UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

# Administración de Sistemas Corporativos basados en Windows 2012 Server: Directivas de Grupo

Trabajo Fin de Grado

**Grado en Ingeniería Informática**

**Autor**: María de la Almudena Igualá Villarroya

**Tutor**: Juan Luis Posadas Yagüe

Juan Carlos Cano Escribá

2013-2014

# Resumen

En el siguiente documento se explican las bases para crear un sistema corporativo desde cero, incluyendo la instalación de los servidores y las máquinas cliente, así como la creación de los servidores de DNS y DHCP y el controlador de dominio del Directorio Activo de Windows, además de la creación de usuarios y grupos de usuarios, poniendo especial atención a la instauración de las políticas de grupo, tanto a nivel de usuario como a nivel de máquina.

**Palabras clave:** sistema corporativo, políticas de grupo, Active Directory.

# Abstract

The following document explains the basis for creating a corporate system from scratch, including the installation of servers and client machines, as well as the creation of DHCP and DNS servers and the domain controller in Windows' Active Directory, and the creation of users and user groups, paying particular attention to group policies implementation, both at user level and at machine level.

**Keywords:** operating system, group policies, Active Directory.

# Tabla de contenidos

# 1. Introducción

Hoy en día, vivimos en una sociedad en la que se trabaja con grandes volúmenes de datos, incluso en las pequeñas empresas, y debido al crecimiento constante de este volumen de información, no se puede concebir una empresa sin un sistema de información que la organice y controle el acceso a la misma. Supongamos una pequeña empresa con diez empleados, todos ellos deben acceder diariamente a varias bases de datos de clientes, productos, precios, etc. Además, supongamos que quieren expandirse y abrir una nueva sede en otra ciudad.

Con estas características queda patente la necesidad de esta empresa de disponer de un sistema de información el cual le proporcione los medios necesarios para controlar el acceso y el tratamiento de la información, pues replicar la información en todos los ordenadores sería un gasto enorme e inútil, ya que cada vez que se actualizaran los datos se tendría que ir equipo a equipo actualizando los posibles cambios, renovando software, etc.

Los sistemas corporativos basados en red suponen una solución sencilla y económica al tratamiento de grandes volúmenes de datos, facilitando también el acceso a otros recursos como impresoras, escáneres, etc., además de garantizar un acceso seguro a los datos.

En este marco, Microsoft ofrece su propia solución informática para el mantenimiento de sistemas de información, el directorio activo o Active Directory, que permite la creación y mantenimiento de este tipo de sistemas. Estos sistemas tienen gran aceptación en el entorno empresarial, siendo Microsoft uno de los proveedores de Sistemas Operativos más utilizados en éste.

## 1.1 Objetivo y diseño

El objetivo principal de este Trabajo de Fin de Grado es el de proporcionar una sencilla guía de creación de un sistema en Active Directory basado en Windows Server 2012, poniendo especial atención al estudio de las directivas de grupo, qué son, cómo se aplican, etc.

Para ello se ha diseñado un pequeño sistema ficticio, bastante similar a los sistemas que un ingeniero pueda encontrar en su futuro laboral, aunque a menor escala. Este sistema contará con varias máquinas, tanto servidoras como clientes, y una serie de usuarios que se conectarán a ellas.

En nuestro diseño habrá dos servidores, uno principal y otro secundario que, además de replicar las características del principal, actuará como servidor de archivos, y dos máquinas clientes, a las que se conectarán los usuarios.

# 2. Instalación de los sistemas

Para poder implementar el diseño propuesto en el apartado anterior, se van a utilizar dos servidores con sendas instalaciones de Windows Server 2012. Ambos servidores actuarán como controlador de dominio para dotar de mayor robustez al sistema, además el servidor principal también hará las veces de servidor DNS y DHCP. Por otro lado, se dispone también de dos máquinas cliente con sistema operativo Windows 7.

Las cuatro instalaciones se llevarán a cabo utilizando máquinas virtuales, con VirtualBox como entorno de virtualización.

Ambas máquinas servidoras cuentan con la misma configuración hardware, 40 GB de disco duro, 1.5 GB de memoria RAM, procesador de 64 bits a 2.4 GHz y un adaptador Ethernet en modo puente. Las máquinas cliente tienen una configuración hardware similar, solo que en este caso, los discos duros son de 20 GB.

Una vez las máquinas han sido creadas en el entorno de virtualización, se procede a la instalación de los servidores. Para ello, en este caso se dispone de una imagen del servidor en el ordenador, y simplemente se le indica al entorno de virtualización dónde se encuentra ésta para que se pueda proceder a la instalación.

Al arrancar la máquina, ésta detecta la presencia de la imagen y comienza con el proceso de instalación.

En la primera pantalla, que podemos observar en la Figura 1, se eligen el idioma de la instalación, el formato de hora y moneda y el idioma del teclado.

Una vez seleccionado el idioma y el modo de entrada del teclado, nos da la opción de instalar o reparar el equipo, en este caso, se pulsa el botón de instalar.

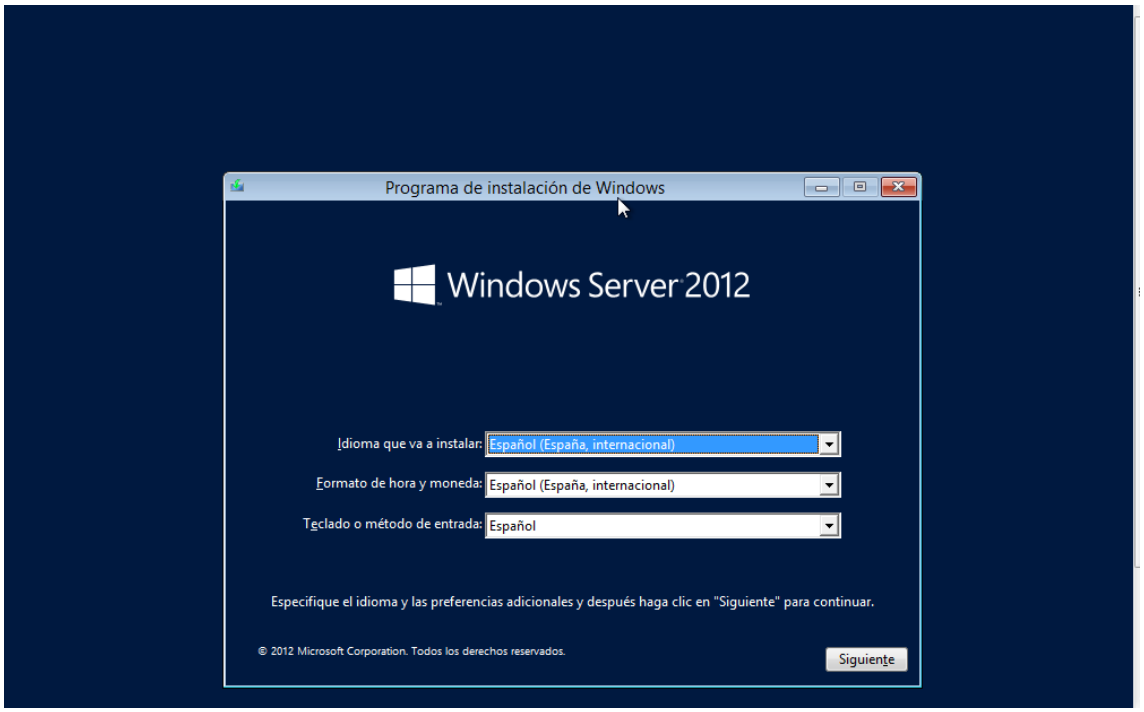


*Figura 1: Pantalla inicial de la instalación*

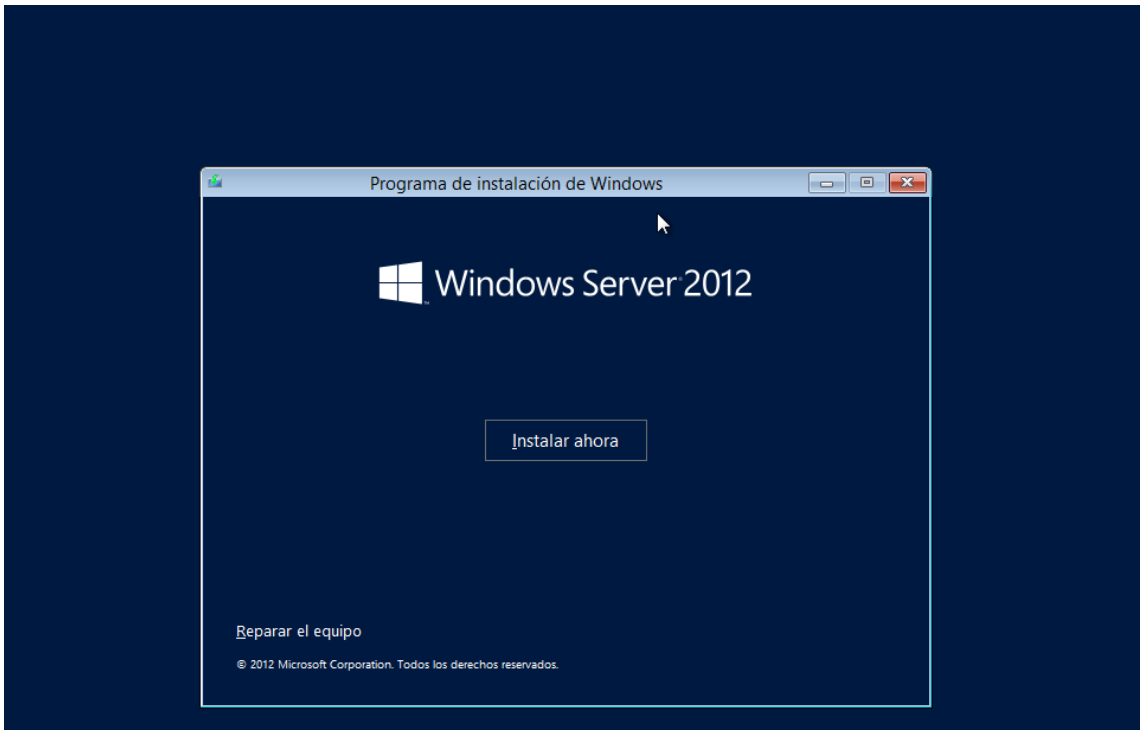


*Figura 2: Instalación*

A continuación, se nos pide la clave de activación que hemos conseguido mediante la herramienta Microsoft DreamSpark.

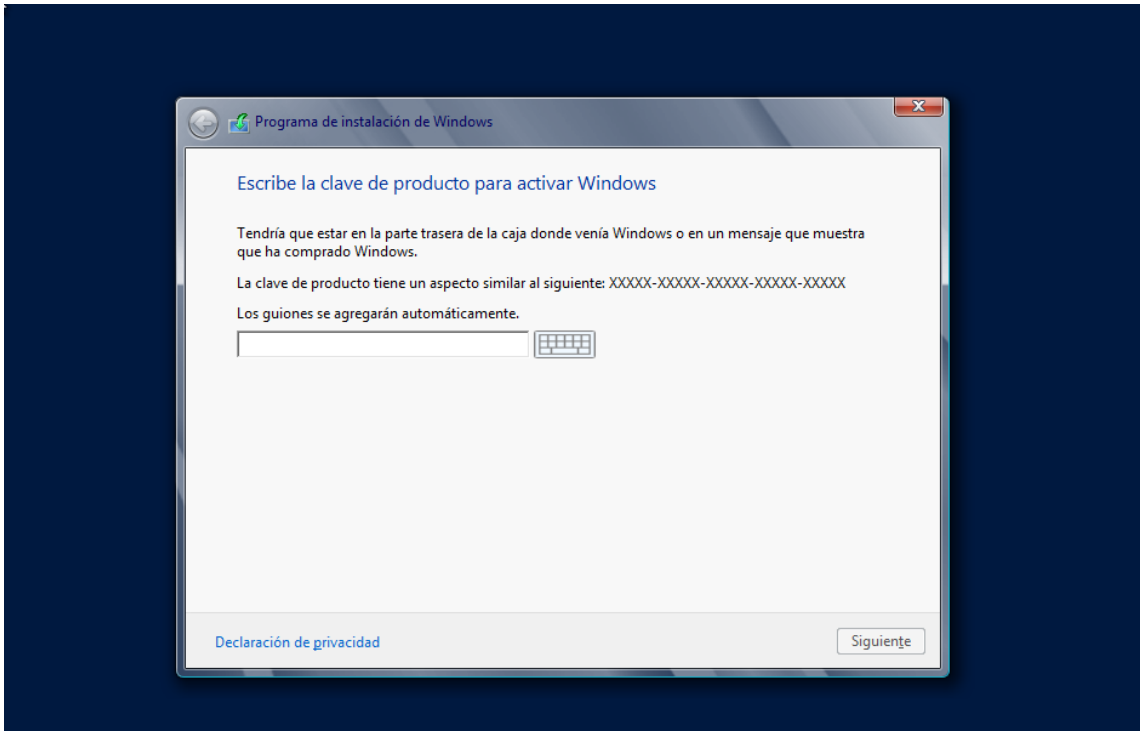


*Figura 3: Clave de activación*

A continuación se nos da a elegir entre la posibilidad de instalar el servidor como "Server Core", o como "Servidor con una GUI".

El modo "Server Core" no posee ningún tipo de interfaz, y todas las tareas de administración, como por ejemplo la creación de usuarios o la instalación de roles y características se realizan por consola de comandos. El "Servidor con una GUI" posee una potente y cómoda interfaz gráfica, además de las características incluidas en la versión Server Core. Dependiendo del uso que se les vaya a dar a los servidores, es importante saber seleccionar la versión a instalar. Nosotros seleccionaremos la opción servidor con una GUI,  pues nos facilitará las tareas de creación de los servidores y usuarios.

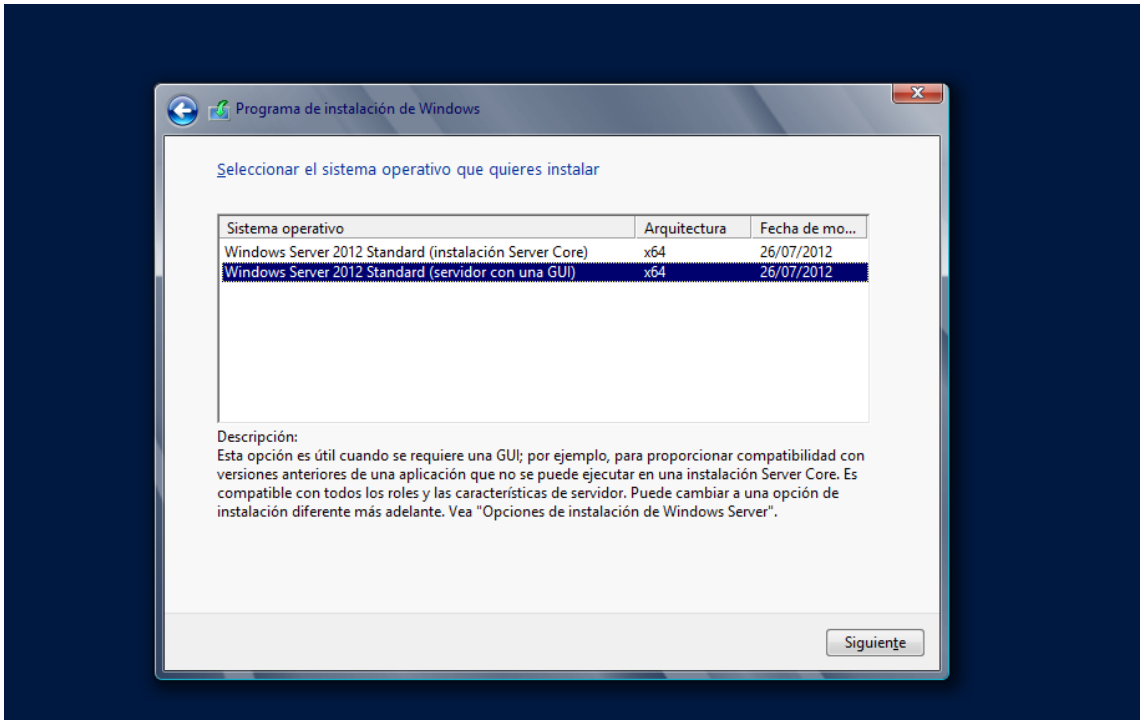


*Figura 4: Selección del Sistema operativo*

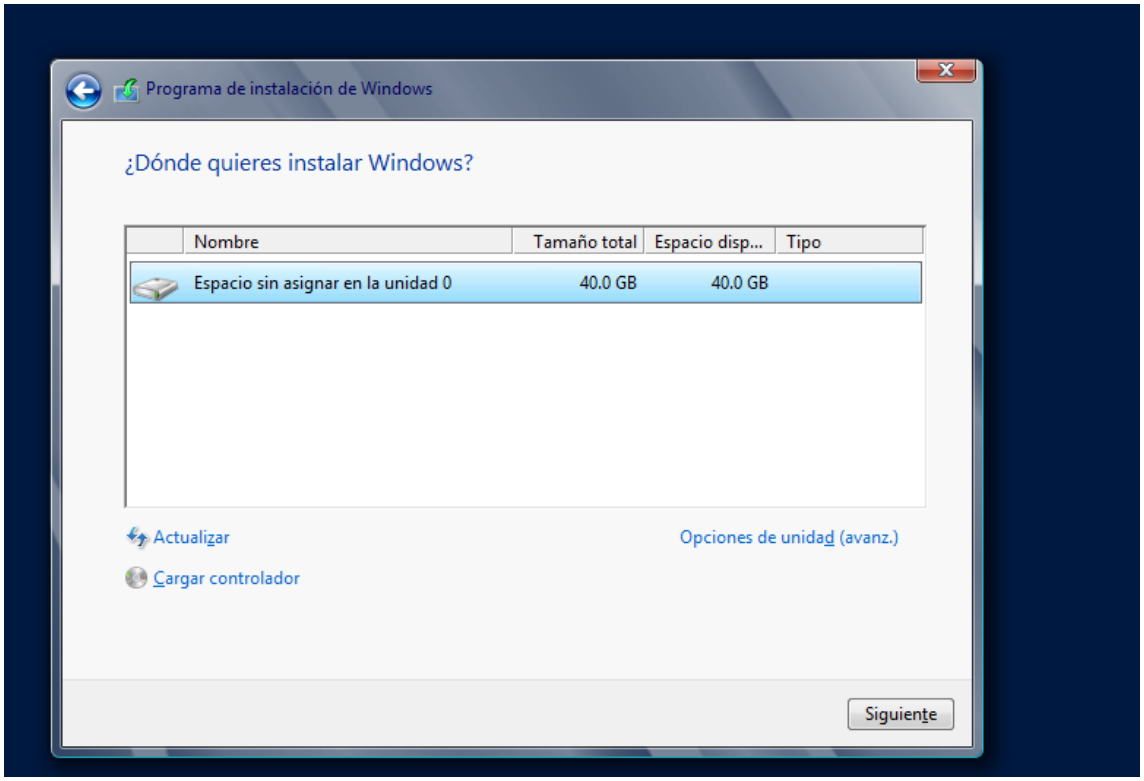


*Figura 5: Asignación del disco duro*

Tras seleccionar el disco duro para instalar el sistema y aceptar el acuerdo de licencia, el programa de instalación está preparado para comenzar a extraer los archivos y empezar con la instalación.

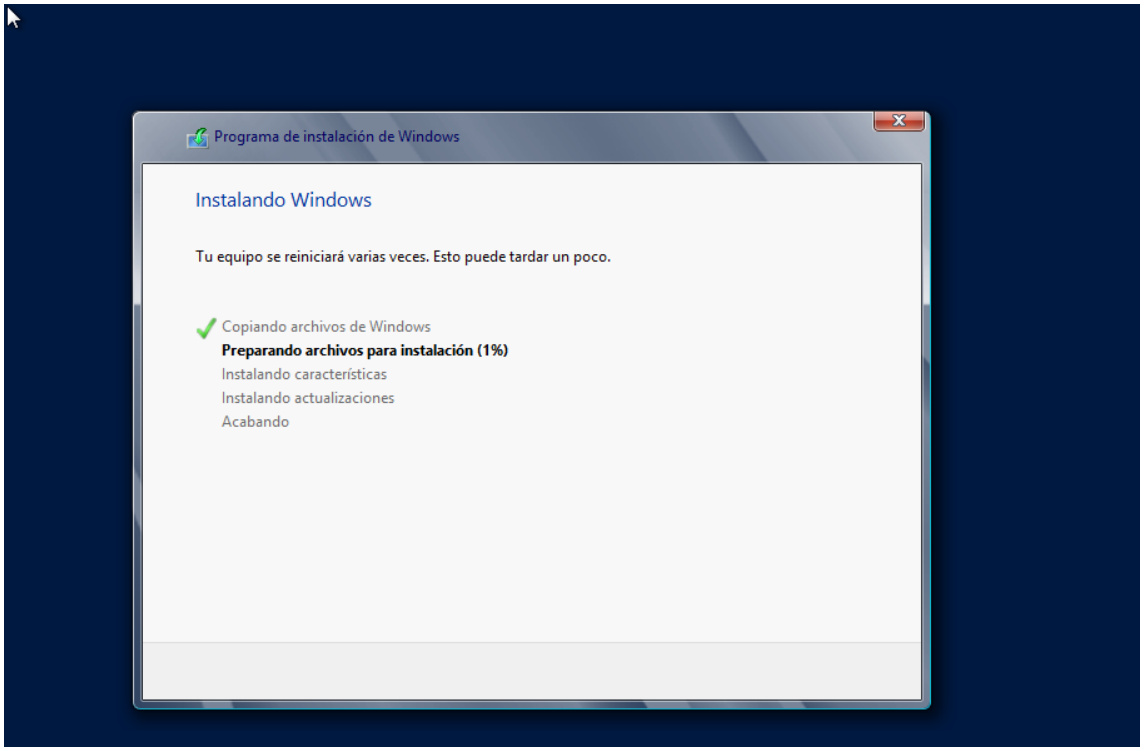


*Figura 6: Instalación*

Finalmente, se elige una contraseña para la cuenta de administrador y se inicia sesión, siendo la consola de administración del servidor lo primero que se carga automáticamente al iniciar la sesión en el servidor.

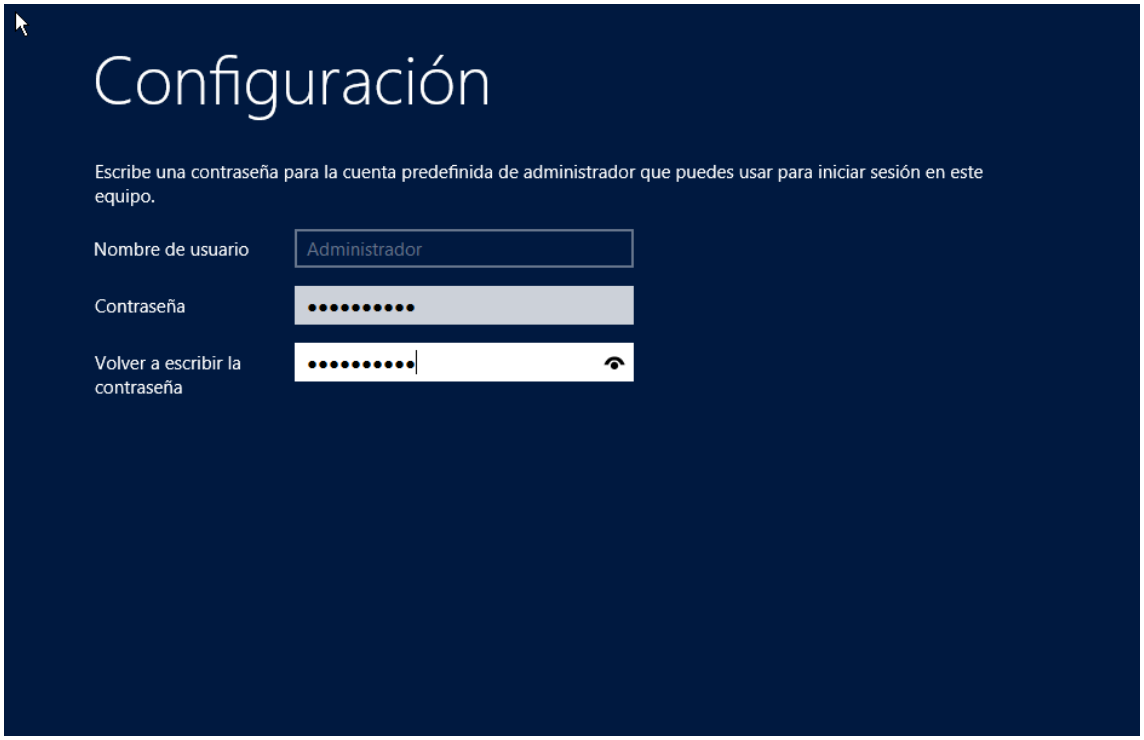


*Figura 7: Establecimiento de la contraseña de Administrador*

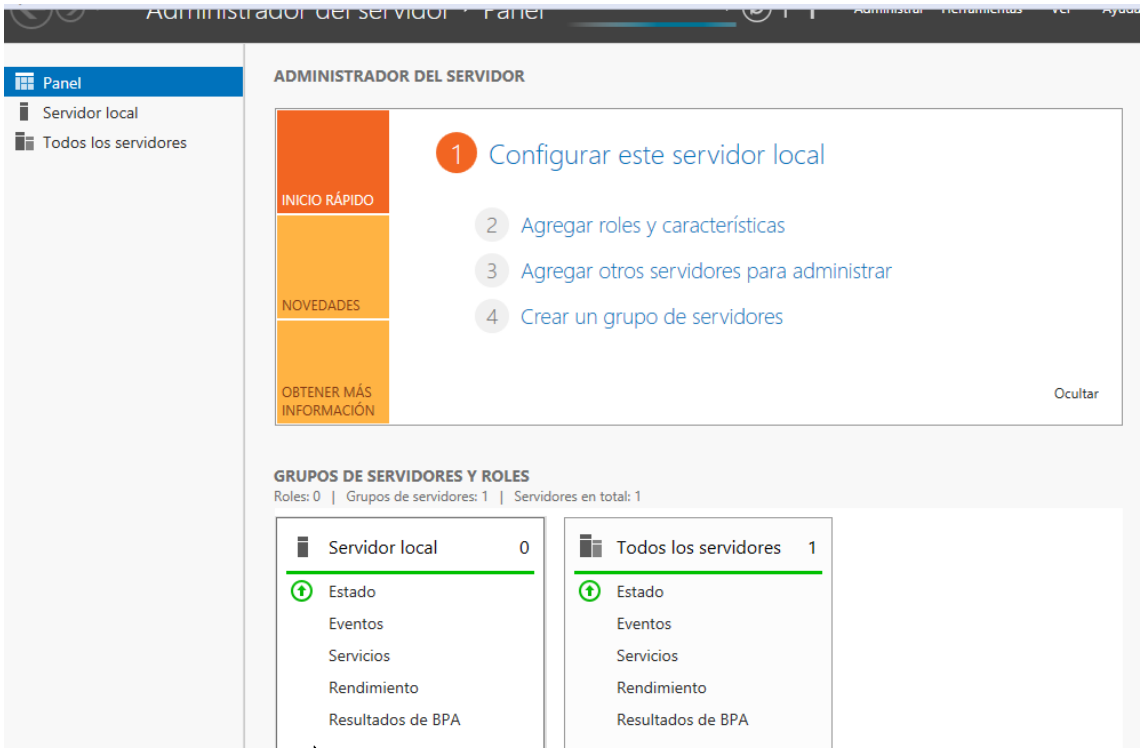


*Figura 8: Consola de Administración del servidor*

# 3. Active Directory

Active Directory es el término por el que se conoce a la implementación de Microsoft del servicio de directorio en una red distribuida de computadores. El servicio de directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red, facilitando así su localización y administración.

Este servicio proporciona una estructura jerárquica que permite mantener objetos relacionados con la red tales como usuarios, grupos de usuarios, permisos, políticas de acceso etc., además de facilitar a los administradores las tareas de actualización, despliegue de programas en varios ordenadores, y el establecimiento de políticas a nivel de empresa.

## 3.1 Estructura del directorio activo

El funcionamiento de Active Directory se basa en el estándar LDAP (Lightweight Directory Access Protocol), "un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red".

Un sistema distribuido en Active Directory se compone de dominios y subdominios, éstos a su vez están compuestos de unidades organizativas, todo ello englobado en un bosque como se muestra en la Figura 9, extraída de las transparencias de la asignatura Administración de Sistemas.

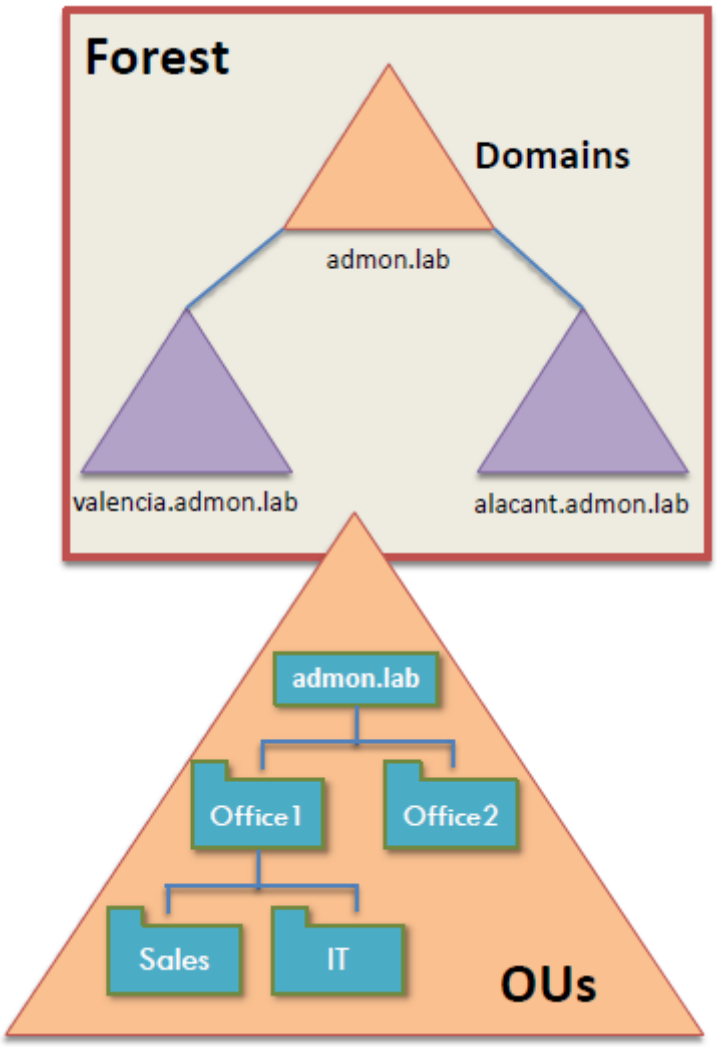


*Figura 9: Estructura del sistema*

Gracias a esta estructura en forma de árbol, un usuario creado en un dominio, podrá ser utilizado en todo el árbol que se genera a partir del mismo, sin necesidad de que este pertenezca a todos los subdominios.

Los dominios están formados por varios sistemas que comparten una base de datos de Active Directory y están nombrados a partir de un nombre de dominio del servidor DNS. Éstos se componen de uno o más controladores de dominio, que deben ser servidores de Windows y cero o más miembros, que pueden ser tanto servidores de Windows, como cualquier otra máquina cliente con sistema operativo Windows.

Además el bosque, o cada dominio pueden estar en distintos niveles funcionales, cada nivel determina tanto las funcionalidades disponibles como la retro compatibilidad con versiones anteriores de AD. Entre los distintos dominios se pueden establecer relaciones de confianza, éstas permiten que usuarios de un dominio puedan ser reconocidos en otros dominios.

Finalmente, el catálogo global es una partición que almacena una vista parcial de todos los objetos del bosque, permitiendo así la búsqueda de objetos en el mismo, el catálogo global debe existir en, al menos, uno de los controladores de dominio.

## 3.2 Creación del bosque y configuración del servidor DNS.

Antes de crear el bosque y asignar el servidor como controlador de dominio y servidor de DNS, sería interesante explicar qué es un servidor DNS y para qué se utiliza.

Un servidor DNS es una máquina que posee una base de datos en la que están registradas las relaciones que se establecen entre cada nombre de dominio y su dirección IP. En el caso de internet, se utiliza para traducir las url's que utilizamos habitualmente en direcciones IP, en el caso de un sistema distribuido utilizando Active Directory, los clientes y las herramientas de cliente de AD lo utilizan para localizar los controladores de dominio con el fin de realizar tareas de administración e inicios de sesión.

Un DNS puede trabajar de tres formas distintas:

-Resolución de nombres: es el modo de funcionamiento habitual del DNS, convierte un nombre de host en una dirección IP.

-Resolución inversa de direcciones: es el mecanismo inverso al anterior, al proporcionarle la IP de un host, nos devuelve el nombre correspondiente.

-Resolución de servidores (por ejemplo, correo): Dado un nombre de dominio, obtiene la IP del servidor a través del cual se debe encaminar la petición.

Para poder crear el bosque y configurar el servidor DNS, primero se debe asignar al servidor una IP fija. Para ello se abre el "Centro de redes y recursos compartidos" de Windows, y se selecciona nuestra conexión de internet.

A continuación se hace clic en Detalles, y se abrirá una ventana donde podremos ver cuál es la IP pública que tiene asignada nuestra máquina, la máscara de subred, la puerta de enlace y el servidor DNS. Una vez conocemos estos datos, cerramos la ventana de Detalles y clicamos en Propiedades, en el listado de elementos se selecciona Protocolo de Internet versión 4(TCP/IPv4) y pulsamos nuevamente en Propiedades.

En la ventana que aparece a continuación vemos que tanto la IP como la dirección del servidor DNS se obtienen automáticamente, en este caso vamos a configurarlas manualmente, ya que así nos aseguraremos de que nuestro servidor siempre tendrá la misma IP.

Para ello, en la pestaña General, se marca la opción Usar la siguiente dirección IP e introducimos como IP: 192.168.1.217, que es la IP pública que nos había asignado nuestro servidor DHCP, como máscara de subred 255.255.255.0 y como puerta de enlace 192.168.1.1. Para el DNS utilizaremos como DNS principal la dirección 62.81.16.164, y como DNS secundario 62.81.16.213 y, finalmente pulsamos aceptar en las demás ventanas.

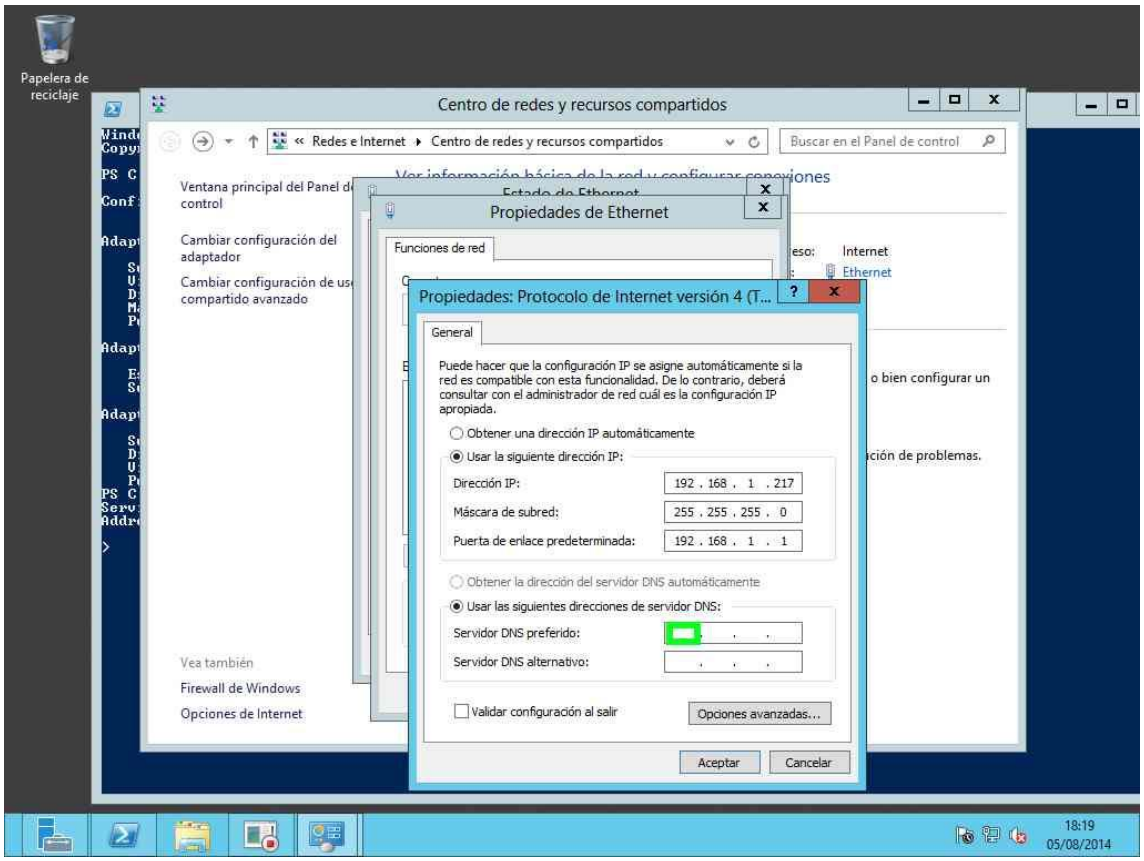


*Figura 10: Asignación de la dirección IP*

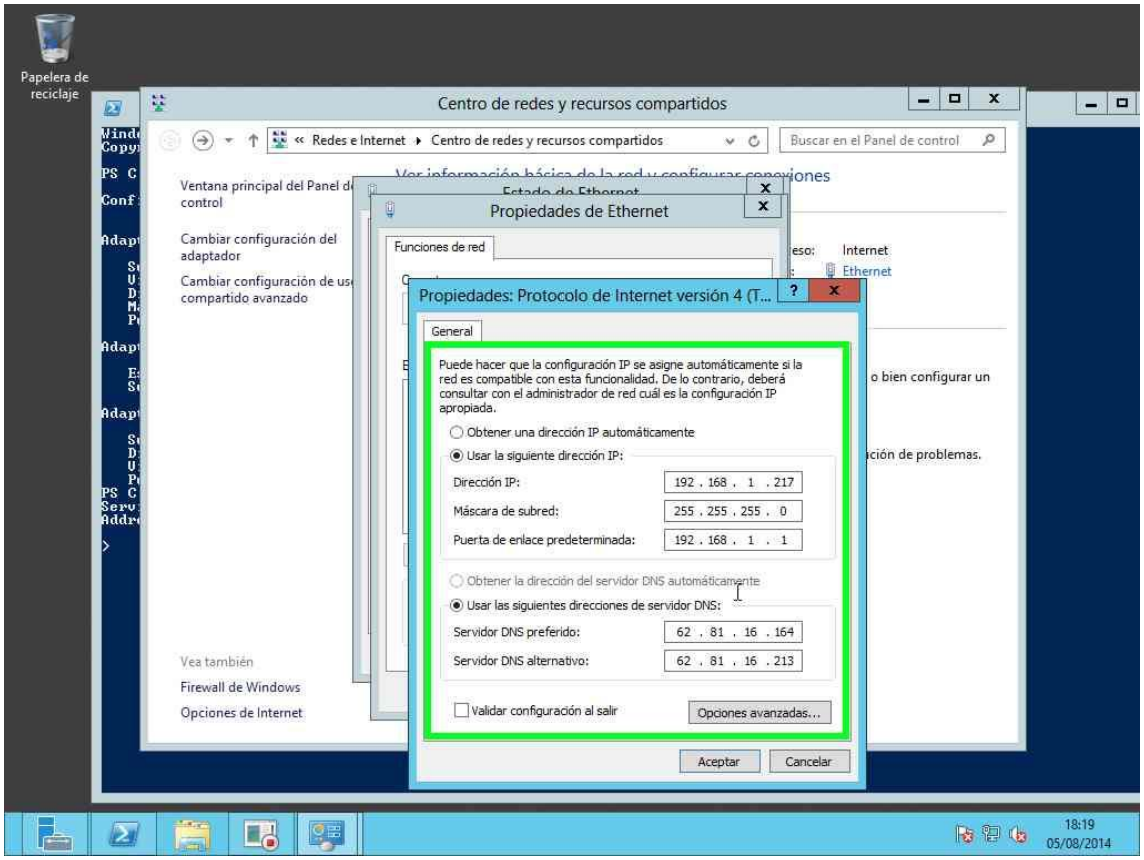


*Figura 11: Asignación de los DNS*

Una vez está fijada nuestra IP, ya podemos abrir el panel de Administración del Servidor y seleccionar la opción Agregar roles y características.

La primera pantalla que nos aparece son una serie de recomendaciones a la hora de instalar roles, como por ejemplo asegurarse de que la contraseña es segura, que la dirección IP de las máquinas es fija, etc. Pulsamos siguiente.

En la siguiente pantalla seleccionamos la opción "Instalación basada en características o en roles" y, nuevamente, pulsamos siguiente. A continuación nos da la opción de seleccionar un servidor de un listado o de un disco duro virtual. En el listado solamente aparece nuestro servidor principal, pulsamos siguiente. Seguidamente, el asistente nos proporciona un listado de roles para instalar. En este caso, escogemos Servicios de Dominio de Active Directory, y se abrirá una ventana emergente donde nos pregunta si queremos instalar las características requeridas para los Servicios de dominio, pulsamos Agregar características.

En la siguiente ventana, dejamos las opciones por defecto y pulsamos siguiente. Volvemos a pulsar siguiente en la nueva ventana y, finalmente aparece una ventana con un resumen de las configuraciones que hemos ido seleccionando a lo largo del proceso, revisamos que están bien y pulsamos instalar.

En este momento, aparece una ventana con el progreso de la instalación, y, llegados a cierto punto nos indica que se necesitan pasos adicionales para convertir el servidor en controlador de dominio.

Pulsamos en “Promover este servidor a controlador de dominio” y nos aparecerá un nuevo asistente en el que podremos crear el bosque.

En la primera ventana de este nuevo asistente nos da varias opciones: “Agregar un controlador de dominio a un dominio existente”, “Agregar un nuevo dominio a un bosque existente” y “Agregar un nuevo bosque”. En este caso seleccionaremos “Agregar un nuevo bosque” y como nombre del dominio raíz ponemos tfg.test.

En la siguiente ventana del asistente seleccionamos el nivel funcional del bosque, nos da opción de seleccionar desde Windows Server 2003 en adelante, en este caso seleccionamos Windows Server 2012 tanto como nivel funcional del bosque, como del dominio, dejamos las opciones marcadas por defecto y escribimos una contraseña para el modo de restauración de servicios de directorio DSRM.

Al no detectar una zona DNS para el dominio, el propio asistente la creará.

A continuación, el asistente nos solicita de verifiquemos el nombre NetBIOS del dominio y, de ser necesario, lo cambiemos. El nombre NetBIOS de nuestro dominio es TFG.

Después, el asistente solicitará las rutas de almacenamiento para la base de datos, el archivo de registro y el volumen del sistema, para las cuales él mismo nos proporciona unas rutas por defecto, aceptamos y continuamos.

Al igual que en el asistente anterior, cuando estamos a punto de finalizar la instalación, nos da un resumen de las configuraciones asignadas por el momento, aceptamos y, finalmente, el sistema hace una comprobación de requisitos, si el sistema pasa éstas comprobaciones se podrá pulsar Instalar y proceder finalmente a la promoción del servidor como controlador de dominio.

Al finalizar la instalación, el servidor se reinicia automáticamente y, al pulsar Ctrl+Alt+Supr para iniciar la sesión, vemos que el usuario aparece como TFG\Administrador, indicándonos así que el bosque ha sido creado.

Ahora que ya está creado el bosque y su dominio raíz, el Administrador del sistema ya puede empezar a crear usuarios, grupos de usuarios, etc. Sin embargo, teniendo en cuenta que toda la información del sistema está guardada en un solo servidor, a estas alturas deberíamos plantearnos la creación de un controlador adicional en el dominio tfg.test.

# 3.3 Configuración del servidor DHCP

También se ha asignado al servidor principal la tarea de asignar las IPs a los demás ordenadores de la red. Para ello le hemos otorgado además el rol de servidor DHCP.

Primero, y como en el caso anterior, en la consola de Administración del Servidor hacemos clic en Agregar roles y características, seleccionamos el servidor y en la selección de roles elegimos Servidor DHCP. A partir de aquí la instalación es idéntica a la de los servicios de Active Directory explicada en el apartado anterior.

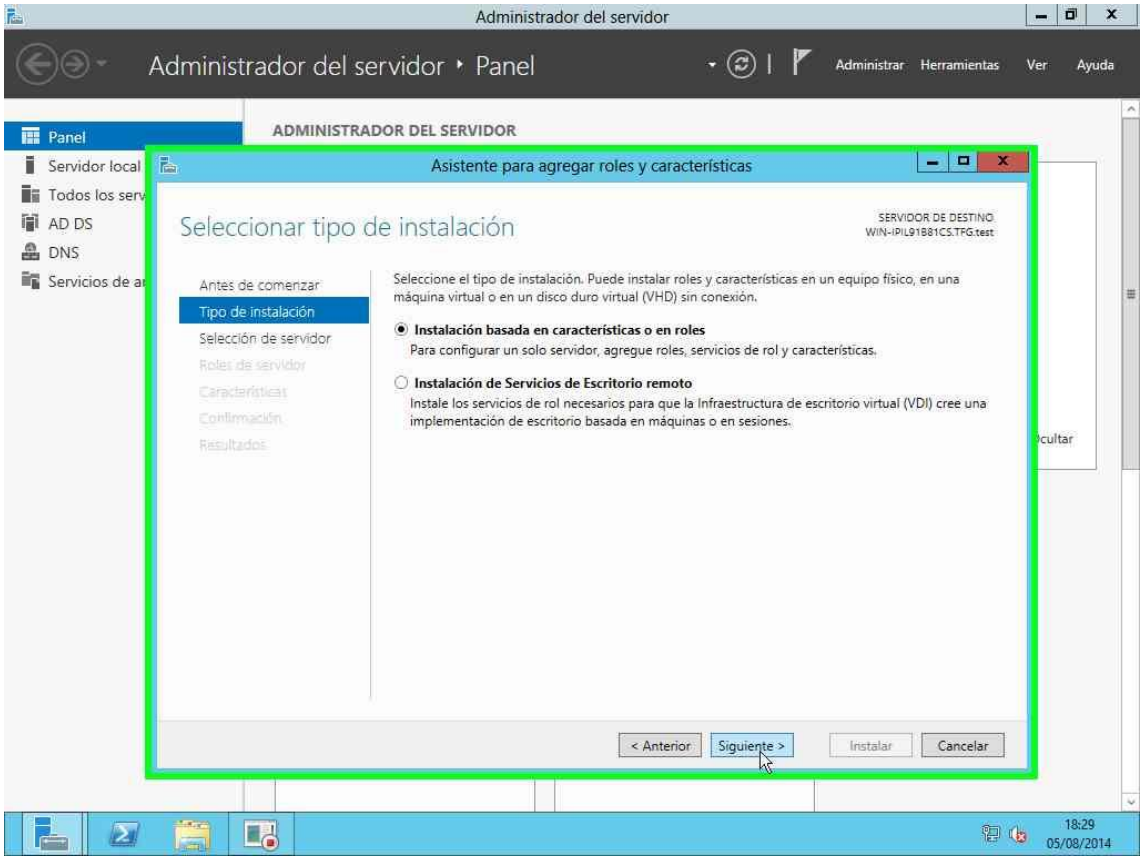


*Figura 12: Primera fase Instalación servidor DHCP*

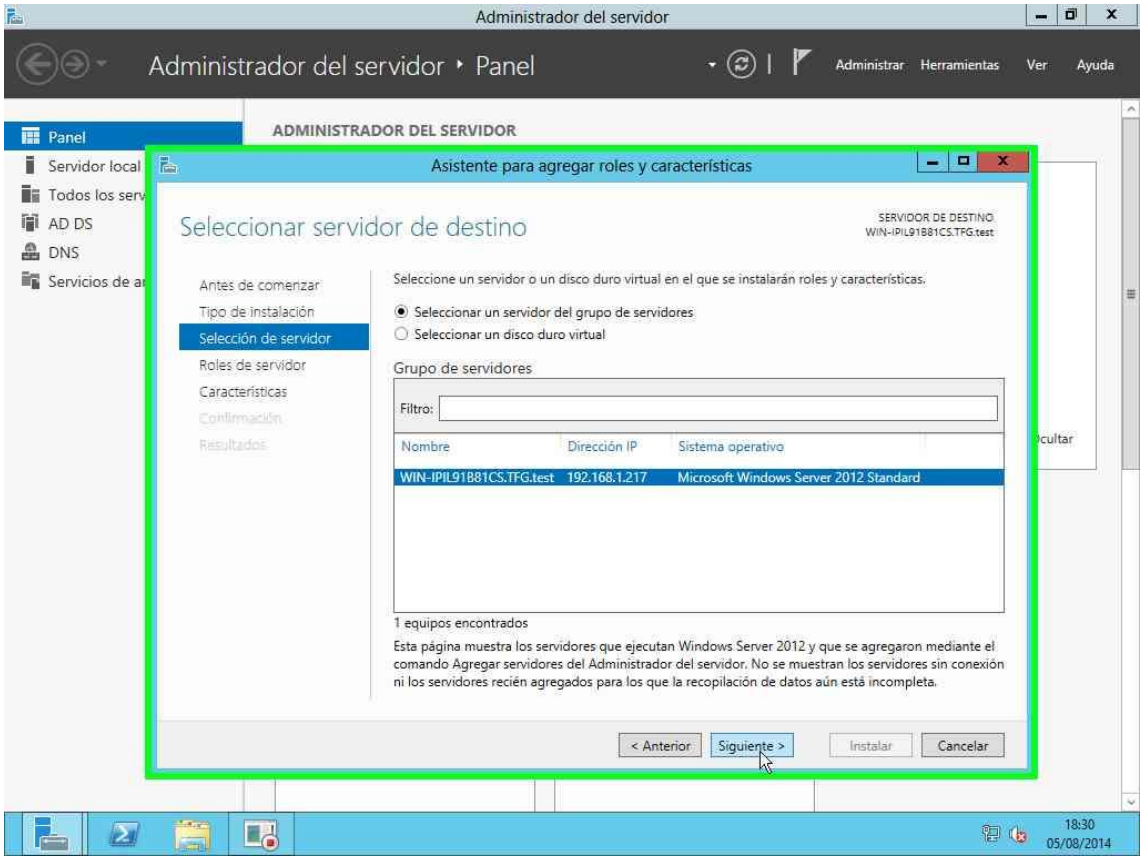


*Figura 13: Selección del servidor*

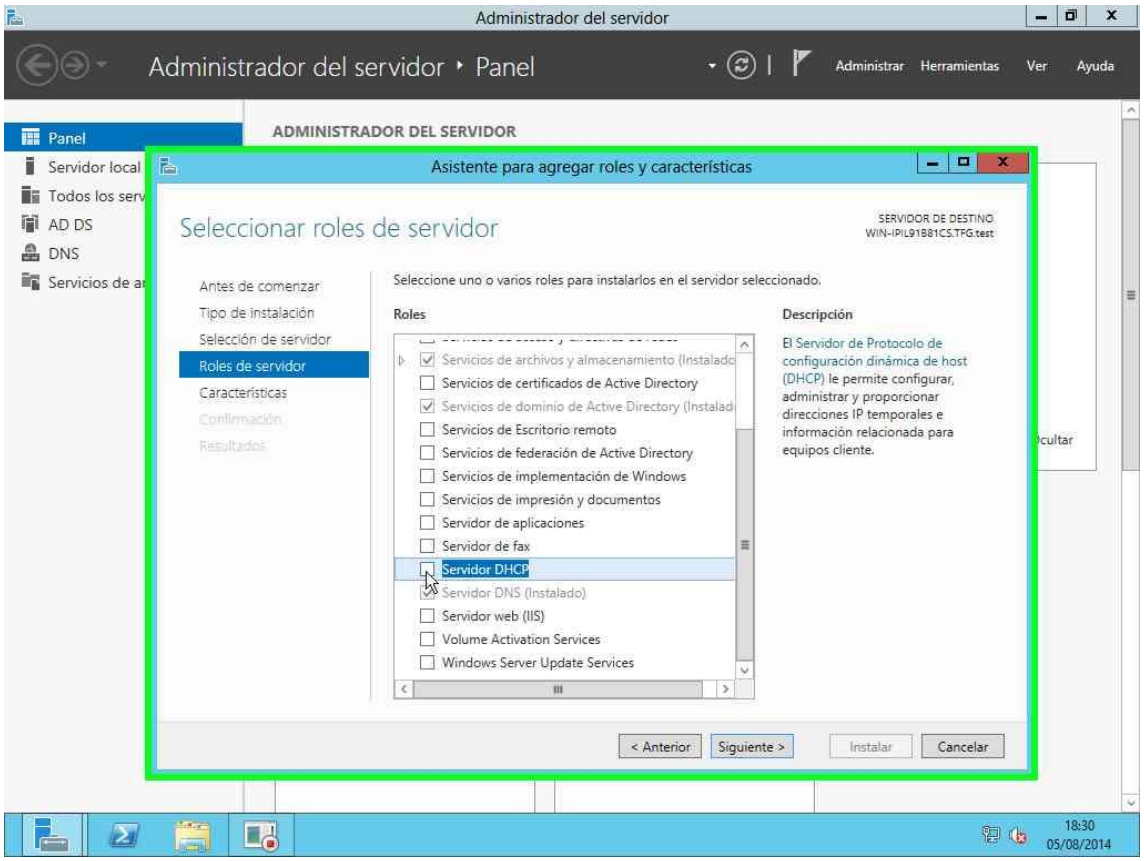


*Figura 14: Selección del rol Servidor DHCP*

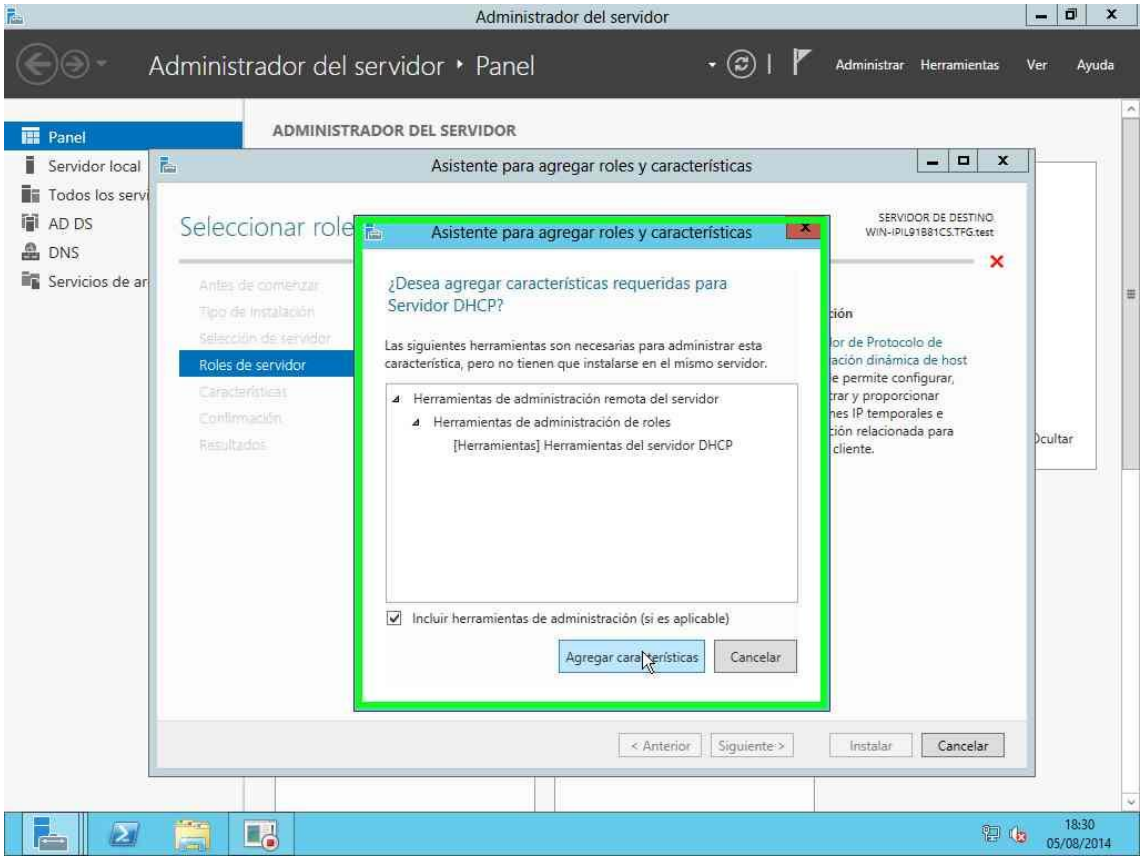


*Figura 15: Características I*

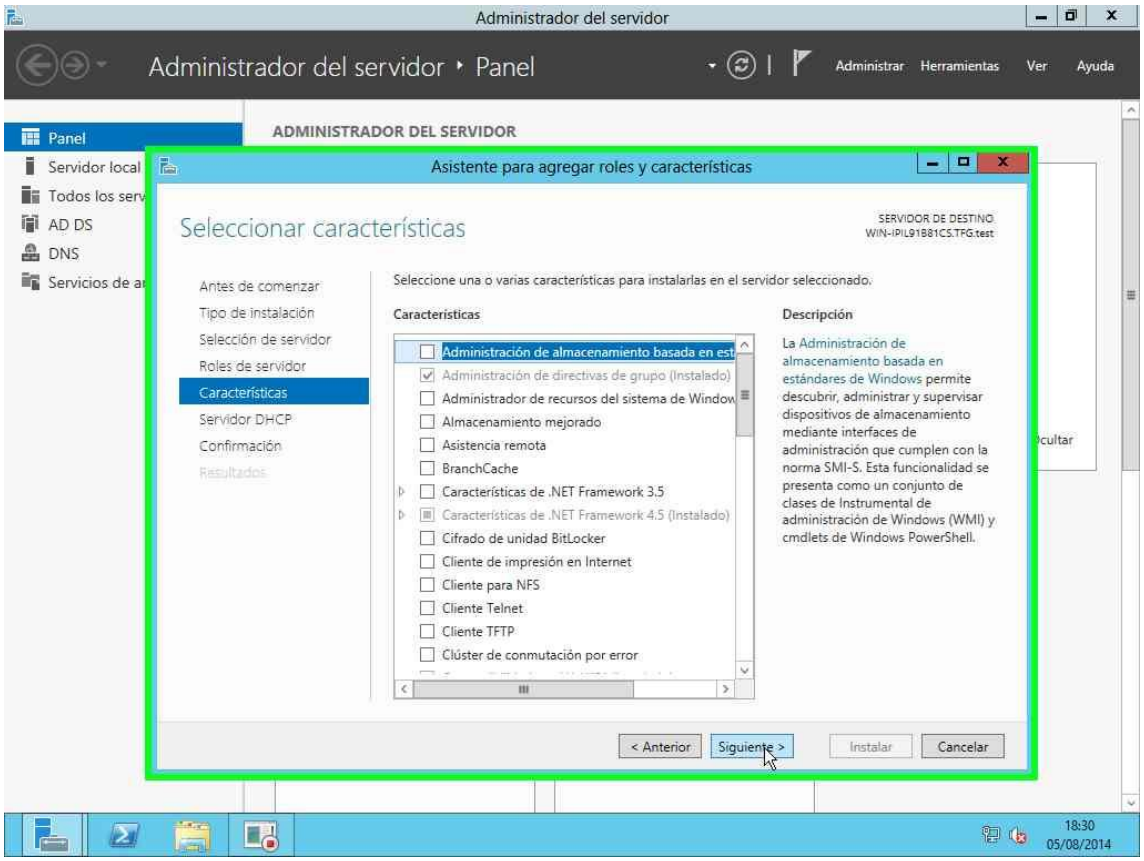


*Figura 16: Características II*

Una vez terminada la instalación inicial, el asistente nos da la opción "Completar configuración de DHCP", seleccionamos ésta opción y se nos abre un nuevo asistenta para configurar el servidor.

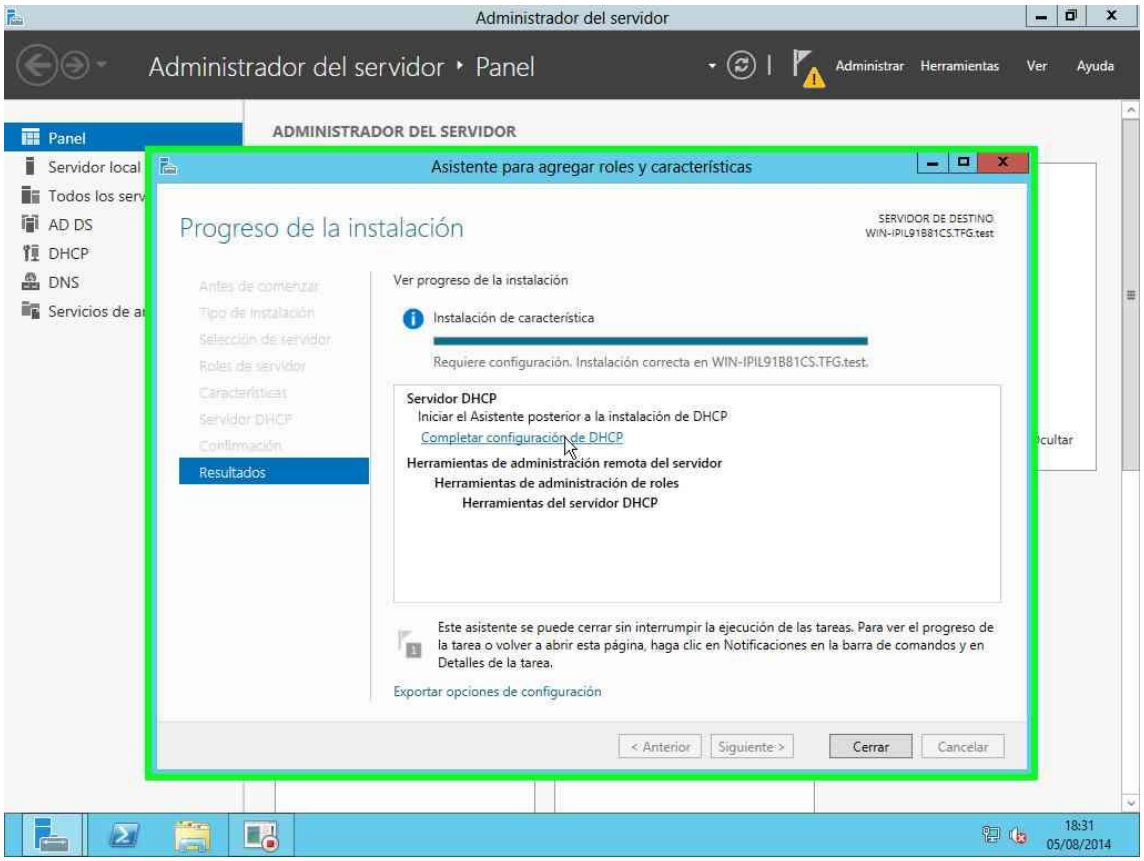


*Figura 17: Instalación finalizada*

En las siguientes capturas de pantalla se muestran los pasos a seguir en el asistente post-instalación del servidor DHCP. En este asistente se asignarán las credenciales de seguridad al servidor.

Como credenciales de seguridad utilizaremos las del usuario administrador del dominio, para ello seleccionaremos la opción "Usar las credenciales del siguiente usuario" y confirmamos las credenciales de un usuario con los permisos suficientes, en nuestro caso el administrador del dominio.

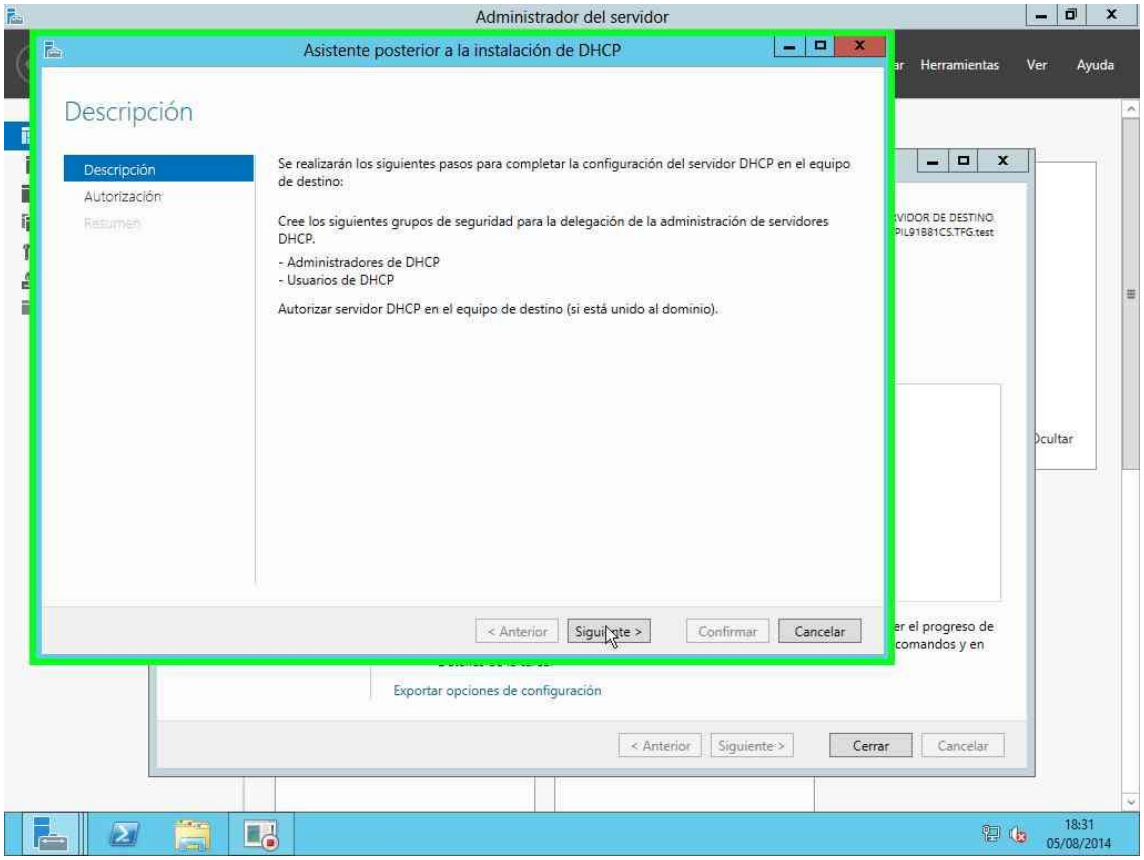


*Figura 18: Completar la configuración*

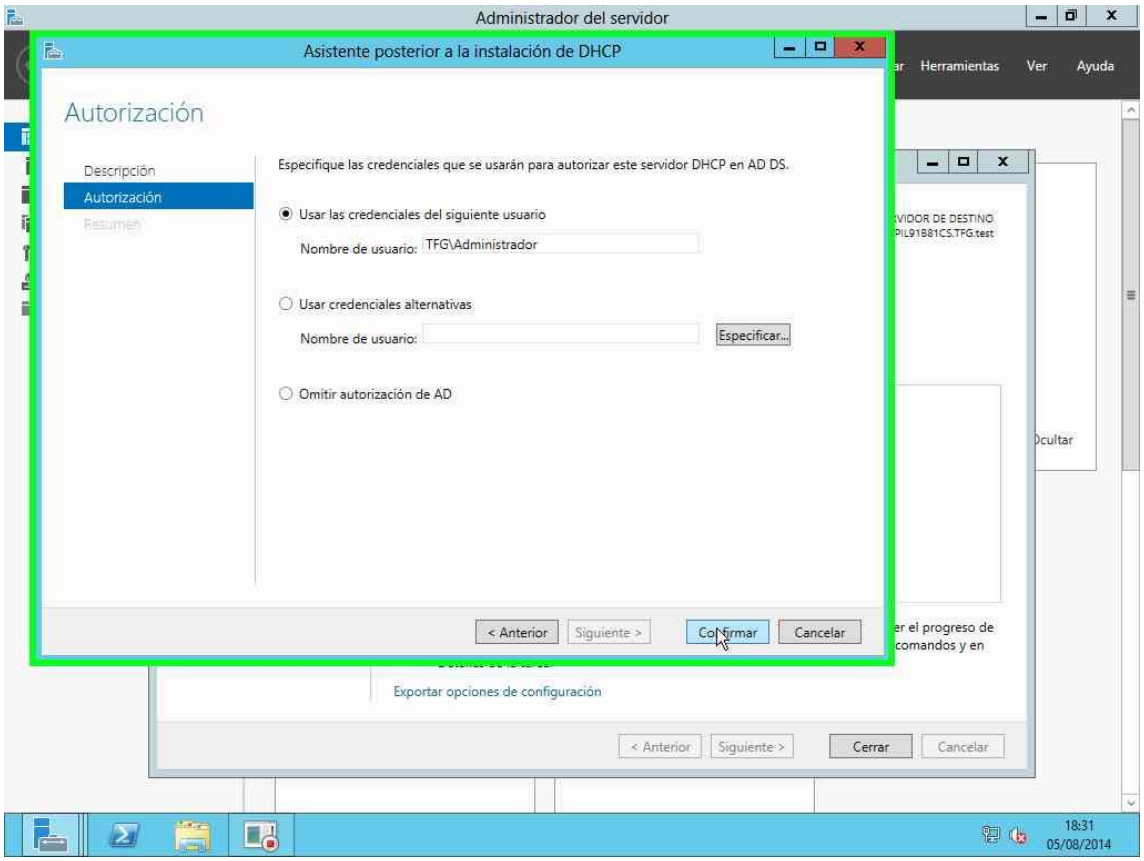


*Figura 19: Autorización del servidor*

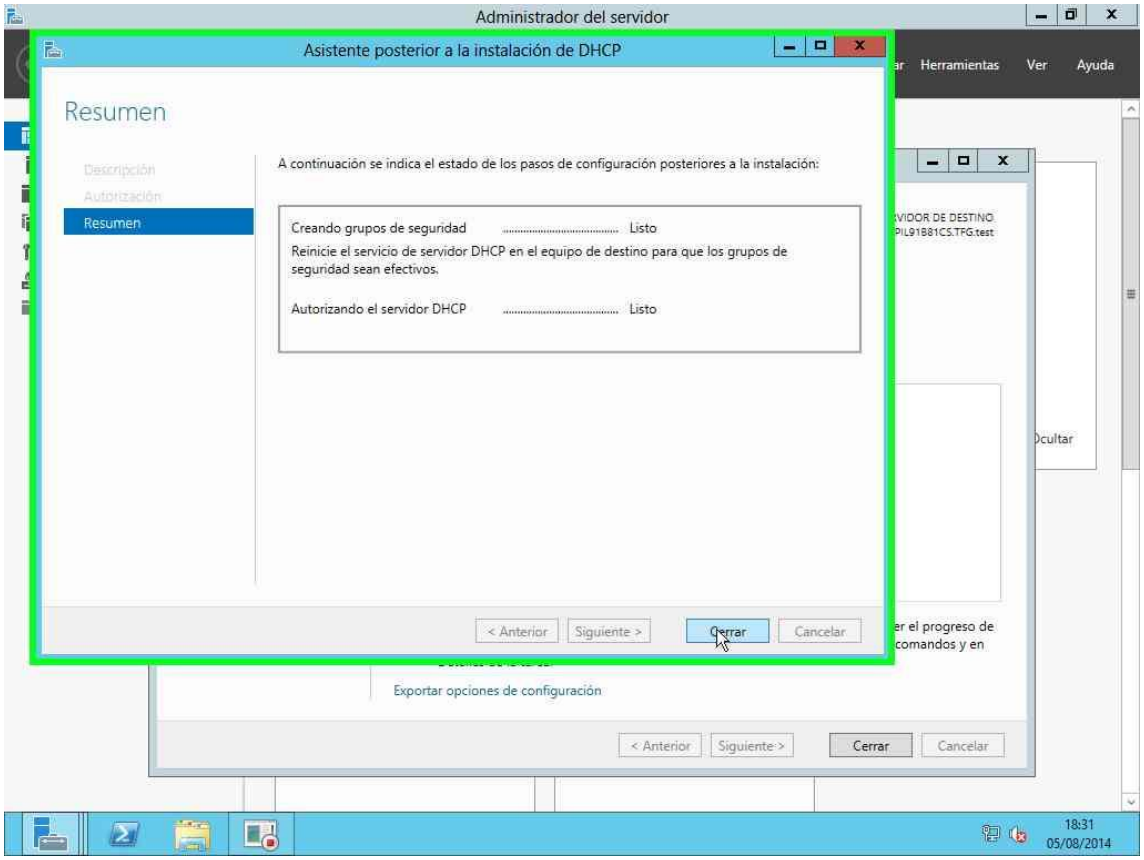


*Figura 20: Progreso*

Una vez hecho esto, salimos del asistente y nos dirigimos al menú de inicio, dónde encontraremos el acceso a la consola de administración del servidor DHCP y la abrimos.

