

# Sistemes Operatius en xarxa

## UD12. Part 1. Introducció als SO en xarxa



# Índex

1.	Sistema Operatiu en Xarxa .....	2
1.1.	Característiques .....	2
2.	Arquitectura client/servidor .....	2
2.1.	Elements de l'arquitectura client/servidor .....	3
2.2.	El funcionament bàsic .....	4
3.	Tipus d'arquitectures client/servidor .....	4
3.1.	Classificació segons la grandària del costat client i del costat servidor .....	4
3.2.	Classificació segons la mena de servei que s'ofereix .....	5
4.	Avantatges i inconvenients de l'arquitectura client/servidor .....	5
4.1.	Avantatges de l'arquitectura client/servidor .....	5
4.2.	Inconvenients de l'arquitectura client/servidor .....	5
5.	Sistemes operatius més freqüents en una infraestructura client/servidor .....	6
6.	Requisits dels sistemes operatius més comuns en el costat servidor .....	7
6.1.	Requisits mínims per a Windows Server 2019 / 2016 .....	7
6.2.	Requisits mínims per a Windows Server 2012 / 2012 R2 .....	7
6.3.	Requisits mínims per a Ubuntu Server 18.04 LTS / Ubuntu Server 16.04 LTS .....	7
7.	Annexos .....	8
7.1.	Requisits mínims per a Windows 2008 Server .....	8
7.2.	Requisits mínims per a Ubuntu Server 14.04 LTS .....	8
8.	Bibliografia .....	8

## 1. Sistema Operatiu en Xarxa

En temes anteriors vèiem que, depenent de la configuració dels equips, podem distingir dos **tipus de xarxes**:

- **Grups de treball:** els equips són **tots iguals** (tots comparteixen els seus recursos d'igual a igual) i no es disposa de cap equip servidor dedicat exclusivament a això. En aquesta mena de xarxes, per tant, no existeix una gestió centralitzada de recursos. Exemples de SO instal·lats en equips que formen grups de treball són els Sistemes Operatius Monolloc, com: Windows 7/8/10/11...
- **Xarxes client/servidor:** existeix dos tipus d'equips: clients i servidors. Els equips **clients** són emprats pels usuaris d'una xarxa per a sol·licitar informació (dades) i serveis (impressió de documents, transferència de fitxers, correu electrònic,...) al equip **servidor** (o als equips servidors si hi ha més d'un). Els equips clients tenen instal·lats Sistemes Operatius Monolloc i l'equip servidor disposa d'un Sistema Operatiu en Xarxa.

Per tant, un **sistema operatiu en xarxa** (servidor) és aquell que permet la creació d'una xarxa **client/servidor**, es dir, és aquell que manté dos o més equips units a través d'algún mitjà de comunicació amb l'objectiu de compartir a altres equips (clients) els diferents recursos i la informació del sistema, els quals són gestionats de forma centralitzada des d'aquest SO. Exemples de SO en xarxa són Windows Server i Linux Server.

### 1.1. Característiques

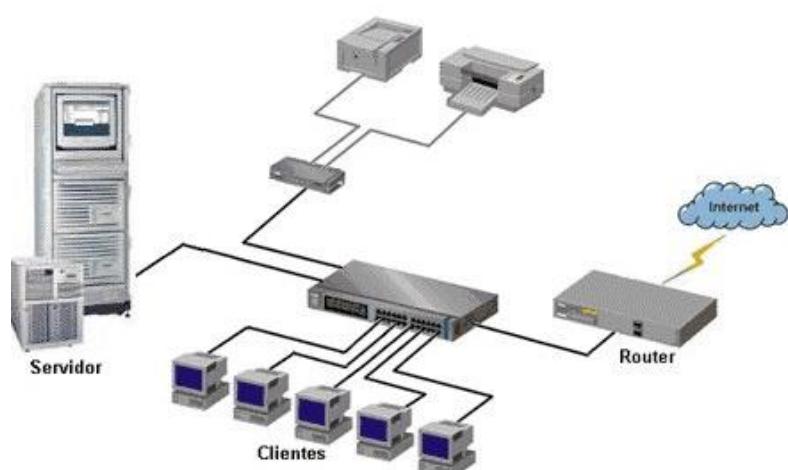
Les característiques genèriques d'un sistema operatiu en xarxa són:

- Connecta tots els equips i recursos de la xarxa.
- Gestió d'usuaris centralitzada.
- Proporciona seguretat, controlant l'accés a les dades i recursos. Ha de validar els accessos (claus, certificats, sistemes biomètrics, etc.) i aplicar les polítiques de seguretat.
- Coordina les funcions de tots els perifèrics i recursos.
- Comparteix recursos (duu a terme la coordinació i els privilegis a l'hora de compartir). Per tant, millora notablement la utilització dels recursos.
- Permet monitorar i gestionar la xarxa i els seus components (equips i recursos) de forma centralitzada.

## 2. Arquitectura client/servidor

L'arquitectura client/servidor persegueix l'objectiu de **processar la informació d'una manera distribuïda**. D'aquesta manera, els usuaris finals poden estar dispersos en una àrea geogràfica més o menys extensa (un edifici, una localitat, un país, ...) i accedir a un conjunt comú de recursos compartits.

A més, l'accés ha de ser **transparent** (el client pot desconèixer la ubicació física del recurs que pretén utilitzar) i, preferiblement, **multiplataforma**, és a dir, independent del sistema operatiu, del programari d'aplicació i fins i tot del maquinari.



En definitiva, quan parlem de la implantació d'una arquitectura client/servidor, ens referim a un **sistema d'informació distribuït**.

A més de la **transparència** i la **independència** del maquinari i del programari, una implantació client/servidor ha de tindre les següents característiques:

- Ha d'utilitzar **protocols asimètrics**, on el servidor es limita a escoltar, en espera que un client inicie una sol·licitud.
- El servidor oferirà **recursos**, tant lògics com físics a una quantitat variable i diversa de clients (per exemple, espai d'emmagatzematge, bases de dades, impressores, etc.)
- El servidor oferirà també una sèrie de **serveis**, que seran usats pels clients. Aquests serveis estaran encapsulats, per a ocultar als clients els detalls de la seua implementació (per exemple, acceptar el requeriment d'un client sobre una base de dades o formatar les dades obtingudes abans de transmetre'ls al client).
- Es facilitarà la **integritat** i el manteniment tant de les dades com dels programes pel fet que es troben centralitzats en el servidor o servidors.
- Els sistemes estaran **feblement acoblats**, ja que interactuen mitjançant l'enviament de missatges.
- Es facilitarà la **escalabilitat**, de manera que siga fàcil afegir nous clients a la infraestructura (escalabilitat horitzontal) o augmentar la potència del servidor o servidors, augmentant el seu número o la seua capacitat de càlcul (escalabilitat vertical)

#### Recorda:

Les característiques d'una implantació client/servidor han de ser:

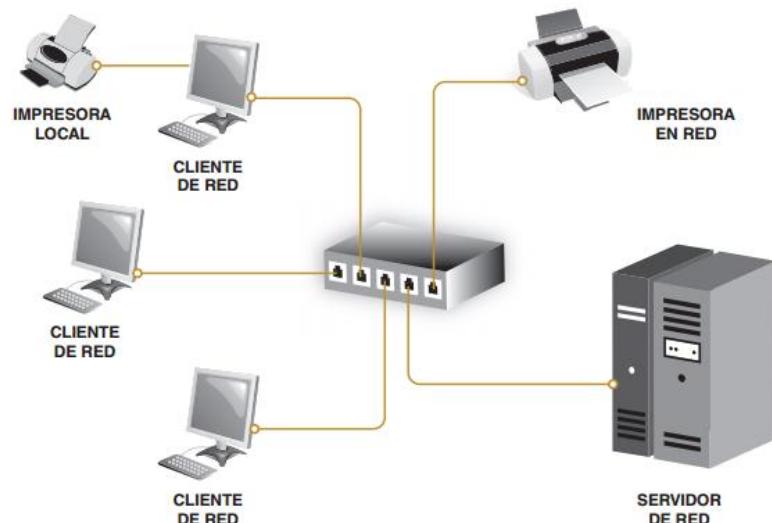
- Transparència.
- Independència.
- Protocols asimètrics.
- Recursos compartits.
- Servei.
- Encapsulament.
- Integritat.
- Acoblament dèbil.
- Escalabilitat.

## 2.1. Elements de l'arquitectura client/servidor.

Del que s'ha dit fins ara, podem deduir que els principals elements que conformen l'arquitectura client/servidor són els següents:

Components dels sistemes operatius de xarxa habituals són:

- **Servidors:** Són equips amb **sistemes operatius en xarxa** que proporcionen recursos als clients, fent-los accessibles als equips de la xarxa, siga a altres servidors o, habitualment, a clients.
- **Clients:** Són equips amb un **sistema operatiu monolloc** connectats per a començar a treballar en xarxa. A diferència dels servidors, no comparteixen els seus recursos.

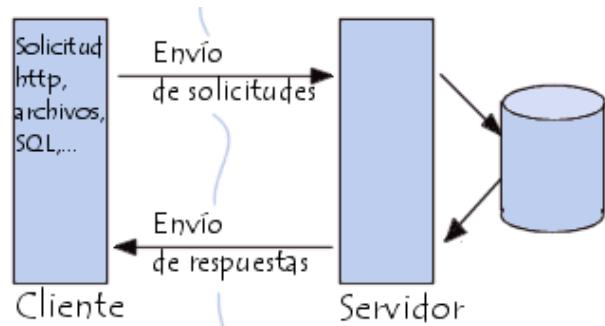


Dependent del sistema operatiu, es pot donar el cas que en una determinada xarxa un equip siga servidor d'uns certs recursos i client d'uns altres.

## 2.2. El funcionament bàsic

Encara que és probable que a hores d'ara ja et faces una idea sobre el funcionament general del model client/servidor, el concretarem a continuació:

1. El primer que ha d'ocórrer és que s'inicie el servidor. Això ocorrerà durant l'arranada del sistema operatiu o amb la intervenció posterior de l'administrador del sistema. Quan acabe d'iniciar-se, esperarà de manera passiva les sol·licituds dels clients.
2. En algun moment, un dels clients connectats al sistema realitzarà una sol·licitud al servidor.
3. El servidor rep la sol·licitud del client, realitza qualsevol verificació necessària i, si tot és correcte, la processa.
4. Quan el servidor dispose del resultat sol·licitat, l'envia al client.
5. Finalment, el client rep el resultat que va sol·licitar. A continuació realitza les comprovacions oportunes (si són necessàries) i, si era aqueix l'objectiu final, li ho mostra a l'usuari.



## 3. Tipus d'arquitectures client/servidor

### 3.1. Classificació segons la grandària del costat client i del costat servidor

Una de les característiques del model client/servidor és que permet balancejar la potència de càlcul aplicada cap al costat servidor o cap al costat client, segons convinga.

Per exemple, si el nombre de clients anara elevat, i la majoria del procés es realitzara en el costat servidor, no necessitaríem clients molt potents, però probablement necessitaríem ampliar la potència de càlcul del costat servidor i, com a situació complementària, hauríem de valorar l'augment de trànsit en la xarxa.

D'altra banda, amb clients més potents, bona part del càlcul pot realitzar-se en el costat client, accedint al servidor de manera esporàdica. Això derivaria en un servidor amb menys necessitats de recursos, un menor trànsit en la xarxa i un major cost dels equips en el costat client.

Per tant, com pot deduir-se, disposem de dues alternatives:

- **Client pesat, servidor lleuger** (en anglès, Thick Client, Thin Server): Ací, tant el nivell de presentació com el nivell d'aplicació s'executen en el costat client. Fins i tot podrien processar-se continguts multimèdia amb un alt consum de recursos. El servidor s'utilitza per a tasques com l'hostalatge del SGBD (Sistema Gestor de Bases de dades) o fins i tot per a altres tasques menors, com administrar les tasques d'impressió. En aquesta mena d'esquemes, fins i tot podria interrompre's de manera momentània el servei de xarxa sense perjudicar de manera significativa als clients.
- **Servidor pesat, client lleuger** (en anglès, Thick Server, Thin Client): El costat client s'empra només per al nivell de presentació (moltes vegades utilitzant simplement un navegador web) i el costat servidor s'encarrega d'executar l'aplicació. En aquesta mena d'esquemes podríem disposar, fins i tot, de clients sense disc dur. Una altra dels avantatges d'aquesta opció és que ofereixen una major seguretat enfront d'intents d'accés indegut.



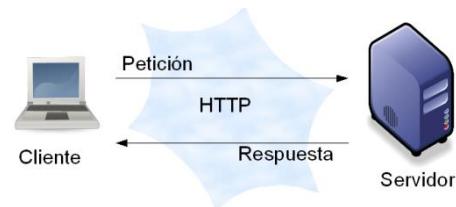
### 3.2. Classificació segons la mena de servei que s'ofereix

Òbviament, són molts els serveis que es poden oferir en una arquitectura client/servidor: encaminament, DHCP, DNS, servei de directori, servei d'accés remot, d'impressió... els quals anirem coneixent al llarg de aquest tema. No obstant això, a continuació, es mostren alguns exemples de tipus de servidor atenent als serveis que poden oferir:

- **Servidors d'arxius:** Se solen utilitzar per a crear magatzems de documents en un lloc centralitzat de la xarxa (Còpies de seguretat, imatges, plantilles de documents, etc.)
- **Servidors de bases de dades:** Normalment estan associats a la utilització d'aplicacions client/servidor on un procés client requerís dades al servidor de bases de dades. Lògicament, l'accés a les dades serà compartit per diferents clients de manera simultània (aplicant-se els mecanismes de protecció necessaris sobre les dades davant la concurrència de diferents clients i l'existència de diferents nivells de privilegi). Aquest tipus d'estructures solen basar-se en el concepte de **transacció**.
- **Servidors d'impressió (Print Server):** Faciliten la compartició d'impressores i administra els treballs d'impressió en la xarxa. D'aquesta manera es permet als clients que utilitzen una impressora sense importar la seua ubicació física. Un servidor d'impressió utilitza una cua per a emmagatzemar, de forma ordenada, els treballs que rep. Aquesta cua pot ser administrada amb diferents privilegis en funció del client que realitze la sol·licitud. És comú que un servidor d'impressió englobe també a un servidor de fax, ja que es gestionen de manera similar.
- **Servidors web:** La seua funció consisteix a retornar un determinat document quan un client el sol·licita. La comunicació utilitza el protocol HTTP (que està basat en RPC).

#### Nota:

En una transacció, una sèrie d'operacions que estan relacionades entre si s'efectuen com un tot (per exemple, l'actualització de les dades de diferents taules en la base de dades). Si una part de l'operació fracassa, fracassa la transacció completa. Això assegura la integritat de les dades emmagatzemades.



## 4. Avantatges i inconvenients de l'arquitectura client/servidor

### 4.1. Avantatges de l'arquitectura client/servidor

El model client/servidor està especialment indicat en xarxes mitjanes o grans que necessiten un alt nivell de fiabilitat. Els principals avantatges que ofereix són:

- **Administració centrada en el servidor.** Els clients tenen poca transcendència en l'esquema i les seues necessitats d'administració són menors.
- **Centralització dels recursos.** Els recursos comuns a tots els usuaris s'administren en el servidor. Així s'eviten situacions com la redundància o inconsistència d'informació en les bases de dades.
- **Millora de la seguretat.** En disposar d'un mecanisme central d'autenticació, les possibilitats d'accés indegit es redueixen considerablement.
- **Escalabilitat de la instal·lació.** Es poden afegir o suprimir clients sense que el funcionament de la xarxa es veja afectat.

### 4.2. Inconvenients de l'arquitectura client/servidor

Una infraestructura client/servidor també té els seus inconvenients:

- **Cost elevat.** Tant la instal·lació com el manteniment són més elevats a causa del perfil molt tècnic del costat servidor.
- **Dependència del servidor.** Tota la xarxa està construïda al voltant del servidor i si aquest deixa de funcionar o ho fa amb un rendiment inadequat, afectarà a tota la infraestructura. Afortunadament, aquest inconvenient està superat, almenys en part, gràcies a sistemes com els servidors redundants, la tolerància a fallades i els sistemes d'emmagatzematge en RAID.

## 5. Sistemes operatius més freqüents en una infraestructura client/servidor

En el costat **servidor**, els sistemes més habituals són:

- Microsoft Windows Server
- GNU/Linux Server (són freqüents les distribucions (RedHat, Ubuntu Server, CentOS, SuSE Linux Enterprise Server, ...))
- UNIX (IBM AIX, HP-UX)
- Solaris/OpenSolaris
- Apple US X Server



D'altra banda, tots els sistemes anteriors poden actuar, si fora necessari, com a clients en una infraestructura client/servidor, encara que no estiguin específicament dissenyats per a això. Fins i tot poden actuar com a servidors per a un grup de clients i, per a dur a terme la seu comesa, actuar al mateix temps com a clients d'un altre, o altres servidors.

No obstant això, els sistemes que solem cridar "d'escriptori" són els que estan dissenyats per a constituir la part de **client** en aquesta mena d'entorns. Els més freqüents són aquests:

- Microsoft Windows (7, 8, 10, 11, ...)
- GNU/Linux Desktop (Ubuntu Desktop, Fedora, Debian, SuSE Linux)
- Apple US X



## 6. Requisits dels sistemes operatius més comuns en el costat servidor

Com hem vist abans, existeix una gran diversitat de sistemes operatius en xarxa del costat servidor (i això que només nomenàvem els més representatius). Per aquest motiu, seria molt extens incloure ací els requisits de cadascun d'ells. A més, dependrà de la versió concreta que anem a instal·lar (per exemple, en Windows 2019 trobem les edicions Datacenter, Standard i Essential, i en cadascuna d'elles poden variar lleugerament els requisits).

Per tot això, ací ens limitarem a incloure tres exemples i t'animes que investigues una mica per a obtindre la informació referent al sistema i a la versió concreta que pretengues instal·lar a cada moment.

Els exemples triats són Windows Server 2019, 2012 R2 i Ubuntu Server 18.04. No obstant això, hem d'esmentar que la configuració més estàndard de Windows Server inclou interfície gràfica (encara que existeix la versió Core, que només conté els serveis necessaris per a la funció que realitza i no té interfície gràfica).

Pel seu costat, la configuració predeterminada d'Ubuntu Server no inclou ni interfície gràfica ni serveis que no siguin imprescindibles.

### Recorda:

L'objectiu d'eliminar la interfície gràfica i els serveis que no siguin imprescindibles en un sistema operatiu del costat servidor és augmentar el seu rendiment, reduir les seues tasques de manteniment i reduir la superfície d'exposició als atacs a la seguretat. Lògicament, l'inconvenient és la seua major incomoditat per als administradors menys experts.

### 6.1. Requisits mínims per a Windows Server 2019 / 2016

Requisits mínims	
<b>Processador</b>	1,4 GHz (64 bits)
<b>Memòria RAM</b>	512 MB (2 GB per a l'opció d'instal·lació Servidor amb Experiència d'escriptori) Tipus ECC

Més info en: <https://docs.microsoft.com/es-es/windows-server/get-started-19/sys-reqs-19>

### 6.2. Requisits mínims per a Windows Server 2012 /2012 R2

Requisits mínims	
<b>Processador</b>	1,4 GHz (64 bits)
<b>Memòria RAM</b>	512 MB

Més info en: <https://docs.microsoft.com/es-es/windows-server/get-started/system-requirements>

### 6.3. Requisits mínims per a Ubuntu Server 18.04 LTS / Ubuntu Server 16.04 LTS

	Requisits mínims Instal·lació "Standard"	Requisits mínims Instal·lació "Minimal"
<b>Processador</b>	1 GHz	300 Mhz
<b>Memòria RAM</b>	512 MB	192 MB

Més info en: <https://help.ubuntu.com/lts/serverguide/preparing-to-install.html>

## 7. Annexos

### 7.1. Requisits mínims per a Windows 2008 Server

Requisits mínims	
<b>Processador</b>	1 Ghz en x86 1.4 Ghz en x86-64
<b>Memòria RAM</b>	512 MB (a costa d'un rendiment reduït i la pèrdua d'algunes característiques)

### 7.2. Requisits mínims per a Ubuntu Server 14.04 LTS

	Requisits mínims Instal·lació "Standard"	Requisits mínims Instal·lació "Minimal"
<b>Processador</b>	1 GHz	300 Mhz
<b>Memòria RAM</b>	512 MB	192 MB

## 8. Bibliografia

- Somebooks.es (2014). Sistemes Operatius en Xarxa. Disponible en <http://somebooks.es/?p=4787>
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows Server 2012.
- Wikipedia. Sistema Operatiu de xarxa. Disponible en [http://es.wikipedia.org/wiki/sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/sistema_operativo_de_red)
- Elaboració pròpria

# Sistemes Informàtics

## UD12. Part 2. Instal·lació de Windows Server



# Índex

1.	Objectius.....	2
2.	Requisits dels sistemes Windows Server.....	2
2.1.	Requisits mínims i recomanats per a Windows Server 2019.....	2
2.2.	Requisits mínims i recomanats per a Windows Server 2012 R2 .....	2
2.3.	Requisits mínims i recomanats per a Windows 2008 Server.....	2
3.	Instal·lació dels Sistemes Operatius Windows en VirtualBox .....	3
3.1.	Windows Server 2019 .....	3
3.2.	Windows Server 2012.....	12
3.3.	Windows Server 2008 .....	21
4.	Bibliografia .....	26

## 1. Objectius

- Instal·lar el sistema operatiu client Windows 10.
- Instal·lar el sistema operatiu servidor Windows 2012 Server/R2 i Windows 2019 Server.
- Conéixer les diferents edicions de Windows 2012 Server i Windows 2019 Server.

## 2. Requisits dels sistemes Windows Server

### 2.1. Requisits mínims i recomanats per a Windows Server 2019

	<b>Requisits mínims</b>
<b>Processador</b>	1,4 GHz (64 bits)
<b>Memòria RAM</b>	512 MB (2 GB per a l'opció d'instal·lació Servidor amb Experiència d'escriptori) Tipus ECC
<b>Espai en disc</b>	32 GB

En <https://docs.microsoft.com/es-es/windows-server/get-started-19/sys-reqs-19> Microsoft indica que donada la diversitat d'implementacions possibles (diferents rols) no indiquen "requisits recomanats" per a aquesta versió de Windows Server.

### 2.2. Requisits mínims i recomanats per a Windows Server 2012 R2

Els requisits genèrics per a Windows Server 2012 R2 són aquests:

	<b>Requisits mínims</b>	<b>Requisits recomanats</b>
<b>Processador</b>	1,4 GHz (64 bits)	2 Ghz o més
<b>Memòria RAM</b>	512 MB	2 GB o més
<b>Espai en disc</b>	32 GB	40 GB instal·lació completa

### 2.3. Requisits mínims i recomanats per a Windows 2008 Server

Els requisits genèrics per a Windows 2008 Server són aquests:

	<b>Requisits mínims</b>	<b>Requisits recomanats</b>
<b>Processador</b>	1 Ghz en x86 1.4 Ghz en x86-64	2 Ghz o més
<b>Memòria RAM</b>	512 MB (a costa d'un rendiment reduït i la pèrdua d'algunes característiques)	2 GB o més Edició estàndard: <ul style="list-style-type: none"><li>• Màxim en x86: 6 GB</li><li>• Màxim en x86-64: 32 GB</li></ul> Edicions Enterprise i DataCenter: <ul style="list-style-type: none"><li>• Màxim en x86: 64 GB</li><li>• Màxim en x86-64: 2 TB</li></ul>
<b>Espai en disc</b>	10 GB	40 GB o més Si l'ordinador té més de 16 GB de RAM necessitarà espai complementari per a paginació i bolcat de memòria.

## 3. Instal·lació dels Sistemes Operatius Windows en VirtualBox

La nostra principal limitació en l'equip serà la memòria RAM, per la qual cosa haurem de triar acuradament els valors de memòria que configurarem en les màquines virtuals. A continuació, es mostren els valors recomanats per a cadascuna de les màquines virtuals amb les que treballarem:

Sistema Operatiu	RAM	Disc dur	Xarxa
<b>Windows Server 2019</b>	1.5-2GB	50 GB (expansió dinàmica)	2 targetes de xarxa (configurades com "NAT" i "Xarxa interna")
<b>Windows Server 2012</b>	1.5-2GB	25-30 GB (expansió dinàmica)	2 targetes de xarxa (configurades com "NAT" i "Xarxa interna")
<b>Windows Server 2008 R2</b>	1.5-2GB	25-30 GB (expansió dinàmica)	2 targetes de xarxa (configurades com "NAT" i "Xarxa interna")
<b>Windows 8/10 (32 bits)</b>	1GB	15 GB (expansió dinàmica)	1 targeta de xarxa (configurada com a "Xarxa interna")
<b>Windows 7 (32 bits)</b>	512 MB	15 GB (expansió dinàmica)	1 targeta de xarxa (configurada com a "Xarxa interna")

### 3.1. Windows Server 2019

#### 3.1.1. Edicions

Informació general sobre preus i llicències:

Edició de Windows Server 2019	Ideal per a	Model de llicència	Requisits de CALÇ
<b>Datacenter</b>	Entorns de cloud i centres de dades amb una gran virtualització	Basada en nucli	CALÇ de Windows Server
<b>Standard</b>	Entorns físics o mínimament virtualitzats	Basada en nucli	CALÇ de Windows Server
<b>Essentials</b>	Petites empreses amb un màxim de 25 usuaris i 50 dispositius	Servidors especialitzats (llicència de servidor)	No requereix CALÇ

#### Comparació de característiques de Windows Server 2019:

Llegenda de compatibilitat de característiques:

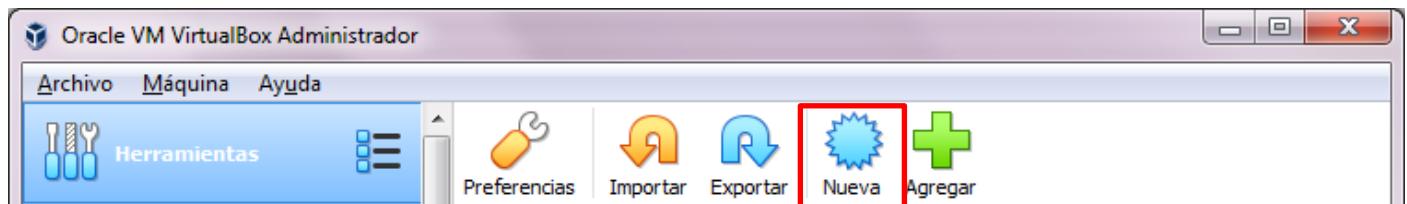
● Característica disponible ○ Característica no disponible

Característica	Edició Standard	Edició Datacenter
Funcionalitat bàsica de Windows Server	●	●
Integració híbrida	●	●
Infraestructura hiperconvergent	○	●
GOSE*/contenidors Hyper-V	2	Sense límit
Contenidors de Windows Server	Sense límit	Sense límit
Servei de protecció d'host	●	●
Rèplica d'emmagatzematge	●	●
Màquines virtuals blindades	○	●
Programari-defined networking	○	●
Emmagatzematge definit per programari	○	●

Més info en <https://www.microsoft.com/es-es/cloud-platform/windows-server-pricing>

### 3.1.2. Creació de la màquina virtual

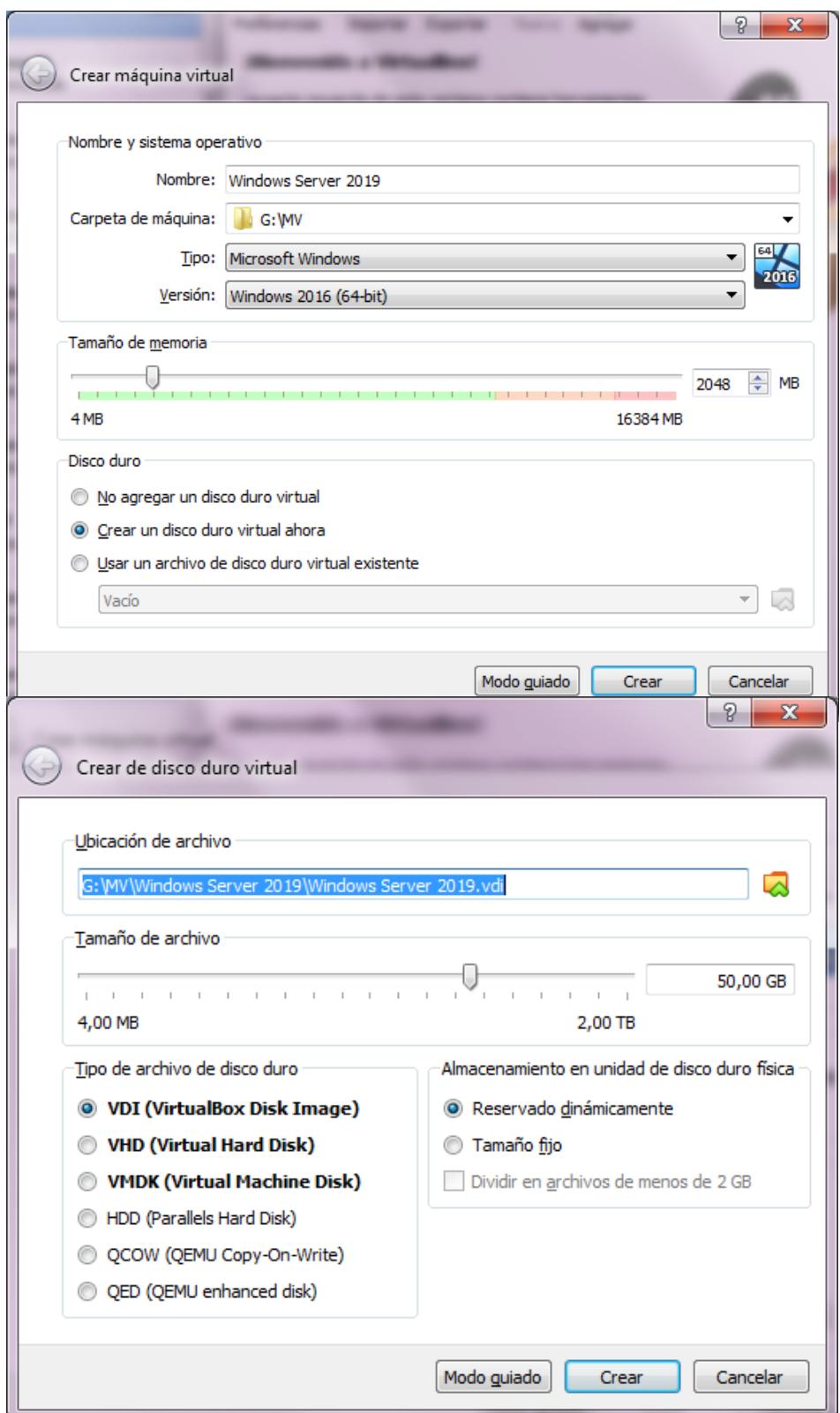
En primer lloc, obrirem VirtualBox i crearem una màquina virtual nova.



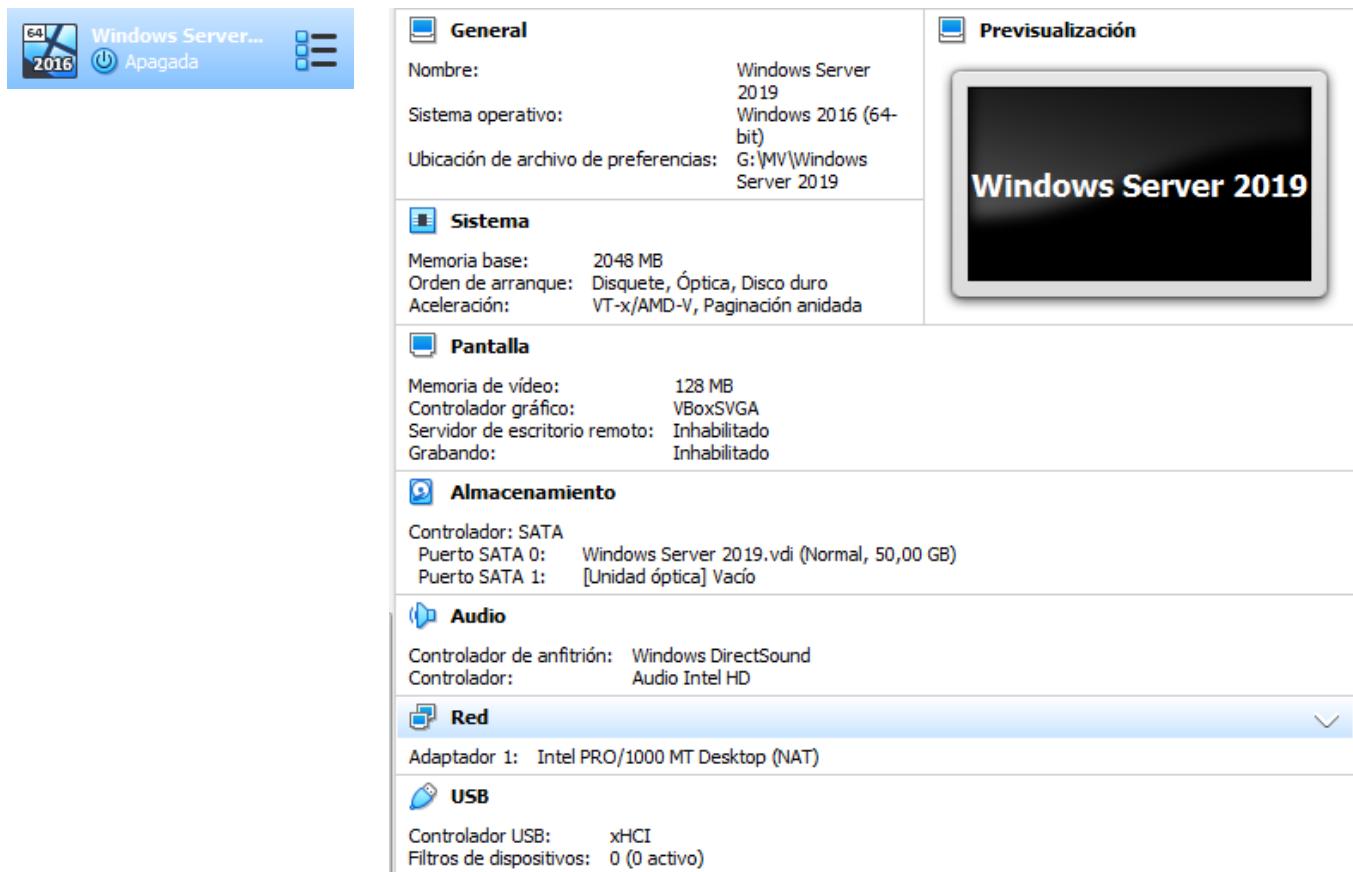
S'obrirà l'assistent per a la creació de màquines virtuals, el qual ens preguntarà per la mena de màquina virtual que volem crear. En aquest cas li indicarem que es tracta d'una màquina virtual de tipus Windows Server 2016 (64 bit).

També li indicarem la memòria RAM que li assignarem. Podria funcionar bastant bé amb 1.5GB de RAM. No obstant això, si el nostre equip de classe disposa de RAM suficient, millor assignar-li 2GB. De tota manera, com durant la instal·lació del sistema únicament tindrem funcionant simultàniament una màquina virtual, podem donar-li un valor més aviat elevat. En posteriors pràctiques ho ajustarem per a no penalitzar en excés el rendiment del sistema en tindre diverses màquines en funcionament.

També ens demana que creem un disc dur virtual per al servidor. Crearem un disc virtual nou amb una grandària d'uns 50GB, de tipus "VDI" i amb emmagatzematge "Reservat dinàmicament".



Acabat el procés obtenim un resum del sistema creat.

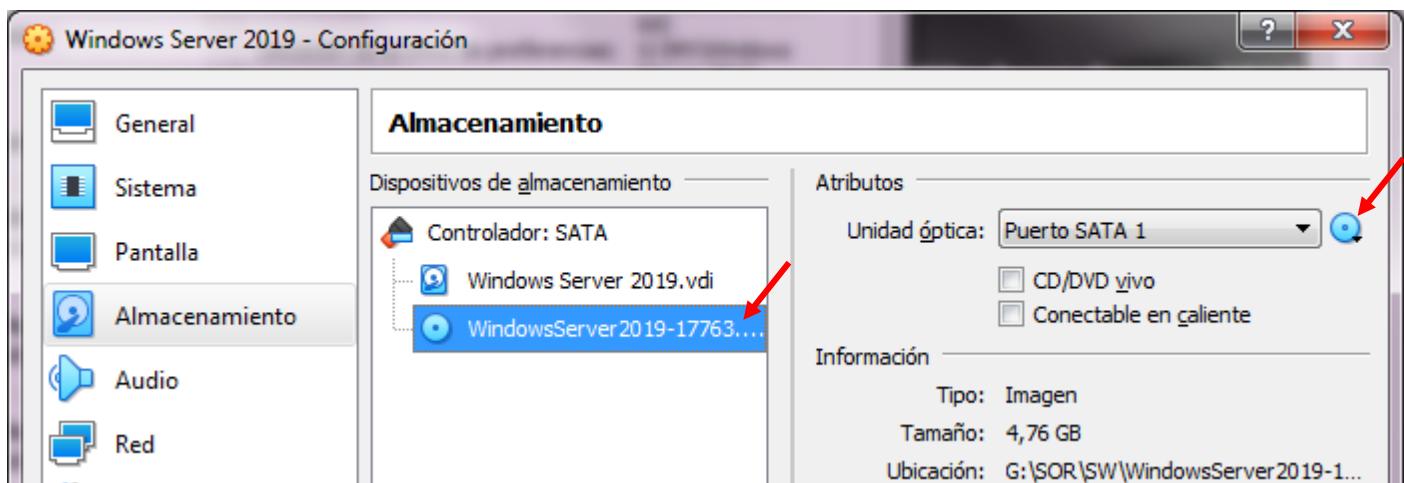


Abans de començar la instal·lació de Windows Server, hem de tindre preparada l'ISO. Podem descarregar una versió d'avaluació de 180 dies de:

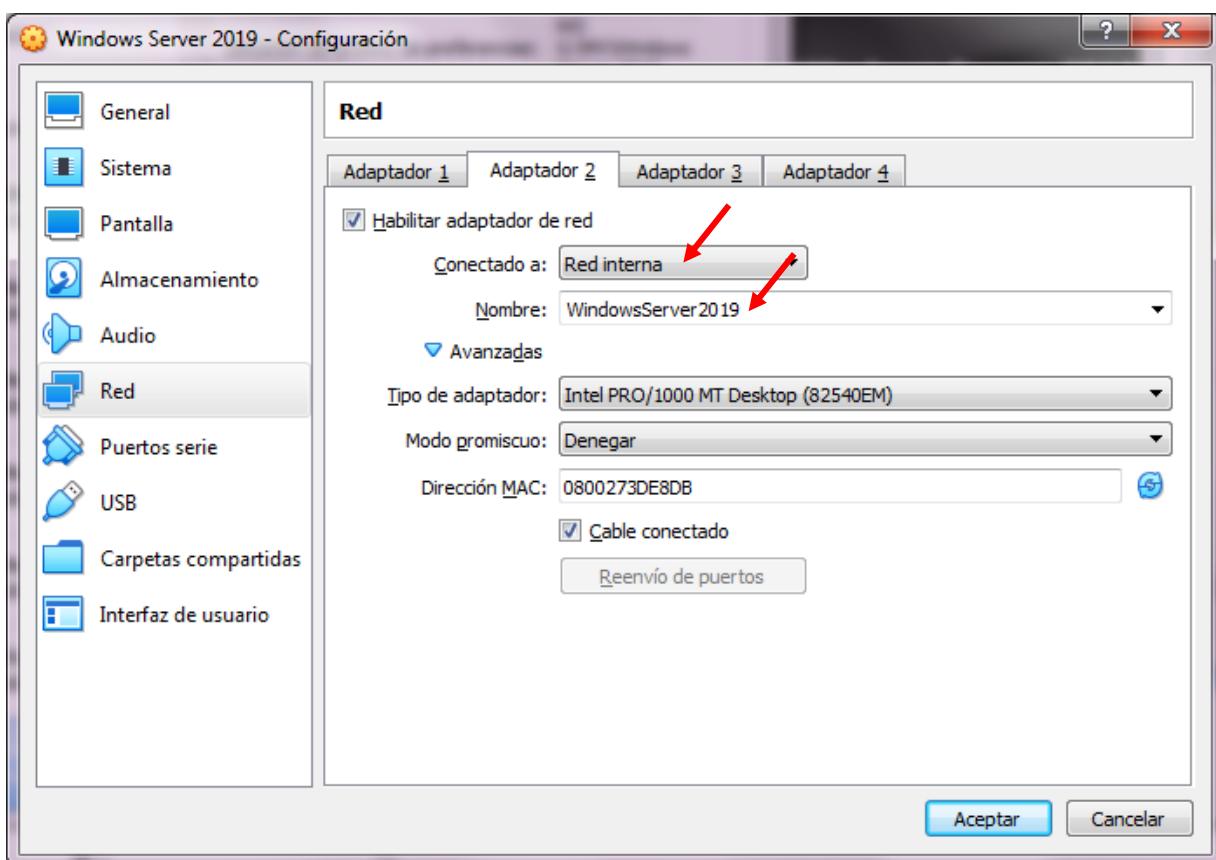
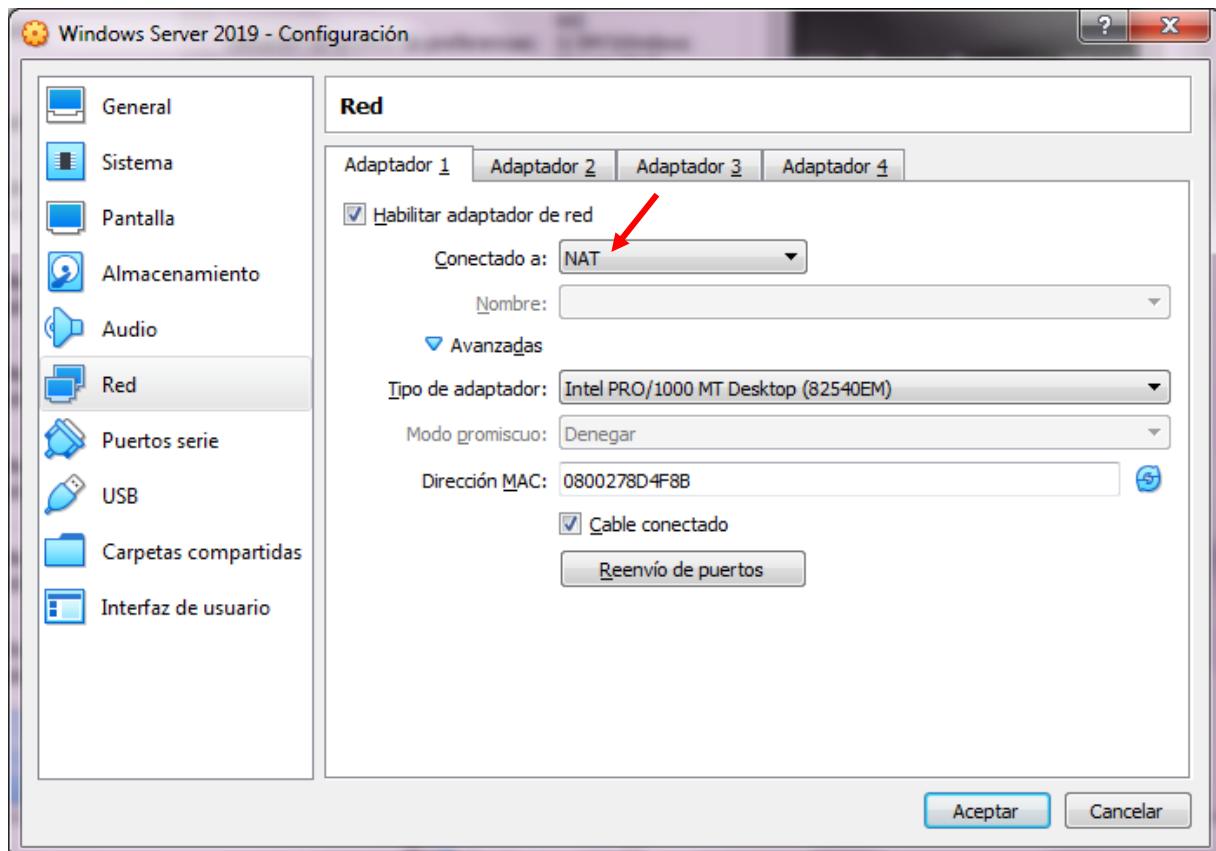
<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019?filetype=iso>

A continuació, haurem d'indicar-li a la màquina virtual on es troba la imatge ISO amb la qual volem que arranque i associar-la a un CD/DVD virtual.

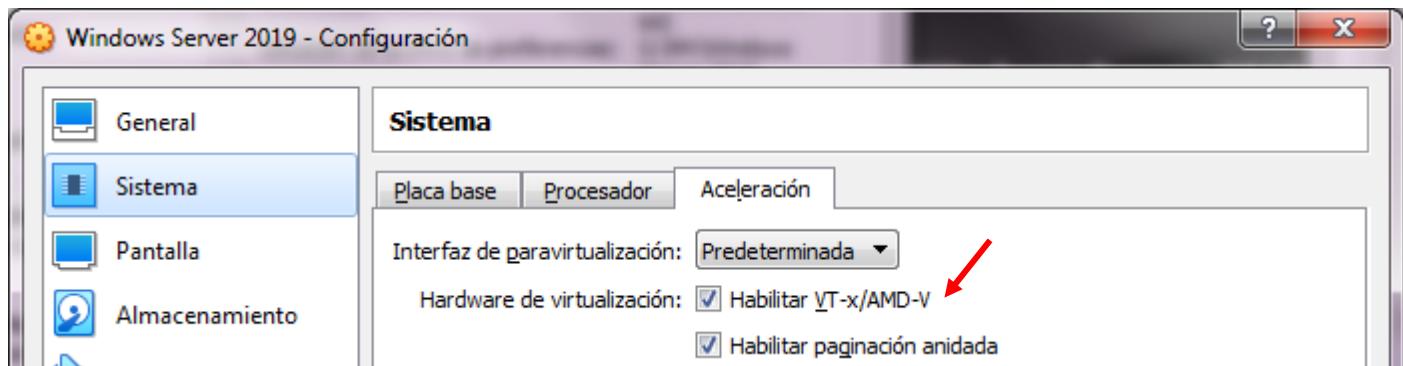
Per a això anem a "Configuració" → Emmagatzematge



En el desenvolupament de les pràctiques, es demanarà que es configuren en el cas de Windows 2019 dos adaptadors: un d'ells configurat com NAT i l'altre com a xarxa interna (en el cas dels clients Windows 7/8/10 es configurarà el seu adaptador de xarxa com a xarxa interna).



És molt important revisar que estan habilitades les optimitzacions de virtualització Intel VT-x/AMD-V en l'apartat "Sistema → Acceleració" de la màquina virtual perquè el rendiment del sistema siga acceptable.

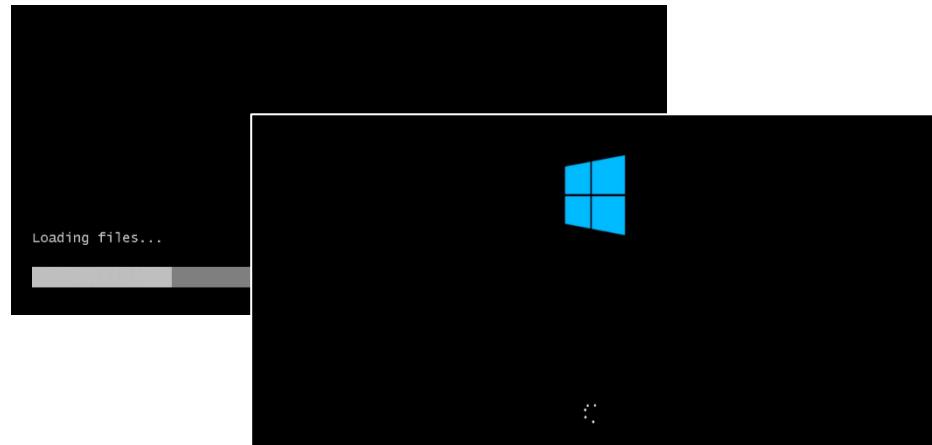


Després d'aquest procés, ja podem arrancar la màquina virtual.

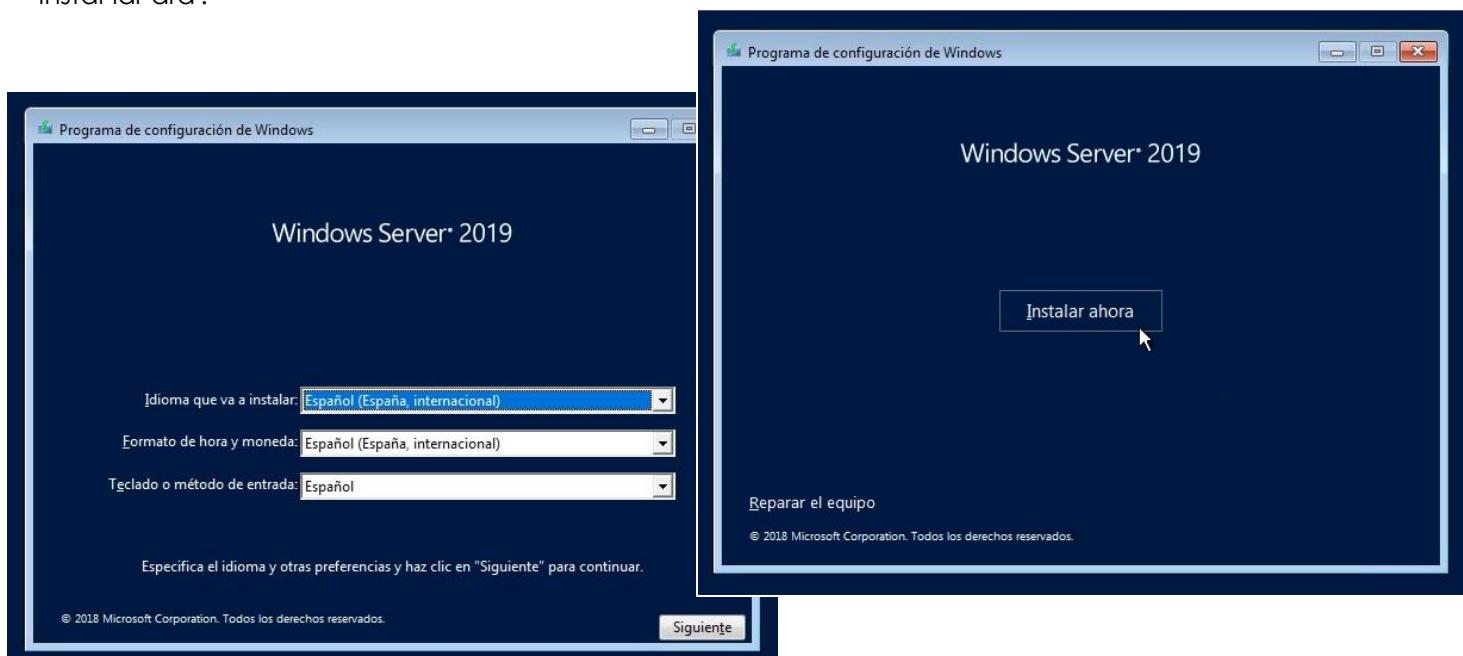


### 3.1.3. Instal·ació

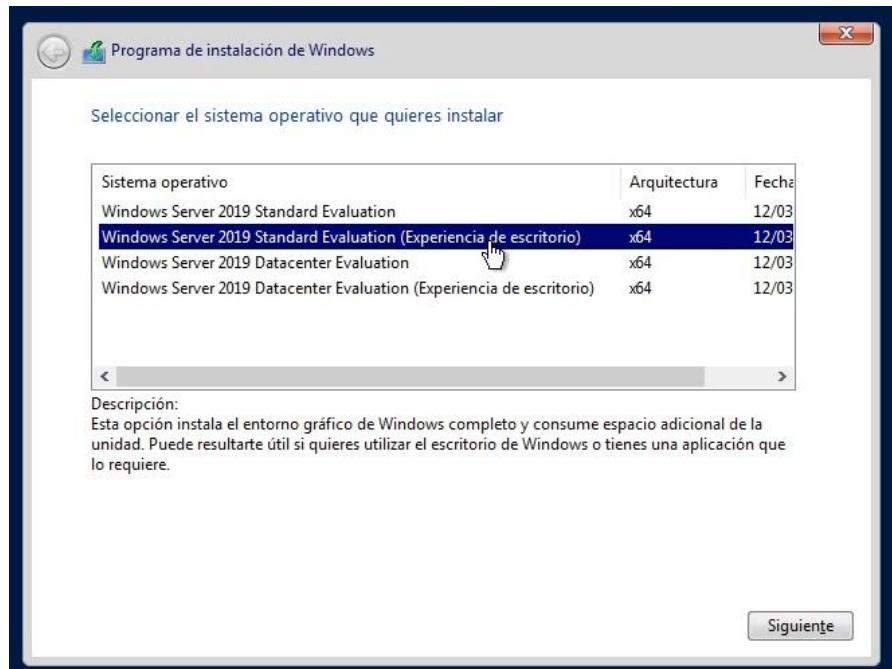
Després d'arrancar la màquina virtual, apareixerà la clàssica pantalla d'inici de la instal·ació.



Després de seleccionar l'idioma en el qual volem realitzar la instal·ació, premem 'Siguiente', i a continuació 'Instalar ara'.



Després d'uns instants en els quals se'n indicarà que està començant el procés d'instal·lació, ens apareixerà una finestra en la qual podrem seleccionar el tipus d'instal·lació a realitzar. Ara indicarem que volem instal·lar la versió 'Windows Server 2019 Standard Evaluation (Experiència d'escriptori)'.



A continuació , acceptarem els termes de llicència, si estem d'acord amb ells, i indicarem que volem realitzar una instal·lació de tipus 'Personalitzada: instal·lar només Windows (avançat)', ja que l'altra opció 'Actualització' només és vàlida si ja disposem d'un sistema de la família Windows en l'equip sobre el qual instal·larem el nou servidor.

**Nota:**  
Depenent de la versió del SO, les opcions disponibles per a instal·lar poden variar.

Términos de licencia y avisos aplicables

**AVISO IMPORTANTE** (seguido de los TÉRMINOS DE LICENCIA)

**Información de uso y diagnóstico.** Microsoft recopila esta información, que puede estar relacionada con su organización, en forma automática a través de Internet, y la utiliza para ayudar a mejorar su experiencia del usuario, y la calidad y seguridad de Microsoft. Windows Server incluye cuatro (4) informaciones (Seguridad, Básico, Mejorado y Completado) en forma predeterminada. El nivel de información requerida para: (i) ejecutar nuestras informaciones antimalware y de uso y diagnóstico del dispositivo, y el uso y compatibilidad de las identificar los problemas de calidad en el uso y sistema operativo y aplicaciones.

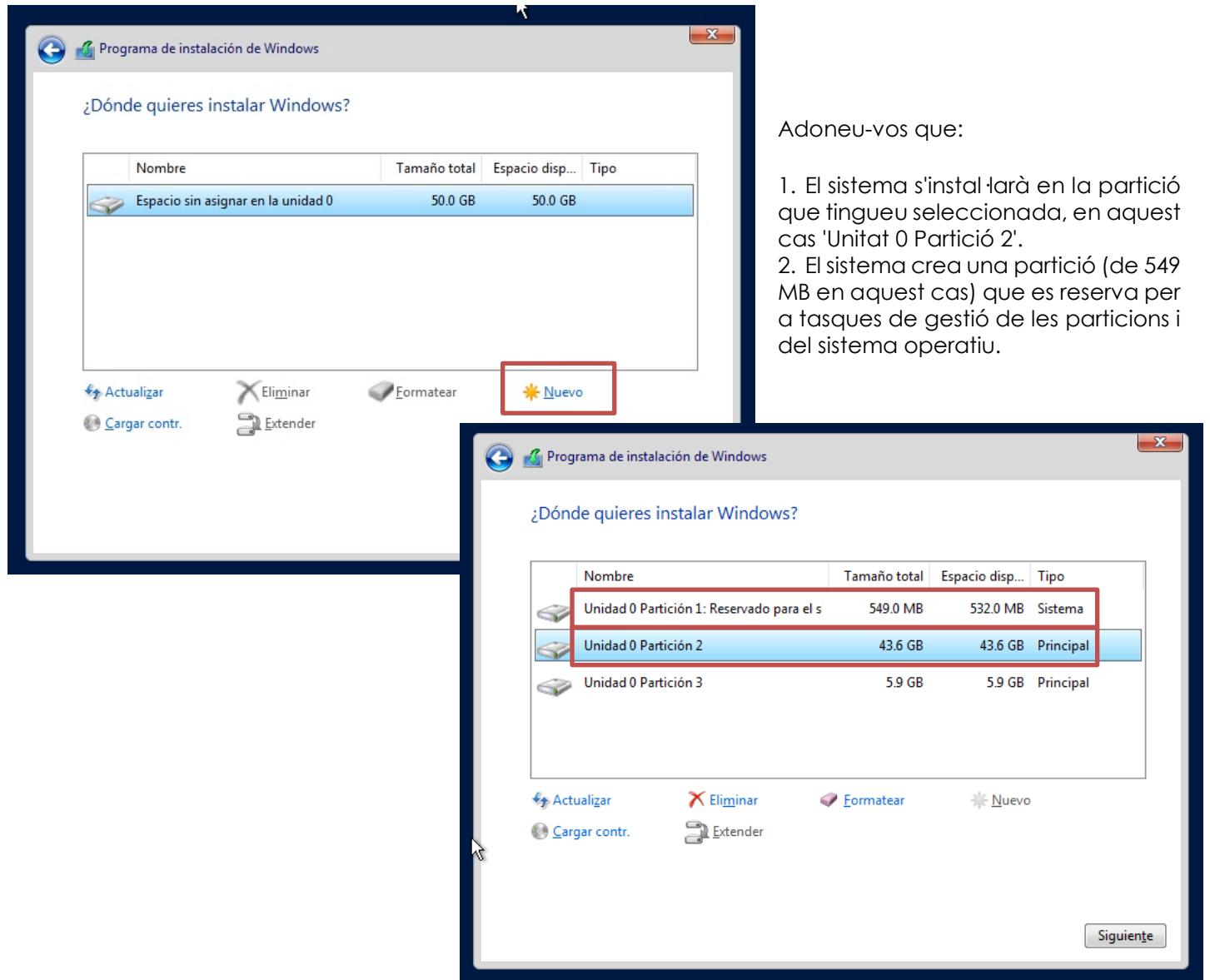
Acepto los términos de licencia

¿Qué tipo de instalación quieres?

**Actualización: instalar Windows y conservar archivos, configuraciones y aplicaciones**  
Los archivos, configuraciones y aplicaciones se migran a Windows con esta opción, que solo está disponible si el equipo ya ejecuta una versión compatible de Windows.

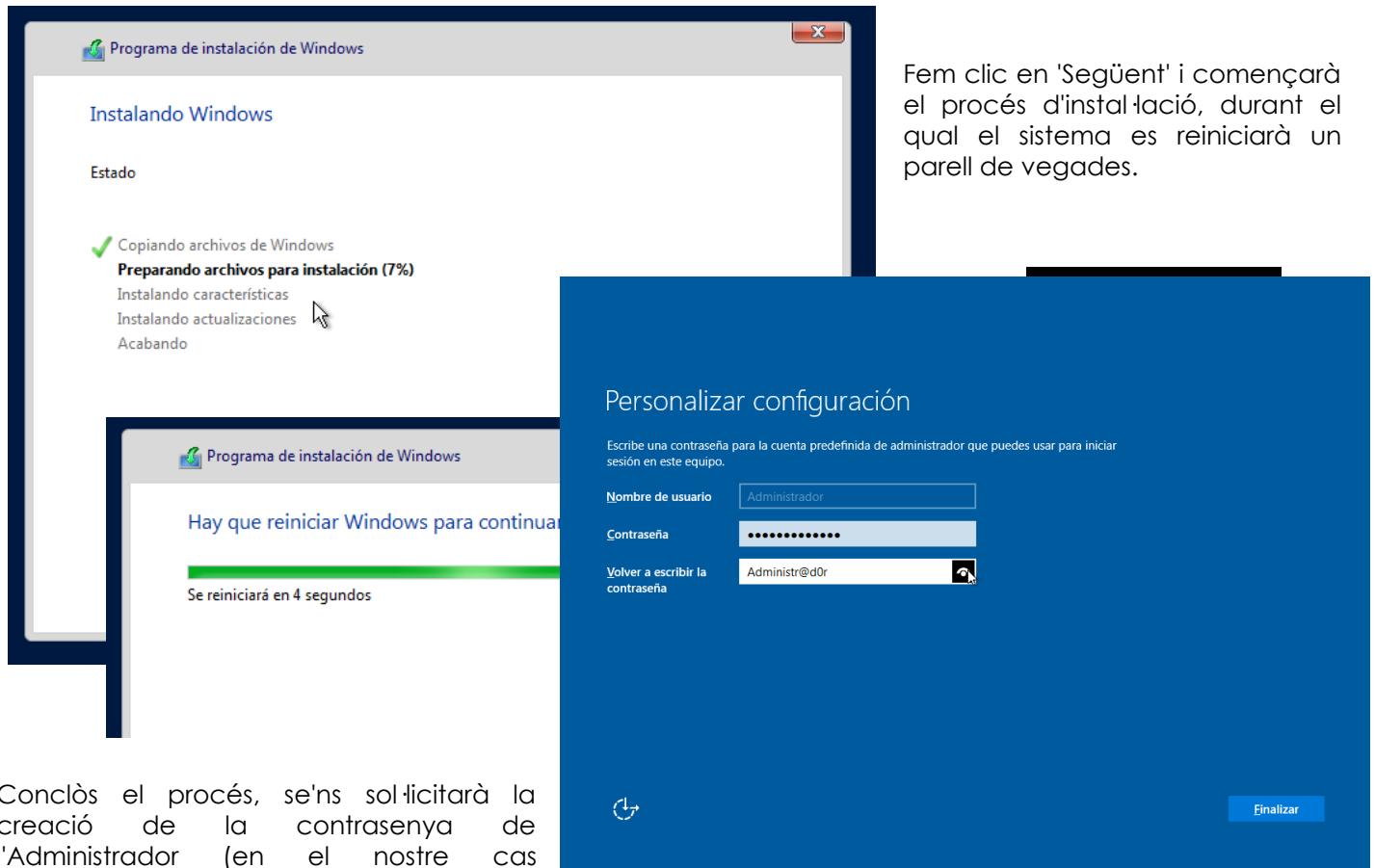
**Personalizada: instalar solo Windows (avanzado)**  
Los archivos, las configuraciones y las aplicaciones no se migran a Windows con esta opción. Si quieras hacer cambios en las particiones y las unidades, inicia el equipo con el disco de instalación. Te recomendamos que hagas una copia de seguridad de tus archivos antes de continuar.

Encara que no és imprescindible, en aquest cas crearem dues particions: una per a C: i una altra per a D:



Adoneu-vos que:

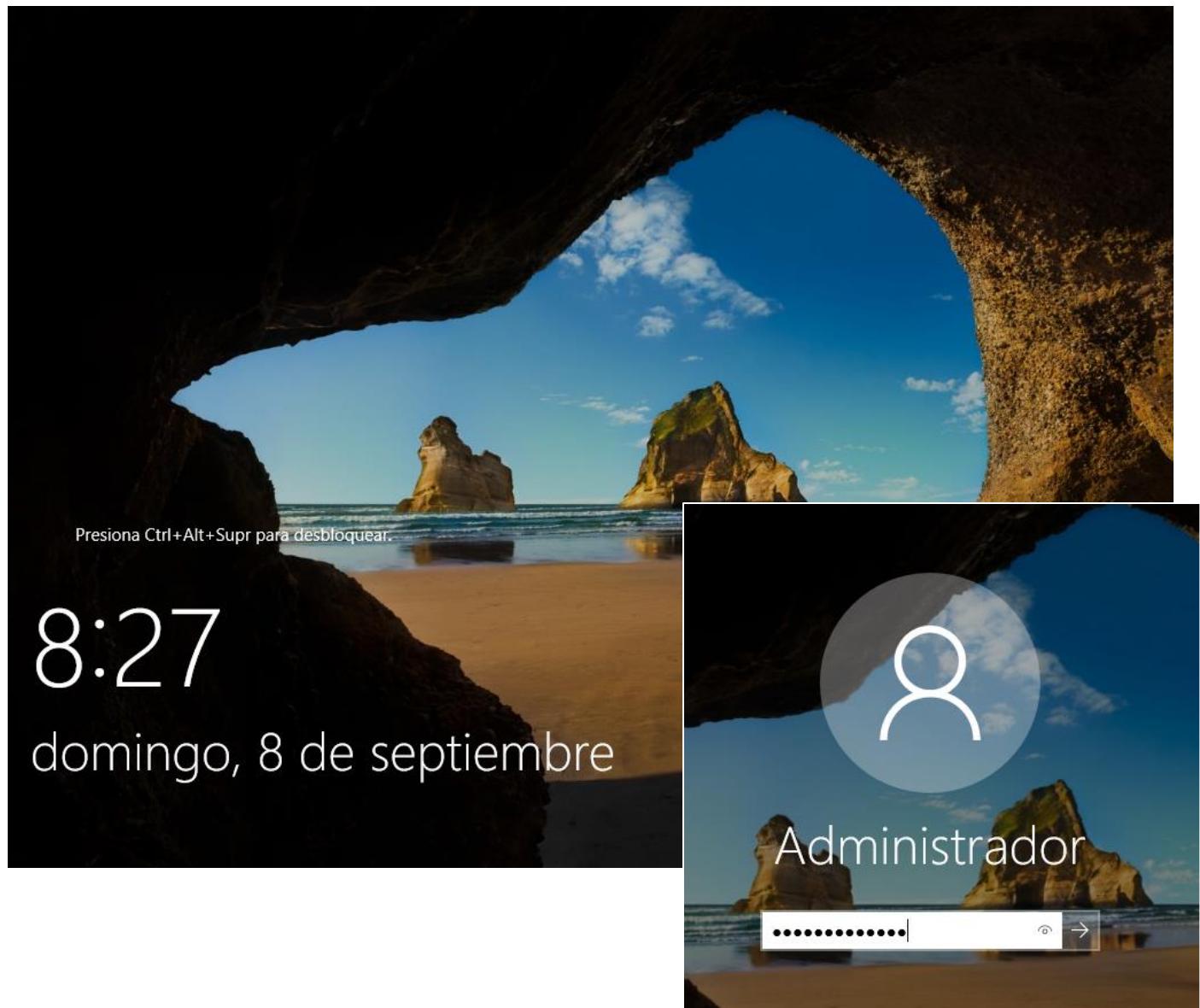
1. El sistema s'instal·larà en la partició que tingueu seleccionada, en aquest cas 'Unitat 0 Partició 2'.
2. El sistema crea una partició (de 549 MB en aquest cas) que es reserva per a tasques de gestió de les particions i del sistema operatiu.



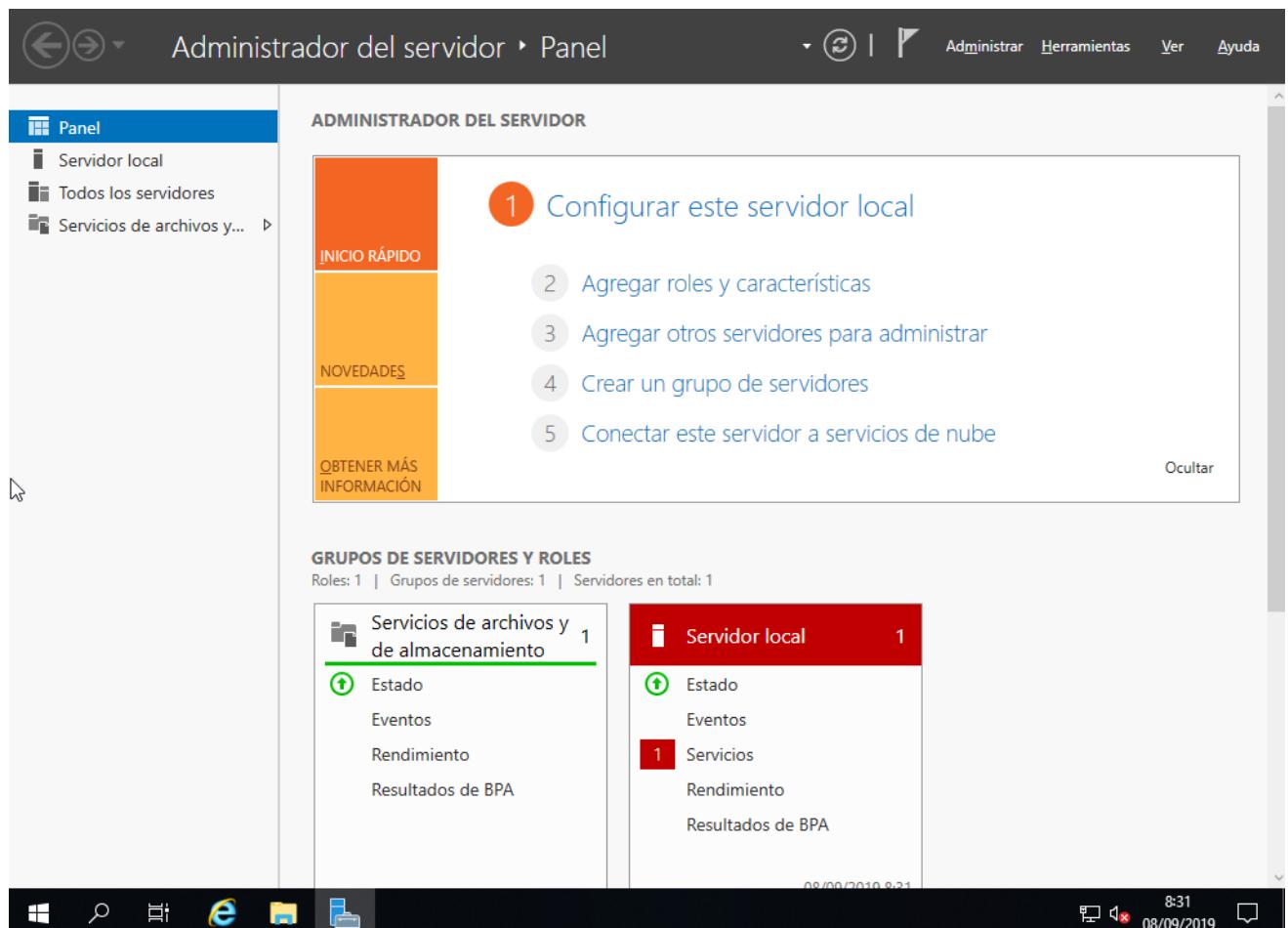
Conclòs el procés, se'n sol·licitarà la creació de la contrasenya de l'Administrador (en el nostre cas Administristr@d0r).

Fem clic en 'Següent' i començarà el procés d'instal·lació, durant el qual el sistema es reiniciarà un parell de vegades.

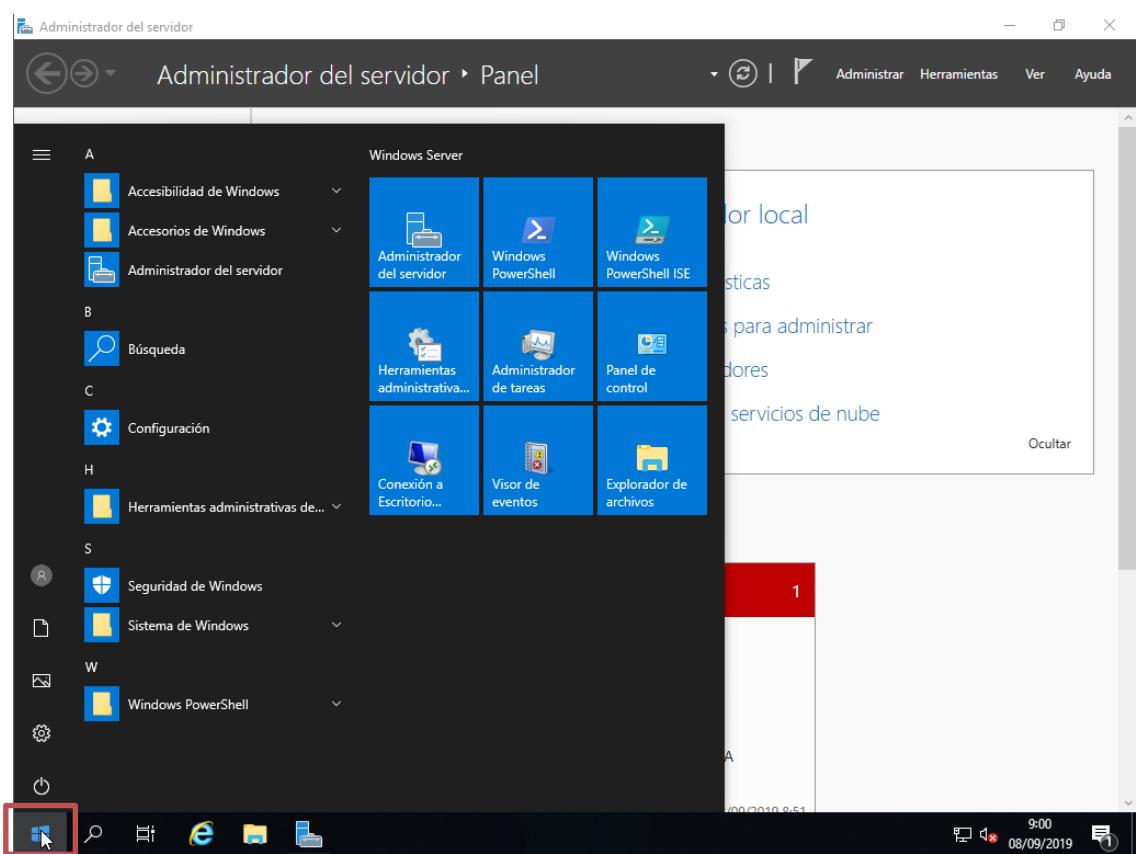
A continuació, ens apareixerà la pantalla d'accés el sistema característica. Introduirem Ctr+Alt+Supr (com treballem amb màquines virtuals, cal teclejar Ctr dreta + Supr)



D'aquesta manera ja tindrem conclòs el procés d'instal·lació i podrem accedir al sistema. Automàticament s'obrirà l'Administrador del Servidor. La interfície és molt similar a les versions anteriors 2016 i 2012 de Windows Server (i radicalment diferent a la 2008).



