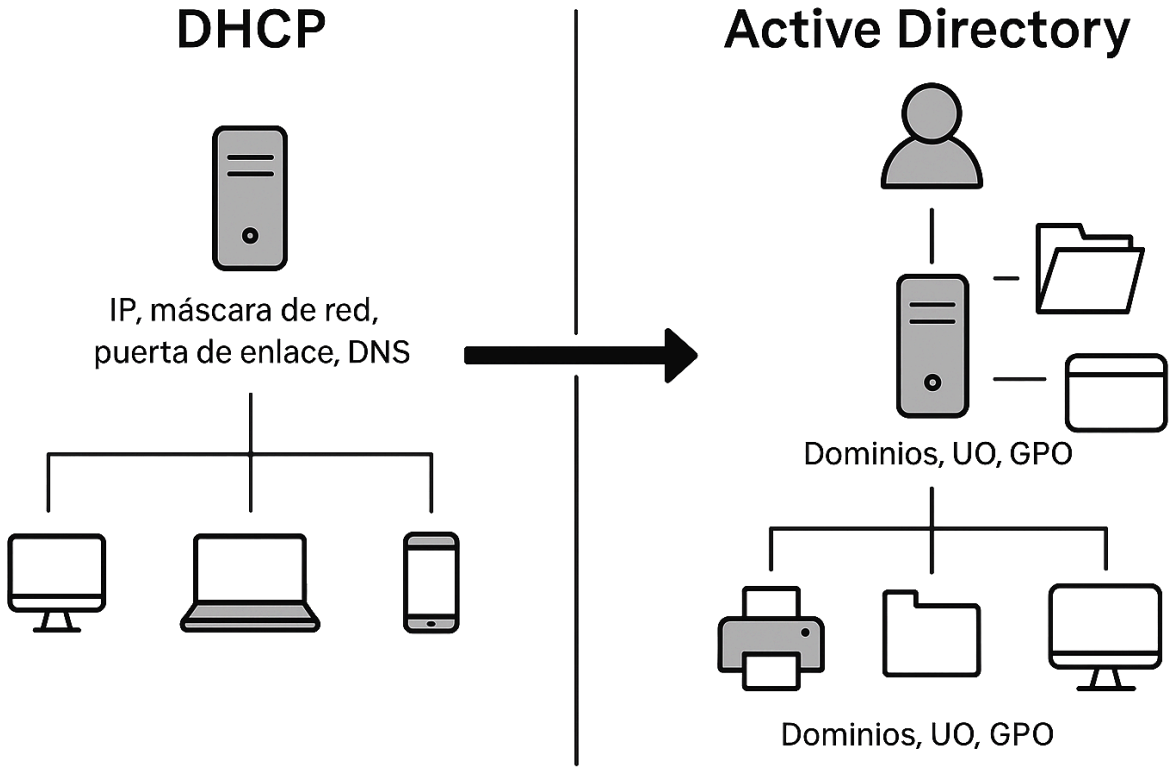
Active Directory y DHCP



Nombre: Sonia Rufino Ruiz
Fecha: 15/10/2025

Índice

Introducción **3**
Protocolo DHCP **3**
Funcionamiento detallado del protocolo 4
Ventajas del uso de DHCP 4
Desventajas y posibles fallas 5
Ejemplos prácticos de implementación 5
Buenas prácticas en la administración de DHCP 5
Active Directory **6**
Concepto 6
Importancia en la administración de redes empresariales 6
Estructura lógica de Active Directory 7
Ventajas principales del uso de AD 7
Componentes adicionales relacionados 8
4. Instalación y configuración de Active Directory en Windows Server **8**
Requisitos previos 8
Instalación del rol AD DS 9
Promoción a controlador de dominio 9
Creación y administración de usuarios y grupos 9
Configuración de políticas de grupo (GPO) 10
Comprobaciones y administración básica 10
Práctica en Virtual Box **11**

Introducción

En el ámbito de las redes informáticas modernas, la automatización y centralización de la administración son factores determinantes para lograr eficiencia, seguridad y escalabilidad. Dos herramientas esenciales para lograrlo en entornos Windows Server son el protocolo DHCP (Dynamic Host Configuration Protocol) y Active directory (AD).

El primero permite asignar directamente direcciones IP automáticamente a los dispositivos de una red, eliminando la necesidad de configuraciones manuales y reduciendo los errores humanos.El segundo proporciona una infraestructura jerárquica que permite administrar usuarios, grupos, equipos y políticas de seguridad de forma centralizada.

Este informe desarrolla en profundidad ambos conceptos, su funcionamiento, ventajas y desventajas, así como un ejemplo práctico de instalación y configuración de Active Directory en un servidor Windows. Con esto se busca comprender no sólo la teoría, sino también la aplicación real en entornos corporativos.

Protocolo DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los dispositivos obtener automáticamente parámetros de configuración IP, como la dirección IP, máscara de subred, puerta de enlace predeterminada y servidores DNS.

Sin DHCP, cada host tendría que configurarse manualmente, lo cual es ineficiente en redes medianas y grandes. DHCP simplifica este proceso al centralizar la administración de direcciones IP en un único servidor.

Funcionamiento detallado del protocolo

El funcionamiento de DHCP se basa en un intercambio de mensajes entre el cliente y el servidor, conocido como DORA (**Discover**, **Offer**, **Request**, **Acknowledge**):

1. **Discover:**
   Cuando un cliente se conecta a la red y no tiene una IP, envía un mensaje broadcast buscando un servidor DHCP disponible.

2. **Offer:**
   El servidor DHCP responde con una oferta de dirección IP, indicando qué IP puede asignar y otros parámetros de red.

3. **Request:**
   El cliente responde aceptando la oferta y solicita formalmente la IP propuesta.

4. **Acknowledge:**
   El servidor confirma la asignación de la IP al cliente, cerrando el proceso de negociación.

Adicionalmente, el DHCP administra tiempos de arrendamiento (lease) para liberar IPs que ya no estén en uso y optimizar el uso de direcciones.

Ventajas del uso de DHCP

- **Automatización**: elimina la necesidad de configuración manual.
- **Centralización**: un único servidor administra toda la red.
- **Reducción de errores**: evita duplicación de IPs y configuraciones incorrectas.
- **Escalabilidad**: ideal para redes con muchos dispositivos.
- **Flexibilidad**: permite cambios rápidos en la infraestructura sin reconfigurar equipos.

Desventajas y posibles fallas

- **Dependencia del servidor:** si el servidor DHCP falla, los nuevos equipos no recibirán IP.
- **Seguridad:** si no está protegido, podría haber servidores DHCP no autorizados (rogue DHCP).
- **Control limitado:** los dispositivos pueden cambiar de IP si no se reserva una fija.
- **Configuración incorrecta:** un error en la red puede afectar a todos los clientes.

Ejemplos prácticos de implementación

- **Escenario 1:** una oficina con 100 estaciones de trabajo y 10 impresoras. Con DHCP, todas las estaciones obtienen automáticamente IP y DNS. Solo las impresoras tienen IPs reservadas para garantizar su localización.
- **Escenario 2:** un laboratorio educativo donde los estudiantes traen sus portátiles. DHCP asigna dinámicamente IPs temporales sin necesidad de soporte técnico.

Buenas prácticas en la administración de DHCP

- Reservar IPs para servidores y dispositivos críticos.
- Definir un rango de IPs adecuado y evitar solapamientos.
- Establecer tiempos de arrendamiento según las necesidades reales.
- Activar registros y monitoreo de actividad DHCP.
- Proteger la red contra servidores DHCP no autorizados.

Active Directory

Concepto

Active Directory (AD) es un servicio de directorio de Microsoft que permite gestionar identidades y recursos en una red Windows de manera centralizada y segura. Su función principal es autenticar usuarios y controlar el acceso a recursos, además de facilitar la administración a gran escala.

Importancia en la administración de redes empresariales

En redes corporativas con decenas o miles de equipos, administrar permisos, accesos y configuraciones de forma individual es inviable. Active Directory permite:

- Controlar cuentas de usuario desde un único punto.
- Aplicar políticas de seguridad uniformes.
- Administrar accesos a carpetas compartidas, impresoras y sistemas internos.
- Integrar otros servicios (DNS, DHCP, GPO, WSUS, etc.) en un ecosistema unificado.

Estructura lógica de Active Directory

- Dominios: son la unidad principal de organización. Agrupan usuarios, grupos y equipos bajo un nombre común (por ejemplo, empresa.local).

- Bosques: conjunto de uno o más dominios que comparten una misma base de datos y relaciones de confianza.

- Unidades Organizativas (OU): subdivisiones dentro de un dominio para organizar usuarios y aplicar políticas específicas.

- Controladores de dominio (DC): servidores que almacenan y replican la base de datos de AD, gestionando autenticaciones.

Ventajas principales del uso de AD

- Administración centralizada de todos los usuarios y equipos.

- Implementación sencilla de políticas de grupo (GPO).

- Seguridad reforzada mediante autenticación Kerberos.

- Alta disponibilidad mediante replicación entre controladores de dominio.

- Integración con otras soluciones Microsoft y de terceros.

Componentes adicionales relacionados

- DNS (Domain Name System): fundamental para el funcionamiento de AD.
- GPO (Group Policy Object): herramienta para aplicar configuraciones de forma masiva.
- LDAP (Lightweight Directory Access Protocol): protocolo utilizado por AD para consultas y autenticaciones.
- FSMO Roles: funciones críticas que coordinan la operación del bosque o dominio.

4. Instalación y configuración de Active Directory en Windows Server

Requisitos previos

- Windows Server instalado (2022, 2019 o 2016).
- Dirección IP estática configurada.
- Nombre de equipo definido.
- DNS configurado adecuadamente (puede instalarse junto con AD).
- Cuenta de administrador local.

Instalación del rol AD DS

1. Abrir el Administrador del Servidor.
2. Seleccionar “Agregar roles y características”.
3. Elegir instalación basada en roles.
4. Marcar “Servicios de dominio de Active Directory (AD DS)”.
5. Continuar e instalar.

Promoción a controlador de dominio

1. Una vez instalado el rol, aparecerá una alerta en el Administrador del Servidor.
2. Seleccionar “Promover este servidor a un controlador de dominio”.
3. Crear un nuevo bosque (por ejemplo, empresa.local).
4. Definir contraseña del modo de recuperación de AD.
5. Completar la instalación y reiniciar.

Creación y administración de usuarios y grupos

- Abrir “Usuarios y equipos de Active Directory”.
- Crear OU para organizar departamentos (Ej: *Ventas*, *TI*, *Recursos Humanos*).
- Crear usuarios dentro de cada OU.
- Asignar contraseñas y pertenencias a grupos.
- Definir permisos de acceso a carpetas compartidas, impresoras y otros recursos.

Configuración de políticas de grupo (GPO)

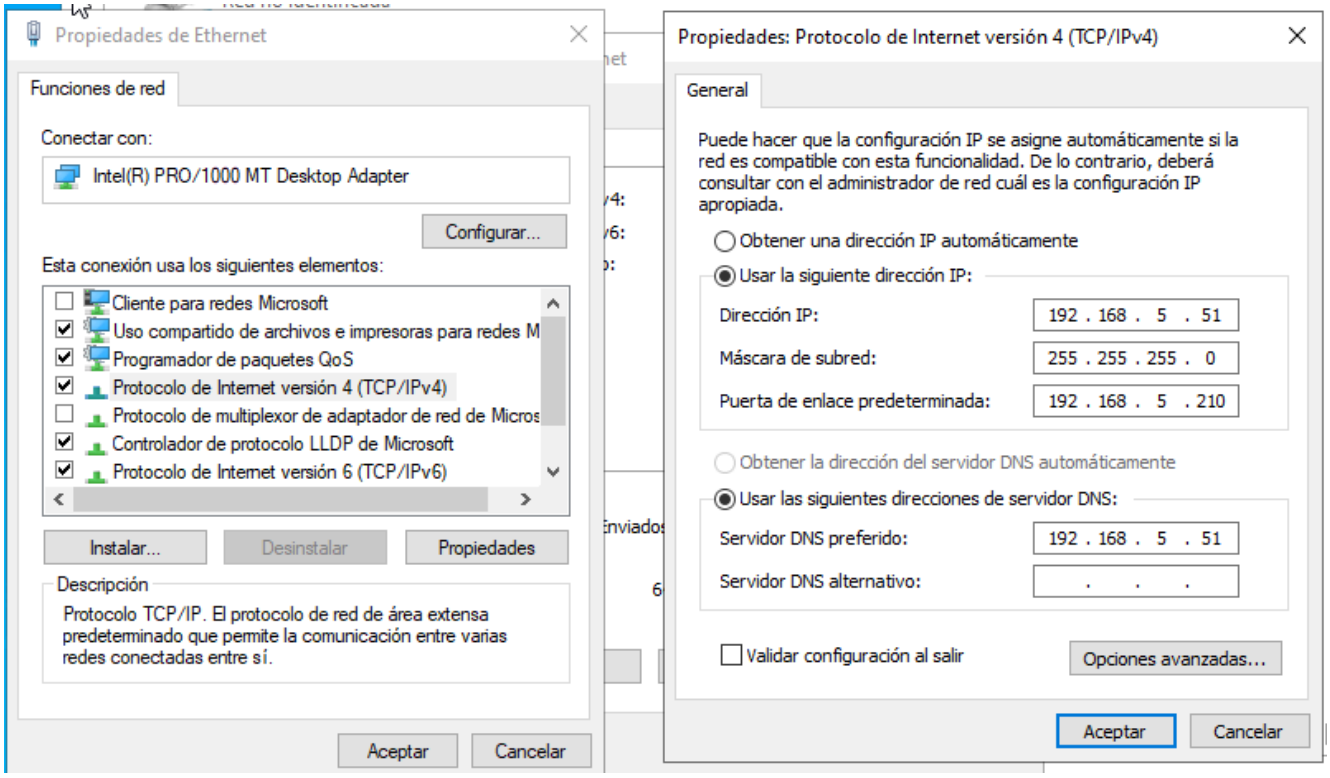
- Abrir Administrador de directivas de grupo.
- Crear GPO nueva y vincularla a la OU deseada.
- Configurar políticas de seguridad, escritorio, contraseñas, acceso a aplicaciones, etc.
- Forzar actualización con gpupdate /force en los equipos clientes.

Comprobaciones y administración básica

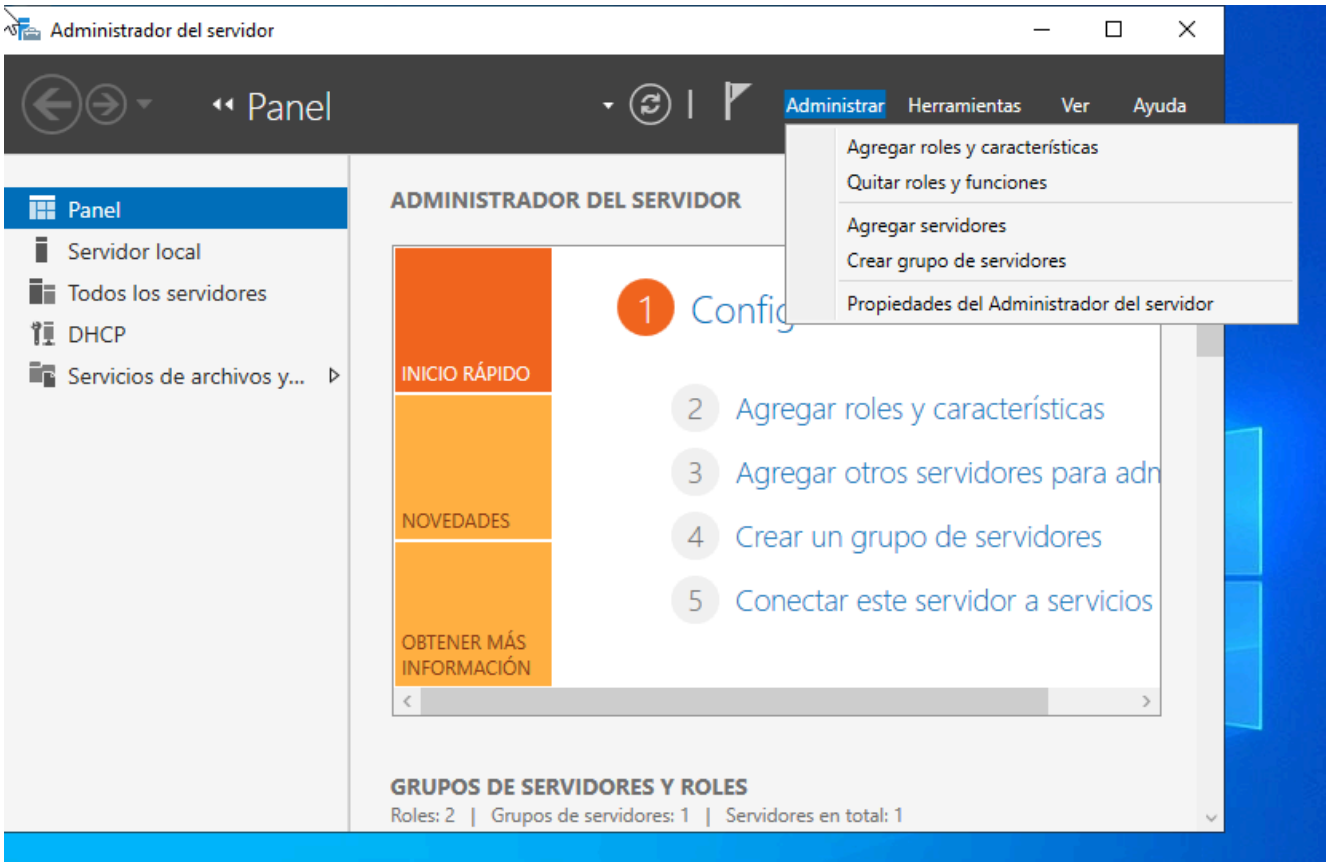
- Probar inicio de sesión de usuarios desde clientes unidos al dominio.
- Verificar replicación y servicio DNS.
- Revisar registros de eventos para posibles errores.
- Realizar copia de seguridad de AD periódicamente.