En el menú lateral izquierdo encontramos un desplegable con la estructura del servidor dónde podemos configurar distintos ámbitos para asignar direcciones tanto de IPv4 como de IPv6, en nuestro caso seleccionamos IPv4 y hacemos click derecho y seleccionamos la opción “Ámbito nuevo”.

Como nombre del nuevo ámbito elegiremos IPs clientes (Figura23), y como espacio de direccionamiento, seleccionaremos la subred comprendida entre las direcciones 192.168.1.220 y 192.168.1.250 (Figura 24).

Tras elegir el rango de direcciones, el asistente nos ofrece la posibilidad de excluir un cierto rango de direcciones, que se podría utilizar después para asignarlas manualmente a otros servidores, impresoras, etc., además del tiempo de retraso de la subred que dejamos por defecto (Figura 25). En este caso lo hemos dejado en blanco.

A continuación se nos ofrece la posibilidad de modificar el tiempo de concesión de las IPs, es decir, cada cuanto tiempo el servidor proveerá a un equipo de una nueva IP, en nuestro caso dejamos el tiempo por defecto, es decir, ocho días (Figura 26).

Seguidamente nos da la opción de configurar las opciones DHCP del ámbito, tales como la puerta de enlace y el servidor DNS y, en caso de contar con él, el servidor WINS (Figuras 27 a 29). Todo este proceso se puede observar en las siguientes figuras:

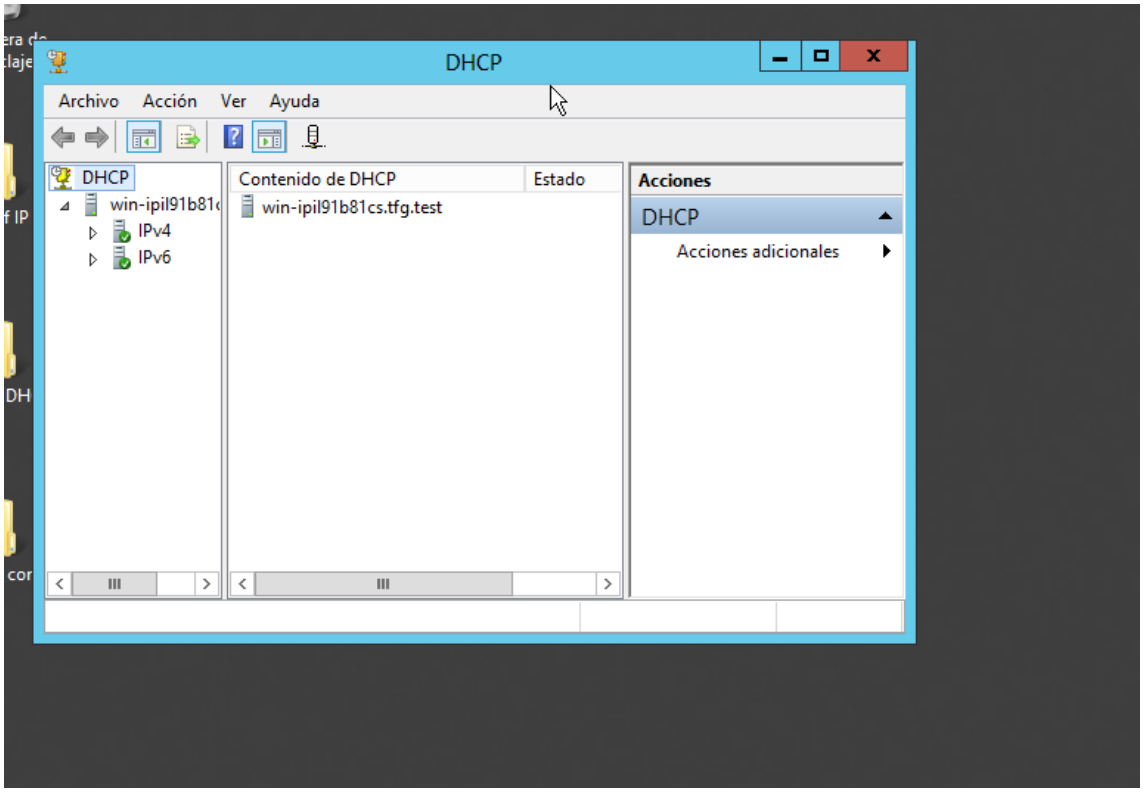


*Figura 21: Pantalla de administración del servidor DHCP*

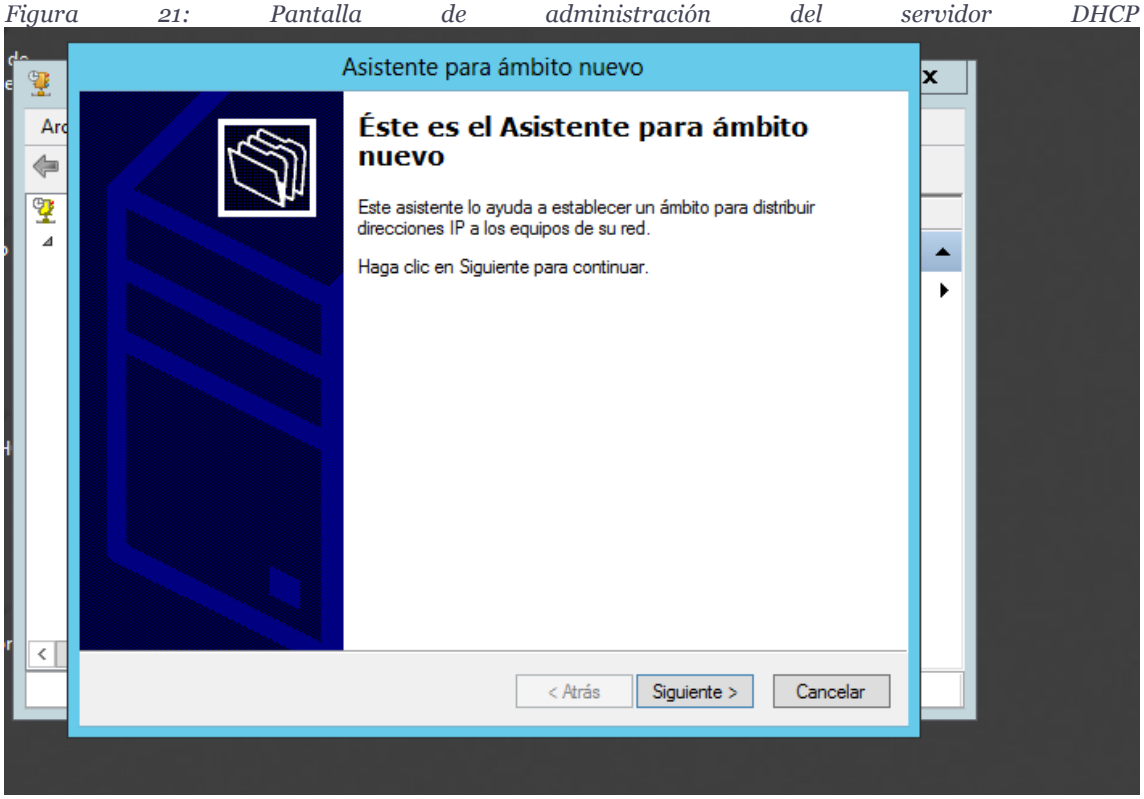


*Figura 22: Asistente para la creación del nuevo ámbito*

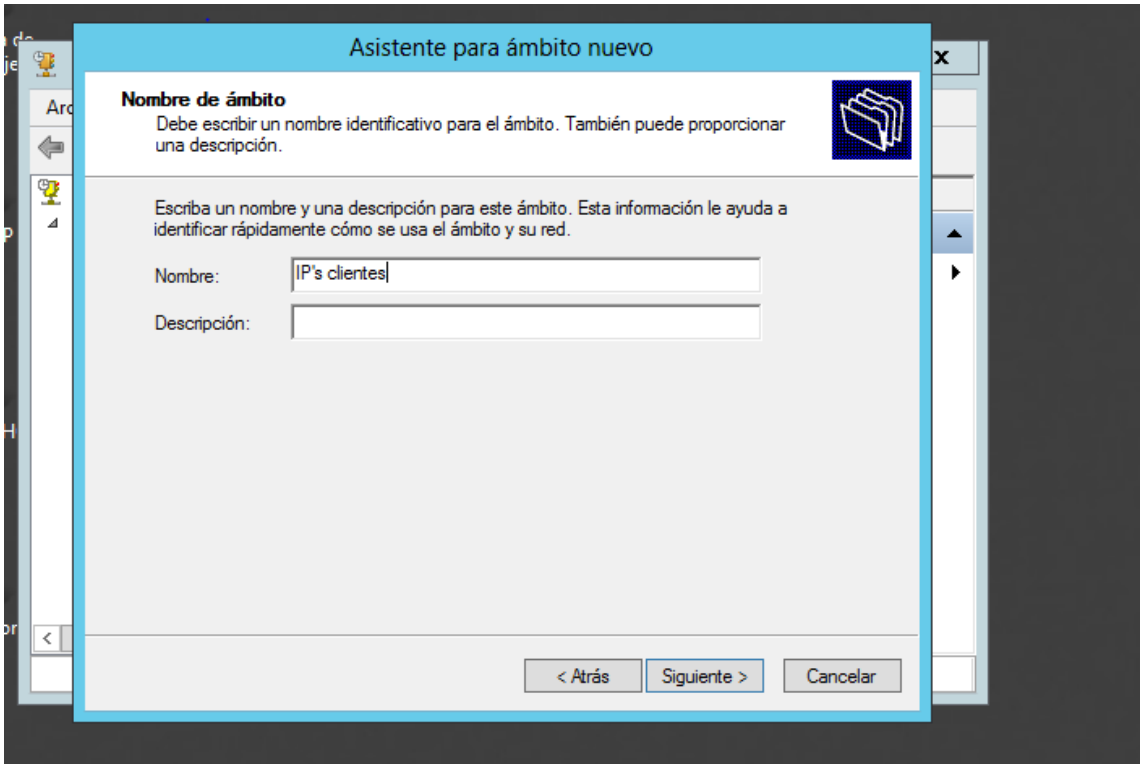


*Figura 23: Selección del nombre del ámbito*

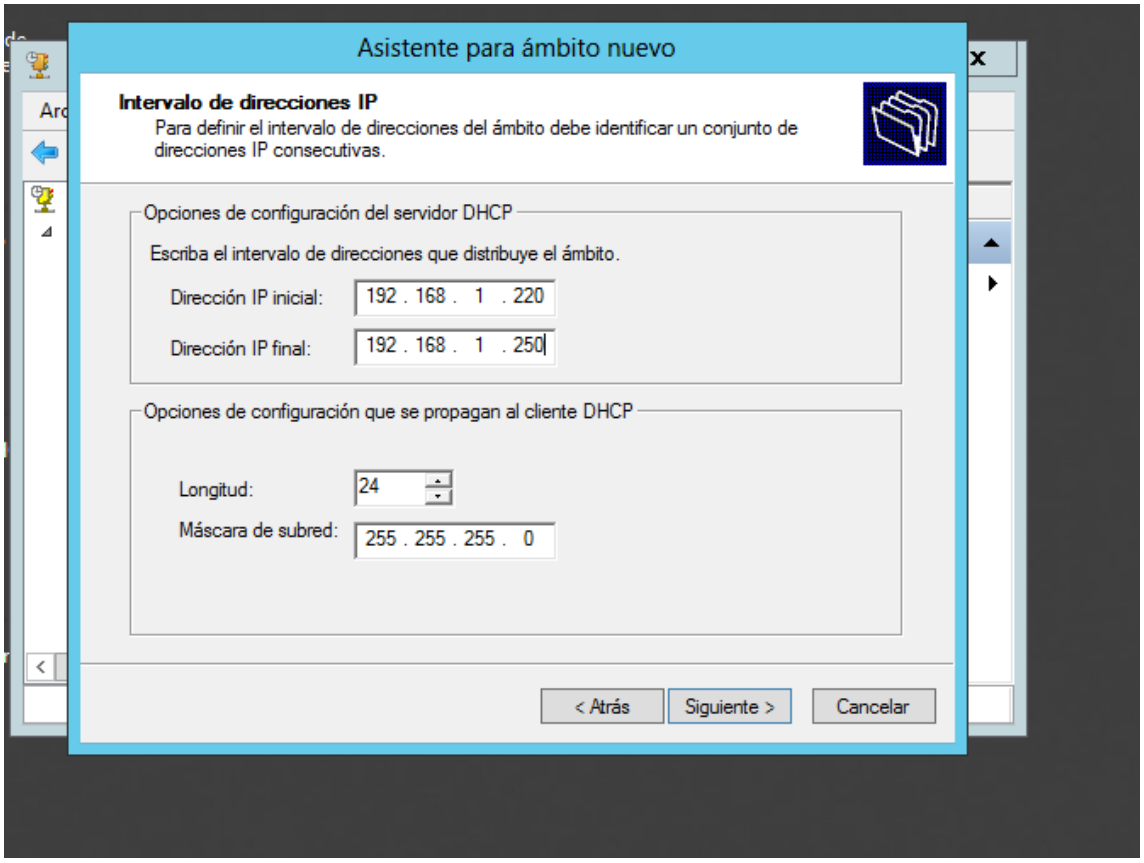


*Figura 24: Selección del rango de IPs asignables*

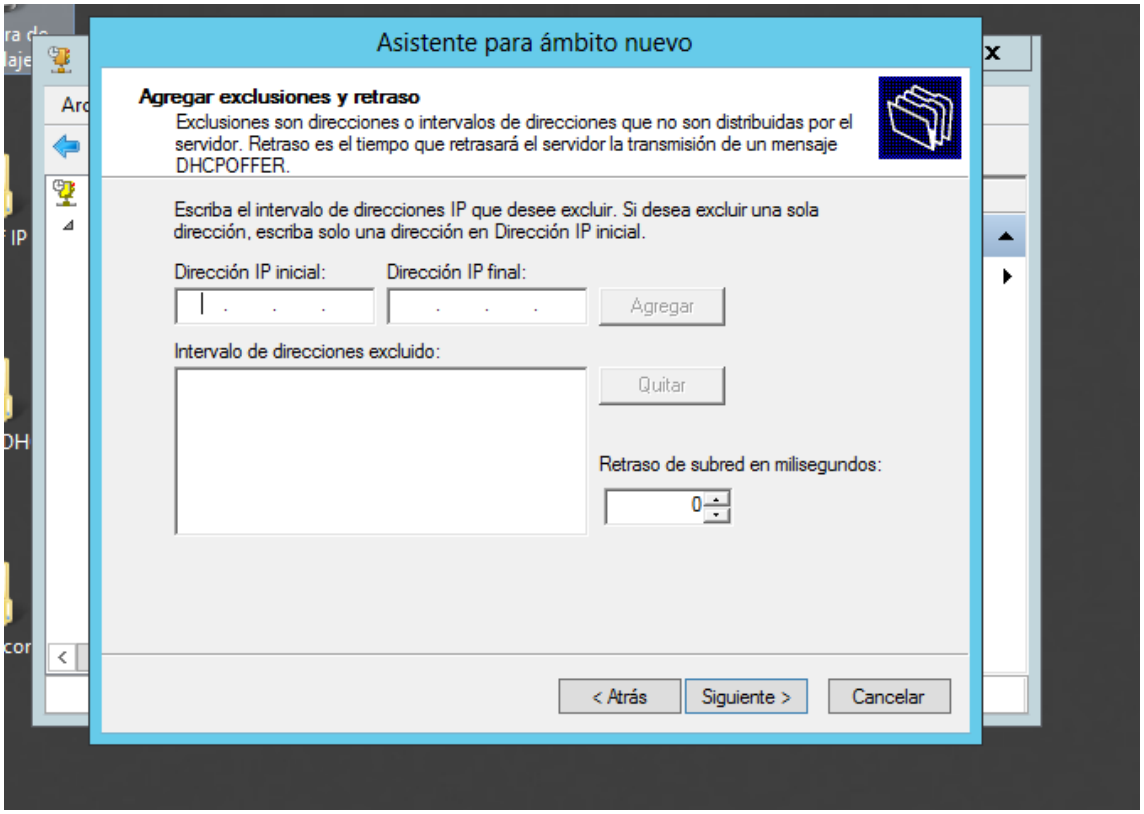


*Figura 25: Rango de exclusión*

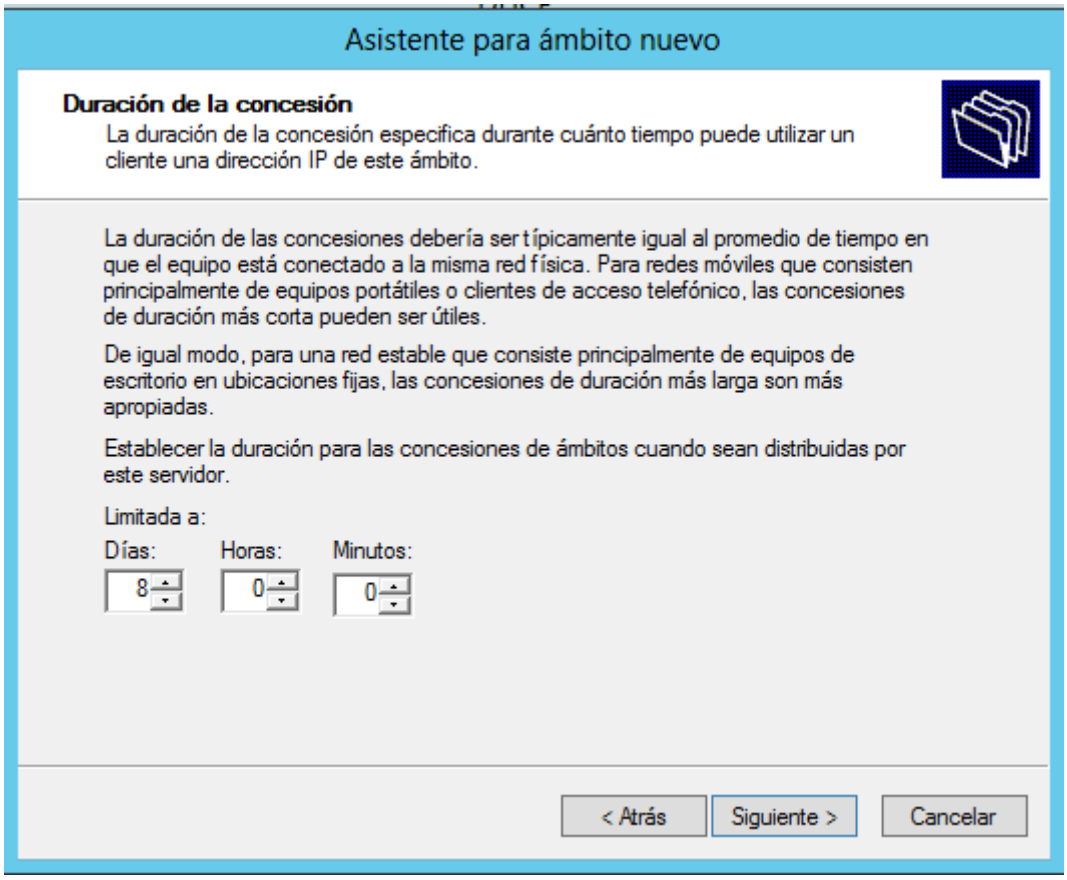


*Figura 26: Duración de la concesión*

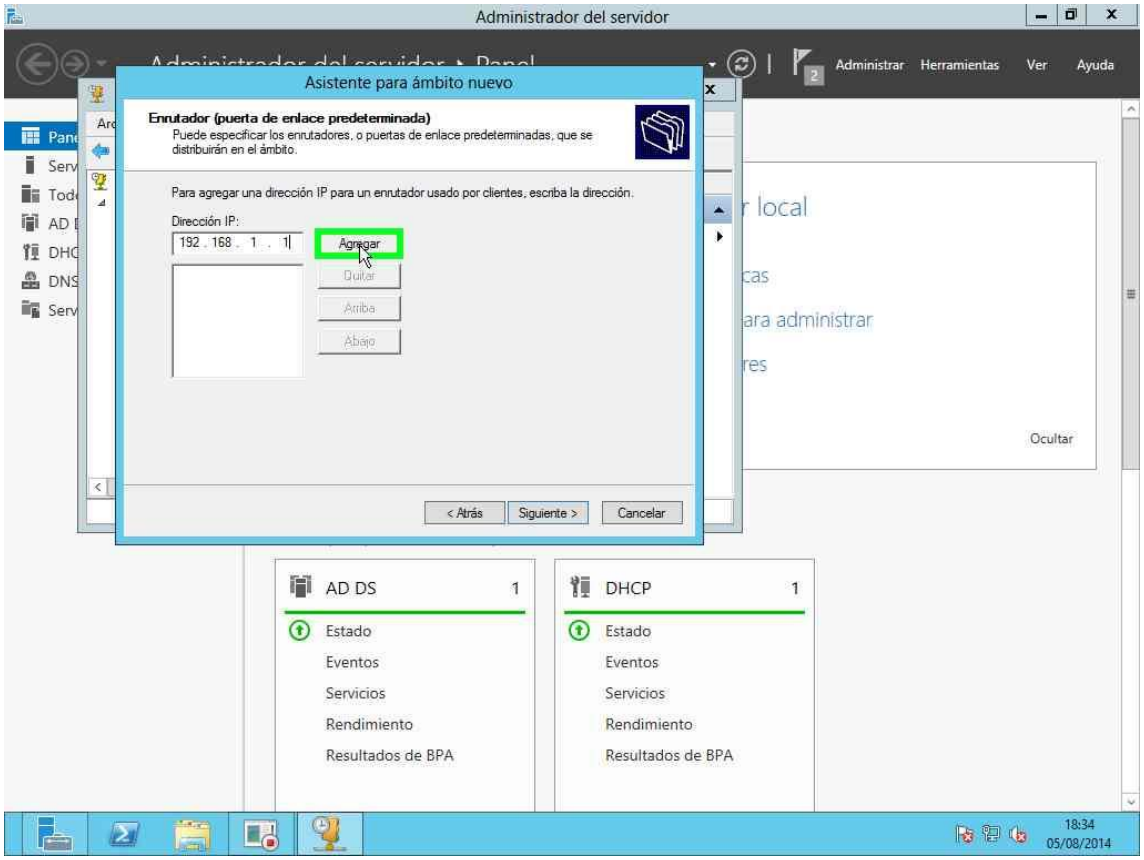


*Figura 27: Asignación puerta de enlace*

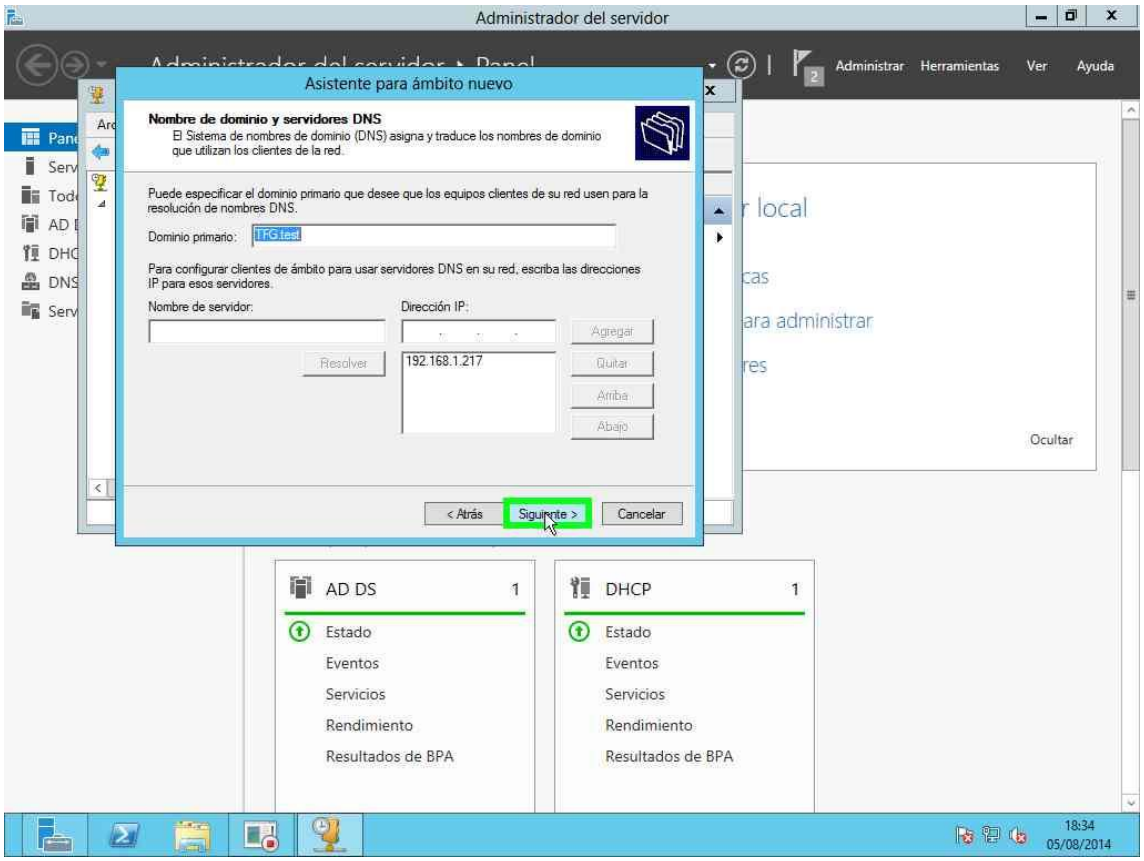


*Figura 28: Asignación DNS*

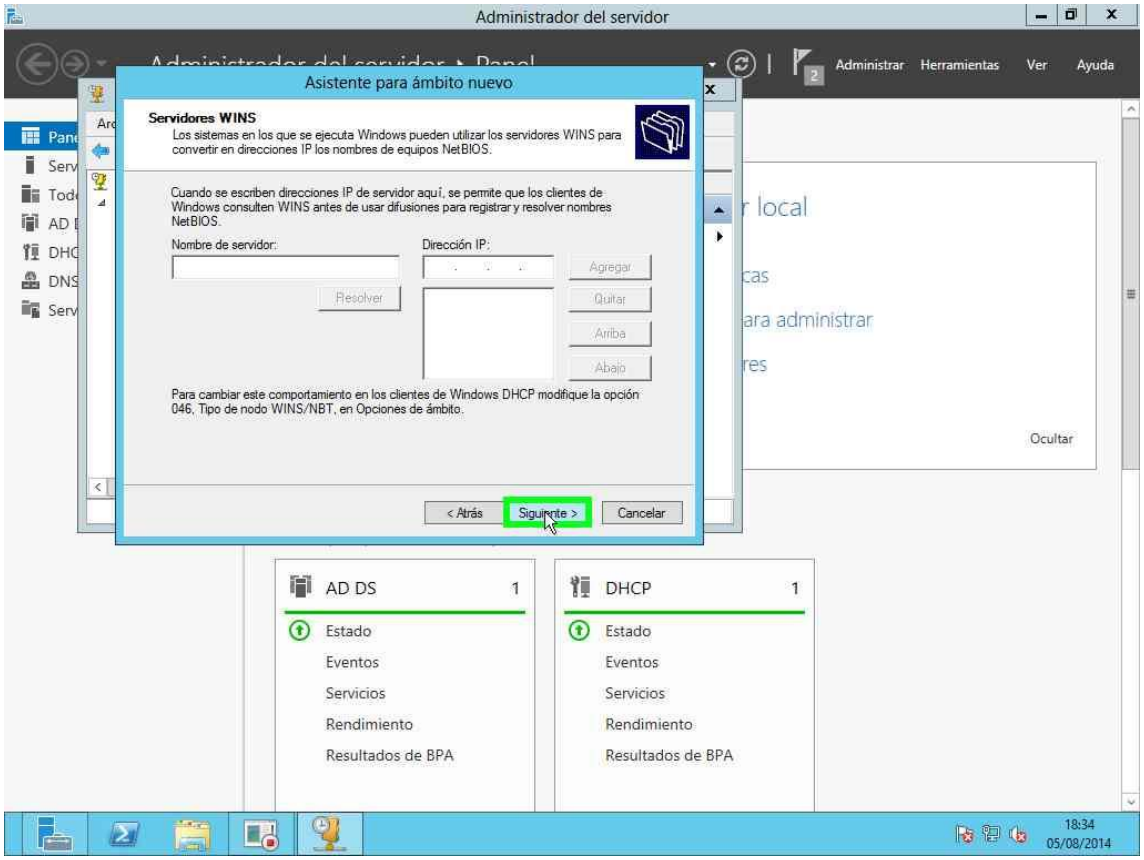


*Figura 29: Asignación servidor WINS*

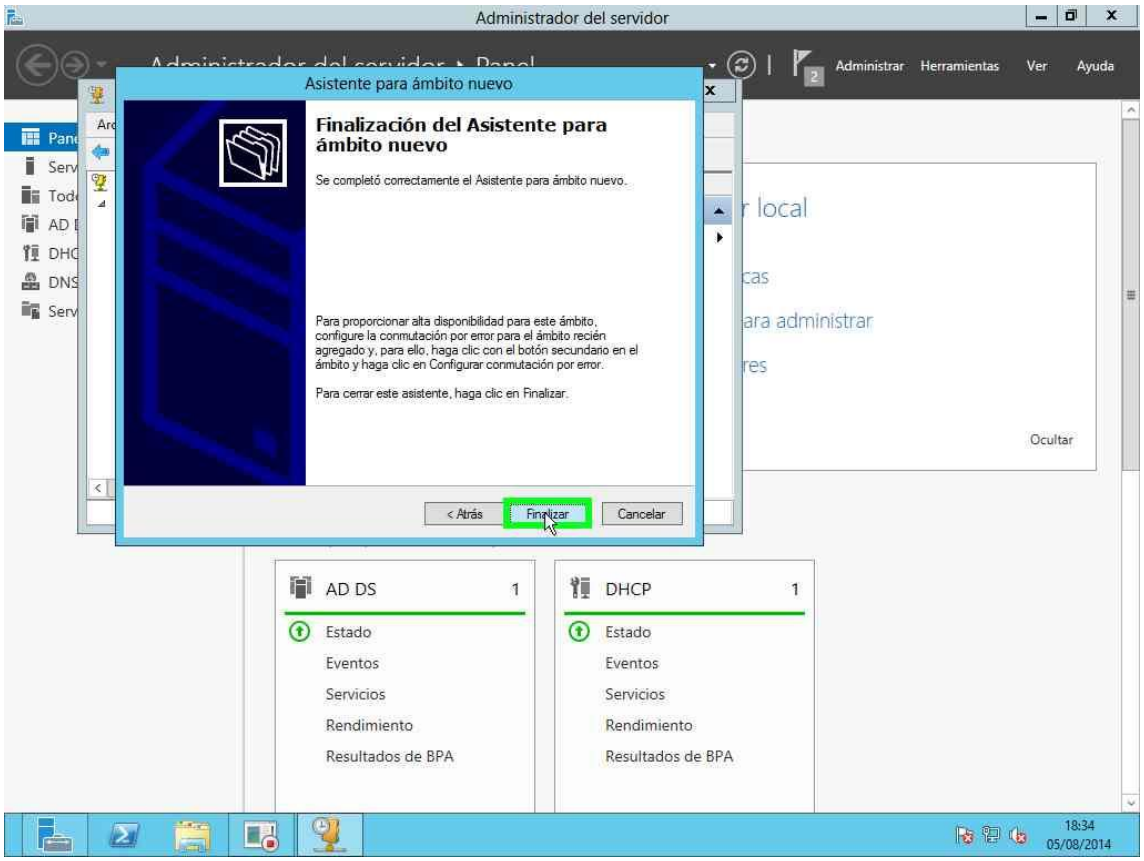


*Figura 30: Final del asistente*

Una vez configurado el servidor DHCP, ya nos podemos disponer a agregar equipos al dominio.

## 3.4 Replicación de Active Directory y del DNS

El primer paso para poder replicar el controlador de dominio, es dar de alta nuestro servidor secundario en el dominio, para ello, le indicamos como DNS principal el controlador de dominio actual, que como ya sabemos, ejerce como DNS del dominio y, a continuación tomamos la IP que le asigna nuestro servidor DHCP y la asignamos como IP estática, esto es importante, ya que además de como segundo controlador de dominio, también ejercerá las veces de DNS.

Una vez hecho esto, vamos a instalar los servicios de controlador de domino de Active Directory en este servidor, para ello abrimos el Administrador del servidor y seleccionamos "Agregar roles y características", a continuación seleccionamos la opción de "Instalación basada en roles" y repetimos los pasos que ya explicamos anteriormente en la instalación de Active Directory como se puede observar en las siguientes capturas de pantalla:

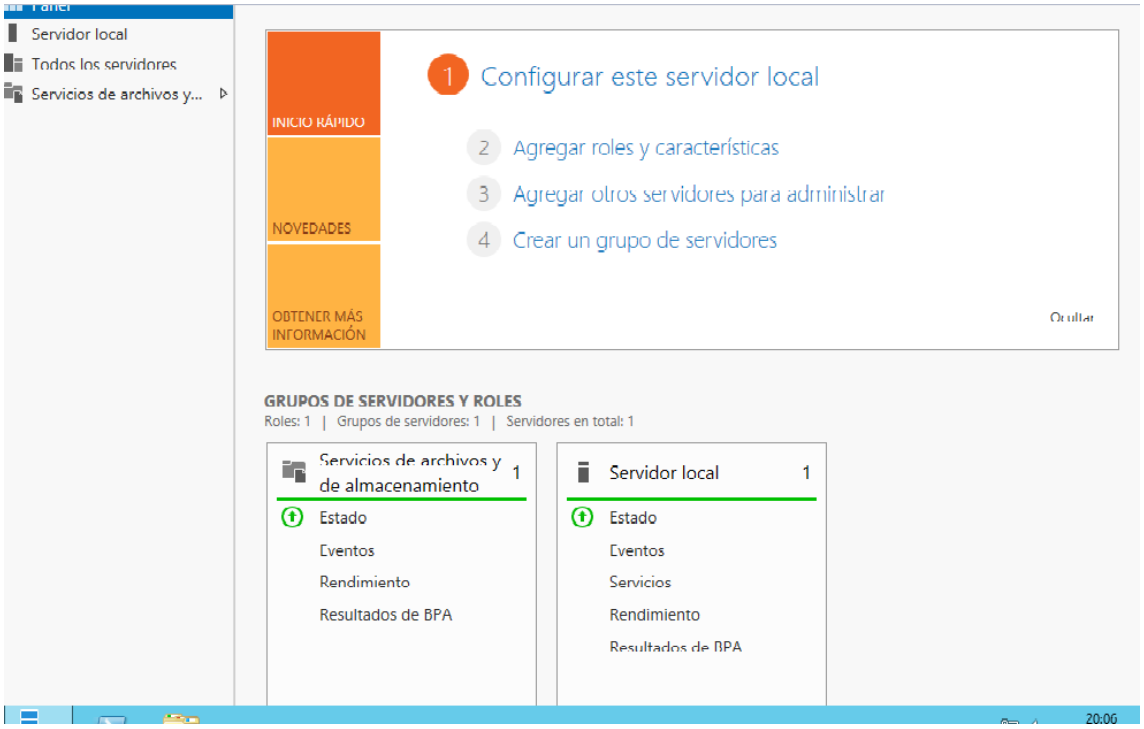


*Figura 31: Administrador del servidor*

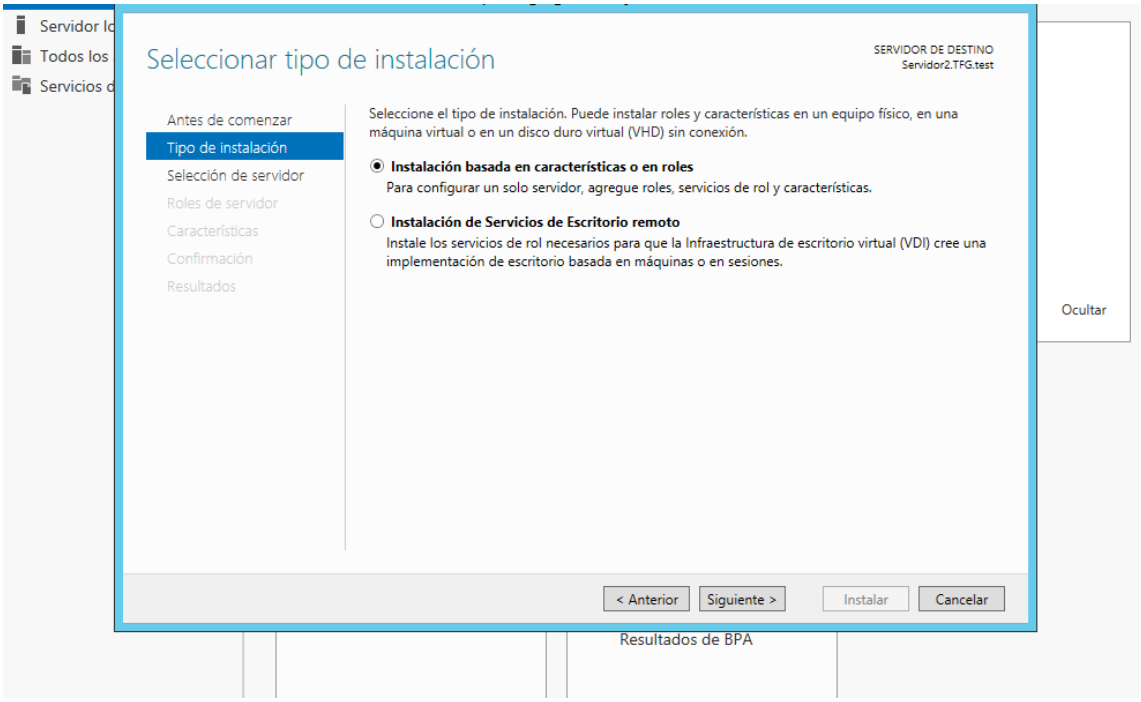


*Figura 32: Instalación basada en roles*

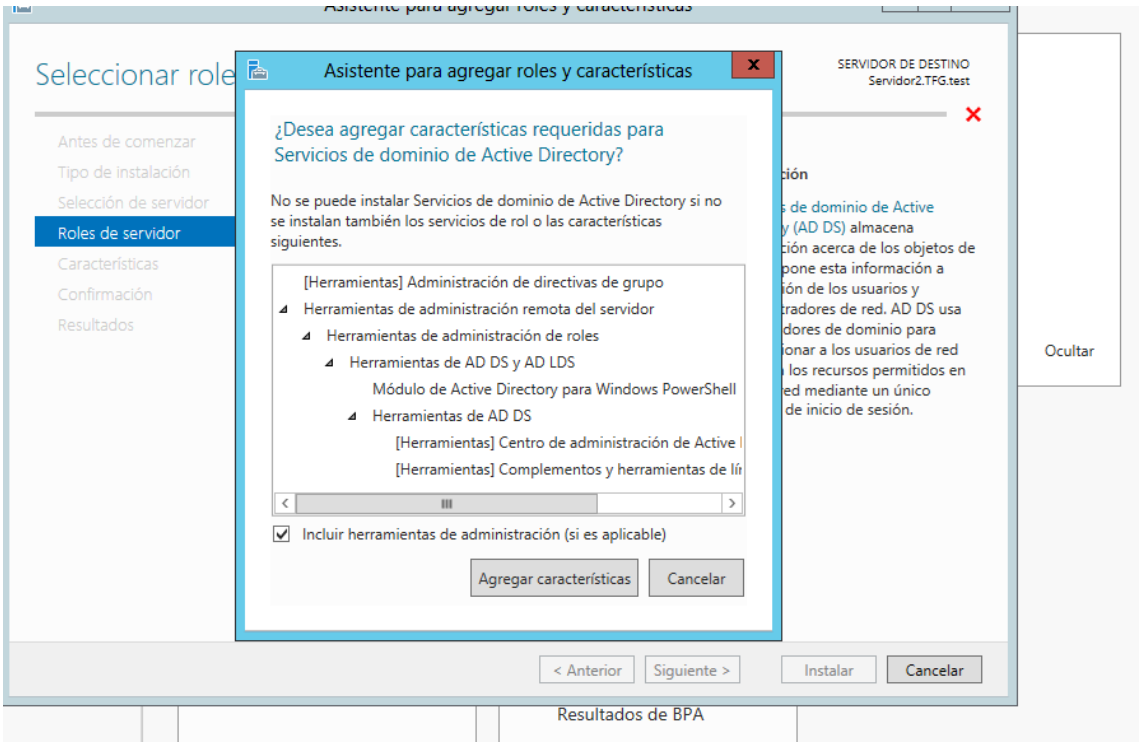


*Figura 33: Instalación de características de AD DS*

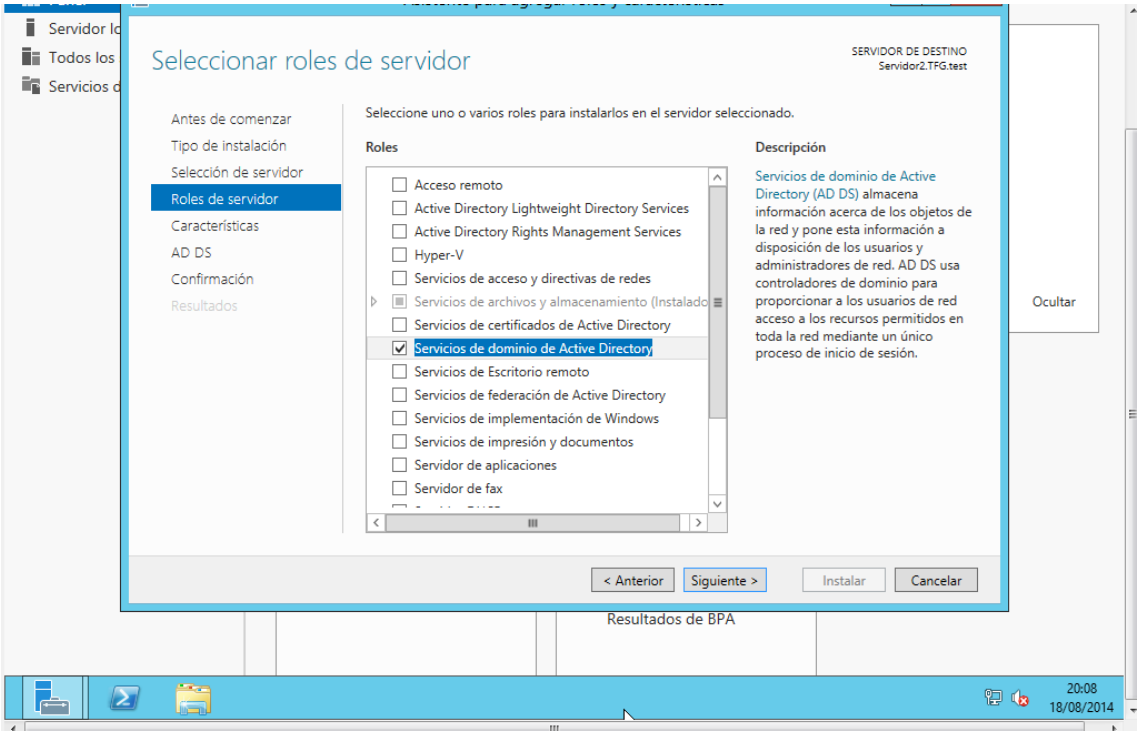


*Figura 34: Instalación de características para AD DS*

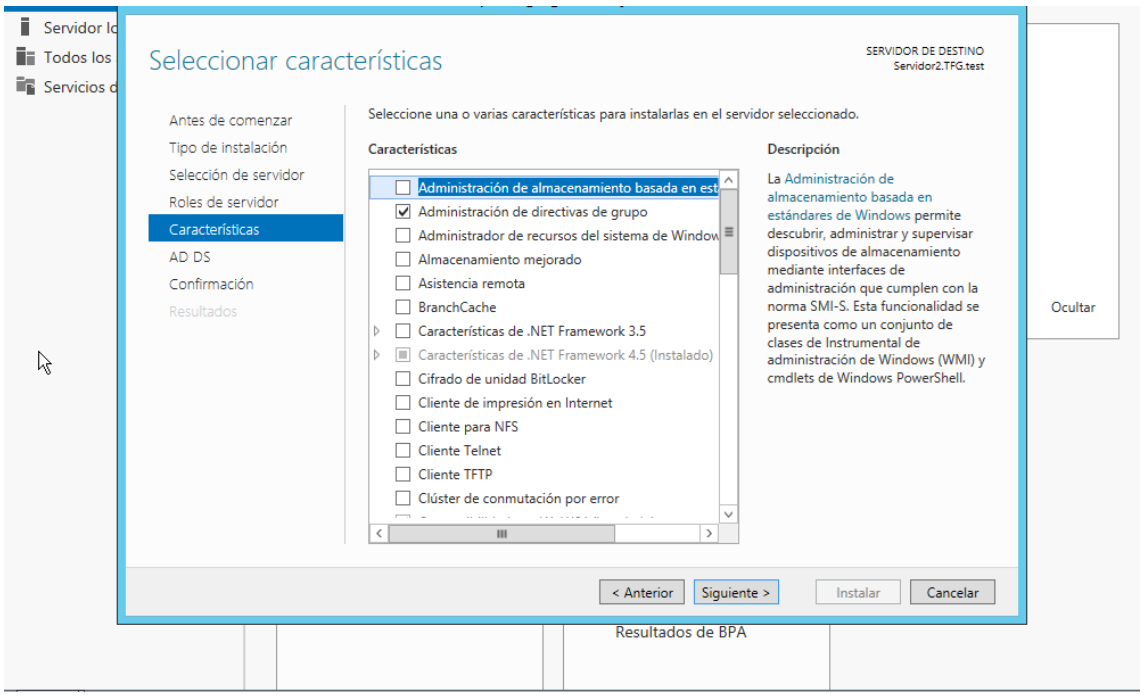


*Figura 35: Instalación de Active Directory*

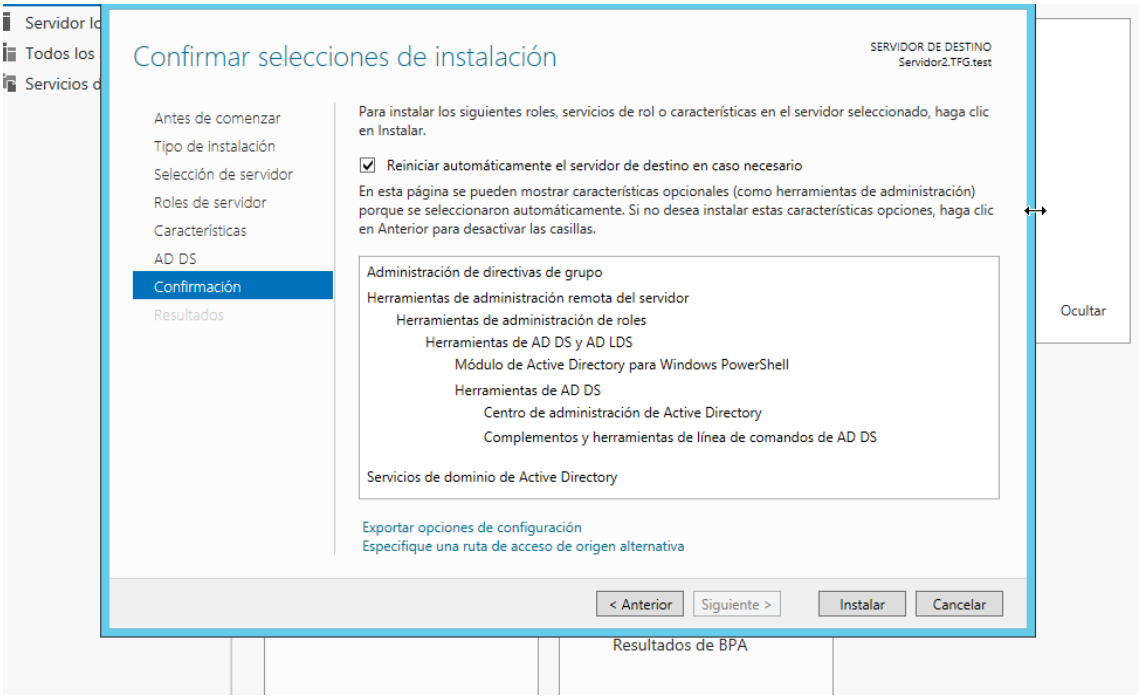


*Figura 36: Confirmación de las opciones*

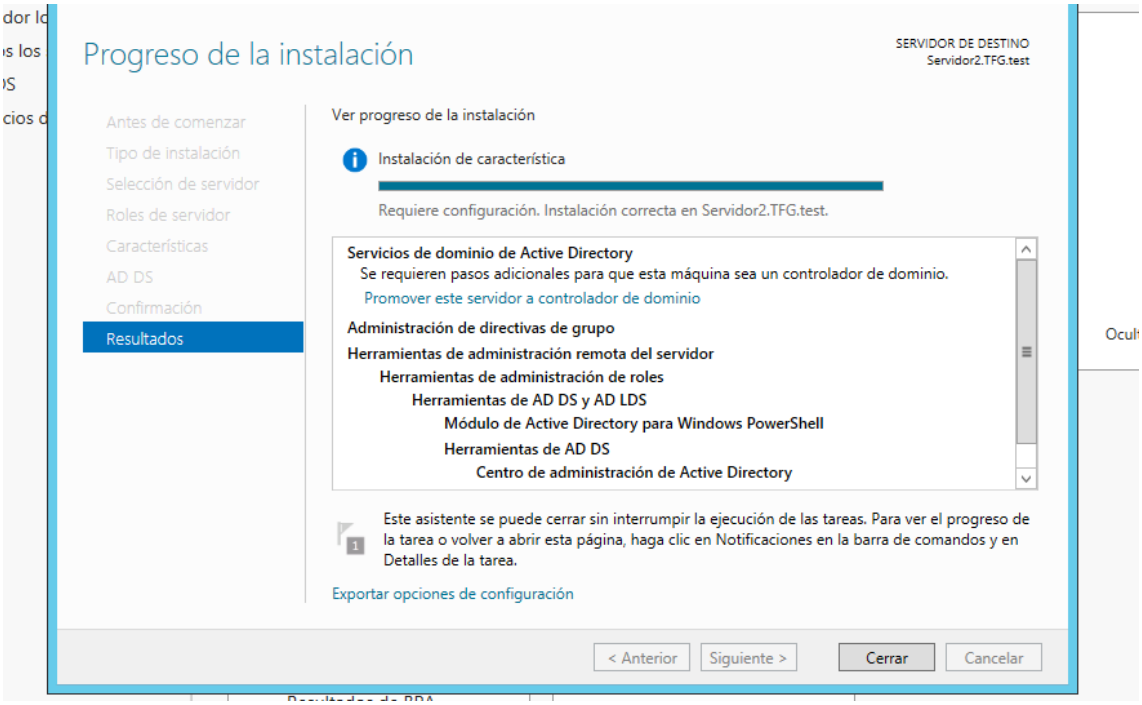


*Figura 37: Progreso*

En este momento, ya tenemos instalado Active Directory en este servidor y, ahora vamos a hacer que este servidor también sea controlador de dominio.

Pulsamos en “Promover este servidor a controlador de dominio” y nos aparece un nuevo asistente que nos da a elegir entre varias opciones: “Agregar un controlador de dominio a un domingo existente”, “Agregar un nuevo dominio a un bosque existente” y “Agregar un nuevo bosque”.

En este caso seleccionaremos “Agregar un controlador de dominio a un domingo existente” ya que lo que pretendemos es dar mayor tolerancia a fallos a nuestro sistema y vemos que nos detecta automáticamente el dominio TFG.test, ya que es el único dominio en la red, además nos pide las credenciales para poder realizar la unión al dominio, en este caso como hemos entrado en el servidor con la sesión del administrador del dominio, no será necesario cambiarlas, si estuviéramos conectados con la sesión propia del servidor, deberíamos proporcionar las credenciales de una sesión con los suficientes permisos para poder realizar ésta operación.

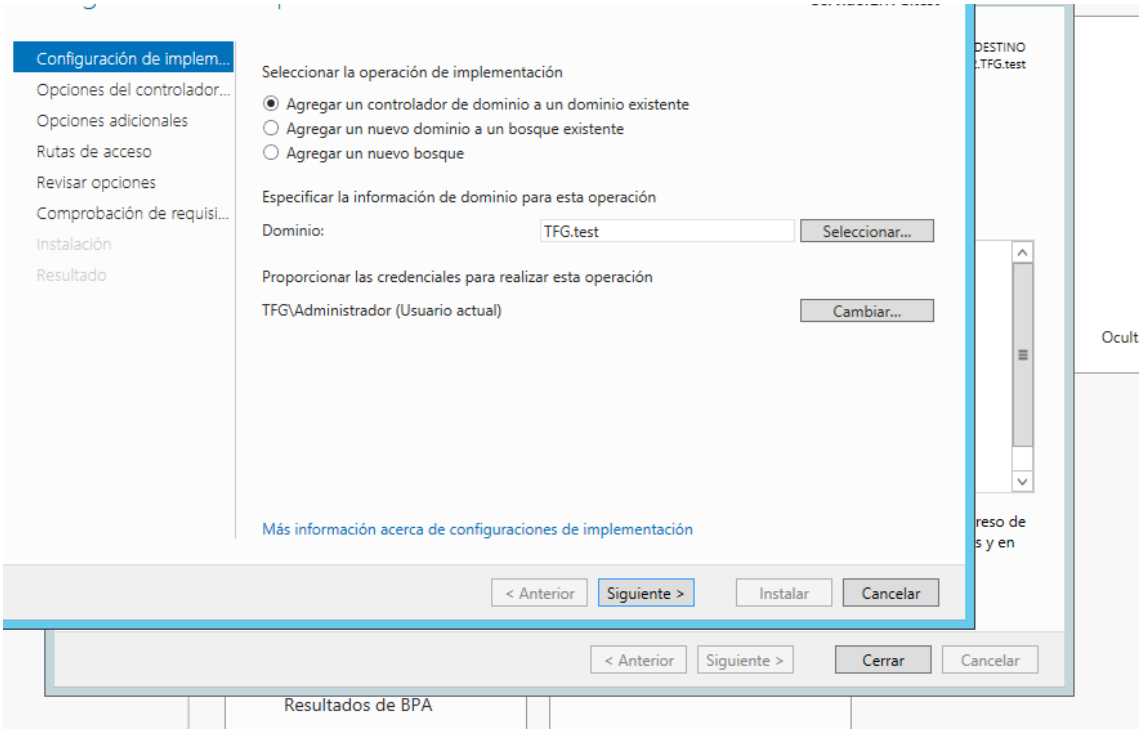


*Figura 38: Promoción a controlador del dominio*

En la siguiente ventana del asistente, al igual que en la creación del dominio, nos ofrece la posibilidad de asignarle al servidor también las capacidades de Catálogo Global y servidor DNS, de momento dejaremos el servidor como Controlador de Dominio y, más adelante lo promocionaremos a Catálogo Global e instalaremos el rol de Servidor DNS.

A continuación, nos solicita que indiquemos desde que servidor deseamos replicar la información. Como se puede observar en la Figura 40, el asistente detecta al servidor que ya ejercía como controlador de dominio y nos lo rellena por defecto.

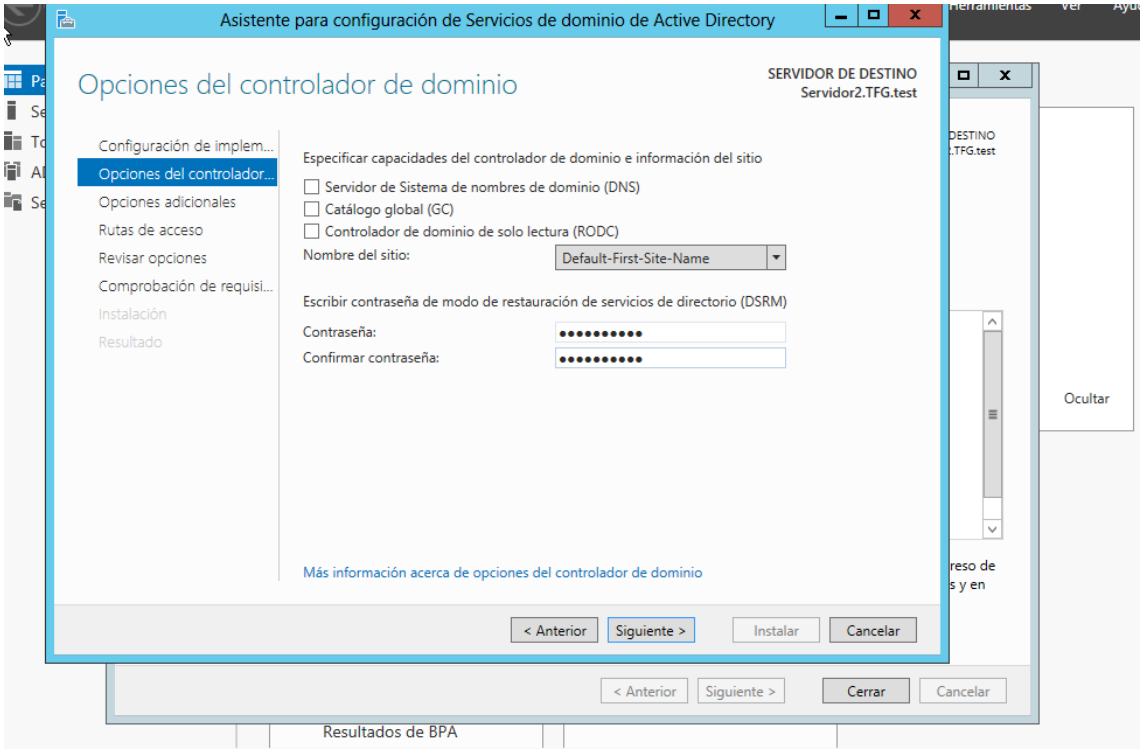


*Figura 39: Selección de las opciones.*

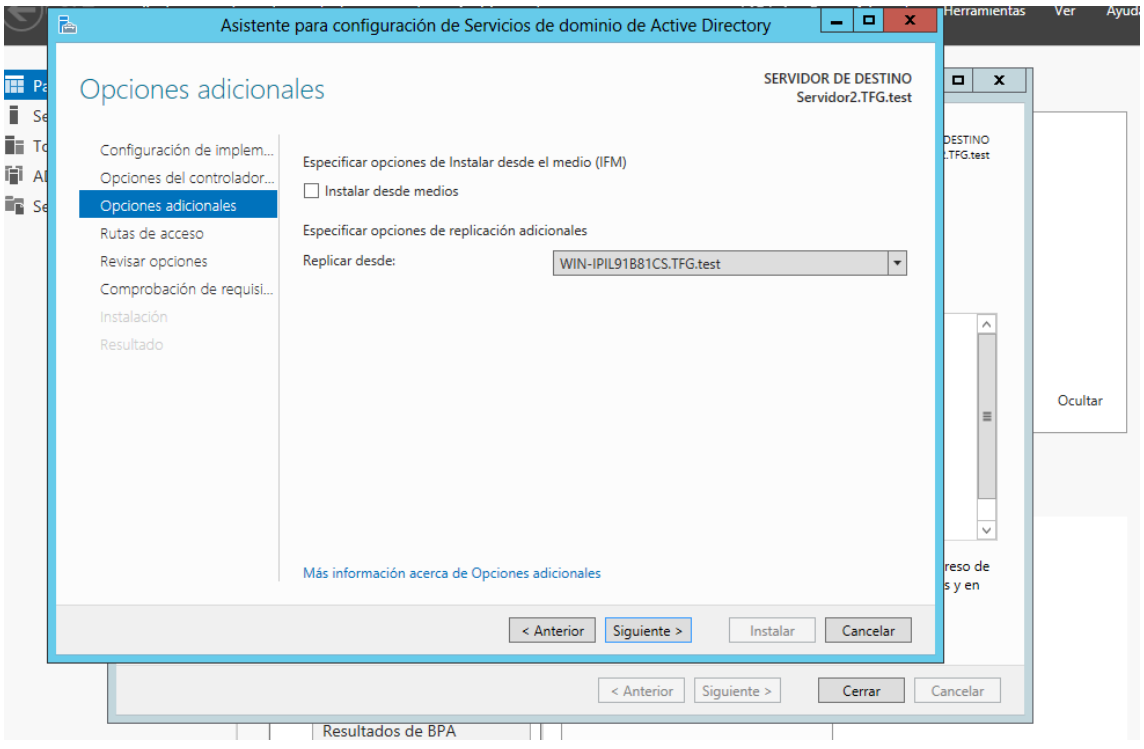


*Figura 40.*

Una vez el asistente posee la información necesaria para saber desde donde replicar el servidor, pasamos a la siguiente ventana, a partir de la cual la instalación vuelve a ser idéntica a la de la instalación en el servidor principal.