Per a accedir al menú d'inici, al menú de configuració o per a realitzar cerques, situarem el ratolí en el límit inferior esquerre de l'escriptori.



A continuació, podem instal·lar les "Guest Additions".

## 3.2. Windows Server 2012

### 3.2.1. Edicions

Microsoft Windows Server 2012 només compta amb 4 edicions:

- Datacenter
- Standard
- Essentials
- Foundation

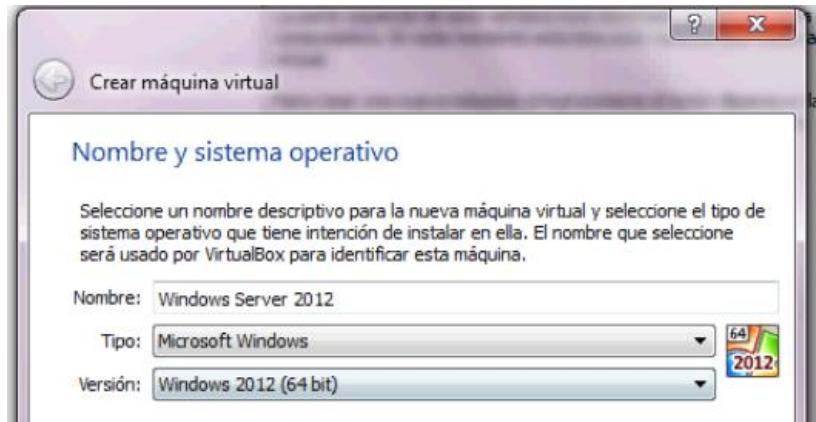
	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2 Standard	Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation
<b>Locks and Limits</b>				
Maximum number of users	based on licenses	based on licenses	25	15
Maximum SMB Connections	16,777,216	16,777,216	16777216	30
Maximum RRAS Connections	unlimited	unlimited	50	50
Maximum IAS Connections	2,147,483,647	2,147,483,647	50	10
Maximum number of 64-bit sockets	64	64	2	1
Maximum RAM	4 TB	4 TB	64 GB	32 GB
Server can join a domain	Yes	Yes	For migration only	For migration only
DirectAccess	Yes	Yes	See documentation	Yes
<b>Server Roles</b>				
Active Directory® Certificate Services	Yes	Yes	Yes	Yes
Active Directory Domain Services	Yes	Yes	Required	Yes (optional)
Active Directory Federation Services	Yes	Yes	Yes	Yes
AD Lightweight Directory Services	Yes	Yes	No	Yes
AD Rights Management Services	Yes	Yes	Yes	Yes
Application Server	Yes	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes	Yes
DNS Server	Yes	Yes	Yes	Yes
Fax Server	Yes	Yes	Yes	Yes
File Services	Yes	Yes	Yes	Yes
Hyper-V	Yes	Yes	No	No
Network Policy and Access Services	Yes	Yes	Yes	Yes
Print and Document Services	Yes	Yes	Yes	Yes
Remote Access	Yes	Yes	Yes	Yes
Terminal Services Application Sharing	Yes	Yes	No	Yes
Terminal Services Gateway	Yes	Yes	No	See documentation
Web Services (IIS)	Yes	Yes	Yes	Yes
Windows Deployment Services	Yes	Yes	Yes	Yes
Windows Essentials	Yes	Yes	Default	No
Windows Media Services support (Streaming Media Services)	See Installation Options documentation	See Installation Options documentation	Yes	See Installation Options documentation
WINS Server	Yes	Yes	Yes	Yes
<b>Features</b>				
RODC – read only domain controller	Yes	Yes	No	No
Automatic Virtual Machine Activation	Both guest and host	As guest	As guest	No
Best Practices Analyzer	Yes	Yes	Yes	Yes
BranchCache Hosted Server	Yes	Yes	Yes	Yes
BranchCache P2P Cache	Yes	Yes	Yes	Yes
Windows Control Panel	Yes	Yes	Yes	Yes
Distributed File System Replication	Yes	Yes	Yes	Yes
Data Deduplication	Yes	Yes	No	No
iSCSI target support	Yes	Yes	Yes	Yes

### 3.2.2. Creació de la màquina virtual

En primer lloc obrirem VirtualBox i crearem una màquina virtual nova.



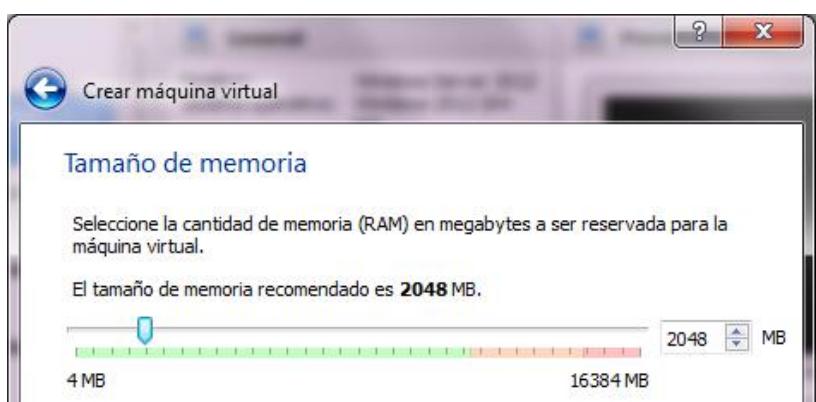
S'obrirà l'assistent per a la creació de màquines virtuals, el qual ens preguntarà per la mena de màquina virtual que volem crear. En aquest cas li indicarem que es tracta d'una màquina virtual de tipus Windows Server 2012.



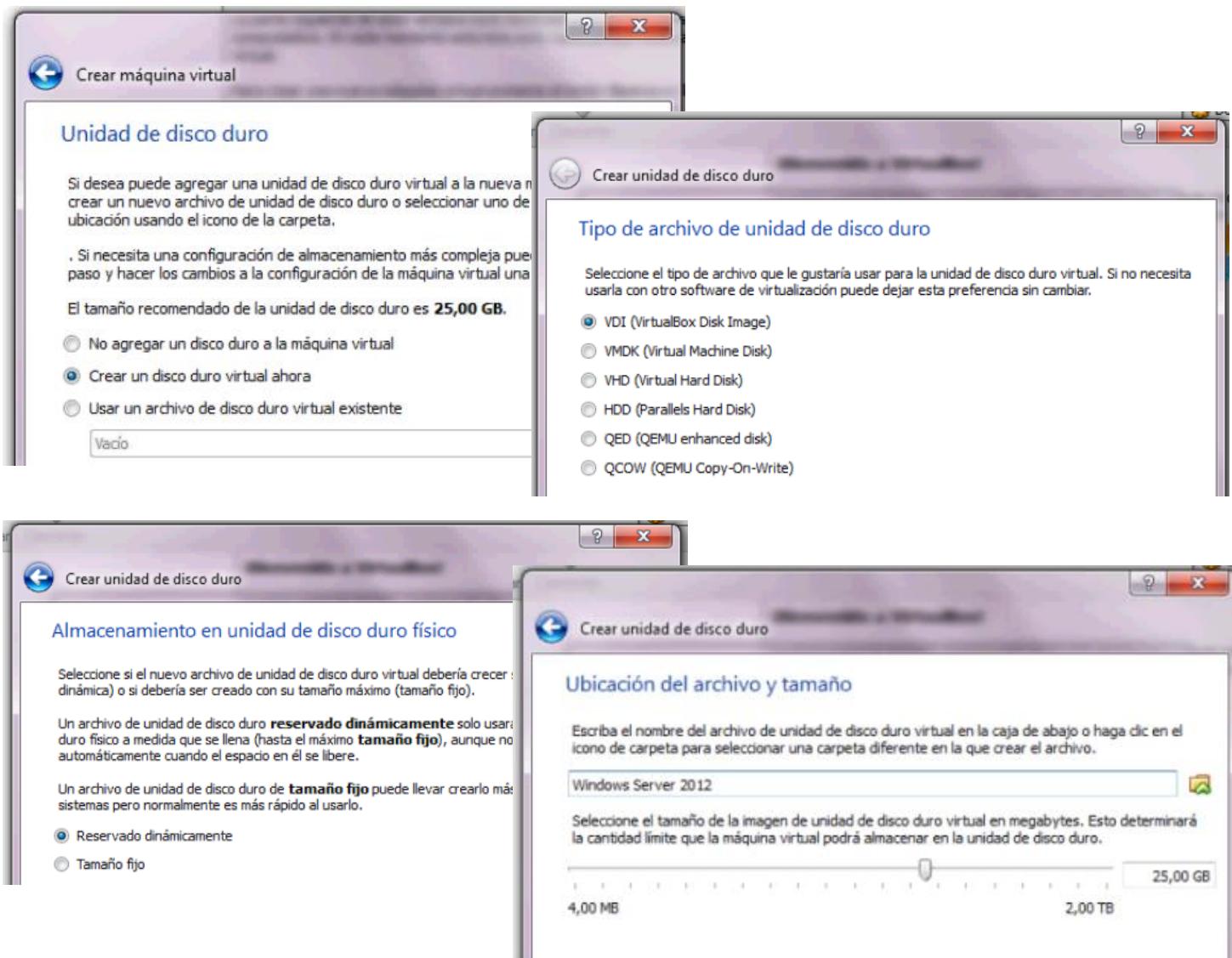
En el següent pas li indicarem la memòria RAM que li assignarem. Com abans, aquest valor dependrà de la quantitat de RAM que hi haja instal·lada en els equips reals.

Un sistema Windows Server 2012 pot funcionar bastant bé amb 1.5GB de RAM. No obstant això, si el nostre equip de classe disposa de RAM suficient, millor assignar-li 2GB.

De tota manera, com durant la instal·lació del sistema únicament tindrem funcionant simultàniament una màquina virtual, podem donar-li un valor més aviat elevat. En posteriors pràctiques ho ajustarem per a no penalitzar en excés el rendiment del sistema en tindre diverses màquines en funcionament.

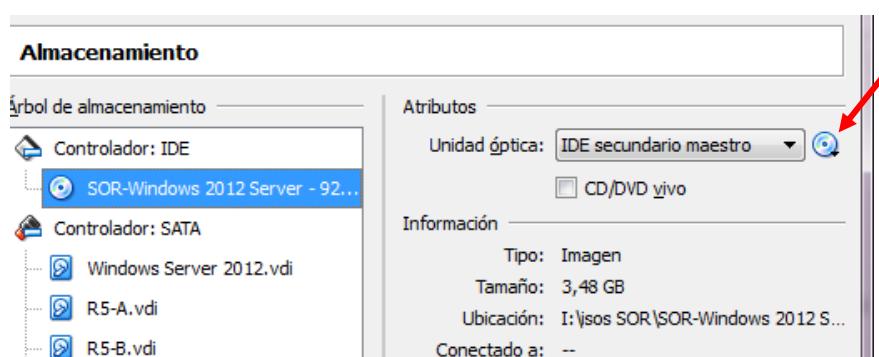


A continuació ens demanarà que creem un disc dur virtual per al servidor. Crearem un disc virtual nou amb emmagatzematge d'expansió dinàmica i una grandària d'uns 25-30GB.

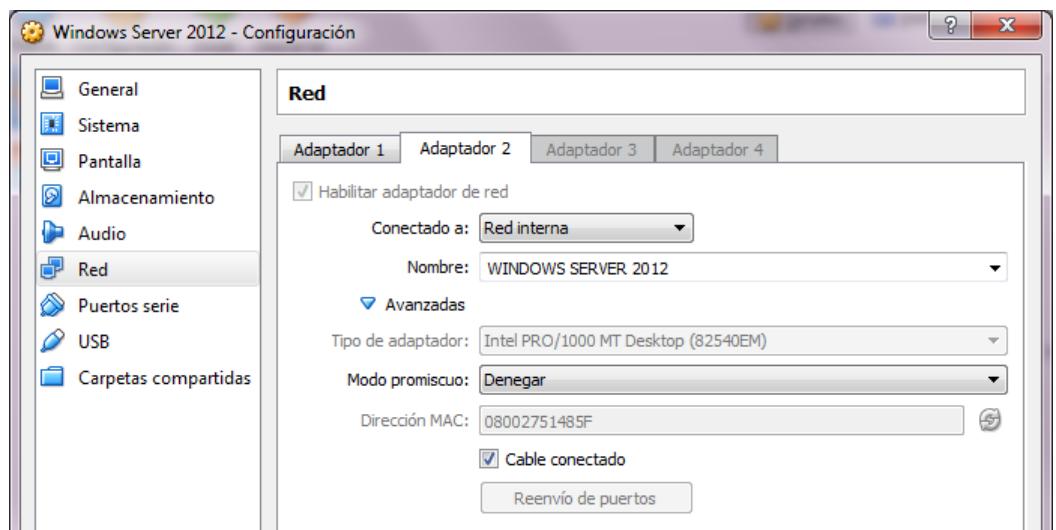
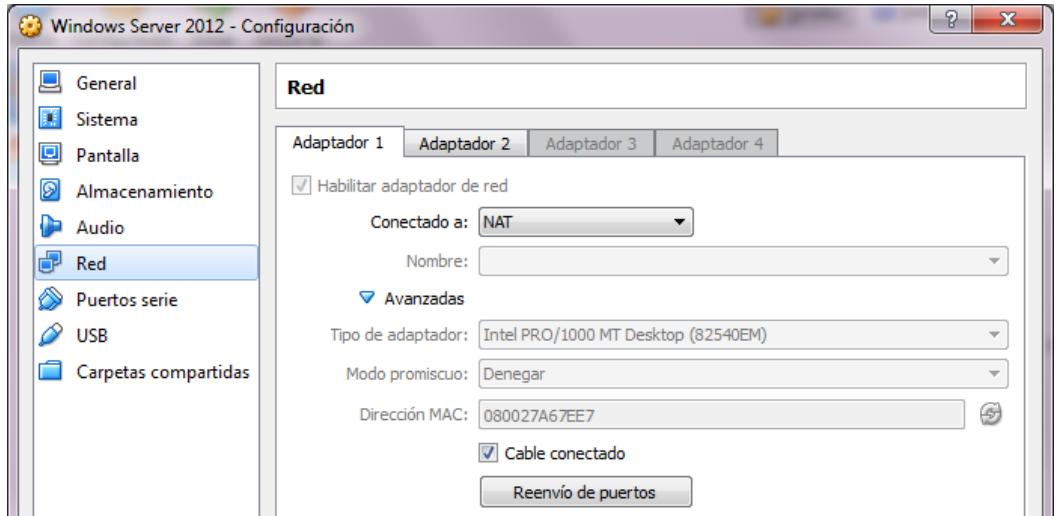


Acabat el procés obtenim un resum del sistema creat.

Abans de començar la instal·lació de Windows Server, haurem d'indicar-li a la màquina virtual on es troba la imatge iso amb la qual volem que arranque i associar-la a un CD virtual.

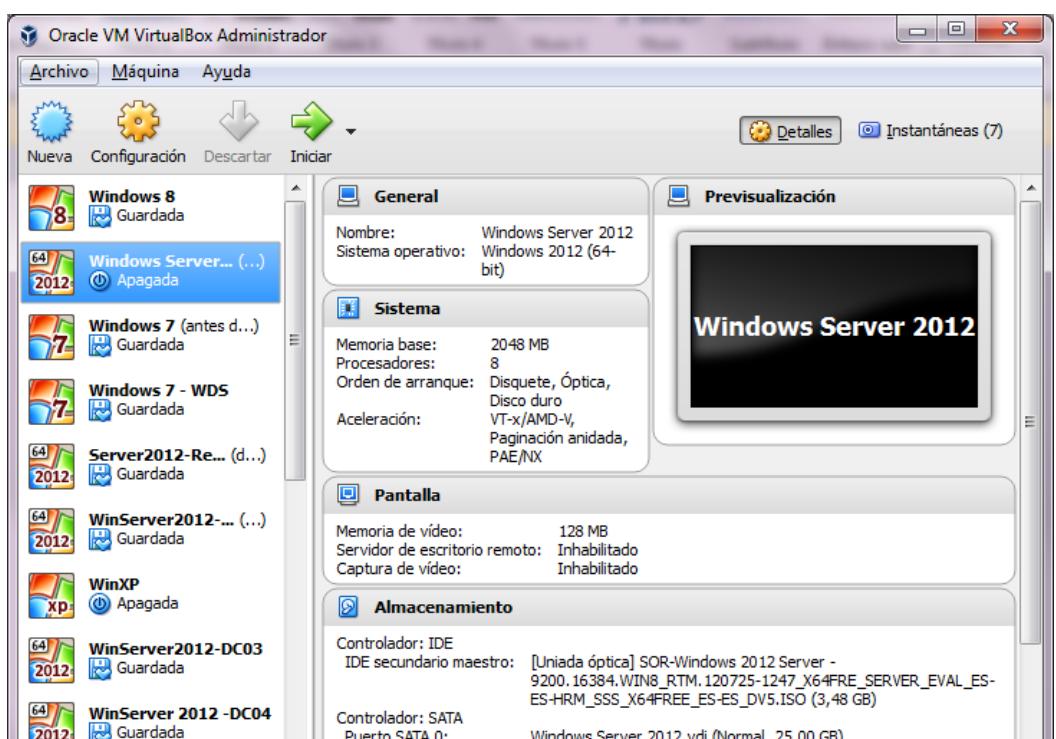


En el desenvolupament de les pràctiques, es demanarà que es configuren en el cas de Windows 2012 dos adaptadors: un d'ells configurat com NAT i l'altre com a xarxa interna (en el cas dels clients Windows 7/8/10 es configurarà el seu adaptador de xarxa com a xarxa interna).



També caldrà indicar que el sistema ha d'arrancar des de la [imatge iso de Windows Server 2012](#) que haurem descarregat prèviament.

És molt important habilitar les optimitzacions de virtualització Intel VT-x/AMD-V en l'apartat "Sistema → Acceleració" de la màquina virtual perquè el rendiment del sistema siga acceptable.



Després d'aquest procés, ja podem arrancar la màquina virtual.

### 3.2.3. Instal·ació

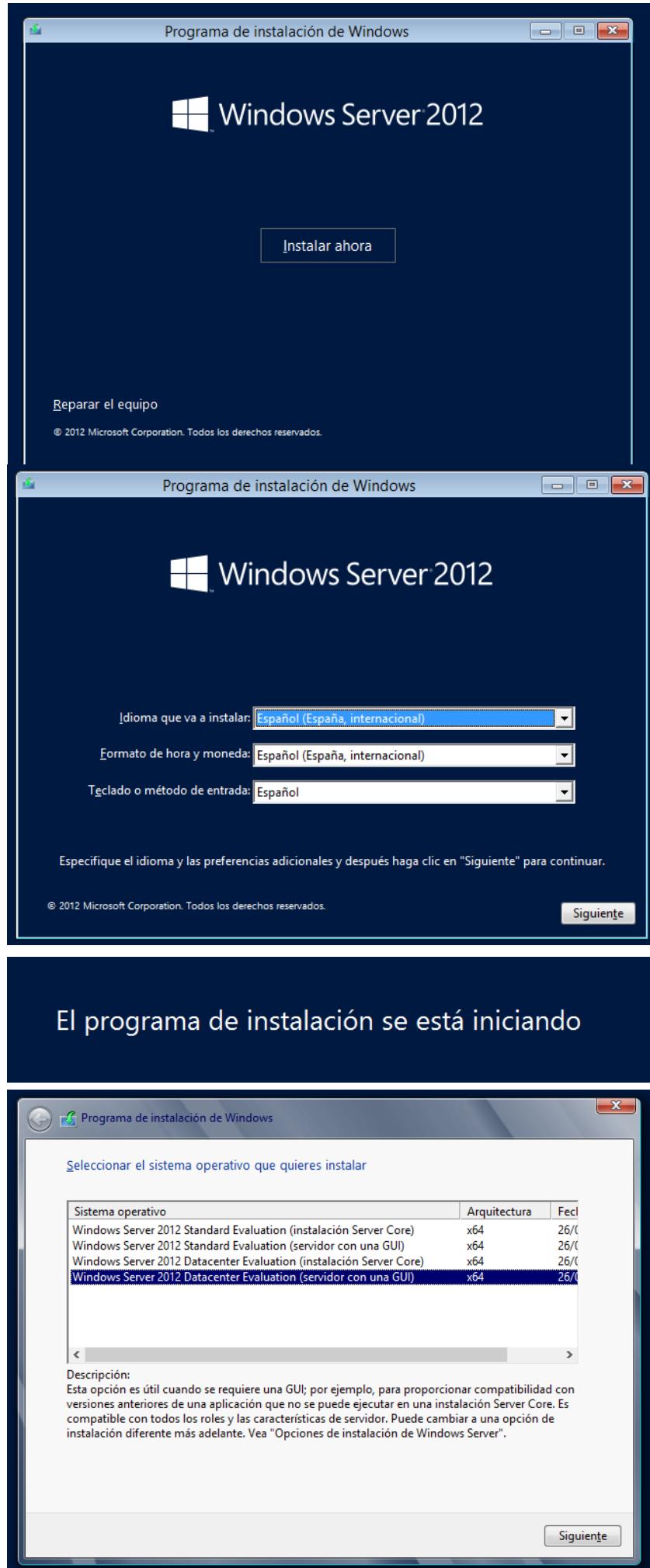
Després d'arrancar la màquina virtual, apareixerà la clàssica pantalla d'inici de la instal·lació.

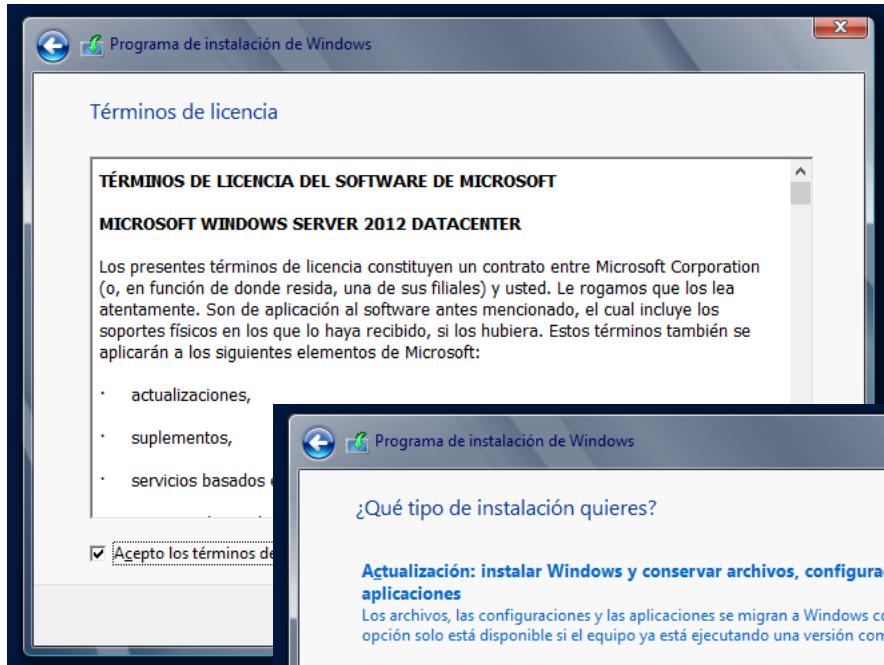
Després de seleccionar l'idioma en el qual volem realitzar la instal·lació, premem 'Siguiente', i a continuació 'Instalar'.

Després d'uns instants en els quals se'n indicarà que està començant el procés d'instal·lació, ens apareixerà una finestra en la qual podrem seleccionar el tipus d'instal·lació realitzar. Ara indicarem que volem instal·lar la versió 'Windows Server 2012 Datacenter Evaluation (servidor amb una GUI)'.

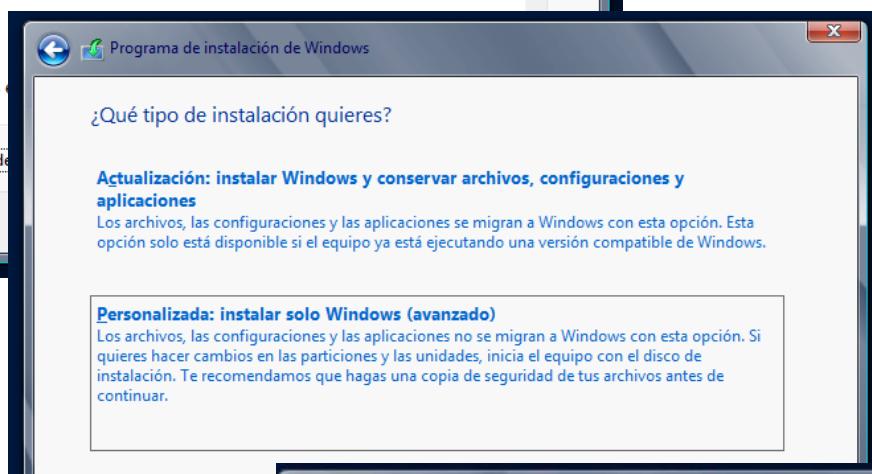
#### Recorda:

Les instal·lacions de tipus Core no tenen una interfície gràfica.





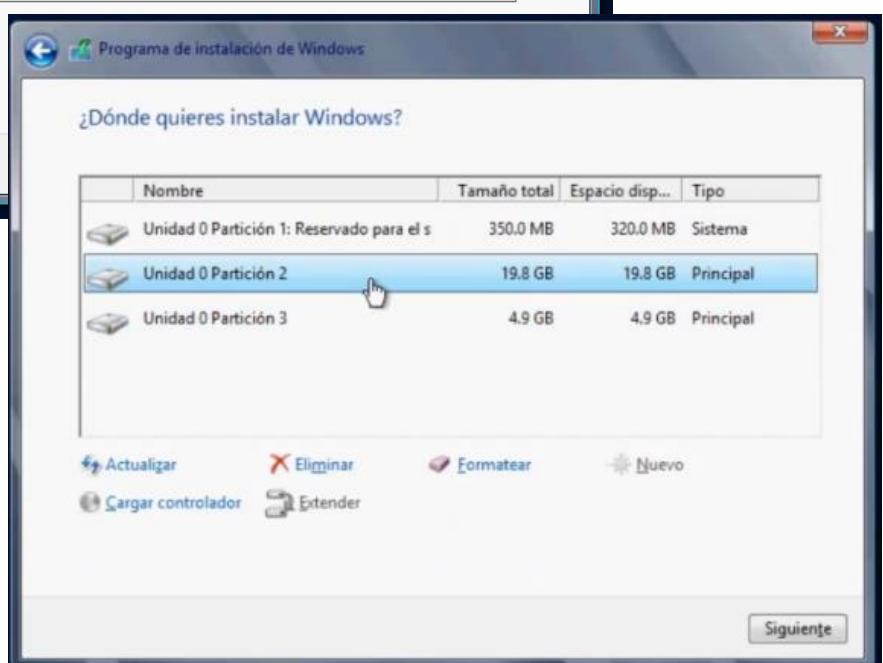
A continuació , acceptarem els termes de llicència, si estem d'acord amb ells, i indicarem que volem realitzar una instal·lació de tipus 'Personalitzada': instal·lar només Windows (avançat), ja que l'altra opció 'Actualització' només és vàlida si ja disposem d'un sistema de la família Windows en l'equip sobre el qual instal·larem el nou servidor.



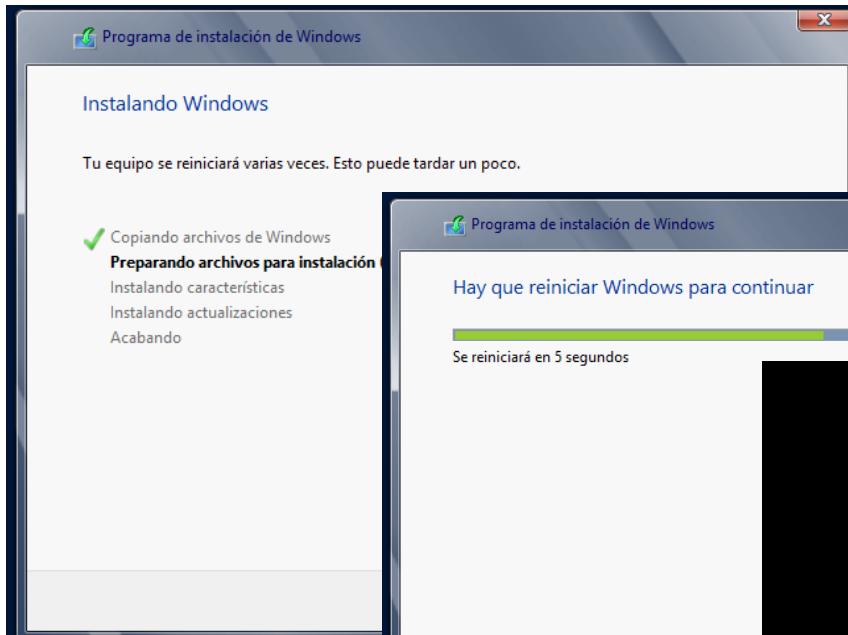
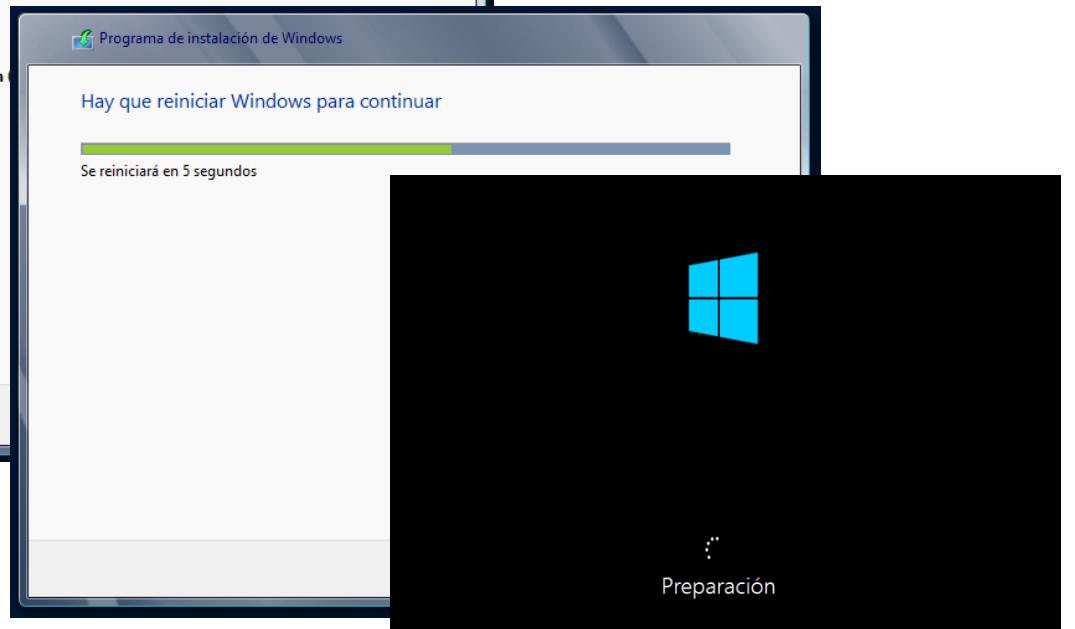
Encara que no és imprescindible, en aquest cas crearem dues particions: una per a C: i una altra per a D:

Adoneu-vos que:

3. El sistema s'instal·larà en la partició que tingueu seleccionada, en aquest cas 'Unitat 0 Partició 2'.
4. El sistema crea una partició (de 350 MB en aquest cas) que es reserva per a tasques de gestió de les particions i del sistema operatiu.



Fem clic en 'Següent' i començarà el procés d'instal·lació, durant el qual el sistema es reiniciarà un parell de vegades.

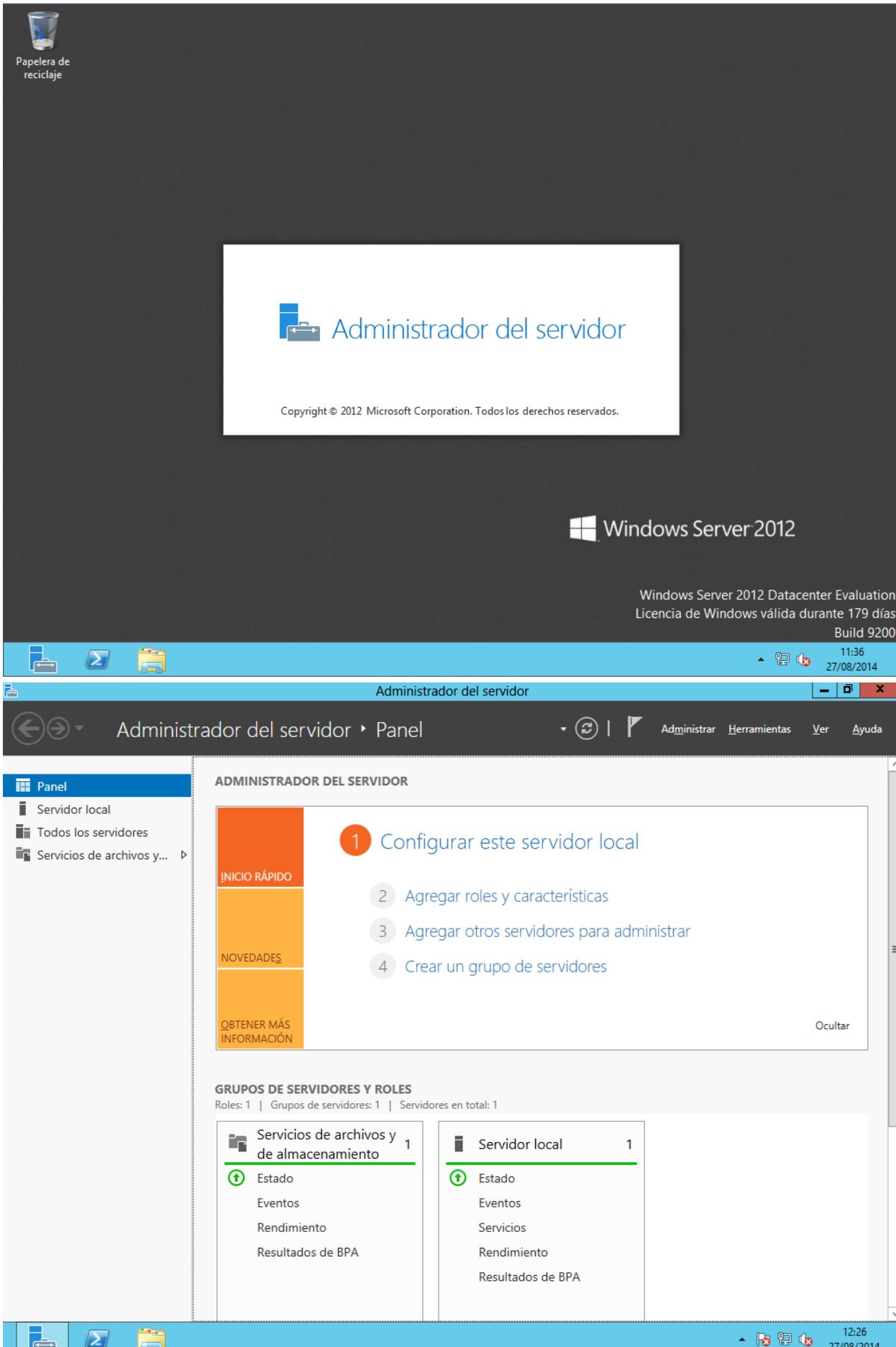



Preparación

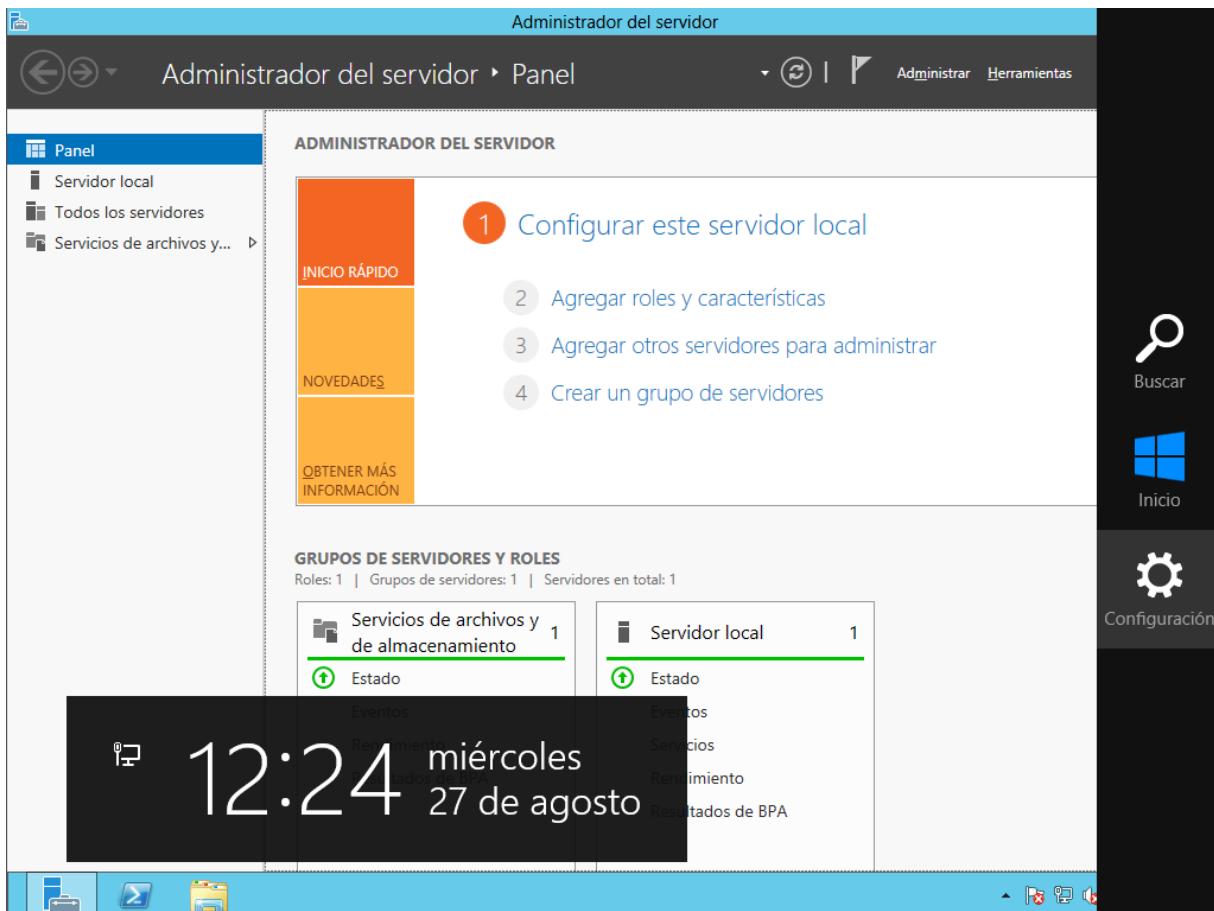
Conclòs el procés, ens apareixerà la pantalla d'accés al sistema característica. Introduirem Ctrl+Alt+Supr, i se'ns sol·licitarà la creació de la contrasenya de l'Administrador.



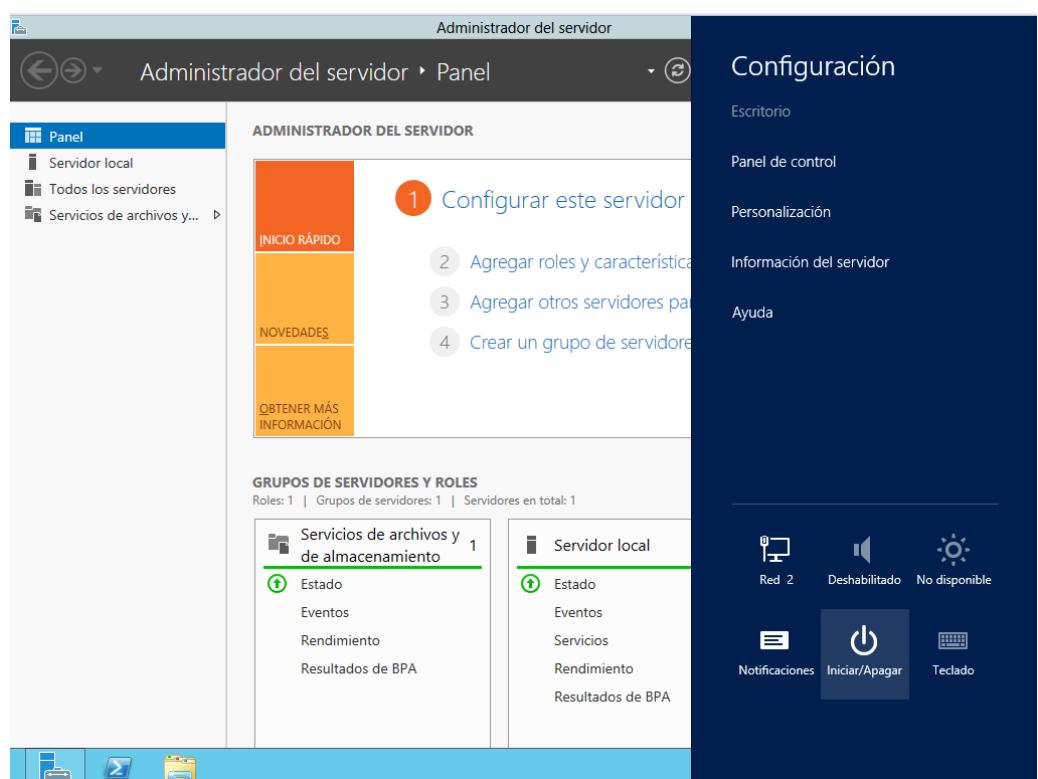
D'aquesta manera ja tindrem conclòs el procés d'instal·lació i podrem accedir al sistema. Automàticament s'obrirà l'Administrador del Servidor.



La interície és radicalment diferent a la de versions anteriors de Windows Server. Per a accedir al menú d'inici, al menú de configuració o per a realitzar cerques, situarem el ratolí en el límit inferior dret de l'escriptori i apareixerà una barra vertical.



Si fem clic en 'Configuració' podrem accedir a apartats com el Panell de control, la configuració de la xarxa, o **el botó d'apagat/reinici**.



A continuació, podem instal·lar les "Guest Additions".

### 3.3. Windows Server 2008

#### 3.3.1. Edicions

Existeixen diferents edicions de Windows Server 2008, en funció dels serveis que poden implementar. Aquestes versions són:

- Enterprise
- Datacenter
- Standard
- Itanium
- Web
- HPC Server
- Foundation

Les funcions típiques dels servidors i les versions de Windows Server 2008 que les suporten venen recollides en la següent taula:

KEY:  = Not Available  = Partial/Limited  = Full

Server Role	Enterprise	Datacenter	Standard	Itanium	Web	Foundation	HPC
Active Directory Certificate Services			 <sup>1</sup>			 <sup>1</sup>	 <sup>1</sup>
Active Directory Domain Services							
Active Directory Federation Services							
Active Directory Lightweight Directory Services							
Active Directory Rights Management Services							
Application Server							
DHCP Server							
DNS Server							
Fax Server							
File Services			 <sup>2</sup>			 <sup>2</sup>	 <sup>2</sup>
Hyper-V							
Network Policy and Access Services			 <sup>3</sup>			 <sup>5</sup>	 <sup>3</sup>
Print and Document Services							
Remote Desktop Services			 <sup>4</sup>			 <sup>6</sup>	 <sup>4</sup>
Web Services (IIS)							
Windows Deployment Services							
Windows Server Update Services (WSUS)							

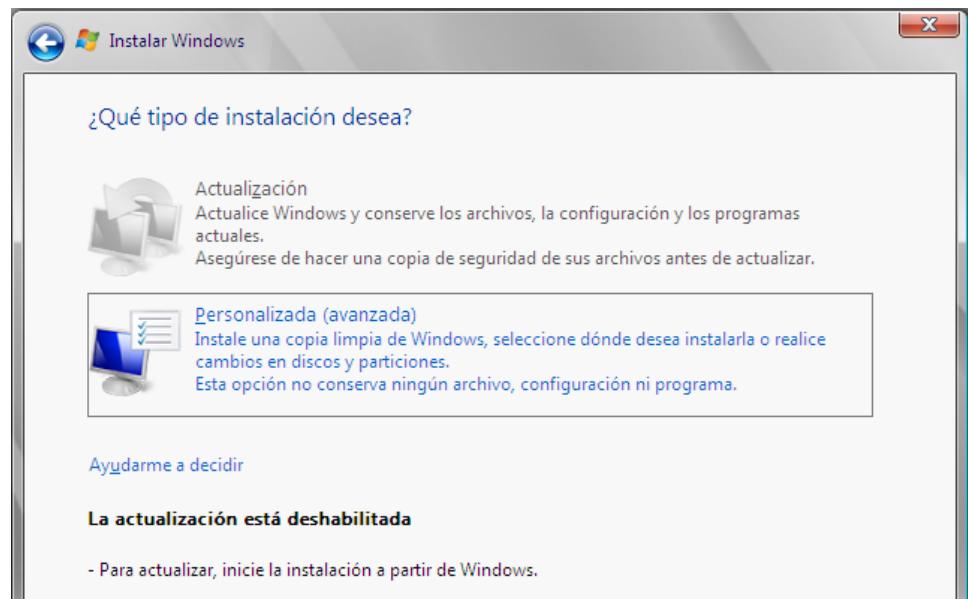
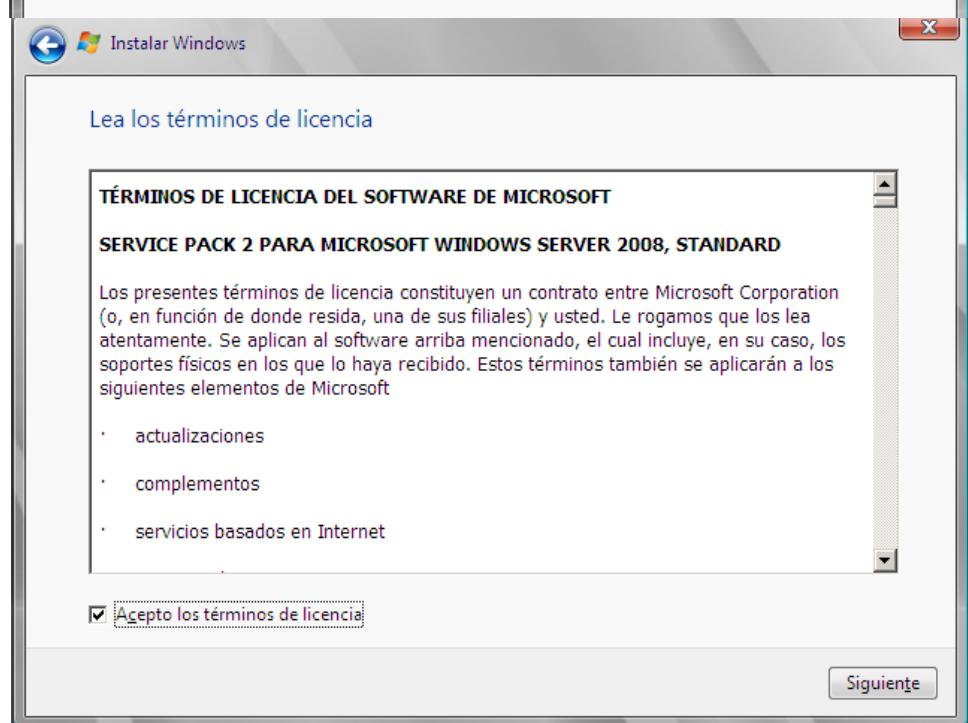
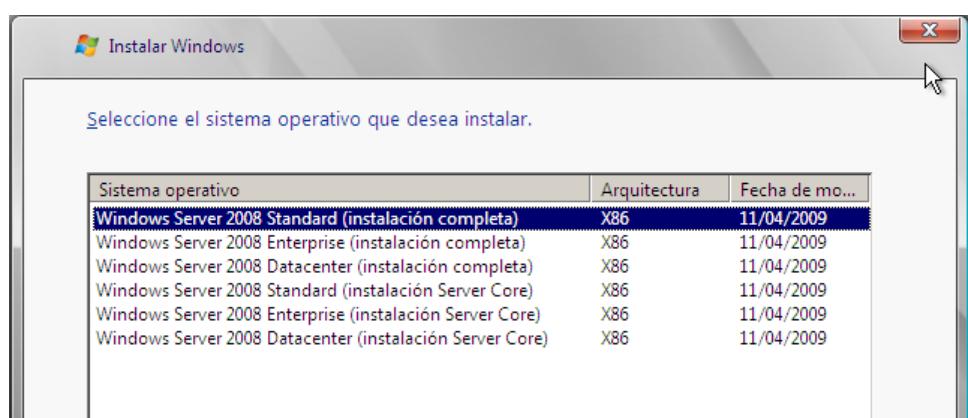
HPC Edition is limited in use to running clustered HPC applications or providing job scheduling services for HPC applications.

### 3.3.2. Instal·lació

Una vegada que està llena la màquina virtual, l'arranquem amb el botó "Iniciar" en la part superior de la interfície de VirtualBox. Als pocs instants, el programa d'instal·lació ens preguntarà quina versió de Windows Server 2008 volem instal·lar.

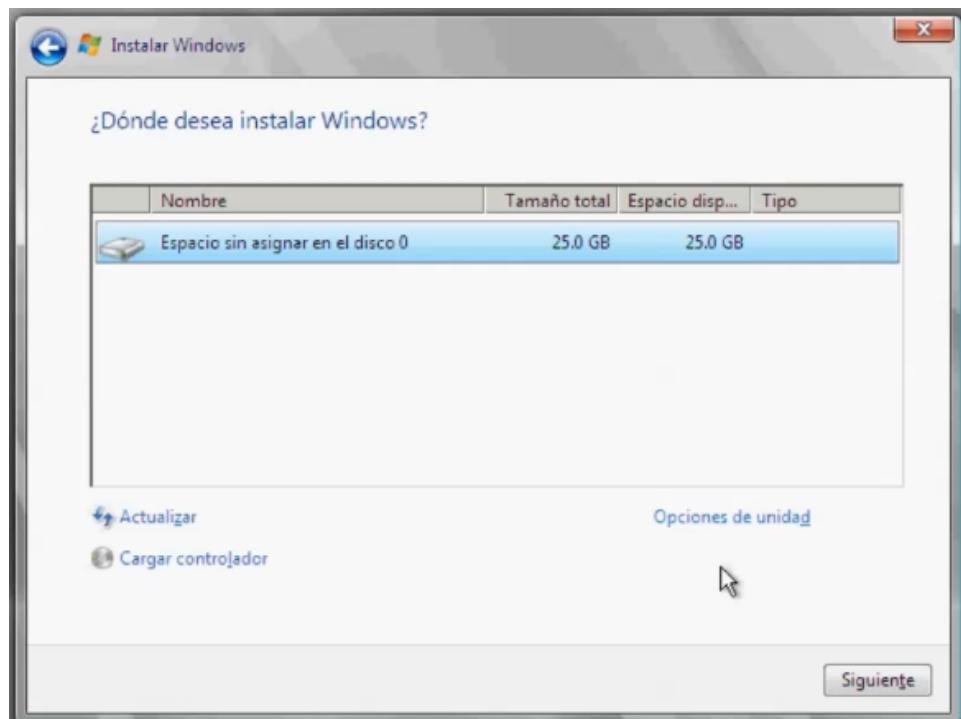
En el nostre cas seleccionarem la versió ressaltada en la imatge anterior: Windows Server 2008 Standard (instal·lació completa). Més endavant analitzarem les característiques de cada versió.

A continuació es mostraran els termes de la llicència. Si estem d'acord amb els termes, acceptarem i prosseguirem amb el procés.

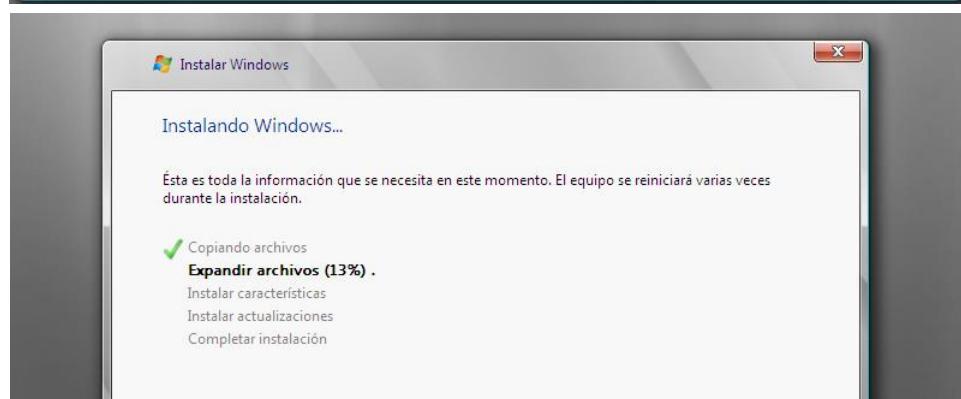


En el següent pas se'n pregunta si desitgem fer una actualització o una instal·lació personalitzada. En cas de dubte, farem clic en l'enllaç 'Ajudar-me a triar'. En el nostre cas seleccionarem l'opció 'Personalitzada'.

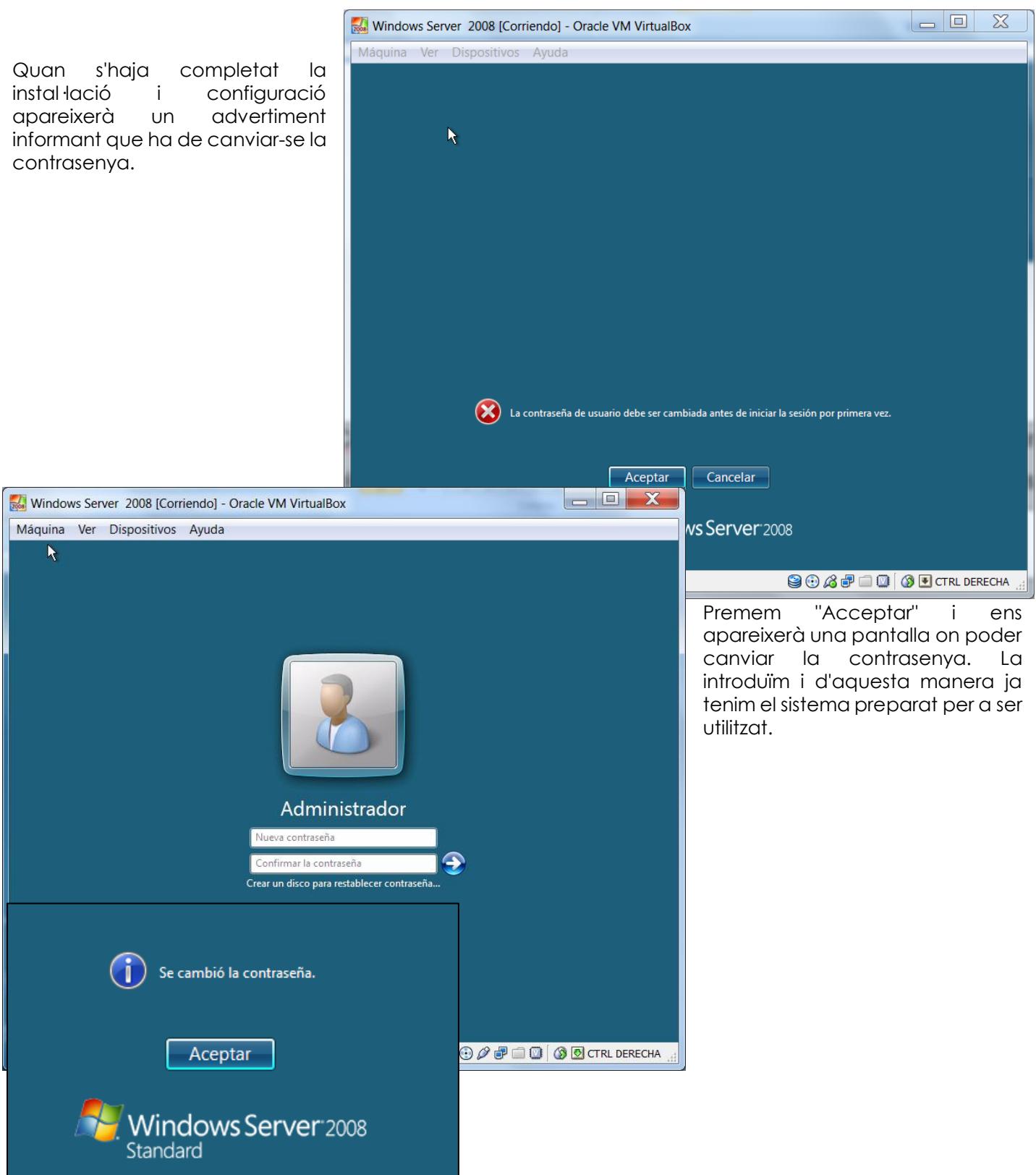
La següent pantalla ens preguntarà per l'espai a partitionar. Utilitzarem completament el disc dur que hem creat per a la partició del sistema (c:\), per la qual cosa indicarem a l'assistent d'installació que utilitze el disc sencer. En temes posteriors afegirem discs virtuals per a ampliar la capacitat d'emmagatzematge del sistema.



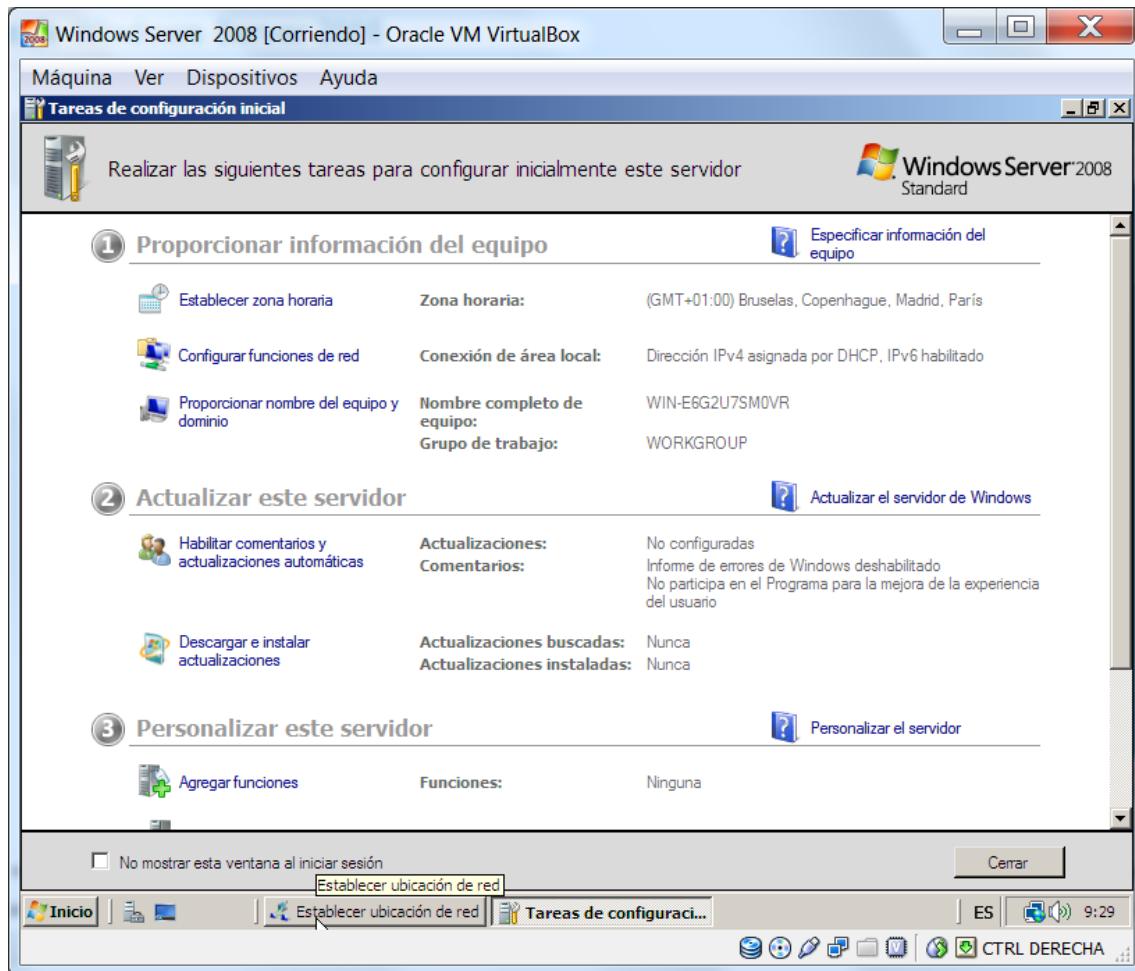
Després d'aquest pas començarà el procés d'installació pròpiament dit.



Finalment l'equip es reiniciarà un parell de vegades.



Premem "Aceptar" i ens apareixerà una pantalla on poder canviar la contrasenya. La introduïm i d'aquesta manera ja tenim el sistema preparat per a ser utilitzat.



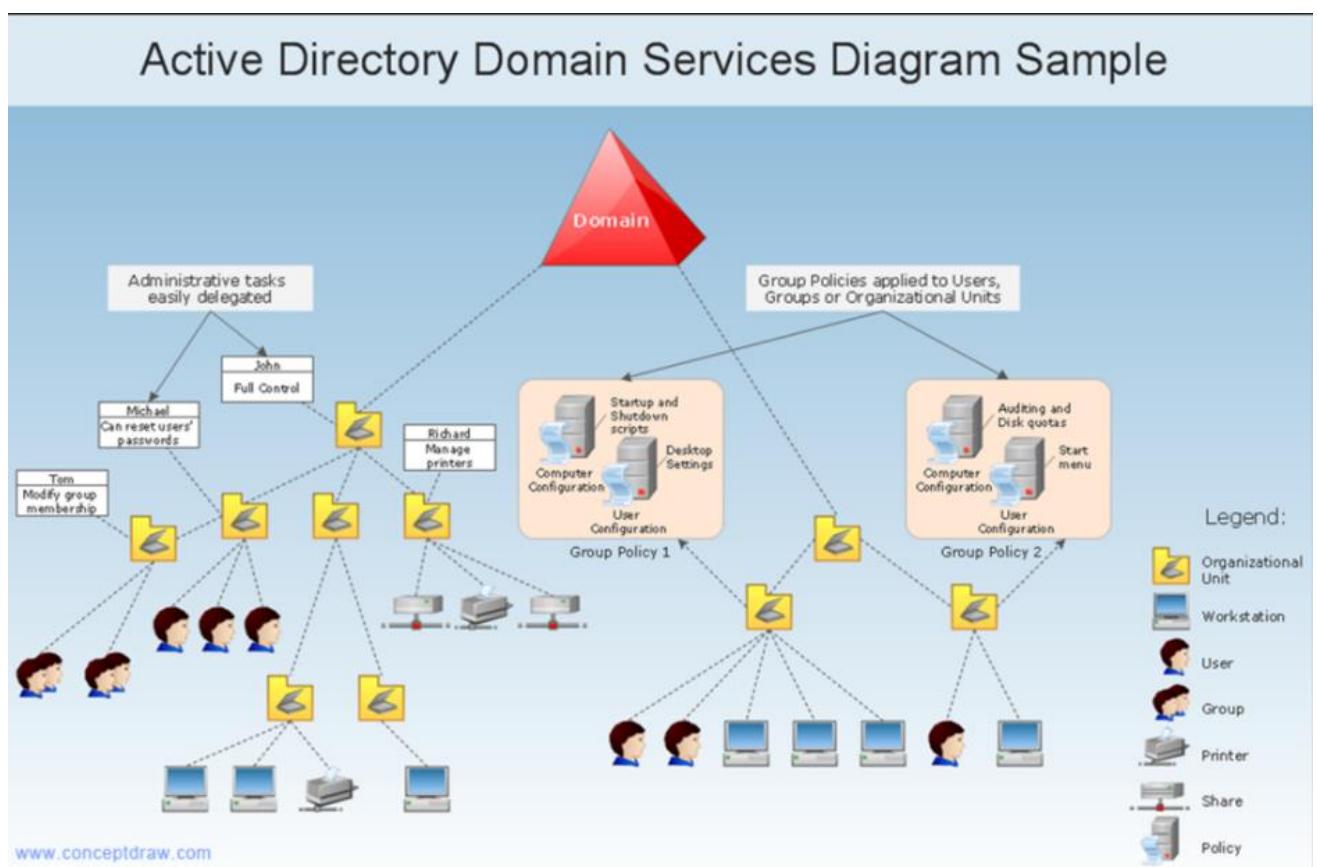
A continuació, podem instal·lar les "Guest Additions".

#### **4. Bibliografia**

- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows Server 2012.
- Somebooks.es (2014). Sistemes Operatius en Xarxa. Disponible en <http://somebooks.es/?p=4787>
- Wikipedia. Sistema Operatiu de xarxa. Disponible en [http://es.wikipedia.org/wiki/sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/sistema_operativo_de_red)
- Blog de SoporteTI. Disponible en: <http://blog.soporteti.net/>
- Elaboració pròpria

# Sistemes Informàtics

## UD12. Part 3. Dominis en Windows Server i serveis de AD, DNS, encaminament i DHCP



# Índex

1.	Objectius.....	2
2.	Introducció: Grups de treball vs dominis (client/servidor) .....	2
3.	Conceptes bàsics en una estructura d'Active Directory.....	3
3.1.	Directori.....	3
3.2.	Servei de directori.....	3
3.3.	Domini .....	3
3.4.	Objectes de l'Active Directory o Directori Actiu .....	3
3.5.	Unitat organitzativa .....	4
3.6.	Controlador de domini .....	4
3.7.	Subdomini .....	4
3.8.	Arbre .....	4
3.9.	Bosc .....	4
3.10.	Resum gràfic de la jerarquia d'AD: .....	5
4.	L'administrador del servidor.....	6
5.	Passos previs a la creació d'un domini: configuració d'IP fixa i nom d'equip.....	7
5.1.	Configuració del nom del servidor.....	8
5.2.	Configuració de la IP del servidor .....	9
6.	Serveis a instal·lar en Windows Server 2019: Active Directory, DNS, encaminament, DHCP .....	11
7.	Instal·lació dels serveis d'Active Directory i de DNS: creació d'un domini.....	11
8.	Instal·lació de l'servei d'encaminament. ....	22
8.1.	El servei d'encaminament. ....	22
8.2.	Instal·lació del servei d'encaminament. ....	22
8.3.	Configuració del servei d'encaminament. ....	26
9.	Instal·lació del servei de DHCP .....	28
9.1.	El servei de DHCP (Dynamic Host Configuration Protocol).....	28
9.2.	Instal·lació del servei DHCP .....	28
9.3.	Configuració del servei DHCP .....	31
10.	Introducció d'equips client en un Domini Windows 2019 .....	38
10.1.	Introducció de Clients Windows 10 .....	38
10.2.	Introducció de Clients Windows 7 .....	43
11.	Bibliografia .....	45

## 1. Objectius

- Promocionar equips servidors a controlador de domini.
- Crear estructures centralitzades d'administració de xarxes.
- Instal·lar el servei DNS en els controladors de domini.
- Configurar la xarxa dels equips membres del domini.
- Instal·lar el servei d'encaminament i DHCP.
- Unir equips clients a un domini.
- Conéixer estructures jeràrquiques més complexes (arbres i boscos).

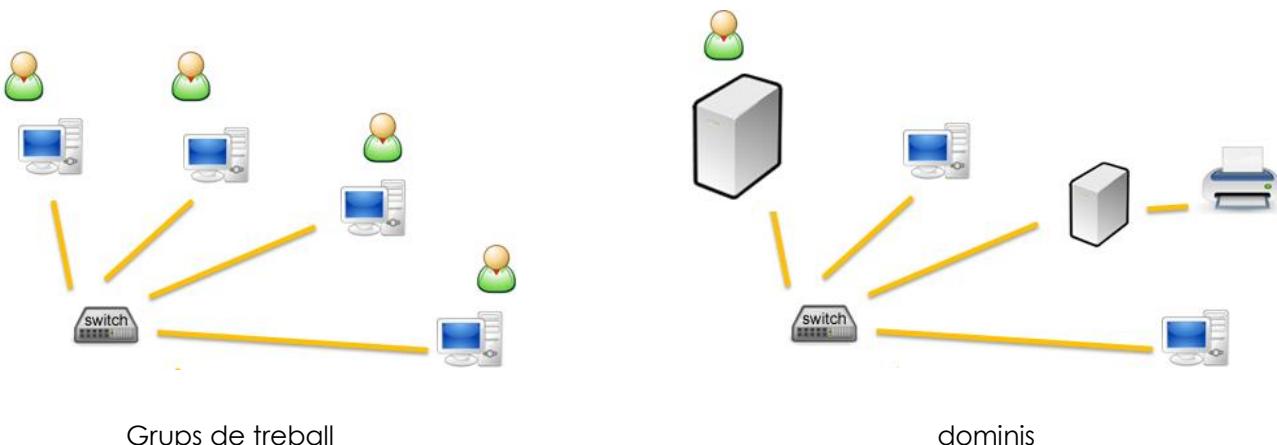
## 2. Introducció: Grups de treball vs dominis (client/servidor)

En la configuració d'una xarxa d'ordinadors que treballaran junts cal prendre una decisió de disseny important: treballar com a **grup de treball** o treballar com un **domini**.

Quan desitgem tindre una **gestió** mínimament **centralitzada** o necessitem un **control sobre els recursos** dels quals disposa cada usuari en la xarxa, hauríem de passar-nos a un **domini**, ja que el grup de treball ens dificulta bastant arribar a aquests objectius.

D'aquesta manera, podríem destacar les següents **diferències entre grup de treball i domini**:

- **Administració centralitzada:** en el grup de treball no existeix. Cada equip és independent i es relaciona amb els altres d'igual a igual, el que disposa d'un recurs decideix si el comparteix o no. Si una persona va actuar com a Administrador en tots els equips, haurà de mantenir un control com tal de tots i cadascun d'ells .  
En un domini, la gestió de l'Administrador és més senzilla, ja que el que modifique des del Controlador del domini podrà tindre efecte en tots els usuaris i ordinadors que pertanguen al domini.
- **Usuaris:** els usuaris en un grup de treball són locals a la màquina on es creen , en canvi en un domini, cada usuari podrà obrir sessió en qualsevol ordinador del domini, i només cal crear-lo en el controlador de domini (servidor).
- **Accedir a recursos compartits:** en un domini, es comparteix un recurs i es donen permisos a usuaris del domini, obliguen sessió on obliguen. En un grup de treball de Windows XP/Vista/7/8 (per exemple ) es comparteix el recurs per a un usuari que tinguem creat localment, de manera, que si volem que entre un usuari des d'un altre ordinador haurem d'anar allí i crear-lo amb el mateix nom d'usuari i la mateixa contrasenya.



## 3. Conceptes bàsics en una estructura d'Active Directory

### 3.1. Directori

Un **directorí** és una base de dades jeràrquica (un magatzem de dades) que guarda la informació sobre els objectes d'una xarxa (usuaris, grups i recursos de l'empresa).

### 3.2. Servei de directori

El **servei de directori** gestiona la base de dades de directori. D'aquesta manera, ens permet administrar de forma centralitzada i senzilla tots els objectes d'un domini, és a dir, ens permet organitzar i controlar de forma centralitzada els usuaris, grups, impressores, pcs, servidors, unitats organitzatives, dades... de la xarxa d'una empresa.