Práctica en Virtual Box

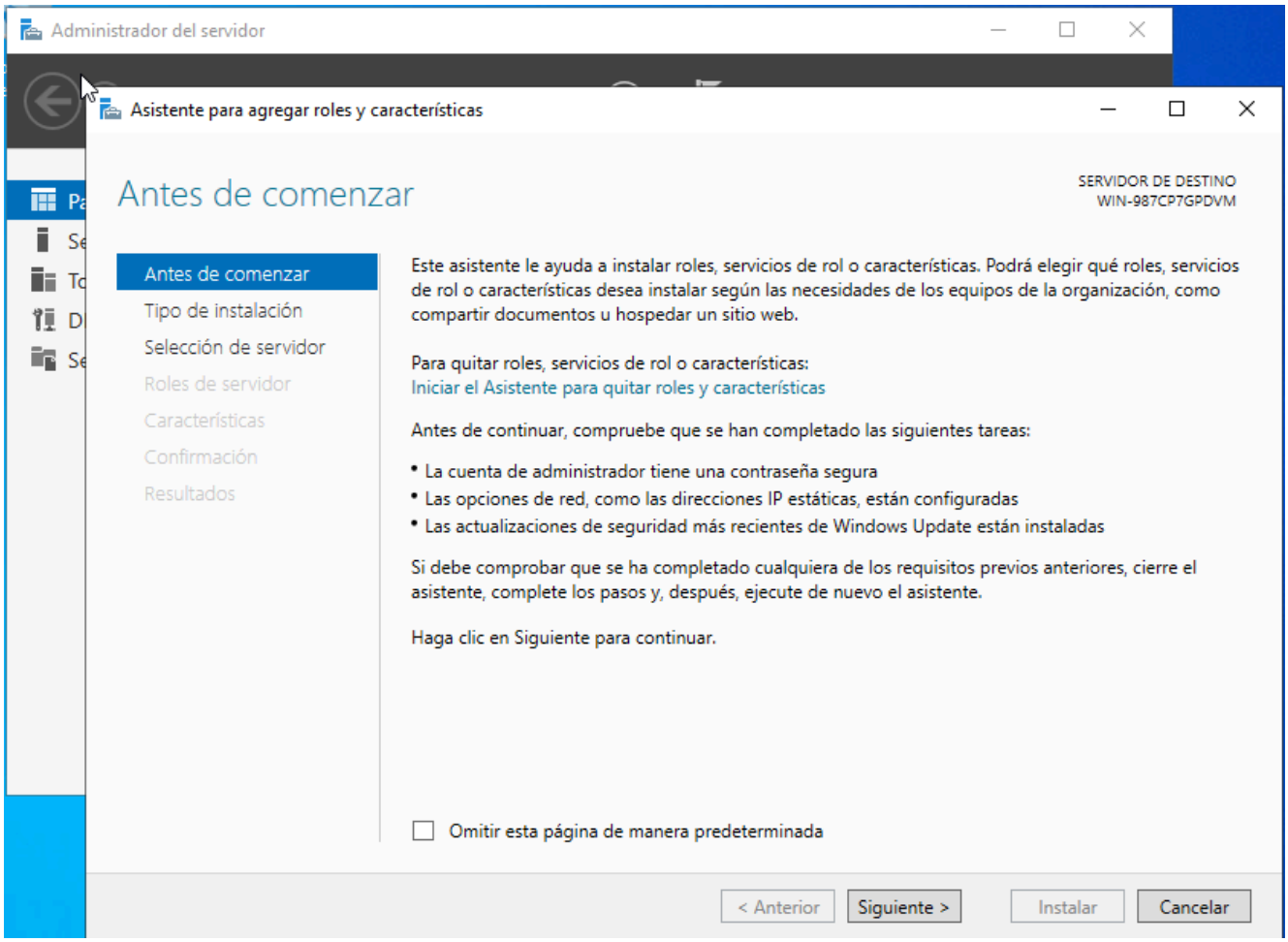
Iniciamos la configuración del servidor de dominio estableciendo un nombre identificativo y asignándole una IP fija. Además, configuramos su propia dirección IP como servidor DNS, ya que será el responsable de administrar todo el sistema de nombres de dominio dentro de nuestra infraestructura.



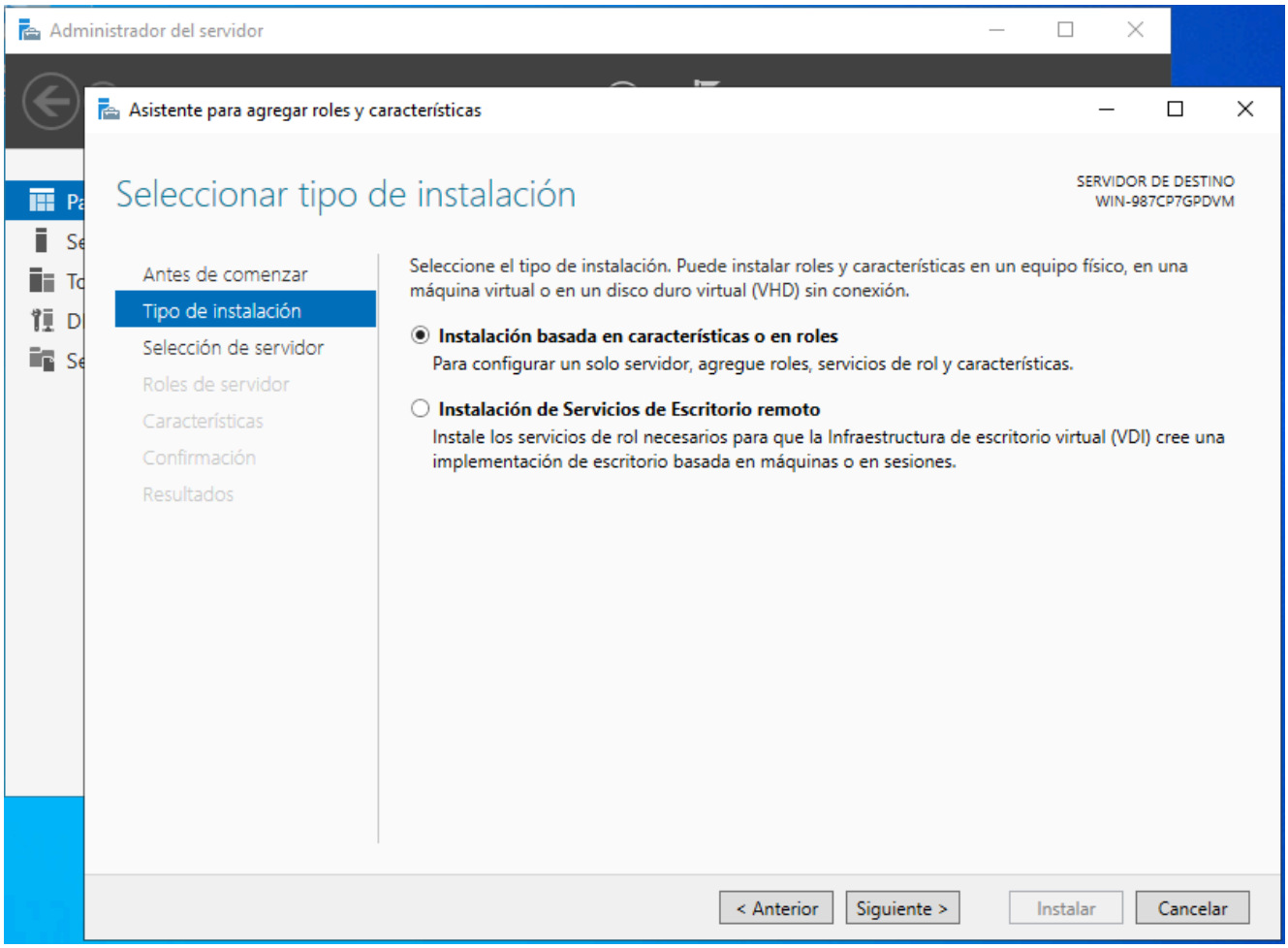
Accedemos al Administrador del servidor para incorporar los roles y características necesarios que permitirán al sistema cumplir con sus funciones específicas dentro de la infraestructura.



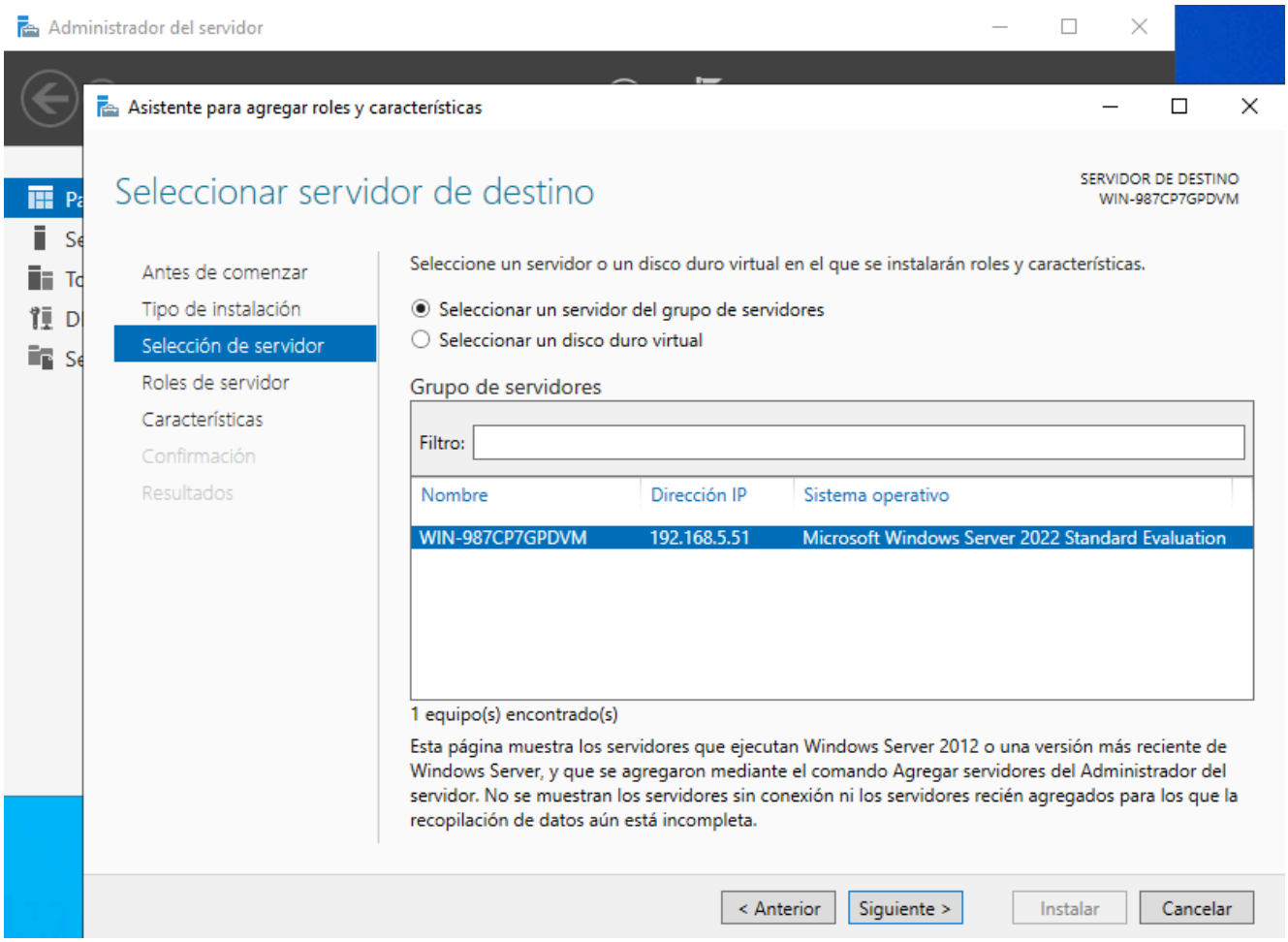
Aparece el asistente de instalación, donde simplemente avanzamos haciendo clic en “Siguiente” para continuar con el proceso de configuración.



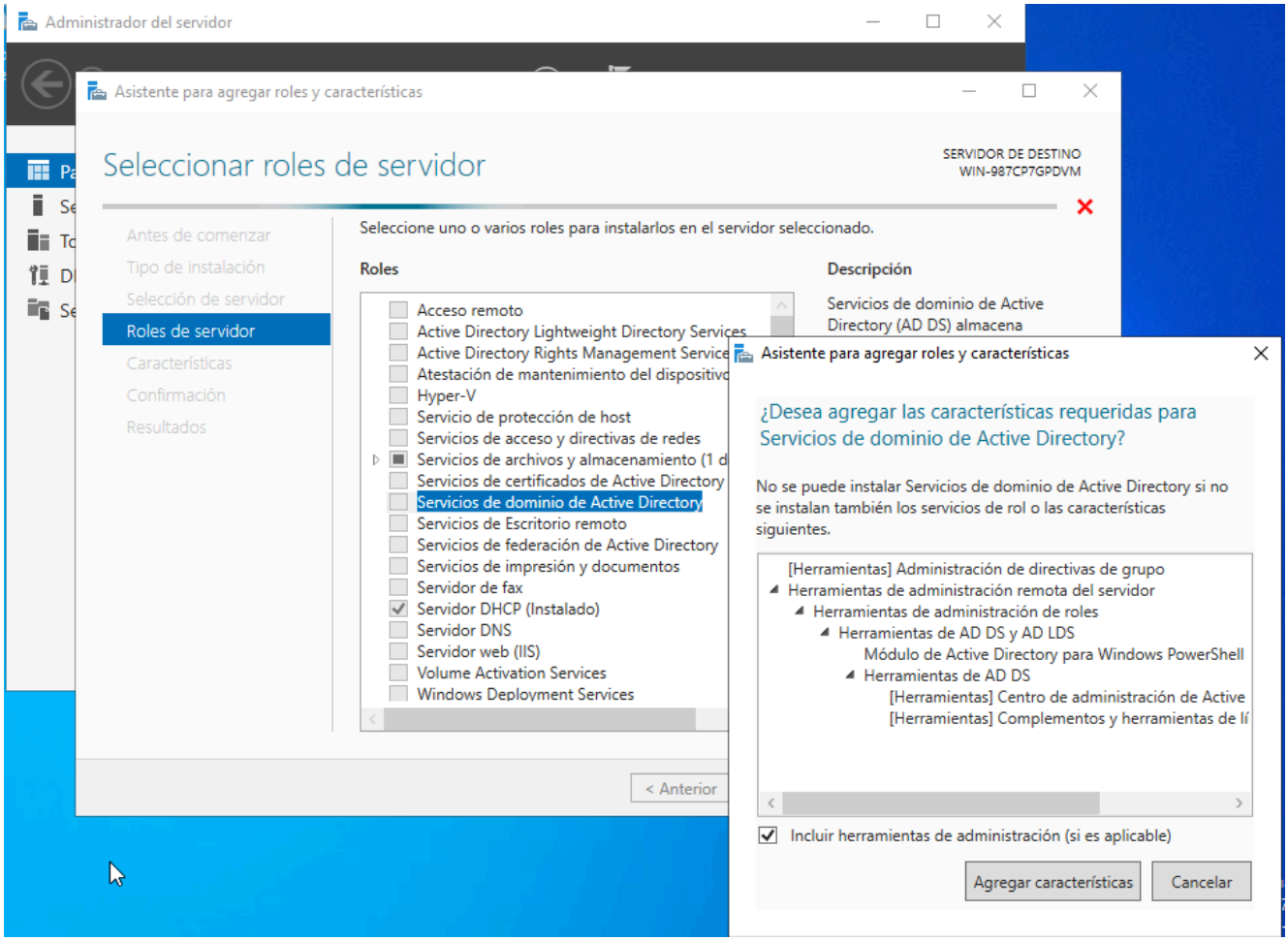
Seleccionamos la modalidad de instalación que se centra en roles y características, lo que nos permite personalizar el servidor según las funciones específicas que deseamos implementar.



Elegimos el servidor identificado como "dco1aso" dentro de la lista disponible, asegurándonos de que sea el equipo sobre el cual vamos a aplicar la instalación de roles y características.