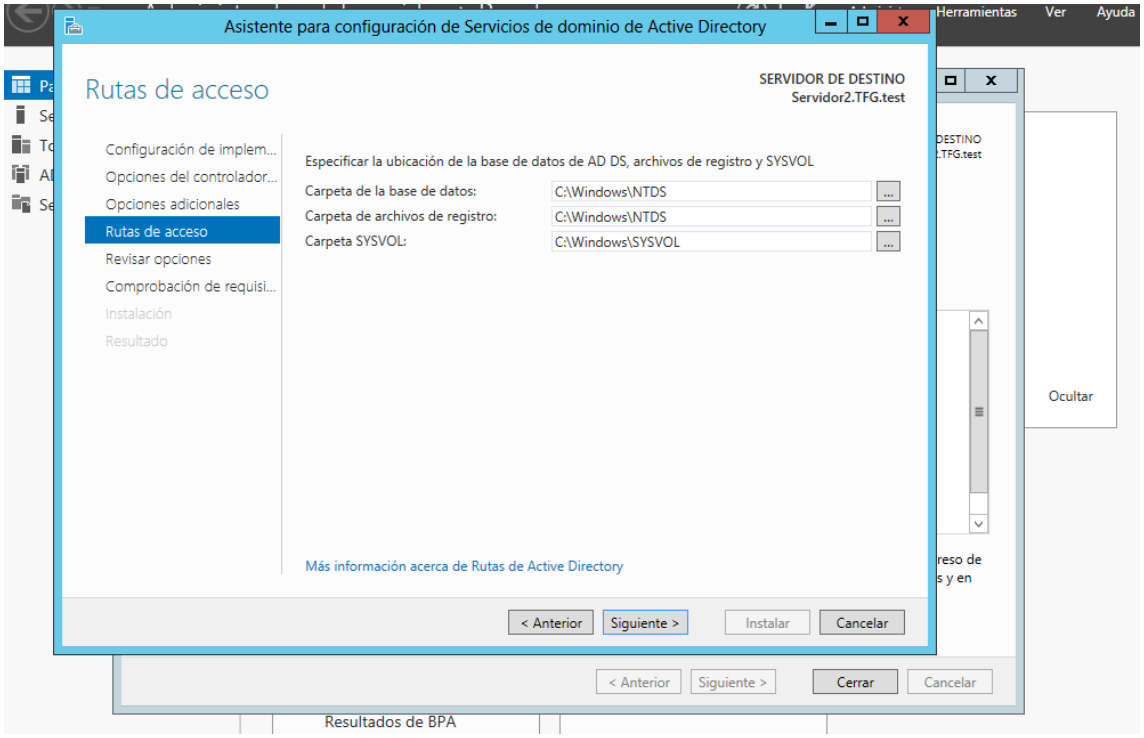


*Figura 41: Rutas de carpetas*

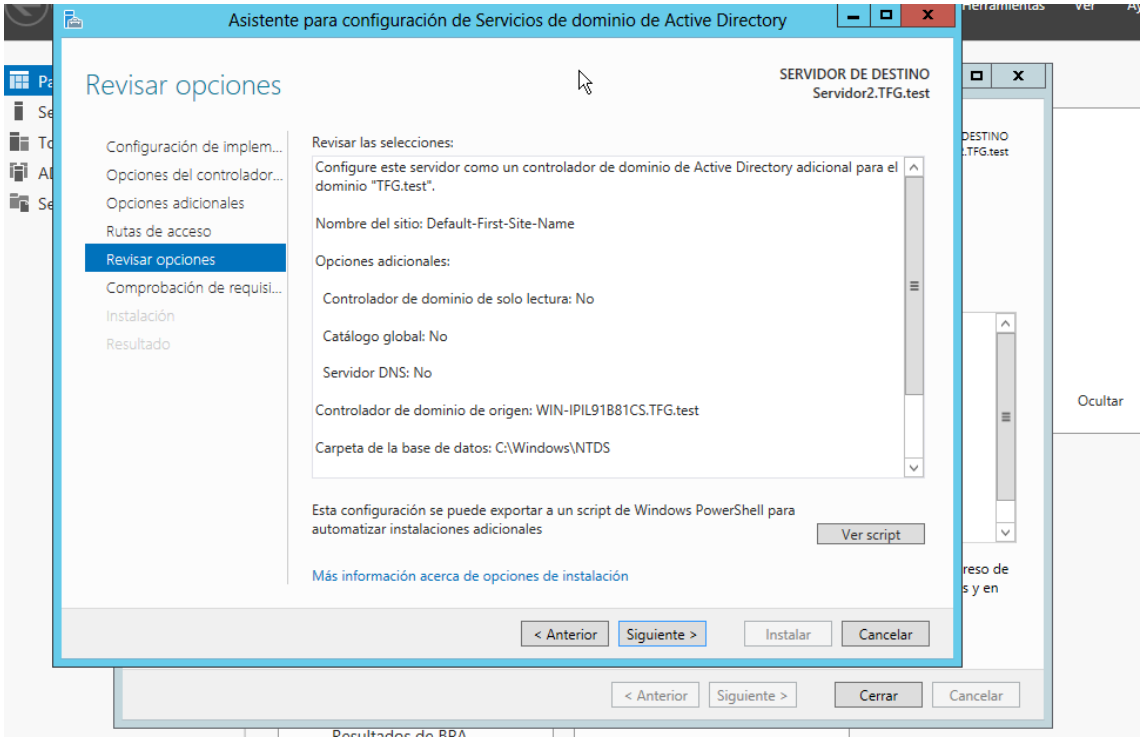


*Figura 42: Confirmación de las opciones*

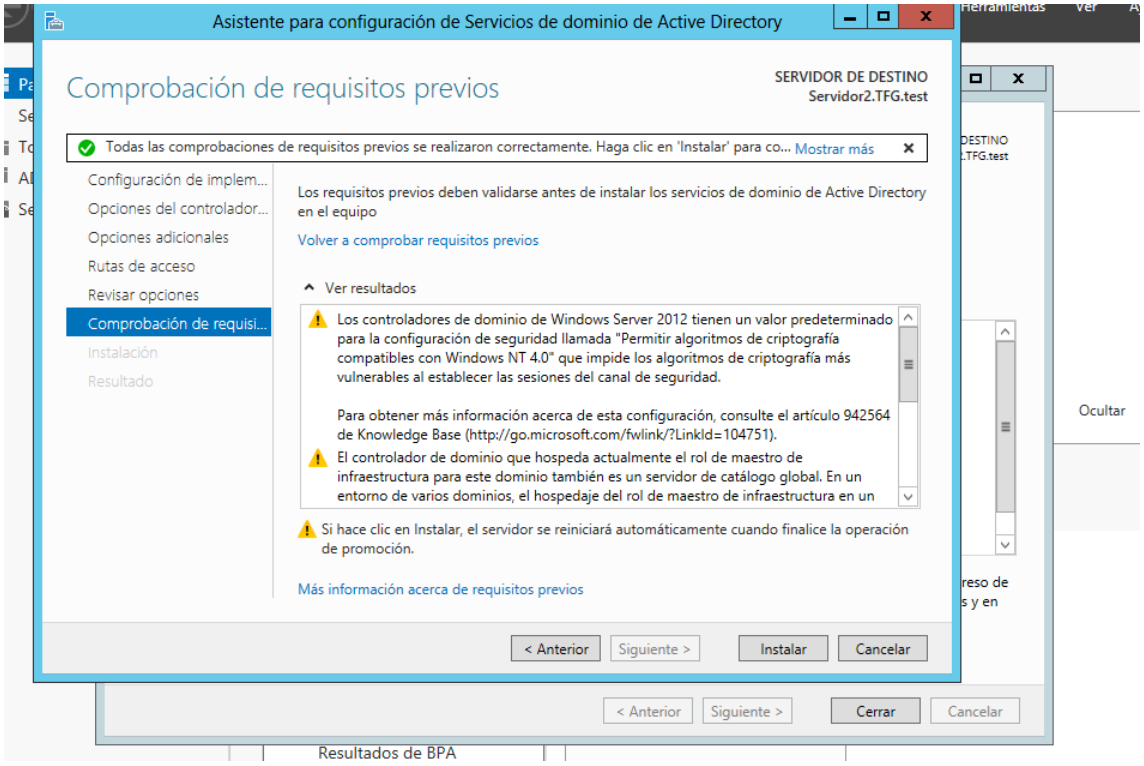


*Figura 43: Comprobación de requisitos previos*

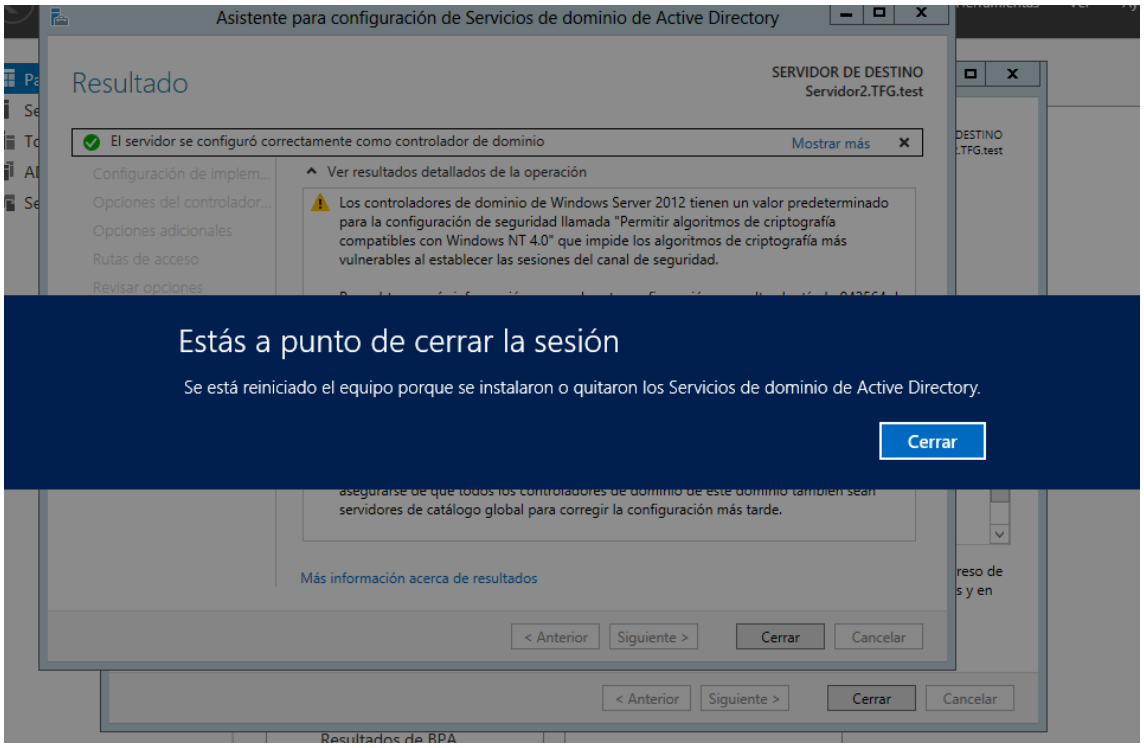


*Figura 44: Cierre de sesión post-instalación*

Una vez finalizada la promoción a controlador de dominio, es necesario cerrar la sesión para que los cambios se hagan efectivos.

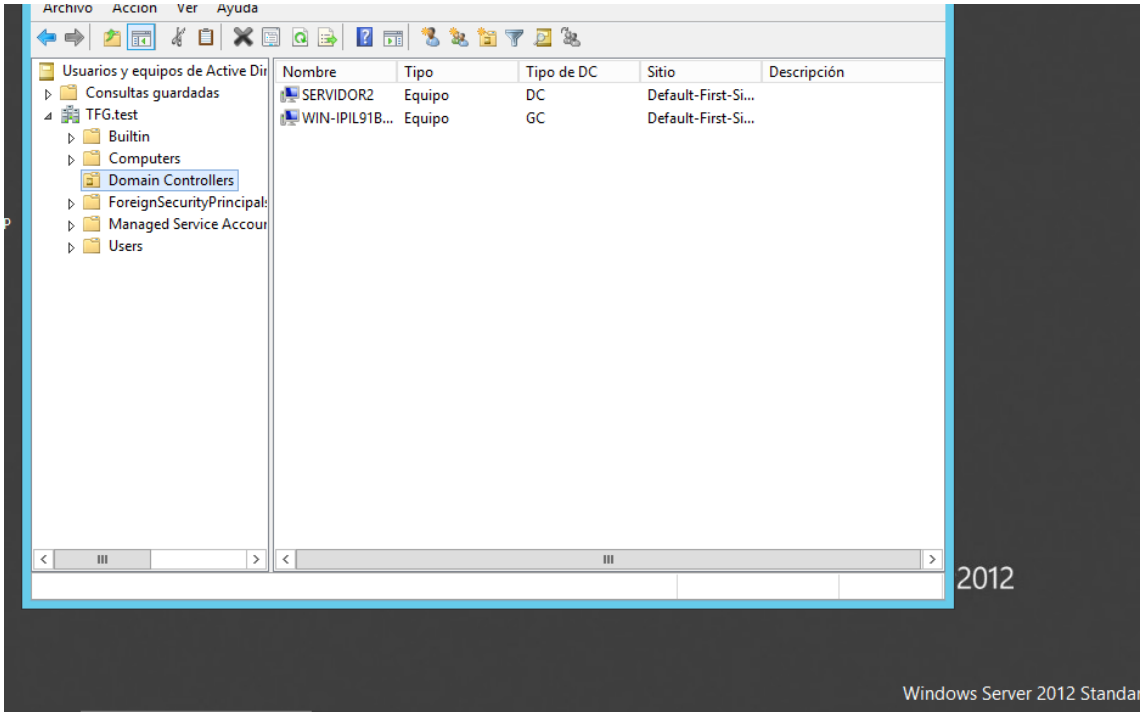


*Figura 45: Servidor 2 como DC*

Como se puede observar en la Figura 45, si ahora entramos en Usuarios y equipos de Active Directory desde el servidor principal, podemos ver que ya se detecta al servidor secundario como DC, abreviatura de Domain Controller (Controlador de dominio en inglés).

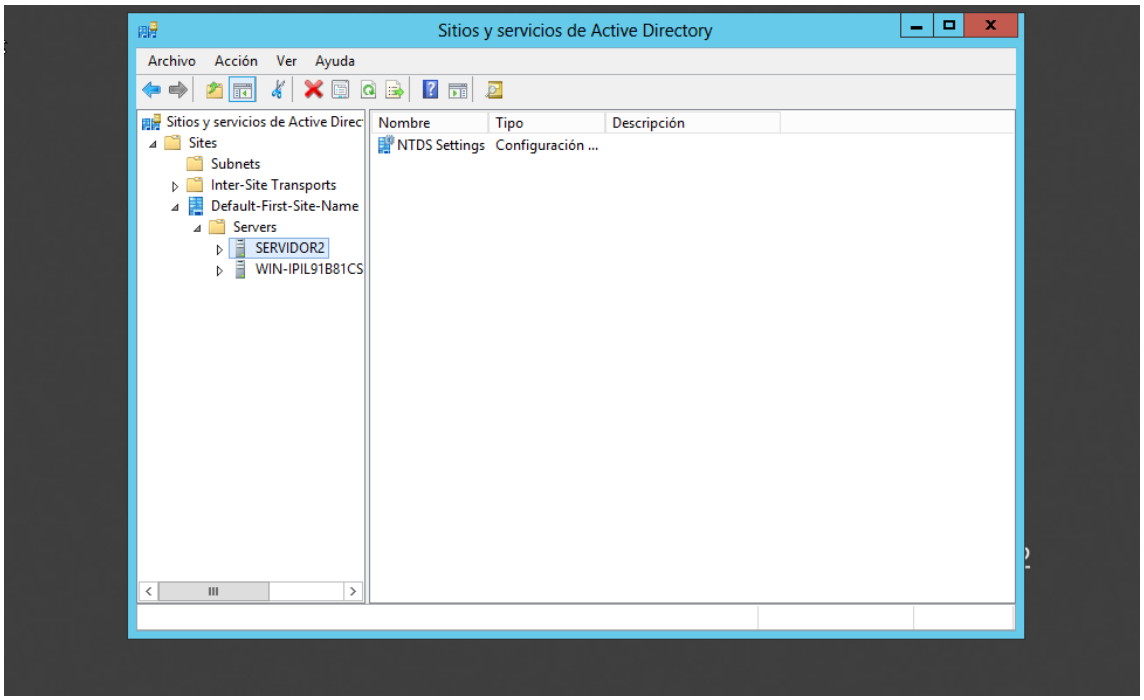


*Figura 46: Sitios y servicios de Active Directory*

Volviendo al servidor secundario, abrimos la consola de Sitios y Servicios de Active Directory y en Servers seleccionamos Servidor2. Hacemos clic

derecho sobre NTDS Settings y seleccionamos Propiedades y en la pestaña General hacemos check en Catálogo Global.

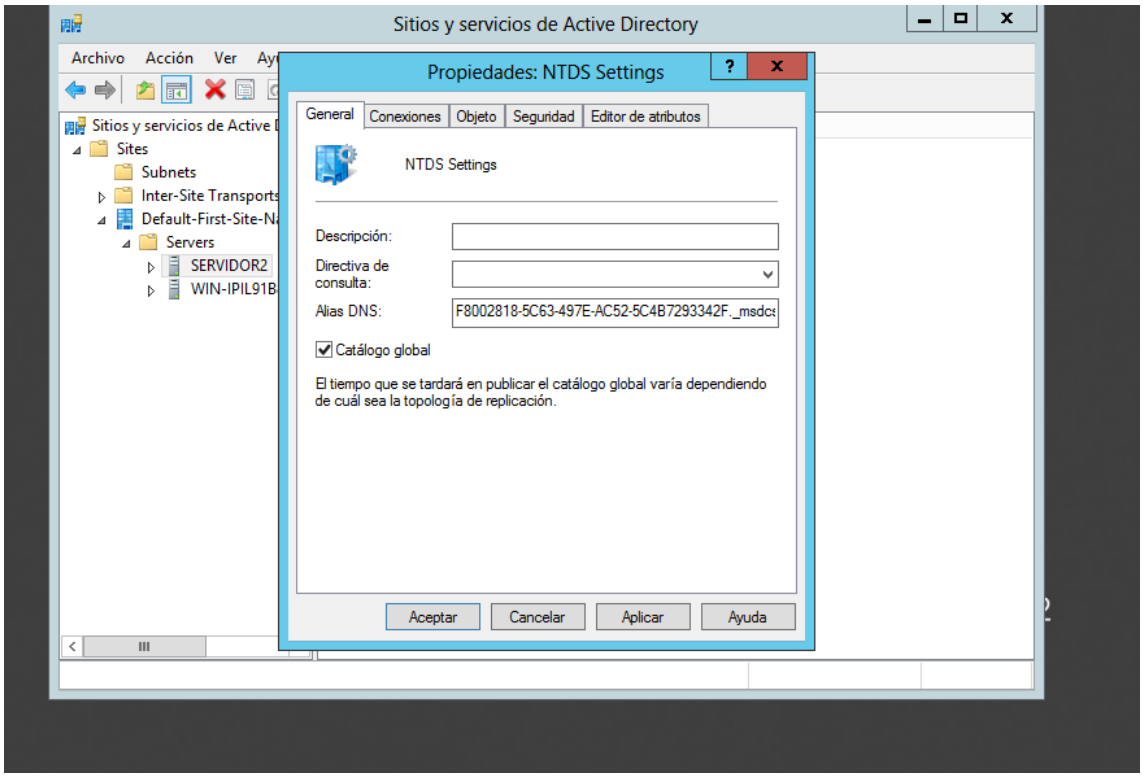


*Figura 47: Asignación de servidor 2 como Catálogo Global*

Tras unos cinco o diez minutos, si volvemos a revisar la consola de Usuarios y equipos de Active Directory en el servidor principal, veremos como el servidor secundario ya no aparece como DC, sino como GC o Catálogo Global.

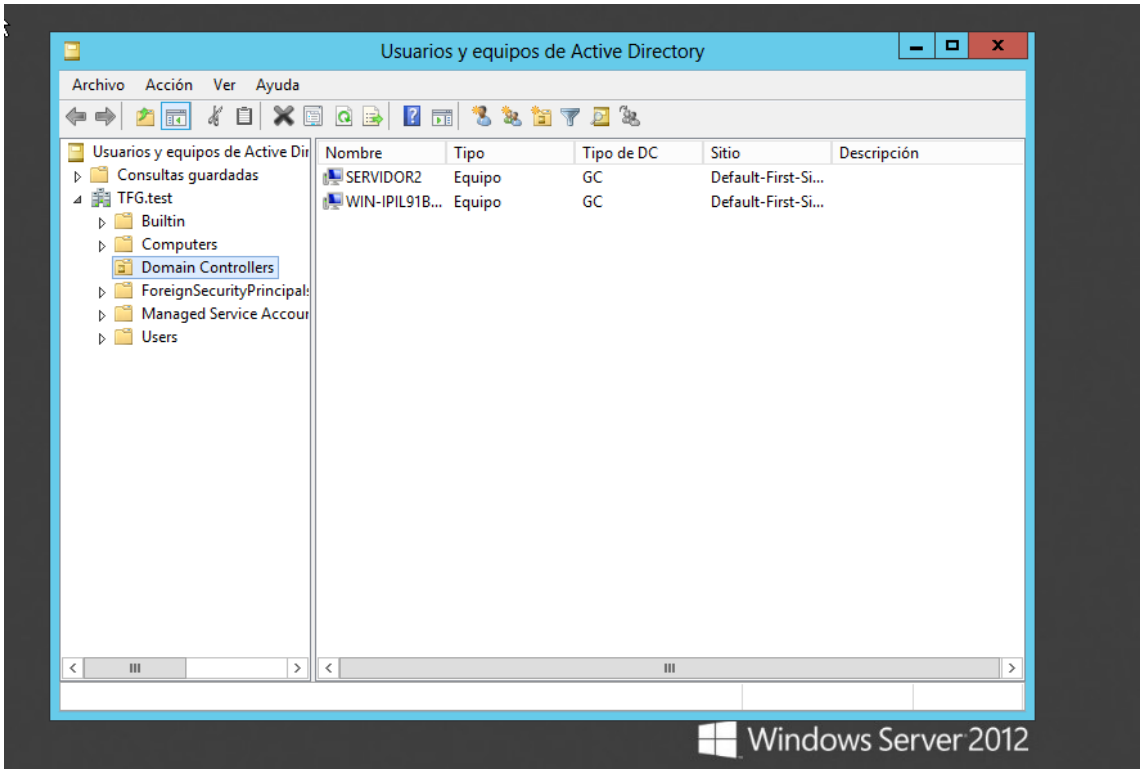


*Figura 48: Servidor 2 como Catálogo Global*

Una vez el servidor ya está configurado como Catálogo Global, vamos a designarlo también como DNS. Nuevamente, en la consola de Administración del servidor seleccionamos "Agregar roles y características" y seleccionamos la instalación basada en roles.

Cuando llegamos a la pantalla de selección de roles de servidor, escogemos el rol de Servidor DNS, aceptamos la instalación de características adicionales y pulsamos Siguiente.

Vamos siguiendo el asistente hasta que finaliza la instalación del rol de Servidor DNS.

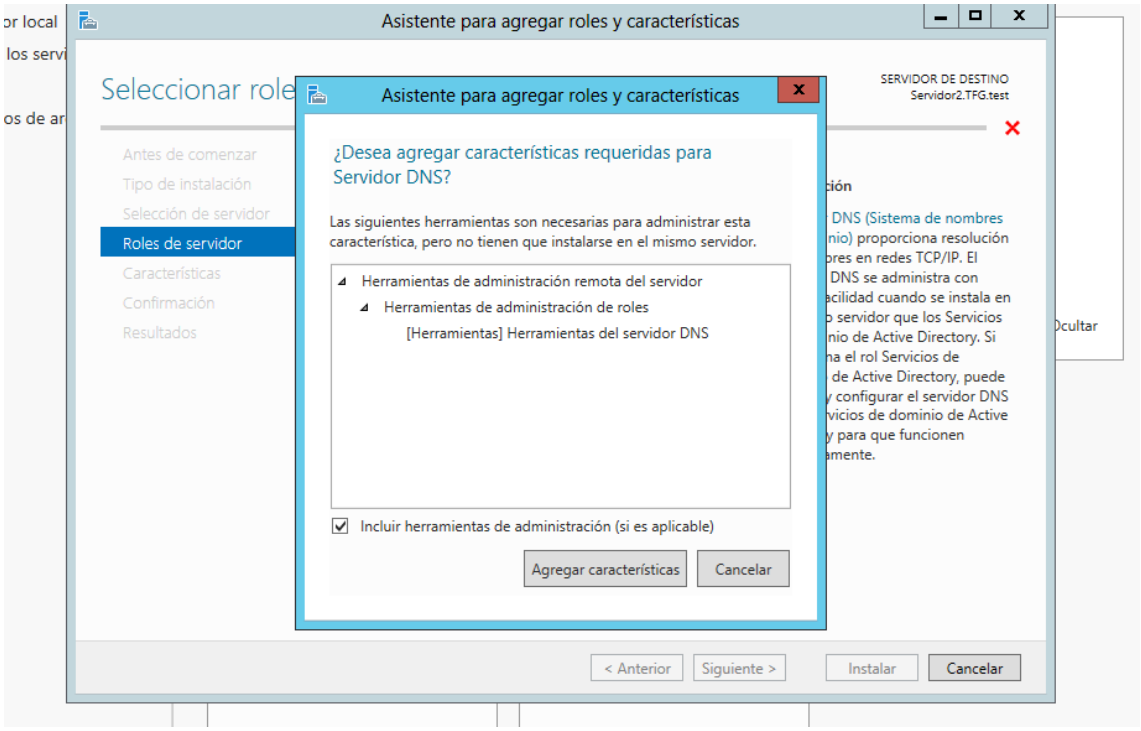


*Figura 49: Características adicionales*

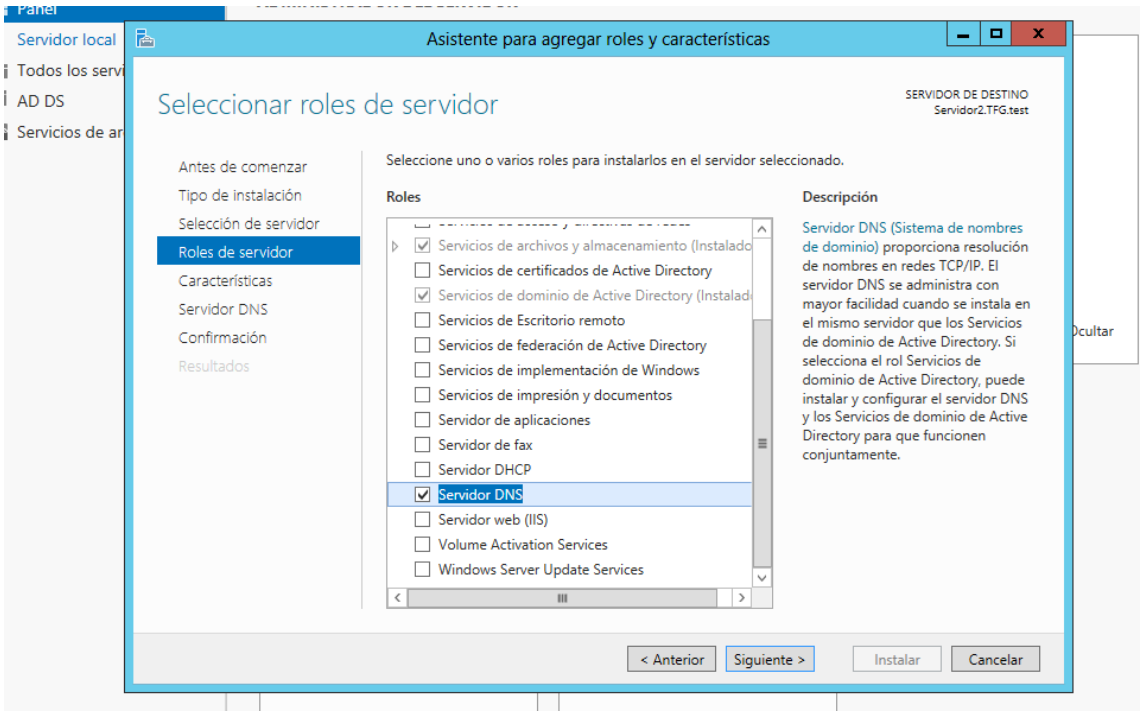


*Figura 50: Selección del rol Servidor DNS*

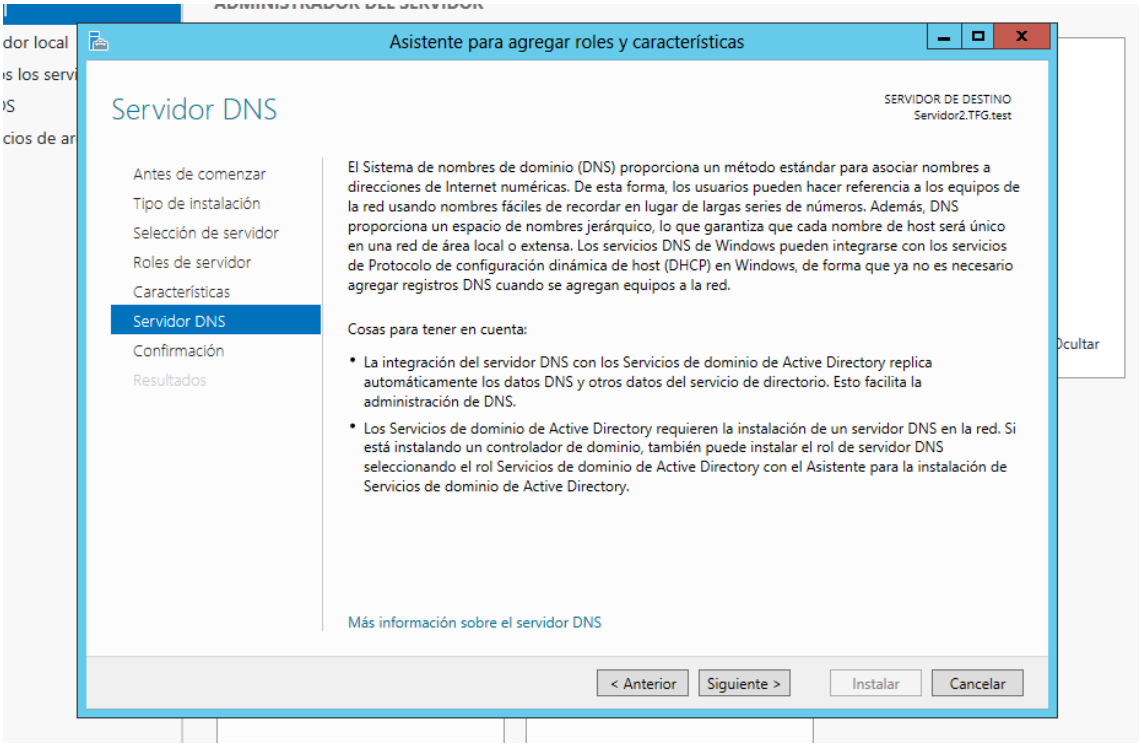


*Figura 51: Información sobre el DNS*

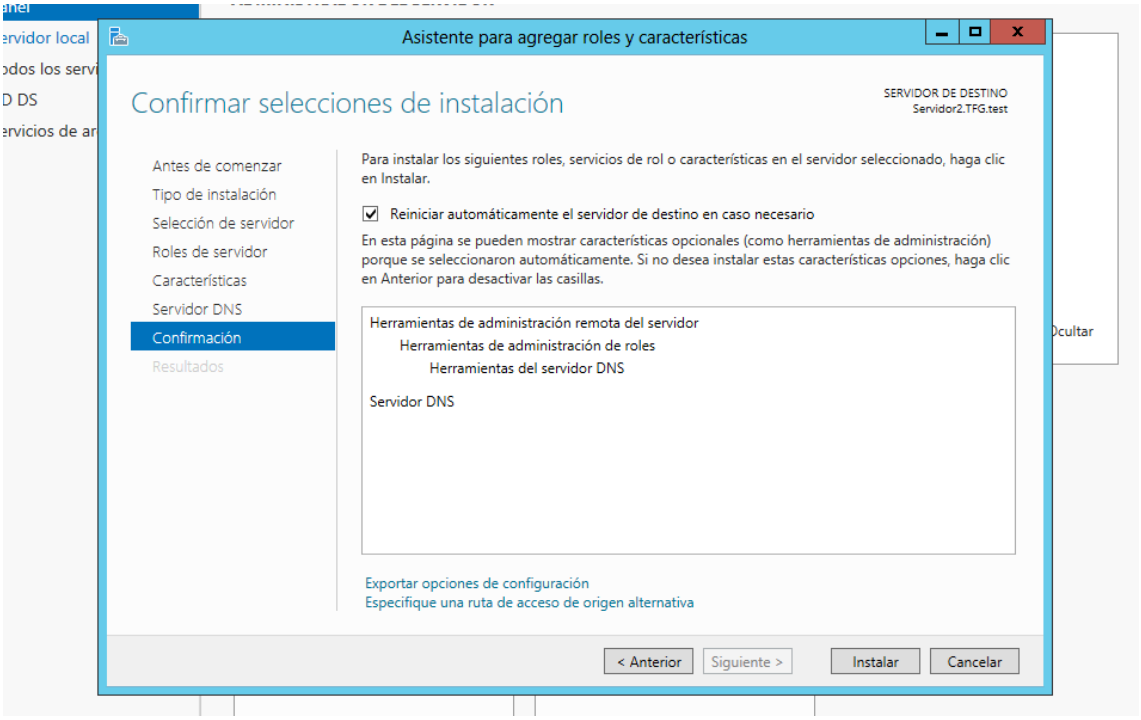


*Figura 52: Confirmación*

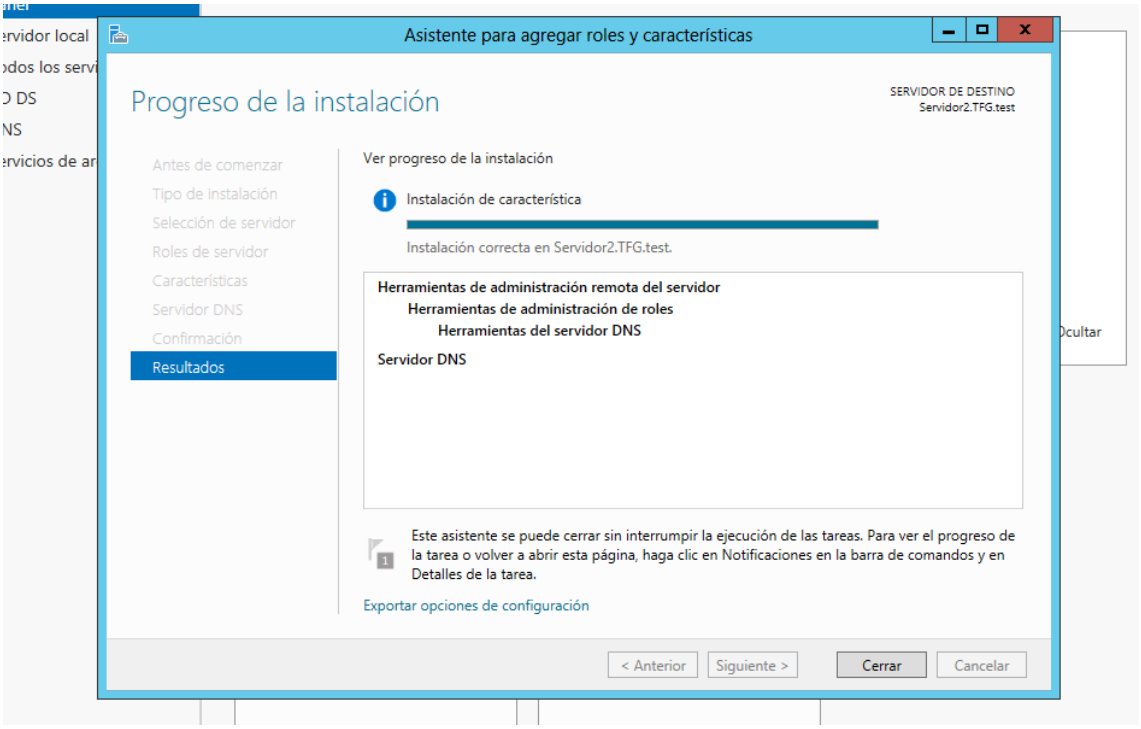


*Figura 53: Progreso*

Una vez finalizada la instalación, ahora es el momento de configurarlo y asegurarse de que funciona. Para ello, abrimos el Centro de redes y recursos compartidos y entramos en Propiedades del Protocolo IPv4. Como DNS principal ponemos la dirección de este servidor, y trasladamos la dirección que ya teníamos como DNS, la del servido principal, al Servidor DNS alternativo.

Una vez hecho esto (Figura 54) nos dirigimos a la consola de administración del Servidor DNS en el servidor principal, y lo configuramos para que escuche también las peticiones del servidor secundario.

Dentro de la consola de administración del DNS seleccionamos Zonas de búsqueda directa, y hacemos clic derecho sobre _mcds.TFG.test (Figura 55) y seleccionamos Propiedades. A continuación seleccionamos la pestaña Servidores de nombre y pulsamos “Agregar…”

En la nueva ventana escribimos el nombre de nuestro servidor secundario “Servidor2” y pulsamos Resolver, veremos como en el cuadro inferior aparece la IP de nuestro servidor secundario (Figura 57), pulsamos aceptar y con esto finalizamos la configuración de ésta máquina como servidor de respaldo.

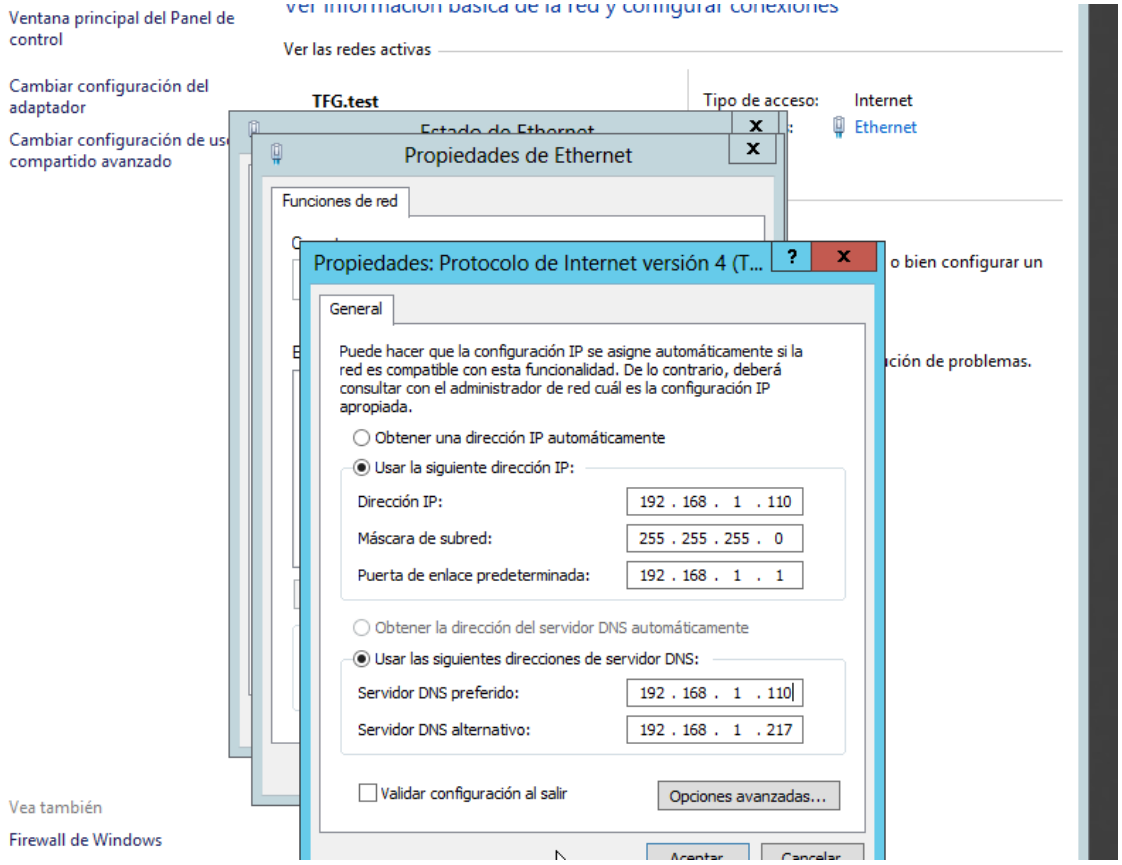


*Figura 54: Configuración I*

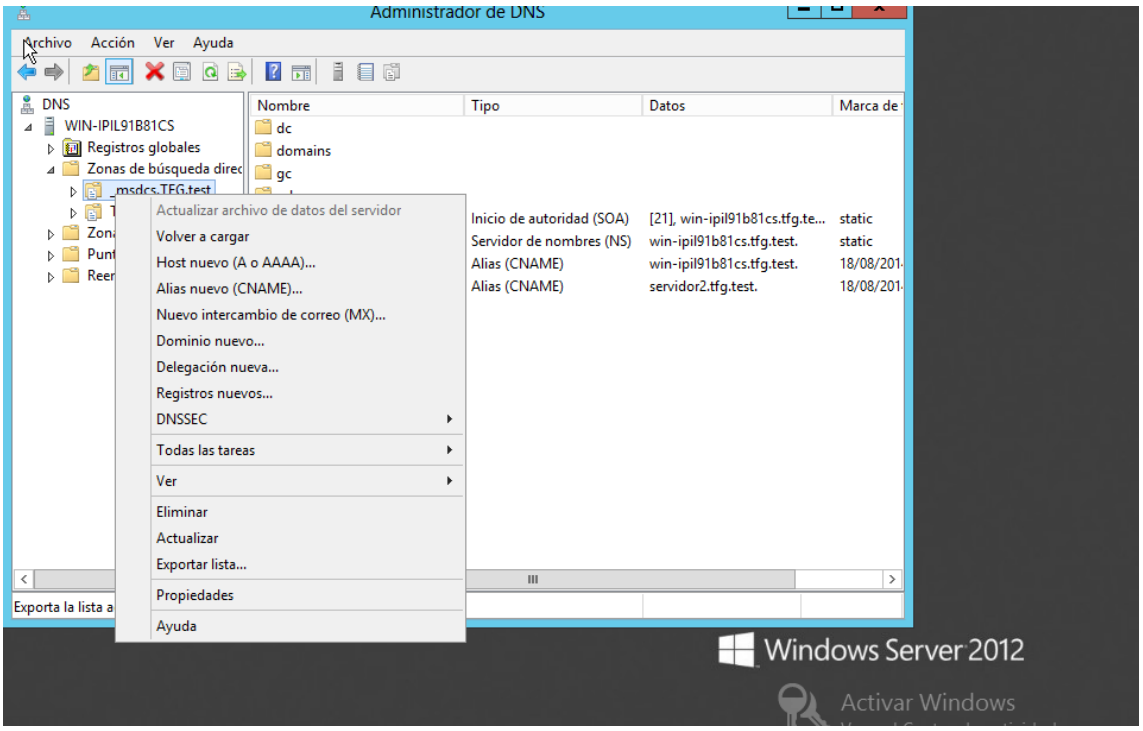


*Figura 55: Configuración II*

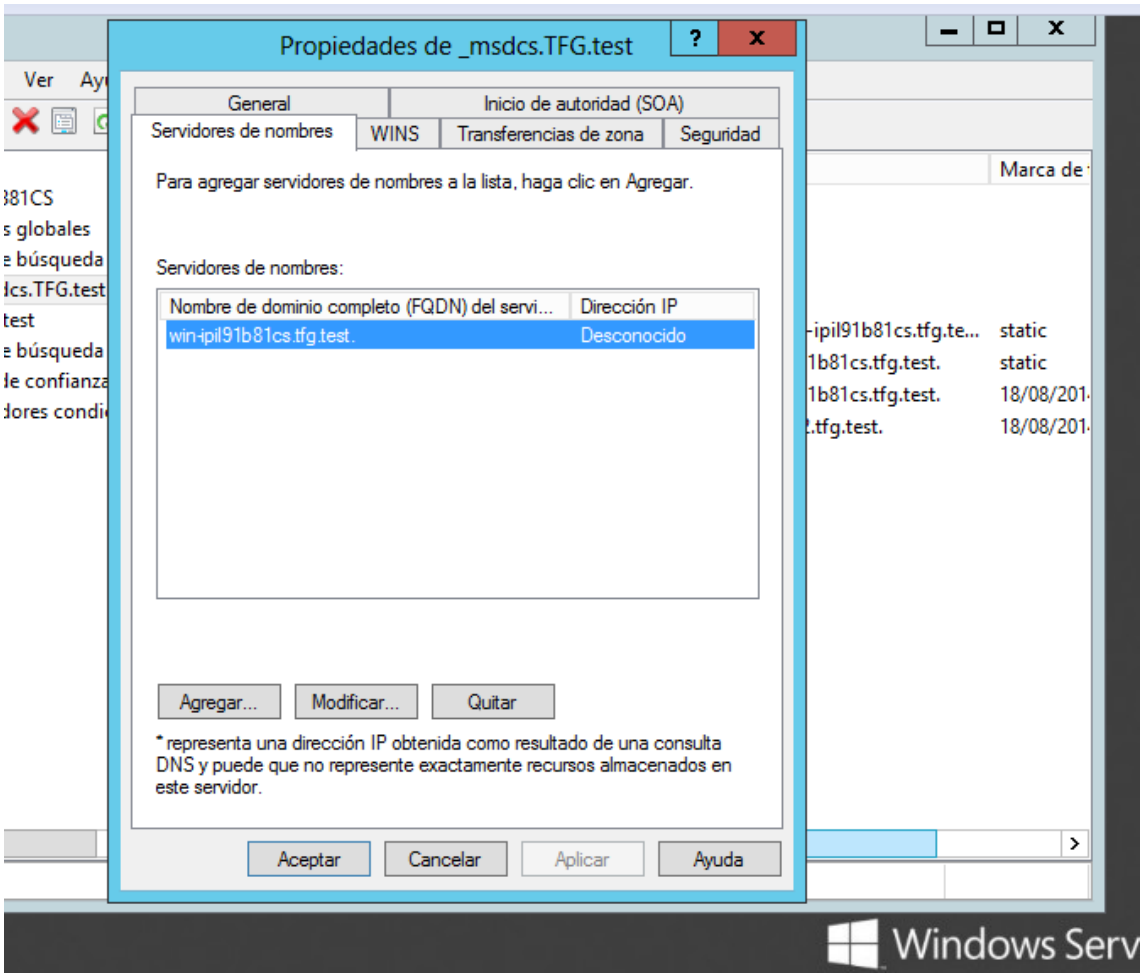


*Figura 56: Configuración III*

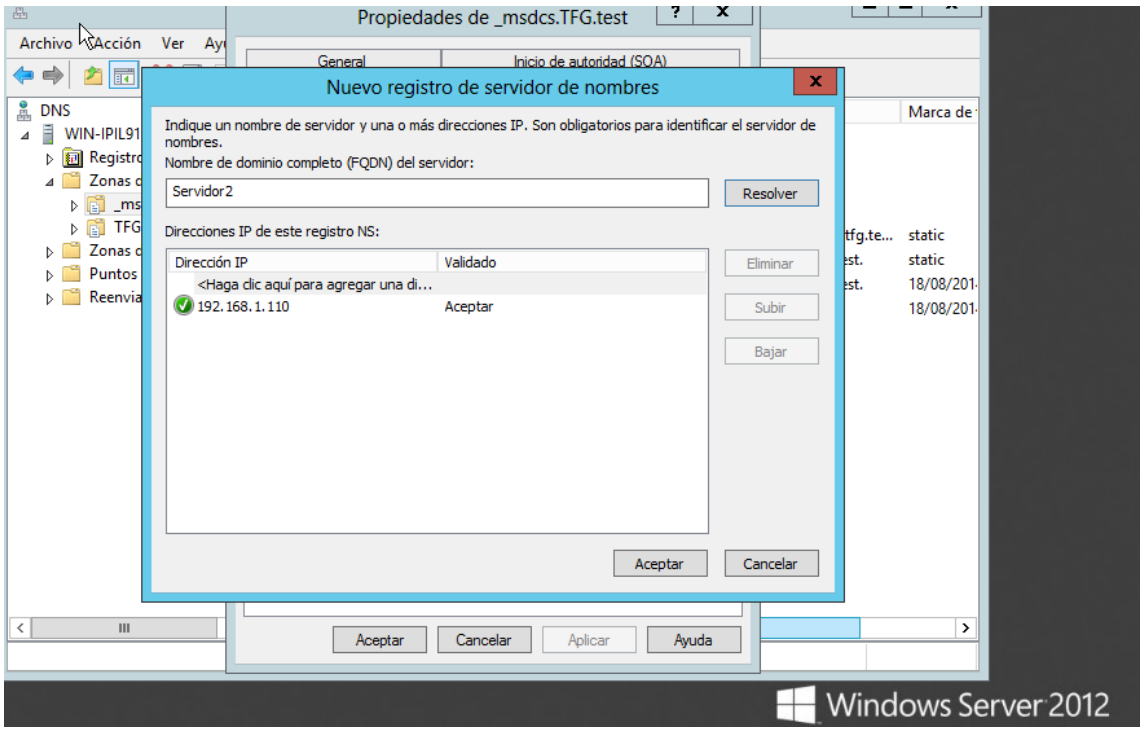


*Figura 57: Configuración IV*

# 3.5 Adición de los equipos al dominio

Ahora que ya tenemos tanto el servidor DNS como el servidor DHCP configurados, ya podemos agregar equipos al dominio. Para ello nos dirigimos al "Centro de redes y recursos compartidos" de Windows y realizaremos un proceso muy similar al que ya llevamos a cabo a la hora de asignar la IP estática al servidor. Ésta vez, dejaremos seleccionada la opción de "Asignar una IP dinámicamente" y como dirección del servidor DNS asignaremos la IP de nuestro servidor principal, es decir, 192.168.1.217.

Con esto conseguimos que este equipo ya se encuentre en la subred que el servidor nos direcciona, ya que le asigna una de las IPs del rango establecido en el DNS.

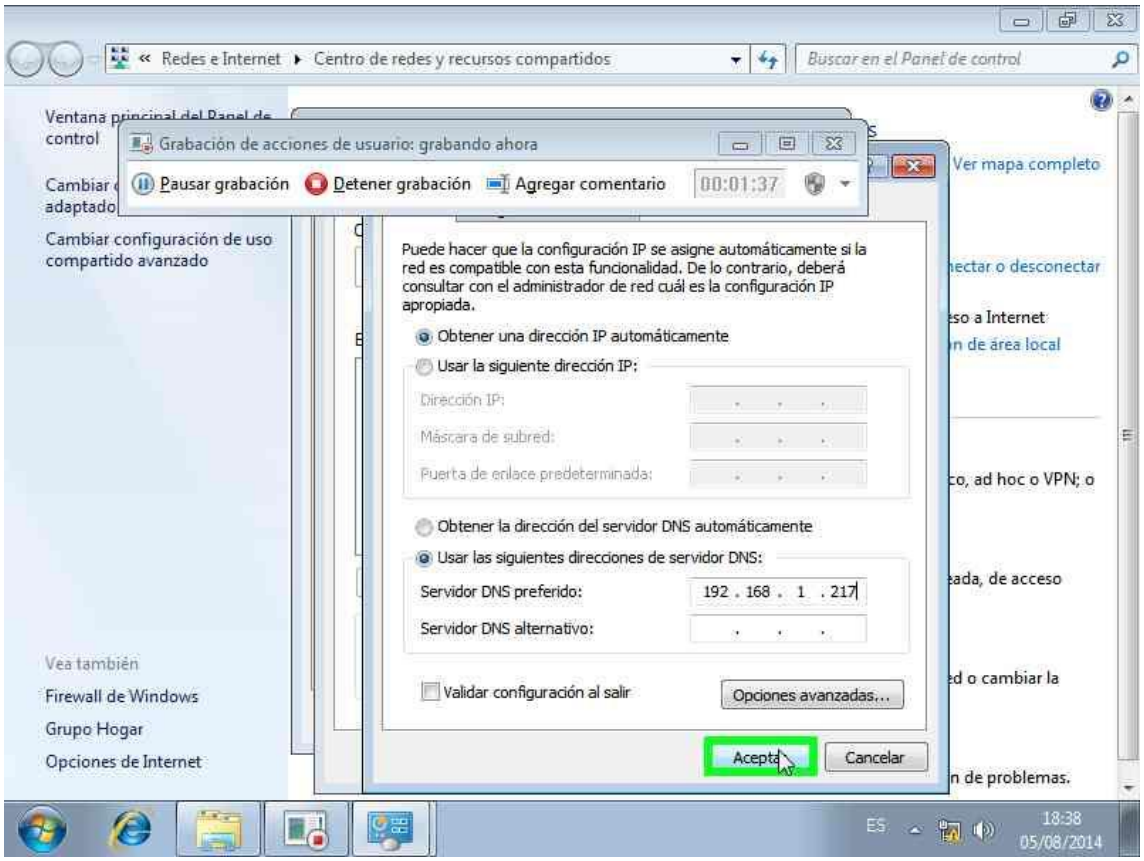


*Figura 58: Asignación DNS e IP*

A continuación, nos dirigimos a Equipo -> Propiedades

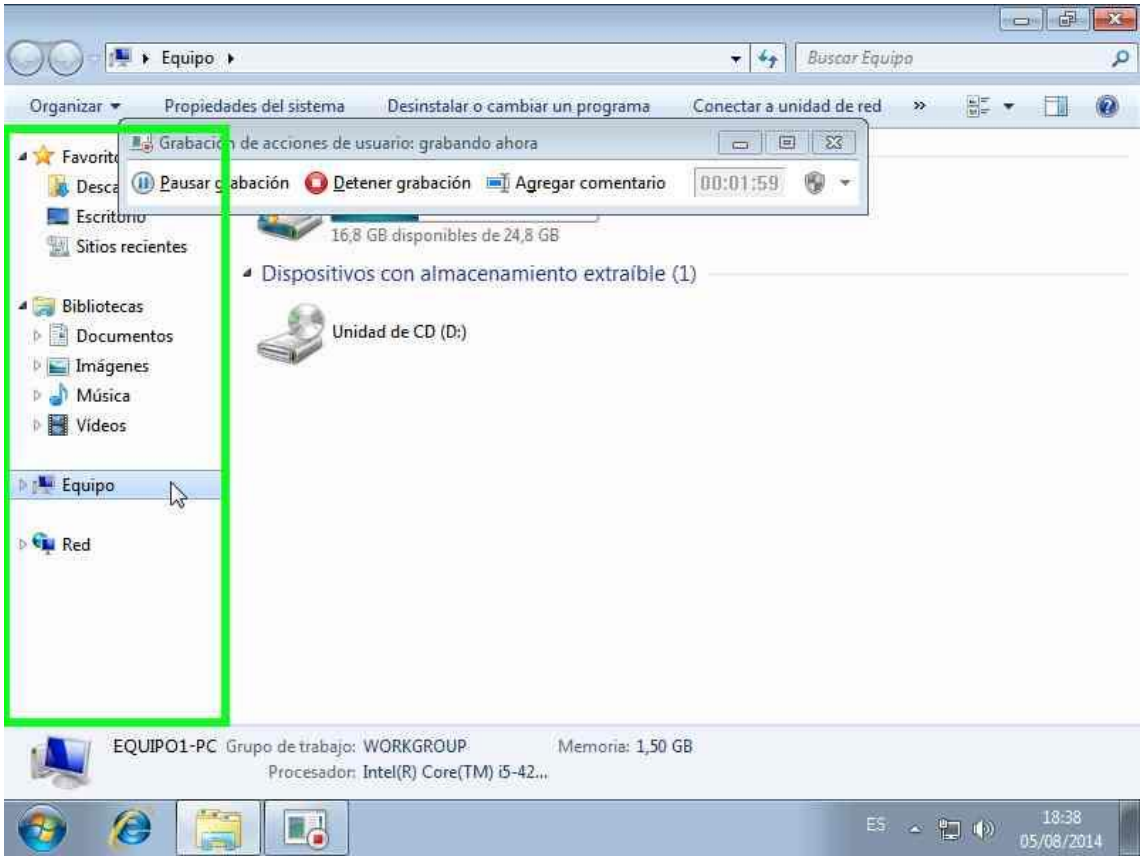


*Figura 59*

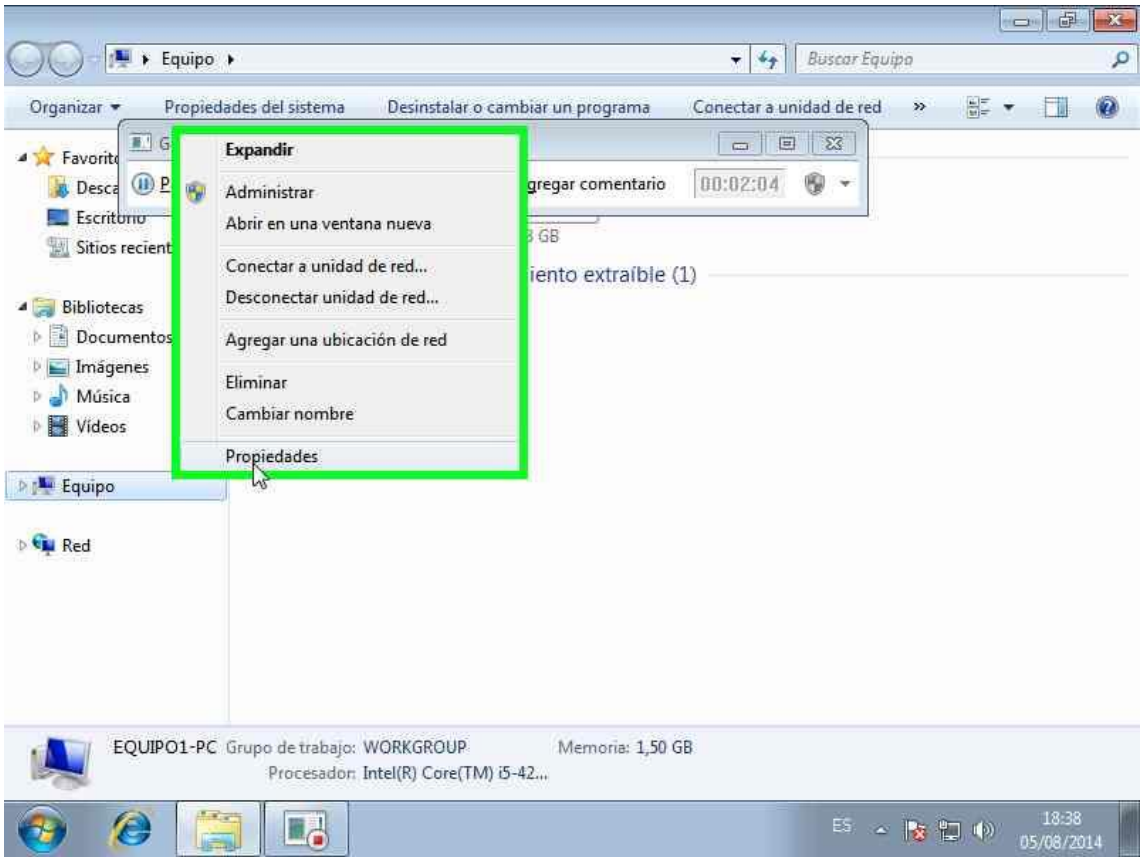


*Figura 60*

Tras esto, se nos abre la pantalla de información del sistema, donde pulsamos “Cambiar configuración

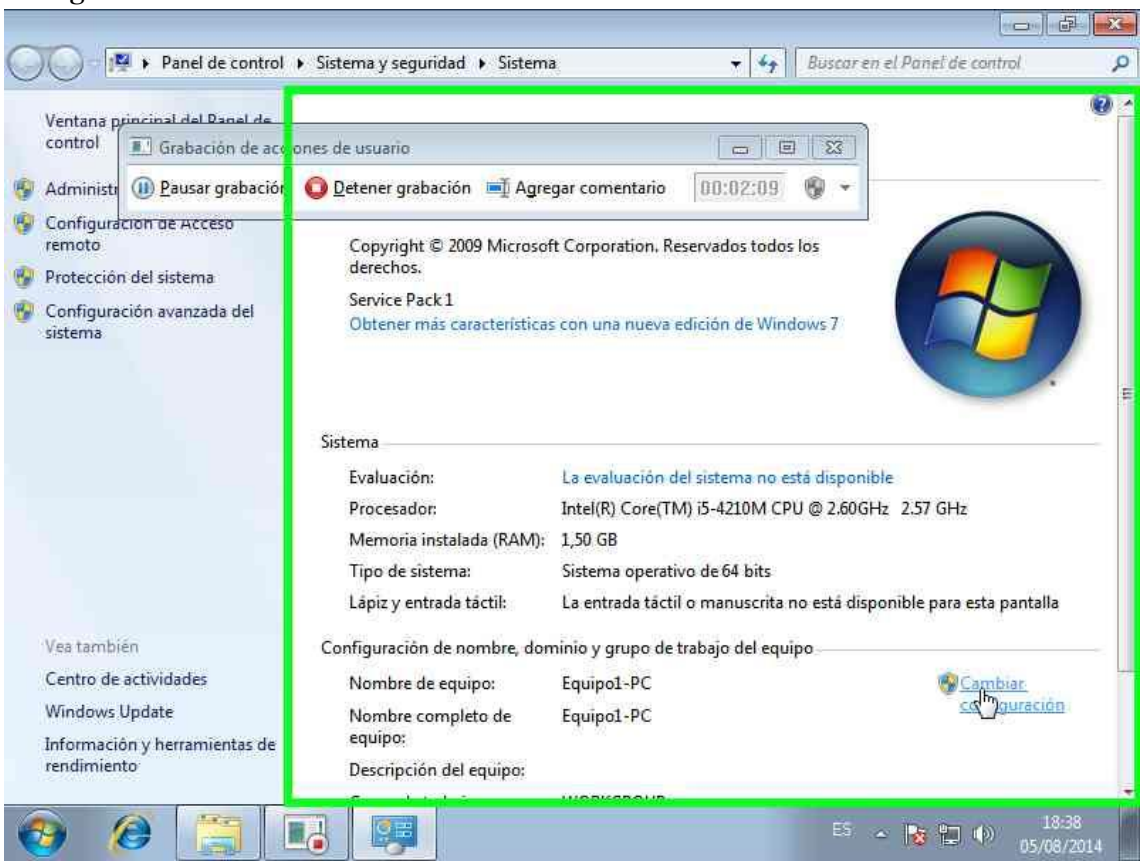


*Figura 61: Información del sistema*

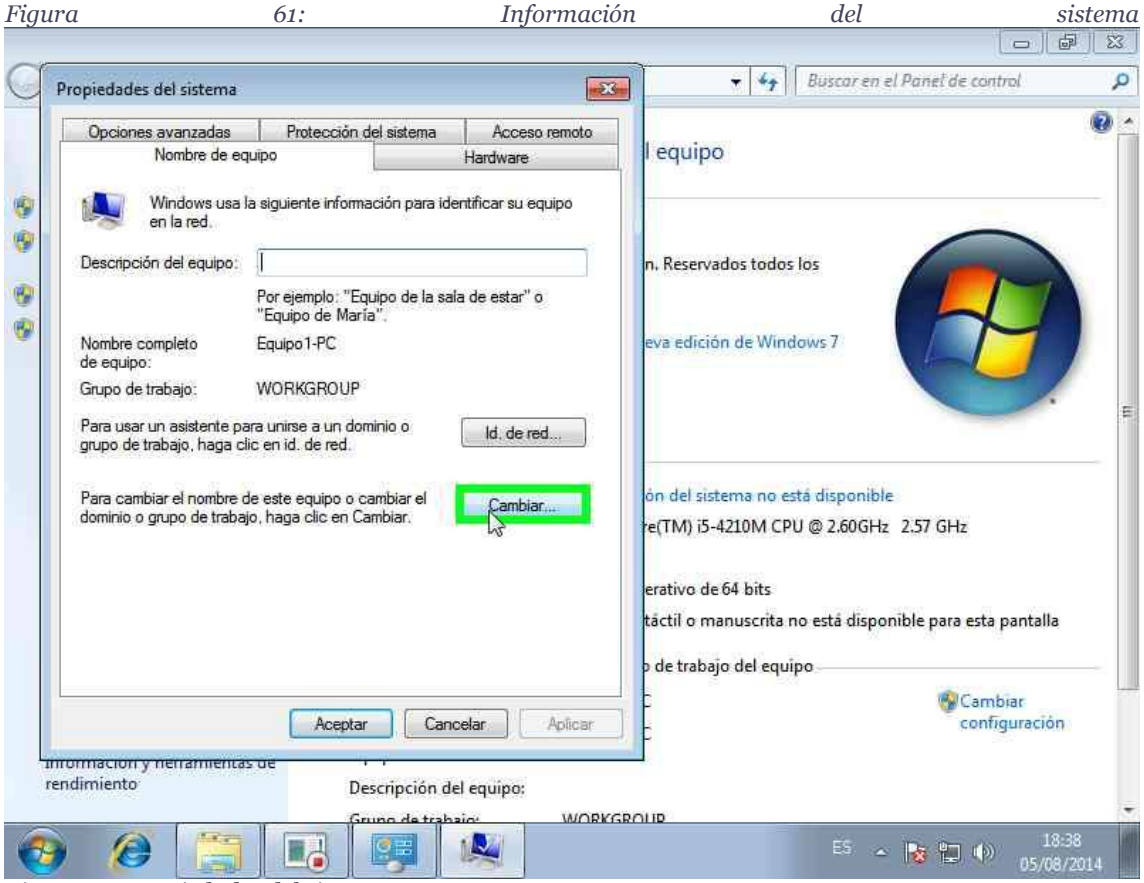


*Figura 62: Propiedades del sistema*

En ésta nueva ventana que se nos abre, pulsamos “Cambiar” como se observa en la Figura 35, y en la nueva ventana seleccionamos “Dominio” y escribimos como nombre del dominio TFG

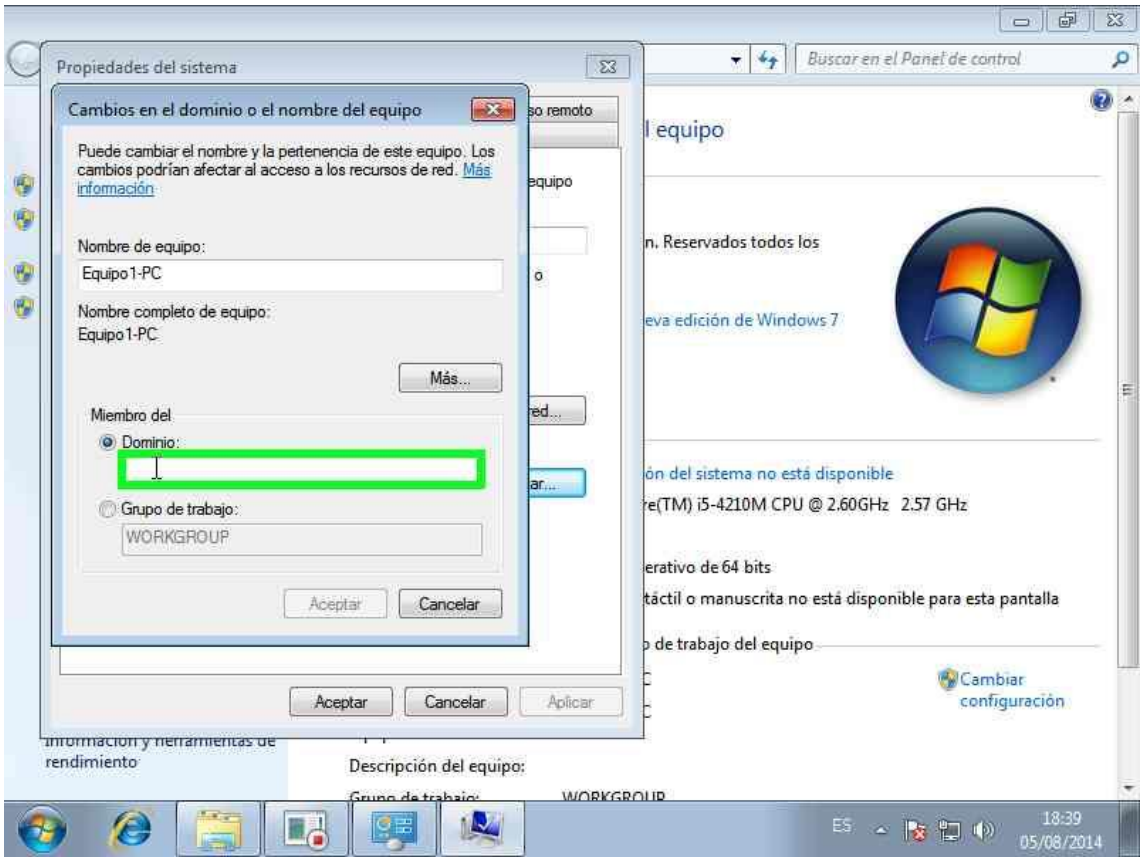


*Figura 63: Cambio al dominio*

Acto seguido se nos abrirá una nueva ventana donde Windows nos solicitará las credenciales de inicio de sesión de una cuenta con los suficientes permisos como para permitir al equipo la unión al dominio, al igual que en los casos anteriores, seleccionaremos la cuenta de Administrador.

Tras introducir el nombre de usuario y la contraseña, aparece una ventana en la que se nos indica que el equipo se ha unido satisfactoriamente al dominio. A continuación reiniciaremos el equipo para poder hacer efectivos los cambios.

Esta operación la repetiremos cada vez que añadamos un equipo al dominio.


*Figura 64: Asignación de las credenciales*

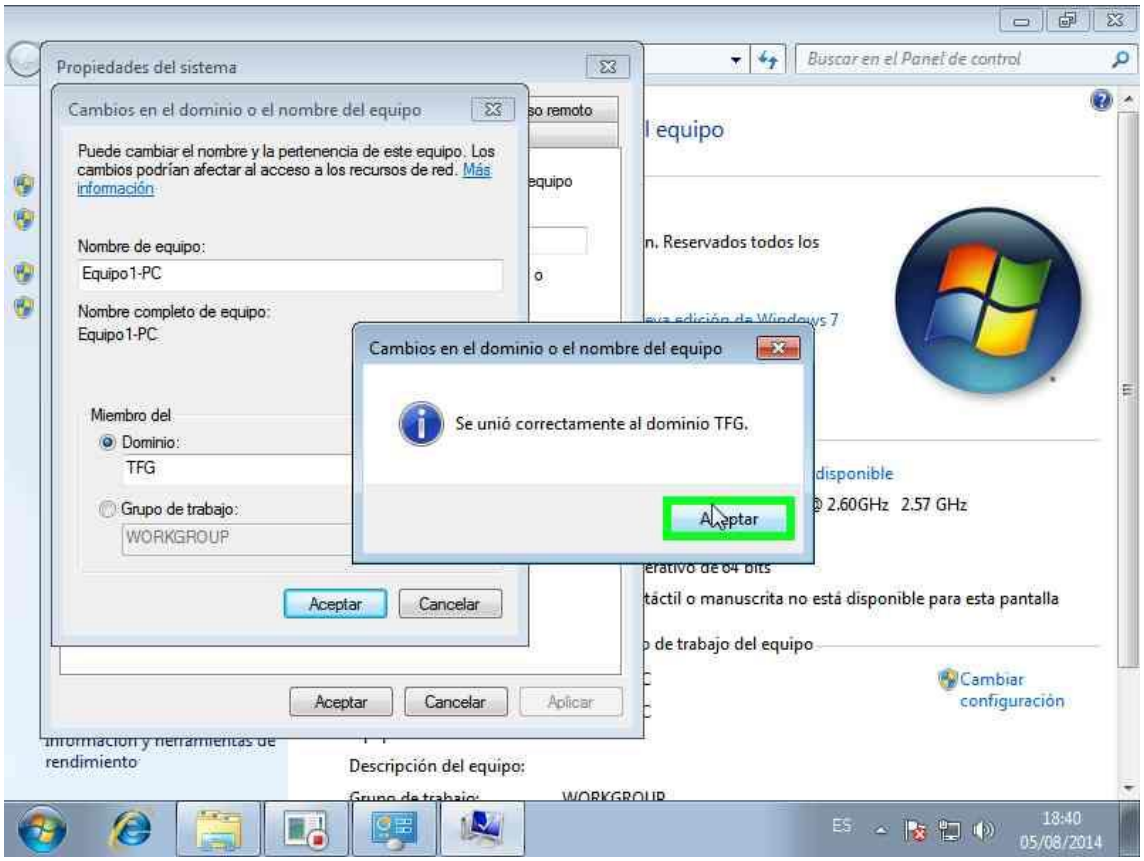


*Figura 65*

## 3.6 Creación de los usuarios y grupos de usuario

Ahora que ya tenemos creado el dominio, configurados todos los servidores y sus roles, y los equipos se han unido al dominio, ha llegado el momento de crear usuarios y grupos de usuarios y distribuirlos en las distintas unidades organizativas.

En este caso se han creado tres unidades organizativas: Análisis, Desarrollo y Dirección.

Para este trabajo, se han creado un total de 7 usuarios utilizando el asistente de creación de usuarios al que podemos acceder desde el menú Usuarios y Equipos de Active Directory haciendo doble clic sobre nuestro dominio TFG.test, abriéndose así una nueva ventana con las distintas carpetas con distinta información relacionada con el dominio, como por ejemplo la carpeta Computers donde nos aparecen los ordenadores asociados al dominio, la carpeta Domain Controllers, donde nos parecen los servidores controladores del dominio, o la carpeta Users, donde nos aparecen los distintos usuarios y grupos de usuario existentes en el dominio. Es en ésta carpeta Users donde procederemos a crear los distintos usuarios.

Para ello, hacemos clic derecho sobre la carpeta Users y seleccionamos la opción Nuevo -> Usuario abriéndose una nueva ventana en la que podremos rellenar los datos personales del usuario: nombre, apellidos, iniciales, además de otorgarle un nombre de inicio de sesión y asignarle un dominio, en este caso el único que hemos creado, TFG.test.