Usant un servei de directori se centralitzarà el procés d'autenticació d'usuaris i es concedeix o denega permisos als usuaris sobre els recursos de forma centralitzada. Per exemple, es pot permetre iniciar sessió en determinats equips del domini amb un determinat horari, denegar la impressió en determinades impressores, usar perfils mòbils permetent que els usuaris tinguen els seus arxius i configuracions, siga com siga l'ordinador en el qual inicien sessió...

Els serveis de directori solen basar-se en els estàndards DNS, LDAP, Kerberos i Certificats x.509.

Existeixen multitud d'implementacions de serveis de directori. Els més coneguts són: **Active Directory de Microsoft**, **Open LDAP** (implementació lliure i de codi obert), eDirectory de Novell i Sun Directory Server (Oracle Directory Server Enterprise Edition).

En el cas **d'Active Directory**, podríem citar les següents característiques generals:

- Implementació de Microsoft de serveis de directori llançat alhora que Windows 2000 i millorat en Windows 2003, 2008, 2012, 2016, 2019 i 2022.
- Necessita un Windows 2000/2003/2008/2012/2016/2019/2022 Server per a convertir-ho en DC (controlador de domini).
- Haurà d'existir almenys un DC per cada domini que emmagatzemarà els comptes, grups, equips, impressores, carpetes compartides, perfils d'usuaris, directives de seguretat, serveis de xarxa, etc. Si existeixen diversos DC, es replicarà la informació dels uns als altres.
- Requereix la instal·lació d'un servidor DNS (que pot instal·lar-se en el propi DC) que s'utilitzarà per a la resolució de noms i localitzar equips i DC.

### 3.3. Domini

D'altra banda, definim **domini** com un conjunt d'equips interconnectats que comparteixen informació administrativa centralitzada (usuaris, grups, contrasenyes...). En aquest cas, comparteixen la mateixa base de dades de directori. Per a posar nom als dominis s'utilitza el protocol DNS (s'identifica únicament per un nom de domini DNS). Per aquest motiu, Active Directory necessita almenys un servidor DNS instal·lat en la xarxa. Un exemple de nom de domini d'una empresa seria empresa.local

### 3.4. Objectes de l'Active Directory o Directori Actiu

El Directori Actiu és una implementació concreta del protocol LDAP, el qual tracta els elements de la xarxa com a **objectes**. L'objecte és la unitat lògica més bàsica d'Active Directory. Els tipus d'objectes **bàsics** que existeixen en el Directori Actiu són:

- Usuaris.
- Grups.
- Equips.
- Impressores.
- Unitats Organitzatives.

No obstant això, els administradors de sistemes poden crear nous tipus d'objectes o afegir propietats a alguna classe dels objectes modificant el **esquema** del Directori Actiu, per a adaptar l'estructura de la xarxa a les necessitats particulars de l'organització.

### 3.5. Unitat organitzativa

Una unitat organitzativa és un conjunt d'objectes d'un domini o subdomini, com ara equips, usuaris, impressores,... L'objectiu és administrar aquest conjunt amb unes directives diferents a la resta del domini.

### 3.6. Controlador de domini

Un **controlador de domini (DC)** és un servidor que manté la base de dades de l'**Active Directory** (amb la informació dels objectes del domini: usuaris, equips, grups...). A través de les eines d'administració es poden administrar els usuaris, grups, equips, permisos,... del domini. Ha de ser un equip preparat per a aguantar altes càrregues de treball amb una alta disponibilitat, i amb un sistema operatiu servidor instal·lat.

### 3.7. Subdomini

És un domini secundari o domini fill que es crea en un arbre existent.

Exemple: institut.local (domini principal o domini arrel o domini pare)  
informatica.institut.local (domini secundari o subdomini o domini fill)

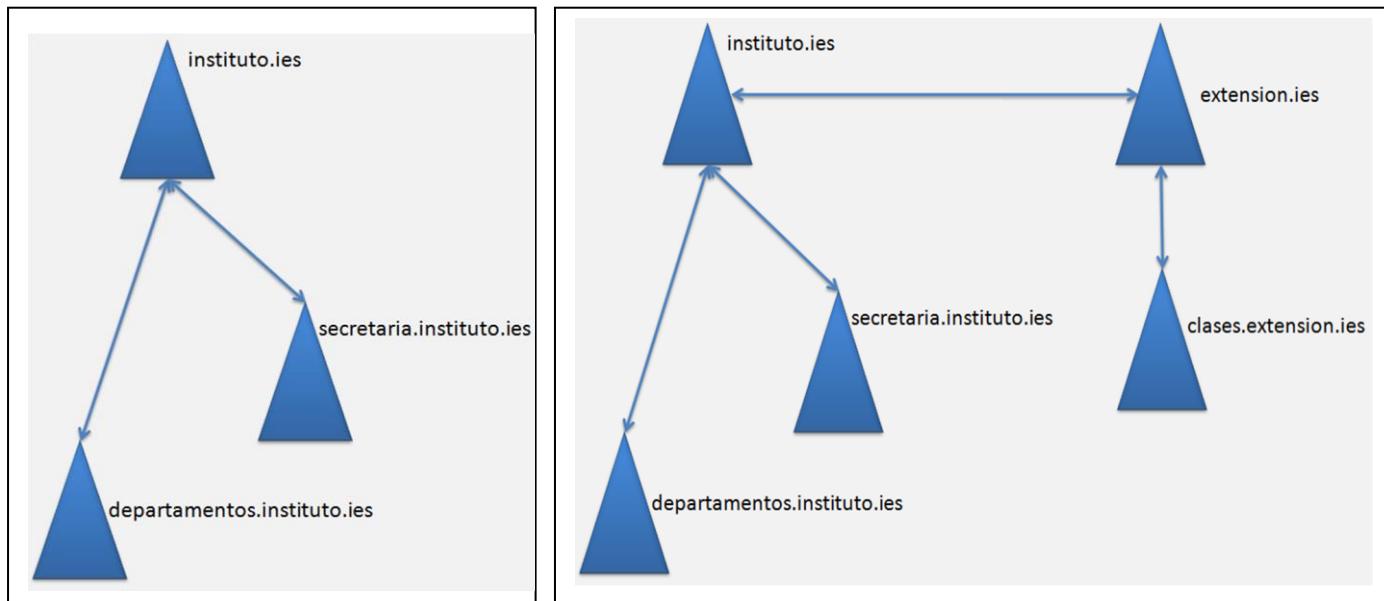
### 3.8. Arbre

Pot donar-se el cas que hi haja altres dominis sota el domini principal, és a dir, que tinguem un o més dominis fill. Quan ens trobem amb aquesta configuració el que tenim és un Arbre.

De totes maneres, cada nou domini que creguem (malgrat que encara no tinga dominis fill) en el nostre bosc serà ja un arbre. Quan creguem el domini inicial serà l'arbre arrel del bosc.

### 3.9. Bosc

Si continuem ascendint jeràrquicament, una agrupació lògica d'arbres de dominis conforma un **bosc**. En les següents imatges es mostra un bosc amb un únic arbre de dominis i un bosc amb dos arbres de dominis. Depenent de la complexitat de l'organització, implantarem una estructura de xarxa més o menys complexa. D'aquesta manera, serà el nostre bosc tot el conjunt de dominis i subdominis que necessitem crear per a l'organització de la nostra empresa.



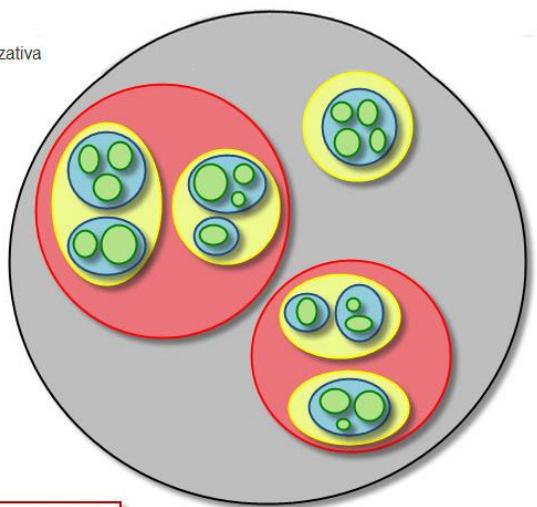
L'estrucció del Directori Actiu es pot considerar com un arbre que conté una col·lecció de dominis. Tots aquests dominis comparteixen el mateix **catàleg global**, que és alguna cosa així com el repositori central de tots els objectes d'un arbre de dominis.

### 3.10. Resum gràfic de la jerarquia d'AD:

Objecte > Unitat Organitzativa > Domini > Arbre > Bosc

- L'objecte és la unitat lògica més bàsica d'Active Directory
- Una **Unitat Organitzativa** pot contindre diversos objectes, incloses altres Unitats Organitzatives.
- El **domini** pot albergar Unitats Organitzatives i aquestes al seu torn albergar Objectes del Directori Actiu
- Un **arbre** està format per dominis, havent-hi sempre un domini Pare i un o més dominis Fill.
- Un **bosc** és una agrupació d'arbres de dominis.

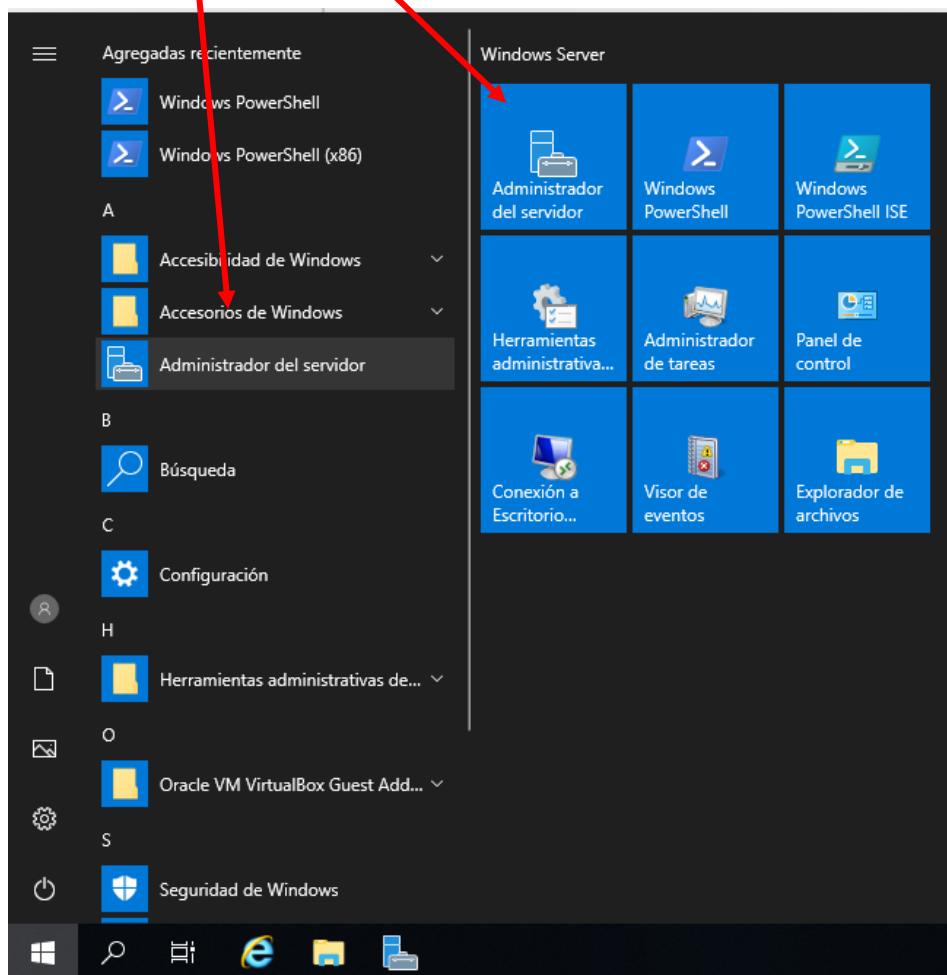
- Objeto
- Unidad Organizativa
- Dominio
- Árbol
- Bosque



Jerarquía del Directorio Activo

## 4. L'administrador del servidor

En l'**Administrador del Servidor** es troben les eines de configuració i administració més freqüents, però en moltes ocasions necessitarem accedir a altres utilitats que no es troben en l'**Administrador del Servidor**. Com a norma general, les utilitats que permeten configurar aspectes locals de la configuració de l'ordinador podran trobar-se en el **Panell de Control**, mentre que les utilitats relacionades amb l'estrucció de xarxa centralitzada es trobaran en **Eines (Administratives)**.



## 5. Passos previs a la creació d'un domini: configuració d'IP fixa i nom d'equip

En instal·lar Windows Server 2019, l'adreçament IP per defecte es troba configurat mitjançant DHCP ("obtindre una adreça IP automàticament"), la qual cosa no és una política adequada ja que les peticions realitzades al servidor no sempre es fan mitjançant la resolució de nom, sinó també mitjançant l'adreça IP, per la qual cosa si aquesta canvia (com podria ocórrer en utilitzar l'assignació d'IP mitjançant DHCP), es podrien donar problemes en la xarxa.

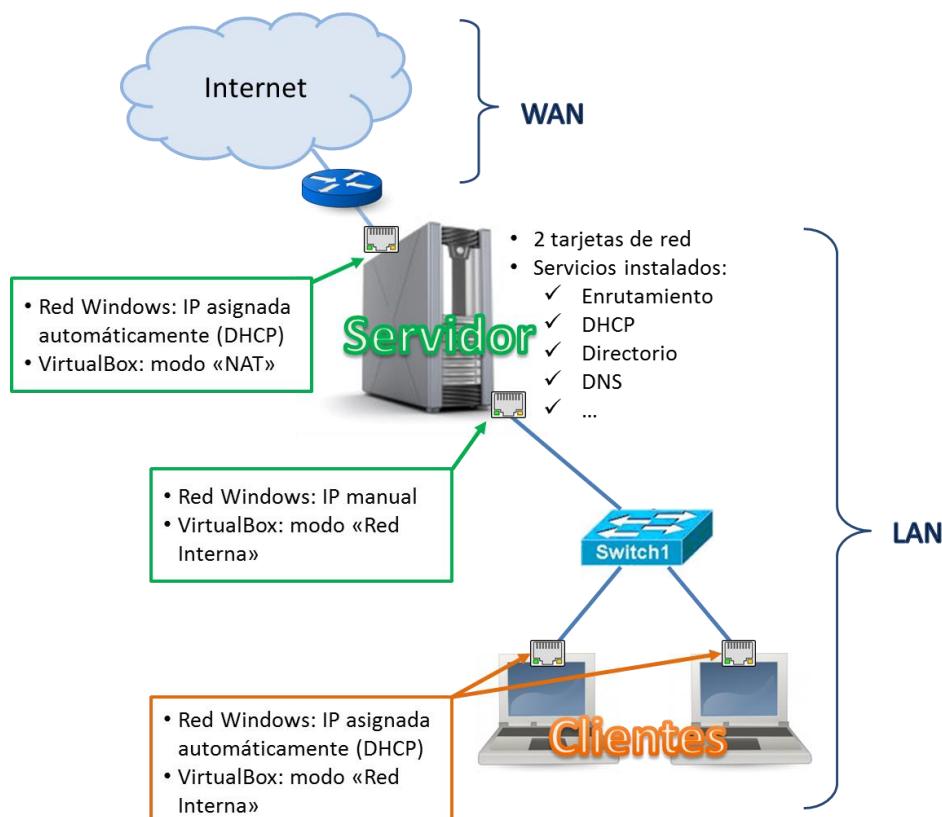
Per tant, **abans d'instal·lar els serveis del Directori Actiu** en l'equip servidor, ens assegurarem que posseeix una **adreça IP fixa**, i a més aprofitarem per a **canviar-li el nom a l'equip** per un més senzill de recordar.



En el nostre cas, configurarem el servidor amb 2 targetes de xarxa:

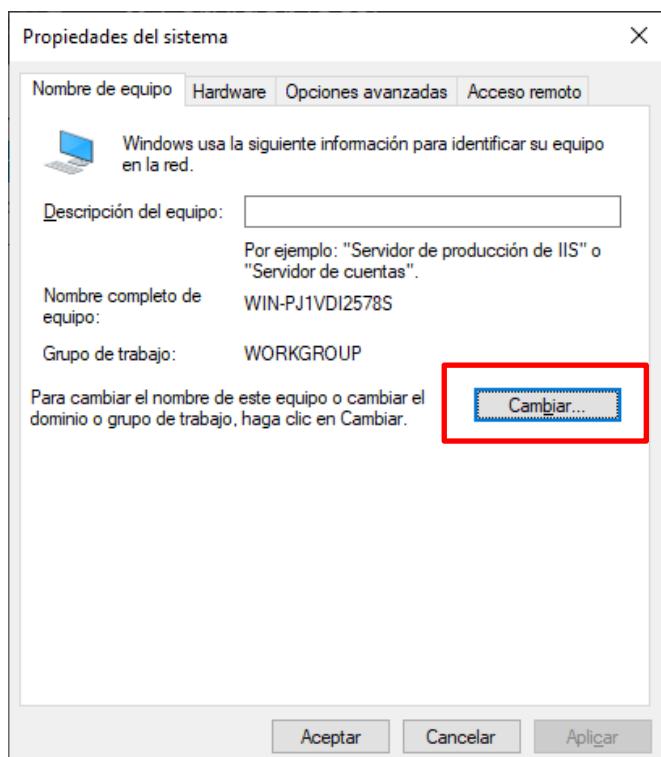
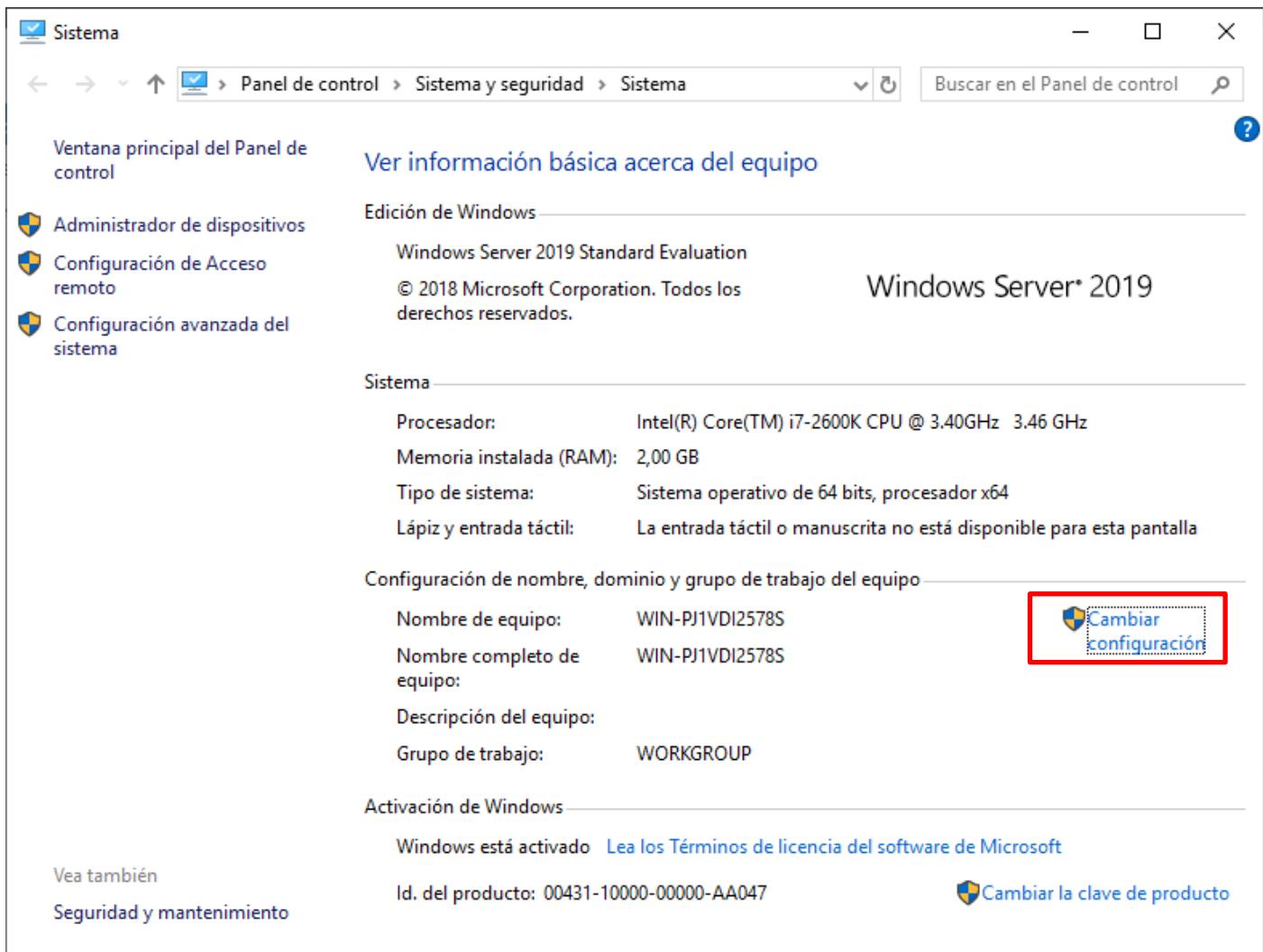
- Una targeta de xarxa es connectarà a la xarxa WAN i la seu IP la rebrà per DHCP. En VirtualBox aquesta targeta estarà en manera "NAT".
- L'altra targeta de xarxa es connectarà a la LAN i sí que tindrà una IP assignada manualment i dins del rang d'IPs privades que hagem establert per a nostra LAN. En VirtualBox aquesta targeta estarà en manera "Xarxa Interna".

En el cas dels clients de la LAN, cadascun d'ells tindrà la seu targeta de xarxa amb IP assignada automàticament per DHCP (el DHCP del servidor).

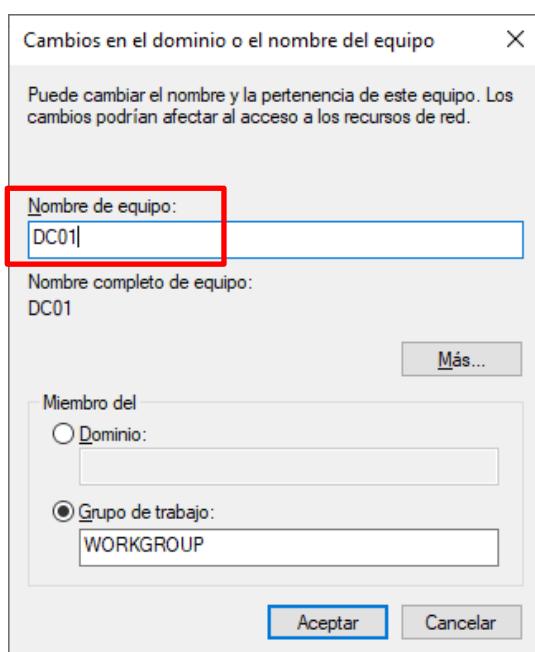


## 5.1. Configuració del nom del servidor

Estrenyem tecles "Windows"+Pausa i accedim a la pantalla de configuració del nom de l'equip



Després de canviar-li el nom a l'equip, necessitarem **reiniciar-lo** perquè els canvis facen efecte.

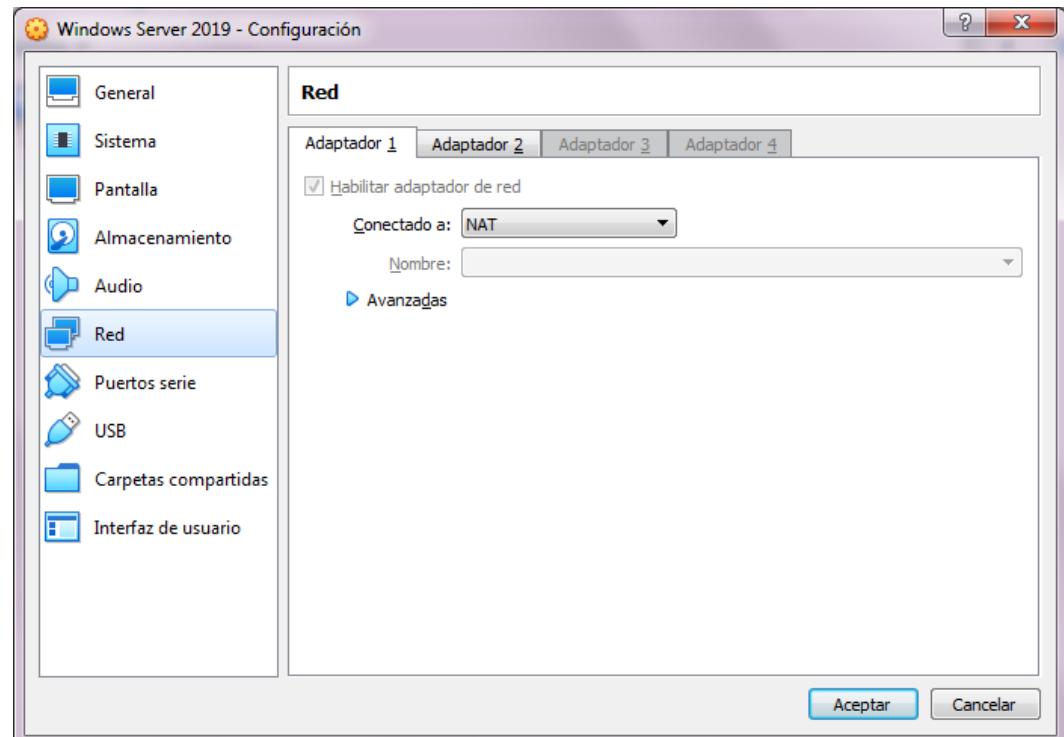


## 5.2. Configuració de la IP del servidor

Per a veure la configuració de xarxa, el més ràpid és escriure a "executar" o "buscar": ncpa.cpl

Així quedaría la configuració de les targetes de xarxa del servidor:

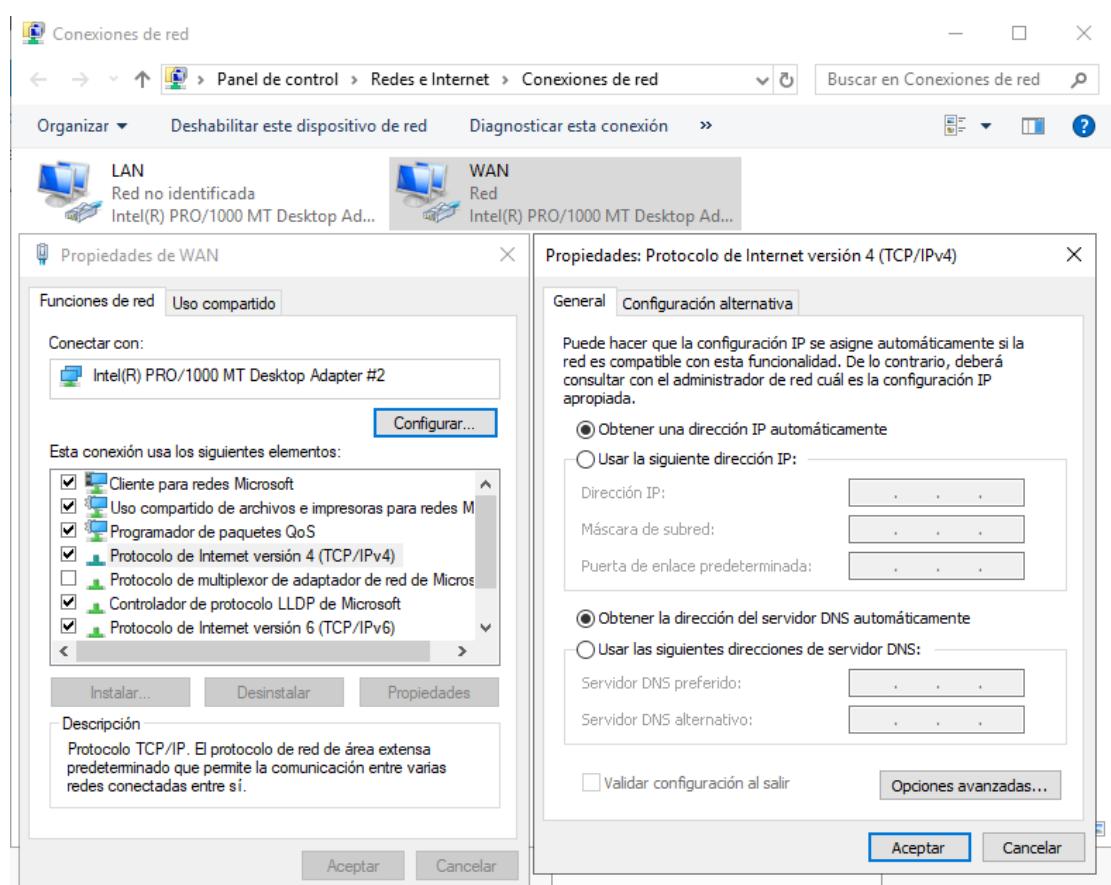
a) Per al cas de la **targeta de xarxa amb accés a la WAN**:



Ens assegurem que en VirtualBox estiga en manera "NAT" (a través d'aquesta targeta es connectarà a internet, és a dir a la WAN, el servidor)

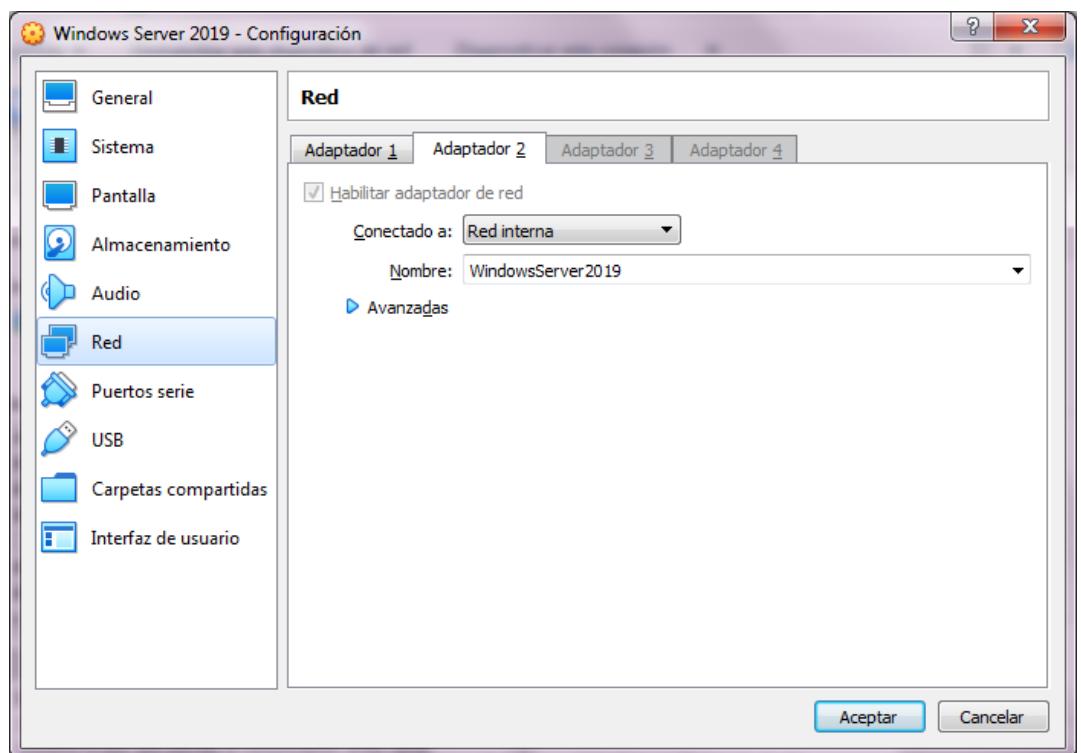
En connexions de xarxa, li canviarem el nom a aquesta connexió i li posarem "WAN" per a identificar-la més fàcilment.

Com la IP l'obtindrà automàticament, no modifiquem res de les propietats del TCP/IP.



b) Per al cas de la **targeta de xarxa amb accés a la LAN**:

Ens assegurem que en VirtualBox estiga en manera "Xarxa Interna" (a través d'aquesta targeta es connectarà a la LAN)

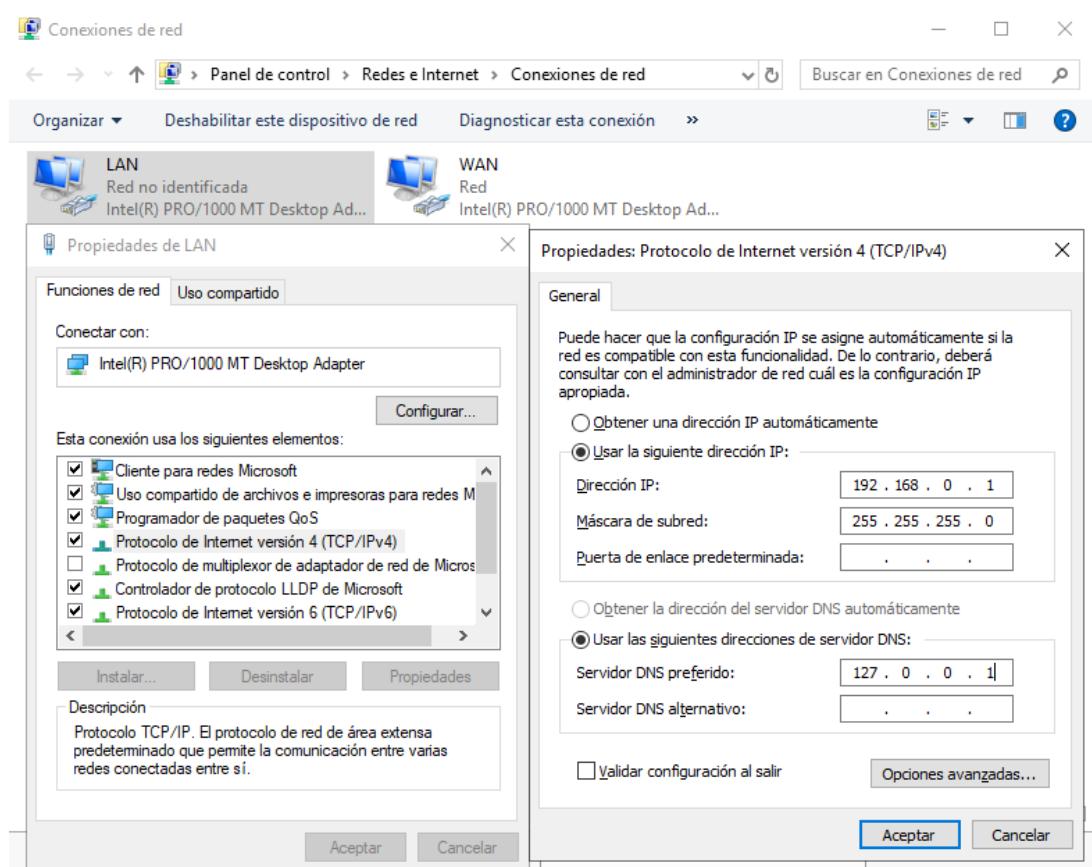


En connexions de xarxa, li canviarem el nom a aquesta connexió i li posarem "LAN" per a identificar-la més fàcilment.

És en aquesta connexió de xarxa on hem de configurar una IP fixa. En aquest exemple, hem posat aquests valors:

- IP: 192.168.0.1
- MS: 255.255.255.0

Atés que instal·larem en el nostre servidor el servei de DNS, podem posar ja el valor 127.0.0.1 o esperar que en el procés d'instal·lació d'Active Directory l'afija automàticament.



## instal·lar en Windows Server 2019: Active Directory, DNS, encaminament, DHCP

Durant el curs, aprendrem a instal·lar i configurar diversos serveis de Windows Server. Concretament, en aquest tema coneixerem els següents:

- **Active Directory/Directorí Actiu:** permet organitzar, controlar i administrar centralitzadament els usuaris i recursos d'una xarxa. Quan un usuari s'autentifica en un domini, té disponibles tots els recursos donats d'alta en aquest domini. La gestió d'aquest domini es realitza de forma centralitzada, ja que tota la informació es troba en una base de dades emmagatzemada en el Controlador de Domini (DC).
- **DNS:** permet mantenir una equivalència entre un nom i la seua adreça IP. Per exemple , el nom [www.elseñordelosanillos.es](http://www.elseñordelosanillos.es) equival a 64.190.62.111
- **Encaminament:** permet a un servidor actuar com a encaminador per a permetre la comunicació entre dues o més xarxes. Per exemple LAN ↔ WAN
- **DHCP:** permet assignar automàticament la configuració IP dels equips clients de la xarxa. Aquest servei és molt important, ja que facilita la connexió dels equips a la xarxa. Per exemple , quan un portàtil es connecta a una xarxa, obté la seua configuració IP a través d'un servidor DHCP.

## 7. Instal·lació dels serveis d'Active Directory i de DNS: creació d'un domini

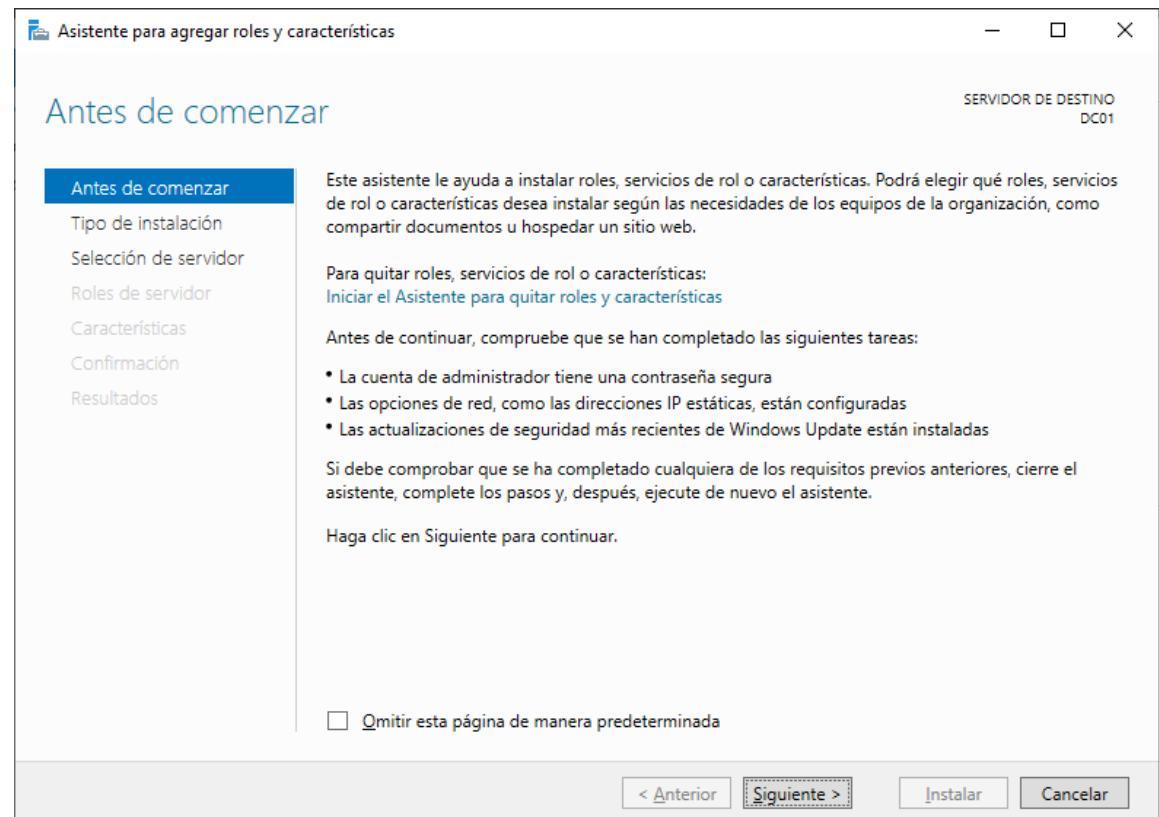
Per a instal·lar les funcions de Controlador de Domini, podríem intentar executar `dcpromo`, com féiem en Windows Server 2008 i anteriors. No obstant això , si ho fem, obtindrem una fallada com el següent:



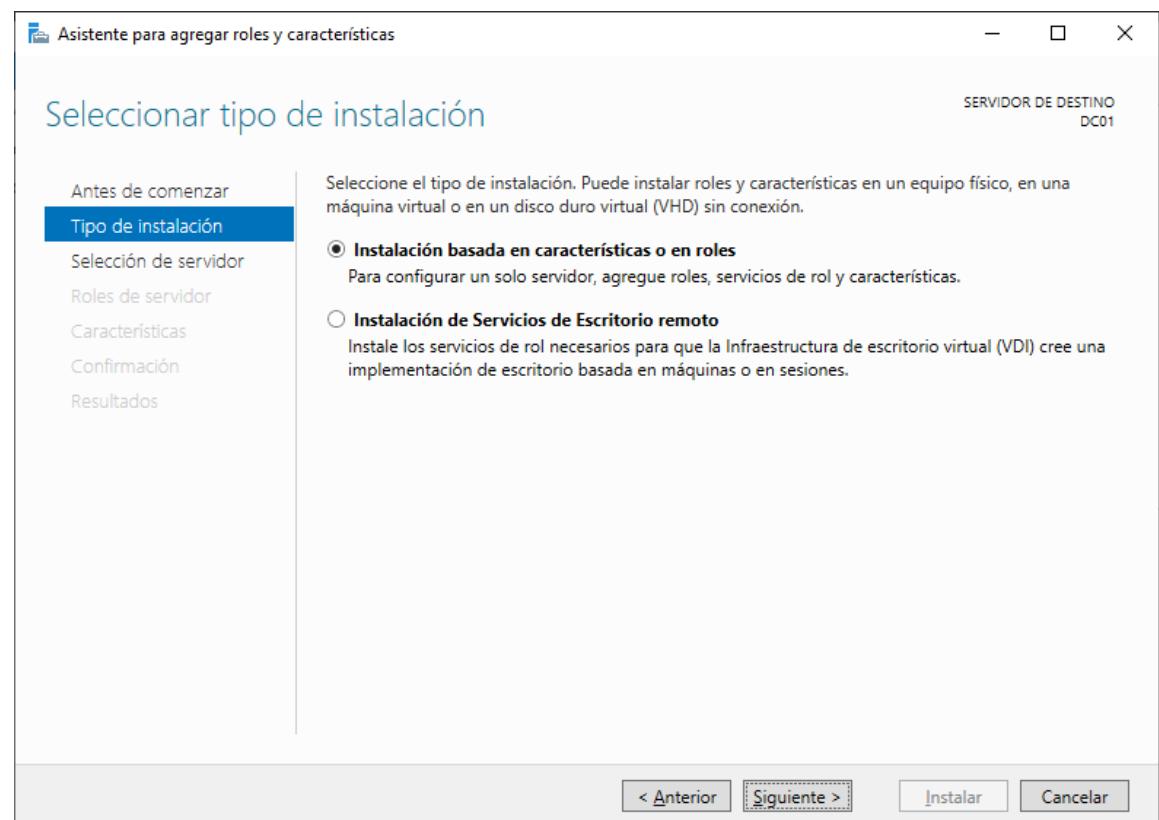
En Windows Server 2012/2016/2019/2022, per a instal·lar els serveis de domini, obrirem l'administrador del servidor i accedirem a l'opció 'Agregar roles y características'.



Se'n obrirà un assistent que ens permetrà agregar (o obrir l'assistent per a llevar) rols i característiques.

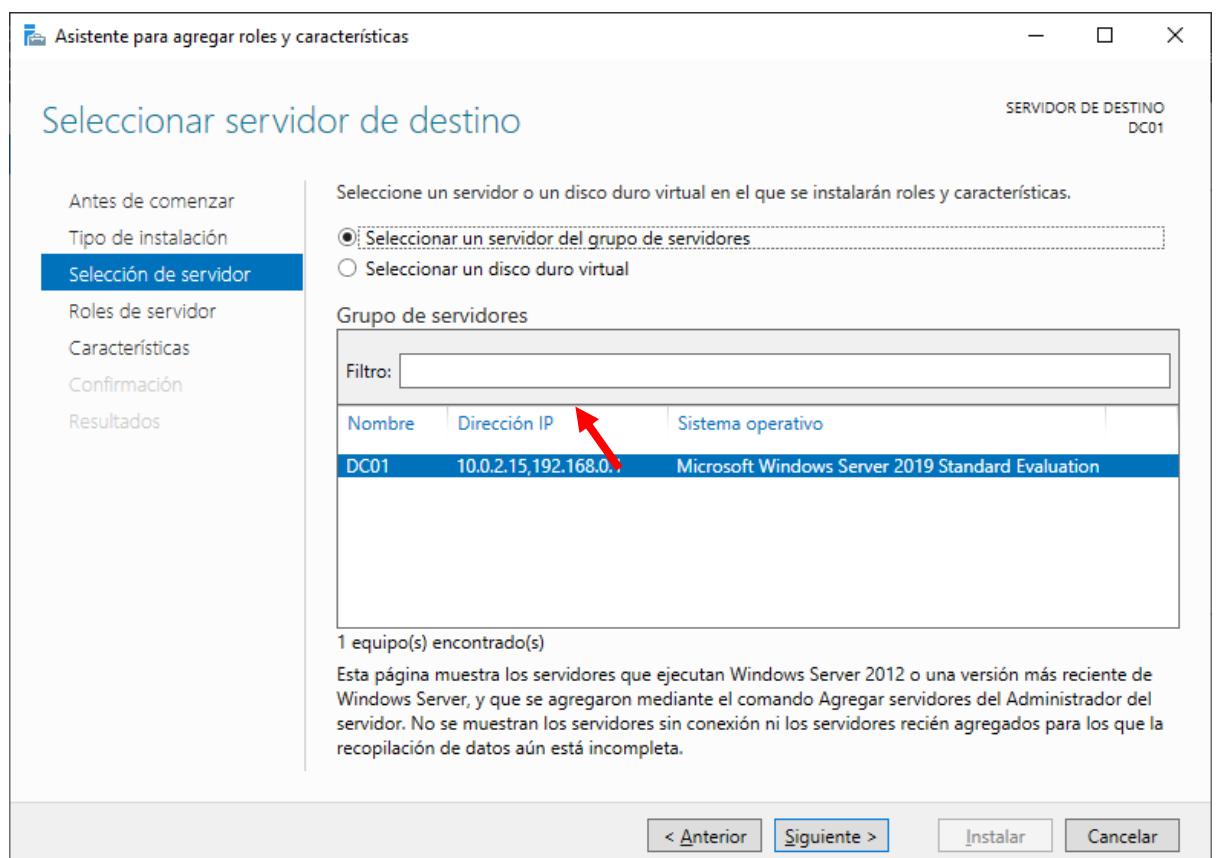


Com configurarem un únic servidor, indicarem que la instal·lació estarà basada en característiques o en rols.

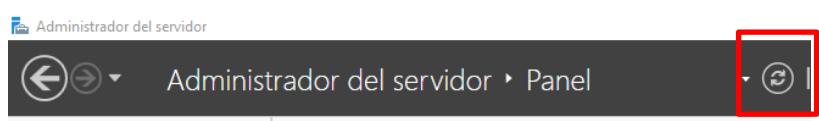


A continuació seleccionarem l'únic servidor de destí que tenim disponible.

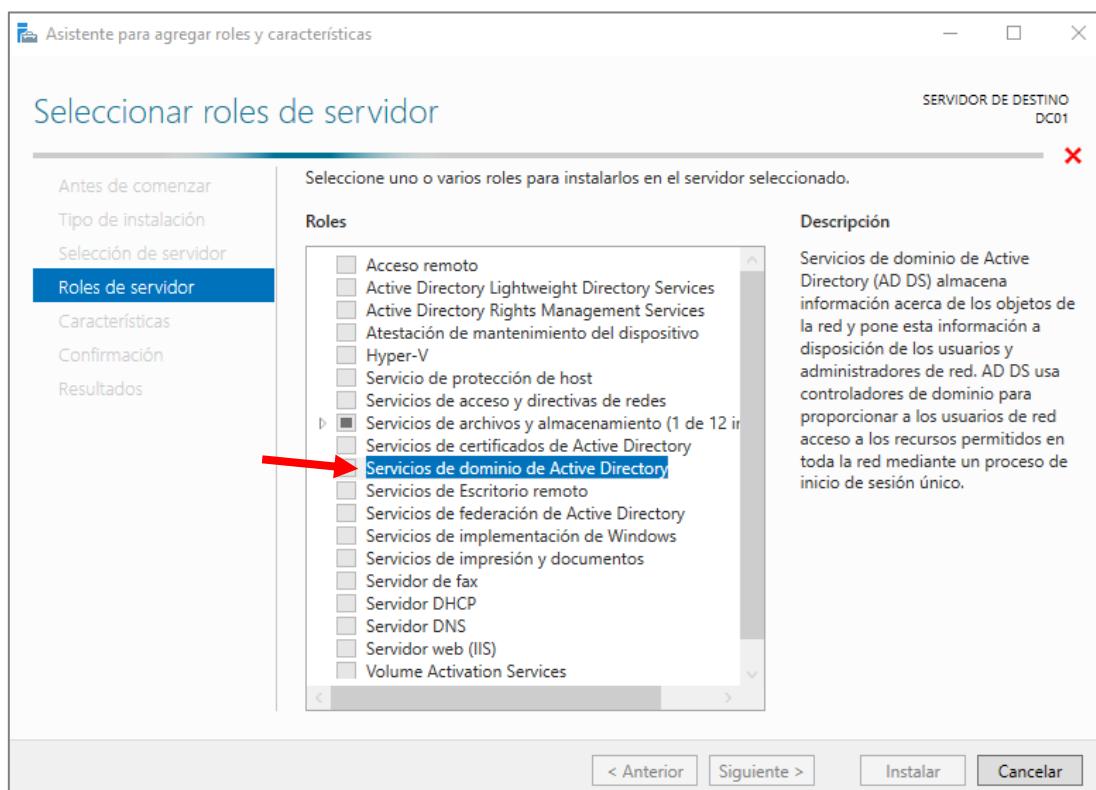
Fixeu-vos que ja apareix amb el nou nom i amb la nova IP assignada.



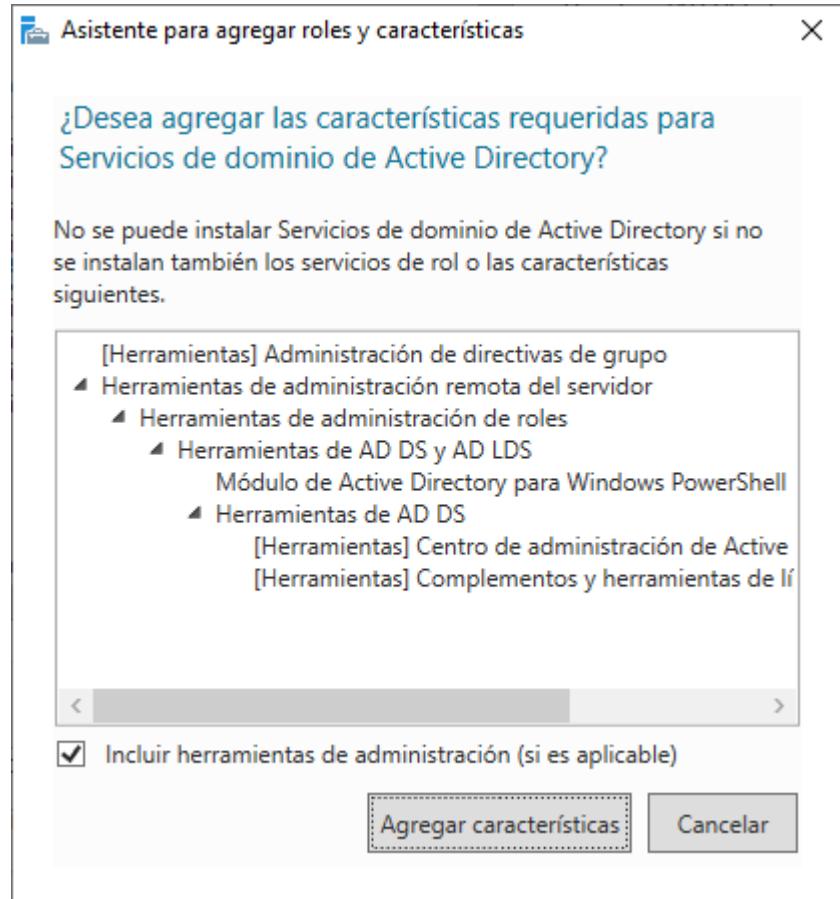
Atenció: Si en el pas anterior no us posa la IP fixa assignada (192.168.0.1), cancel·leu el procés i feu clic en el botó 'Actualitzar Panell' del 'Administrador del Servidor' i torneu a intentar-lo.



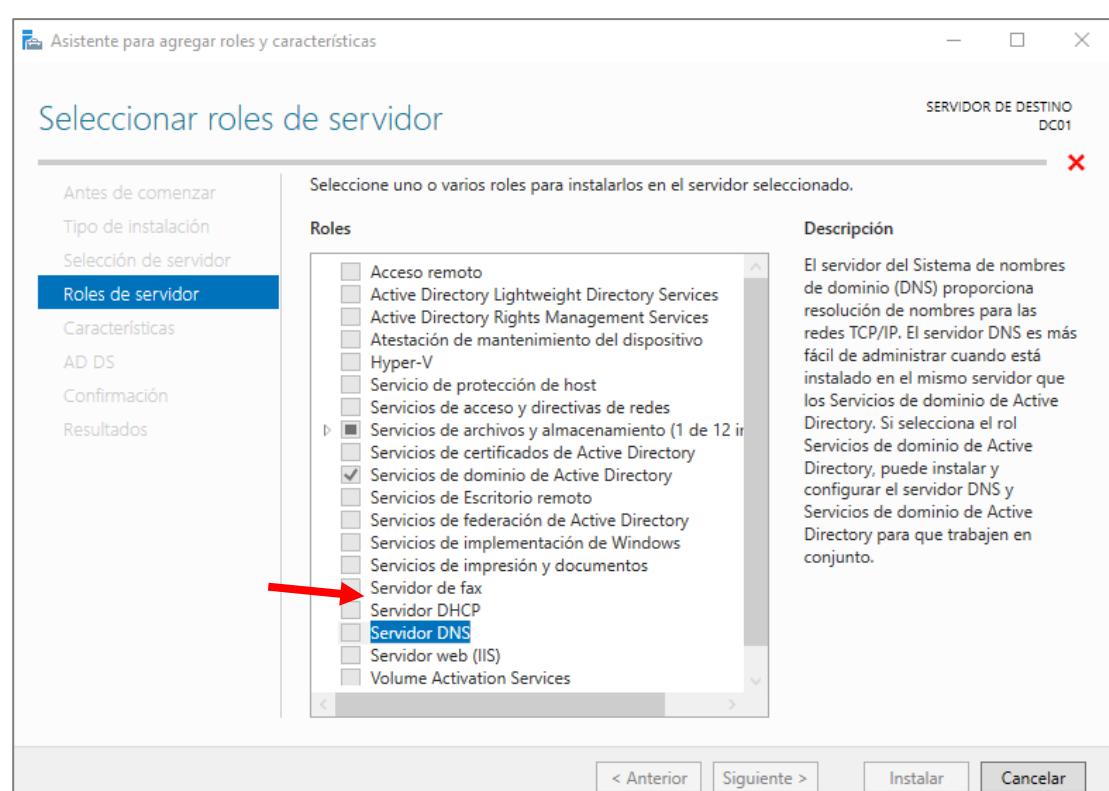
A continuació , se ens mostraran els rols instal·lables en el nostre equip, seleccionarem els '**Serveis de domini d'Active Directory**'.



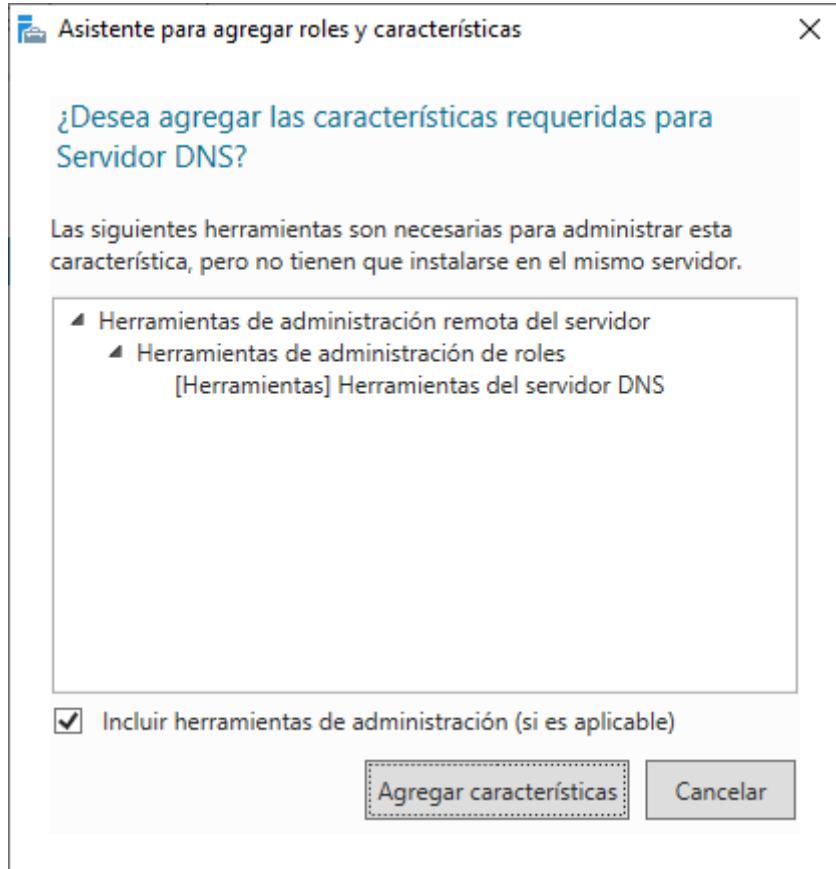
A continuació se'n obrirà una finestra indicant que hem d'instal·lar també una sèrie de cada característica d'Active Directory. Premerem a 'Aregar característiques'.



Com també volem implementar el **servidor DNS** en el nostre equip, el seleccionarem també en el menú de rols del servidor.



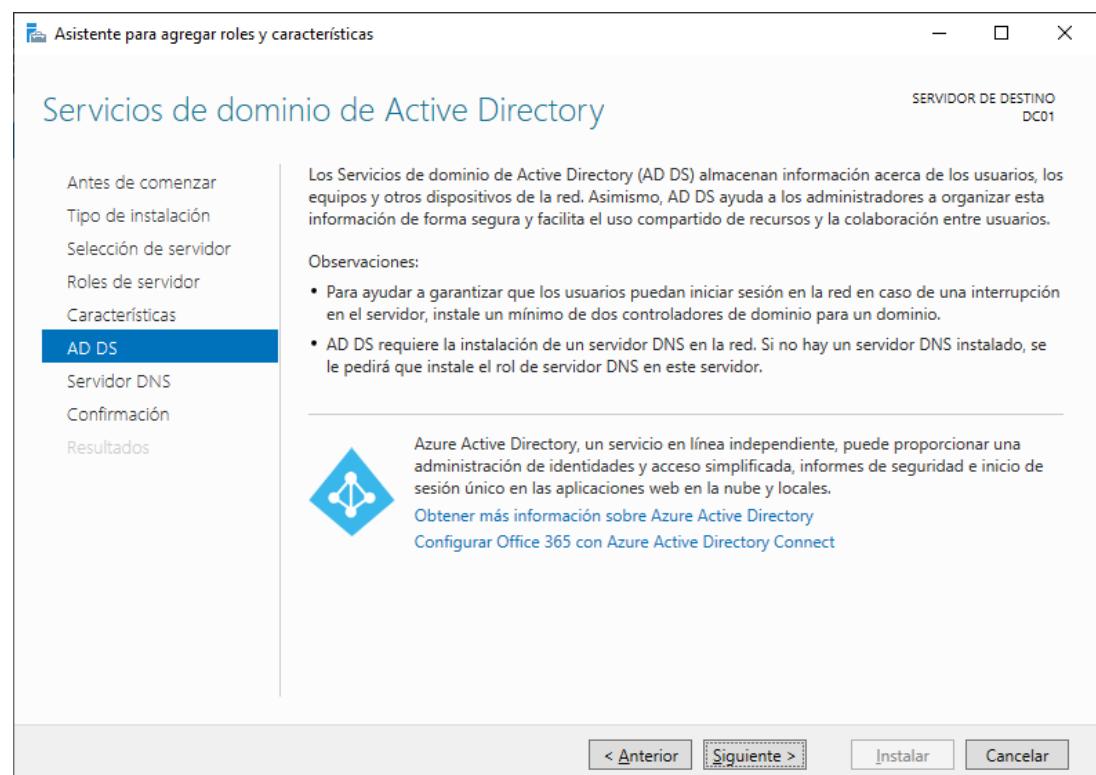
Ens demanarà la següent confirmació i farem clic en 'Agregarem característiques'.



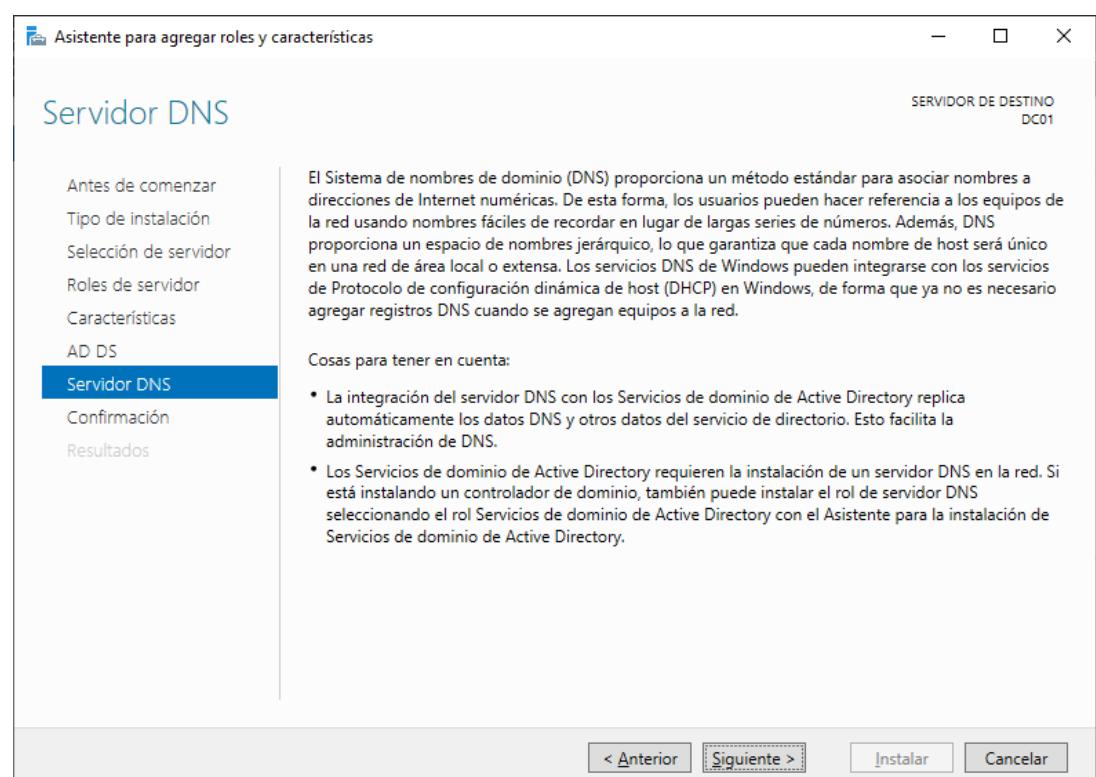
En el següent pas de l'assistent se'n indicarà que també hem d'instalar les característiques de '**Administració de directives de grup**' (element clau per a l'administració d'una estructura centralitzada gestionada per Active Directory).

The screenshot shows the 'Seleccionar características' (Select Features) step of the wizard. The title bar says 'Asistente para agregar roles y características'. The left sidebar shows navigation steps: 'Antes de comenzar', 'Tipo de instalación', 'Selección de servidor', 'Roles de servidor', 'Características' (highlighted with a blue background), 'AD DS', 'Servidor DNS', 'Confirmación', and 'Resultados'. The main area has a header 'Seleccione una o varias características para instalarlas en el servidor seleccionado.' and a 'Características' table. The table lists various features with checkboxes. Several checkboxes are selected, including 'Administración de almacenamiento basada en est...' (unchecked), 'Administración de directivas de grupo' (checked and highlighted in blue), 'Almacenamiento mejorado' (unchecked), 'Asistencia remota' (unchecked), 'BranchCache' (unchecked), 'Calidad de servicio de E/S' (unchecked), 'Características de .NET Framework 3.5' (unchecked), 'Características de .NET Framework 4.7 (2 de 7 instaladas)' (checked), 'Cifrado de unidad BitLocker' (unchecked), 'Cliente de impresión en Internet' (unchecked), 'Cliente para NFS' (unchecked), 'Clúster de conmutación por error' (unchecked), 'Compatibilidad con WoW64 (Instalado)' (checked), 'Compatibilidad de Hyper-V con Host Guardian' (unchecked), 'Compresión diferencial remota' (unchecked), 'Containers' (unchecked), 'Copias de seguridad de Windows Server' (unchecked), 'Data Center Bridging' (unchecked), and 'Desbloqueo de redes con BitLocker' (unchecked). The 'Descripción' column provides a detailed explanation for the selected feature. At the bottom, there are buttons for '< Anterior', 'Siguiente >', 'Instalar' (highlighted with a dashed border), and 'Cancelar'.

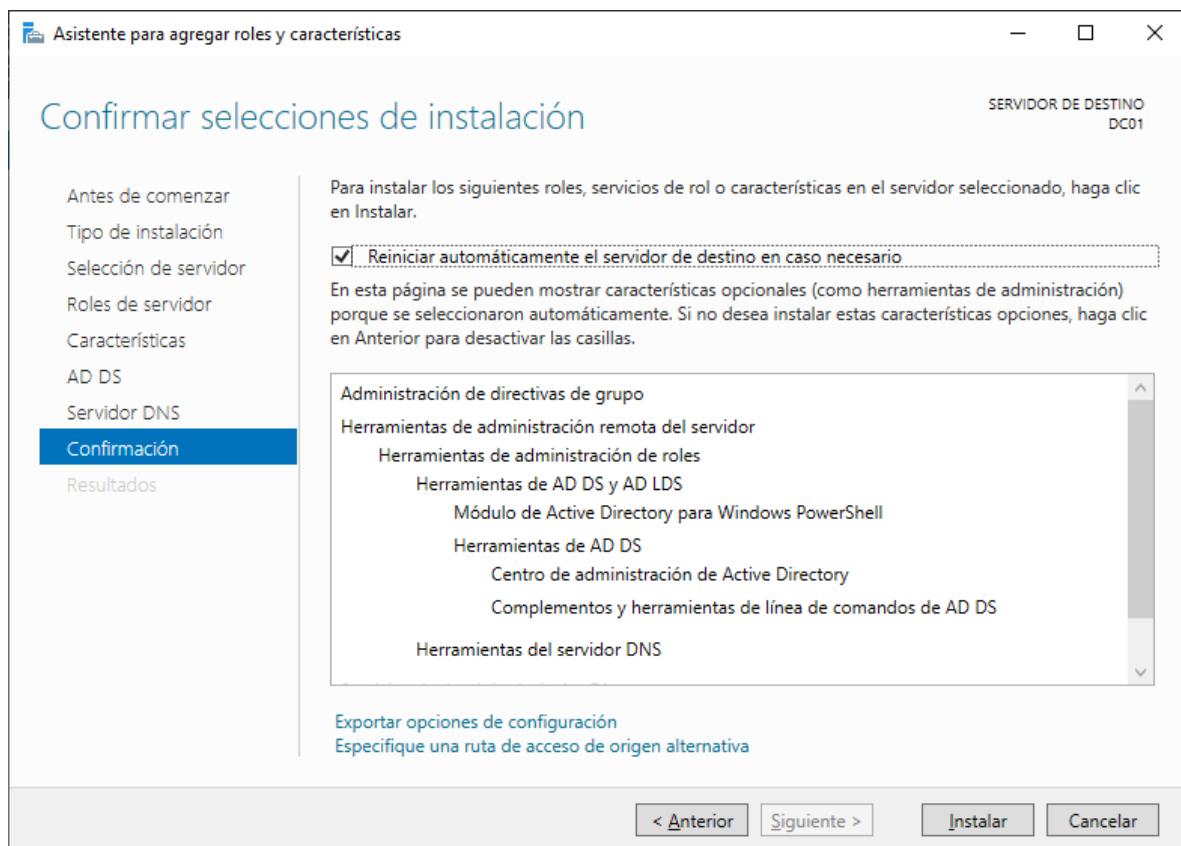
A continuació , se'ns mostraran unes observacions relacionades amb els Serveis de domini d'Active Directory, com la **recomanació d'instal·lar també un controlador de domini de suport**, la **instal·lació d'un DNS** -si no existeix ja-, i se'ns advertirà que també s'instal·laran **les funcions del Distributed File System (DFS)**, que permet una optimització del servei d'emmagatzematge de fitxers.



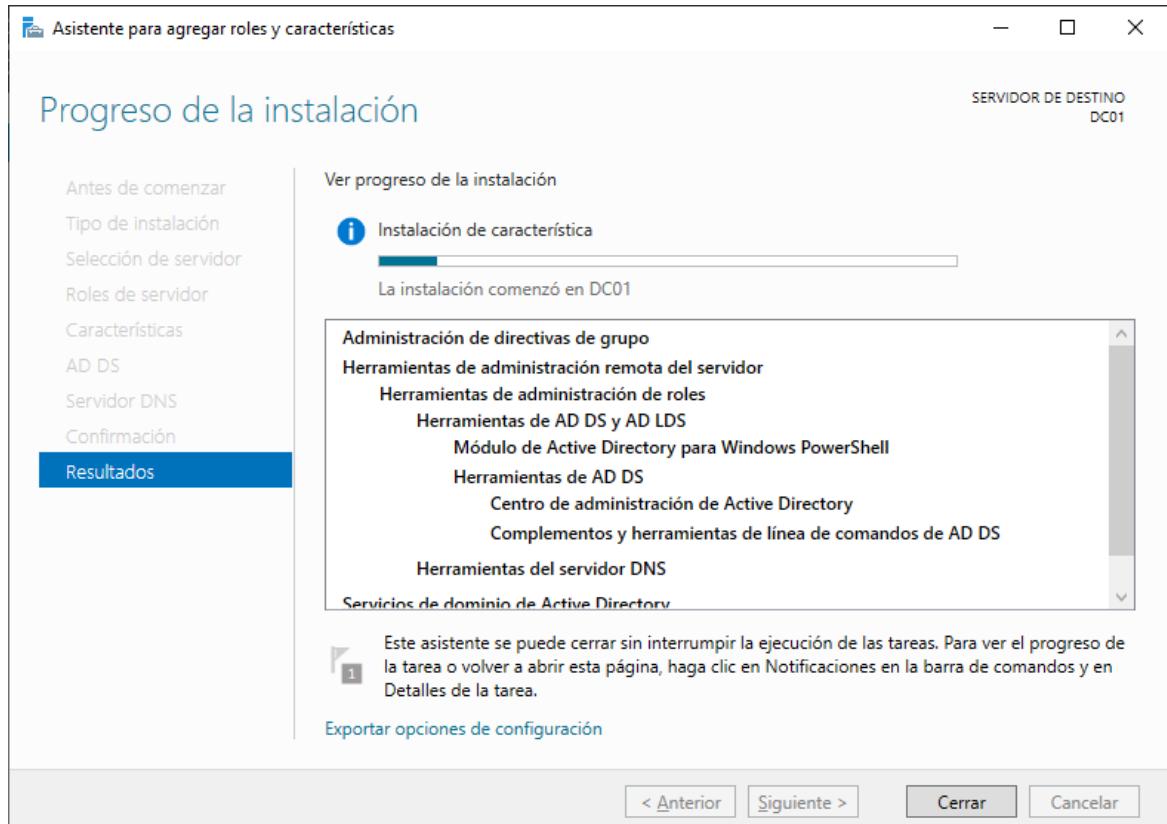
De la mateixa manera que en el cas anterior, també se'ns mostraran unes observacions a tindre en compte durant la instal·lació del DNS.