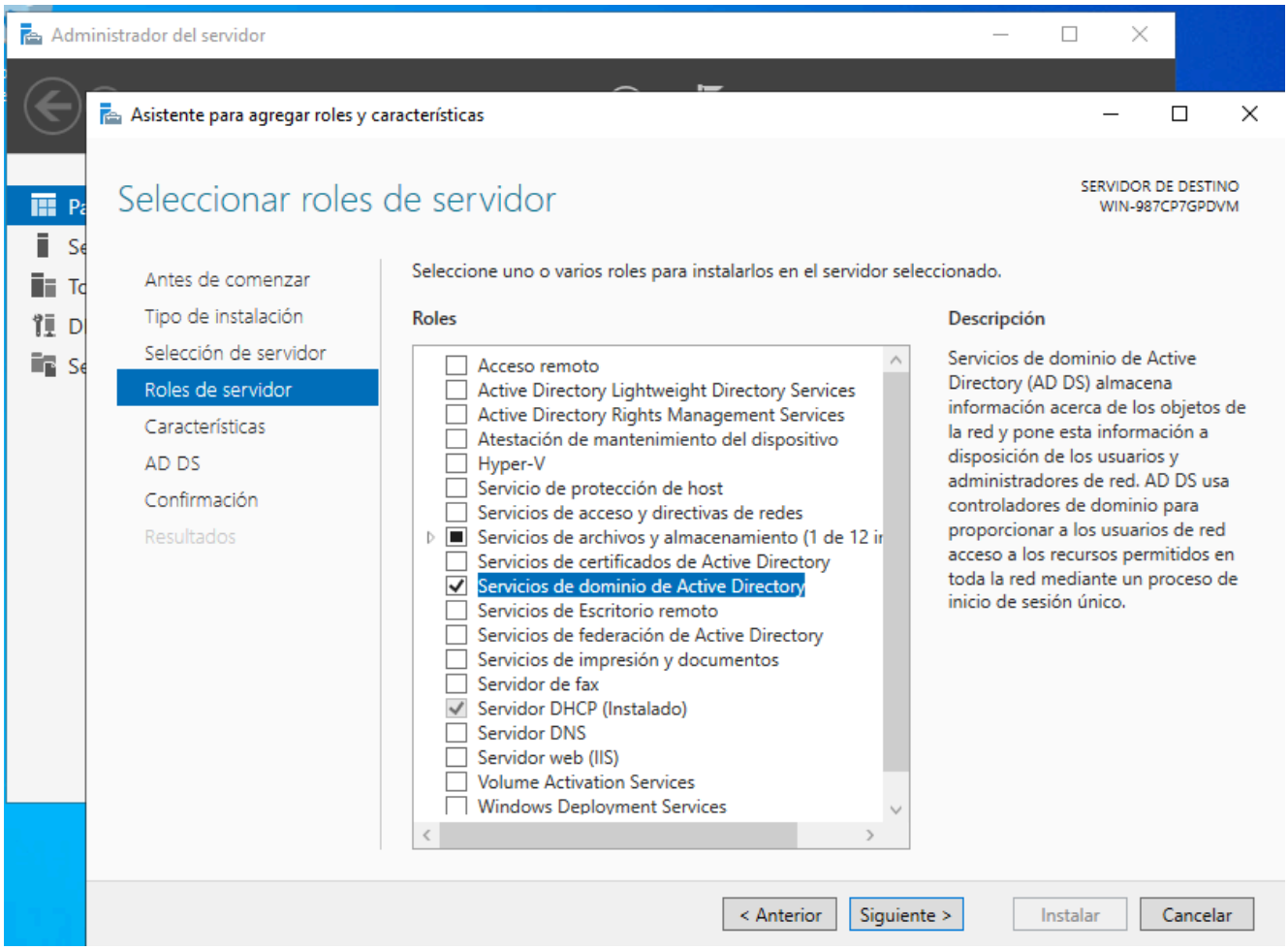


Procedemos a añadir el rol de Servicios de dominio de Active Directory, el cual permitirá que nuestro servidor funcione como controlador de dominio, gestionando usuarios, equipos y políticas dentro del entorno de red.

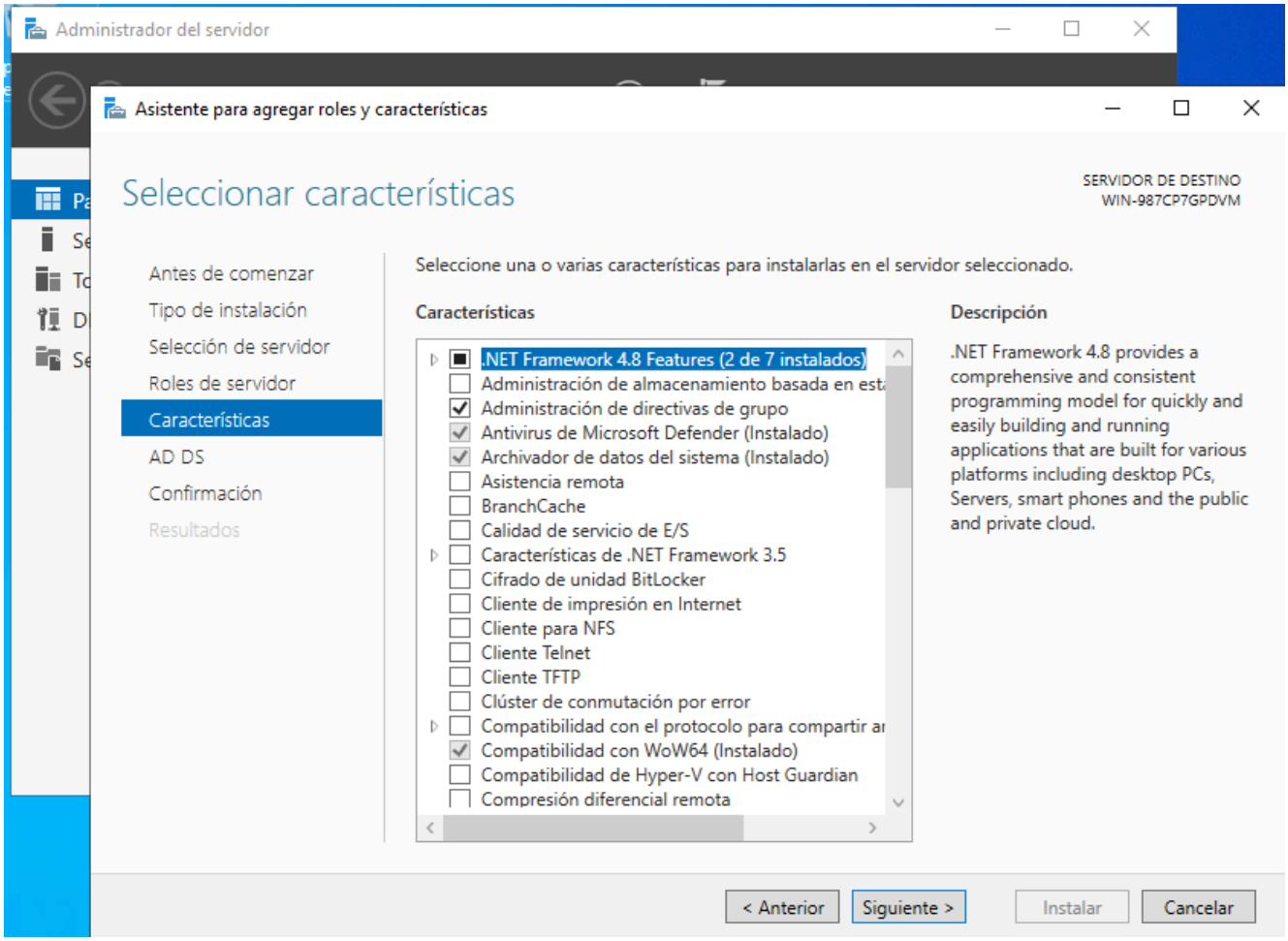


Incorporamos las características necesarias que complementan el rol seleccionado, asegurando que el servidor disponga de todas las funcionalidades requeridas para operar correctamente como controlador de dominio en nuestro entorno.

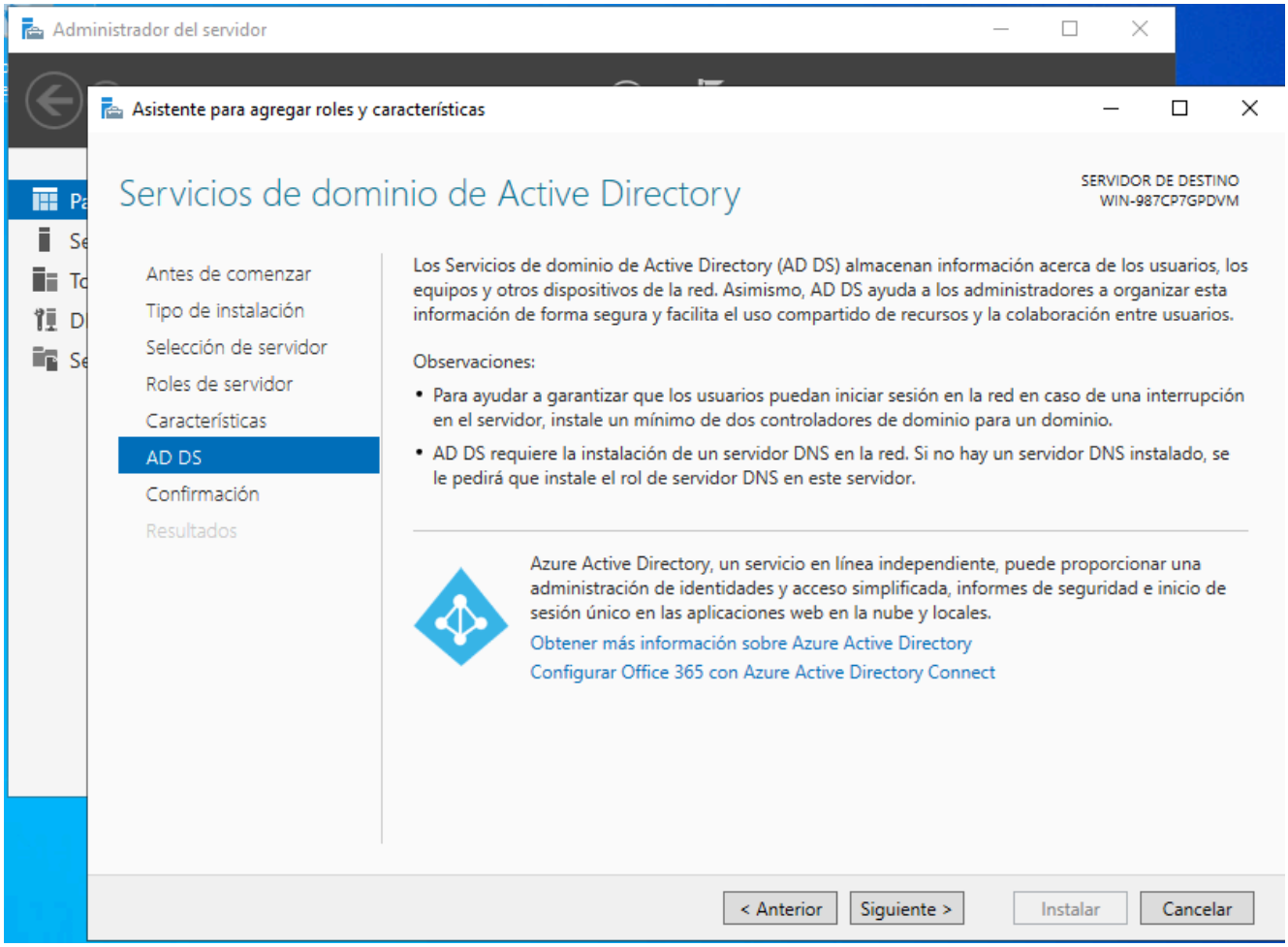
Procedemos con la instalación del rol seleccionado, lo que iniciará el proceso de configuración automática de los componentes necesarios para que el servidor pueda operar como controlador de dominio dentro de nuestra red.



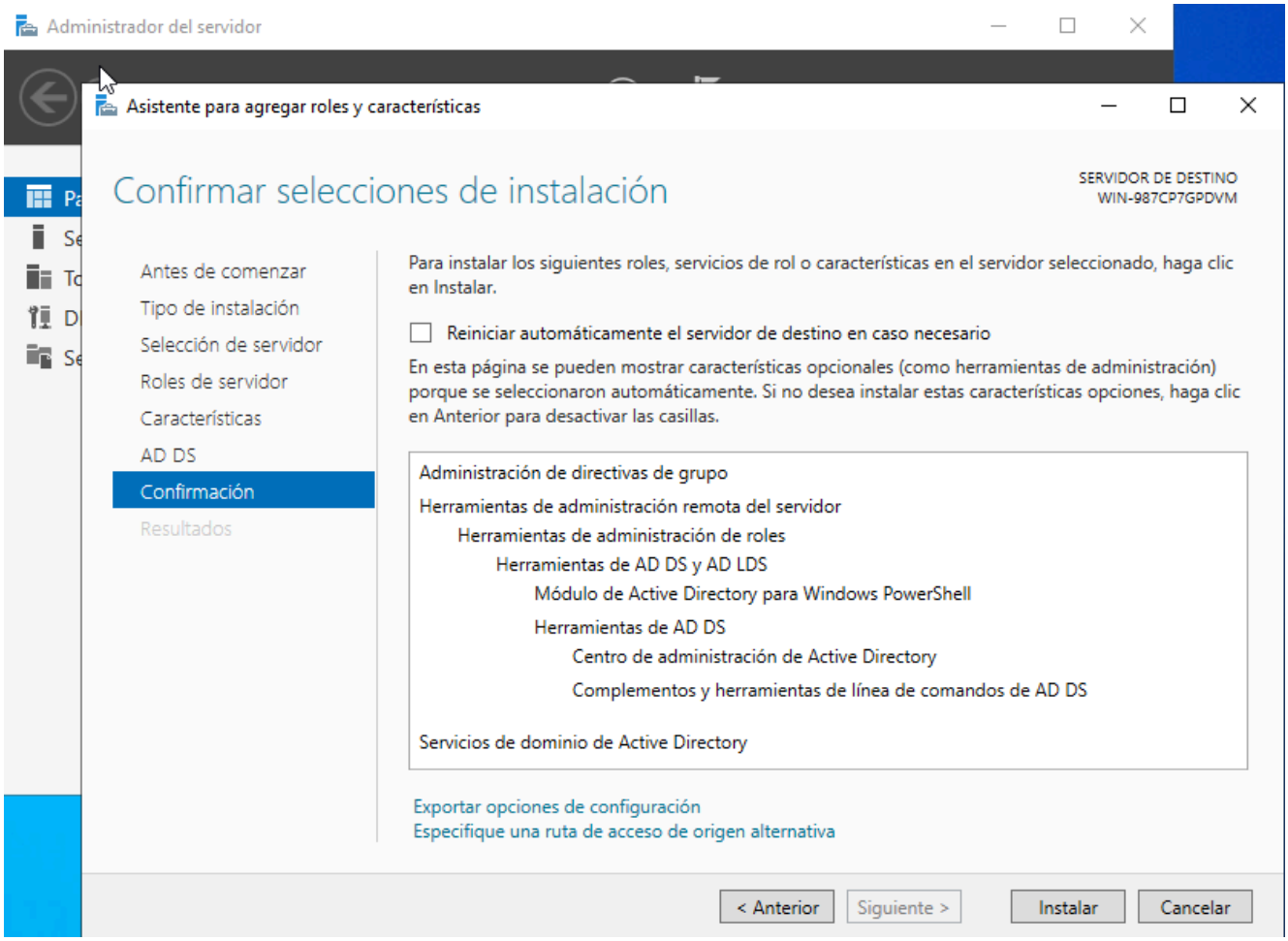
Las características necesarias para el rol de Servicios de dominio de Active Directory ya vienen preseleccionadas automáticamente, por lo que simplemente continuamos el proceso haciendo clic en “Siguiente”.



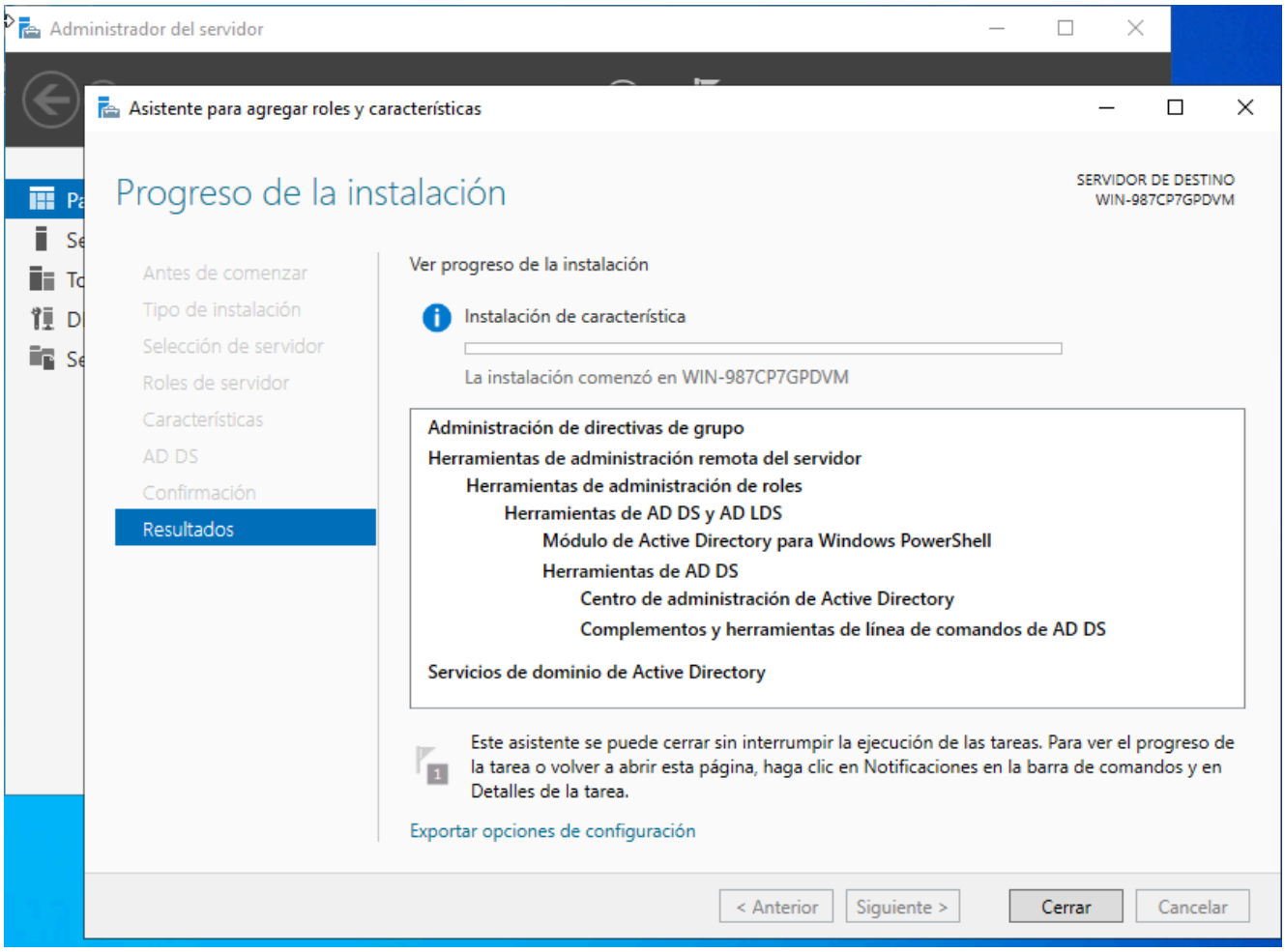
Se despliega una pantalla informativa sobre Active Directory, donde se detallan sus funciones y beneficios. Tras revisar el contenido, avanzamos haciendo clic en “Siguiente” para continuar con la instalación.



