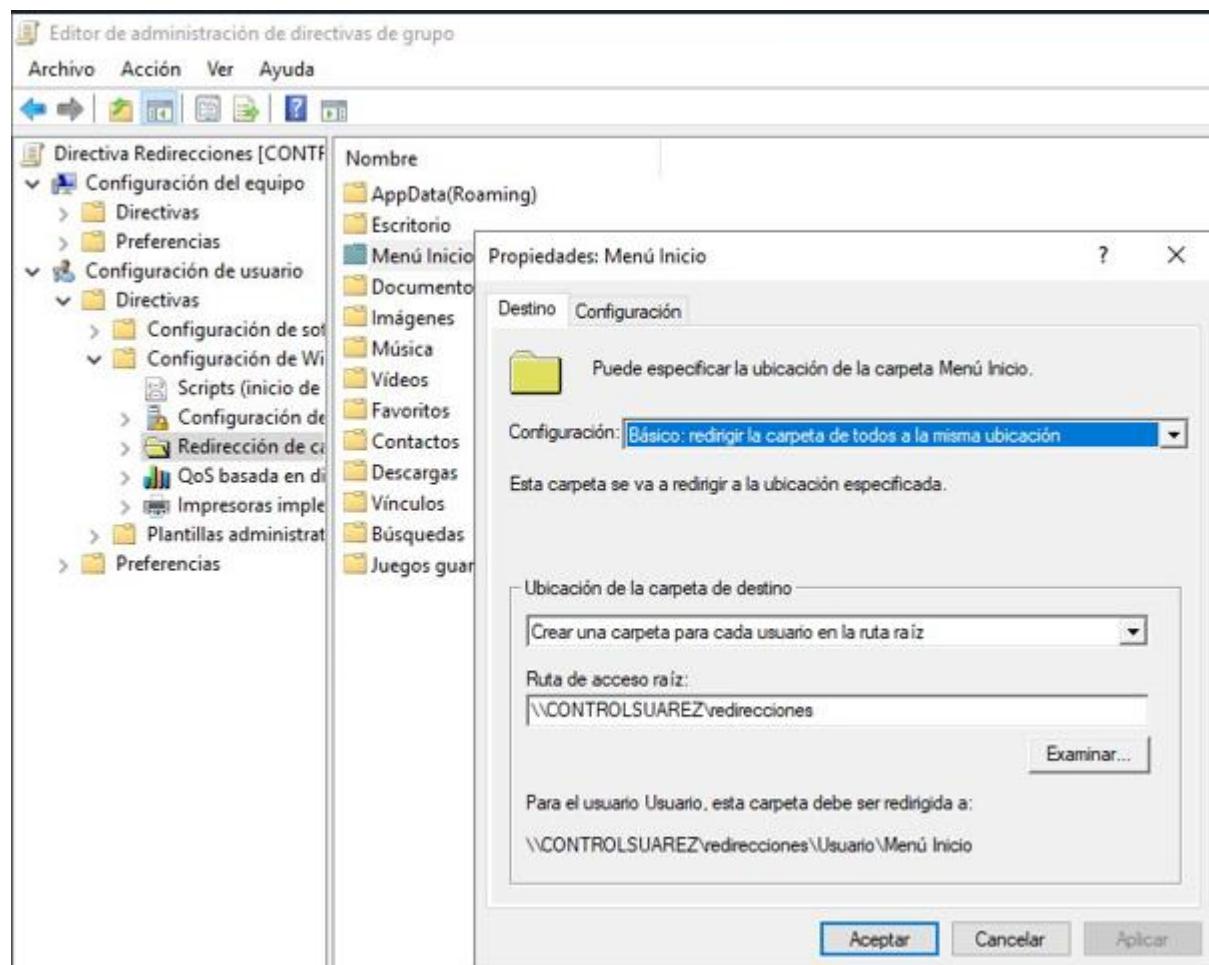


Una vez creada, la buscamos dentro de **Objetos de directiva de grupo** y le damos a **Editar...**

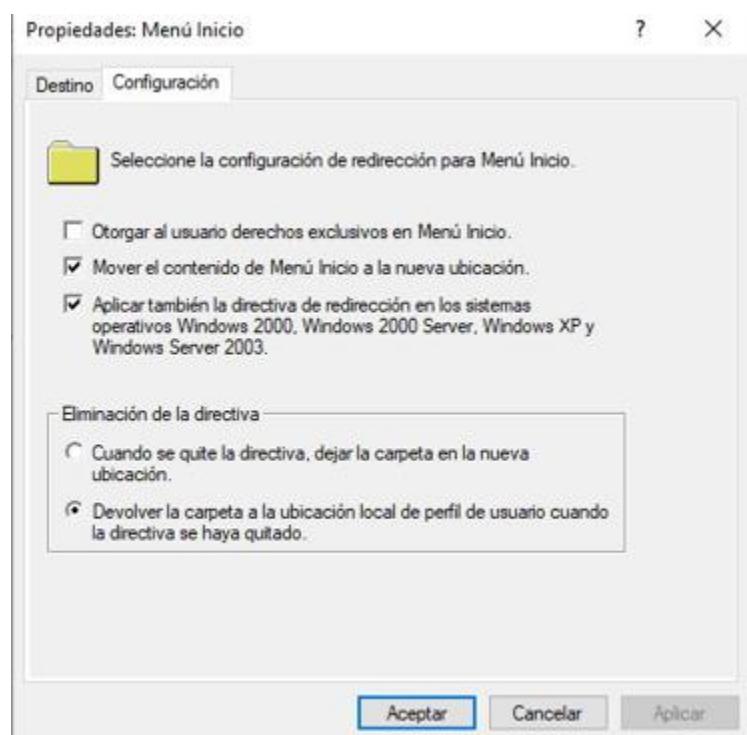


Navegamos: **Configuración de usuario → Directivas → Configuración de Windows → Redirección de carpetas**. Aquí tenemos una selección de carpetas predefinidas del usuario que podemos redirigir. En este caso vamos a usar “Menú inicio” y “Documentos”. La configuración para ambas es la misma.