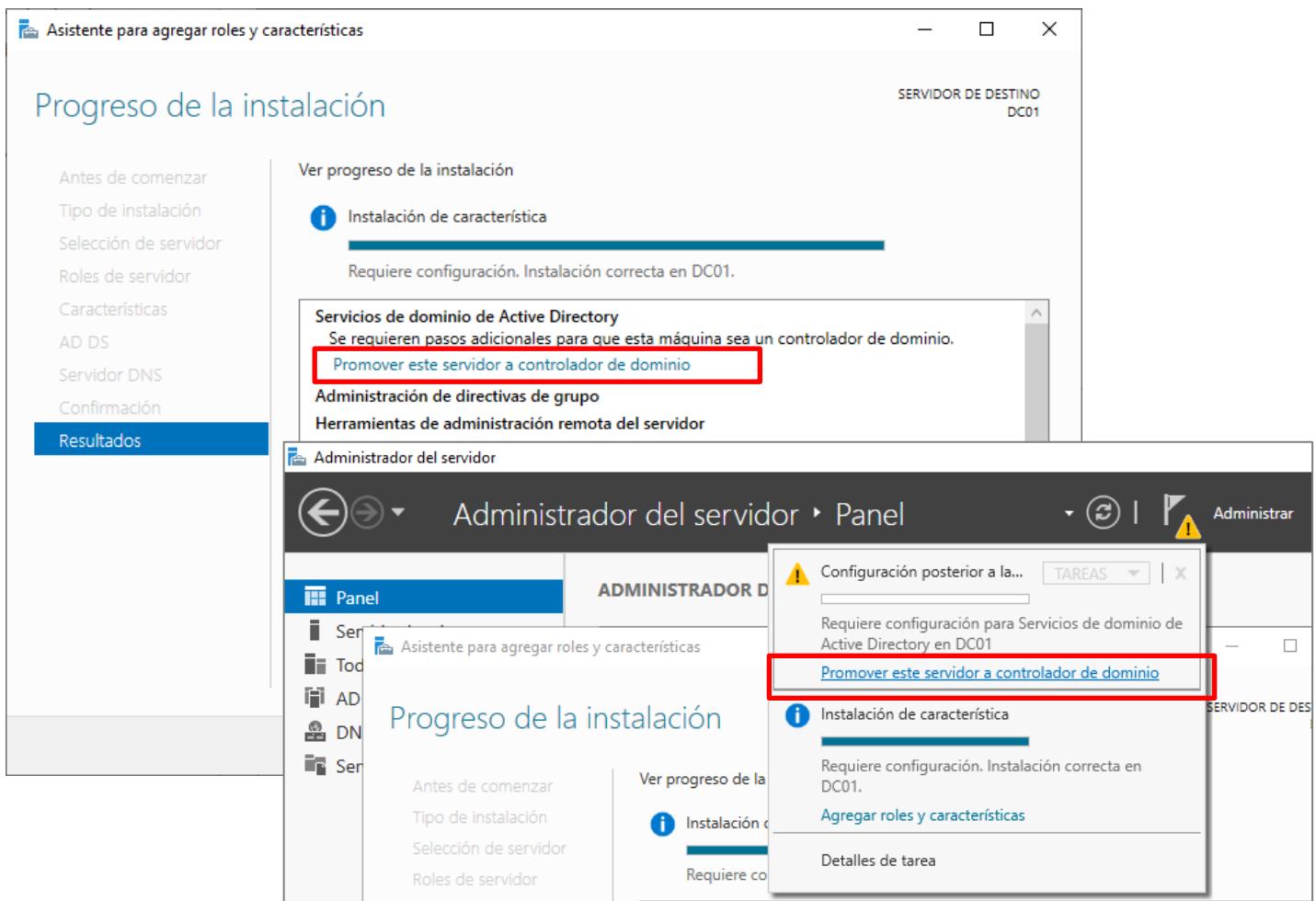
Per a concluir el procés d'instalació (que no de configuració) dels serveis seleccionats, se'n mostrarà un resum de totes les funcions que s'instal·laran, i se'n demanarà que confirmem les accions a realitzar. Opcionalment, marcarem la casella de permetre el reinici automàtic del sistema durant la instalació dels serveis.



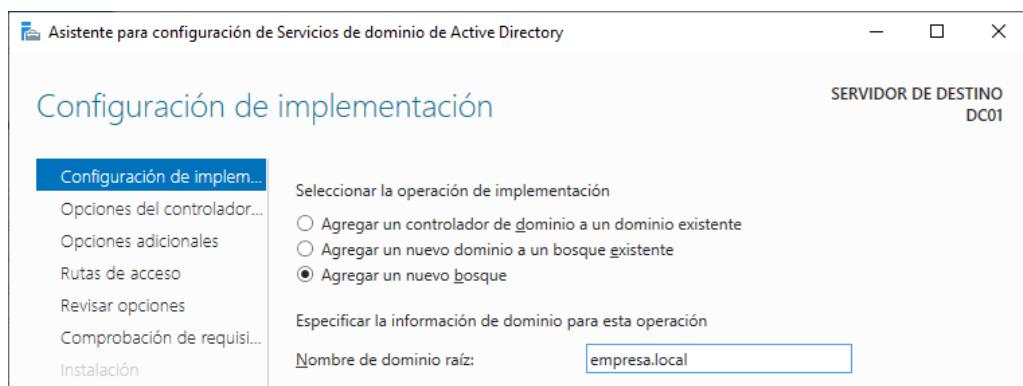
En la següent imatge es mostra la finestra de progrés de la instalació, la qual pot ser tancada mentre es duu a terme la instalació perquè puguem continuar fent les tasques d'administració del servidor, si fora necessari.



Una vegada que haja conclòs el procés d'instal·lació , podrem observar com tant en el resultat de la instal·lació del rol com en la "bandereta" de notificacions de l'administrador del servidor apareixerà un missatge indicant que tenim pendent la configuració del Directori Actiu. Per a continuar amb la configuració, farem clic a '**Promoure aquest servidor a controlador de domini**'.



I s'obrirà un assistent que ens permetrà configurar aquest servei. En el curs anterior vam veure les diferents estructures que podíem crear amb el Directori Actiu. Com en aquest cas, encara no existeix cap domini en la nostra xarxa, seleccionarem l'opció 'Aregar un nou bosc'. Com a nom de domini arrel proposeu el següent:  
empresa.local



En la següent finestra de l'assistent seleccionarem el nivell funcional, tant del bosc, com del domini. Windows Server 2019 permet treballar com a màxim amb el nivell funcional de Windows Server 2016, per la qual cosa triarem aqueixa opció. (En cas contrari, per exemple, si férem proves d'integració amb controladors de domini Windows Server 2008, seleccionarem 2008 com a nivell funcional).

De la mateixa manera introduirem una contrasenya d'administrador si hem de arrancar el servidor en 'Manera de recuperació' ([DSRM](#)).

A continuació ens apareixerà el clàssic avís de la impossibilitat de crear una delegació per al servidor DNS, ja que encara no està posat en marxa i no podem establir una referència del tipus ns1.empresa.local->127.0.0.1

Premereu 'Següent' i durant el procés de post-instal·lació es crearan les delegacions necessàries.

Introduirem el nom del domini NetBIOS, el qual sol corresponder a la primera part del nom del domini, en aquest cas EMPRESA. Igual que el servei WINS, el servei NetBIOS es manté per a garantir la compatibilitat amb sistemes antics.

Indicarem les rutes dels arxius propis de gestió del Directori Actiu. Si no tenim unes preferències específiques, deixarem les propostes que ens apareixen per defecte.

A punt de concloure el procés, podrem revisar les opcions de configuració que hem introduït. En aquesta finestra de l'assistent, és molt interessant adonar-se que se'n proporciona un script de PowerShell que ens permetria executar totes les accions que hem realitzat fins ara.

**Opciones adicionales**

Verifique el nombre NetBIOS asignado al dominio y cámbielo si es necesario

**Rutas de acceso**

Especificar la ubicación de la base de datos de AD DS, archivos de registro y SYSVOL

Carpeta de la base de datos: C:\Windows\NTDS  
Carpeta de archivos de registro: C:\Windows\NTDS  
Carpeta SYSVOL: C:\Windows\SYSVOL

**Revisar opciones**

Configuración de implementación: Configura este servidor como el primer controlador de dominio de Active Directory en un nuevo bosque.

Nombre del nuevo dominio: empresa.local

Nombre NetBIOS del dominio: EMPRESA

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Opciones adicionales:

- Catálogo global: Sí
- Servidor DNS: Sí

Esta configuración se puede exportar a un script de Windows PowerShell para automatizar instalaciones adicionales

**Comprobación de requisitos previos**

Todas las comprobaciones de requisitos previos se realizaron correctamente. Haga clic en 'Instalar' para comenzar la instalación.

Los requisitos previos deben validarse antes de instalar los servicios de dominio de Active Directory en el equipo

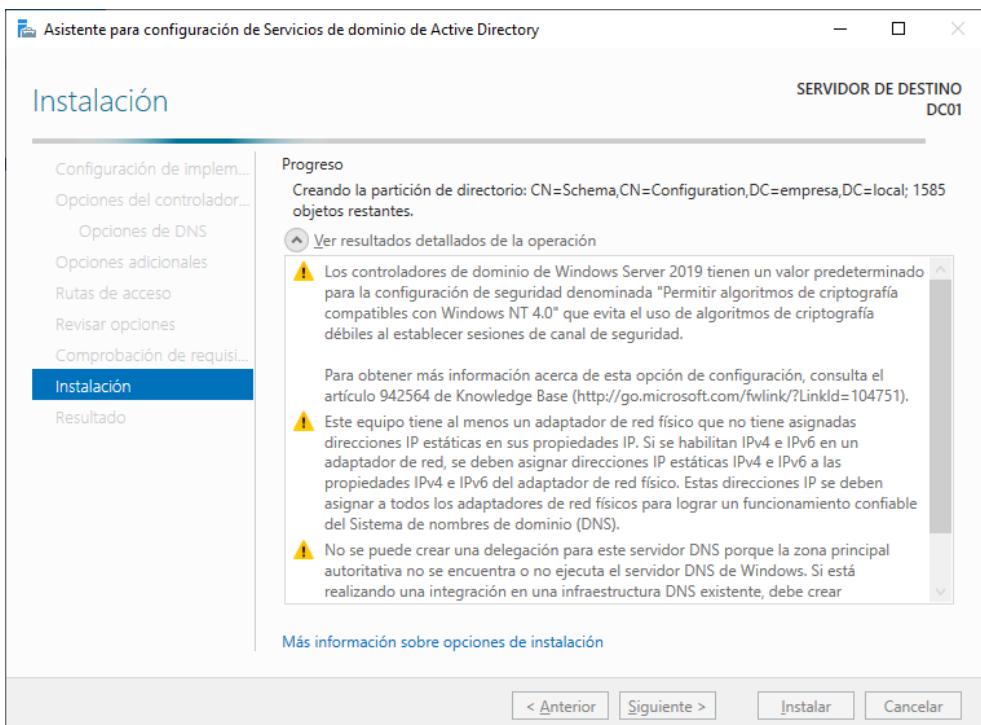
Ver resultados

- Los controladores de dominio de Windows Server 2019 tienen un valor predeterminado para la configuración de seguridad denominada "Permitir algoritmos de criptografía compatibles con Windows NT 4.0" que evita el uso de algoritmos de criptografía débiles al establecer sesiones de canal de seguridad.
- Este equipo tiene al menos un adaptador de red físico que no tiene asignadas direcciones IP estáticas en sus propiedades IP. Si se habilitan IPv4 e IPv6 en un adaptador de red, se deben asignar direcciones IP estáticas IPv4 e IPv6 a las interfaces.
- Si hace clic en Instalar, el servidor se reiniciará automáticamente cuando finalice la operación de promoción.

Finalment, començarà la

Si fem clic a 'Veure script', s'obrirà el bloc de notes amb la sintaxi necessària. Guardarem aquest fitxer, ja que més endavant el modificarem per a posar en marxa estructures de suport redundants amb Windows Server Core.

creació del Directori Actiu, després de fer clic a 'Instalar'.



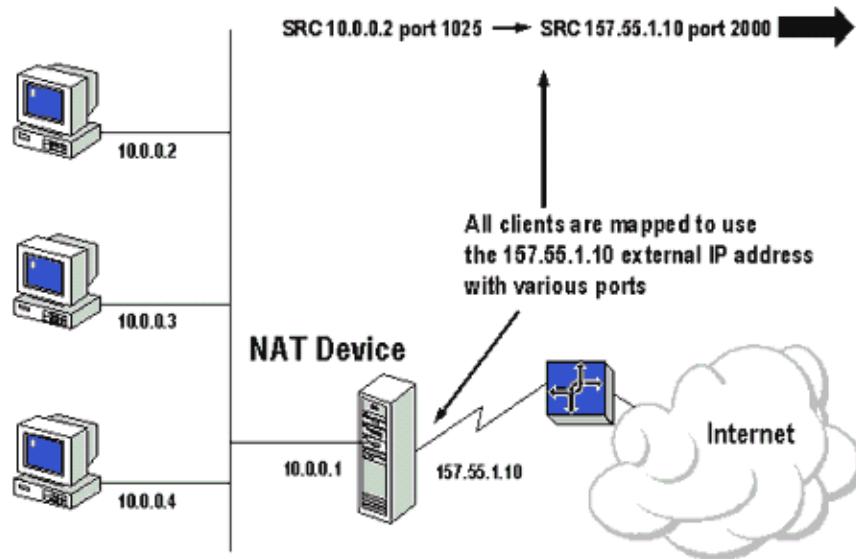
Després de reiniciar-se automàticament el servidor, podrem comprovar que l'entrada al mateix difereix, ja que ara ho farem amb el compte de l'Administrador del domini empresa.local



## 8. Instal·ació de l'servei d'encaminament.

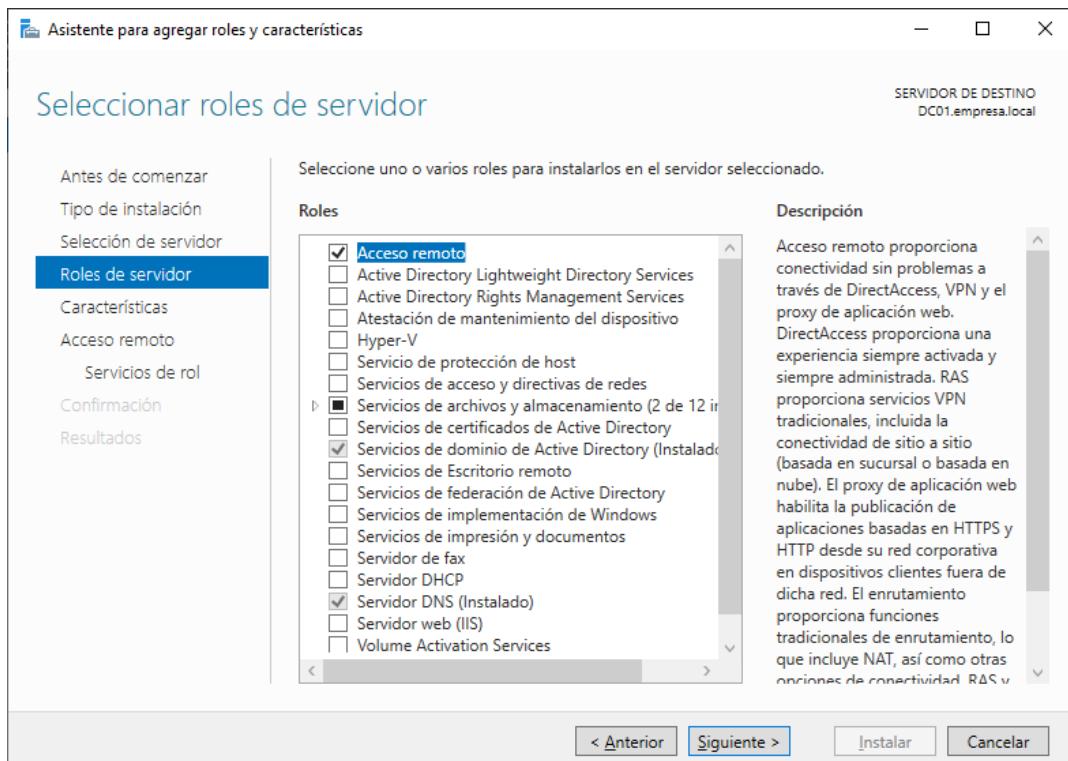
### 8.1. El servei d'encaminament.

El servei d'encaminament permet a un servidor actuar com a encaminador per a permetre la comunicació entre dues o més xarxes. Per exemple LAN  $\leftrightarrow$  WAN. Per tant, aquest servei ens permetrà que la xarxa interna puga tindre accés a internet a través del nostre Windows Server. Això és possible gràcies a NAT (Network Address Translation o traducció de direccions de xarxa).

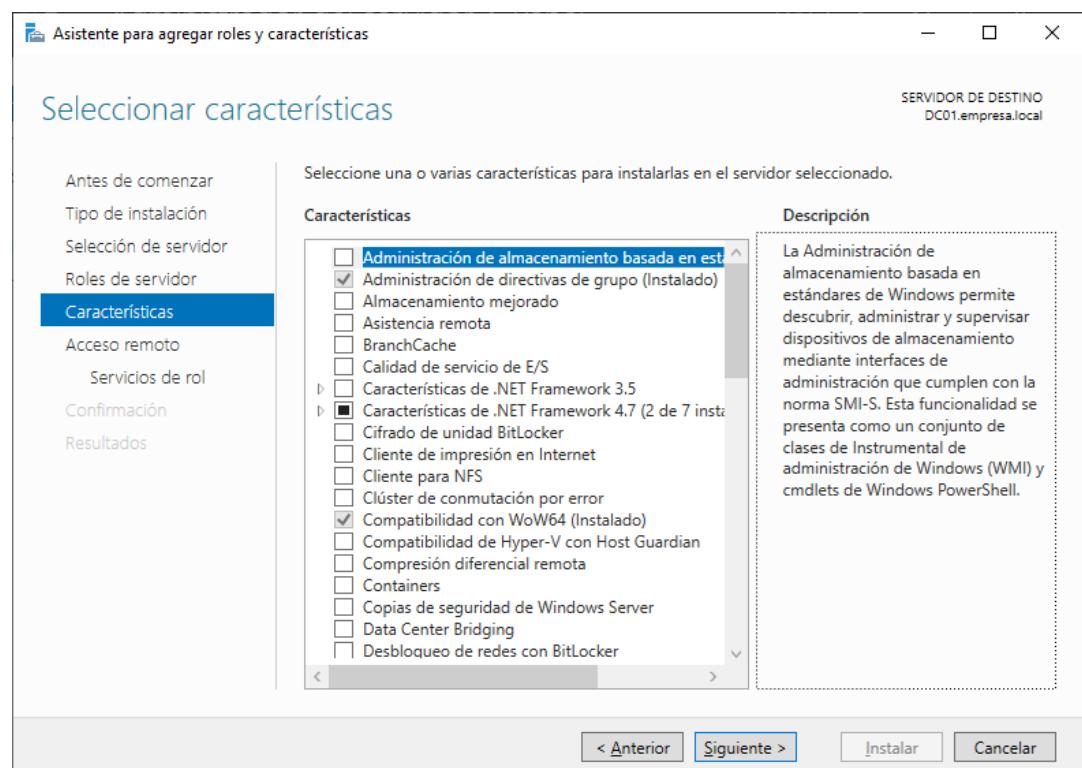


### 8.2. Instal·ació del servei d'encaminament.

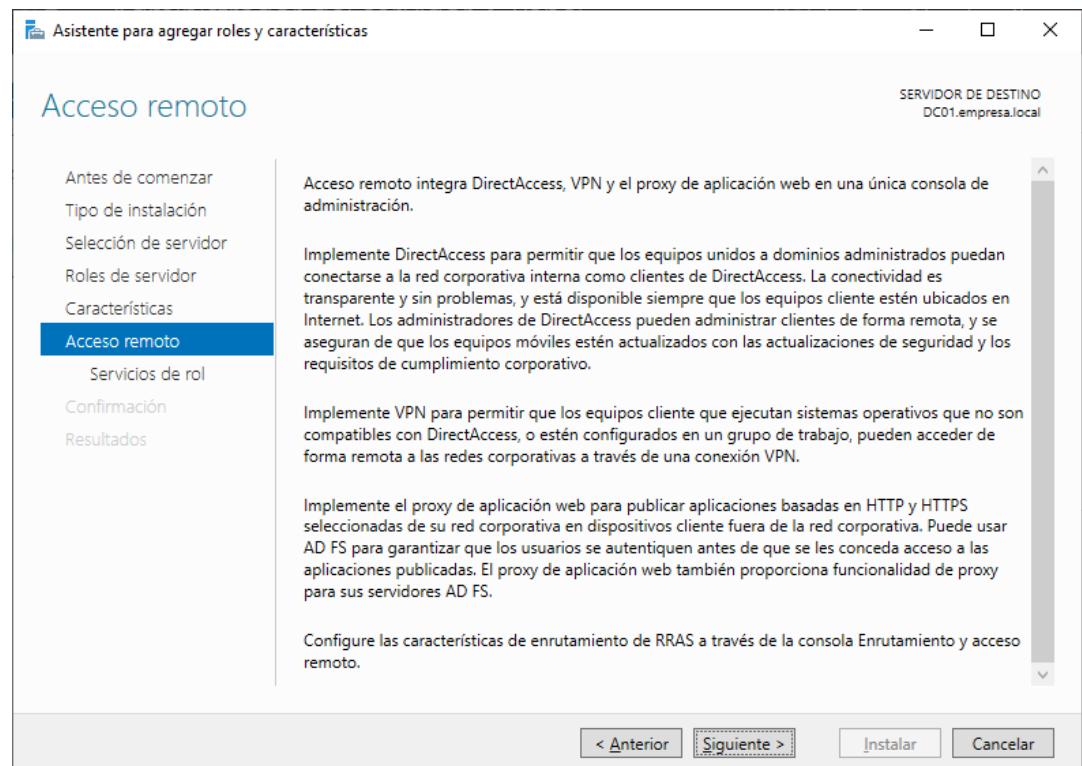
Per a instal·lar el servei DHCP anirem a "Agregar roles i característiques" del "Administrador del servidor" i seleccionarem el rol "Accés remot".



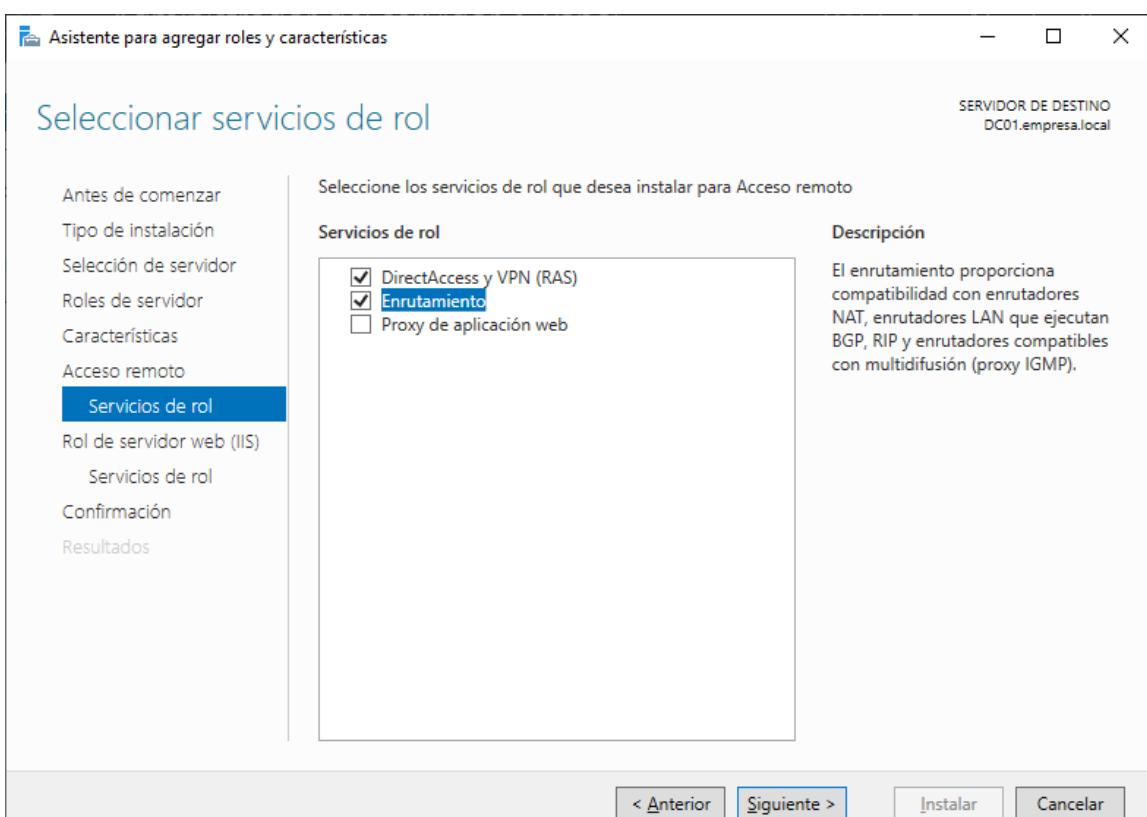
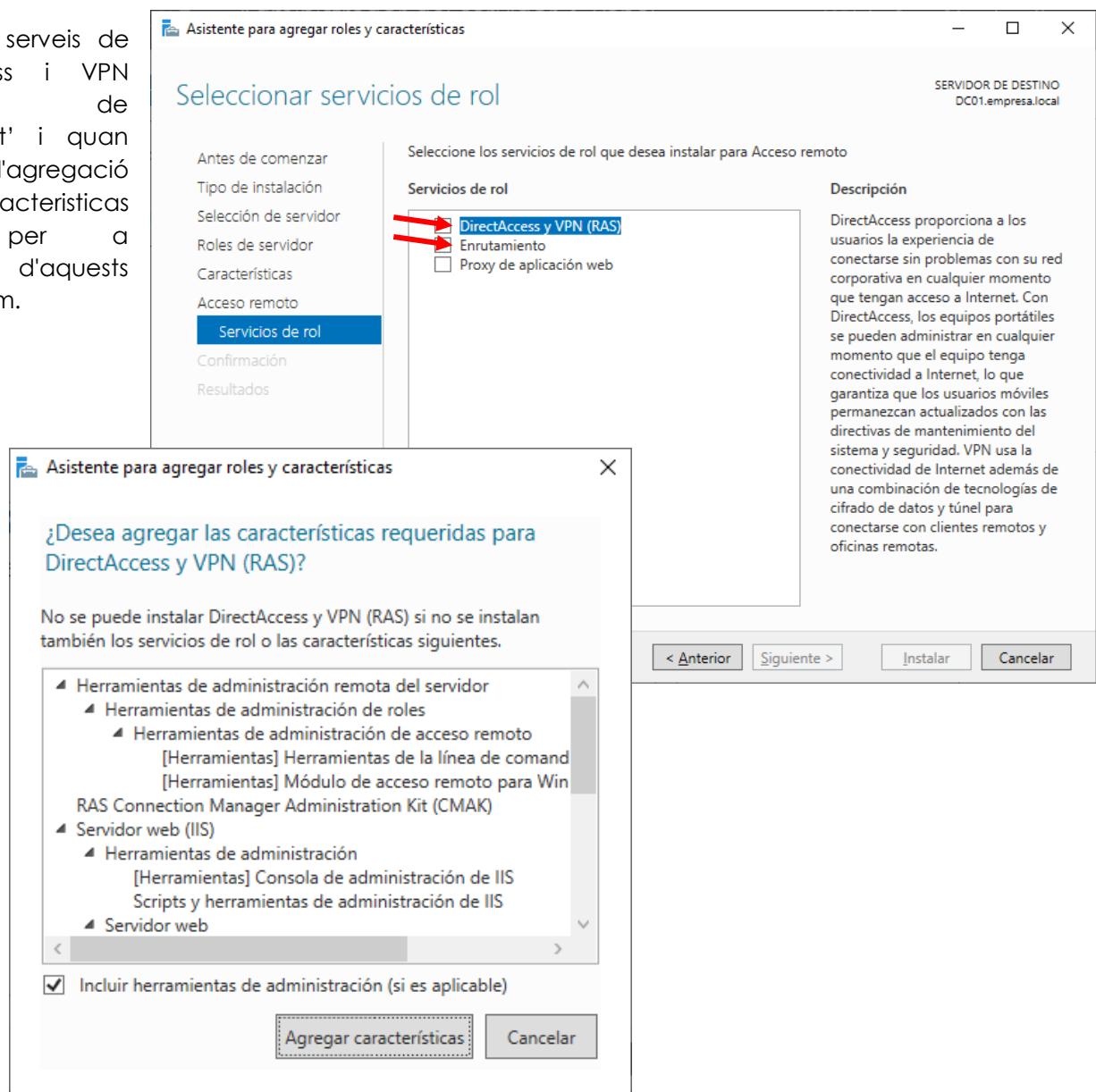
A continuació se'n obrirà una finestra indicant que hem d'instal·lar també una sèrie de característiques per a Accés Remot. Premerem en 'Següent'.



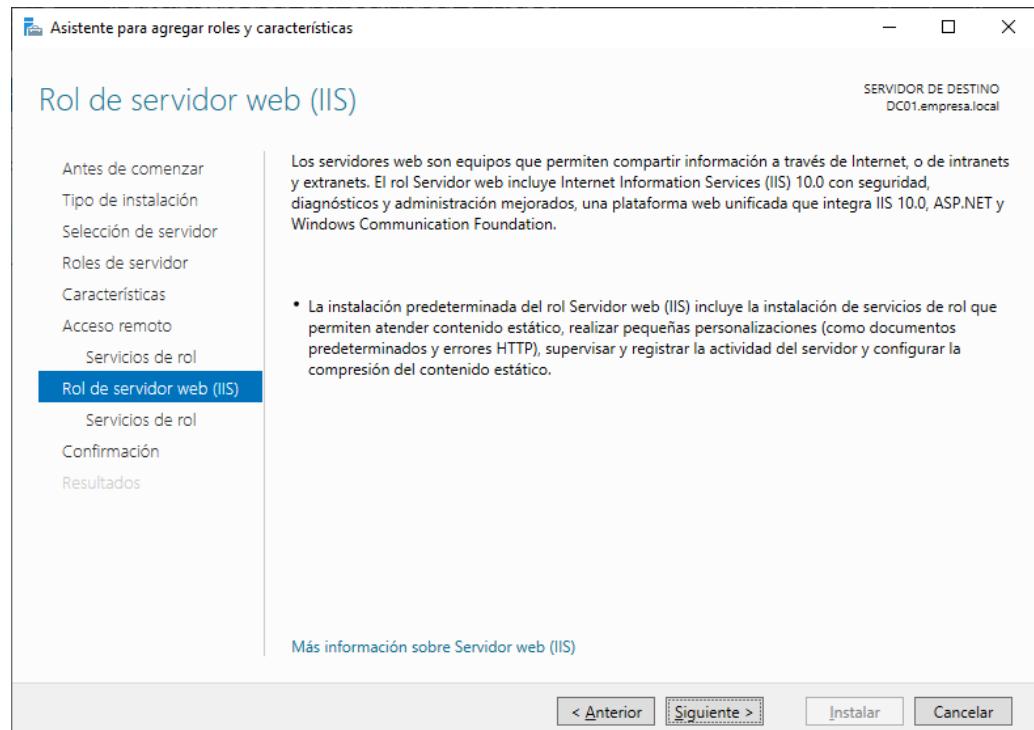
A continuació, se'n mostra una finestra amb informació sobre els serveis de rol que integren el rol de 'Accés remot':



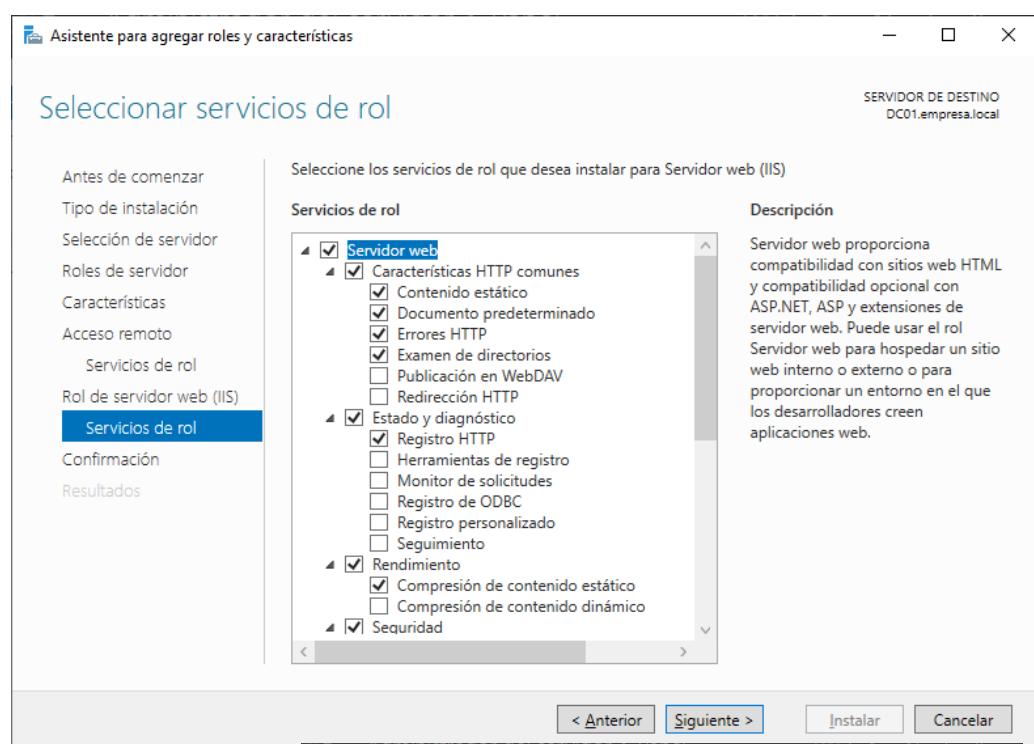
Marcarem els serveis de 'Direct Access i VPN (RAS)' i de 'Encaminament' i quan se'n sol·licite l'agregació de les característiques requerides per a cadascun d'aquests serveis, ho farem.



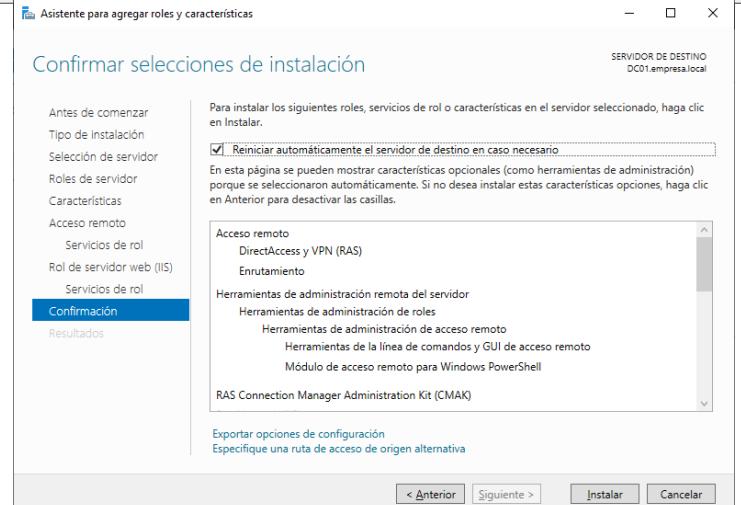
A continuació se'n obrirà una finestra indicant que hem d'instal·lar el rol de "Servidor web (IIS)". Premerem en 'Següent' i a 'Agregar características'.



A continuació , se'n mostraran unes observacions relacionades amb el rol de servidor web i ens sol·licitarà que indiquem quins serveis volem instal·lar. Deixarem les opcions indicades per defecte i premerem 'Següent'.

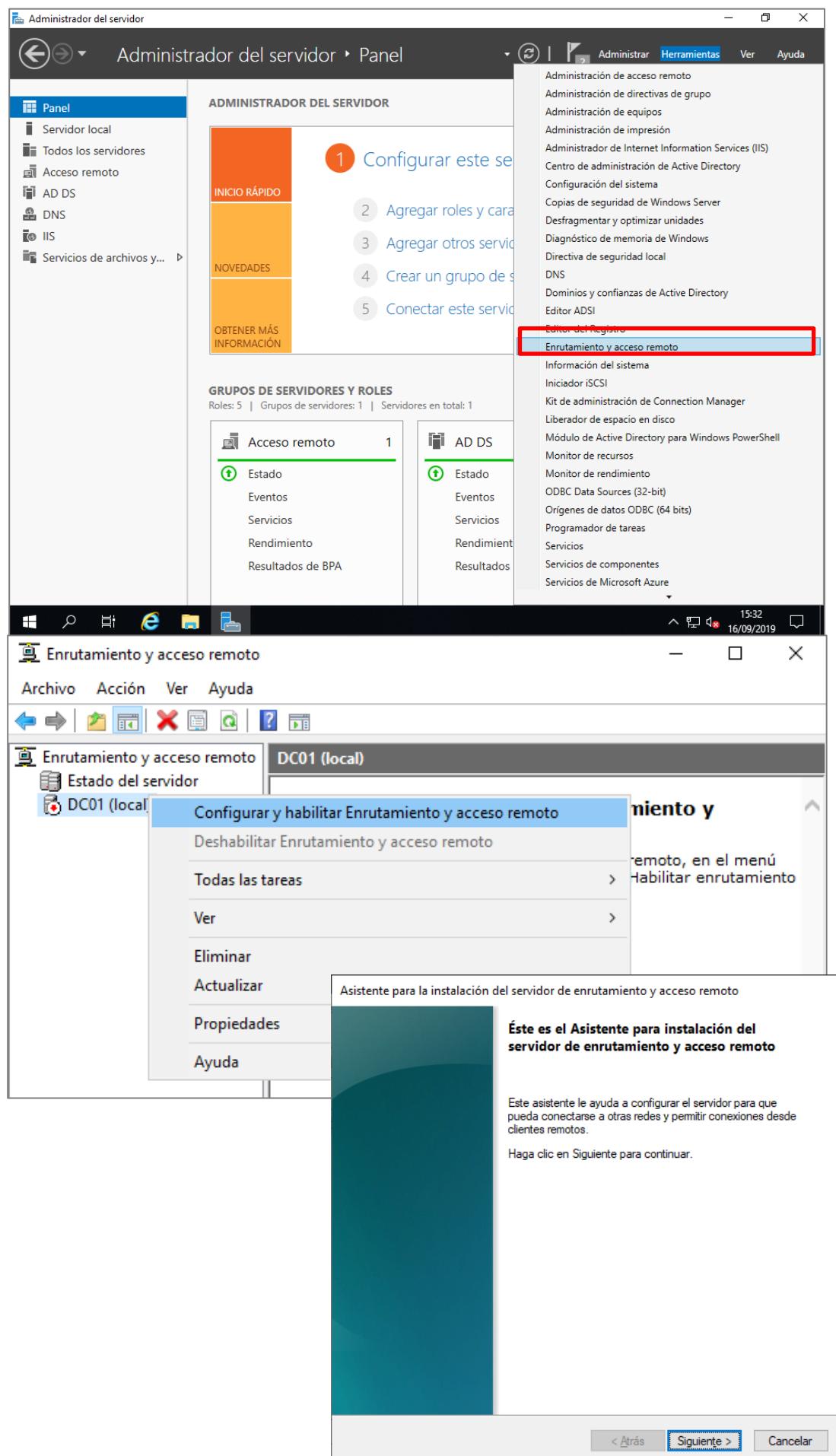


Per a concloure el procés d'instal·lació (que no de configuració) del servei seleccionat, se'n mostrarà un resum de totes les funcions que s'instal·laran , i se'n demanarà que confirmem les accions a realitzar prement a 'Instalar'. Opcionalment, marcarem la casella de permetre el reinici automàtic del sistema durant la instal·lació del servei.



### 8.3. Configuració del servei d'encaminament.

En "administrador del servidor" anirem a Eines  
→ Encaminament i accés remot



Seleccionarem el servidor DC01 i amb el botó dret del ratolí, triarem l'opció "Configurar i habilitar Encaminament i accés remot", després de la qual cosa se'ns obrirà un assistent.

A continuació , seleccionarem el servei de “NAT” (traducció de direccions de xarxa).

**Asistente para la instalación del servidor de enrutamiento y acceso remoto**

**Configuración**  
Puede habilitar cualesquier de las siguientes combinaciones de servicios o puede personalizar este servidor.

- Acceso remoto (acceso telefónico o red privada virtual)  
Permitir a clientes remotos conectarse a este servidor a través de una conexión de acceso telefónico o una conexión segura a Internet de red privada virtual (VPN).
- Traducción de direcciones de red (NAT)  
Permitir a clientes internos conectarse a Internet usando una dirección IP pública.
- Acceso a red privada virtual (VPN) y NAT  
Permitir que los clientes remotos se conecten a este servidor a través de Internet y que los clientes locales se conecten a Internet usando una sola dirección IP pública.
- Conexión segura entre dos redes privadas  
Conectar esta red a una red remota, como a una oficina sucursal.
- Configuración personalizada  
Seleccionar cualquier combinación de características disponibles en Enrutamiento y acceso remoto.

**Asistente para la instalación del servidor de enrutamiento y acceso remoto**

**Conexión a Internet NAT**  
Puede seleccionar una interfaz existente o crear una nueva interfaz de marcado a petición para equipos clientes a fin de conectarse a Internet.

- Utilizar esta interfaz pública para conectarse a Internet:  
**Interfaces de red:**

Nombre	Descripción	Dirección IP
LAN	Intel(R) PRO/1000 MT...	192.168.0.1
WAN	Intel(R) PRO/1000 MT...	10.0.2.15 (DHCP)

- Crear una conexión a Internet de marcado a petición  
Una interfaz de marcado a petición se activa cuando un cliente usa Internet. Seleccione esta opción si el servidor se conecta con un módem o usando el protocolo punto a punto a través de Ethernet. El Asistente para interfaz de marcado a petición se iniciará al final de este asistente.

**Asistente para la instalación del servidor de enrutamiento y acceso remoto**

**Finalización del Asistente para instalación del servidor de enrutamiento y acceso remoto**  
Ha completado con éxito el Asistente para instalación de Servidor de enrutamiento y acceso remoto.

Resumen:

NAT configurada para la siguiente interfaz de Internet:WAN  
NAT depende de servidores externos DNS y DHCP. Confirme que estos servicios están configurados correctamente.

Para habilitar servidores para responder a consultas de Internet, configure asignaciones de puerto y actualice su firewall.

Para cerrar el asistente, haga clic en Finalizar.

**< Atrás** **Finalizar** **Cancelar**

Finalment, ens mostrarà un resum de les configuracions seleccionades i farem clic a “finalitzar”.

**Enrutamiento y acceso remoto**

Archivo Acción Ver Ayuda

General

Interfaz	Tipo	Dirección IP
WAN	Dedicado	10.0.2.15
LAN	Dedicado	192.168.0.1
Interno	Interno	No disponible
Bucle invertido	Bucle invertido	127.0.0.1

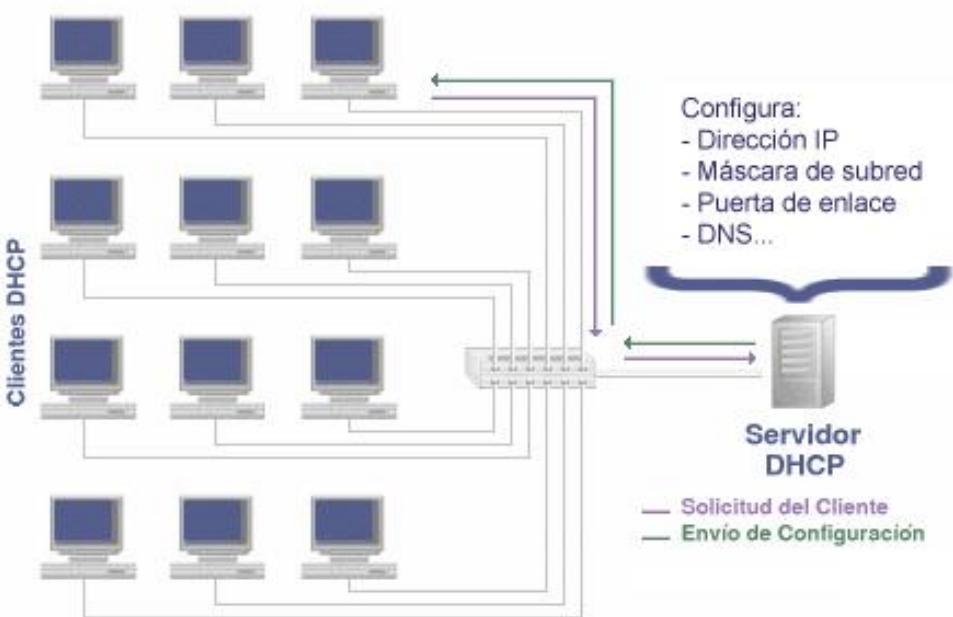
## 9. Instal·lació del servei de DHCP

### 9.1. El servei de DHCP (Dynamic Host Configuration Protocol)

El protocol DHCP té com a objectiu fonamental l'assignació d'adreses IP als equips d'una xarxa d'una manera desatesa. Per tant, permet assignar automàticament la configuració IP dels equips clients de la xarxa.

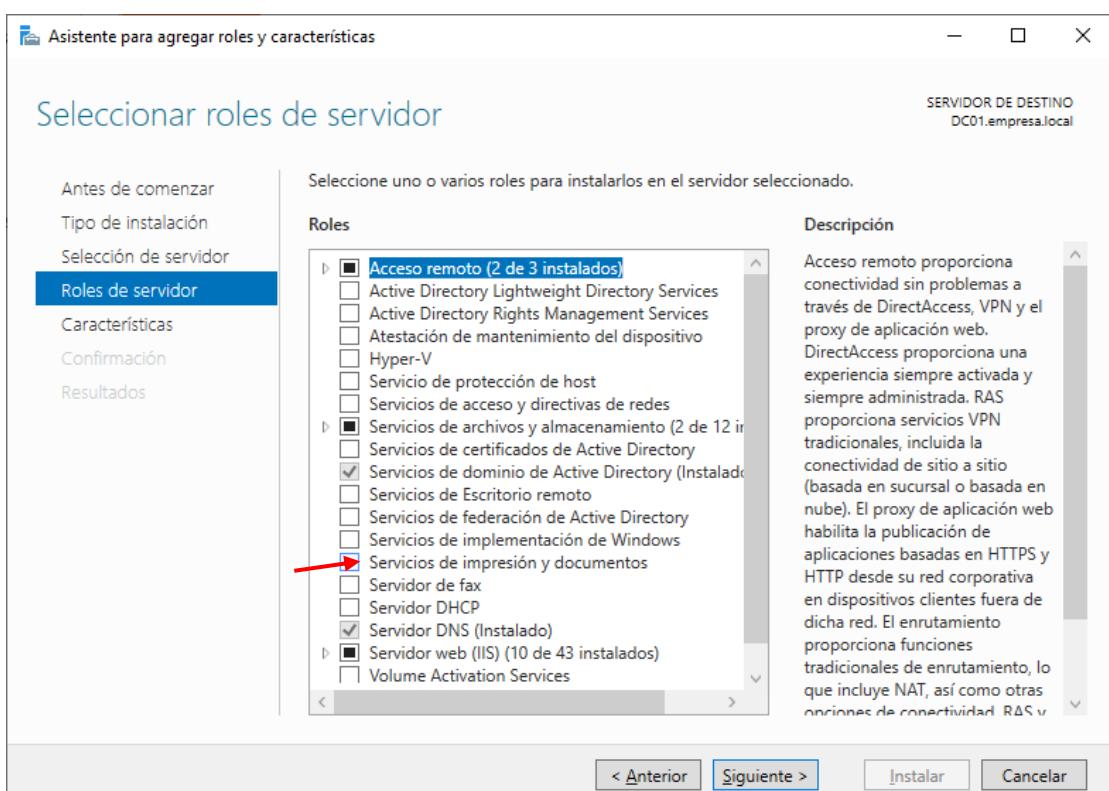
En xarxes xicotetes l'assignació manual d'adreses IP no és una tasca massa complexa per a l'administrador, però a partir d'una certa grandària de xarxa, aquesta tasca es pot tornar un autèntic problema, no ja per la càrrega de treball manual, sinó també per la possibilitat de comissió d'errors.

En el següent apartat posarem en marxa el servei DHCP en un la nostra xarxa perquè els equips clients puguen obtindre automàticament una adreça IP, i aspectes de configuració com l'adreça del DNS i de la porta d'enllaç. En aquest cas, en lloc de tindre aquest servei corrent en un equip dedicat, o en l'encaminador, l'instal·larem en el Controlador de Domini. Depenent de les característiques de la xarxa, podria no ser adequat instal·lar serveis extra en el controlador de domini per a no augmentar la seua càrrega, però en un entorn de desenvolupament com el que estem implantant, no serà cap problema.

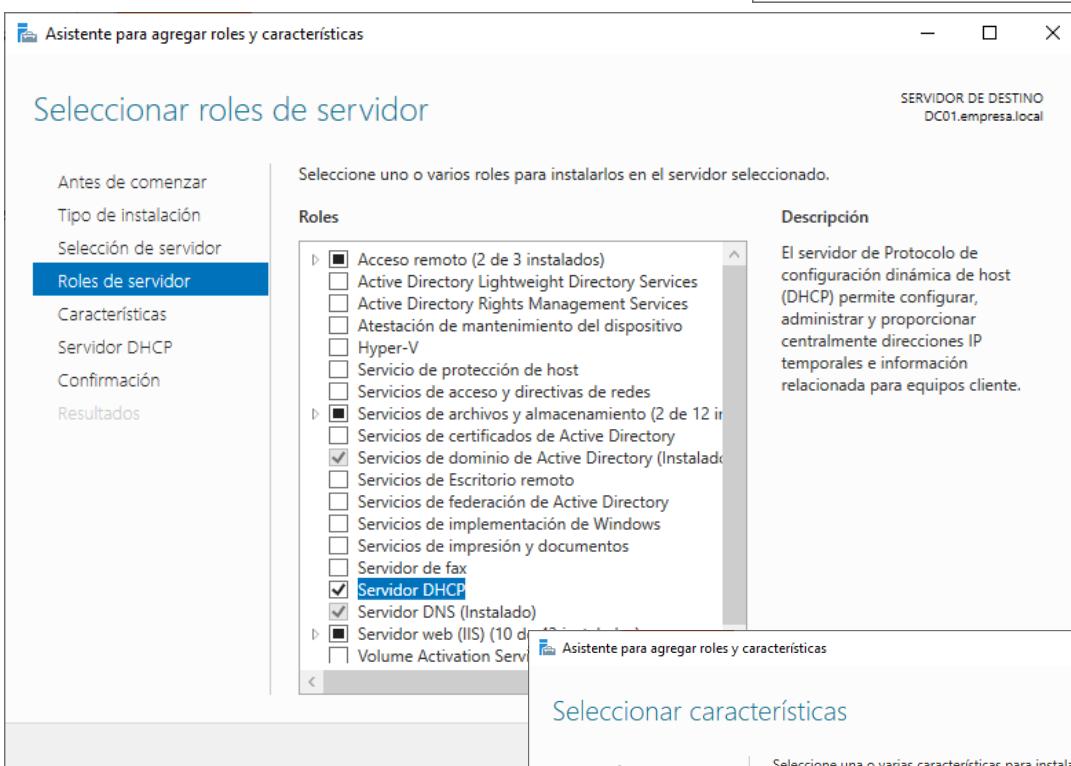
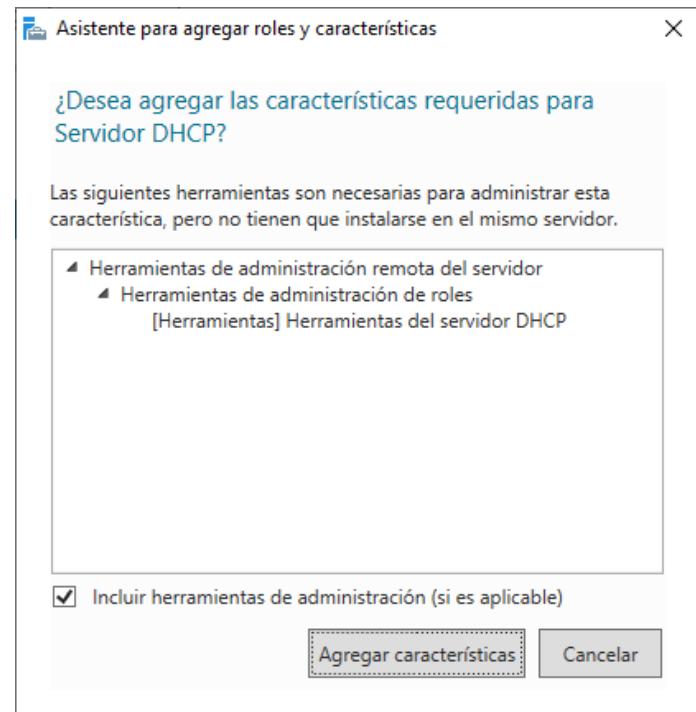


### 9.2. Instal·lació del servei DHCP

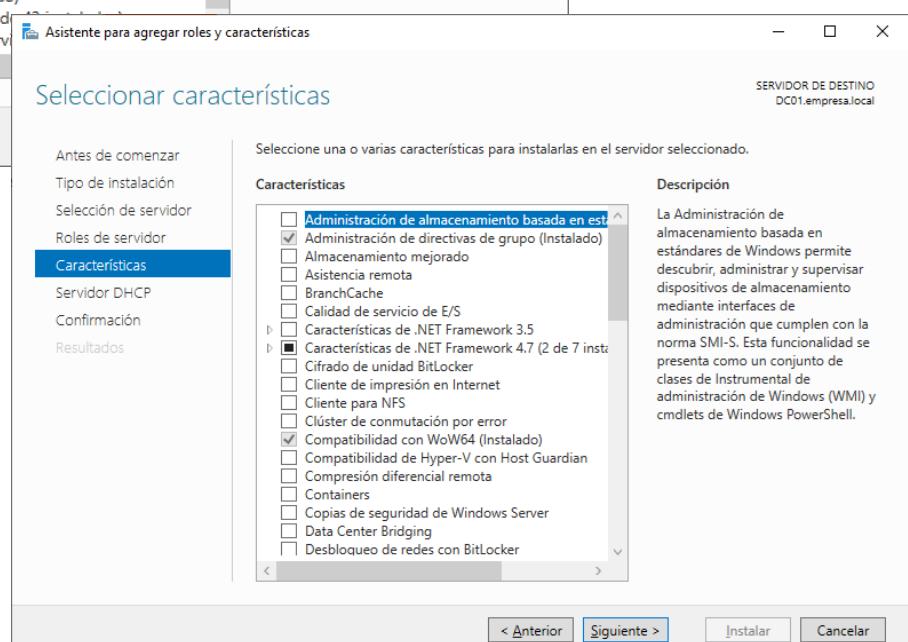
Per a instal·lar el servei DHCP anirem a "Agregar rols i característiques" del "Administrador del servidor" i seleccionarem posteriorment el rol "Servidor DHCP".



A continuació se'n obrirà una finestra indicant que hem d'instal·lar també una sèrie de característiques. Premerem a 'Aregar característiques'.



Atés que , en aquest moment, no instal·larem més rols ni més característiques, premerem 'Següent' en totes dues finestres:



A continuació , se'ns mostraran unes observacions relacionades amb el rol de servidor DHCP.

**Servidor DHCP**

El Protocolo de configuración dinámica de host permite a los servidores asignar, o conceder, direcciones IP a equipos y otros dispositivos que están habilitados como clientes DHCP. La implementación de un servidor DHCP en la red proporciona a los equipos y otros dispositivos de red basados en TCP/IP direcciones IP válidas así como los parámetros de configuración adicionales que estos dispositivos necesitan, denominados opciones de DHCP. Esto permite a los equipos y dispositivos conectarse a otros recursos de red, como servidores DNS, servidores WINS y enruteadores.

**Observaciones:**

- Debe configurar al menos una dirección IP estática en este equipo.
- Antes de instalar el servidor DHCP, debe planear las subredes, los ámbitos y las exclusiones. Guarde el plan en un lugar seguro para poder consultararlo en el futuro.

Per a concloure el procés d'instal·lació (que no de configuració) del servei seleccionat, se'ns mostrarà un resum de totes les funcions que s'instal·laran , i se'ns demanarà que confirmem les accions a realitzar. Opcionalment, marcarem la casella de permetre el reinici automàtic del sistema durant la instal·lació del servei.

**Confirmar selecciones de instalación**

Para instalar los siguientes roles, servicios de rol o características en el servidor seleccionado, haga clic en Instalar.

Reiniciar automáticamente el servidor de destino en caso necesario

En esta página se pueden mostrar características opcionales (como herramientas de administración) porque se seleccionaron automáticamente. Si no desea instalar estas características opcionales, haga clic en Anterior para desactivar las casillas.

**Herramientas de administración remota del servidor**

Herramientas de administración de roles  
Herramientas del servidor DHCP

**Servidor DHCP**

Exportar opciones de configuración  
Especifique una ruta de acceso de origen alternativa

< Anterior Siguiente > Instalar Cancelar

**Progreso de la instalación**

Ver progreso de la instalación

**Instalación de característica**  
Requiere configuración. Instalación correcta en DC01.empresa.local.

**Servidor DHCP**  
Iniciar el Asistente posterior a la instalación de DHCP  
[Completar configuración de DHCP](#)

**Herramientas de administración remota del servidor**

Herramientas de administración de roles  
Herramientas del servidor DHCP

Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

Exportar opciones de configuración

< Anterior Siguiente > Cerrar Cancelar

Després d'acabar la instal·lació del servei de DHCP, veurem un missatge indicant-nos que hem de "completar configuració DHCP".

### 9.3. Configuració del servei DHCP

D'aquesta manera, després de la instal·lació de l'servei, procedirem a configurar-ho. Per a això, podem fer clic en el missatge que hem comentat abans de la pantalla de finalització del servei "completar configuració de DHCP" o si obrim l'Administrador del Servei, veurem que en la part superior la icona de notificacions (bandereta) mostra un missatge. Si fem clic en ell, veurem que se'n adverteix que el servei DHCP està pendent de ser configurat.

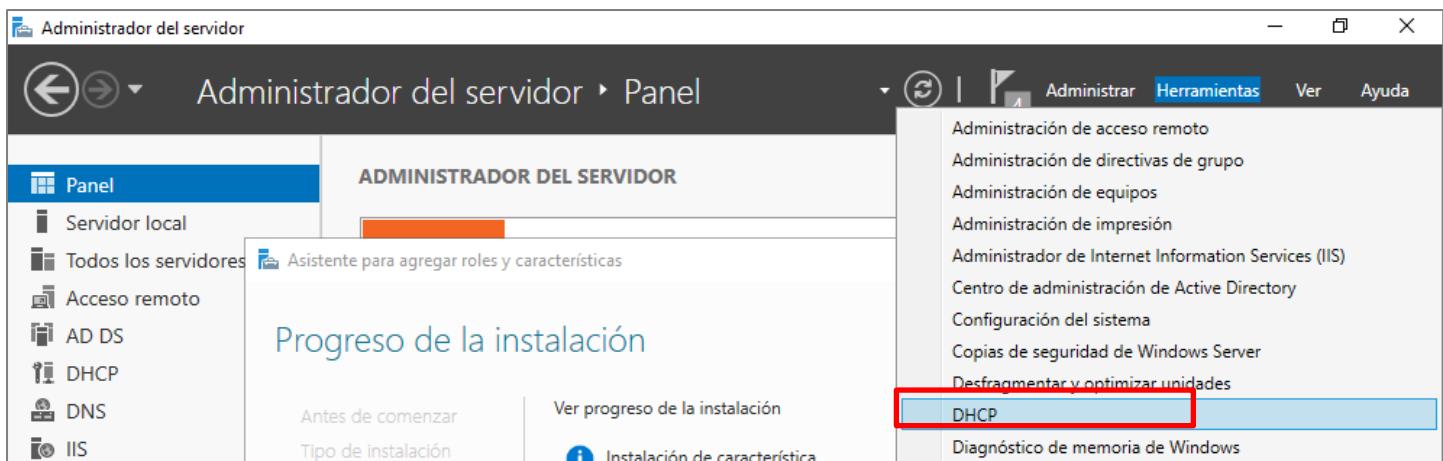
Fem clic a 'Completar configuració de DHCP', i s'obrirà un assistent que ens indicarà uns passos a realitzar que es duran a terme automàticament.

Després de prémer 'Següent' marcarem l'opció per defecte.

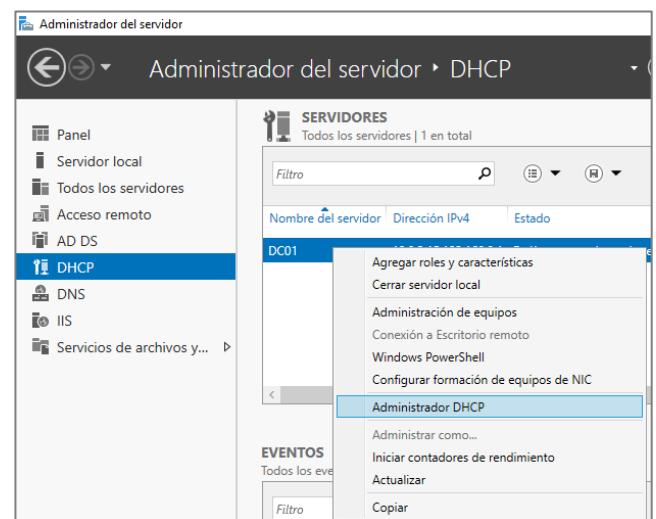
The screenshots illustrate the 'Post-Installation Wizard for DHCP' process:

- Descripción:** This step shows the summary of steps to complete DHCP server configuration. It includes instructions to create security groups for delegation, authorize DHCP administrators and users, and enable the DHCP server on the destination machine if it's joined to a domain.
- Autorización:** This step specifies credentials for authorizing the DHCP server in AD DS. The 'Usar las credenciales del siguiente usuario' option is selected, with the user name set to 'EMPRESA\Administrador'. Other options include 'Usar credenciales alternativas' and 'Omitir autorización de AD'.
- Resumen:** This step provides a summary of the post-installation configuration steps:
  - Creando grupos de seguridad ..... Listo
  - Reinic peace el servicio de servidor DHCP en el equipo de destino para que los grupos de seguridad sean efectivos.
  - Autorizando el servidor DHCP ..... Listo

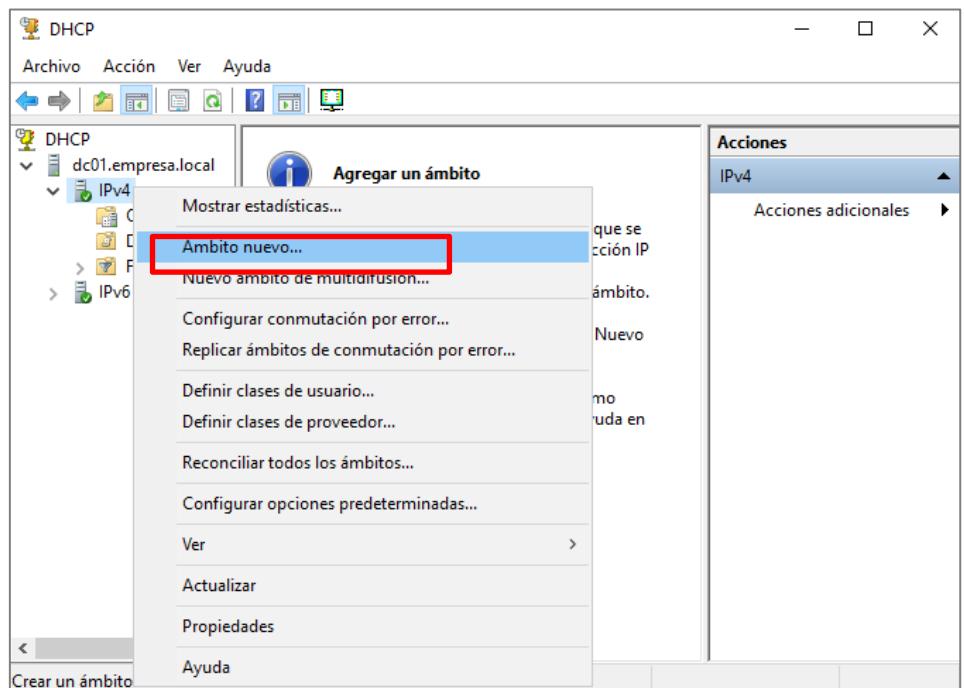
Tanquem l'assistent, i ja podrem **administrar el servei DHCP**. Per a això anem a Administrador del Servei → Eines → DHCP



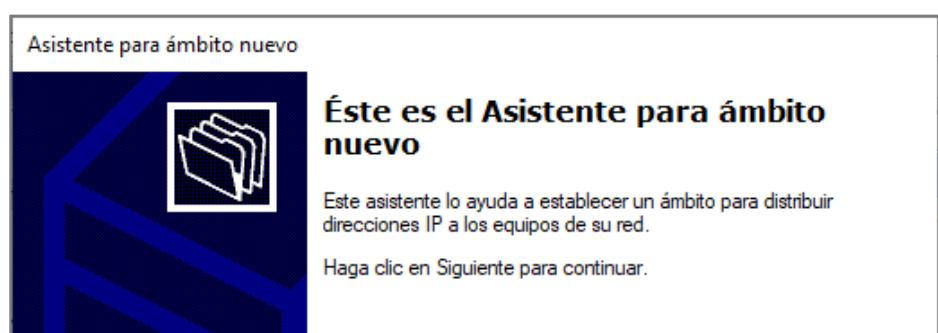
Una altra forma per a configurar el servei de DHCP, és seleccionar DHCP, fem clic amb el botó secundari sobre l'equip que tinga instal·lat el servidor DHCP (recordeu que encara que no siga el cas, podríem tindre muntat un clúster de servidors on els serveis estigueren corrent en diferents equips físics), i seleccionem 'Administrador DHCP'.



S'obrirà l'Administrador DHCP, i crearem un '**Àmbit nou**' IPv4, o rang d'adreses IP que el servidor podrà proporcionar als clients que facen la petició d'adreça .



S'obrirà un assistent que ens permetrà crear el nou àmbit.



El primer aspecte que haurem de configurar serà el nom que li assignarem (per exemple domini), i una descripció d'aquest.

A continuació introduirem el rang de direccions que podrem atorgar mitjançant el servei, en aquest cas les direccions aniran des de la 192.168.0.10 fins a la 192.168.0.250. De la mateixa manera introduirem la màscara de subxarxa.

L'assistent també ens permet incloure un rang de direccions que no es proporcionaran via DHCP, d'alguna manera ens les reservarem per a atorgar-les manualment a equips determinats de la xarxa, com per exemple controladors de domini de suport, servidors d'aplicacions, etc.

En la següent pantalla de l'assistent introduirem el període durant el qual els equips client

<p><b>Asistente para ámbito nuevo</b></p> <p><b>Nombre de ámbito</b> Debe escribir un nombre identificativo para el ámbito. También puede proporcionar una descripción.</p> <p>Escriba un nombre y una descripción para este ámbito. Esta información le ayuda a identificar rápidamente cómo se usa el ámbito y su red.</p> <p>Nombre: <input type="text" value="Cientes del dominio"/> </p> <p>Descripción: <input type="text" value="Direcciones para los clientes del dominio"/></p>
<p><b>Asistente para ámbito nuevo</b></p> <p><b>Intervalo de direcciones IP</b> Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.</p> <p>Opciones de configuración del servidor DHCP</p> <p>Escriba el intervalo de direcciones que distribuye el ámbito.</p> <p>Dirección IP inicial: <input type="text" value="192 . 168 . 0 . 10"/> Dirección IP final: <input type="text" value="192 . 168 . 0 . 250"/></p> <p>Opciones de configuración que se propagan al cliente DHCP</p> <p>Longitud: <input type="text" value="24"/> Máscara de subred: <input type="text" value="255 . 255 . 255 . 0"/></p>
<p><b>Asistente para ámbito nuevo</b></p> <p><b>Agregar exclusiones y retraso</b> Exclusiones son direcciones o intervalos de direcciones que no son distribuidas por el servidor. Retraso es el tiempo que retrasará el servidor la transmisión de un mensaje DHCPoffer.</p> <p>Escriba el intervalo de direcciones IP que desea excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.</p> <p>Dirección IP inicial: <input type="text"/> Dirección IP final: <input type="text"/> Agregar</p> <p>Intervalo de direcciones excluido:</p>
<p><b>Asistente para ámbito nuevo</b></p> <p><b>Duración de la concesión</b> La duración de la concesión especifica durante cuánto tiempo puede utilizar un cliente una dirección IP de este ámbito.</p> <p>La duración de las concesiones debería ser típicamente igual al promedio de tiempo en que el equipo está conectado a la misma red física. Para redes móviles que consisten principalmente de equipos portátiles o clientes de acceso telefónico, las concesiones de duración más corta pueden ser útiles.</p> <p>De igual modo, para una red estable que consiste principalmente de equipos de escritorio en ubicaciones fijas, las concesiones de duración más larga son más apropiadas.</p> <p>Establecer la duración para las concesiones de ámbitos cuando sean distribuidas por este servidor.</p> <p>Limitada a:</p> <p>Días: <input type="text" value="8"/> Horas: <input type="text" value="0"/> Minutos: <input type="text" value="0"/></p>

disposaran de la IP assignada. Per defecte l'assistent ens indica 8 dies, però depenent de la mena de xarxa, aquest valor podria incrementar-se o disminuir-se.

En quins casos se t'ocorre que el període de concessió de la IP via DHCP podria ser major i en quins menor?

A més de el vist fins ara , també podem configurar altres opcions com l'assignació de la porta d'enllaç i de l'espai de resolució de noms DNS. Per a això marcarem l'opció 'Configurar aquestes opcions ara'.

#### Asistente para ámbito nuevo

##### Configurar opciones DHCP

Para que los clientes puedan utilizar el ámbito debe configurar las opciones DHCP más habituales.



Cuando los clientes obtienen una dirección, se les da opciones DHCP tales como las direcciones IP de los enrutadores (puertas de enlace predeterminadas), servidores DNS y configuración WINS para ese ámbito.

La configuración que ha seleccionado aquí es para este ámbito e invalida la configuración de la carpeta Opciones de servidor para este servidor.

¿Desea configurar ahora las opciones DHCP para este ámbito?

- Configurar estas opciones ahora  
 Configuraré estas opciones más tarde

La primera opció que podem indicar és la(s) porta(s) d'enllaç que assignarem als clients. En aquest cas, la tenim situada en el nostre servidor Windows server 2019, ja que hem instal·lat en ell el servei d'encaminament , per tant, serà la direcció 192.168.0.1.

#### Asistente para ámbito nuevo

##### Enrutador (puerta de enlace predeterminada)

Puede especificar los enrutadores, o puertas de enlace predeterminadas, que se distribuirán en el ámbito.



Para agregar una dirección IP para un enrutador usado por clientes, escriba la dirección.

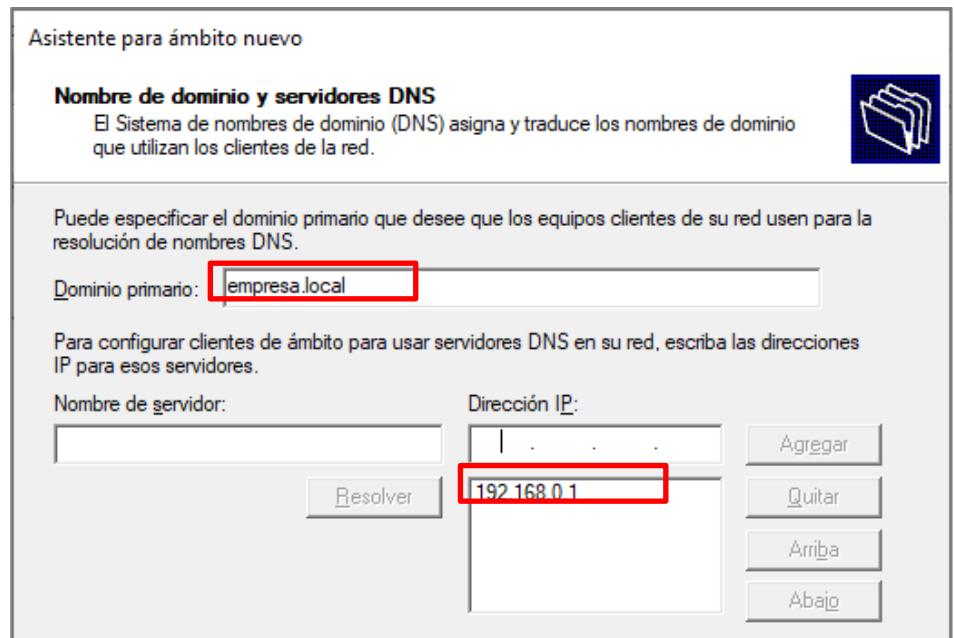
Dirección IP:

...	Agregar
192.168.0.1	Quitar
	Arriba
	Abajo

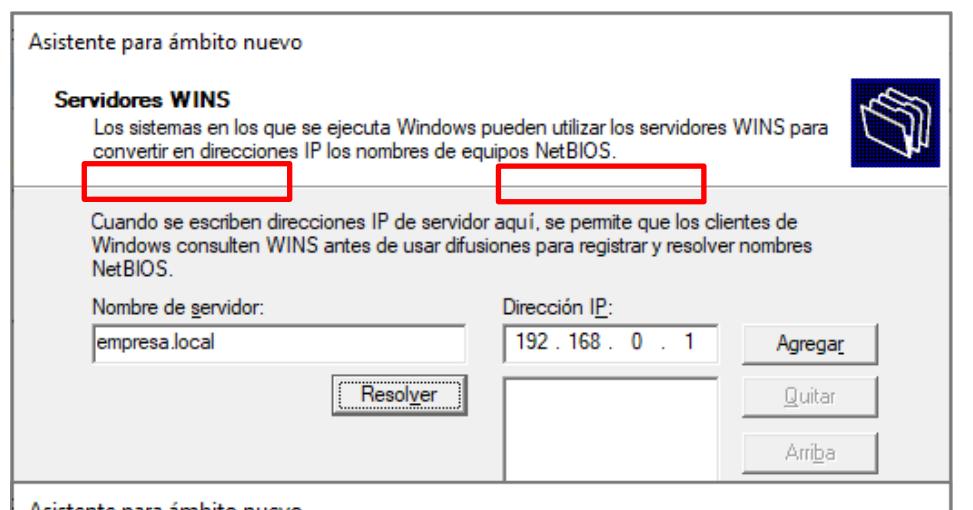
< Atrás Siguiente > Cancelar

La següent opció és l'assignació del servidor DNS (o dels servidors DNS) mitjançant la seu IP.

