UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Seguretat en Sistemes Informàtics en Windows Server 2012

Treball Fi de Grau

Grau en Enginyeria Informàtica

Autor: Carles Pedrola i Tortajada

Tutor: Juan Luis Posadas Yagüe
Juan Carlos Cano Escribá

2017/2018

Resumen

En aquest treball s'ha creat un sistema informàtic bàsic en un entorn virtual en VMWare, basat en Windows Server 2012 i s'ha realitza un estudi sobre les configuracions de seguretat que permet aquest sistema: grups de seguretat, directives de grup d'autenticació, directives de grup d'auditoria i directives de grup per bloquejar l'equip de treball quan està inactiu.

Paraules clau: Windows Server 2012, VMWare, seguretat, auditoria.

Abstract

In this work, a basic computer system has been created in a virtual environment in VMWare, based on Windows Server 2012 and a study has been carried out on the security configurations that this system allows: security groups, authentication group directives , audit group directives and group directives to block the work team when it is inactive.

Keywords : Windows Server 2012, VMWare, security, audit.

Taula de continguts

Índex de captures

Índex de Figures

1. Introducció

En l'era tecnològica en que vivim, per a les empreses, és molt important la gestió i optimització dels recursos informàtics i la seguretat d'aquests. És per això, que les empreses han d'estudiar com s'estructura l'empresa i amb quines ferramentes ho van a fer.

En l'actualitat, un dels programaris més utilitzats per a la gestió dels sistemes informàtics corporatius és Windows Server, desenvolupat per Microsoft. Windows Server te una línia de productes per a servidors, que permeten gestionar els recursos informàtics d'una empresa i configurar-los com més s'adeqüi a les necessitats d'aquesta.

Altre punt a tenir en compte per a la gestió d'un sistema informàtic, a part de la gestió del servidor, és la seguretat. El procés de transformació digital en que estan la majoria d'empreses i organitzacions, així com la societat en general, permet que des de la pròpia empresa o qualsevol part del món la seguretat de la informació digital estiga compromesa, afectant als clients i les pròpies empreses.

1.1 Objectius

Els objectius d'aquest treball són realitzar un estudi de les opcions de configuració de seguretat que permet Windows Server 2012 i la realització d'una memòria que servisca de guia per a la instal·lació i configuració de Windows Server 2012 en entorns virtualitzats.

L'estudi es va a centrar en l'utilització de grups de seguretat per a gestionar els permisos dels usuaris a un recurs compartit, definint diferents tipus de permís per a cada departament d'una empresa inventada, que permetra diferents configuracions per les necessitats d'aquesta. També s'estudiaran les directives de compte, formades per la directiva Kerberos, la directiva de Bloqueig de compte i la Directiva de contrasenyes així com les diferents configuracions de les opcions d'autenticació. A més, es configurarà el bloqueig de l'equip de treball per inactivitat mitjançant directives. Finalment s'estudiarà l'auditoria d'accés a objectes i l'auditoria d'esdeveniments d'inici de sessió, així com el seguiment d'aquests esdeveniments a través del visor d'esdeveniments que proporciona Windows Server 2012.

1.2 Pla de treball

Per tal de dur a terme els objectius mencionats, l'estructura del pla de treball s'ha establert de la següent forma:

1. Descripció de l'empresa exemple sobre la que es realitza el treball i les necessitats d'aquesta.

2. Instal·lació i configuració del programari VMware Workstation Pro, a l'ordinador base on es va a realitzar el treball.
3. Creació dels equips virtuals i instal·lació dels sistemes operatius corresponents.
4. Creació del domini Active Directory.
5. Instal·lació dels rols i característiques dels servidors: DHCP i DNS.
6. Addició del segon controlador de domini.
7. Configuració de l'ordinador client i addició al domini.
8. Crear l'estructura virtual de l'empresa, en els Usuaris, Grups i Unitats Organitzatives.

Quan l'entorn de l'empresa queda configurat s'estudien les mesures de seguretat mencionades en els objectius:

9. Configuració dels permisos mitjançant grups de seguretat sobre un recurs compartit.
10. Configuració de les diferents directives de grup mencionades en els objectius d'aquest treball.

1.3 Estructura del document

El document esta estructurat en quatre blocs:

- En el primer bloc es descriuen els objectius del treball i es fa una introducció per tal de contextualitzar-lo. També és descriu l'empresa exemple sobre la que es va a realitzar el treball i les necessitats d'aquesta.

- En el segon bloc s'expliquen les ferramentes i serveis necessaris per a crear l'entorn de treball sobre el que es va a realitzar l'estudi proposat en els objectius. Les instal·lacions corresponents a aquest bloc estan explicades pas a pas en l'apartat de l'Annex.

- En el tercer bloc es desenvolupa el treball i es realitza l'estudi de seguretat sobre les ferramentes i serveis proposats als objectius.

- En l'últim bloc es presenten les conclusions del projecte i la bibliografia.

2. Empresa exemple

L'empresa sobre la que es va a fer l'estudi de seguretat, és una empresa inventada que va a permetre estudiar diferents tipus de configuracions, per les necessitats que aquesta necessita. Aquesta empresa es dedica a la creació d'aplicacions per a telèfons i tabletes. En els següents apartats es descriu l'estructura del sistema informàtic, els departaments i els usuaris de l'empresa, així com algunes descripcions dels departaments, que serviran per poder fer diferents configuracions en les polítiques de seguretat de l'empresa.

2.1 Estructura

L'estructura que es planteja és una estructura bàsica, composada per dos equips en els quals s'instal·larà Windows Server 2012 i que actuaran com a primer i segon controlador de domini i un tercer equip on s'instal·larà Windows 10, que actuarà com equip de treball de l'empresa. Aquests equips formaran part d'un mateix domini nombrat "Empresa.local". En l'arrel del disc del controlador del domini es crearà una carpeta de "Recursos" i una estructura de subcarpetes per a cada departament amb diferents permisos per als usuaris.

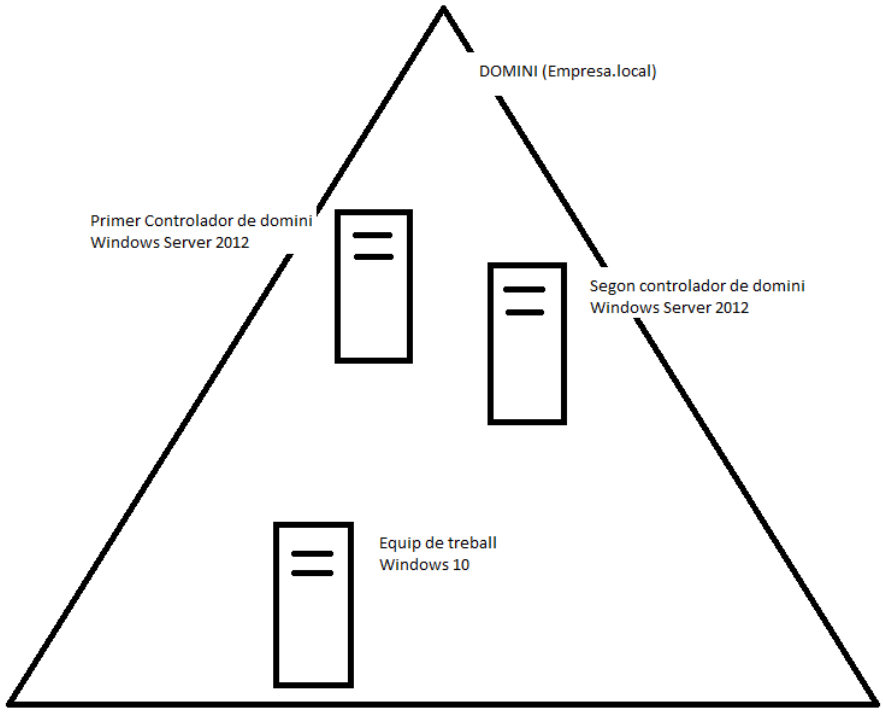


Figura 1 - Estructura del domini

2.2 Departaments i usuaris

Pel que fa a l'estructura de l'empresa que s'ha creat per a la realització d'aquest treball, s'han diferenciat cinc departaments:

- **Directius:** aquest departament és el que gestiona l'empresa i pren les decisions finals de totes les qüestions que tenen a veure amb aquesta. Aquest departament està format per Diana i Dani, socis fundadors de l'empresa.

- **Recursos Humans:** aquest departament és l'encarregat de gestionar tot el que te a veure amb els treballadors de l'empresa. Principalment, la gestió de els nòmines i la contractació de nous treballadors. Aquest departament està format per Rubén i Raquel. Rubén s'encarrega de la gestió de les nòmines i Raquel de la contractació de nous treballadors. Les dues gestions estan supervisades pels directius.

- **Sistemes:** aquest departament és l'encarregat de gestionar tot el sistema informàtic de l'empresa. Sandra és l'únic membre d'aquest departament.

- **Aplicacions:** aquest departament és l'encarregat de desenvolupar les aplicacions per a tables i mòbils sol·licitades per els clients. El departament està format per Andreu, Andrea i Adrià. Adrià és el cap del departament. Andreu és l'encarregat del desenvolupament d'aplicacions per a Android i Andrea per al desenvolupament les aplicacions per a sistemes iOS. Adrìa és l'encarregat de supervisar totes les aplicacions abans d'entregar-les als clients.

- **Comercial:** aquest departament és l'encarregat de gestionar la relació entre els clients i l'empresa. Carme és l'únic membre d'aquest departament.

3. Entorn de Treball

Per a la realització del treball cal instal·lar Windows Server 2012 en els dos equips virtuals creats en VMware que actuaran com controladors de domini. Seguidament, i per tal de crear l'entorn de treball virtualizat sobre el que es va a realitzar aquest treball es configuraran els següents rols y es realitzaran les següents configuracions:

- Active Directory
- DNS
- DHCP
- Afegir segon controlador de domini i l'equip de treball.
- Afegir grups, usuaris i unitats organitzatives

Amb totes aquestes configuracions quedarà configurat l'entorn de treball que servirà per a desenvolupar les tasques d'estudi sobre seguretat indicades en els objectius.

3.1 VMware

VMware és un sistema de virtualització per programari. Aquest, simula un sistema físic amb unes característiques determinades i permet executar diversos equips en un mateix maquinari simultàniament.

Per a la realització del treball s'ha optat per aquest programari, encara que no és l'únic programari de virtualització que existeix.

Va a permetre crear l'estructura bàsica de l'empresa per tal de poder realitzar l'estudi de la seguretat mencionat en els objectius del treball. L'estructura escollida per a l'empresa consistirà en un domini amb tres màquines, dels quals, hi ha dos controladors de domini i un equip de treball.

Així que el primer pas per a la realització del treball és instal·lar VMware en l'equip amfitrió. Seguidament es creen les màquines virtuals necessàries per a la realització del treball, amb les característiques requerides per a la instal·lació dels sistemes operatius corresponents: Windows Server 2012 per als servidor i Windows 10 per a l'equip de treball.

3.2 Windows Server 2012

Windows Server 2012 és la sisena i penúltima versió de Microsoft Windows per a servidors. Aquest sistema operatiu és el que permet gestionar i instal·lar els rols del servidor que satisfacin les necessitats de l'empresa.

Entre els serveis que ofereix Windows Server 2012, trobem el Servei de domini Active Directory (AD DS), que permet crear una infraestructura escalable, segura i administrable per a l'administració d'usuaris i recursos.

Altres rols que permet instal·lar per a configurar el domini son el servidor DHCP, el servidor DNS, servidor d'accés remot i servidor Windows Server Update entre altres.

Referent a la seguretat, Windows Server 2012 permet a l'empresa poder gestionar els recursos de manera eficient i segura. Proporciona accés segur autenticat als recursos de l'empresa, així com permisos sobre aquests. D'aquesta manera, la informació i els recursos de l'empresa queden protegits per aquest de l'accés d'usuaris no desitjats.

3.3 Active Directory

Com s'ha mencionat en l'apartat anterior, el Servei de domini Active Directoy (AD DS), permet crear una infraestructura escalable, segura i administrable per a l'administració d'usuaris i recursos. El servidor que executa AD DS s'anomena controlador de domini.

Els administradors poden organitzar els elements de la xarxa, com els usuaris, els equips i altres dispositius en una estructura jerarquitzada i permet establir polítiques a nivell d'empresa. L'estructura jerarquitzada que s'ha utilitzat per a la realització del treball consta d'un bosc, que actua com a límit de seguretat de l'empresa y del domini arrel d'aquest bosc.

Per tal de que el servidor creat actue com a primer controlador de domini, s'ha instal·lat el rol d'AD DS i s'ha promocionat a Controlador de Domini del domini Active Directory creat.

3.4 Configuració DNS

Domain Name System (DNS) és una tecnologia que serveix per a la resolució de noms en la xarxa, es a dir, per a conèixer l'adreça IP d'un equip connectat a una xarxa informàtica.

Existeixen dos tipus de cerques DNS:

- La **cerca directa**: aquesta cerca retorna l'adreça IP del recurs sol·licitat.
- La **cerca inversa**: aquesta cerca retorna el nom del recursos sol·licitat a partir de l'adreça IP.

La cerca directa, s'ha instal·lat en el pas anterior, quan es crea el domini d'Active Directory, que s'instal·la el **Servidor DNS** i es configura automàticament. Per contra, cal configurar manualment la zona inversa DNS.

3.5 Configuració DHCP

DHCP (Dynamic Host Configuration Protocol) és un protocol de xarxa que permet que els equips que es connecten a una xarxa es configuren automàticament, assignant a cada equip que es connecta a la xarxa una adreça IP per a aquesta xarxa.

Al instal·lar el rol DHCP, s'està configurant una mesura de seguretat important per a la xarxa, que permet a l'administrador assignar un rang de direccions ip que perteneixen a la xarxa. També proporciona una configuració de red TCP/IP segura i evita conflictes de direccions IP repetides. També es una manera de tenir centralitzades totes les IP utilitzades en la xarxa.

3.6 Segon controlador de domini

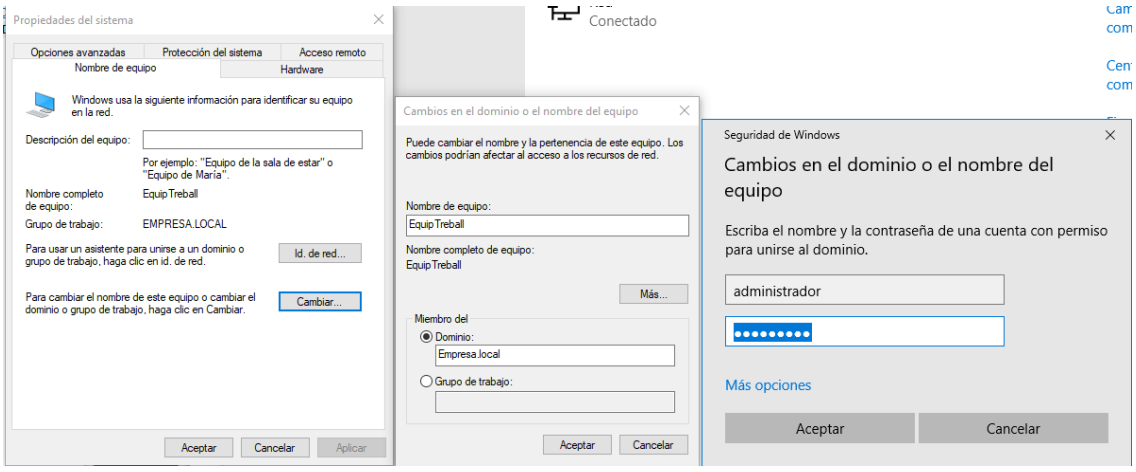
El principal avantatge d'unir un segon controlador de domini a un domini existent, es que permet mantenir una replica constant del primer controlador del domini, assegurant la disponibilitat dels recursos en cas de que el primer controlador de domini es quede fora de servei.

Aquesta unió permet augmentar la confiabilitat de la instal·lació, ja que com s'ha mencionat, seguirà funcionant el servei encara que un servidor deixe de funcionar. Per altra banda també pot ser utilitzat per distribuir la càrrega entre els dos servidors i augmentant la velocitat de resposta de cara als clients.

3.7 Equip de treball

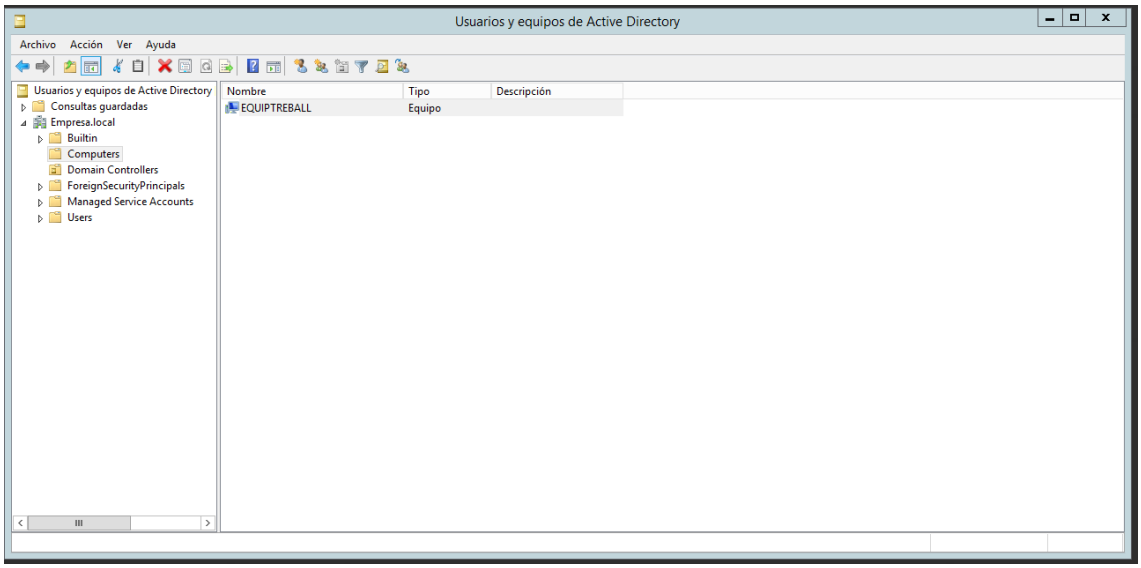
L'equip de treball és un equip amb Windows 10 com a sistema operatiu. Aquest equip s'afegeix al domini Empresa.local i és l'equip que utilitzaran els treballadors de l'empresa per a realitzar les seues tasques i des d'on accediran als seus recursos compartits i de la resta de companys de l'empresa.

Per afegir l'equip amb Windows 10, cal accedir a la configuració de Propietats del sistema, i clicar en **"Cambiar"**. Seguidament, cal escriure el domini al que es desitja unir l'equip, en aquest cas **"Empresa.local"** i clicar en acceptar. Es sol·licitarà les credencials de l'usuari administrador del domini per poder afegir l'equip.



Captura 1 - Unió de l'equip de treball al domini

Després de realitzar aquest canvi cal reiniciar l'equip per a que es configuren els canvis. Des del tauler d'Usuaris i Equips d'Active Directory, es pot observar que s'ha afegit l'equip com un equip del domini.



Captura 2 - Comprovació de la unió de l'equip de treball al domini

Després d'aquesta comprovació ja estan configurats els equips i el domini per poder començar a fer l'estudi de les ferramentes de seguretat que l'Active Directory proporciona a les empreses.

4.Ferramentes de seguretat

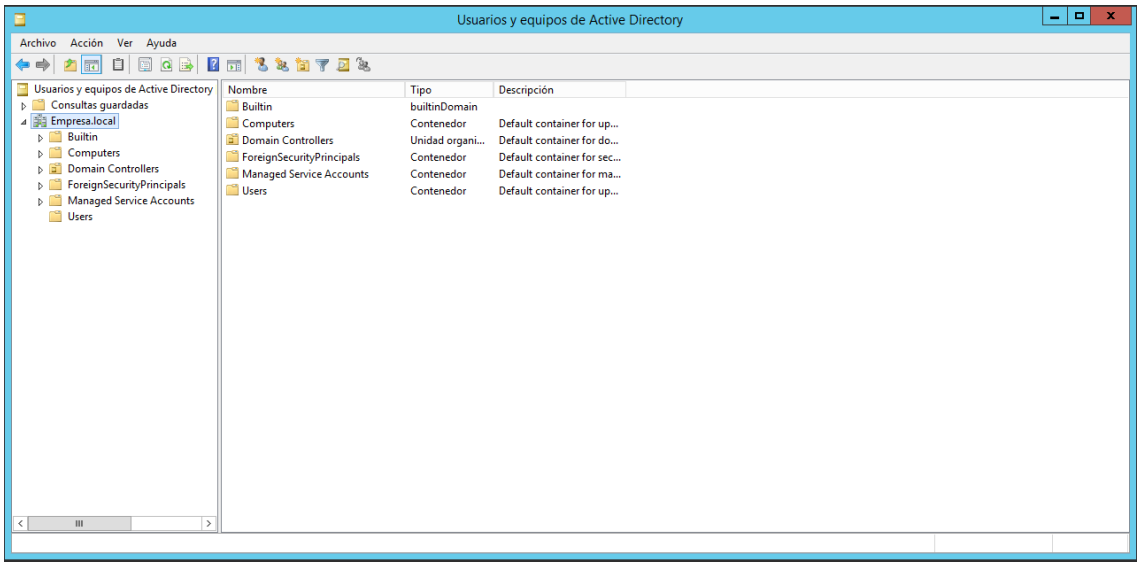
4.1 Usuaris

Els usuaris és un mecanisme de control per a l'accés al domini i als recursos que aquest proporciona. Un compte d'usuari consisteix en un nom d'usuari i una contrasenya, amb la que l'usuari podrà autenticar-se.

Els usuaris són una clau important pel que es refereix a la seguretat, ja que utilitzant els usuaris es pot restringir a que accedeix cada usuari i configurar unes característiques de privacitat per a cada usuari. També és pot controlar a que accedeix cada usuari i quines accions realitza sobre cada recurs al que te accés.

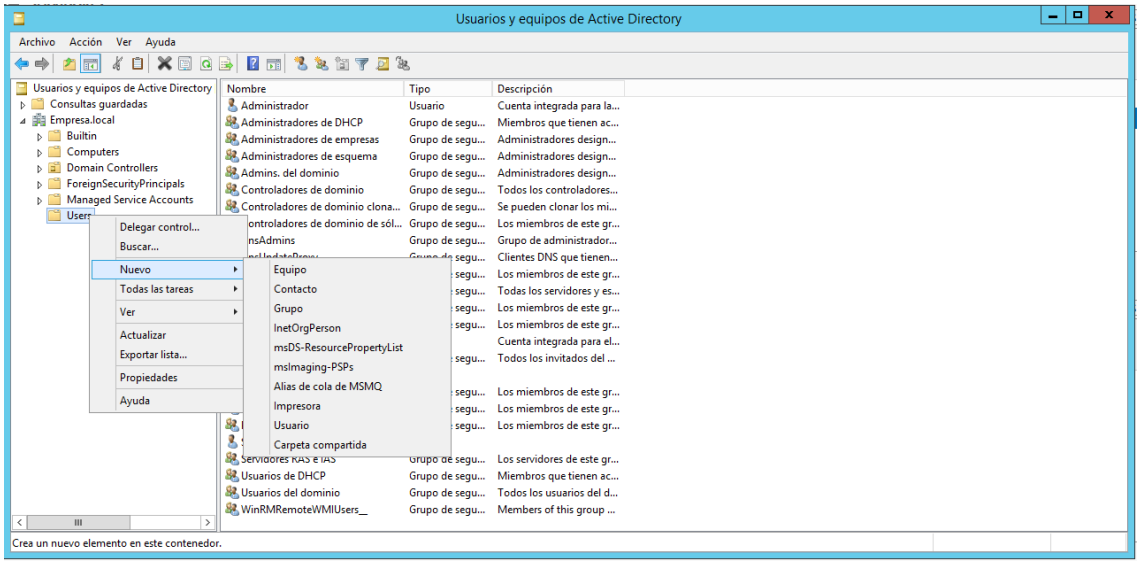
També va a permetre, en aquest cas en el que l'empresa únicament disposa d'un equip de treball, que cada usuari accedisca identificat a l'equip de treball i es puga configurar l'equip segons les seues necessitats.

Per tal d'afegir usuaris al domini, des del primer controlador de domini, s'accedeix al tauler d'usuaris i equips d'Active Directory.



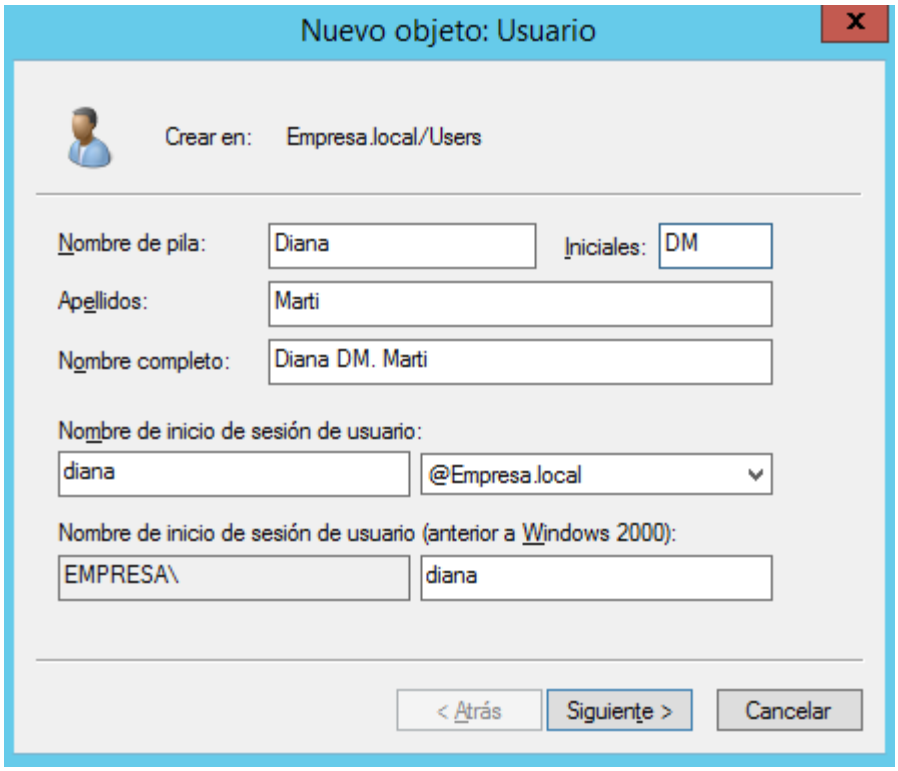
Captura 3 - Tauler d'Usuaris i equips d'Active Directory

Seguidament es selecciona el domini al que es desitja afegir l'usuari i es clica amb el botó dret sobre **"Users"**, **"Nuevo"** y es selecciona **"Usuario"**.



Captura 4 - Crear nou usuari

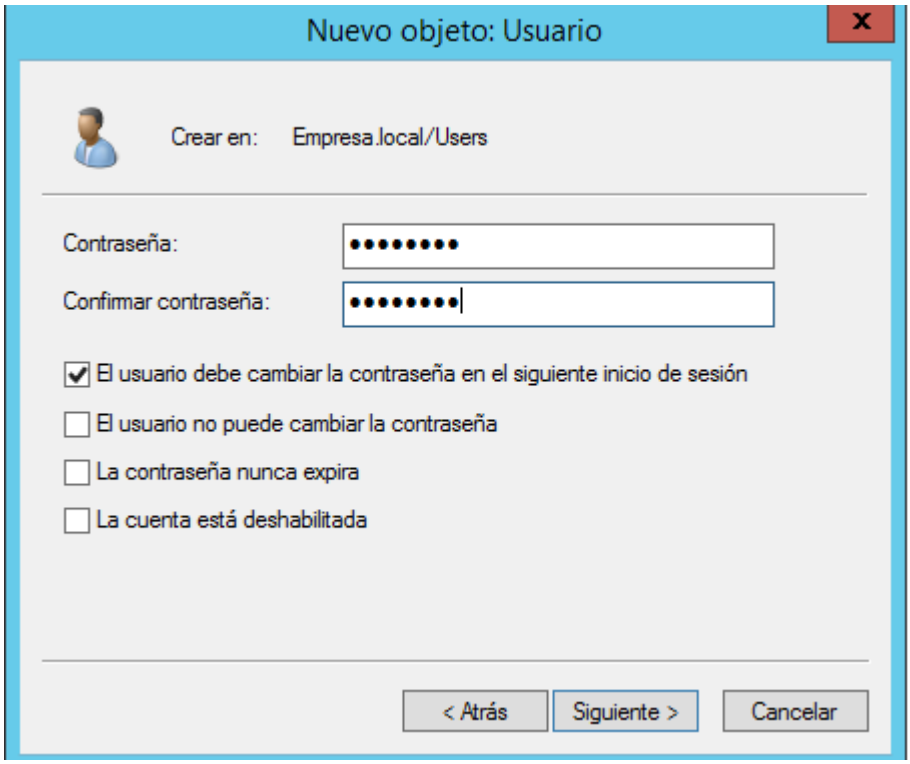
En la finestra que s'obri, cal introduir les dades de l'usuari que es vol afegir, en aquest cas s'ha començat per Diana, pertinent al departament Directius:



Captura 5 - Dades de l'usuari

A continuació es clica en **"Siguiente"** i es mostra la següent finestra per a la configuració referent a la contrasenya. Cal introduir una contrasenya per al primer accés i seleccionar l'opció **"El usuario debe cambiar la contrasenya en el**

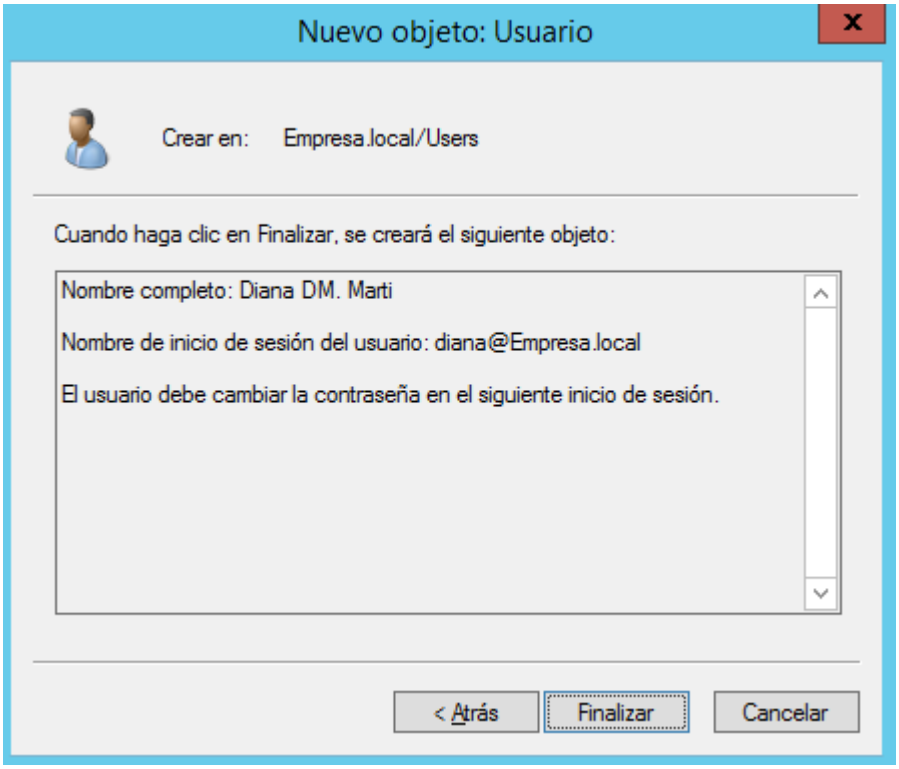
siguiente inicio de sesión" per tal que l'usuari siga l'únic que coneix la contrasenya d'accés per al seu usuari.



Captura 6 - Afegir contrasenya d'usuari

En l'apartat Autenticació d'aquest treball s'estudiarà d'una manera més precisa les opcions de les contrasenyes i el funcionament de l'autenticació en el domini.

Per a finalitzar l'addició de l'usuari s'ha de clicar en **"Siguiente"** i en **"Finalizar"** en la següent finestra on es mostra un resum de l'acció a realitzar.



Captura 7 - Finalitzar la creació del nou usuari

D'aquesta manera es poden afegir la resta d'usuaris de l'empresa, per tal que cada treballador s'identifique en un usuari i una contrasenya en el domini, a través de qualsevol equip del domini.

4.2 Grups de Seguretat

Els grups de seguretat son agrupacions d'usuaris, comptes d'equip i/o altres grups, que permeten simplificar l'administració d'aquests, ja que permet assignar l'accés als recursos al grup de manera individual i que s'apliquen als membres del grup.

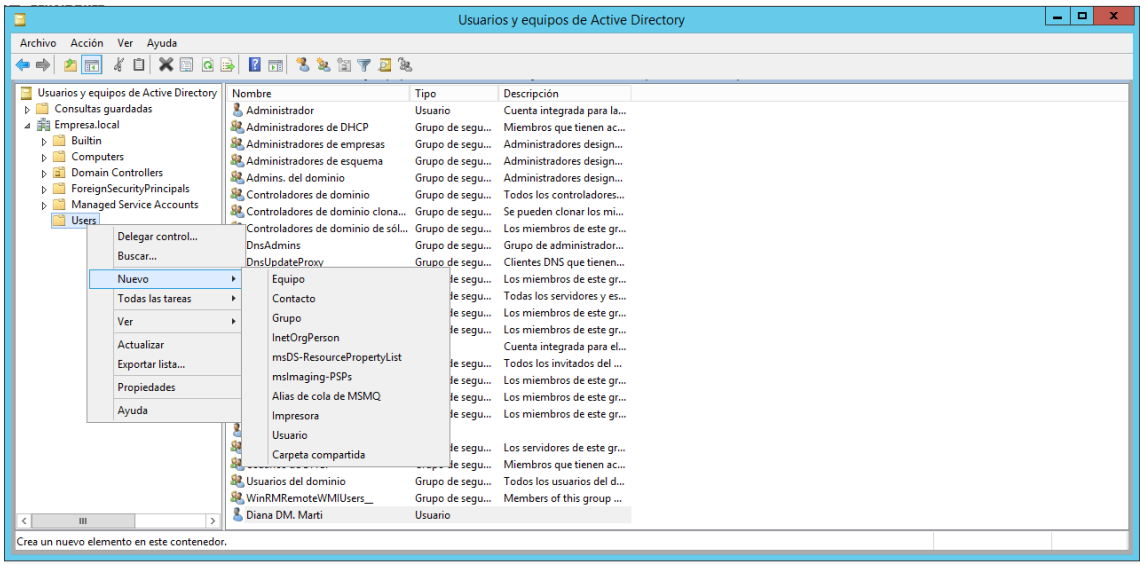
Hi ha tres àmbits en que és classifiquen els grups de seguretat:

Grup Local: poden ser membres d'aquest grup usuaris, grups locals, grups globals i grups universals. Tenen visibilitat a nivell de domini. Es solen utilitzar per a concedir permisos sobre els equips del domini.

Grup Global: poden ser membres d'aquest grup usuaris i grups globals del mateix domini. Tenen visibilitat a nivell de bosc. Es solen utilitzar per a classificar als usuaris segons les tasques que realitzen i atorgar-los permisos per a realitzar eixes tasques.

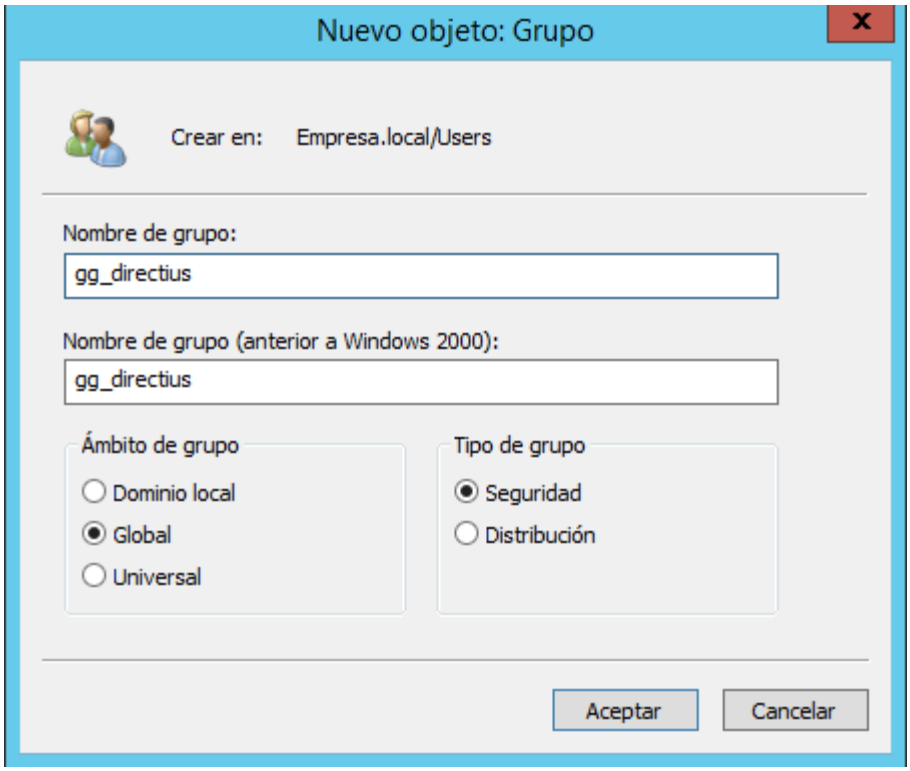
Grup Universal: poden ser membres d'aquest grup usuaris i grups globals i universals de tot el bosc. Tenen visibilitat a nivell de bosc.

Per crear un grup cal obrir el tauler d'usuaris i equips d'Active Directory. Seleccionar el domini, en aquest cas **Empresa.local** i picant en el botó dret on es desitge crear el grup, en aquest cas **"Users"**, es selecciona **"Nuevo"** i piquem sobre **"Grupo"**.



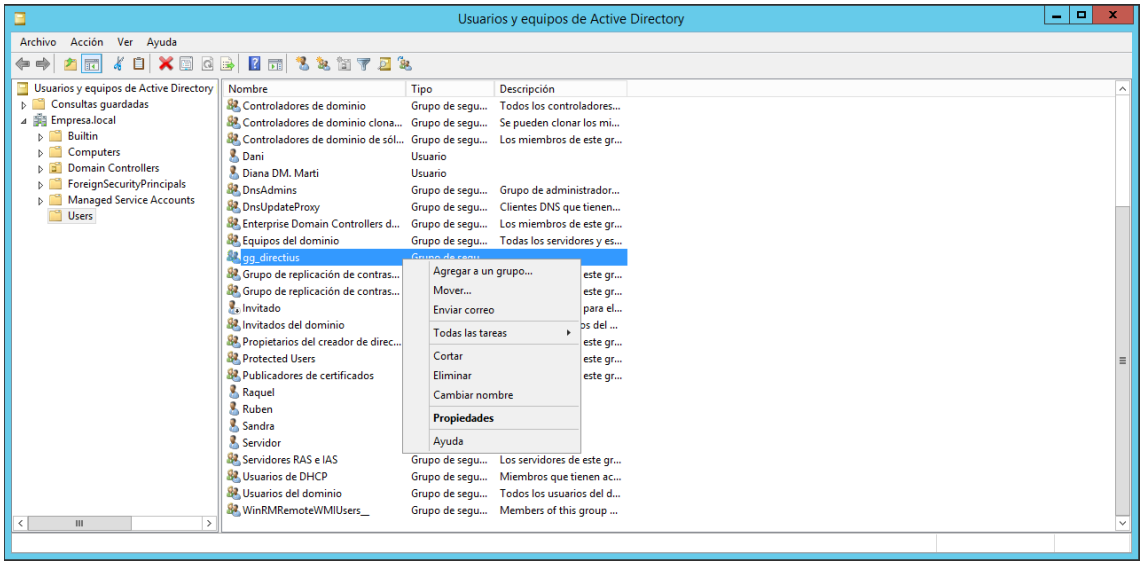
Captura 8 - Crear un grup de seguretat

En la següent finestra de configuració cal afegir el nom del grup, l'àmbit i el tipus de grup, en aquest cas, un grup de seguretat d'àmbit global.

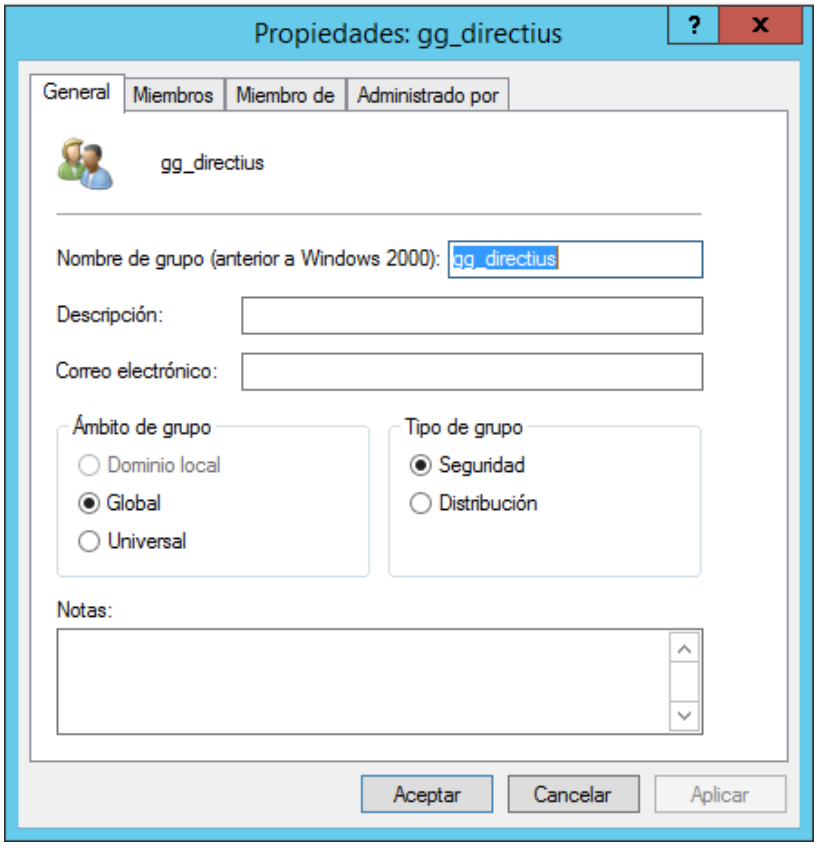


Captura 9 - Caracterísitques del grup

A l'assignar un usuari a un grup, se li assignen automàticament totes les propietats, drets, característiques, permisos i privilegis del grup. Per tal d'afegir un usuari a un grup es pica amb el botó dret sobre el grup i en les opcions que es mostren es selecciona **"Propiedades".**

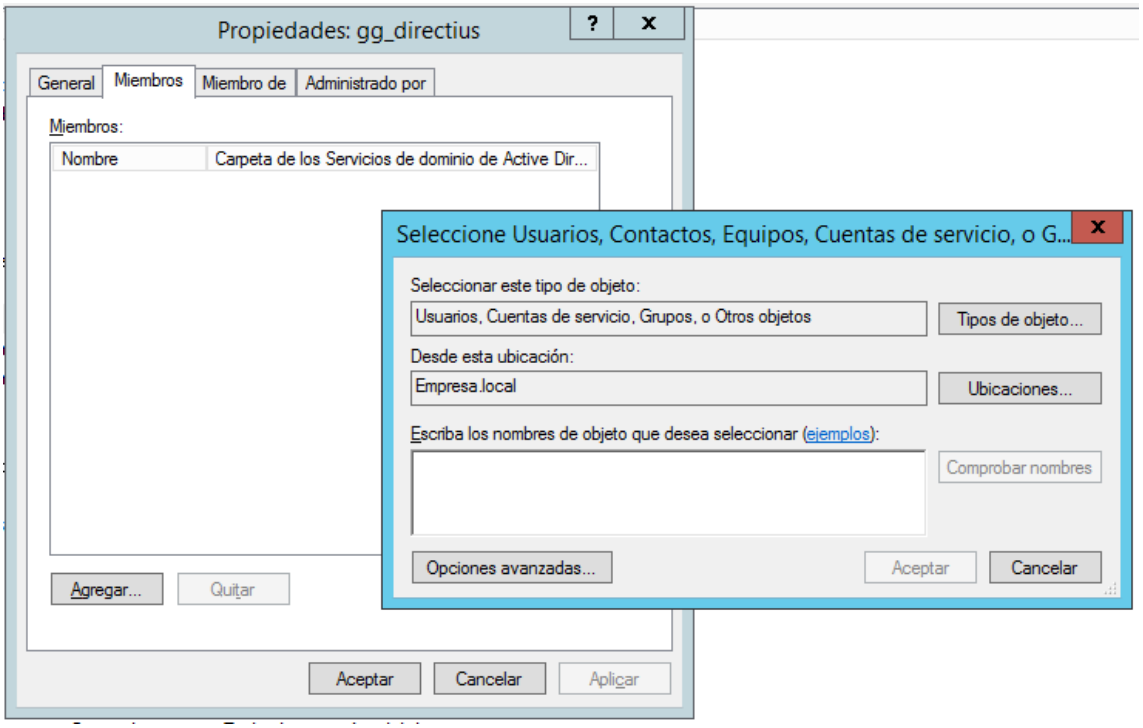


Captura 10 - Accedir a les propietats d'un grup



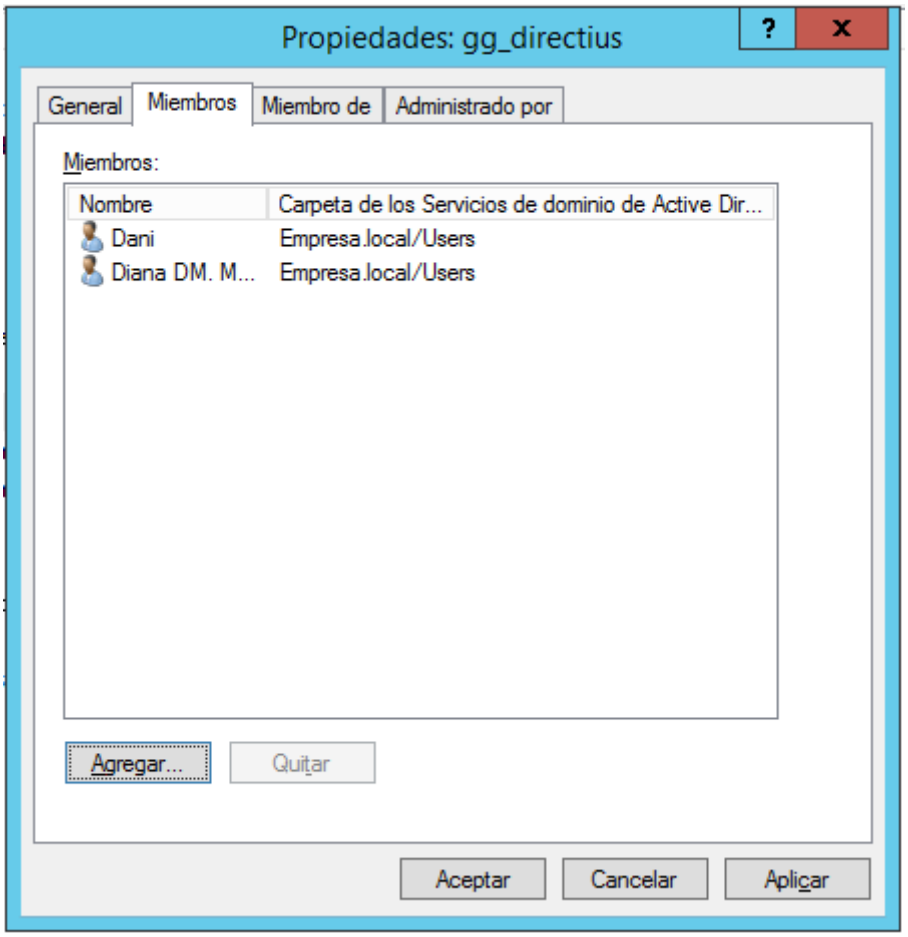
Captura 11 - Propietats del grup

En la finestra de Propietats, seleccionar la pestanya **"Miembros"** i a continuació picar sobre el botó **"Agregar".**



Captura 12 - Afegir membres a un grup de seguretat

S'escriu el nom dels usuaris que es vol afegir al grup i es comprova que existeix en el domini, picant sobre el botó **"Comprobar nombres".** Després d'afegir tots els usuaris, s'accepta i es comprova que s'han afegit els usuaris i apareixen com a membres del grup, finalment cal picar en **"Aceptar"** per confirmar l'operació.



Captura 13 - Membres d'un grup de seguretat

Per a la realització del treball, s'han afegit els usuaris creats en l'apartat anterior als següents grups globals creats:

- gg_directius: Diana, Dani
- gg_rrhh: Ruben, Raquel
- gg_sistemes: Sandra
- gg_app: Adria, Andrea, Andreu
- gg_cap_app: Adria
- gg_comercial: Carme

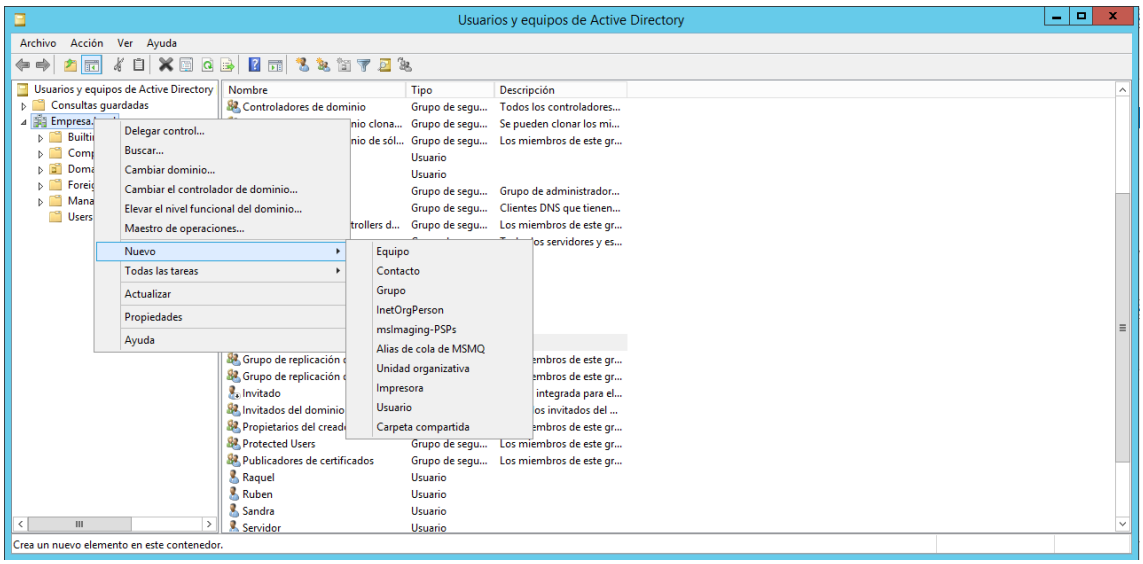
Tot i que hi ha grups que solament estan formats per un usuari, s'ha escollit aquesta configuració ja que l'empresa està en creixement i és molt probable que s'incorporen nous treballadors, per tant, és més fàcil gestionar els usuaris afegint, eliminant o canviant a aquests mitjançant els grups de seguretat.

A més, la utilització de grups de seguretat permet assignar els permisos directament a un càrrec a través d'un grup, com és el cas del grup "gg_cap_app", en el que s'ha afegit a l'usuari Adria com a cap del departament. Així, si en un futur Adria ja no és el cap del departament, eliminant a l'usuari Adria com a membre del grup gg_cap_app i afegint l'usuari al que pertany el nou cap de departament, no caldrà fer cap modificació més pel que fa a la gestió de permisos.