Comenzamos la implementación del rol de Servicios de dominio de Active Directory haciendo clic en “Instalar”, lo que dará inicio al proceso de configuración automática de los componentes necesarios para convertir el servidor en un controlador de dominio.

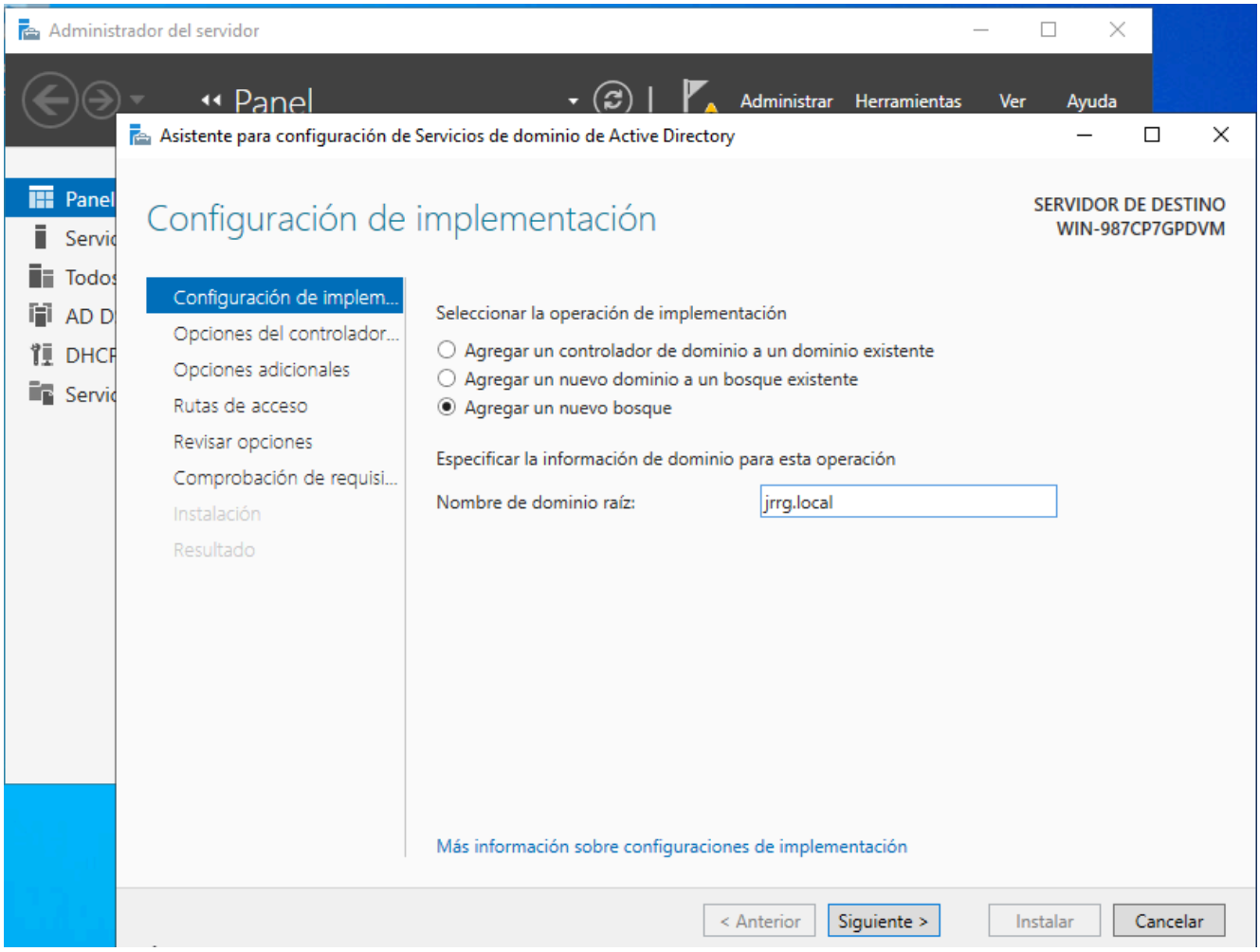


Tras completar la instalación, cerramos el asistente y reiniciamos el servidor para aplicar correctamente los cambios y activar el rol de controlador de dominio en el entorno.



Después de reiniciar el sistema, accedemos nuevamente al Administrador del servidor y seleccionamos la opción para promover el servidor a controlador de dominio, iniciando así el proceso de configuración del entorno de Active Directory.

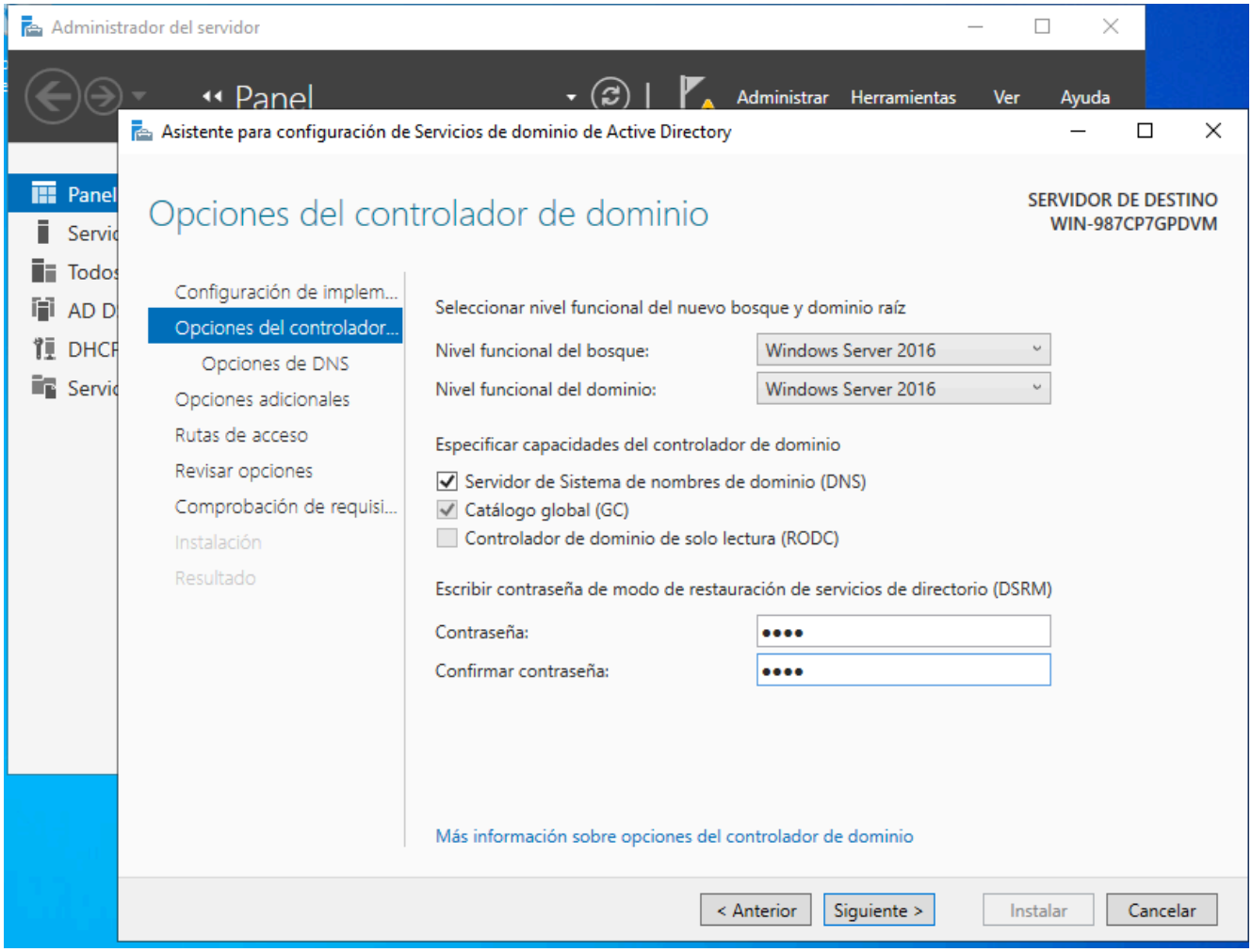
Al abrirse el asistente de configuración, seleccionamos la opción para crear un nuevo bosque, ya que estamos configurando el primer controlador de dominio en nuestra red. En este paso, introducimos el nombre del dominio raíz, que será la base jerárquica de toda nuestra infraestructura de Active Directory.



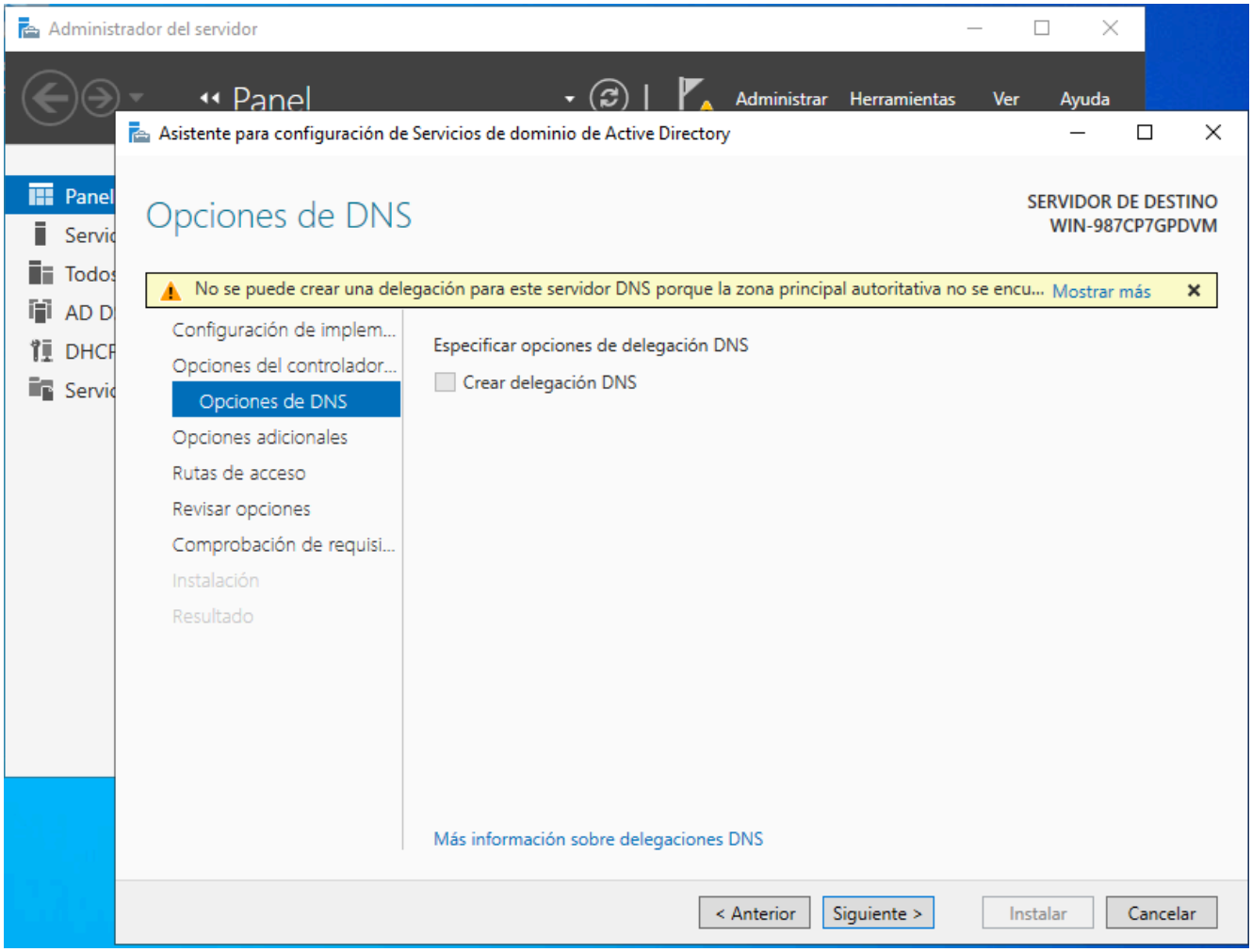
Establecemos el nivel funcional del bosque en Windows Server 2016, ya que no contamos con controladores de dominio que utilicen versiones anteriores como Windows Server 2003, 2008 o 2012.

Activamos también la función de servidor DNS, que será la base para la resolución de nombres dentro de nuestra red, cumpliendo además con un requisito esencial para el correcto funcionamiento de Active Directory.

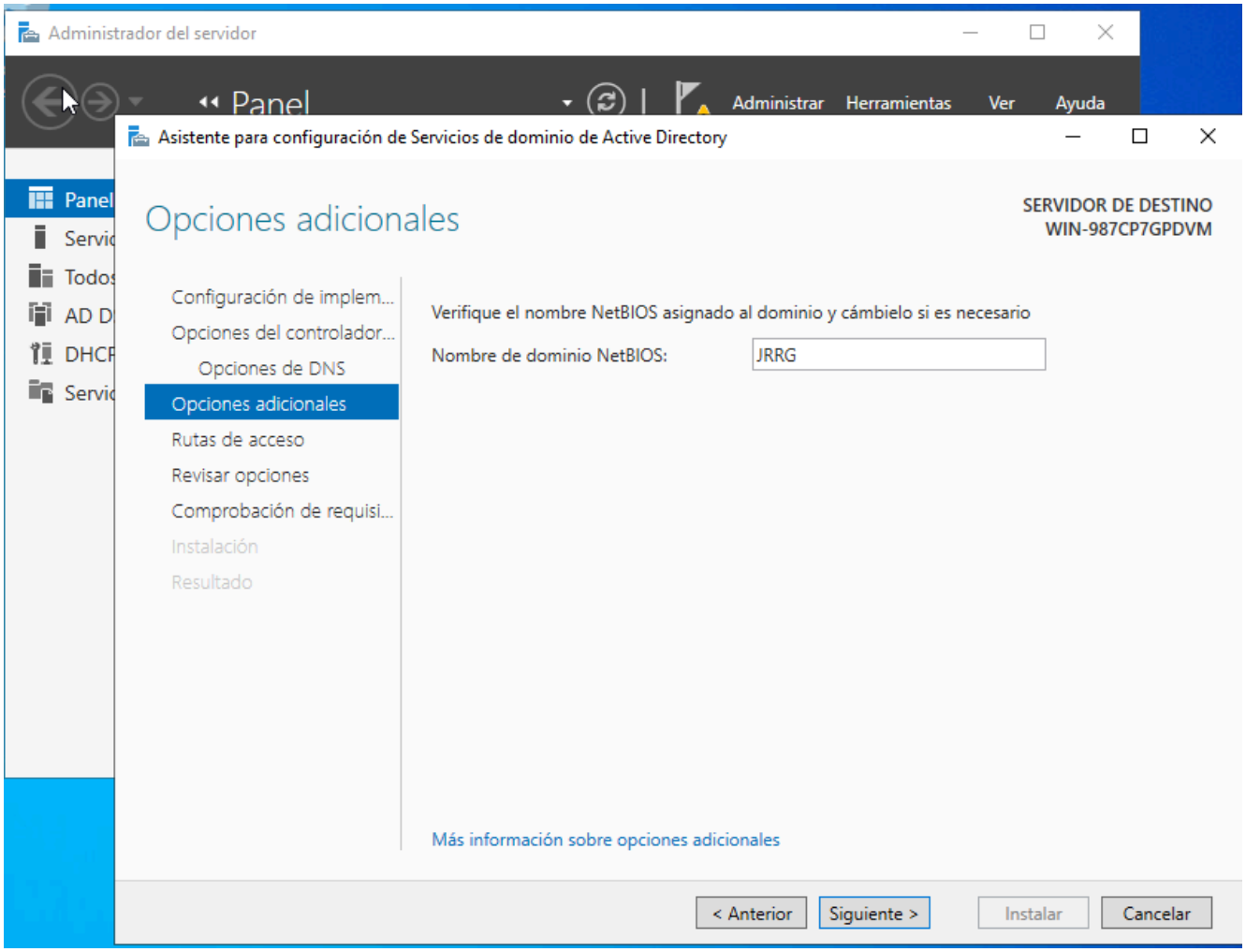
Finalmente, **definimos una contraseña segura para el modo de restauración de servicios de directorio (DSRM)**, la cual será necesaria en situaciones de recuperación del entorno de Active Directory.