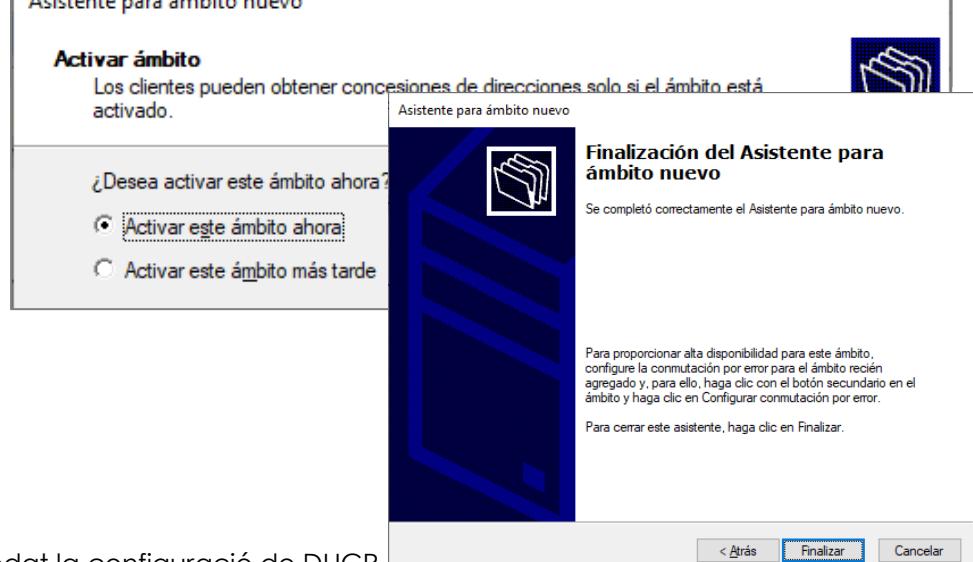
Recorda que el servei de DNS està instal·lat en el servidor Windows 2019.



La següent pantalla de l'assistent ens sol·licita que introduïm els servidors WINS de la nostra xarxa. Recordeu que el servei WINS era usat antigament en les xarxes Windows per a resoldre noms. Hui dia ha sigut completament substituït per DNS, però per a garantir la compatibilitat amb equips antics, continua implementant-se. En aquest cas indicarem el nom del servidor empresa.local, i en premer 'Resoldre' ens apareixerà la seu IP.



Finalment, només restarà activar l'àmbit i tancar l'assistent.



Si donem una ullada a com ha quedat la configuració de DHCP,

En "conjunt de direccions" observarem l'interval d'IPs a entregar als clients, així com l'interval d'IPs que quedaran excloses.

The screenshot shows the Windows Server DHCP Management console. On the left, the navigation pane shows a tree structure under 'dc01.empresa.local' with 'IPv4' selected. Under 'IPv4', 'Clients of the domain' is expanded, showing 'Conjunto de direcciones', 'Concesiones de direcciones', 'Reservas', 'Opciones de ámbito', and 'Directivas'. The main pane displays a table for the scope 'Clients of the domain' with two entries: '192.168.0.10' and '192.168.0.100'. The table columns are 'Dirección IP inicial', 'Dirección IP final', 'Descripción', and 'Acciones'. The 'Descripción' column contains 'Intervalo de direcciones para distribución' and 'Direcciones IP excluidas de la distribución'. The 'Acciones' column has a single item: 'Conjunto ...'.

En “Concessions d’adreces ” podrem veure les adreces IP entregades, així com el nom dels equips als quals han sigut entregades.

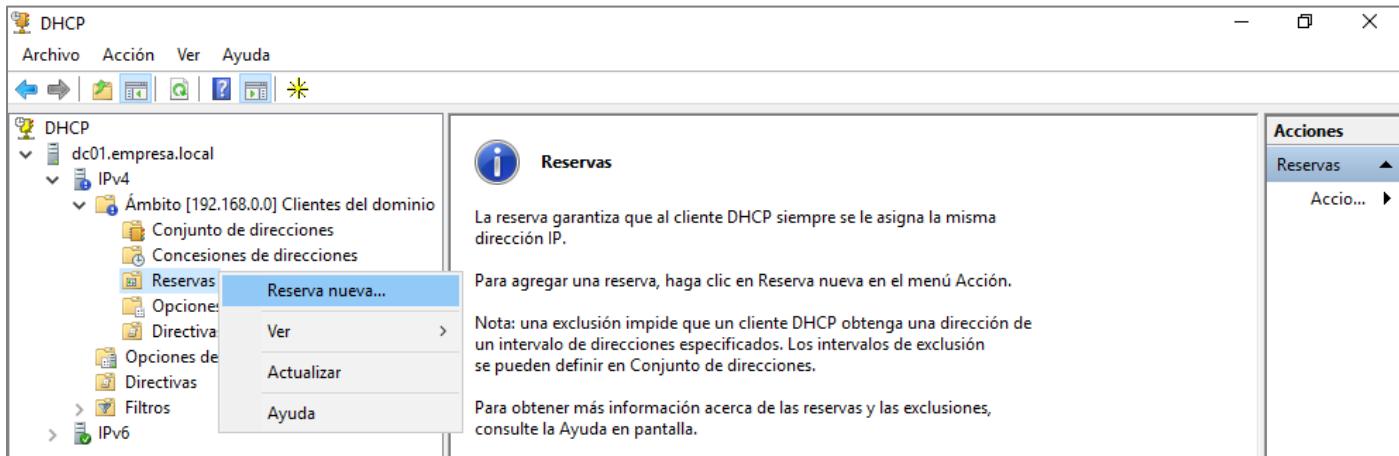
The screenshot shows the Windows Server DHCP Management console. The navigation pane is identical to the previous screenshot. The main pane displays a table titled 'No hay elementos disponibles en esta vista.' (There are no elements available in this view). The table has columns: 'Dirección IP del cliente...', 'Nombre', 'Expiración de cesión', 'Tipo', and 'Id. exclusivo'. The 'Acciones' column has a single item: 'Concesion...'. A note at the bottom of the table area says 'No hay elementos disponibles en esta vista.'

En “opcions d’àmbit ” podrem modificar la configuració que hem establiti per a aquest àmbit.

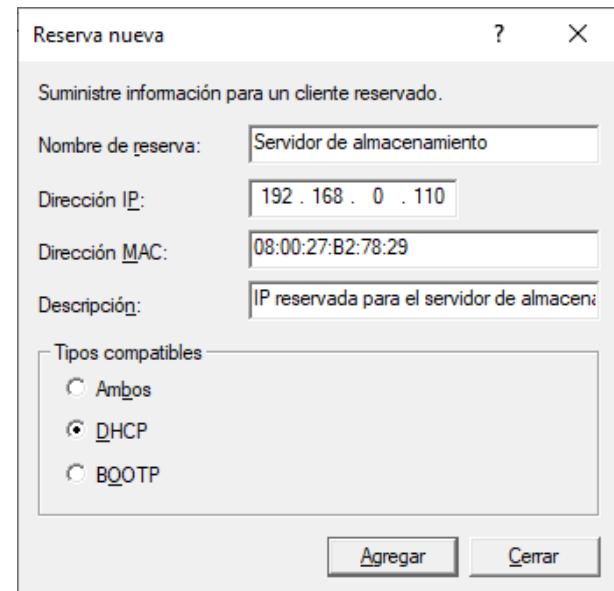
The screenshot shows the Windows Server DHCP Management console. The navigation pane is identical to the previous screenshots. The main pane displays a table for 'Opciones de ámbito' (Scope Options) under the 'Clients of the domain' scope. The table has columns: 'Nombre de opción', 'Proveedor', 'Valor', and 'Nombre de directiva'. Three options are listed: '003 Enrutador' (Proveedor: Estándar, Valor: 192.168.0.1, Nombre de directiva: Ninguno), '006 Servidores DNS' (Proveedor: Estándar, Valor: 192.168.0.1, Nombre de directiva: Ninguno), and '015 Nombre de dominio DNS' (Proveedor: Estándar, Valor: empresa.local, Nombre de directiva: Ninguno). The 'Acciones' column has a single item: 'Opciones ...'.

## Assignació manual de direccions

Una altra opció que ens permet DHCP és l'assignació manual d'adreses IP en funció de la MAC de l'equip client (sempre que aquest tinga configurada l'obtenció d'IP mitjançant DHCP). Això pot ser útil, per exemple per a configurar l'assignació d'IPs a equips singulars, com a servidors secundaris mitjançant DHCP, però assignant una adreça IP a la seua MAC, de manera que si per qüestions de planificació de la xarxa sorgeix la necessitat de canviar l'adreçament, es pot fer des del propi servidor DHCP. Per a això obrirem el camp 'Reserves' que es troba en l'àmbit i farem clic en 'Reserva nova...'.



En aquest cas la nostra reserva es denominarà 'Servidor d'Emmagatzematge', i assignarà la direcció 192.168.0.110 a un equip que la seua MAC siga 08:00:27:B2:78:29.



## 10. Introducció d'equips client en un Domini Windows 2019

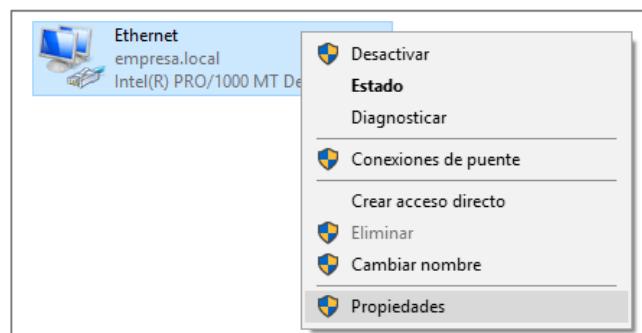
### 10.1. Introducció de Clients Windows 10

La introducció d'equips client en un domini Windows no és en absolut un procés complex o problemàtic, sempre que es configure adequadament la xarxa. Potser, la major complexitat que puga sorgir en introduir un equip Windows 10 en un domini vinga derivada de la nova interfície, en la qual a vegades costa trobar les coses.

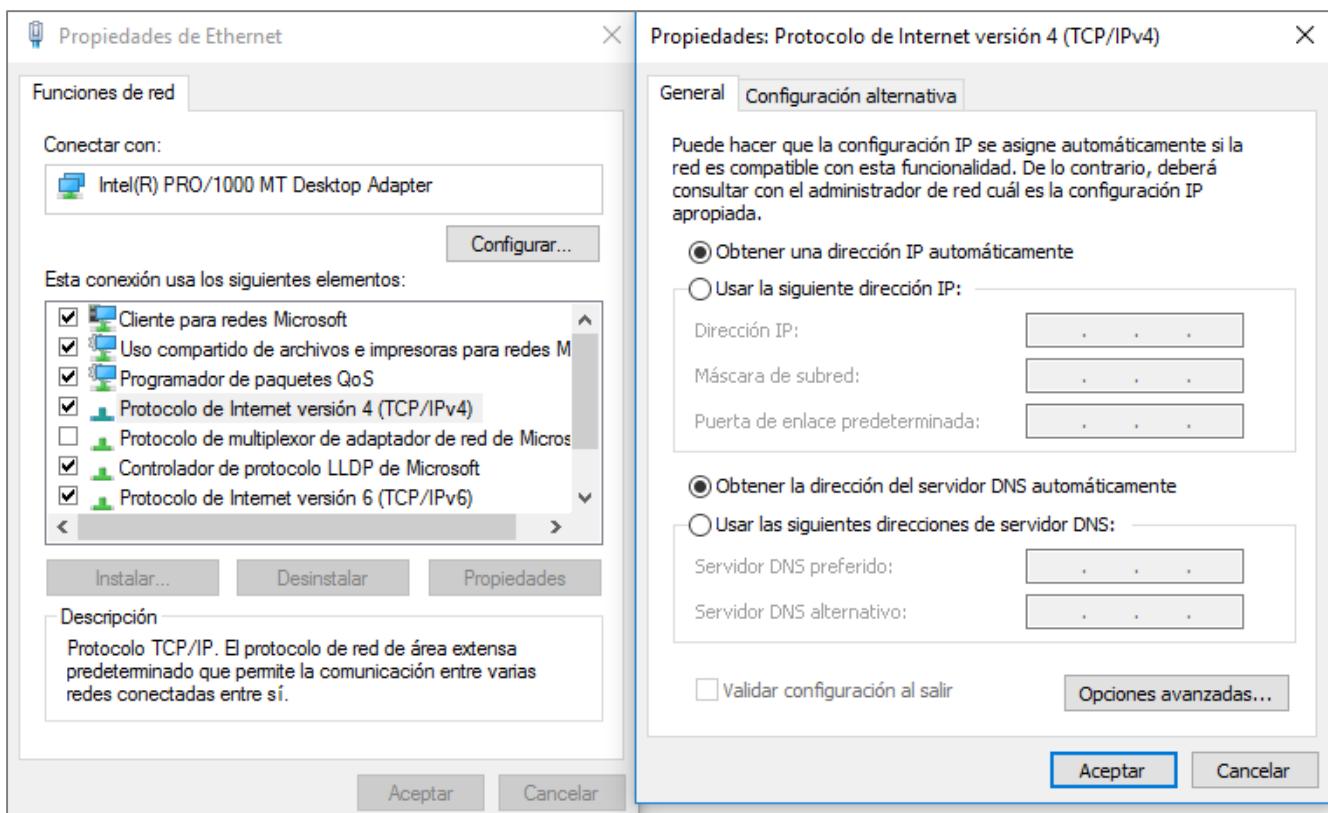
Per a introduir un equip Windows 10 en un domini, en primer lloc haurem de comprovar que la configuració de la xarxa és correcta, tenint en compte que hem habilitat el servei DHCP en el controlador de domini. Existeixen diverses alternatives per a arribar a la pantalla de "connexions de xarxa":

- Buscar: ncpa.cpl
- Botó dret sobre la icona de xarxa del costat del rellotge → "Obrir el centre de xarxes i recursos compartits" → Canviar configuració de l'adaptador
- 'Panell de Control' → 'Xarxes i Internet' → 'Veure l'estat i les tasques de xarxa' → 'Canviar la configuració de l'adaptador'.

Farem clic amb el botó secundari sobre la connexió de xarxa, i accedirem a l'opció 'Propietats'.



En les propietats d'Ethernet, obrirem el 'Protocol d'Internet versió 4 (TCP/IPv4)' i comprovarem que estan marcades les opcions 'Obtindre una adreça IP automàticament' i 'Obtindre l'adreça del servidor DNS automàticament'. L'obtenció dels paràmetres de xarxa es realitzarà mitjançant el servei DHCP que tenim corrent en el controlador de domini.



Si obrim una consola cmd i escrivim ipconfig /all comprobarem que la configuració de la xarxa, obtinguda via DHCP és correcta.

```
C:\ Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-26C3V2E
Sufijo DNS principal . . . . : 
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: empresa.local

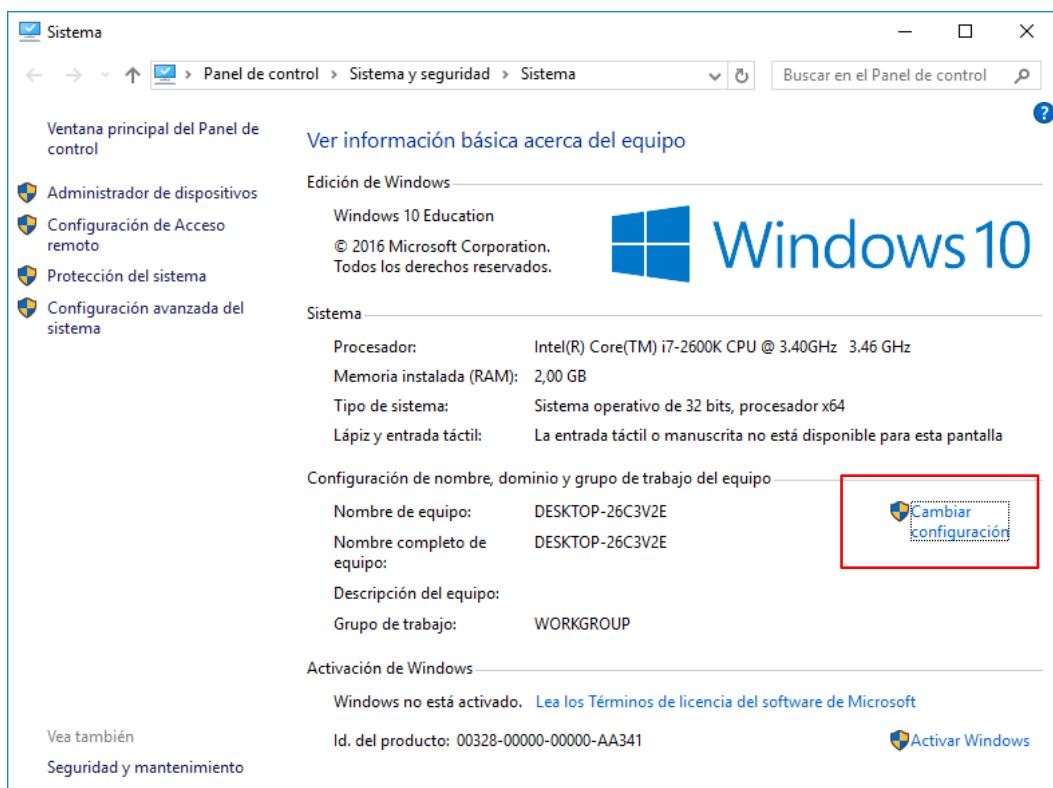
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : empresa.local
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-82-A6-F5
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . : sí
Vínculo: dirección IPv6 local. . . . : fe80::682b:5a37:4348:8e2d%6(Preferido)
Dirección IPv4. . . . . : 192.168.0.10(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 16 de septiembre de 2019 16:38:14
La concesión expira . . . . . : miércoles, 25 de septiembre de 2019 7:13:17
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 50855975
DUID de cliente DHCPv6. . . . . : 00-01-00-01-25-11-52-40-08-00-27-82-A6-F5
Servidores DNS. . . . . : 192.168.0.1
NetBIOS sobre TCP/IP. . . . . : habilitado

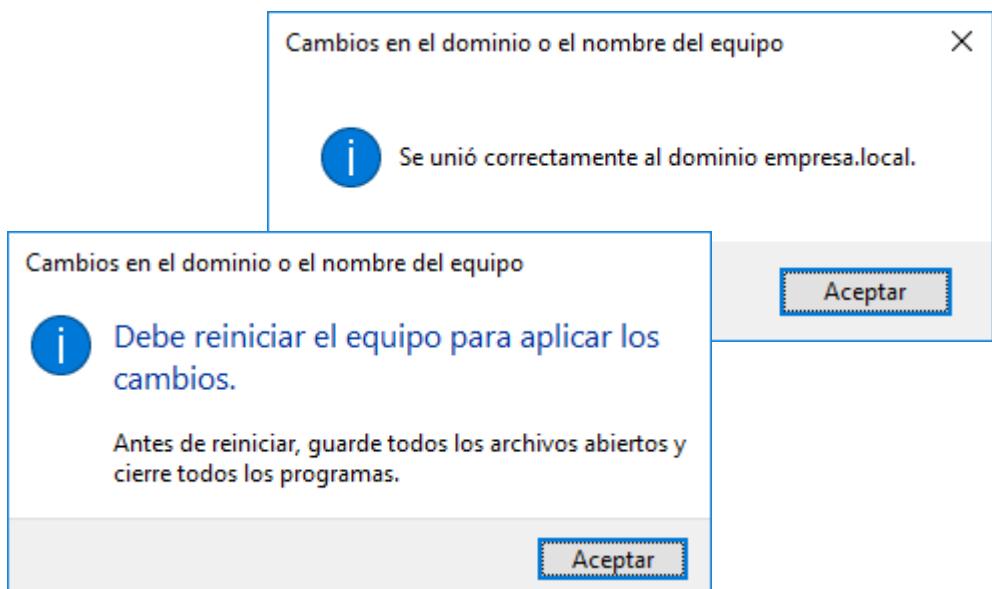
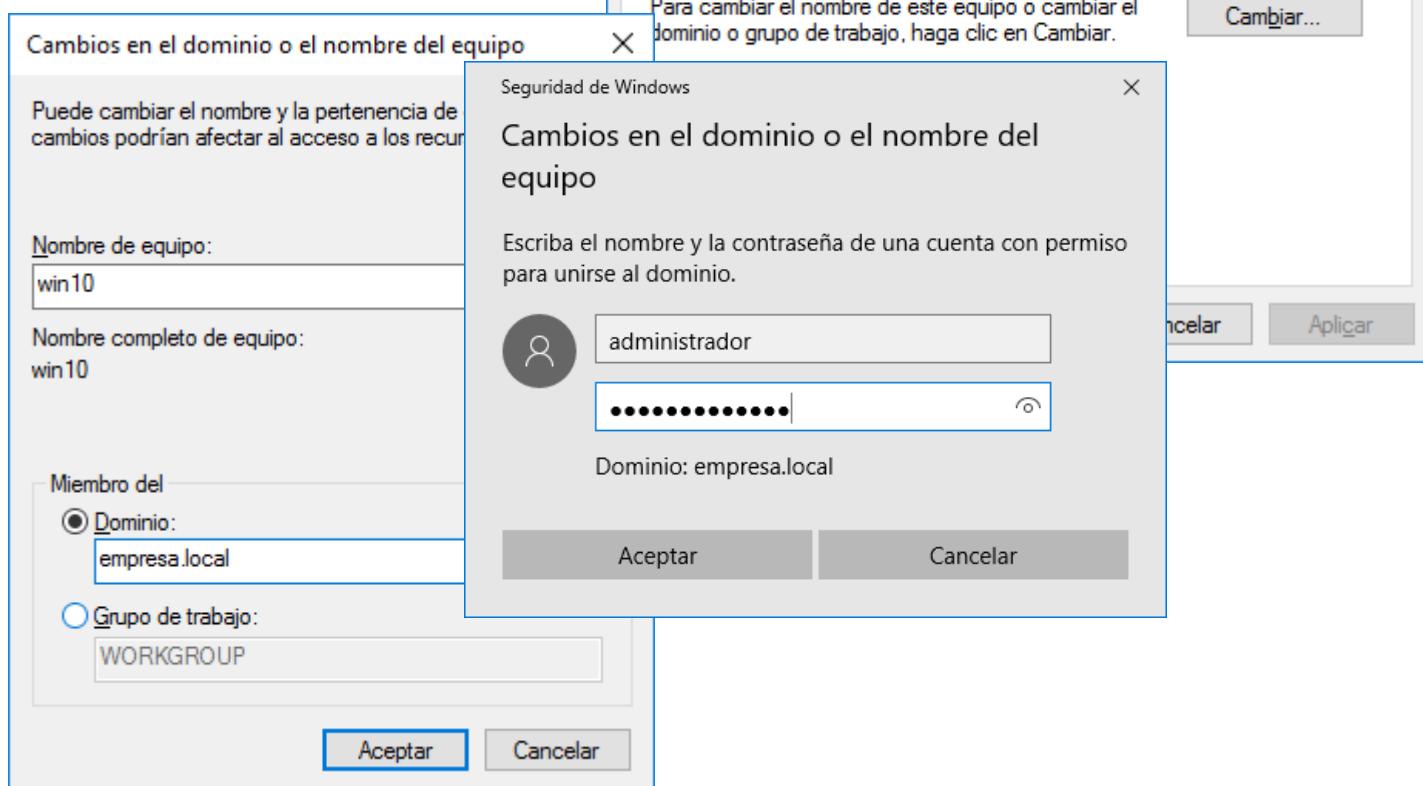
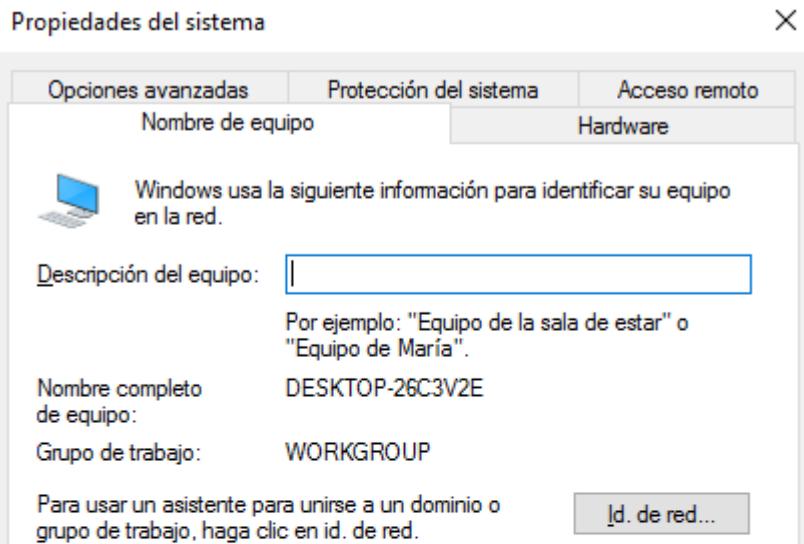
Adaptador de túnel isatap.empresa.local:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . : empresa.local
Descripción . . . . . : Microsoft ISATAP Adapter #2
Dirección física. . . . . : 00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . . : sí
```

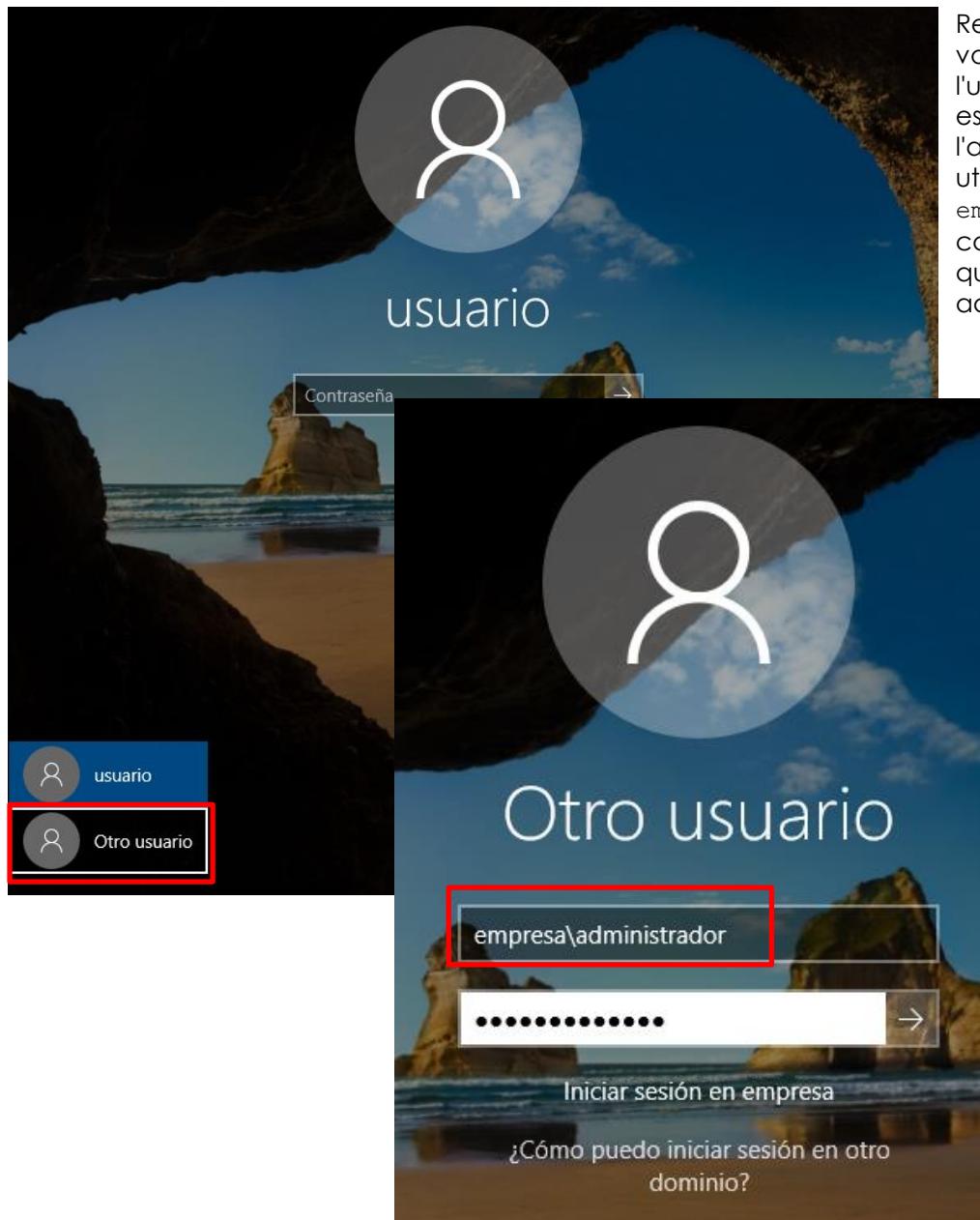
Una vegada realitzades aquestes comprovacions, per a unir el client Windows 10 al domini, estrenyerem les tecles Windows + Pausa i accedirem a les "Propietats del sistema" des d'on fent clic a "Canviar configuració" podrem canviar l'equip del grup de treball al domini empresa.local.



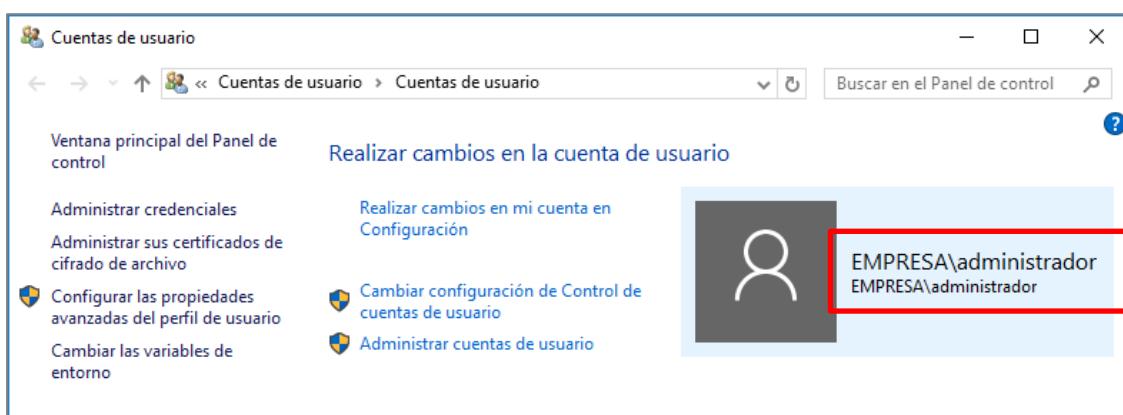
Se'n sol·licitarà la introducció de les credencials d'un usuari del domini con privilegis d'administració , i si són correctes, se'n notificarà la unió correcta al domini, i la necessitat de reiniciar perquè els canvis en la configuració facen efecte .



Quan tornem a autenticar-nos en l'equip client, podrem fer-lo amb usuaris del domini.



Recordeu que en el cas de voler accedir al client amb l'usuari Administrador, caldrà especificar que es tracta de l'administrador del domini utilitzant el prefix empresa\Administrador. En cas contrari el sistema entendrà que volem accedir amb un administrador local.



D'altra banda, si comprovem el costat servidor (Eines→usuaris i equips d'Active Directory), veurem que efectivament ha sigut donat d'alta en el domini la màquina amb Windows 10.

The screenshot shows the Windows Server 'Usuarios y equipos de Active Directory' (User and Computer) snap-in. The left pane displays the navigation tree for the 'empresa.local' domain, with 'Computers' selected. The right pane shows a table of computers, with 'WIN10' selected. A detailed properties dialog box is open for 'WIN10', showing the following information:

Nombre	Tipo	Descripción
WIN10	Equipo	

Properties for WIN10:

Ubicación		Administrado por	Marcado
General	Sistema operativo	Miembro de	Delegación
WIN10			
Nombre del equipo (anterior a Windows 2000):	WIN10		
Nombre DNS:	win10.empresa.local		
Tipo de DC:	Estación de trabajo o servidor		
Sitio:			
Descripción:			

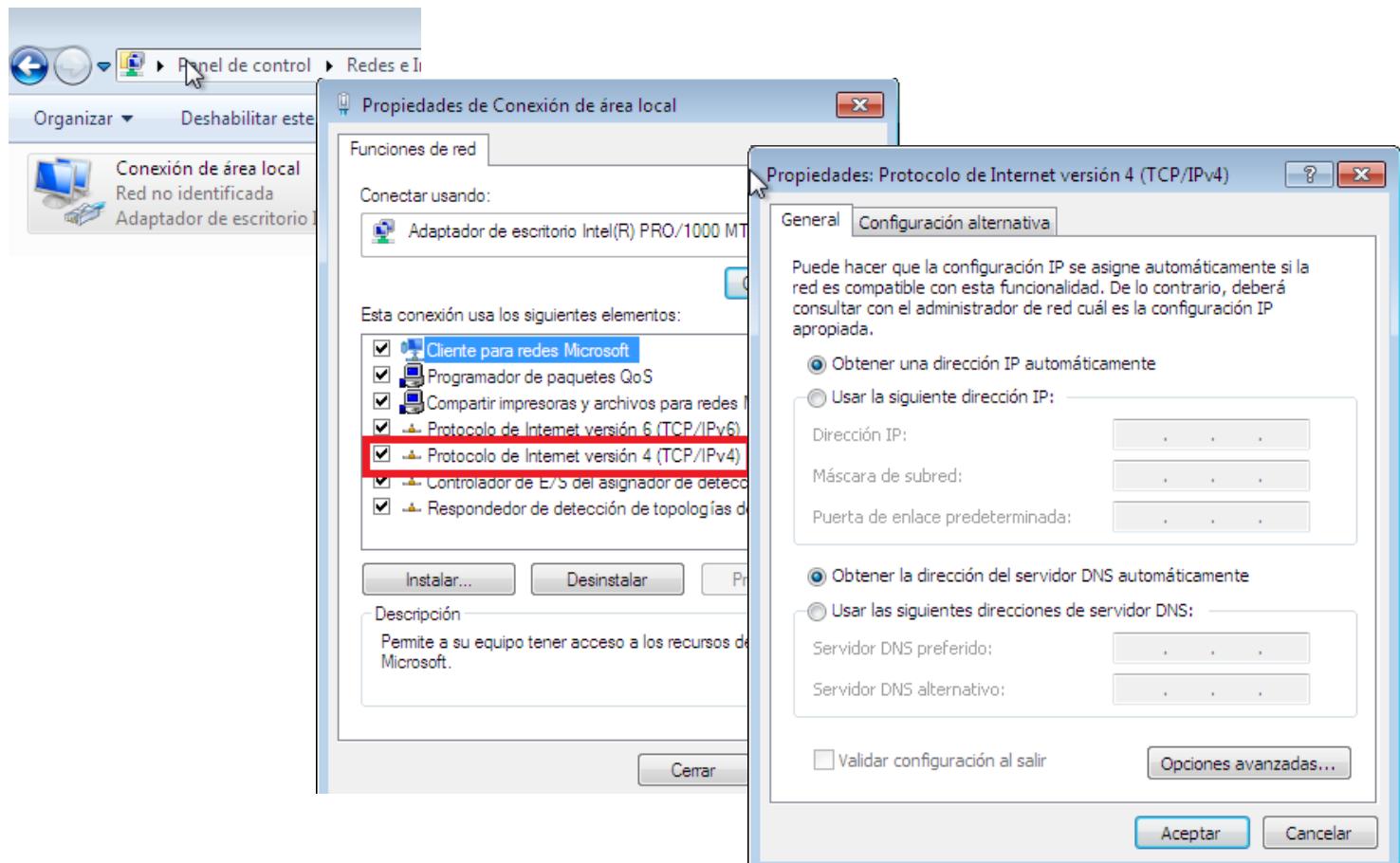
Properties for WIN10 (continued):

Ubicación		Administrado por	Marcado
General	Sistema operativo	Miembro de	Delegación
Nombre:	Windows 10 Education		
Versión:	10.0 (14393)		
Service Pack:			

## 10.2. Introducció de Clients Windows 7

La introducció de clients Windows 7 és pràcticament idèntica a la realitzada per al client Windows 10, per la qual cosa no l'examinarem amb el mateix grau de detall.

En primer lloc comprovarem que la configuració IP s'obté automàticament mitjançant el servei DHCP per a facilitar les labors d'administració .



Podem comprovar a través de la línia de comandos que la configuració de xarxa és correcta mitjançant ipconfig /all.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\alumno>ipconfig /all

Configuración IP de Windows

    Nombre de host...: win7
    Sufijo DNS principal...: híbrido
    Tipo de nodo...: híbrido
    Enrutamiento IP habilitado...: no
    Proxy WINS habilitado...: no
    Lista de búsqueda de sufijos DNS: empresa.local

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión...: empresa.local
    Descripción...: Adaptador de escritorio Intel(R)
PRO/1000 MT
    Dirección física...: 08-00-27-92-65-D7
    DHCP habilitado...: sí
    Configuración automática habilitada...: sí
    Vínculo: dirección IPv6 local...: fe80::3d88:925c:b6b9:b8a9%11(Preferido)

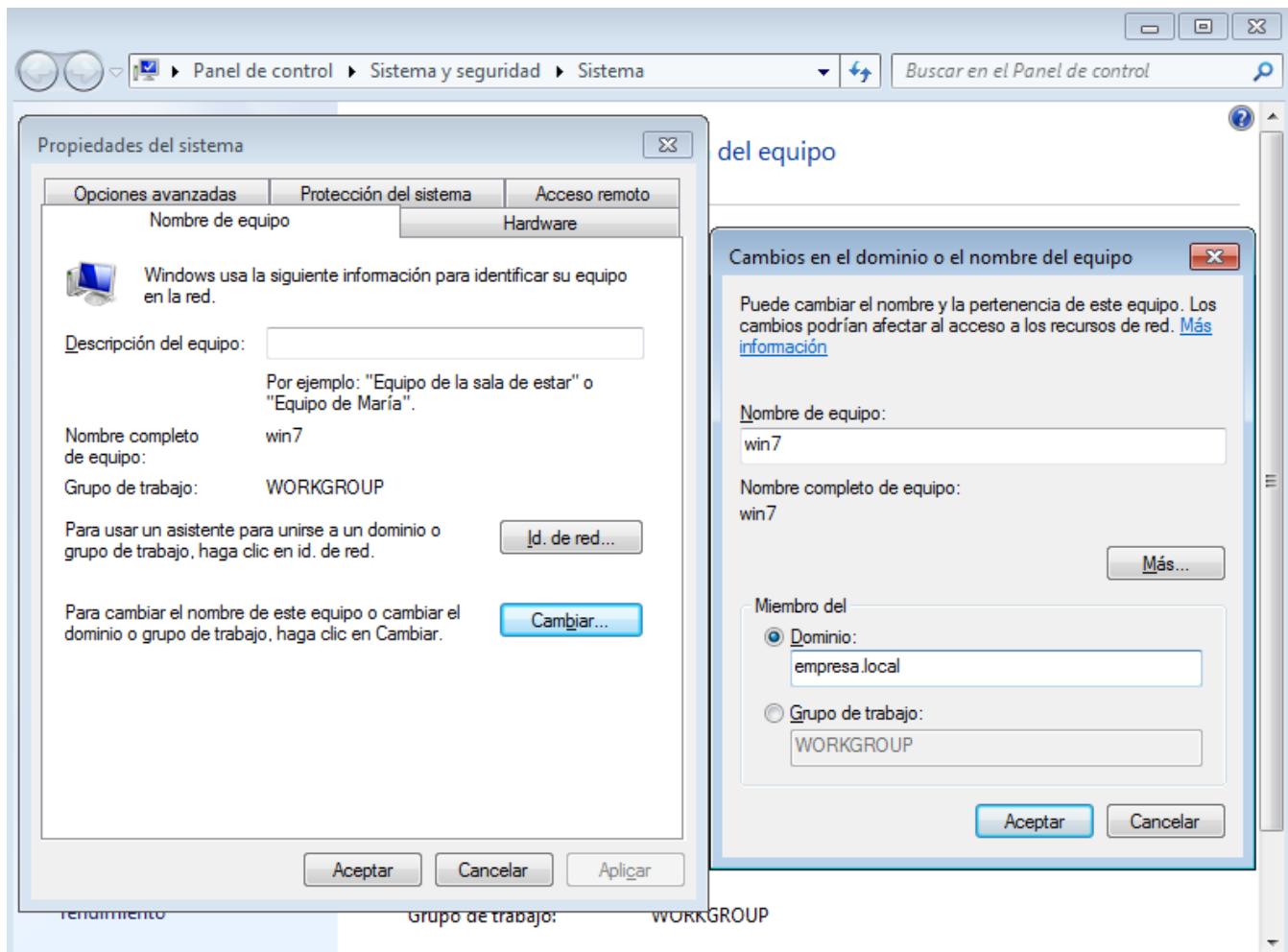
    Dirección IPv4...: 192.168.0.11(Preferido)
    Máscara de subred...: 255.255.255.0
    Concesión obtenida...: martes, 23 de septiembre de 2014
    La concesión expira...: miércoles, 01 de octubre de 2014
    Puerta de enlace predeterminada...: 192.168.0.1
    Servidor DHCP...: 192.168.0.1
    Servidores DNS...: 192.168.0.1
    NetBIOS sobre TCP/IP...: habilitado

Adaptador de túnel isatap.empresa.local:

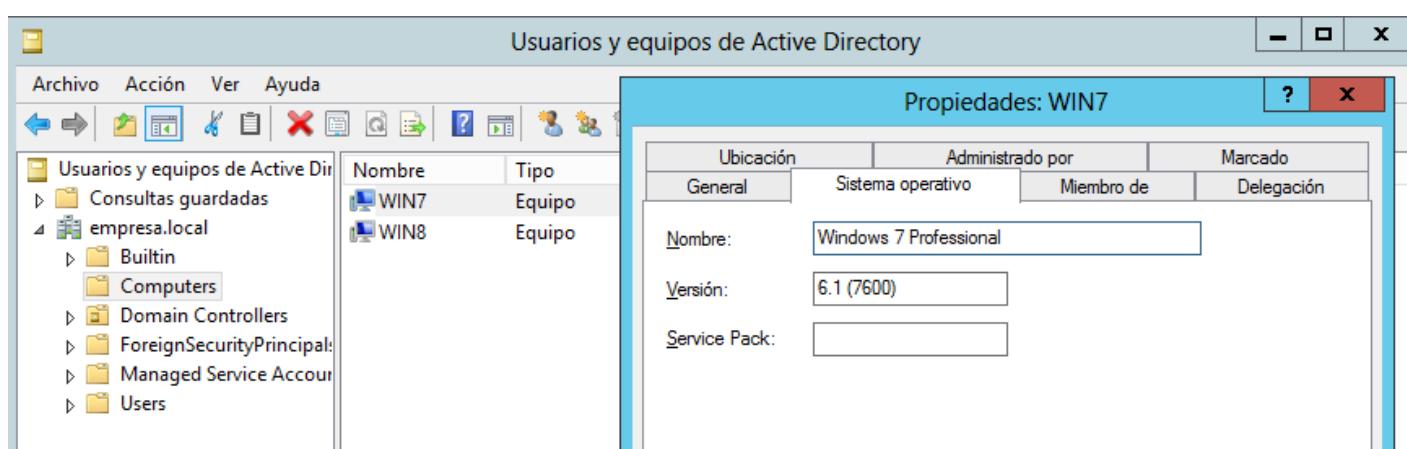
    Estado de los medios...: medios desconectados
    Sufijo DNS específico para la conexión...: empresa.local
    Descripción...: Adaptador ISATAP de Microsoft
    Dirección física...: 00-00-00-00-00-00-E0
    DHCP habilitado...: no
    Configuración automática habilitada...: sí
```

Una vegada hem comprovat la configuració

correcta de xarxa, accedirem a les propietats del sistema (tecla Windows + Pausa → canviar configuració), i ací entrarem a la pestanya 'Nom de l'equip'. Canviarem el domini al qual pertany el client en la finestra que s'obri en fer clic sobre 'Canviar'.



Després d'introduir les credencials d'un usuari amb privilegis d'administració del domini, i reiniciar, l'equip es trobarà correctament donat d'alta en el domini, tal com es pot apreciar en la següent imatge.

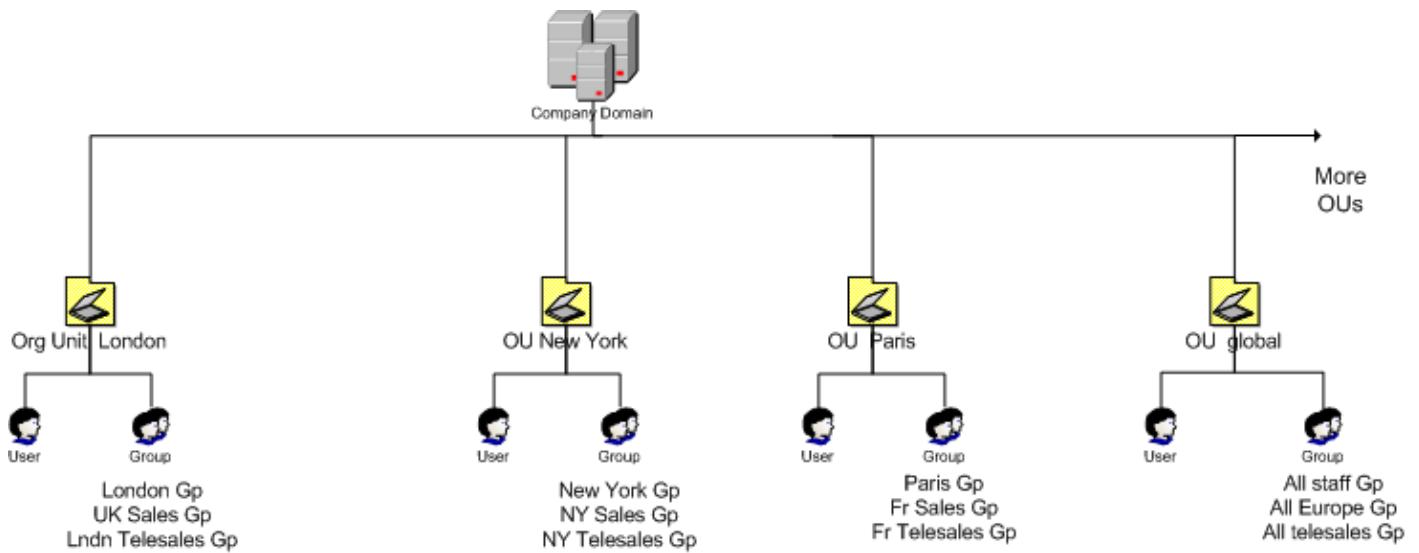


## 11. Bibliografia

- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows Server 2012.
- Somebooks.es (2014). Sistemes Operatius en Xarxa. Disponible en <http://somebooks.es/?p=4787>
- Wikipedia. Sistema Operatiu de xarxa. Disponible en [http://es.wikipedia.org/wiki/sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/sistema_operativo_de_red)
- Blog de SoporteTI. Disponible en: <http://blog.soporteti.net/>
- Elaboració pròpria.

# Sistemes Informàtics

## UD12. Part 4. Usuaris, grups i equips



# Índex

1.	Objectius.....	3
2.	Usuaris.....	3
2.1.	Comptes d'usuari predefinides o integrades .....	3
2.2.	Creació d'usuaris en manera gràfica .....	3
2.3.	Creació d'usuaris des de la línia de comandos .....	6
2.4.	Eliminació i deshabilitació de comptes d'usuari .....	8
2.5.	Configuració del compte d'usuari .....	10
2.6.	Configuració d'inici de sessió.....	10
3.	Grups en Active Directory .....	12
3.1.	Grups Predefinitos o integrats.....	13
3.2.	Creació de grups mitjançant la interfície gràfica.....	14
3.3.	Creació de grups mitjançant la línia de comandos .....	17
3.4.	Eliminació de grups .....	17
4.	Unitats Organitzatives.....	18
4.1.	Creació d'UO .....	18
4.2.	Eliminació d'UO .....	19
5.	Cas Pràctic: Creació de l'estructura d'una organització mitjançant la línia de comandos .....	21
5.1.	Creació dels grups .....	22
5.2.	Creació de les unitats organitzatives.....	23
5.3.	Creació d'usuaris .....	24
6.	Consultes sobre objectes del domini: dsquery .....	28
7.	Bibliografia .....	29

## 1. Objectius

- Crear i configurar usuaris tant per la interfície gràfica com per línia de comandos.
- Crear i configurar grups tant per la interfície gràfica com per línia de comandos.
- Crear i administrar Unitats Organitzatives.

## 2. Usuaris

Un compte d'usuari és un objecte que possibilita l'accés als recursos del domini de dues maneres diferents:

- Permet **autenticar la identitat d'un usuari**, perquè només podran iniciar una sessió aquells usuaris que disposen d'un compte en el sistema associada a una determinada contrasenya.
- Permet **autoritzar, o denegar, l'accés als recursos del domini**, perquè, una vegada que l'usuari haja iniciat la seu sessió només tindrà accés als recursos per als quals haja rebut els permisos corresponents.

Quan creuem un compte d'usuari nova, se li assigna un **Identificador de Seguretat (SID)**, Security Identifier que és únic en el domini. De fet, l'únic valor imprescindible perquè el compte mantinga la seu identitat és la seu SID (totes les altres dades o configuracions del compte els podem modificar sense problemes). D'aquesta manera, encara que eliminem un compte i tornem a crear una altra amb el mateix nom, aquesta serà diferent, perquè el seu SID també ho és, cosa que significa que no coincidiran ni els seus certificats de seguretat, ni els seus permisos ni la seu pertinença a determinats grups.

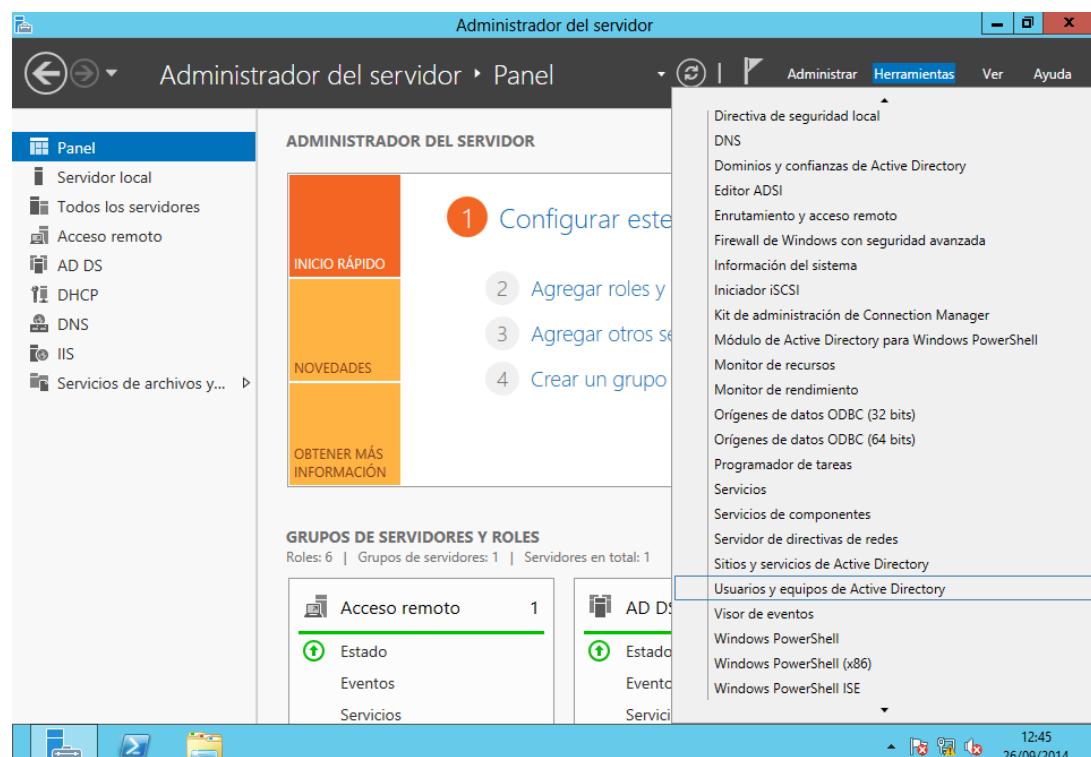
### 2.1. Comptes d'usuari per defecte

Quan es crea el domini, es creen també dos nous comptes: Administrador i Convidat:

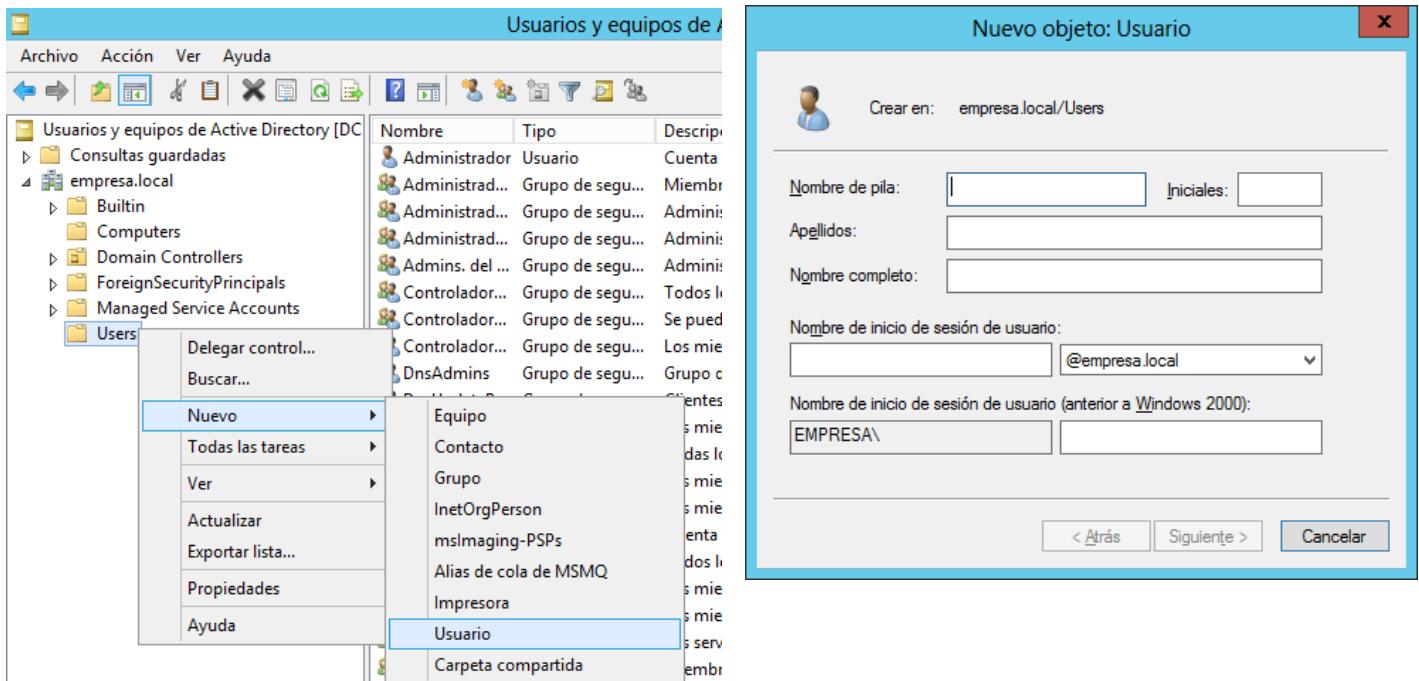
- Administrador: Té control total sobre el domini i no es podrà eliminar ni retirar del grup Administradors (encara que sí que podem canviar-li el nom o desabilitar-la).
- Convidat: Està deshabilitada de manera predeterminada i, encara que no es recomana, pot habilitar-se, per exemple, per a permetre l'accés als usuaris que encara no tenen compte en el sistema o que la tenen deshabilitada. De manera predeterminada no requereix contrasenya, encara que aquesta característica, com qualsevol altra, pot ser modificada per l'administrador.

### 2.2. Creació d'usuaris en manera gràfica

Els usuaris del domini han de tindre un compte per a poder accedir als recursos del mateix després de la seu autenticació enfront del controlador de domini. Per a crear un compte d'usuari mitjançant la interfície gràfica accedirem a l'eina 'Usuaris i equips d'Active Directory' des de 'Eines' del 'Administrador del servidor'.



Una vegada obert l'administrador de 'Usuaris i equips d'Active Directory', es fa clic amb el botó dret sobre 'Users' i en el menú que apareix, se selecciona 'Nou' i a continuació 'Usuari'.



Com a normes generals en crear un nom d'usuari cal observar que:

- Els comptes d'usuari han de ser úniques.
- Els noms d'inici de sessió es poden formar amb una combinació de lletres, majúscules o minúscules, i caràcters alfanumèrics. No s'accepten els caràcters: / \ | [ ] : ; = < > + \* " @ ?
- El compte d'usuari pot tindre fins a 20 caràcters.

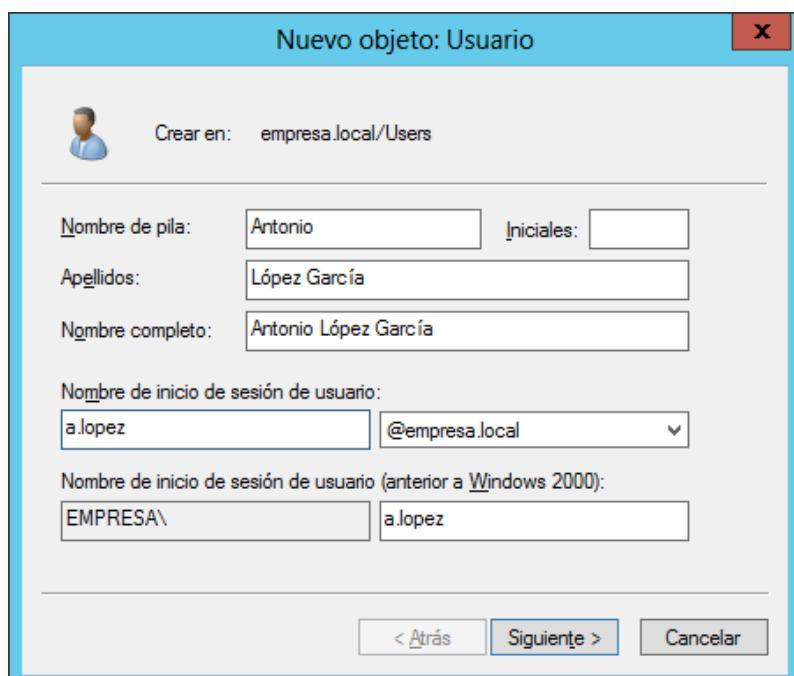
En el quadre de diàleg de creació d'un nou usuari es pot introduir el nom, la(s) inicial(és) del segon nom i els cognoms de l'usuari. Fins ací tota aquesta informació és merament informativa, podria haver-hi, per exemple, dos usuaris el nom complet dels quals fora "Antonio López García".

En el quadre de text 'Nom d'inici de sessió d'usuari' s'introduceix el nom d'usuari seguint l'estruccura que haja predefinit l'administrador del sistema (com s'ha indicat anteriorment, aquest nom **ha de** ser únic en tot el domini).

Alguns exemples de criteris per a la creació del nom d'usuari podrien ser els següents:

- Dues primeres lletres del nom i cognoms. El nom d'inici de sessió de l'usuari Antonio López García seria: anloga.
- Inicial del primer nom i primer cognom complet. El nom d'inici de sessió de l'exemple anterior seria: alopez.
- Diferents caràcters per a separar la inicial del primer nom i el cognom complet: a.lopez, a-lopez, etc.
- Primer nom complet i primer cognom complet separats per un punt: antonio.lopez.

Adoptant el tercer dels criteris anteriors obtindriem el que es mostra en la imatge.

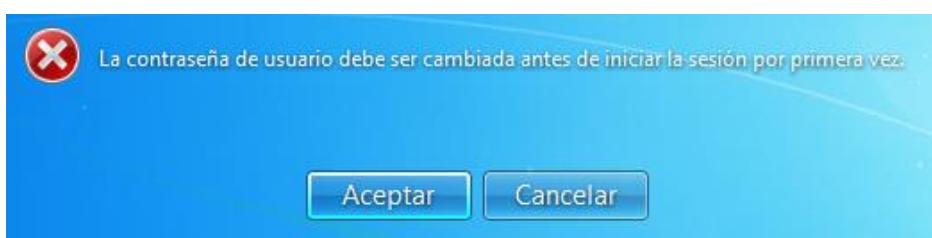


A continuació se sol·licitarà que s'introduïsca la contrasenya de l'usuari. Aquesta ha de complir amb els criteris de complexitat establits. A més apareixen una sèrie d'opcions per a configurar les propietats de la contrasenya:

En la imatge apareixen quatre opcions per a la contrasenya:

- L'usuari ha de canviar la contrasenya en el següent inici de sessió.
- L'usuari no pot canviar la contrasenya.
- La contrasenya mai expira.
- El compte està desabilitat.

La primera de les opcions és útil perquè l'administrador cree el nou usuari amb una contrasenya convencional. L'usuari quan s'autentique per primera vegada en el sistema entrarà amb la contrasenya que li ha proporcionat l'administrador, però automàticament, el sistema li indicarà que ha de ser canviada. D'aquesta manera, l'administrador ja no coneixerà la contrasenya de l'usuari, garantint-se la privacitat d'aquesta.



El segon dels casos ('L'usuari no pot canviar la contrasenya') està pensat per a crear usuaris genèrics, suposem que creuem un compte d'usuari per a utilitzar un ordinador connectat a un escàner, i volem que els usuaris que desitgen utilitzar aqueix escàner, sempre entren amb el mateix compte a l'equip associat a l'escàner. Podríem pensar a utilitzar un usuari genèric del tipus:

- login: escaner
- pass: escaner

En un cas així, no voldríem que accidentalment, o com a acte de vandalisme, la contrasenya fora canviada, invalidant qualsevol possible accés d'altres persones a aqueix compte.

La inhabilitació del tercer cas ('La contrasenya mai expira'), té per objectiu evitar que el sistema demane a l'usuari que canvie la contrasenya periòdicament. Resulta interessant mantindre aquesta opció, encara que puga resultar incòmode canviar la contrasenya cada, per exemple, sis mesos. D'aquesta manera estem protegint-nos de possibles accessos indeguts per part d'algú que haja esbrinat la contrasenya d'alguna manera.

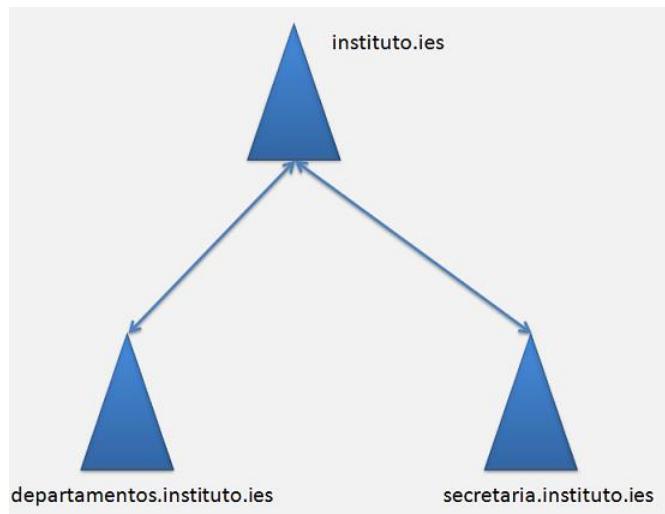
Finalment, la quarta opció ('El compte està desabilitat') serveix per a bloquejar usuaris que no volem que tinguen accés al sistema, però tampoc volem eliminar-los, ja que s'invalidarien els permisos referits a aquest usuari. També pot servir per a crear usuaris que no volem que estiguin operatius fins a un moment determinat.

### 2.3. Creació d'usuaris des de la línia de comandos

L'opció més correcta per a crear usuaris del domini és mitjançant el comando **dsadd user**. Aquest comando ens permetrà definir la ubicació en la qual es creará l'usuari referent a:

- Domini o subdomini.
- Unitat Organitzativa.

Suposem que tenim una estructura de xarxa amb diversos dominis un domini arrel i diversos subdominis), com la que es mostra en la imatge.



Per a crear des del controlador del domini arrel, l'usuari **jgomez** del domini **departaments.institut.ies** hauríem d'executar el següent comando:

```
>>dsadd user "CN=jgomez, CN=Users,  
DC=departaments, DC=institut, DC=ies"  
-pwd Contraseña -disabled no
```

L'eixida de l'execució del comando seria:

```
C:\>dsadd user "CN=jgomez, CN=Users, DC=departamentos, DC=instituto, DC=ies" -pwd Hol@hola -disabled no  
dsadd correcto:CN=jgomez,CN=Users,DC=departamentos,DC=instituto,DC=ies  
C:\>
```

Comprovem efectivament s'ha creat el usuari **jgomez** en el subdomini.

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la ...
Admins. del d...	Grupo de seguri...	Administradores designad...
Controladore...	Grupo de seguri...	Todos los controladores d...
Controladore...	Grupo de seguri...	Los miembros de este gru...
DnsAdmins	Grupo de seguri...	Grupo de administradores ...
DnsUpdatePr...	Grupo de seguri...	Clientes DNS que tienen p...
Equipos del d...	Grupo de seguri...	Todas los servidores y est...
Grupo de rep...	Grupo de seguri...	Los miembros de este gru...
Grupo de rep...	Grupo de seguri...	Los miembros de este gru...
Invitado	Usuario	Cuenta integrada para el ...
Invitados del...	Grupo de seguri...	Todos los invitados del do...
<b>jgomez</b>	<b>Usuario</b>	
Propietarios ...	Grupo de seguri...	Los miembros de este gru...
Publicadores ...	Grupo de seguri...	Los miembros de este gru...
Servidores R...	Grupo de seguri...	Los servidores de este gr...
Usuarios del ...	Grupo de seguri...	Todos los usuarios del do...

És important que els diferents controladors de domini estiguin sincronitzats, ja que en cas contrari la creació dels usuaris donarà error.

Podríem utilitzar un comando una mica més complex per a configurar més detalladament el compte d'un nou usuari:

```
>>dsadd user "CN=rperez, CN=Users, DC=departaments, DC=institut, DC=ies"
-pwd Hola@hola -disabled no -ln "Pérez García" -fn Roberto -mustchpwd
yes -canchpwd yes -memberof "CN=Alumnes, CN=Users, DC=departaments,
DC=institut, DC=ies"
```

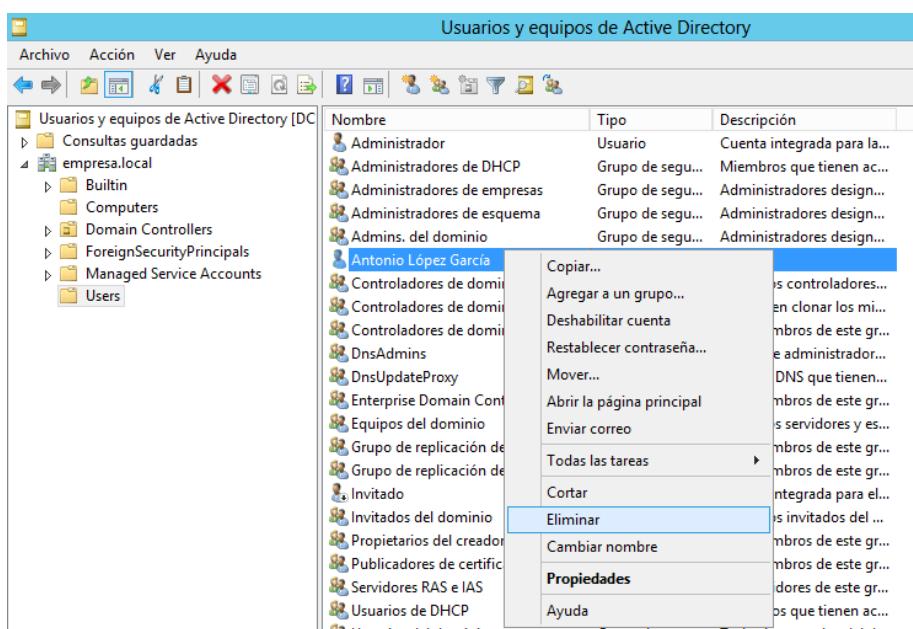
Algunes de les opcions utilitzades són:

- -ln: cognoms de l'usuari.
- -fn: nom de l'usuari.
- -mustchpwd: obligació de canviar la contrasenya en el primer inici de sessió.
- -canchpwd: l'usuari pot canviar la contrasenya.
- -memberof: grup del qual és membre l'usuari.

## 2.4. Eliminació i deshabilitació de comptes d'usuari

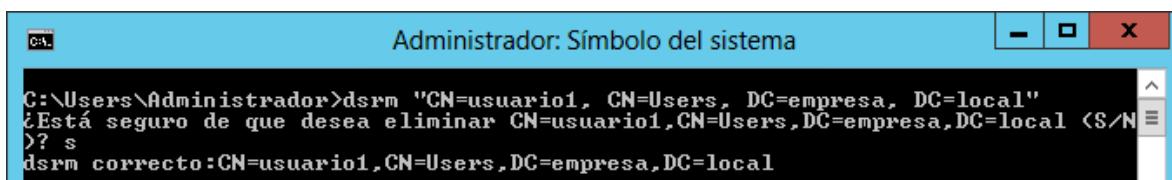
Com hem comentat anteriorment, cada compte d'usuari creada en un domini té un **identificador de seguretat (SID)** únic. Si eliminem un compte d'usuari i després tornem a crear-la exactament igual, l'identificador SID serà diferent. Això es tradueix en què no es podran recuperar els permisos i privilegis del compte eliminat.

Si finalment decidim eliminar el compte, accedirem a 'Usuaris i equips d'Active Directory', seleccionarem l'usuari a eliminar, farem clic amb el botó dret i després 'Eliminar'.



Per a eliminar un compte d'usuari mitjançant la línia de comandos utilitzarem el comando `dsrm`. En l'exemple següent eliminariem el compte de l'usuari `usuari1` del domini `empresa.local`.