4.3 Unitats Organitzatives

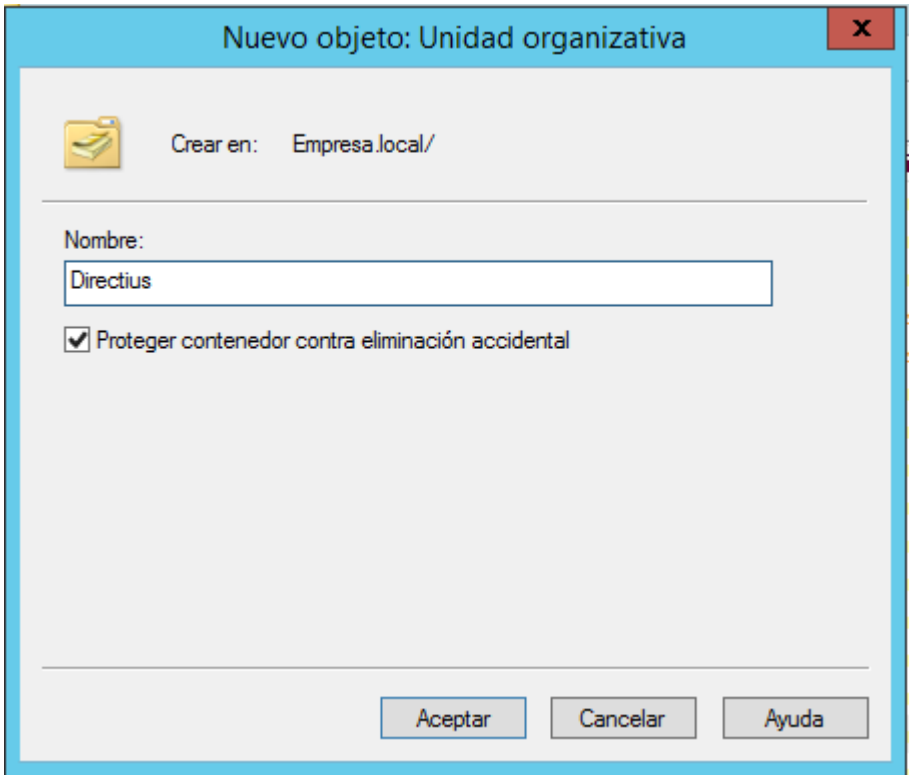
Una unitat organitzativa és un contenidor d'objectes del domini com usuaris, grups, equips o altres unitats organitzatives. S'utilitzen per poder agrupar i organitzar objectes i aplicar directives per a cada unitat organitzativa. També es solen utilitzar per esquematitzar els recursos de l'empresa, per exemple, per departaments, introduint els recursos d'aquests en la unitat organitzativa, com usuaris, grups, impressores,...

Per a crear una unitat organitzativa, des del tauler d'usuaris i equips d'Active Directory, es pica en el botó dret sobre el domini, es selecciòna **"Nueva"** i es pica sobre **"Unidad Organizativa".**



Captura 14 - Crear unitat organitzativa

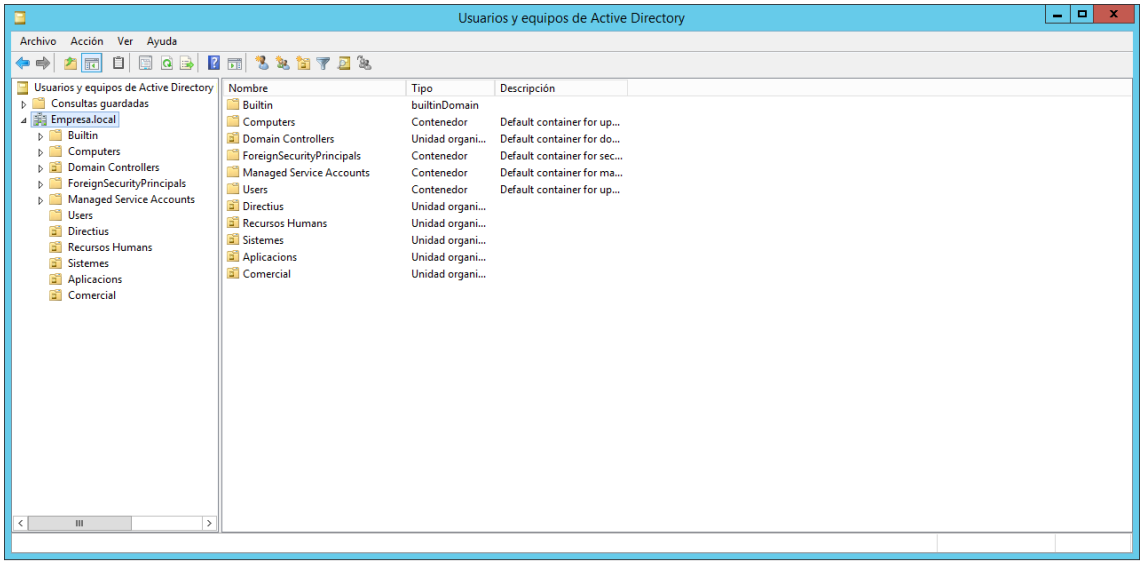
En la finestra que s'obri cal introduir el nom de la unitat organitzativa i acceptar l'operació.



Captura 15 - Nom de la Unitat Organitzativa

En aquest treball s'ha creat una unitat organitzativa per cada departament i s'han introduït els usuaris i grups pertanyents a cada departament en cada una de les unitats organitzatives. Les unitats organitzatives creades son:

- Directius
- Recursos Humans
- Sistemes
- Aplicacions
- Comercial



Captura 16 - Objectes del domini

4.4 Permisos sobre recurs compartit

En aquest apartat, es va a crear una carpeta compartida que els usuaris podran utilitzar per emmagatzemar i organitzar els arxius que utilitzen en el treball. Aquesta carpeta compartida es va a crear en el primer controlador de domini i es compartirà des d'aquest a la resta dels usuaris, que accediran des de l'equip de treball Windows 10, on treballen habitualment.

La carpeta es va a estructurar en subcarpetes per als diferents departaments i subcarpetes dins d'aquest departaments. L'estructura de la carpeta es mostra en el següent esquema:

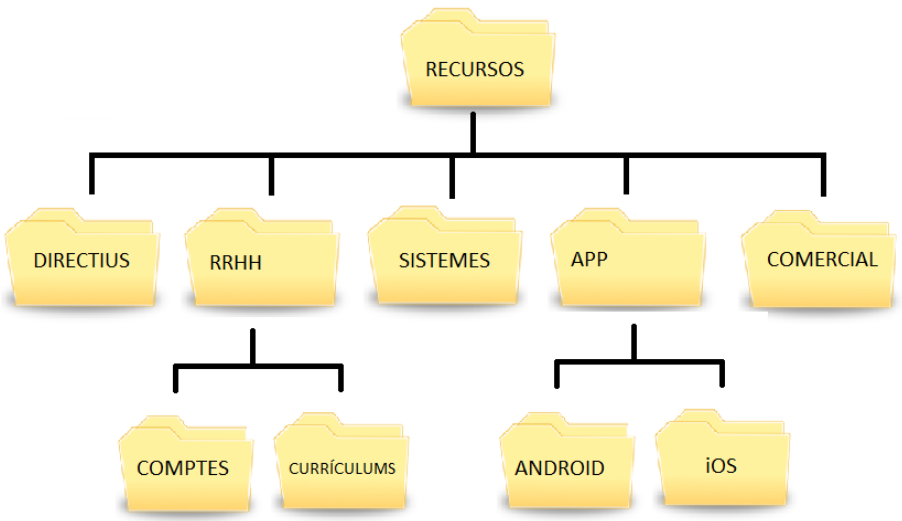


Figura 2 - Estructura de permisos sobre Recurs compartit

Aquestes carpetes es van a configurar en diferents paràmetres de seguretat. Els paràmetres de seguretat que es van a configurar per a cada carpeta son els següents:

- Recursos: a aquesta carpeta han de tenir tots els usuaris de l'empresa permís de lectura, per poder accedir als seus continguts.

- Directius: solament els directius tenen accés a la carpeta i aquests han de poder crear, modificar i eliminar el contingut de la carpeta.

- RRHH: a aquesta carpeta han de tenir accés Rubén, Raquel per poder accedir a les subcarpetes Comptes i Currículums respectivament i els directius per poder supervisar aquestes carpetes.

- Comptes: Rubén ha poder crear, llegir i modificar el contingut de la carpeta. Els directius han de tenir permís de lectura per tal de supervisar el contingut.

- Currículums: Raquel ha poder crear, llegir i modificar el contingut de la carpeta. Els directius han de tenir permís de lectura per tal de supervisar el contingut.

- Sistemes: Sandra ha de tenir permís per poder crear, modificar i eliminar el contingut de la carpeta.

- APP: Adrià ha de tenir control total en la carpeta per poder gestionar els permisos d'accés a les subcarpetes així com crear-ne de noves. Andreu i Andrea han de poder accedir als continguts de la carpeta per accedir a les seues subcarpetes.

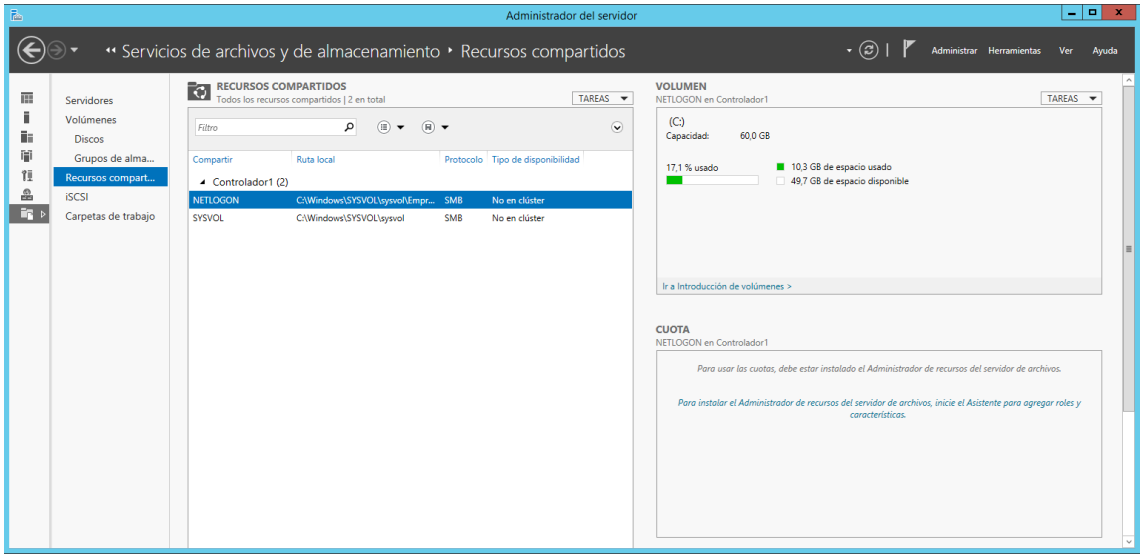
- Android: Andreu ha de tenir permís de lectura, escriptura i eliminar sobre aquesta carpeta. A més ha de rebre l'herència dels permisos de la carpeta pare APP per tal que Adrià gestione els permisos i puga afegir membres als projectes.

- iOS: Andrea ha de tenir permís de lectura, escriptura i eliminar sobre aquesta carpeta. A més ha de rebre l'herència dels permisos de la carpeta pare APP per tal que Adrià gestione els permisos i puga afegir membres als projectes.

- Comercial: Carme ha de tenir permís de lectura, escriptura i eliminar per tal de poder crear les subcarpetes dels clients. La resta d'usuaris de l'empresa han de tenir accés per poder veure els treballs que està realitzant l'empresa.

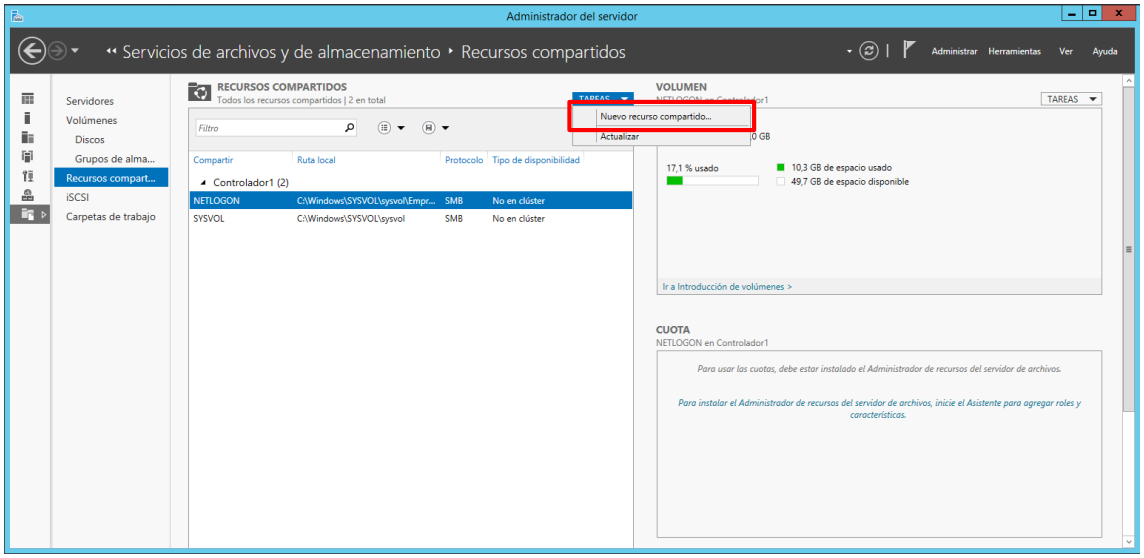
4.4.1 Crear un recurs compartit

Per crear l'estructura de carpetes, s'ha de crear primerament el recurs compartit Recursos. Per a crear un recurs compartit s'ha d'accedir al tauler d'Administració del servidor i seleccionar la pestanya de Recursos Compartits.



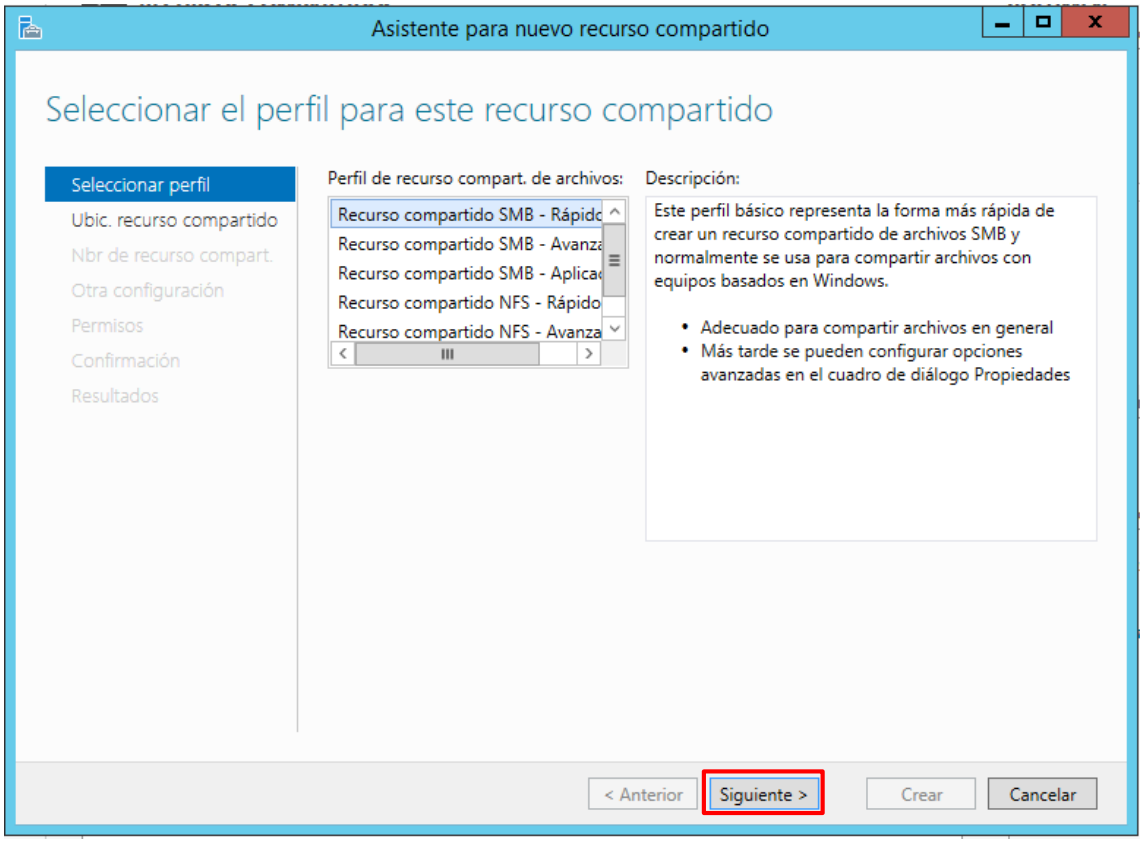
Captura 17 - Tauler de Recursos Compartits

Després d'obrir el tauler de control dels recursos compartits cal picar sobre **"Tareas"** i seleccionar **"Nuevo recurso compartido",** tal i com es mostra en la següent imatge.



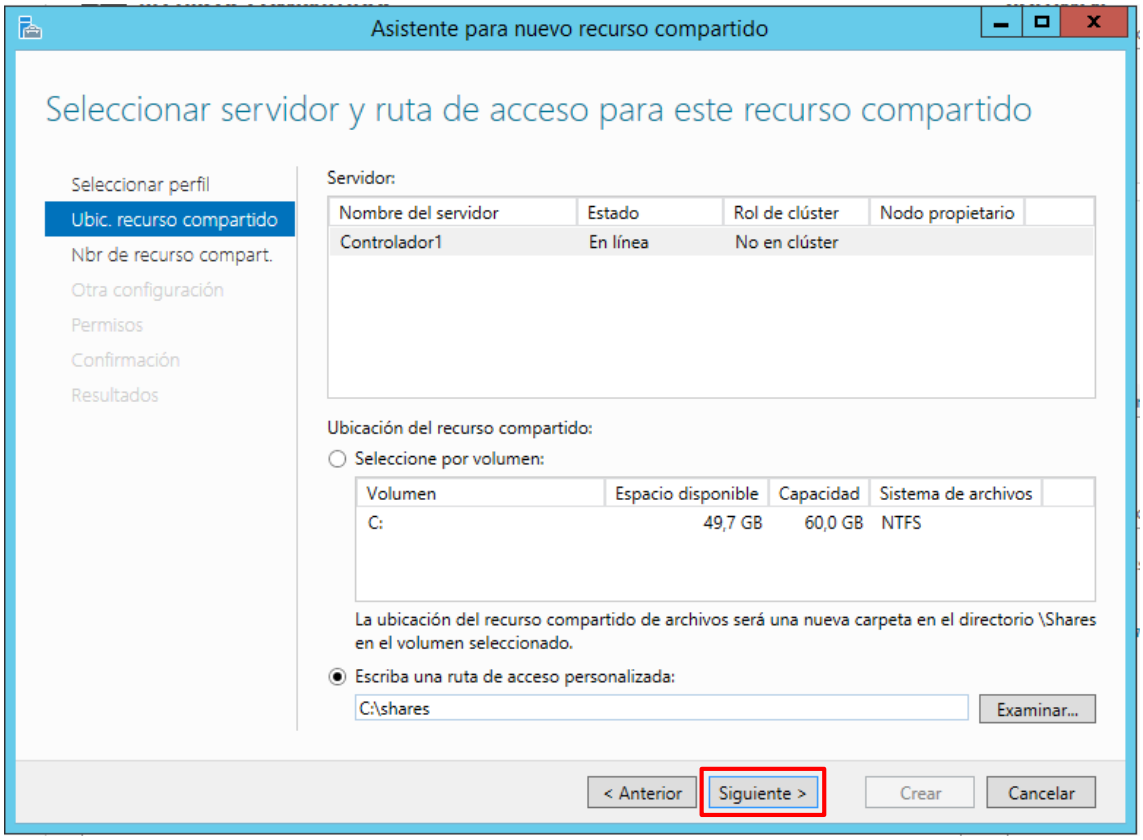
Captura 18 - Crear recurs compartit

En la primera finestra es pica en **"Siguiente"** deixant la configuració per defecte.



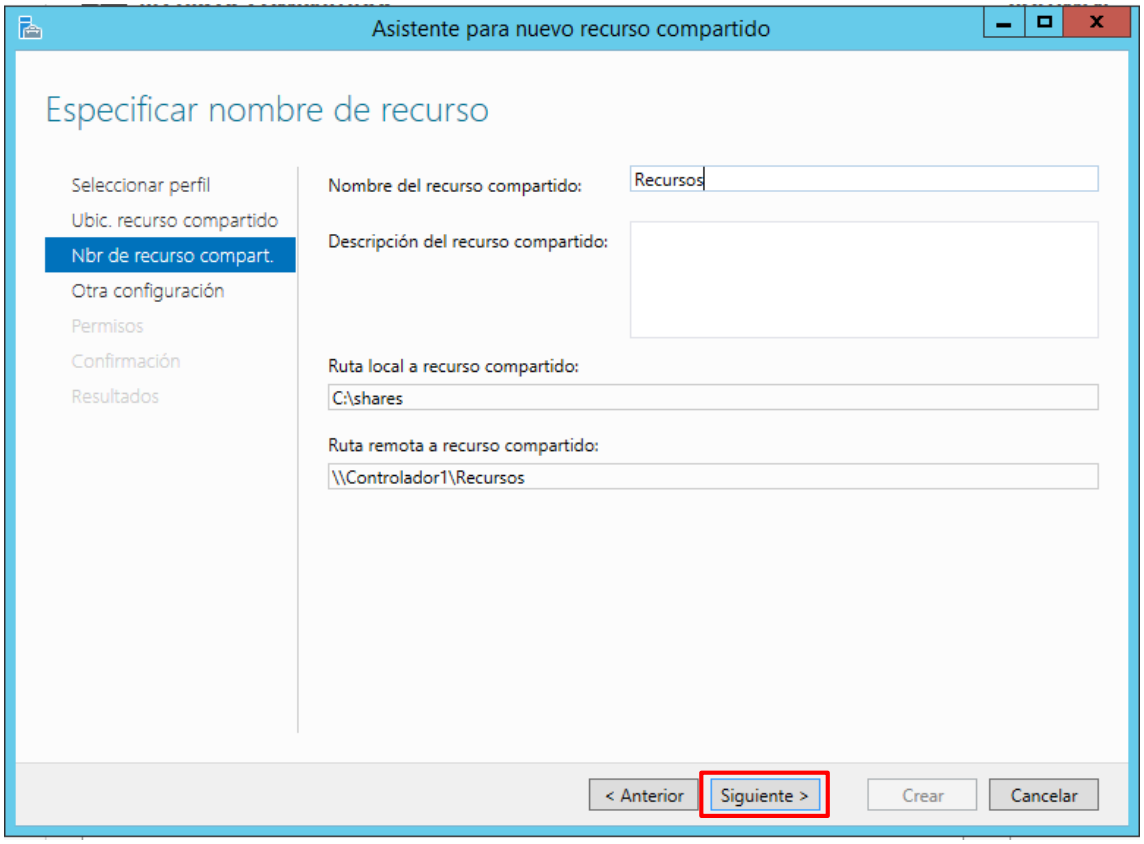
Captura 19 - Selecció de perfil per a recurs compartit

En la següent finestra cal introduir la ruta on es vol crear el recurs compartit. En aquest cas, com l'objectiu principal de crear un recurs compartit es estudiar les opcions de seguretat, es va a crear en el disc del controlador del domini, però en una empresa és més habitual utilitzar un servidor extern d'emmagatzematge per tal de que la disponibilitat no depenga del controlador del domini i no sobregarregar el controlador de domini amb els accessos al recurs. Per tant la ruta escollida per a poder fer l'estudi és **C:\Shares**. Seguidament cal clicar sobre **"Siguiente"** per continuar en la configuració del recurs compartit.



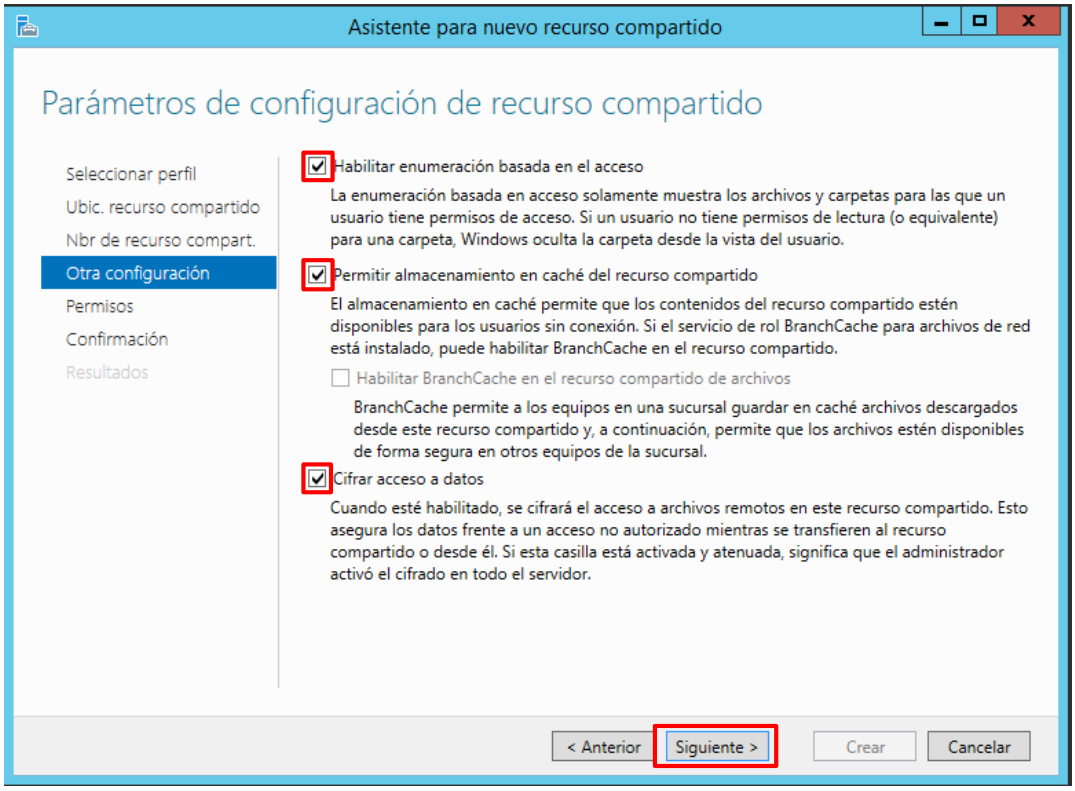
Captura 20 - Ubicació del recurs compartit

En la finestra que apareix a continuació cal indicar el nom del recurs compartit, en aquest cas **Recursos**.



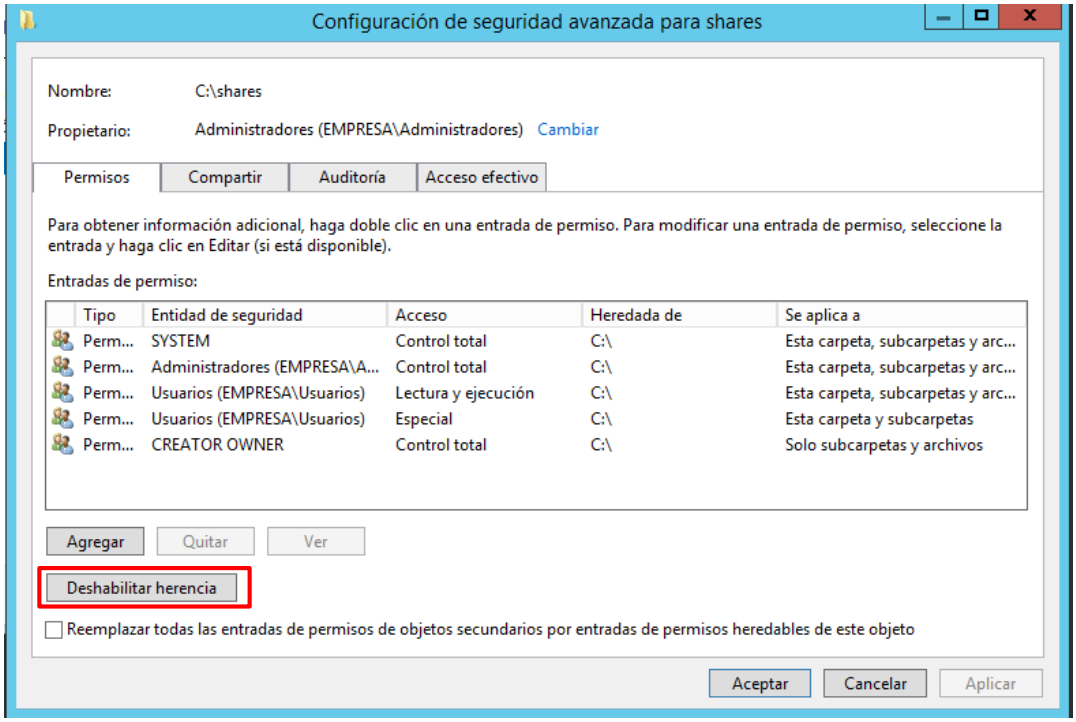
Captura 21 - Nom del recurs compartit

Cal marcar totes les opcions excepte la opció **"Habilitar BranchCache"** i picar en **"Siguiente"** per accedir a la finestra de permisos, on es configuren els permisos per a cada grup/usuari segons els requisits de l'empresa, descrits a l'inici d'aquest apartat.



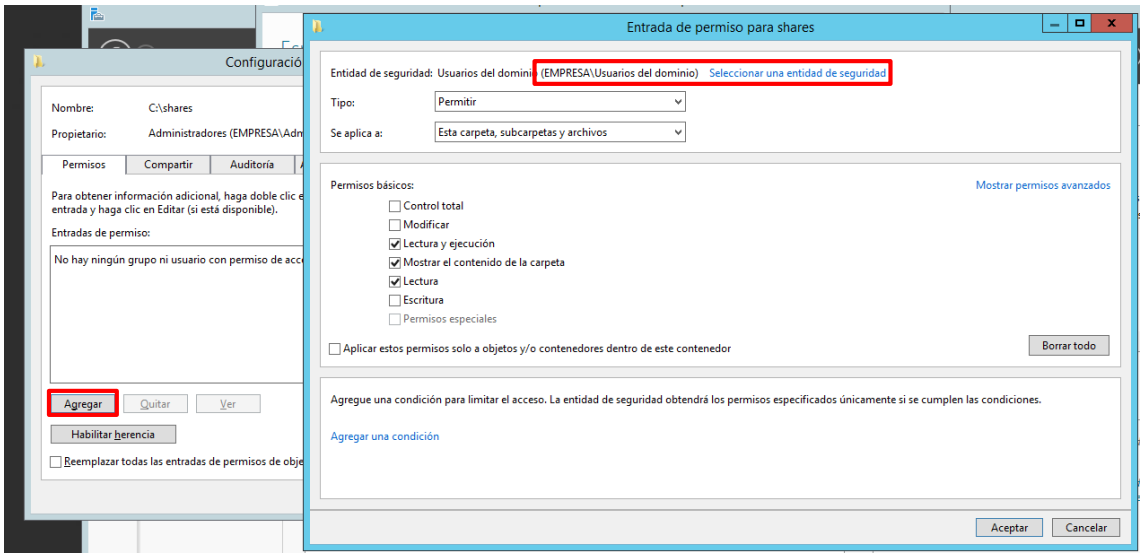
Captura 22 - Paràmetres del recurs compartit

Cal picar en personalitzar permisos. I en la finestra que apareix cal picar en **"Deshabilitar herència"**, per tal de poder assignar els permisos descrits abans.



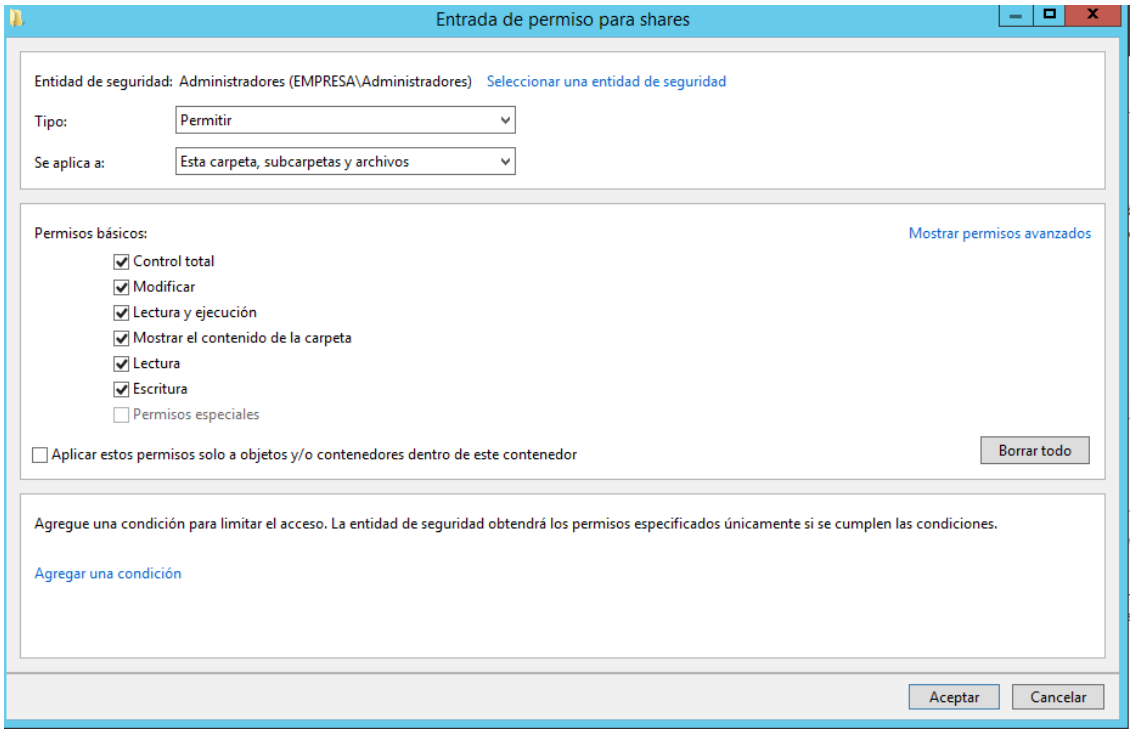
Captura 23 - CoNfiguració de seguretat del recurs compartit

Seguidament, cal picar sobre **"Agregar"** i en la finestra que s'obri seleccionar el grup d'usuaris el domini, per tal d'atorgar permís d'accés i de lectura al recurs compartit.



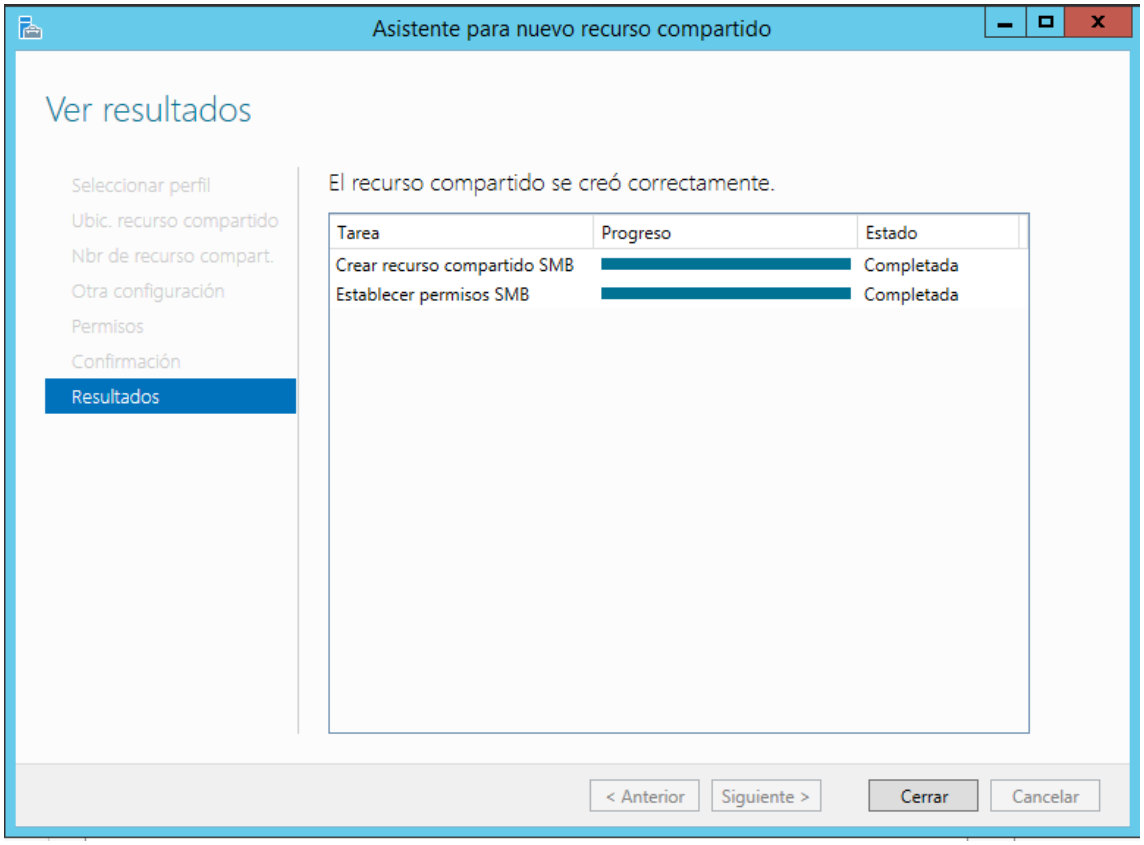
Captura 24 - Afegir grup de seguretat per atorgar permisos

També cal afegir al grup d'administradors i atorgar-li permís de control total, per poder crear les subcarpetes del recurs i modificar-los en cas e ser necessari.



Captura 25 - Selecció de permisos

Després cal acceptar i acabar el procés de creació del recursos compartit en les opcions per defecte.



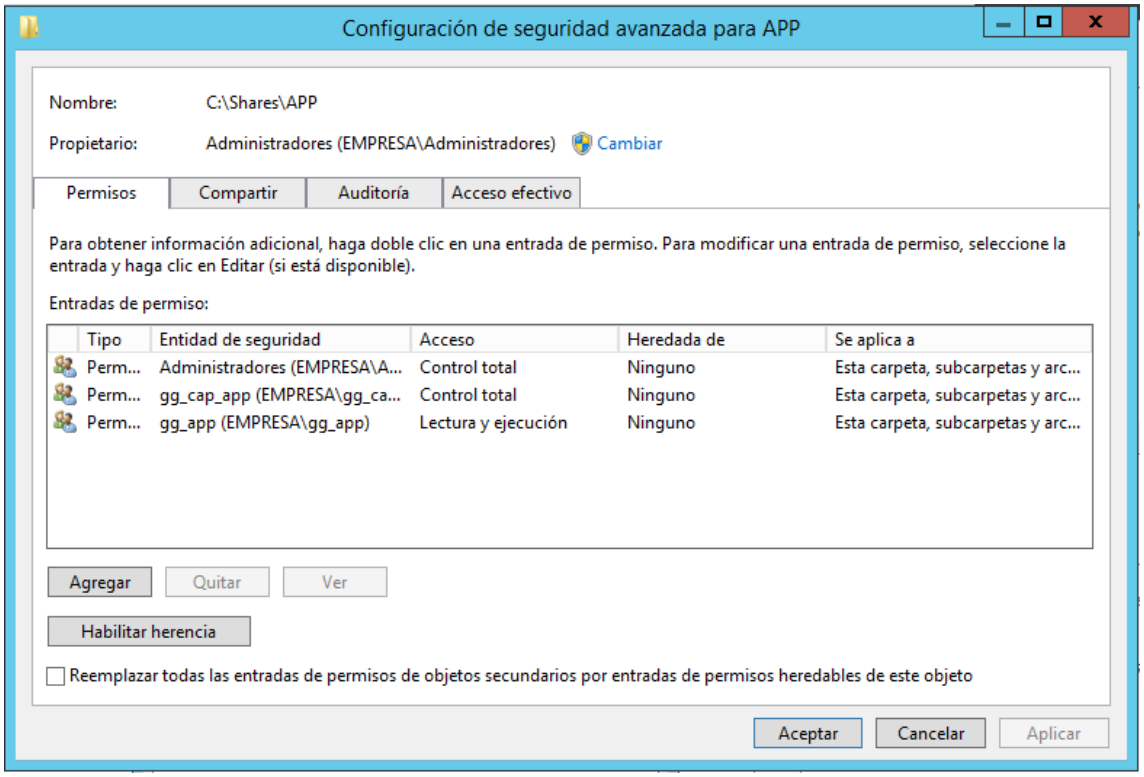
Captura 26 - Finalització de creació de recurs compartit

Després de crear el recurs compartit, es crea l'estructura de carpetes i s'atorga els permisos per a cada carpeta. Per atorgar els permisos, cal desmarcar l'herència en els recursos i afegir els permisos per grups. D'aquesta manera, al atorgar els permisos per grups, facilita la feina d'administrar els permisos, ja que si per exemple, s'incorpora un membre nou al departament de sistemes per a desenvolupar aplicacions Android, només cal afegir-lo als grups gg_app i gg_app_android i automàticament tindrà permís d'accés a la carpeta APP i permís de modificació sobre la carpeta Android.

A continuació es mostra com han quedat els permisos de cada carpeta creada en el recurs compartit.

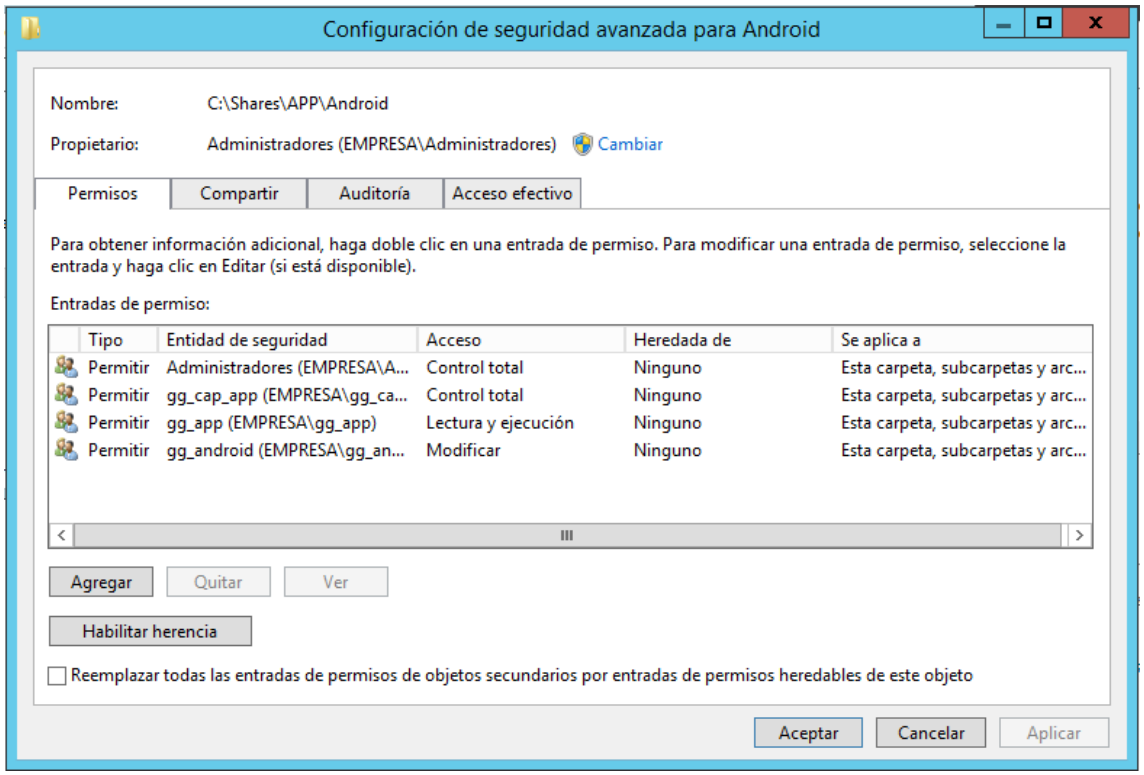
4.4.2 Assignació de permisos

Per a la carpeta APP s'ha afegit al grup gg_cap amb permís control total i al grup gg_app amb permís de lectura.



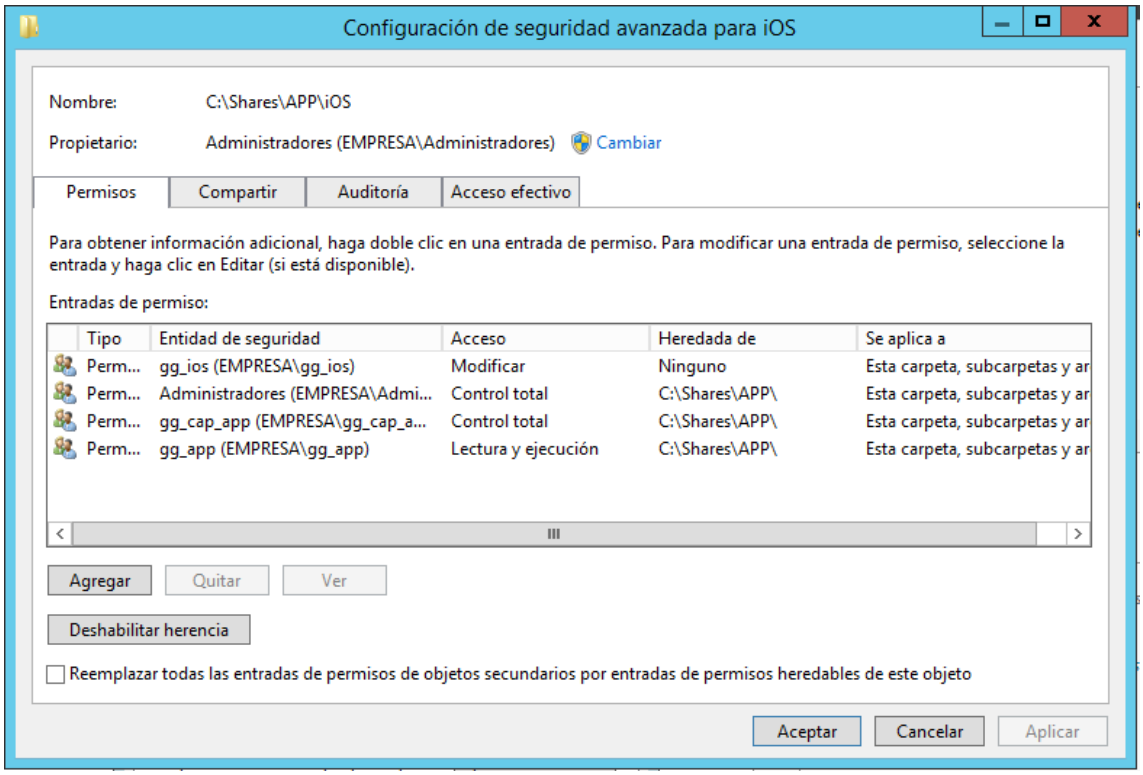
Captura 27 - Configuració de seguretat avançada

En la subcarpeta Android s'ha afegit permís de modificar per al grup gg_andorid, a més dels permisos que obté per herència.



Captura 28 - Atorgar permisos a grups sobre recurs compartit Android

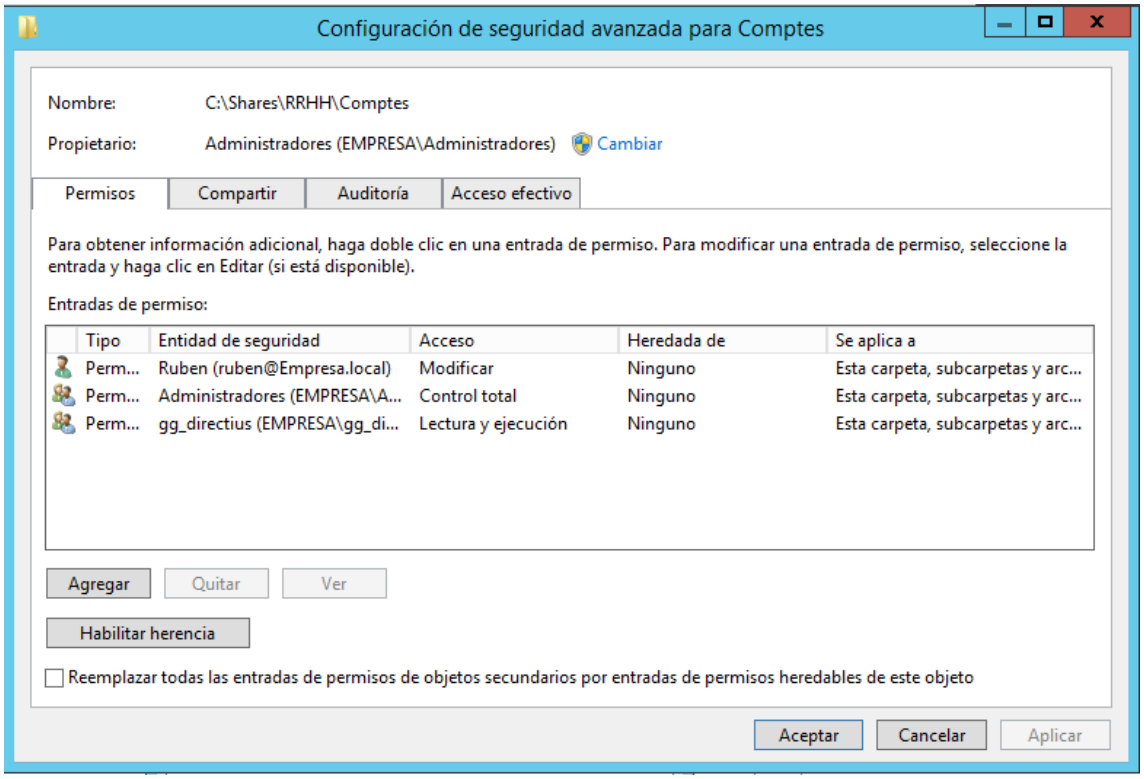
I per a la subcarpeta iOS s'ha afegit al grup gg_ios amb permís de modificar, a més dels heretats.



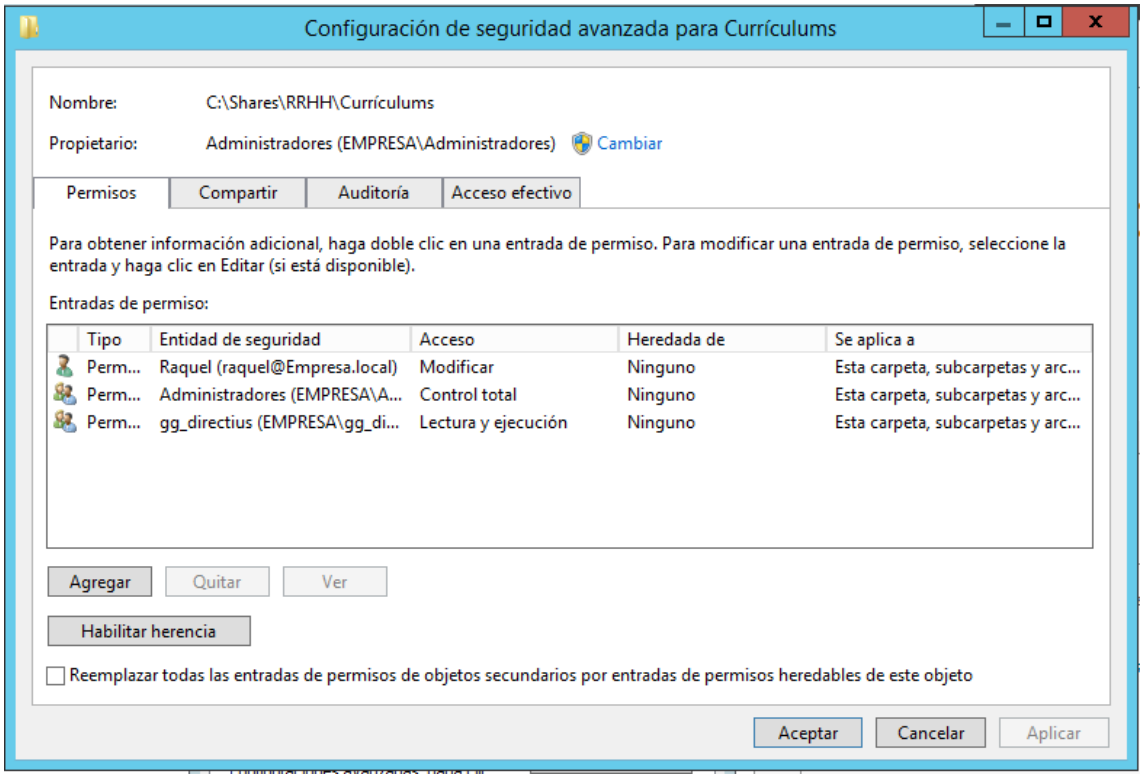
Captura 29 - Atorgar permisos a grups sobre recurs compartit iOS

En el cas de la carpeta RRHH, s'ha afegit el grup gg_directius amb permís de lectura per poder supervisar el contingut de la carpeta i del les subcarpetes i al grup gg_rrhh amb permís de lectura per poder accedir als seus recursos en la carpeta compartida.