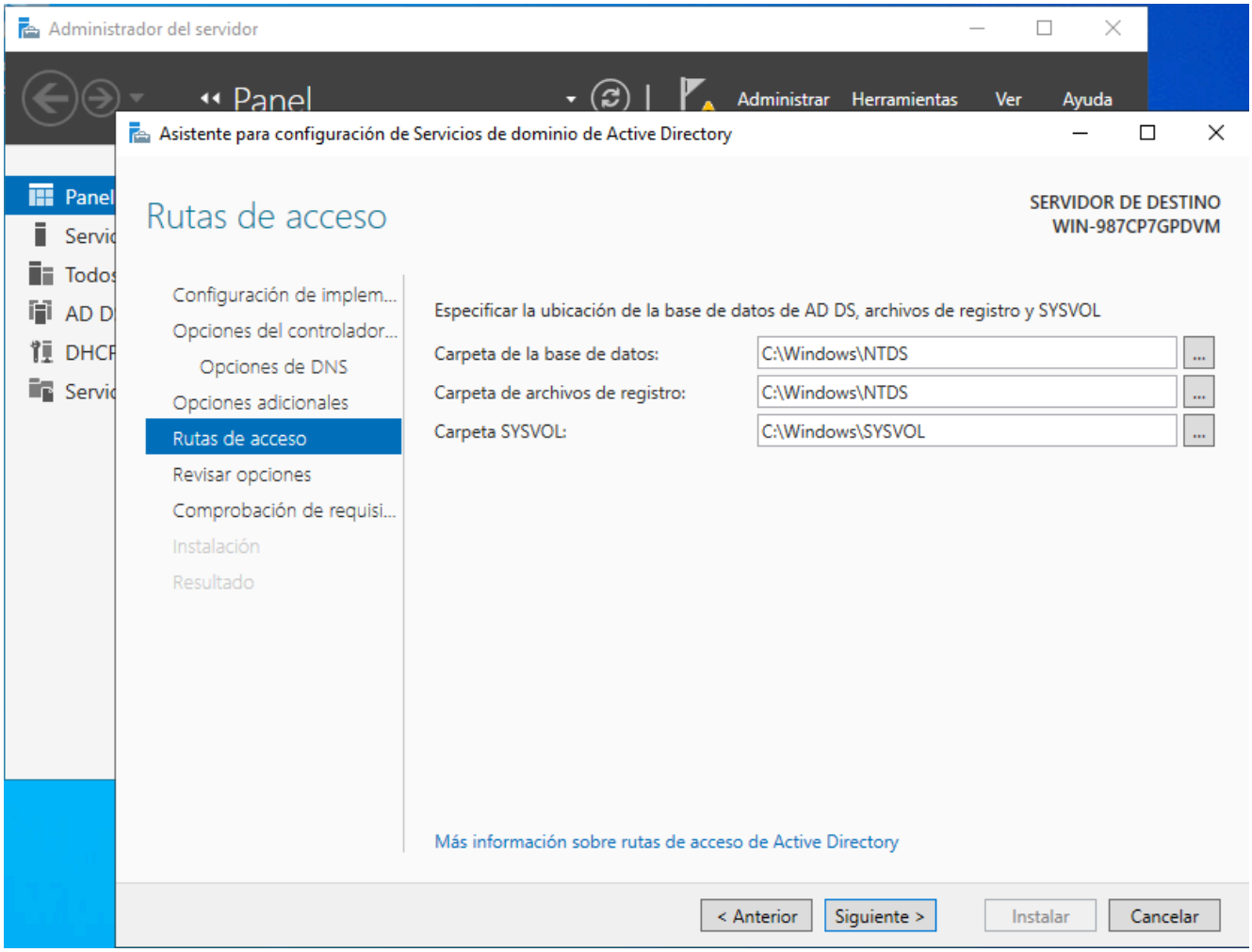
Como este servidor está configurando el primer bosque de Active Directory en nuestra infraestructura, Windows no detecta una delegación existente para el servidor DNS. Esto es completamente normal en este contexto, así que simplemente continuamos el proceso haciendo clic en “Siguiente”.



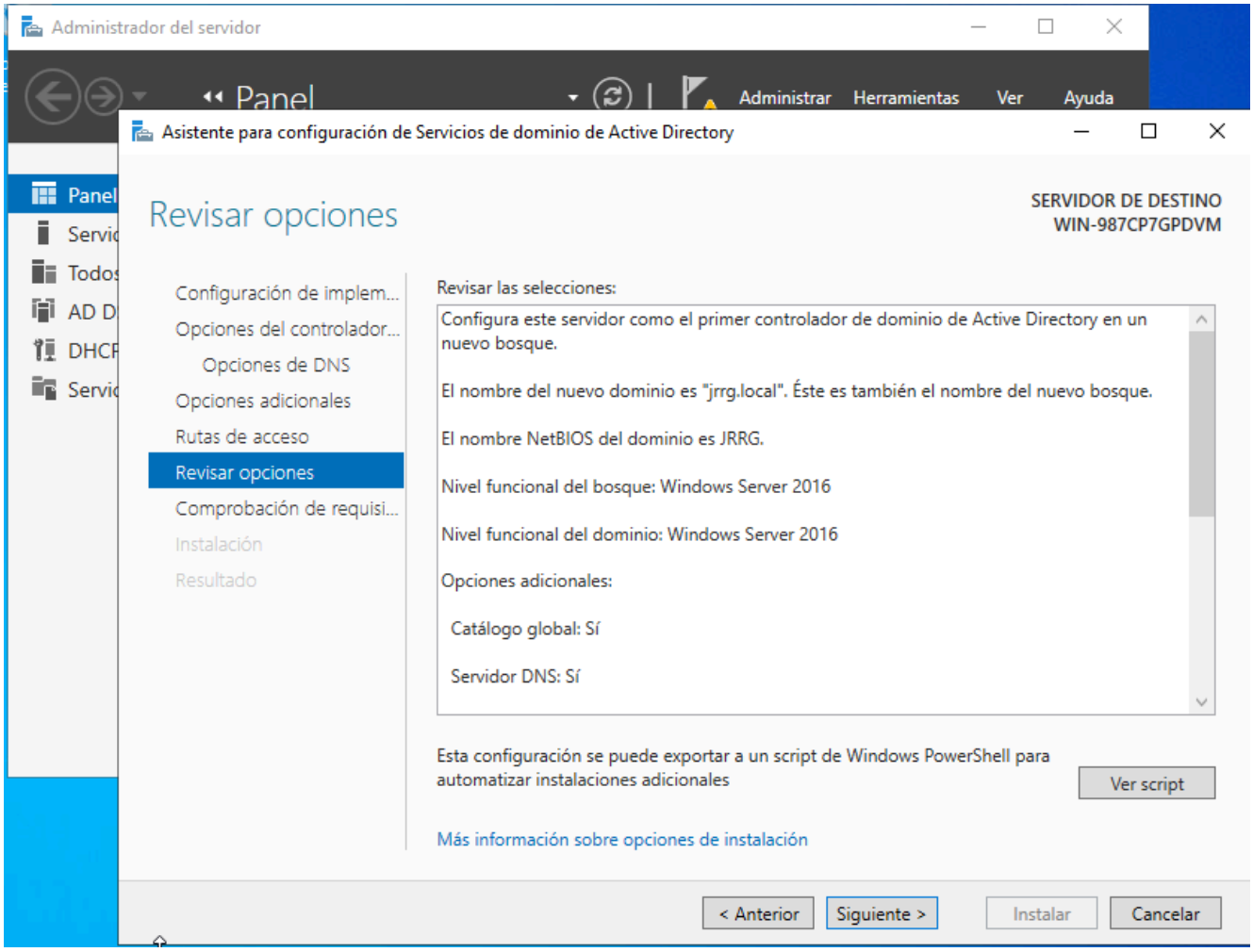
Asignamos el nombre JRRG al dominio, el cual servirá como identificador corto y compatible con versiones anteriores de Windows. Este nombre facilita la comunicación entre equipos en redes que aún utilizan protocolos antiguos o aplicaciones que requieren este formato.



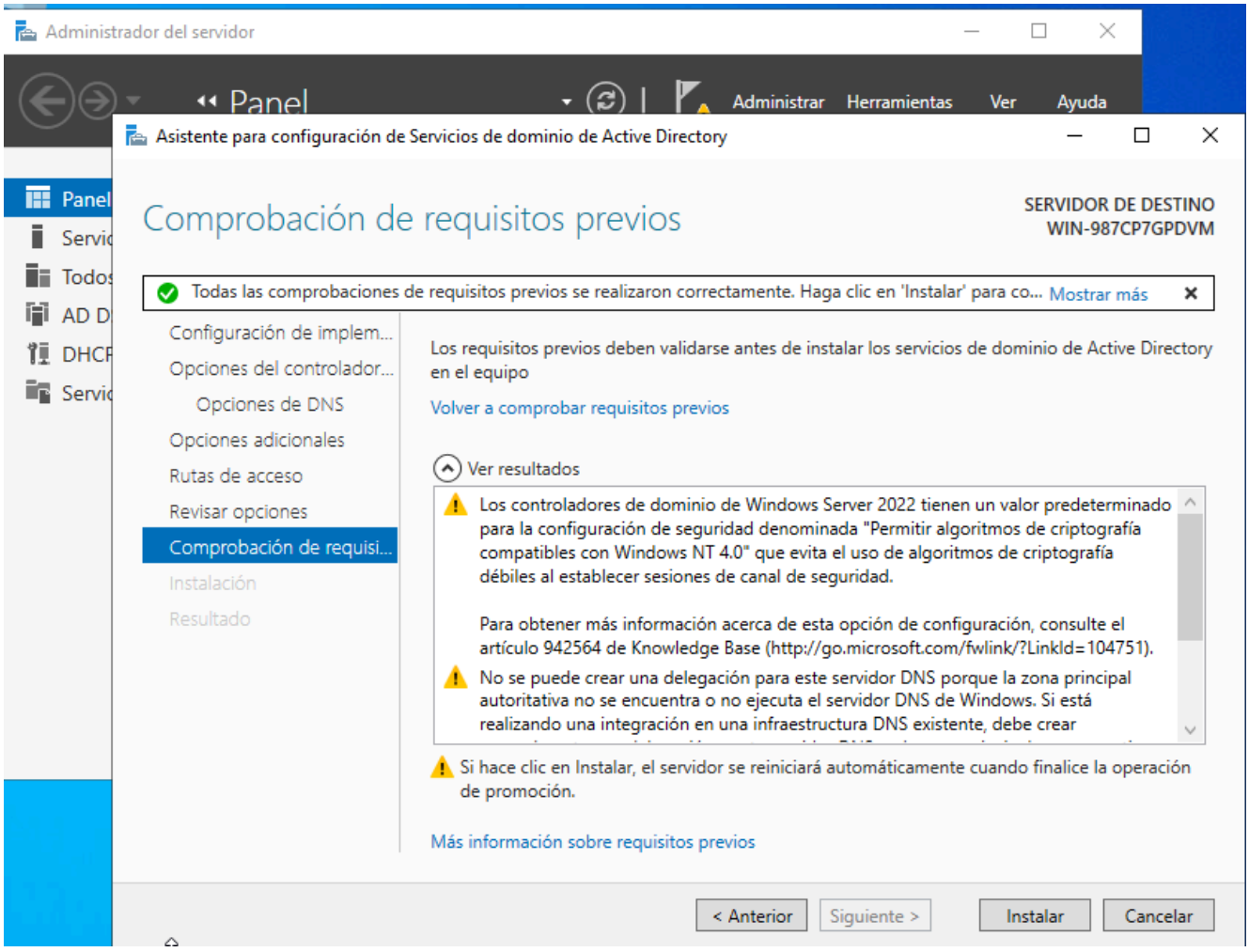
Mantenemos las rutas de instalación predeterminadas, ya que son adecuadas para la mayoría de entornos y aseguran una correcta organización de los archivos del sistema relacionados con Active Directory. Simplemente continuamos haciendo clic en “Siguiente”.



El asistente presenta un resumen detallado de todas las opciones que hemos configurado, incluyendo el nombre del dominio, el nivel funcional del bosque, las funciones seleccionadas como DNS, y la contraseña de restauración. Este paso nos permite verificar que todo esté correcto antes de continuar con la instalación definitiva.



La verificación de los requisitos previos se ha completado con éxito, lo que indica que el sistema está listo para proceder. Hacemos clic en “Instalar” para iniciar la promoción definitiva del servidor como controlador de dominio en nuestro entorno de Active Directory.



Se inicia el proceso de instalación y promoción del servidor como controlador de dominio, lo que implica:

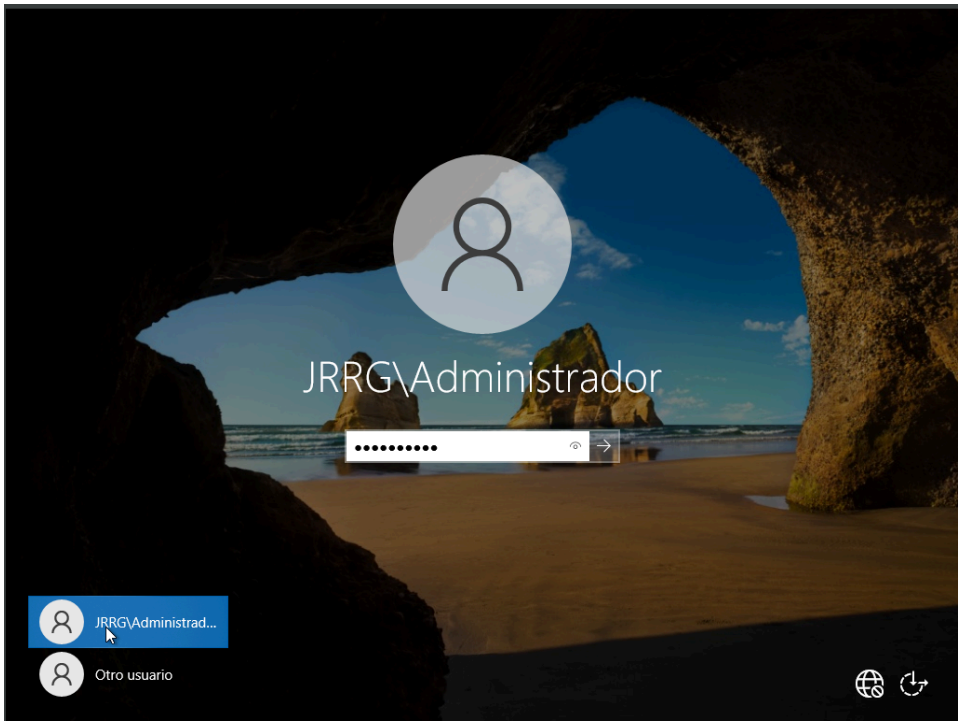
- La configuración de los servicios de Active Directory.
- La integración del servidor en el nuevo bosque y dominio.
- La instalación del servicio DNS si se seleccionó.
- La aplicación de las políticas de seguridad y replicación necesarias.

Este proceso puede tardar unos minutos y, al finalizar, el servidor se reiniciará automáticamente para completar la promoción.

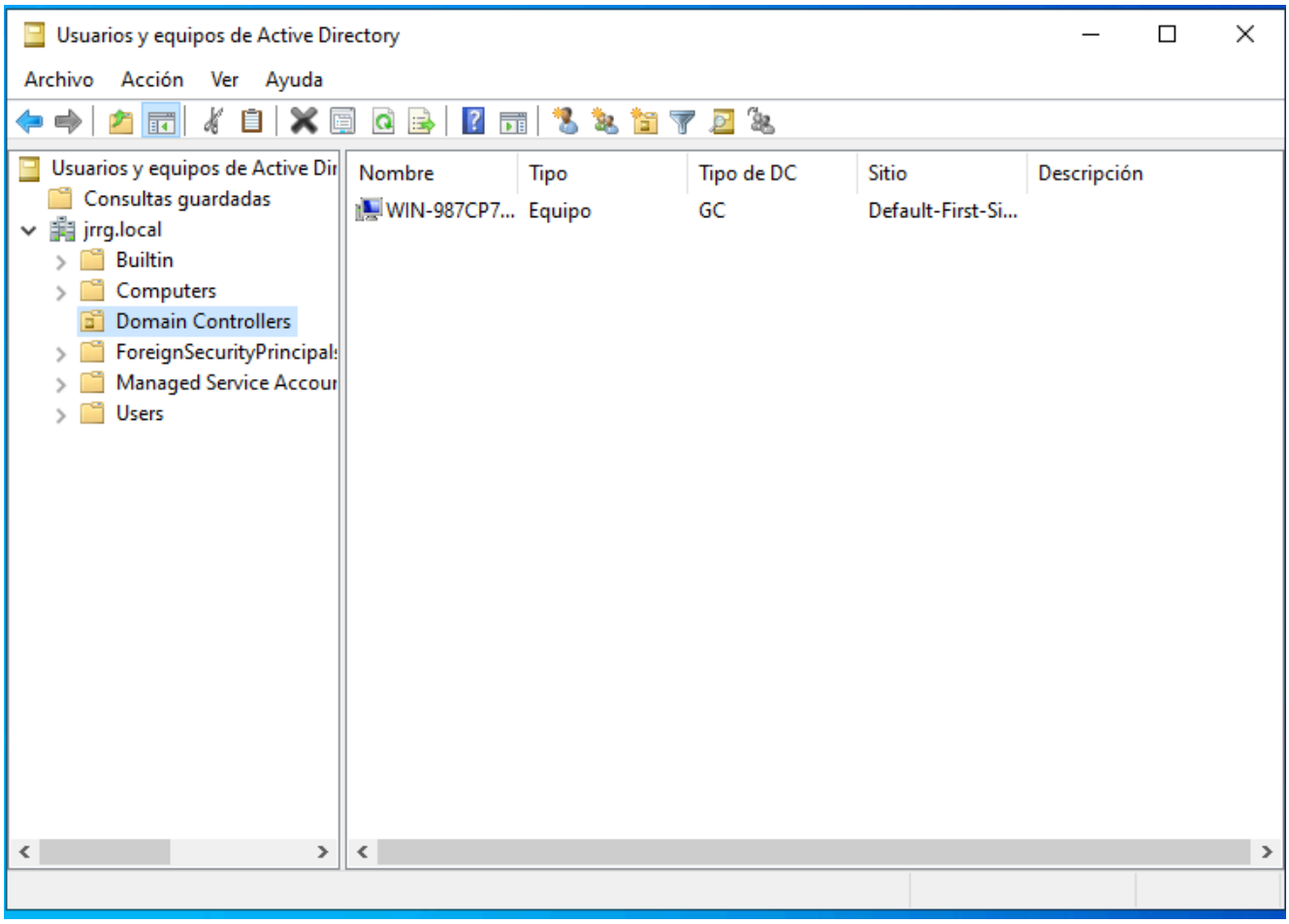
Después del reinicio automático, el sistema nos solicita las credenciales de inicio de sesión. En este punto, introducimos las credenciales de la cuenta de Administrador del dominio, que ahora tiene privilegios para gestionar toda la infraestructura de Active Directory.