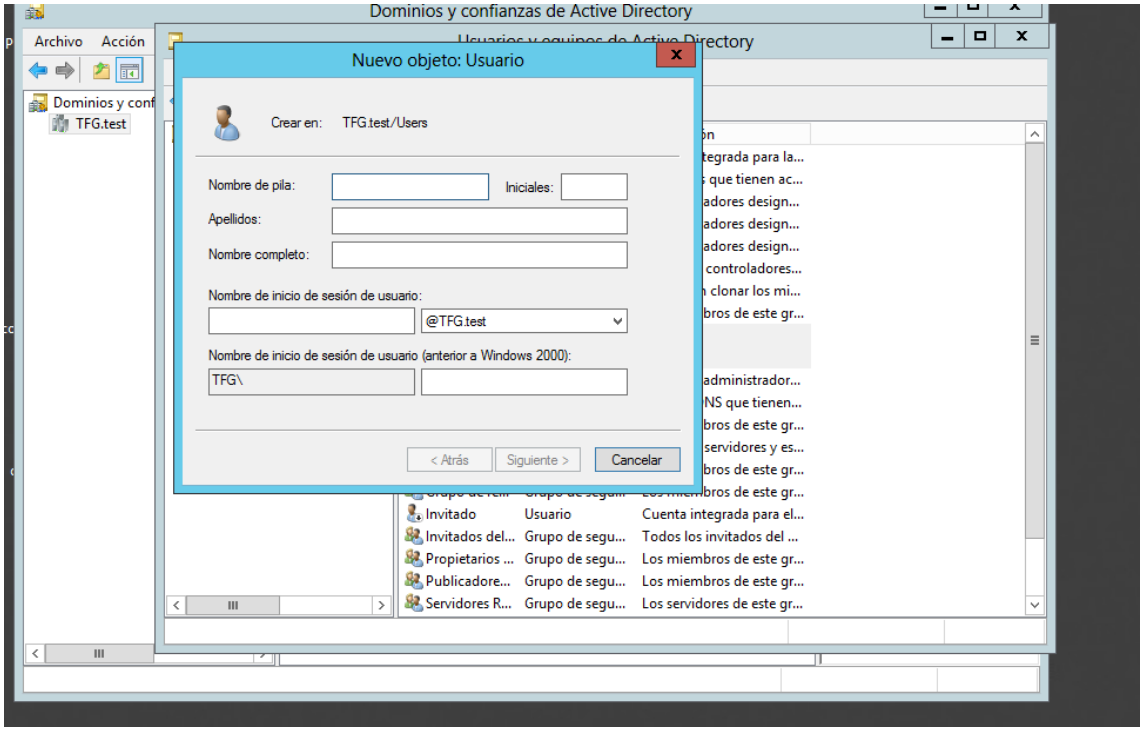


*Figura 66: Creación de usuarios I*

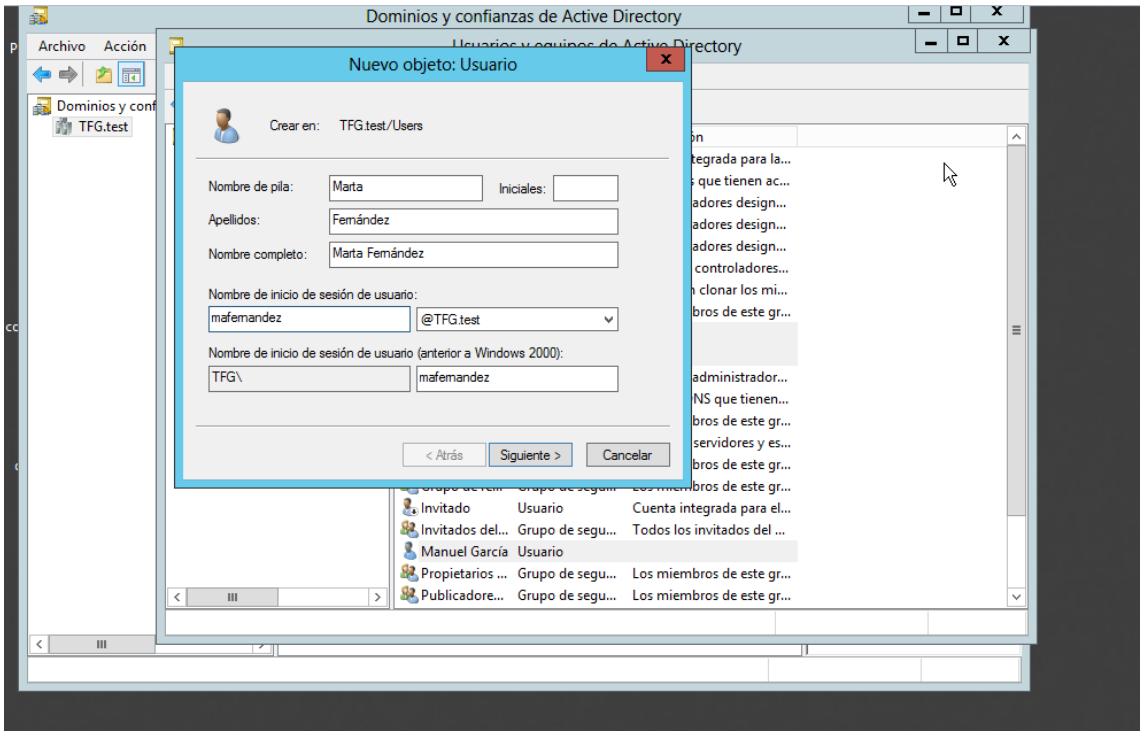


*Figura 67: Creación de usuarios II*

Al pulsar siguiente, se abre una nueva ventana donde debemos escribir la contraseña de acceso para el nuevo usuario y las opciones de seguridad de la misma. En este caso se ha seleccionado la opción “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”, ya que es más seguro, y también más cómodo para el usuario, que la contraseña sea cambiada por él.

A la hora de elegir la contraseña, hay ciertos detalles a tener en cuenta, por ejemplo la contraseña no puede contener el nombre del usuario, y es conveniente que sea una contraseña alfanumérica con letras mayúsculas y minúsculas.

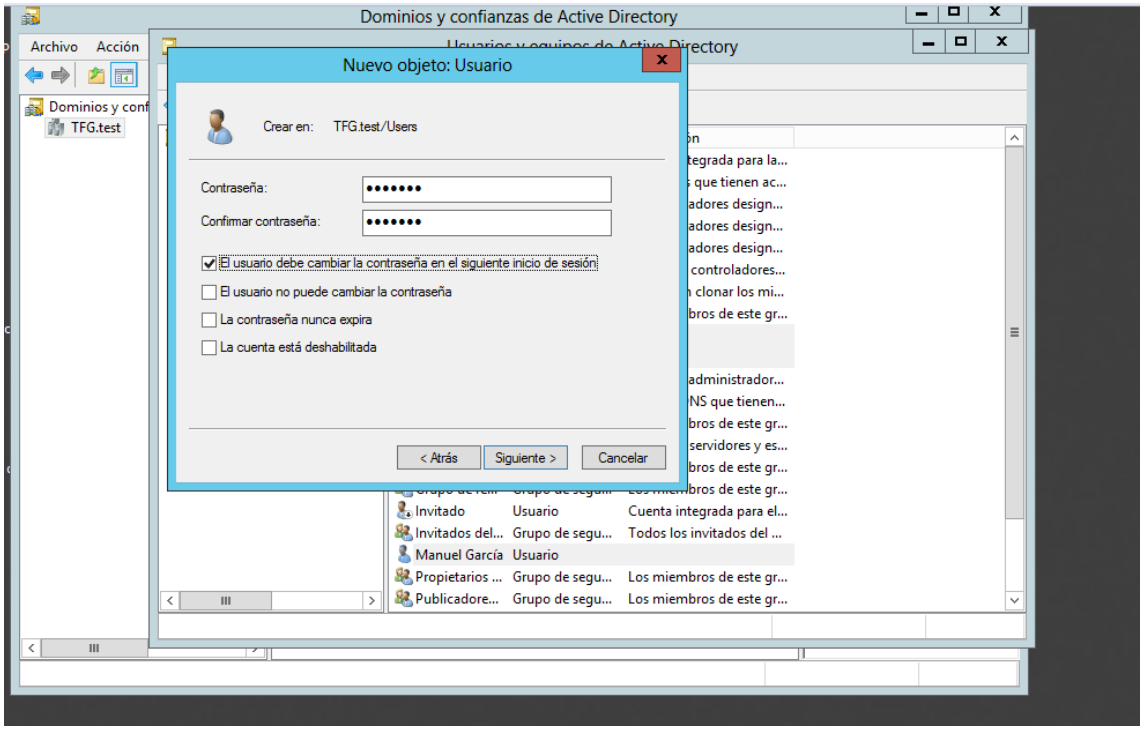


*Figura 68: Selección de la contraseña*

A continuación, una vez creada la contraseña, nos aparece un resumen de los datos del nuevo usuario. Observamos que los datos son correctos y pulsamos “Finalizar”.

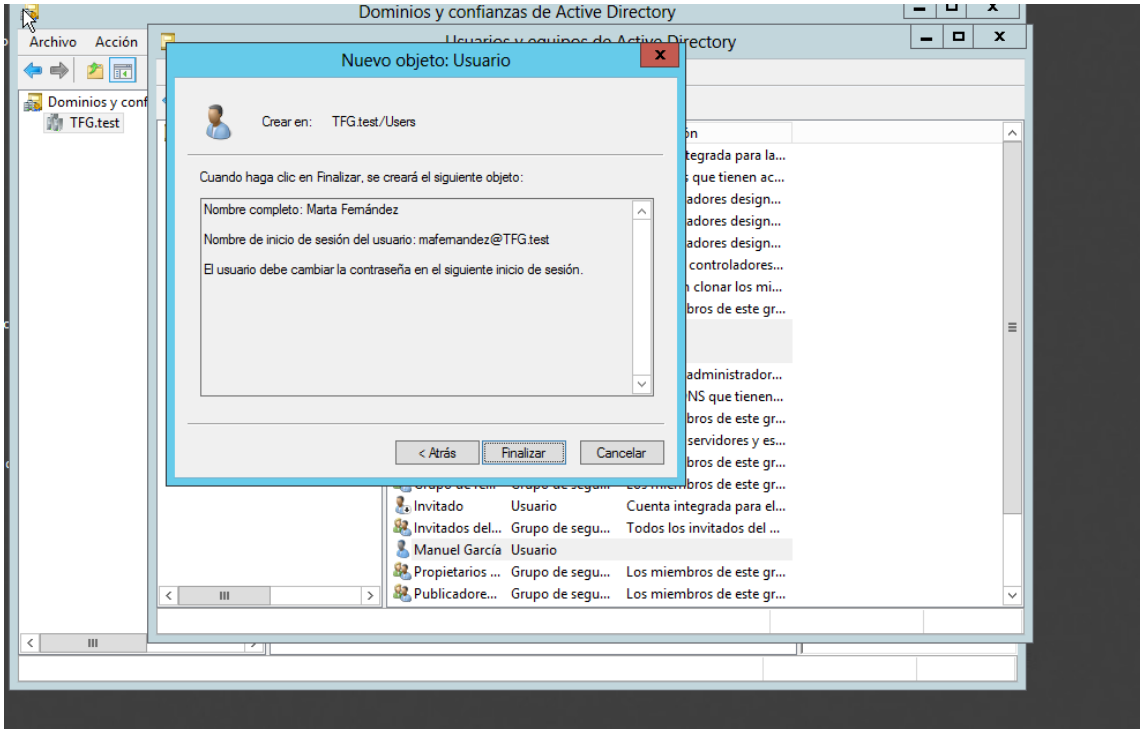


*Figura 69: Resumen de la creación*

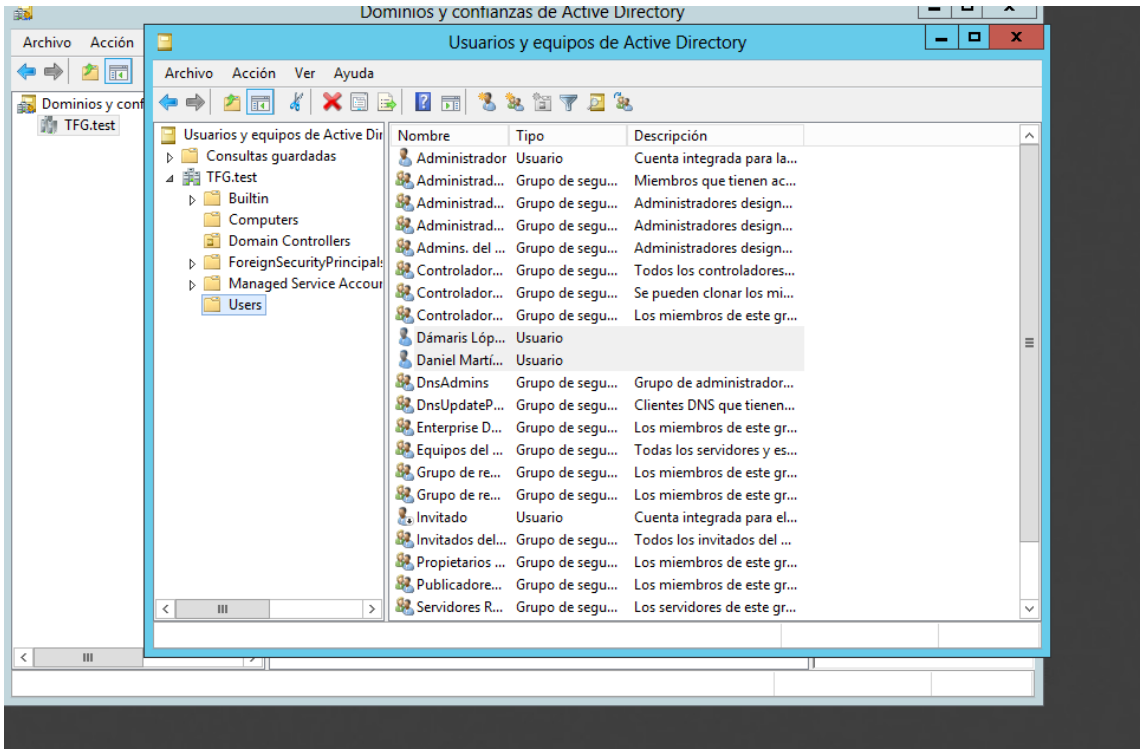


*Figura 70: Vista de los Usuarios en la carpeta Users*

Este proceso se repite varias veces, tantas como usuarios decidamos crear.

Finalmente, una vez los usuarios han sido creados, realizamos una prueba en uno de los equipos asociados al dominio con uno de los usuarios recién creados

y comprobamos que, efectivamente podemos iniciar sesión en los equipos asociados al dominio.

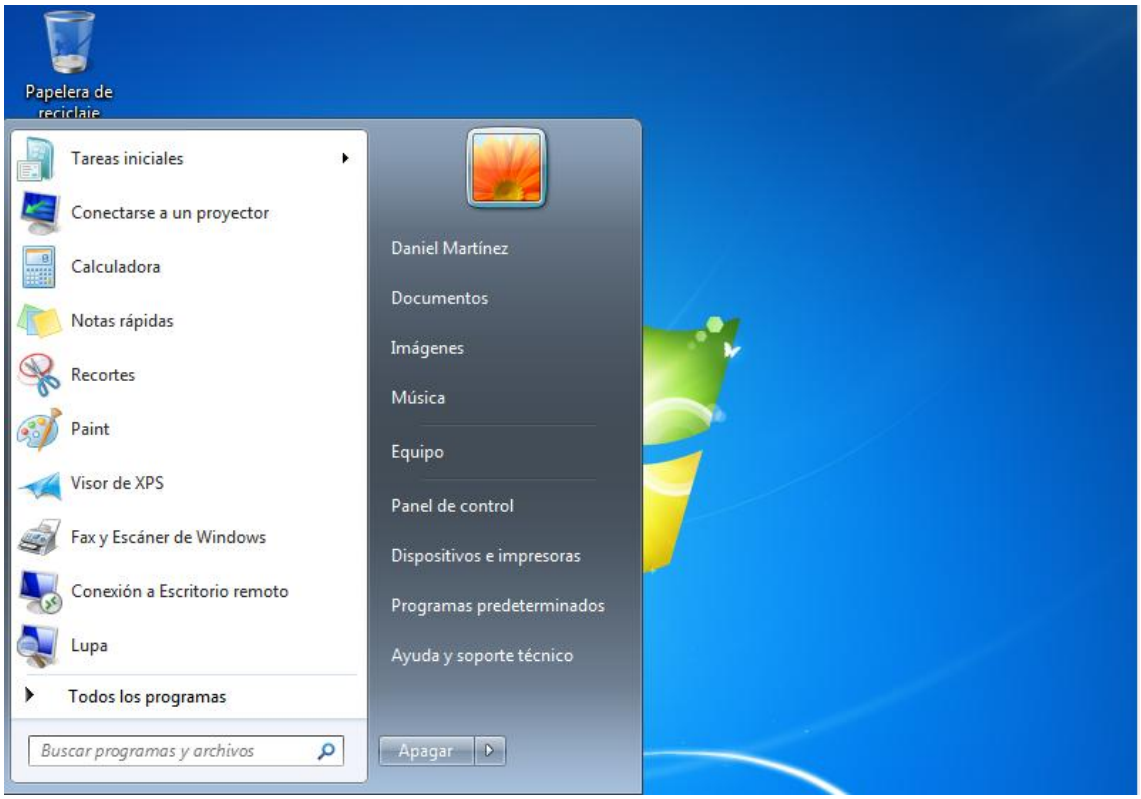


*Figura 71: Prueba de inicio de sesión con uno de los usuarios*

Ahora que ya disponemos de usuarios, debemos organizarlos en grupos de usuarios. Para ello crearemos los grupos de usuarios DesarrolladoresP1, AnalistasP1, ManagerP1, DesarrolladoresP2, AnalistasP2 y ManagerP2, que serán grupos globales. Los dos grupos de Analistas se situarán en la unidad organizativa Análisis, los dos grupos de Desarrolladores se situarán en la unidad organizativa Desarrollo y, finalmente, los dos grupos de Manager se situarán en la unidad organizativa Dirección. Además, para evitar futuros problemas cuando vayamos a aplicar las GPOs a estas unidades organizativas, también hemos movido los usuarios de la carpeta Users a sus correspondientes unidades organizativas.

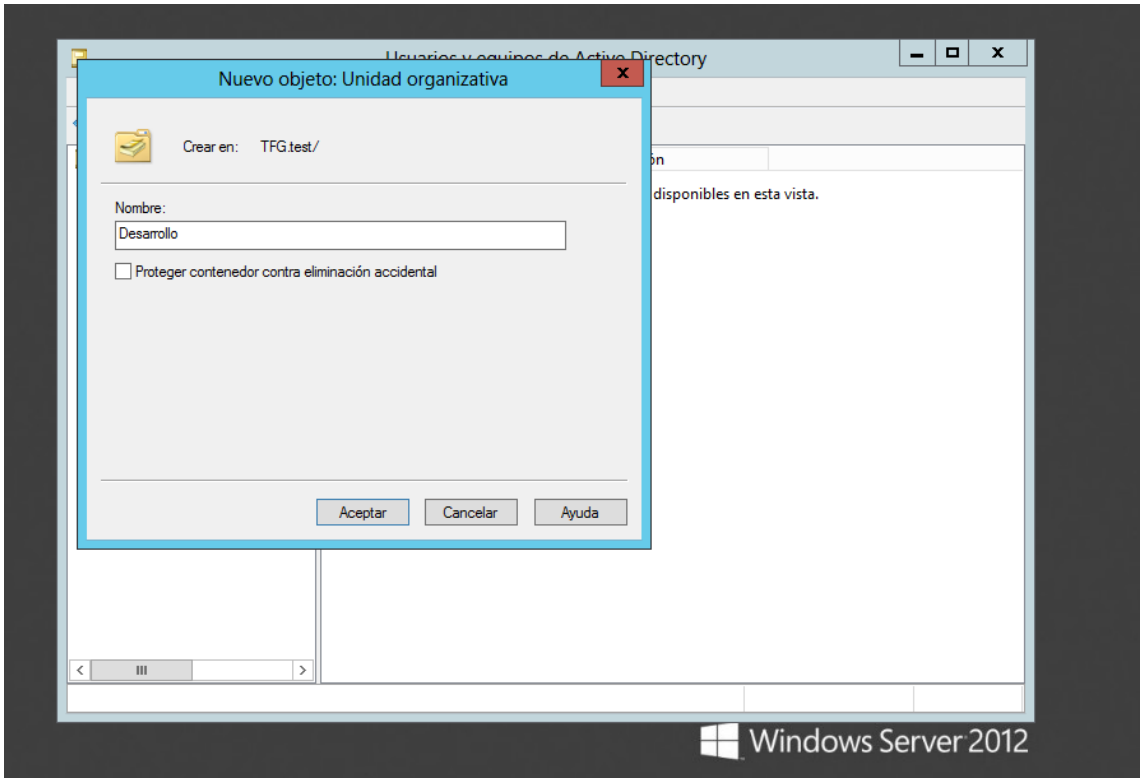


*Figura 72: Creación de la unidad organizativa*

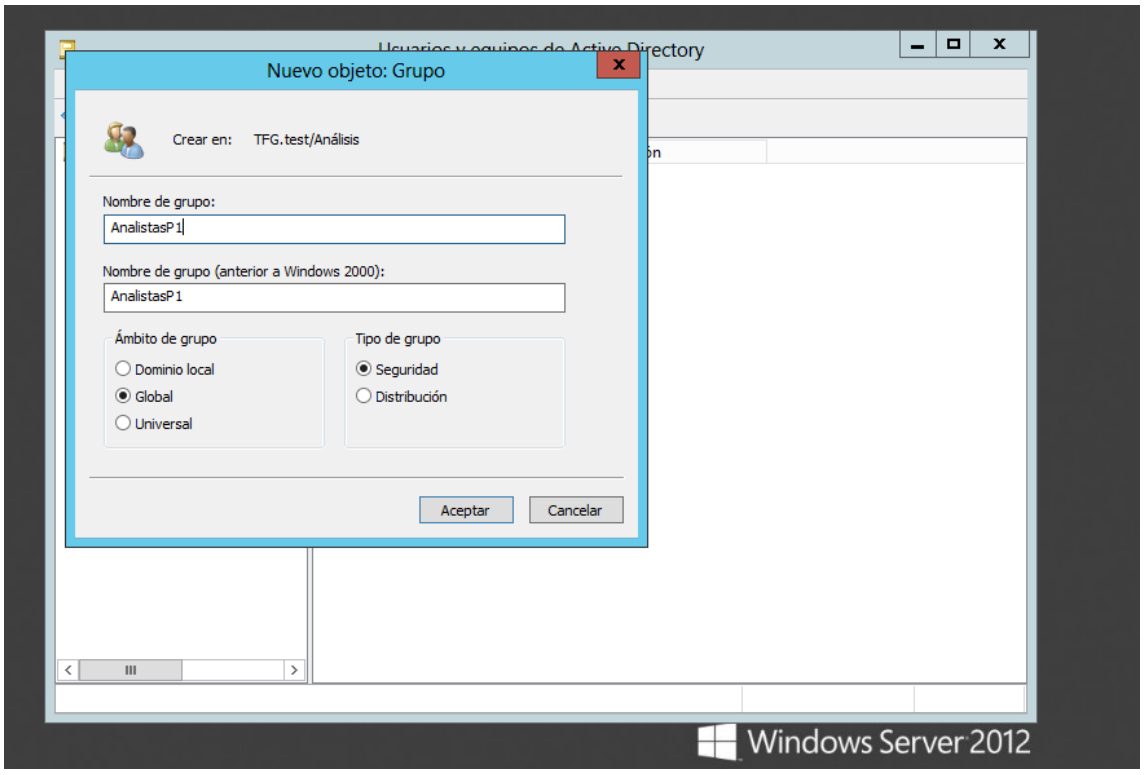


*Figura 73: Creación grupo de usuarios*

Una vez creados los grupos, podemos seleccionar uno de ellos y hacer clic derecho sobre él. En el menú desplegable seleccionamos la opción "Propiedades" y en la nueva ventana nos dirigimos a la pestaña miembros.

En esta pestaña, nos aparece un listado de los usuarios del grupo, si los hubiere, y también podemos agregar o quitar usuarios del grupo. Para agregar usuarios pulsamos el botón "Agregar" y se abre una nueva ventana desde la que podemos seleccionar los tipos de objetos que queremos añadir al grupo, el dominio en el que se encuentran los usuarios a los que queremos añadir y, finalmente un bloque en el que podemos escribir los nombres de los usuarios para añadirlos.

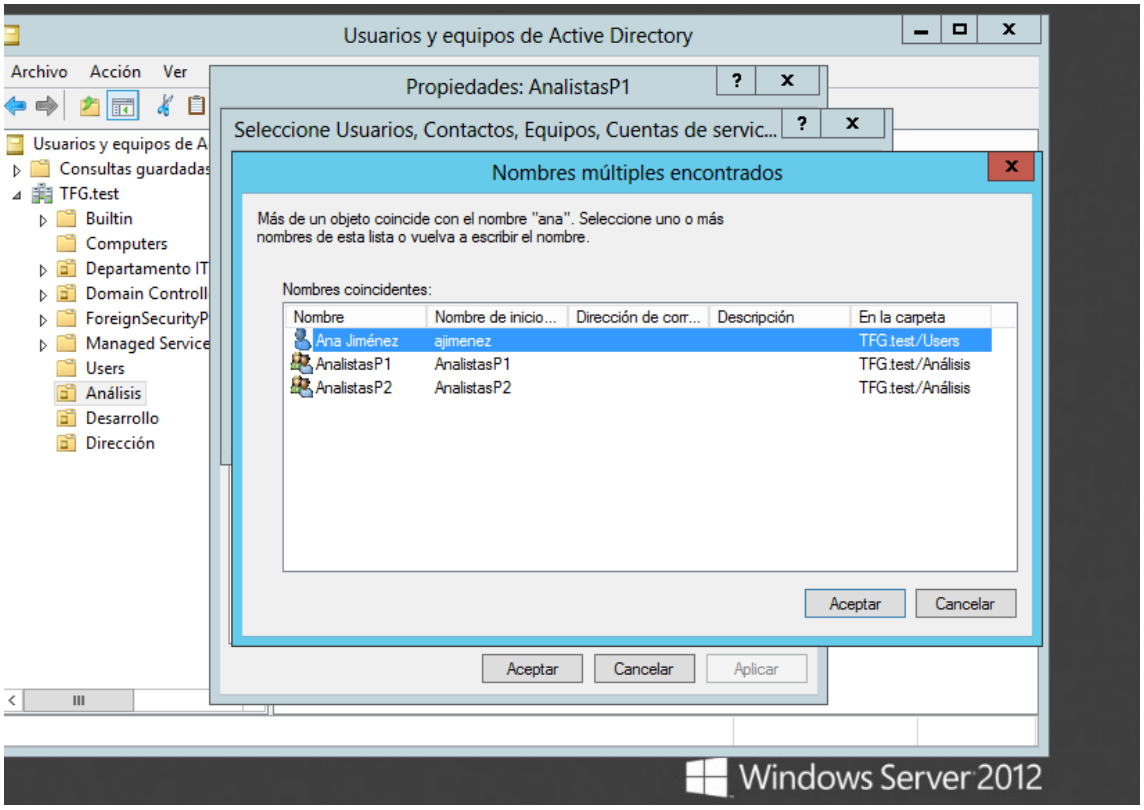


*Figura 74: Comprobar nombres*

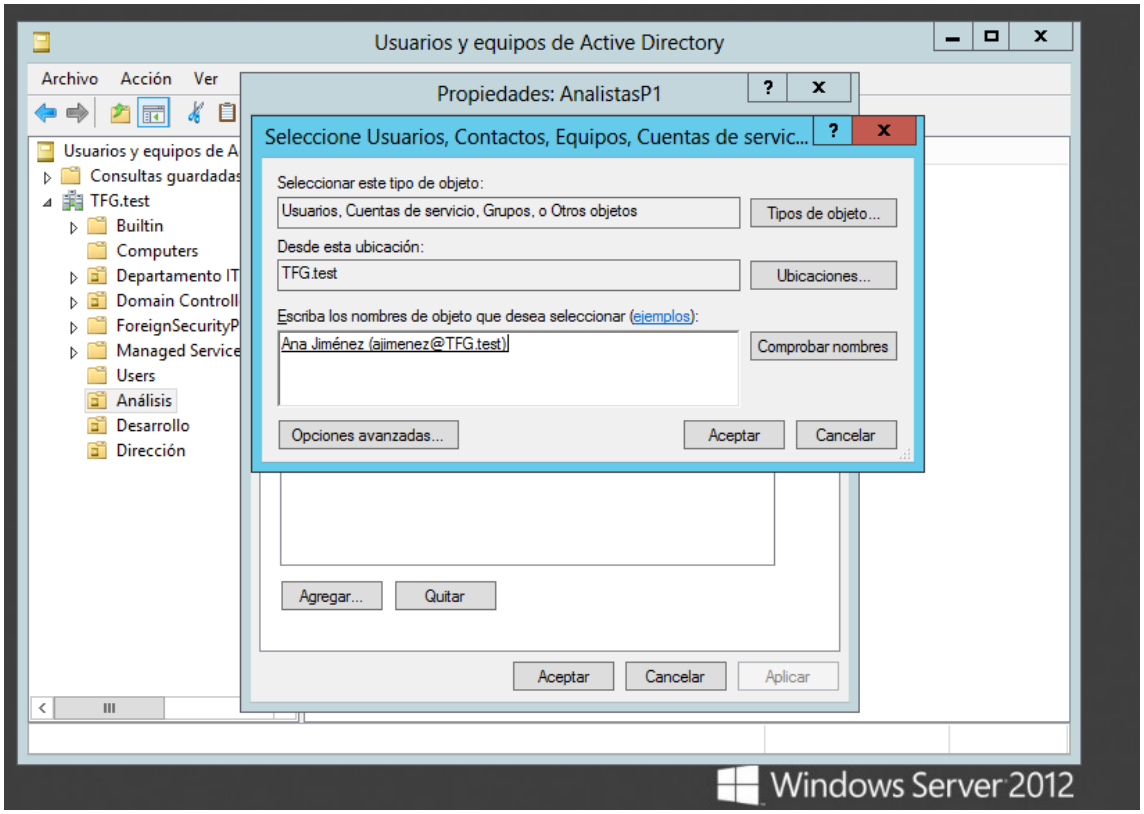


*Figura 75: Añadir usuarios al grupo*

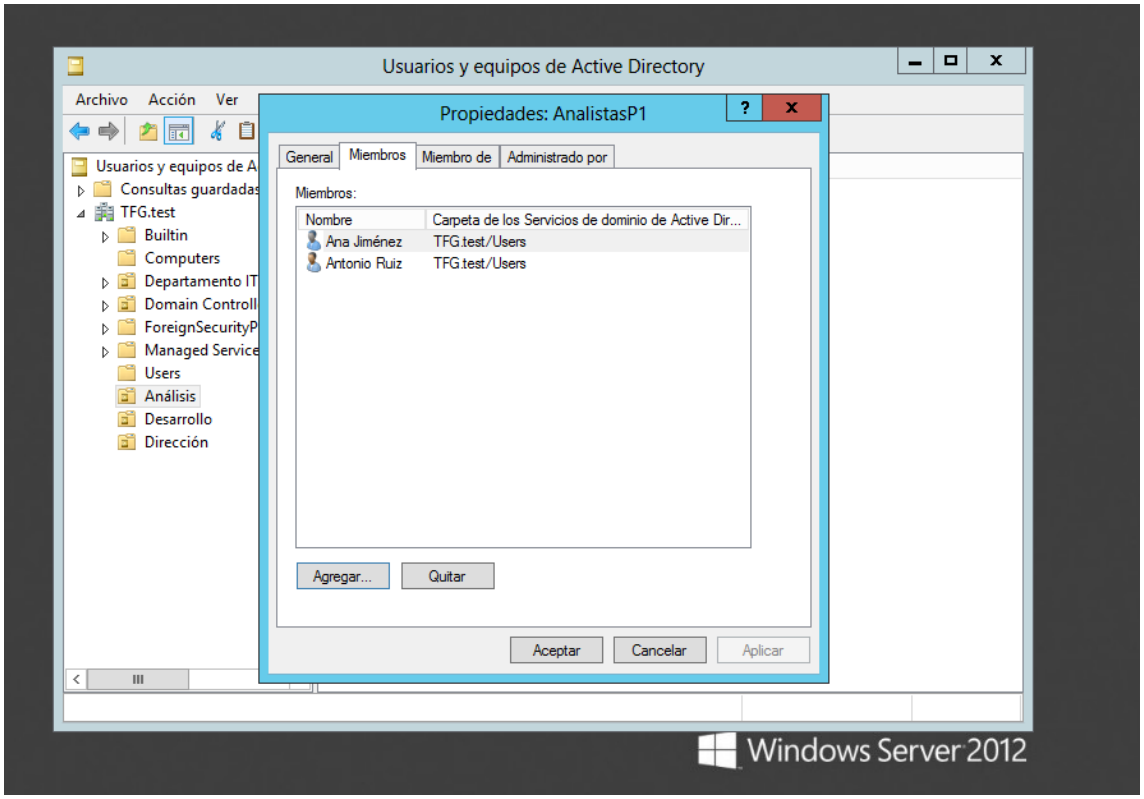


*Figura 76: Usuarios del grupo*

Así pues la distribución de usuarios y grupos es la siguiente:

| Proyecto1 | | | Proyecto2 | | |
|---|---|---|---|---|---|
| Analistas | Desarrolladores | Manager | Analistas | Desarrolladores | Manager |
| Ana Jiménez | Daniel Martínez | Marta Fernández | Antonio Ruiz | Damaris López | Marta Fernández |
| Antonio Ruiz | Damaris López | | Amparo Suárez | David Pérez | |

Además de estas unidades organizativas, vamos a crear un tercera, llamada Departamento TI al que añadiremos como equipo SERVIDOR2 y en el que crearemos algunas carpetas compartidas, haciendo así que actúe como servidor de archivos, y para ello, primero debemos crear estas carpetas en el disco duro del servidor.

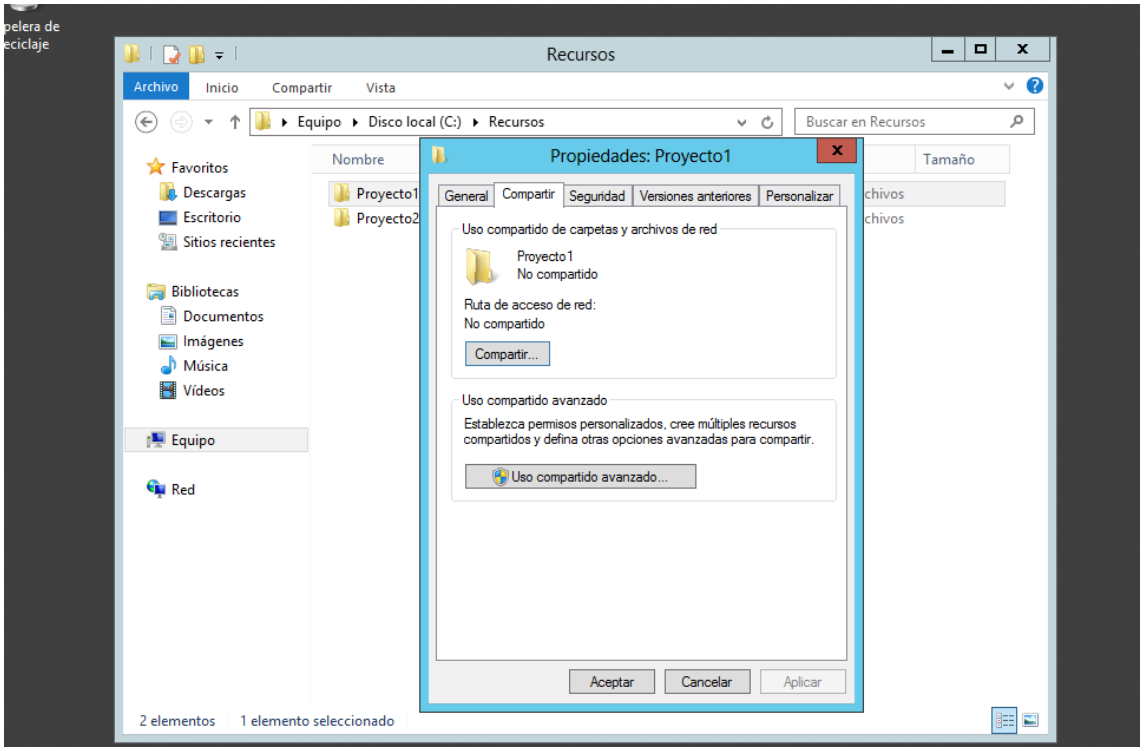


*Figura 77: Compartir Proyecto1*

Una vez creadas las carpetas, debemos establecer con quien se comparten y con qué permisos. Pulsado con el botón secundario del ratón sobre la carpeta Proyecto 1 y seleccionando Propiedades, se abre una nueva ventana, nos dirigimos a la pestaña compartir y abrimos “Uso compartido avanzado”, abriéndose una nueva ventana donde podemos ver y agregar usuarios y grupos de usuario y darles distintos permisos sobre la carpeta. De forma predeterminada, en el momento de compartir la carpeta nos deja que todos los usuarios tengan permisos de lectura y que el Administrador tenga permisos de Control total, además de estos permisos por defecto, añadimos que los Analistas, Desarrolladores y Managers de P1 tengan también Control Total, al igual que el Administrador. Todo este proceso se puede observar en las siguientes figuras.

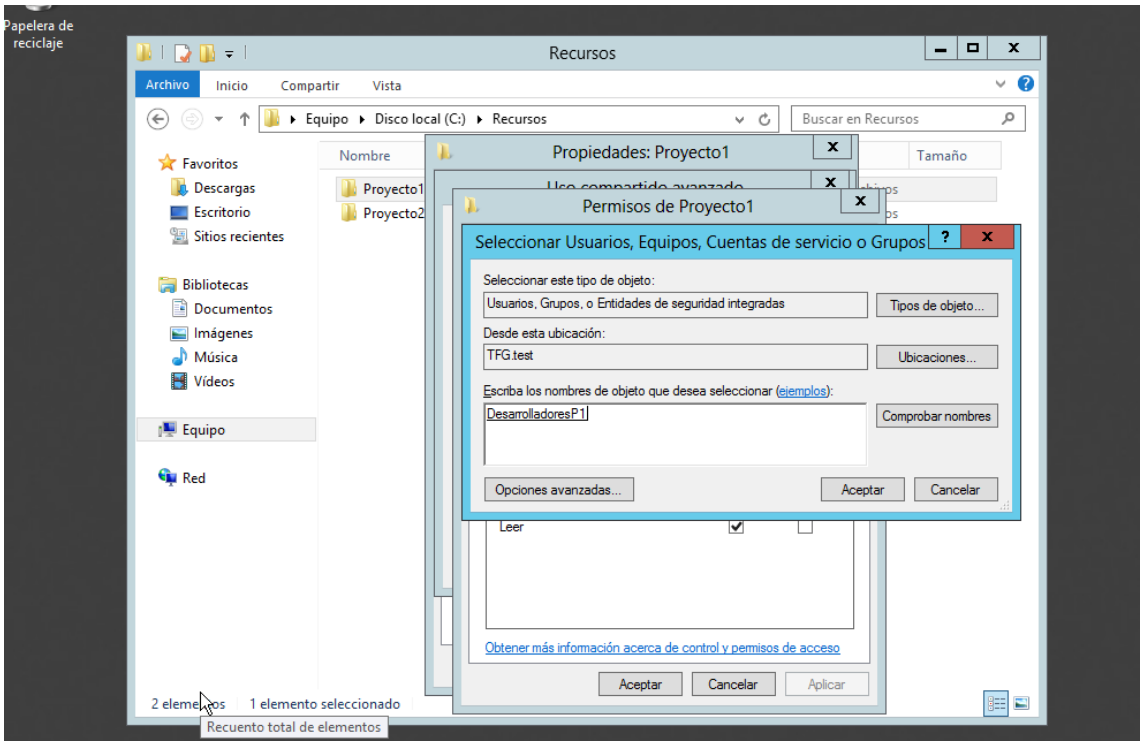


*Figura 78: Asignación de grupos*

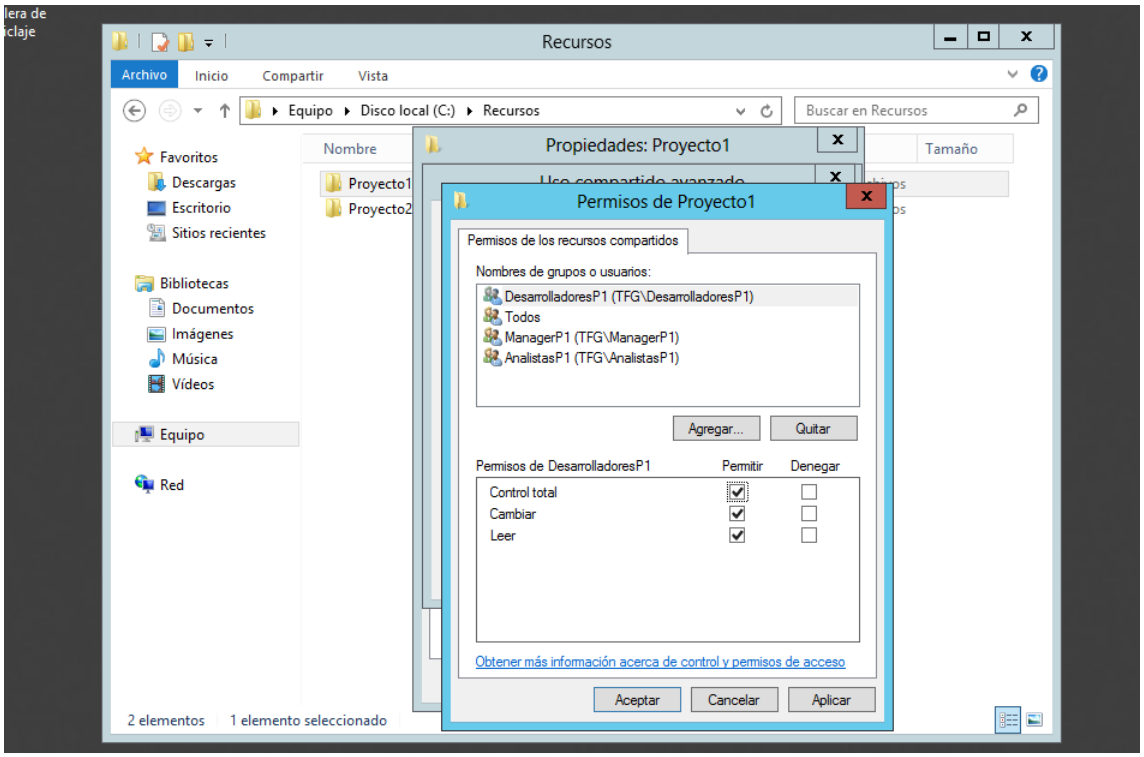


*Figura 79: Asignación de permisos sobre la carpeta*

A continuación repetimos la misma acción con la carpeta Proyecto2 y, hecho esto, volvemos a la unidad organizativa Departamento TI, donde creamos las

carpetas compartidas Proyecto1 y Proyecto2 y les asignamos las rutas de las carpetas que hemos creado en SERVIDOR2.

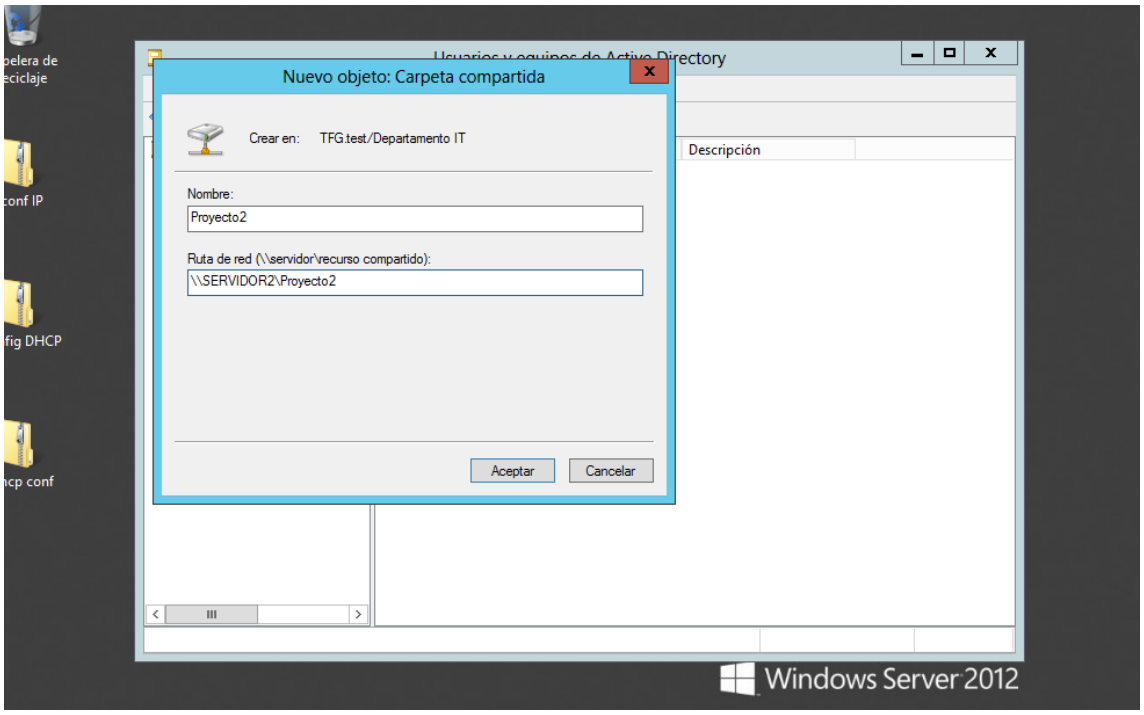


*Figura 80: Adición de la carpeta compartida a la unidad organizativa*

Además en la unidad organizativa Análisis se ha añadido el ordenador EQUIPO1-PC y en Desarrolladores el ordenador EQUIPO2-PC.

# 4. Directivas de grupo

Según la web de Microsoft, las directivas de grupo son infraestructuras que permiten especificar configuraciones administradas para los usuarios y equipos a través de la configuración de directiva de grupo y las preferencias de directiva de grupo en un entorno de servicios de dominio de Active Directory a través de la consola de administración de directivas de grupo.

Las configuraciones se encuentran en los objetos de directiva de grupo, que se vinculan con los siguientes contenedores de servicio de directorio de Active Directory: sitios, dominios y unidades organizativas. Luego, los destinos afectados evalúan las configuraciones dentro de las GPO.

Los Grup Policy Objects (GPOs) son objetos de Active Directory que contienen políticas de usuario y de ordenador. Como ya se ha explicado antes, cada GPO se configura y vincula a un contenedor, que en nuestro caso será unidades organizativas. Cada ordenador dentro de la unidad organizativa recibirá las políticas de ordenador del GPO en el momento del arranque del ordenador y cada usuario recibirá las políticas de usuario del GPO cuando inicie sesión en alguno de los equipos.

# 4.1 Conceptos generales

Todos los GPOs contienen el mismo número de políticas, que superan las 2600, no se pueden añadir o borrar políticas de un GPO. Existen dos GPOs por defecto en todo dominio que no deben ser modificadas ni borradas, Default Domain Policy, o Política de Dominio por defecto, y Default Domain Controllers Policy, o Política por Defecto de los Controladores de Dominio.

La Default Domain Policy está vinculada al objeto raíz del dominio y configura algunas políticas de ordenador que se aplicarán a todos los equipos del dominio, como por ejemplo la política de contraseñas.

La Default Domain Controller Policy está vinculada a la unidad organizativa Domain Controllers y configura algunas políticas de ordenador que se aplicarán a todos los Domain Controllers (controladores de dominio) del dominio en cuestión, como por ejemplo, restringir el derecho de inicio de sesión a los grupos Administrators y Operators.

Al crear un nuevo GPO ninguna de sus políticas está configurada, así ninguna es aplicada a ordenadores o usuarios, sino que es el administrador quien debe editar el GPO y configurar las políticas que se requiere aplicar en ordenadores y usuarios.

## 4.1.1 Configuración de ordenador

Se dividen en dos grupos: políticas y preferencias, que a su vez también se dividen en otros grupos más pequeños.

- Políticas
    - Configuración de software: permisos sobre instalación de software.
    - Configuraciones de Windows: scripts de arranque y apagado, políticas de seguridad (políticas de cuentas, derechos de usuario, etc.)
    - Plantillas administrativas: componentes de Windows, configuración del sistema (inicio de sesión, rastreador de sucesos de apagado, etc.)
- Preferencias
    - Configuraciones de Windows: Recursos compartidos, accesos directos, variables de entorno, etc.
    - Configuraciones del panel de control: usuarios y grupos locales, impresoras, opciones de carpetas, etc.

### 4.1.2 Configuración de usuario

Al igual que las configuraciones a nivel de ordenador, las configuraciones de usuario se dividen en dos grupos: políticas y preferencias, que a su vez también se dividen en otros grupos más pequeños.

- Políticas
    - Configuración de software: instalación de software.
    - Configuración de Windows: scripts de inicio y cierre de sesión, redirección de carpetas (documentos, menú de inicio, etc.)
    - Plantillas administrativas: funcionalidad del menú de inicio, barra de tareas, etc., acceso al panel de control, etc.
- Preferencias
    - Configuración de Windows: asignación de unidades, accesos directos, variables de entorno, etc.
    - Configuraciones del panel de control: usuarios y grupos locales, impresoras, opciones de carpetas, etc.

## 4.2 Aplicación de las GPOs

### 4.2.1 Ámbito de aplicación de las GPOs

El ámbito de un GPO es el conjunto de usuarios y ordenadores a los que se aplican las políticas de la GPO y se determina inicialmente cuando un GPO se vincula a un contenedor de Active Directory, por defecto, éstas políticas se aplican a todo usuario y ordenador del contenedor o sub-contenedores. Este ámbito de aplicación puede ser refinado utilizando el filtro de seguridad del GPO, característica por la cual el GPO solo se aplica a los usuarios y ordenadores incluidos en una lista de permisos.

### 4.2.2 Aplicación de las directivas de grupo en el proyecto

Para cada unidad organizativa se ha definido un set distinto de GPOs. En la unidad organizativa Análisis hemos creado la GPO Analistas, y en la unidad organizativa Desarrollo, hemos creado la GPO desarrolladores.

A la hora de aplicar las directivas definidas en las GPOs hay algunas consideraciones a tener en cuenta.

Los ordenadores reciben las políticas de ordenador configuradas, los usuarios reciben las políticas de usuario configuradas y los sub-contenedores heredan el GPO completo. Además, el resto de objetos, como los grupos de usuario, no son afectados, por ello es necesario tener los usuarios dentro de la unidad organizativa, ya que si están simplemente dentro de los grupos de usuario, las políticas no les afectarían.

Finalmente, la relación entre contenedores y GPOs es muchos a muchos, es decir, un contenedor puede tener varios GPOs vinculados, y un GPO puede estar vinculado a varios contenedores, de aquí se concluye que las políticas son acumulables y heredables.

Una vez explicadas éstas consideraciones, ya podemos explicar las GPOs que hemos aplicado y cómo las hemos aplicado.

### *4.2.2.1 Configuración de escritorio*

En la GPO Análisis hemos dado de alta las siguientes directivas:

Directivas de equipo:

- No permitir que los usuarios cambien el color de las ventanas (habilitada).

Directivas de usuario:

- Prohibir el acceso a Configuración de PC y a Panel de Control (habilitada).
- Impedir el acceso a símbolo de sistema (habilitada).

Para poder aplicar éstas directivas, basta con dirigirse a la consola de Administración de directivas de grupo y dentro de nuestro bosque, seleccionar el dominio y la unidad organizativa a la que queramos aplicar las GPOs.

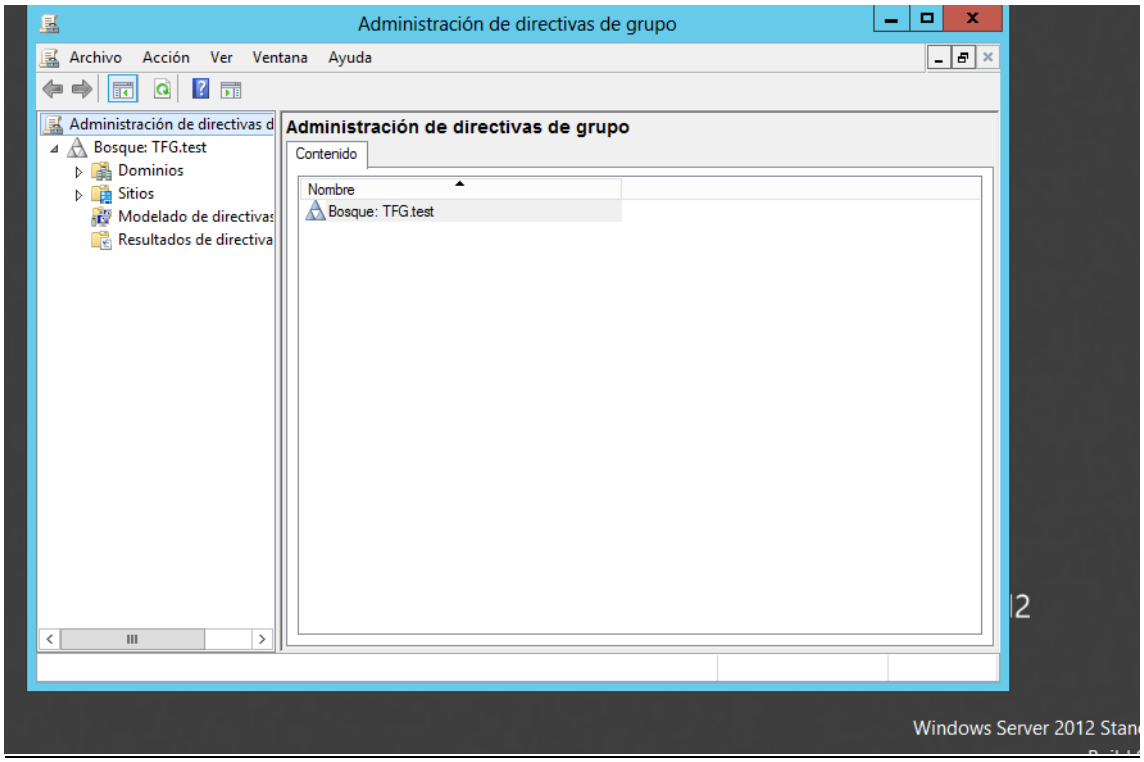


*Figura 81: Administración de directivas de grupo*

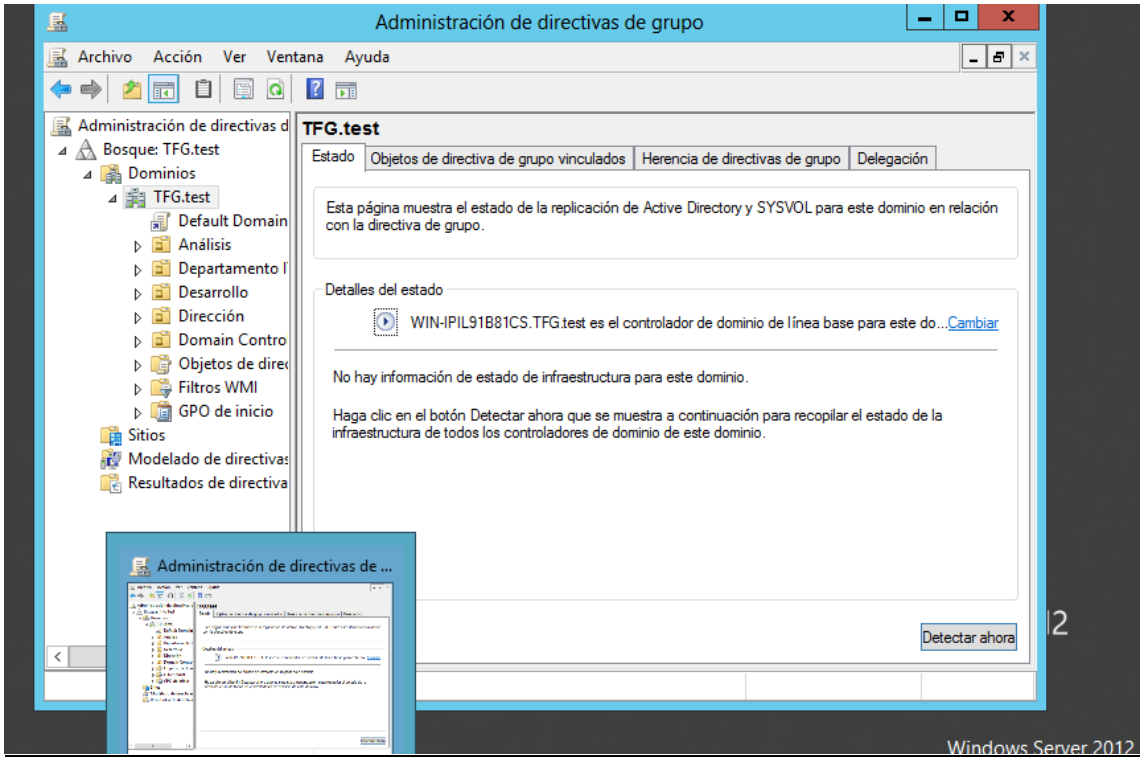


*Figura 82: Vista general GPOs del dominio*

Las GPOs se pueden crear de dos formas, la primera, es crear la GPO en el dominio y después vincularla a la GPO, y la segunda, que es por la que hemos optado para la unidad organizativa Análisis, consiste en crearla ya vinculada a la unidad organizativa. Para ello, haremos clic con el botón secundario del ratón sobre la unidad organizativa Análisis y escogeremos la opción “Crear un GPO en este dominio y vincularlo aquí…”. Tras elegir esta opción se abre una nueva ventana (Figura 83) en la que podemos dar nombre a nuestra GPO y asignarle un GPO de inicio si tuviéramos alguna.

Una vez creada la GPO, podemos asignarle a ésta ciertos filtros de aplicación. Por defecto en los filtros aparece el grupo Usuarios autentificados, además de este grupo hemos añadido también los grupos AnalistasP1 y AnalistasP2, y también el EQUIPO1, como se puede observar en la Figura 84.

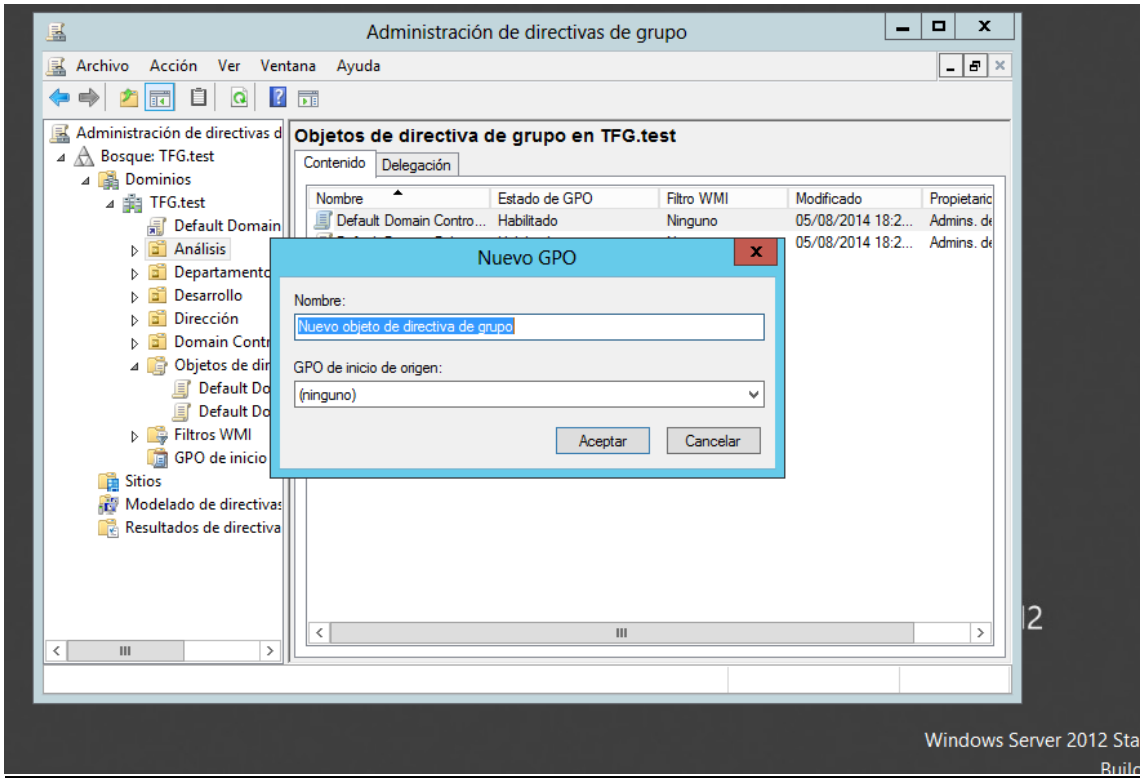


*Figura 83: Creación de la GPO Analistas*

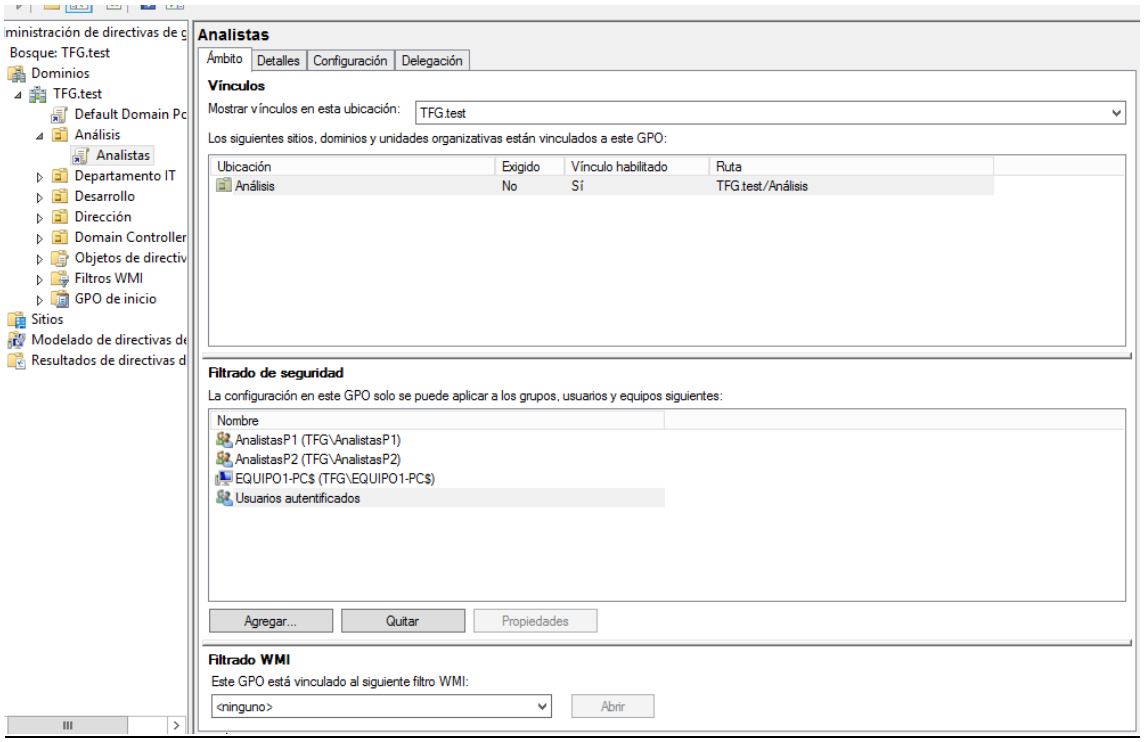


*Figura 84: Filtros de la GPO Analistas*

Una vez configurados los filtros, ya podemos editar la GPO y configurar las directivas que queremos aplicar. Haciendo clic derecho sobre la GPO, se abre un menú en el que seleccionaremos la opción “Editar” (Figura 85).

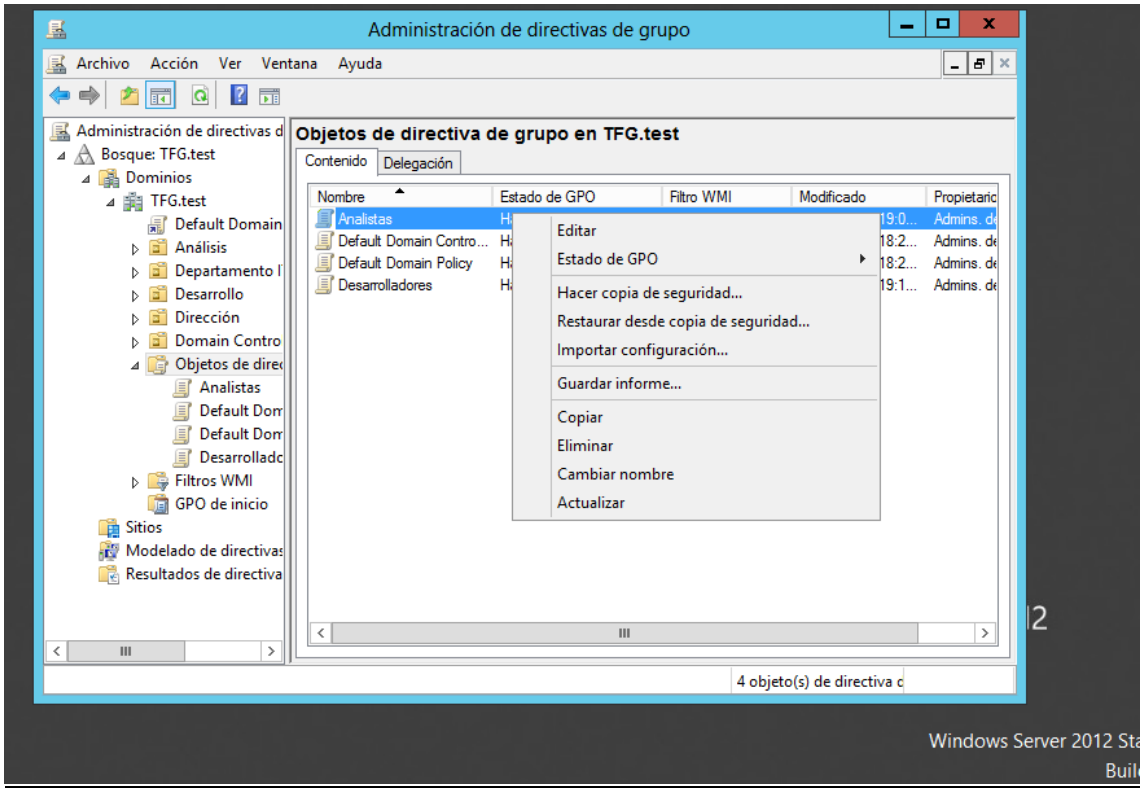


*Figura 85: Menú de la GPO*

Tras pulsar la opción "Editar", se abre una nueva ventana en la que aparecen las distintas configuraciones que podemos aplicar, equipo y usuario.

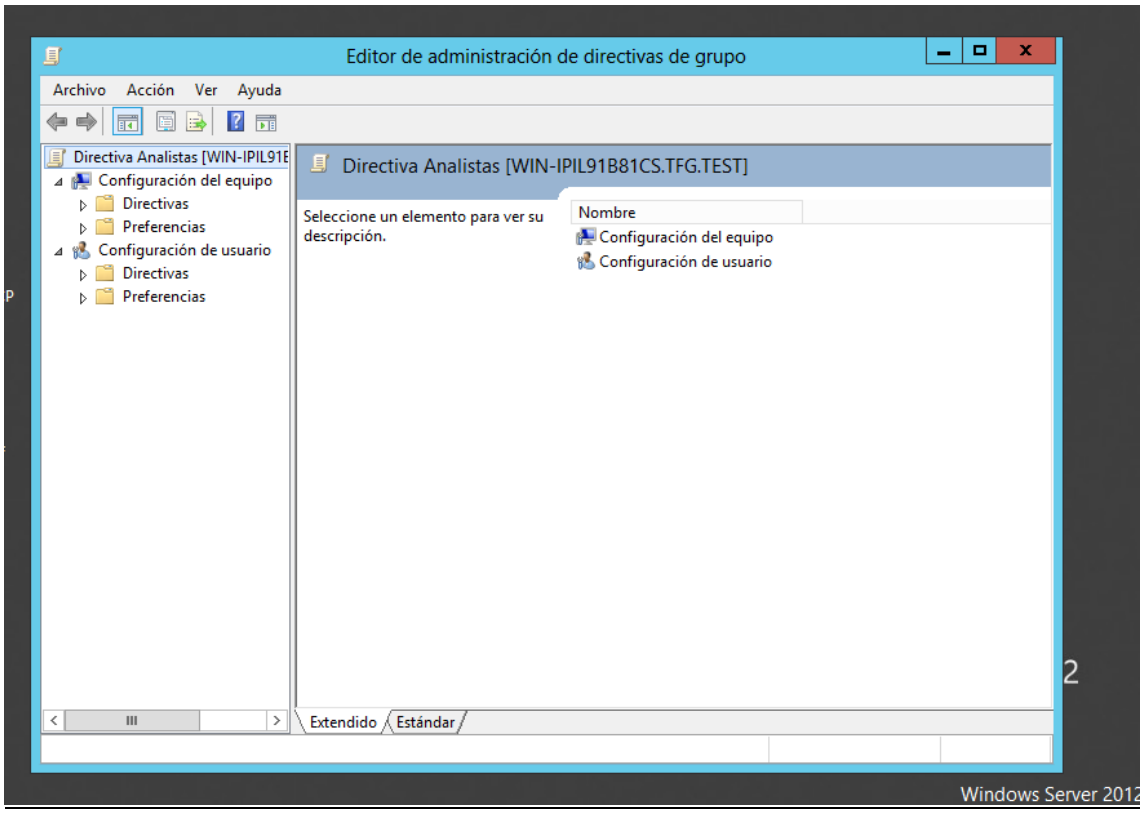


*Figura 86: Menú de edición de la GPO*

Para configurar directivas en la GPO, basta con buscar la directiva que nos interese en el árbol de directivas y hacer doble clic sobre ella, lo que hará que se abra una nueva ventana en la que podremos editar su estado. Por defecto todas las directivas están como “No configurada” y en esta ventana podremos cambiar el estado a “Habilitada” o a “Deshabilitada”. En la Figura 87 se muestra la configuración de la directiva “No permitir cambios de color”. Hemos accedido a ésta directiva desde “Configuración de equipo” -> “Directivas” -> ”Plantillas administrativas” -> “Componentes de Windows” -> “Administrador de ventanas de escritorio”->”Color del marco de las ventanas”.