A les subcarpetes Comptes i Currículums, a diferència que en les subcarpetes d'APP, s'han afegit els usuaris Rubén i Raquel respectivament. D'aquesta manera es mostra que també es poden assignar permisos per usuari, però, tal i com s'ha exposat en el cas de les subcarpetes d'APP, és recomanable assignar els permisos als grups, perquè facilita la gestió d'aquests a curt i llarg termini. A continuació es mostra com han quedat els permisos per a les carpetes Comptes i Currículums.



Captura 30 - Permisos sobre recurs compartit Comtes



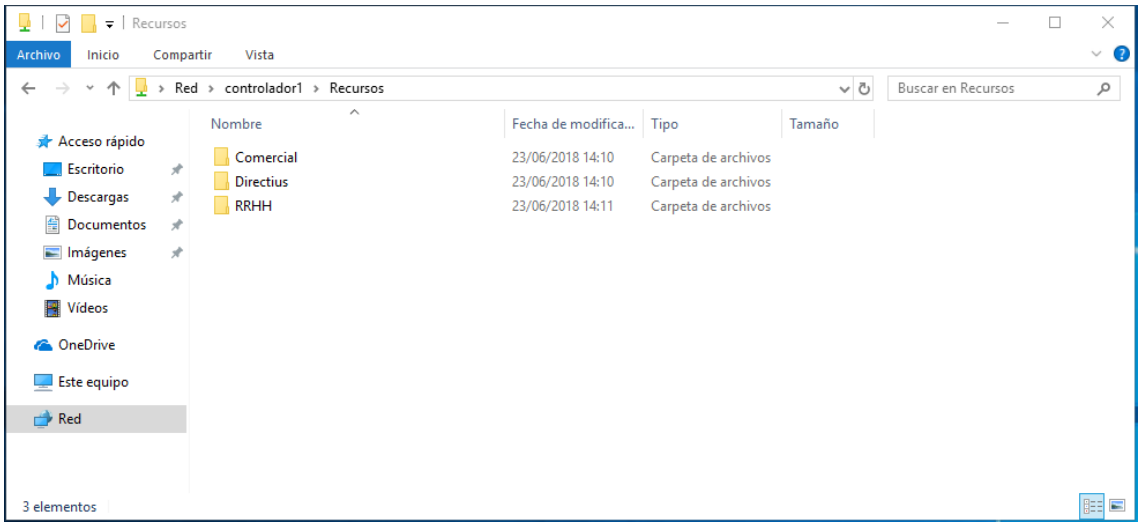
Captura 31 - Permisos sobre recurs compartit Currículums

D'aquesta manera s'han assignat els permisos a la resta de carpetes del recurs compartit, Sistemes, Comercial i Directius.

4.4.3 Comprovació del funcionament dels permisos asignats

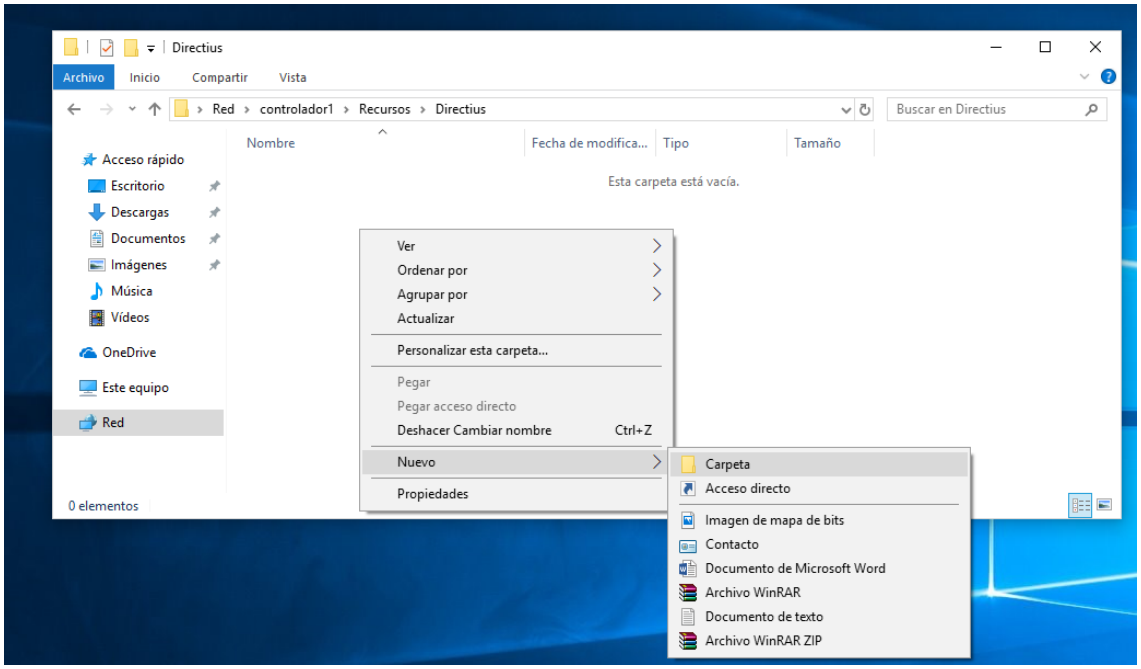
Per tal de comprovar el funcionament dels permisos assignats a cada grup/usuari, s'ha accedit al recurs compartit des de l'equip de treball amb l'usuari Dani, membre del grup gg_directius.

Com es pot veure en la imatge següent, Dani te accés a la carpeta Directius, a RRHH i a Comercial.

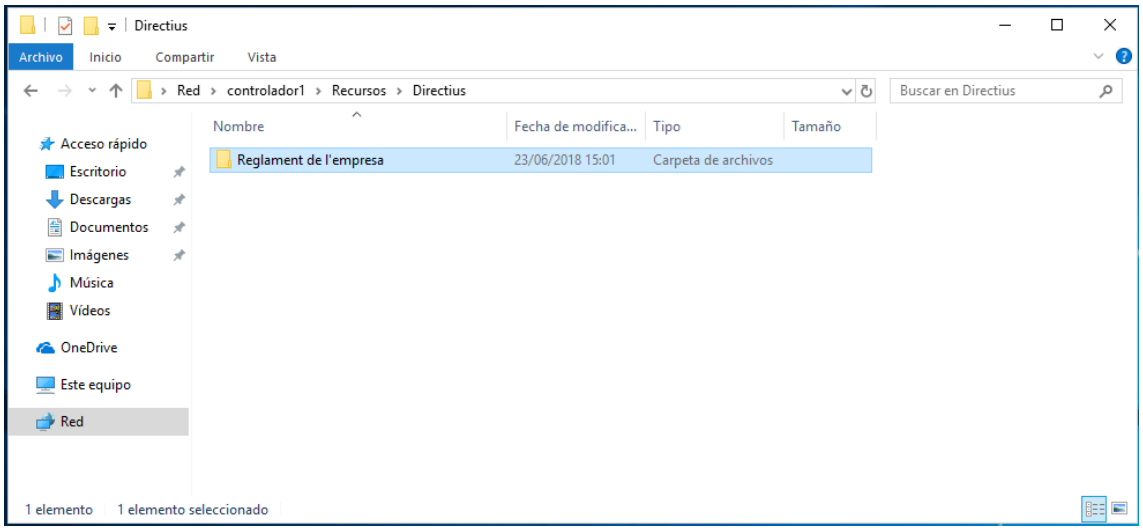


Captura 32 - Accés sobre el recurs compartit de l'usuari Dani

En la carpeta Directius pot crear i modificar les arxius existents, tal i com es pot observar en l'exemple de la creació de la carpeta Reglament de l'empresa en la carpeta Directius.

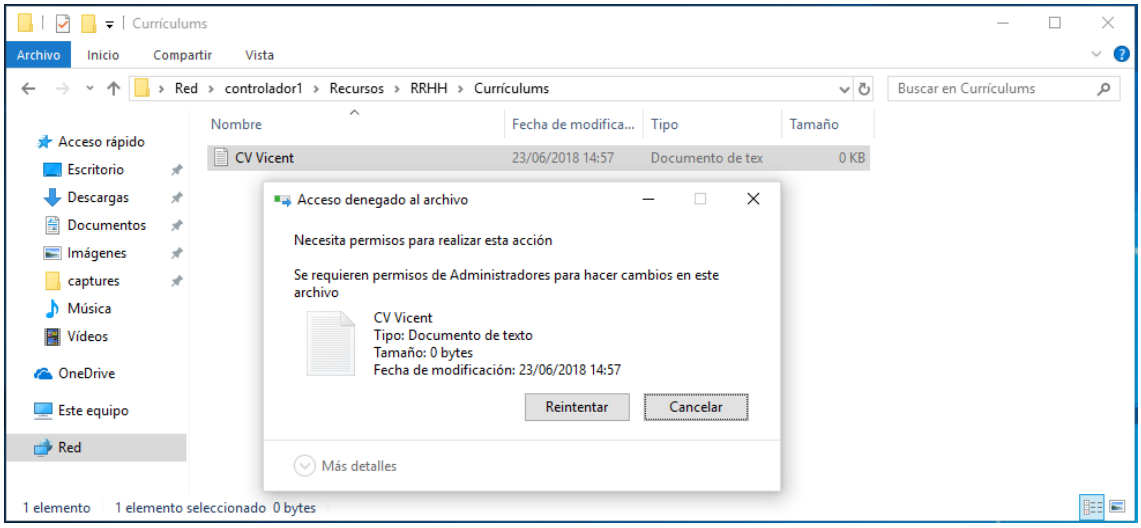


Captura 33 - Exemple de permís modificació de l'usuari Dani sobre recurs compartit Directius

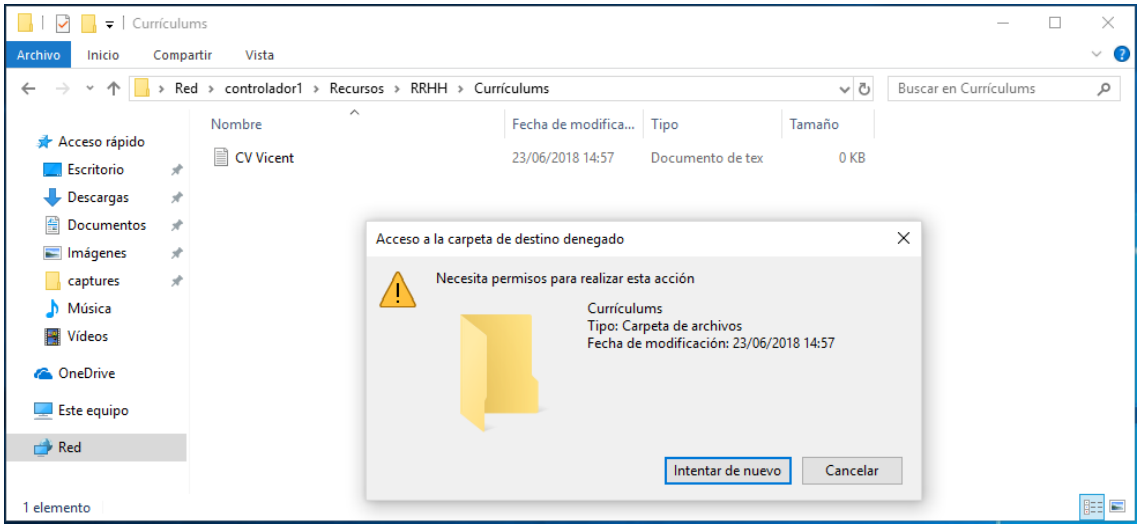


Captura 34 - Creació de carpeta per l'usuari Dani sobre el recurs compartit Directius

En canvi, en la carpeta RRHH i les subcarpetes d'aquesta així com en la carpeta Comercial solament té permís de lectura, per tant, no pot crear ni modificar cap arxiu. A l'intentar crear una carpeta o eliminar un arxiu en la subcarpeta Currículums, mostra un avís informant que calen permisos i aquest usuari no els té, tal i com es pot observar en les següents captures de pantalla.

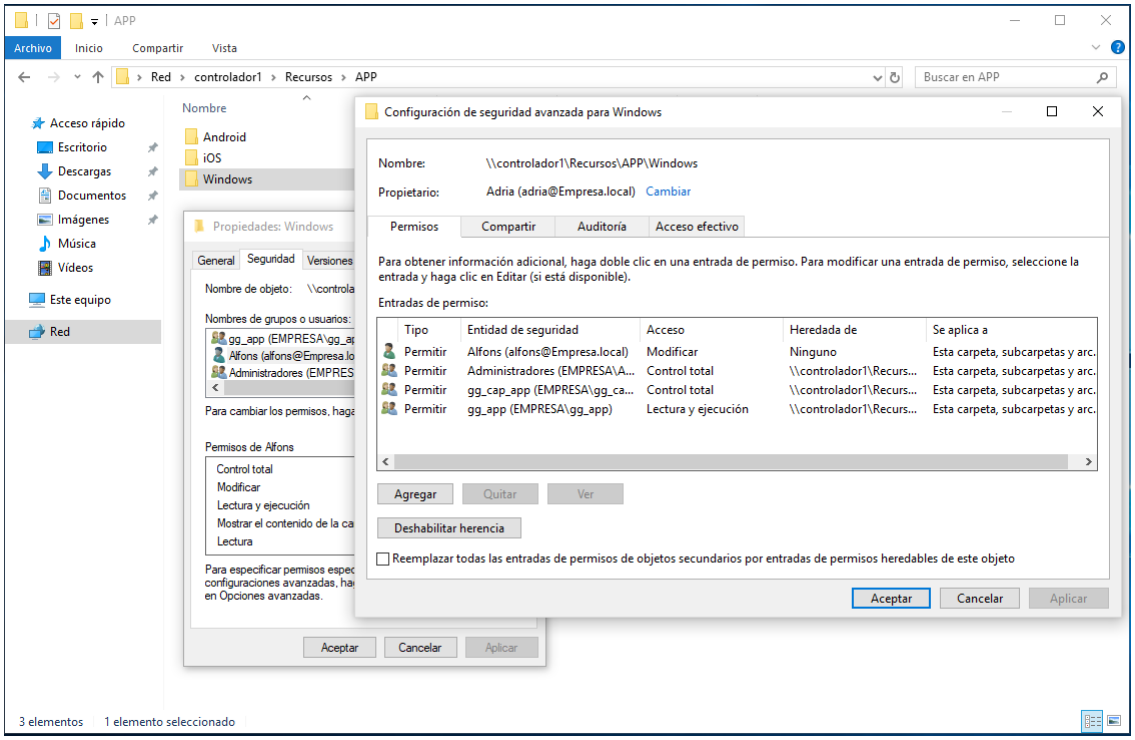


Captura 35 – Missatge de denegació de permís per a eliminar document



Captura 36 - Missatge de denegació de permís per a crear carpeta

Per un altra banda, l'usuari Adrià, membre del grup gg_cap_app, ha accedit a la carpeta APP i ha creat una subcarpeta per a un projecte de desenvolupament en Windows Phone, i a atorgat permís de modificació a Alfons, un treballador que ha contractat l'empresa per a desenvolupar aquests tipus de projectes. Adrià a pogut realitzar aquestes accions perquè el grup gg_cap_app té control total sobre aquesta carpeta. A continuació es mostra una captura de pantalla dels permisos de la nova carpeta creada.



Captura 37 - Permissos sobre el recurs compartit Windows

4.5 Directives de grup

La directiva de grup es una infraestructura que permet especificar configuracions i preferències específiques per als usuaris i equips. Les configuracions d'aquestes directives es troben en els objectes de directiva de grup (GPO). Els GPO es poden aplicar en diversos agents de l'Active Directory, com els dominis, els llocs (sites), o unitats organitzatives. A través de la consola d'administració de directives de grup (GPMC) es poden administrar la configuració i preferències de les directives de grup.

Es possible que diverses GPO entren en conflicte i es per això que tenen un ordre jeràrquic de preferència respecte als diferents agents als que es poden assignar. Aquest ordre va des dels llocs, menys preferència, passant per els dominis i finalment, les unitats organitzatives com a més prioritaris. A més, les directives de grup son acumulatives. Per tant, si dues directives son contradictòries, es tindrà en compte la de més prioritat, en canvi, si no ho son, s'acumlen.

La configuració de les directives de grup son d'una gran complexitat, però permeten reduir considerablement la gestió i configuració de tots els recursos de de l'empresa.

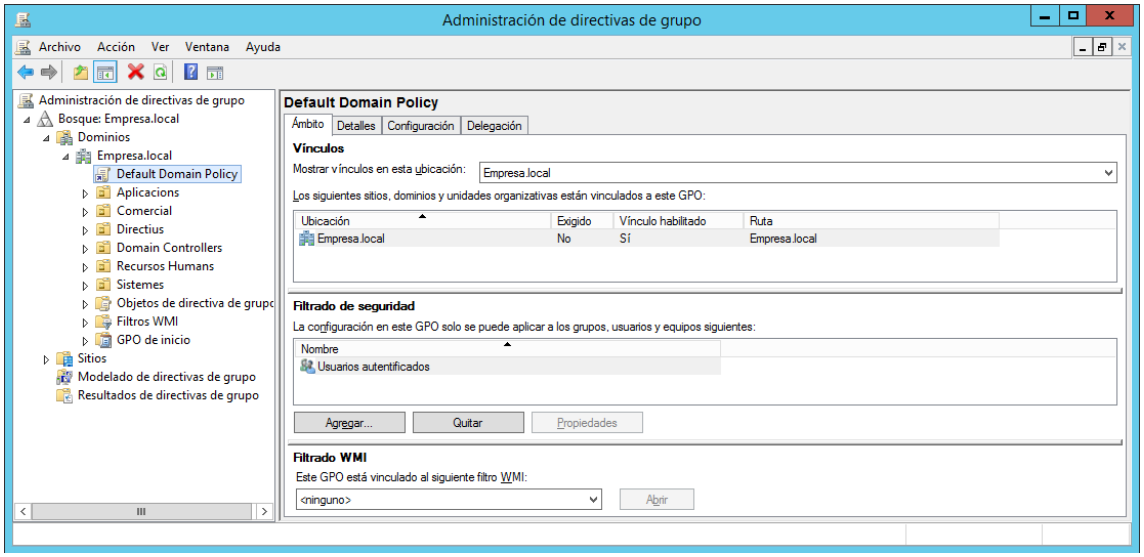
Per defecte, després de la creació del domini, es creen dues polítiques per defecte:

- **Default Domain Policy:** Aquesta directiva afecta a totes les unitats organitzatives del domini, ja que es situa en l'arrel d'aquest. A través d'aquesta directiva es pot configurar paràmetres de contrasenya i bloqueig, i paràmetres que afecten a tots els objectes del domini o paràmetres d'auditoria.

- **Default Domain Controller Policy:** Aquesta directiva afecta a la unitat organitzativa Domain Controlers i permet configurar els paràmetres d'assignació de drets i d'opcions de seguretat.

En els següents apartats es va a mostrar quins paràmetres ofereix Windows Server per a configurar el mètode d'autenticació a través de les directives de grup i també quines opcions existeixen per dur a terme una auditoria a través de directives de grup.

Per poder gestionar les polítiques de seguretat, cal obrir el tauler d'administració de directives de grup.



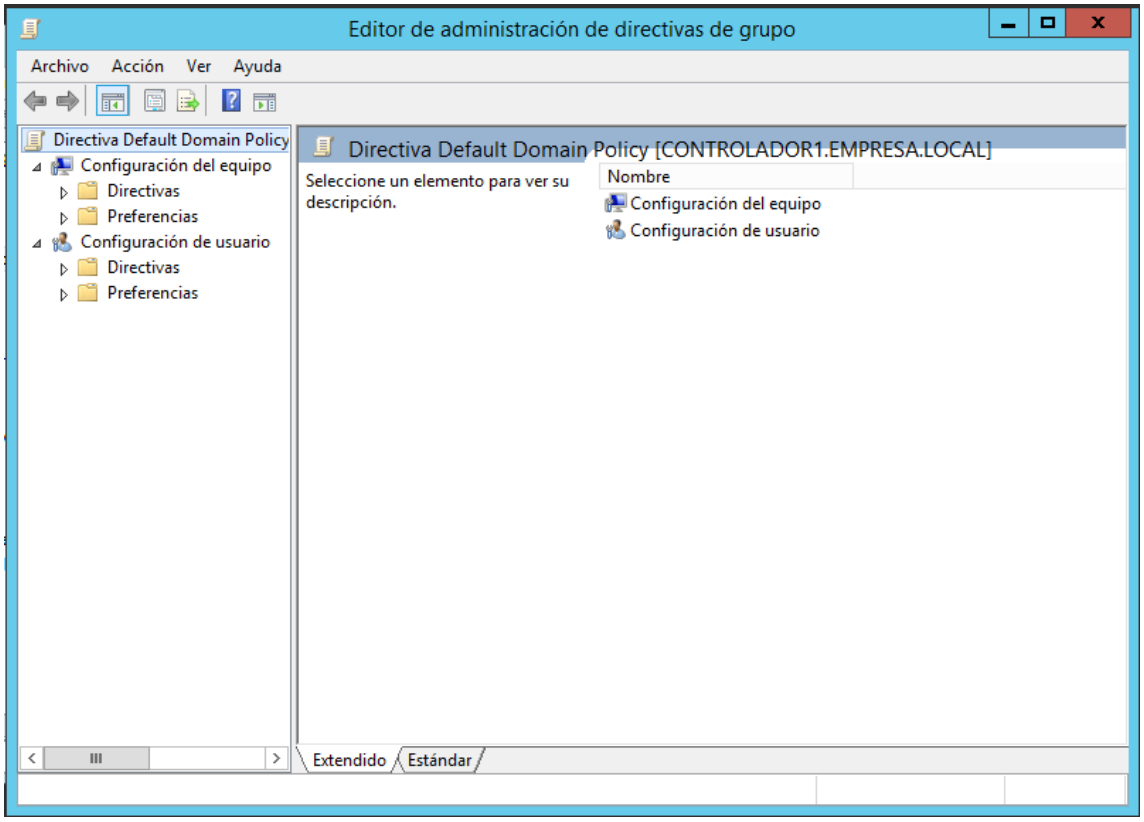
Captura 38 - Tauler d'administració de directives de grup

Com es pot observar, a l'arrel del domini, està la GPO Default Domain Policy.

4.5.1 Configuració directiva de compte

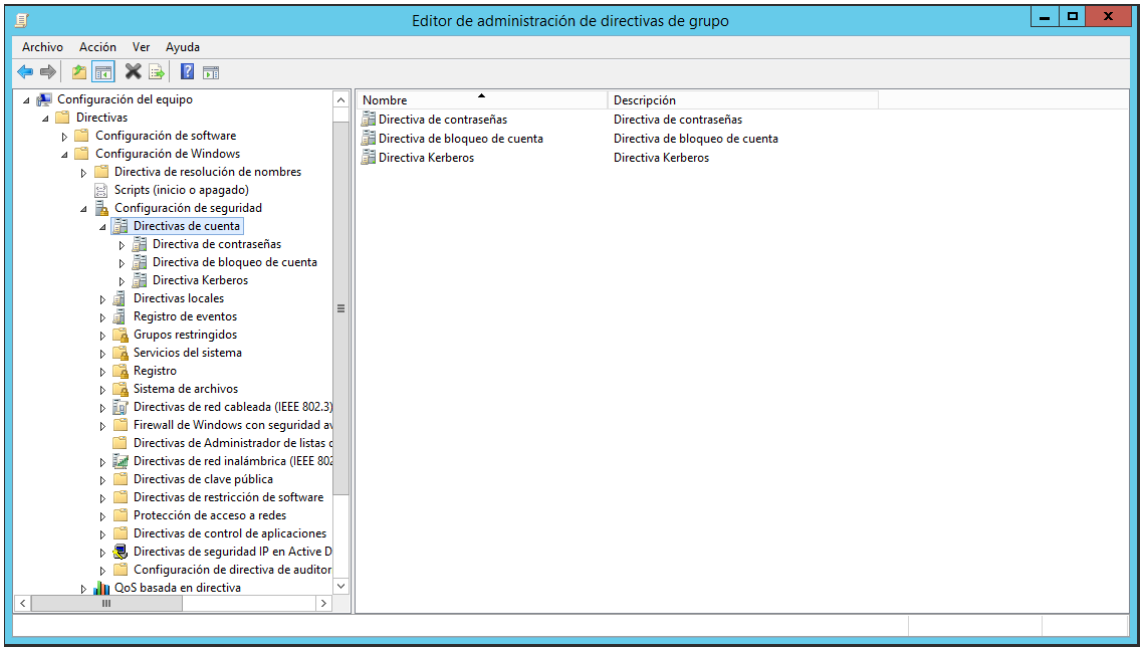
La directiva de compte inclou la configuració de la **directiva de contrasenyes**, la **directiva de bloqueig** de compte i la **directiva de Kerberos**. Tots els ajustaments que es modifiquen en aquestes directives afecten a nivell de domini i per tant es converteix en la directiva predeterminada local de tots els equips del domini.

Per tal de modificar la directiva de compte Default Domain Policy es pica en el botó dret sobre aquesta GPO i es selecciona editar.



Captura 39 - Editor de directives de grup

Per tal d'editar la configuració d'autenticació en aquesta GPO, cal accedir a la Configuració de Windows, Configuració de Seguretat i Directives de compte.



Captura 40 - Directives de compte

Kerberos

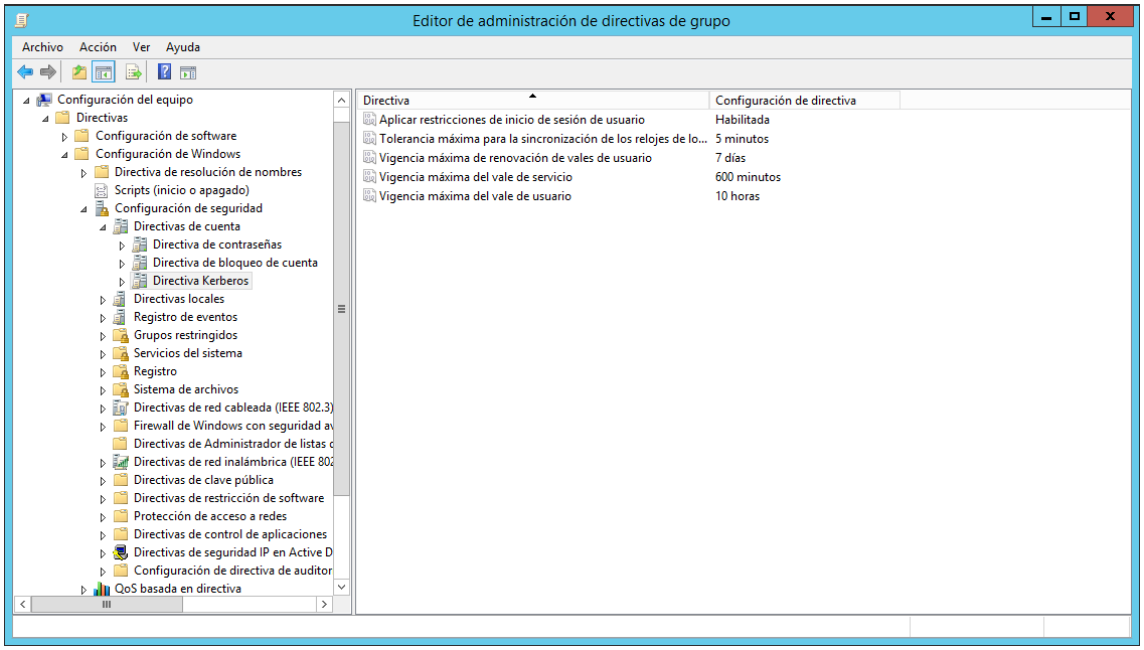
Windows Server 2012 implementa les extensions i el protocol d'autenticació de la versió 5 de Kerberos per a l'autenticació de la clau pública, el transport de les dades d'autorització i la delegació. Aquest protocol d'autenticació s'utilitza per comprovar la identitat d'un usuari o d'un equip.

Per a l'autenticació d'un usuari en el directori actiu a través de Kerberos s'han de tenir en compte tres elements:

- La **màquina client**, on es troba l'usuari que vol accedir al servei.
- La **màquina que ofereix el servei**.
- El **Centre de distribució de claus Kerberos (KDC)**, que és un servidor central que s'encarrega d'autenticar els usuaris a través de tiquets per a que s'identifiquen contra les màquines que ofereixen els serveis. En aquest cas, el KDC està integrat en el controlador de domini.

El KDC proveeix dos serveis fonamentals: el d'autenticació (AS, Authentication Service) i el de tiquets (TGS, Ticket Granting Service. El servei AS, te com a funció autenticar inicialment als clients i proporcionar un tiquet per comunicar-se en el TGS, que proporcionarà als clients les credencials necessàries per a comunicar-se en el servidor final que ofereix el servei mitjançant un tiquet (TGT, Ticket-Granting Ticket), el qual inclou el període de validació del tiquet a més de la informació necessària per a dur a terme l'autenticació.

Mitjançant les directives de grup es poden configurar diferents paràmetres per a l'autenticació amb Kerberos. Si es selecciona les Direcitves de Kerberos, es pot observar els diferents paràmetres que es poden configurar.



Captura 41 - Directiva Kerberos

Aplicar restriccions d'inici de sessió d'usuari: Aquesta configuració de directiva determina si el KDC valida cada sol·licitud de val de sessió en la directiva de drets d'usuari del compte d'usuari.

Tolerància màxima per a la sincronització dels rellotges: Aquesta configuració de directiva determina el màxim de temps en minuts que el protocol Kerberos tolera com a diferència entre el rellotge del client i l'hora del controlador de domini.

Vigència màxima de renovació de vals d'usuari: Aquesta configuració de directiva determina els dies durant el que es pot renovar el val de concessió de vals d'usuari.

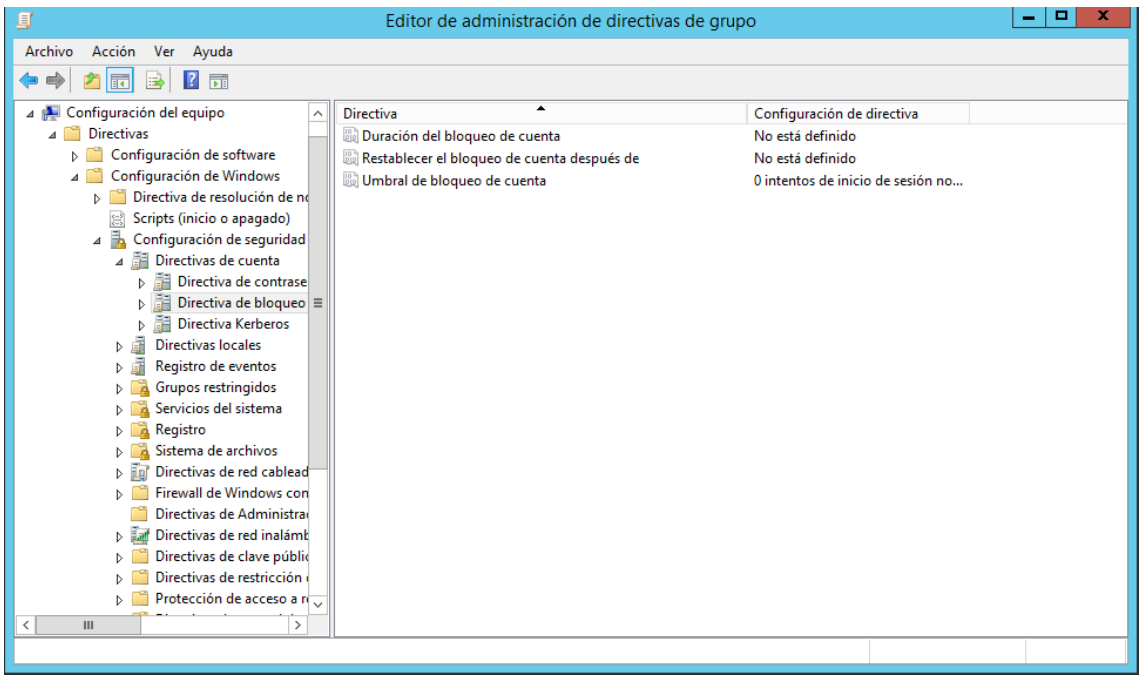
Vigència màxima del val de servei: Aquesta configuració de directiva determina el número màxim de minuts que un val de sessió pot utilitzar-se per tenir accés a una servei determinat.

Vigència màxima del val d'usuari: Aquesta configuració de directiva determina el número màxim d'hores en que es pot utilitzar un val de concessió de vals d'usuari.

Directiva de Bloqueig de compte

Els controladors de domini fan un seguiment dels intents d'inici de sessió d'un usuari per tal de controlar que un usuari malintencionat no probe accedir utilitzat intentant encertar les contrasenyes d'un altre usuari. En la directiva de Bloqueig de compte, es poden configurar els controladors de domini per a respondre a aquests tipus d'atacs, deixant el compte sense ús durant un període de temps o bloquejant el compte.

Els paràmetres que es poden configurar són els següents:



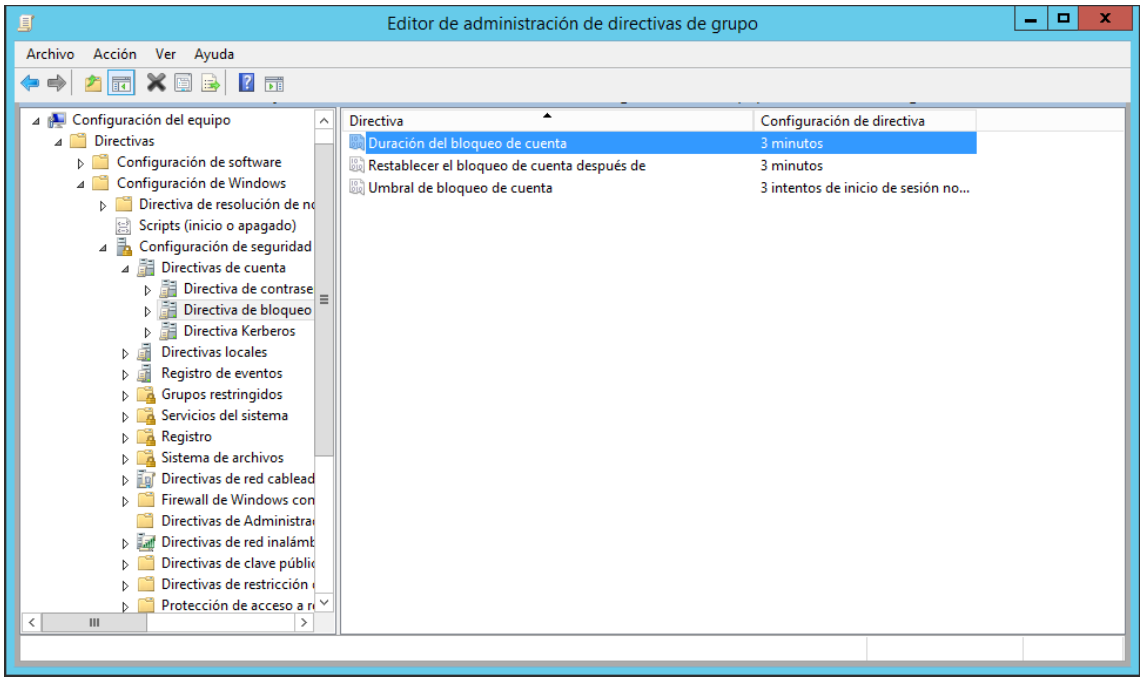
Captura 42 - Directiva de Bloqueig de compte

Umbral de bloque de cuenta: Aquesta configuració de seguretat determina el número d'intents d'inici de sessió incorrectes que fan que un compte d'usuari es bloquegi. Aquest compte no podrà utilitzar-se fins que l'administrador el restablisca o fins que expire la duració de bloqueig. Si el valor s'estableix en 0, el compte mai es bloquejarà.

Duración del bloque de cuenta: Aquesta configuració de seguretat defineix en número de minuts que un compte roman bloquejat abans de desbloquejar-se automàticament. Si el valor s'estableix en 0, el compte queda bloquejat fins que l'administrador el desbloquege.

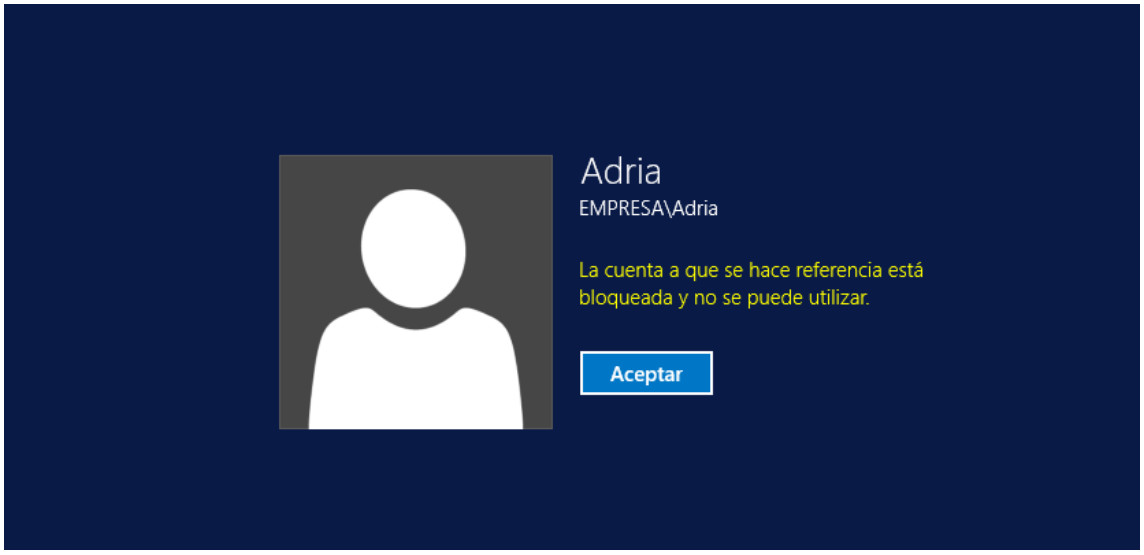
Restablecer el bloqueo de cuenta después de: Aquesta configuració de seguretat determina el número de minuts que han de transcorres fins que el controlador d'intents d'inici de sessió incorrectes es restablisca a 0 després d'un intent incorrecte.

Per tal de comprovar el funcionament d'aquestes directives s'ha fet una prova on s'ha establert l'umbral en 3 intents, la duració del bloqueig de compte de 3 minuts i el restabliment del bloqueig de 3 minuts.



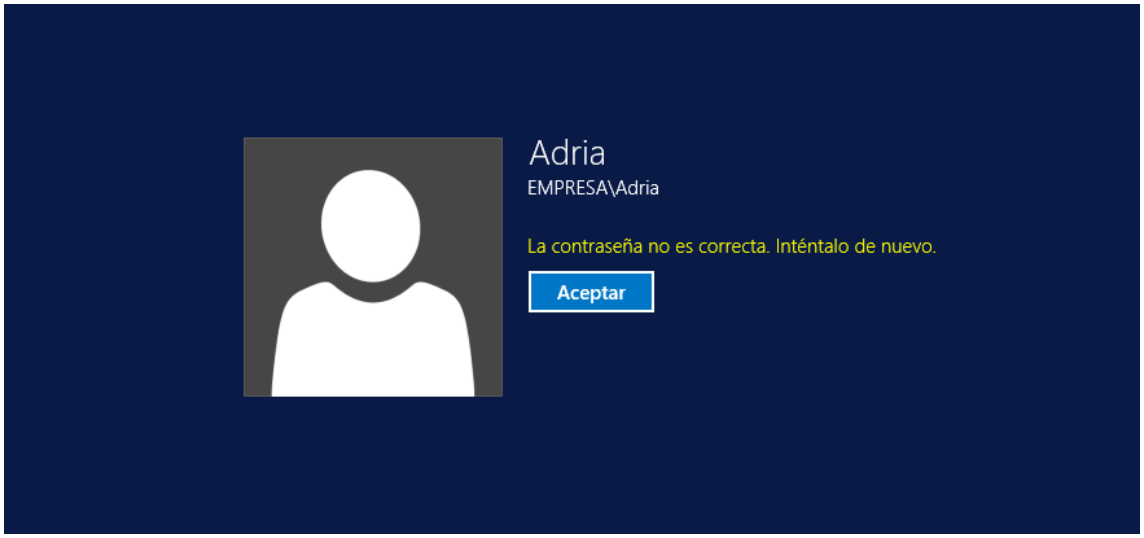
Captura 43 - Configuració dels paràmetres de la directiva de bloqueig

Al intentar iniciar sessió en l'usuari Adria tres vegades amb una contrasenya incorrecta el compte es bloqueja i no es pot utilitzar.



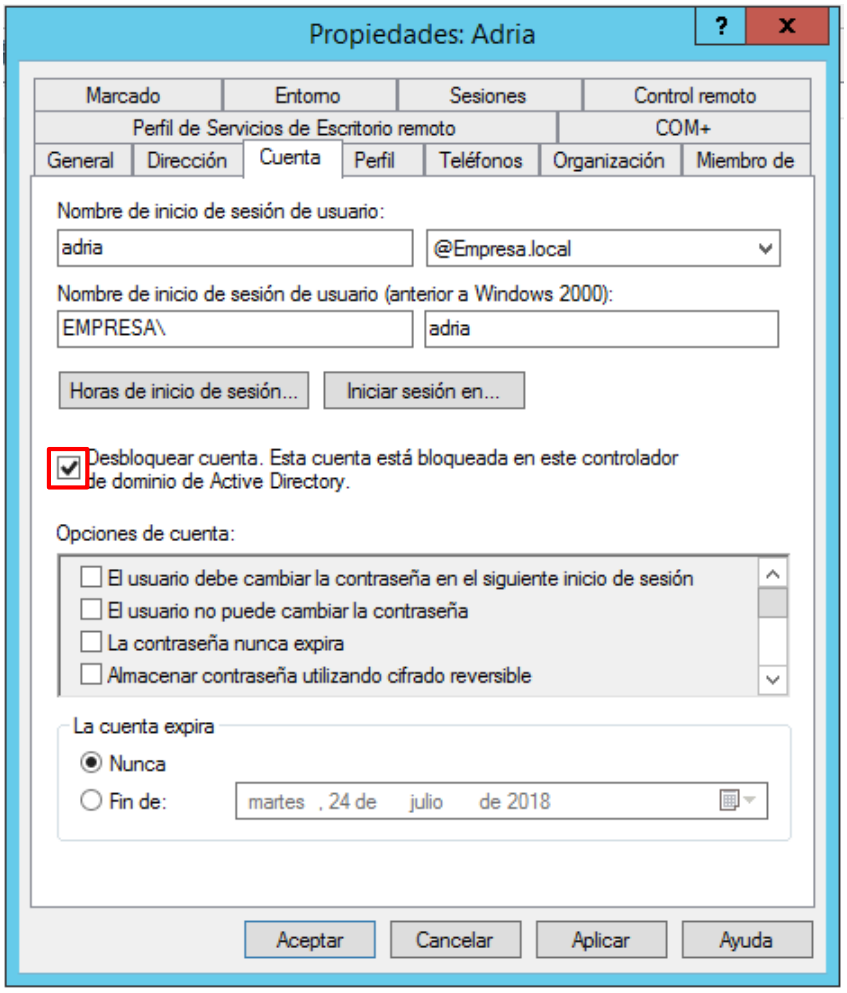
Captura 44 - Bloqueig compte de l'usuari Adria

Passats 3 minuts ja es pot tornar a utilitzar el compte.



Captura 45 - Restabliment del bloqueig de compte de l'usuari Adria per temps

Un altra configuració més estricta es deixar la duració del bloqueig en 0, així l'única forma de restablir el compte ha de ser mitjançant l'autorització de l'administrador. Després d'intentar tres voltes accedir en el comte d'Adria, el compte s'ha bloquejat i l'única manera de desbloquejar el compte ha sigut amb l'autorització de l'administrador.

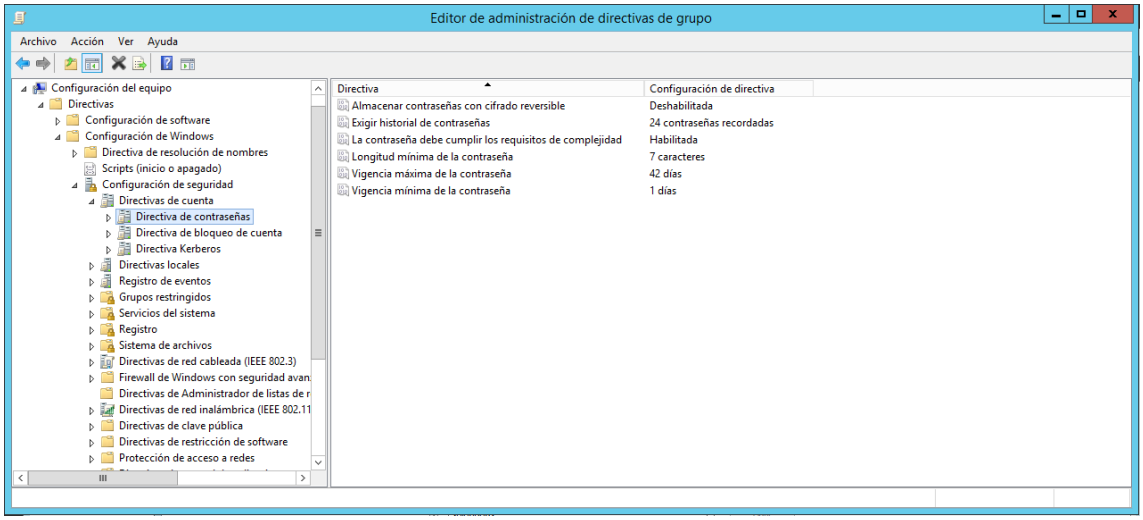


Captura 46 - Desbloqueig del compte de l'usuari Adria per l'administrador

Directiva de Contrasenyes

La forma que tenen els usuaris d'autenticar-se es mitjançant una contrasenya. Aquesta contrasenya ha de tenir uns paràmetres de seguretat per tal que a usuaris malintencionats no els resulte fàcil esbrinar les contrasenyes dels usuaris i poder accedir al sistema sense estar autoritzat.

Mitjançant les directives de contrasenya, es poden definir els següents paràmetres per configurar les contrasenyes d'una manera més segura.



Captura 47 - Directiva de contrasenyes

"Almacenar contraseñas con cifrado reversible": Aquesta configuració de seguretat determina si el sistema operatiu emmagatzema contrasenyes de xifrat reversible, que vol dir que emmagatzema versions de text simple de les contrasenyes. Aquesta directiva no hauria d'habilitar-se, menys en els casos que els requisits de l'aplicació tinguen més importància que la necessitat de protegir la informació de contrasenyes.

"Exigir historial de contraseñas": Aquesta configuració de seguretat determina el número de noves contrasenyes que es poden associar a un compte d'usuari abans de poder reutilitzar una contrasenya antiga. Aquesta directiva permet garantir que no es reutilitzen contínuament contrasenyes antigues.

"La contrasenya debe cumplir los requisitos de complejidad": Aquesta configuració de seguretat permet establir els requisits de complexitat definits com que una contrasenya ha d'acomplir els següents requisits:

- No ha de contenir el nom de compte de l'usuari o parts el nom complet d'aquests en més de dos caràcters consecutius.
- Ha de tenir una longitud mínima de sis caràcters.
- Ha d'incloure caràcters de tres de les següents categories:
  - Majúscula (de la A a la Z)
  - Mínuscula (de la a a la z)
  - Dígits de base 10 (del 0 al 9)
  - Caràcters no alfanumèrics (per exemple, !, @, ?, %)

"Longitud mínima de la contraseña": Aquesta configuració de seguretat estableix el número mínim de caràcters que ha de contenir la contrasenya.

"Vigencia màxima de la contraseña": Aquesta configuració estableix un període de caducitat per ala contrasenya.

"Vigencia mínima de la contraseña": Estableix una durada mínima abans de poder canviar la contrasenya.

4.5.2 Auditoria

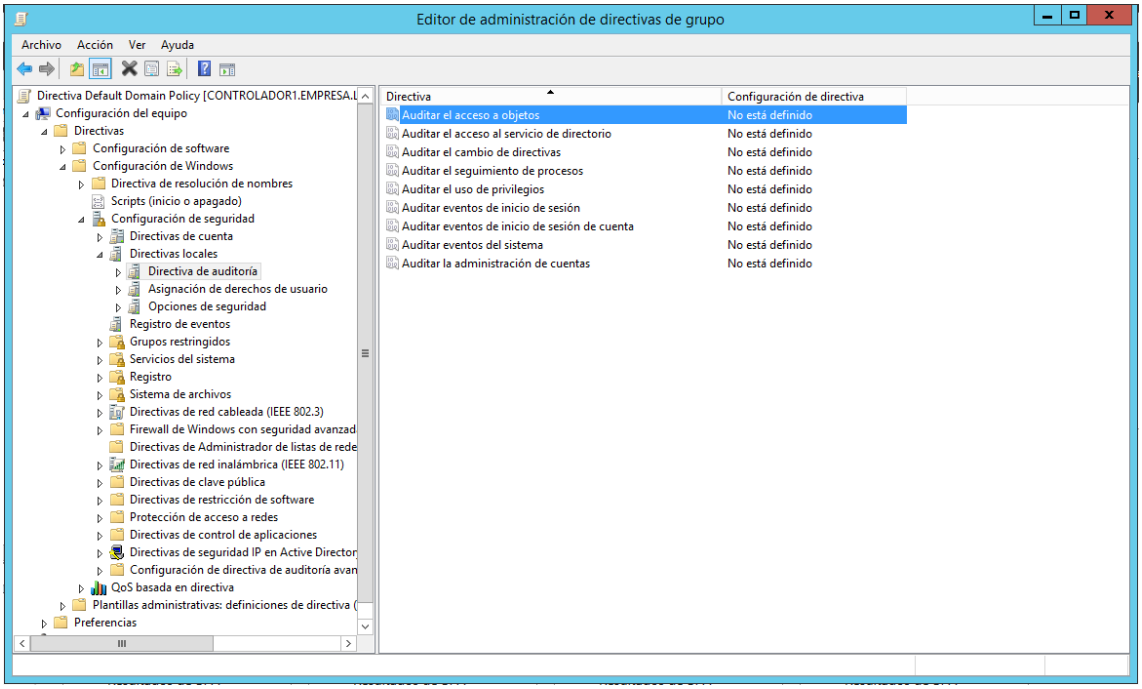
Una de les principals característiques dels paràmetres de seguretat es poder auditar que està passant en el sistema. D'aquesta manera, l'administrador pot centrar-se en les errades de configuració del sistema per poder corregir-les i saber que esta passant en tot moment.

Mitjançant directives de grup, es poden definir diversos tipus d'auditories de seguretat. En aquest apartat es van a implementar les directives de seguretat de d'accés a objectes i esdeveniments d'inici de sessió.