Esta cuenta será clave para:

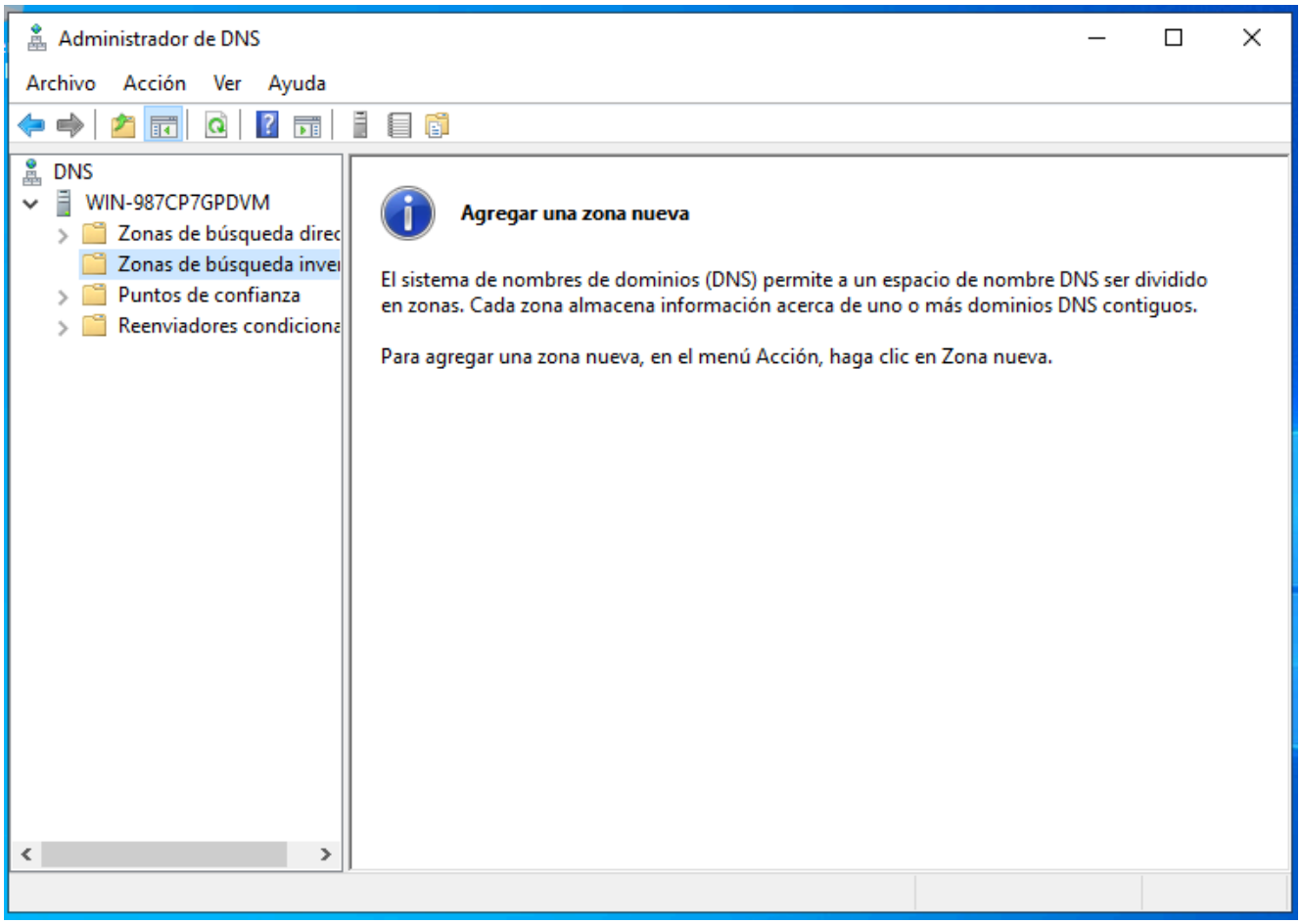
- Crear y administrar usuarios, grupos y equipos.
- Configurar políticas de grupo (GPO).
- Supervisar la replicación entre controladores de dominio (si se añaden más).
- Gestionar servicios como DNS y DHCP integrados en el entorno.

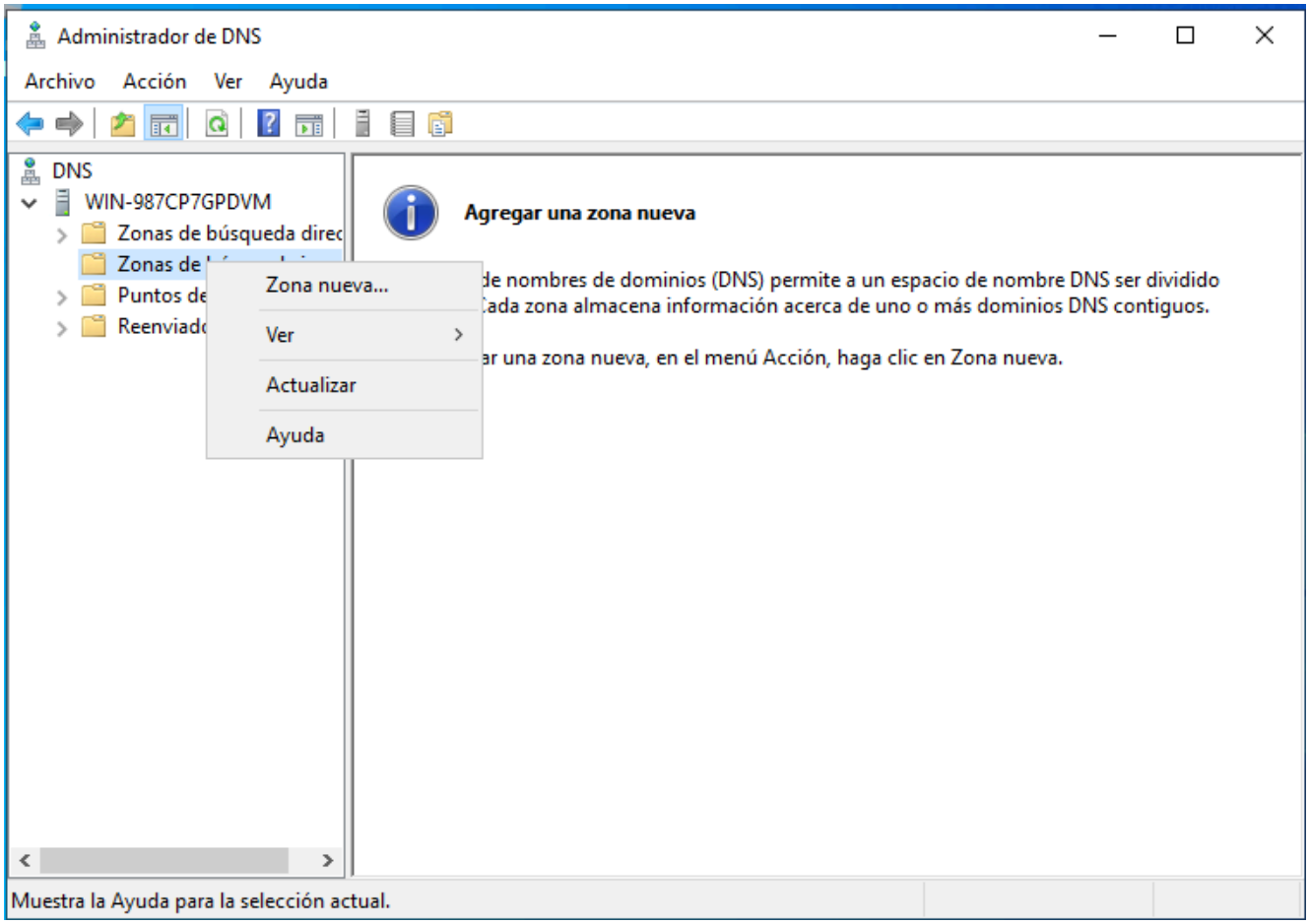


Con esto hemos completado la promoción del servidor a controlador de dominio

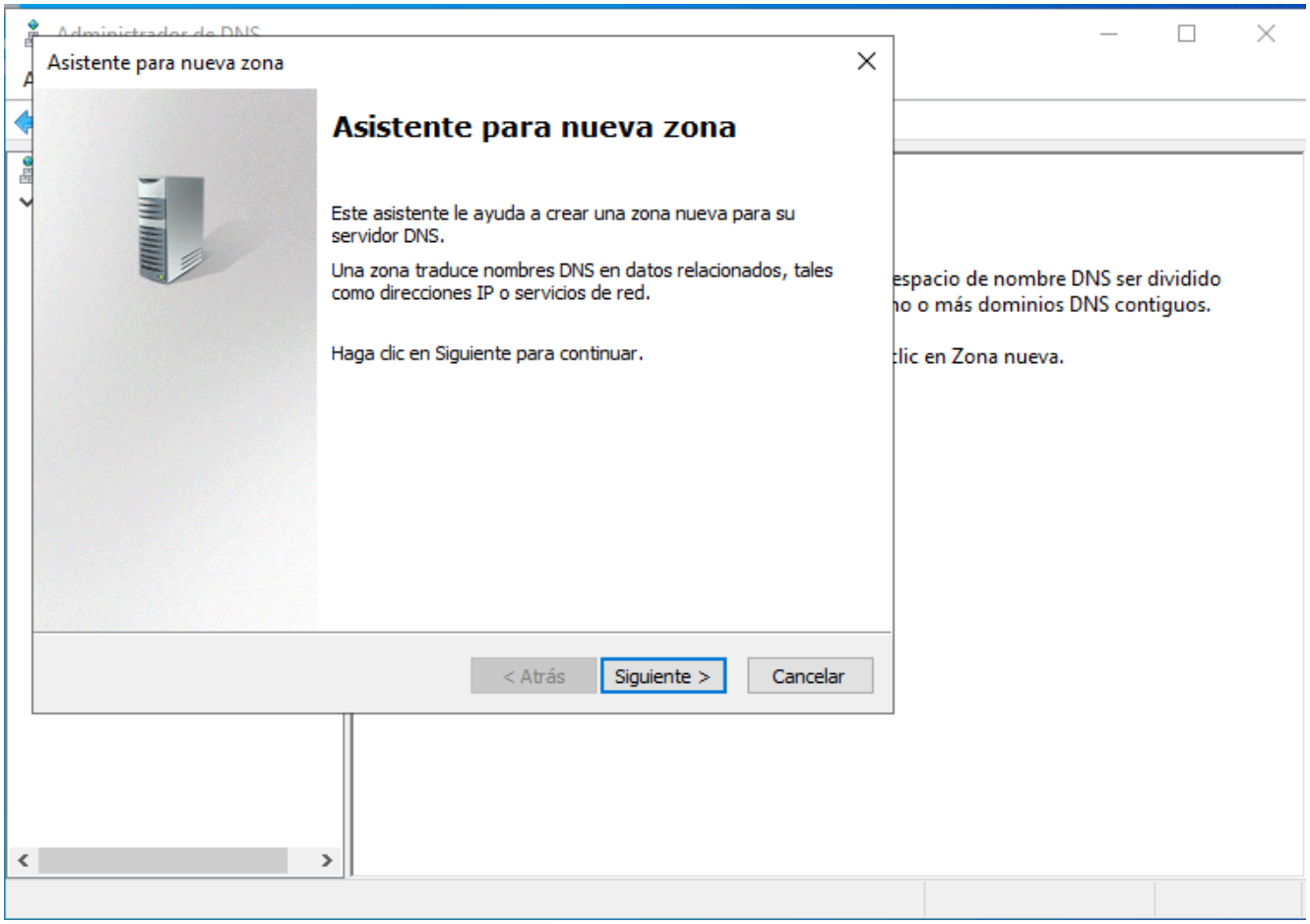


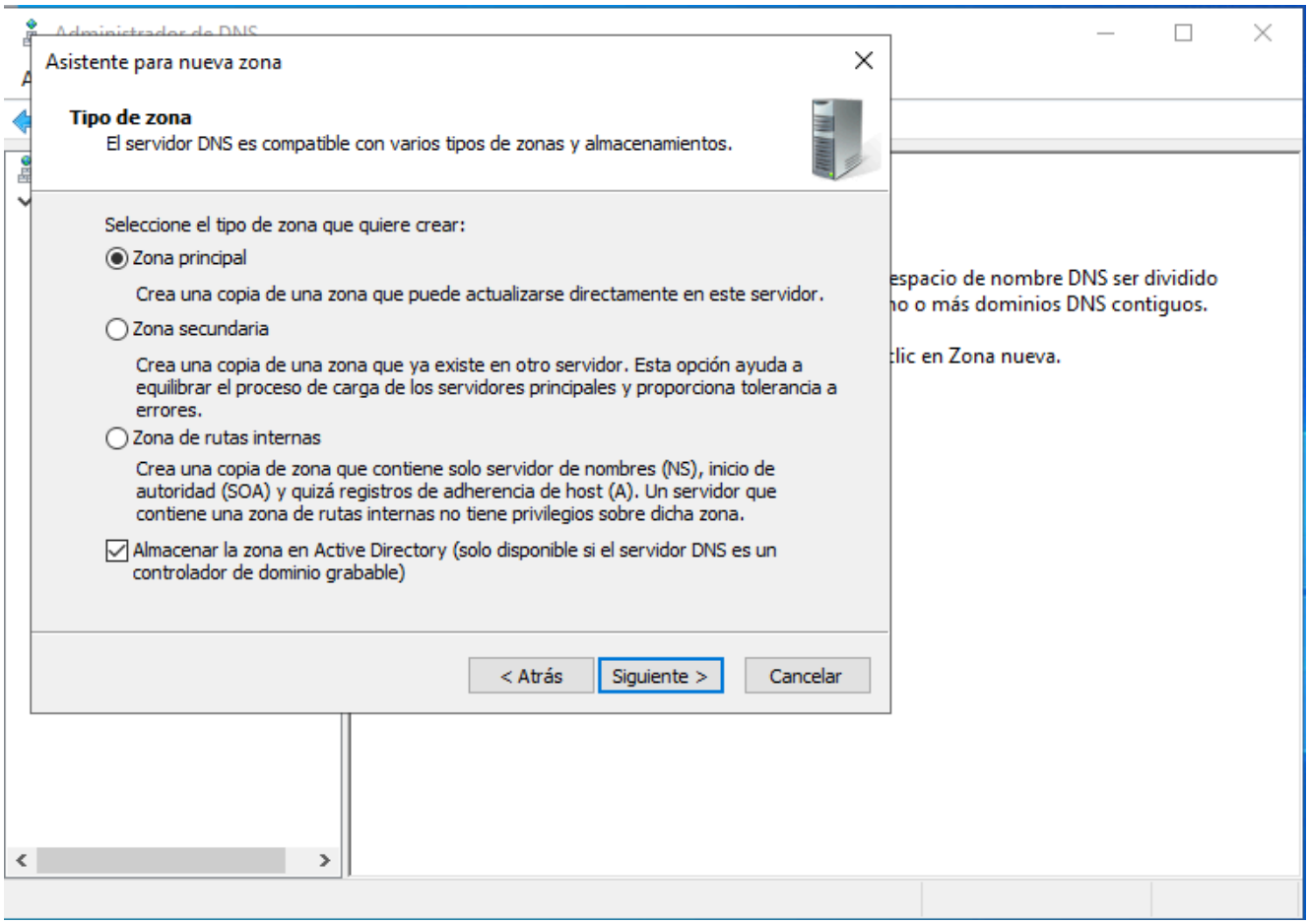
Abrimos la consola de administración DNS y procedemos a crear una nueva zona de búsqueda inversa, esencial para que el servidor pueda resolver direcciones IP en nombres de host. Este paso es clave para mejorar la administración de red y permitir la creación de registros PTR que facilitan la resolución inversa.