Al habilitar ésta directiva, ningún usuario que se conecte al EQUIPO1 podrá cambiar el color de las ventanas.

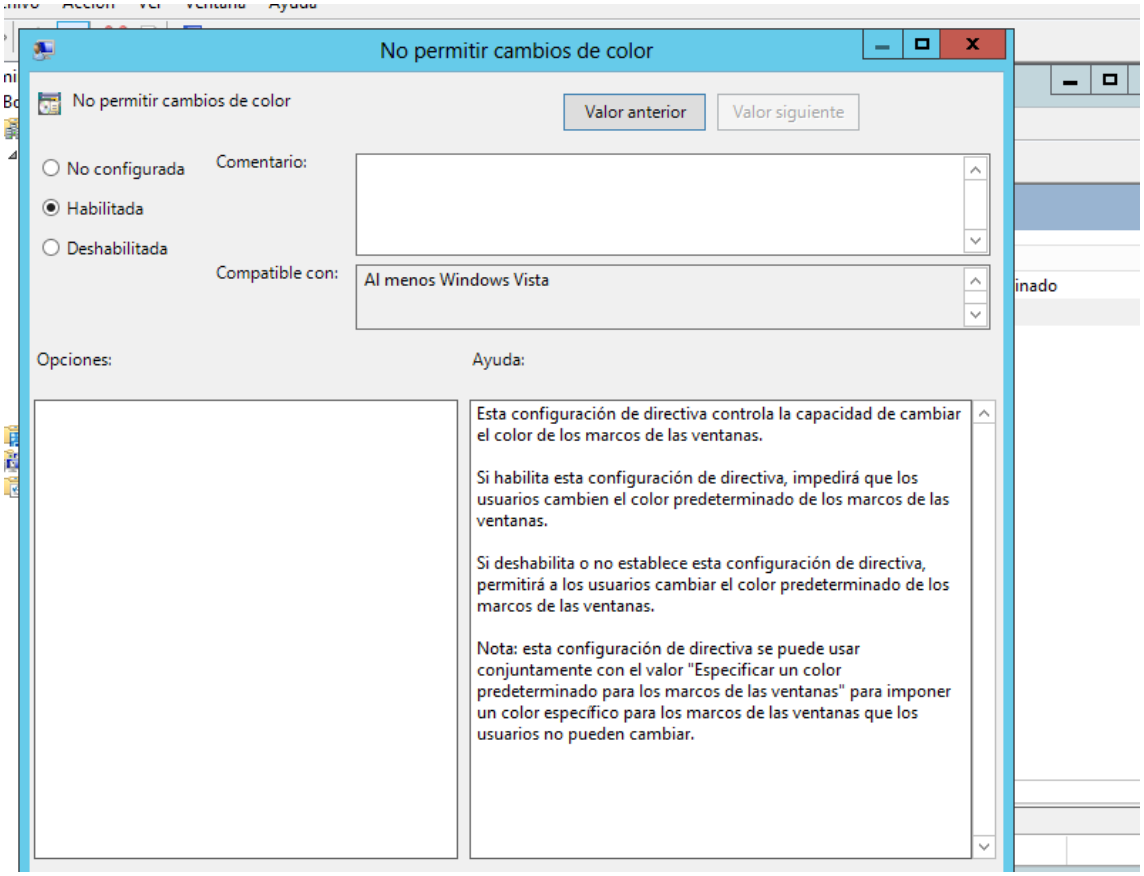


*Figura 87: Prohibir cambiar los colores de ventanas de escritorio*

Lo mismo ocurre con las directivas de usuario, para alcanzar la directiva “Impedir acceso al símbolo del sistema” hemos seguido el siguiente camino:

“Configuración del usuario” -> “Directivas” -> “Plantillas administrativas” -> “Sistema”.

Para la directiva de Panel de control se han seguido los mismos pasos hasta “Plantillas administrativas” donde en lugar de acceder a la carpeta “Sistema”, hemos accedido a la carpeta “Panel de Control”.

Las directivas de usuario se aplicarán durante el inicio de sesión, así pues, estos usuarios no podrán acceder al símbolo del sistema ni al panel de control en

ninguno de los ordenadores de la compañía. En las figuras 88 y 89 se puede ver la configuración de ambas directivas.

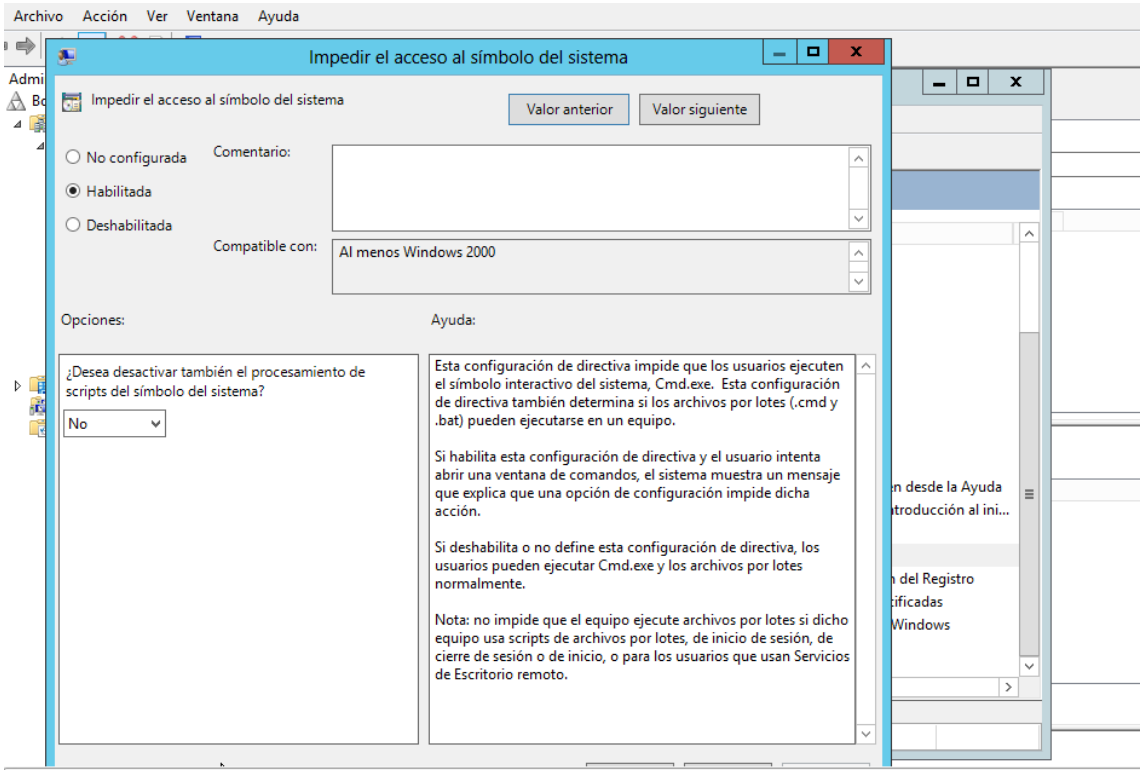


*Figura 88: Impedir acceso al símbolo del sistema*

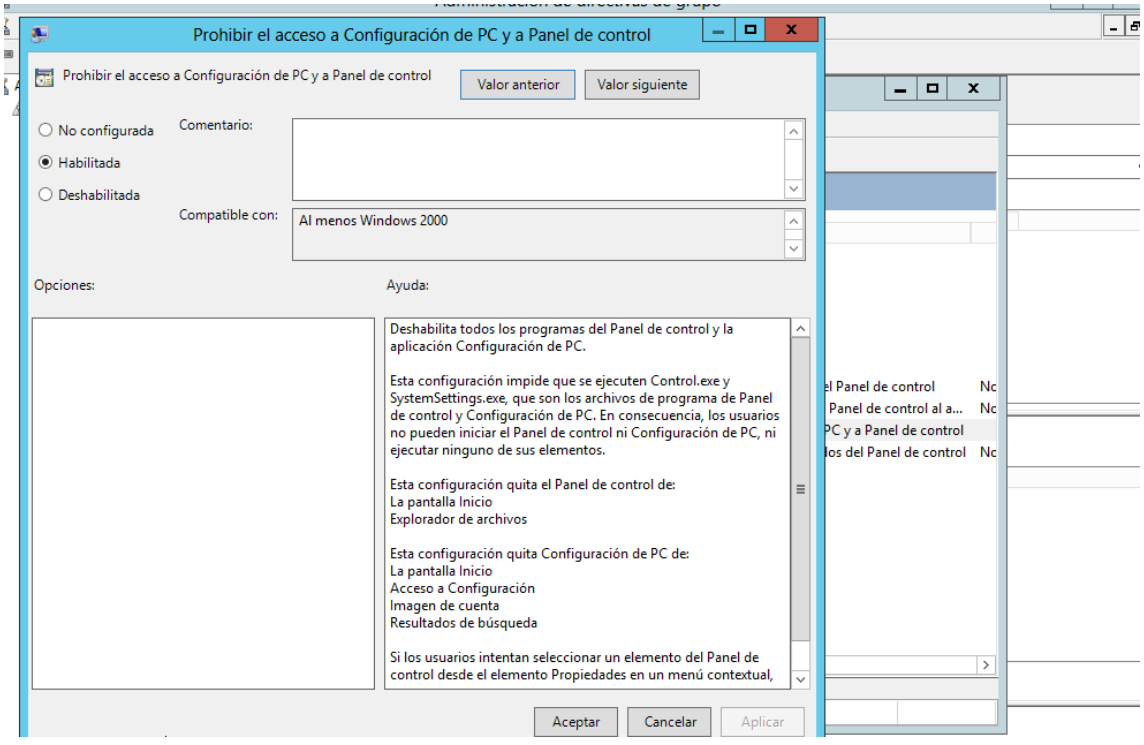


*Figura 89: Prohibir el acceso a Configuración del PC y a Panel de Control*

Las GPOs pueden tardar en actualizarse unos 90 minutos, pero en el caso de necesitar realizar pruebas rápidamente para asegurarse de que la configuración aplicada es la deseada y funciona correctamente, se puede utilizar el comando de consola gpupdate o gpudate/force, que hará que las directivas de grupo se actualicen inmediatamente. Este proceso se puede realizar abriendo la consola y escribiendo gpupdate en ella, no es necesario hacerlo desde la consola del Administrador, ya que los grupos AnalistasP1 y AnalistasP2 tienen permisos de lectura y aplicación sobre la GPO, pero para asegurarnos de que no falla nada es preferible hacerlo desde ésta.

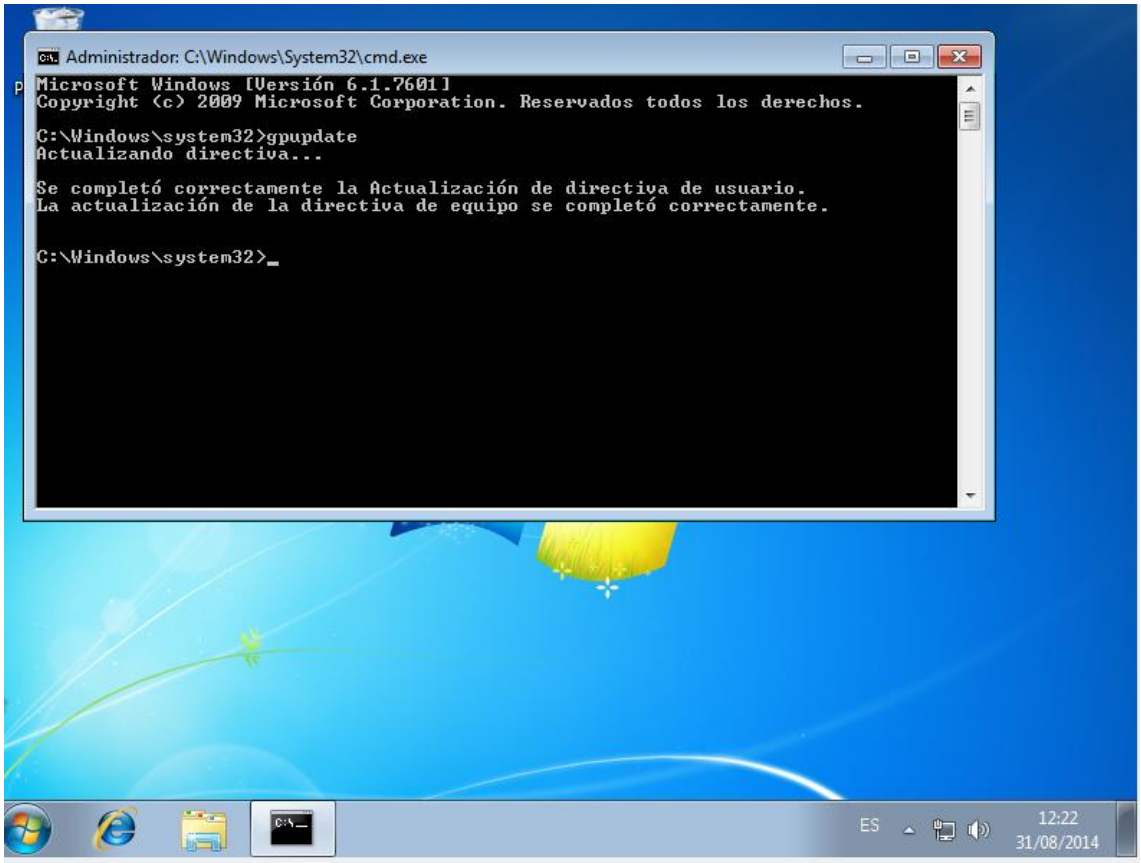


*Figura 90: Comando gpupdate*

En la siguiente captura se puede ver un resumen de las directivas aplicadas, al cual se accede pulsando sobre la GPO y dirigiéndose a la pestaña Configuración.

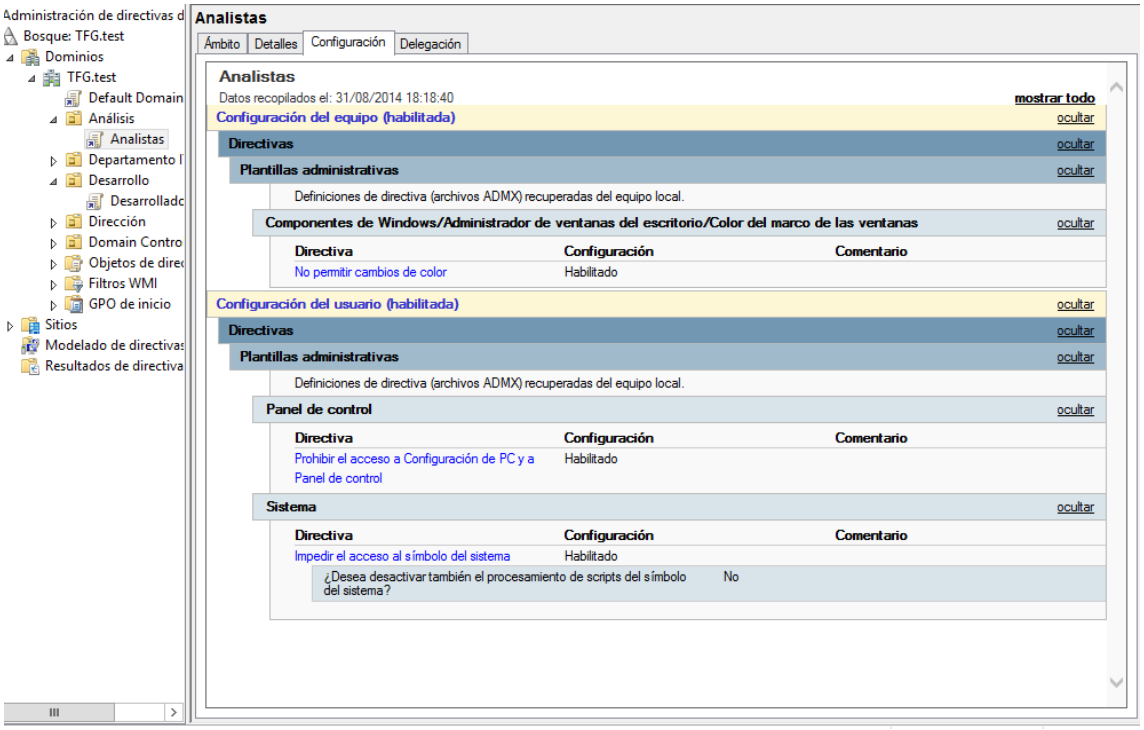


*Figura 91: Resumen de aplicación de las directivas*

Una vez las directivas han sido aplicadas, ya podemos probarlas, como se observa en las siguientes figuras, al iniciar sesión con el usuario Ana Jiménez que pertenece a la unidad organizativa Análisis, no se puede acceder al símbolo del sistema ni al Panel de Control, además de que no se puede cambiar la personalización del escritorio, sin embargo, al iniciar sesión con un usuario de la unidad organizativa Desarrollo, éstas funcionalidades sí que están activas.

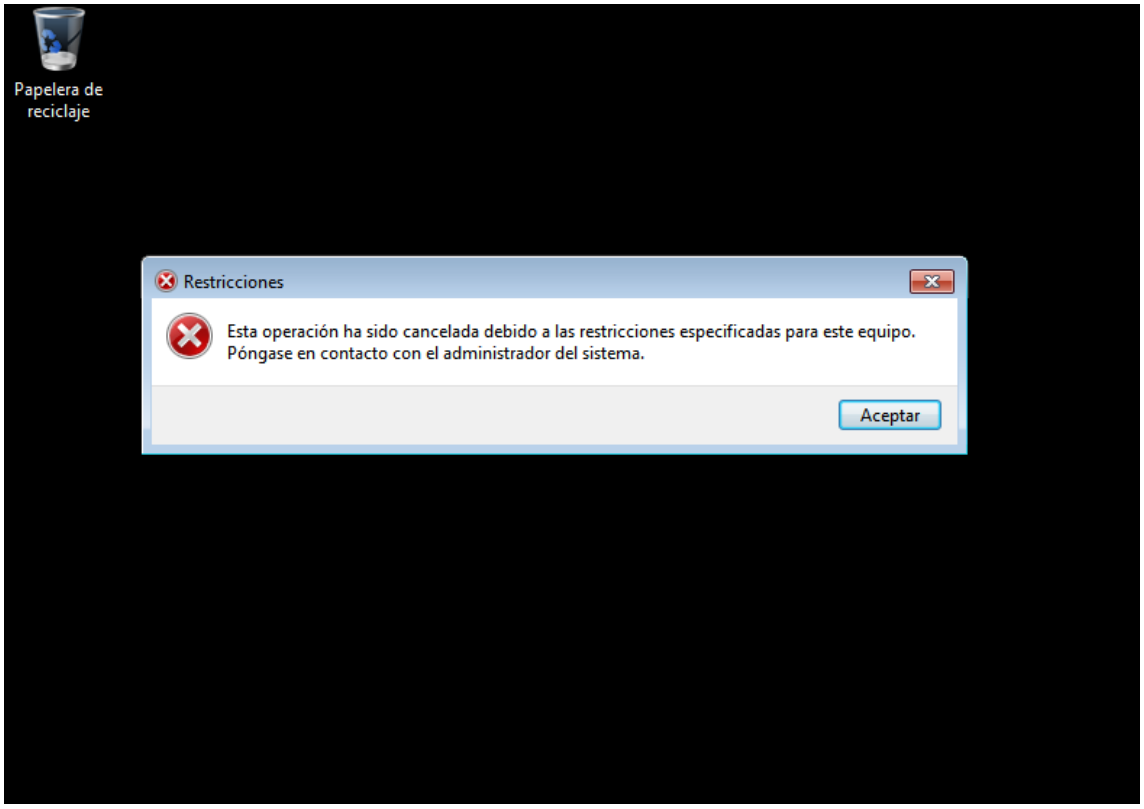


*Figura 92: Menú de personalización deshabilitado*

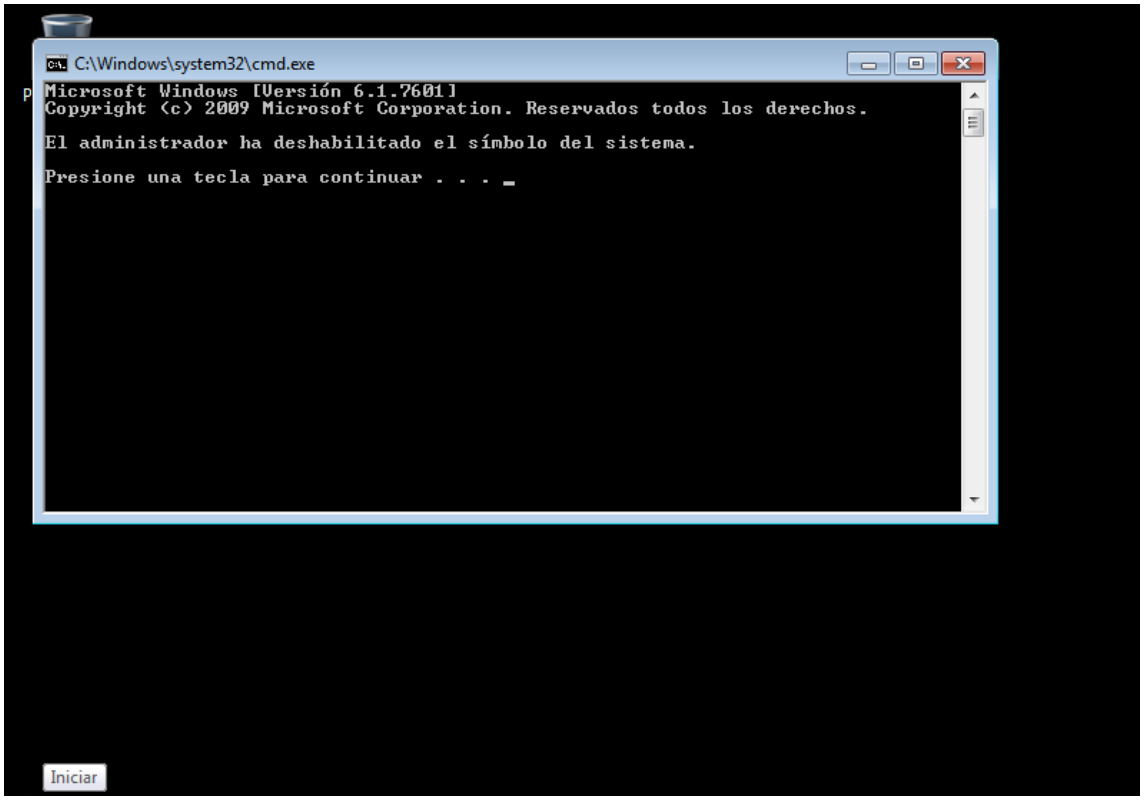


*Figura 93: CMD deshabilitado*

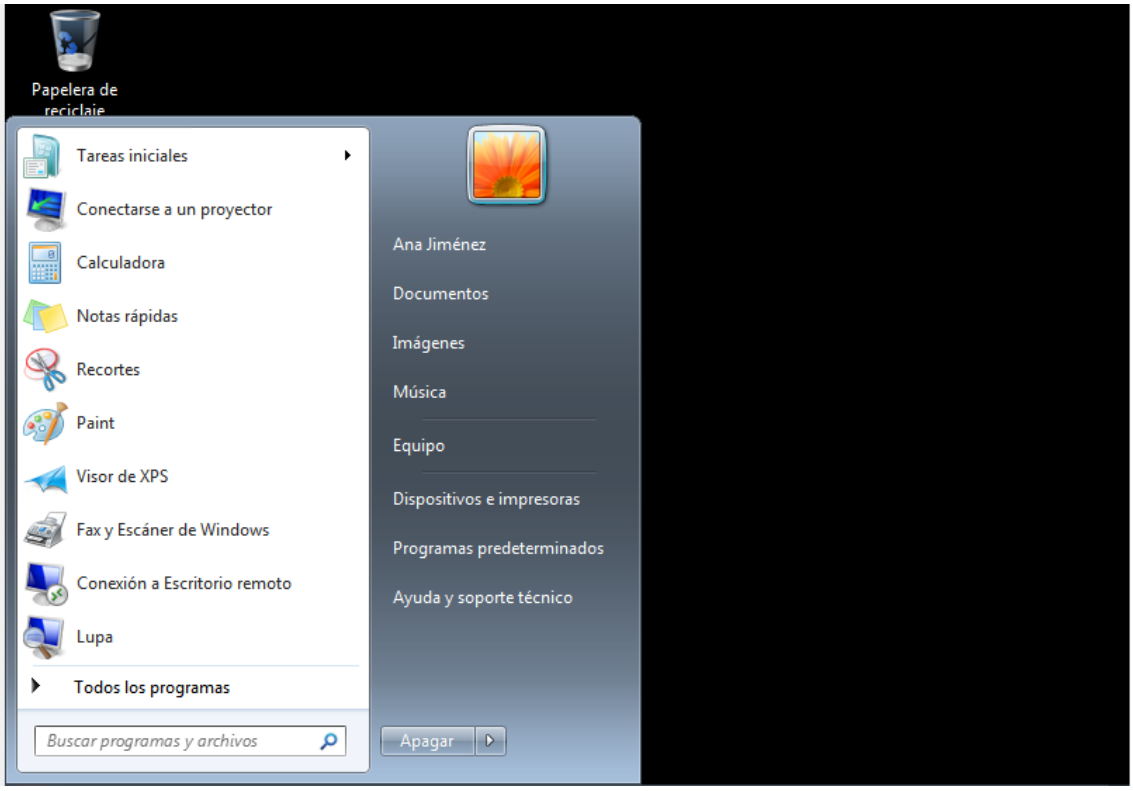


*Figura 94: Panel de Control deshabilitado*

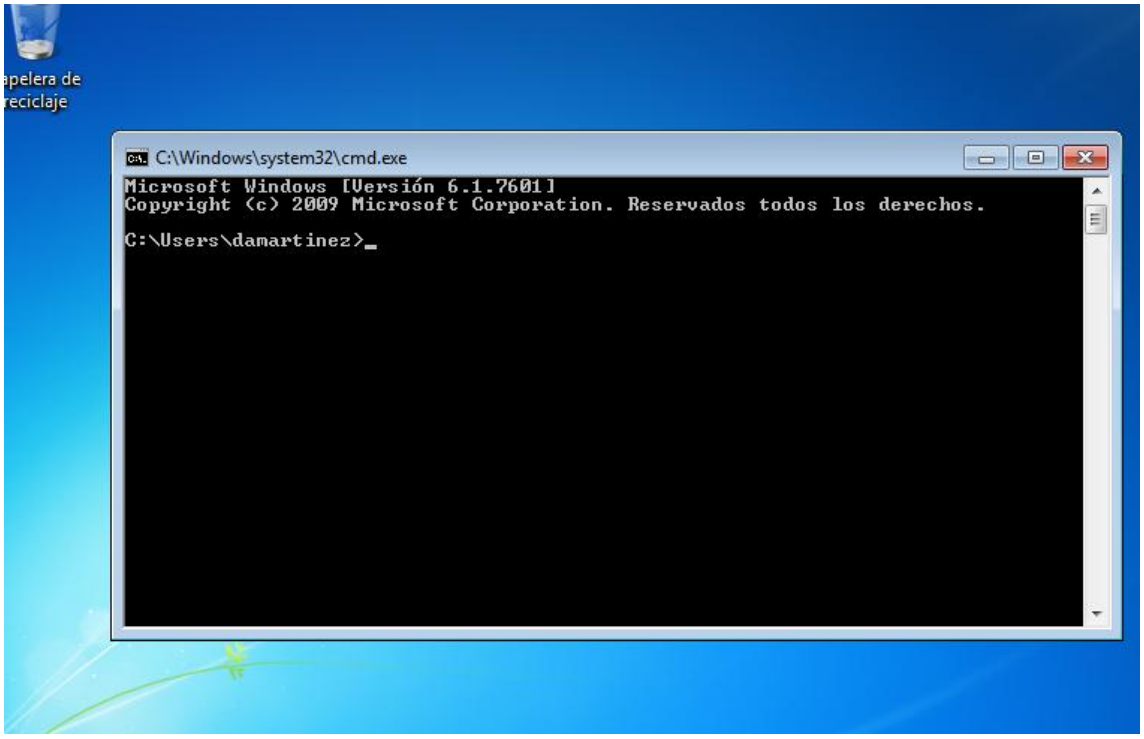


*Figura 95: Acceso con Daniel Martínez al CMD*

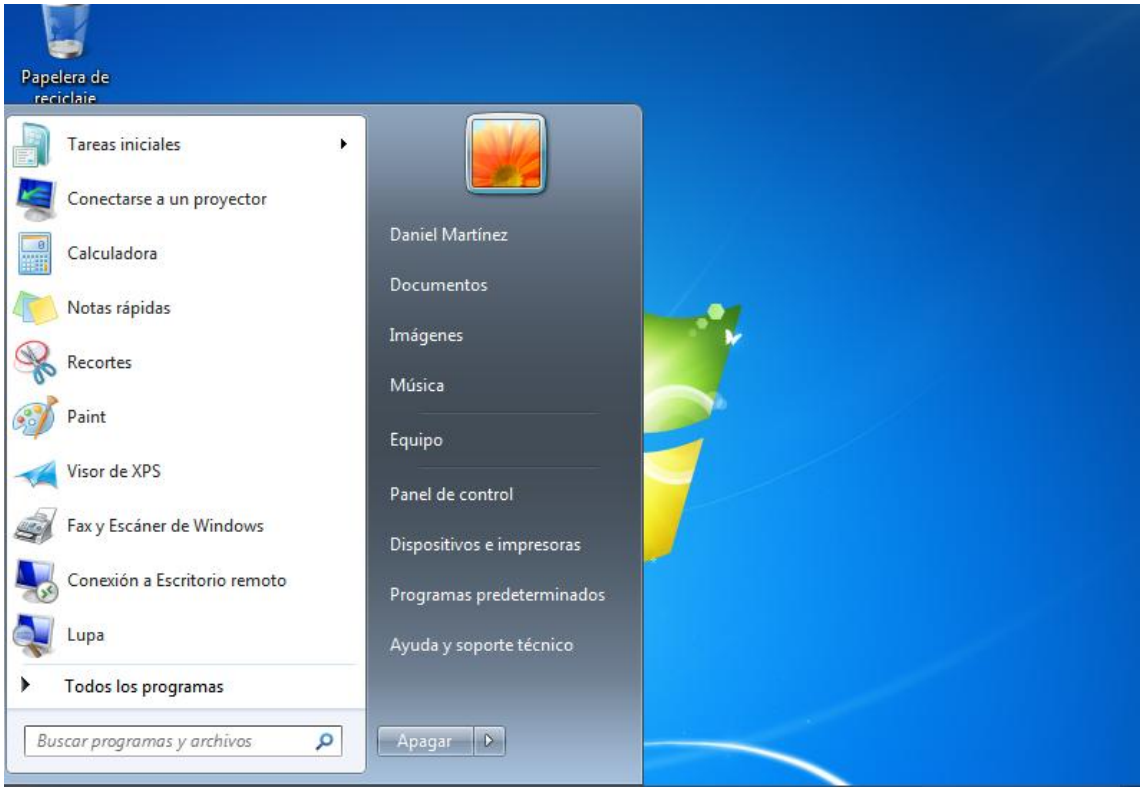


*Figura 96: Acceso al Panel de Control con Daniel Martínez*

En la GPO Desarrollo, que corresponde a la unidad organizativa Desarrolladores, hemos dado de alta las siguientes directivas de grupo:

Directivas de equipo:

- Impedir el acceso al diálogo Eliminar el historial de exploración (Internet Explorer) (habilitada).

Directivas de usuario:

- Tapiz del escritorio (habilitada).
- Quitar el bloqueo de equipos al pulsar Ctrl+Alt+Supr (habilitada).
- Redirección de la carpeta Mis Documentos (habilitada).
- Quitar Conectarse a una unidad de red / Desconectarse de una unidad de red (habilitada).
- Quitar el icono de Ubicación de red del escritorio (habilitada).

Al igual que en el caso anterior, hemos creado la GPO vinculándola directamente a la unidad organizativa y, nuevamente hemos aplicado los filtros correspondientes, que en este caso son: como grupos de usuario DesarrolladoresP1 y DesarrolladoresP2 y como equipo EQUIPO2.

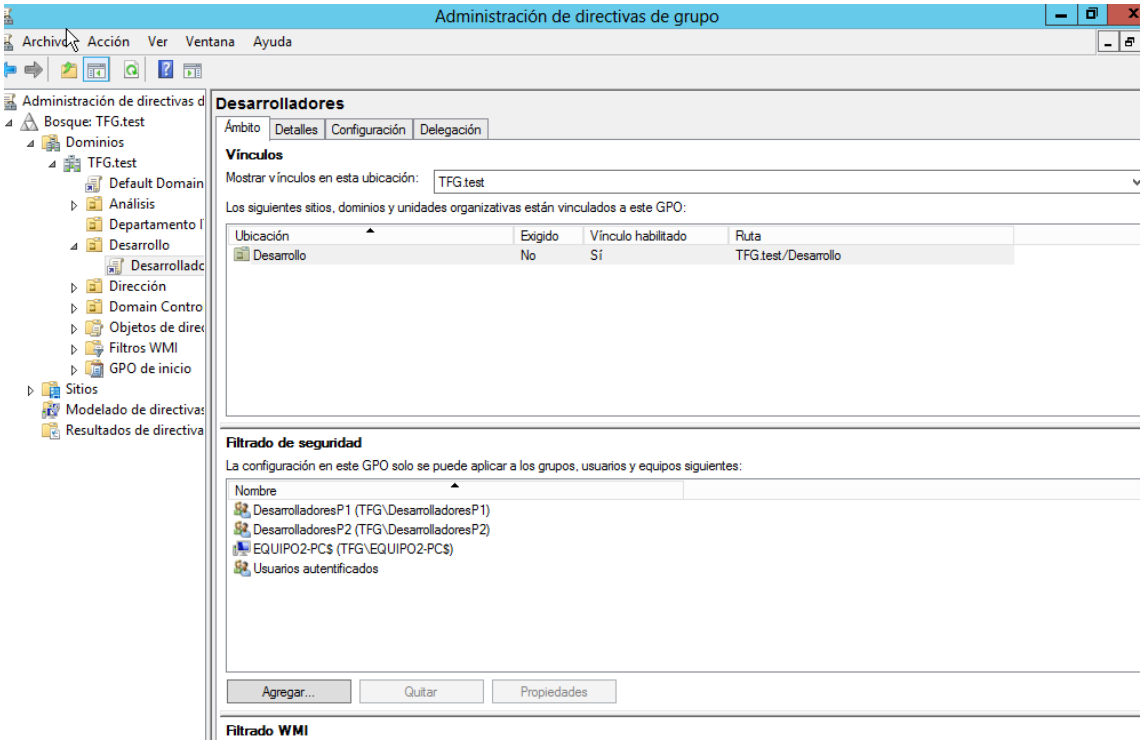


*Figura 97: Filtros de aplicación*

Y, al igual que en la GPO Análisis, para poder configurar las directivas de grupo pulsamos con el botón derecho en la GPO y seleccionamos “Editar” abriéndose la ventana de administración de la GPO donde encontramos el árbol de directivas.

La ruta seguida para configurar la directiva Impedir el acceso a diálogo Eliminar el historial de exploración es la siguiente: “Configuración del equipo” -> “Directivas” -> “Plantillas administrativas” -> “Componentes de Windows” -> “Internet Explorer” -> “Eliminar el historial de exploración”.

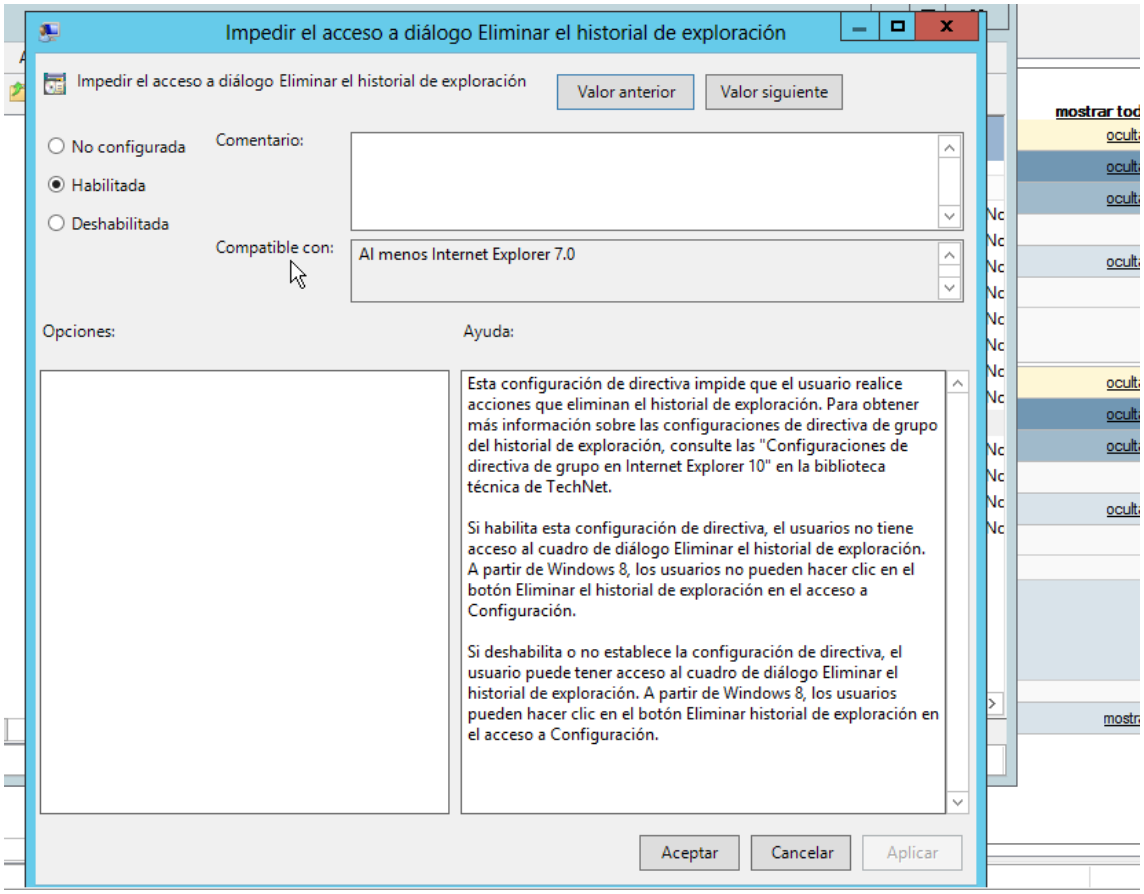


*Figura 98: Impedir eliminar el historial de IE*

Para la siguiente directiva, además de la configuración que podemos observar en la siguiente figura, hemos tenido que seguir un proceso similar al que seguimos al crear las carpetas Proyecto1 y Proyecto2. Primero, hemos creado la carpeta en el disco duro del servidor, y acto seguido la hemos compartido con el grupo "Todos" dándole únicamente permisos de lectura, de esta forma todos los usuarios podrán leer la imagen para así poder utilizarla como fondo de escritorio.

La ruta seguida para poder configurarla ha sido la siguiente: "Configuración del usuario" -> "Directivas" -> "Plantillas administrativas" -> "Active Desktop" -> "Active Desktop".

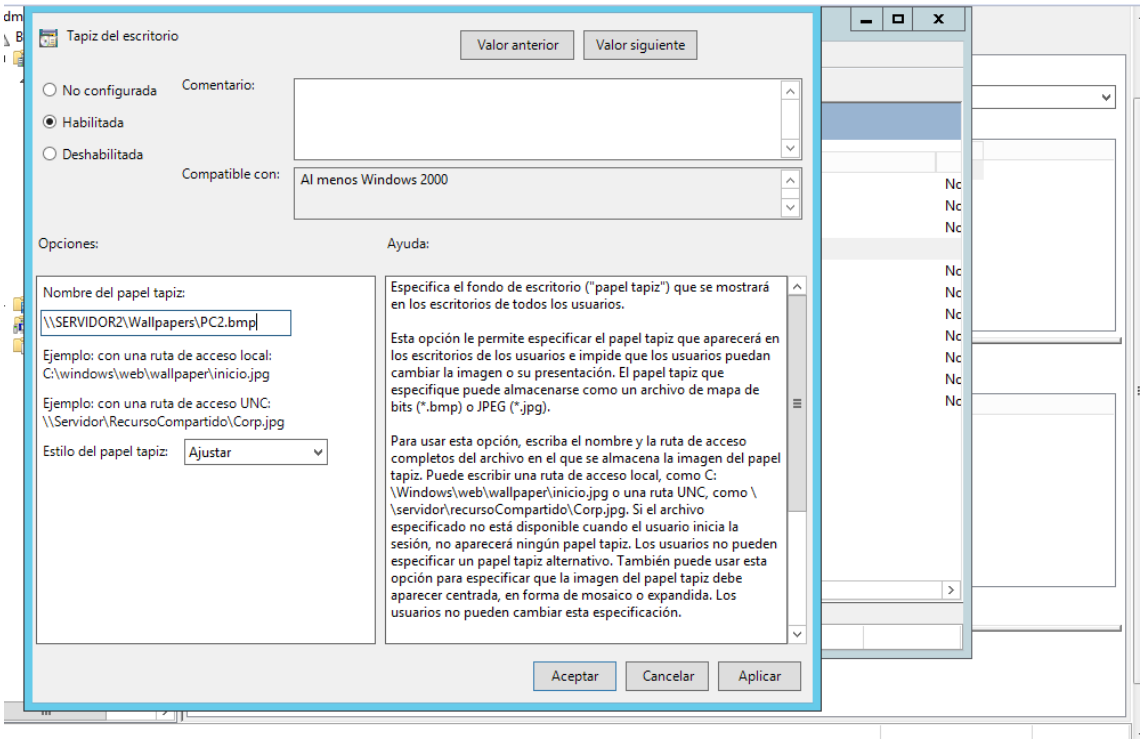


*Figura 99: Directiva Papel Tapiz*

Para configurar la siguiente directiva, hemos seguido la ruta “Configuración de usuario” -> “Directivas” -> “Plantillas administrativas” -> “Active Desktop”.

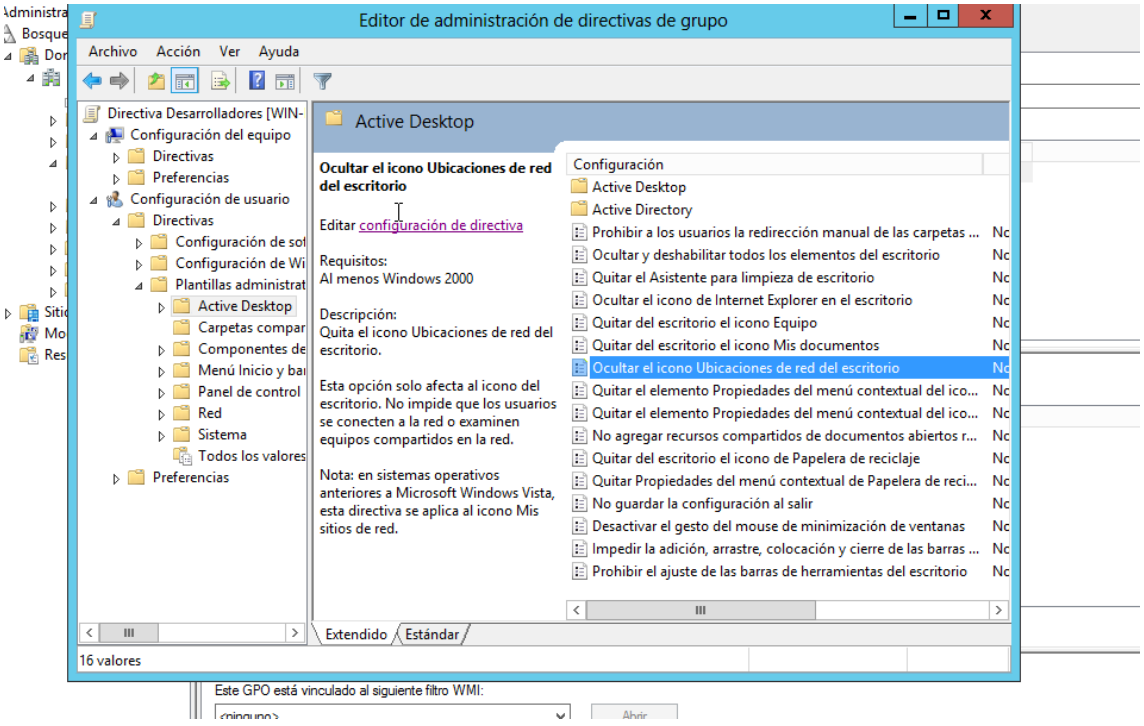


*Figura 100: Quitar icono ubicaciones de red del escritorio*

Para la siguiente directiva, hemos seguido la ruta: “Configuración de usuario” -> “Plantillas administrativas” -> “Componentes de Windows” -> “Explorador de archivos”.

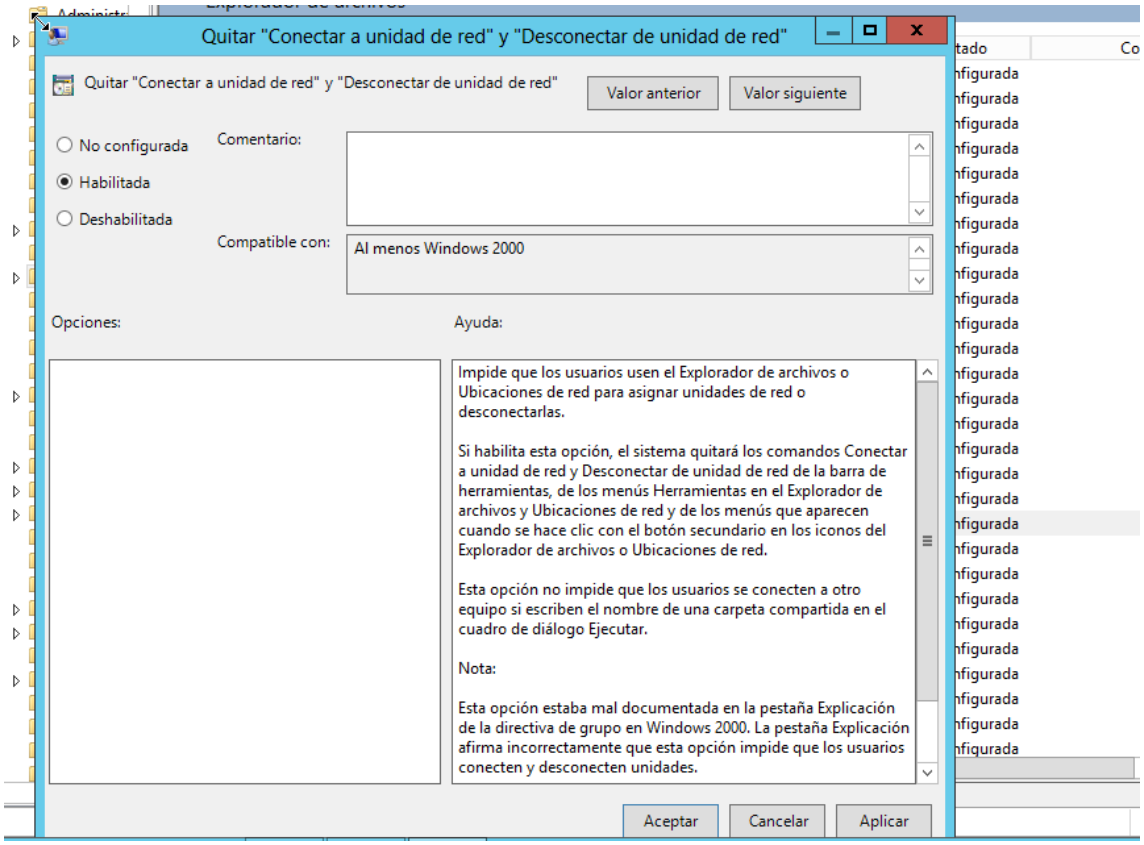


*Figura 101: Quitar "Conectar a unidad de red" y "Desconectar de unidad de red"*

Para la siguiente directiva, es necesario seguir algunos pasos extra. Primero, nos conectamos con cualquiera de los usuarios de OU Desarrollo, y comprobamos la ruta de la carpeta Mis Documentos.

A continuación, en SERVIDOR2 creamos en C: la carpeta Redirect y la compartimos con el grupo Todos con permisos de Control Total.

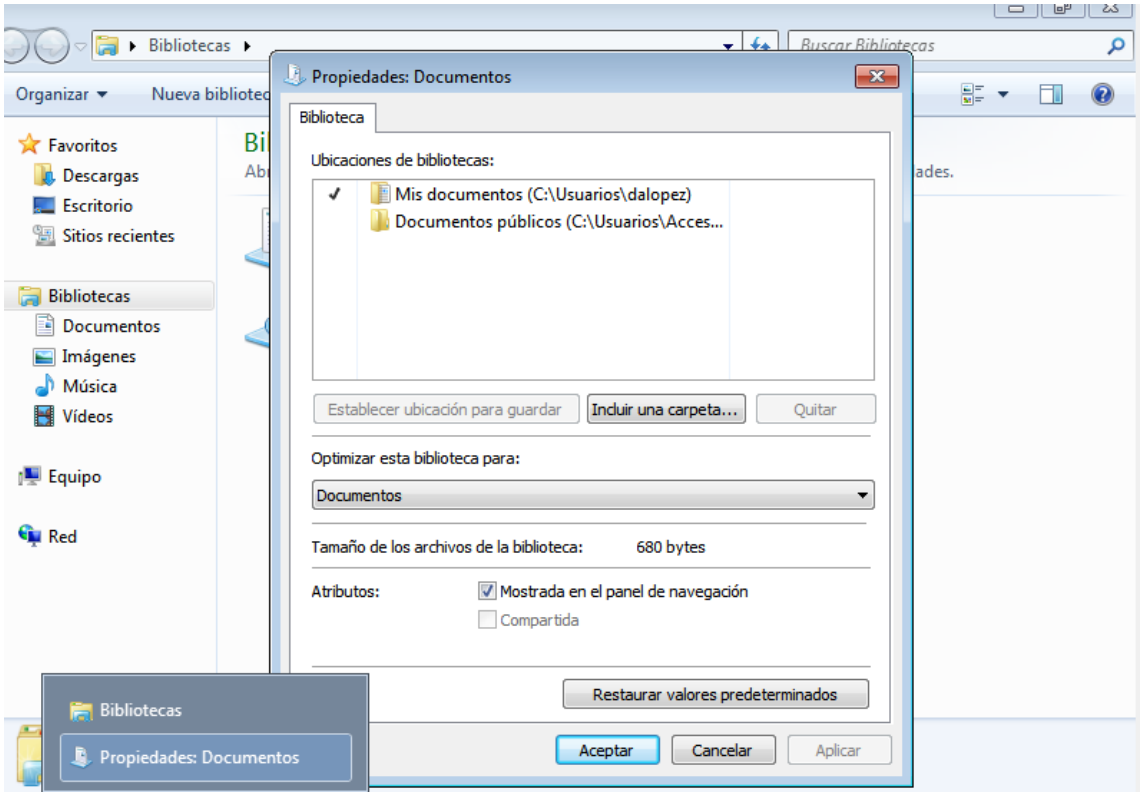


*Figura 102: Comprobación ruta de Mis Documentos*

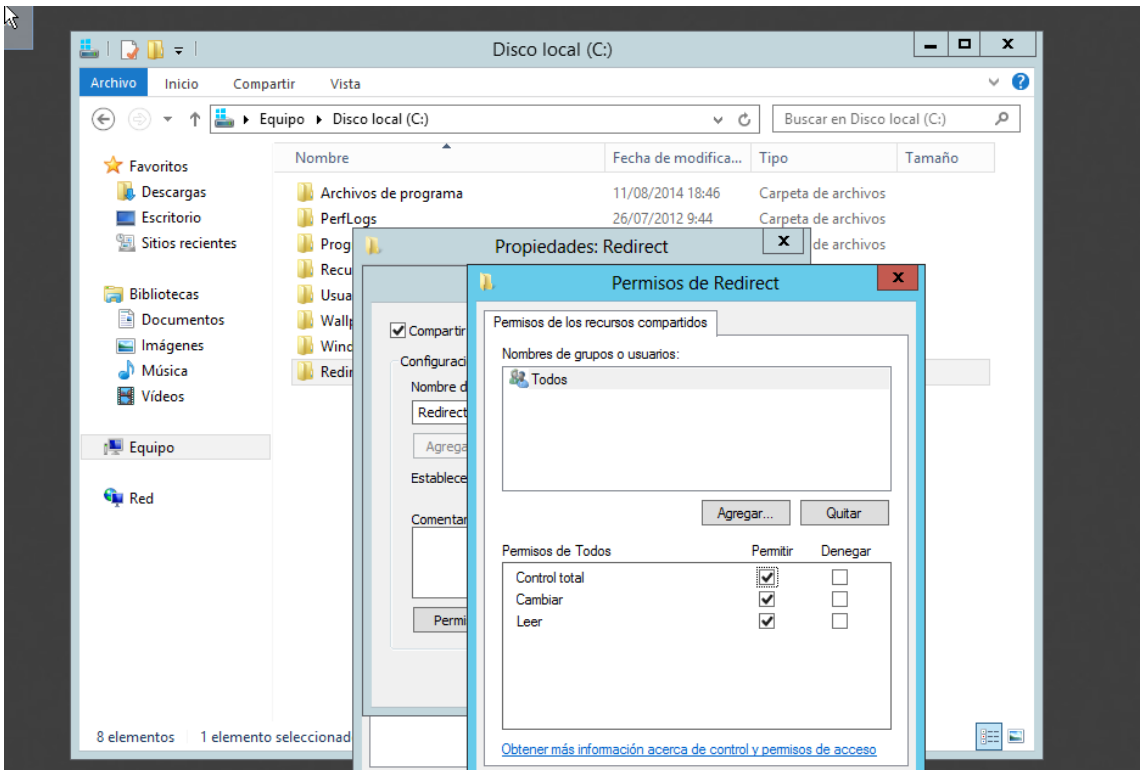


*Figura 103: Crear y compartir carpeta Redirect en SERVIDOR2*

Una vez hechos los pasos anteriores, volvemos a la edición de la GPO y seguimos la siguiente ruta: “Configuración de usuario” -> “Directivas” -> “Configuración de Windows” -> “Redirección de carpetas” -> “Documentos”.

Hacemos clic derecho en la carpeta "Documentos" y seleccionamos "Propiedades", abriéndose así una ventana como la de la Figura 104, en la cual podemos configurar los parámetros de la redirección.

Como configuración elegimos "Básico: redirigir la carpeta de todos a la misma ubicación", y en la configuración de la ubicación elegimos la opción "Crear una carpeta para cada usuario en la carpeta raíz" y como ruta para la carpeta raíz le indicamos la de la carpeta Redirect que acabamos de crear: \\SERVIDOR2\Redirect. Para terminar, aplicamos y aceptamos.

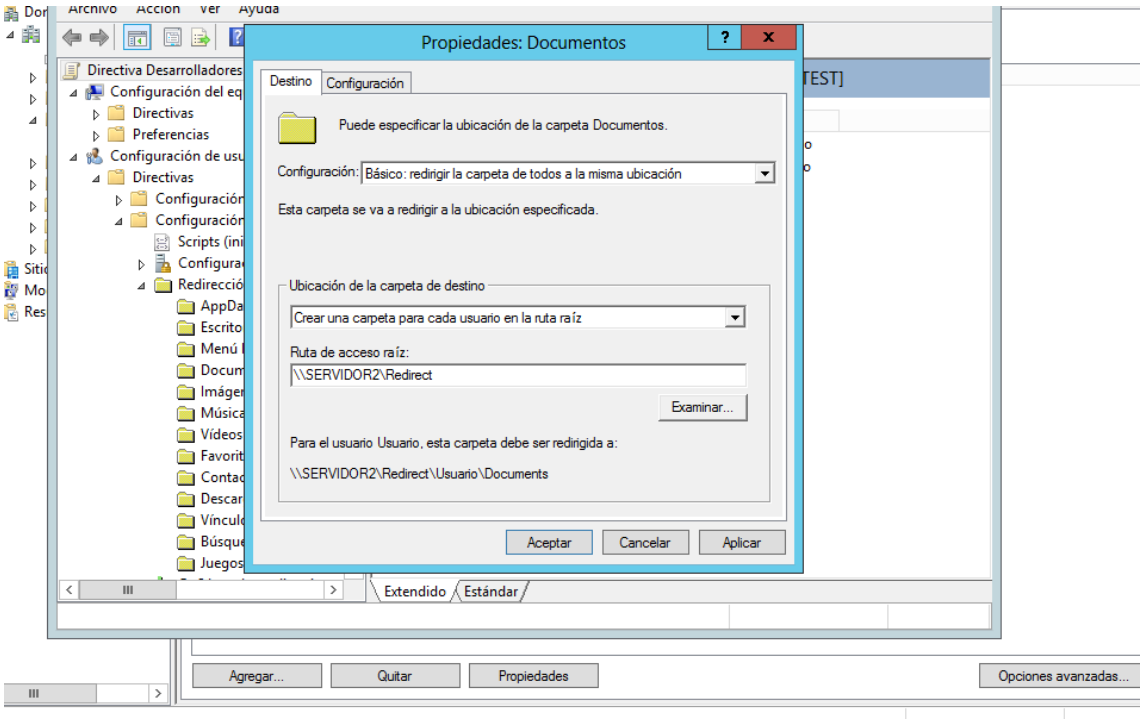


*Figura 104: Configuración de la redirección de carpeta*

Finalmente, para la siguiente y última directiva, hemos seguido el siguiente camino: "Configuración de usuario" -> "Directivas" -> "Plantillas administrativas" -> "Sistema" -> "Opciones de Ctrl+Alt+Supr".

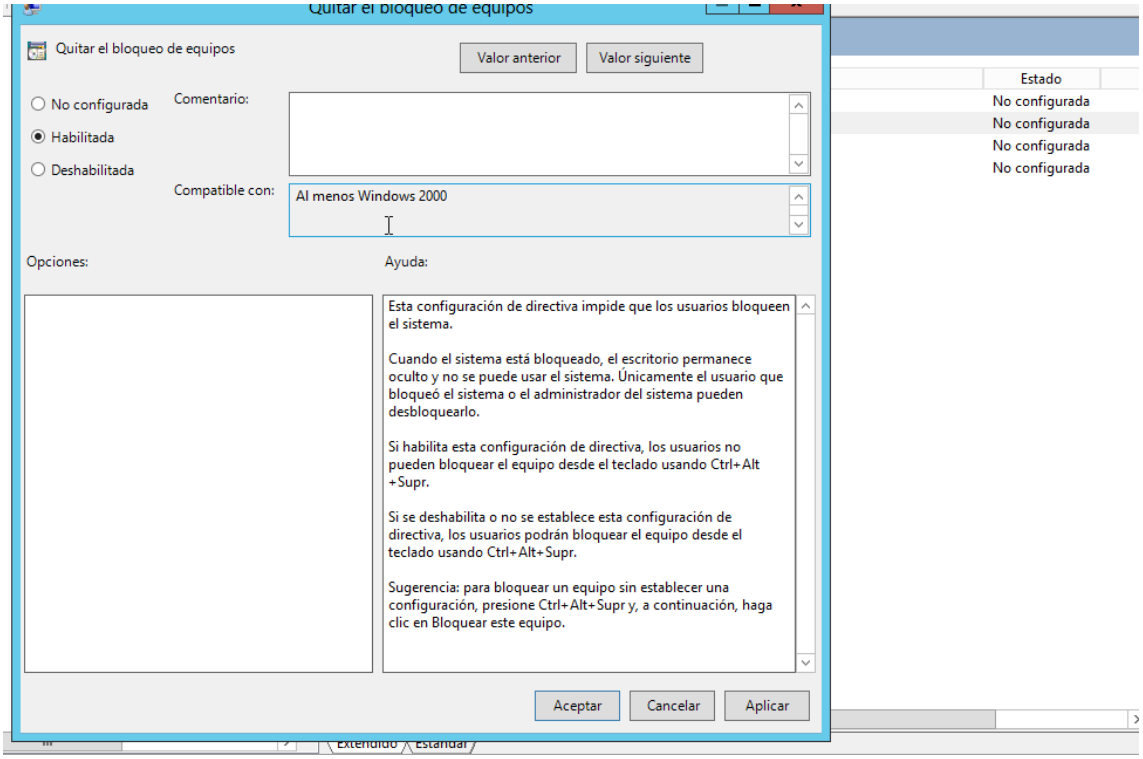


*Figura 105: Quitar bloqueo de equipos desde Ctrl+Alt+Supr*

Además, desde la pestaña Delegación, denegamos el permiso Aplicar directiva de grupo a uno de los usuarios de la UO, Daniel Martínez, esto hará que no se le apliquen ninguna de las directivas de usuario configuradas en la GPO, sin embargo, si le afectarán las directivas de equipo.

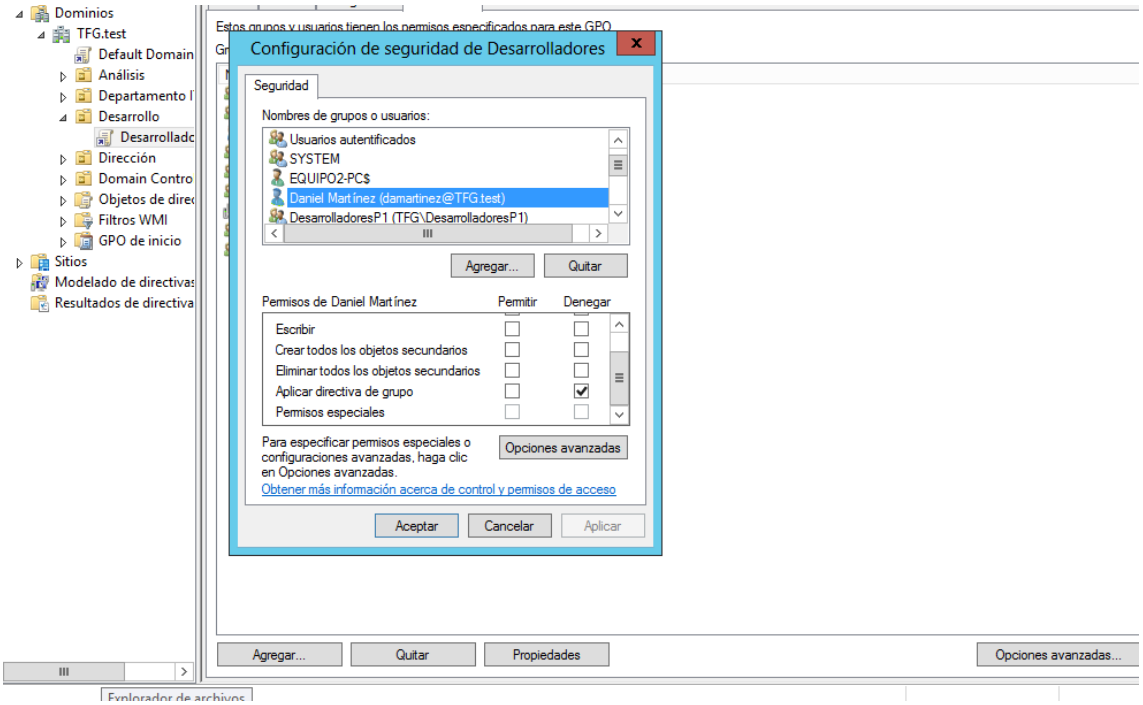


*Figura 106: Denegar permiso Aplicar directiva de grupo a Daniel Martínez*

En las siguientes figuras, se muestra un resumen de las directivas aplicadas, a este resumen se accede desde la pestaña configuración.

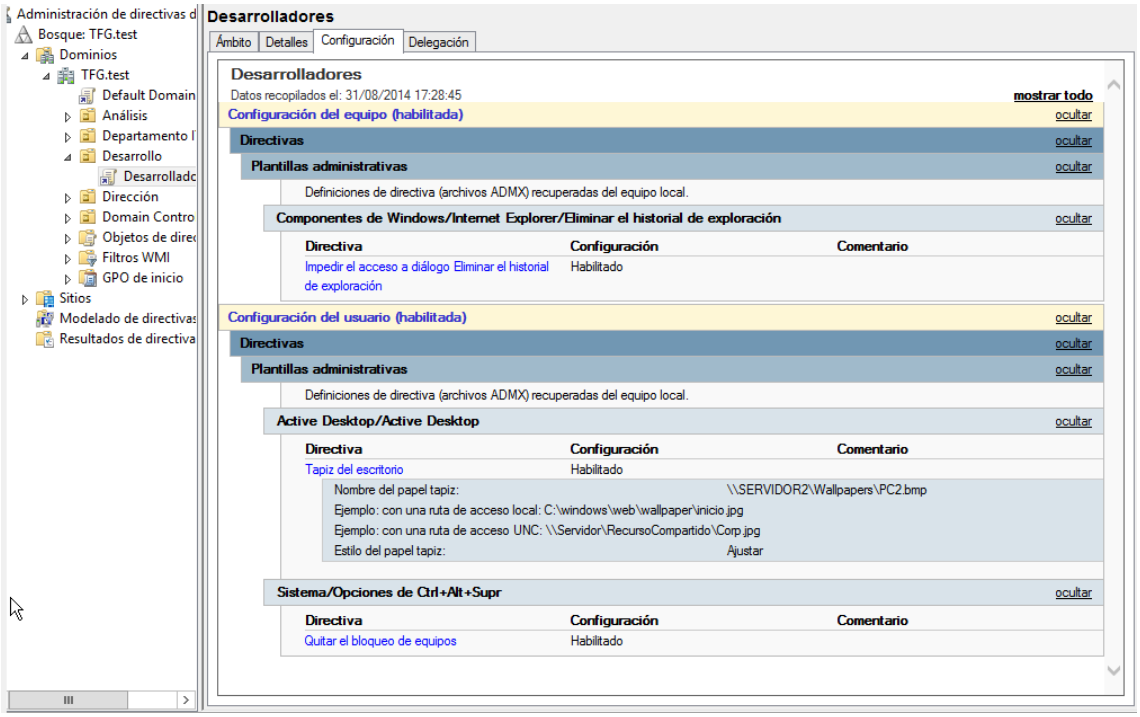


*Figura 107: Resumen de las directivas aplicadas I*

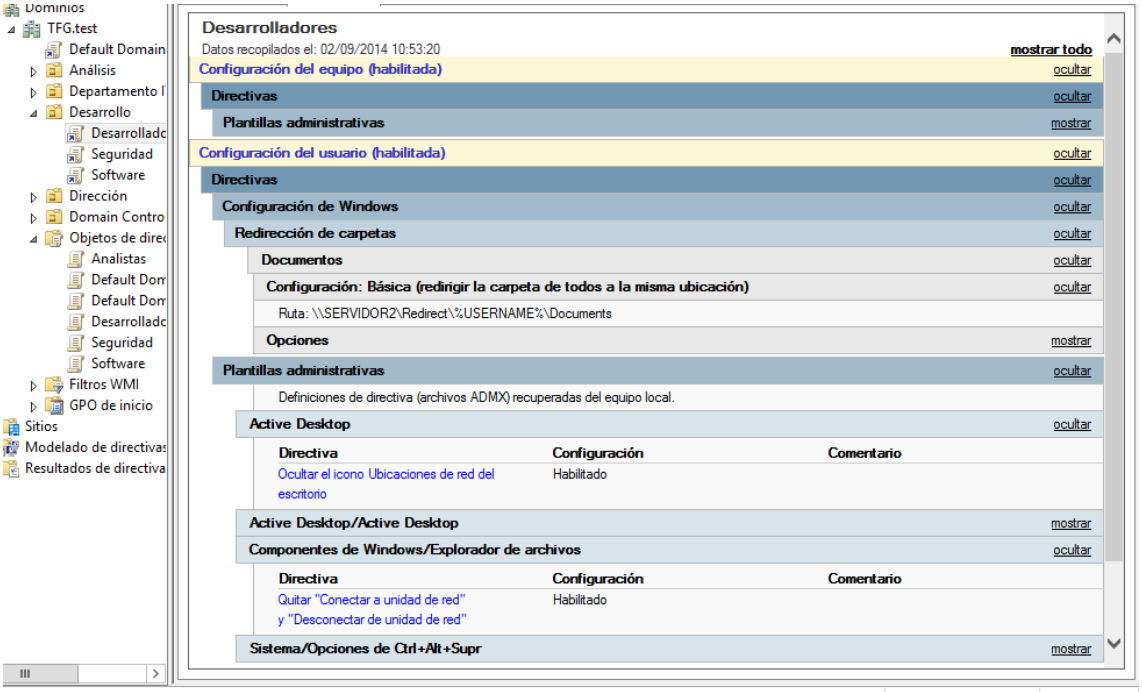


*Figura 108: Resumen de las directivas aplicadas II*

Como en la GPO Análisis, las directivas de equipo se asignarán al poner en marcha la máquina, esto quiere decir que ningún usuario que inicie sesión en este equipo podrá acceder al menú de eliminar el historial de internet explorer.

Las directivas de usuario se inicializarán al iniciar sesión un usuario al que se le haya asignado esta GPO, ese implica que, sin importar en que equipo inicie sesión, ningún usuario de la unidad organizativa Desarrolladores podrá

bloquear el equipo utilizando Ctrl+Alt+Supr, y todos los usuarios de esta OU tendrán el mismo fondo de escritorio.