```
>>dsrm "CN=usuari1, CN=Users, DC=empresa, DC=local"
```



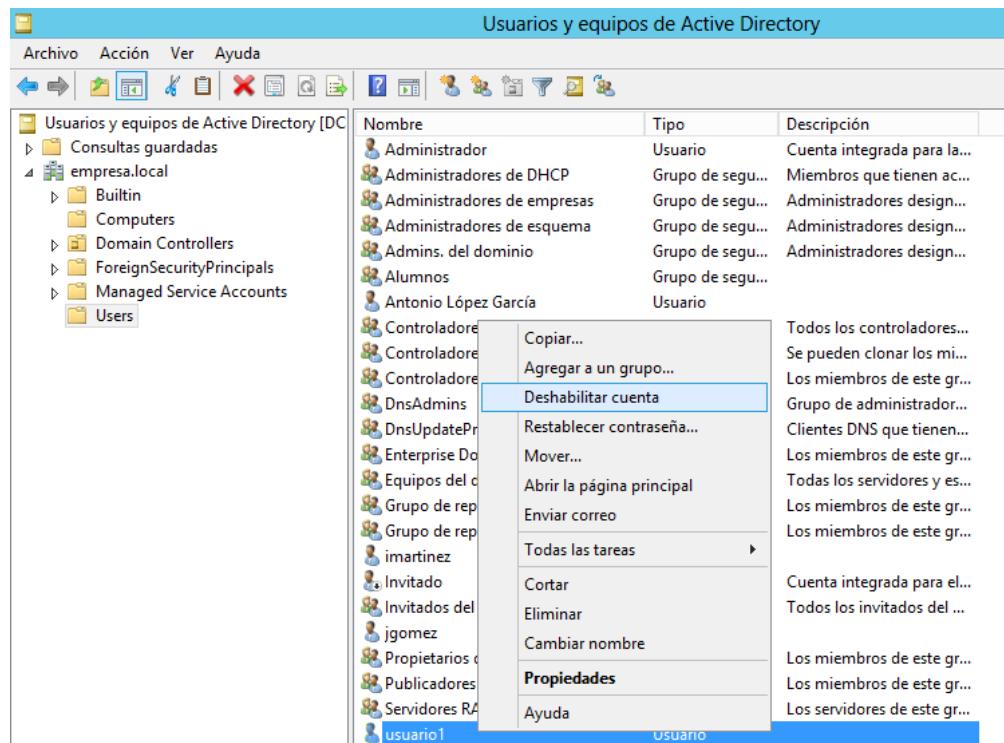
Per a evitar possibles problemes amb l'eliminació de comptes, el qual és un procés definitiu, se sol optar per la **deshabilitació de comptes**.

Suposem una empresa en la qual un treballador cessarà la seu activitat. L'administrador de sistemes deshabilitarà el seu compte en la data en la qual el treballador vaja a deixar de prestar els seus serveis.

D'aquesta manera el treballador cessat ja no podrà iniciar sessió en el domini, però si passat un temps fera falta tornar a iniciar sessió, bastaria amb habilitar de nou el compte.

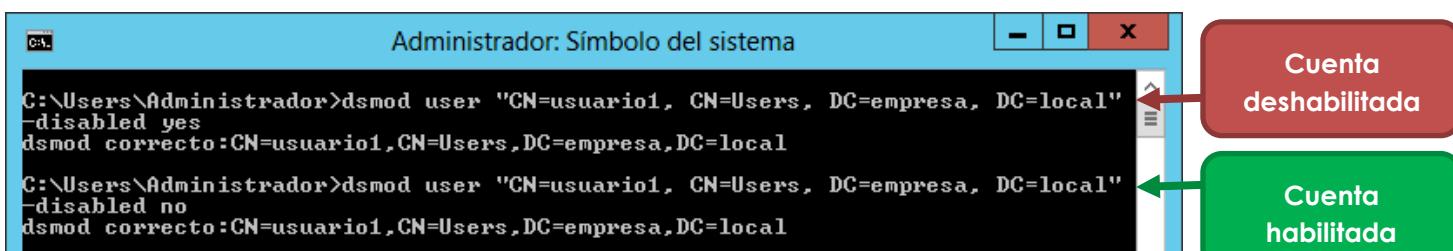
Un altre exemple real podria ser una universitat, en la qual cada alumne té un compte d'usuari. Quan finalitza els seus estudis, el compte és deshabilitat, però si posteriorment cursa altres estudis, el compte tornaria a habilitar-se.

Com abans, accedirem a 'Usuaris i equips d'Active Directory' i fent clic amb el botó secundari sobre l'usuari a bloquejar, seleccionarem l'opció 'Deshabilitar el compte'.



Per a **deshabilitar** un compte d'usuari mitjançant la línia de comandos utilitzarem el comando **dsmod** amb el modificador **-disabled** amb valor **yes**:

```
>>dsmod user "CN=usuari1, CN=Users, DC=empresa, DC=local" -disabled yes
```



## 2.5. Configuració del compte d'usuari

Els comptes d'usuaris creades en el domine es poden configurar d'una manera detallada en la finestra 'Propietats del compte', per a això es fa clic amb el botó dret del ratolí sobre el compte d'usuari que es desitja editar.

Les propietats del compte d'usuari quin més utilitzarem durant aquest curs seran:

- **General:** Es pot modificar el Nom, Cognom, etc. i a més modificar informació administrativa com la descripció, oficina, telèfon, email i pàgina web.
- **Compte:** Es pot configurar algunes característiques de la contrasenya d'usuari, les hores d'inici de sessió, la caducitat del compte, **desbloquejar** el compte, etc.
- **Perfil:** En aquesta fitxa es poden editar aspectes importants com són la ubicació física del perfil de l'usuari i el fitxer de comandos d'inici de sessió.
- **Membre de:** Es mostra el llistat de grups als quals l'usuari pertany.

Propiedades: Antonio López García

Marcado	Entorno	Sesiones	Control remoto			
Perfil de Servicios de Escritorio remoto		COM+				
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de

Antonio López García

Nombre de pila: Antonio Iniciales:

Apellidos: López García

Nombre para mostrar: Antonio López García

Descripción:

Oficina:

Número de teléfono:

Correo electrónico:

Página web:

Aceptar Cancelar Aplicar Ayuda

## 2.6. Configuració d'inici de sessió

Windows Server 2019 permet configurar els horaris en els quals es pot iniciar sessió. Aquesta funcionalitat pot ser útil per a controlar accessos al sistema a hores 'anòmals', o per a evitar que usuaris de, per exemple, el torn de vesprada, puguen accedir al sistema amb el compte d'un usuari del torn de demà.

Per a establir els horaris en els quals es pot iniciar sessió se seguiran els següents passos.

- En 'Usuaris i Equips d'Active Directory' se selecciona l'usuari buscat, i fent clic amb el botó dret s'accedeix a 'Propietats'.
- S'obre el quadre de diàleg 'Propietats' del compte seleccionat. Es fa clic en la fitxa 'Compte' i després es fa clic en el botó 'Hores d'inici de sessió'.

Propiedades: ANTONIO LOPEZ GARCIA

Marcado	Entorno	Sesiones	Control remoto			
Perfil de Servicios de Escritorio remoto		COM+				
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de

Nombre de inicio de sesión de usuario: a.lopez @empresa.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000): EMPRESA\ a.lopez

Horas de inicio de sesión... Iniciar sesión en...

Desbloquear cuenta

Opciones de cuenta:

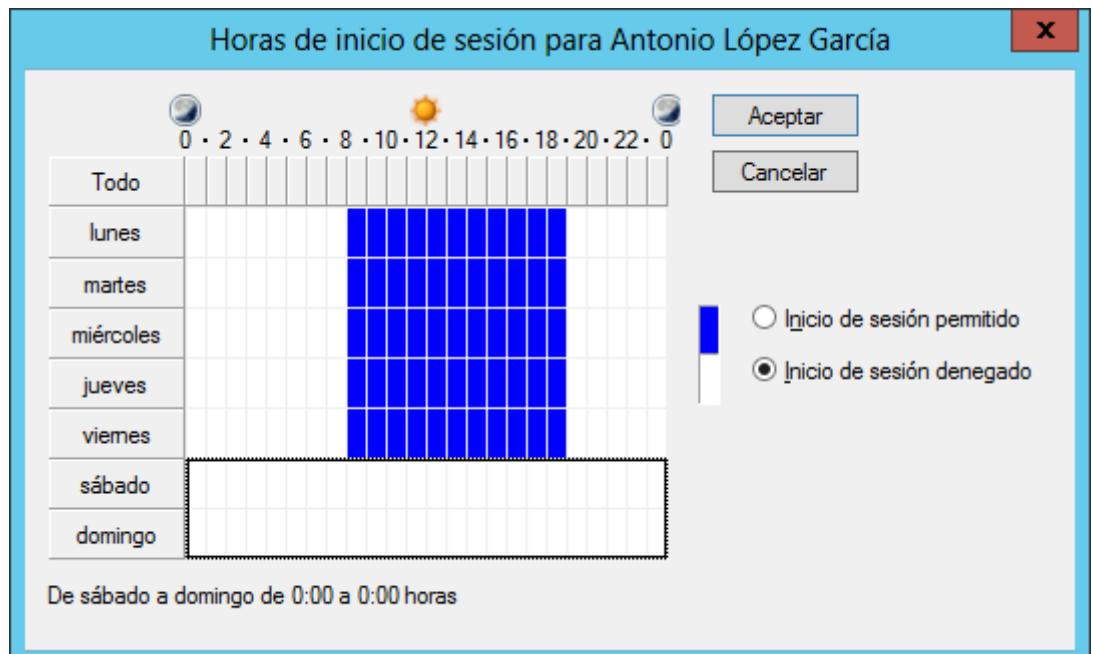
El usuario debe cambiar la contraseña en el siguiente inicio de sesión  
 El usuario no puede cambiar la contraseña  
 La contraseña nunca expira  
 Almacenar contraseña utilizando cifrado reversible

La cuenta expira

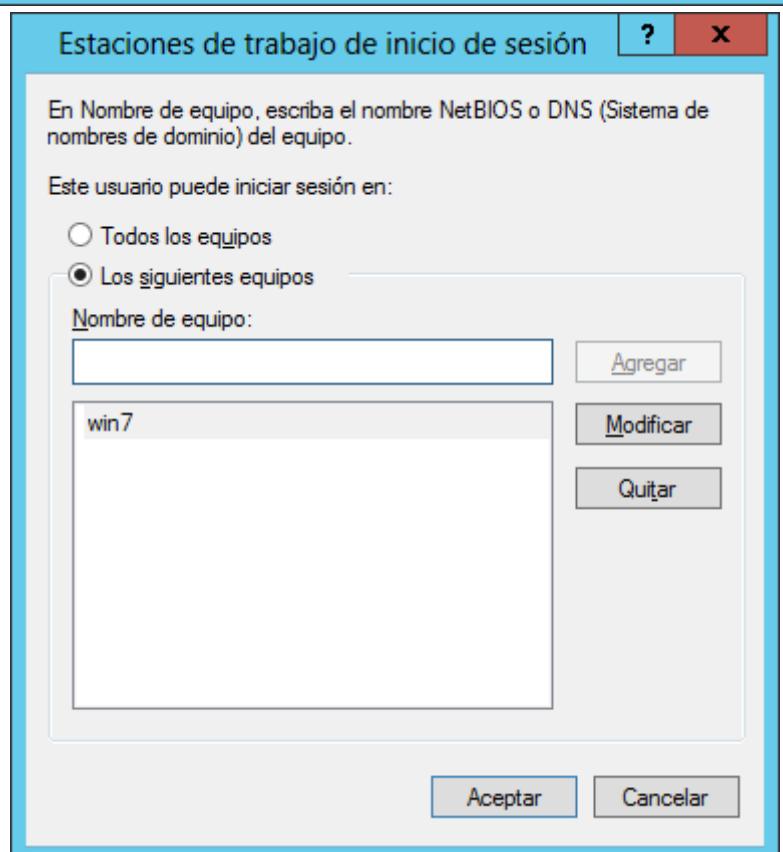
Nunca  
 Fin de: domingo , 26 de octubre de 2014

Aceptar Cancelar Aplicar Ayuda

En color blau es mostren les hores d'inici permeses. Per a denegar l'accés n'hi ha prou amb seleccionar les hores a les quals es desitja limitar l'accés i es marca l'opció 'Inici de sessió denegat'.



A tot això cal afegir que es pot configurar l'inici de sessió en determinats equips. Per a això n'hi ha prou amb fer clic en el botó 'Iniciar sessió en...'. Es pot seleccionar si l'usuari pot iniciar sessió en 'Tots els equips' o solo en alguns equips determinats.



X

?

X

Aceptar

Cancelar

10

### 3. Grups en Active Directory

Els grups són un tipus de contingut que permeten definir conjunts d'usuaris i definir permisos basant-nos en aquella pertinença al grup, en lloc de fer-lo de manera individual, usuari per usuari. Això no sols facilita l'administració del domini sinó que també permet treballar d'una manera menys propensa a errors. Com a pauta general, l'agrupació d'objectes sol facilitar les tasques d'administració reduint les possibilitats d'error.

Existeixen dos grans tipus de grups en el Directori Actiu de Windows:

- **Grups de seguretat:** aquest tipus de grups permet definir permisos per a recursos del domini. Són els utilitzats en les llistes de control d'accés (ACLs) que s'estudiaran més endavant. Aquest tipus de grups són els que s'utilitzaran en l'administració de la xarxa.
- **Grups de distribució:** no posseeixen característiques de seguretat, únicament són un llistat d'usuaris per a missatgeria.

Dins dels grups de seguretat existeixen al seu torn tres àmbits:

- **Grup Universal:** és un grup els permisos del qual s'estenen a diversos dominis. A més aquest tipus de grups pot estar format per usuaris o grups d'usuaris de diferents dominis.
- **Grup Global:** és molt similar als grups universals, és a dir poden permetre l'accés a recursos de qualsevol dels dominis de l'arbre del Directori Actiu, però amb l'excepció que tots els membres del grup han de pertànyer **al mateix domini**.
- **Grup Local del Domini:** és un grup creat en un domini amb membres que poden provindre d'altres dominis i que únicament pot tindre accés a recursos dins del seu domini.

#### En quins casos utilitzar un àmbit o un altre de grup?

Els grups universals soLEN tindre la seua utilitat en grans empreses en les quals s'ha definit un bosc de dominis assignant dominis a cadascun dels seus departaments o divisions. En aquesta mena d'estructures, quan es realitza una modificació en el grup, aquesta ha de replicar-se en tots els controladors de domini que estiguin configurats com a catàleg global.

En xarxes de domini únic es poden aplicar grups globals que tindran major sentit quan es definisca un segon domini, la qual cosa pot ocórrer en el moment en el qual hi haja una ampliació de l'organització.

Com a pautes generals per a l'administració de xarxes tindrem en compte les següents consideracions:

1. No s'ha d'assignar un àmbit més ampli del necessari.
2. Els grups locals de domini no es poden processar en altres dominis.
3. Un grup global no es replica fora del domini ja que no forma part del pla de replicació del catàleg global.
4. Els grups universals es repliquen per tota la xarxa generant trànsit que pot tindre una certa incidència en el rendiment d'aquesta (encara que aquest aspecte s'ha optimitzat en Windows Server 2008 i posteriors enfront d'edicions anteriors).
5. Si un grup universal està compost per grups globals i es produueixen canvis dins dels grups globals, no es produeix un canvi en el catàleg global, i per tant aquella modificació no comporta una replicació en tots els controladors de domini del bosc.

### 3.1. Grups predefinits o integrats

En instal·lar el Directori Actiu podem comprovar que s'han generat automàticament una sèrie de grups predefinits amb uns permisos concorde a les seues funcions assignades.

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la administración del equipo
Administradores de empresas	Grupo de seguridad - Universal	Administradores designados de la empresa
Administradores de esquema	Grupo de seguridad - Universal	Administradores designados del esquema
Admins. del dominio	Grupo de seguridad - Global	Administradores designados del dominio
Controladores de dominio	Grupo de seguridad - Global	Todos los controladores de dominio del dominio
Controladores de dominio clonables	Grupo de seguridad - Global	Se pueden clonar los miembros del grupo que se creen
Controladores de dominio de sólo lectura	Grupo de seguridad - Global	Los miembros de este grupo son controladores de sólo lectura
DnsAdmins	Grupo de seguridad - Dominio local	Grupo de administradores de DNS
DnsUpdateProxy	Grupo de seguridad - Global	Clientes DNS que tienen permiso para efectuar actualizaciones
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de este grupo son controladores de sólo lectura
Equipos del dominio	Grupo de seguridad - Global	Todas los servidores y estaciones de trabajo unidos al dominio
Grupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local	Los miembros de este grupo no pueden replicar las contraseñas
Grupo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden replicar las contraseñas
Invitado	Usuario	Cuenta integrada para el acceso como invitado
Invitados del dominio	Grupo de seguridad - Global	Todos los invitados del dominio
Propietarios del creador de directivas de grupo	Grupo de seguridad - Global	Los miembros de este grupo pueden modificar las directivas de grupo
Publicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden publicar certificados
Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden obtener proveedores de servicios
Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios del dominio
WinRMRemoteWMIUsers__	Grupo de seguridad - Dominio local	Members of this group can access WMI resources

Usuaris i grups creats automàticament en instal·lar el Directori Actiu.

Nombre	Tipo	Descripción
Acceso compatible con versiones anteriores de Windows 2000	Grupo de seguridad - Dominio local	Un grupo de compatibilidad anterior a Windows 2000
Administradores	Grupo de seguridad - Dominio local	Los administradores tienen acceso completo
Administradores de Hyper-V	Grupo de seguridad - Dominio local	Los miembros de este grupo tienen acceso a Hyper-V
Certificate Service DCOM Access	Grupo de seguridad - Dominio local	Los miembros de este grupo se pueden autorizar para acceder a servicios de certificado
Creadores de confianza de bosque de entrada	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden crear relaciones de confianza
Duplicadores	Grupo de seguridad - Dominio local	Pueden replicar archivos en un dominio
Grupo de acceso de autorización de Windows	Grupo de seguridad - Dominio local	Los miembros de este grupo tiene acceso a recursos
IIS_IUSRS	Grupo de seguridad - Dominio local	Grupo integrado usado por Internet Information Services
Invitados	Grupo de seguridad - Dominio local	De forma predeterminada, los invitados no tienen permisos
Lectores del registro de eventos	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden leer el registro de eventos
Operadores criptográficos	Grupo de seguridad - Dominio local	Los miembros tienen autorización para operaciones criptográficas
Operadores de asistencia de control de acceso	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden administrar el control de acceso
Operadores de configuración de red	Grupo de seguridad - Dominio local	Los miembros en este equipo pueden administrar la red
Operadores de copia de seguridad	Grupo de seguridad - Dominio local	Los operadores de copia de seguridad tienen permisos
Opers. de cuentas	Grupo de seguridad - Dominio local	Los miembros pueden administrar cuentas
Opers. de impresión	Grupo de seguridad - Dominio local	Pueden administrar impresoras del dominio
Opers. de servidores	Grupo de seguridad - Dominio local	Los miembros pueden administrar servidores
Servidores de acceso remoto RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo permiten la ejecución de aplicaciones remotas
Servidores de administración RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden administrar RDS
Servidores de extremo RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo ejecutan aplicaciones remotas
Servidores de licencias de Terminal Server	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden administrar licencias
Usuarios	Grupo de seguridad - Dominio local	Los usuarios no pueden hacer cambios
Usuarios COM distribuidos	Grupo de seguridad - Dominio local	Los miembros pueden iniciar, activar y detener servicios
Usuarios de administración remota	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden administrar el sistema
Usuarios de escritorio remoto	Grupo de seguridad - Dominio local	A los miembros de este grupo se les permite iniciar sesiones remotas
Usuarios del monitor de sistema	Grupo de seguridad - Dominio local	Los miembros de este grupo tienen acceso a los datos del sistema
Usuarios del registro de rendimiento	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden registrar datos

Grups integrats denominats Built-in.

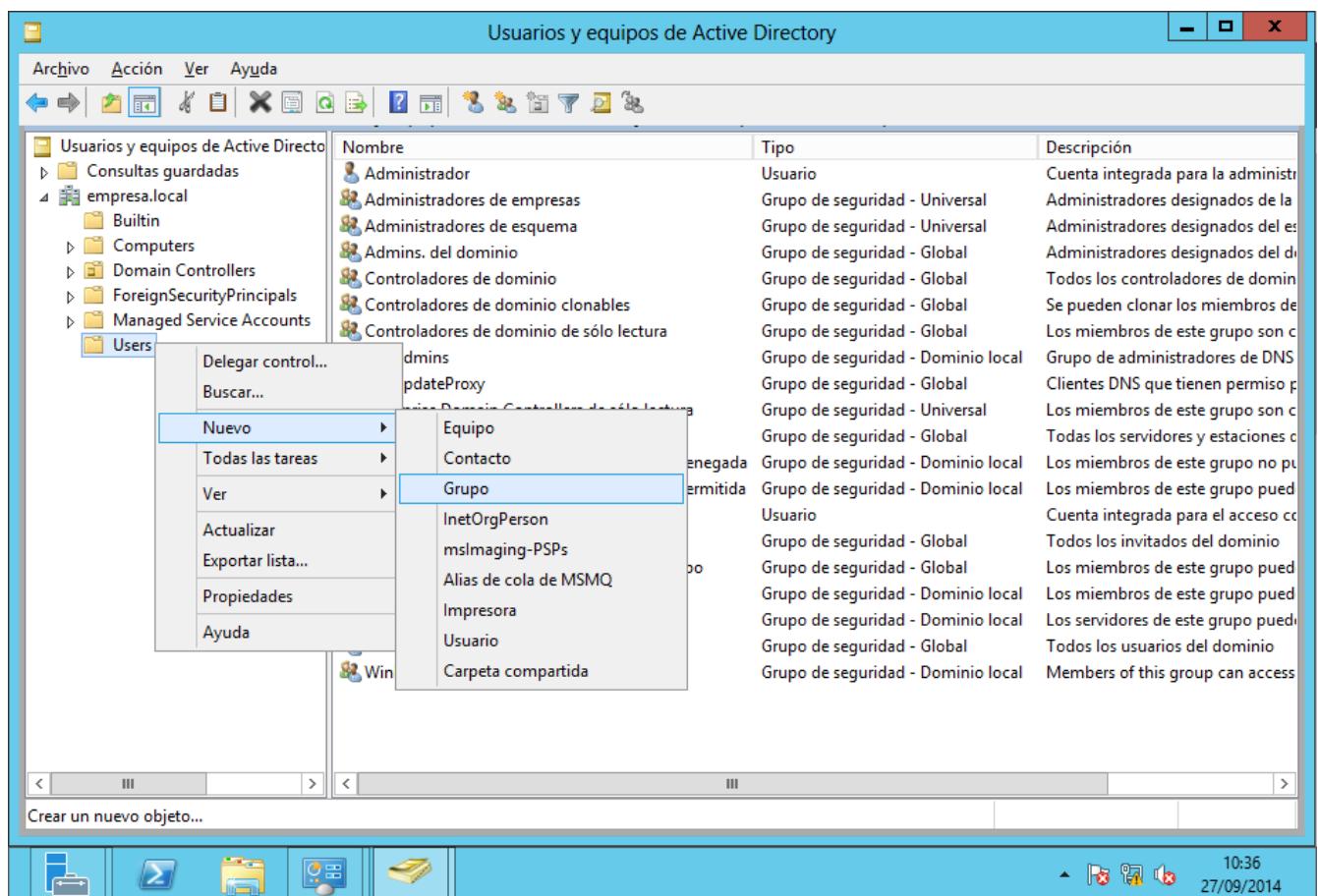
Examinem les funcions d'alguns dels grups més utilitzats:

- **Usuaris del domini:** grup global que conté **tots** els comptes d'usuaris el domini.
- **Administradors del domini:** grup global que permet als seus membres fer tasques d'administració del domini.
- **Administradors d'empresa:** grup universal que permet als seus membres fer tasques d'administració en **tots els dominis de la xarxa**.
- **Administradors d'esquema:** grup universal que permet als seus membres modificar l'estructura dels objectes del Directori Actiu.
- **Administradors:** grup local que permet als seus membres fer tasques d'administració en el controlador de domini.
- **Operadors de còpies de seguretat:** grup local que permet als seus membres realitzar còpies de seguretat o restaurar arxius dins del domini.
- **Operadors de compte:** grup local que permet als seus membres crear, editar i eliminar comptes d'usuari i grups.
- **Operadors d'impressió:** grup local que permet als seus membres configurar i administrar l'ús d'impressores de xarxa.
- **Operadors de servidor:** grup local que permet als seus membres crear carpetes compartides en el servidor i realitzar còpies de seguretat o restaurar arxius en el controlador de domini.
- **Usuaris:** grup local que limita les possibilitats que un usuari faça un canvi accidental en el sistema però sí que permet executar la majoria de les aplicacions.

És important adonar-se del considerable estalvi de temps per a l'administrador que permet l'existència de grups predefinits per a tasques molt concretes.

### 3.2. Creació de grups mitjançant la interfície gràfica

Els grups es creen de manera molt similar a com es creaven els usuaris en el Directori Actiu.



S'obrirà un quadre de diàleg que ens permetrà introduir el nom del grup, així com el seu àmbit i tipus.

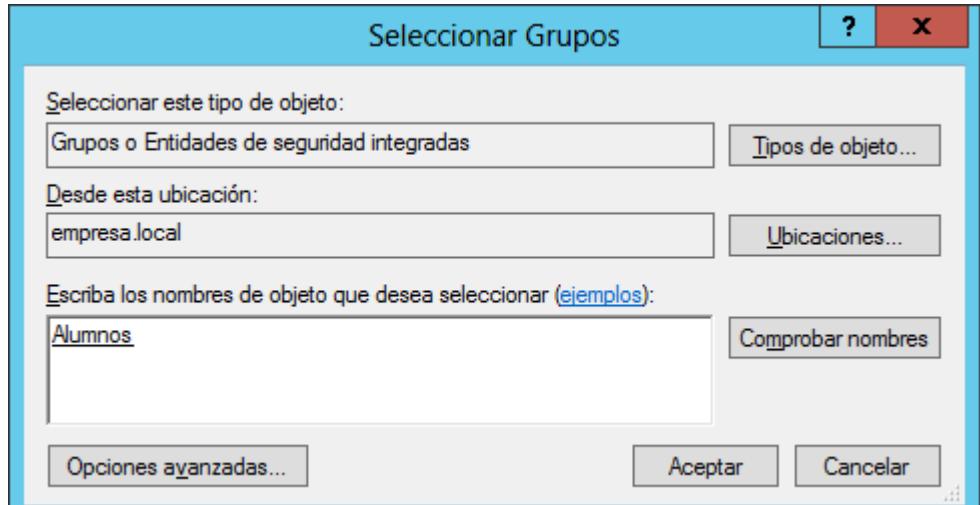


Per defecte se'n indica que l'àmbit del grup serà 'Global' i el tipus de grup serà de 'Seguretat'. En principi, si no tenim unes necessitats que justifiquen el contrari, crearem els grups amb aqueixes propietats. Després de prémer 'Acceptar' ens apareixerà el nou grup en el llistat de 'Usuaris i equips d'Active Directory'.

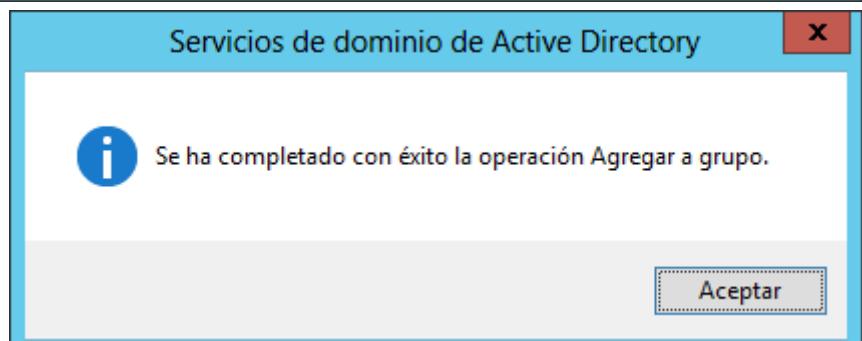
Nombre	Tipo
Administrador	Usuario
Administradores de empresas	Grupo de seguridad - Universal
Administradores de esquema	Grupo de seguridad - Universal
Admins. del dominio	Grupo de seguridad - Global
<b>Alumnos</b>	<b>Grupo de seguridad - Global</b>
Controladores de dominio	Grupo de seguridad - Global
Controladores de dominio clonables	Grupo de seguridad - Global
Controladores de dominio de sólo lectura	Grupo de seguridad - Global
DnsAdmins	Grupo de seguridad - Dominio local

Si volem afegir usuaris en el grup n'hi ha prou amb seleccionar l'usuari i en el menú que s'obrirà en fer clic amb el botó dret, accedir a l'opció 'Agregar a un grup'.

S'obrirà un quadre en el qual podrem indicar/buscar el grup al qual volem afegir l'usuari.



Després d'acceptar, apareixerà un missatge indicant que l'operació s'ha realitzat amb èxit i podrem comprovar en les propietats de l'usuari que efectivament és membre del grup 'Alumnes'.



Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para
Administradores de DHCP	Grupo de segu...	Miembros que tienen a
Administradores de empresas	Grupo de segu...	Administradores desig
Administradores de esquema	Grupo de segu...	
Admins. del dominio	Adm...	
Alumnos	Grupo de segu...	
<b>Antonio López García</b>	<b>Usuario</b>	
Controladores de dominio	Copiar...	
Controladores de dominio clor	Agregar a un grupo...	
Controladores de dominio de s	Deshabilitar cuenta	
DnsAdmins	Restablecer contraseña...	
DnsUpdateProxy	Mover...	
Enterprise Domain Controllers	Abrir la página principal	
Equipos del dominio	Enviar correo	
Grupo de replicación de contra	Todas las tareas	
Grupo de replicación de contra	Cortar	
imartinez	Eliminar	
Invitado	Cambiar nombre	
Invitados del dominio		
igomez		
Propietarios del creador de dire		
Publicadores de certificados		
Servidores RAS e IAS		

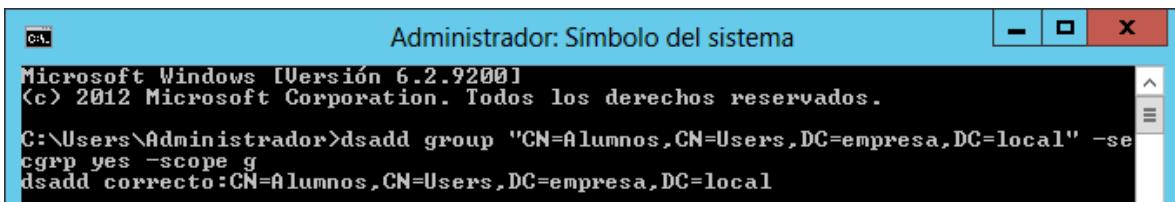
Marcado		Entorno		Sesiones		Control remoto							
Perfil de Servicios de Escritorio remoto						COM+							
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de							
<b>Miembro de:</b>													
<table border="1"> <thead> <tr> <th>Nombre</th> <th>Carpetas de los Servicios de dominio de Active Dir..</th> </tr> </thead> <tbody> <tr> <td>Alumnos</td> <td>empresa.local/Users</td> </tr> <tr> <td>Usuarios del dominio</td> <td>empresa.local/Users</td> </tr> </tbody> </table>								Nombre	Carpetas de los Servicios de dominio de Active Dir..	Alumnos	empresa.local/Users	Usuarios del dominio	empresa.local/Users
Nombre	Carpetas de los Servicios de dominio de Active Dir..												
Alumnos	empresa.local/Users												
Usuarios del dominio	empresa.local/Users												
<input type="button" value="Agregar..."/> <input type="button" value="Quitar"/>													
<b>Grupo principal:</b> Usuarios del dominio <input type="button" value="Establecer grupo principal"/> No es necesario cambiar Grupo principal si no tiene clientes de Macintosh o aplicaciones compatibles con POSIX.													
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/> <input type="button" value="Ayuda"/>													

### 3.3. Creació de grups mitjançant la línia de comandes

Per a crear un grup des de la consola, el comando utilitzat és: dsadd group. Per a especificar si el grup és de seguretat o de distribució s'utilitza l'opció: -secgrp yes ( o -secgrp no si es tracta d'un grup de distribució). Per a especificar l'àmbit del grup com a universal, global o local s'utilitza -scope seguit de o, g o l, respectivament.

Si volem crear el grup 'Alumnes' com en el cas anterior escriuríem el següent comando:

```
>>dsadd group "CN=Alumnes,CN=Users,DC=empresa,DC=local" -secgrp yes  
-scope g
```

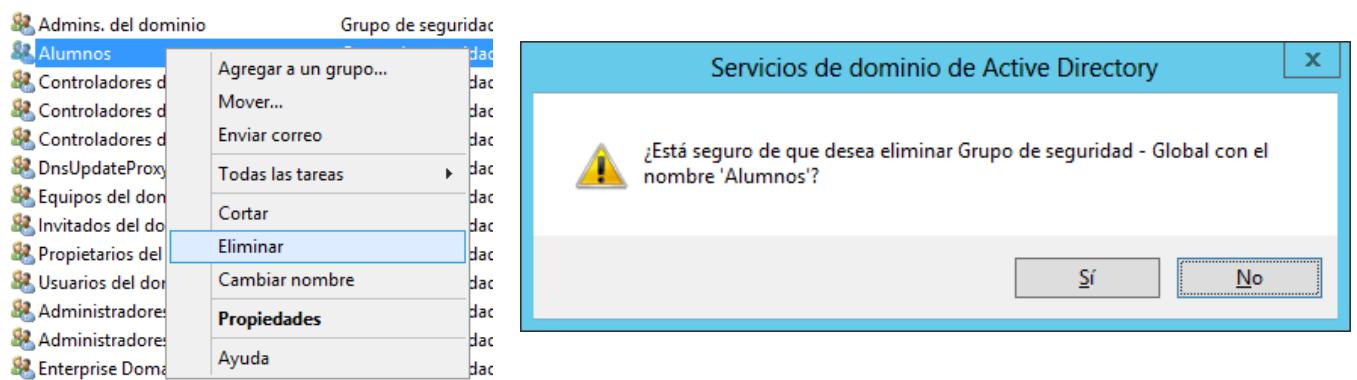


Si observem l'administrador de 'Usuaris i Equips d'Active Directory', veiem que el grup s'ha creat correctament.

Es pot obtindre més informació sobre l'administració dels grups per la línia de comandos en [el següent enllaç del Technet de Microsoft](#).

### 3.4. Eliminació de grups

Fent clic amb el botó dret sobre el grup triem l'opció "eliminar".



## 4. Unitats Organitzatives

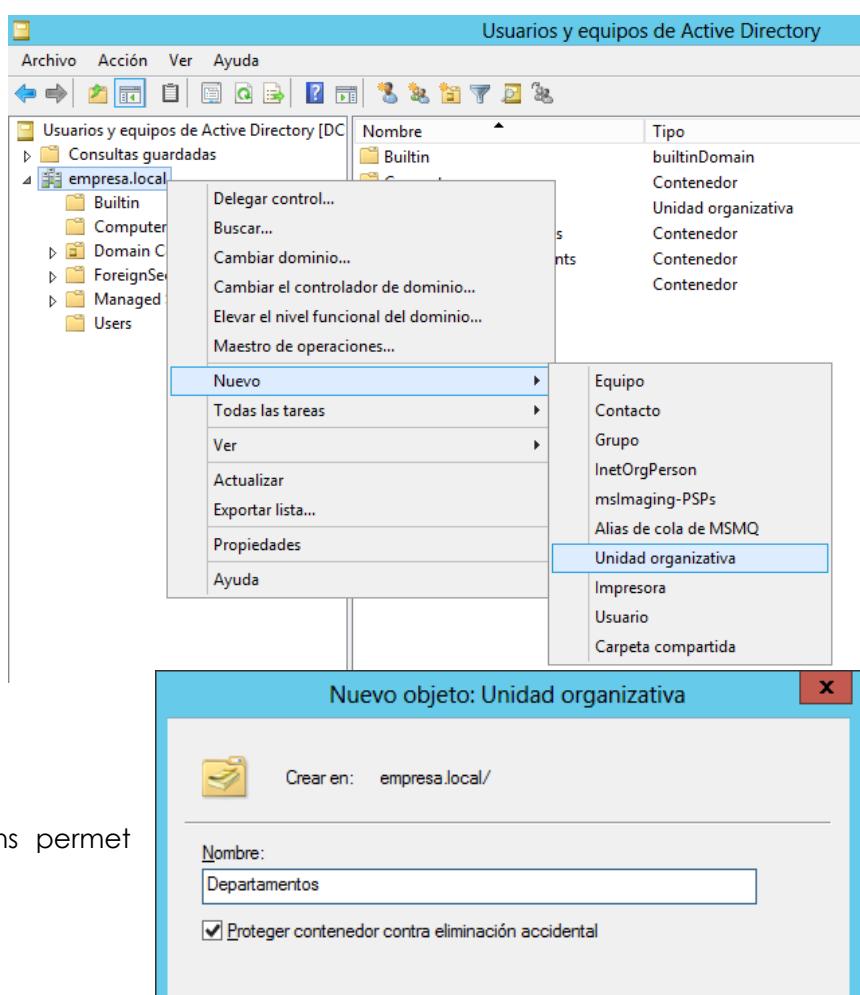
Una unitat organitzativa és un contenidor d'objectes (usuaris, grups, equips, altres unitats organitzatives, etc.) pertanyents a un **mateix** domini. Són especialment útils per a reproduir l'estructura de l'empresa on es trobe el domini. És a dir, si per exemple, una empresa està dividida en tres departaments (direcció, vendes i producció), podem crear tres unitats organitzatives corresponents a aquests tres departaments, on incloguem tots els objectes del domini corresponents a cadascuna de les àrees de l'empresa.

La seua utilitat radica en dos aspectes fonamentals:

1. D'aquesta manera és molt senzill establir directives de seguretat (les veurem en el tema 5) que s'apliquen a tots els objectes de cada departament.
2. Com dins de la unitat organitzativa, es poden introduir altres unitats organitzatives, es pot replicar l'estructura jeràrquica de l'empresa sense necessitat de crear més dominis o subdominis.

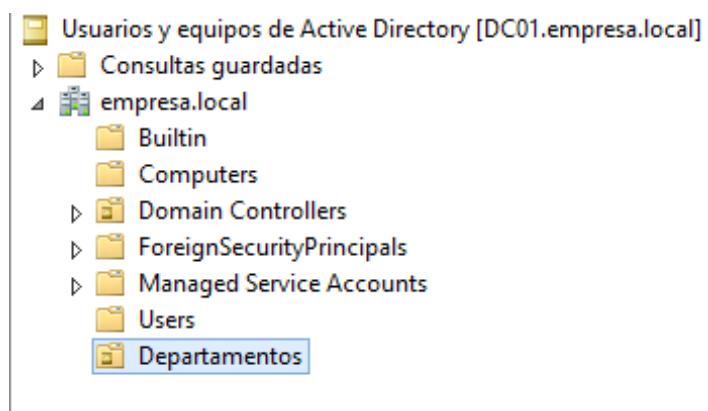
### 4.1. Creació d'UO.

Per a crear una unitat organitzativa obrirem la finestra 'Usuaris i Equips d'Active Directory' (menú de 'Inici', 'Eines Administratives'). A continuació, ens situem sobre el domini i fent clic amb el botó secundari seleccionem 'Nou' i 'Unitat Organitzativa'.

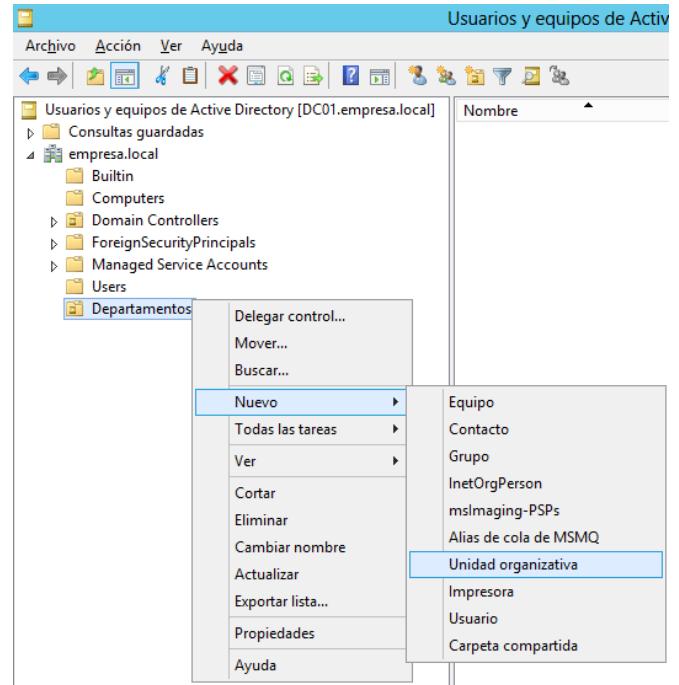


A continuació s'obrirà el diàleg que ens permet indicar el nom del nou objecte.

Després de prémer 'Acceptar', podem comprovar que efectivament s'ha creat la unitat organitzativa dins del domini.



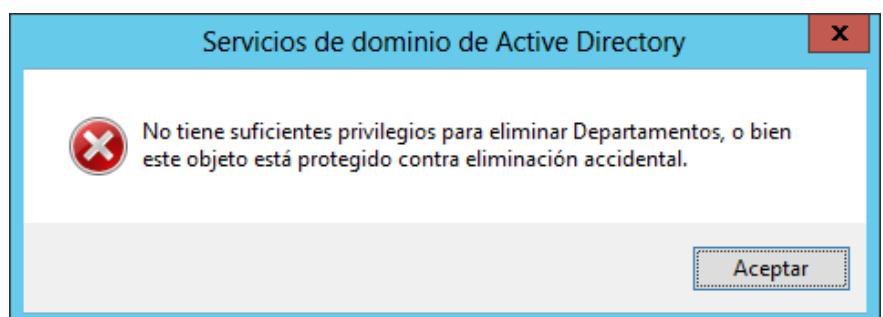
Fent clic amb el botó secundari sobre la unitat organitzativa creada, podem comprovar els elements que podem incloure dins d'aquesta.



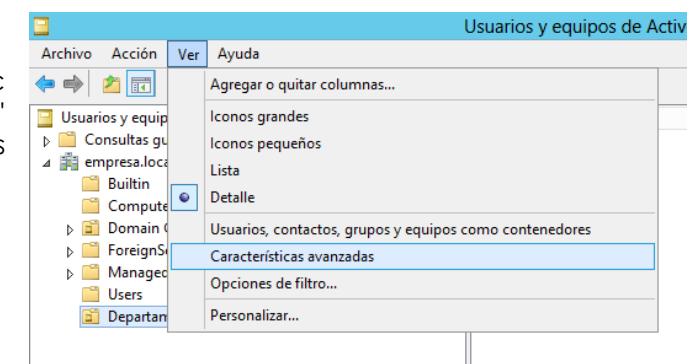
Per a agregar objectes a una unitat organitzativa, bastarà amb seleccionar-los i arrossegitar-los fins a la unitat organitzativa en la qual volem que estiguin inclosos.

## 4.2. Eliminació d'UO

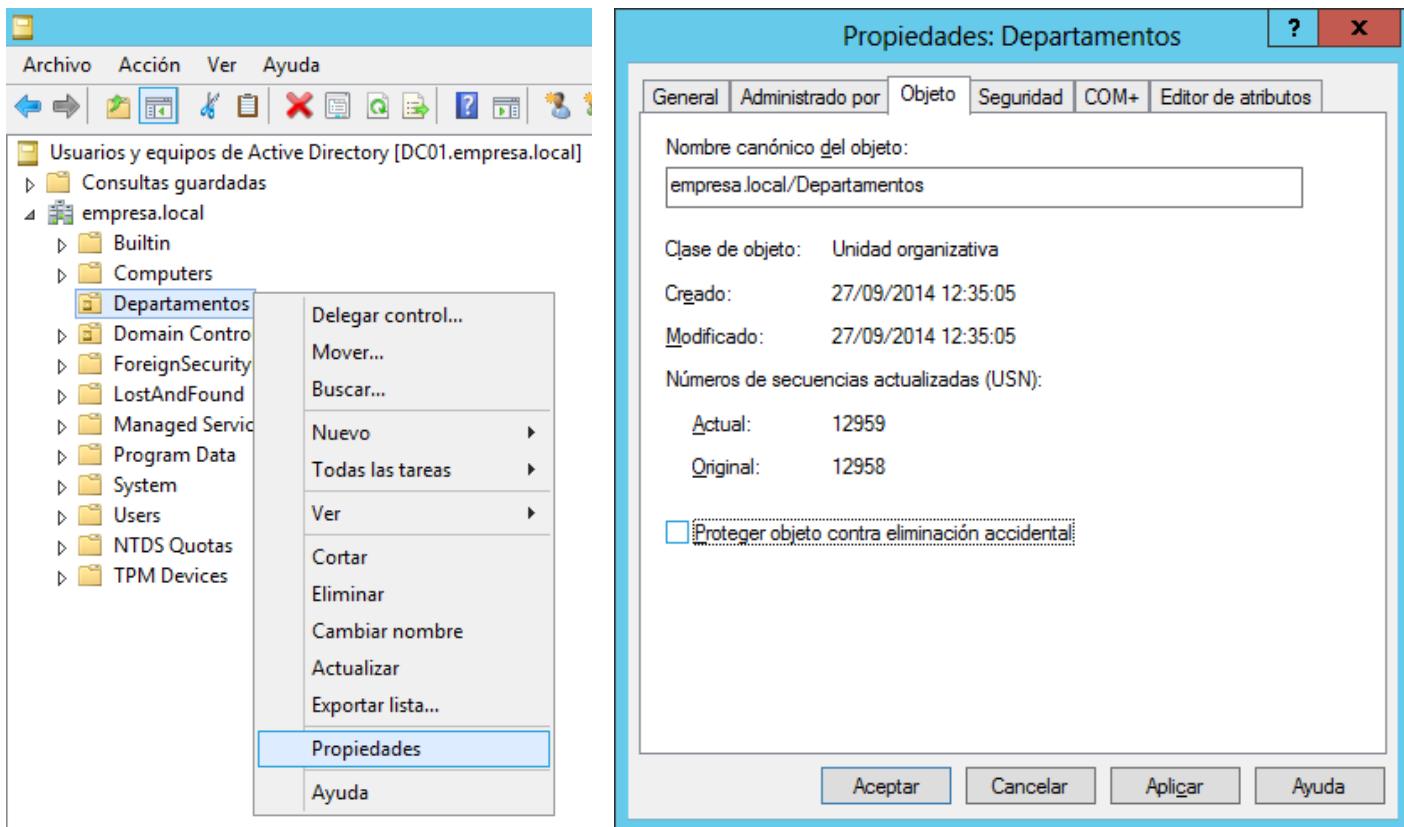
Si tractem d'esborrar una unitat organitzativa, en estar protegides contra eliminacions accidentals, ens apareixerà el següent missatge.



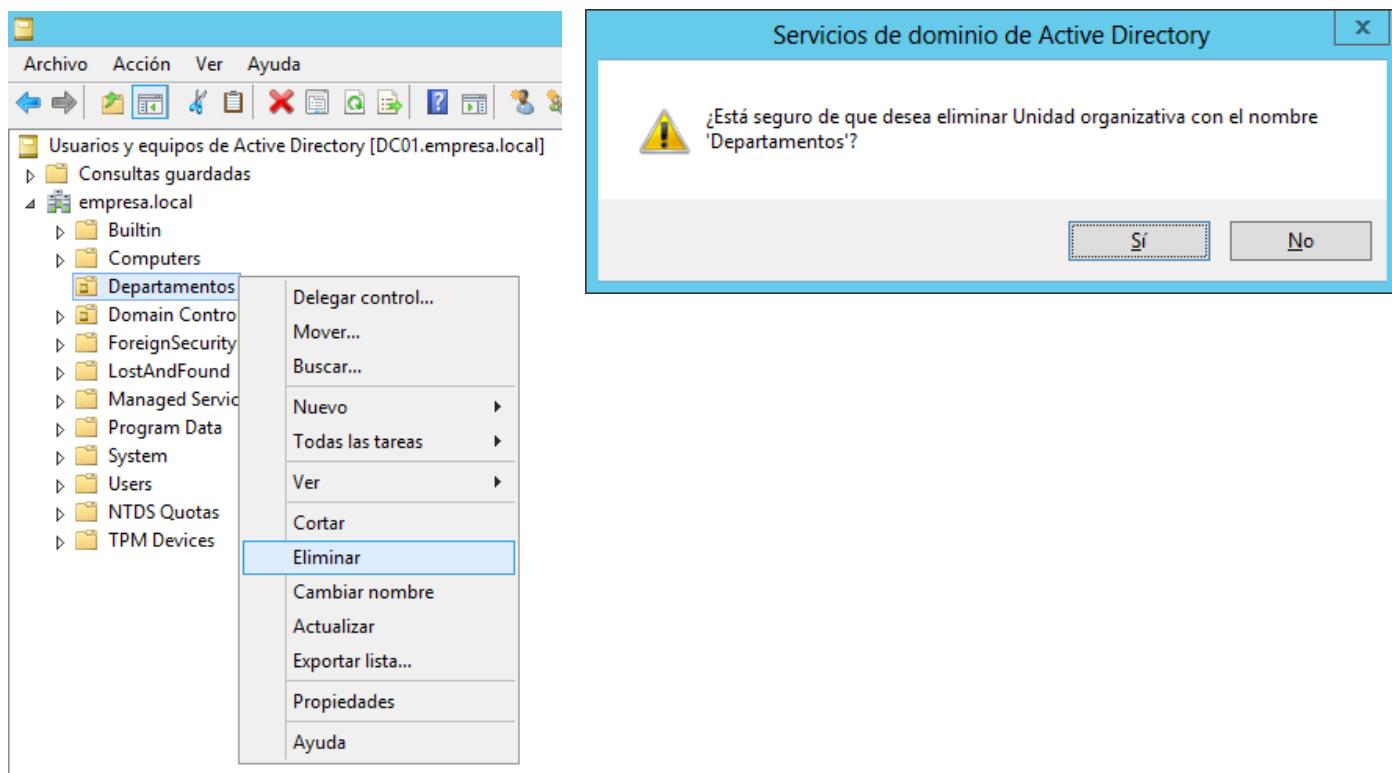
Per a eliminar les unitats organitzatives, en primer lloc haurem d'activar les 'característiques avançades' seleccionant en el menú 'Veure' l'opció 'Características Avançades'.



Ara ja podem desmarcar l'opció de 'Proteger contra eliminació accidental' en les propietats de la unitat organitzativa.



Ara, per a eliminar la unitat organitzativa 'Departaments', bastarà amb fer clic amb el botó secundari i seleccionar 'Eliminar'.



En els pròxims temes, utilitzarem les unitats organitzatives per a gestionar de manera eficaç el domini, aplicant directives de seguretat específiques a cada unitat organitzativa.

## 5. Cas Pràctic: Creació de l'estructura d'una organització mitjançant la línia de comandos

L'administració del domini és una tasca senzilla mitjançant la interfície gràfica, però pot ser molt tediosa si cal repetir en innombrables ocasions seqüències d'accions. Pensem, per exemple, en el cas típic en el qual cal **donar d'alta a una quantitat molt gran d'usuaris**, creant l'estructura completa de l'organització. Aquest tipus de processos pot facilitar-se enormement mitjançant la utilització de **scripts**.

Concretament, en aquest exemple es planteja la creació dels comptes d'usuari d'una organització, així com els seus grups i unitats organitzatives.

Suposarem que l'organització està formada per cinc departaments:

1. Direcció.
2. Finances.
3. Producció.
4. Ventes.
5. Serveis.

Aquesta empresa està formada per 40 treballadors, per la qual cosa és complicat donar-los a tots d'alta mitjançant la interfície gràfica correctament, sense equivocar-se en l'assignació de grups, adreces de correu, etc. Per a automatitzar el procés, es podria extraure del sistema ERP (openERP, openBravo, SAP, Navisión, etc.) un fitxer de text, per exemple en format csv. El fitxer de text podria estar estructurat amb els següents camps:

1. Nom.
2. Cognoms.
3. Contrasenya.
4. Departament.
5. Càrrec.

	A	B	C	D	E	F
1	Nombre	Primer Apellido	Segundo Apellido	Contraseña	Departamento	Cargo
2	Luis	Navarro	Ruiz	Abc123!	Ventas	Mandos Intermedios
3	Susana	Alabau	Sancho	Abc123!	Produccion	Directores
4	Pedro	Gomis	Zambujo	Abc123!	Direccion	Directores

A més dels grups associats a departaments, s'ha decidit crear tres unitats organitzatives en el domini per a gestionar les directives de seguretat (aquestes les veurem en el tema 5). En aquestes s'inclouran únicament a usuaris. Les tres unitats organitzatives seran:

1. Directors (per exemple podrien estar els directors de departament).
2. Comandaments intermedis.
3. Treballadors.

Com es pot comprovar, la tasca és molt àrdua si ha de realitzar-se manualment. Per a automatitzar-la, es planteja la **creació de tres scripts**:

1. Creació dels **grups**.
2. Creació de les **unitats organitzatives**.
3. Creació dels **usuaris** del domini a partir del fitxer CSV obtingut de l'ERP, i configuració dels comptes, així com la seua inclusió en grups i unitats organitzatives

A continuació es presenten els tres scripts (fitxers amb extensió .bat) proposats per a crear l'estructura completa de l'empresa (crearem tota aquesta estructura en el domini empresa.local).

## 5.1. Creació dels grups

Crearem els grups globals per a cada departament amb el següent script (que us podeu descarregar en departaments.bat).

```
@tire off  
  
for /F %%a in (departaments.csv) do (  
  
    tire Processant el grup %%a  
  
    dsadd group "CN=%%a,CN=Users,DC=empresa,DC=local" -secgrp yes -scope g  
  
)
```

En aquest cas, departaments.csv és un fitxer que conté els departaments de l'empresa. Com únicament es tracta de cinc departaments, podrien crear-se manualment.

El comando anterior recorre el fitxer departaments.csv amb l'opció /F. El contingut de cada línia s'emmagatzema en la variable %%a. Finalment per a cada línia s'executa el comando dsadd que crea el grup de seguretat d'àmbit global (-secgrp yes -scope g) amb el nom contingut en la variable %%a.

A més, crearem manualment per la línia de comandos un grup local de domini extra per a incloure a usuaris i grups que vulguem que tinguen permisos d'accés especials als recursos compartits. Farem membres d'aquest grup a tots els usuaris del grup Direcció i a tots els usuaris del grup Finances utilitzant l'opció -members.

```
>>dsadd group "CN=Accés_extra,CN=Users,DC=empresa,DC=local" -secgrp yes  
-scope 1 -members "CN=Direcció,CN=Users,DC=empresa,DC=local"  
"CN=Finances,CN=Users,DC=empresa,DC=local"
```

En les següents imatges es mostra el resultat de l'execució dels comandos anteriors.

The left screenshot shows a list of security groups in Active Directory. Several groups are highlighted with red boxes: 'Acceso extra', 'Direccion', 'Finanzas', 'Produccion', 'Servicios', and 'Ventas'. The right screenshot shows the 'Properties' dialog for the 'Acceso\_extra' group, specifically the 'Members' tab. It lists two members: 'Direccion' and 'Finanzas', both belonging to the 'empresa.local/Users' security group.

Nombre

Tipo

Acceso extra

Direccion

Finanzas

Produccion

Servicios

Ventas

Grupos creados

Propiedades: Acceso\_extra

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Direccion	empresa.local/Users
Finanzas	empresa.local/Users

Aceptar Cancelar Aplicar Ayuda

Membres del grup Accés\_extra

## 5.2. Creació de les unitats organitzatives

Encara que probablement no val la pena confeccionar un script per a crear les tres unitats organitzatives previstes, utilitzarem el mateix patró del cas anterior per a crear-les.

En aquest cas el script (unitats.bat) seria així:

```
@tire off  
  
for /F "tokens=1,2 delims=;" %%a in (unitats_org.csv) do (  
  
    tire Processant la unitat organitzativa %%a  
  
    dsadd ou "OU=%%a,DC=empresa,DC=local" -desc "%%b"  
  
)
```

unitats\_org.csv és el fitxer que conté el nom de les unitats organitzatives planificades per al domini, i la seua descripció, la qual adjuntem a la unitat organitzativa mitjançant l'opció -desc

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view shows the domain structure under 'Usuarios y equipos de Active Directory' (Domain Controller: DC01.empresa.local). Several organizational units (OU) are highlighted with red boxes: 'Directores', 'Trabajadores', and 'Mandos intermedios'. In the center, a search results window lists these OUs. On the right, a detailed properties dialog box for the 'Directores' OU is open, titled 'Propiedades: Directores'. The 'General' tab is selected, showing fields for 'Nombre' (set to 'Racilio Dual'), 'Descripción' ('OU para aplicar las directivas a los directores'), 'Calle', 'Ciudad', 'Estado o provincia', 'Código postal', and 'País o región'. At the bottom of the dialog are 'Aceptar', 'Cancelar', and 'Aplicar' buttons. A caption below the dialog reads 'Descripción de las Unidades Organizativas'.

### 5.3. Creació d'usuaris

El següent script (usuaris.bat) crea els usuaris assignant-los al seu departament i unitat organitzativa.

```
@tire off

for /F "tokens=1,2,3,4,5,6 delims=;" skip=1" %%a in (usuaris.csv) do (
    tire Processant l'usuari %%a %%b %%c

    dsadd user "CN=%%a.%%b,OU=%%f,DC=empresa,DC=local" -fn %%a -ln "%%b %%c" -pwd %%d
    -upn %%a.%%b@empresa.local -email %%a.%%b@empresa.local -mustchpwd yes -Display
    "%%a %%b %%c" -canchpwd yes -disabled no -memberof
    "CN=%%e,CN=Users,DC=empresa,DC=local"
)
```

En les següents imatges podem comprovar la creació dels usuaris.

The image contains three separate windows of the Active Directory Users and Computers management console. Each window shows a list of users under a specific organizational unit (OU).

**Left Window:** Titled "Usuarios y equipos de Active Director" and "Trabajadores". It lists users such as Antonio.Alabau, Basilio.Moncho, Claudio.Gomis, Claudio.Moncho, Eva.Moncho, Eva.Pellicer, Francisco.Campos, Francisco.Coello, Ignacio.Chaves, Isabel.Ruiz, Johann.Aguilar, Jorge.Carvalho, Jorge.CarvalhoGomis, Laura.AlbaAlabau, Manuel.Carvalho, Mario.Juan, Pedro.Chaves, Pepe.Chaves, Piedad.Alba, Piedad.Valencia, and Rodrigo.Gallego.

**Middle Window:** Titled "Usuarios y equipos de Active Director" and "Mandos Intermedios". It lists users such as Antonio.Campos, Ignacio.ChavesJuan, Isabel.Carvalho, Javier.Arias, Javier.Campos, Johann.Alba, Luis.Navarro, Sara.Zambujo, and Susana.Valencia.

**Bottom Window:** Titled "Usuarios y equipos de Active Director" and "Directores". It lists users such as Basilio.Pujol, Laura.Alba, Manuel.Vargas, Mario.JuanPujol, Pedro.Gomis, Pepe.Sancho, Rodrigo.Chaves, Sara.Alba, and Susana.Alabau.

Below each window, there is a caption indicating the OU where the users were created:

- Users created in the organizational unit Trabajadores
- Users created in the organizational unit Mandos Intermedios
- Users created in the organizational unit Directores

Examinem detalladament la sintaxi anterior per a poder comprendre-la millor, i així poder modificar-la per als casos reals que puguen sorgir-nos.

Com s'ha explicat anteriorment, el bucle `for /F ... do ( ... )` recorre **línia a línia** el fitxer que se li passa com a paràmetre `in (usuaris.csv)`.

El modificador `tokens=1,2,3,4,5,6` emmagatzema el contingut de les columnes de la 1 a la 6 del fitxer en les variables correlatives a la variable `%%a` de la següent manera:

- Columna 1 (Nom): variable `%%a`
- Columna 2 (Primer cognom): variable `%%b`
- Columna 3 (Segon cognom): variable `%%c`
- Columna 4 (Contrasenya): variable `%%d`
- Columna 5 (Departament): variable `%%e`
- Columna 6 (Càrrec): variable `%%f`

En aquest cas cal destacar que les columnes estan delimitades amb punt i coma (`delims=;`). Modificant la sintaxi anterior, podríem adaptar el script a qualsevol mena de caràcter de separació de columnes. D'altra banda, com la primera fila del fitxer són les capçaleres de cada columna, no ens interessa per a crear els usuaris, així que la saltem amb `skip=1`. Aquest modificador serveix per a saltar un nombre determinat de línies, en aquest cas 1.

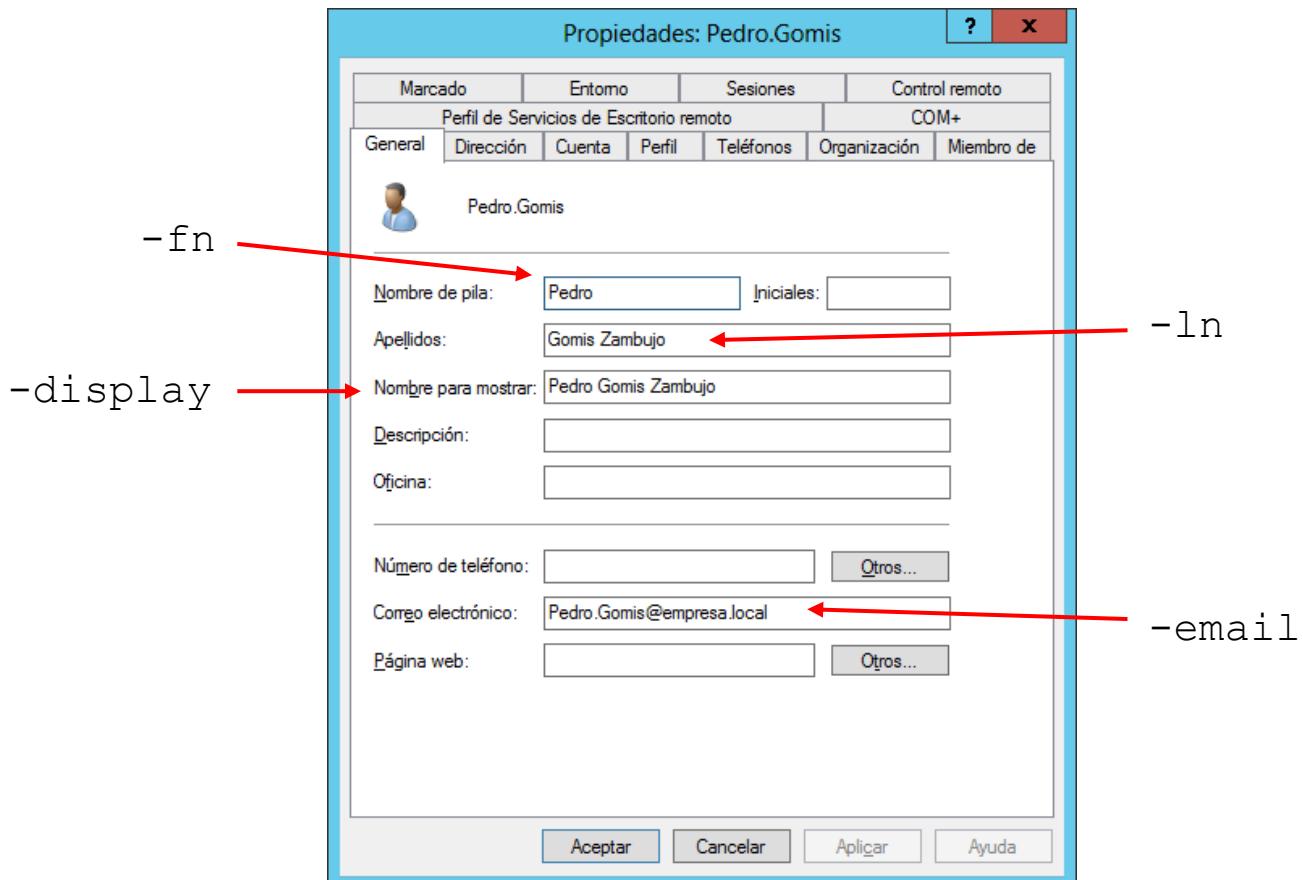
La següent línia (`tire ...`) simplement mostra per la pantalla l'usuari que s'està processant en aqueix instant. Aquesta línia es pot obviar perfectament.

A continuació ve la part més interessant del script, on utilitzem la variables que hem creat per a introduir-les en el comando `dsadd user`.

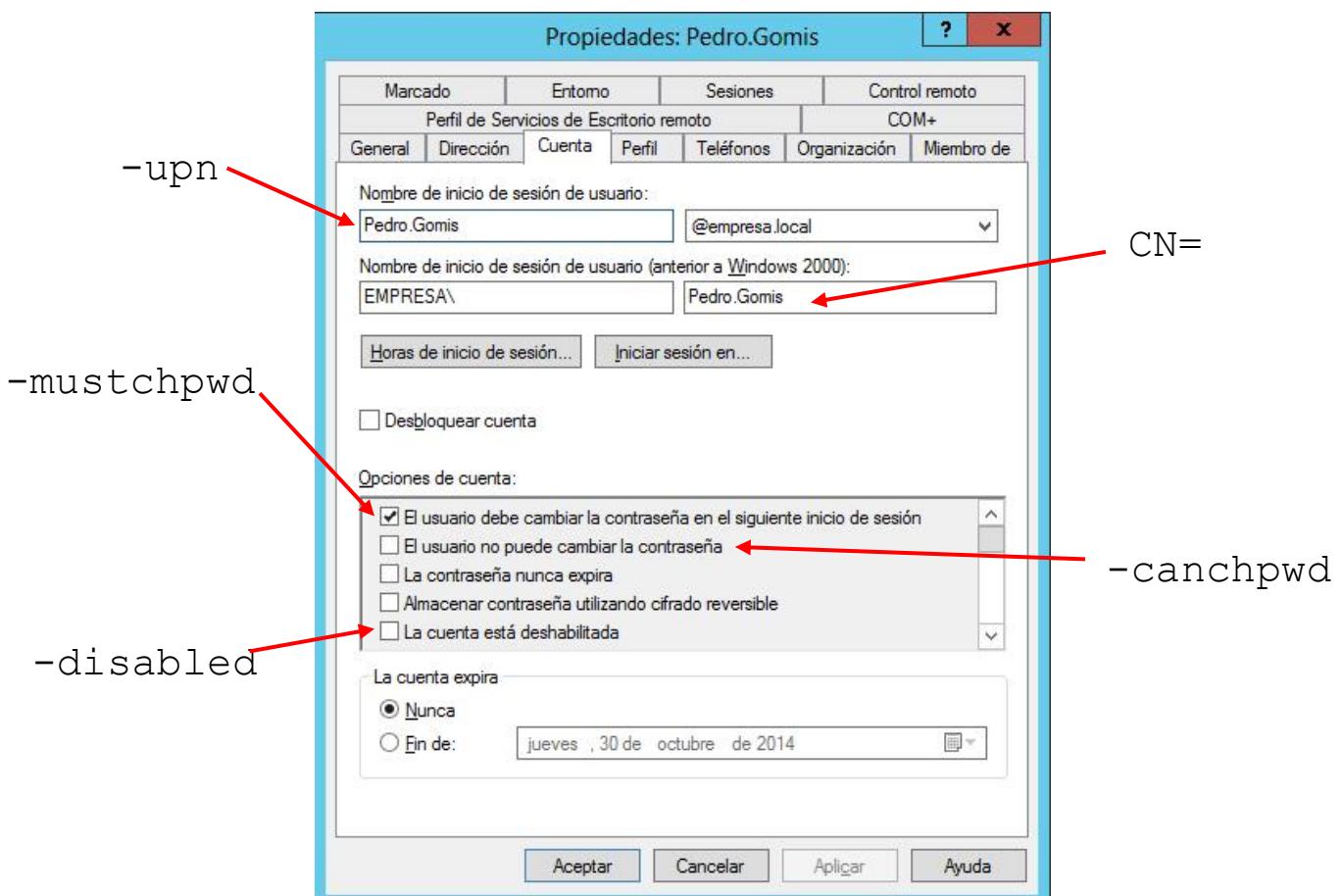
- El primer que fa el comando és crear l'usuari amb el Common Name definit per les variables `%%a` i `%%b`, unides per un punt: "`CN=%%a.%%b`,
- Aqueix usuari es crea en la unitat organitzativa assignada al càrrec que tinga dins de l'organització aqueix usuari (Directors, Comandaments Intermedis o Treballadors): `OU=%%f`,
- `DC=empresa, DC=local`" indiquen el domini dins del qual es troba la unitat organitzativa en la qual es crearà l'usuari.
- `-fn %%a` indica el nom de pila de l'usuari.
- `-ln "%%b %%c"` indica els cognoms de l'usuari.
- `-pwd %%d` indica la contrasenya de l'usuari.
- `-upn %%a.%%b@empresa.local` indica el nom de sistema de l'usuari (se segueix el criteri `nomene.primerApellido`).
- `-email %%a.%%b@empresa.local` indica el correu electrònic de l'usuari, creat amb el criteri `Nom.PrimerApellido@empresa.local`.
- `-mustchpwd yes` obliga l'usuari a canviar la contrasenya.
- `-display "%%a %%b %%c"` indica el nom de l'usuari que es mostrarà ("Nom Primer Cognom Segon Cognom").
- `-canchpwd yes` atorga a l'usuari la possibilitat de canviar la contrasenya.
- `-disabled no` indica que el compte està habilitat.
- `-memberof "CN=%%e,CN=Users,DC=empresa,DC=local"` indica el grup o grups als quals pertany l'usuari.

Aquest comando pot enriquir-se molt més per a cenyir-se en major mesura a les necessitats d'administració. En les pàgines de [Microsoft de Technet](#), es troba una explicació bastant exhaustiva sobre més opcions de `dsadd`.

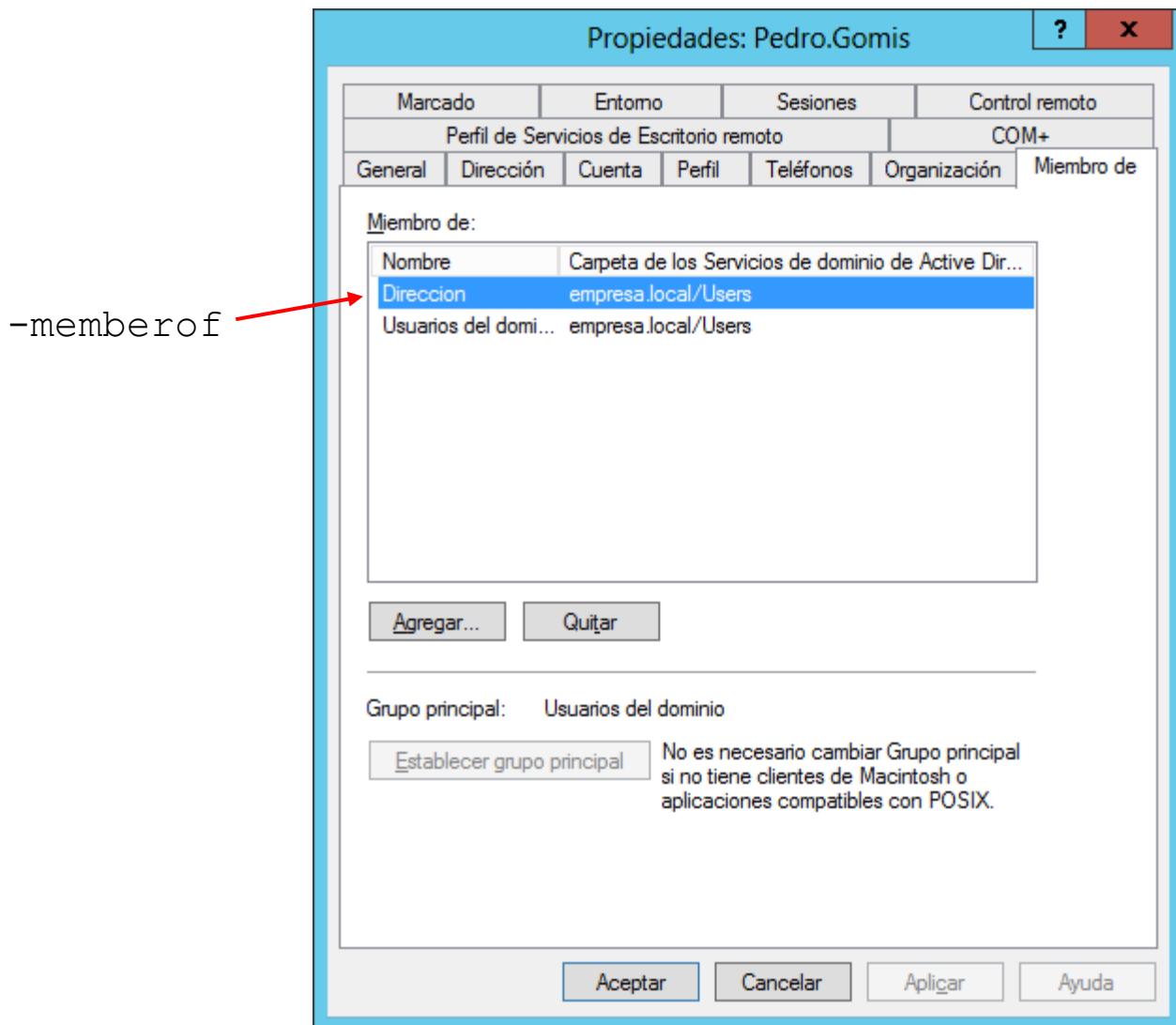
En les següents imatges podem revisar les propietats amb les quals ha sigut creat cada usuari.



Fitxa 'General' de les propietats de l'usuari.



Fitxa 'Compte' de les propietats de l'usuari.



Fitxa 'Membre de' de les propietats de l'usuari.

Si ens fixem amb deteniment, hi ha alguns usuaris el nom dels quals i primer cognom coincideixen. En aqueix cas el script anterior **falla** en tractar de crear el segon compte d'usuari amb el mateix identificador. Si revisem el fitxer `usuaris.csv`, veiem que això ocorre amb els usuaris:

- Jorge Carvalho Pellicer i Jorge Carvalho Gomis,
- Ignacio Chaves Juan i Ignacio Chaves Vargas,
- Mario Juan Pujol i Mario Juan València, i
- Laura Alba Arias i Laura Alba Alabau.

Hem d'establir un mecanisme de control que detecte aquella situació i aportació una alternativa. En aquest exemple s'ha optat per controlar si ja existeix un compte d'usuari, i si ja existeix es canvia el criteri de creació de l'identificador d'usuari al següent:

- Nom.PrimerApellidoSegundoApellido

Ara els identificadors d'usuari 'duplicats' seran:

- Jorge.CarvalhoGomis
- Ignacio.ChavesJuan
- Mario.JuanPujol
- Laura.AlbaAlabau

El següent script (usuaris\_v2.bat) resol la situació anterior (cal adonar-se que no sols cal modificar la manera d'escriure el compte d'usuari ("CN=...") , sinó també l'adreça de correu i el nom del sistema de l'usuari - upn i -email.