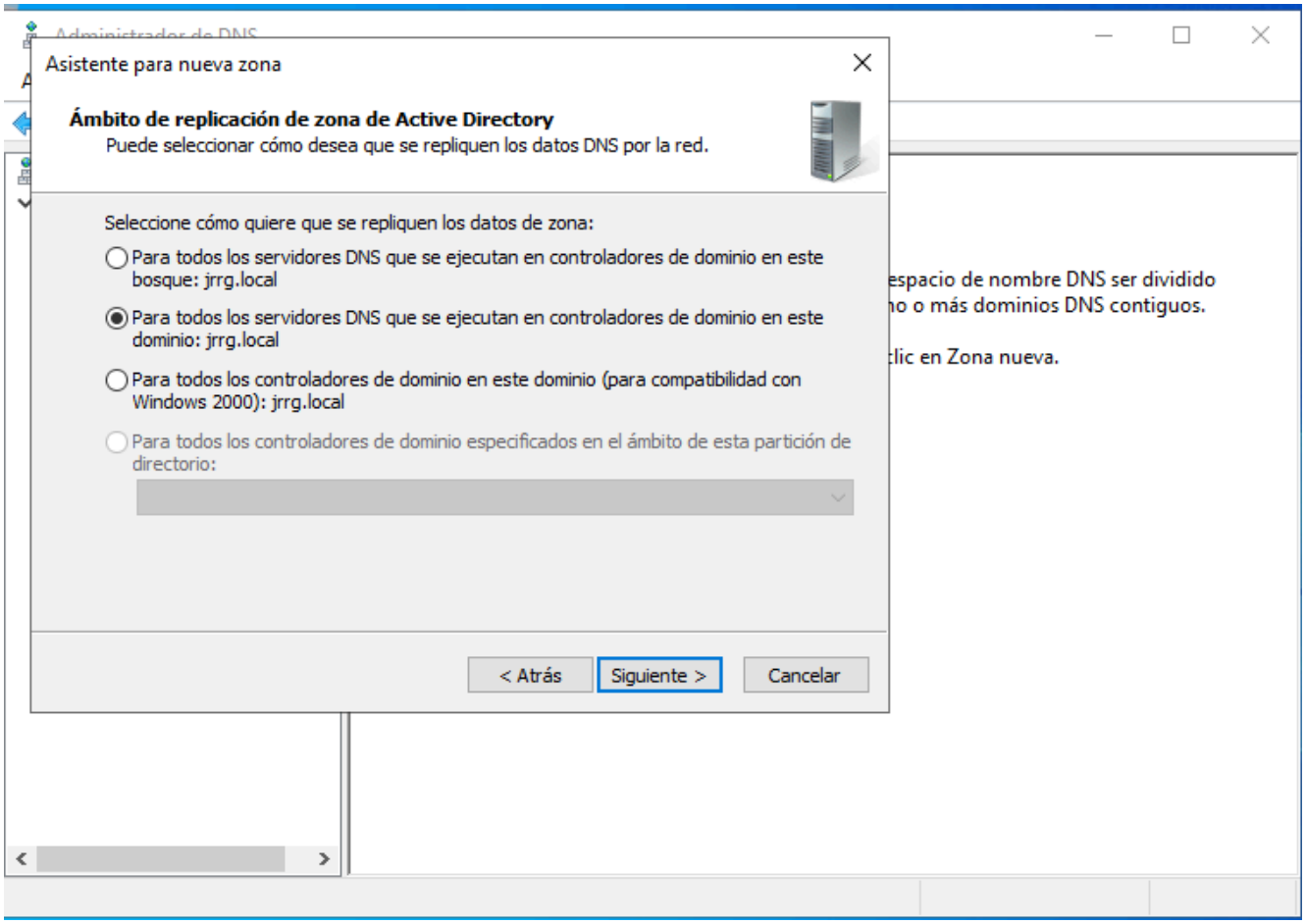

Administrador de DNS
Archivo
Acción
Ver
Ayuda
DNS
WIN-987CP7GPDVM
Zonas de búsqueda direc
Zonas de búsqueda inver
Puntos de confianza
Reenviadores condiciona
Agregar una zona nueva
El sistema de nombres de dominios (DNS) permite a un espacio de nombre DNS ser dividido en zonas. Cada zona almacena información acerca de uno o más dominios DNS contiguos.
Para agregar una zona nueva, en el menú Acción, haga clic en Zona nueva.

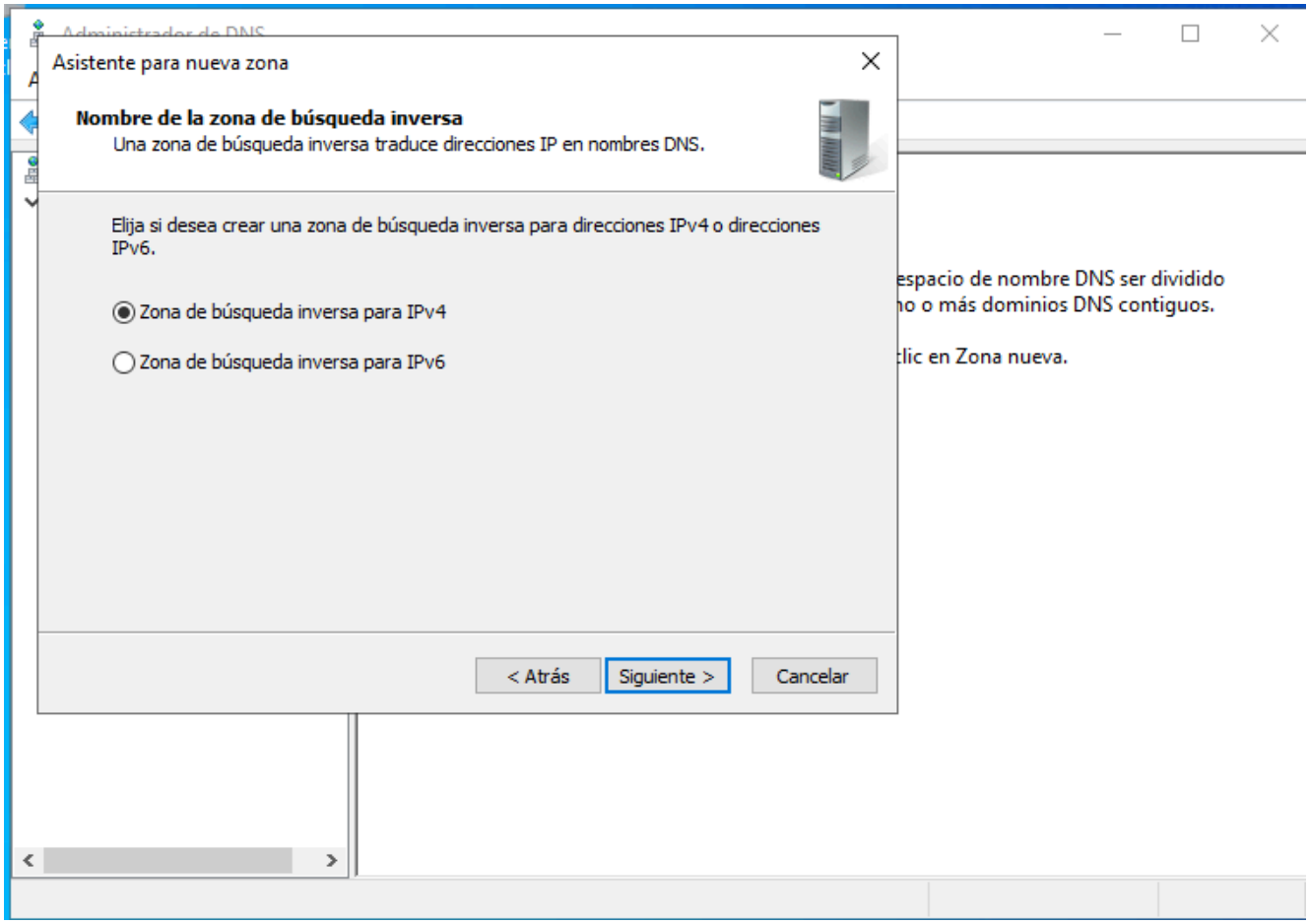

Administrador de DNS
Archivo
Acción
Ver
Ayuda
DNS
WIN-987CP7GPDVM
Zonas de búsqueda direc
Zonas de
Puntos de
Reenviado
Zona nueva...
Ver
Actualizar
Ayuda
Agregar una zona nueva
de nombres de dominios (DNS) permite a un espacio de nombre DNS ser dividido
Cada zona almacena información acerca de uno o más dominios DNS contiguos.
ar una zona nueva, en el menú Acción, haga clic en Zona nueva.
Muestra la Ayuda para la selección actual.

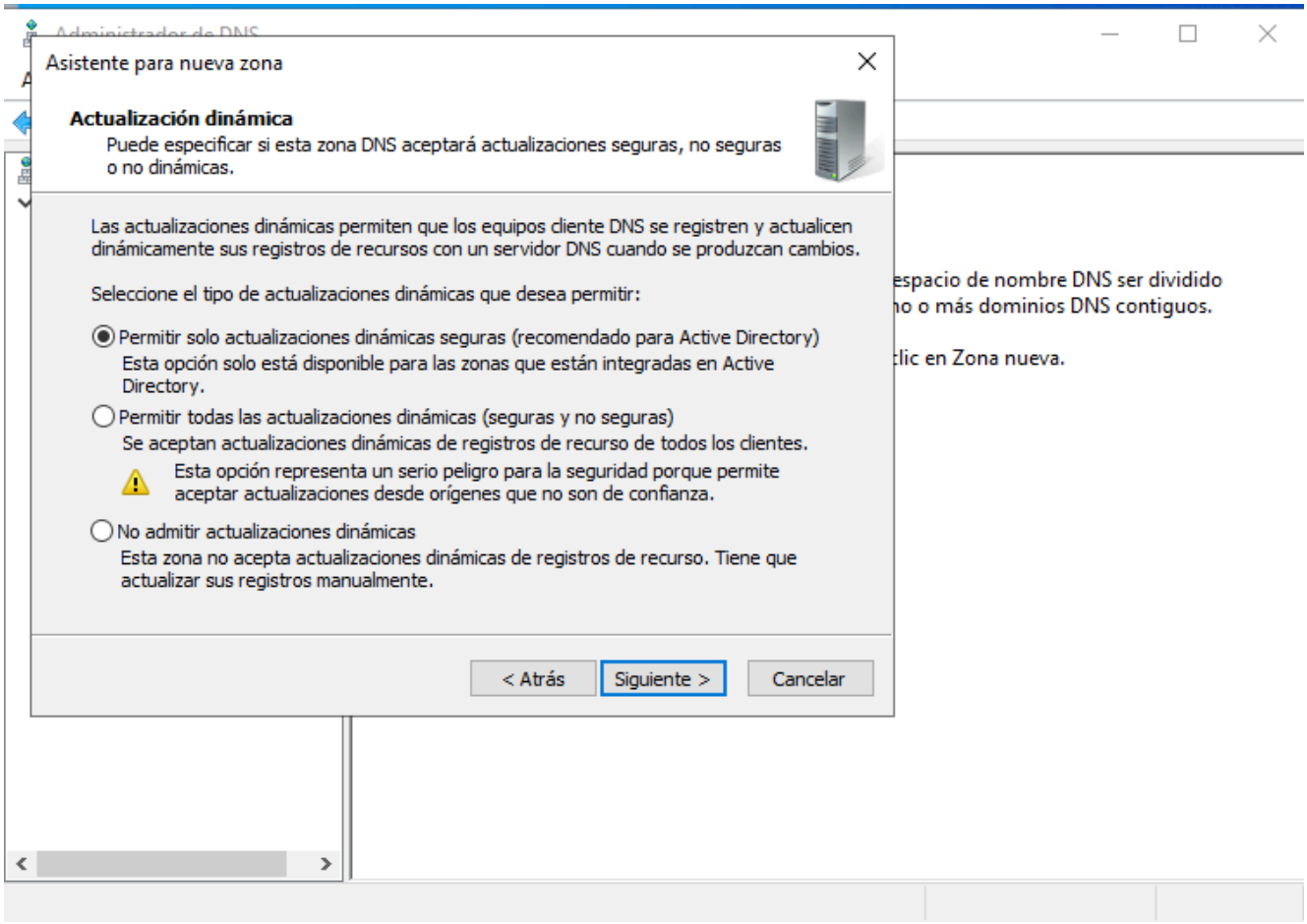
Abrimos la consola de DNS y comenzamos a configurar el asistente para crear una nueva zona de búsqueda inversa. Esta zona permitirá la resolución de direcciones IP hacia nombres de host, lo cual es esencial para una correcta administración de red y para el funcionamiento de ciertos servicios.

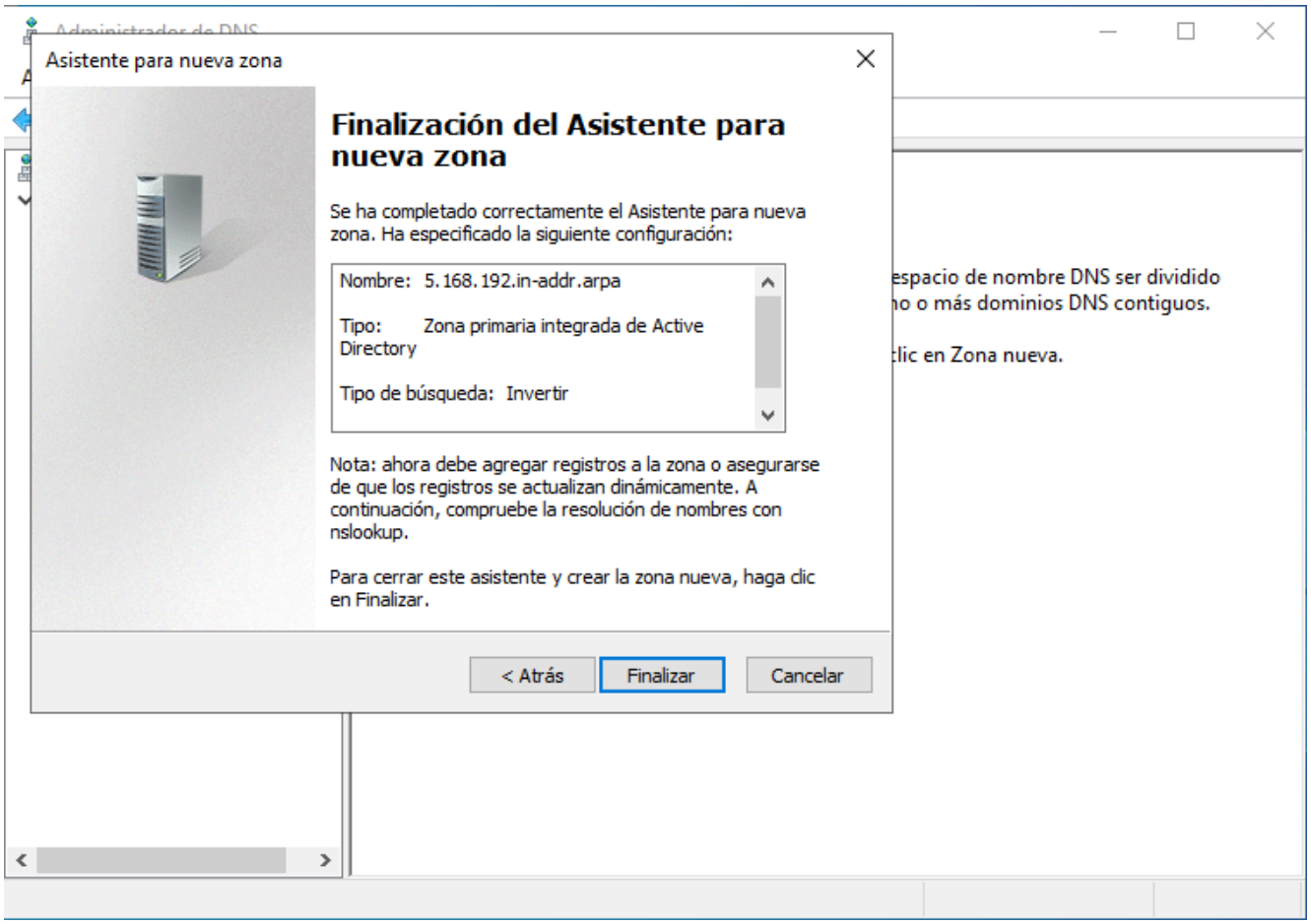



Asistente para nueva zona
Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.
Seleccione el tipo de zona que quiere crear:
Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.
Zona secundaria
Crea una copia de una zona que 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
Siguiente >
Cancelar
espacio de nombre DNS ser dividido
o o más dominios DNS contiguos.
lic en Zona nueva.

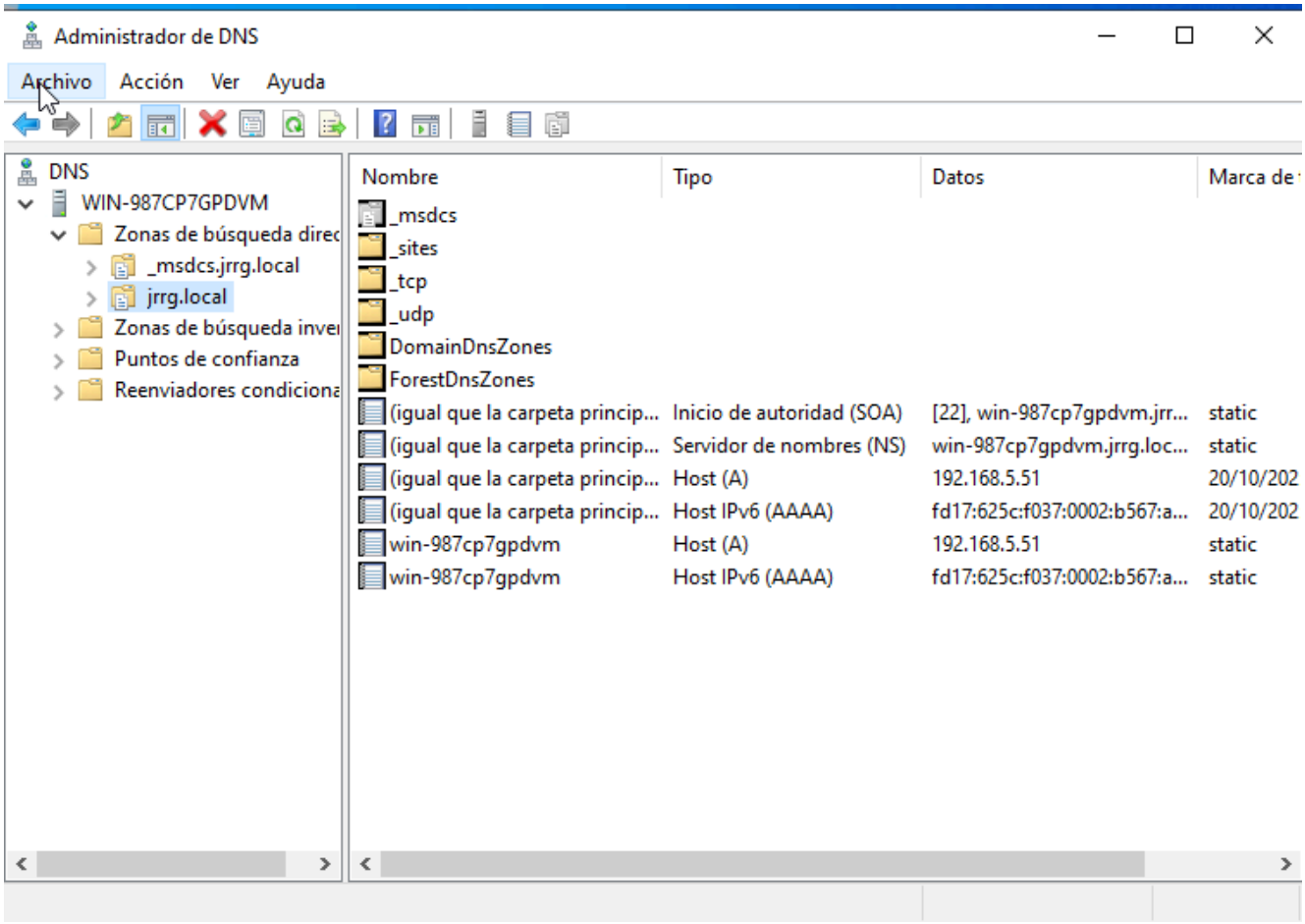

Asistente para nueva zona
Ámbito de replicación de zona de Active Directory
Puede seleccionar cómo desea que se repliquen los datos DNS por la red.
Seleccione cómo quiere que se repliquen los datos de zona:
Para todos los servidores DNS que se ejecutan en controladores de dominio en este bosque: jrrg.local
Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: jrrg.local
Para todos los controladores de dominio en este dominio (para compatibilidad con Windows 2000): jrrg.local
Para todos los controladores de dominio especificados en el ámbito de esta partición de directorio:
< Atrás
Siguiente >
Cancelar
espacio de nombre DNS ser dividido
no o más dominios DNS contiguos.
clic en Zona nueva.