Estas acciones se pueden observar en las siguientes capturas de pantalla que corresponden a las pruebas de aplicación de la GPO, estas pruebas se han realizado después de haber lanzado el comando gpupdate para asegurarnos así de que las directivas se hubieran aplicado.

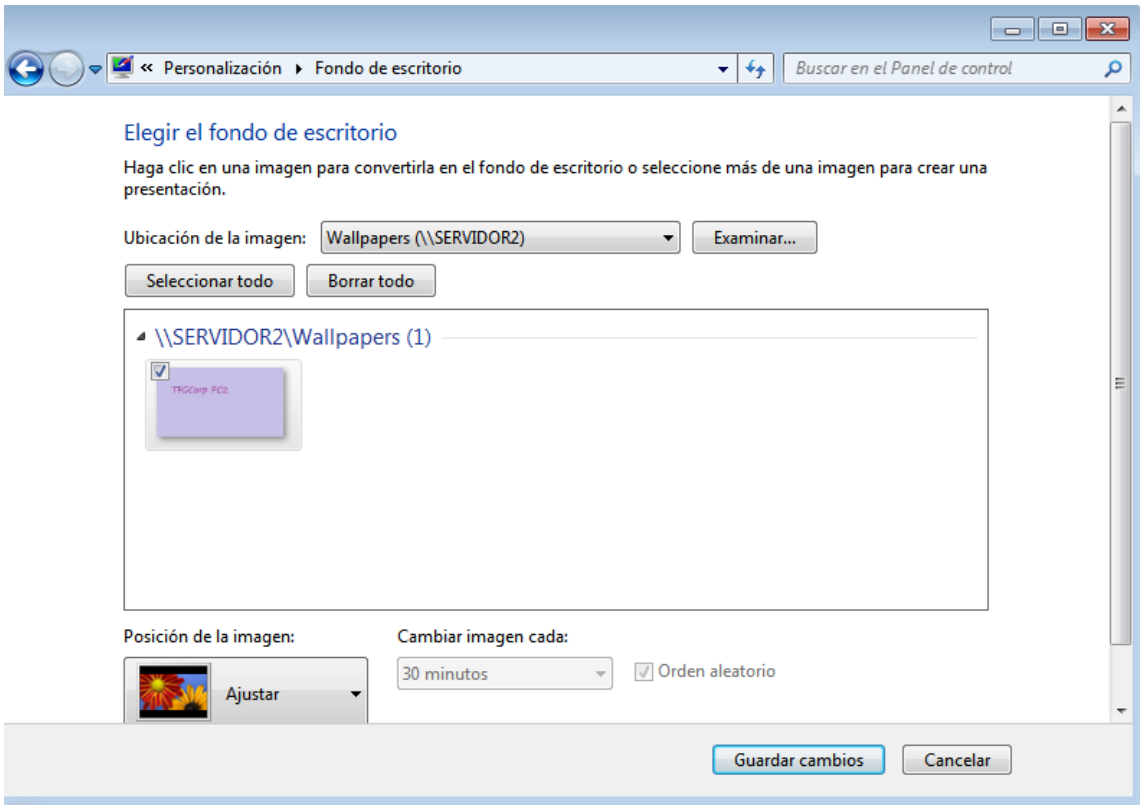


*Figura 109: Fondo de pantalla de la carpeta Wallpapers*

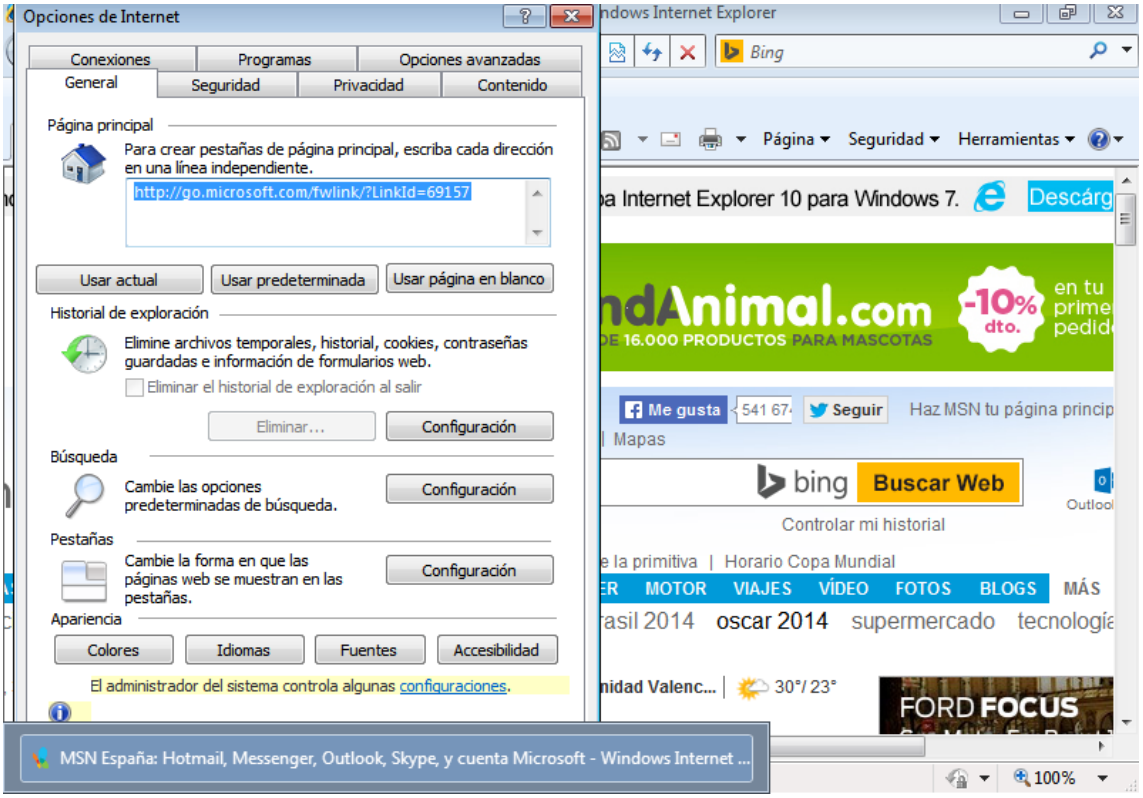


*Figura 110: Botón "Eliminar..." deshabilitado*

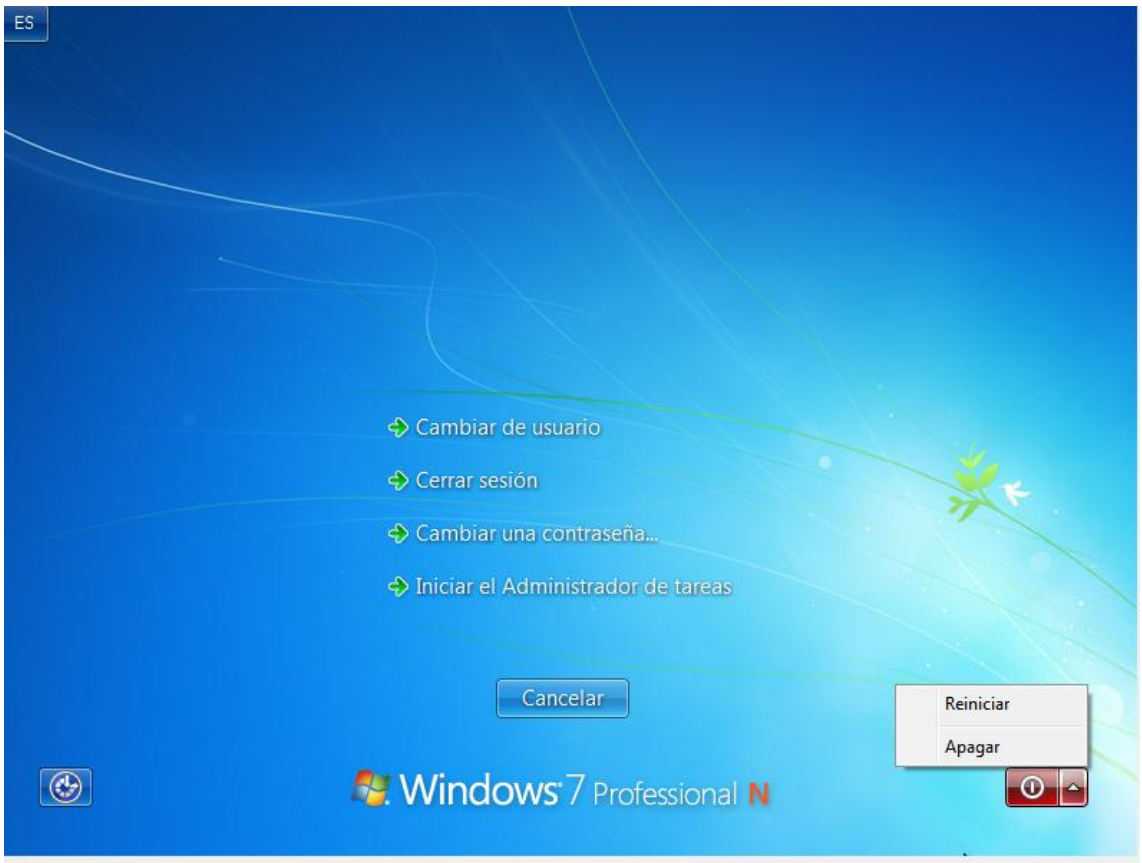


*Figura 111: Sin opción de bloquear ordenador*

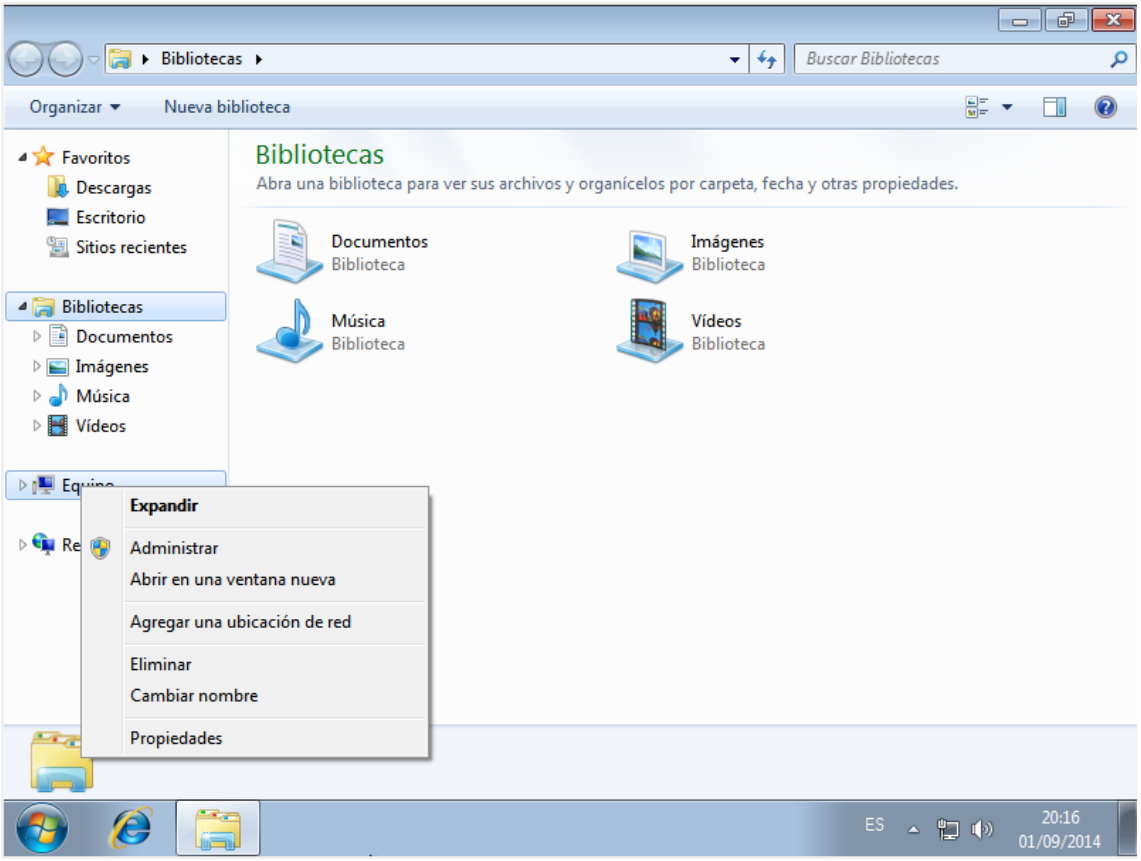


*Figura 112: No aparecen las opciones Conectarse / Desconectarse a una unidad de red*

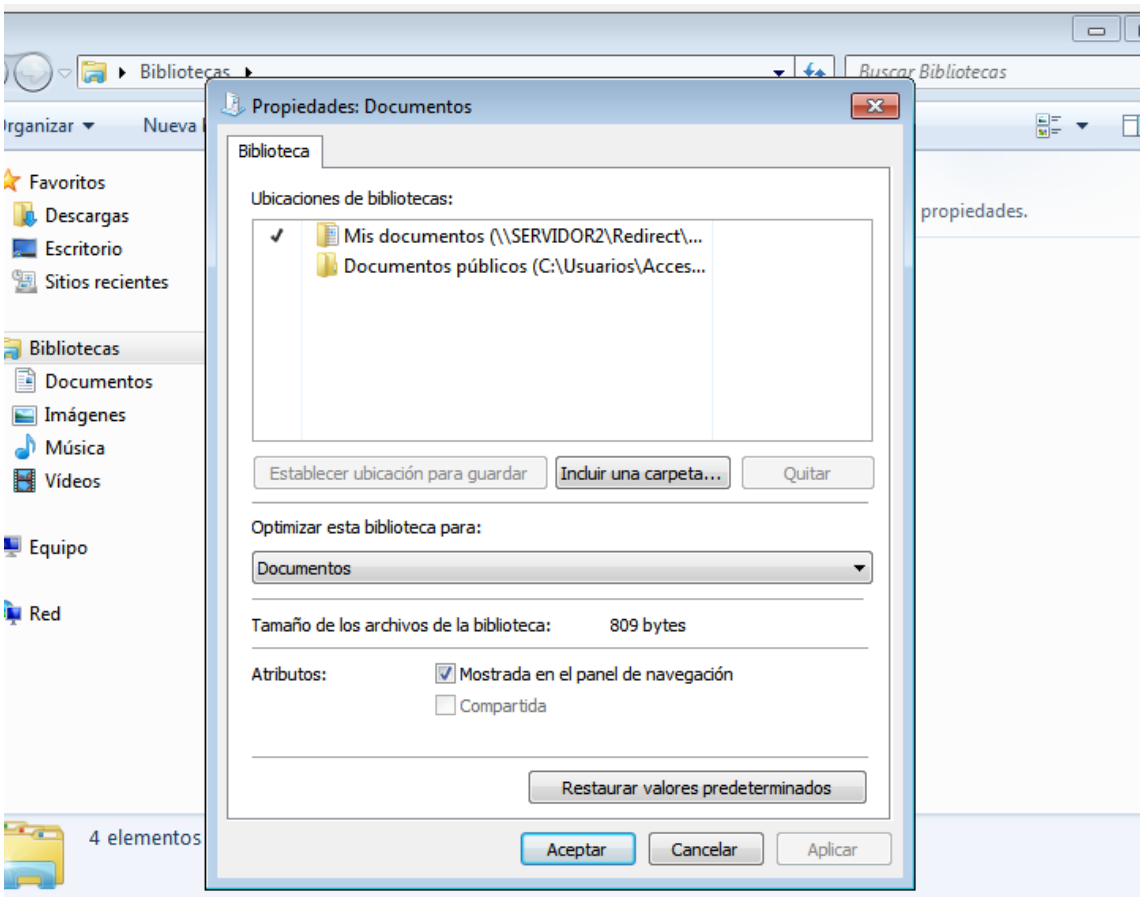


*Figura 113: La carpeta Mis Documentos se redirige a la carpeta Redirect en SERVIDOR2*

Las capturas anteriores han sido realizadas desde el EQUIPO2, conectados con uno de los usuarios de la OU Desarrolladores, las siguientes capturas han sido realizadas desde el EQUIPO2, conectados con el usuario Daniel Martínez, de la OU Desarrollo también, al que le hemos denegado los permisos de aplicación de la GPO asignada.

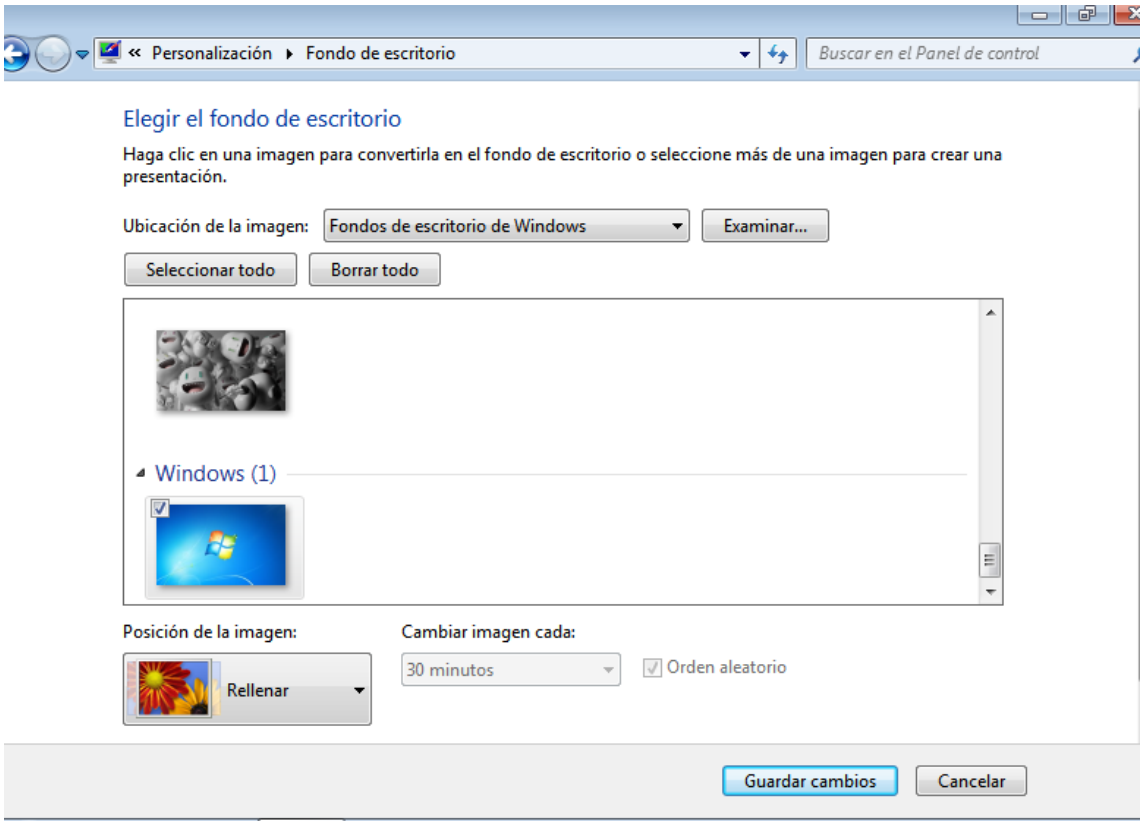


*Figura 114: Fondo básico de Windows al conectar con un usuario de fuera de la OU*

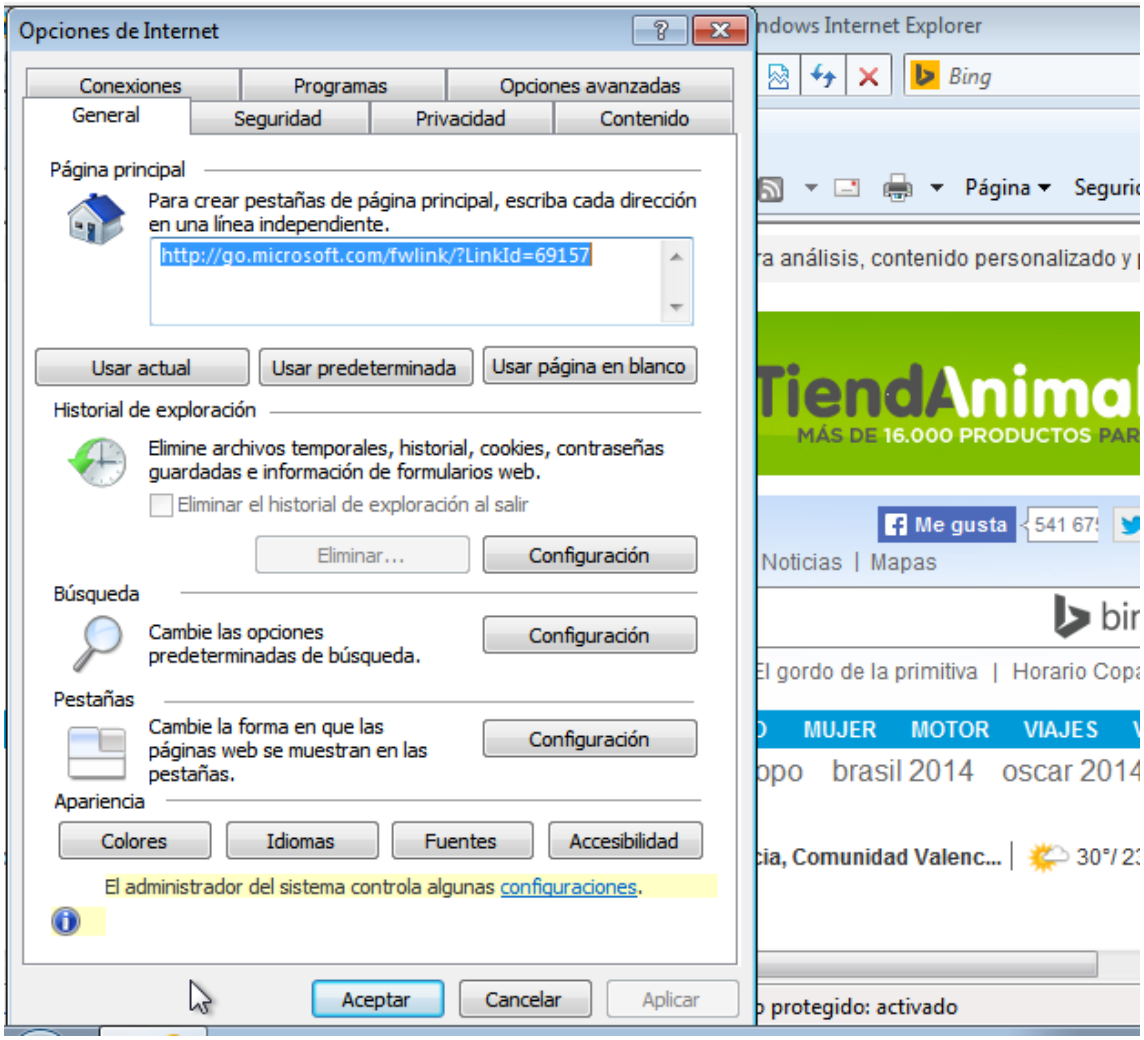


*Figura 115: Botón "Eliminar..." deshabilitado*

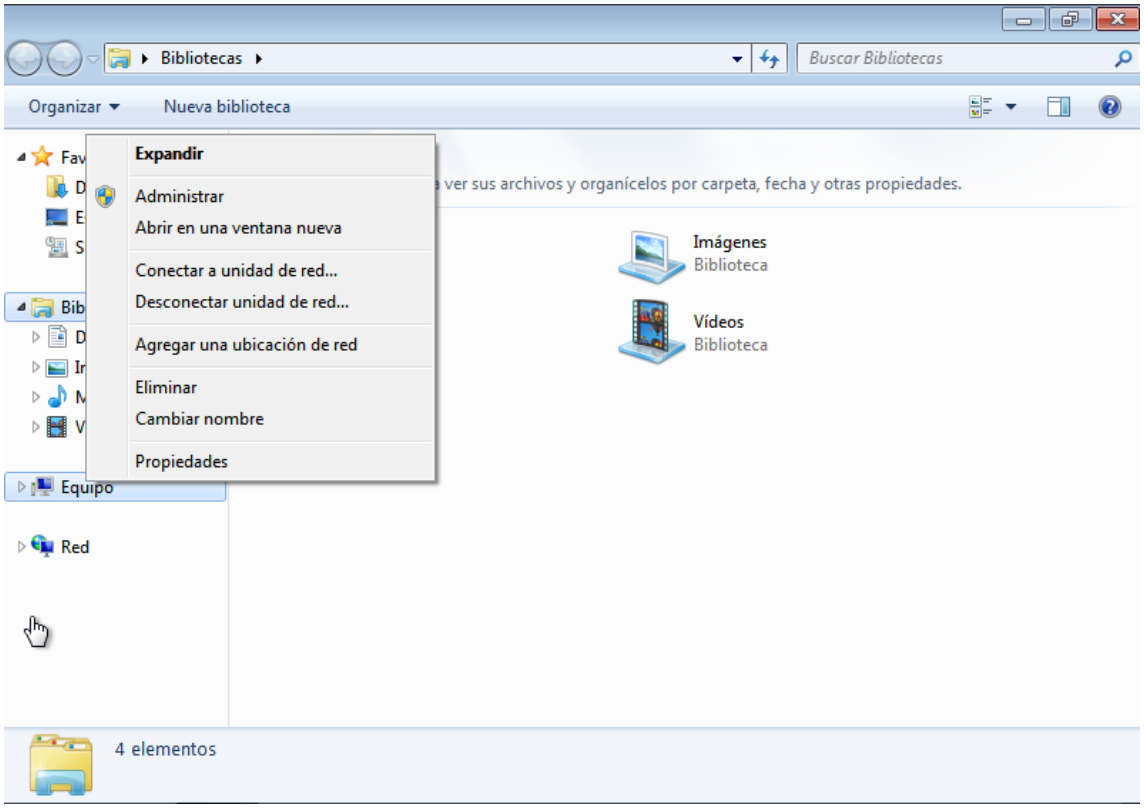


*Figura 116: Sí aparecen las opciones Conectar/Desconectar una unidad de red*


*Figura 117: Opción de bloquear el equipo*

### *4.2.2.2 Directivas de Software*

Mediante las directivas de asignación y publicación de software se pueden publicar aplicaciones para que los usuarios las descarguen e instalen, asignarlas para que se instalen automáticamente, con o sin el consentimiento del usuario final, y la actualización de aplicaciones. En este apartado explicaremos cómo configurar estas directivas de software.

Primero creamos la GPO software en Objetos de directivas de grupo, y la vinculamos a nuestras OUs Análisis y Desarrollo, una vez ya se ha vinculado, hacemos clic con el botón derecho y seleccionamos “Editar”.

En la GPO Software, nos dirigimos a “Configuración de usuario” -> “Directivas” -> “Configuración de software” -> “Instalación de software” y hacemos clic derecho sobre éste último, seleccionando “Nuevo” -> “Paquete...”. Tras esto, se abrirá una ventana en la que podremos seleccionar el paquete a incluir en la lista. Seleccionamos el paquete Green de la carpeta Colorful.

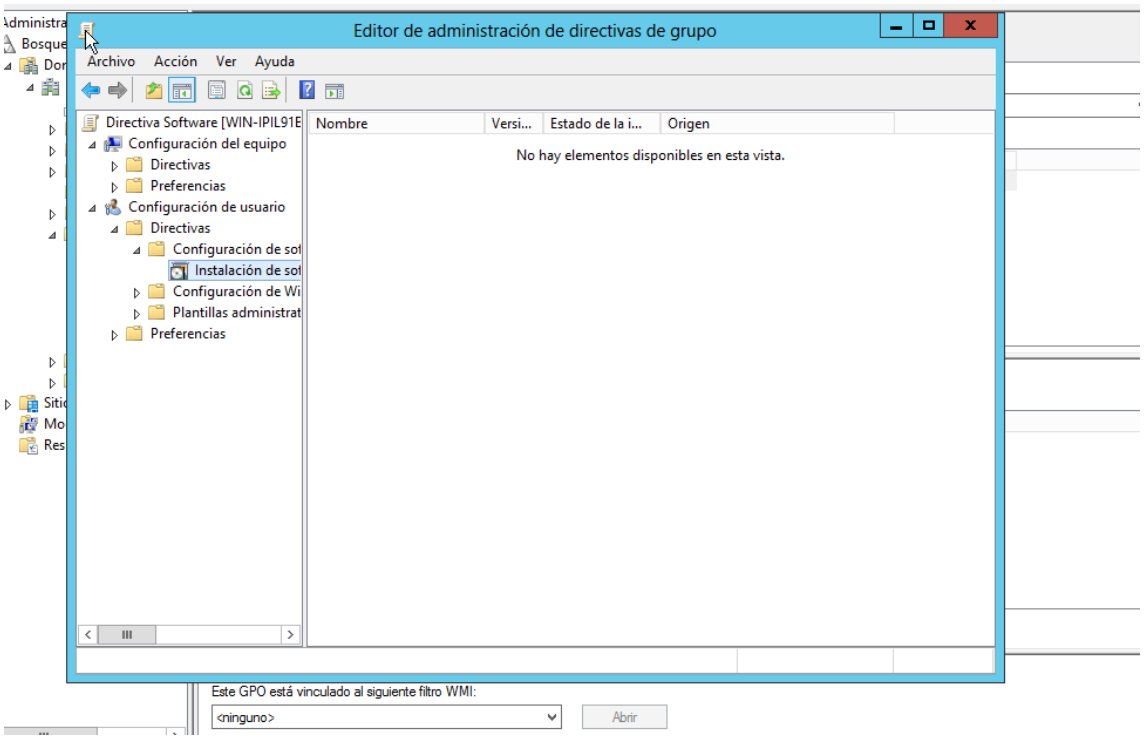


*Figura 118: Instalación de software*

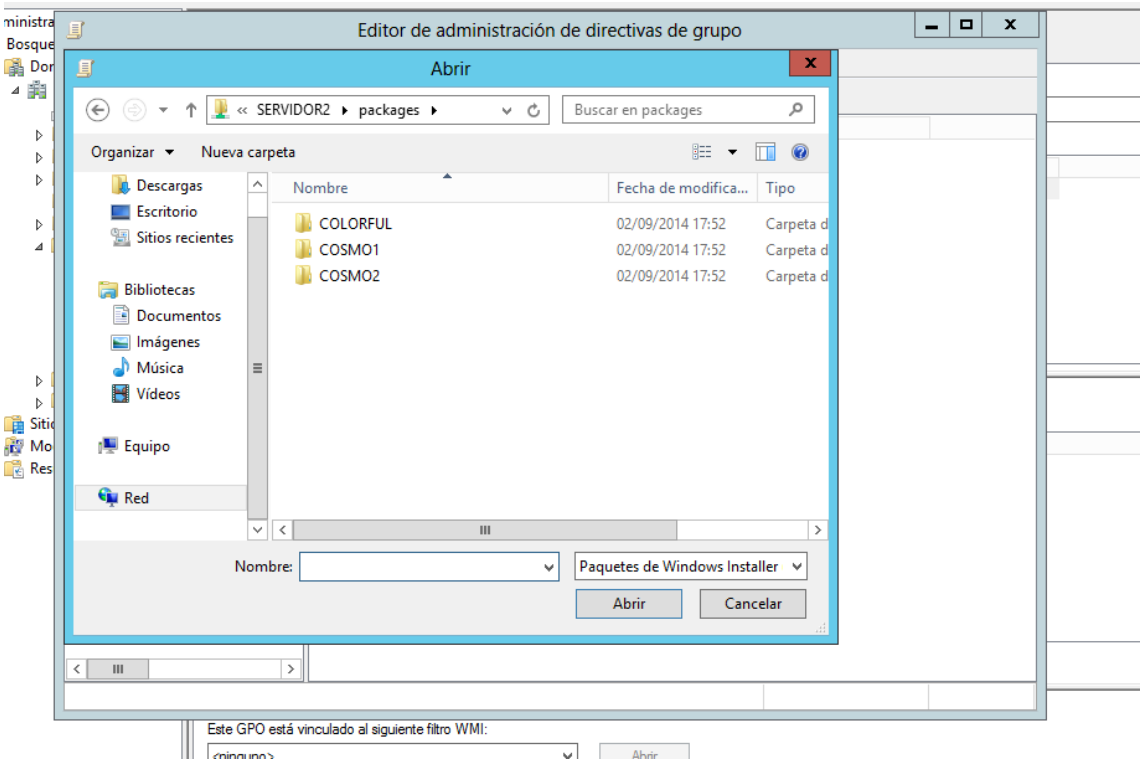


*Figura 119: Paquetes*

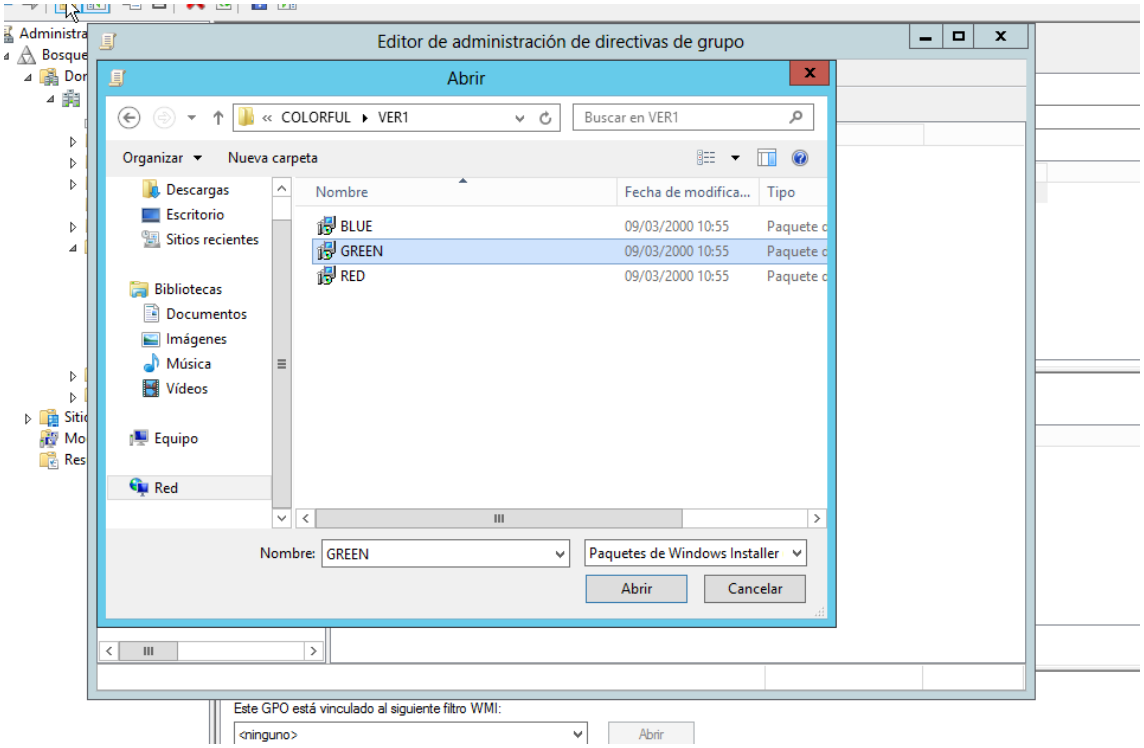


*Figura 120: Selección del paquete GREEN*

Tras pulsar Abrir, aparecerá un nuevo cuadro de diálogo que nos da a elegir entre varios métodos de implementación. Como queremos que todos los usuarios tengan el programa en la lista de programas instalados, seleccionamos la opción “Asignada” y pulsamos Aceptar.

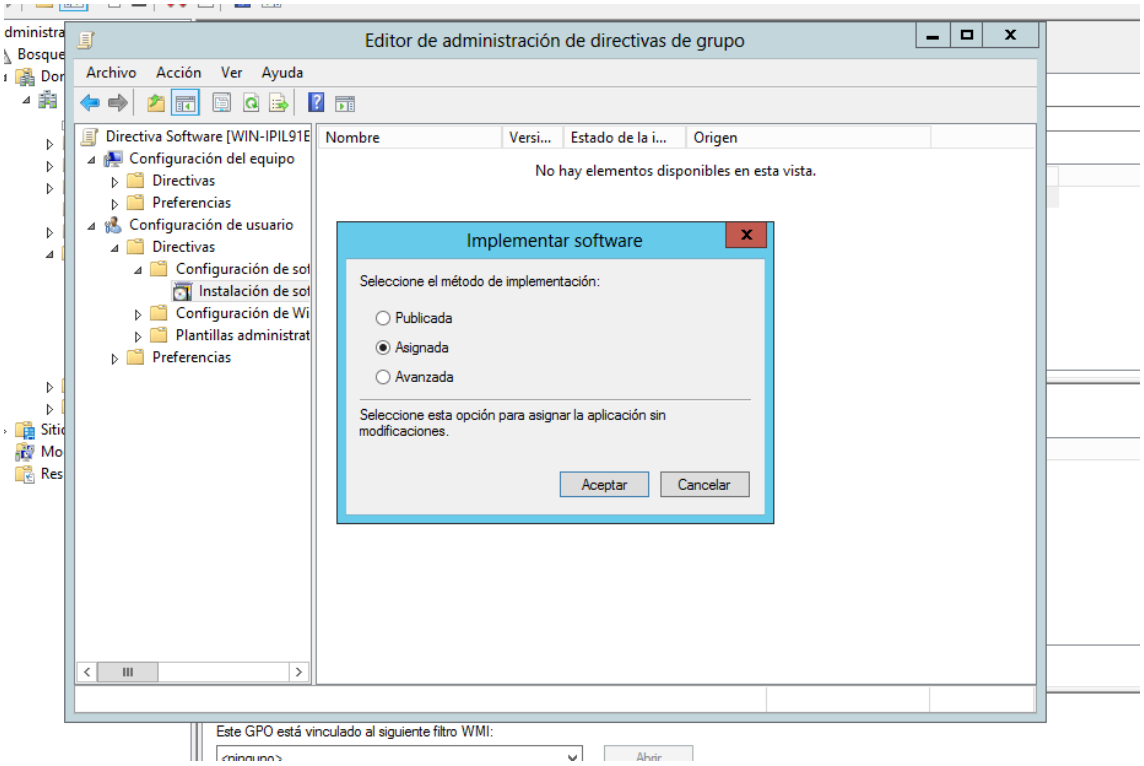


*Figura 121: Método de implementación*

A continuación, y como se puede ver en las siguientes figuras, comprobamos en distintos equipos y con distintos usuarios que la aplicación Green se ha instalado con éxito y se puede utilizar en todos los equipos.

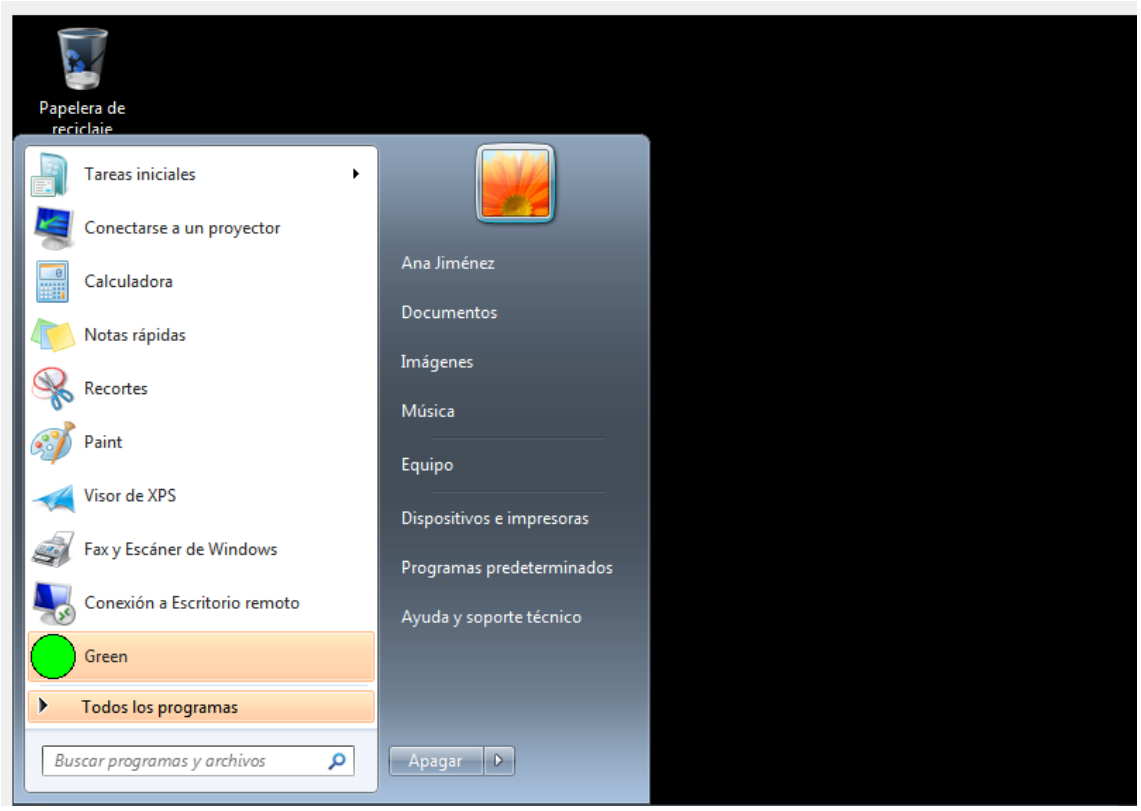


*Figura 122: Green en la lista de programas*

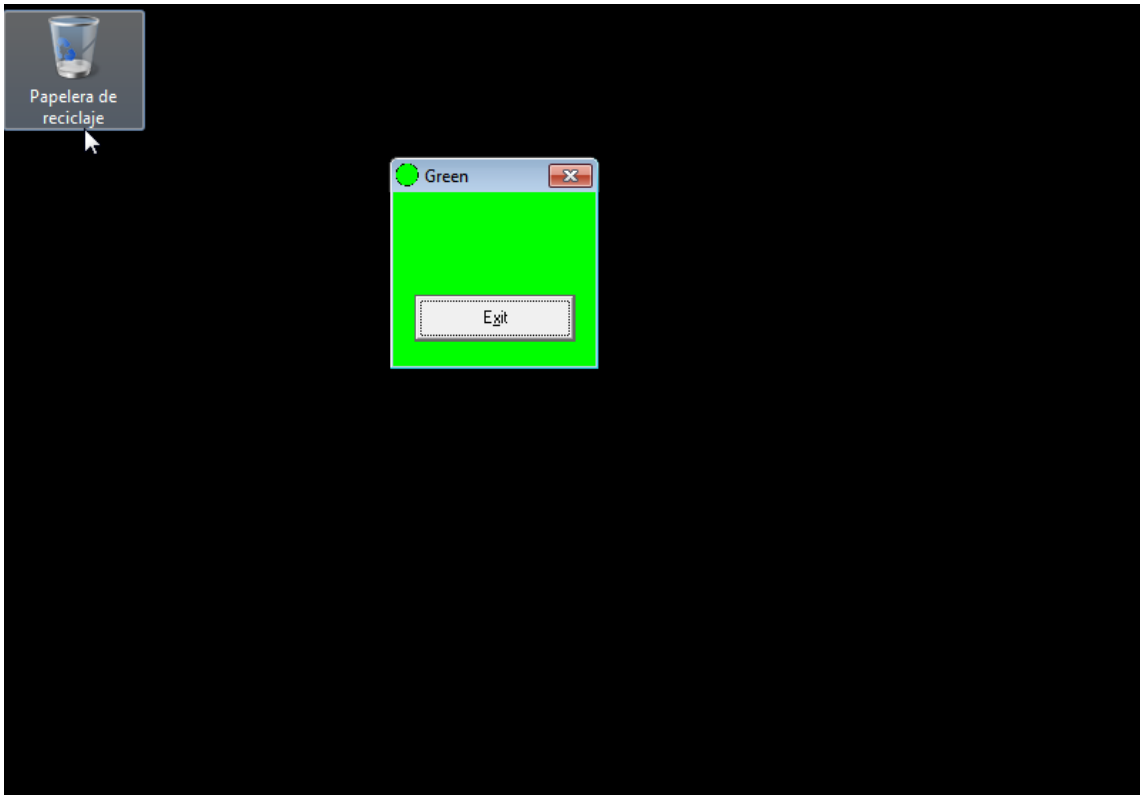


*Figura 123: Ejecución de Green*

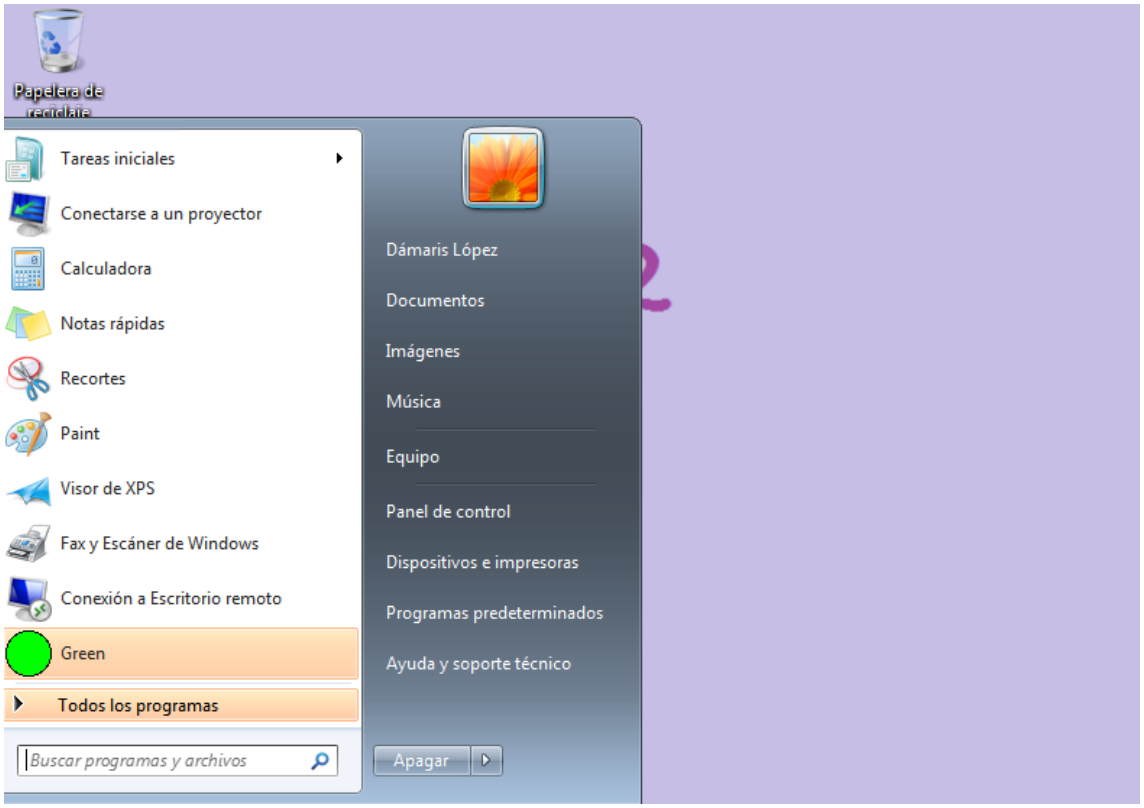


*Figura 124: Green en la lista de programas en otro equipo y con otro usuario*


*Figura 125: Green ejecutándose*

A continuación vamos a publicar la aplicación COSMO1. Para ello vamos a seguir un proceso similar al seguido con GREEN, pero en este caso en lugar de instalarla en todos los equipos, lo que vamos a hacer es que los usuarios puedan instalarla desde el Panel de Control.

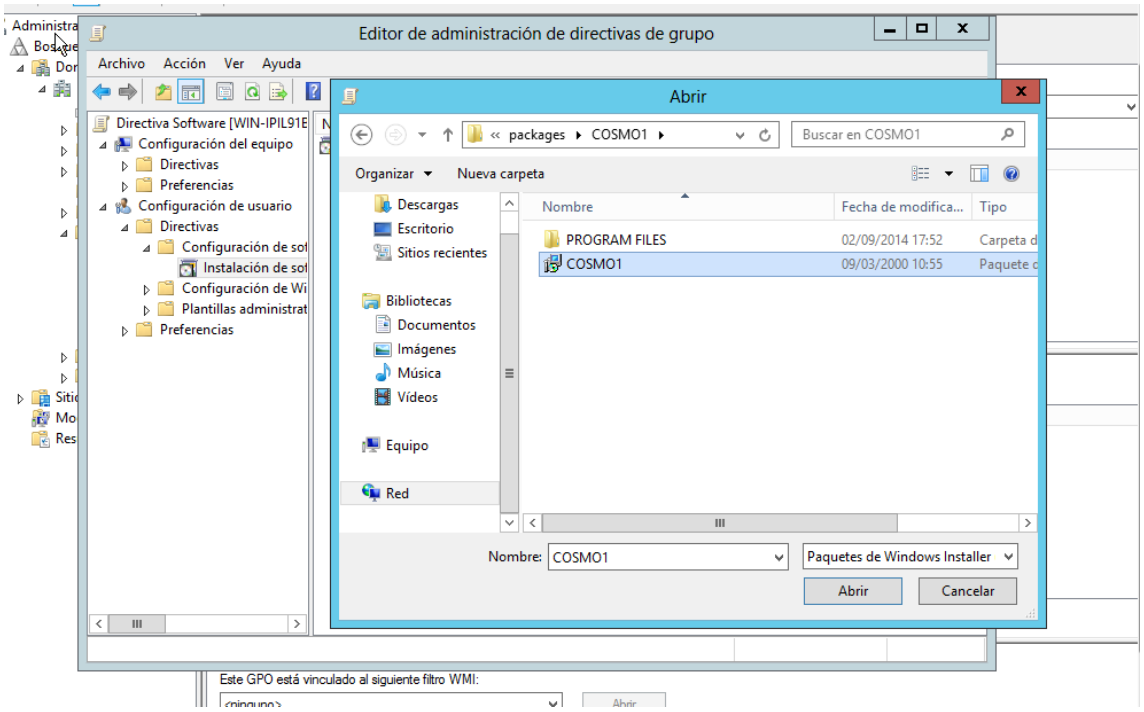


*Figura 126: Añadir paquete COSMO*

Para conseguir este objetivo, seleccionamos como método de implementación la opción “Publicada”.

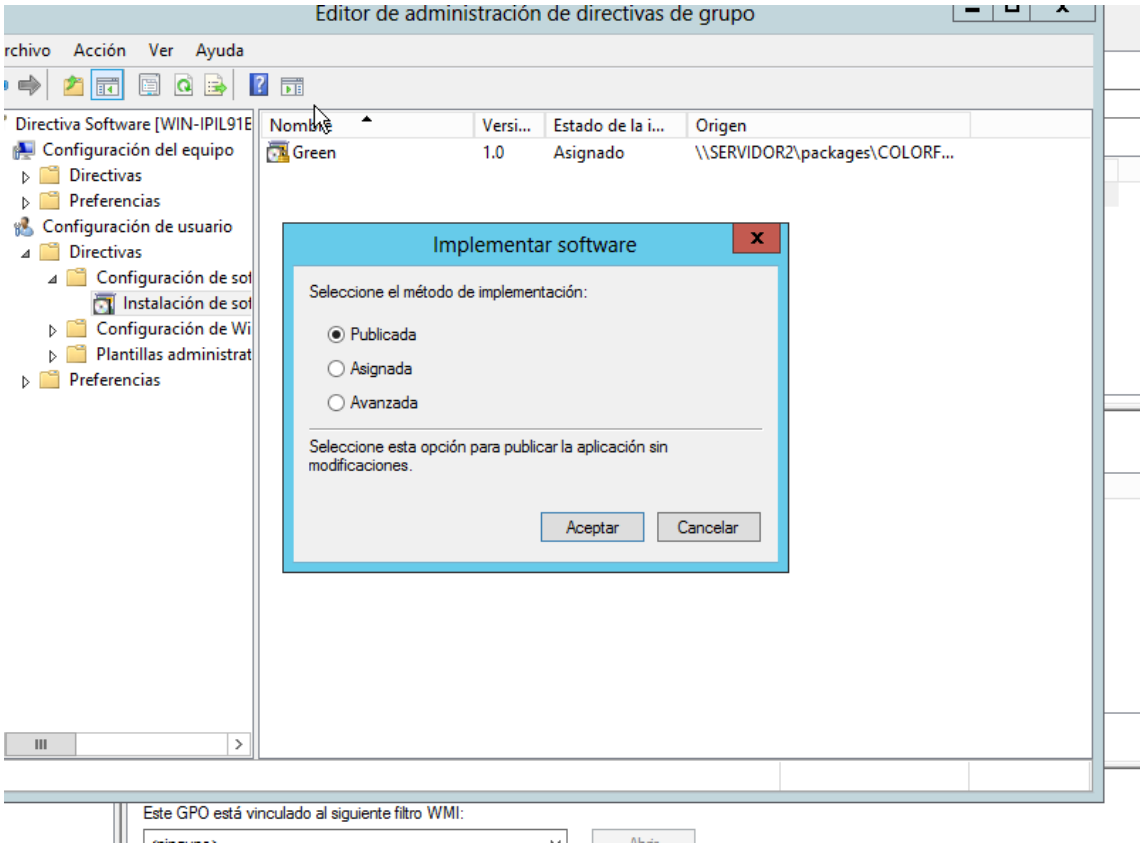


*Figura 127: Marcar aplicación como publicada*

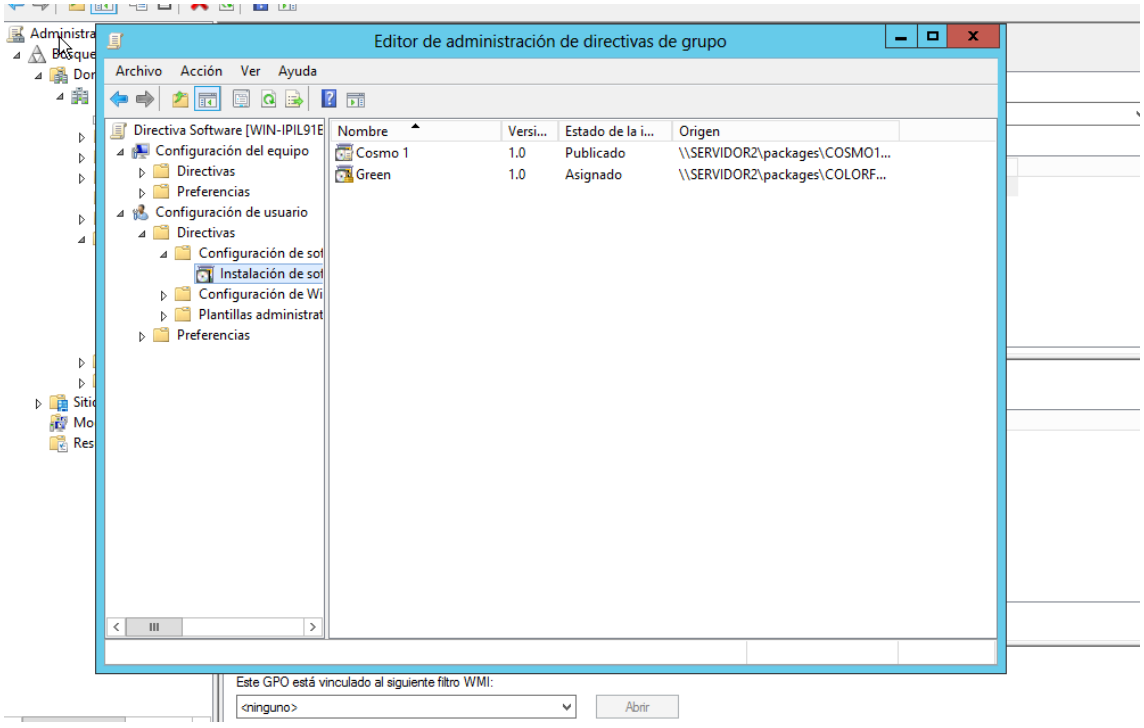


*Figura 128: Resumen de las aplicaciones*

Una vez la aplicación ha sido publicada, iniciamos sesión en cualquier equipo con una cuenta que tenga acceso al Panel de Control, recordemos que los usuarios de Analistas tienen denegado el acceso al mismo, comprobamos que, efectivamente, Cosmo no aparece en el listado de Programas tal y como lo hacía Green. Para poder instalar la aplicación Cosmo necesitaremos hacerlo desde el Panel de Control.

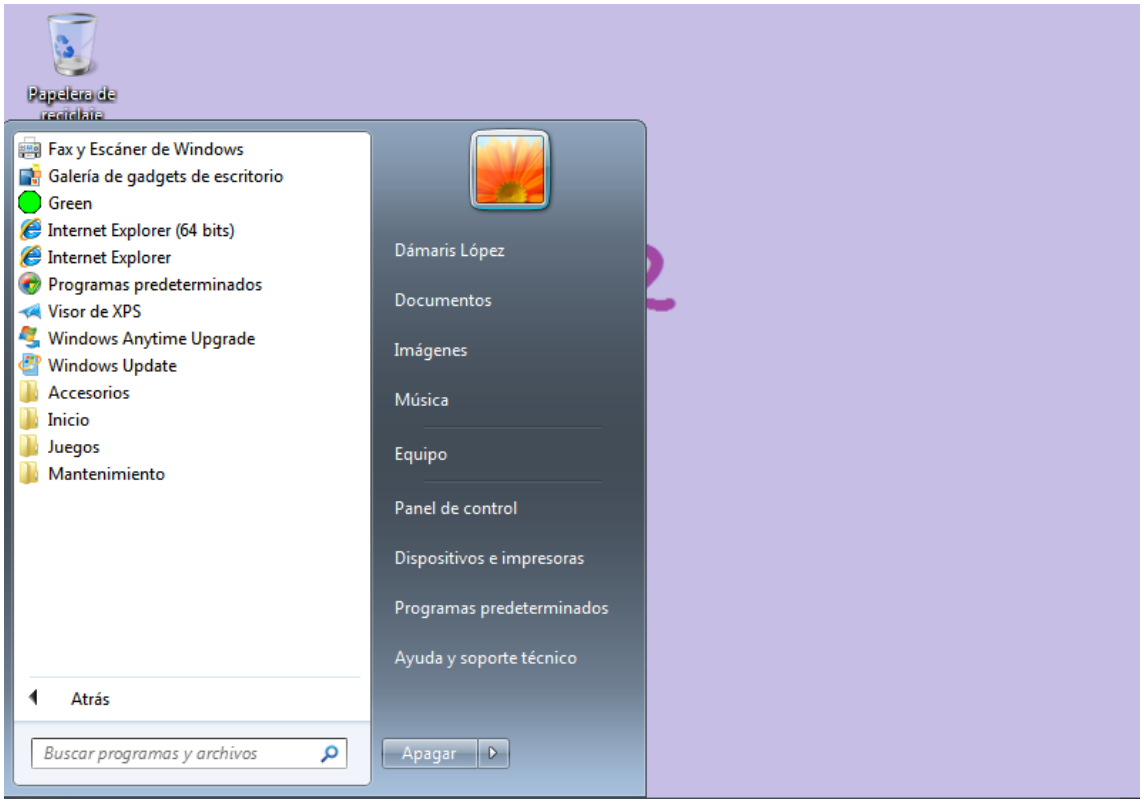


*Figura 129: Cosmo no aparece como aplicación instalada*

Una vez abierto el Panel de Control, seleccionamos Programas, y allí seleccionamos la opción “Instalar un programa desde la red”. Ahora nos aparece un listado de programas en los que se encuentran Green y Cosmo, seleccionamos Cosmo y pulsamos instalar.

Tras un breve periodo de tiempo, el programa ya está instalado y aparece en el menú Programas del menú inicio.

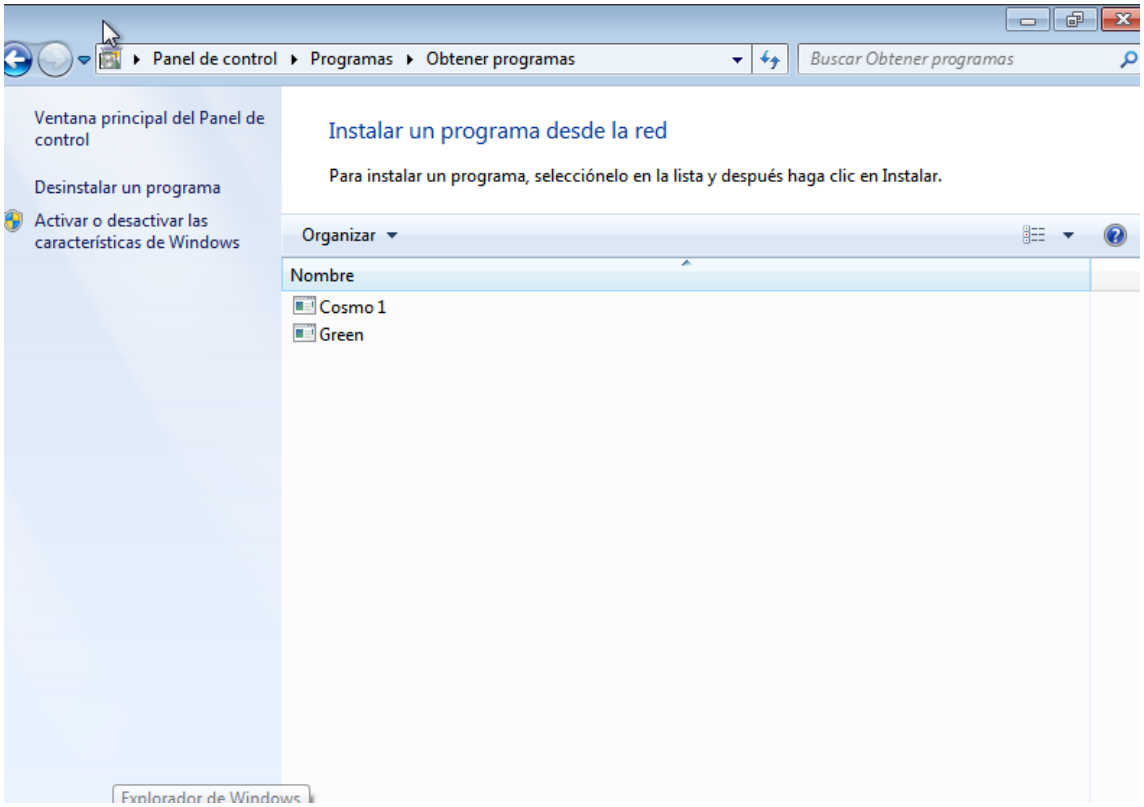


*Figura 130: Panel de Control -> Programas -> Instalar un programa desde la red*

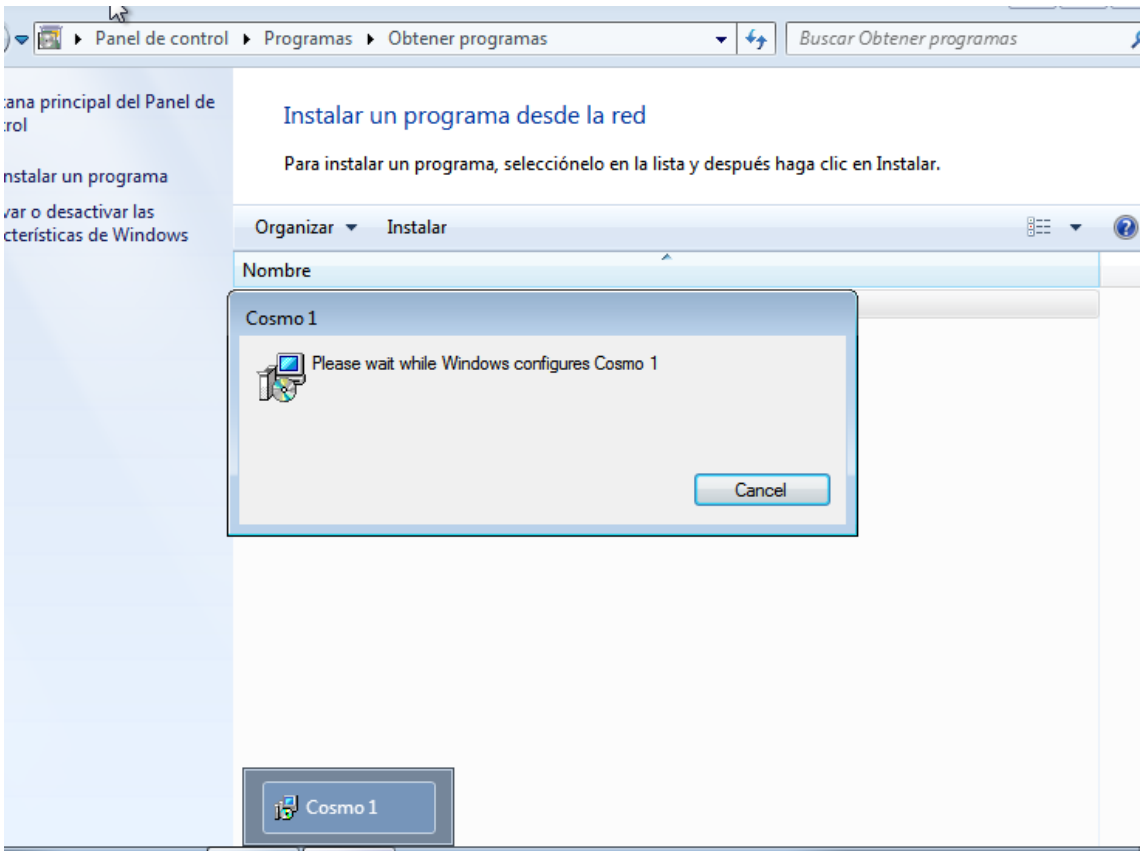


*Figura 131: Instalación de COSMO*

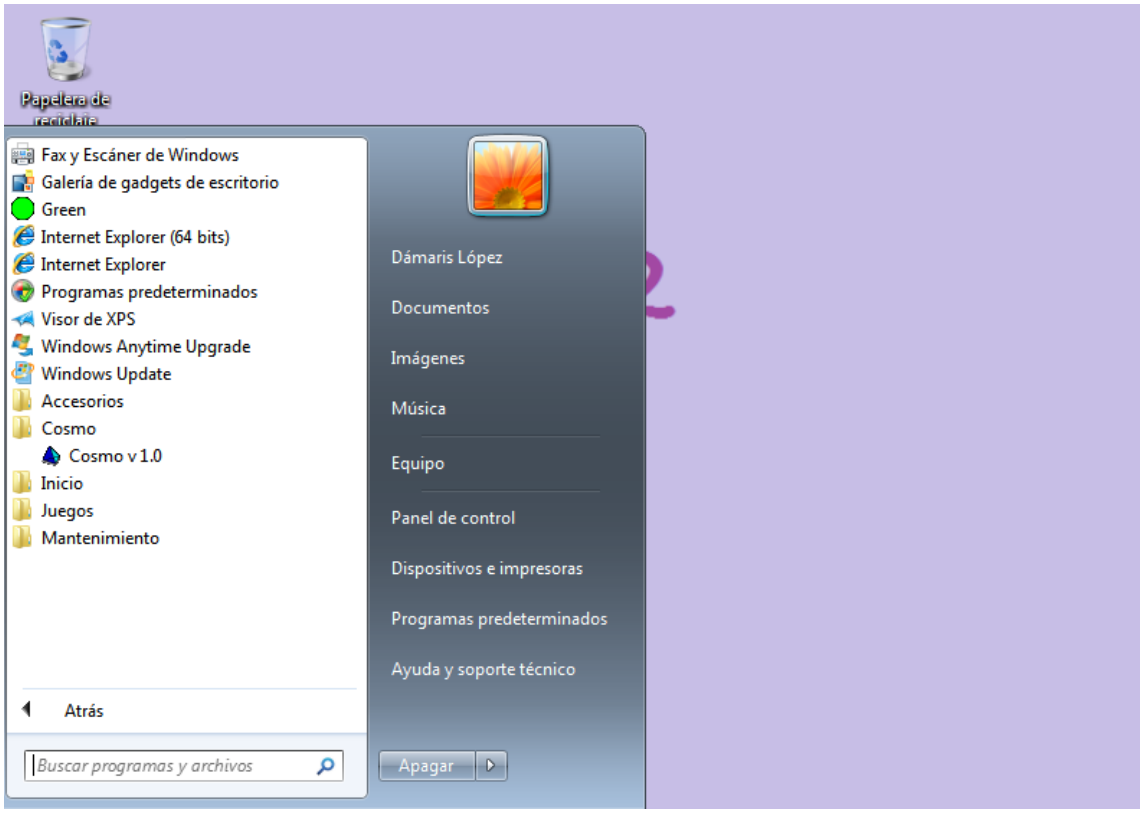


*Figura 132: Cosmo ya aparece en la lista de programas*

Ahora, abrimos sesión con otro usuario, y abrimos Ejecutar, donde insertamos la ruta en la que se encuentran los paquetes de instalación.