Auditar l'accés a objectes

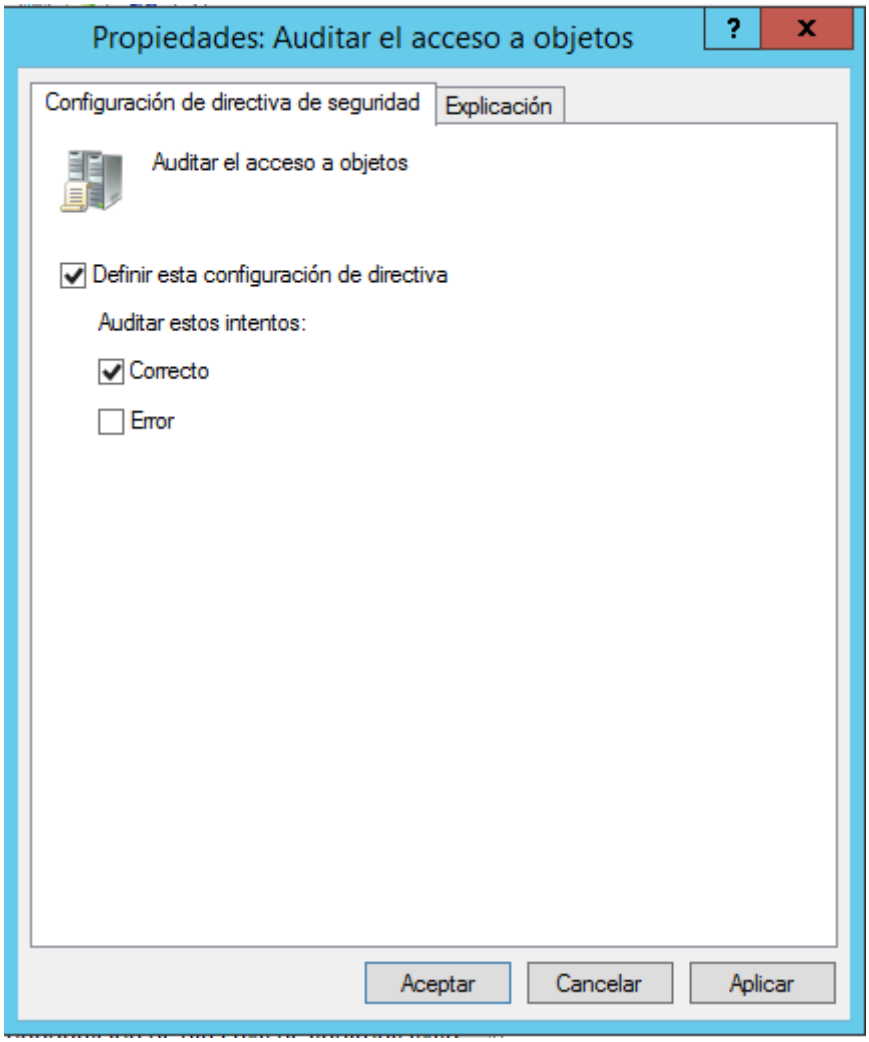
A través de la directiva d'auditoria es va a auditar l'accés al recurs compartit Recursos que s'ha creat en l'apartat 4.4.2. D'aquesta manera, l'administrador pot saber qui ha creat, modificat o eliminat elements del recurs compartit.

Per poder aplicar aquesta directiva s'ha d'anar fins al paràmetre **"Auditar el acceso a objectos"** dintre de la directiva de seguretat.



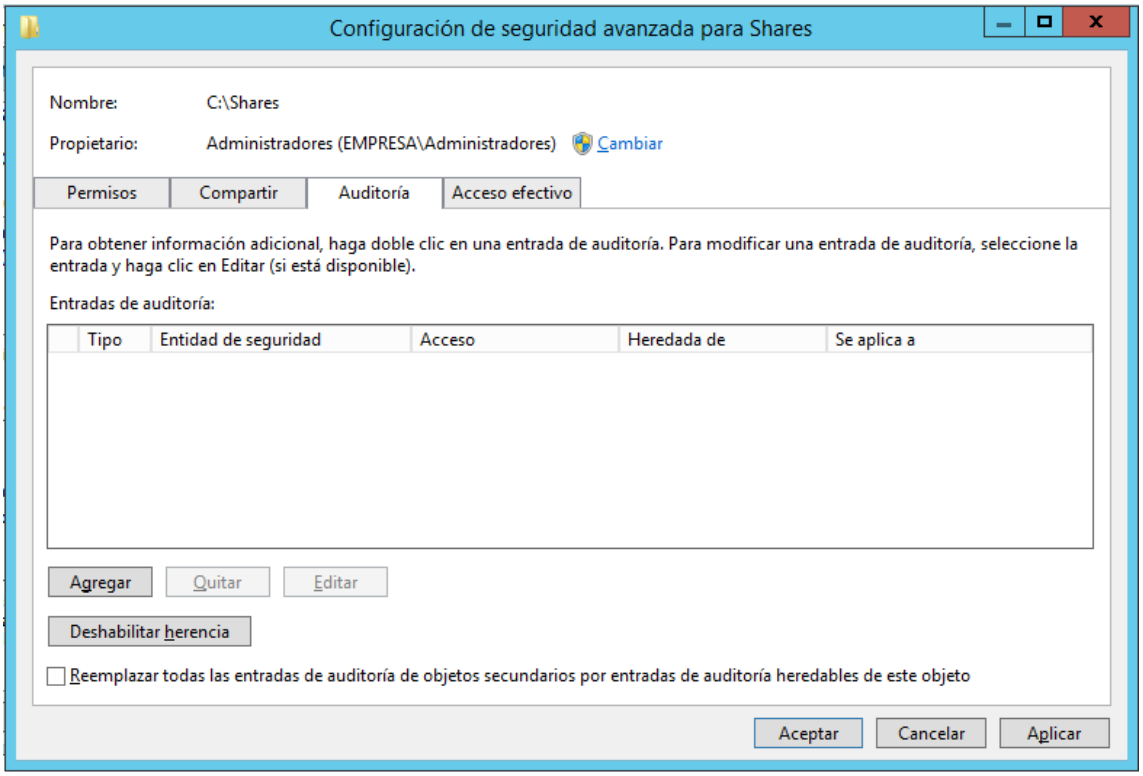
Captura 48 - Directiva d'auditoria

Al accedir a les propietat de la directiva d'auditar el accés a objectes es mosta la opció de seleccionar els intents correctes i de error. En aquest cas solament es van a auditar els intents correctes. Al habilitar aquesta opció es va a generar una entrada d'auditoria cada vegada que un compte obtinga accés correcte.



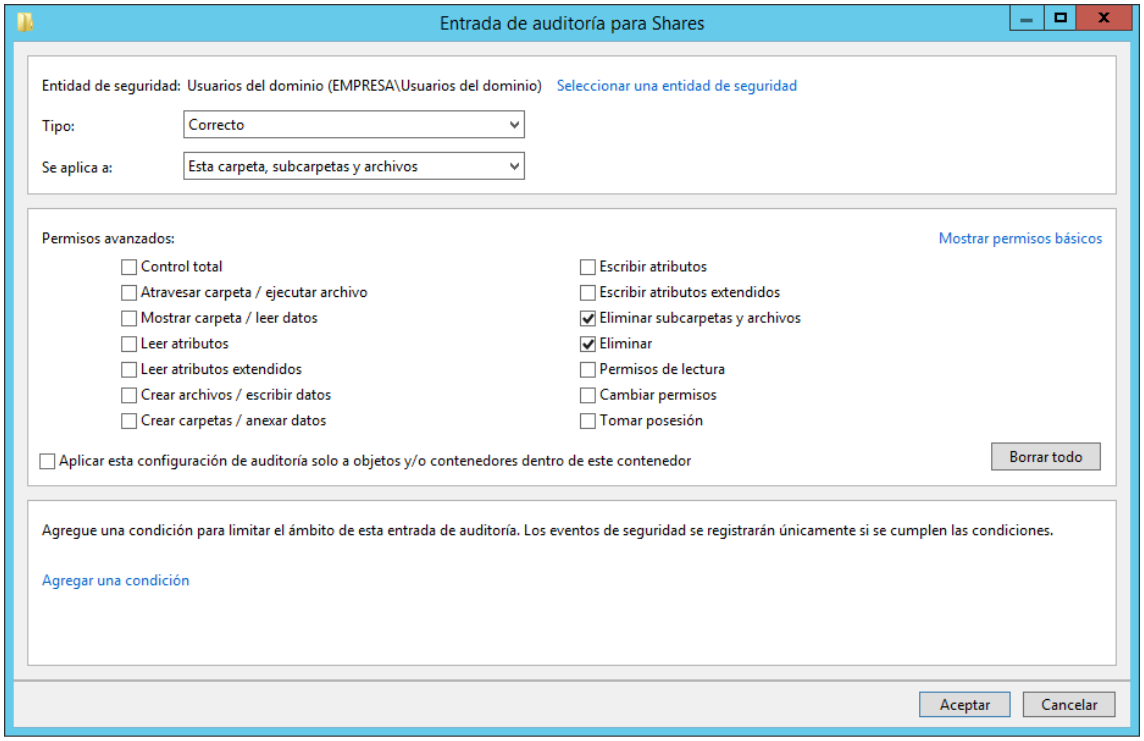
Captura 49 - Auditar l'accés a objectes

Una vegada configurada la directiva, s'accedeixen a les propietats del recurs compartit i en la pestanya de seguretat es picant sobre opcions avançades. En la finestra que s'obri cal anar a la pestanya d'auditoria.



Captura 50 - Configuració de l'auditoria del recurs compartit

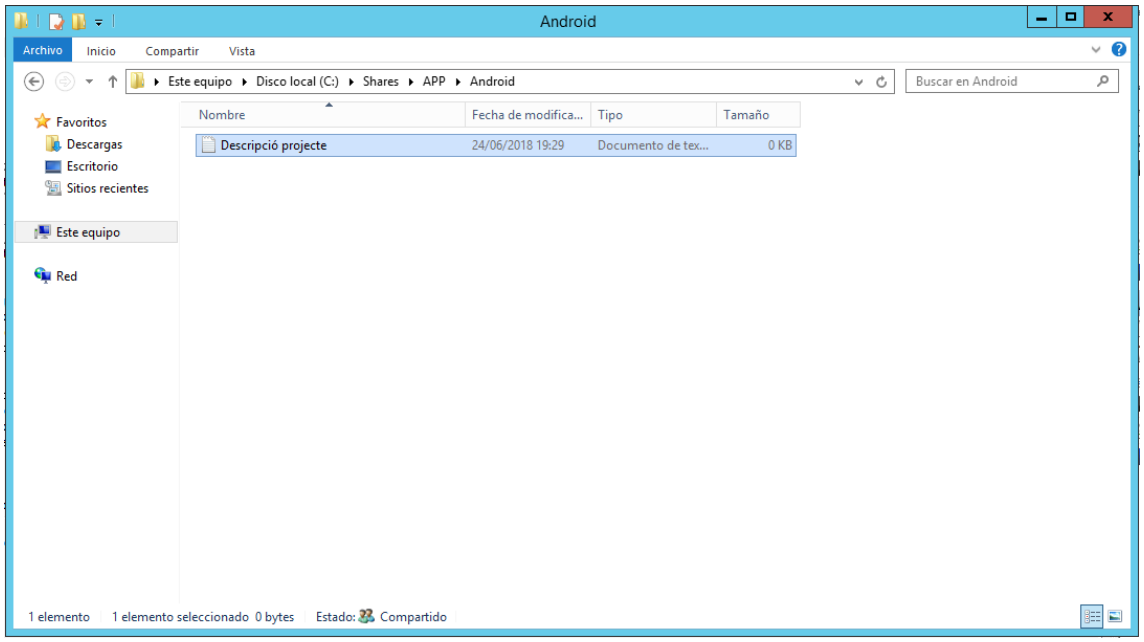
A continuació cal afegir una nova entrada d'auditoria. En aquest cas, s'ha afegit per als usuaris del domini i per auditar les accions d'eliminar. D'aquesta manera, cada vegada que un arxiu o carpeta siga eliminada, quedarà auditat per a que l'administrador del sistema supervise en cas de ser necessari qui ha sigut l'usuari que ha eliminat un arxiu.



Captura 51 - Auditoria d'eliminació sobre recurs compartit

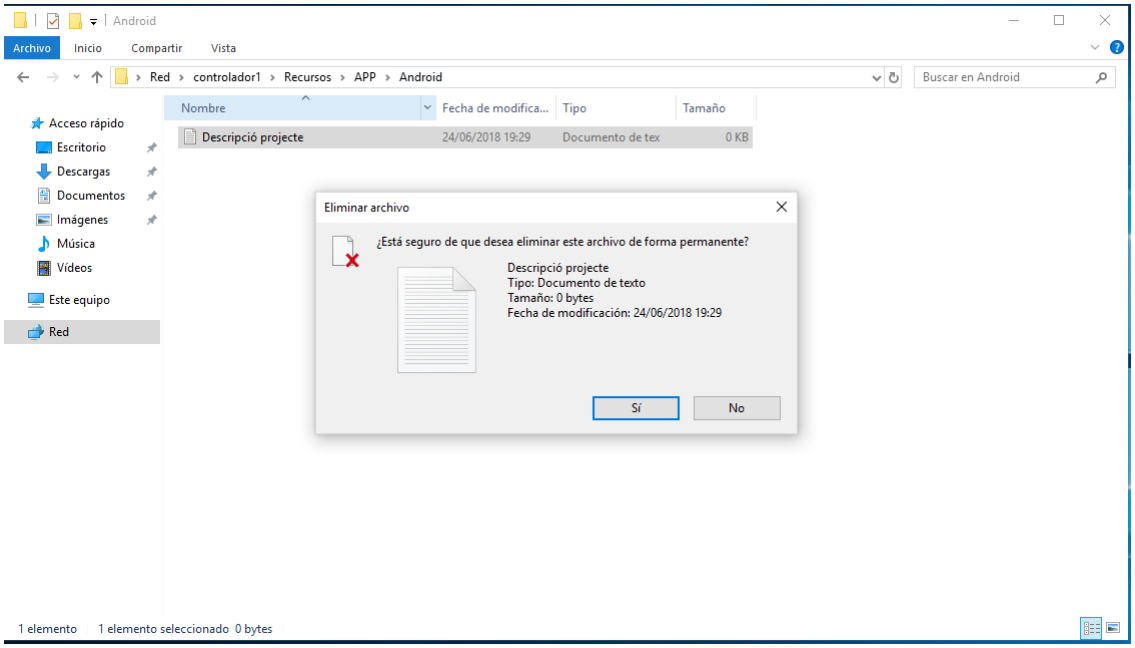
Després de configurar el paràmetre d'auditoria del recurs compartit s'ha realitzat un exemple pràctic per veure el seu funcionament.

Dins del recurs compartit en la subcarpeta d'APP, Android, s'ha creat un arxiu de text on s'indica la descripció d'un projecte.



Captura 52 - Creació d'un arxiu de text en la carpeta compartida Android

Des de l'equip de treball, Andreu, ha eliminat aquest arxiu de text.



Captura 53 – Eliminació de l'arxiu de text en la carpeta compartida Android

Una vegada realitzada l'operació, es registra aquest esdeveniment en el sistema. Per poder veure els esdeveniments del sistema, s'obri el **"visor de eventos"**.

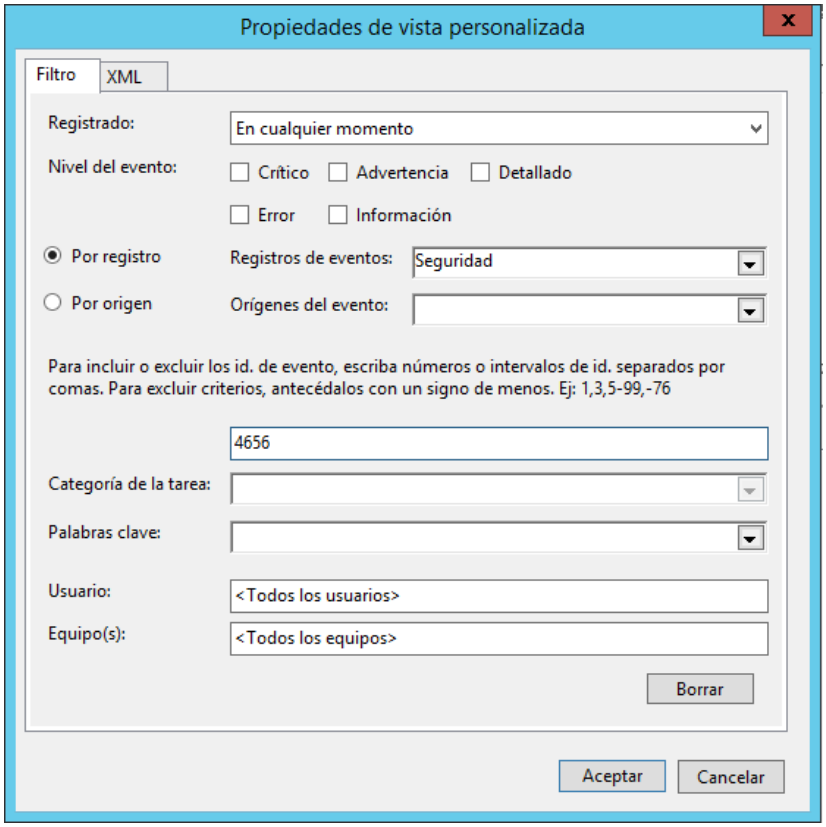
El "visor de eventos", és un compelment de Microsoft Management Console (MMC), que permet consultar i administrar, d'una forma potent i centralitzada, la informació continguda en els múltiples registres d'esdeveniments.

A la part esquerra de la finestra apareix organitzat a mode d'arbre, on s'organitzen diferents categories. En aquest cas, resulta més útil la categoria de "Registros de Windows", que conté una sèrie de subcategories:

- **"Aplicación"**: Ací apareixen els esdeveniments de les aplicacions i serveis que no formen part del sistema.
- **"Seguridad"**: Inclou la informació dels esdeveniments de seguretat del sistema.
- **"Instalación"**: Inclou els esdeveniments relacionats en la configuració de rols i característiques.
- **"Sistema"**: Conté informació relativa als esdeveniments del sistema i els seus components.
- **"Eventos reenviados"**: Conté informació reenviada per altres sistemes de la xarxa.

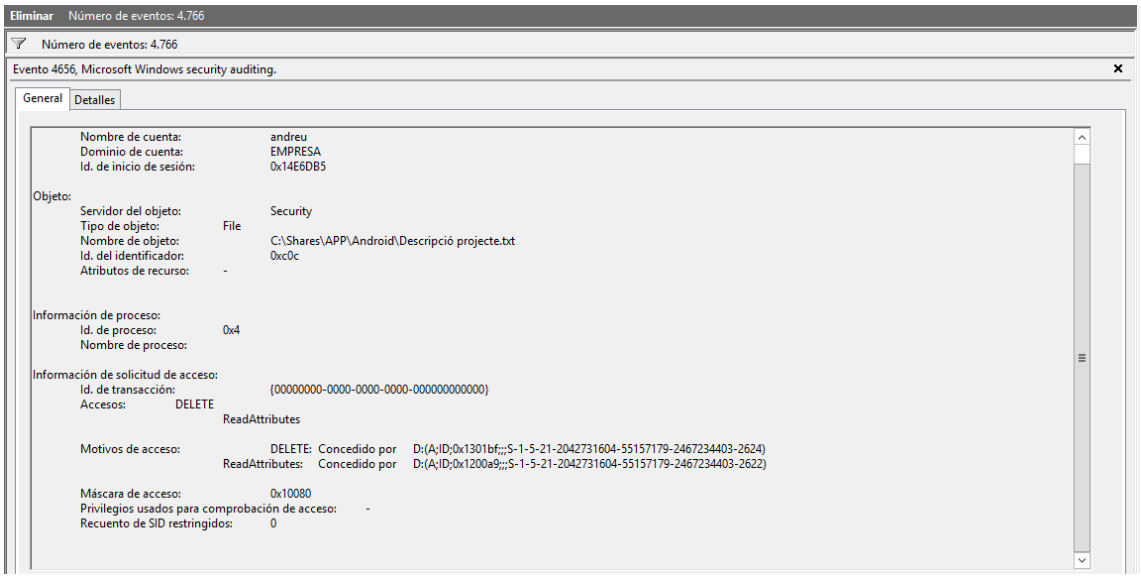
Com que el "visor de eventos" conté molta informació, es convenient crear una vista personalitzada per tal de filtrar els esdeveniments que s'estan buscant, en aquest cas els d'esborrar, al que se li assigna el identificador 4656 en el "ID de evento".

En aquest cas s'ha creat la vista personalitzada de la següent manera:



Captura 54 - Creació d'una vista personalitzada en el registre d'events

Aquesta vista facilita la cerca de l'esdeveniment desitjat. En aquest cas, s'ha pogut localitzar l'esdeveniment i comprovar que l'usuari Andreu ha sigut el que ha esborrat l'arxiu. A continuació es mostra la descripció de l'esdeveniment:



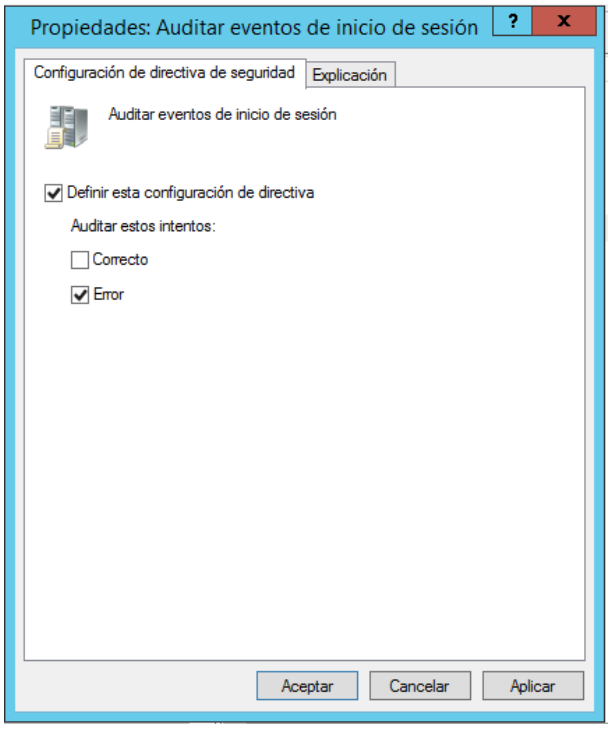
Captura 55 - Esdeveniment d'eliminació de l'arxiu de text

Auditar esdeveniments d'inici de sessió

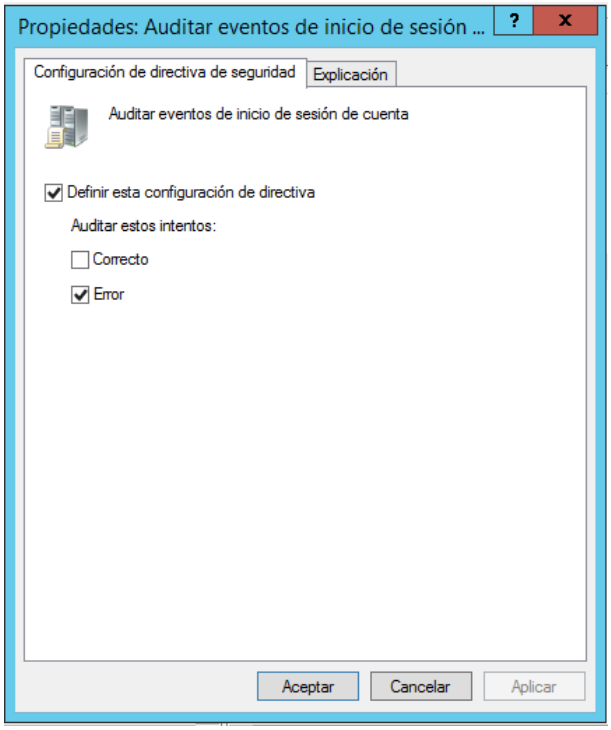
De la mateixa manera que en la directiva d'auditoria d'accés a objectes, aquesta vegada es va a configurar l'auditoria d'esdeveniments d'inici de sessió i d'inici de sessió de compte.

Aquestes directives permeten auditar els intents d'accés, per tenir constància de si algú esta intentant suplantar la identitat d'algun usuari, com per exemple, observant si l'hora de l'intent d'inici de sessió, no es correspon amb l'horari l'aboral de l'usuari.

Per tal de configurar els paràmetres de les directiva s'accedeix a aquestes i en quest cas es configura per a que solament audite el intents erronis.



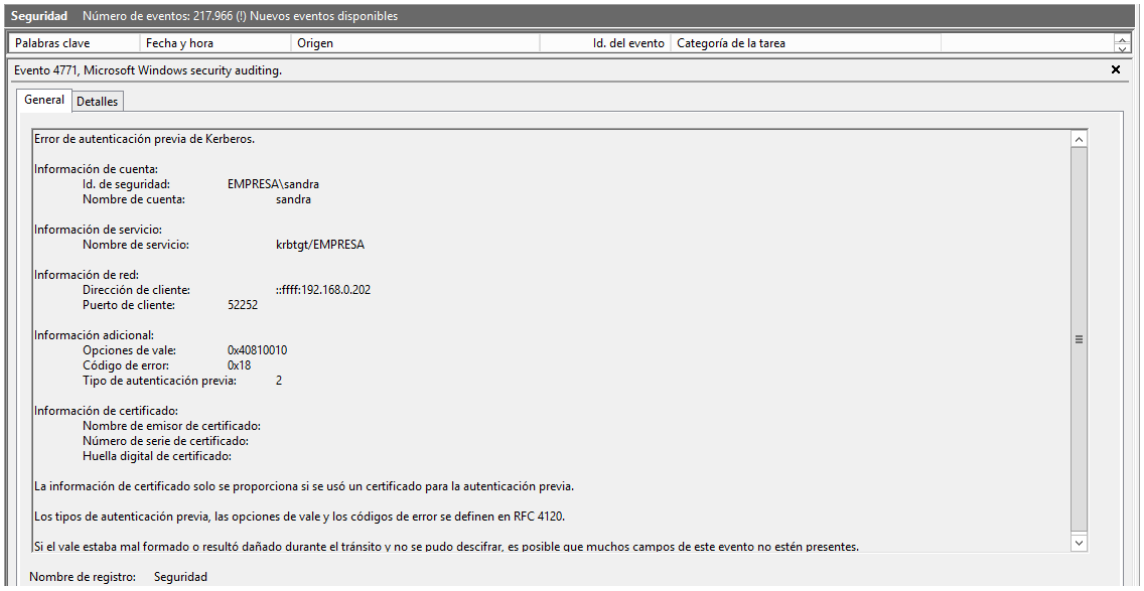
Captura 56 - Auditoria d'esdeveniments d'inici de sessió



Captura 57 - Auditoria d'esdeveniments d'inici de sessió de compte

Per tal de fer la prova del seu funcionament, es va a intentar accedir amb l'usuari Sandra a l'equip de treball, provocant un error d'inici de sessió introduint una contrasenya errònia.

Revisant el "visor de eventos" es pot comprovar que s'ha generat un esdeveniment d' **Error d'autenticació**. Per tant aquesta auditoria pot ser molt útil per comprovar si algun usuari malintencionat està intentant accedir al sistema a través d'un compte d'usuari del que no és propietari.



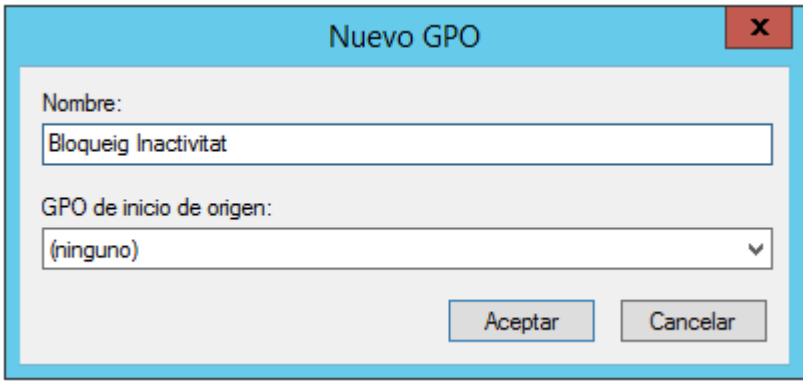
Captura 58 - Esdeveniment d'error d'autenticació

4.5.3 Bloqueig per inactivitat

Una bona pràctica de seguretat, és que els usuaris bloquegen el compte quan no estiguen davant de l'equip de treball, per evitar que cap altre usuari de l'empresa o alguna persona externa com per exemple personal de neteja, proveïdors,... puguen accedir a la xarxa, i a més, amb permisos d'un usuari de l'empresa.

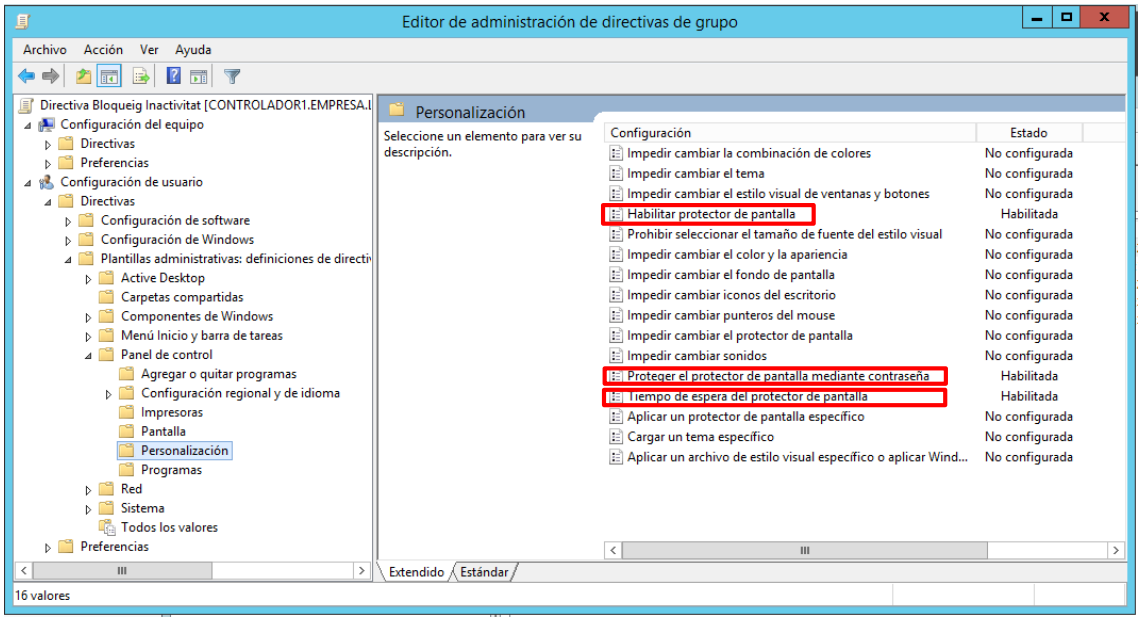
Es per això, que per tal d'evitar aquesta errada de seguretat, mitjançant una directiva de grup, es pot obligar a que l'equip es bloquege davant un temps determinat d'inactivitat. D'aquesta forma, si un usuari no bloqueja l'equip quan deixe el lloc de treball, es bloquejarà automàticament.

Per tal de crear aquesta directiva, s'ha creat un GPO, amb el nom Bloqueig Inactivitat.



Captura 59 - Crear GPO Bloqueig Inactivitat

Seguidament, s'han editat les propietats d'aquesta nova GPO. En **"Configuración de usuario"**, **"Directivas"**, **"Plantillas administrativas"**, **"Panel de Control"** i **"Personalización"**, s'han habilitat els paràmetres següents:

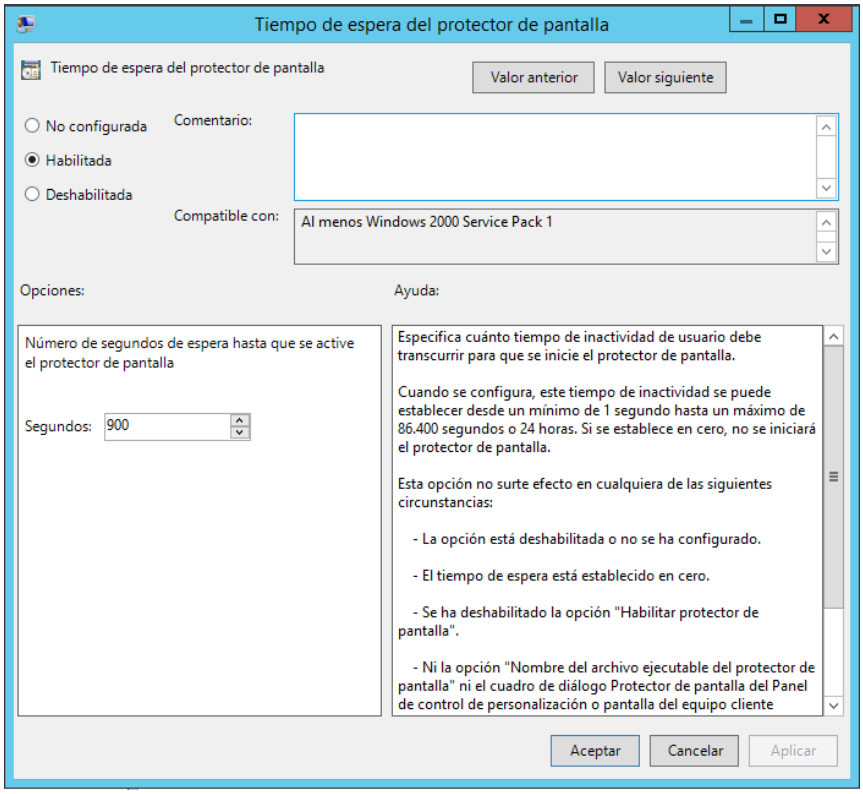


Captura 60 - Personalitar la GPO per bloquejar l'equip de treball per inactivitat

- **"Habilitar protector de pantalla"**: s'utilitza per activar el protector de pantalla.

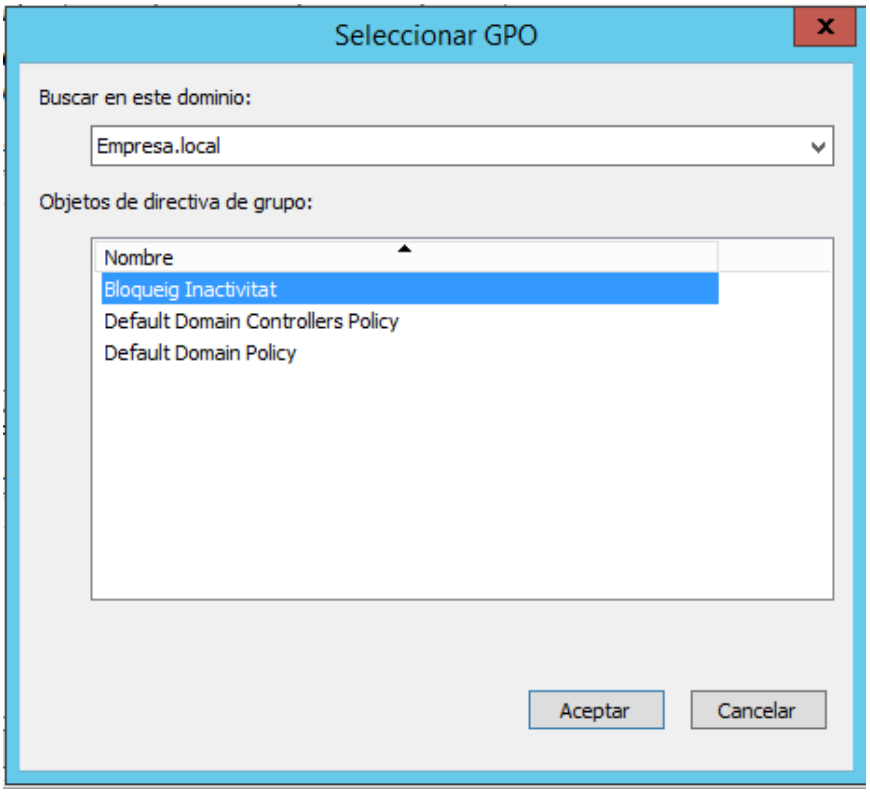
- **"Proteger el protector de pantalla mediante contraseña"**: si el protector de pantalla està activat, protegeix l'accés en la contrasenya de l'usuari.

- **"Tiempo de espera del protector de pantalla"**: s'utilitza per indicar el temps d'inactivitat que ha de transcórrer per a que s'active el protector de pantalla. En aquest cas s'ha configurat en 900 segons (15 min), però es pot establir un temps d'entre 1 segon i 24 hores.



Captura 61 - Temps d'espera per a bloqueig de l'equip de treball

Finalment, cal assignar aquesta nova GPO al domini Empresa.Local.



Captura 62 - Vinculació GPO a domini

5. Conclusions

En aquest apartat es descriuen les conclusions obtingudes després de la realització del treball.

Després de la finalització del treball, s'han pogut dur a terme tots els objectius plantejats. Per una banda, s'han configurat tots els paràmetres de seguretat que s'havien marcat en els objectius i per altra banda, s'ha realitzat aquesta memòria, que serveix com un manual per a la configuració dels paràmetres de seguretat descrits en un entorn basat en Windows Server 2012.

La primera part del treball, s'ha dut a terme sense massa complicació, ja que els coneixements adquirits en la titulació de grau, han permès portar aquesta part d'una manera còmoda i eficient. Per un altra banda, la part dels permisos sobre el recurs compartit i la configuració de les directives de grup, s'han desenvolupat amb un grau més de dificultat que la primera, ja que s'han hagut d'adquirir nous coneixements i les proves de la configuració d'aquest apartat no han sigut efectives en el primer intent, per el que s'ha hagut de trobar quina part de la configuració no estava ben configurada i corregir-la.

Per un altra banda, s'ha pogut comprovar que Windows Server 2012, és una ferramenta molt útil i potent per a les empreses, que permet moltes configuracions diferents que s'adapten a qualsevol tipus d'empresa. També s'ha pogut comprovar la importància de tenir un sistema segur, on tenir tots els recursos de l'empresa, i així, poder evitar l'accés de persones no desitjades als recursos d'aquesta i la possibilitat que ofereix Windows Server 2012 per poder auditar els intents d'accés no autoritzats i seguir millorant la seguretat de l'empresa.

A més del programari Windows Server 2012, cal remarcar la importància que ha tingut el programari VMware, que ha permès fer la simulació de l'empresa en un sol equip, evitant un alt cost econòmic per a la realització del treball i facilitant la tasca de configuració de tres equips en un mateix lloc de treball. A més, s'ha comprovat que es pot utilitzar aquest programari en una empresa real, ja que la potència d'aquest programari permet crear servidors virtuals i gestionar-los de manera eficient. L'únic inconvenient es que te una dependència directa en el maquinari de l'equip amfitrió, ja que aquest te uns recursos limitats i les màquines virtuals creades utilitzen aquest recursos.

6.Referències

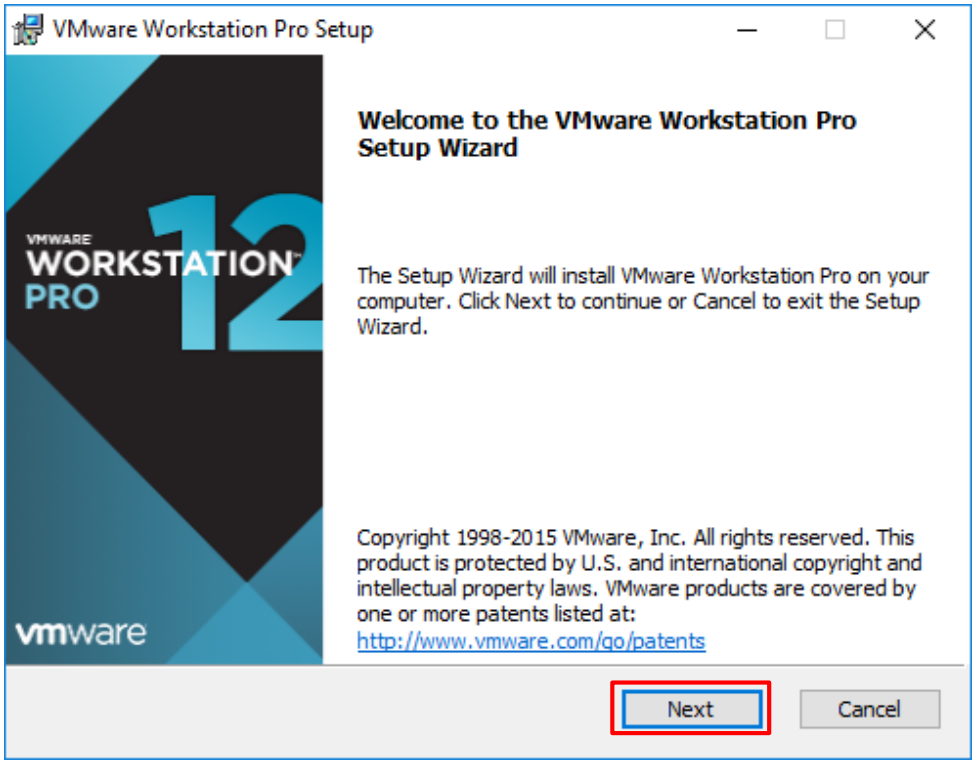
- Francisco Charte (2012), «Manual Avanzado de Windows Server 2012». Editorial Anaya Multimedia.
- Stanek, William R. (2013), « Windows Server 2012: guía del administrador». Editorial Anaya Multimedia.
- VMware, «VMware Community,» VMware, [En línea]. Available: https://communities.vmware.com/
- W. Foundation, «Viquipèdia - L'enciclopèdia lliure,» [En línea]. Available: https://www.wikipedia.org/
- Microsoft, «TechNet - Microsoft,» Microsoft, [En línea]. Available: https://technet.microsoft.com/
- Microsoft, «Microsoft - Developer Network,» Microsoft, [En línea]. Available: https://msdn.microsoft.com/es-es
- Microsoft, «Microsoft - Technical Support,» [En línea]. Available: https://support.microsoft.com/es-es
- Juan Carlos Cano Escribá, Juan Luis Posadas Yagüe (2016). “Curso de Administración y Seguridad de Sistemas Informáticos en Windows Server 2012”. DISCA (Universitat Politècnica de València).

7. Annex

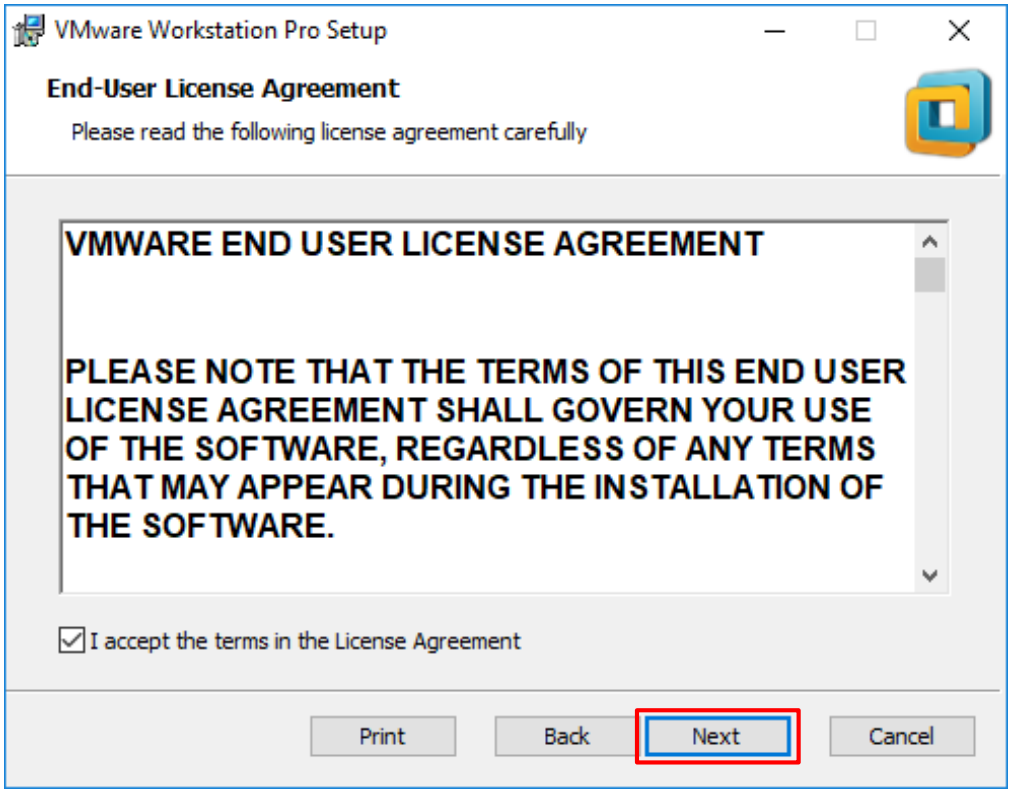
En aquesta apartat es descriuen els procediments per a la preparació de l'entorn de treball per a realitzar aquest treball.

7.1 Instal·lació VMware Workstation

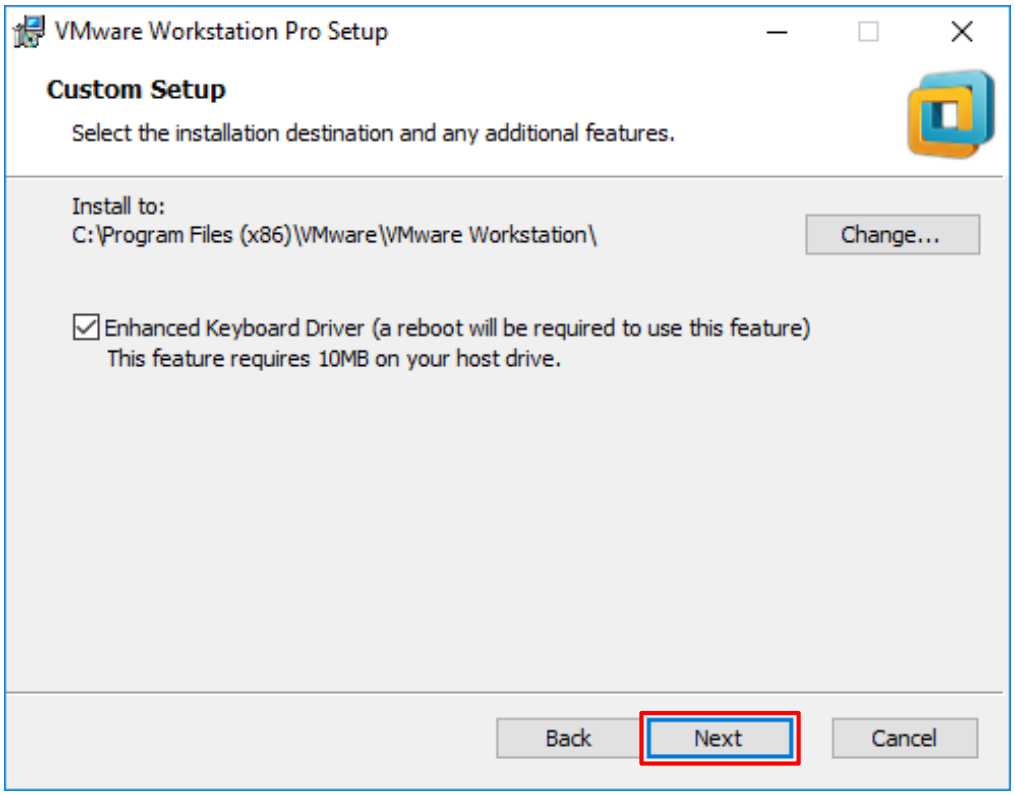
Per a la instal·lació només cal executar el fitxer d'instal·lació i seguir les passes marcades per l'assistent. També cal introduir el numero de llicencia quan aquest el sol·licite.