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)



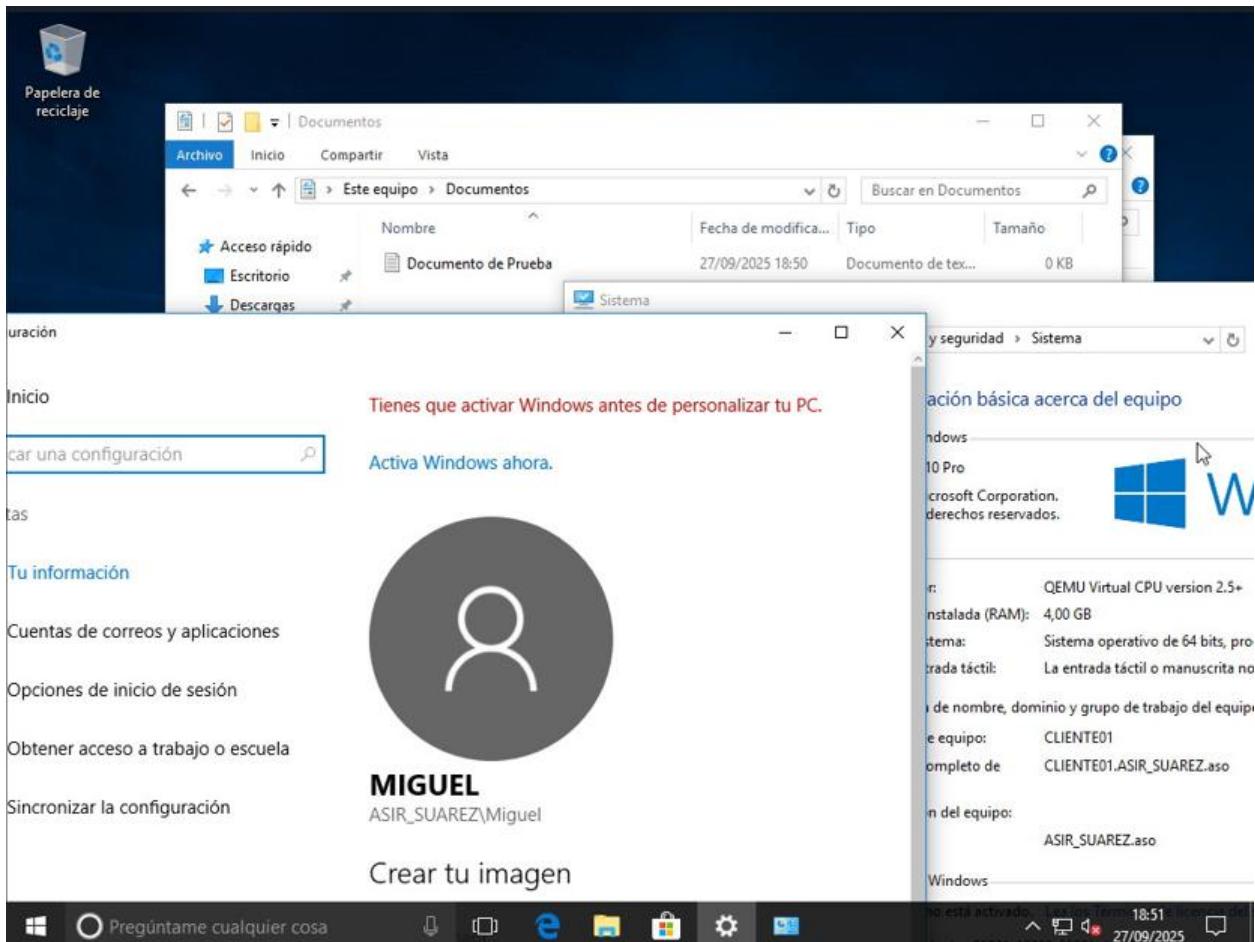
## Pestaña Configuración.



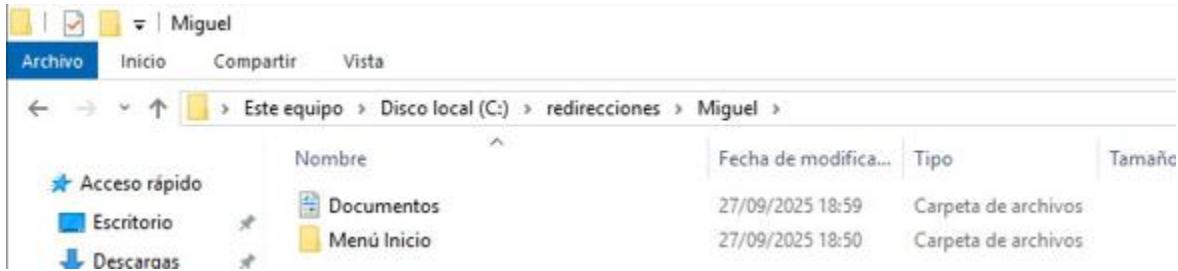
Una vez configurada la GPO, debemos vincularla con la Unidad Organizativa. Para ello seleccionamos la UO y le damos a **Vincular un GPO existente...**



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**.