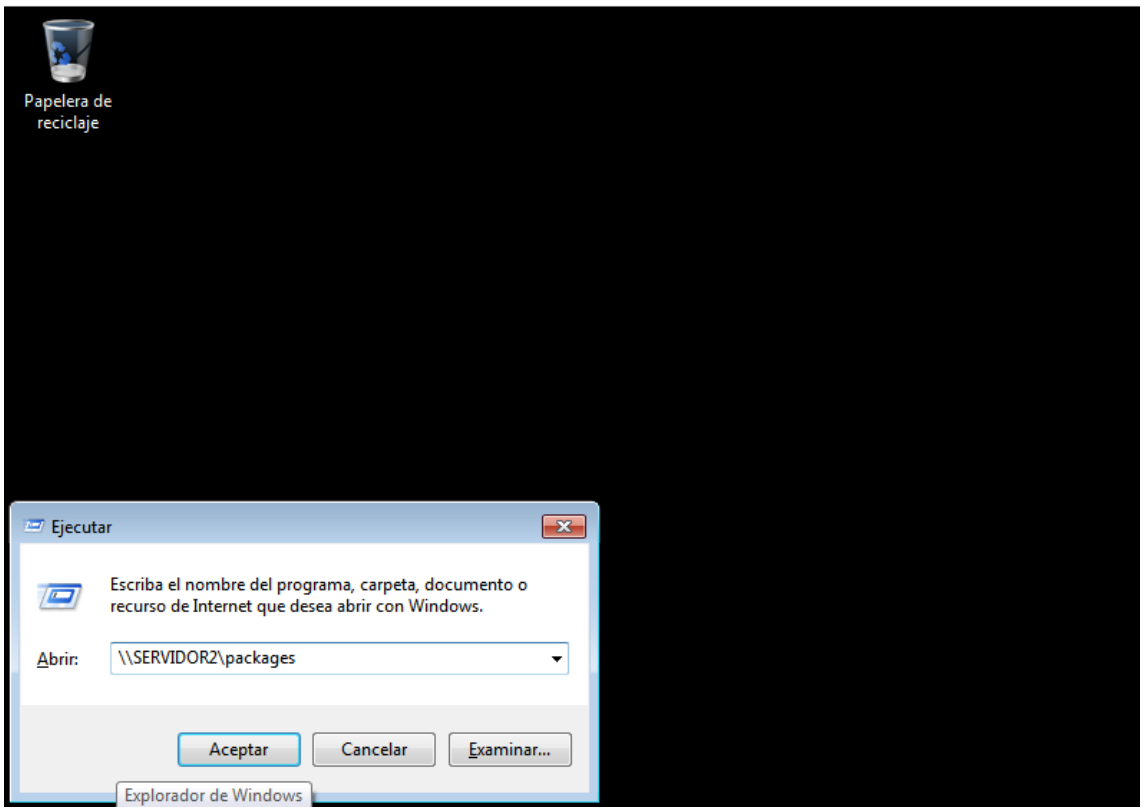


*Figura 133: Abrimos la ubicación SERVIDOR2 -> Packages*

En esta ubicación podemos observar que el archivo COSMO.CS00 no tiene ninguna aplicación asignada, ya que COSMO no se ha instalado automáticamente en los equipos al contrario que Green. Si hacemos doble clic sobre el archivo, comenzará la instalación de Cosmo y, al terminar la instalación se abrirá el archivo, como se muestra en figuras posteriores, además el tipo del archivo cambiará de Archivo CS00 a Cosmo-00.

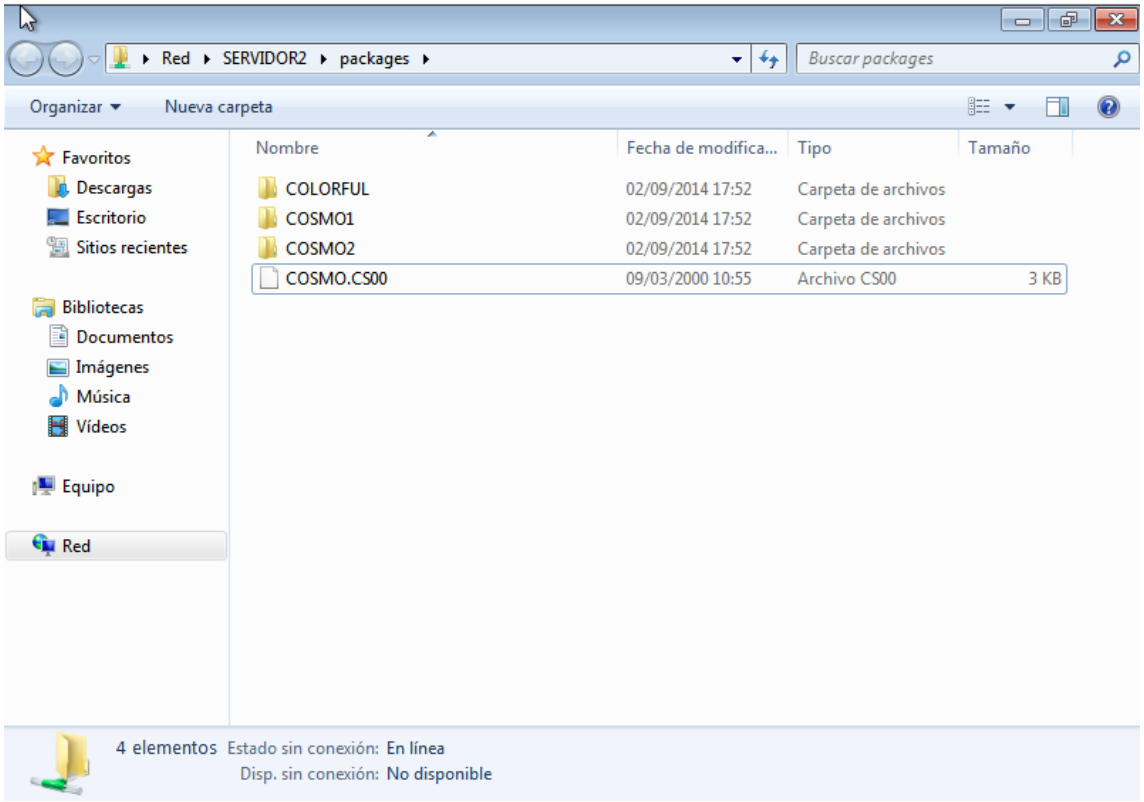


*Figura 134: COSMO.CS00 no tiene un programa asignado*

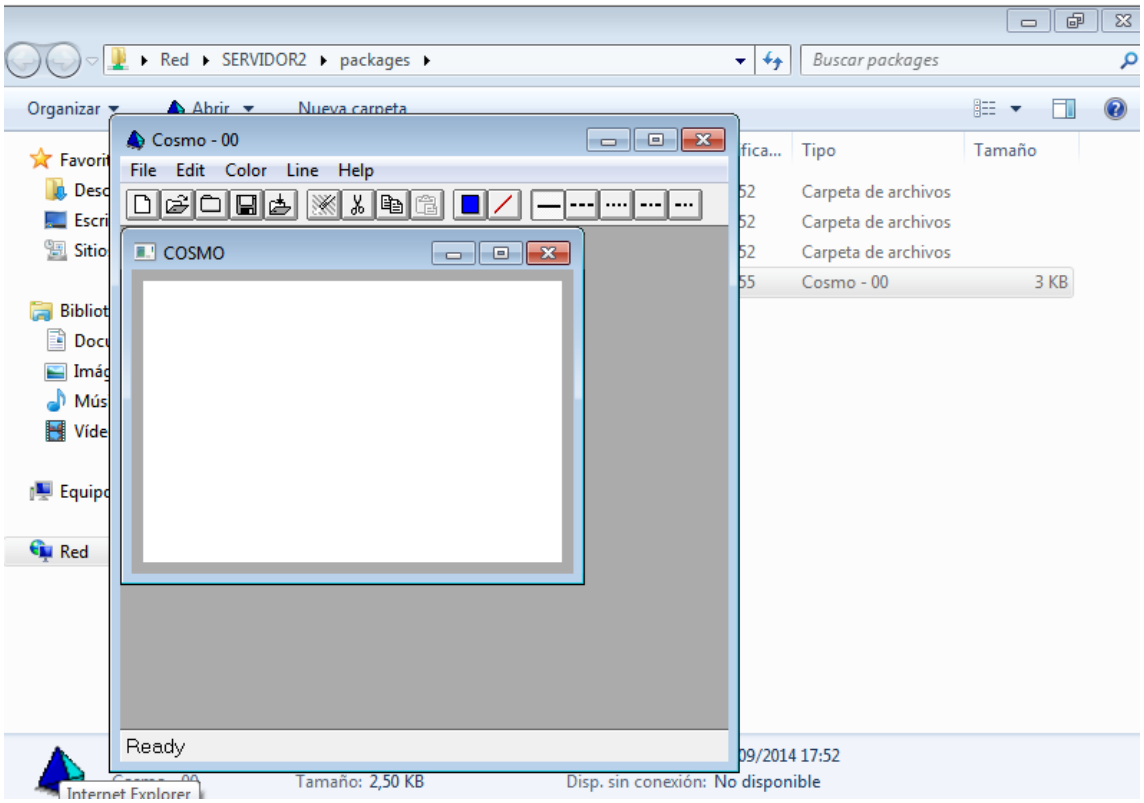


*Figura 135: Cosmo se instala y abre el archivo*

Ahora vamos a configurar una actualización de carácter obligatorio para la aplicación Cosmo1, para ello añadimos el paquete COSMO2 a la lista de aplicaciones, y como método de implementación seleccionamos Avanzada.

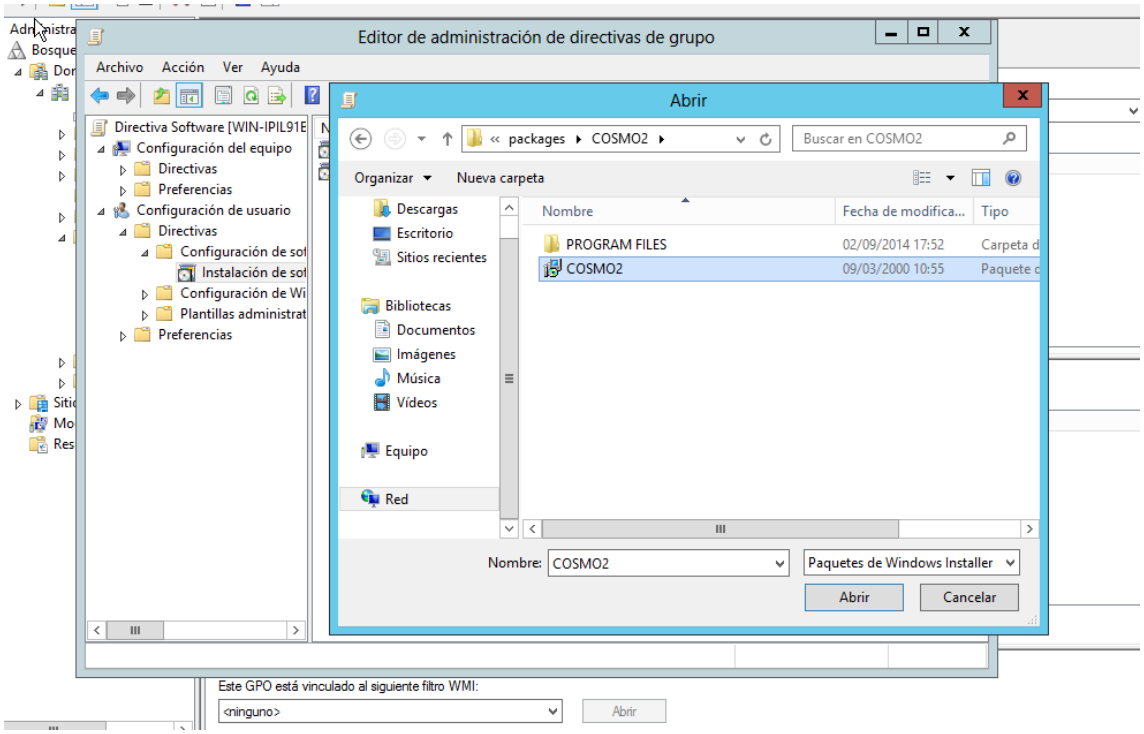


*Figura 136: Selección de paquete COSMO2*

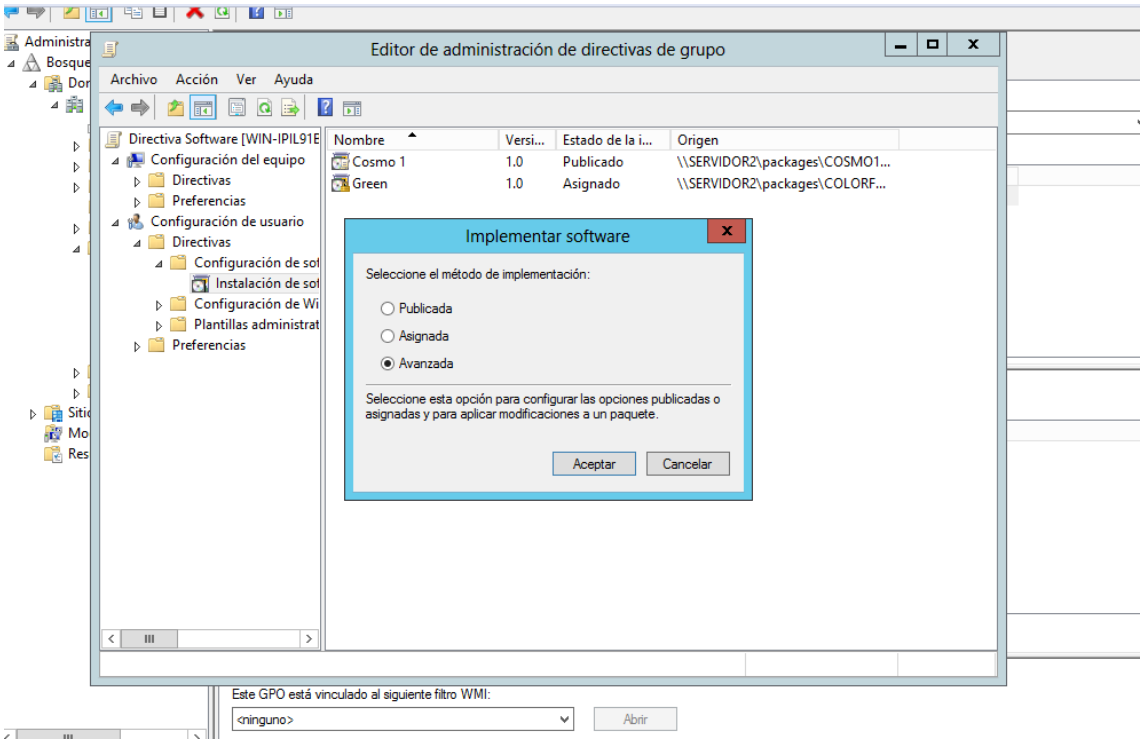


*Figura 137: Método de implementación Avanzada*

Al pulsar Aceptar se abre un nuevo cuadro de diálogo que nos da a elegir la GPO dónde se encuentra el paquete a actualizar y el paquete. Además nos da la opción de "Desinstalar el paquete existente e instalar el paquete actualizado" o bien "El paquete puede actualizar un paquete existente". Seleccionamos la primera opción, ya que queremos forzar la actualización.

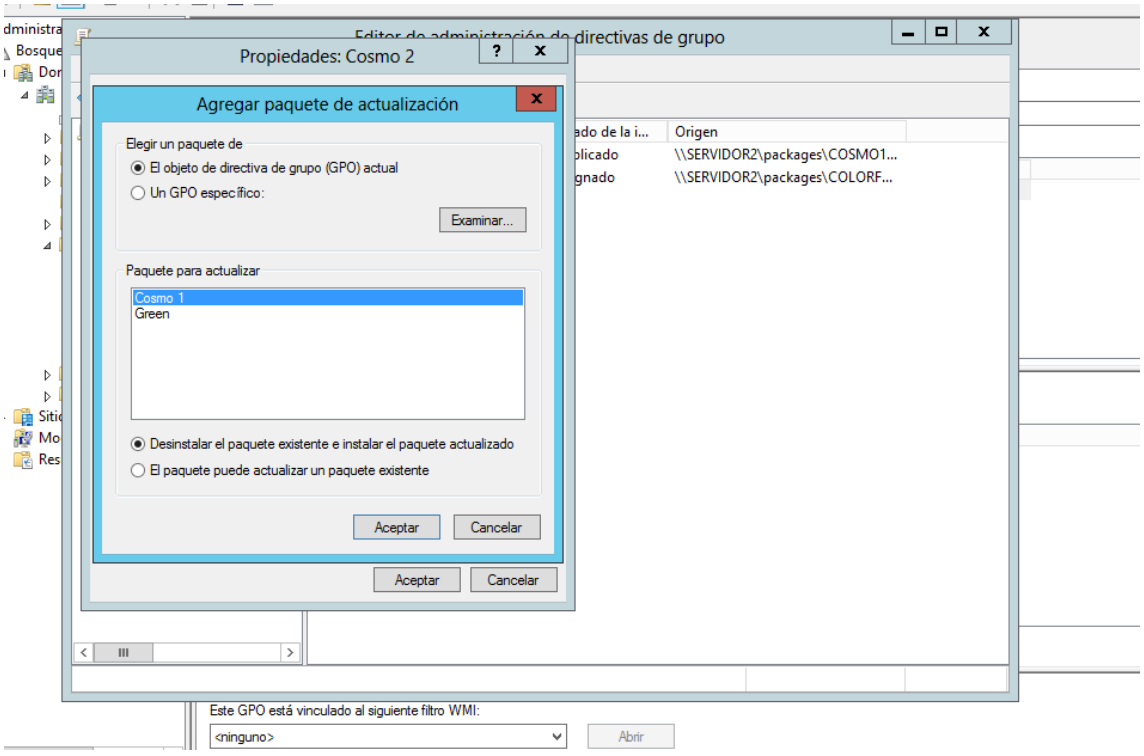


*Figura 138: Selección del paquete a actualizar y de los parámetros de actualización*

En la pestaña “Actualizaciones” del cuadro de diálogo Propiedades de Cosmo2, marcamos la opción “Actualización necesaria para paquetes existentes” y cerramos el diálogo pulsando Aceptar. Ahora Cosmo2 aparece como Publicado y Requerido.

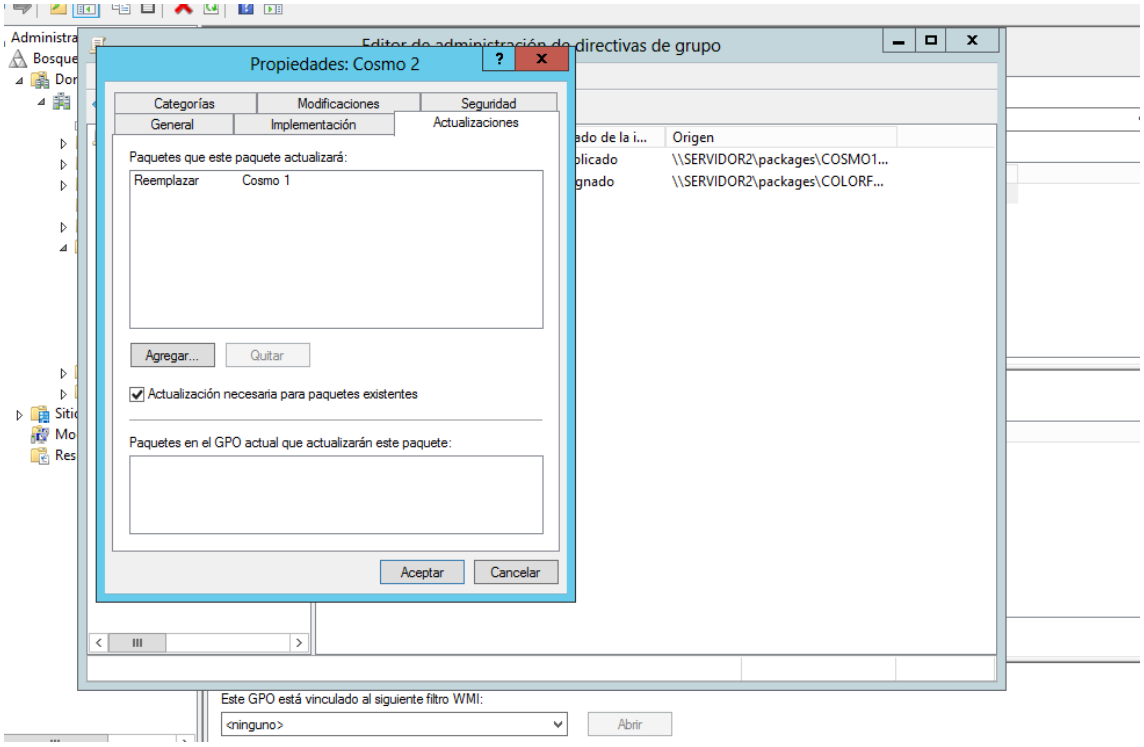


*Figura 139: Se fuerza la actualización del paquete*

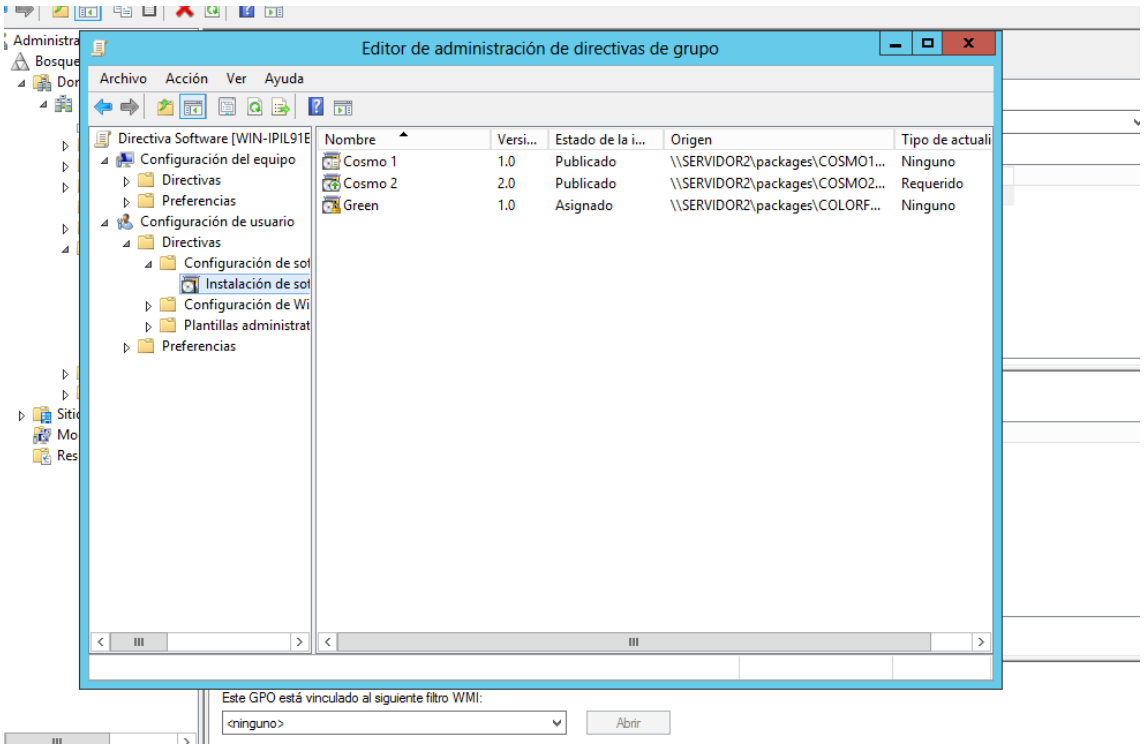


*Figura 140: Cosmo 2 aparece como Publicado y Requerido*

Seguidamente, realizamos un proceso similar con el paquete RED, solo que esta vez queremos que la actualización sea opcional. Para ello, en el cuadro de diálogo “Agregar paquete de actualización” seleccionaremos la segunda opción, y en la pestaña Actualizaciones de Propiedades de Red, no marcaremos la opción “Actualización necesaria para paquetes existentes”.

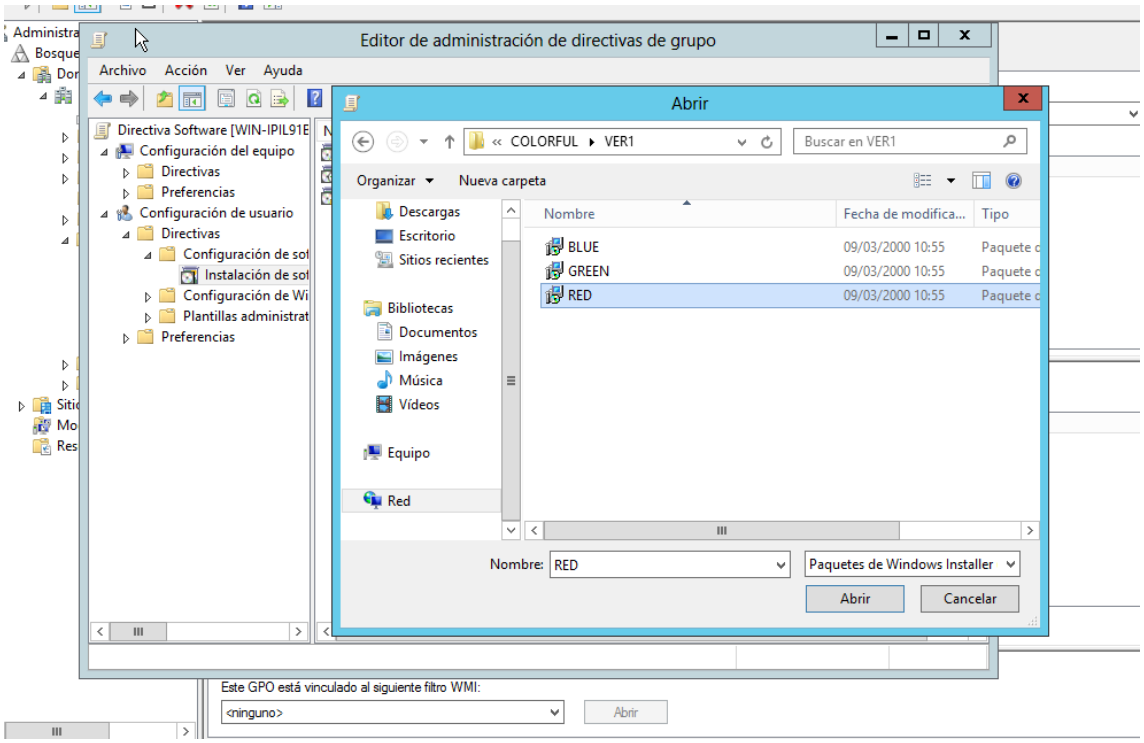


*Figura 141: Selección del paquete RED*

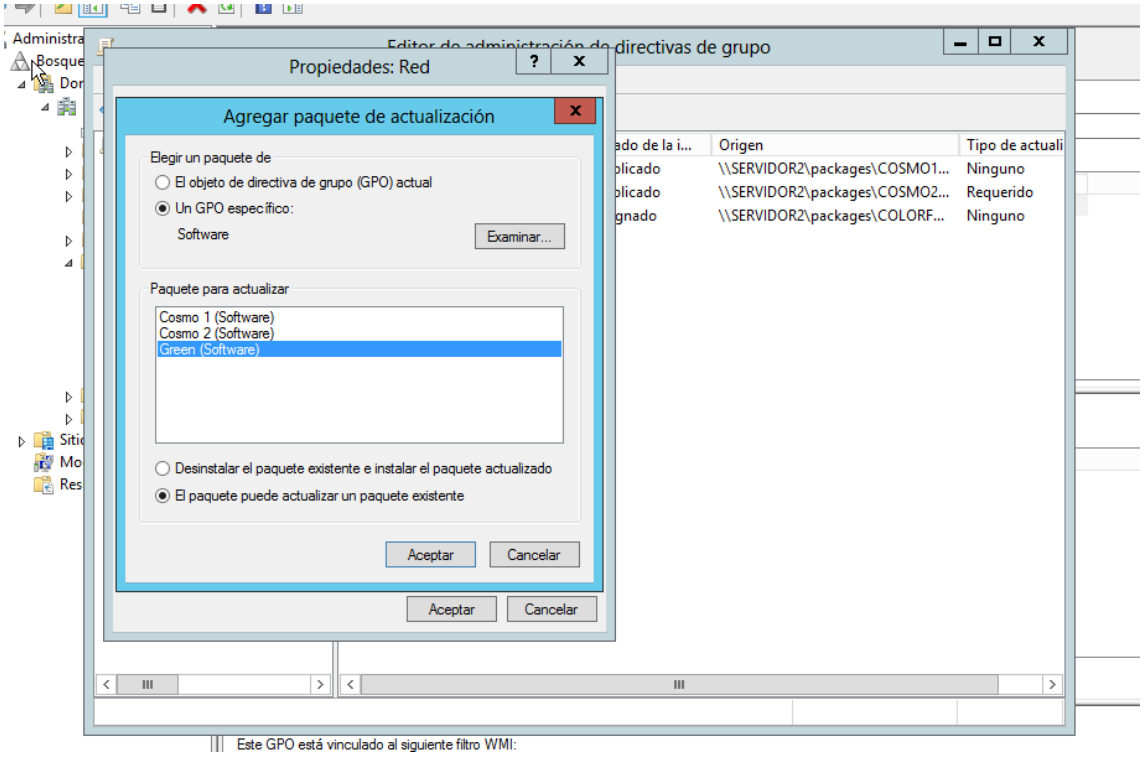


*Figura 142: Selección del paquete a actualizar y del modo de actualización*

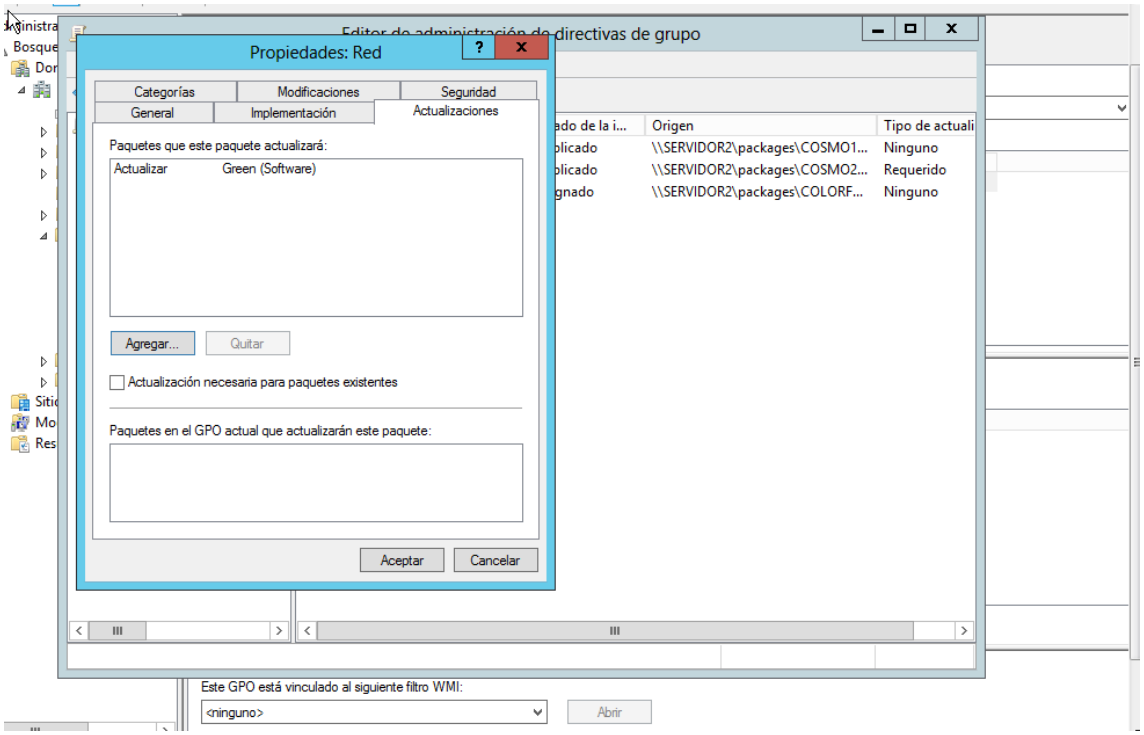


*Figura 143: No se fuerza la actualización*

Como se observa en la siguiente figura, Red aparece como Publicado y Opcional.

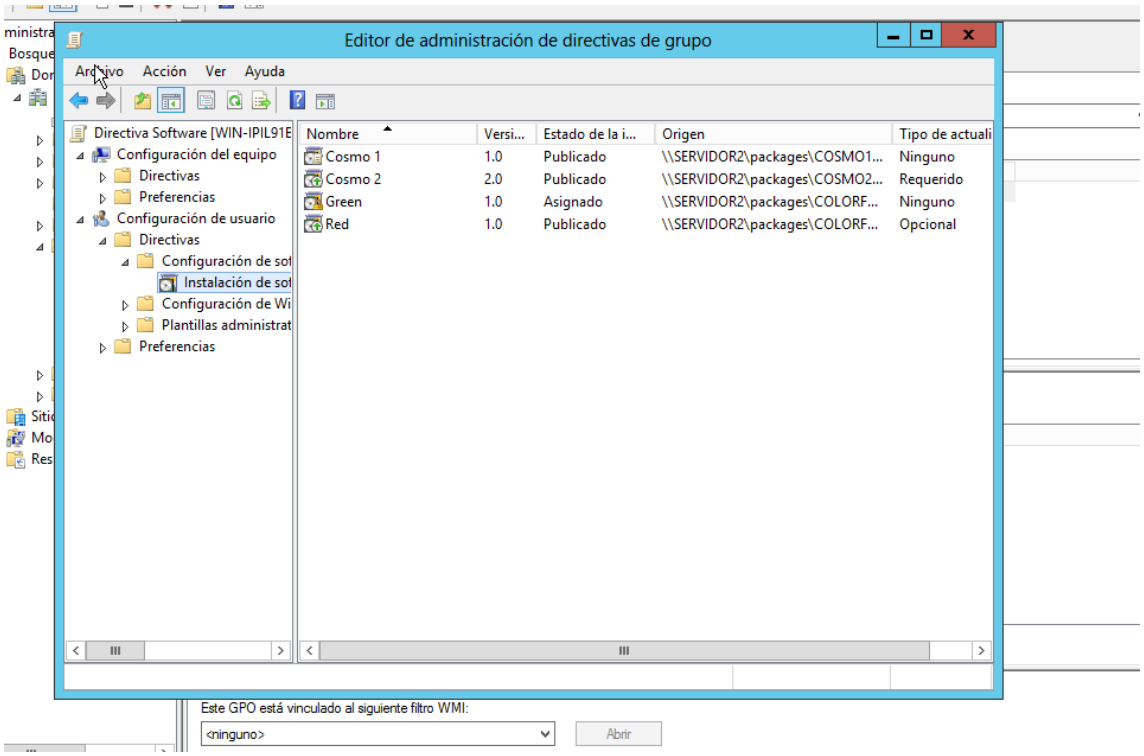


*Figura 144: Red como Publicado y Opcional*

Una vez ya han sido configuradas, iniciamos sesión en cualquiera de los equipos del dominio y con cualquiera de los usuarios de las OUs a las que está vinculado el GPO.

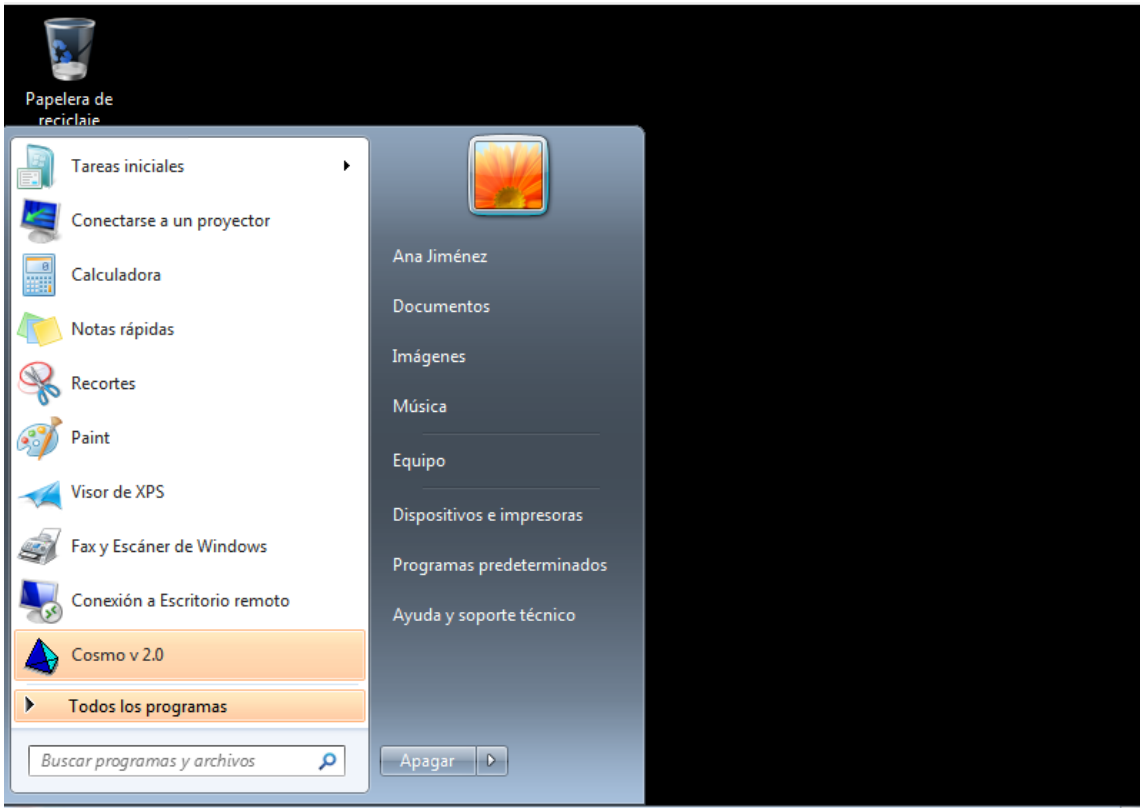


*Figura 145: Cosmo2 en la lista de Programas*

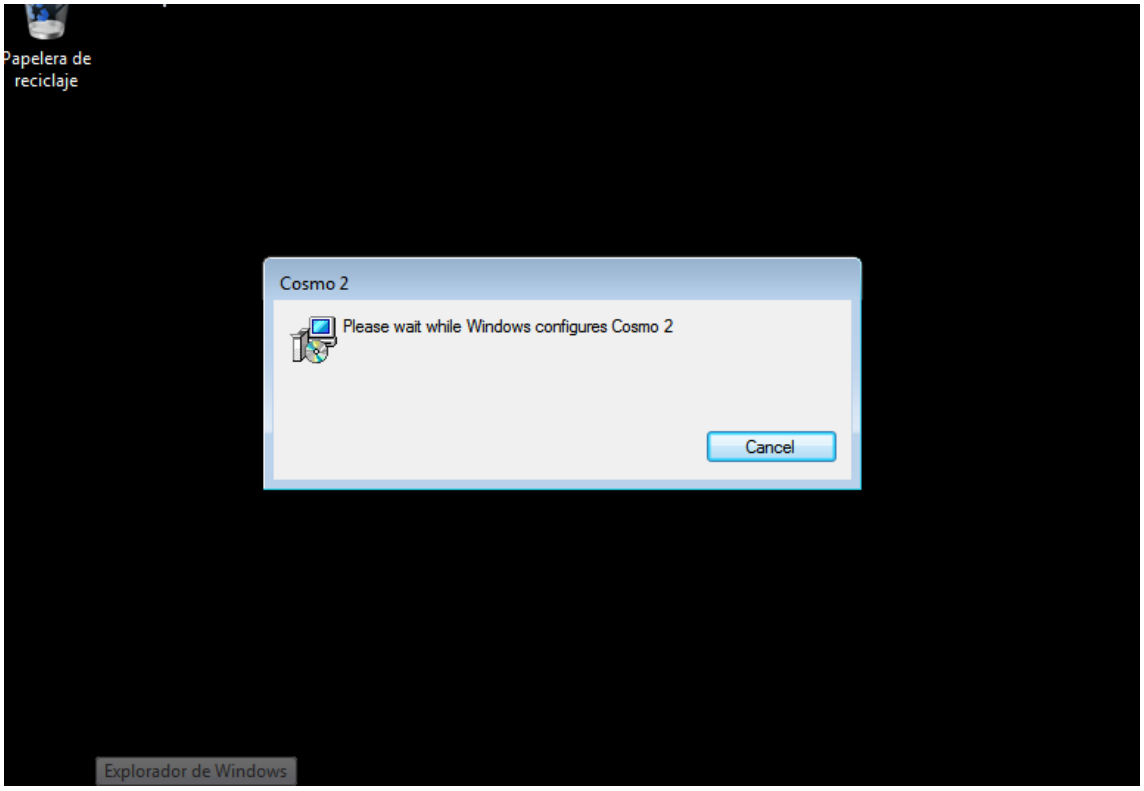


*Figura 146: Configuración del programa al ejecutarlo*

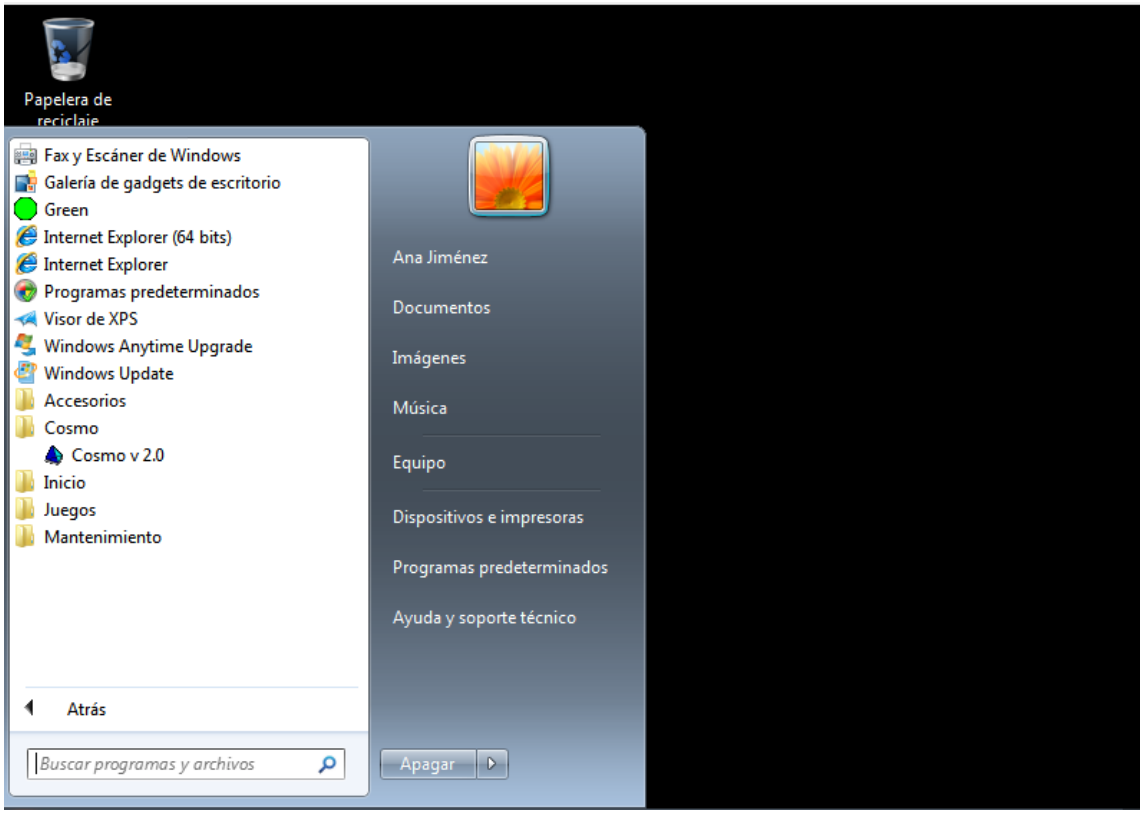


*Figura 147: Cosmo 1 ya no aparece en la lista de programas*

Como se puede observar en las figuras anteriores, Cosmo 2 se instala automáticamente en el equipo, reemplazando a Cosmo 1 tal y como se ha definido en el GPO.

Ahora, cerramos sesión e iniciamos la sesión con uno de los usuarios de Desarrollo, ya que la actualización a Red deberá hacerse mediante el Panel de Control.

En Panel de Control, seleccionamos Instalar un programa de la red, y una vez allí, seleccionamos Red y pulsamos Instalar.

Una vez red se ha instalado, podemos ver que Red ya aparece en Programas, y que Green sigue instalado y se puede seguir utilizando con total normalidad.

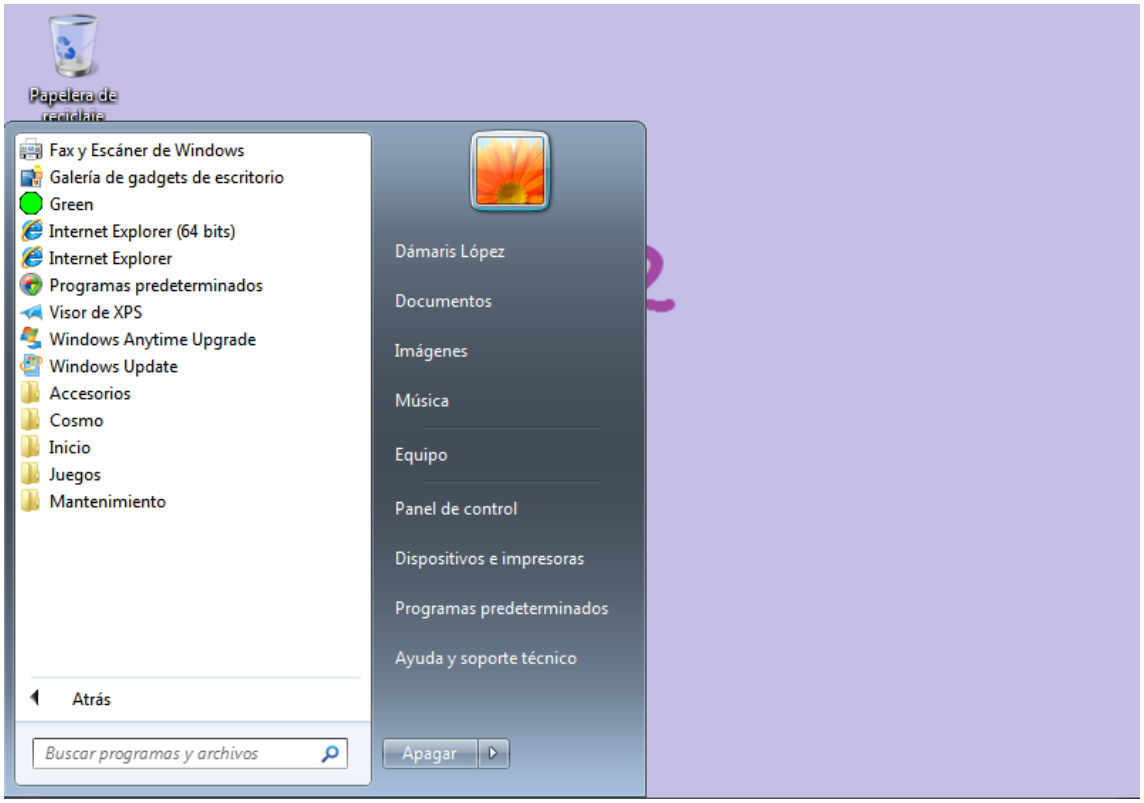


*Figura 148: Red no aparece en Programas*

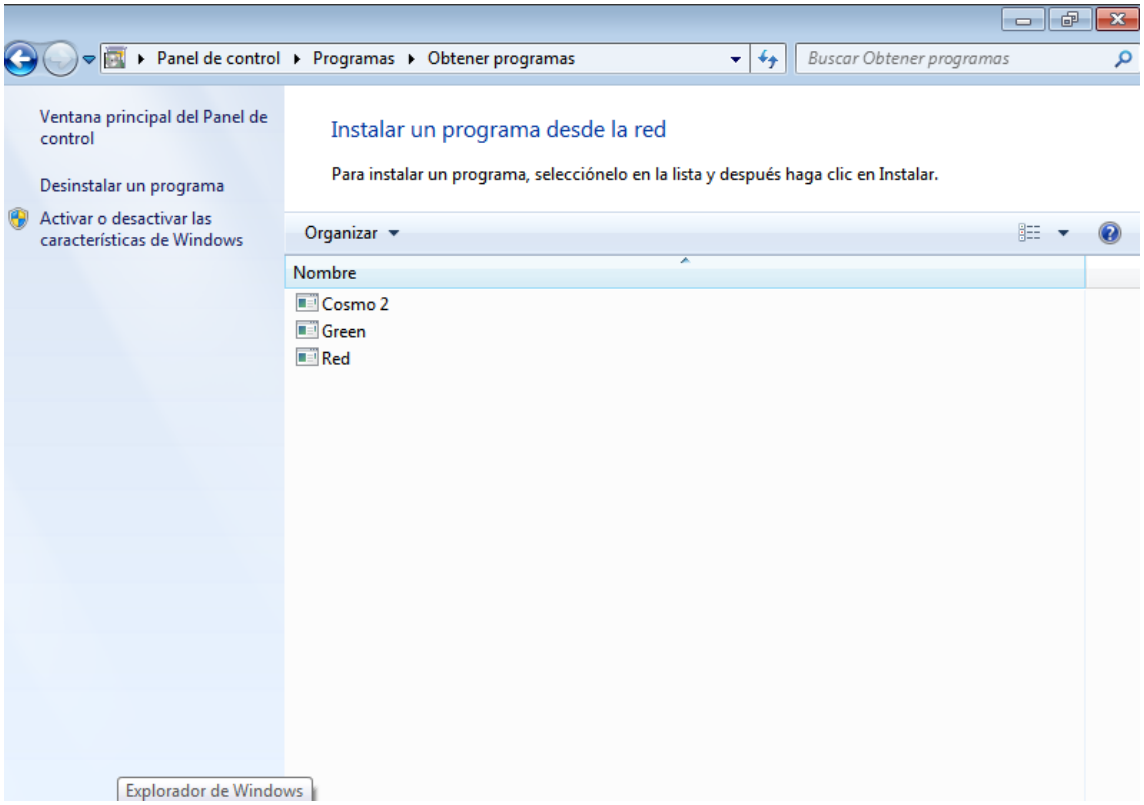


*Figura 149: Instalación de Red*

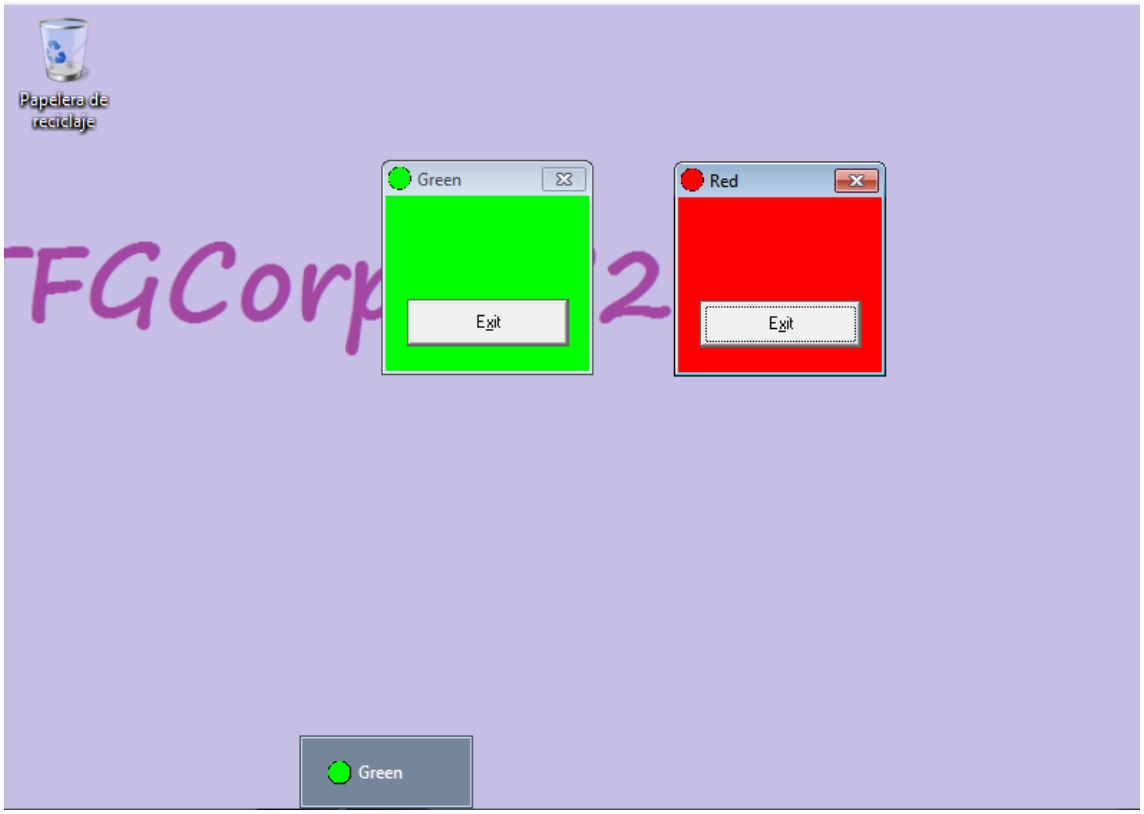


*Figura 150: Green no se borra al instalar Red*

Una vez finalizada la configuración de las tareas de actualización y las pruebas de que dicha configuración se ha aplicado correctamente, nos disponemos a establecer directivas de eliminación de software.

Para ello, hacemos clic derecho sobre Cosmo2 y en el menú “Todas las tareas” seleccionamos la opción Quitar, abriéndose un nuevo diálogo con dos opciones de eliminación “Desinstalar inmediatamente el software de usuarios y equipos” y “Permitir a los usuarios seguir utilizando el software pero impedir nuevas instalaciones”. Como queremos realizar una eliminación inmediata del programa, seleccionamos la primera opción. Al pulsar Aceptar se cierra el asistente y vemos como Cosmo2 ya no está en la lista de aplicaciones.

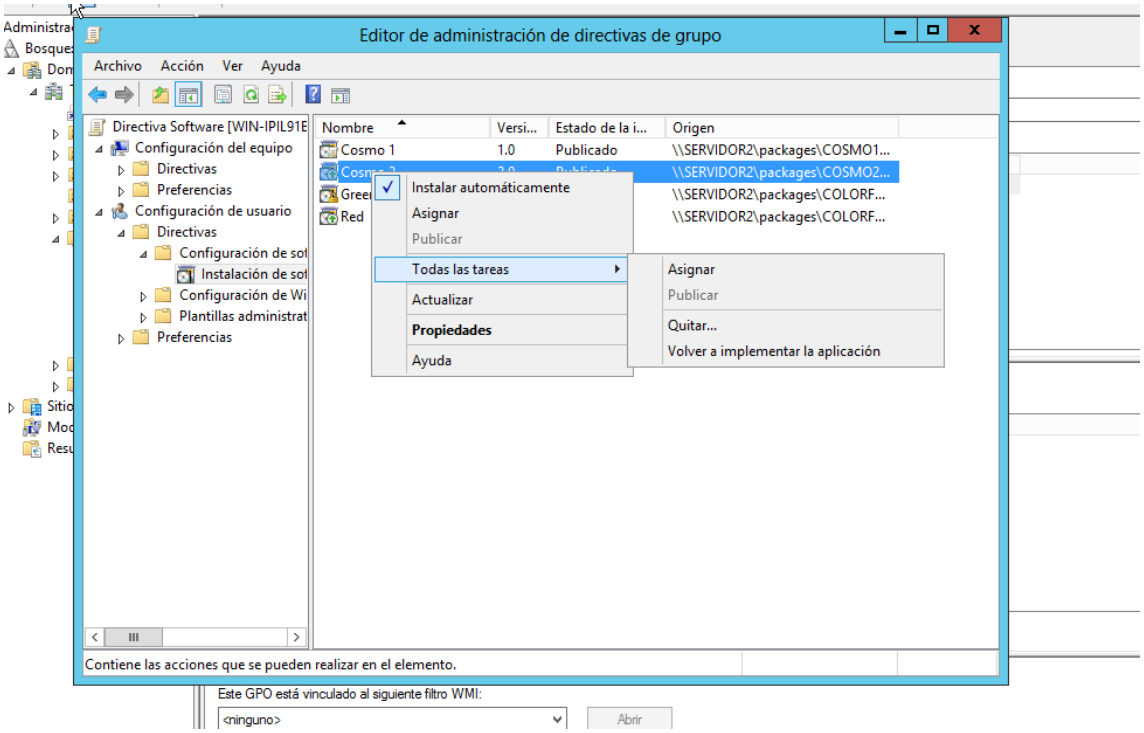


*Figura 151: Eliminación de Cosmo2*

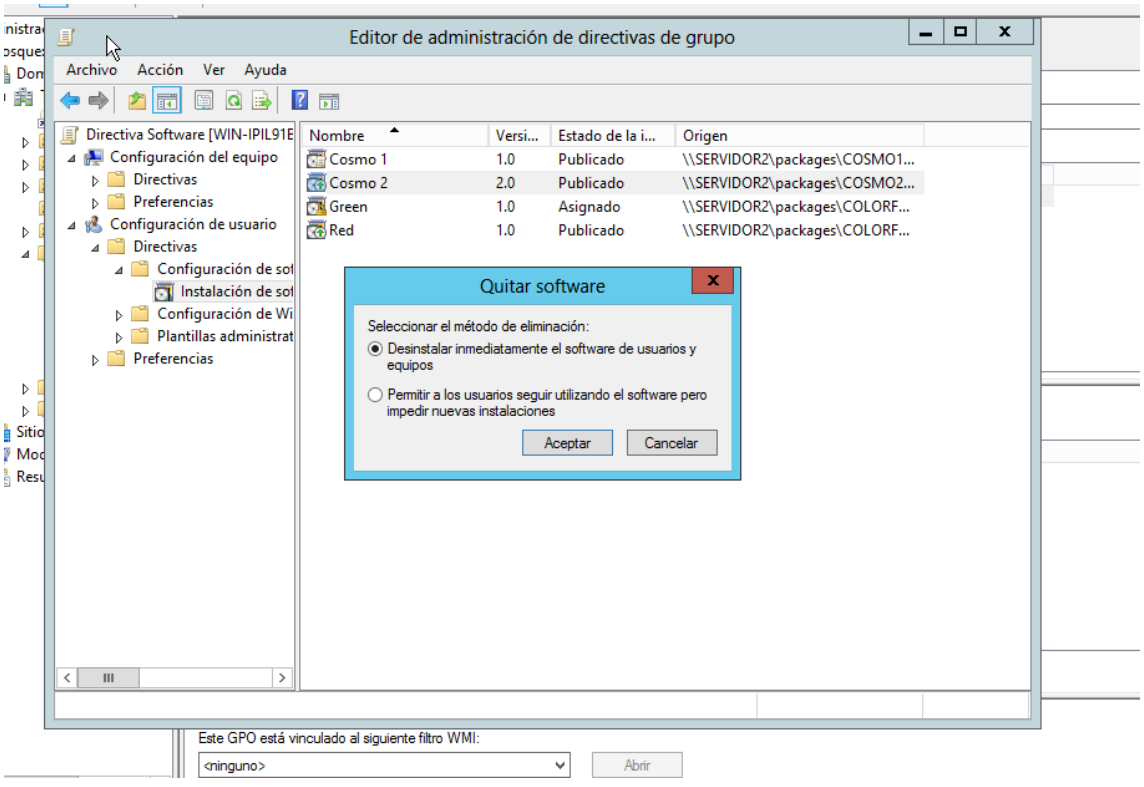


*Figura 152: Opciones de la eliminación de software*

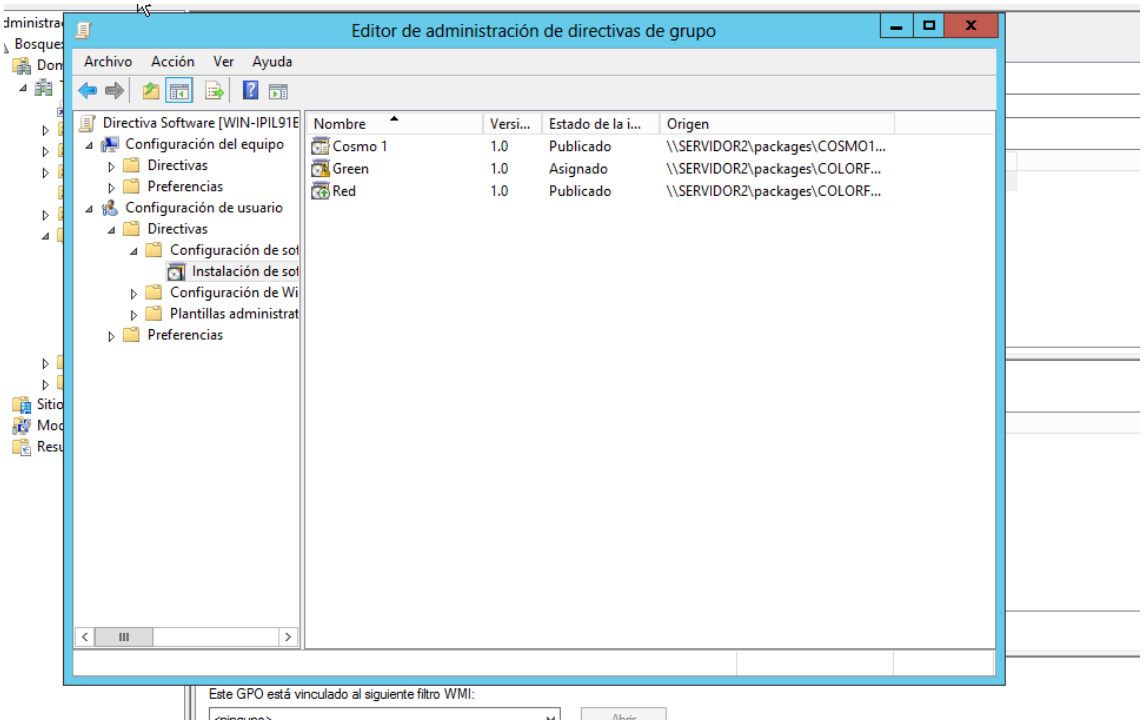


*Figura 153: Cosmo2 ya no aparece en la lista de aplicaciones*

A continuación, realizaremos un proceso similar con Green, solo que en este caso, seleccionaremos la segunda opción.

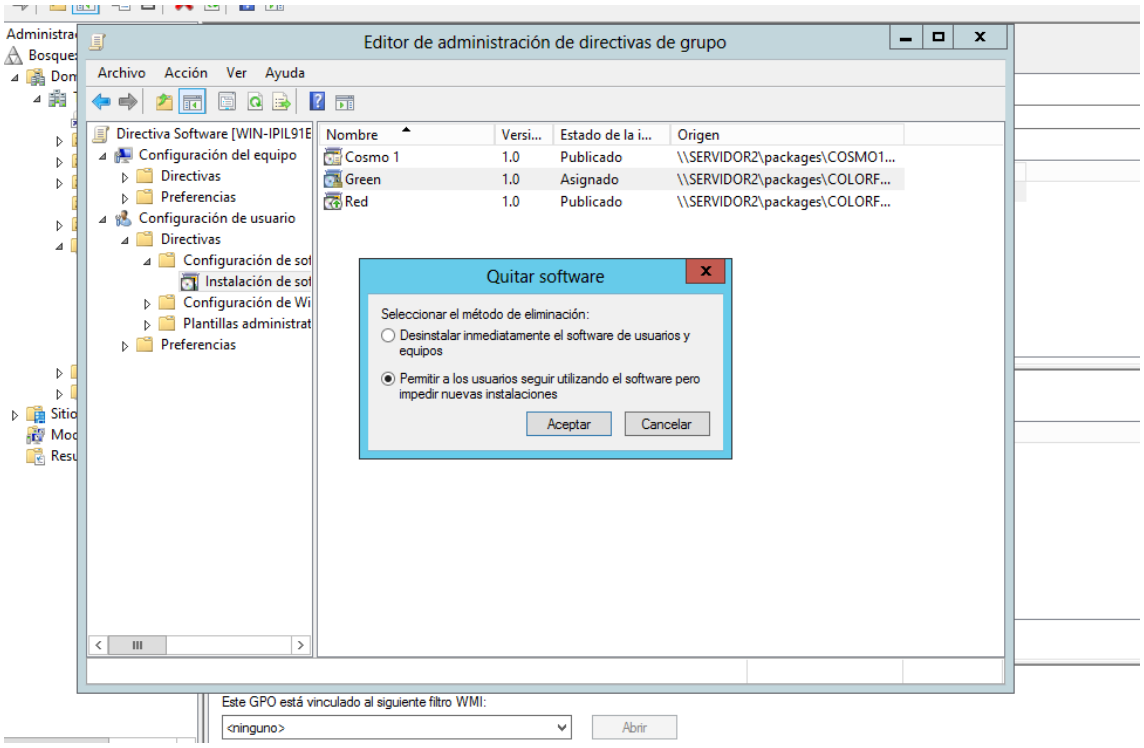


*Figura 154: Eliminación de Green*

Como se puede observar en la siguiente figura, Green también desaparece de la lista de aplicaciones.

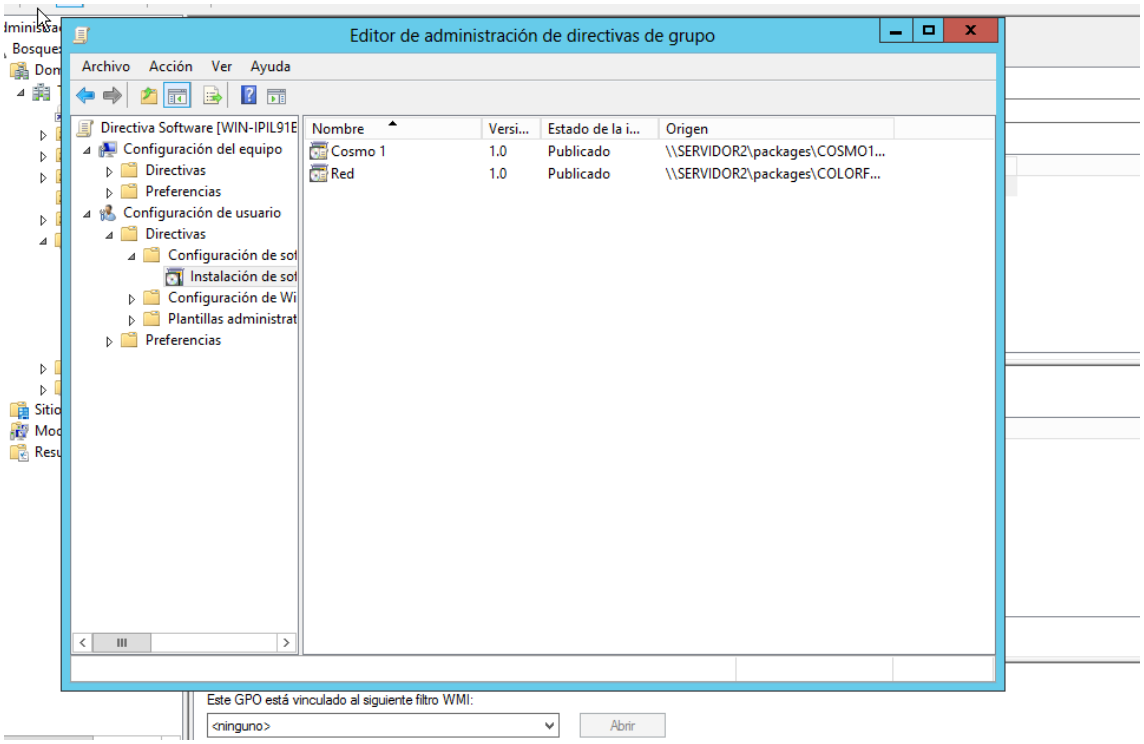


*Figura 155: Green ya no aparece en la lista de aplicaciones*

Para comprobar si se han aplicado las directivas correctamente, iniciamos sesión en uno de los equipos con un usuario que tuviera las dos aplicaciones instaladas, como se puede observar Cosmo2 ha desaparecido, sin embargo Green sigues estando disponible para su uso

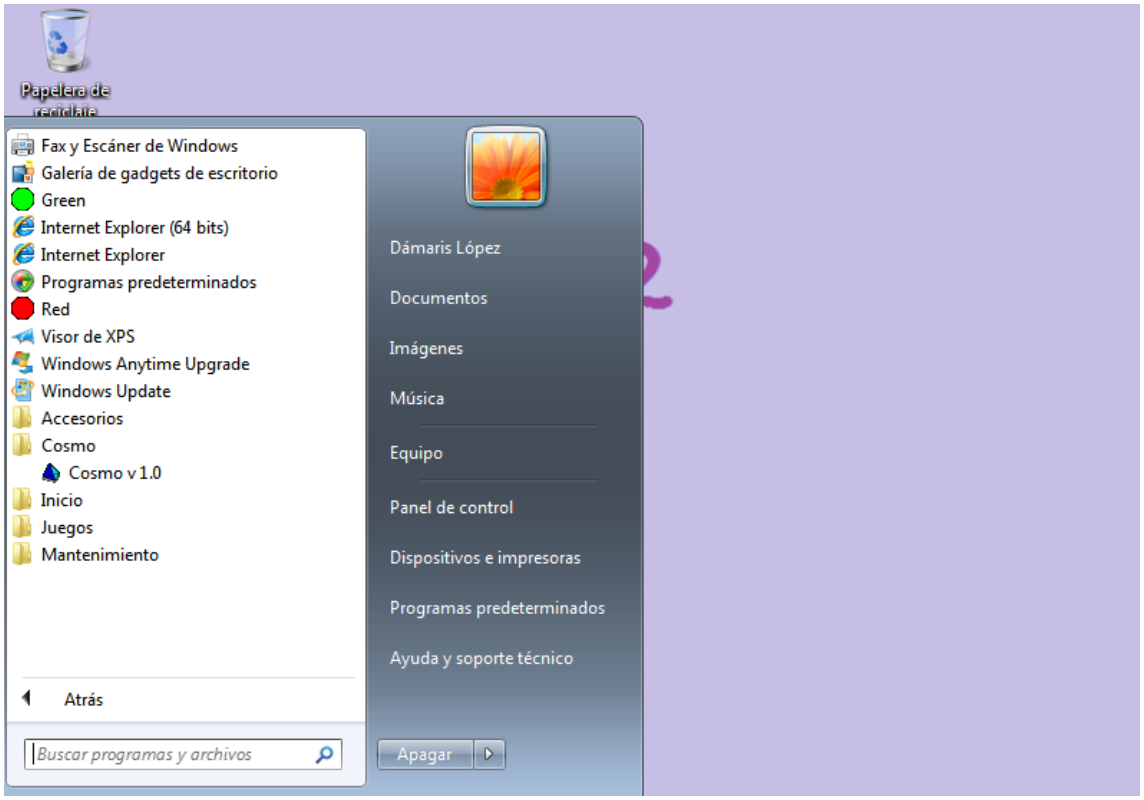


*Figura 156: Estado final de las aplicaciones*

Sin embargo, si nos conectamos con un usuario en el que no se había instalado la aplicación Green, veremos que no nos aparece en Programas.