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
< Atrás
Siguiente >
Cancelar
espacio de nombre DNS ser dividido
o o más dominios DNS contiguos.
lic en Zona nueva.


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
espacio de nombre DNS ser dividido
no o más dominios DNS contiguos.
clic en Zona nueva.


Asistente para nueva zona
Finalización del Asistente para nueva zona
Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:
Nombre: 5.168.192.in-addr.arpa
Tipo: Zona primaria integrada de Active Directory
Tipo de búsqueda: Invertir
Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.
< Atrás
Finalizar
Cancelar

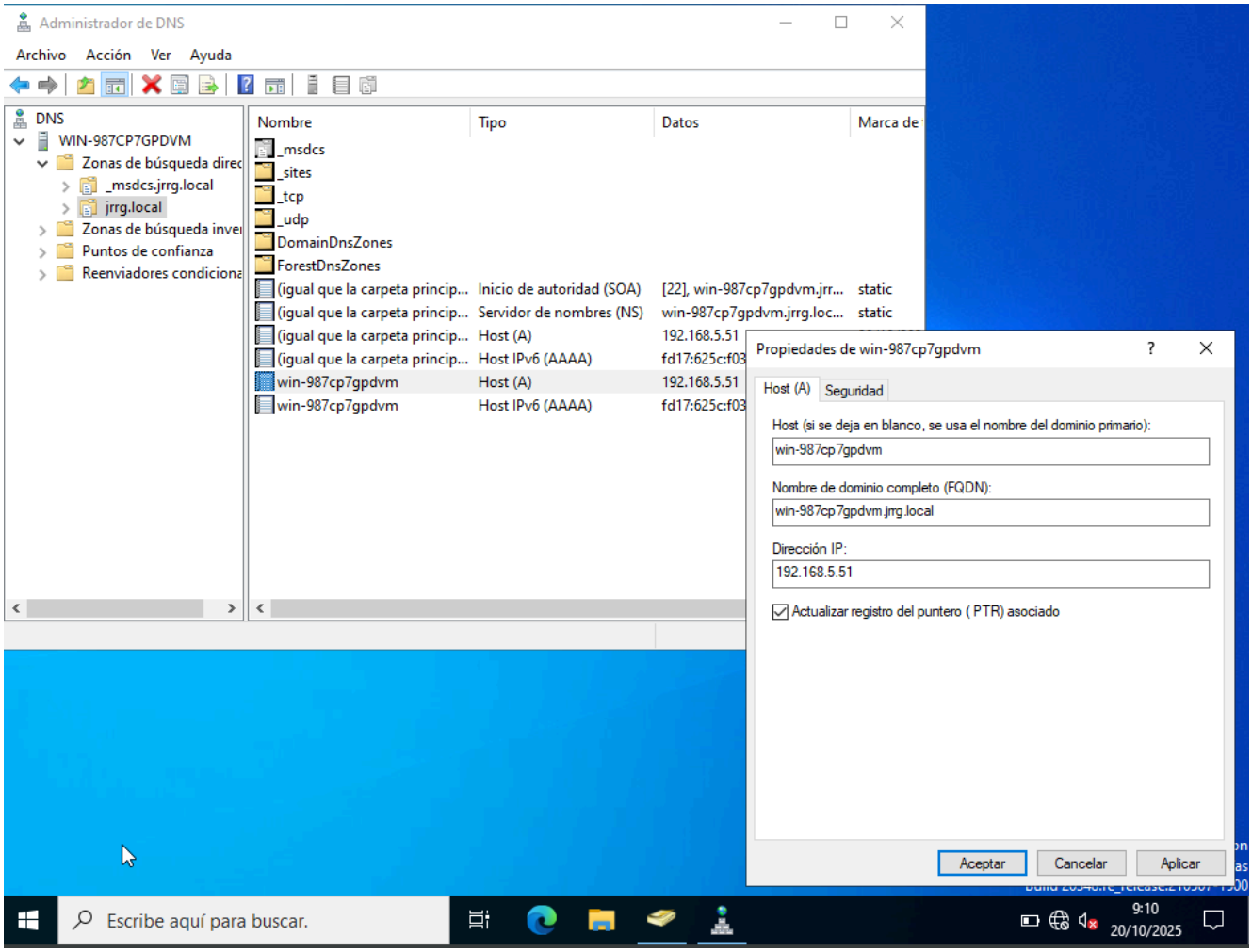
Para comprobar que la zona de resolución inversa está operativa correctamente, accedemos a la zona de búsqueda directa en la consola DNS. Luego, dentro de las propiedades del registro tipo A correspondiente al servidor controlador de dominio, activamos la opción “Crear registro PTR asociado” (marcando el check PTR).



Se ha actualizado correctamente el registro PTR en la zona de búsqueda inversa, lo que valida que la resolución inversa está operativa. Gracias a esto, el servidor DNS puede traducir direcciones IP en nombres de host, una función esencial para:

- Diagnósticos de red más precisos.
- Auditorías y registros de seguridad.
- Compatibilidad con servicios que requieren resolución inversa, como algunos sistemas de correo electrónico y autenticación.

Este paso fortalece la infraestructura DNS y mejora la administración general del entorno de Active Directory.

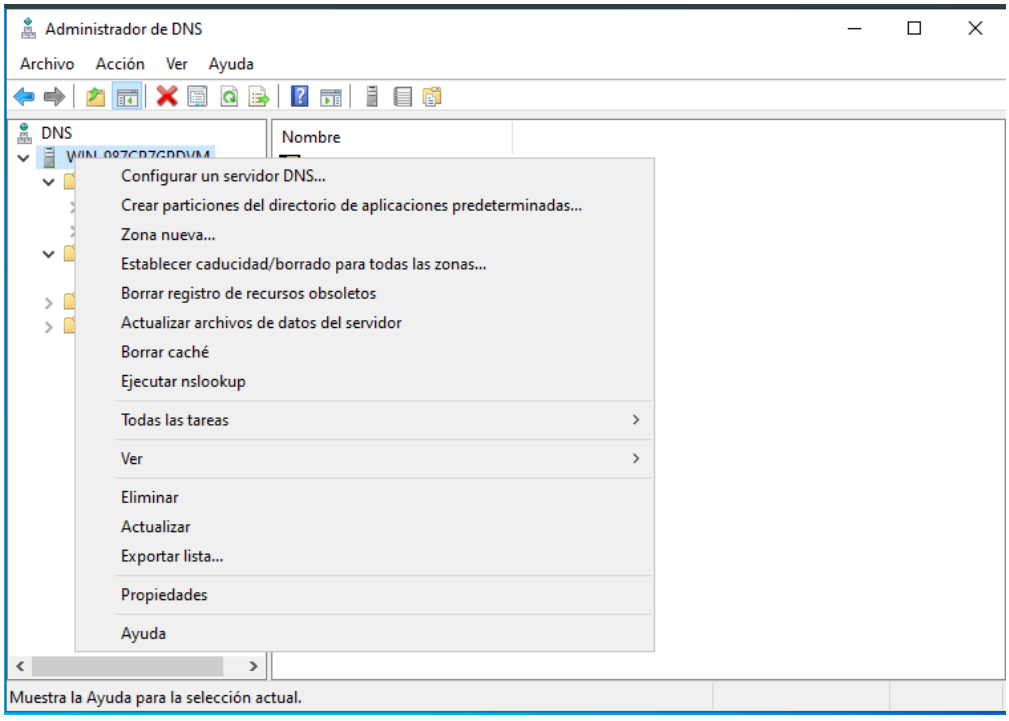


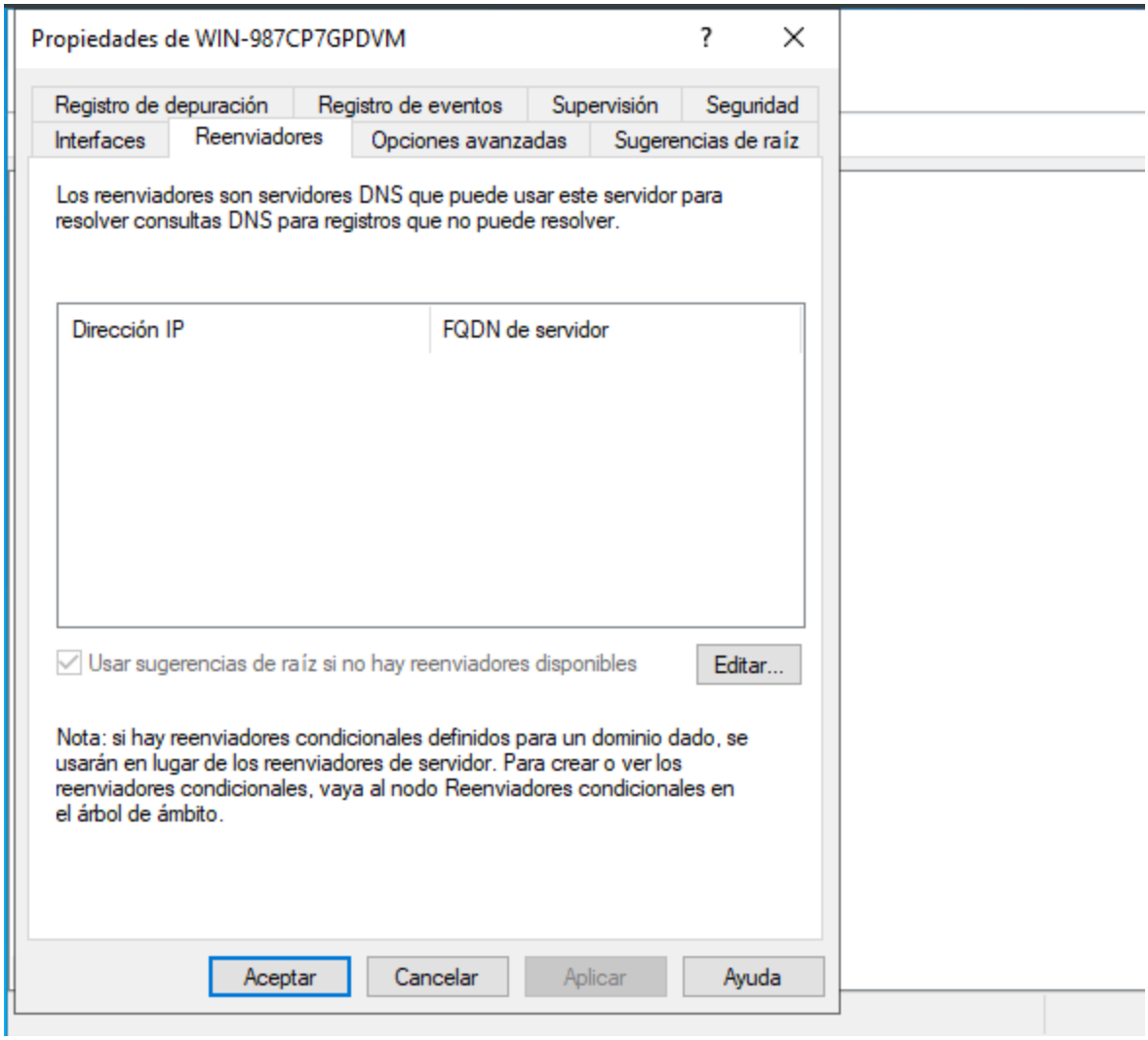
Otra configuración esencial en nuestro servidor DNS es la adición de reenviadores, que permiten que las consultas DNS que no pueden resolverse localmente se redirijan a servidores externos. Esto garantiza la resolución de nombres fuera de nuestro dominio, como sitios web públicos.

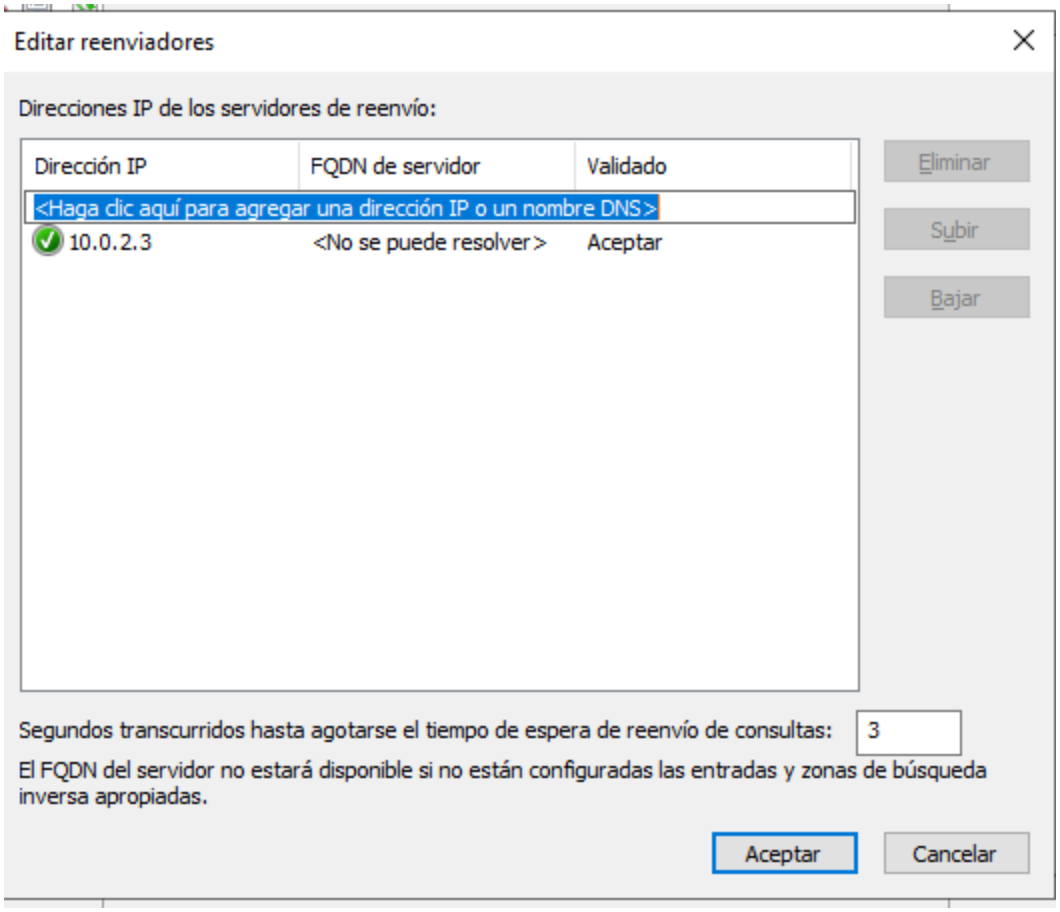
Para configurar los reenviadores, seguimos estos pasos:

1. Abrimos la consola de DNS desde el Administrador del servidor.
2. Hacemos clic derecho sobre el nombre del servidor DNS y seleccionamos Propiedades.
3. En la pestaña Reenviadores, hacemos clic en Editar.
4. Agregamos los siguientes servidores DNS públicos:
    - 8.8.8.8 (Google)
    - 8.8.4.4 (Google)
    - 9.9.9.9 (IBM Quad9, con protección contra malware)
    - 1.1.1.1 (Cloudflare, rápido y seguro)
5. Confirmamos haciendo clic en Aceptar y luego en Aplicar.

Con esto, el servidor DNS podrá resolver nombres externos, mejorando la conectividad y la experiencia de navegación para los equipos dentro del dominio.




Propiedades de WIN-987CP7GPDVM
Registro de depuración
Registro de eventos
Supervisión
Seguridad
Interfaces
Reenviadores
Opciones avanzadas
Sugerencias de raíz
Los reenviadores son servidores DNS que puede usar este servidor para resolver consultas DNS para registros que no puede resolver.
Dirección IP
FQDN de servidor
Usar sugerencias de raíz si no hay reenviadores disponibles
Editar...
Nota: si hay reenviadores condicionales definidos para un dominio dado, se usarán en lugar de los reenviadores de servidor. Para crear o ver los reenviadores condicionales, vaya al nodo Reenviadores condicionales en el árbol de ámbito.
Aceptar
Cancelar
Aplicar
Ayuda


Editar reenviadores
Direcciones IP de los servidores de reenvío:
Dirección IP
FQDN de servidor
Validado
<Haga clic aquí para agregar una dirección IP o un nombre DNS>
10.0.2.3
<No se puede resolver>
Aceptar
Eliminar
Subir
Bajar
Segundos transcurridos hasta agotarse el tiempo de espera de reenvío de consultas:
3
El FQDN del servidor no estará disponible si no están configuradas las entradas y zonas de búsqueda inversa apropiadas.
Aceptar
Cancelar

Configuramos la dirección IP del servidor DNS que responderá a las consultas dentro de nuestra red. Este paso es fundamental para asegurar que los equipos del dominio puedan resolver nombres correctamente.