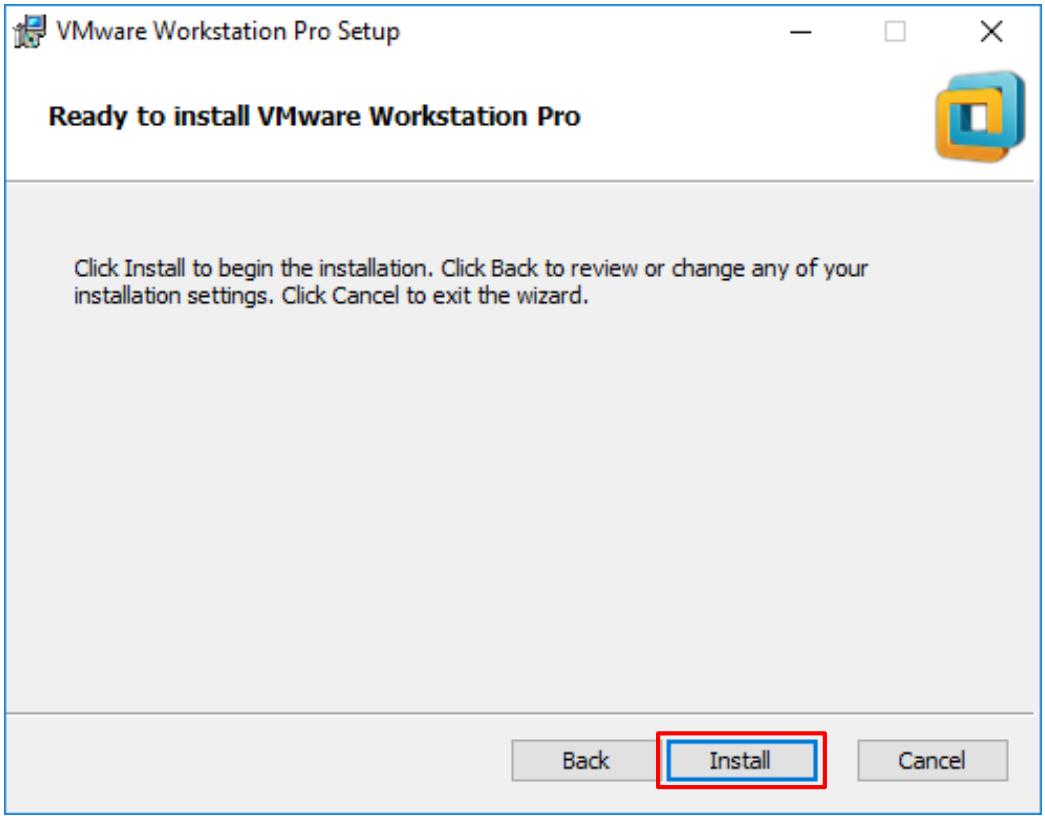
Captura 63 - Instal·lació VMware Workstation 1



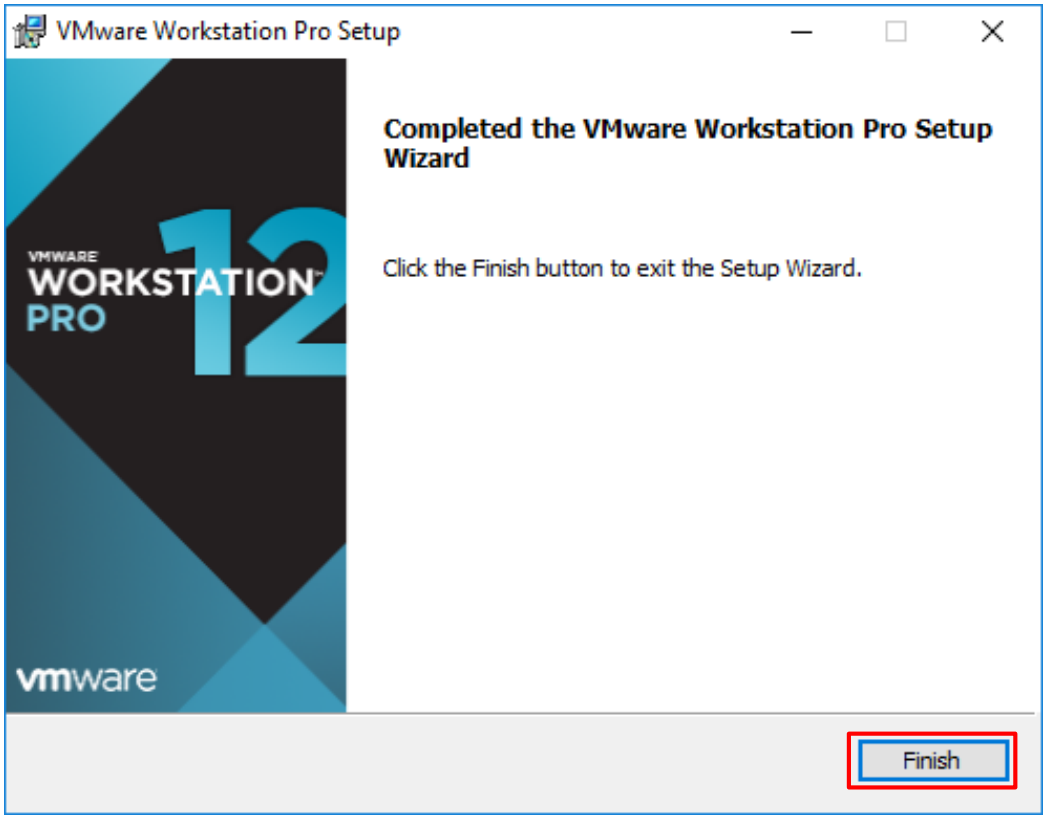
Captura 64 - Instal·lació VMware Workstation 2



Captura 65 - Instal·lació VMware Workstation 3



Captura 66 - Instal·lació VMware Workstation 4

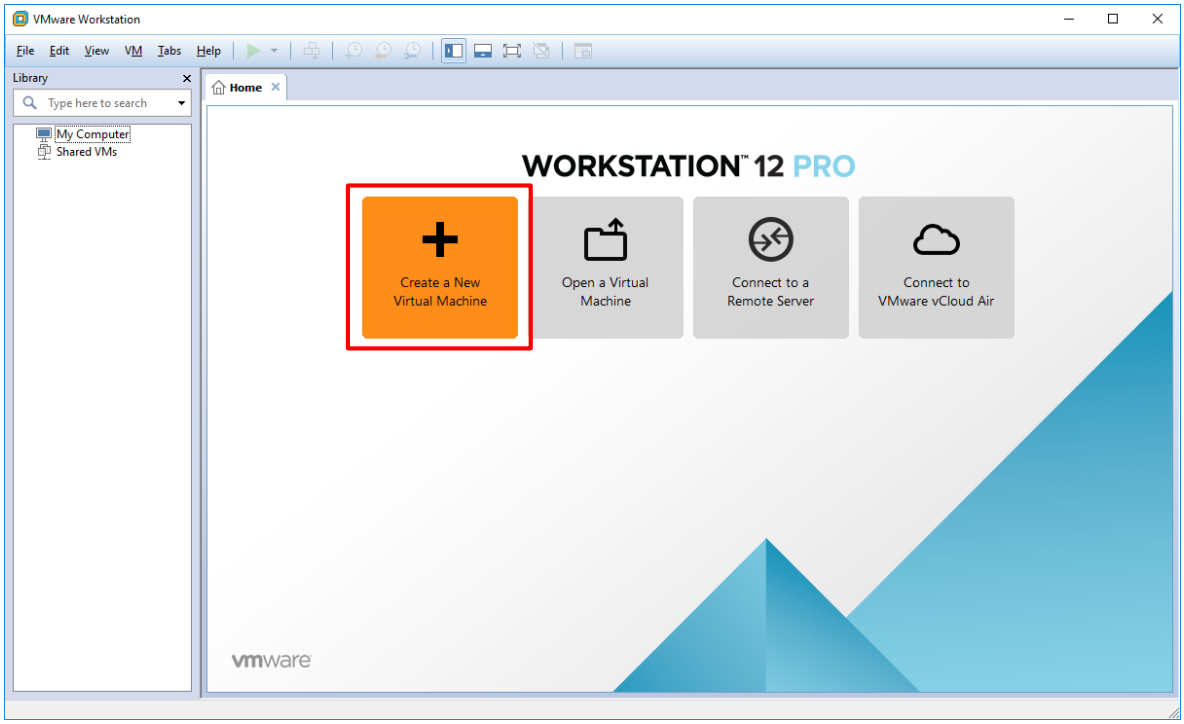


Captura 67 - Instal·lació VMware Workstation 5

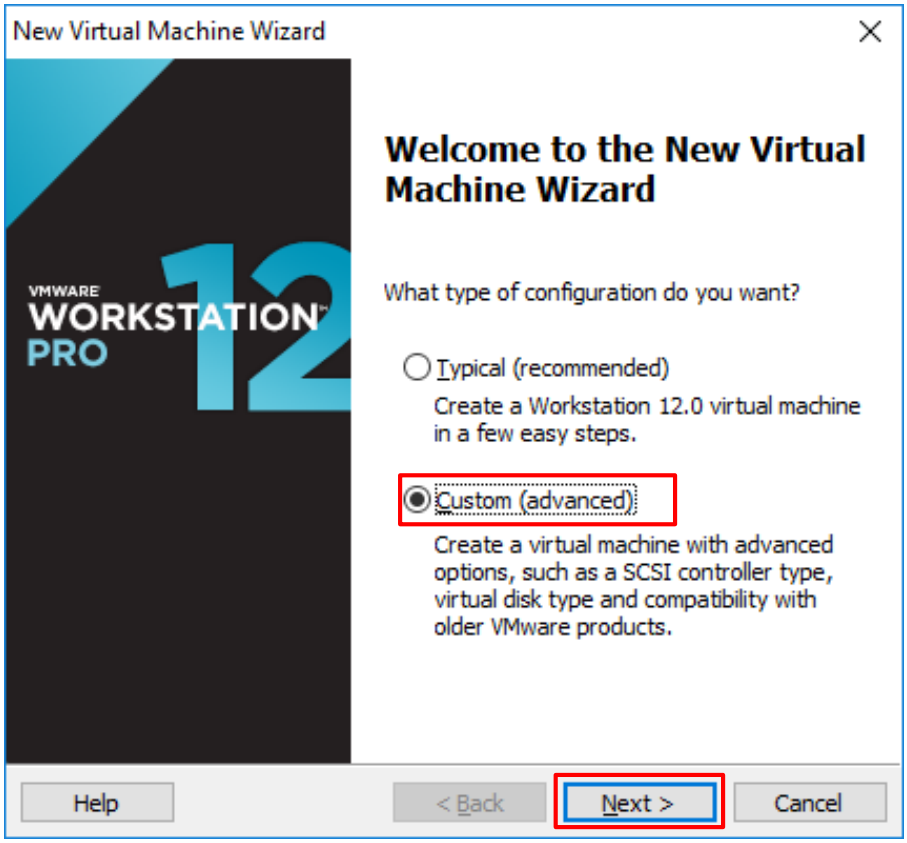
7.2 Crear màquines virtuals

Després d'instal·lar VMware, es creen els tres equips necessaris per a la realització del treball, amb les característiques requerides per a la instal·lació dels sistemes operatius corresponents: Windows Server 2012 per als servidors i Windows 10 per a l'equip de treball.

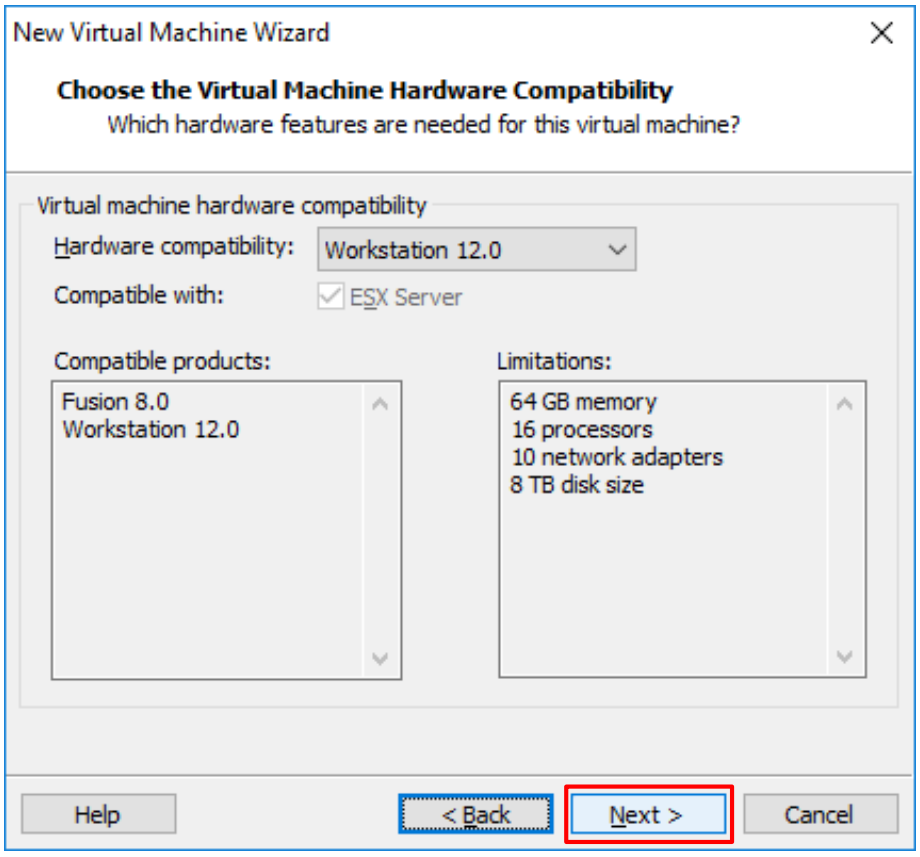
Les passes per a crear les màquines virtual des de VMware són les següents:



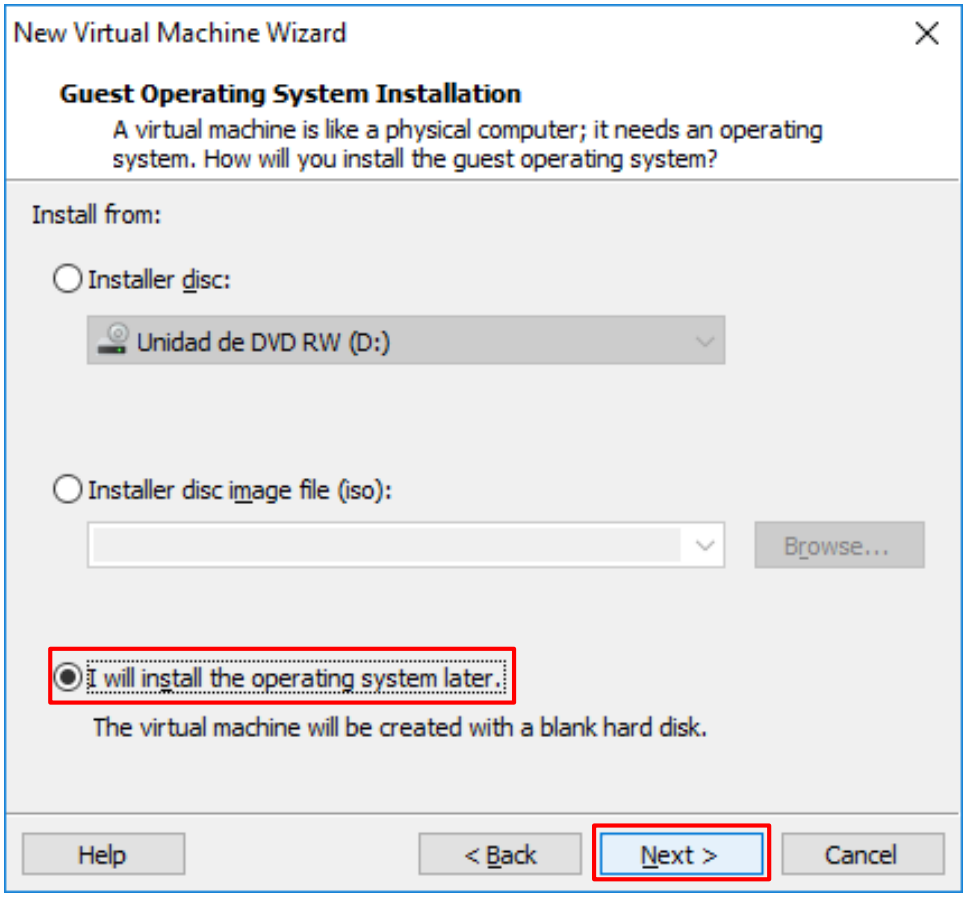
Captura 68 - Creació Màquina Virtual 1



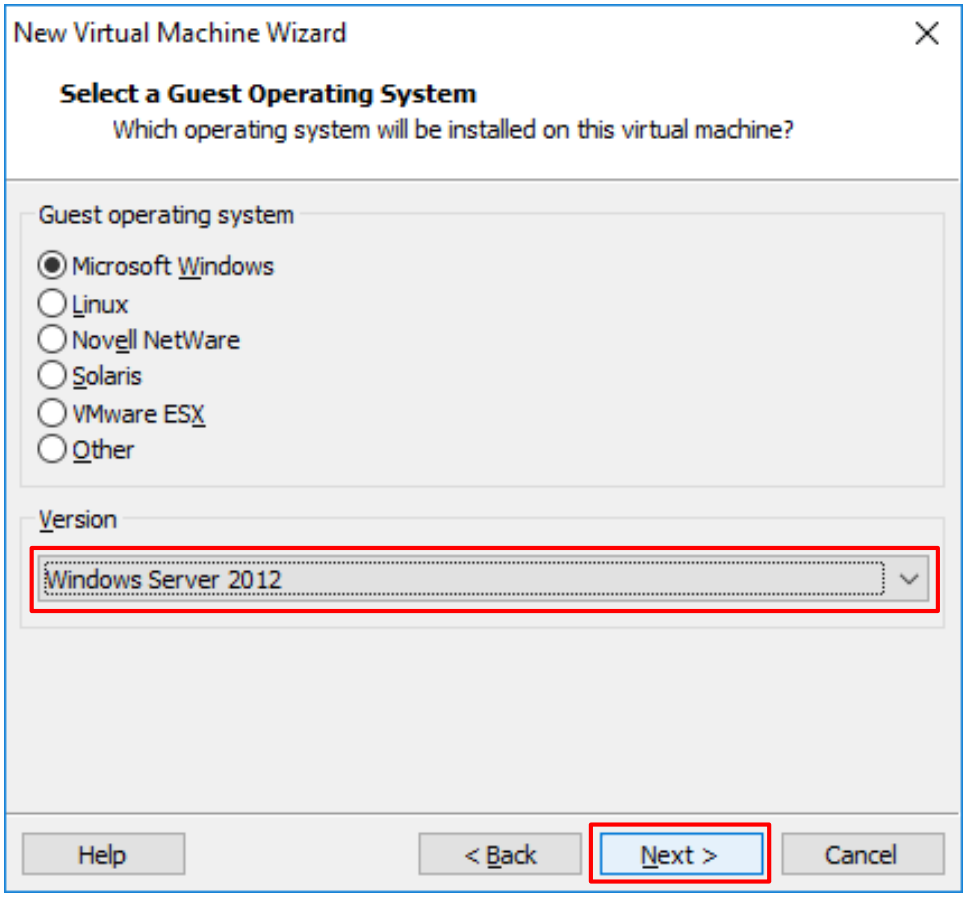
Captura 69 - Creació Màquina Virtual 2



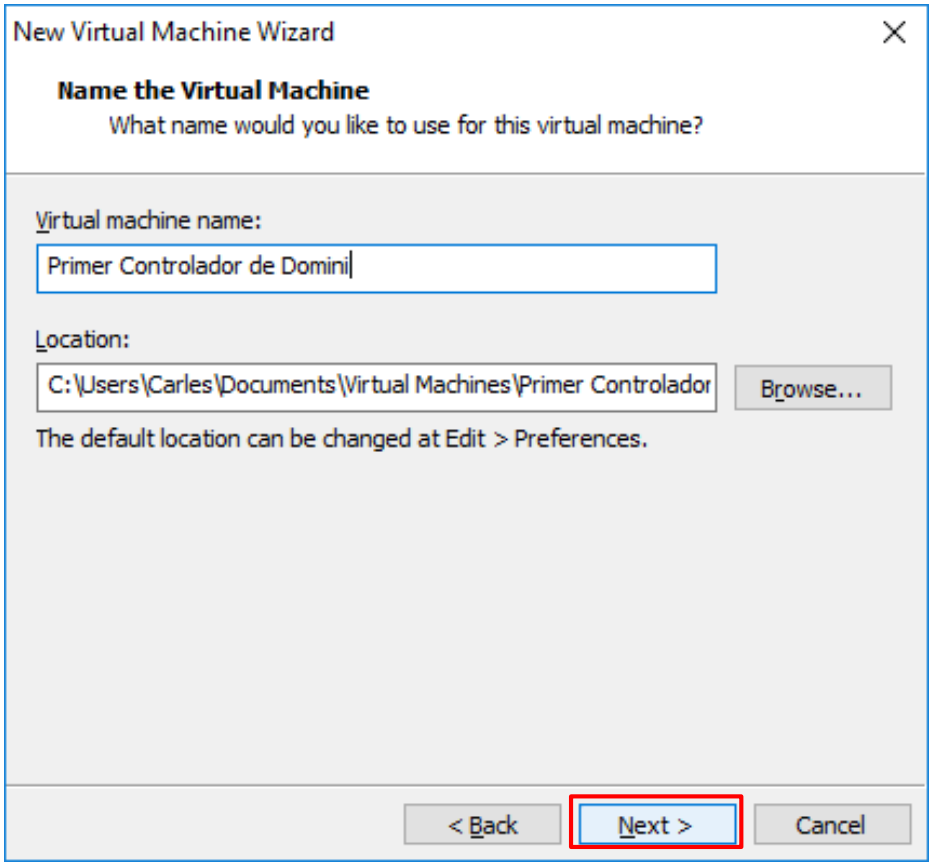
Captura 70 - Creació Màquina Virtual 3



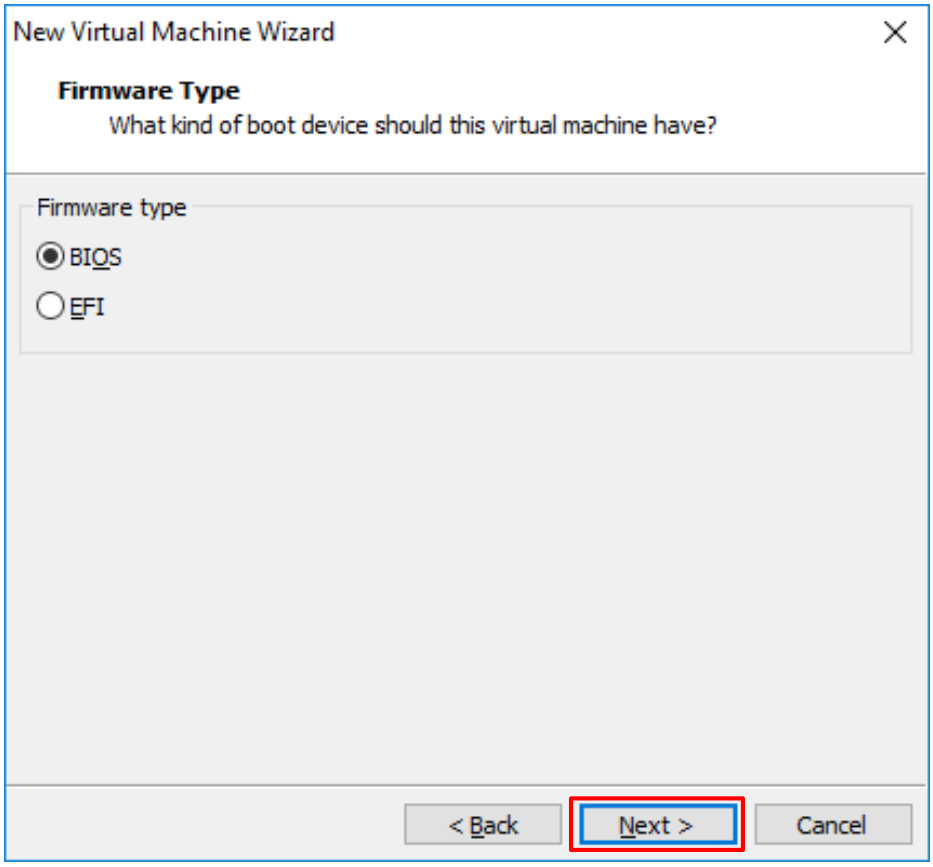
Captura 71 - Creació Màquina Virtual 4



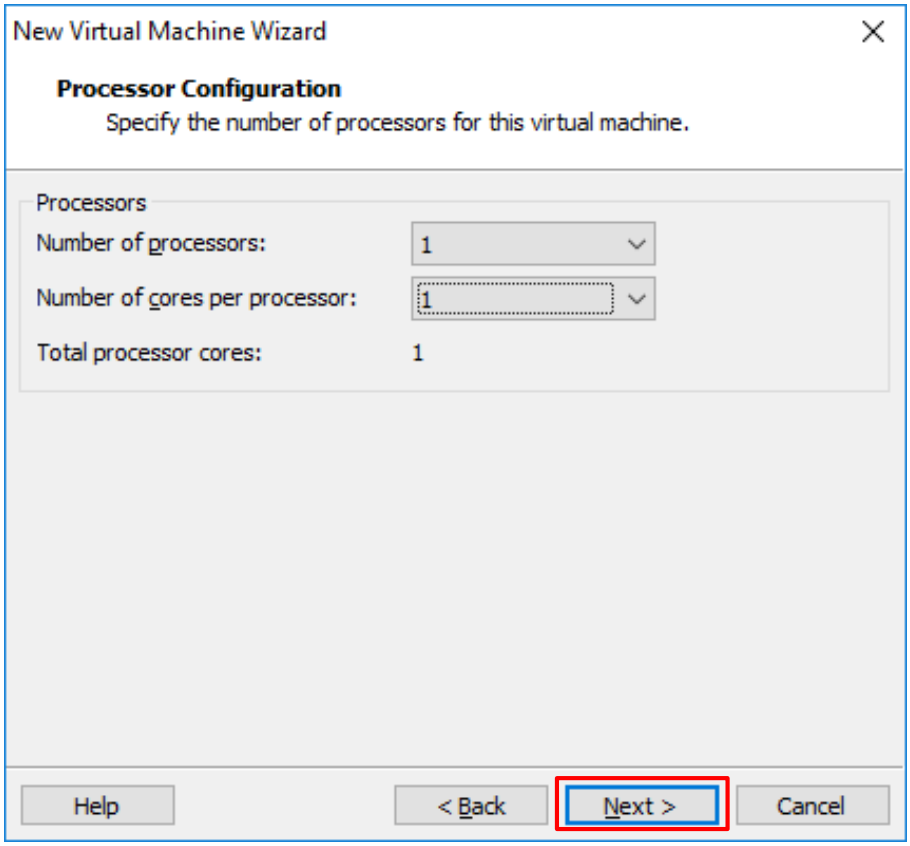
Captura 72 - Creació Màquina Virtual 5



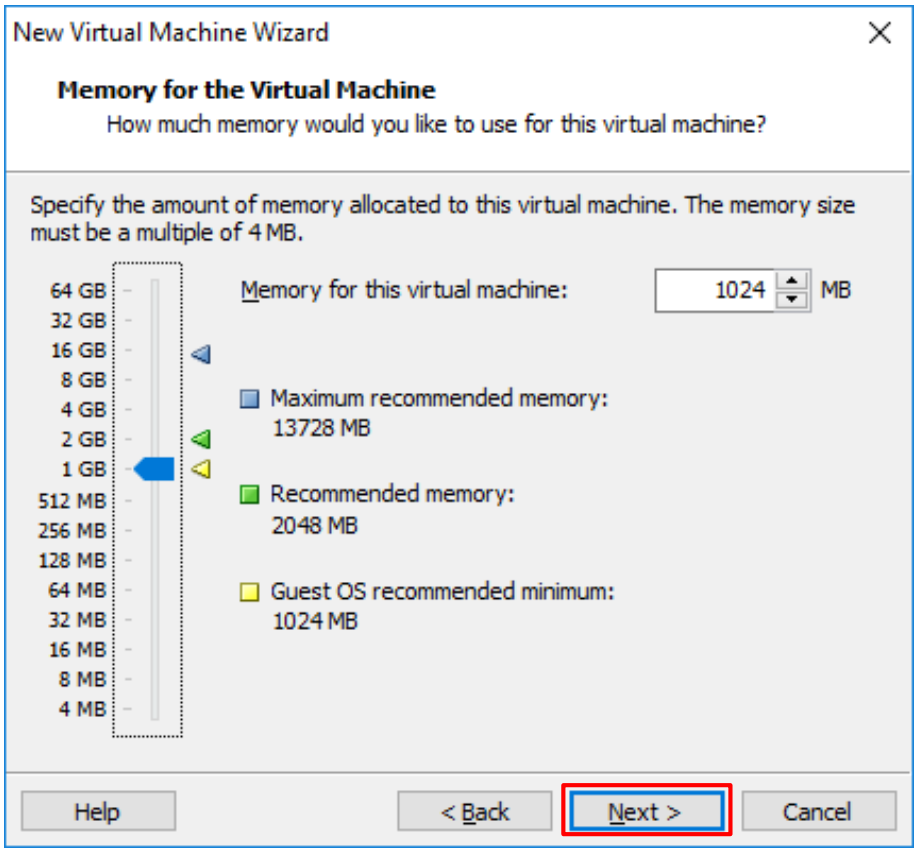
Captura 73 - Creació Màquina Virtual 6



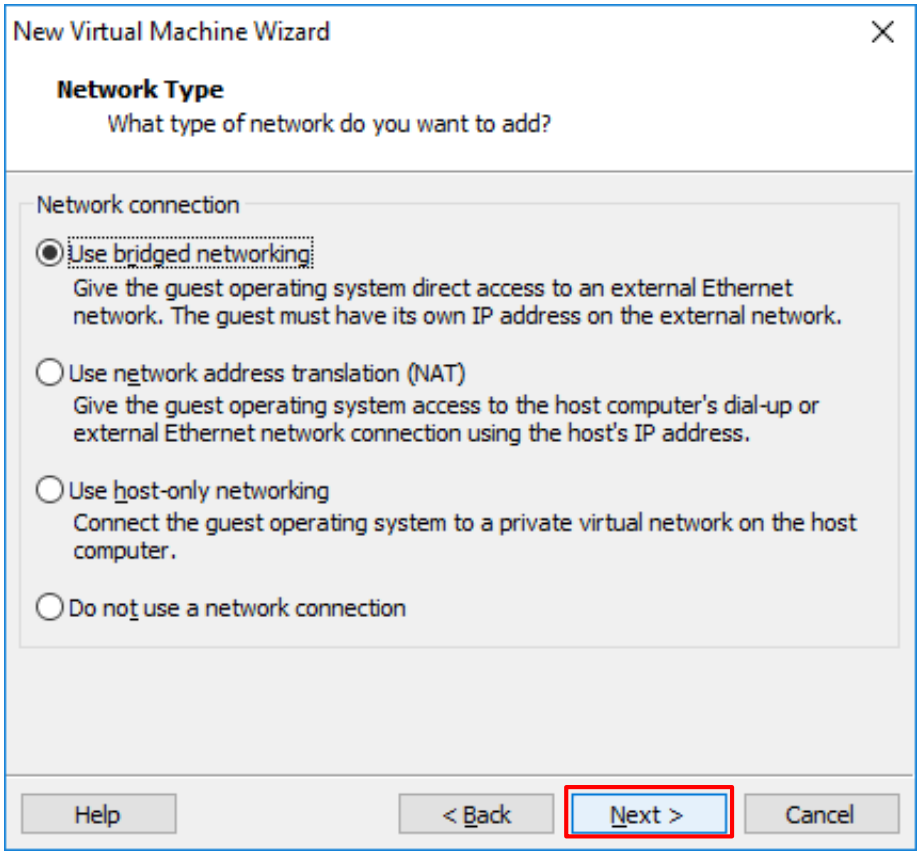
Captura 74 - Creació Màquina Virtual 7



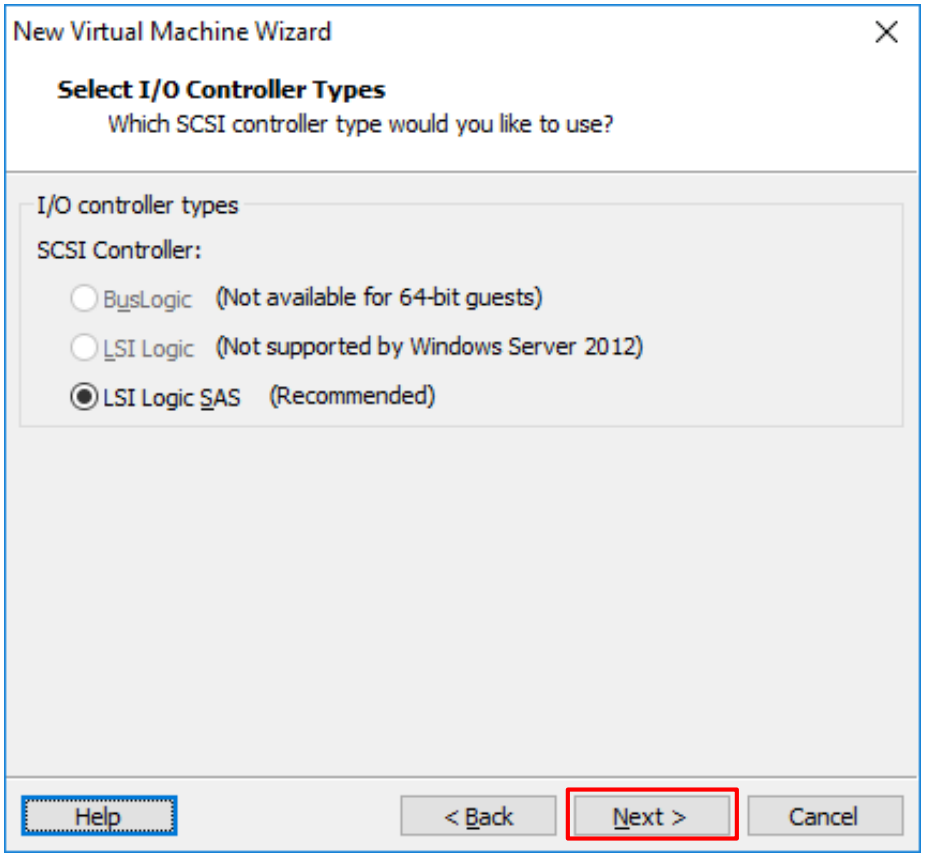
Captura 75 - Creació Màquina Virtual 8



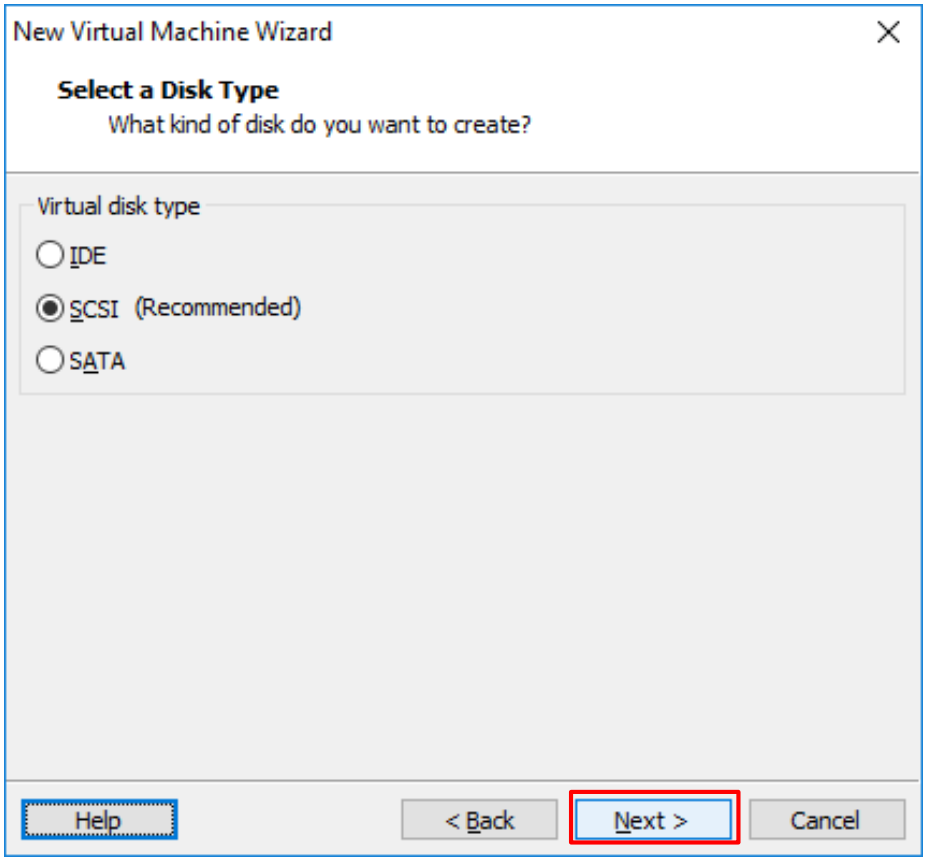
Captura 76 - Creació Màquina Virtual 9



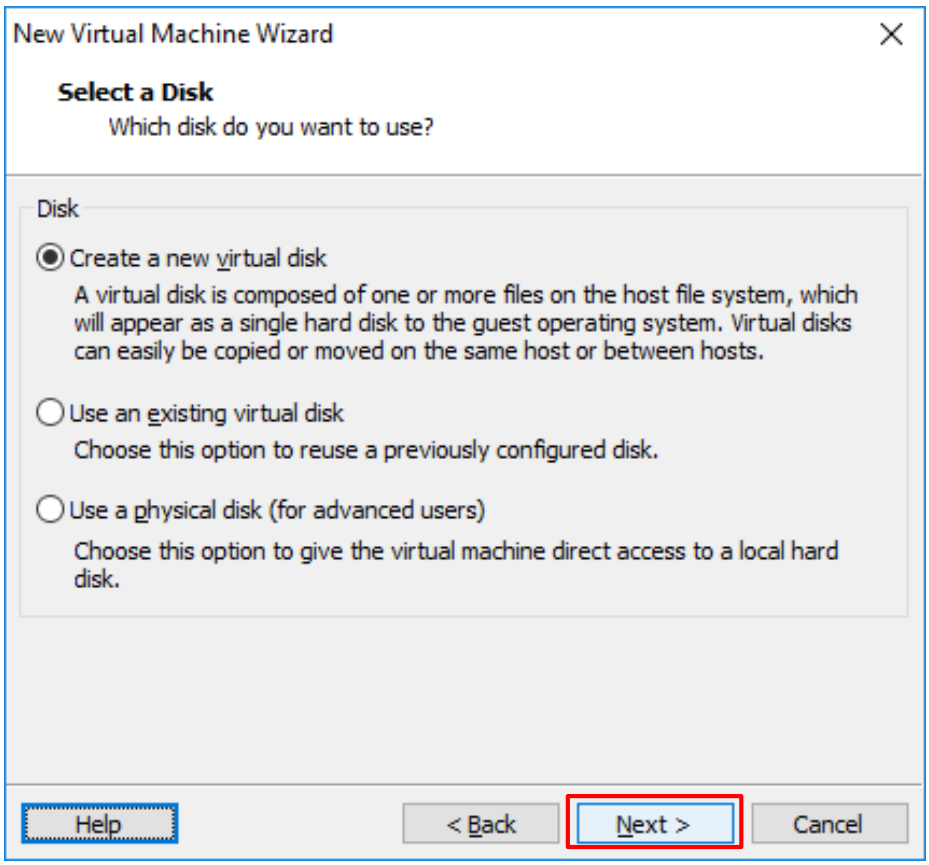
Captura 77 - Creació Màquina Virtual 10



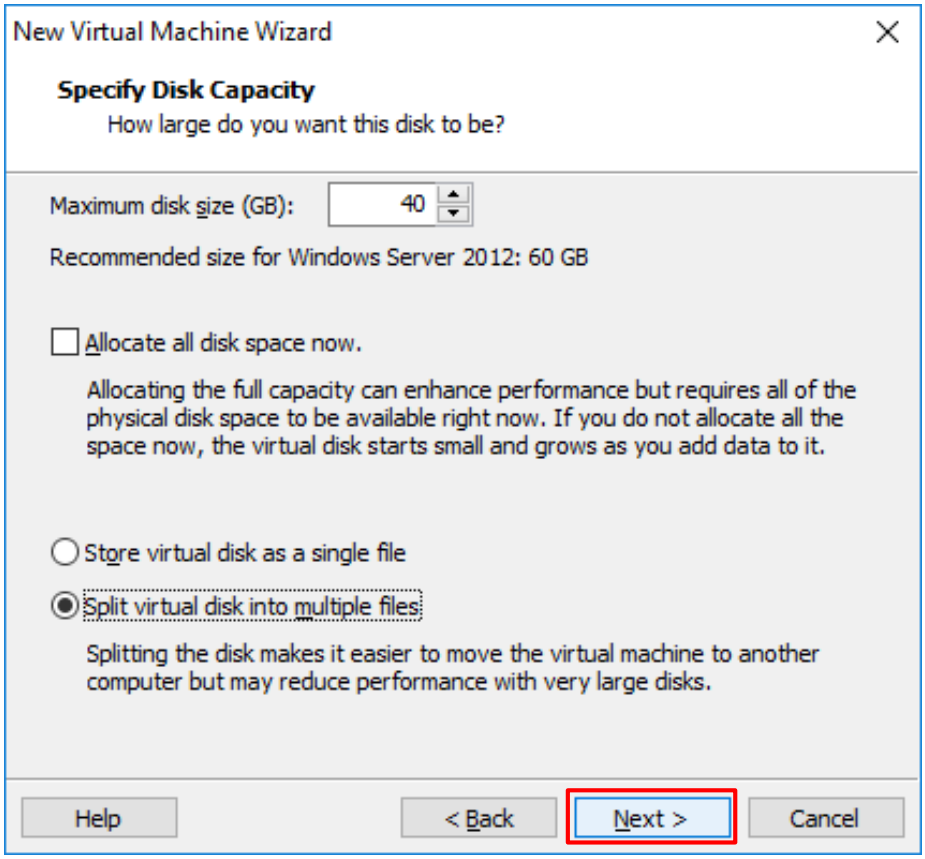
Captura 78 - Creació Màquina Virtual 11



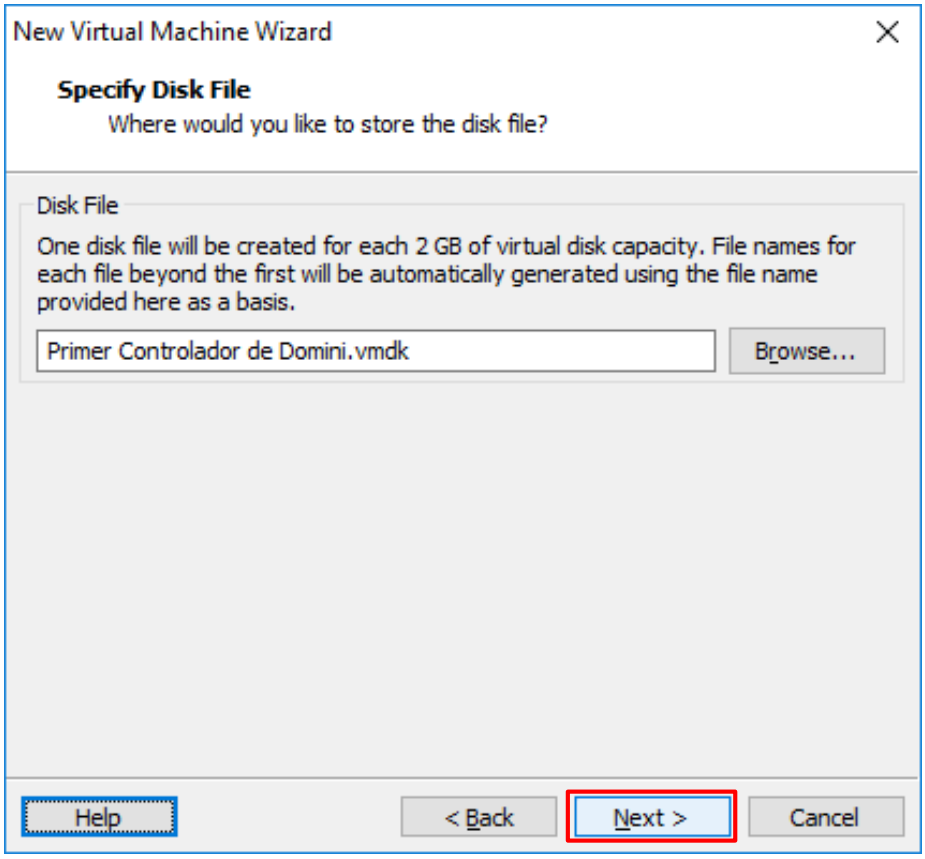
Captura 79 - Creació Màquina Virtual 12



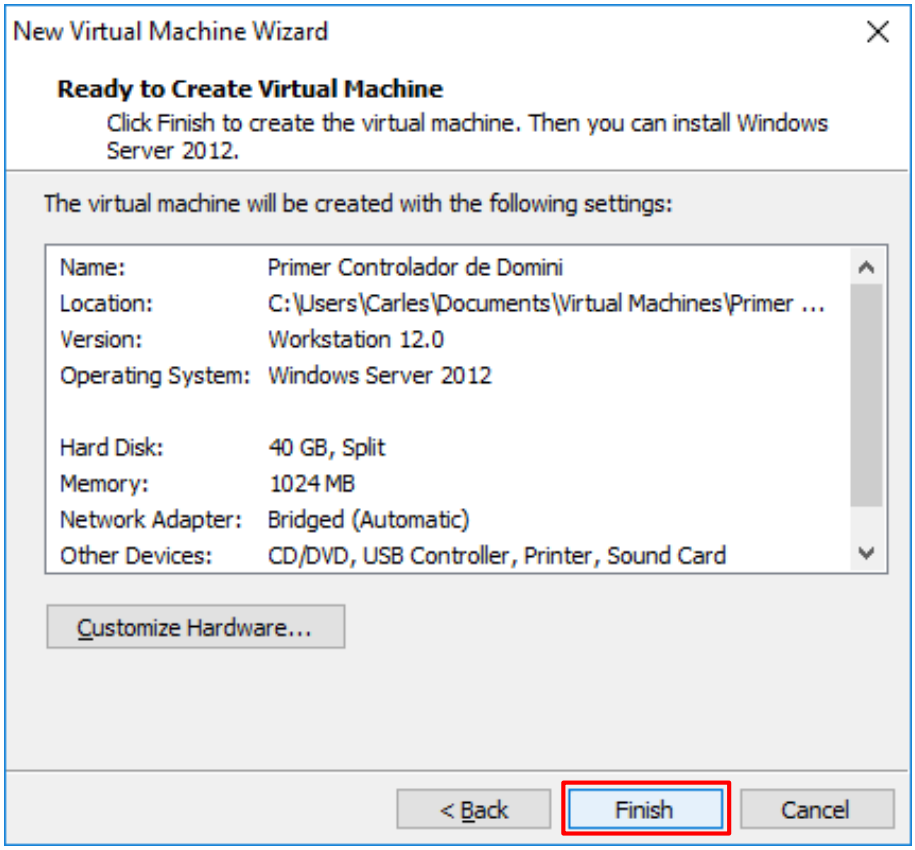
Captura 80 - Creació Màquina Virtual 13



Captura 81 - Creació Màquina Virtual 14



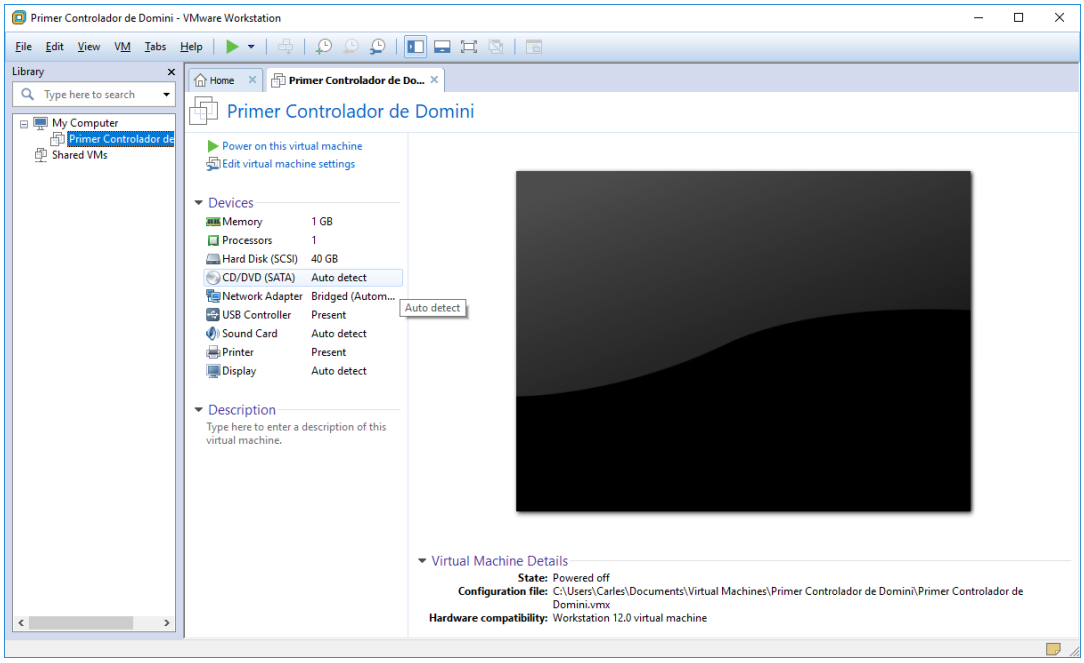
Captura 82 - Creació Màquina Virtual 15



Captura 83 - Creació Màquina Virtual 16

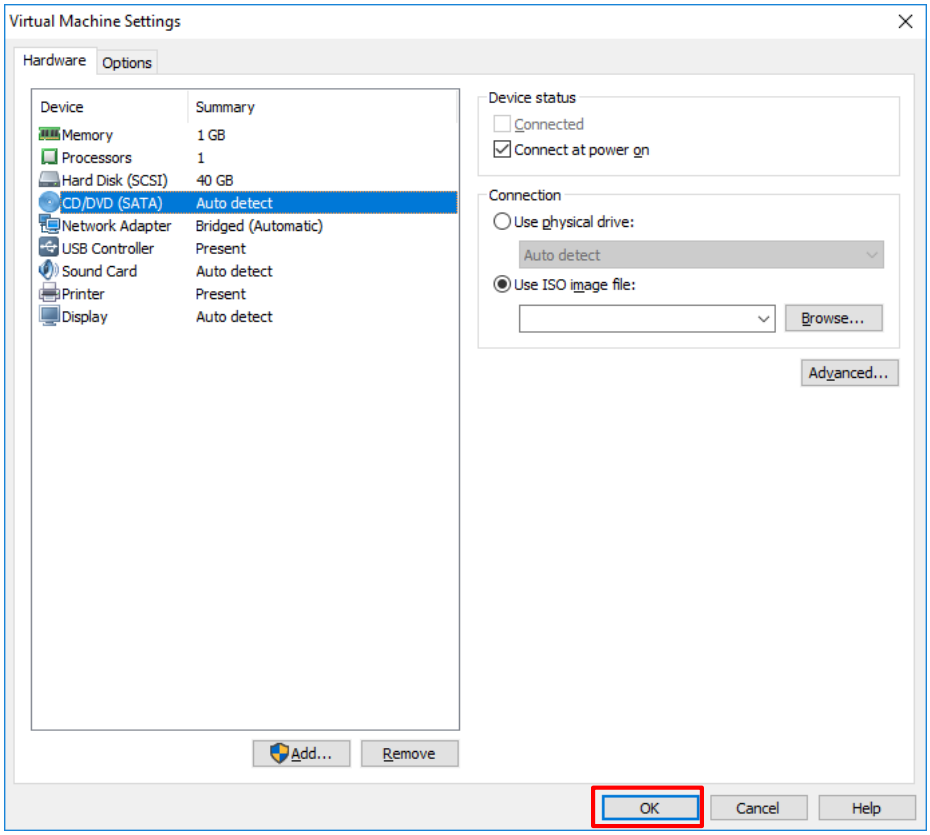
7.3 Instal·lar Windows Server 2012

Després de crear les màquines virtuals s'ha d'instal·lar el sistema operatiu. En aquest apartat s'indiquen les passes que s'han seguit per instal·lar Windows Server 2012 en la màquina virtual del primer controlador de domini.



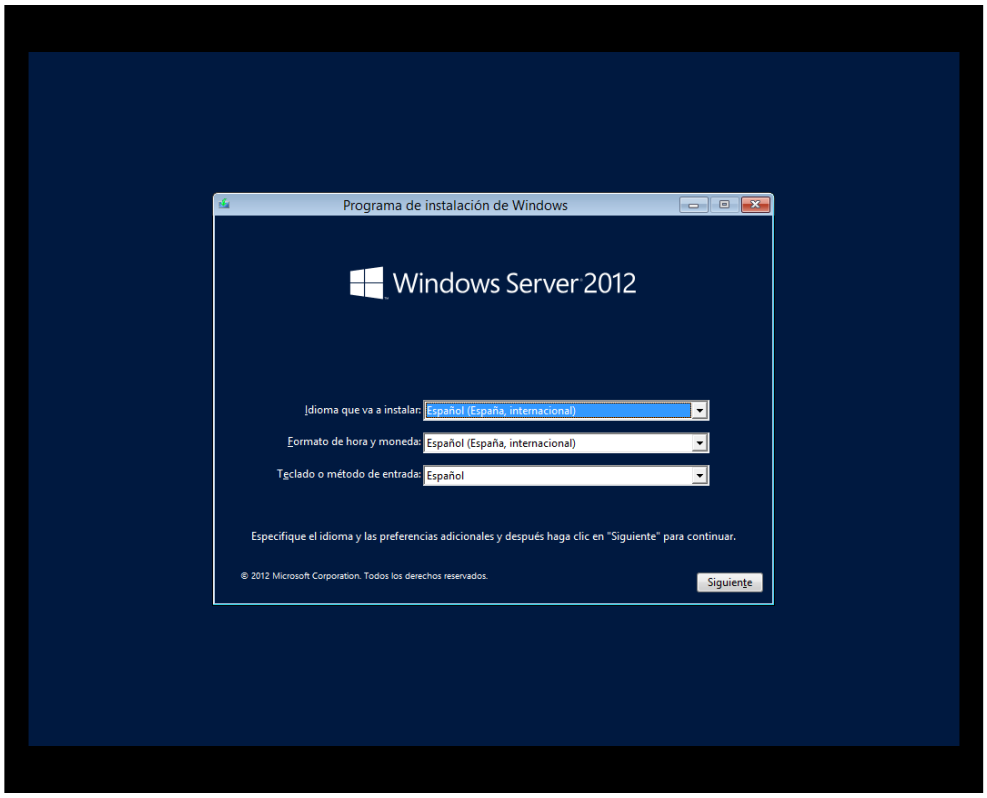
Captura 84 -Instalació Windows Server 2012 1

Cal seleccionar el fitxer de la imatge del sistema operatiu que volem instal·lar en la màquina virtual, en aquest cas Windows Server 2012.