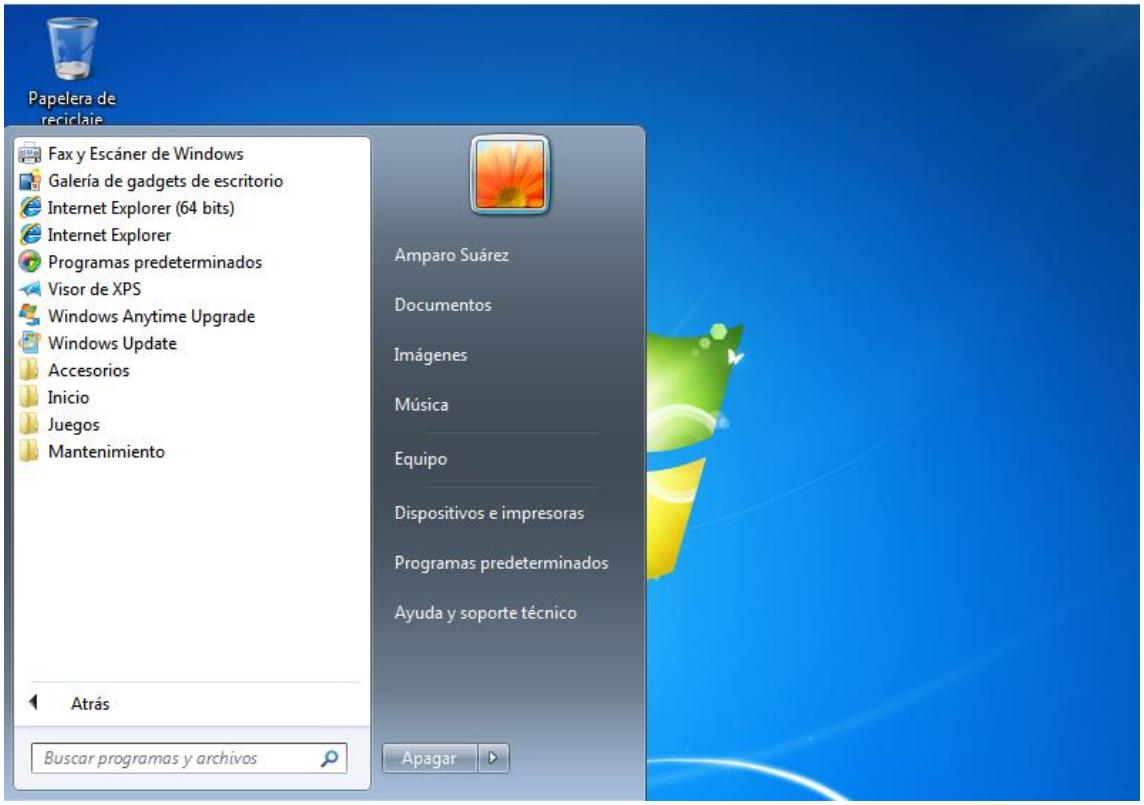


*Figura 157: Green no aparece en Programas*

### *4.2.2.3 Directivas de Seguridad*

Utilizando las plantillas de seguridad podemos definir la seguridad del sistema, todo lo referente a contraseñas, inicios de sesión, logs, mensajes, etc.

Para ello, el primer paso será abrir la consola de Herramientas administrativas y abrir "Directiva de seguridad local". En "Configuración de seguridad" seleccionaremos "Exportar Directiva" y la guardaremos en la ruta predeterminada con el nombre de nuestro servidor principal. Esto nos permitirá recuperar la configuración de seguridad inicial de ser necesario.

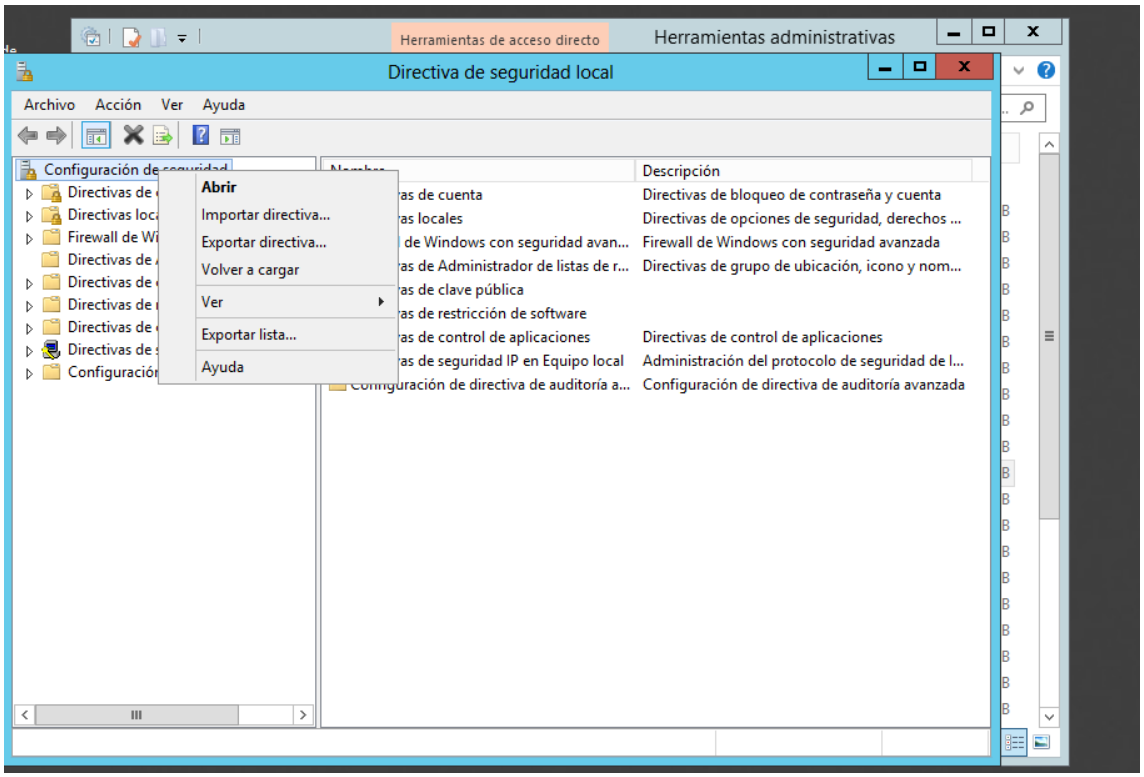


*Figura 158: Exportar la directiva de seguridad*

A continuación, seleccionamos en el menú inicio “Ejecutar” y abrimos una consola mmc. En el menú Archivo seleccionaremos la opción “Agregar o quitar complemento” y en el nuevo diálogo que se abrirá, seleccionaremos la opción “Plantillas de seguridad” en la lista de “Complementos disponibles”.

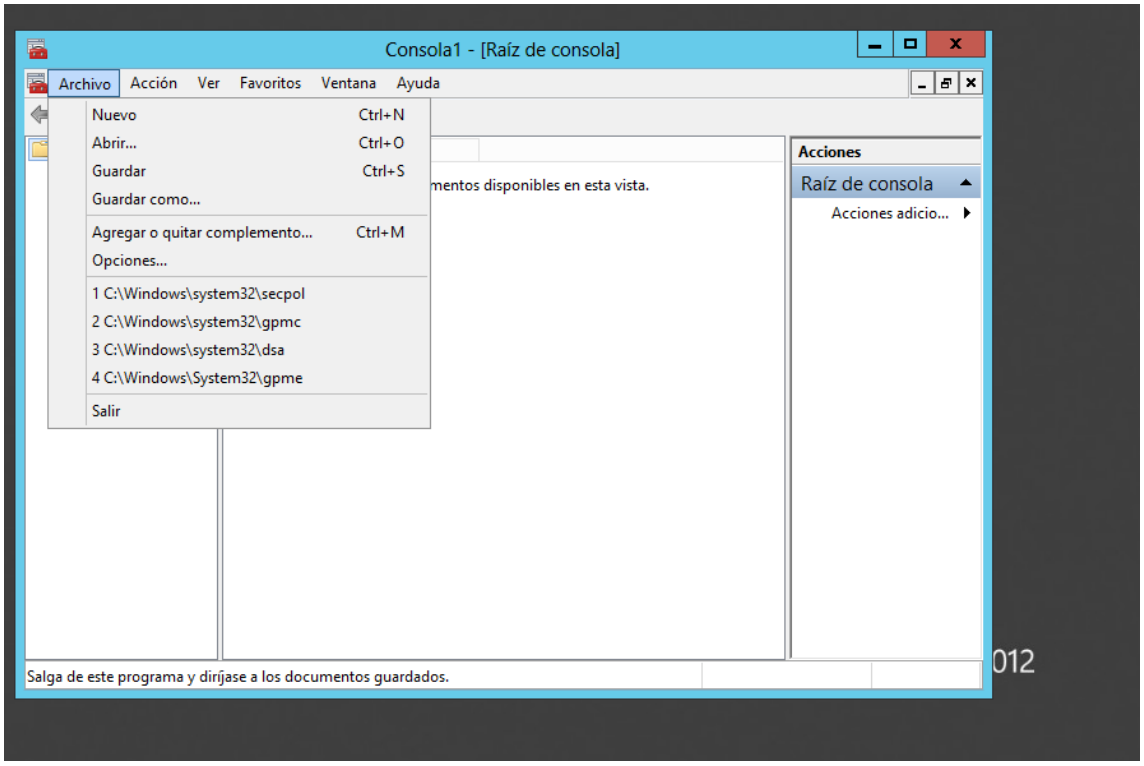


*Figura 159: Consola mmc*

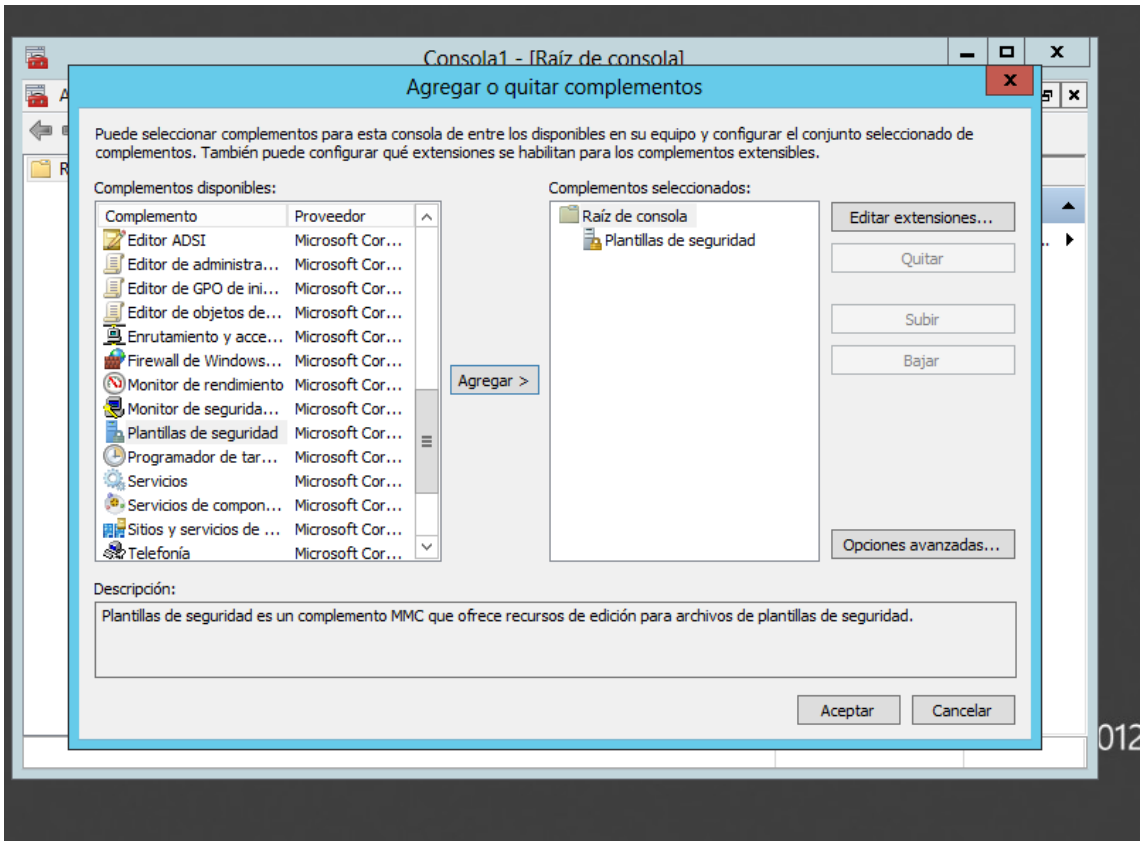


*Figura 160: Agregar complemento Plantillas de seguridad*

A continuación, guardamos la nueva consola como Plantillas de seguridad.

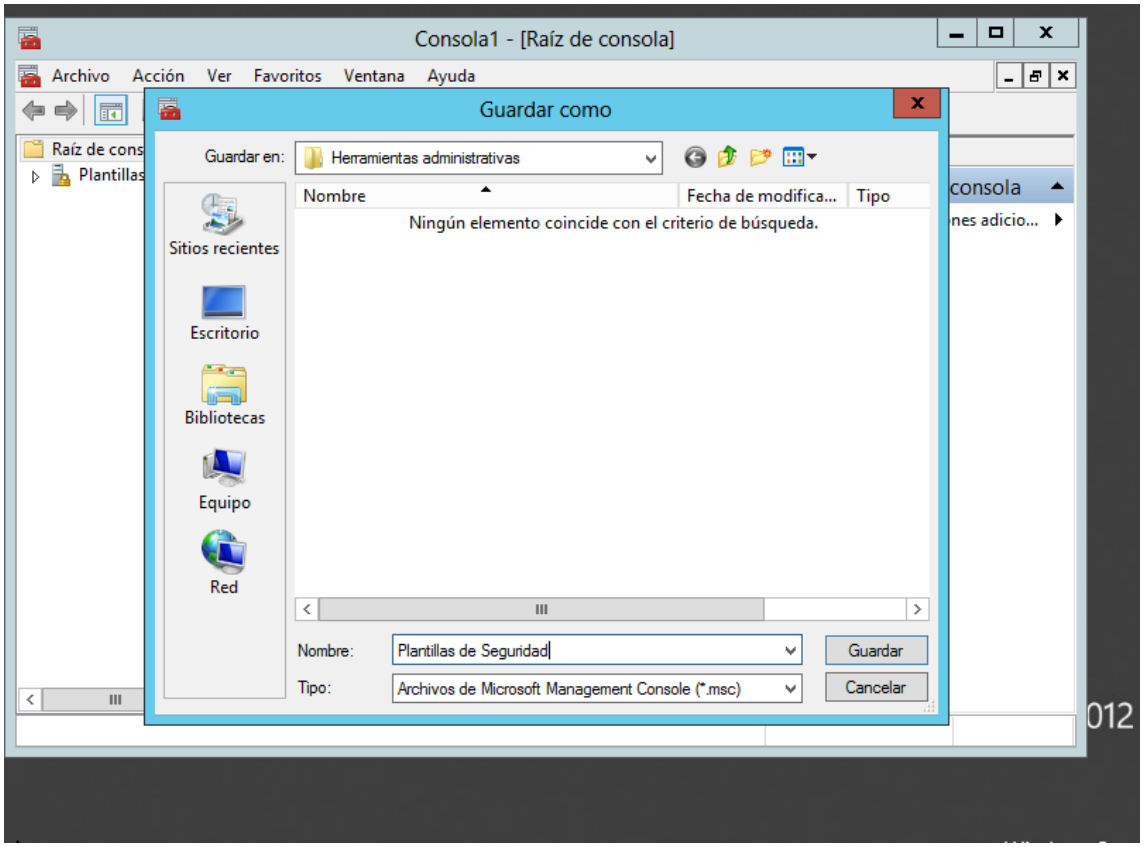


*Figura 161: Guardar la consola*

El siguiente paso a seguir, será crear un nuevo grupo global de seguridad, al que llamaremos WIN-IPIL91B81CSRestringido, donde WIN-IPIL91B81CS es el nombre de nuestro servidor principal, en el que vamos a crear las directivas de seguridad.

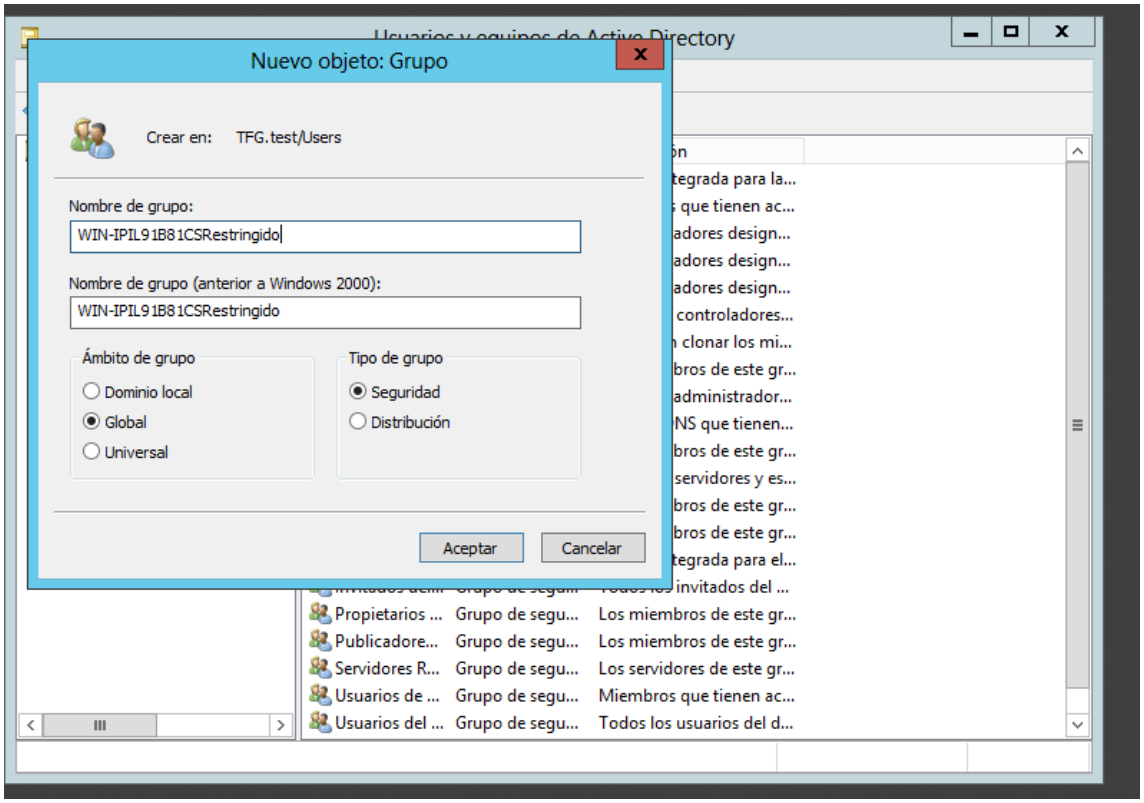


*Figura 162: Creación del grupo de seguridad*

A continuación, en la consola Plantillas de seguridad que acabamos de crear, expandimos el módulo Plantillas de seguridad y seleccionamos la plantilla de nombre WIN-IPIL91B81CS que hemos creado antes.

Expandimos Directivas de cuenta, y seleccionamos Directiva de contraseñas. En el panel de detalles hacemos doble clic sobre “Longitud mínima de la contraseña” y, en el cuadro de diálogo “Configuración de la directiva de seguridad en la plantilla” comprobamos que la opción “Definir esta configuración de la directiva en la plantilla” está seleccionada, a continuación escribimos 10 en el cuadro de texto, forzando así que la longitud mínima de las contraseñas sea esa y hacemos clic en Aceptar.

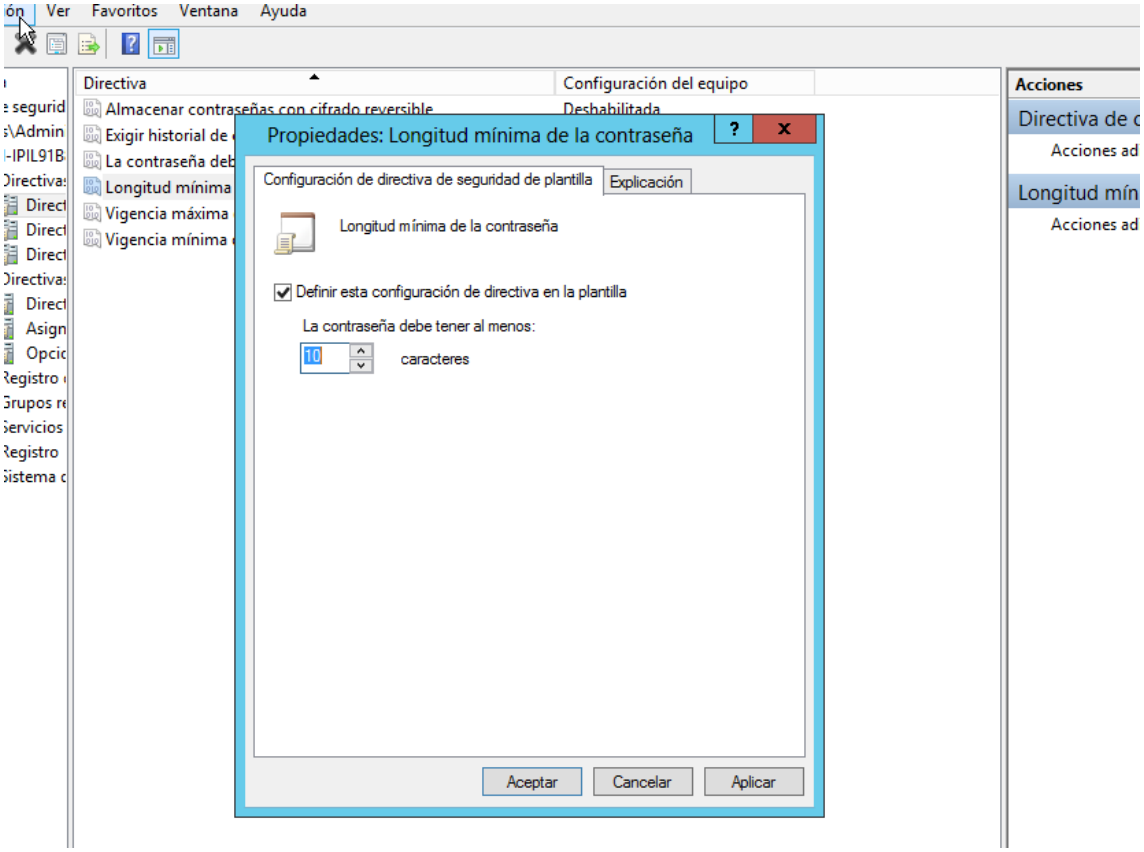


*Figura 163: Longitud mínima de la contraseña*

Ahora, expandimos Directivas locales y seleccionamos en el panel de detalles "Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión", nos aseguramos de que la opción "Definir esta configuración de directiva en la plantilla está seleccionada" y escribimos en el cuadro de texto "Sólo acceso autorizado". A continuación seleccionamos "Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión", y en el cuadro de texto escribimos el nombre de nuestro equipo: WIN-IPIL91B81CS.

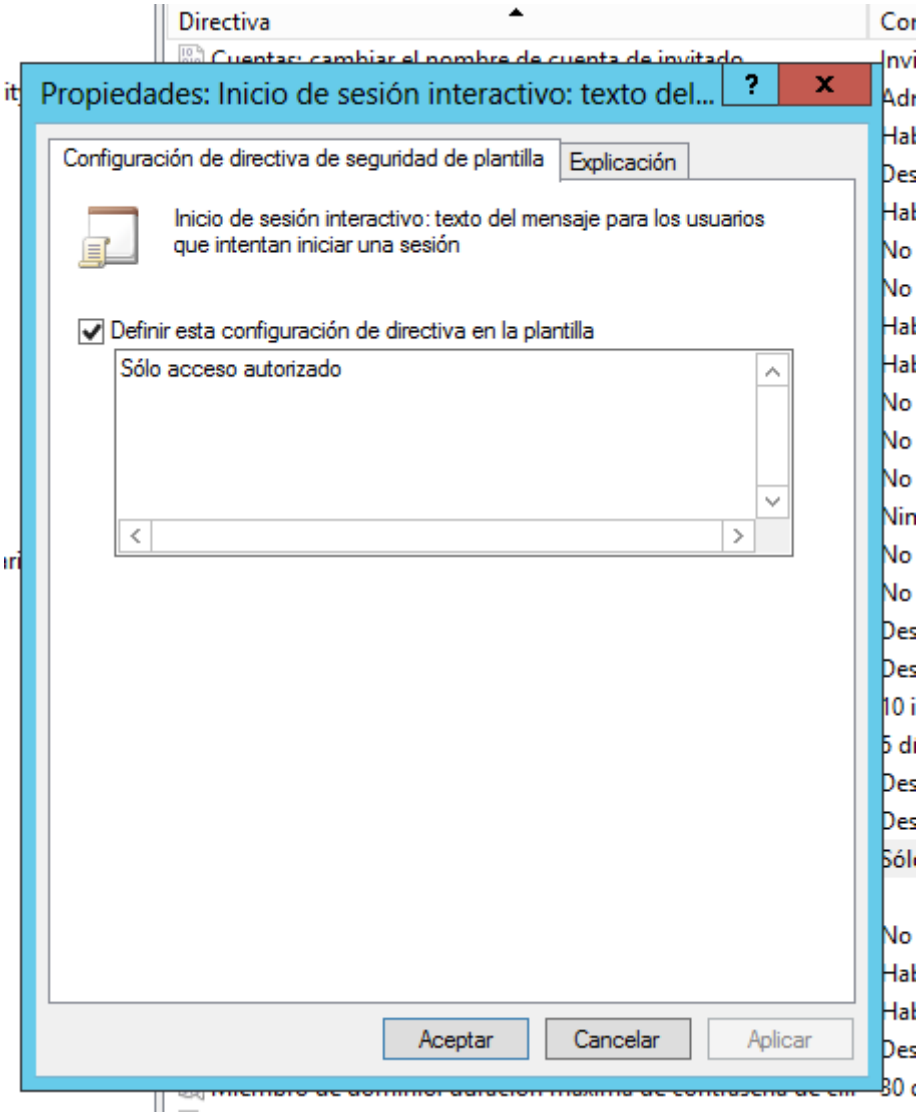


*Figura 164: Texto de inicio de sesión*

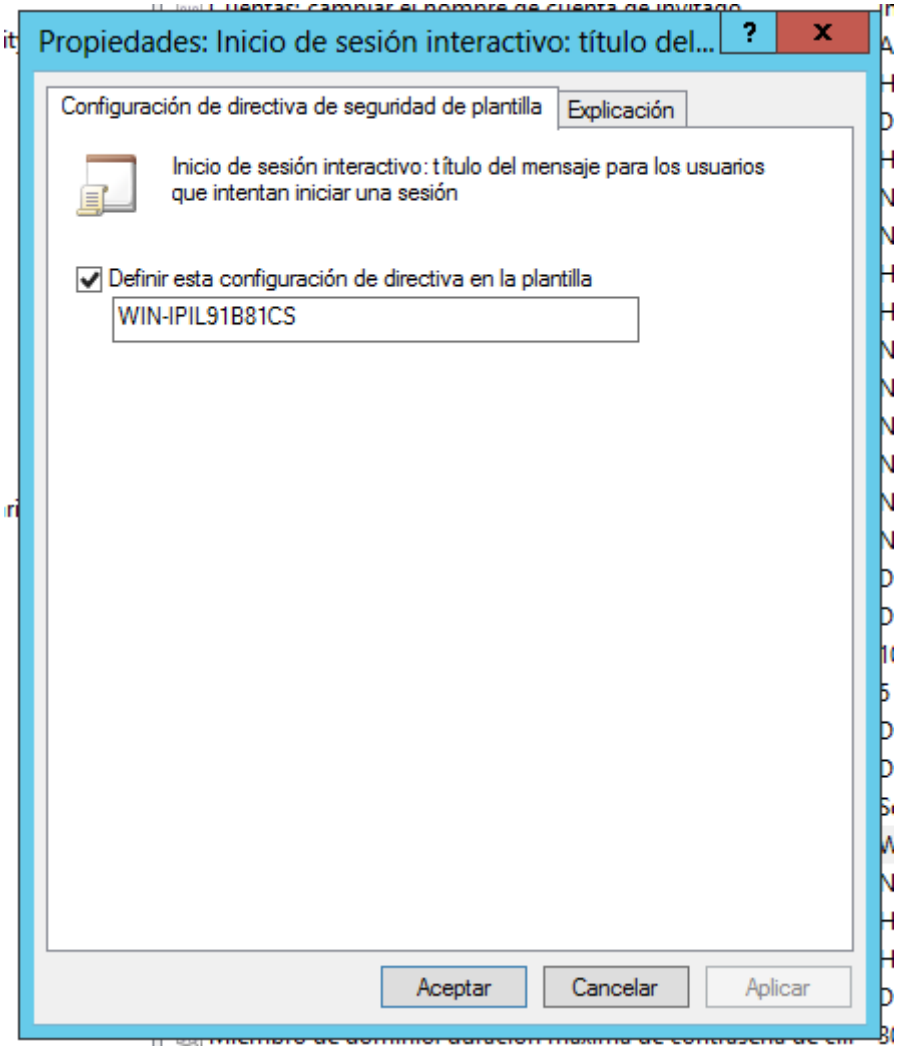


*Figura 165: Título de inicio de sesión*

Para implementar la configuración de seguridad del equipo, hacemos clic con el botón secundario del ratón sobre Grupos Restringidos, o hacemos doble clic sobre el mismo, y seleccionamos Agregar Grupo. En el nuevo diálogo clicamos sobre Examinar y nos aseguramos de que nuestro domino TFG.test está en el cuadro "Desde esta ubicación". Ahora hacemos clic en "Avanzadas", "Buscar ahora" y en los grupos seleccionamos nuestro grupo WIN-IPIL91B81CSRestringido, cerramos todas las ventanas abiertas pulsando Aceptar.

Seguidamente, añadiremos el usuario Administrador al grupo WIN-IPIL91B81CSRestringido, para ello, hacemos doble clic sobre el grupo, y en "Miembros de este grupo" seleccionamos "Agregar miembro". En el nuevo cuadro de diálogo hacemos clic en "Examinar", "Avanzadas", "Buscar ahora", comprobamos que el dominio TFG.test está en "Desde esta ubicación" y hacemos clic sobre Administrador para seleccionarlo como nuevo usuario del grupo. Nuevamente cerramos todas las ventanas pulsando Aceptar.

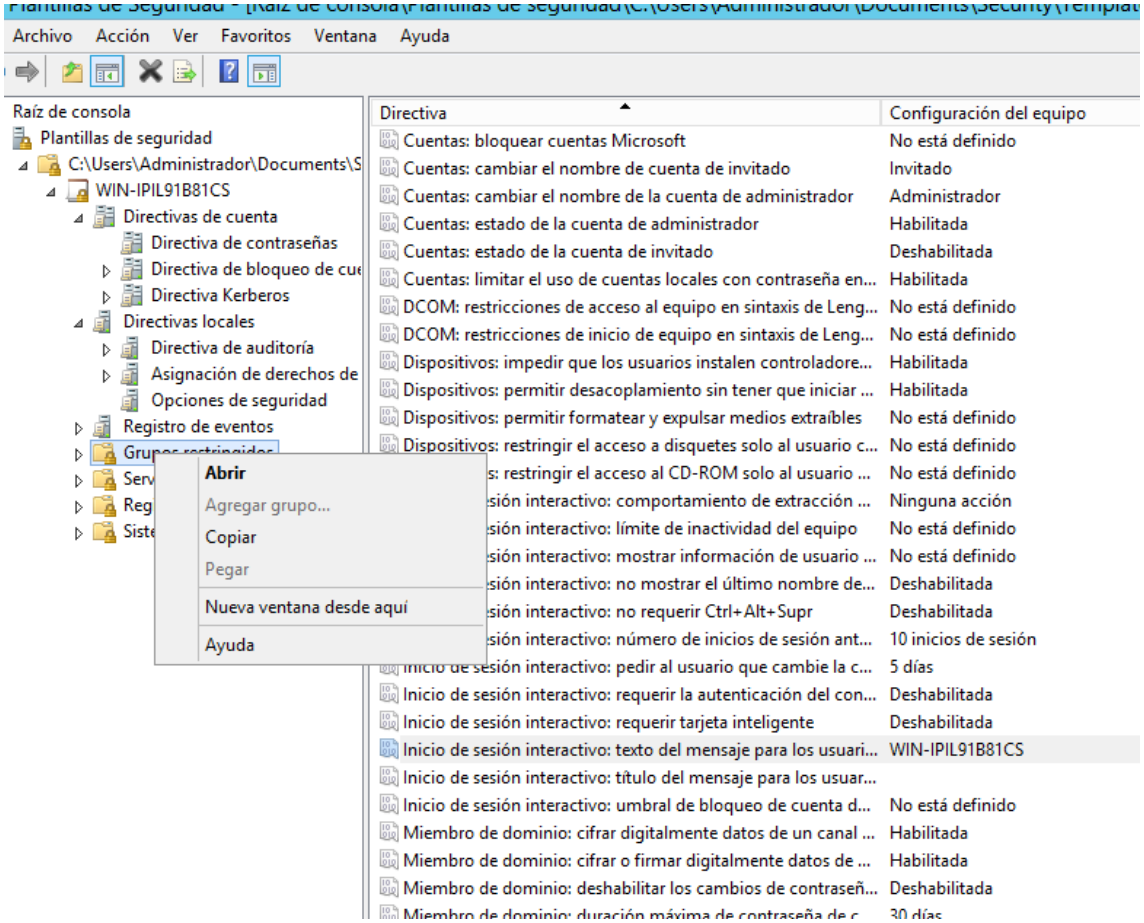


*Figura 166: Grupos restringidos*

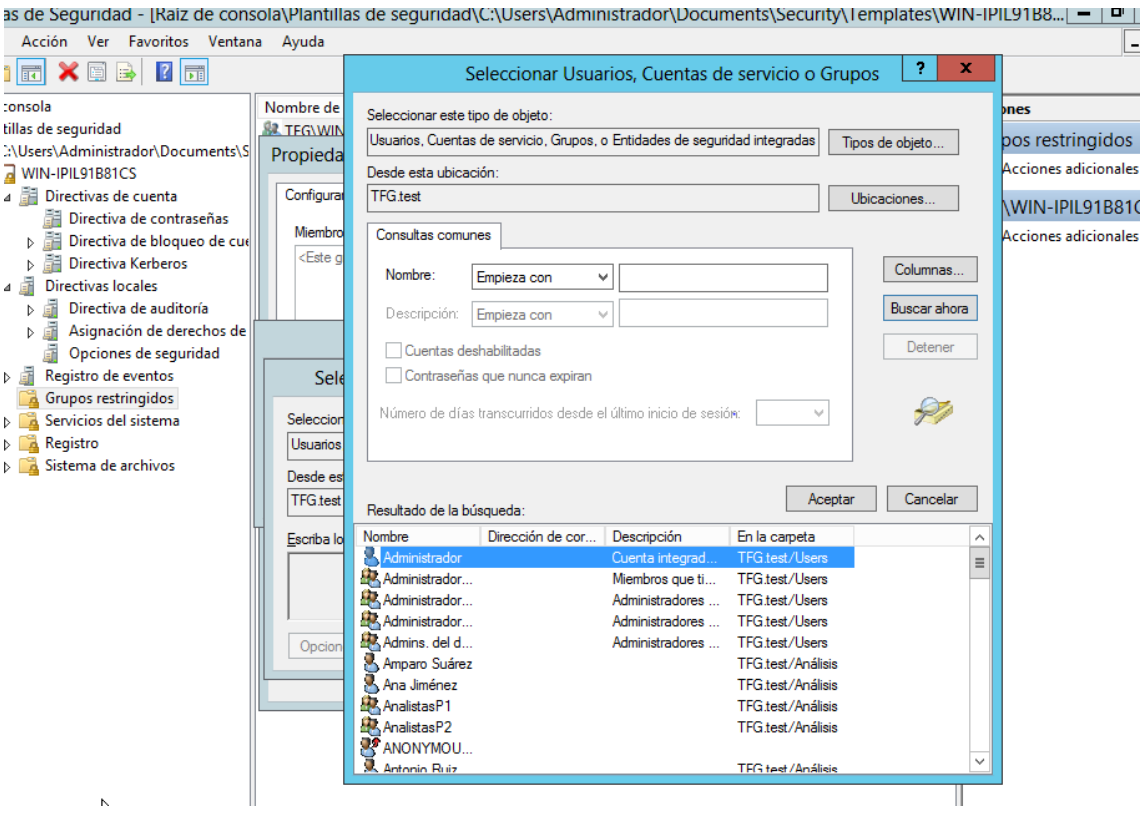


*Figura 167: Agregar Administrador a WIN-IPIL91B81CSRestringido*

A continuación, nos dirigimos a “Servicios del sistema” y seleccionamos Cliente DHCP.

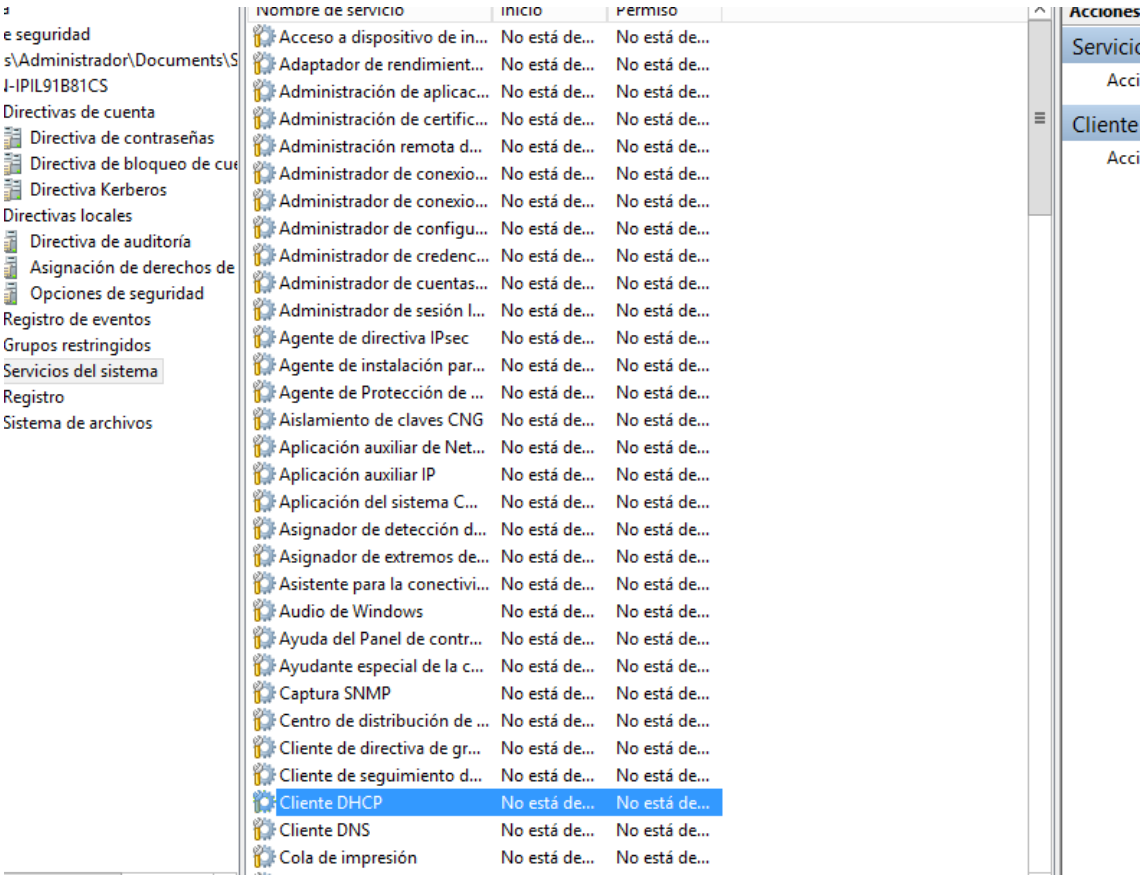


*Figura 168: Cliente DHCP*

Tras hacer doble clic, marcamos la opción “Definir esta configuración de directiva de plantilla” y marcamos el servicio como “Deshabilitado”.

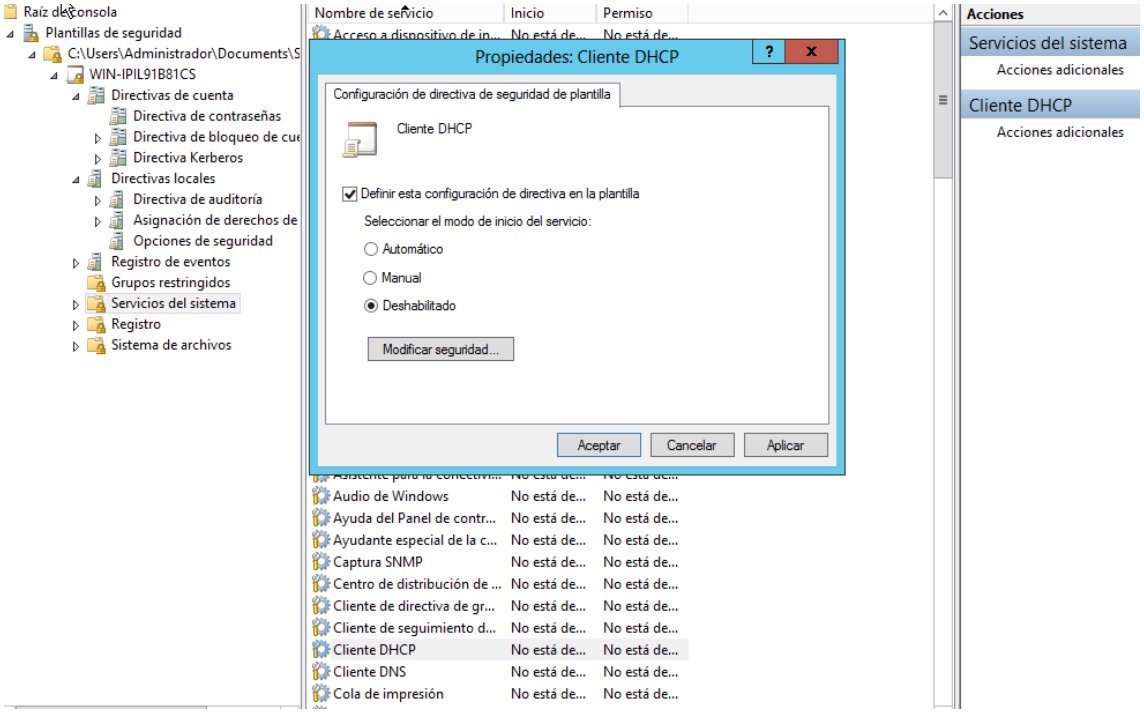


*Figura 169: Deshabilitar servicio DHCP*

Una vez se han configurado todos los cambios en la plantilla, la guardamos como una nueva plantilla, llamada WIN-IPIL91B81CSSeguro. Para ello hacemos clic con el botón derecho del ratón sobre nuestra plantilla y seleccionamos la opción Guardar como, introducimos el nombre de la nueva plantilla y pulsamos Guardar.

Ahora que ya está configurada y guardada nuestra nueva configuración de seguridad, nos disponemos a analizar la seguridad y a crear una base de datos para futuros análisis de seguridad.

Empezamos creando una nueva consola mmc como se ha visto anteriormente, a la que agregaremos el componente Configuración y análisis de seguridad.

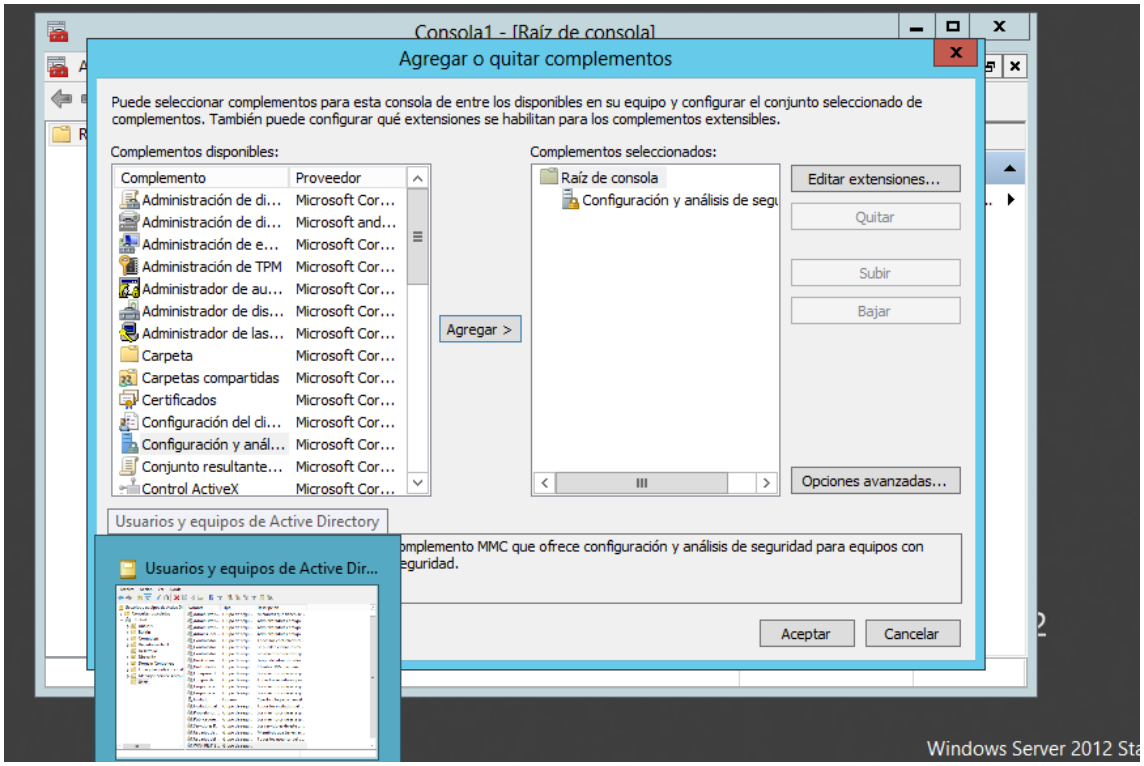


*Figura 170: Configuración y análisis de seguridad*

Seguidamente, haremos clic derecho sobre "Configuración y análisis de seguridad" y seleccionamos la opción "Abrir base de datos". En la ventana "Abir base de datos" escribimos WIN-IPIL91B81CSSeguro como nombre de la base de datos y, a continuación pulsamos nuevamente el botón Abrir.

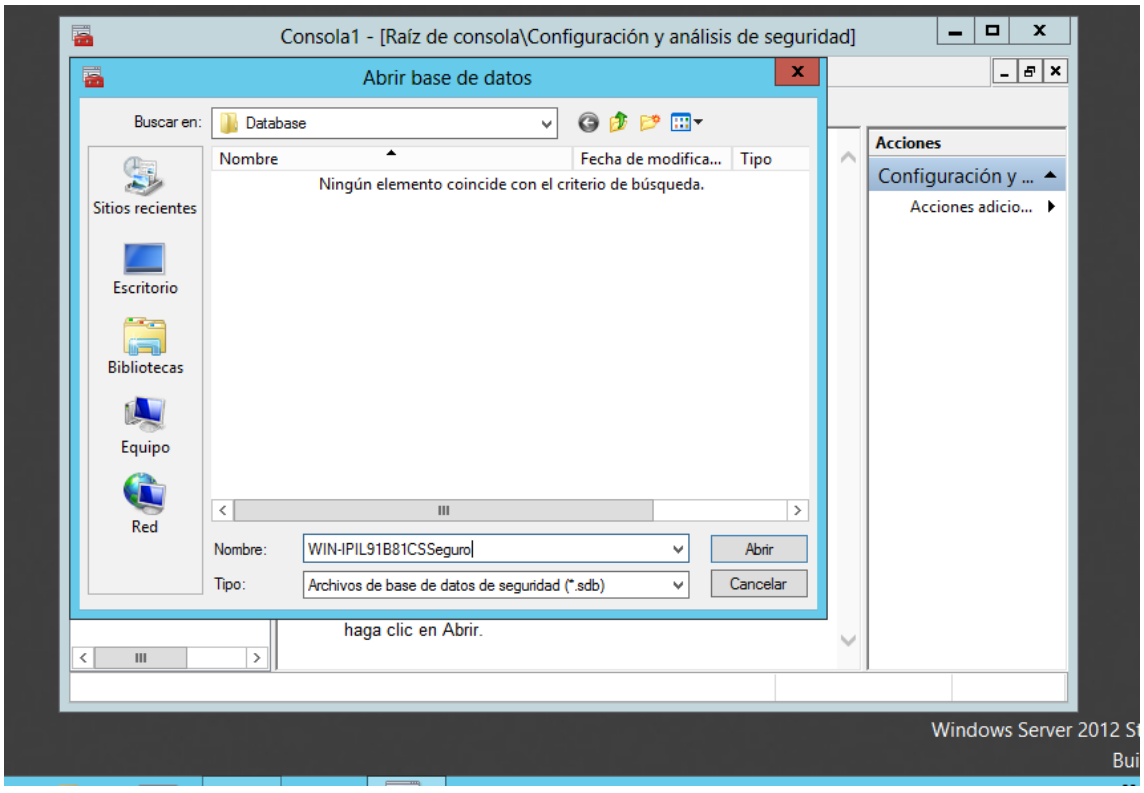


*Figura 171: Agregar base de datos*

Ahora el asistente nos pedirá una plantilla de seguridad, seleccionamos la plantilla que hemos modificado y guardado anteriormente y hacemos clic en Abrir.

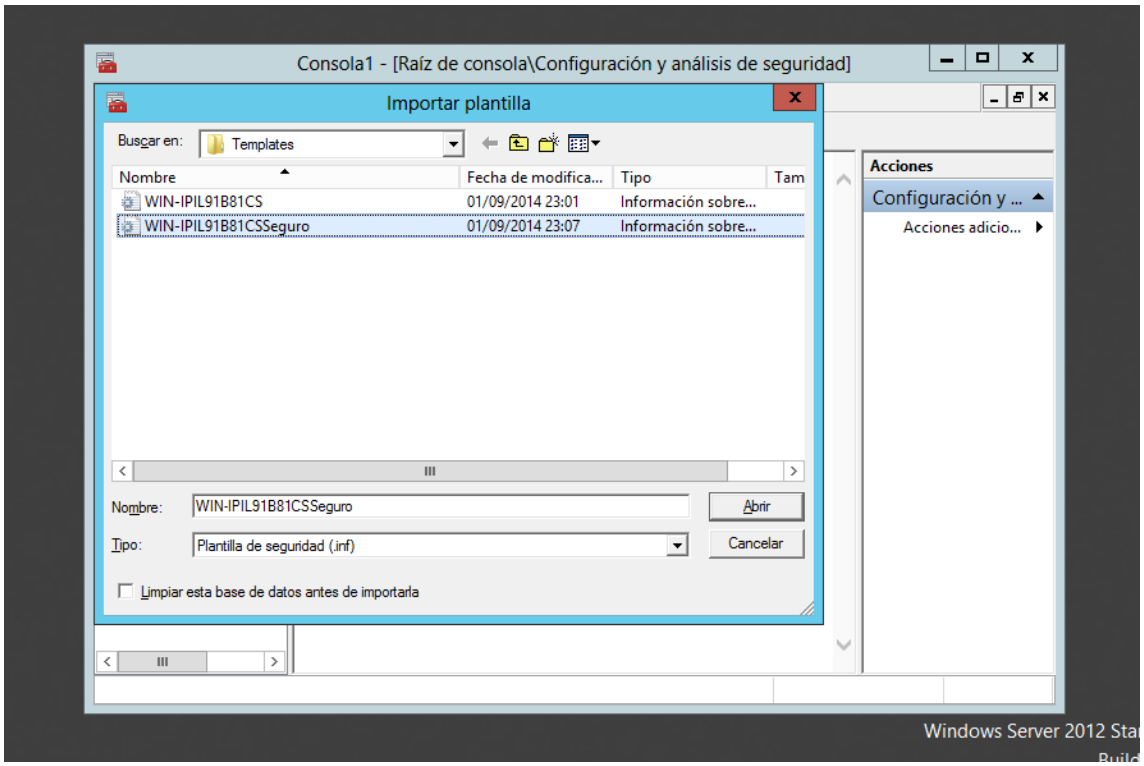


*Figura 172: Importar plantilla*

A continuación, hacemos clic con el botón secundario del ratón sobre Configuración y análisis de seguridad y pulsamos en "Analizar el equipo ahora" y se abrirá un cuadro de diálogo donde nos indica una ruta de acceso, dejamos la ruta y el nombre de archivo de errores por defecto y aceptamos.

Una vez finalizado el Análisis, expandimos "Configuración y análisis de seguridad" y después expandimos "Directivas locales" y observamos que las directivas que hemos modificado anteriormente aparecen con una cruz roja, esto indica que la configuración de plantilla seleccionada no coincide con la que está implementada actualmente.

| Directiva | Configuración de l... | Configuración del equipo |
|---|---|---|
| Dispositivos: permitir desacoplamiento sin tener que iniciar ... | Habilitada | Habilitada |
| Dispositivos: permitir formatear y expulsar medios extraíbles | No está analizada | Administradores |
| Dispositivos: restringir el acceso a disquetes solo al usuario c... | No está analizada | Deshabilitada |
| Dispositivos: restringir el acceso al CD-ROM solo al usuario ... | No está analizada | Deshabilitada |
| Inicio de sesión interactivo: comportamiento de extracción ... | Ninguna acción | Ninguna acción |
| Inicio de sesión interactivo: límite de inactividad del equipo | No está analizada | No está analizada |
| Inicio de sesión interactivo: mostrar información de usuario ... | No está analizada | No está analizada |
| Inicio de sesión interactivo: no mostrar el último nombre de... | Deshabilitada | Deshabilitada |
| Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr | Deshabilitada | Deshabilitada |
| Inicio de sesión interactivo: número de inicios de sesión ant... | 10 inicios de sesión | 10 inicios de sesión |
| Inicio de sesión interactivo: pedir al usuario que cambie la c... | 5 días | 5 días |
| Inicio de sesión interactivo: requerir la autenticación del con... | Deshabilitada | Deshabilitada |
| Inicio de sesión interactivo: requerir tarjeta inteligente | Deshabilitada | Deshabilitada |
| Inicio de sesión interactivo: texto del mensaje para los usuari... | Sólo acceso autori... | WIN-IPIL91B81CS |
| Inicio de sesión interactivo: título del mensaje para los usuar... | WIN-IPIL91B81CS | |
| Inicio de sesión interactivo: umbral de bloqueo de cuenta d... | No está analizada | No está analizada |
| Miembro de dominio: cifrar digitalmente datos de un canal ... | Habilitada | Habilitada |
| Miembro de dominio: cifrar o firmar digitalmente datos de ... | Habilitada | Habilitada |
| Miembro de dominio: deshabilitar los cambios de contraseñ... | Deshabilitada | Deshabilitada |
| Miembro de dominio: duración máxima de contraseña de c... | 30 días | 30 días |
| Miembro de dominio: firmar digitalmente datos de un canal... | Habilitada | Habilitada |
| Miembro de dominio: requerir clave de sesión segura (Wind... | Habilitada | Habilitada |
| Objetos de sistema: reforzar los permisos predeterminados ... | Habilitada | Habilitada |
| Objetos de sistema: requerir no distinguir mayúsculas de mi... | Habilitada | Habilitada |
| Seguridad de red: configurar tipos de cifrado permitidos par... | No está analizada | No está analizada |
| Seguridad de red: forzar el cierre de sesión cuando expire la ... | Deshabilitada | Deshabilitada |
| Seguridad de red: nivel de autenticación de LAN Manager | No está analizada | No está analizada |
| Seguridad de red: no almacenar valor de hash de LAN Mana... | Habilitada | Habilitada |

*Figura 173: Resultados del análisis*

Una vez ya se ha hecho el análisis y se ha creado la base de datos, vamos a proceder a configurar el sistema con la plantilla que hemos creado anteriormente.

Hacemos clic con el botón secundario sobre “Configuración y análisis de seguridad” y seleccionamos “Configurar el equipo ahora”. En el cuadro de diálogo “Configurar el sistema” dejamos como ruta de acceso la del archivo de logs y pulsamos Aceptar. Ahora aparecerá un cuadro de diálogo en el que se ve el progreso de las tareas de configuración, cuando termine este progreso, significará que el equipo ya está configurado con las opciones que hemos modificado en WIN-IPIL91B81CSSeguro.inf

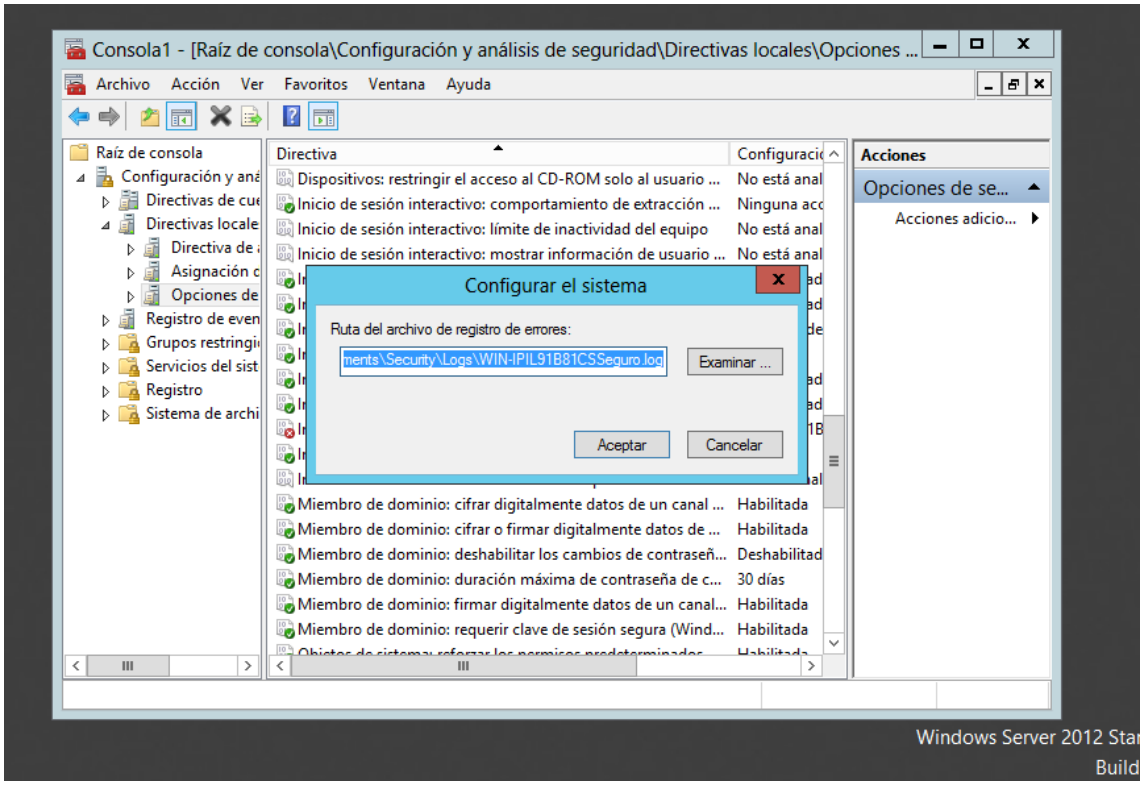


*Figura 174: Log de errores*

Ahora ya podemos guardar la consola y cerrarla, para ello pulsamos cerrar, y nos aparecerá un mensaje de aviso en el que nos da la opción de guardar la consola, le decimos que Sí y como nombre del archivo, ponemos Configuración y Análisis de Seguridad.

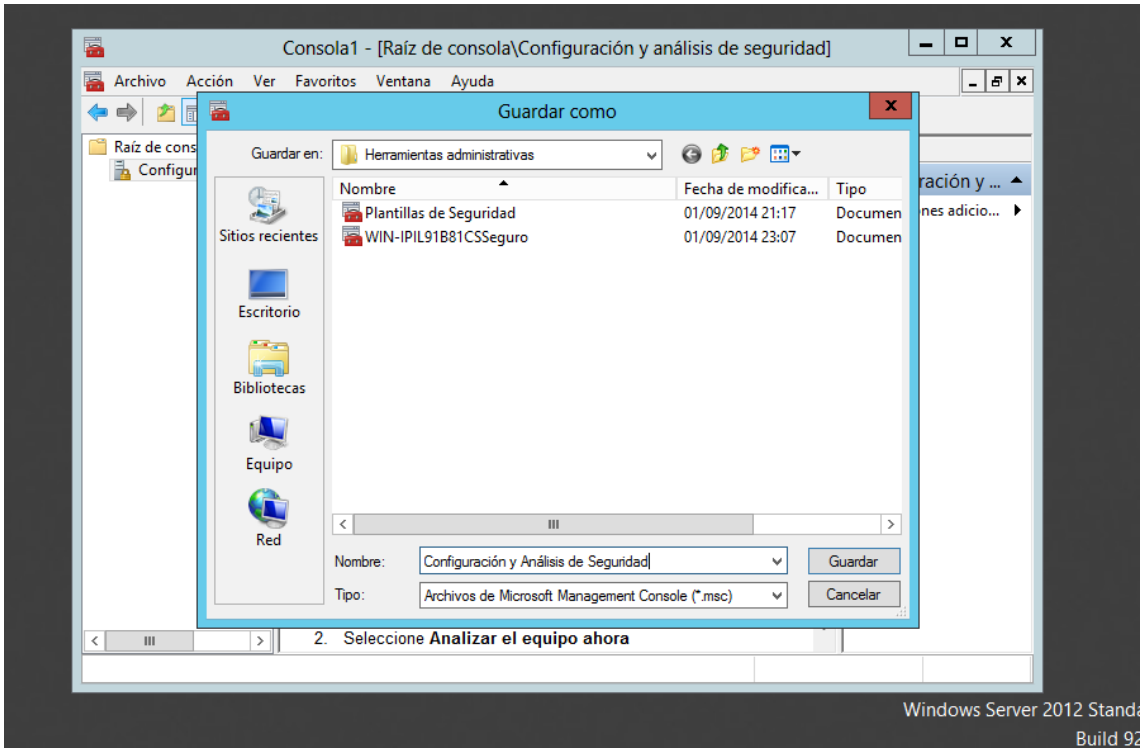


*Figura 175: Guardar consola Configuración y análisis de seguridad*

Ahora, al iniciar sesión, veremos que nos aparece un mensaje como el mostrado en la siguiente figura, esto nos indica que las directivas de seguridad que hemos definido previamente se han aplicado sin problemas.

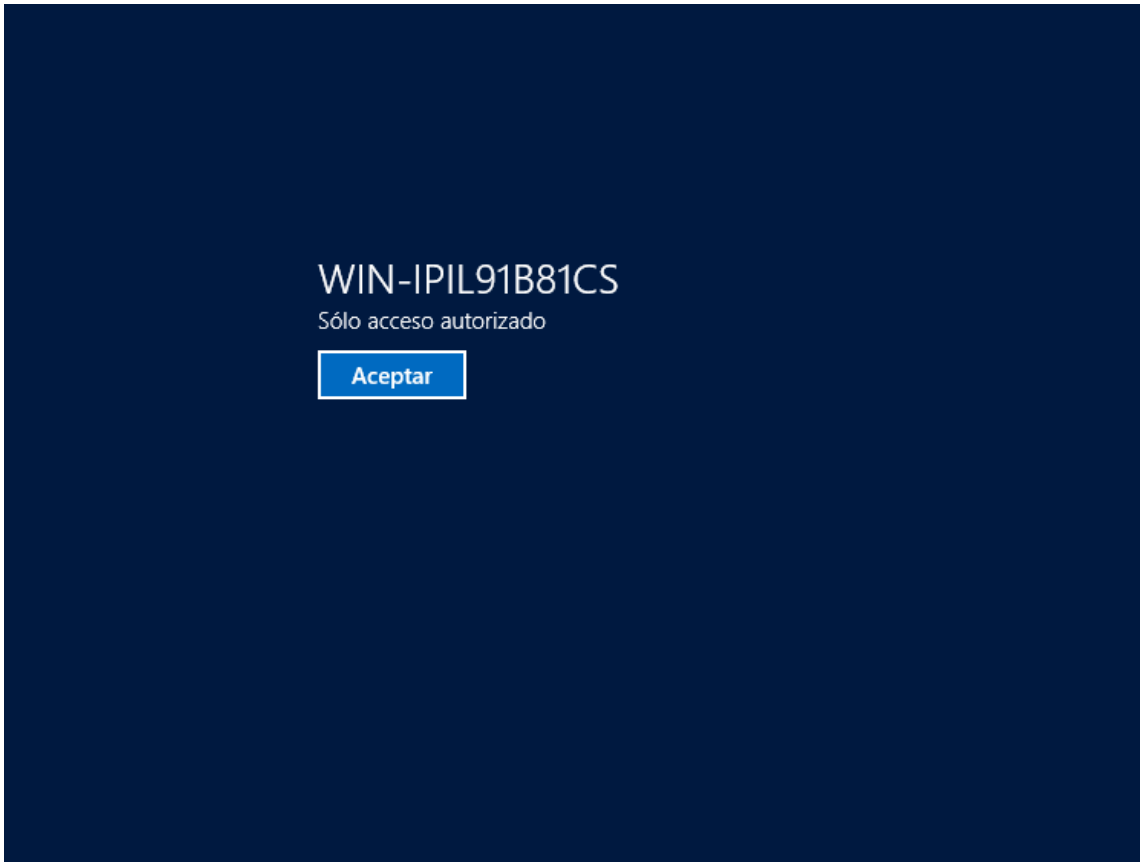


*Figura 176: Mensaje de inicio de sesión*

# 5. Conclusiones

Como se ha podido observar, especialmente en el último capítulo, las directivas de grupo son una herramienta muy potente que facilita increíblemente las labores de la administración de los sistemas de información, ya que permiten habilitar y deshabilitar funcionalidades, componentes y herramientas, o el acceso a ellos en múltiples equipos y usuarios a la vez, sin necesidad de que el administrador del sistema tenga que dedicar horas a realizar estas modificaciones equipo a equipo.

Además, en una empresa en crecimiento, donde cada poco tiempo se realizan contrataciones y se añaden nuevos equipos al sistema, la aplicación de directivas de grupos a contenedores, facilita la adición de nuevos usuarios y equipos, pues basta con añadirlo al contenedor adecuado y no es necesario que cada vez que entra un nuevo trabajador en la empresa, o cada vez que se renueve un equipo, el administrador del sistema esté horas configurando todas las funcionalidades del equipo y todos los permisos para el nuevo usuario.

Personalmente, he encontrado la experiencia de realizar este trabajo bastante enriquecedora, pues he recordado y adquirido nuevos conocimientos sobre el mundo de la administración de sistemas, una de las ramas que más me entusiasma de la informática, aunque también me he encontrado con algunas dificultades en el trascurso de la realización del trabajo, ya que tuve que reorganizar varias veces los usuarios y los grupos, y también tuve algunos problemas a la hora de inicializar las máquinas virtuales de los servidores, ya que nunca había creado un sistema desde cero, pues en las asignaturas en las que traté con Active Directory, las máquinas estaban ya creadas y con los servidores DNS y los controladores de dominio configurados.

# 6. Bibliografía


Introducción a Active Directory (18/10/2000)

http://support.microsoft.com/kb/196464/es Fecha de consulta: 12/08/2014

Active Directory Wikipedia

www.es.wkipedia.org/wiki/Active_Directory Fecha de consulta: 12/08/2014

ETSINF UPV Administración de Sistemas, (2013-2014) Unidad 2 (transparencias)

LDAP Wikipedia

www.es.wikipedia.org/wiki/LDAP Fecha de consulta: 12/08/2014

Los servidores DNS, usos, características y configuración. NorfiPC

www.norfipc.com/internet/servidores-dns.html Fecha de consulta: 13/08/2014

Configurar el Sistema de nombres de dominio para Active Directory

http://support.microsoft.com/kb/237675/es Fecha de consulta: 13/08/2014

Instalación y configuración del servidor DHCP

www.tutorialesit.blogspot.com.es/2012/12/windows-server-2012-instalacion-dhcp.html Fecha de consulta: 03/08/2014

Introducción a la directiva de grupo (agosto de 2012)

http://technet.microsoft.com/es-es/library/hh831791.aspx Fecha de consulta: 25/08/2014

ETSINF UPV Administración de Sistemas, (2013-2014) Unidad 4-1 Políticas Windows ES (transparencias).