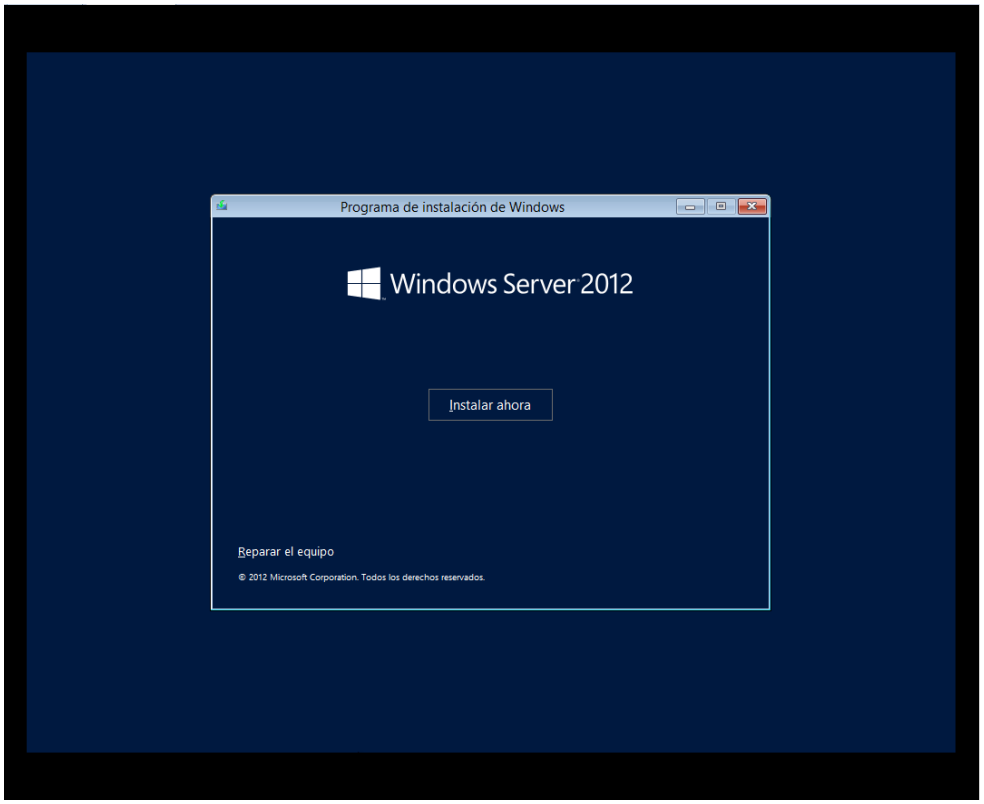


Captura 85 -Instalació Windows Server 2012 2

Seleccionar idioma, format de l'hora i mètode d'entrada de teclat.

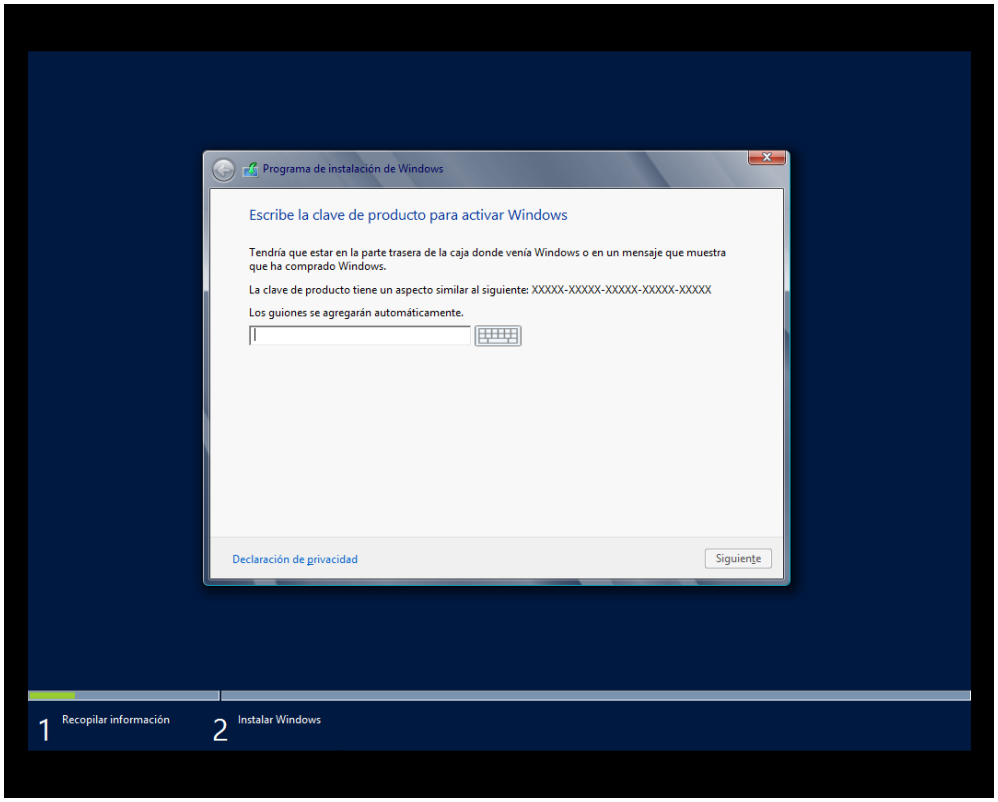


Captura 86 -Instalació Windows Server 2012 3



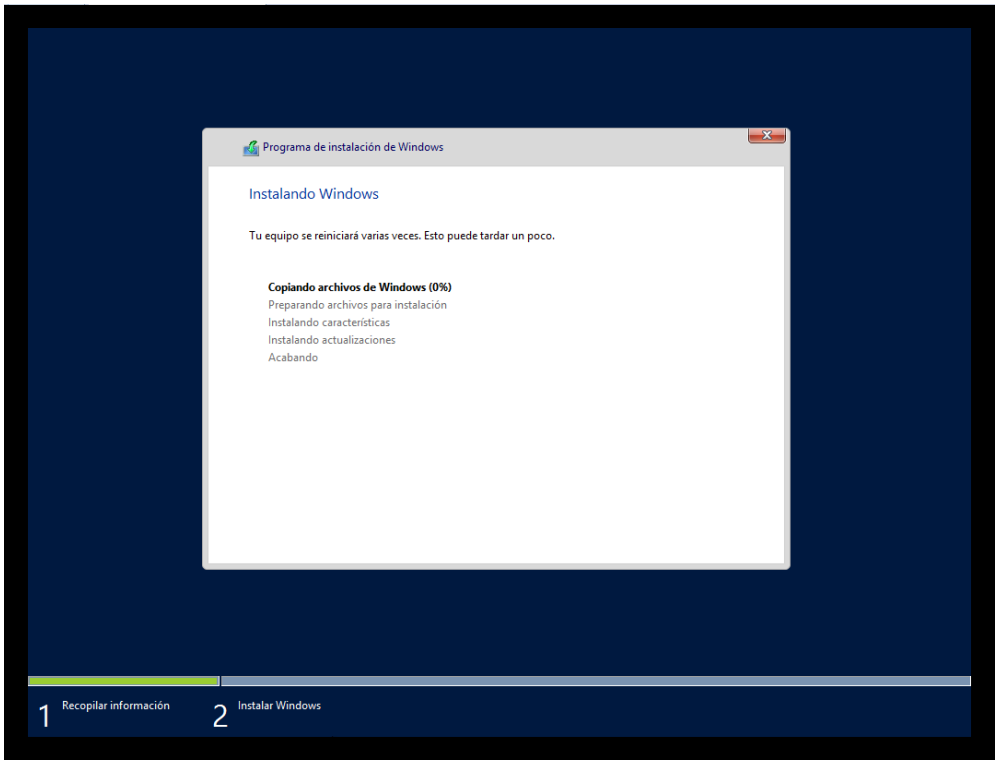
Captura 87 -Instalació Windows Server 2012 4

Cal introduir la clau d'activació del producte.

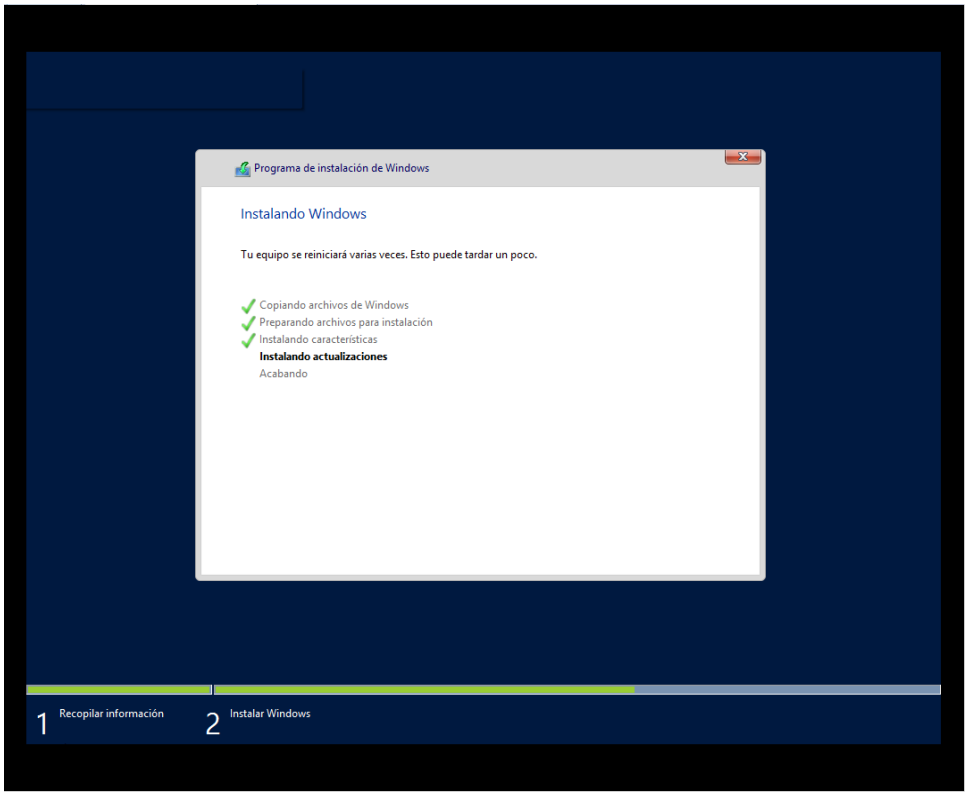


Captura 88 -Instalació Windows Server 2012 5

Comença la instal·lació en la màquina virtual.



Captura 89 -Instalació Windows Server 2012 6

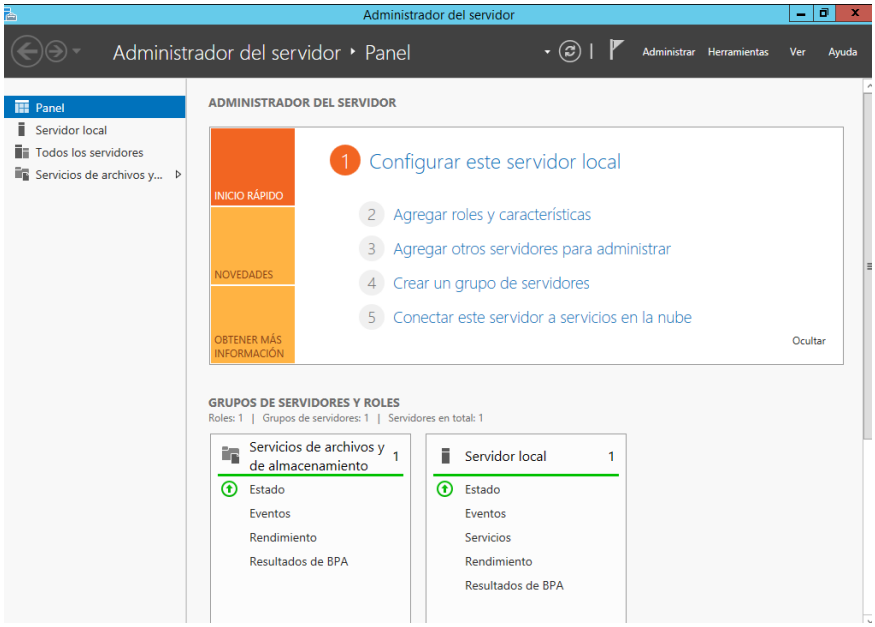


Captura 90 -Instalació Windows Server 2012 7

Una vegada ha finalitzat el procés d'instal·lació ja es pot accedir a la màquina i començar les configuracions del controlador de domini amb Windows Server 2012.

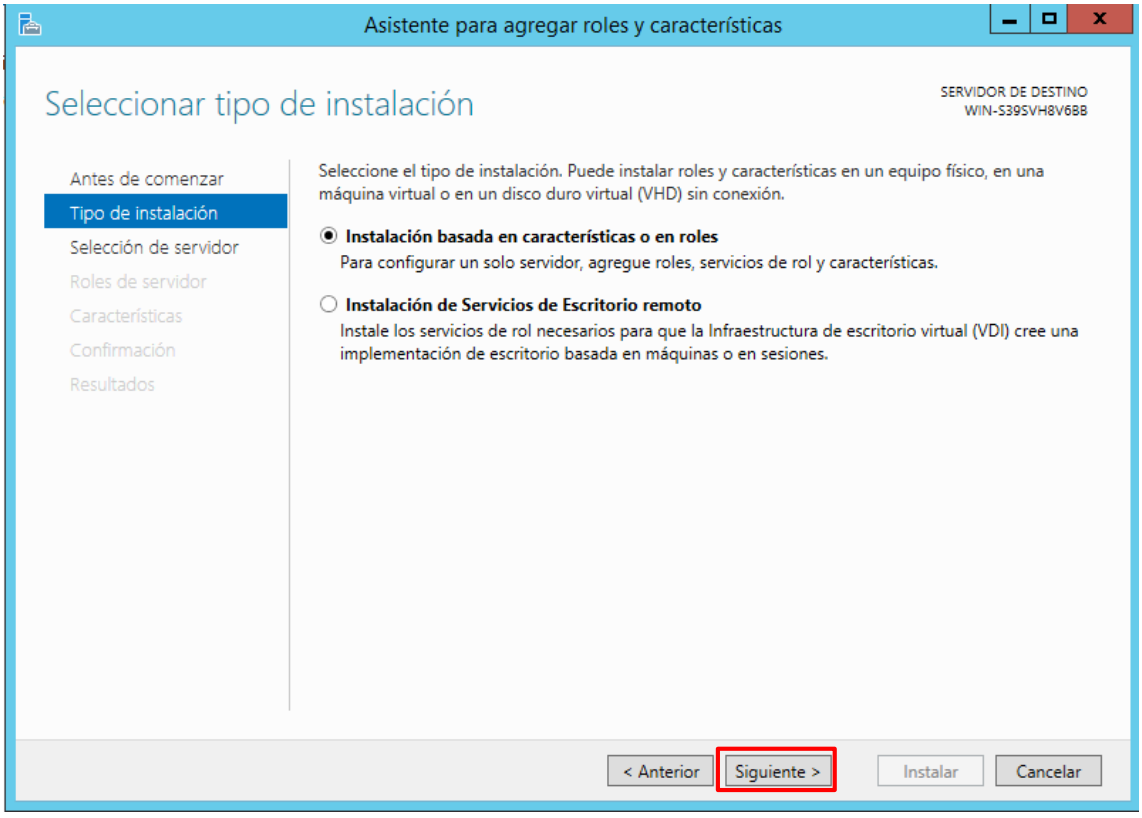
7.4 Instal·lació Servei de Domini Active Directory

Per a instal·lar el Servei de Domin Active Directory, cal obrir l'Administrador del servidor. Clicar en **"Agregar roles y características"** i seguir la configuració tal i com s'indica en les imatges següents:



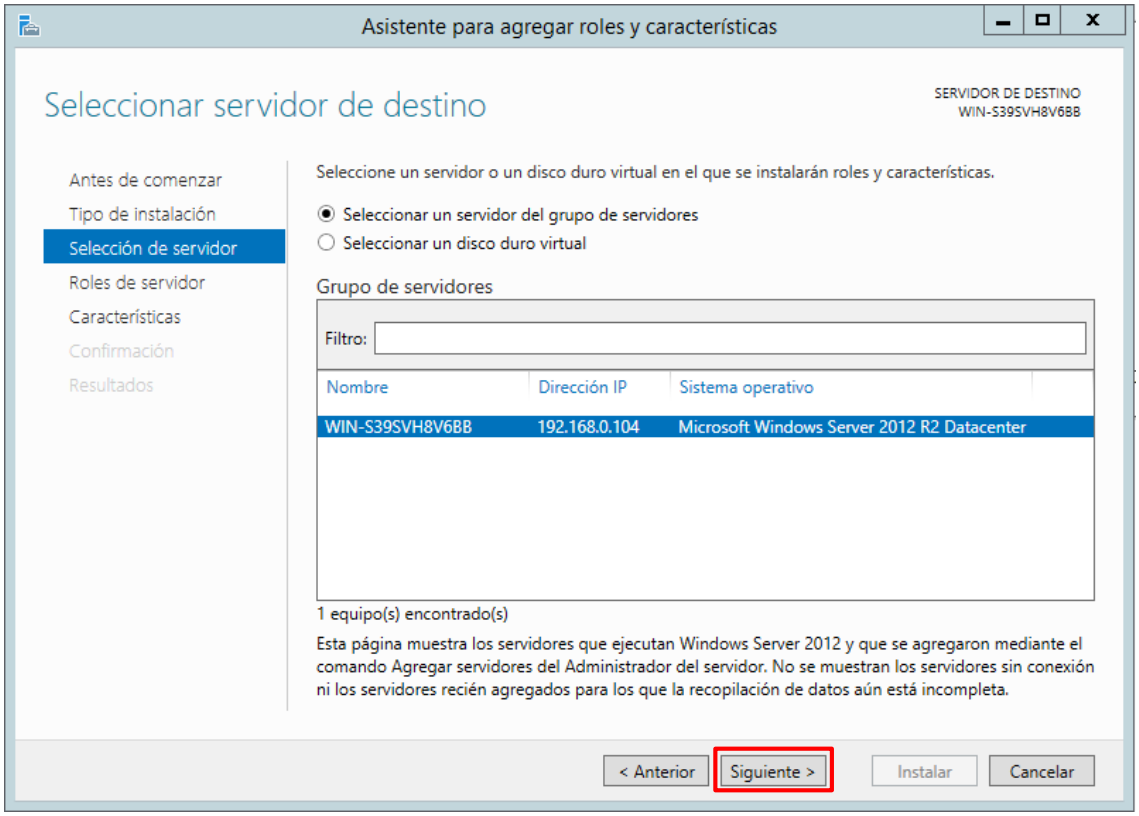
Captura 91 - Instal·lació Servei de Domini Active Directory 1

Seleccionar **"Instalación basada en características o en roles"** i clicar **"Siguiente"**



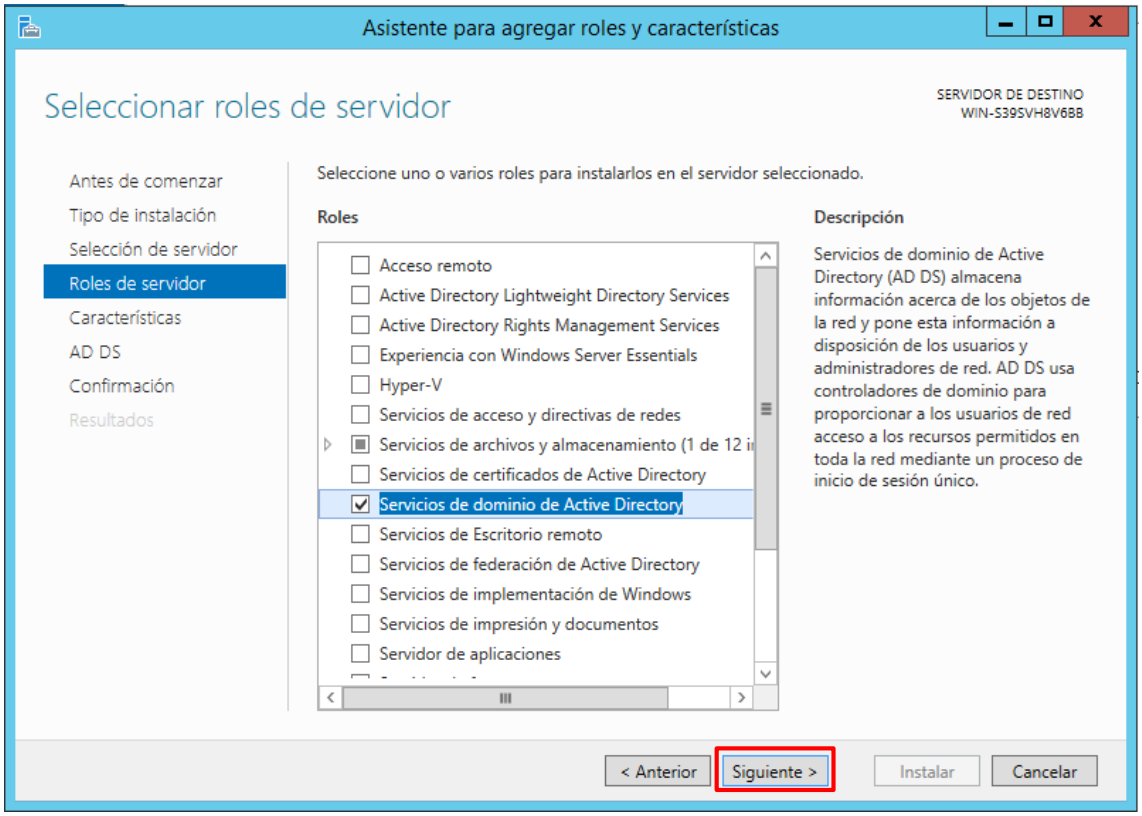
Captura 92 - Instal•lació Servei de Domini Active Directory 2

Ara cal seleccionar el servidor on s'instal·larà el servei.



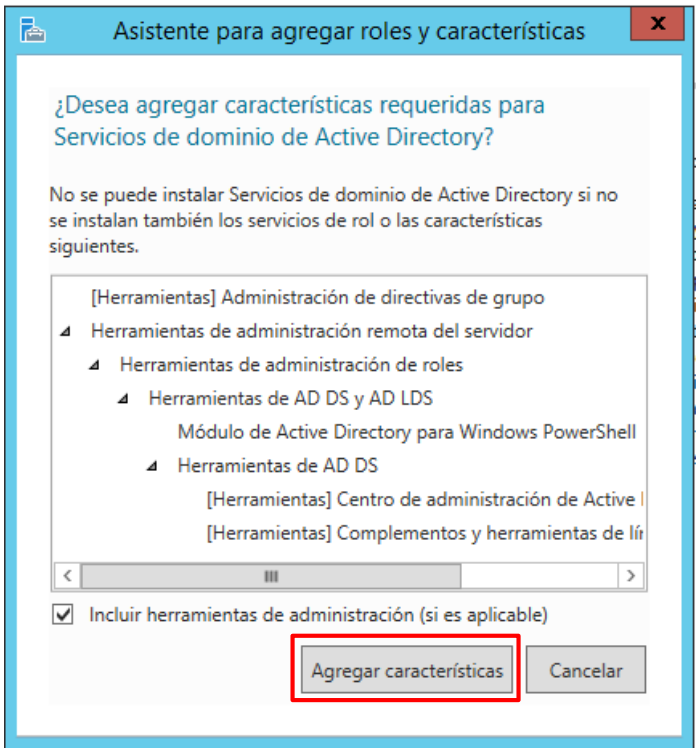
Captura 93 - Instal•lació Servei de Domini Active Directory 3

Seleccionar el rol de **"Servicios de dominio de Active Directory"** i clicar **"Siguiente"**.



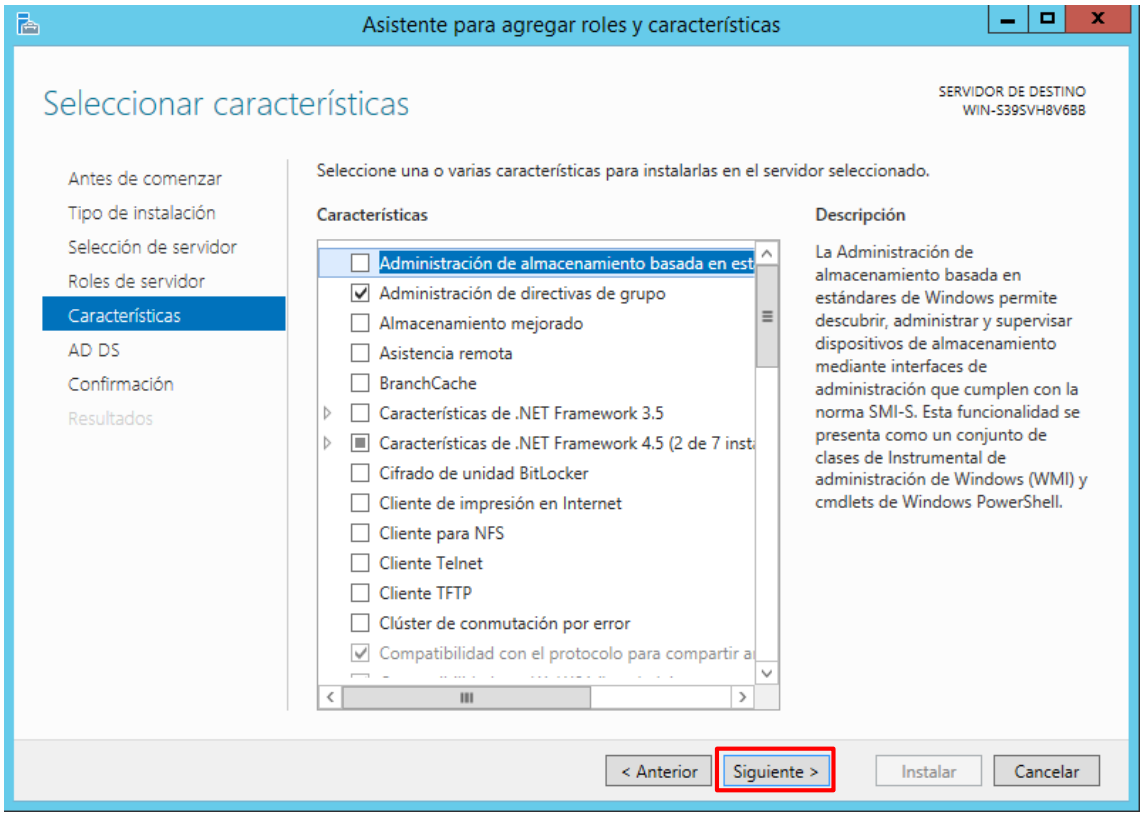
Captura 94 - Instal•lació Servei de Domini Active Directory 4

Clicar en **"Agregar características"**.

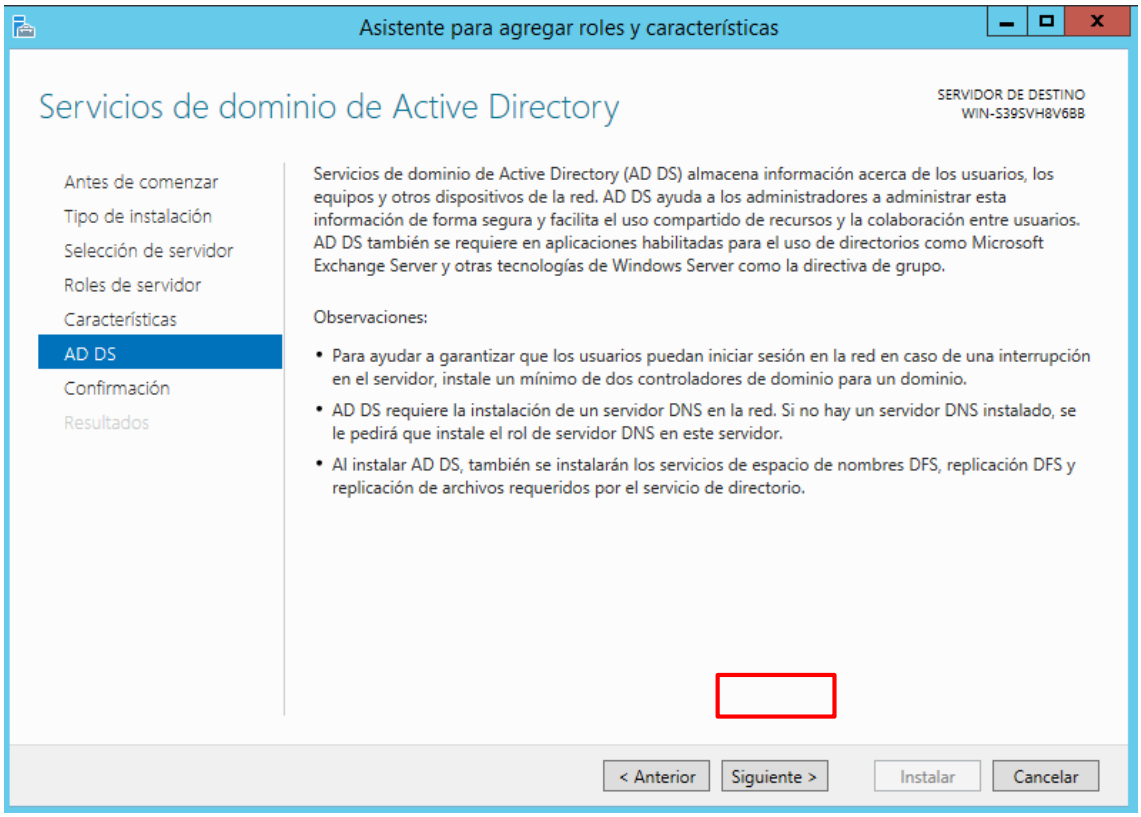


Captura 95 - Instal•lació Servei de Domini Active Directory 5

Picar en **"Siguiente"** fins aplegar al punt d'instal·lació.

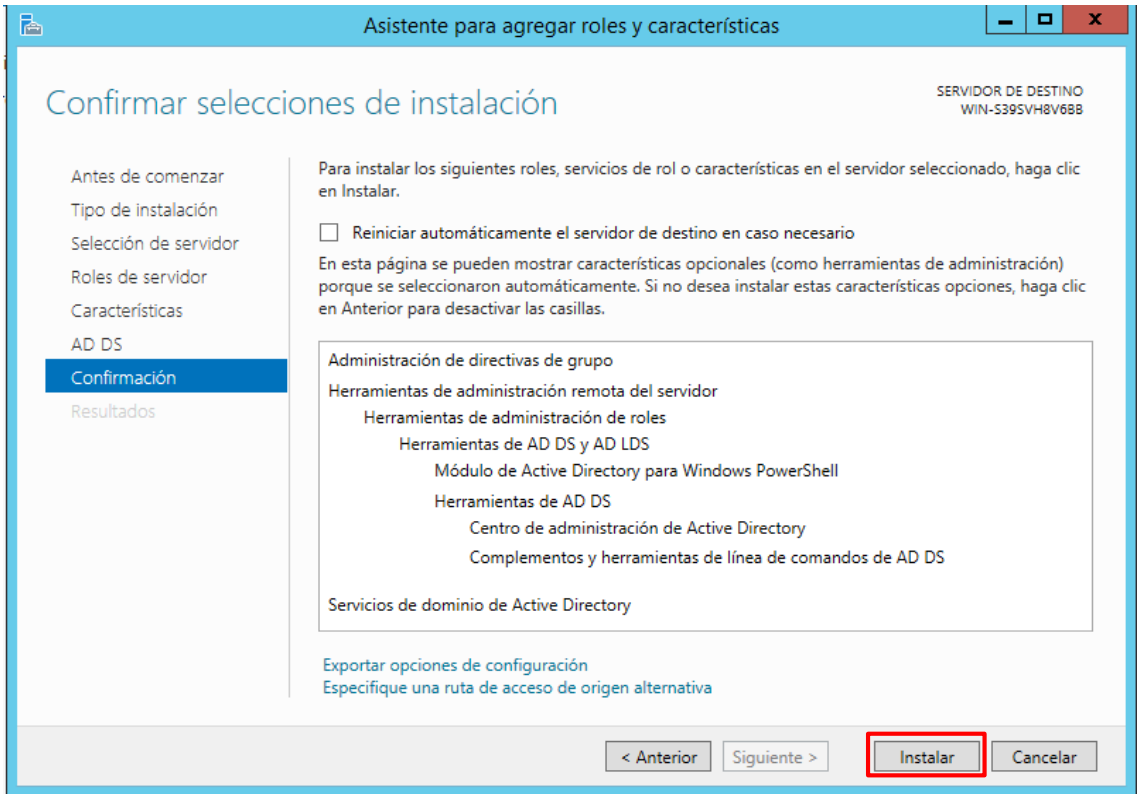


Captura 96 - Instal•lació Servei de Domini Active Directory 6

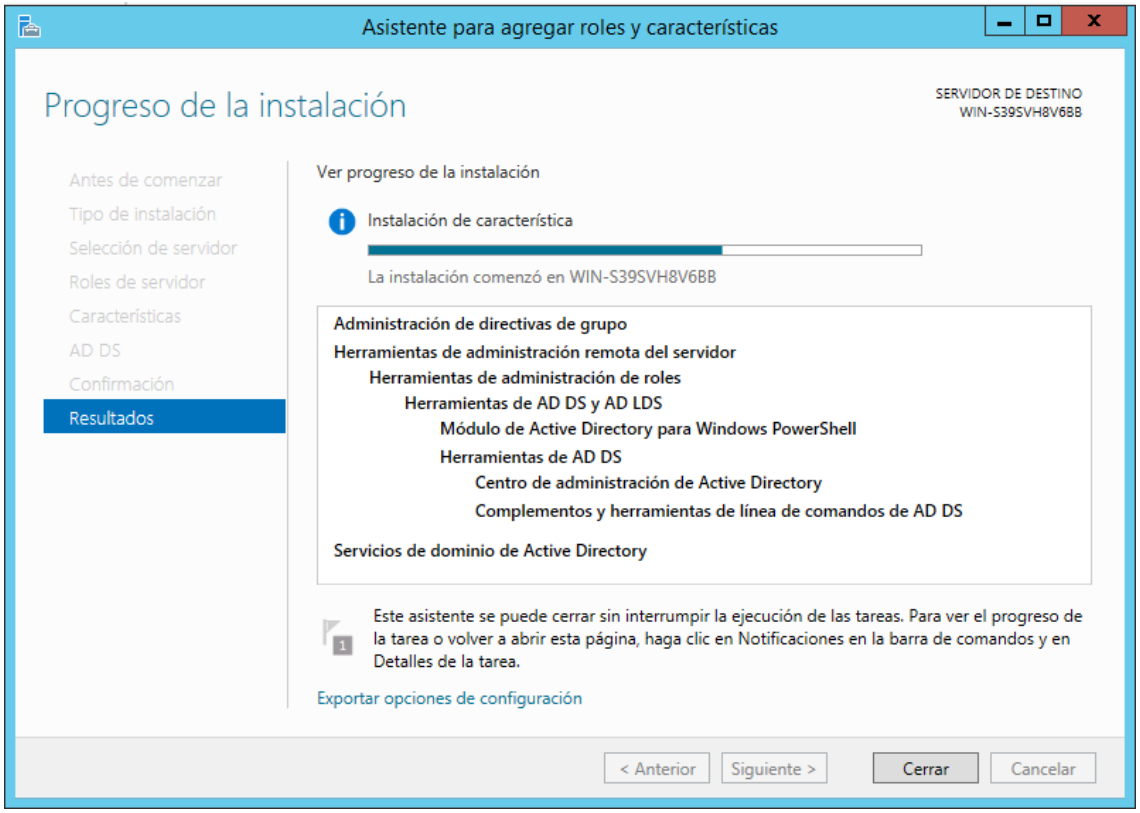


Captura 97 - Instal•lació Servei de Domini Active Directory 7

Clicar en **"Instalar"**.



Captura 98 - Instal•lació Servei de Domini Active Directory 8

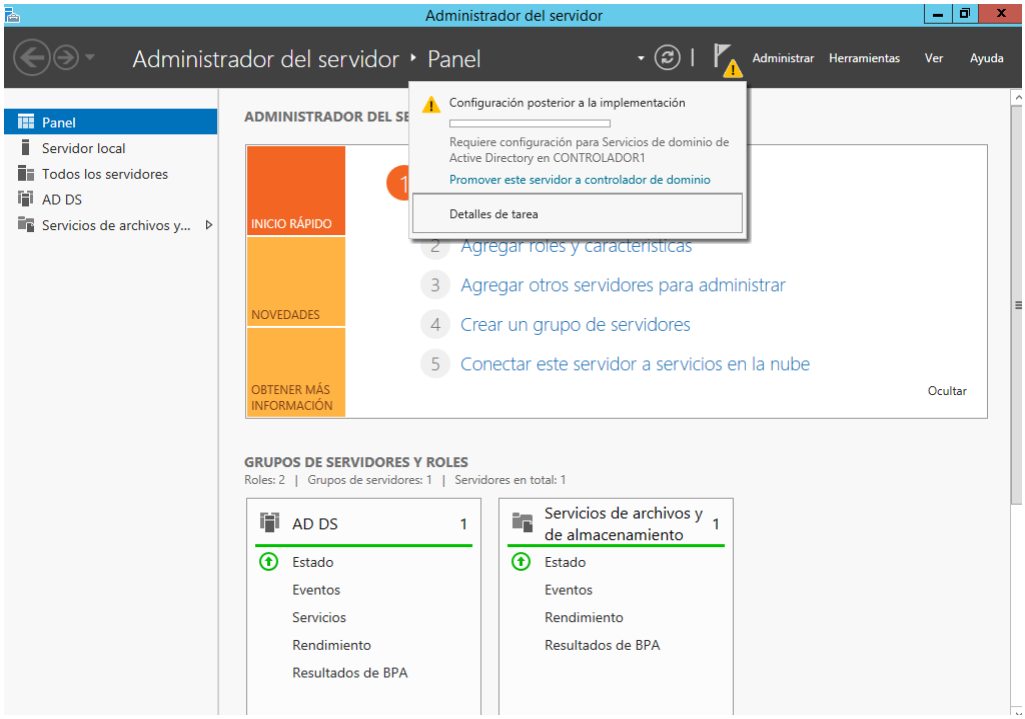


Captura 99 - Instal•lació Servei de Domini Active Directory 9

Una vegada finalitzat el procés d'instal·lació, es tanca la finestra, per tal de continuar en les següents instal·lacions.

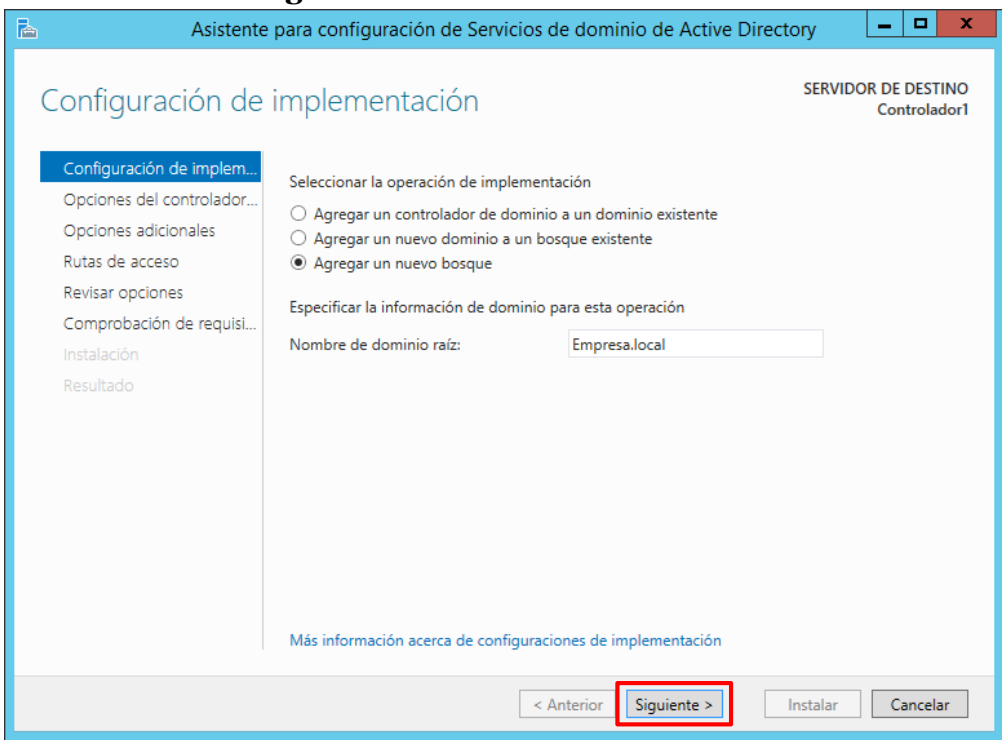
7.5 Promocionar el servidor a Controlador de Domini (DC)

Després d'instal·lar el AD DS, apareix una advertència per a promocionar el servidor a controlador de domini. Clicant a l'advertència apareixerà l'assistent per a dur a terme la promoció.



Captura 100 - Promocionar servidor a Controlador de domini 1

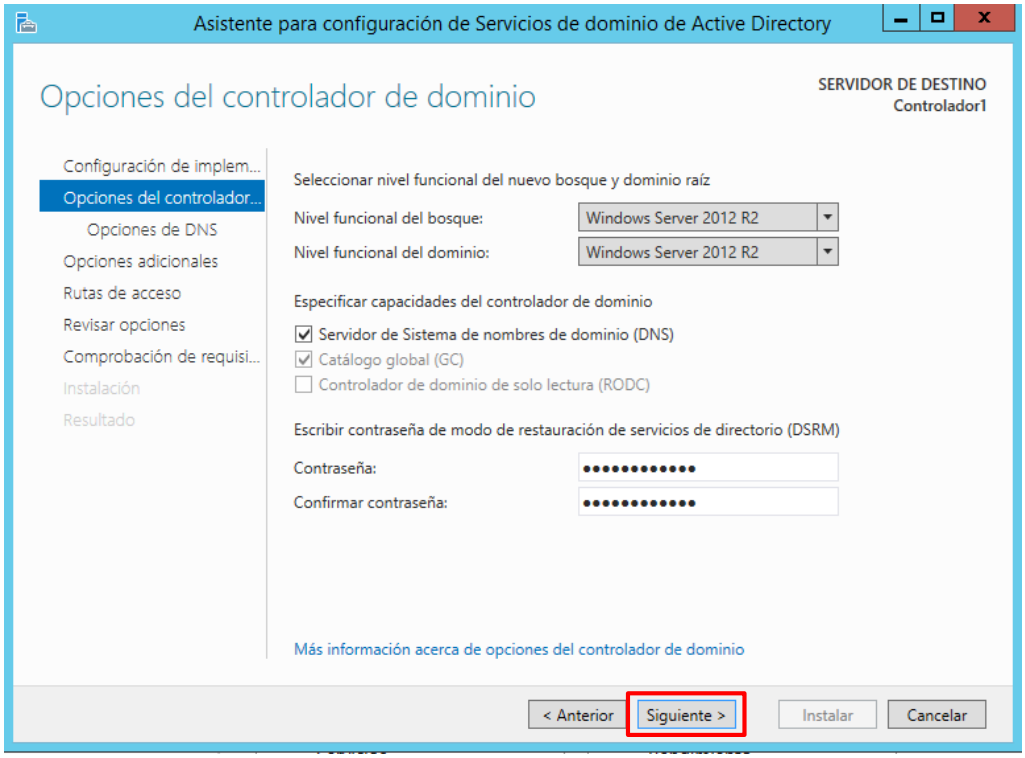
Seleccionar **"Agregar un nuevo bosque"** i escriure el nom del domini arrel. A continuació clicar **"Siguiente".**



Captura 101 - Promocionar servidor a Controlador de domini 2

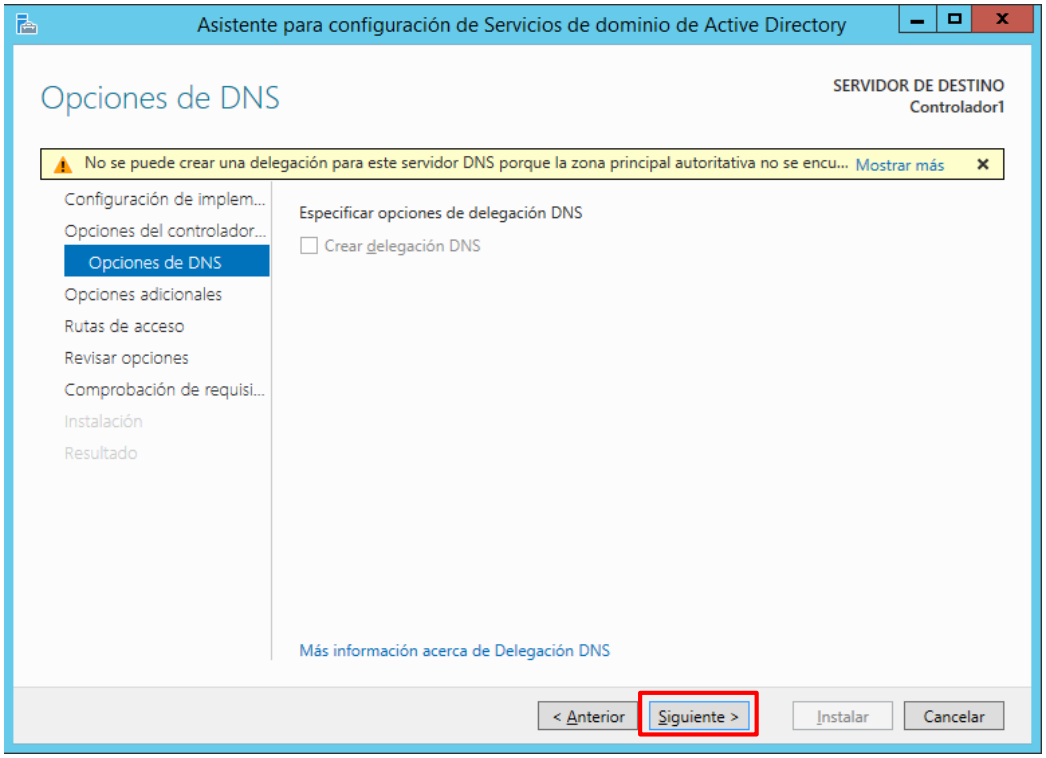
Seleccionar el nivell funcional del bosc i del domini. En aquest cas deixem les opcions per defecte, però podrien ser útils si es pretén afegir controladors de domini d'altres versions de Windows Server.

A més cal introduir una contrasenya que servirà en cas de voler des-promocionar un domini o donar de baixa el domini. Clicar **"Siguiente"**.



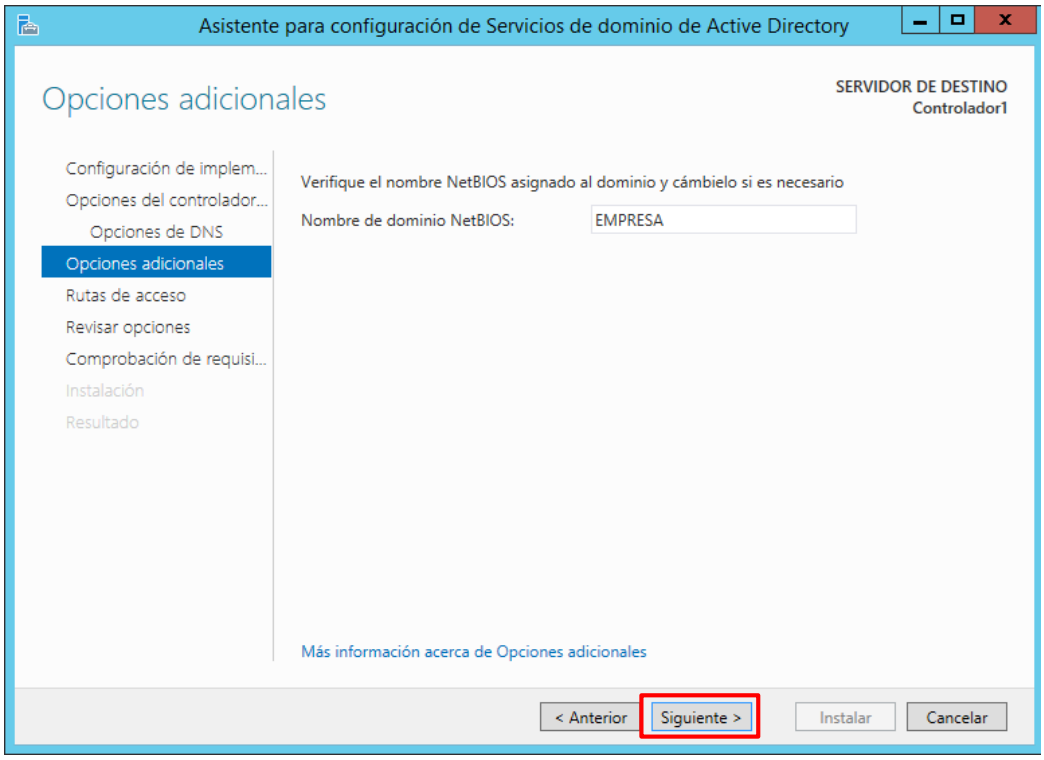
Captura 102 - Promocionar servidor a Controlador de domini 3

Clicar **"Siguiente"**.



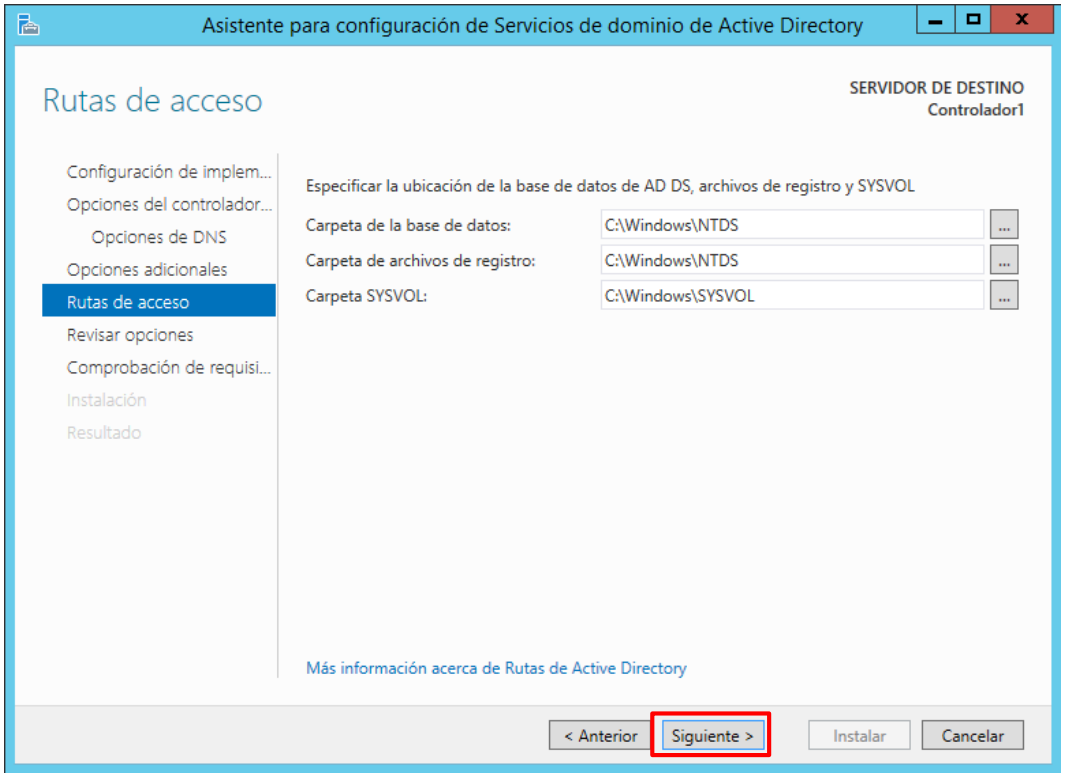
Captura 103 - Promocionar servidor a Controlador de domini 4

Definir el nom de domini NetBIOS, per si es vol afegir al domini sistemes anteriors al Windows 2000.



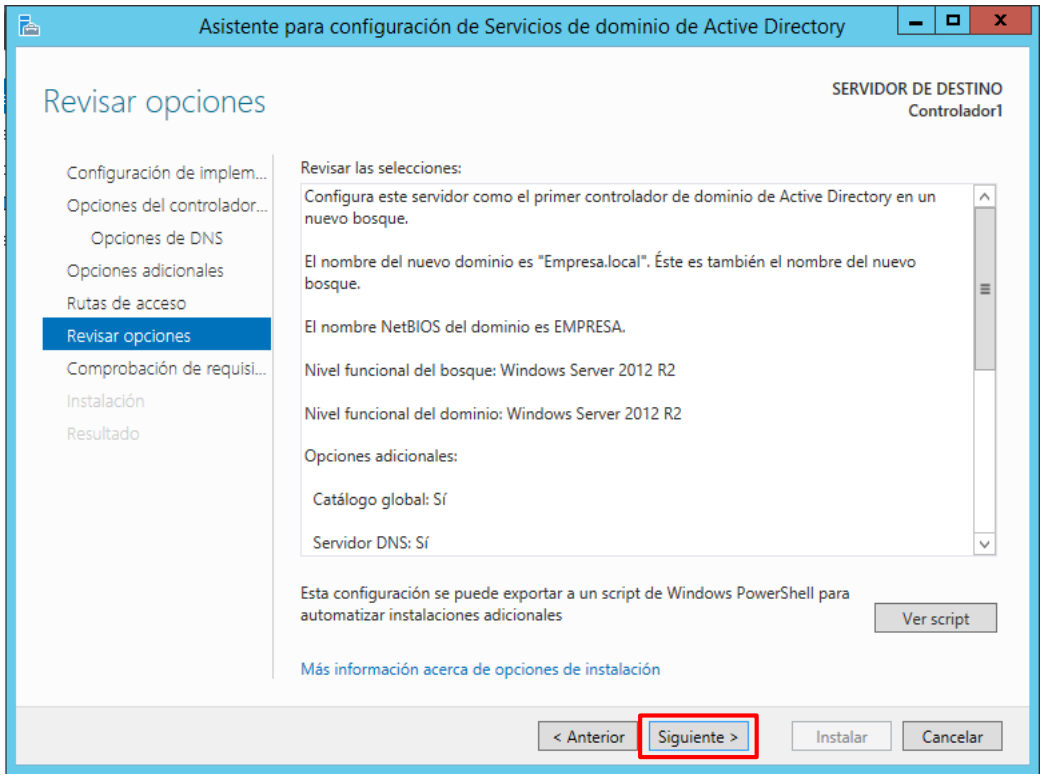
Captura 104 - Promocionar servidor a Controlador de domini 5

Deixar per defecte els directoris on s'emmagatzemaran System Volum (SYSVOL), els fitxers de registre i la base de dades. Picar en **"Siguiente"**.



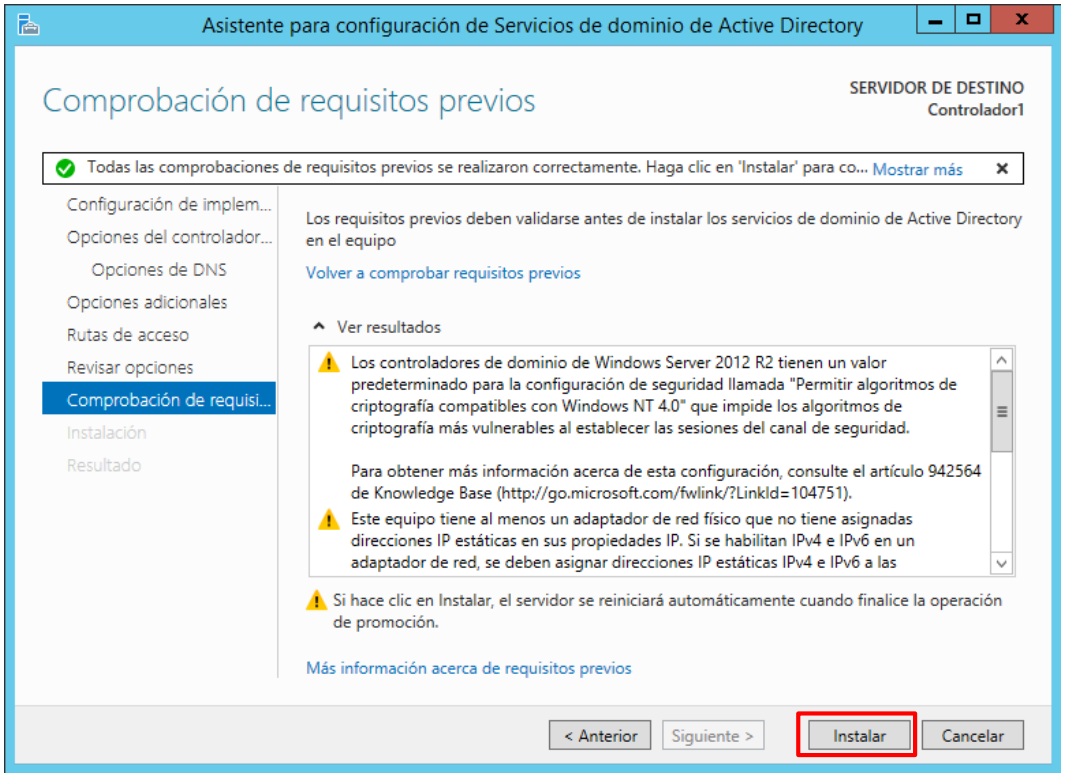
Captura 105 - Promocionar servidor a Controlador de domini 6

Clicar **"Siguiente"**.



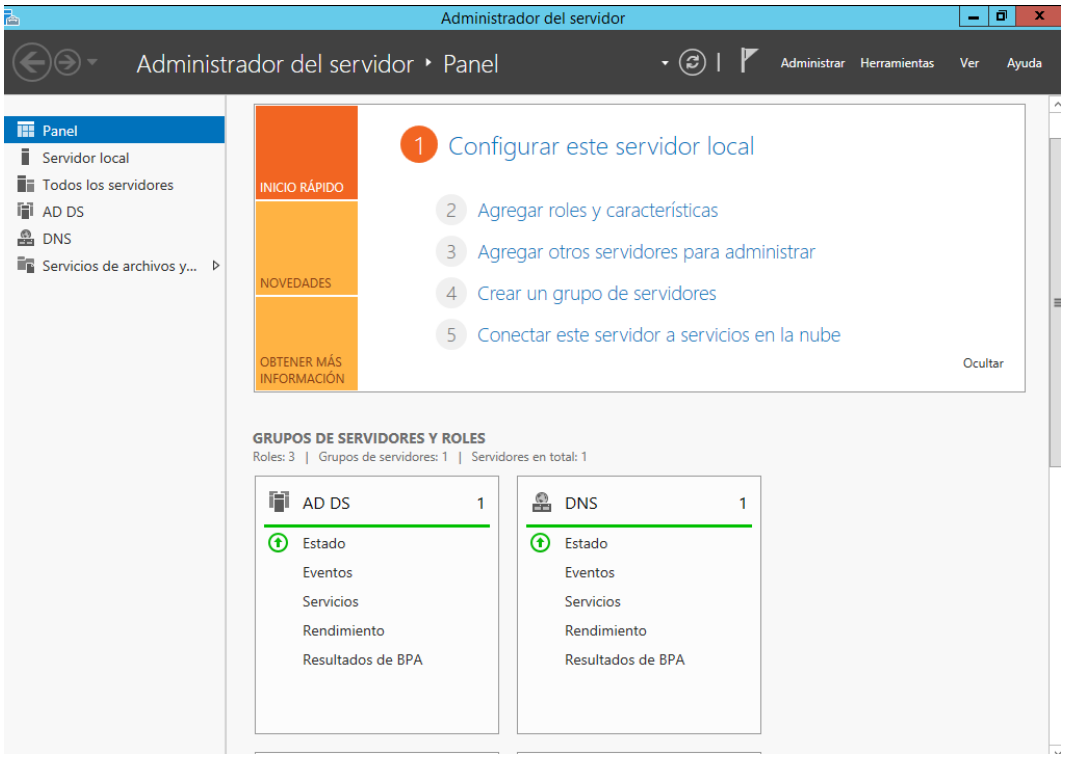
Captura 106 - Promocionar servidor a Controlador de domini 7

Picar en **"Instalar"**.



Captura 107 - Promocionar servidor a Controlador de domini 8

Una volta finalitzada la instal·lació es pot observar en la consola que ja apareix el rol AD DS i el rol DNS instal·lats al servidor.

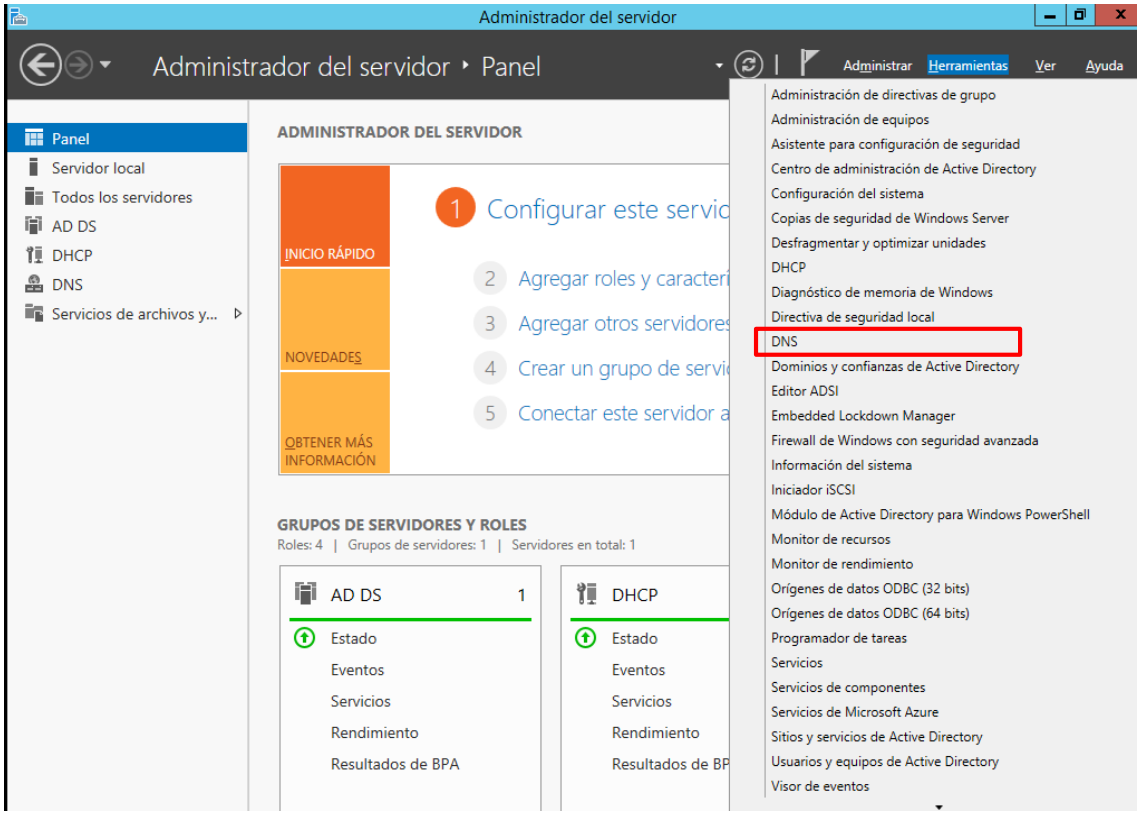


Captura 108 - Promocionar servidor a Controlador de domini 9

7.6 Configurar la zona de cerca inversa DNS

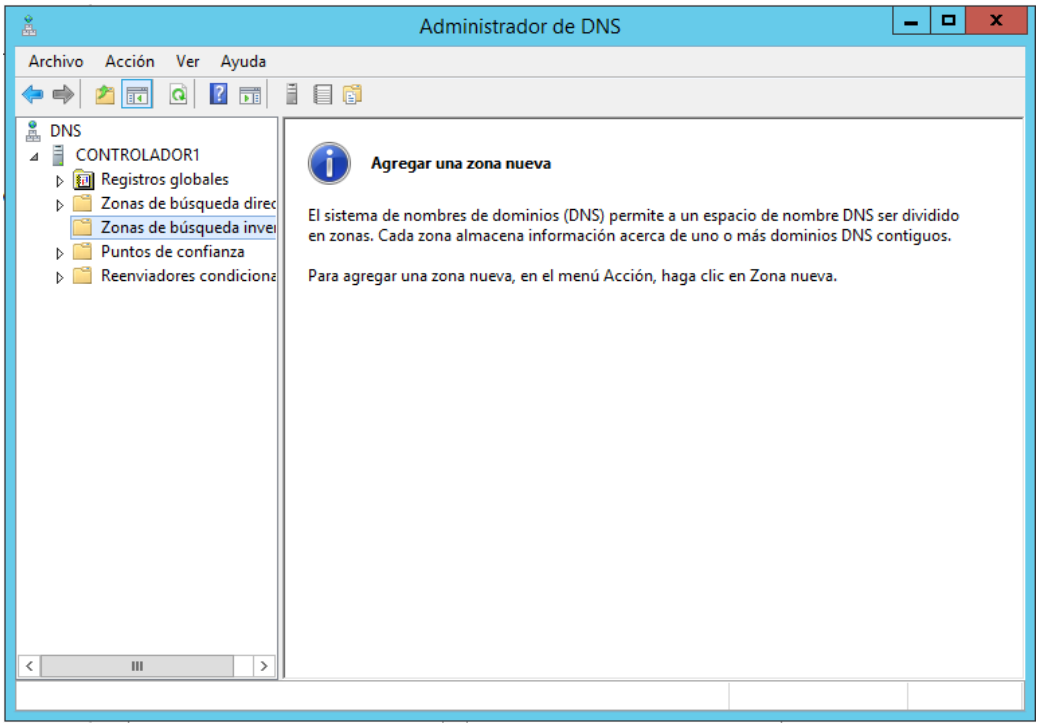
A partir del Servidor DNS, ja instal·lat en l'apartat anterior, s'instal·la i configura la zona de cerca inversa.

En el tauler **"Administrador del servidor"**, es selecciona el menú **"Herramientas"** i es clica en **DNS**.



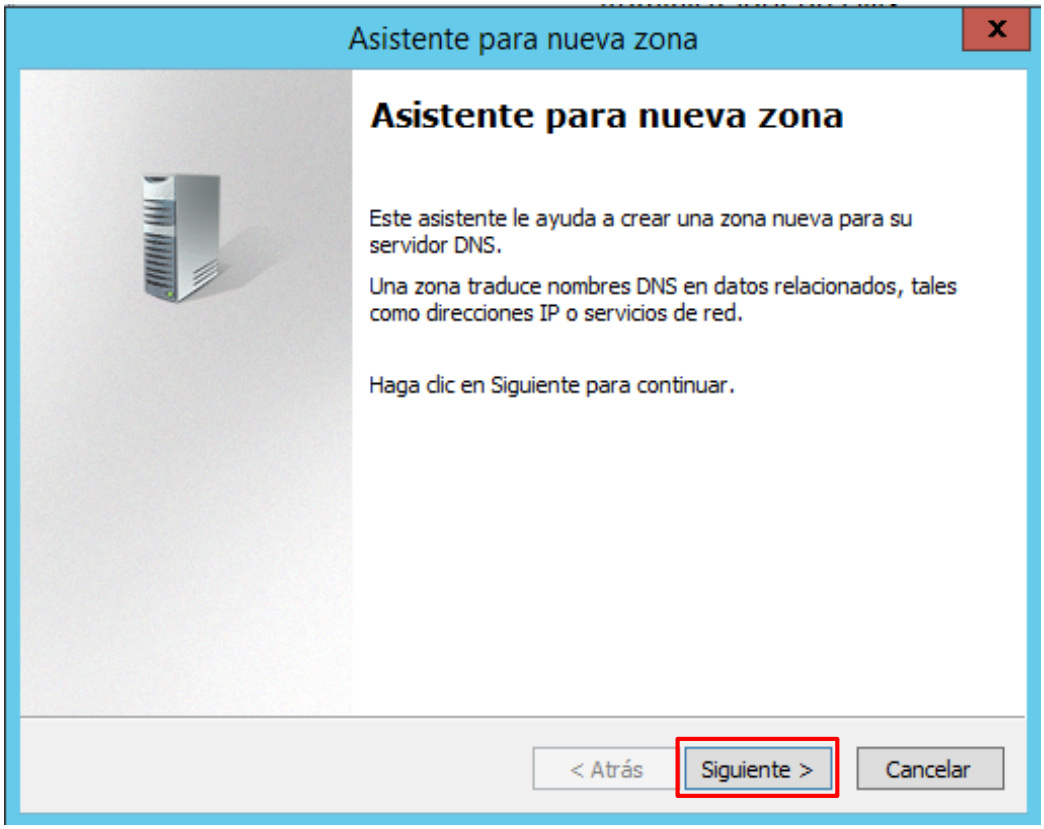
Captura 109 - Configurar zona de cerca inversa DNS 1

A continuació cal picar en el botó dret sobre **"Zona de búsqueda inversa"** i seleccionar **"Nueva zona de búsqueda inversa"**.



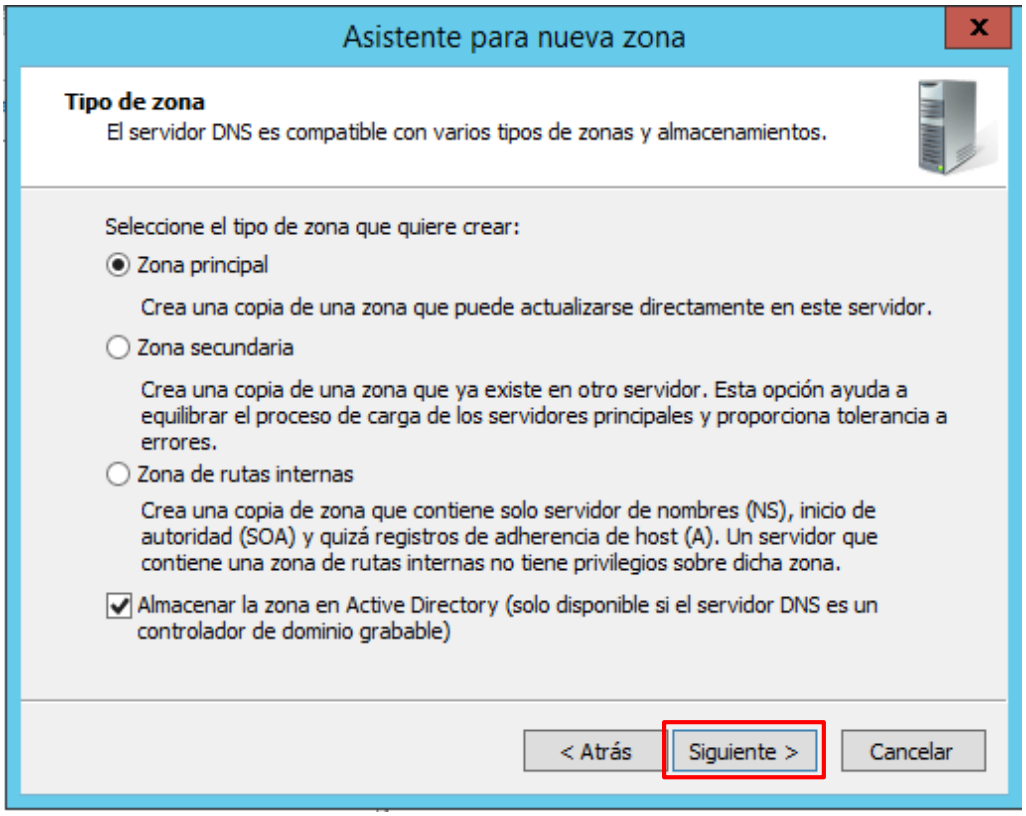
Captura 110 - Configurar zona de cerca inversa DNS 2

S'obrirà l'assistent i es pica en **"siguiente"**.

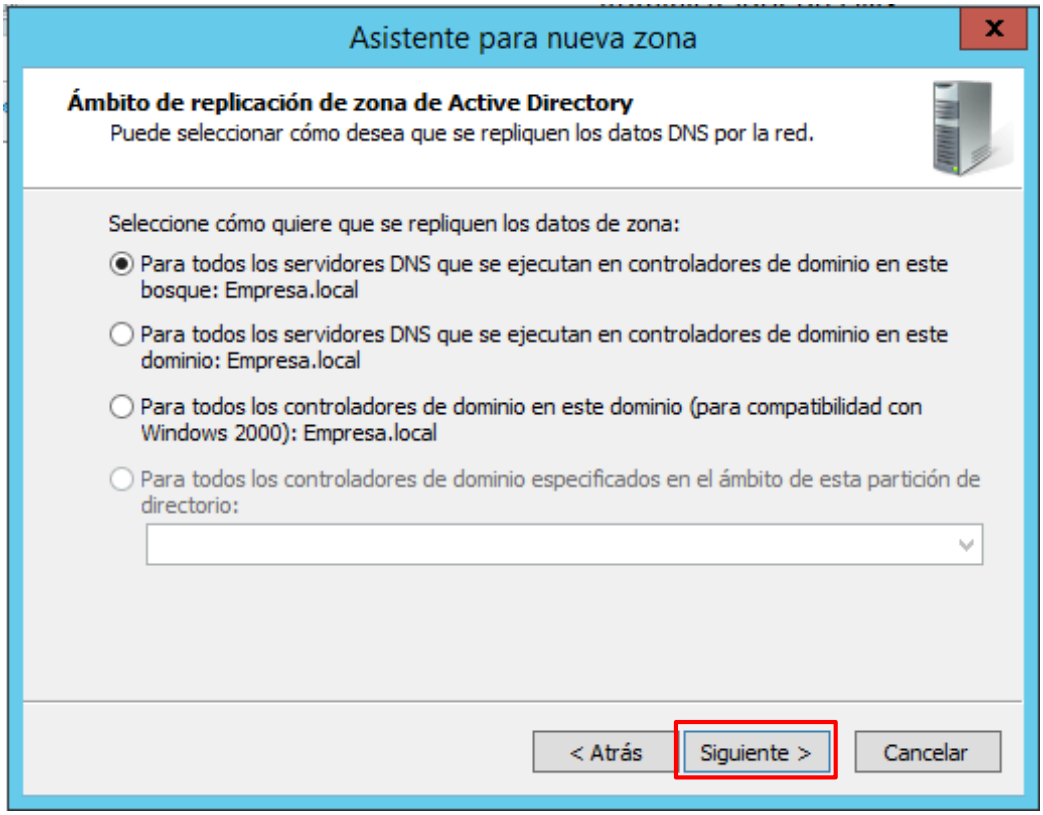


Captura 111 - Configurar zona de cerca inversa DNS 3

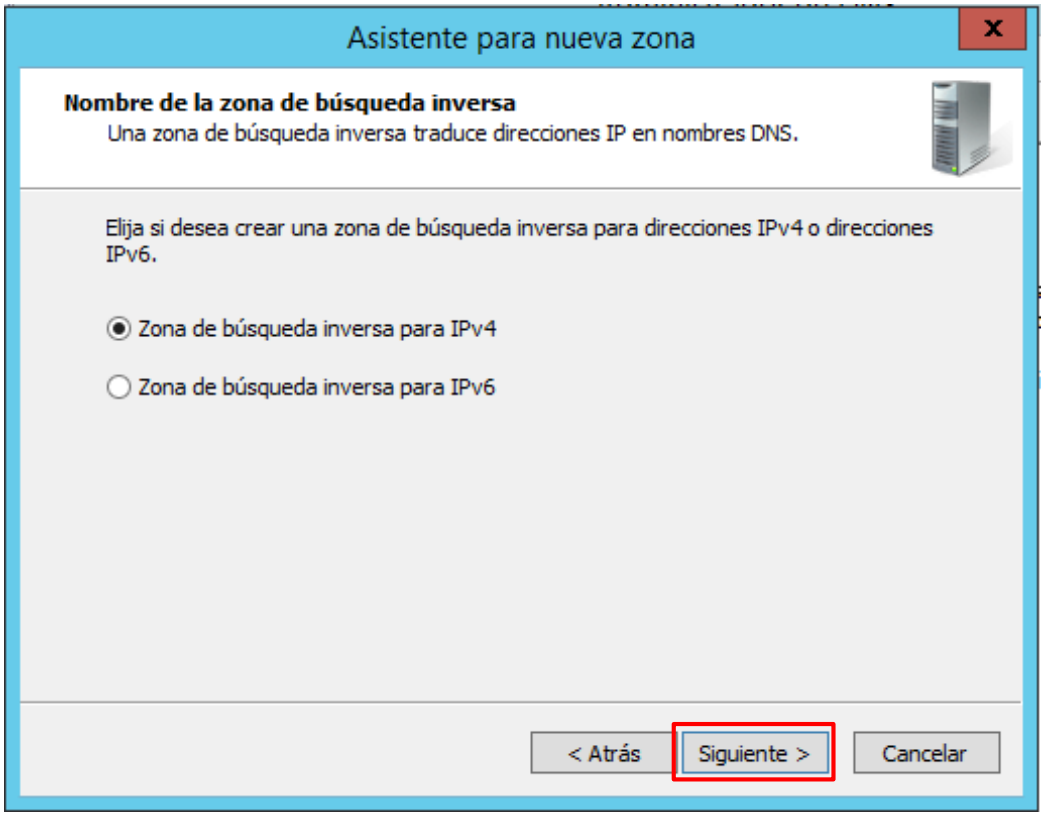
Es deixen les opcions per defecte i es pica sobre **"siguiente"** en les següents tres finestres.



Captura 112 - Configurar zona de cerca inversa DNS 4

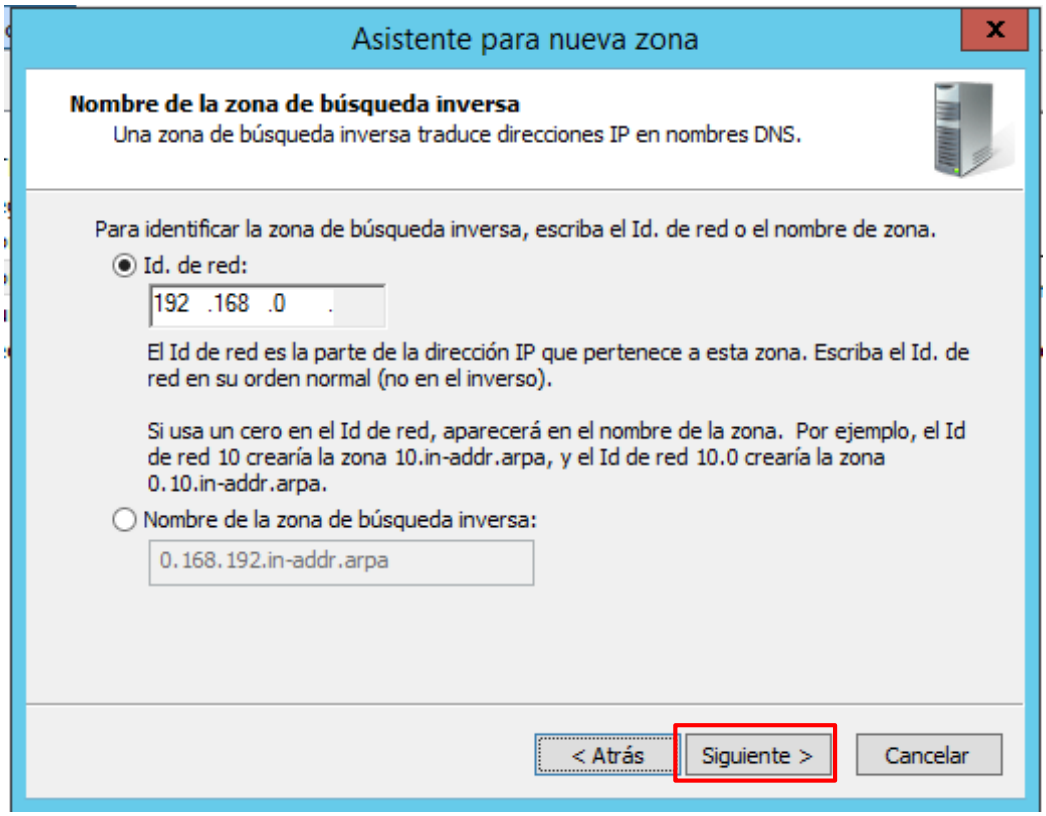


Captura 113 - Configurar zona de cerca inversa DNS 5

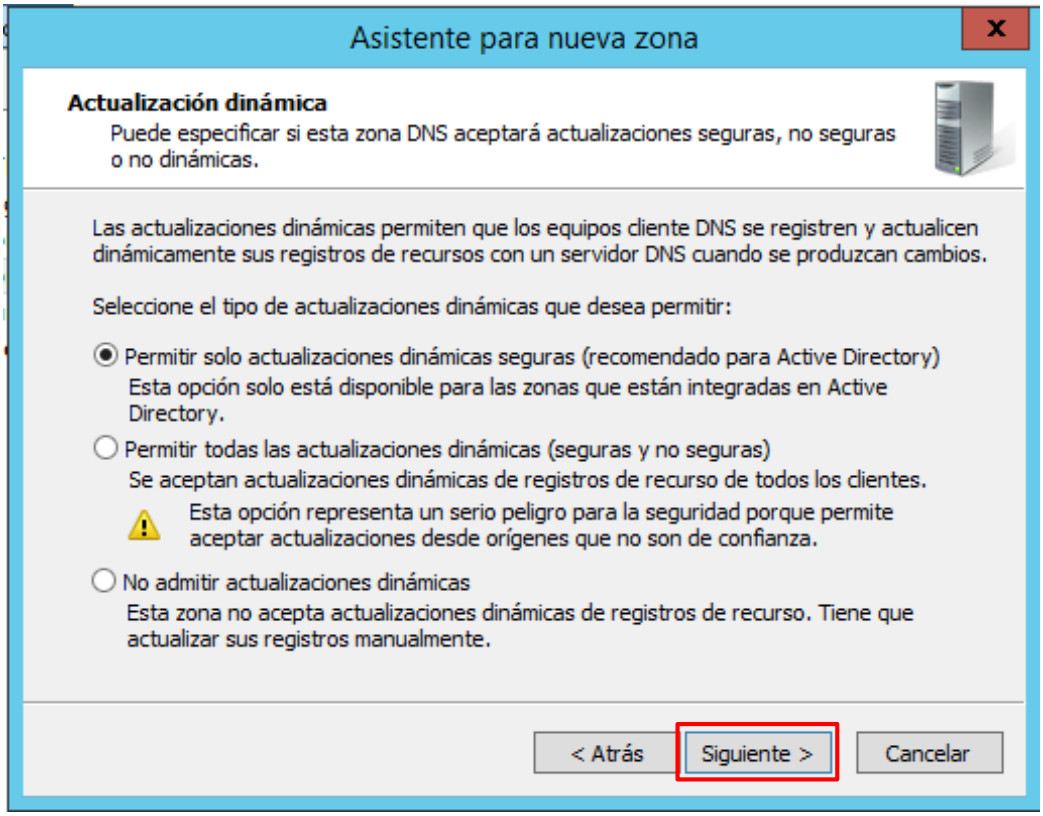


Captura 114 - Configurar zona de cerca inversa DNS 6

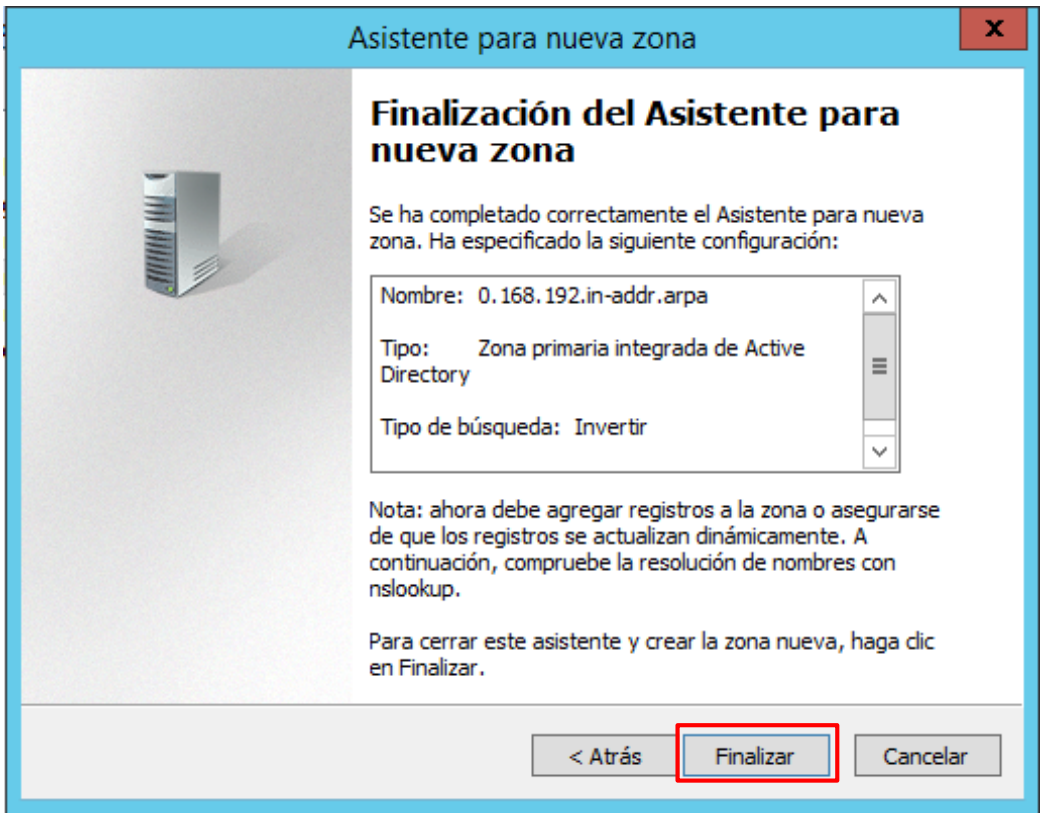
Escriure els tres primer segments del Id. de la xarxa i picar sobre **"siguiente"**.



Captura 115 - Configurar zona de cerca inversa DNS 7

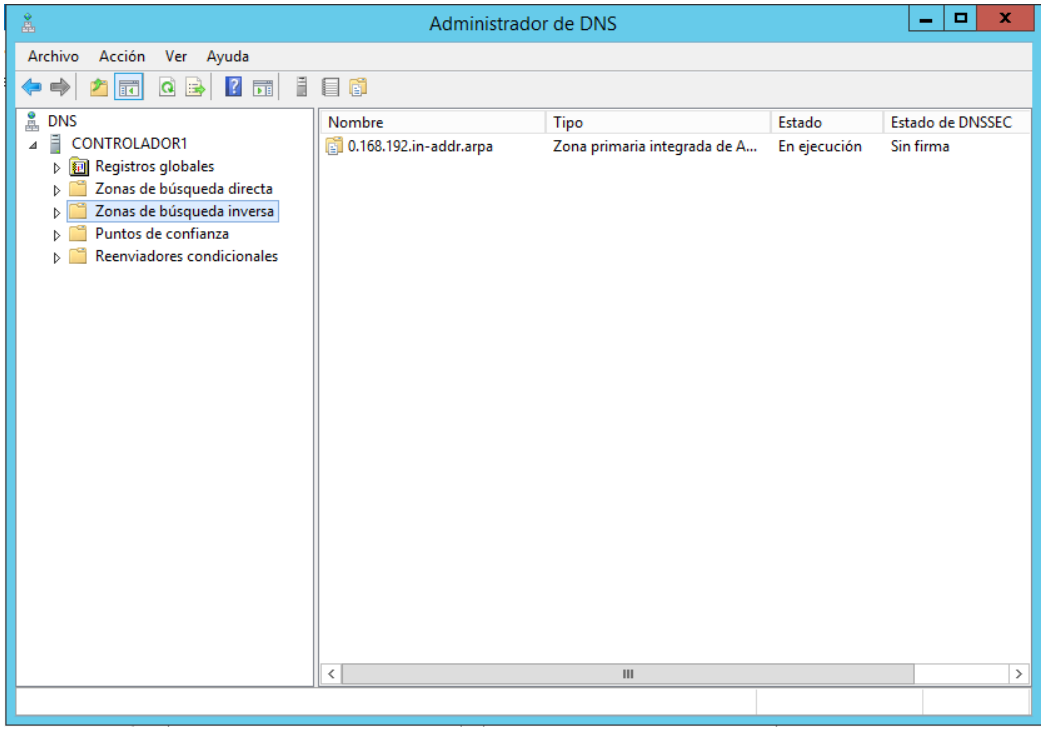


Captura 116 - Configurar zona de cerca inversa DNS 8



Captura 117 - Configurar zona de cerca inversa DNS 9

Ara ja està creada la zona de cerca inversa.



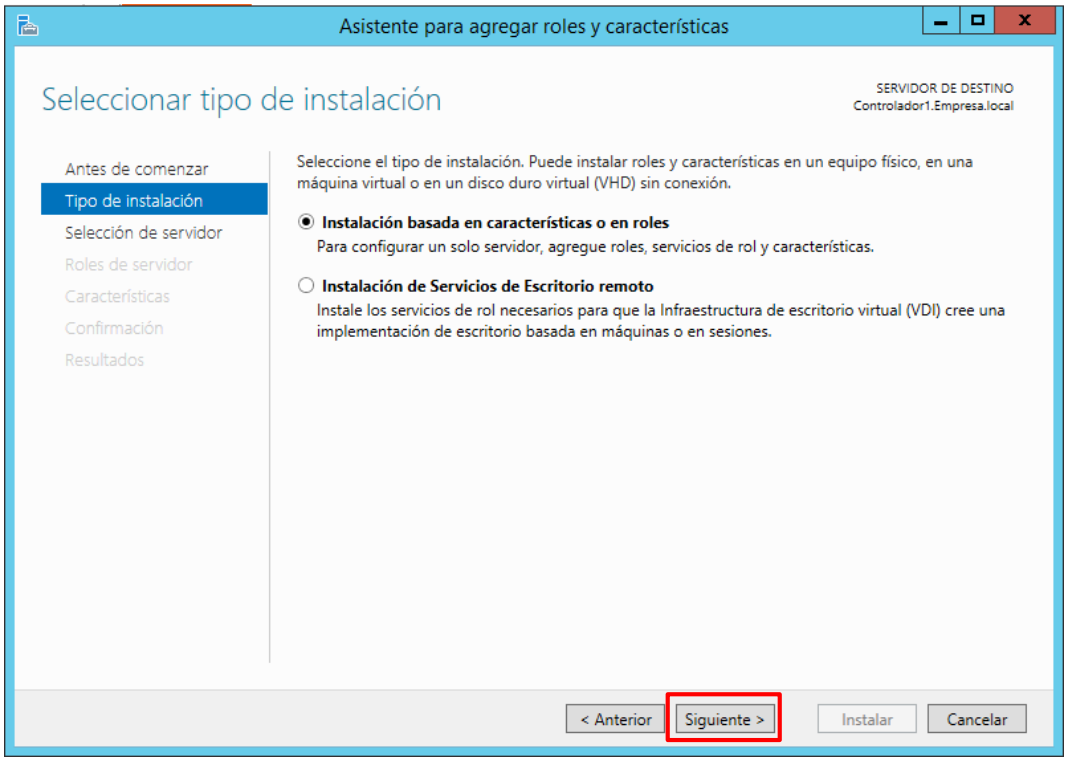
Captura 118 - Configurar zona de cerca inversa DNS 10

7.7 Configurar rol Servidor DHCP

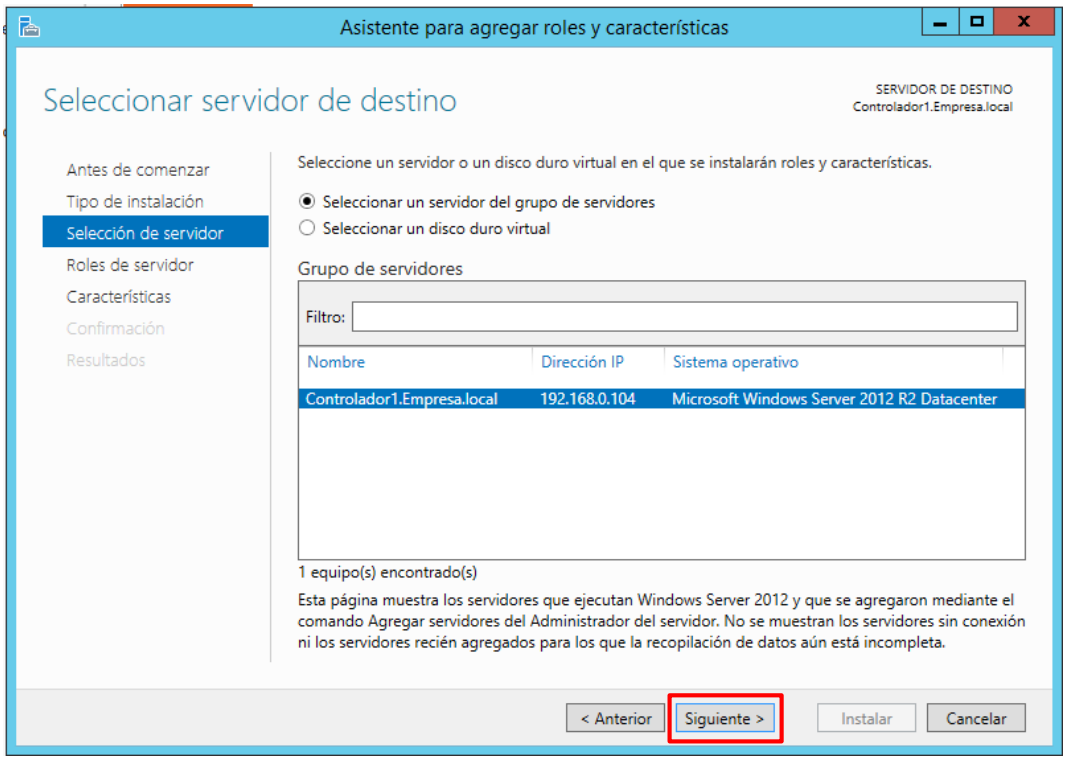
Per tal de configurar el servei DHCP en la xarxa de l'empresa, cal seguir les següents indicacions:

Obrir el l'assistent per afegir rols i característiques.

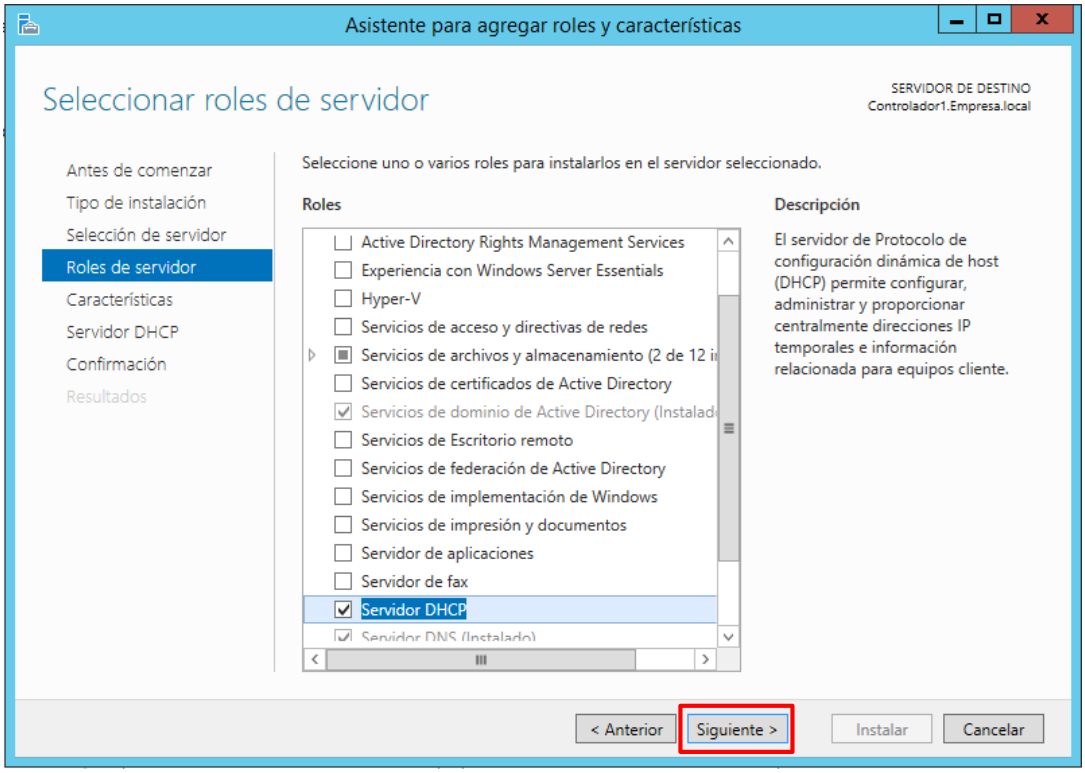
Clicar en **"Siguiente"** seleccionant les opcions que es mostren en les següents imatges.



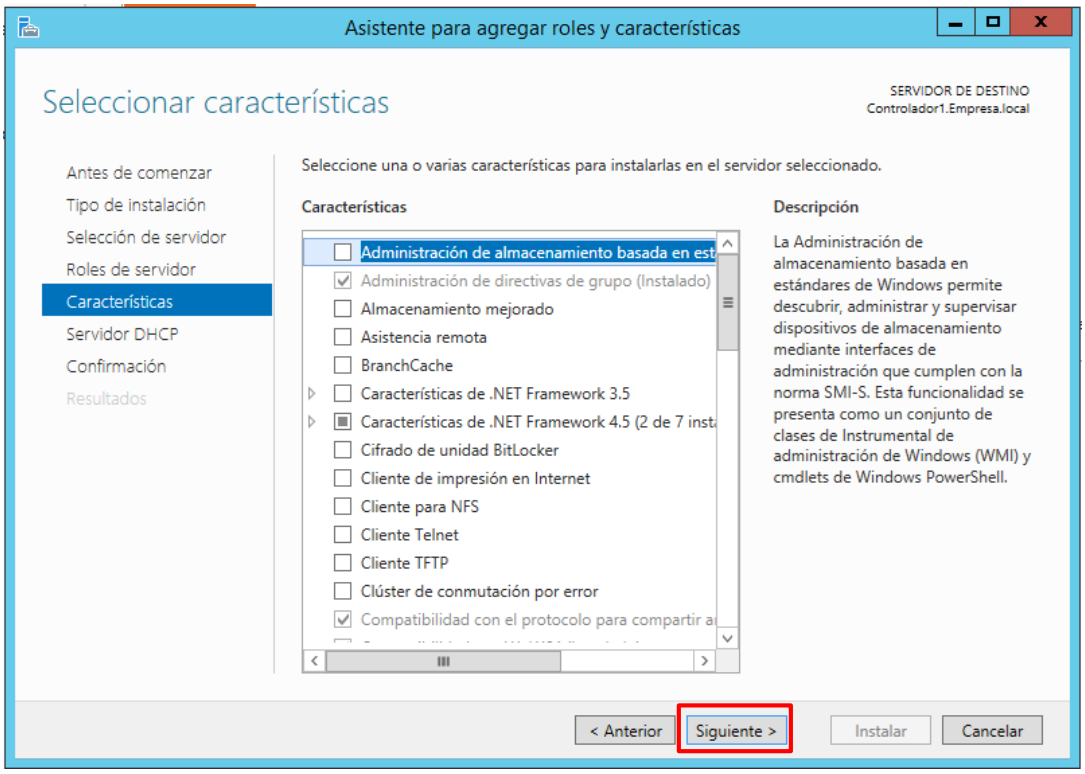
Captura 119 - Configurar DHCP 1



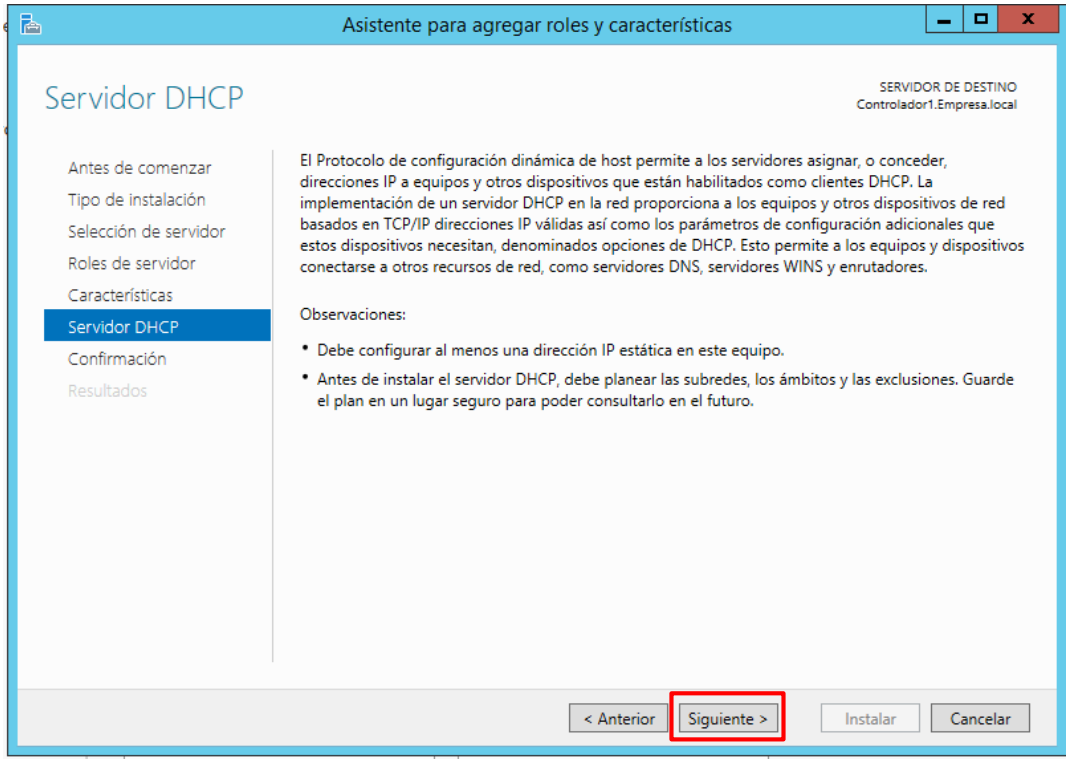
Captura 120 - Configurar DHCP 2



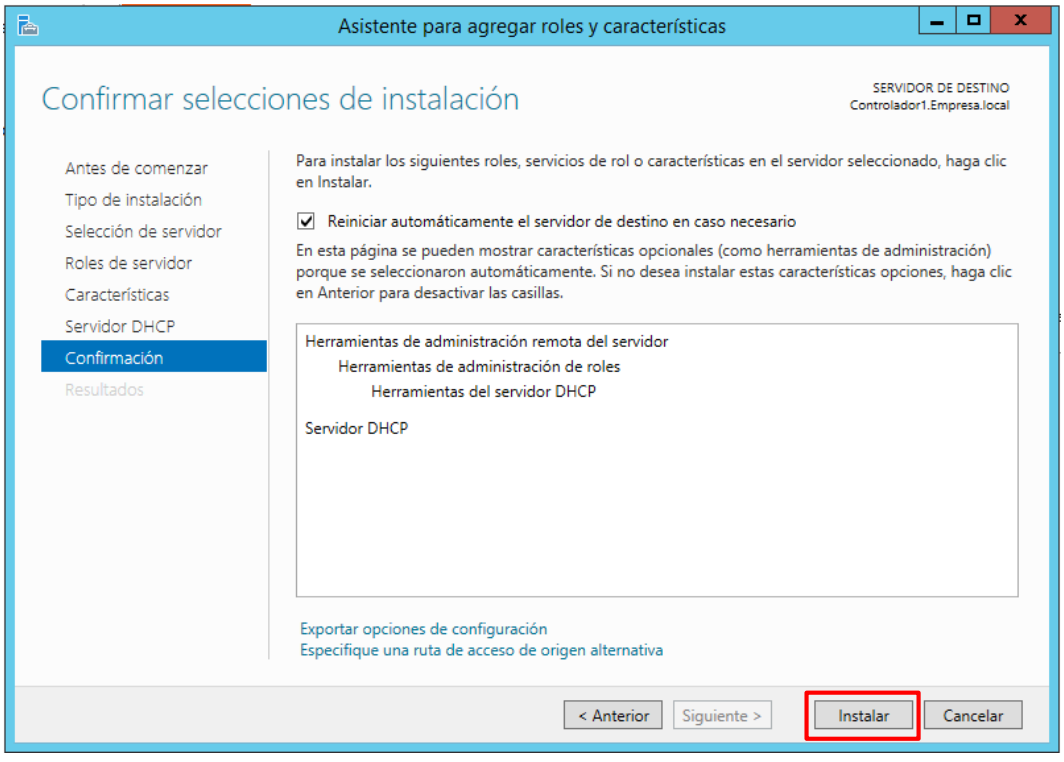
Captura 121 - Configurar DHCP 3



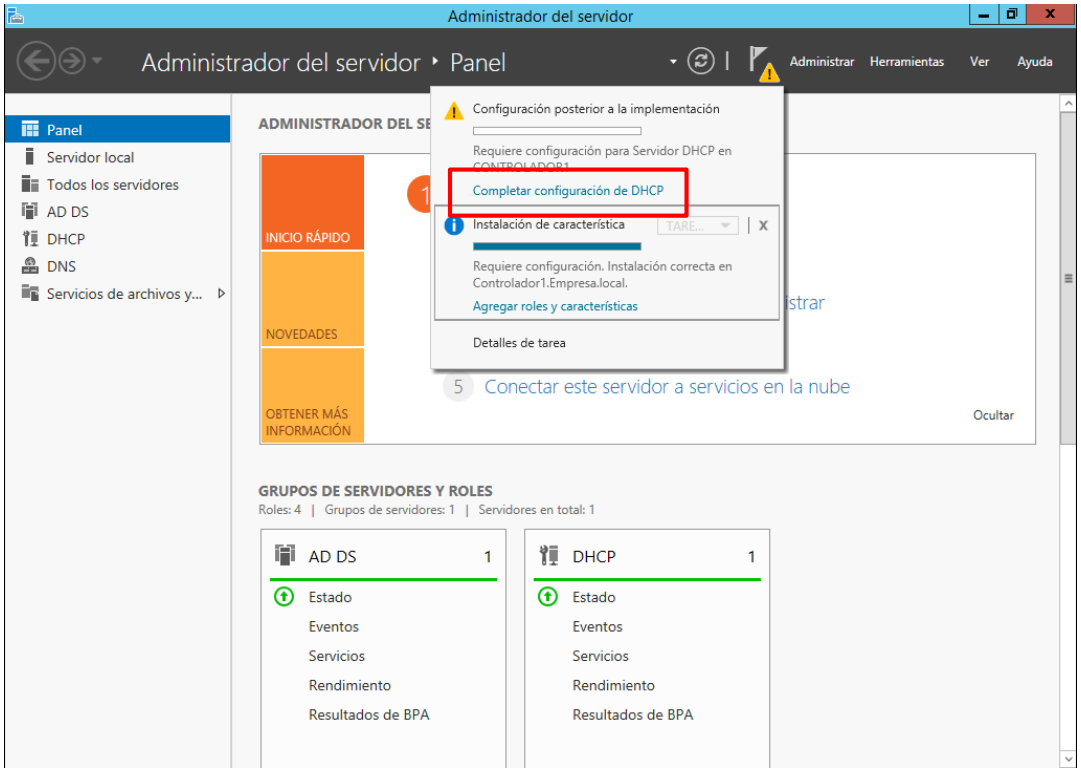
Captura 122 - Configurar DHCP 4



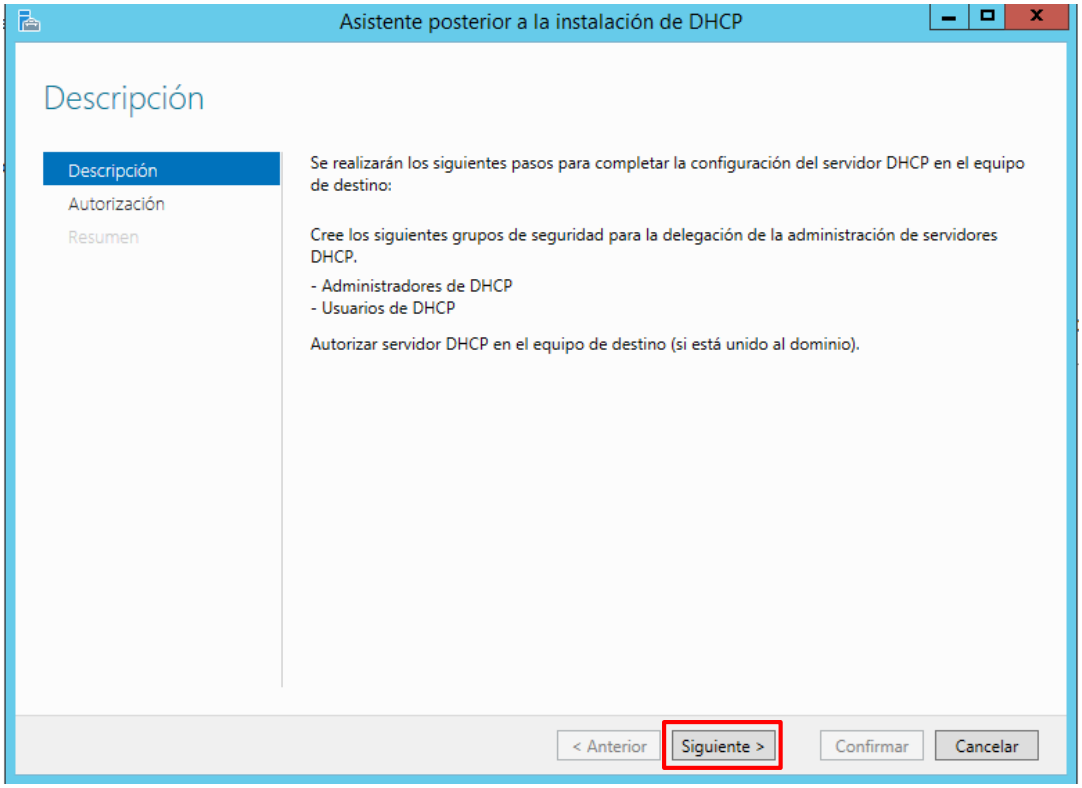
Captura 123 - Configurar DHCP 5



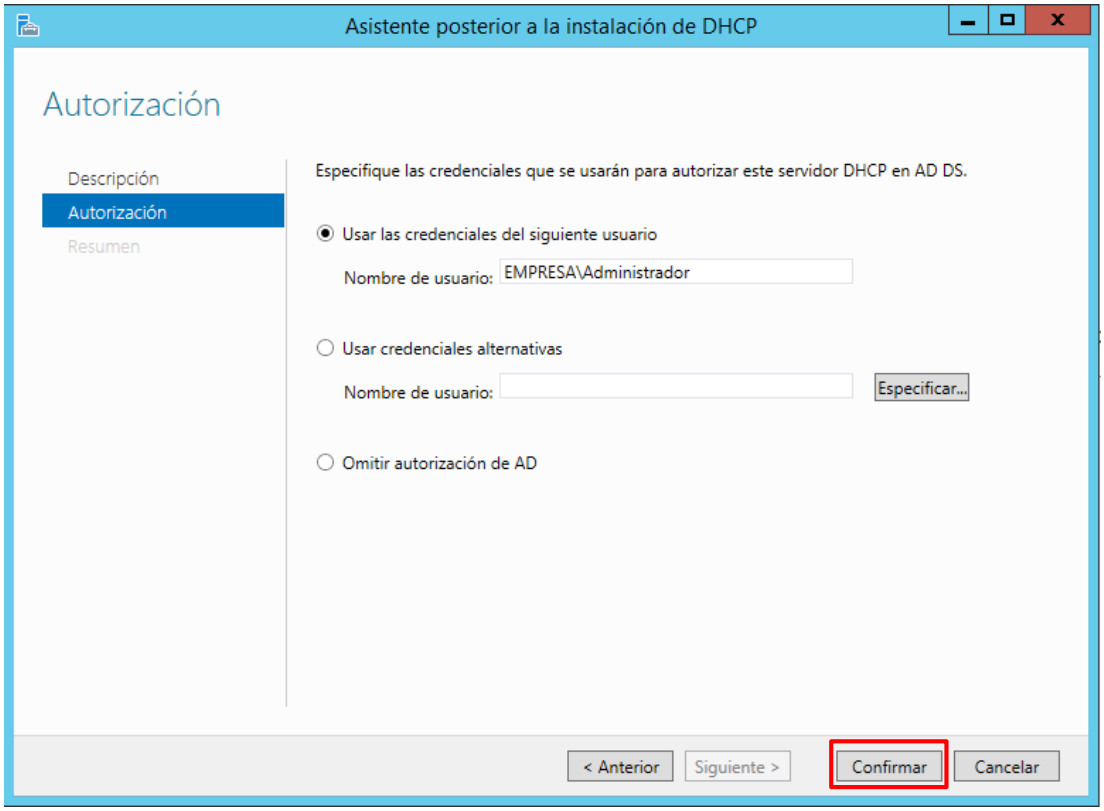
Captura 124 - Configurar DHCP 6



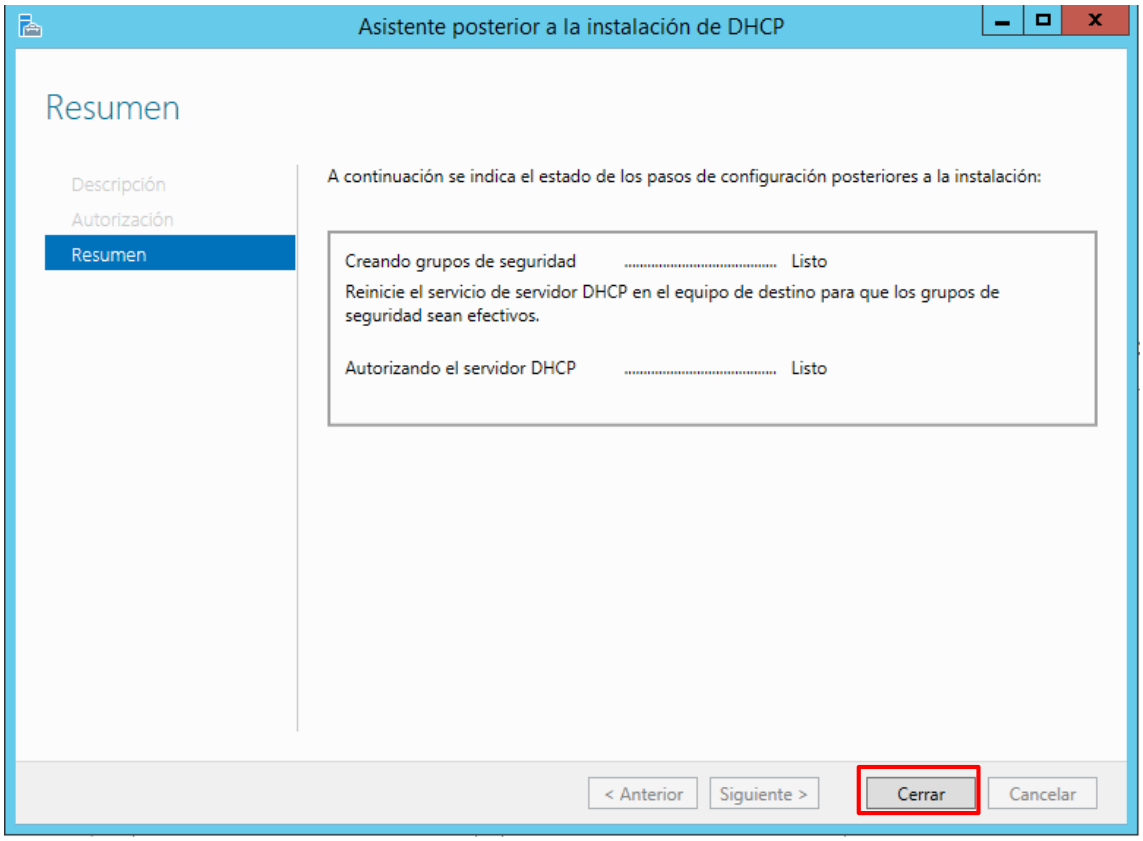
Captura 125 - Configurar DHCP 7



Captura 126 - Configurar DHCP 8

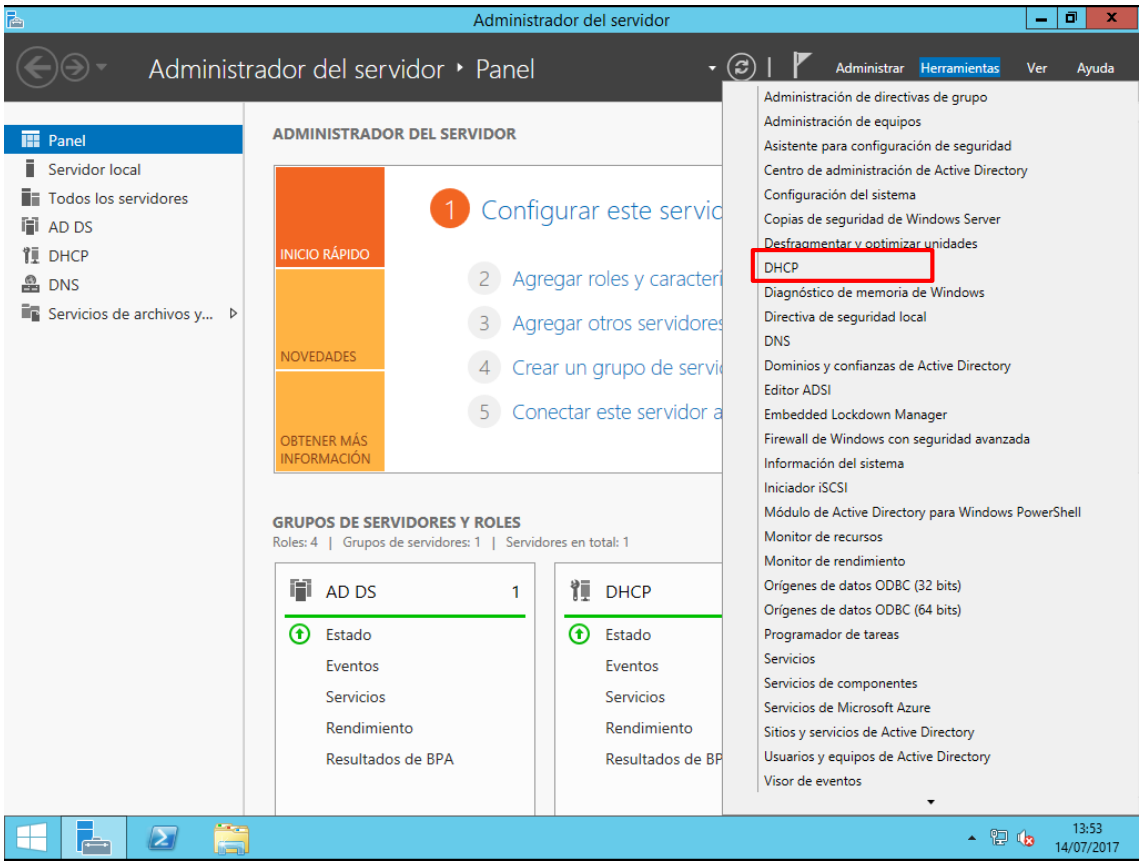


Captura 127 - Configurar DHCP 9

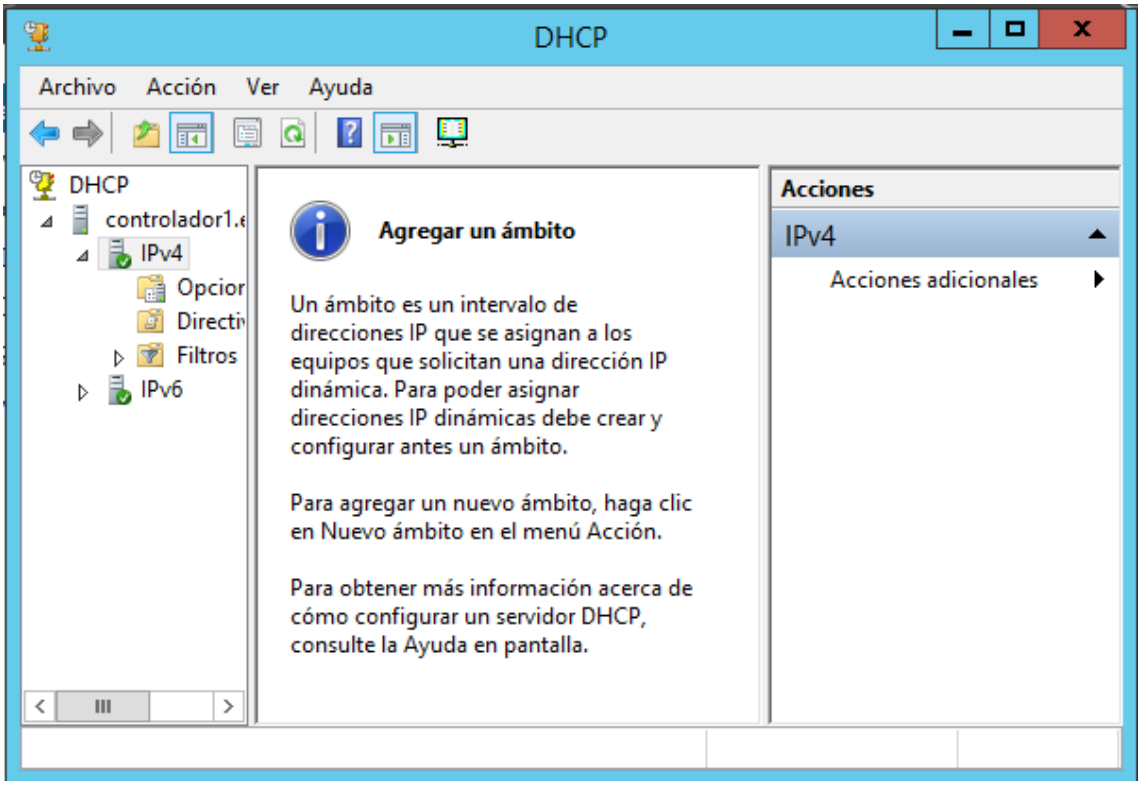


Captura 128 - Configurar DHCP 10

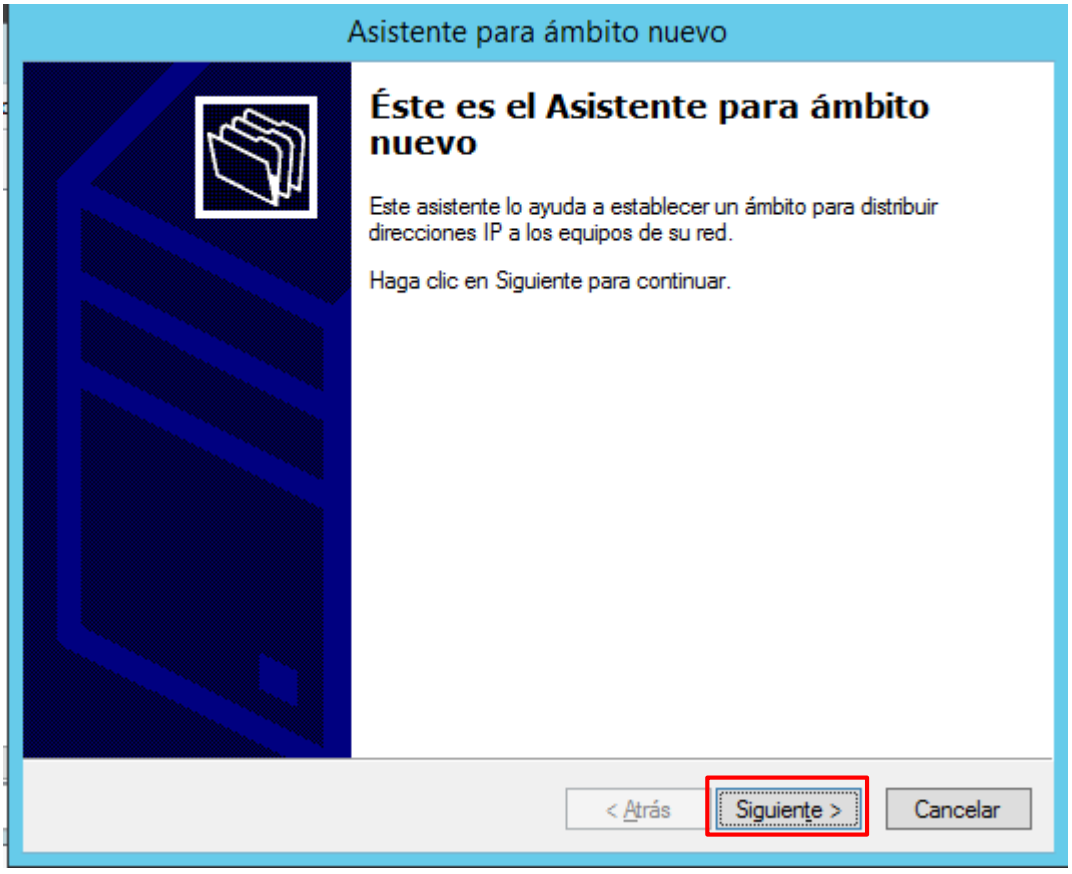
Després d'instal·lar el rol DHCP, es va a crear un Àmbit, per tal de definir un rang IP per als equips que pertanyen al domini. Per a configurar l'àmbit cal obrir el tauler de configuració del DHCP des del menú de Ferramentes de l'Administrador del servidor.



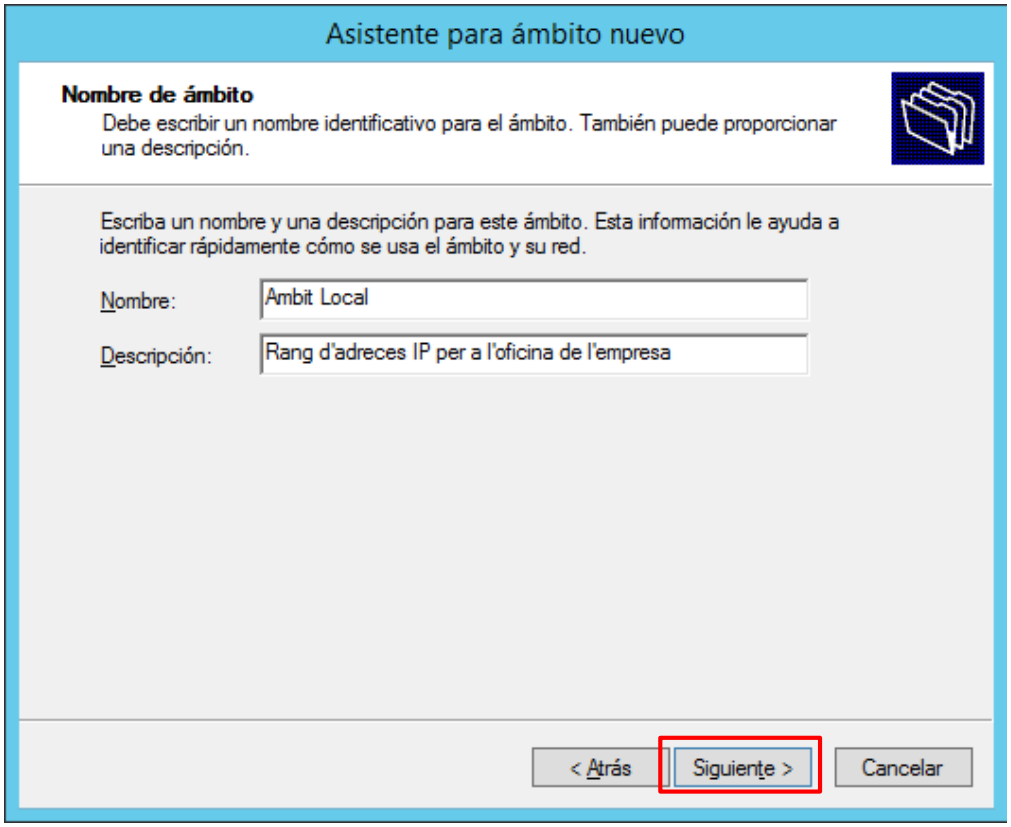
Captura 129 - Configurar DHCP 11



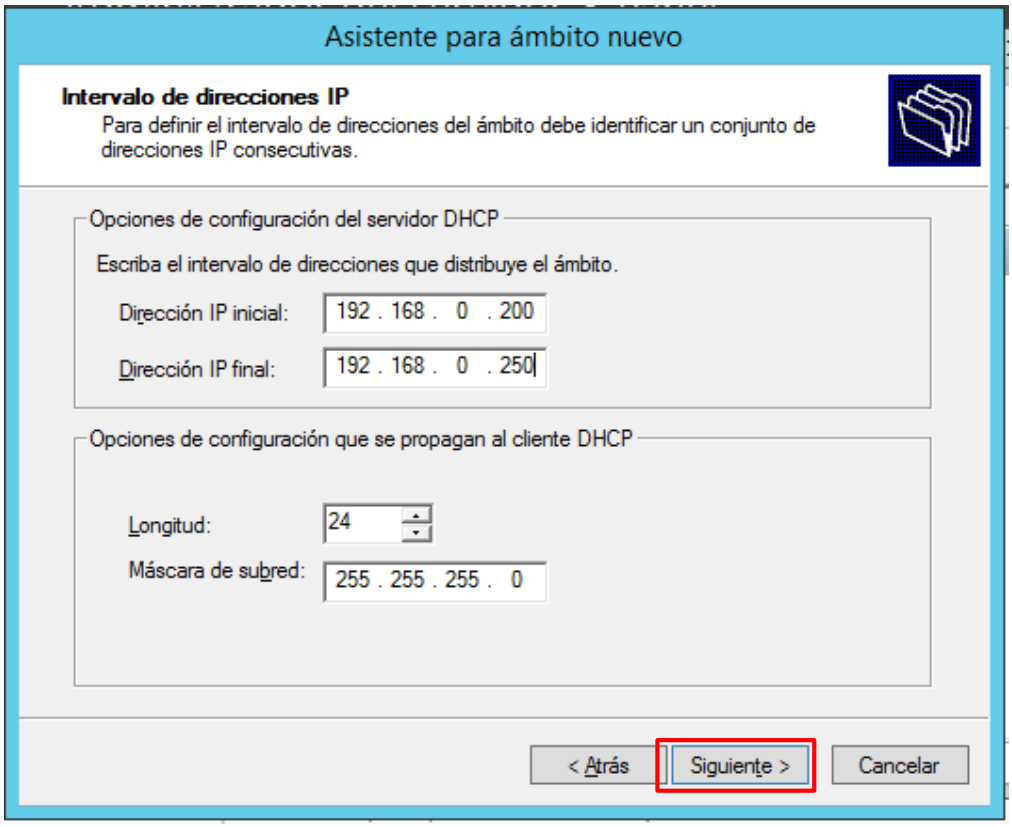
Captura 130 - Configurar DHCP 12



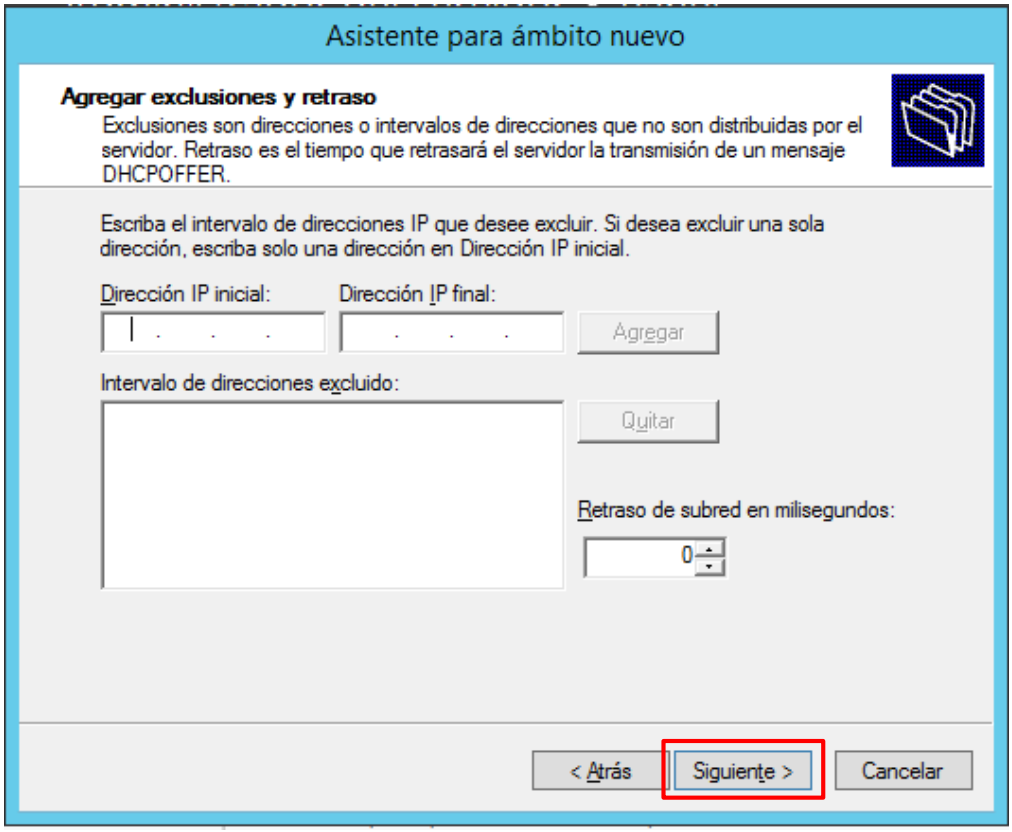
Captura 131 - Configurar un àmbit 1



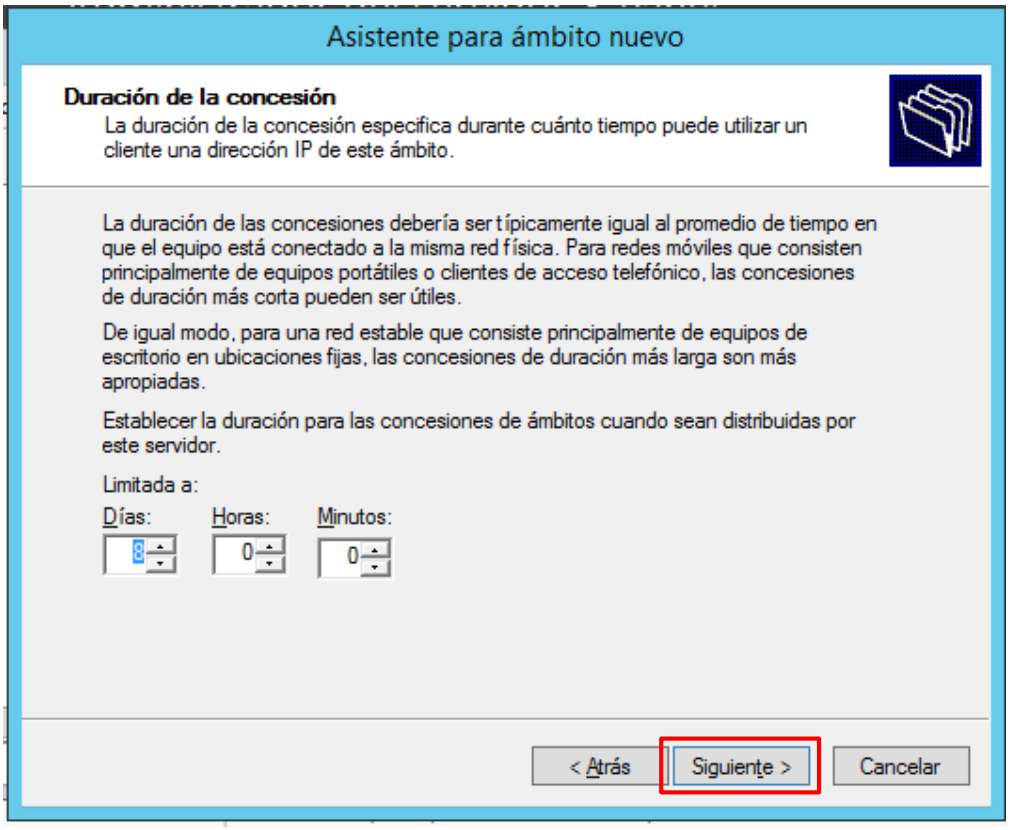
Captura 132 - Configurar un àmbit 2



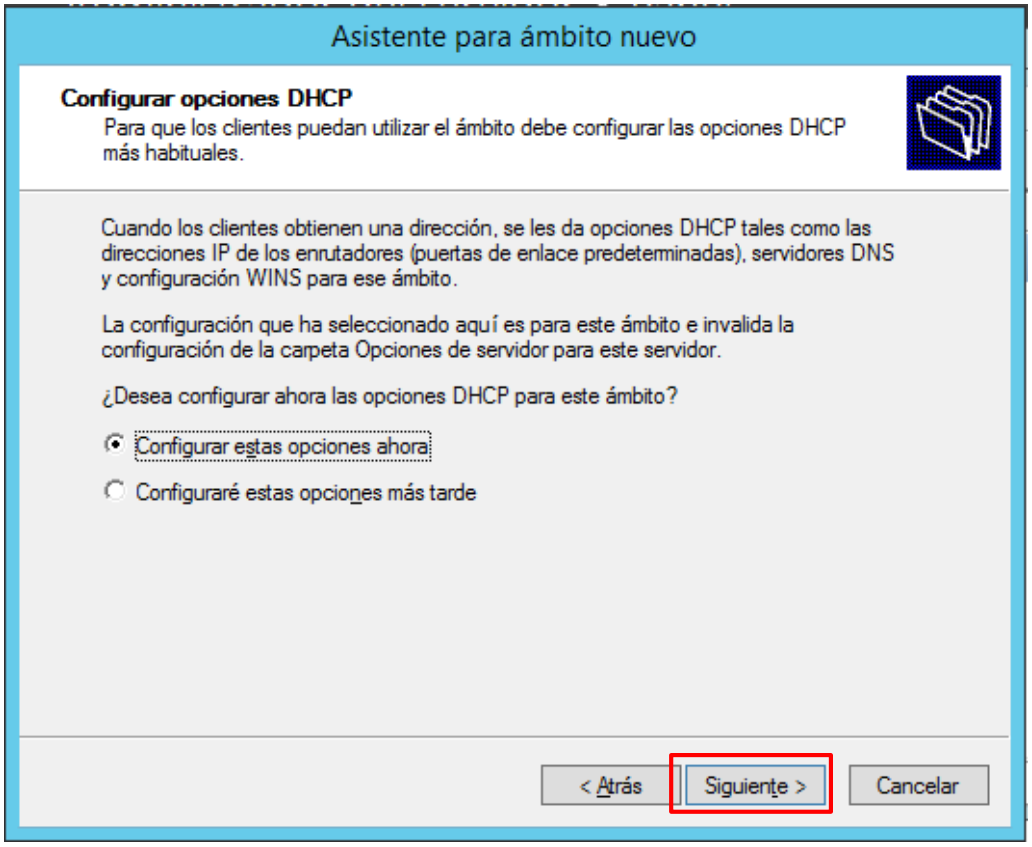
Captura 133 - Configurar un àmbit 3



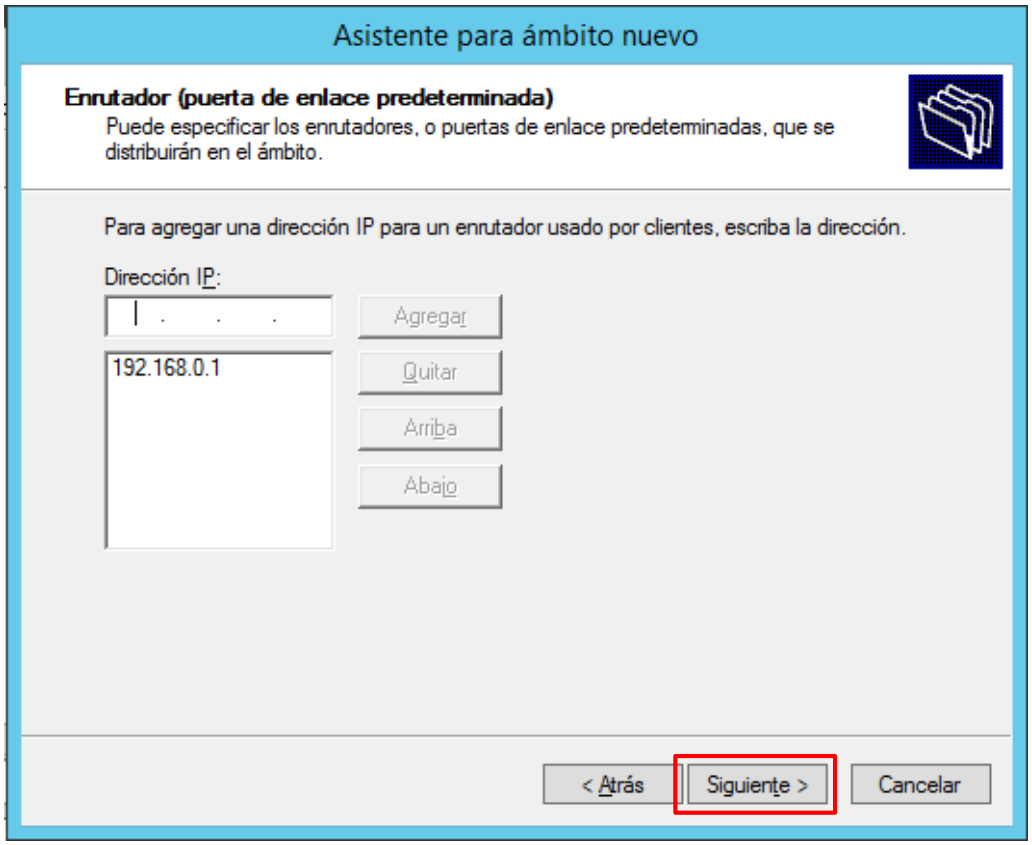
Captura 134 - Configurar un àmbit 4



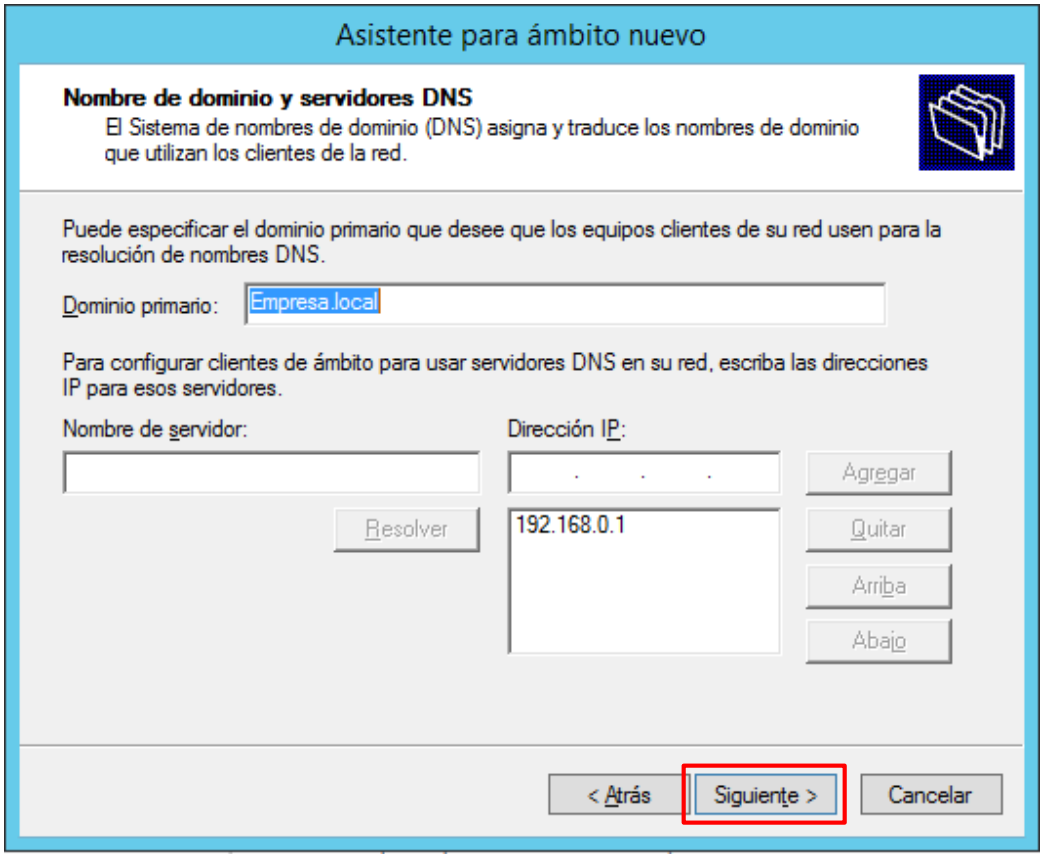
Captura 135 - Configurar un àmbit 5



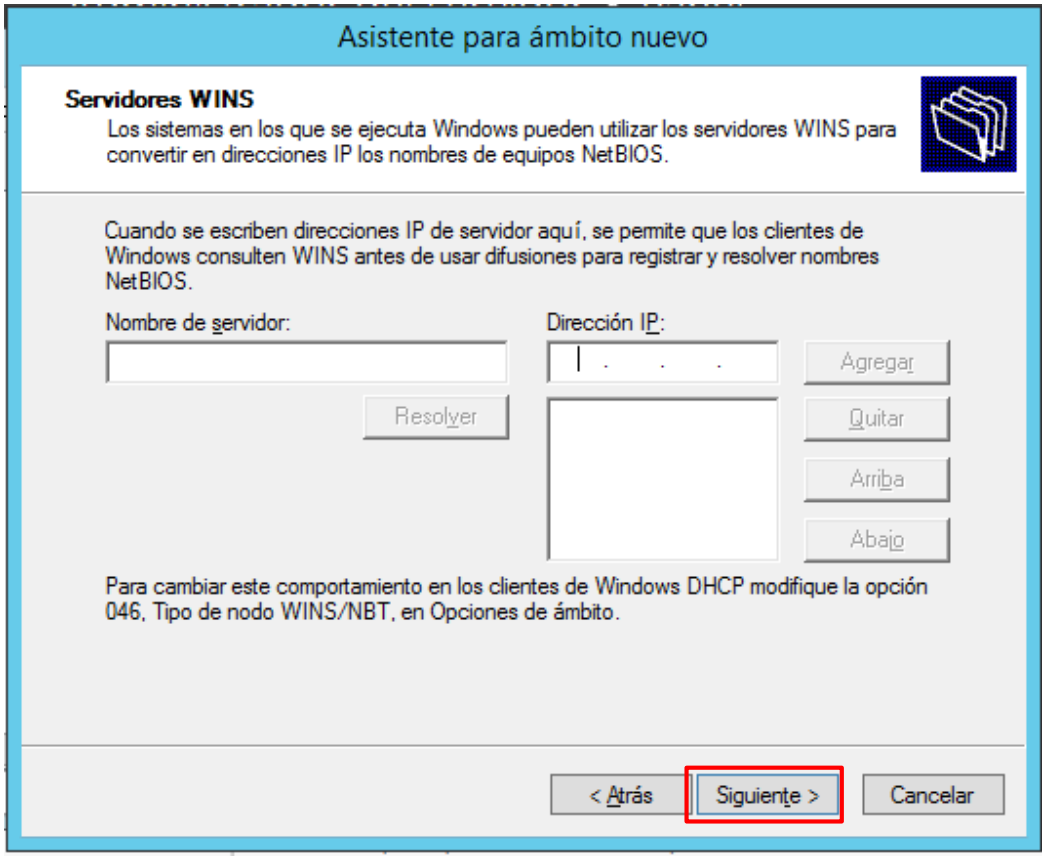
Captura 136 - Configurar un àmbit 6



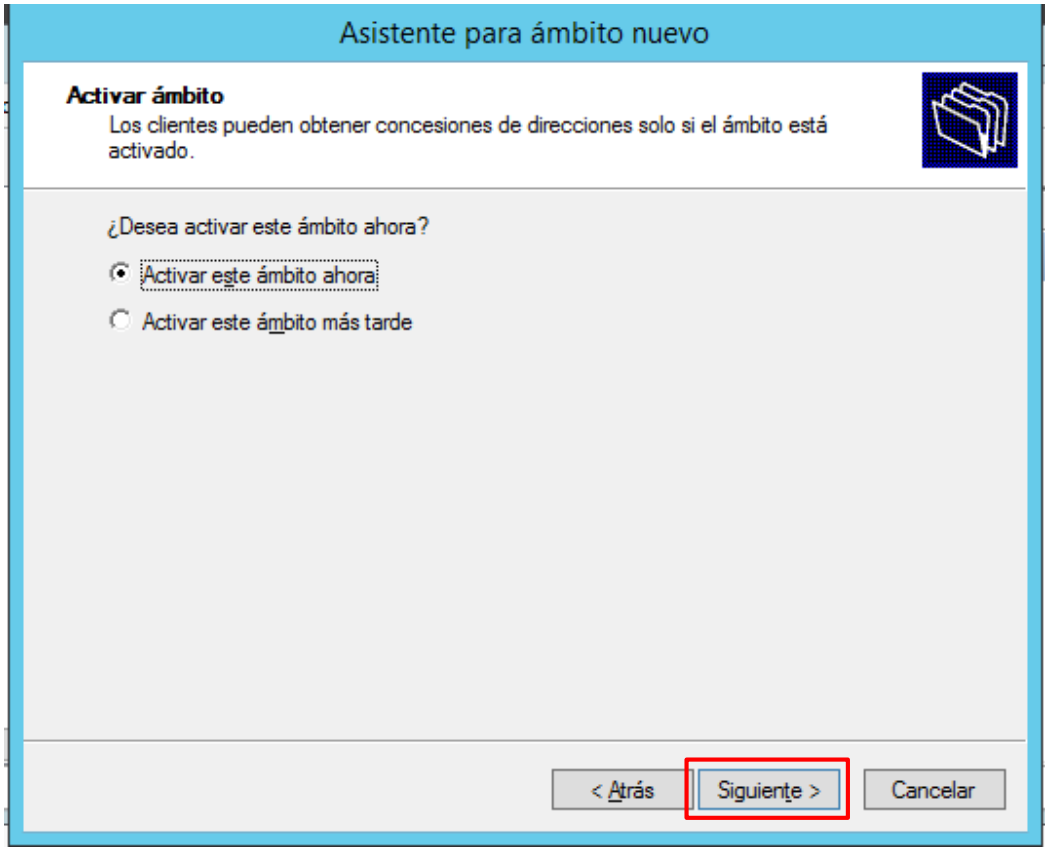
Captura 137 - Configurar un àmbit 7



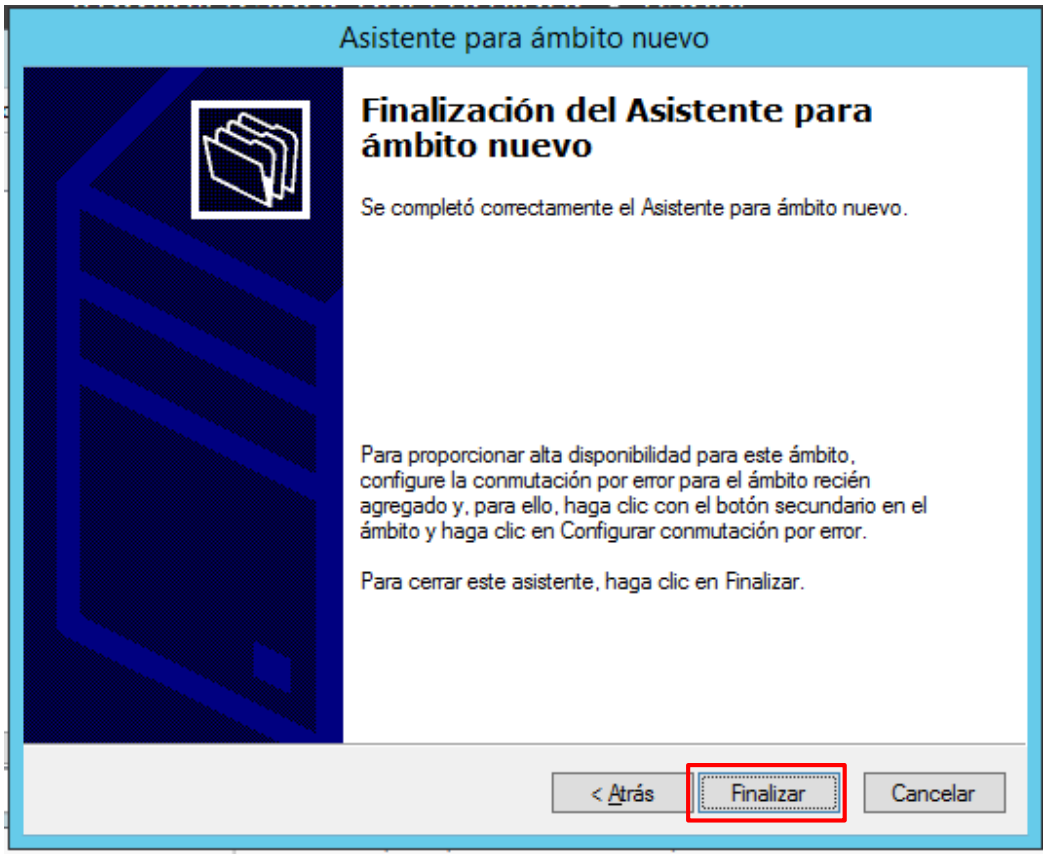
Captura 138 - Configurar un àmbit 8



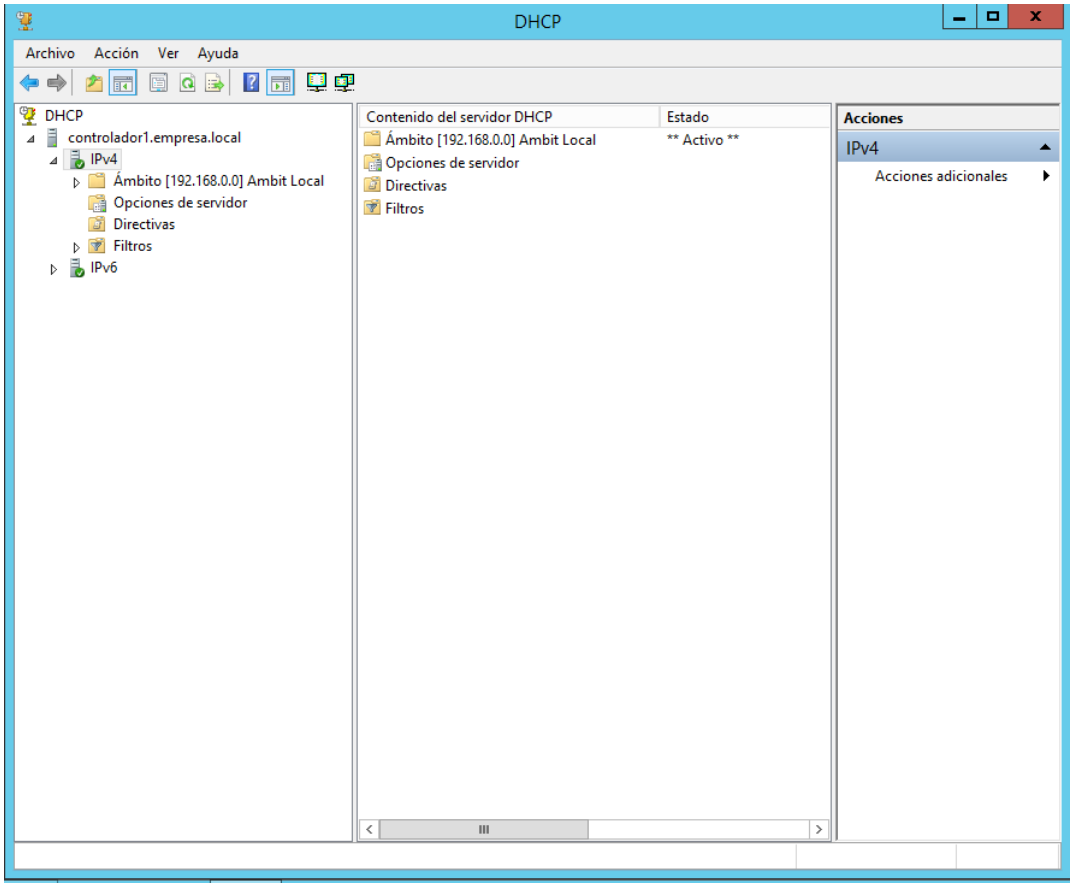
Captura 139 - Configurar un àmbit 9



Captura 140 - Configurar un àmbit 10



Captura 141 - Configurar un àmbit 11



Captura 142 - Configurar un àmbit 12