```
@tire off

for /F "tokens=1,2,3,4,5,6 delims=; skip=1" %%a in (usuaris.csv) do (
    tire Processant l'usuari %%a %%b %%c

    dsadd user "CN=%%a.%%b,OU=%%f,DC=empresa,DC=local" -fn %%a -ln "%%b %%c" -pwd
    %%d -upn %%a.%%b@empresa.local -email %%a.%%b@empresa.local -mustchpwd yes -
    Display "%%a %%b %%c" -canchpwd yes -disabled no -memberof
    "CN=%%e,CN=Users,DC=empresa,DC=local"

    if NOT ERRORLEVEL 0 dsadd user "CN=%%a.%%b%%c,OU=%%f,DC=empresa,DC=elcalç" -fn
    %%a -ln "%%b %%c" -pwd %%d -upn %%a.%%b%%c@empresa.local -email
    %%a.%%b%%c@empresa.local -mustchpwd yes -Display "%%a %%b %%c" -canchpwd yes -
    disabled no -memberof "CN=%%e,CN=Users,DC=empresa,DC=local"
)
```

L'única diferència amb l'anterior script radica en l'últim comando. Fem ús del codi d'estat ERRORLEVEL. Si ens fixem, en el script, si tractem de crear amb dsadd user un usuari que ja existeix, no es creará i retornarà un codi d'error. En aquest cas és menor que 0 (podeu comprovar-ho manualment amb tire %ERRORLEVEL%).

En posar com a condició NOT ERRORLEVEL 0 en el if, **executem el comando dsadd user... amb les noves opcions "CN=%%a.%%b%%c quan ERRORLEVEL és menor que 0**. Si és igual a 0 significa que no hi ha hagut fallada en la creació de l'usuari, per la qual cosa no cal realitzar cap altra acció.

## 6. Consultes sobre objectes del domini: dsquery

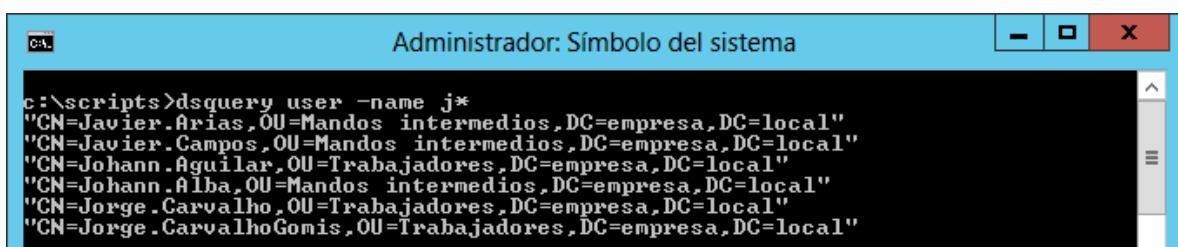
Com hem vist en alguns exemples anteriors, resulta molt tediós introduir per línia de comandos el nom complet d'un usuari o un grup. Recordem el cas de la deshabilitació del compte d'un usuari:

```
>>dsmod user "CN=usuario4, CN=Users, DC=empresa, DC=local" -disabled yes
```

Hem d'introduir el nom complet de l'usuari perquè el comando funcione. Podem facilitar aquesta tasca (encara que amb uns certos riscos) mitjançant el comando dsquery. Entre altres funcions, podem obtindre el nom complet d'un usuari, un grup, un equip, etc. a partir d'un fragment del nom. Per a això escrivim dsquery a continuació user, si busquem informació sobre un usuari, i finalment un fragment del nom:

```
>>dsquery user j*
```

El comando anterior retornarà tots els usuaris el nom dels quals empieza per j.



```
c:\scripts>dsquery user -name j*
"CN=Javier.Arias,OU=Mandos intermedios,DC=empresa,DC=local"
"CN=Javier.Campos,OU=Mandos intermedios,DC=empresa,DC=local"
"CN=Johann.Aguilar,OU=Trabajadores,DC=empresa,DC=local"
"CN=Johann.Alba,OU=Mandos intermedios,DC=empresa,DC=local"
"CN=Jorge.Carvalho,OU=Trabajadores,DC=empresa,DC=local"
"CN=Jorge.CarvalhoGomis,OU=Trabajadores,DC=empresa,DC=local"
```

Si el que

pretenem és estalviar temps en l'escriptura d'un usuari concret, podem introduir el comando de cerca en una variable, de manera que aqueixa variable (nom complet de l'usuari), puguem utilitzar-la per a configurar el seu compte. En aquest cas concret, la deshabilitarem. En primer lloc introdúim el comando de cerca en una variable:

```
>>SET a=dsquery user -name javier.àries
```

Si vam mostrar el valor de la variable a, veurem que s'ha emmagatzemat correctament el comando anterior:

```
>>tire %a%
```

Per a veure el resultat de l'execució de la variable a escrivim el següent:

```
>>%a%
```

Ara que ja tenim el comando de cerca i obtenció del nom complet de l'usuari javier.àries, podem introduir-ho en el comando de deshabilitació de comptes dsmod user -disabled yes. Això ho realitzarem mitjançant una canonada (|).

```
>>%a% | dsmod user -disabled yes
```

Comprovem que efectivament el compte està deshabilitat (veure fletxa cap avall al costat del símbol d'usuari):

Nombre	Tipo
Javier.Arias	Usuario
Javier.Campos	Usuario
Javier.CamposVargas	Usuario
Johann.Alba	Usuario
Luis.Navarro	Usuario
Sara.Zambuj	Usuario
Susana.Valencia	Usuario
Susana.ValenciaMoncho	Usuario

Podeu trobar més informació sobre:

- Fitxers per lots (bat): <http://www.saulo.net/pub/msdos/cap10.htm>
- dsquery: [Technet de Microsoft](#).

## 7. Bibliografia

- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows Server 2012.
- Somebooks.es (2014). Sistemes Operatius en Xarxa. Disponible en <http://somebooks.es/?p=4787>
- Wikipedia. Sistema Operatiu de xarxa. Disponible en [http://es.wikipedia.org/wiki/sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/sistema_operativo_de_red)
- Blog de SoporteTI. Disponible en: <http://blog.soporteti.net/>
- Fitxers per lots (bat): <http://www.saulo.net/pub/msdos/cap10.htm>
- Elaboració pròpria

# Sistemes Informàtics

---

## Part 5. Permisos, directives de grup i perfils



## Índex

1. Objectius .....	3
2. Permisos .....	3
2.1. Com consultar els permisos que té un recurs .....	4
2.2. Permisos de recursos compartits.....	5
2.3. Permisos NTFS.....	10
3. Directives de Grup (GPO) .....	20
3.1. Edició de les directives de grup predefinides.....	20
3.2. Creació de Directives de Grup .....	29
4. Perfilis .....	38
4.1. Perfilis mòbils.....	38
5. Carpetes personals .....	42
7. Bibliografia.....	47

## 1. Objectius

- Creació de recursos compartits.
- Configuració i administració de permisos de carpetes compartides.
- Configuració i administració de permisos NTFS
- Gestió del domini mitjançant directives de grup.
- Configuració de l'entorn de treball de l'usuari mitjançant perfils.
- Establiment de carpetes particulars dels usuaris del domini.
- Execució de comandos d'inici de sessió.

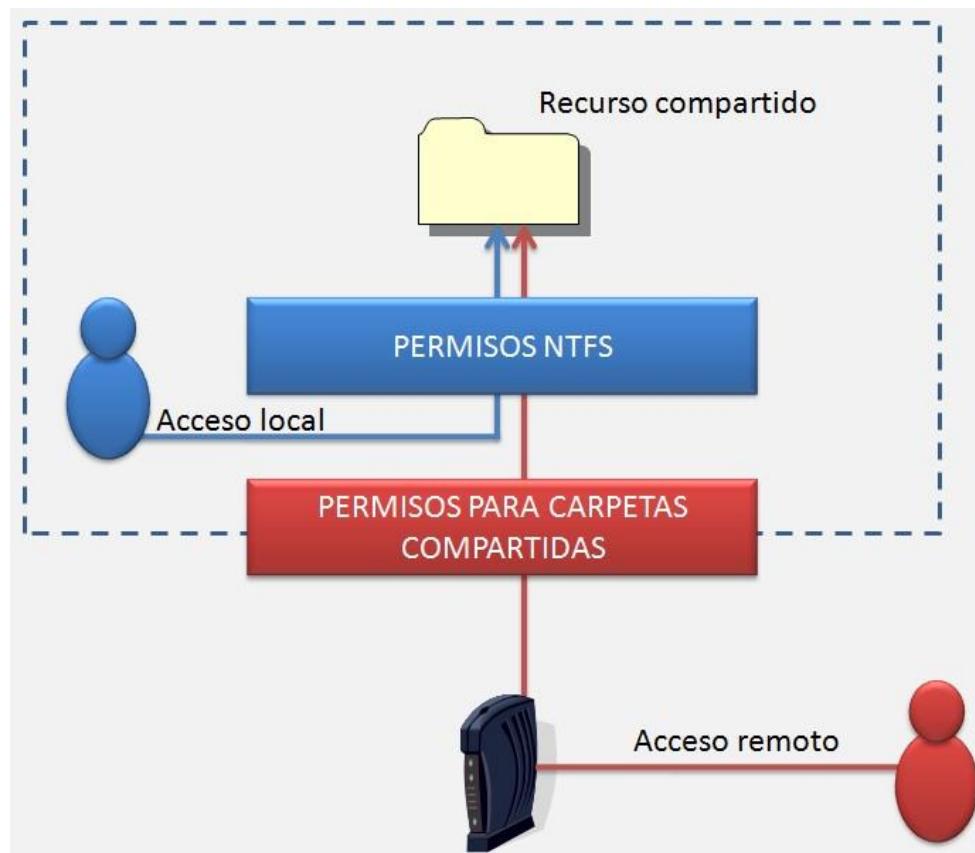
## 2. Permisos

Els sistemes operatius de la família Windows posseeixen dos nivells de permisos per als recursos compartits:

- Permisos per a recursos o carpetes compartides: s'apliquen cada vegada que un usuari vol accedir a un arxiu o carpeta de la xarxa.
- Permisos per a arxius i carpetes NTFS: s'apliquen sobre dispositius amb **format NTFS** per a definir en major detall les accions permeses.

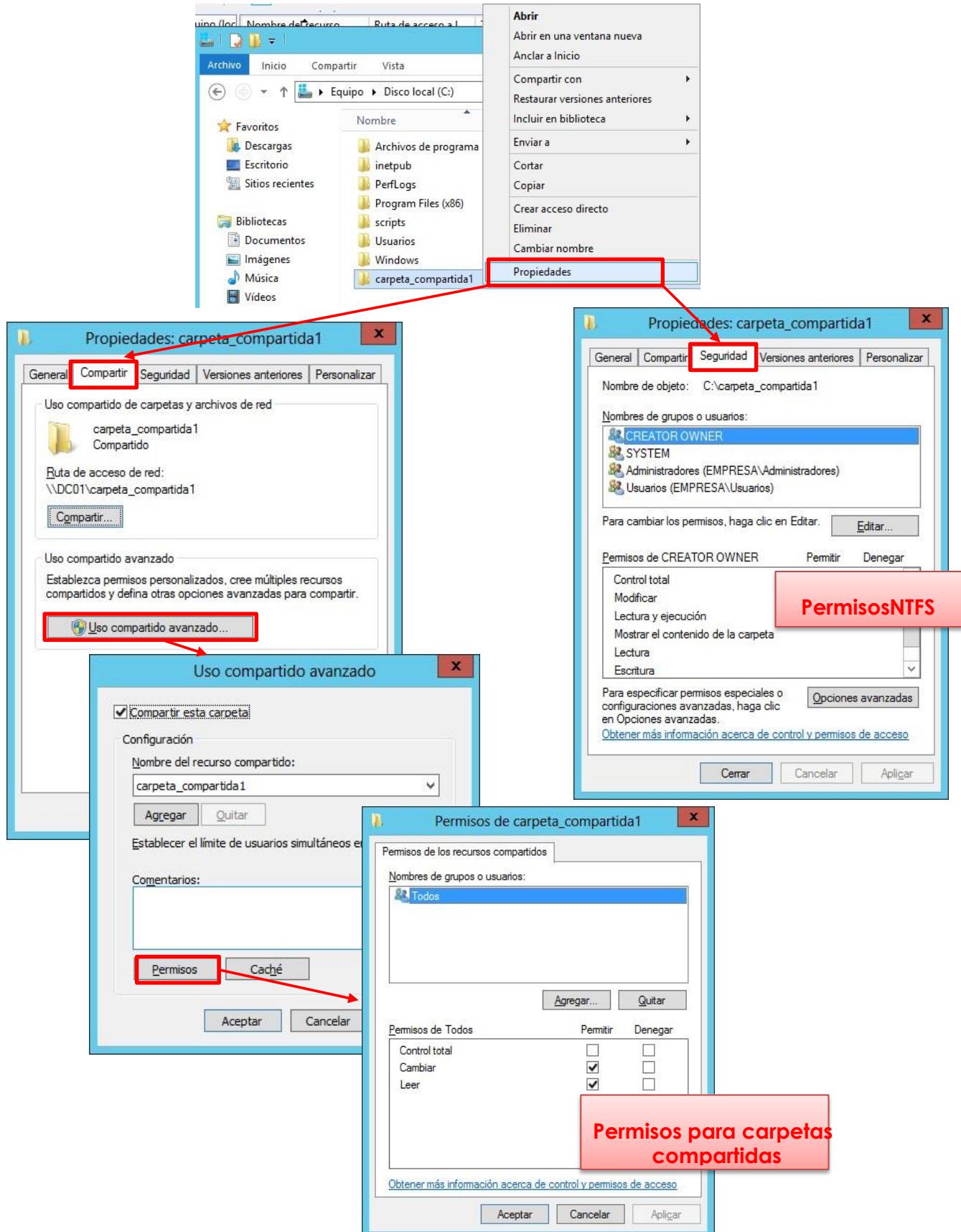
De l'anterior s'extrau que quan s'accedeix en manera local als arxius o carpetes només intervenen els permisos associats al sistema de fitxers, en aquest cas NTFS, no obstant això si s'accedeix a través de la xarxa s'apliquen els dos nivells de permisos: en primer lloc s'apliquen els permisos de carpetes compartides i posteriorment els permisos NTFS.

Com veurem més endavant, en cas que hi haja inconsistències entre els permisos de cada tipus, s'aplicaran els més restrictius.



## 2.1. Com consultar els permisos que té un recurs

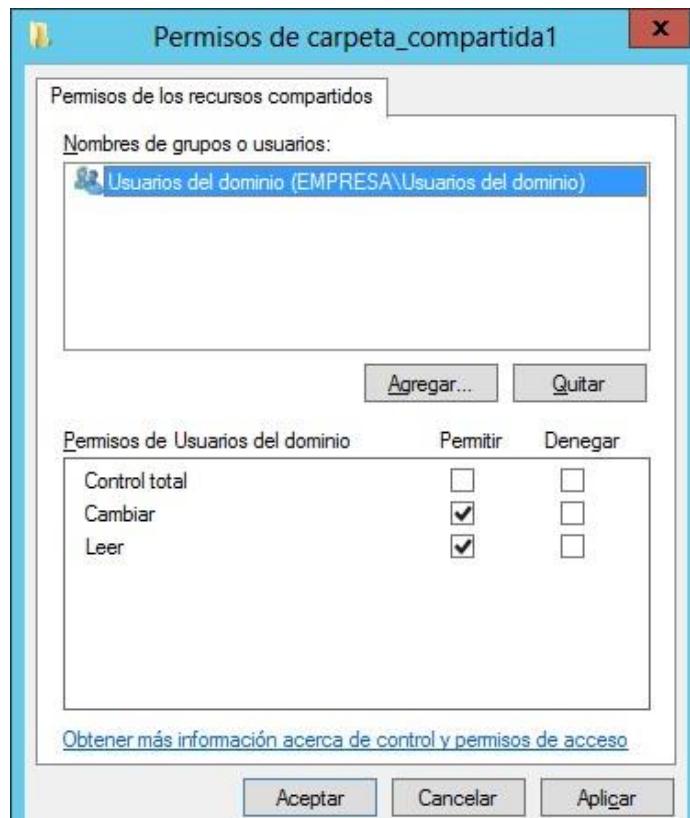
Des de la carpeta a consultar els seus permisos->Botó dret->Propietats:



## 2.2. Permisos de recursos compartits

En el cas dels permisos de recursos compartits, aquests poden ser de tres tipus:

- **Control total:** no sols permet canviar i llegir, sinó modificar els permisos sobre el recurs compartit.
- **Canviar:** es permet crear carpetes i arxius a més de modificar i esborrar els arxius i directoris existents.
- **Lectura:** únicament permet la lectura d'arxius i l'execució d'arxius executables que es troben dins del recurs compartit.



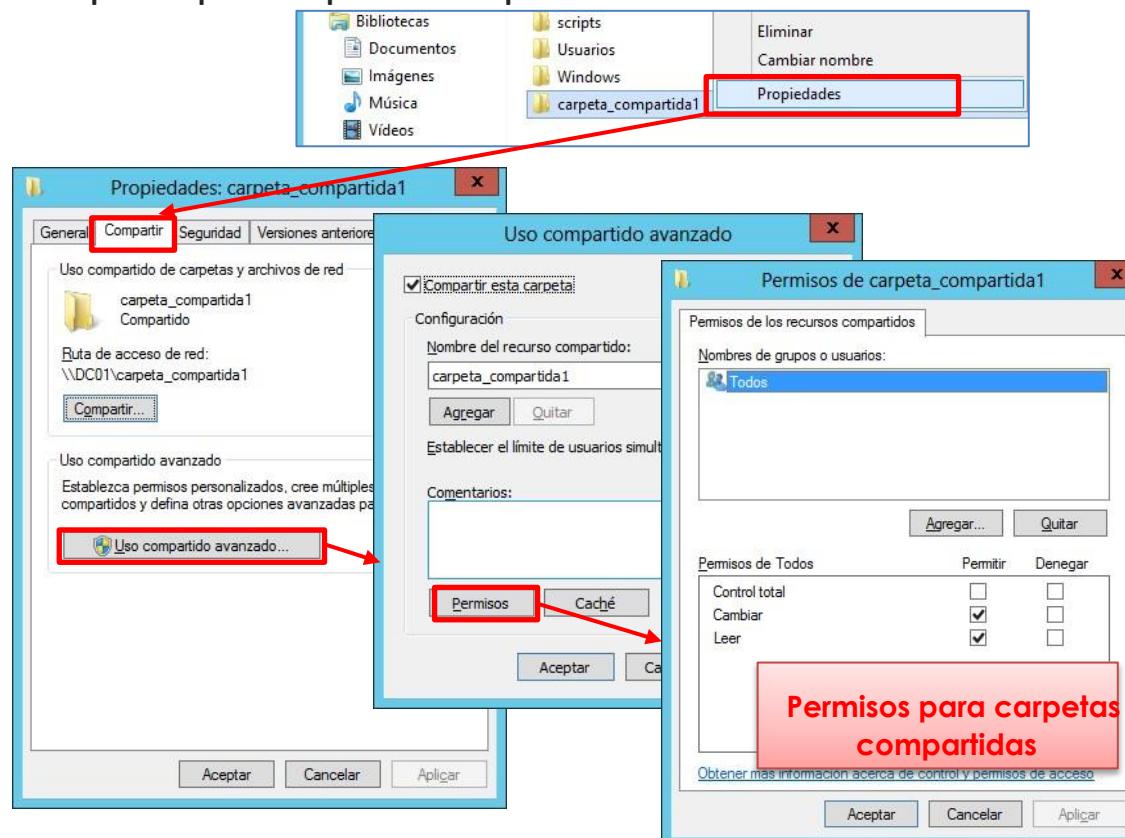
Com es pot comprovar, existeixen dues columnes on assignar permisos: “Permetre” i “Denegar”. És important destacar que l’opció “Denegar” té prioritat sobre altres permisos assignats sobre el recurs compartit.

### Què ocorre si en els permisos dels recursos compartits no marquem “Permetre” ni “Denegar”?

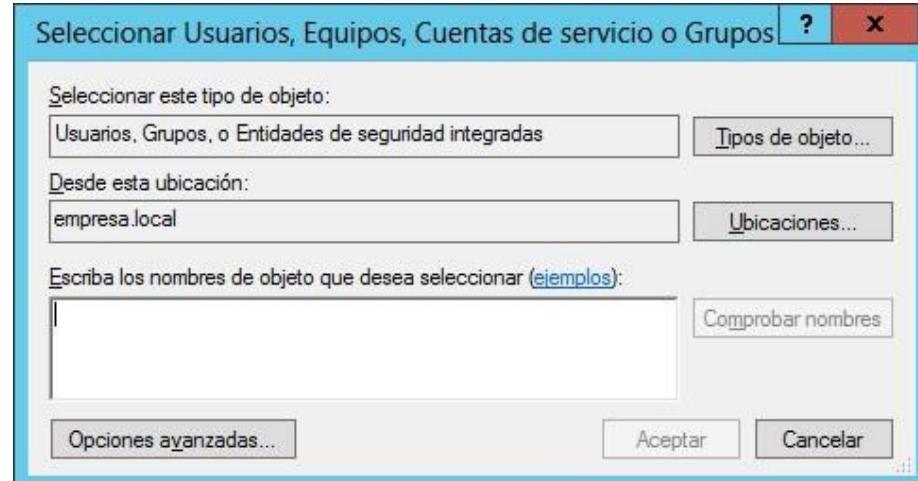
Si no es marca explícitament un permís, s’entén que està implícitamente denegat, per la qual cosa un usuari que no tinga marcat cap permís ni en la casella „Permetre“ ni en la casella „Denegar“ no podrà accedir al recurs compartit.

## 2.2.1. Establir permisos de recursos compartits

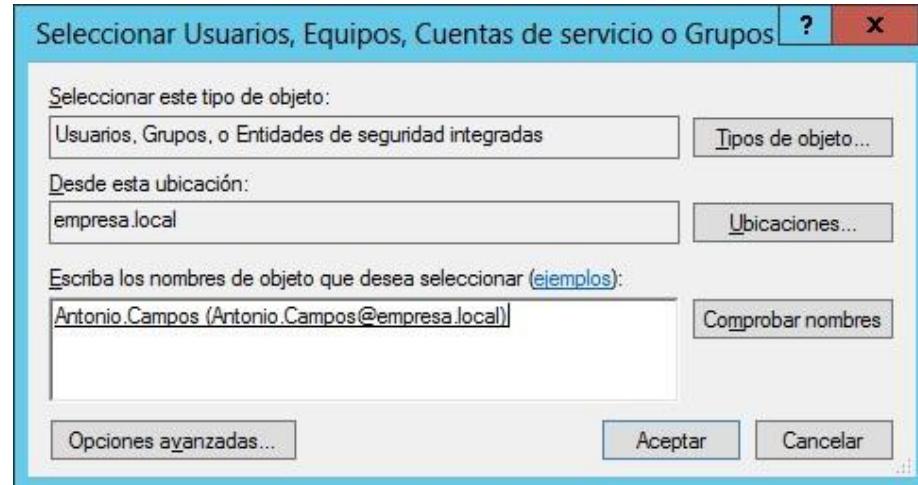
La configuració dels permisos de recursos compartits es pot fer de diverses maneres. La més senzilla és seleccionar el recurs sobre el qual es desitgen configurar els permisos, i fent clic amb el botó dret, triar l'opció **Propietats** -> **Pestanya Compartir**-> **Botó “Ús compartit avançat”** -> **Marquem “Compartir aquesta carpeta”** ->**Botó permisos**



Si volem afegir permisos a un usuari o a un grup, farem clic en el botó “Aregar”. S'obrirà un quadre de diàleg que ens permetrà buscar entre els usuaris i grups del sistema.



En aqueix quadre escriurem el nom de l'usuari o grup al qual volem assignar els permisos. Prement a “Comprovar noms” el sistema buscarà el nom escrit en el quadre i comprovarà si efectivament està donat d'alta en el domini, i en aquest cas apareixerà subratllat.



Seleccionar Usuarios, Equipos, Cuentas de servicio o Grupos ? X

Seleccionar este tipo de objeto:  
Usuarios, Grupos, o Entidades de seguridad integradas Tipos de objeto...

Desde esta ubicación:  
empresa.local Ubicaciones...

Escriba los nombres de objeto que desea seleccionar ([ejemplos](#)):  
pepito Comprobar nombres

[Opciones avanzadas...](#)

En cas contrari apareixerà un missatge d'error com el de la següent imatge , on s'avisa que no s'ha pogut trobar l'objecte cercat.

**Nombre no encontrado**

No se puede encontrar un objeto de nombre "pepito". Compruebe la precisión de los tipos de objeto seleccionados y la ubicación, y asegúrese de que escribió el nombre de objeto correctamente, o quite este objeto de la selección.

Corregir la información de este objeto y volver a buscar

Seleccionar este tipo de objeto:  
Usuarios, Grupos, o Entidades de seguridad integradas Tipos de objeto...

Desde esta ubicación:  
empresa.local Ubicaciones...

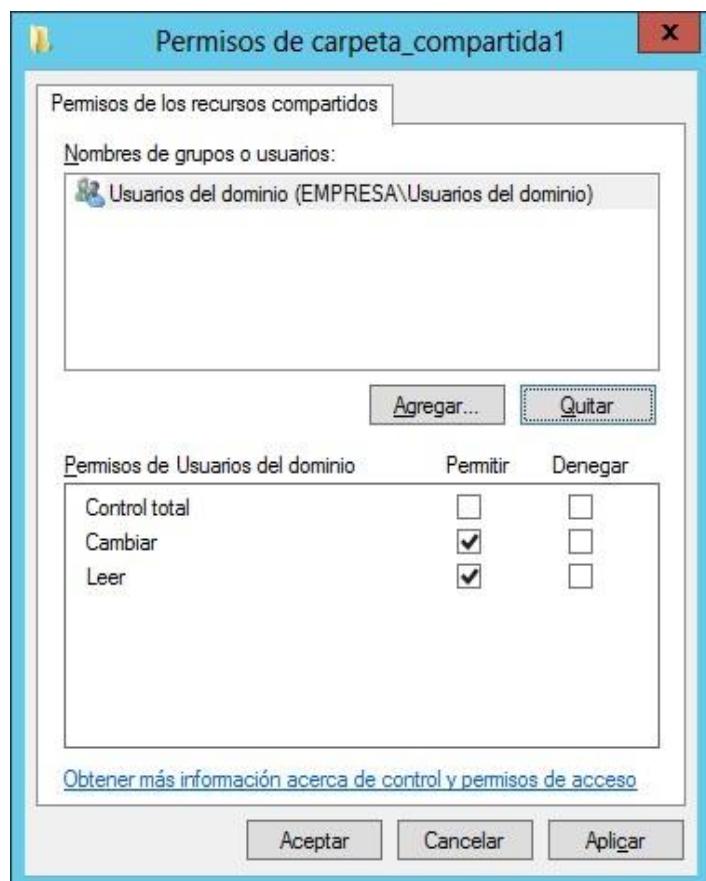
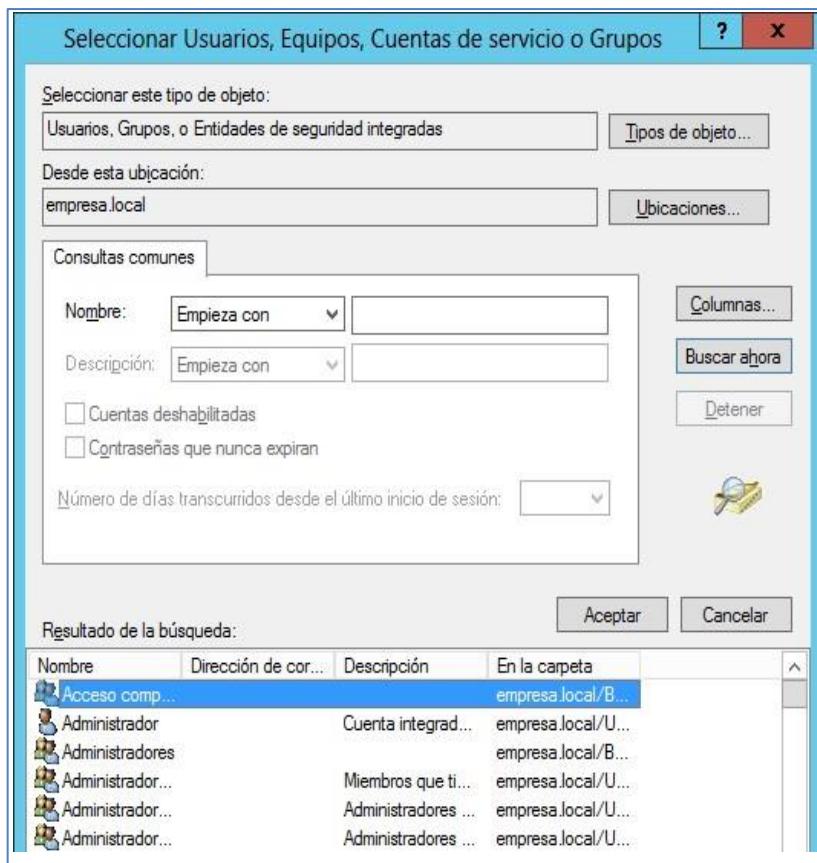
Escriba el nombre de objeto:  
bepeito

Quitar "pepito" de la selección

Aceptar Cancelar

Si no recordem el nom del grup o usuari que volem afegir podem anar a “Opcions avançades”->“Buscar ara” i seleccionar els usuaris o grups que volem.

Una vegada que hagim introduït el nom d'un usuari o grup que existisca en el domini podrem assignar o llevar els permisos com s'ha mostrat més amunt .



Com a política adequada d'administració de sistemes, **en la mesura que siga possible s'evitaran les comparticions amb el grup Tots** (en aqueix grup estan fins i tot els comptes de convidat) encara que en el següent nivell de permisos (NTFS) es bloquegen accessos indeguts. Es tendirà a incloure únicament en els permisos de recursos compartits a aquells grups o usuaris que de veritat vulguem que tinguen algun tipus d'accés sobre el recurs.

## 2.3. Permisos NTFS

Com s'ha comentat anteriorment, els permisos NTFS complementen i amplien els permisos de recursos compartits, sent **efectiu el més restrictiu**.

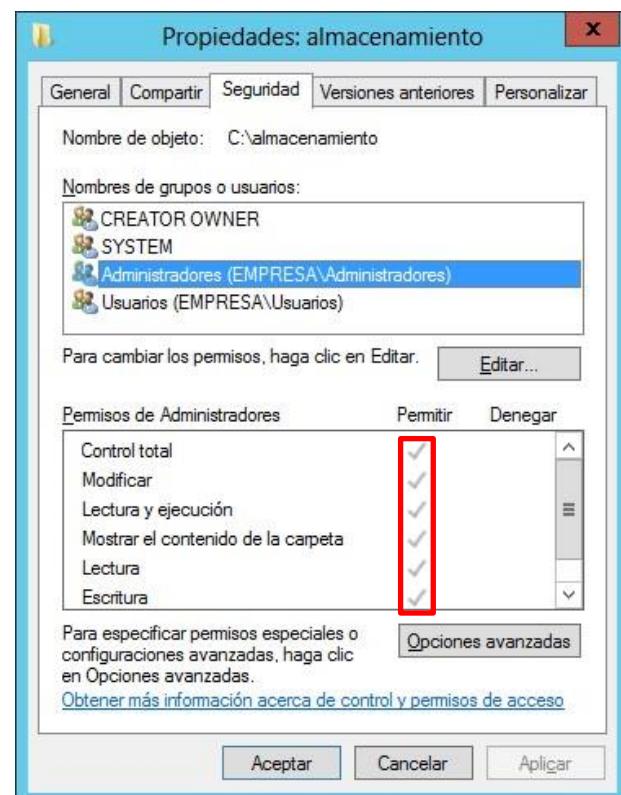
Tots els arxius i carpetes d'un **volum NTFS** tenen associada una **ACL o llista de control d'accés** que fixa el **nivell d'accés d'un usuari o grup que pretenga accedir al recurs**. A més, els permisos NTFS poden ser aplicats a nivell d'arxiu , a diferència dels permisos de recursos compartits, els quals únicament poden aplicar-se a nivell de carpeta.

D'altra banda , sorgeix un nou concepte en aplicar els permisos NTFS que els fa més complexos encara que també més potents: **l'herència** , la qual determinarà els permisos que es reben sobre un determinat recurs provinents d'un nivell superior, encara que això ho veurem detalladament més endavant .

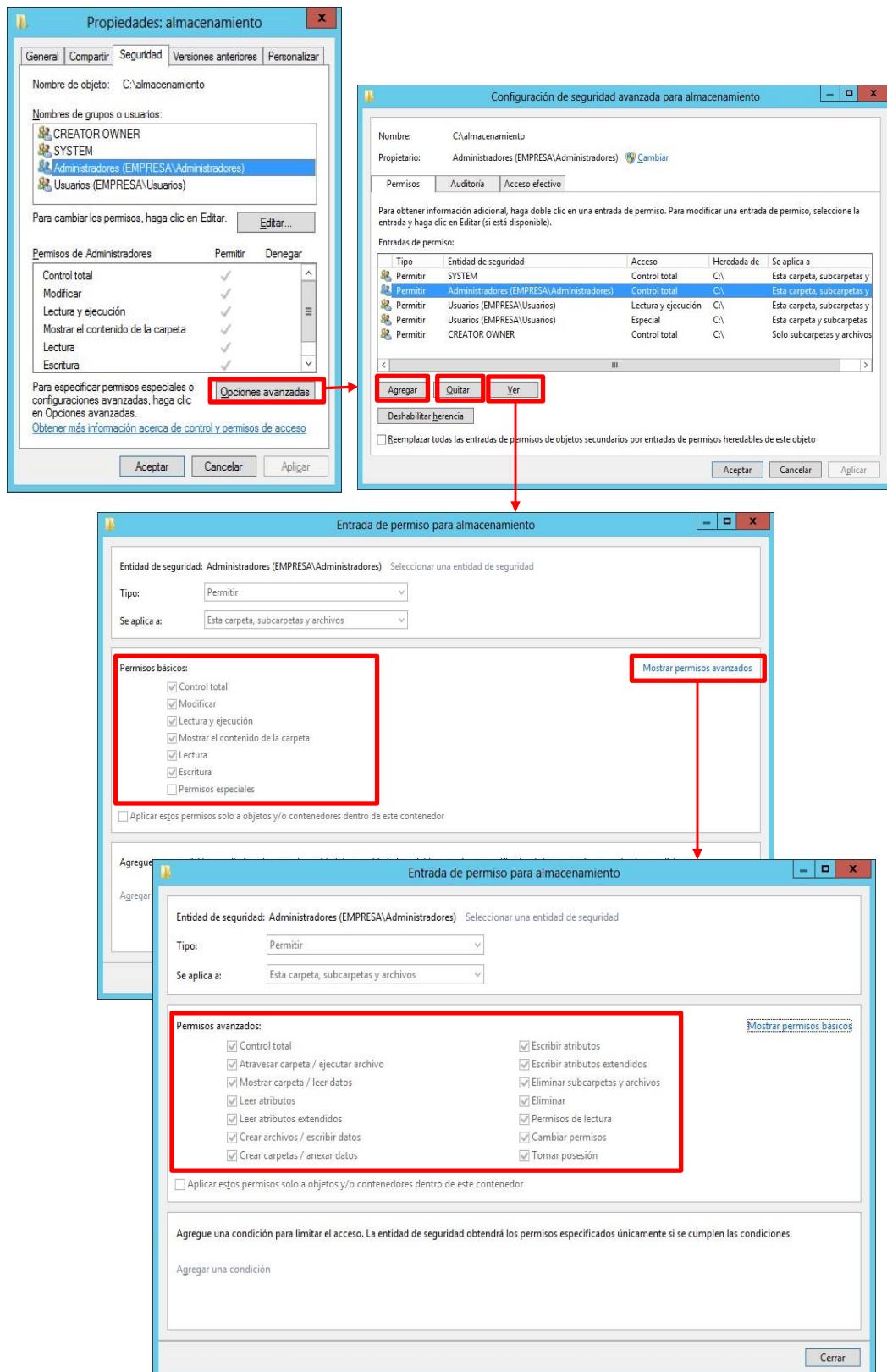
### Tipus de permisos NTFS

Els permisos bàsics (o predeterminats) que poden aplicar-se sobre arxius i carpetes són:

- Control total.
- Modificar.
- Lectura i execució.
- Mostrar el contingut de la carpeta.
- Lectura.
- Escriptura.



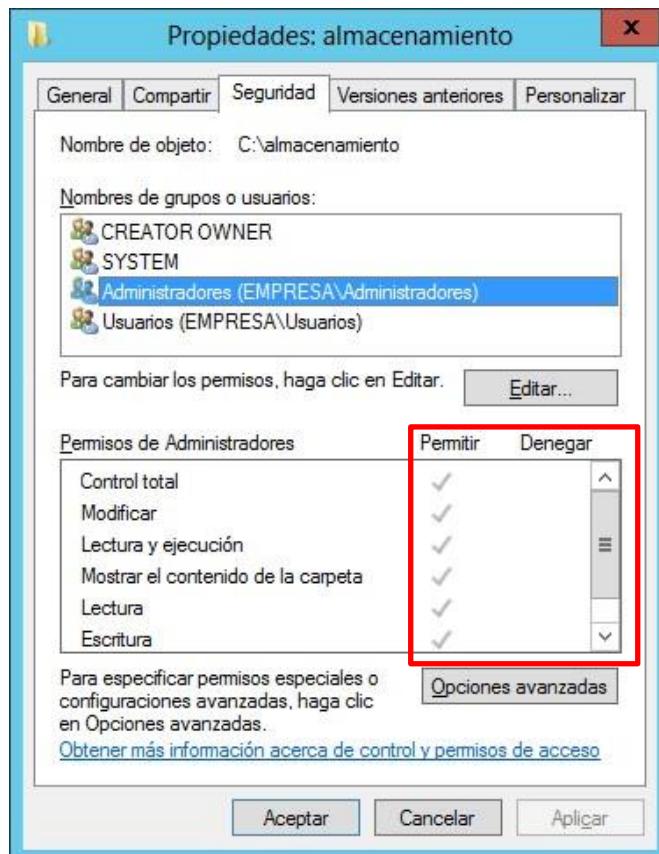
Els permisos específics pot editar-se/consultar-se individualment, tal com es mostra a continuació :



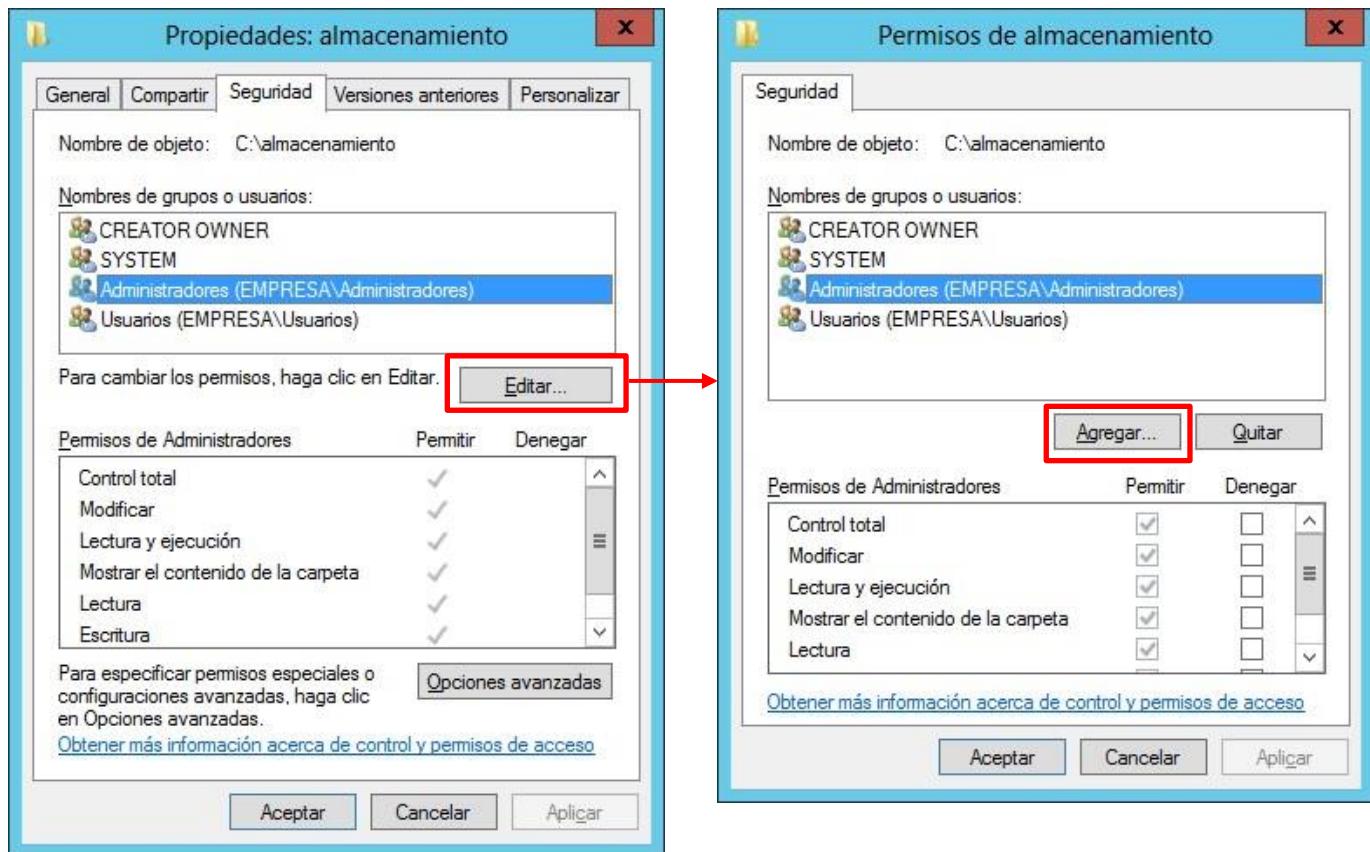
### 2.3.1. Assignació de permisos NTFS

En definir un permís NTFS aquest pot ser un permís o una denegació.

Els permisos NTFS són acumulatius: s'avaluen els permisos atorgats a l'usuari i als grups als quals pertany l'usuari. En el cas que hi haja una incompatibilitat entre els permisos assignats a un usuari i els assignats a un grup del qual siga membre, prevaldrà l'opció més restrictiva: Denegar (si està definit explícitament).



Per a assignar permisos NTFS a un recurs compartit bastarà amb fer clic amb el botó secundari sobre el recurs i accedir a la pestanya 'Seguretat'. A continuació premerem el botó 'Editar'. El botó 'Agregar' permet afegir grups o usuaris als quals atorgar o denegar permisos.



Compte amb el grup Usuaris (del domini) perquè apareix per defecte en els permisos NTFS (amb permisos de lectura), i pot provocar que es produïsquen accessos diferents a la nostra planificació. Com a norma general, si volem limitar l'accés a un recurs compartit, eliminarem el grup Usuaris dels permisos NTFS i explicitarem únicament aquells grups o usuaris que efectivament vulguem que tinguen accés al recurs.

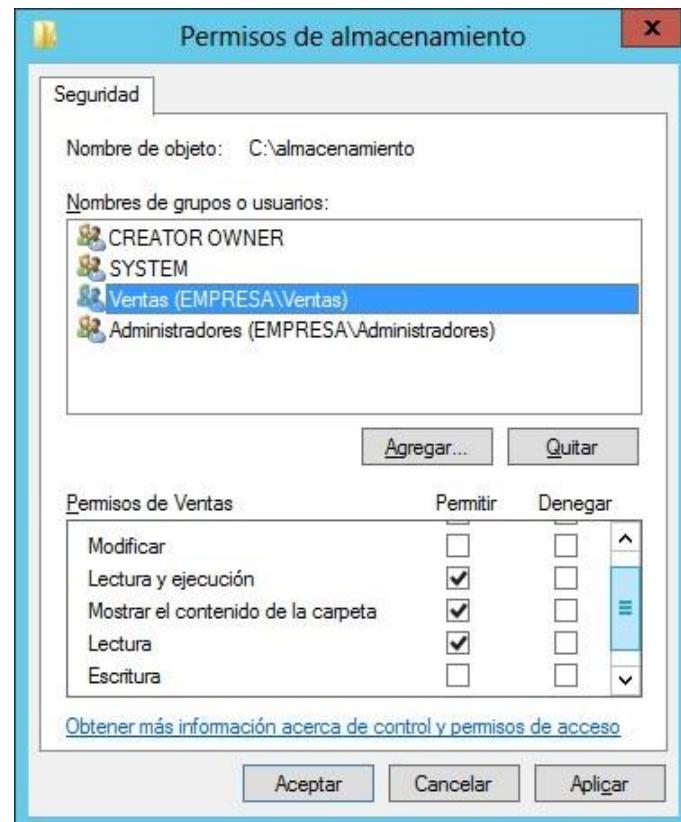
### 2.3.2. Permisos implícits i permisos explícits

Els permisos atorgats de manera implícita o explícita són una qüestió senzilla, en la qual si no ens fixem amb atenció, podem fer que els accessos als recursos no funcionen com teníem previst.

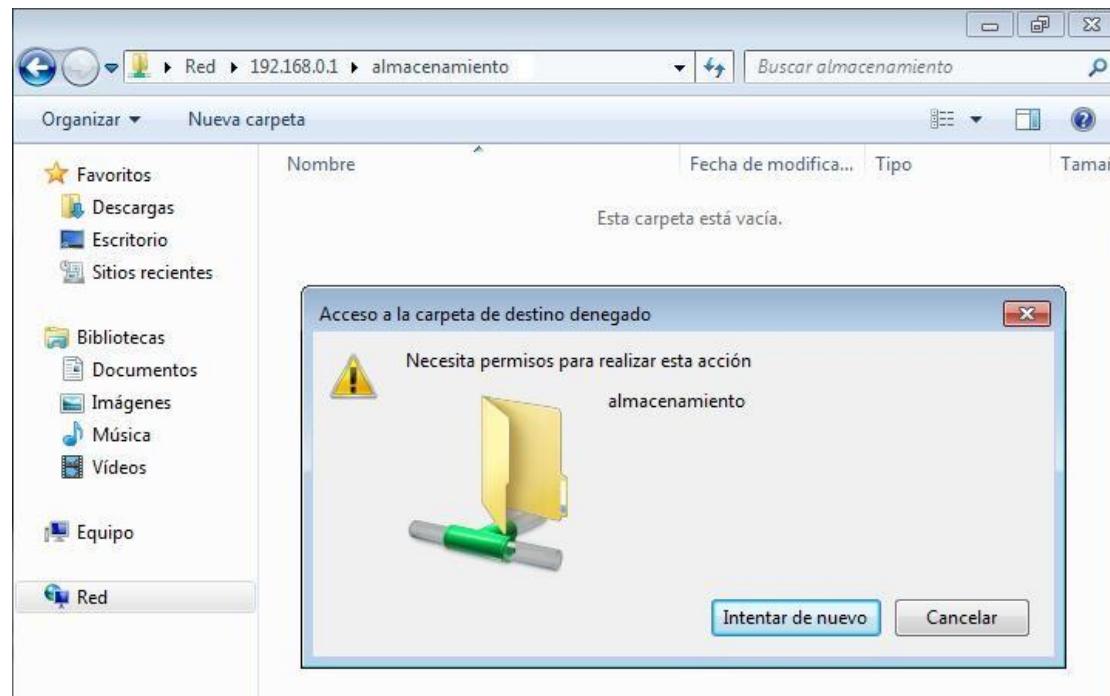
Per a evitar problemes tindrem en compte que:

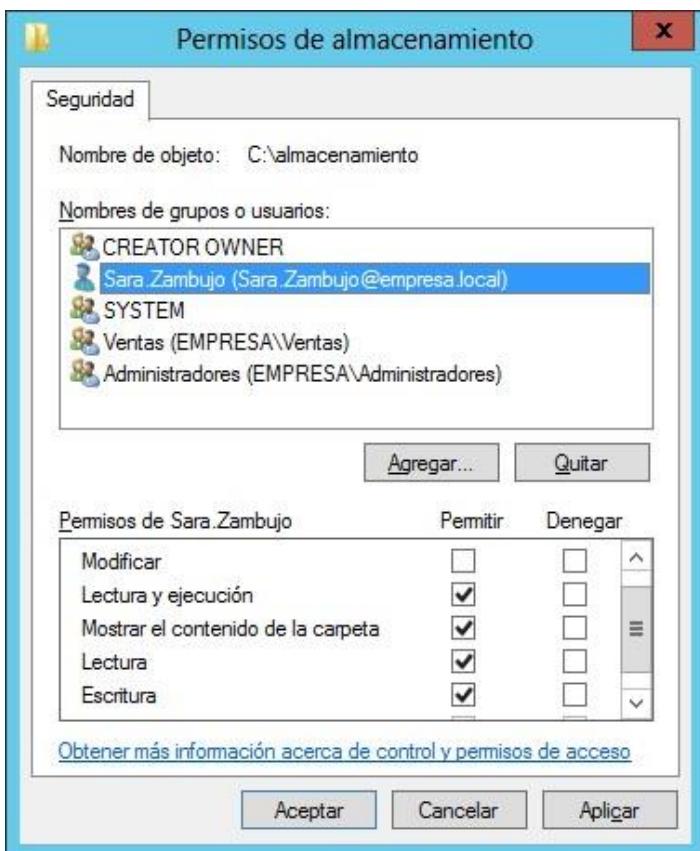
1. Un permís definit de manera explícita sempre prevaldrà sobre un permís definit de manera implícita.
2. Denegar un permís sempre preval sobre atorgar aqueix permís, sempre que tots dos estiguin definits de la mateixa manera (implícita o explícitamente).

Com es defineix un permís de manera explícita? Si ens fixem en la següent imatge, el grup Vendes no té (aparentment) definits permisos d'escriptura . No obstant això aqueixa aparent indefinició, en realitat indica que el permís d'escriptura està denegat implícitament.

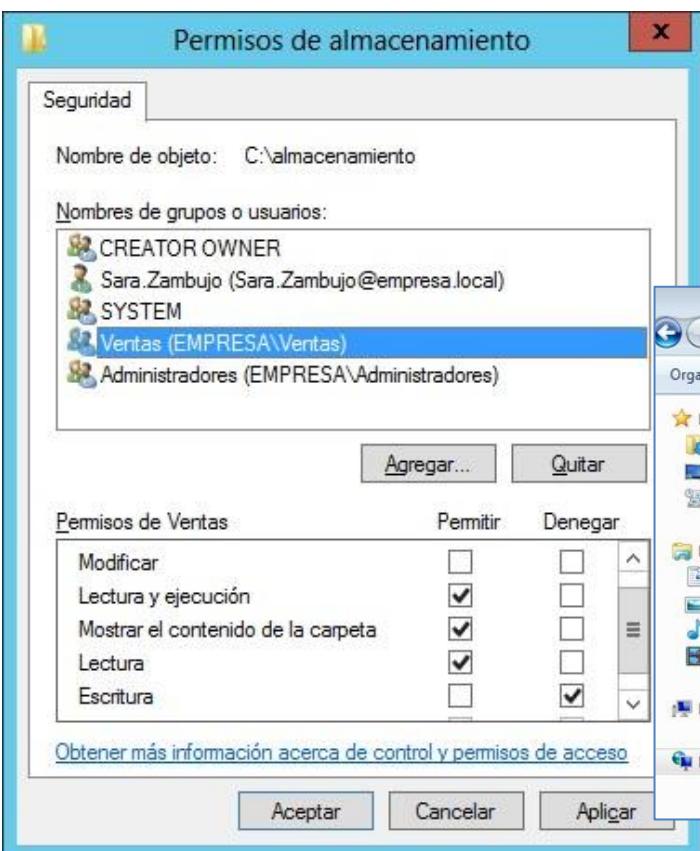
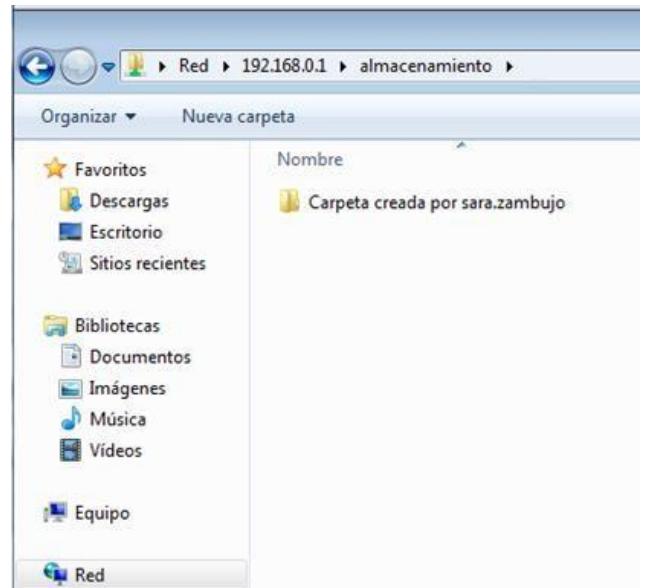


Si un usuari del grup Vendes intenta escriure en la carpeta, es produirà un missatge d'error.

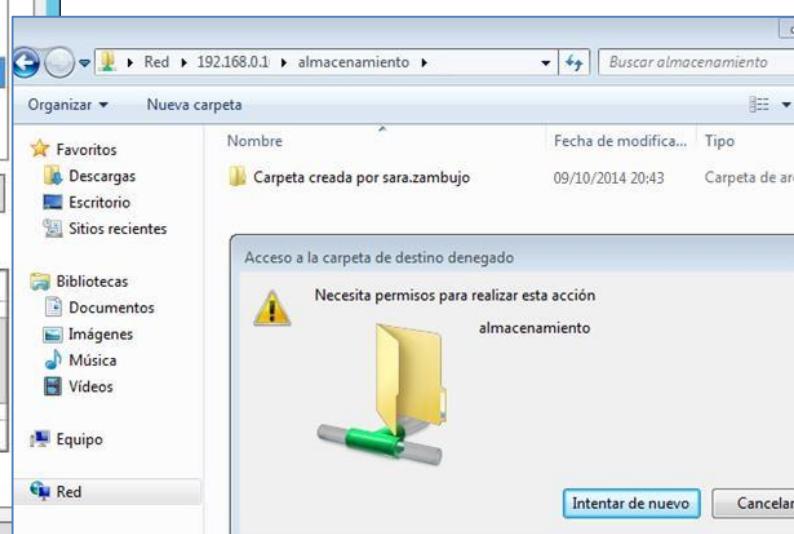




En canvi, si afegim l'usuari sara.zambujo que és membre de Ventas en la fitxa permisos, i li otorgem el permís explícit d'escriptura, veurem que efectivament pot escriure en el recurs. Ja que la definició explícita del permís per a escriure preval sobre la denegació implícita del permís escriure.



Si fem explícita la denegació del permís d'escriptura Per als membres del grup Ventas, podem comprovar que efectivament sara.zambujo **no pot** escriure en la carpeta.



Es recomana evitar l'ús explícit de la denegació de permisos llevat que es considere que no existeix una altra manera per a obtindre un nivell específic de permís per a un determinat grup.

### 2.3.3. Herència de permisos

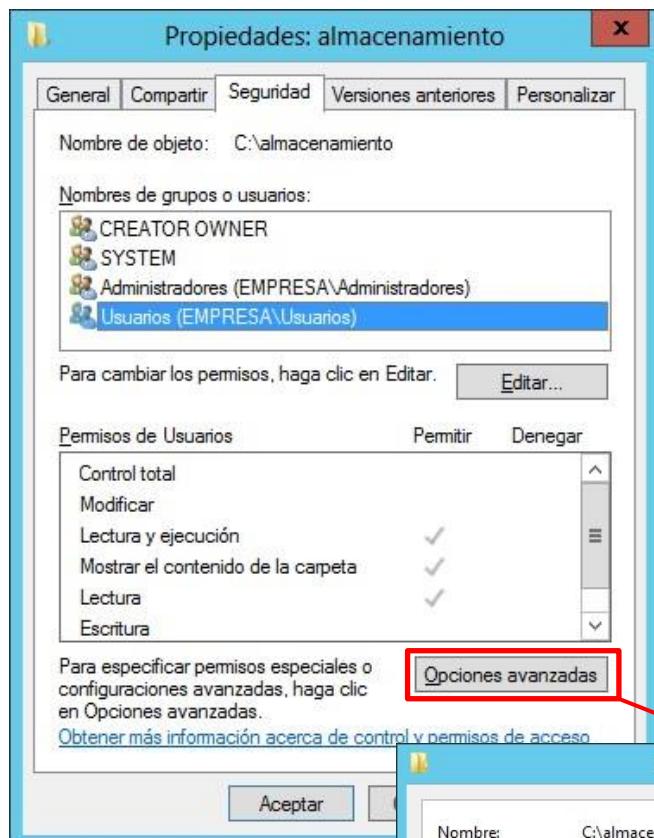
En crear un arxiu o carpeta en un volum NTFS aqueix objecte hereta automàticament els permisos de la seu carpeta contenidora, i al revés: quan assignem permisos a una carpeta contenidora, els permisos es propaguen automàticament cap als arxius i subcarpetes contingudes en el recurs.

No obstant això , poden donar-se ocasions en les quals vulguem eliminar aqueixa herència de permisos. Això pot executar-se de tres maneres diferents:

- Eliminar l'herència a nivell de la carpeta de nivell superior, els objectes continguts en ella deixen d'heretar els permisos.
- Eliminar l'herència a nivell de subcarpeta o arxiu contingut dins del recurs principal.
- Permetre o denegar **explícitament** un permís de manera diferent a com està definit en el recurs contenidor.

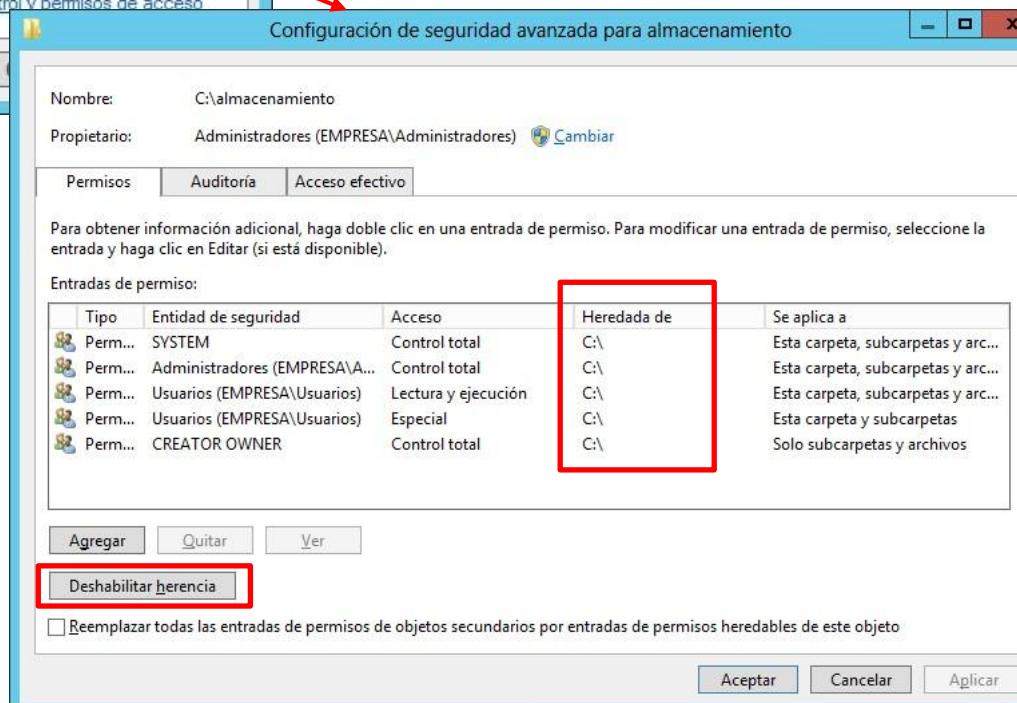
Quina utilitat pràctica penses que pot tindre l'herència de permisos?

## Eliminació d'herència del recurs de nivell superior



Per a eliminar la herència dels permisos configurats en la carpeta de nivell superior, s'ha d'accedir a la fitxa 'Seguridad' i a continuació s'ha de fer clic en 'Opciones Avanzadas'.

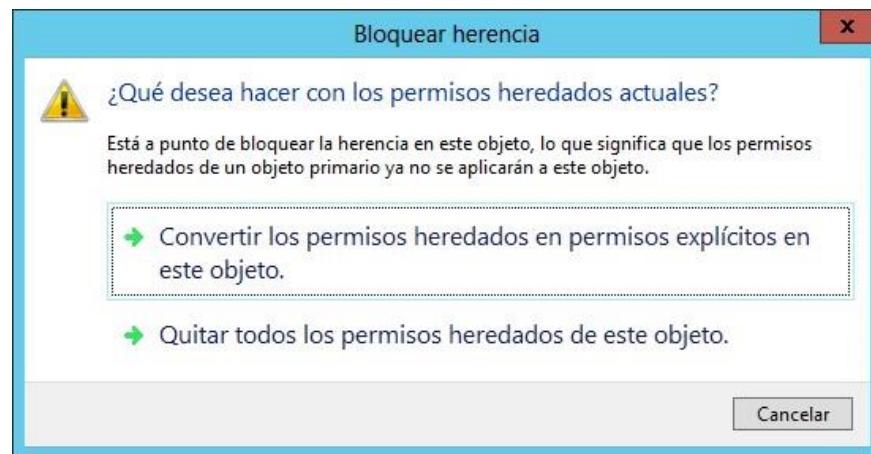
El quadre de diàleg que apareix mostra els permisos actuals i en la columna 'Heredada de' s'indica l'origen del permís.



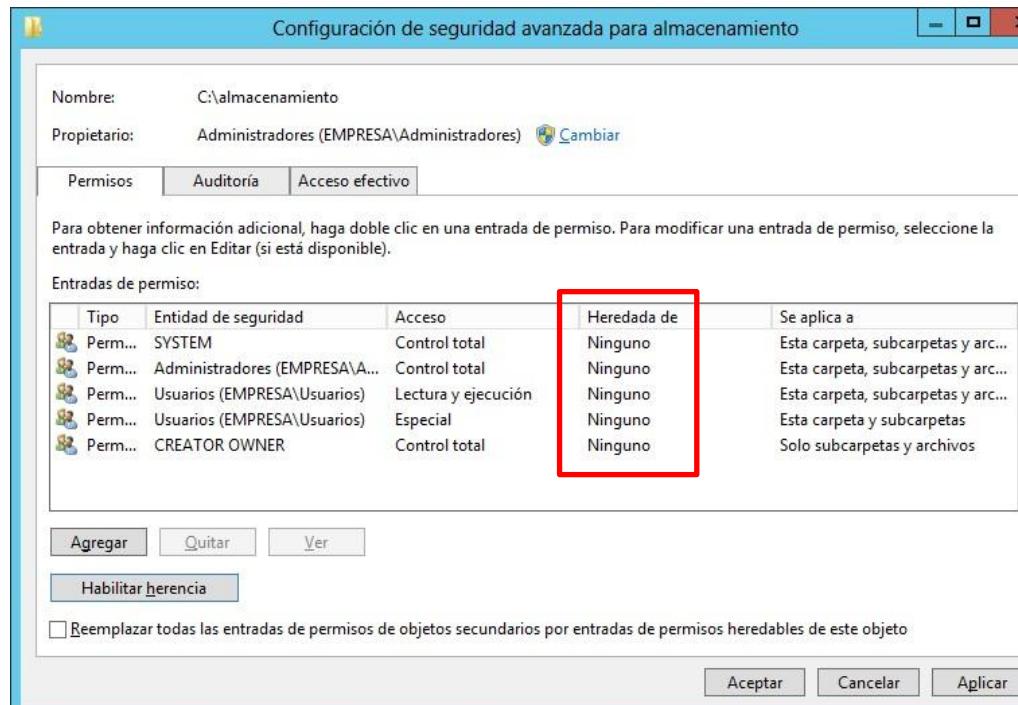
Para eliminar la herencia pulsaremos el botón 'Deshabilitar herencia'.

A continuació apareix un quadre de diàleg que ens dona l'opció de:

- Convertir els permisos heretats en permisos explícits en aquest objecte' (copiar): manté els permisos de tots els arxius i subcarpetas, però no estan vinculats als del nivell superior.
- 'Llevar tots els permisos heretats d'aquest objecte' (llevar): elimina tots els permisos heretats.

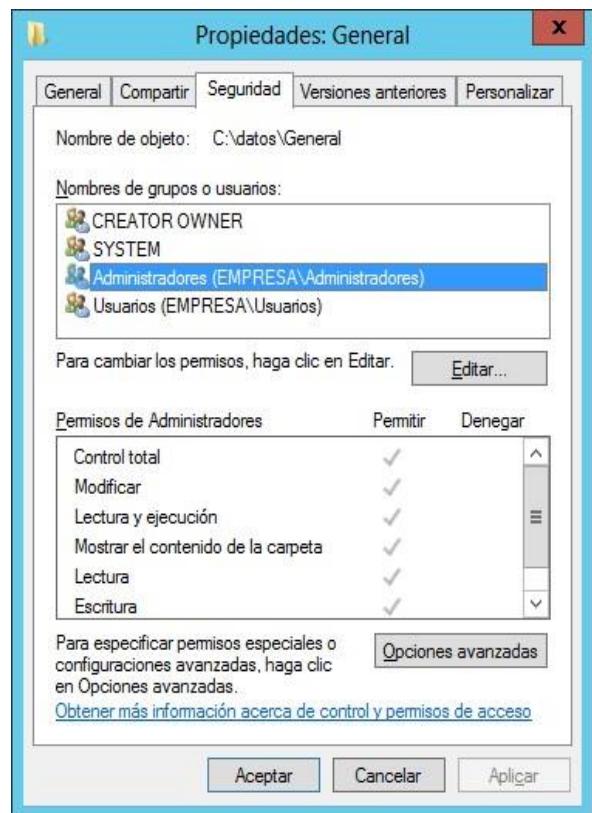


Com norma general farem clic en 'Convertir.../ Copiar'. En el quadre de diàleg de 'Configuración de seguridad avanzada' s'indica els permisos com "Heredada de: ninguno" (no heredados) .

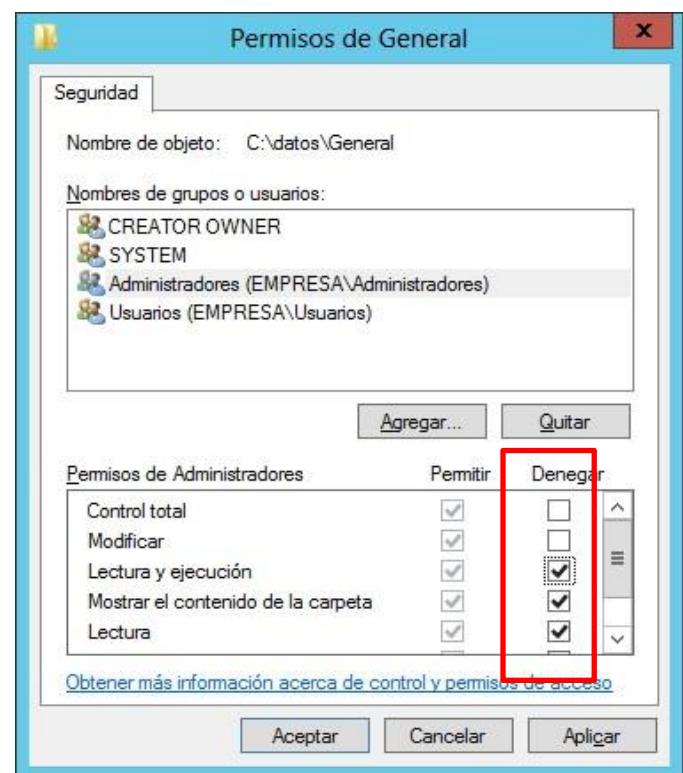


## Canvi dels permisos de l'objecte fill

Si observem els permisos d'un objecte que està heretant permisos, veurem que les caselles de verificació estan (completa o parcialment) inaccessible.



En primer lloc podem interrompre l'herència , denegant explícitament els permisos. Si el permís heretat és de concessió, la denegació està habilitada.



### 3. Directives de Grup (GPO)

Les directives de grup (*Group Policy*) són una sèrie de **configuracions** creades per l'administrador que s'apliquen a objectes del domini. Per mitjà d'aquestes directives, l'administrador controla els entorns de treball dels usuaris del domini, els equips i el comportament de diferents objectes. Són en definitiva un conjunt de regles que faciliten les labors d'administració dels usuaris i equips.

Alguns dels aspectes més útils que es poden definir per part de l'administrador mitjançant les directives són:

- Els comandos d'inici de sessió.
- Característiques de les directives de seguretat dels comptes d'usuari .
- Configuració de l'aparença de la sessió d'usuari .
- Redirecció de l'accés a unes certes carpetes o arxius centralitzats
- Distribució de programari als equips clients.
- Permisos atorgats als comptes d'usuaris i grups, etc.

#### Acumulació de les directives de grup

En existir diferents nivells de directives de grup, aquestes poden entrar en conflicte, fent que apareguen efectes no desitjats en la gestió del domini. En establir directives de grup cal tindre en compte l'ordre d'aplicació d'aquestes :

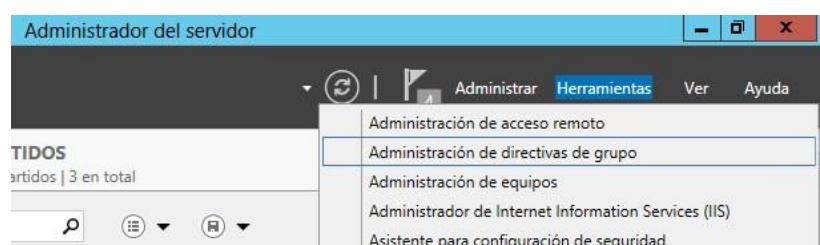
- Directiva de grup local.
- Directiva de grup de lloc.
- Directiva de grup de domini.
- Directiva de grup d'unitat organitzativa.

De manera predeterminada quan existeix una contradicció entre les directives, la que preval serà la que està en un nivell inferior de la llista anterior. Òbviament, en cas de no existir contradiccions, s'apliquen totes les directives.

Si volem saber les directives que estan aplicant-se a un usuari o equip, executarem rsop.msc.

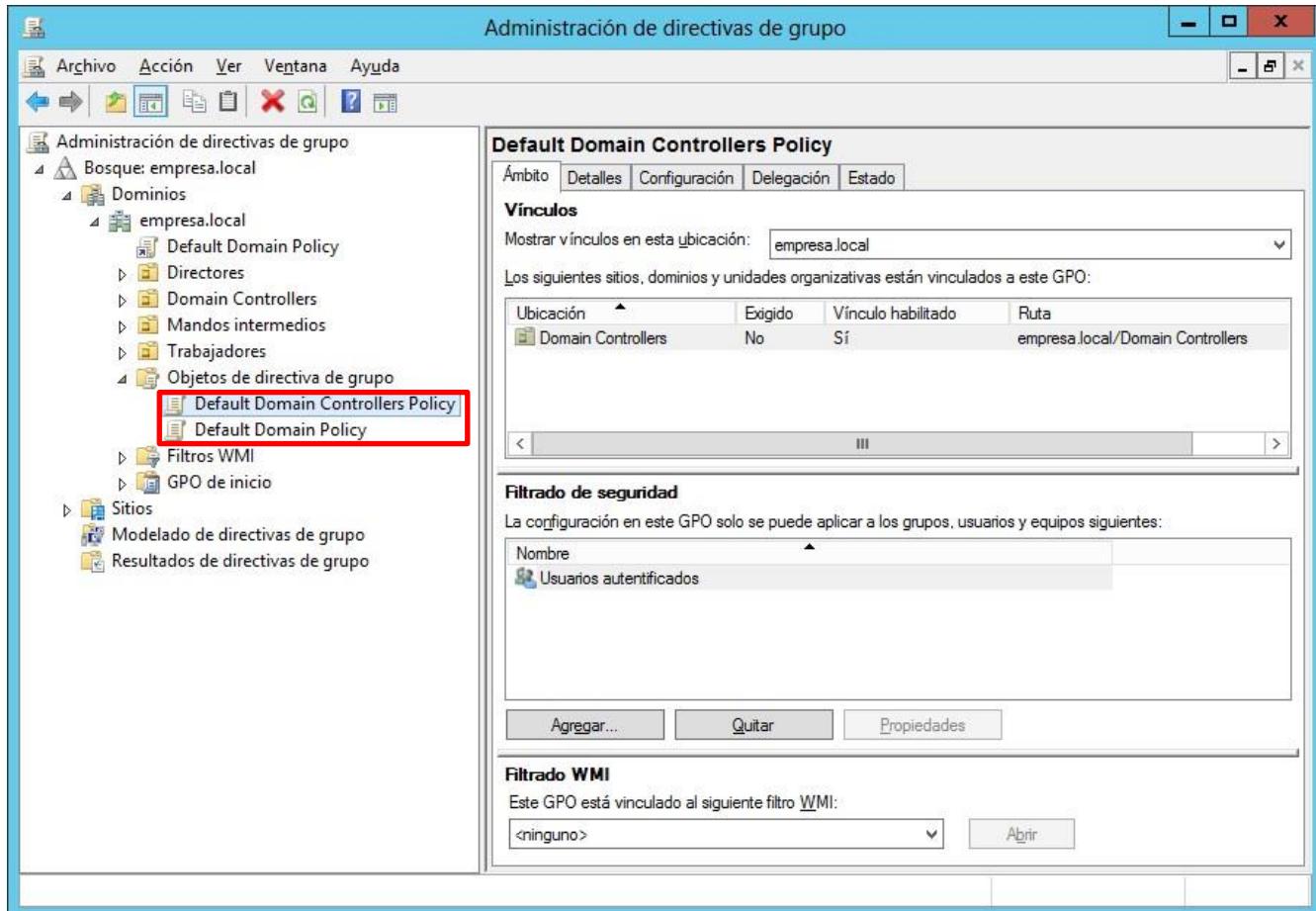
#### 3.1. Edició de les directives de grup predefinides

Per a accedir a la consola d'administració de directives farem clic en "Administrador del servidor->Eines->Administració de directives de grup".



Quan es posa en marxa un domini es creen dues directives de grup anomenades:

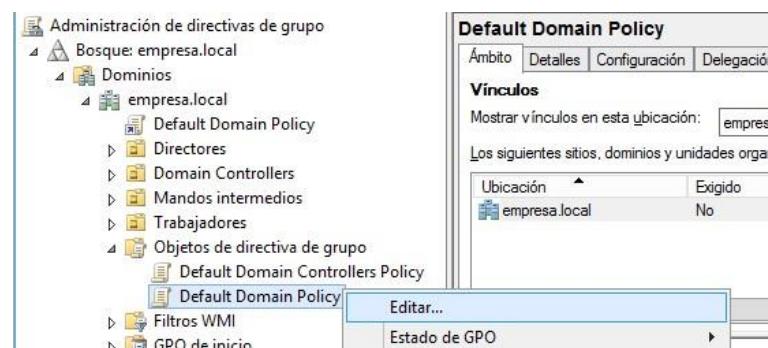
- Default Domain Controllers.
- Default Domain Policy



Aquestes dues directives estableixen la configuració bàsica dels objectes del domini, i estan vinculades respectivament a:

- La unitat organitzativa Domain Controllers.
- El domini.

Aquests dos GPO es componen d'un conjunt molt ampli de directives, com es pot veure en obrir l'editor de directives.



Editor de administración de directivas de grupo

Archivo Acción Ver Ayuda

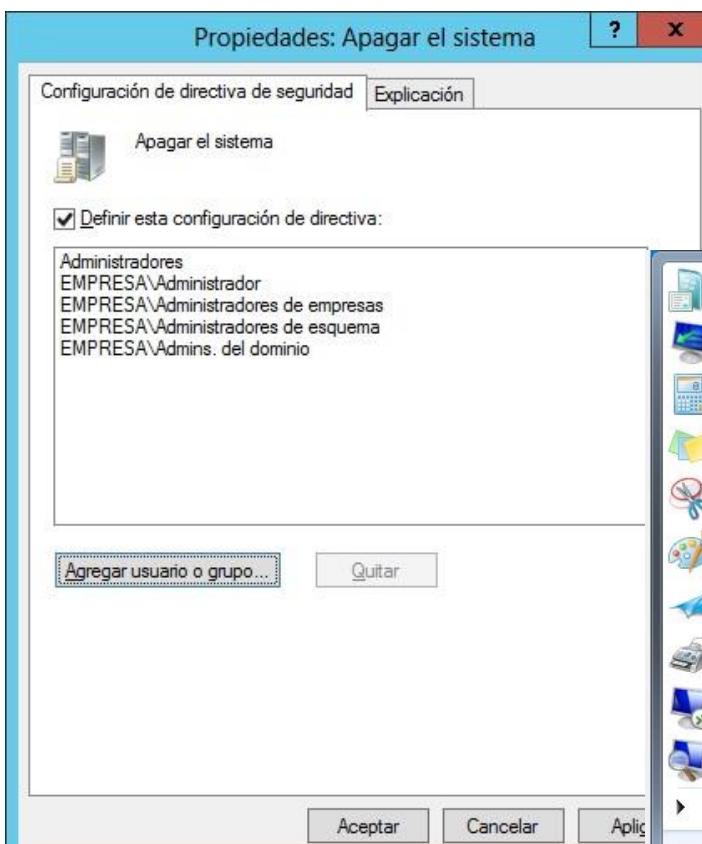
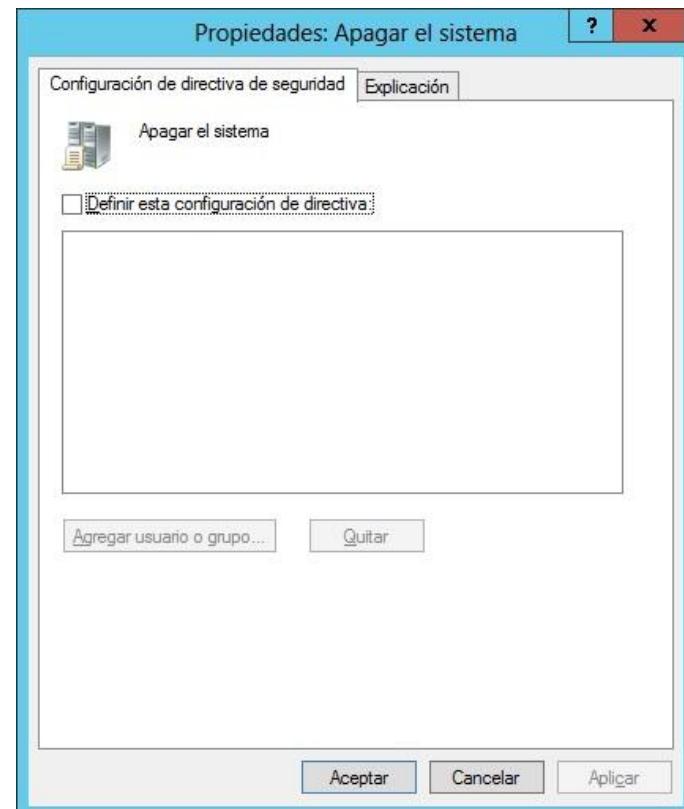
Directiva Default Domain Policy [DC01.EMPRESA.LOCAL]

- Configuración del equipo
- Directivas
  - Configuración de software
  - Configuración de Windows
    - Directiva de resolución de nombres
    - Scripts (inicio o apagado)
  - Configuración de seguridad
    - Directivas de cuenta
    - Directivas locales
      - Directiva de auditoría
      - Asignación de derechos de usuario
      - Opciones de seguridad
    - Registro de eventos
    - Grupos restringidos
    - Servicios del sistema
    - Registro
    - Sistema de archivos
    - Directivas de red cableada (IEEE 802.3)
    - Firewall de Windows con seguridad avanzada
      - Directivas de Administrador de listas de redes
      - Directivas de red inalámbrica (IEEE 802.11)
      - Directivas de clave pública
      - Directivas de restricción de software
      - Protección de acceso a redes
      - Directivas de control de aplicaciones
      - Directivas de seguridad IP en Active Directory (EMPRESA)
      - Configuración de directiva de auditoría avanzada
    - QoS basada en directiva
      - Plantillas administrativas: definiciones de directiva (archivos A)
  - Preferencias
- Configuración de usuario
- Directivas
- Preferencias

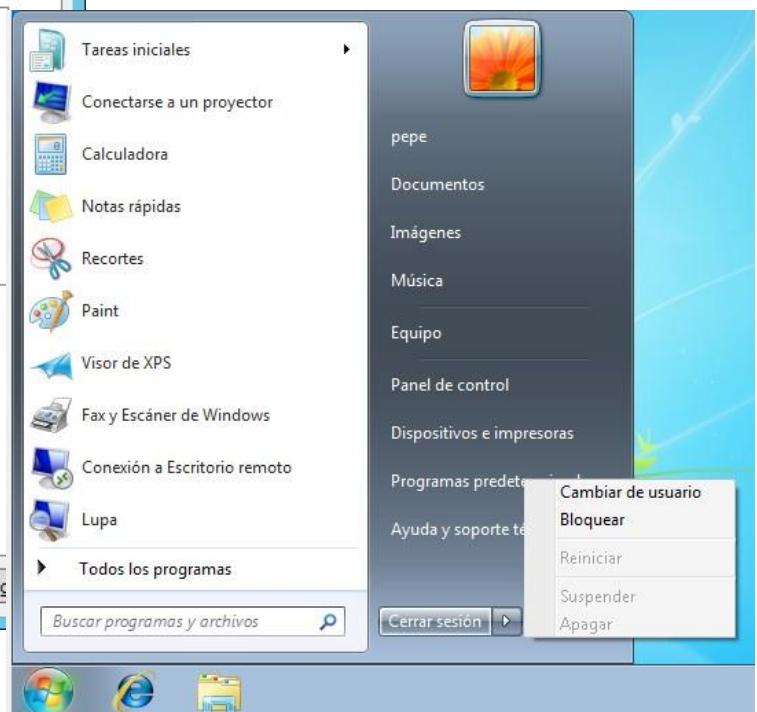
Directiva	Configuración de directiva
[10] Actuar como parte del sistema operativo	No está definido
[10] Administrar registro de seguridad y auditoría	No está definido
[10] Agregar estaciones de trabajo al dominio	No está definido
[10] Ajustar las cuotas de la memoria para un proceso	No está definido
<b>[10] Apagar el sistema</b>	<b>No está definido</b>
[10] Aumentar el espacio de trabajo de un proceso	No está definido
[10] Aumentar prioridad de programación	No está definido
[10] Bloquear páginas en la memoria	No está definido
[10] Cambiar la hora del sistema	No está definido
[10] Cambiar la zona horaria	No está definido
[10] Cargar y descargar controladores de dispositivo	No está definido
[10] Crear objetos compartidos permanentes	No está definido
[10] Crear objetos globales	No está definido
[10] Crear un archivo de paginación	No está definido
[10] Crear un objeto símbolo (token)	No está definido
[10] Crear vínculos simbólicos	No está definido
[10] Denegar el acceso a este equipo desde la red	No está definido
[10] Denegar el inicio de sesión como servicio	No está definido
[10] Denegar el inicio de sesión como trabajo por lotes	No está definido
[10] Denegar el inicio de sesión local	No está definido
[10] Denegar inicio de sesión a través de Servicios de Escritorio remoto	No está definido
[10] Depurar programas	No está definido
[10] Forzar cierre desde un sistema remoto	No está definido
[10] Generar auditorías de seguridad	No está definido
[10] Generar perfiles de un solo proceso	No está definido
[10] Generar perfiles del rendimiento del sistema	No está definido
[10] Habilitar confianza con el equipo y las cuentas de usuario propias	No está definido
[10] Hacer copias de seguridad de archivos y directorios	No está definido
[10] Iniciar sesión como proceso por lotes	No está definido
[10] Iniciar sesión como servicio	No está definido
[10] Modifica la etiqueta de un objeto	No está definido
[10] Modificar valores de entorno firmware	No está definido

Suposem que volem canviar la configuració de la directiva que aplica sobre el permís per a **apagar l'equip**. En aqueix cas la buscaríem entre tot el conjunt de directives dins del GPO Default Domain Policy i faríem doble clic sobre ella.

En el quadre de diàleg que s'ha obert podem comprovar que aquesta directiva no està habilitada.



Si la habilitem i únicament atorguem permís als administradors del domini, podrem comprobar que efectivament un usuari del domini que inicia sessió en un equip client **no pot apagar-lo**, únicament podria un usuari amb privilegis d'administració.



Per a evitar generar un trànsit de gestió excessiu en la xarxa, les directives de grup no s'actualitzen immediatament després de la seua modificació, sinó que està establitz un interval de 5 minuts entre actualitzacions automàtiques. No obstant això , aquest interval es pot modificar en les pròpies directives de grup (veure pàgina de [Microsoft Technet](#)). De tota manera, no és necessari modificar aquest interval per a comprovar la correcta aplicació de les directives de grup, n'hi ha prou amb escriure en la consola cmd:

```
>>gpupdate
```

o

```
>>gpupdate /force
```

Aquesta última pot requerir el reinici del controlador de domini. (Més informació sobre les opcions i característiques de gpupdate en [Technet](#)).

Per a exemplificar tot l'anterior modificarem la *Default Domain Policy* per a implementar les següents configuracions en el domini:

1. Si l'usuari s'equivoca tres vegades en introduir la seu contrasenya, el seu compte queda bloquejat (només la podrà desbloquejar l'administrador). Això protegeix el sistema de possibles atacs.
2. La contrasenya haurà de tindre un mínim de 8 caràcters, però no és necessari obligatòriament que siguin majúscules, minúscules, caràcters alfanumèrics, obligatòriament, etc.
3. La contrasenya que s'haja utilitzat ja, no podrà tornar-se a utilitzar fins a passats almenys 10 canvis de contrasenya (d'aquesta manera vam forçar a l'usuari al fet que no 'recicle' contrasenyes antigues, incrementant la seguretat del sistema).
4. L'usuari ha de canviar la contrasenya cada sis mesos, en establir una 'vida útil' de les contrasenyes tenim un sistema més segur, ja que en cas que algú haja esbrinat la contrasenya de l'usuari , i no s'haja detectat, com tard als sis mesos, perdrà l'accés al compte.

En les següents subseccions s'examina la manera de dur a terme aquestes configuracions del sistema.

Les directives de seguretat relacionades amb les contrasenyes no poden aplicar-se sobre GPOs diferents de la *Domain Default Policy*.

Si per exemple volem que diferents usuaris del domini tinguen diferents característiques de les seues contrasenyes, haurem d'utilitzar la *Fine-Grained Password Policy*, la qual és una mica complexa de configurar. En el següent [enllaç](#) teniu una guia que explica pas a pas com crear-les i configurar-les per a aconseguir la funcionalitat comentada anteriorment. No obstant això la configuració de la *Fine-Grained Password Policy* queda fora de l'abast d'aquest curs.

### 3.1.1. Bloqueig de compte en introduir en tres ocasions una contrasenya errònia

En primer lloc editarem el GPO 'Default Domain Policy' per a configurar la directiva de bloqueig de compte. Aquesta es troba en 'Configuració de l'equip'→'Directives'→'Configuració de Windows'→'Directiva de bloqueig de compte'→'Llindar de bloqueig de compte'

The screenshot shows the 'Editor de administración de directivas de grupo' (Group Policy Management Editor). In the left pane, under 'Directiva Default Domain Policy [DC01.EMPRESA.LOCAL]', the 'Directivas de cuenta' (Account policies) node is expanded, showing 'Directiva de bloqueo de cuenta' (Lockout policy) selected. In the right pane, three configurations are listed:

Directiva	Configuración de directiva
Duración del bloqueo de cuenta	No está definido
Restablecer el bloqueo de cuenta después de	No está definido
<b>Umbral de bloqueo de cuenta</b>	0 intentos de inicio de sesión no...

A separate window titled 'Propiedades: Umbral de bloqueo de cuenta' (Properties: Lockout threshold) is open, showing the configuration details:

Configuración de directiva de seguridad | Explicación

**Umbral de bloqueo de cuenta**

Definir esta configuración de directiva

La cuenta se bloqueará después de:  
3 intentos de inicio de sesión no válidos

Another window titled 'Propiedades: Duración del bloqueo de cuenta' (Properties: Lockout duration) is also visible, showing:

Configuración de directiva de seguridad | Explicación

**Duración del bloqueo de cuenta**

Definir esta configuración de directiva

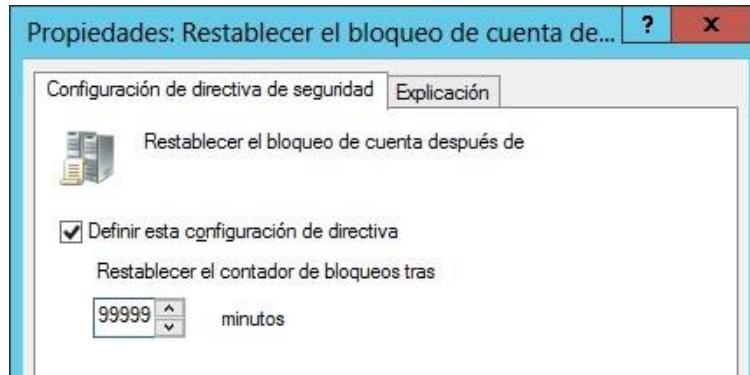
La cuenta está bloqueada hasta que el administrador la desbloquee.  
0 minutos

Modifiquem el valor de llindar a '3 intents' d'inici de sessió erronis.

A més, configurarem la duració del bloqueig, on un valor de 0 indica que el compte haurà de ser desbloquejat manualment per l'administrador.

Finalment també configurarem el temps que ha de transcórrer entre intents perquè el comptador de fallades d'inici de sessió torne a zero abans que es bloquege el compte.

Posarem el màxim valor permès.

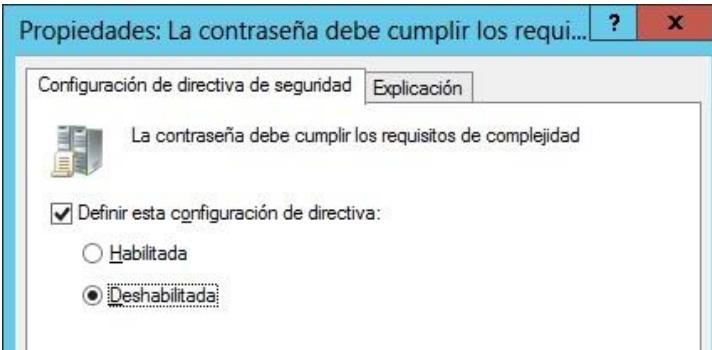
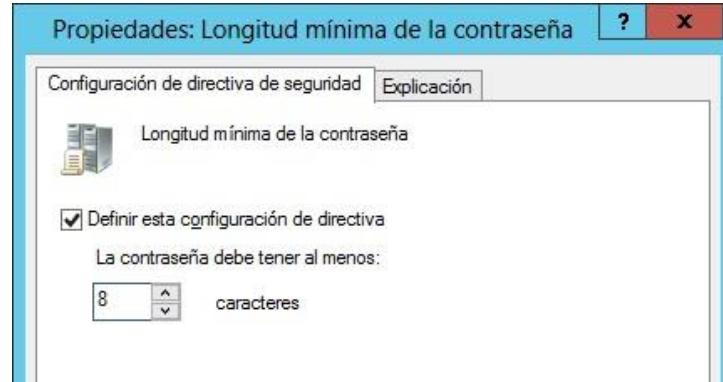


### 3.1.2. Longitud de la contrasenya

Com en el cas anterior editarem el GPO 'Default Domain Policy' per a configurar la longitud i complexitat de les contrasenyes.

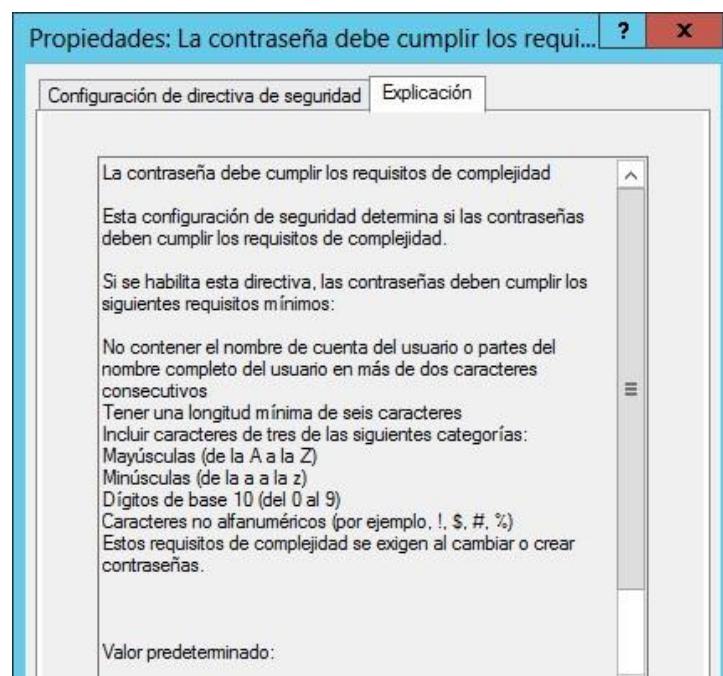
Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	Deshabilitada
Exigir historial de contraseñas	24 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	1 días

Modifiquem el valor de la longitud a 8 caràcters.



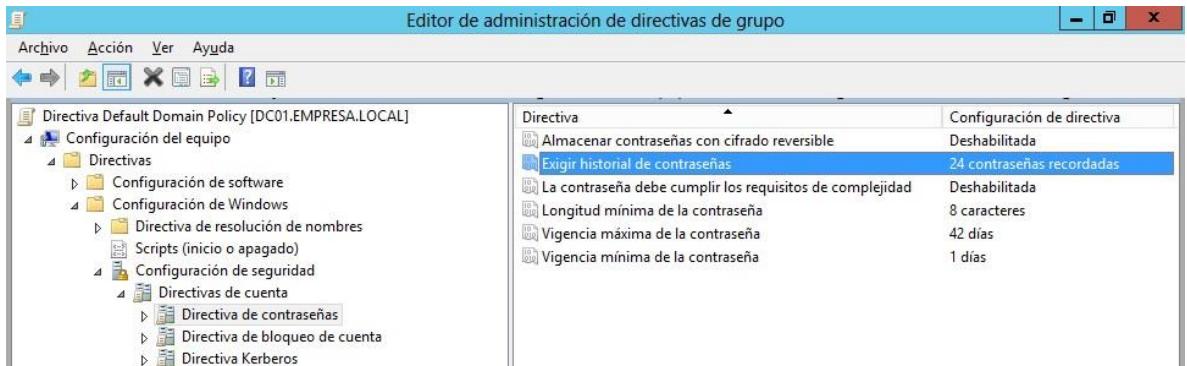
A continuació, deshabilitem els requisits de complexitat de les contrasenyes.

En aquesta imatge es pot veure les característiques de complexitat que aplica aquesta directiva quan està habilitada.

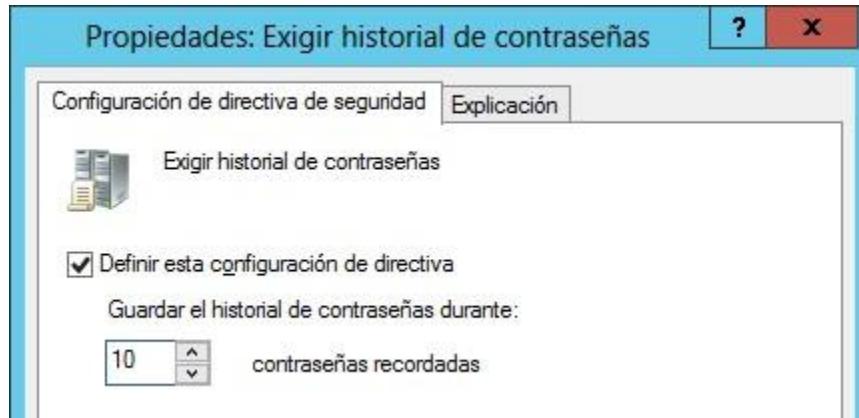


### 3.1.3. Històrial de la contrasenya

Editem de nou el GPO 'Default Domain Policy' i accedim a les directives de contrasenyes.

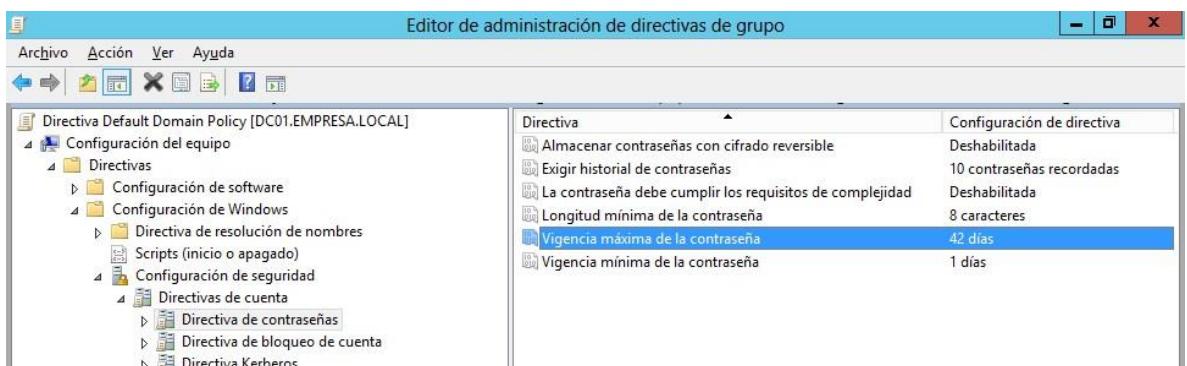


I modifiquem el nombre de contrasenyes diferents que han d'utilitzar-se abans de poder repetir una contrasenya.

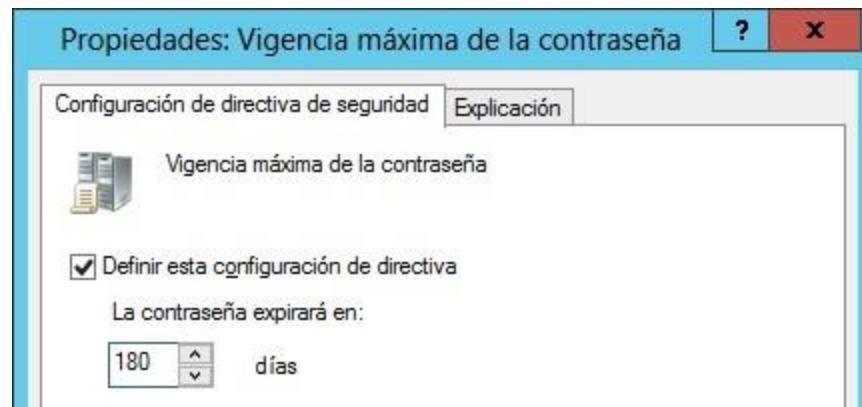


### 3.1.4. Vigència de la contrasenya

Com en casos anteriors accedim a les directives de contrasenyes.



Canviem la duració màxima de les contrasenyes a 180 dies -6 mesos- .



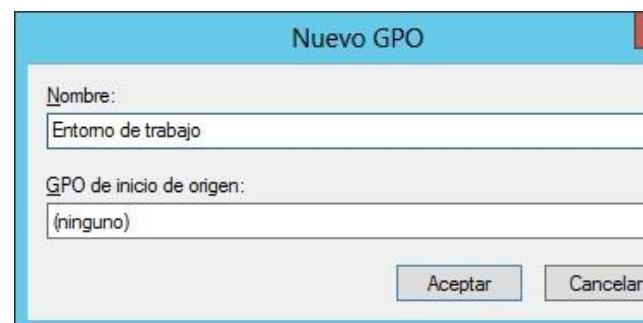
### 3.2. Creació de Directives de Grup

Per a crear una directiva de grup obrirem la consola d'administració de directives com en el punt anterior Administrador del servidor->Eines ->Administració de directives de grup.

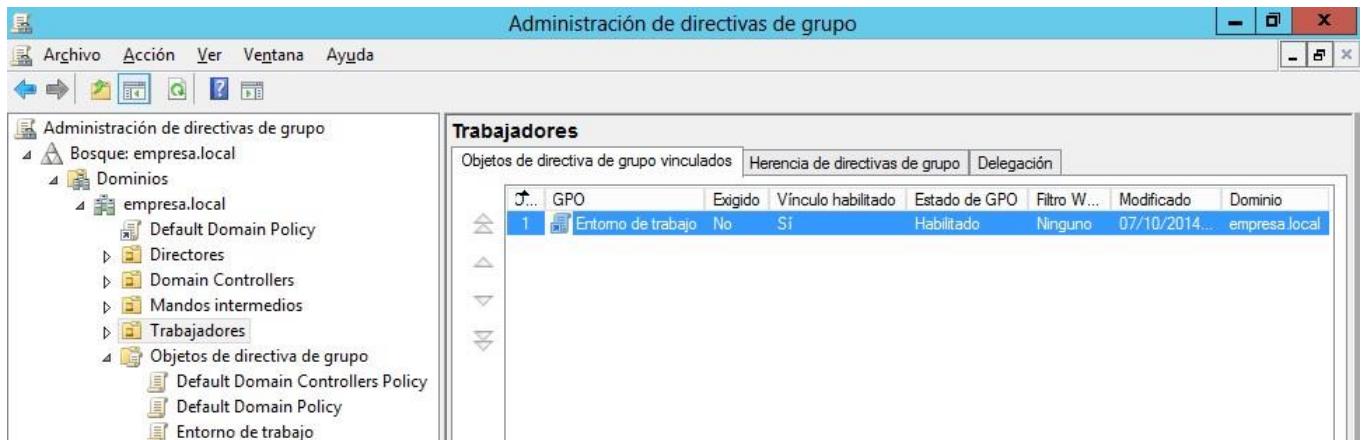
Suposem que volem crear una Directiva de Grup sobre la unitat organitzativa 'Treballadors' creada anteriorment. Fem clic amb el botó secundari i triem l'opció 'Crear un GPO en aquest domini i vincular-lo ací'. treball',



Apareixerà un quadre de diàleg i introduirem el nom desitjat , per exemple 'Entorno de trabajo' ja que posteriorment utilitzarem aquesta directiva per a configurar un entorn de treball homogeni en tots els usuaris que pertanyen a la Unitat Organitzativa 'Trabajadores'.



La nova directiva apareixerà en el panell de detalls.



Seleccionem el GPO i fem clic amb el botó dret, triant l'opció 'Editar'.

Amb la nova directiva estableirem les següents configuracions:

1. Tots els membres de la unitat organitzativa 'Trebballadors' tindran un fons d'escriptori 'corporatiu' que s'instal·larà de manera automàtica i que no podrà ser modificat.
2. Els membres de la unitat organitzativa 'Trebballadors' no poden obrir la consola de comandos.

En les següents subseccions s'examina la manera de conducta per a dur a terme aquestes configuracions del sistema.

### 3.2.1. Fons d'escriptori obligatori

Per a modificar d'una manera centralitzada el fons d'escriptori dels usuaris de la unitat organitzativa 'Trebballadors' hem d'editar la directiva 'Entorn de Treball' i accedir a' Configuració de l'usuari '→'Plantilles administratives'→'Active Desktop'→'Active Desktop'.

**Editor de administración de directivas de grupo**

Archivo Acción Ver Ayuda

← → 🔍 🗂️ 🗃️ 🗁️ 🗁️

Directiva Entorno de trabajo [DC01.EMPRESA.LOCAL]

- Configuración del equipo
  - Directivas
  - Preferencias
- Configuración de usuario
  - Directivas
    - Configuración de software
    - Configuración de Windows
    - Plantillas administrativas: definiciones de
      - Active Desktop
        - Active Desktop
        - Active Directory
        - Carpetas compartidas
      - Componentes de Windows
      - Menú Inicio y barra de tareas
      - Panel de control

Active Desktop

Seleccione un elemento para ver su descripción.

Configuración	Estado
Habilitar Active Desktop	No configurada
Deshabilitar Active Desktop	No configurada
No permitir cambios	No configurada
Tapiz del escritorio	No configurada
Prohibir agregar elementos	No configurada
Prohibir cerrar elementos	No configurada
Prohibir eliminar elementos	No configurada
Prohibir modificar elementos	No configurada
Deshabilitar todos los elementos	No configurada
Agregar o quitar elementos	No configurada
Permitir solo papel tapiz de mapa de bits	No configurada

Habilitem l'Active Desktop, el qual permet posar com a fons d'descriptori imatges jpg o fitxers HTML.

**Habilitar Active Desktop**

**Habilitar Active Desktop**

No configurada Comentario:

Habilitada

Deshabilitada Compatible con:

Solo Windows Server 2003, Windows XP y Windows 2000

Opciones: Permite papel tapiz JPEG y HTML

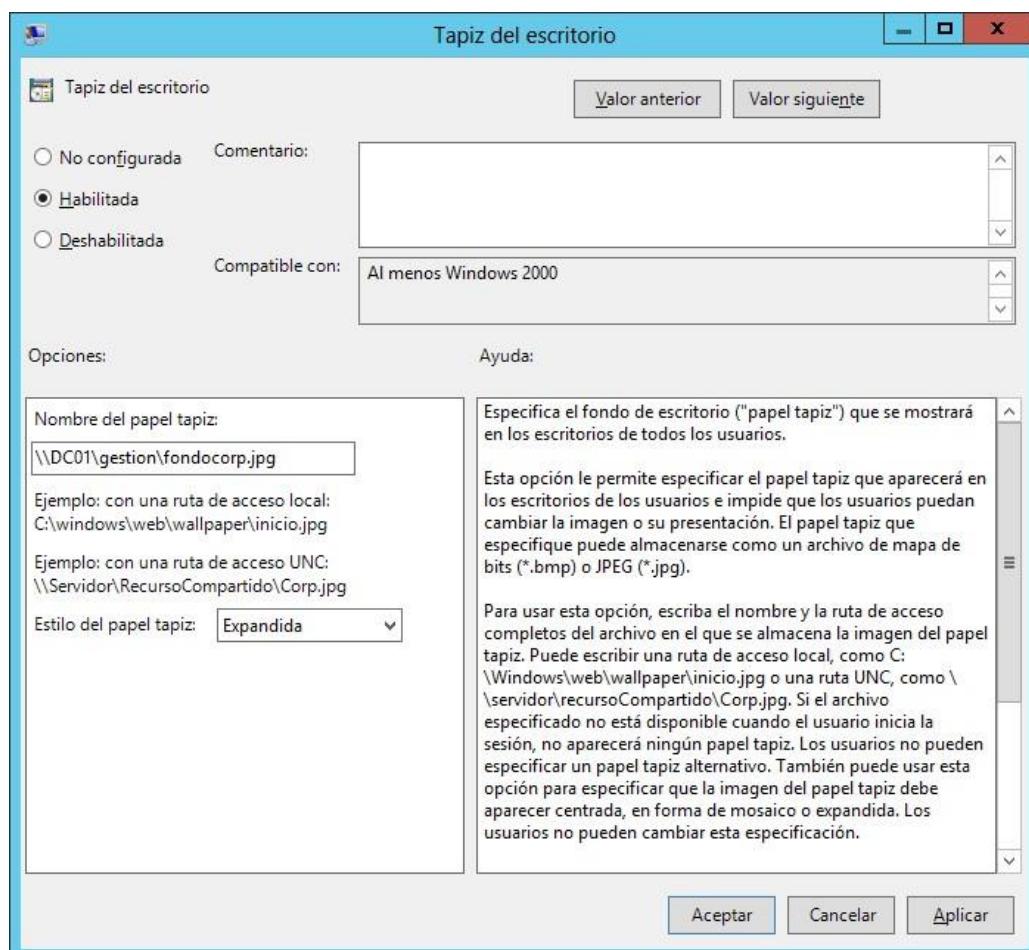
Ayuda: Habilita Active Desktop e impide que los usuarios lo puedan deshabilitar. Esta opción impide que los usuarios intenten habilitar o deshabilitar Active Desktop mientras una directiva lo controla. Si deshabilita esta opción o no la configura, Active Desktop se deshabilita de forma predeterminada, pero los usuarios pueden habilitarlo. Nota: si las opciones "Habilitar Active Desktop" y "Deshabilitar Active Desktop" están habilitadas, la opción "Deshabilitar Active Desktop" se omitirá. Si la opción "Activar Shell clásico" (en Configuración de usuario\Plantillas administrativas\Componentes de Windows\Explorador de Windows) está habilitada, Active Desktop estará deshabilitado y ambas directivas se omitirán.

Aceptar Cancelar Aplicar

Impedirem també que els usuaris puguen modificar el fons d'escriptori .



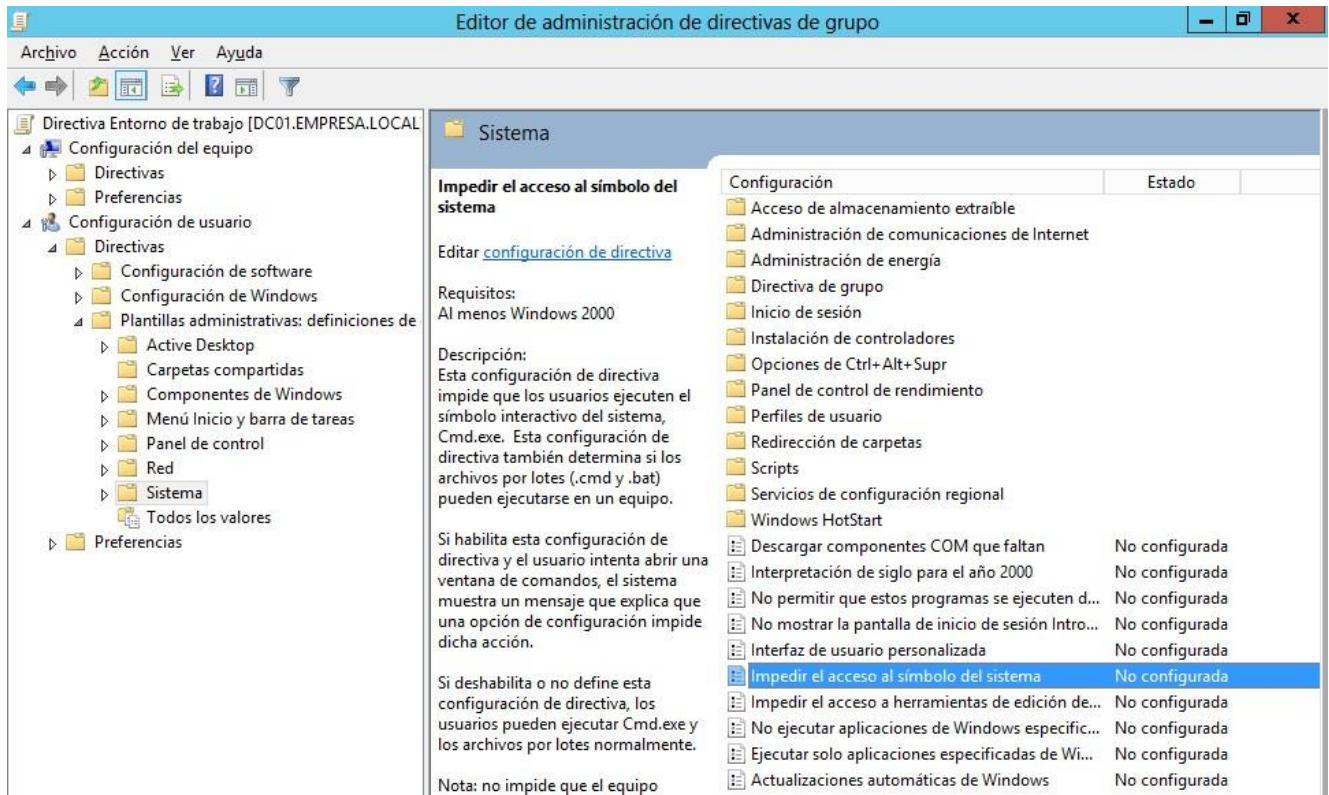
Indiquem la ruta en la qual es troba la imatge que volem posar com a fons d'escriptori . En aquest cas es diu fondocorp.jpg i està en la carpeta compartida 'gestion' albergada en el servidor.



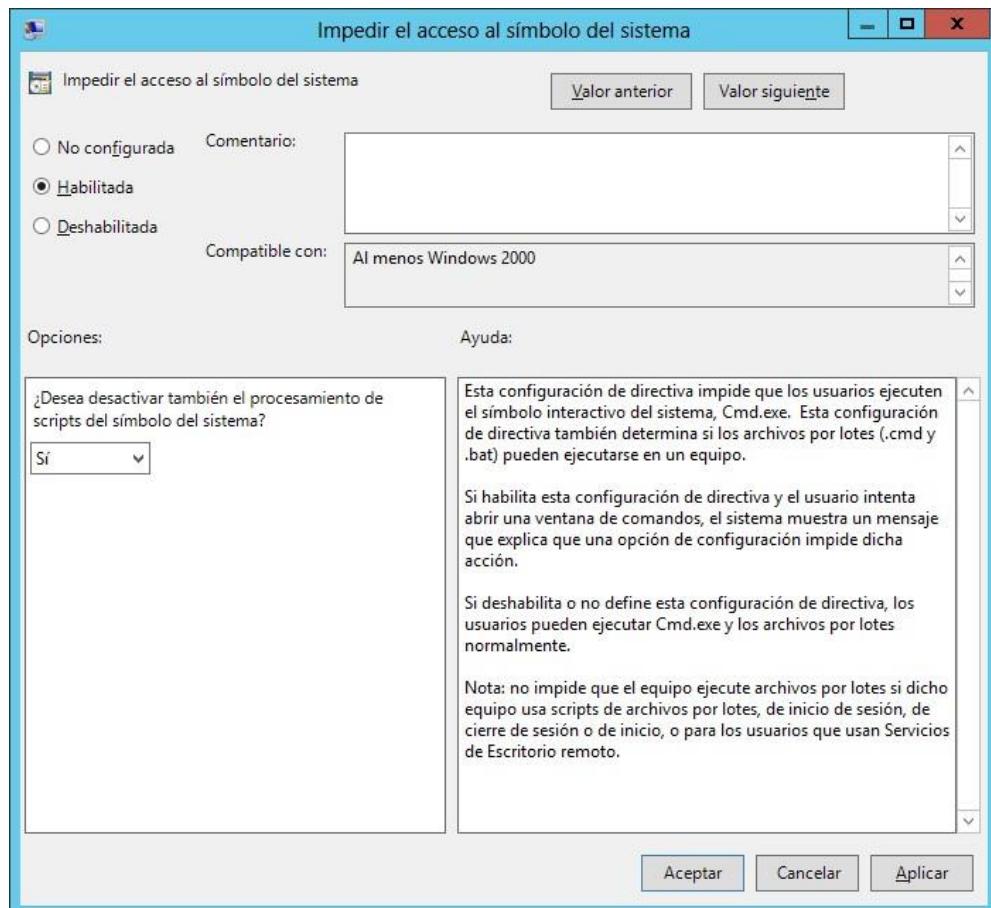
La imatge ha de trobar-se en una carpeta compartida en xarxa (preferiblement en el servidor per qüestions de disponibilitat) on tots els usuaris del domini tinguin permís de lectura.

### 3.2.2. Bloqueig de la línia de comandos

Per a bloquejar la línia de comandos editarem el GPO corresponent accedint a' Configuració de l'usuari '→'Directives→Plantilles administratives'→'Sistema'.



Habilitem el bloqueig i el processament de scripts del símbol del sistema.



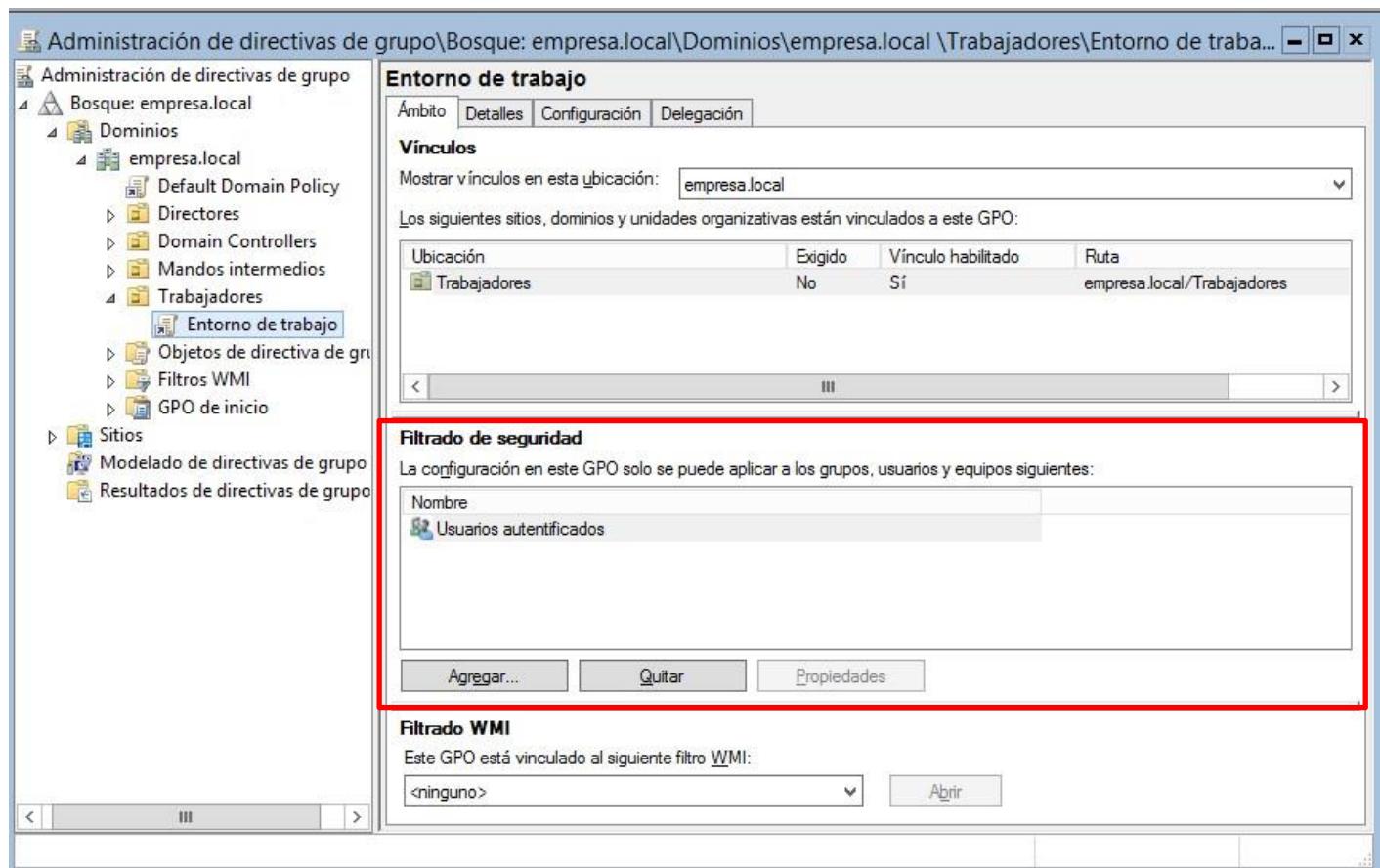
Finalment ja només queda actualitzar mitjançant gpupdate les directives modificades en el GPO 'Treballadors'.

```
Administrator: Símbolo del sistema
Microsoft Windows [Versión 6.2.9200]
(c) 2012 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>gpupdate
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
```

Recordeu que únicament afectaran els membres de la unitat organitzativa treballadors independent del grup al qual pertanguen, si no explicitem el contrari en el camp 'Filtrat de Seguretat'.



### 3.2.3. Comprovació de les directives establides

Ara comprovarem que les directives s'han aplicat correctament. Per a això utilitzarem un usuari qualsevol dins de la unitat organitzativa 'Treballadors' que és sobre la qual s'apliquen el GPO creat 'Entorn de Treball', i obviament el GPO Default Domain Policy, que hem editat. En aquest cas es faran les proves amb l'usuari Mario.Juan (la seua contrasenya inicial la qual podem consultar en el fitxer usuaris.csv és ABC123!).

#### Bloqueig de compte

La primera directiva que hem aplicat consistia a bloquejar el compte indefinidament en introduir en tres ocasions la contrasenya incorrectament. Ens equivoquem voluntàriament en iniciar sessió en un equip client i el compte s'acaba bloquejant.



Comprovem en el controlador de domini que efectivament està bloquejada i la desbloquegem.

**Propiedades: MarioJuan**

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto		COM+	
General	Dirección	Cuenta	Perfil
		Telefonos	Organización
			Miembro de

Nombre de inicio de sesión de usuario:  
Mario.Juan @empresa.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):  
EMPRESA\ Mario.Juan

Horas de inicio de sesión... Iniciar sesión en...

Desbloquear cuenta. Esta cuenta está bloqueada en este controlador de dominio de Active Directory.

Opciones de cuenta:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión
- El usuario no puede cambiar la contraseña
- La contraseña nunca expira
- Almacenar contraseña utilizando cifrado reversible

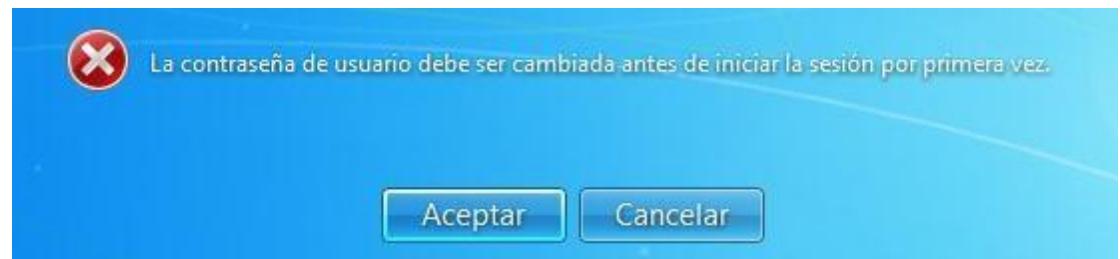
La cuenta expira

Nunca  
 Fin de: jueves , 6 de noviembre de 2014

**Aceptar Cancelar Aplicar Ayuda**

### Longitud de contrasenya

Una vegada desbloquejada el compte, iniciem sessió amb aquest usuari i el primer que se'n indica és que hem de canviar la contrasenya, tal com es va configurar en el tema anterior en crear els usuaris del domini.



Introducimos una nueva contraseña ( mariojuansin caracteres especiales ni números, y lo ngitud al menos de 8 caracteres.

El sistema nos indica que la contraseña se cambió correctamente.



### Fons d'descriptori obligatori

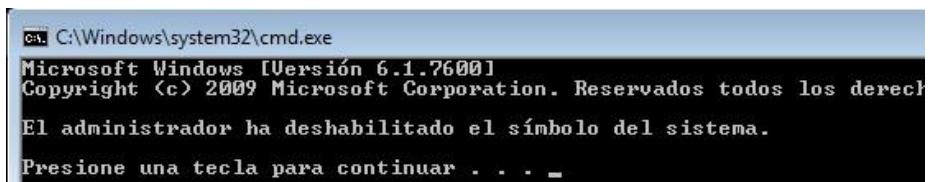
En iniciar sessió es carrega el fons d'descriptori definit amb la directiva de grup, i a més l'usuari no pot modificar-lo.



### Bloqueig de la línia de comandos

Una vegada iniciada la sessió, si s'intenta

executar cmd apareix el següent missatge.



Podeu comprovar que les altres dues directives establides també funcionen correctament.

## 4. Perfs

Podem definir un perfil com aquells aspectes de configuració de l'equip i de l'entorn de treball propis de l'usuari i que a més són exportables a altres màquines de manera transparent a aquest. En altres paraules, mitjançant els perfils aconseguim que l'usuari **independently** de l'equip en el qual inicia la sessió dispose d'un entorn de treball similar. Tot això s'entendrà millor amb els exemples preparats en les seccions següents.

Existeixen tres tipus de perfils:

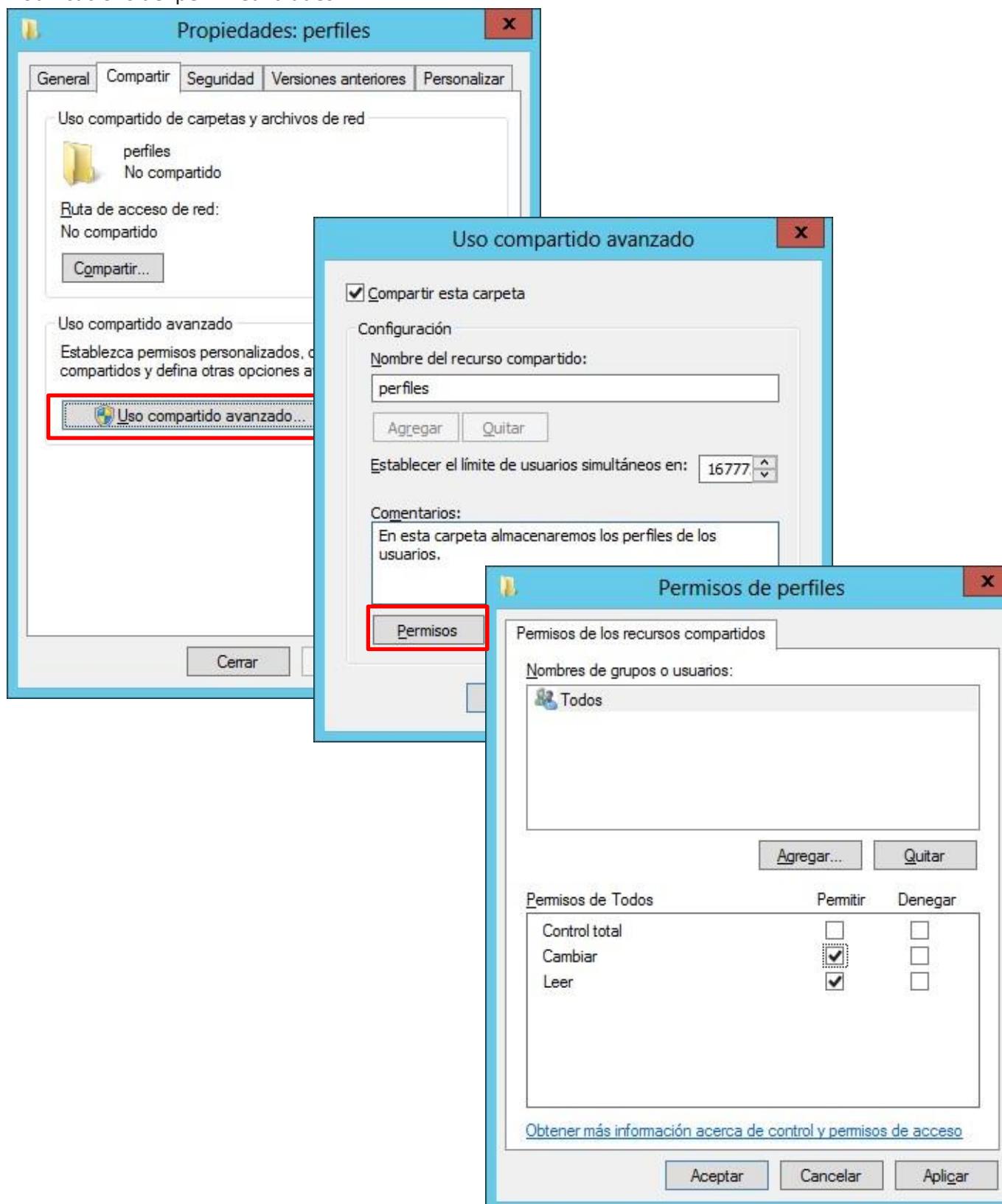
1. Perfs locals: s'emmagatzemen en l'equip, i configuren l'entorn de treball de cada usuari. No els abordarem en aquest curs ja que el que ens interessa és la gestió centralitzada de recursos.
2. Perfs mòbils: l'usuari configura l'entorn de treball al seu gust en un equip, i en iniciar sessió en qualsevol altra estació de treball, la configuració s'importa i aplica a aqueix nou equip. Abordarem aquest tipus de perfils en l'apartat 5.1
3. Perfs obligatoris: un usuari amb permisos d'administració defineix la configuració de l'entorn de treball, i s'aplica als usuaris del domini. Aquests poden modificar-la durant la sessió, però en iniciar una altra sessió, es torna a carregar la configuració del perfil obligatori. En lloc de treballar amb perfils obligatoris, en l'apartat anterior hem vist com configurar entorns de treball definits per als membres d'una unitat organitzativa d'una manera més còmoda i potent.

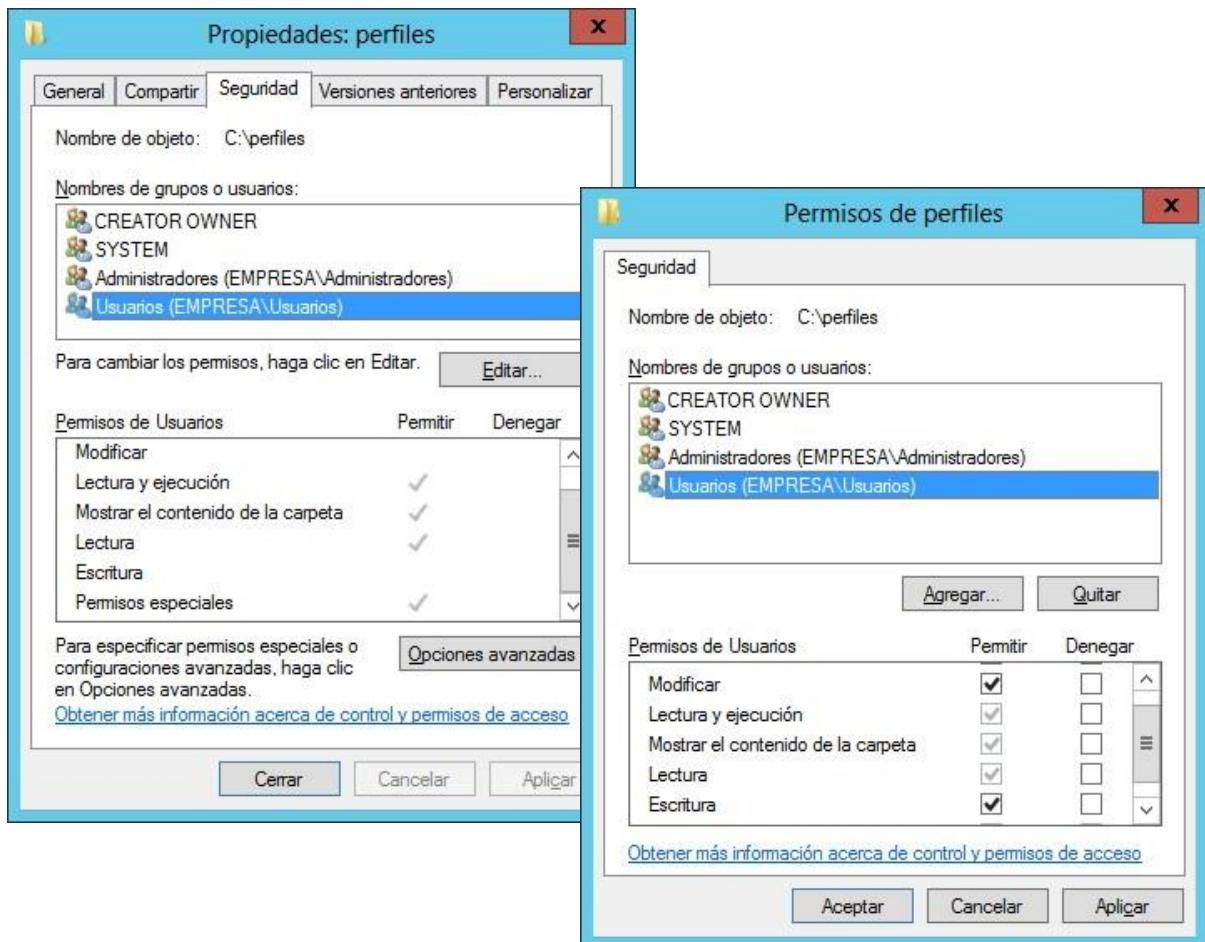
### 4.1. Perfs mòbils

Com s'ha comentat en l'apartat anterior, els perfils consisteixen en una sèrie de fitxers de configuració de l'entorn de treball, que s'apliquen a tots els equips de la xarxa des d'on puga començar sessió l'usuari. Aquests fitxers de configuració han d'emmagatzemar-se en una ubicació accessible pels equips clients, com per exemple el controlador de domini.

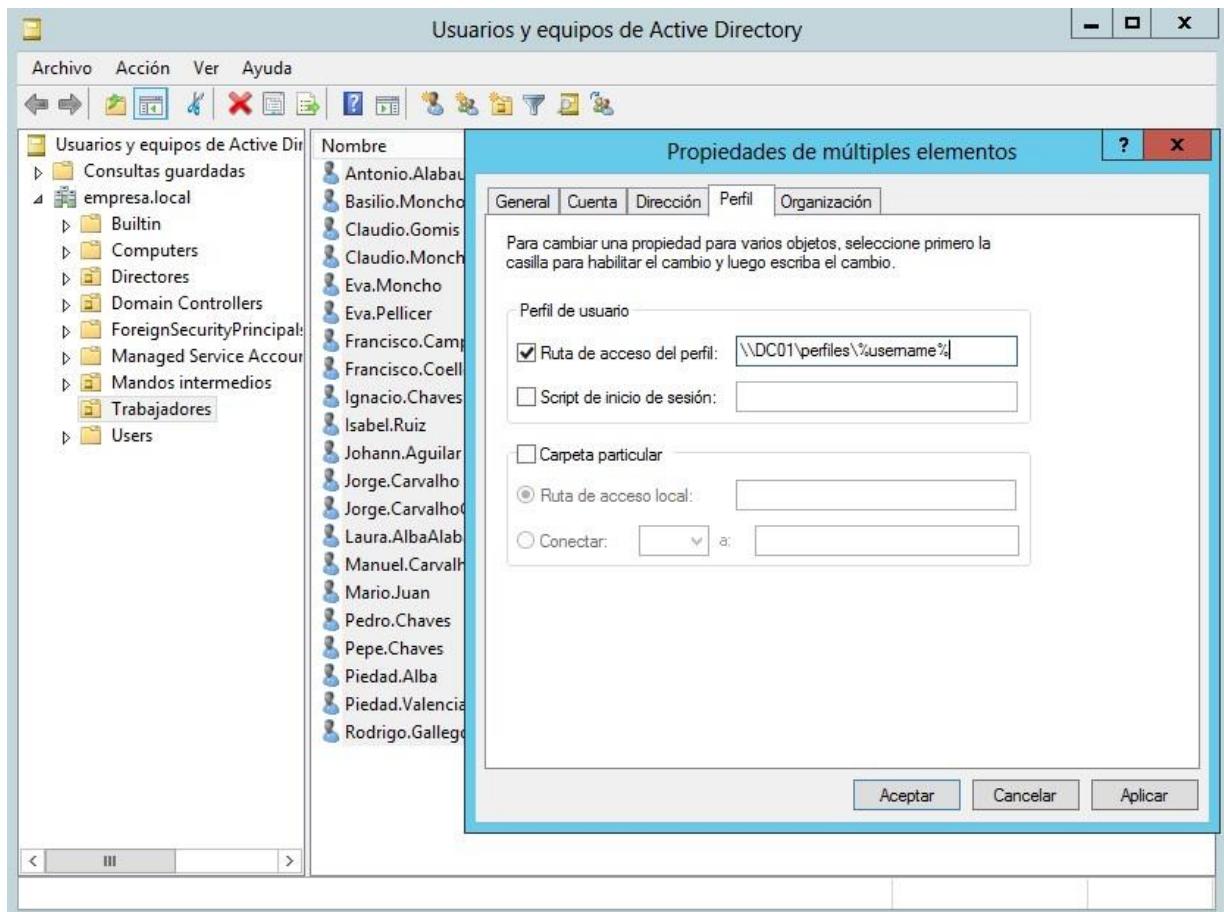
Concretament, emmagatzemarem els perfils en una carpeta del servidor denominada 'Perfs', i que haurem de compartir en xarxa amb els permisos adequats perquè en iniciar

sesió el sistema puga carregar la configuració, i en tancar sessió, en el seu cas , es guarden les modificacions del perfil realitzades.





Ja disposem d'una ubicació en xarxa amb els permisos suficients on s'emmagatzemaran els perfils. Ara cal indicar en els comptes d'usuari la ubicació d'aquesta carpeta. Per a això, anirem a cadascuna de les tres unitats organitzatives que creuem en pràctiques anteriors ('Directors', 'Comandaments Intermedis' i 'Treballadors') i seleccionarem tots els usuaris. A continuació , amb el botó secundari farem clic en propietats i accedirem a la fitxa 'Perfil', la qual és de les poques opcions comunes a tots els usuaris que podem modificar d'aquesta manera.



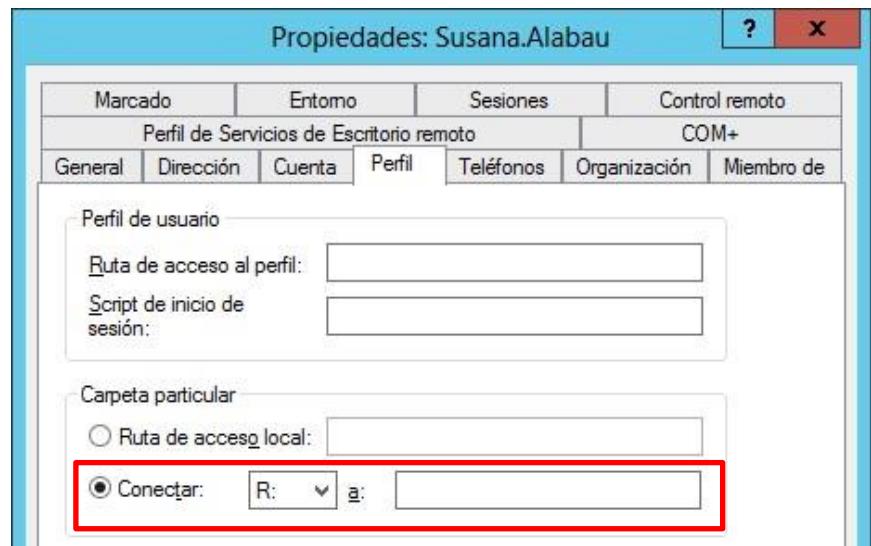
En la imatge anterior, observem que s'ha introduït com a ruta del perfil [\DC01\perfils%\username%](\\DC01\perfils%\username%). En lloc d'introduir-la manualment per a cada usuari, %username% és una variable del sistema que conté el nom de l'usuari, per tant en aplicar aquesta variable al perfil de, per exemple, Sara.Zambujo, es crearà una carpeta en [\DC01\perfils](\\DC01\perfils) que es dirà Sara.Zambujo.V2.

Comprovem que efectivament funciona el perfil mòbil establiti. Per a això l'usuari Sara.Zambujo modificarà el fons d'escriptori (recordeu que els usuaris de la unitat organitzativa 'Comandaments Intermedis' sí que tenen permís per a això), i afegirà algun document en l'escriptori.

Perquè el nou fons d'escriptori s'aplique a diferents equips Windows és necessari que la imatge de fons siga accessible des dels equips Windows en els quals s'iniciarà sessió.

## 5. Carpetes personals

Una altra de les opcions més utilitzades que pot configurar-se en la fitxa 'Perfils' de les propietats del compte d'usuari és l'establiment d'una unitat en xarxa personal per a cada usuari a la qual únicament ell té accés.



Per a configurar-la, basta crear una carpeta a la qual es tinga accés des de la xarxa. En aquest cas la crearem en el controlador de domini (en casos reals podríem situar-la en un dispositiu d'emmagatzematge com un NAS).

A continuació , es mostra les opcions de compartició i permisos NTFS del directori on s'emmagatzemaran les carpetes personals:

**Uso compartido avanzado**

Compartir esta carpeta

Configuración

Nombre del recurso compartido:  
carpetas\_personales\$

Establecer el límite de usuarios simultáneos en: 16777

Comentarios:

Permisos Caché Aceptar Cerrar

**Permisos de carpetas\_personales\$**

Nombres de grupos o usuarios:  
Usuarios del dominio (EMPRESA\Usuarios del dominio)

Agregar... Quitar

Permisos de Usuarios del dominio

	Permitir	Denegar
Control total	<input type="checkbox"/>	<input type="checkbox"/>
Cambiar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Leer	<input checked="" type="checkbox"/>	<input type="checkbox"/>

de control y permisos de acceso Cancelar Aplicar

**Propiedades: carpetas\_personales**

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: C:\carpetas\_personales

Nombres de grupos o usuarios:  
CREATOR OWNER  
SYSTEM  
Administradores (EMPRESA\Administradores)

Para cambiar los permisos, haga clic en Editar. Editar...

Permisos de Administradores Permitir Denegar

Control total	✓
Modificar	✓
Lectura y ejecución	✓
Mostrar el contenido de la carpeta	✓
Lectura	✓
Escrutura	✓

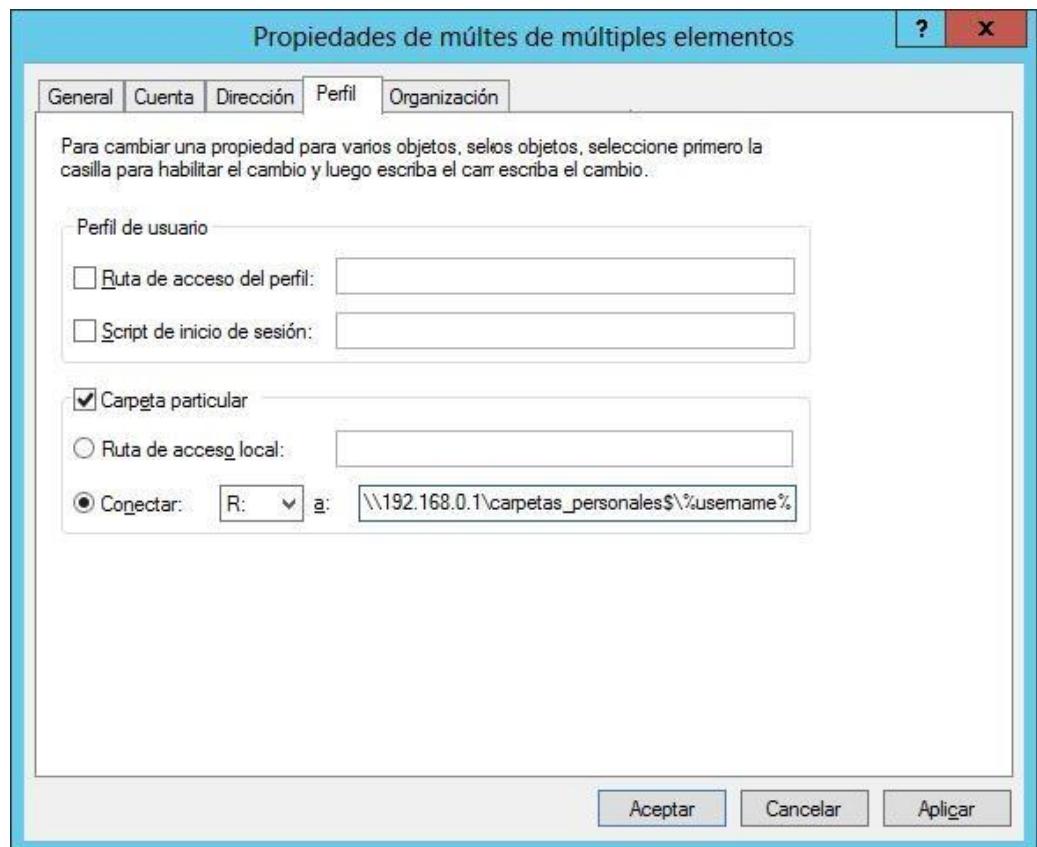
Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas en Opciones avanzadas.

Opciones avanzadas Obtener más información acerca de control y permisos de acceso

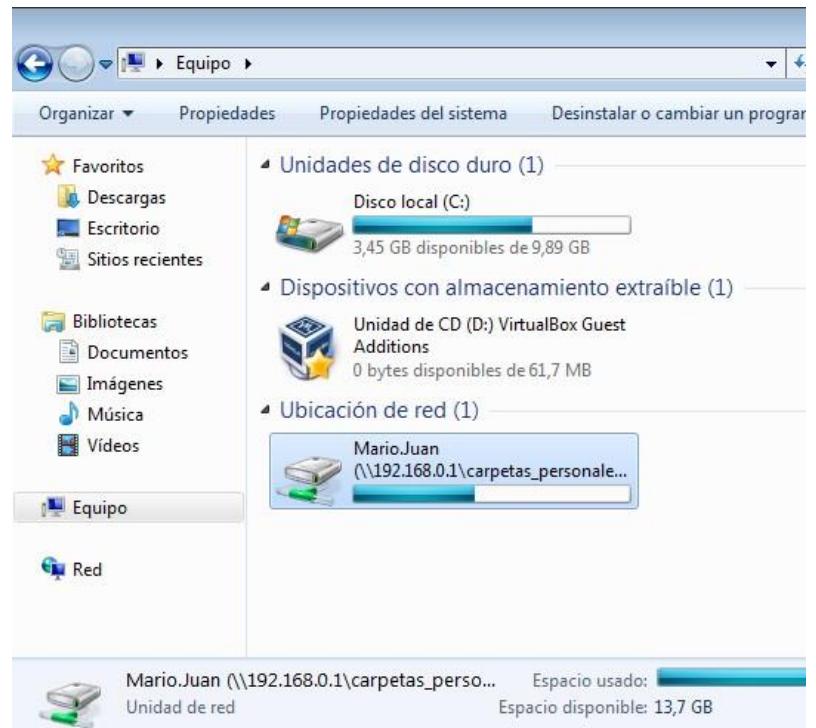
Aceptar Cancelar Aplicar

Compte! Recorda que per a que els usuaris no puguen veure les carpetes dels altres, has de llevar els permisos per al grup "Usuarios" (has de deshabilitar la herència)

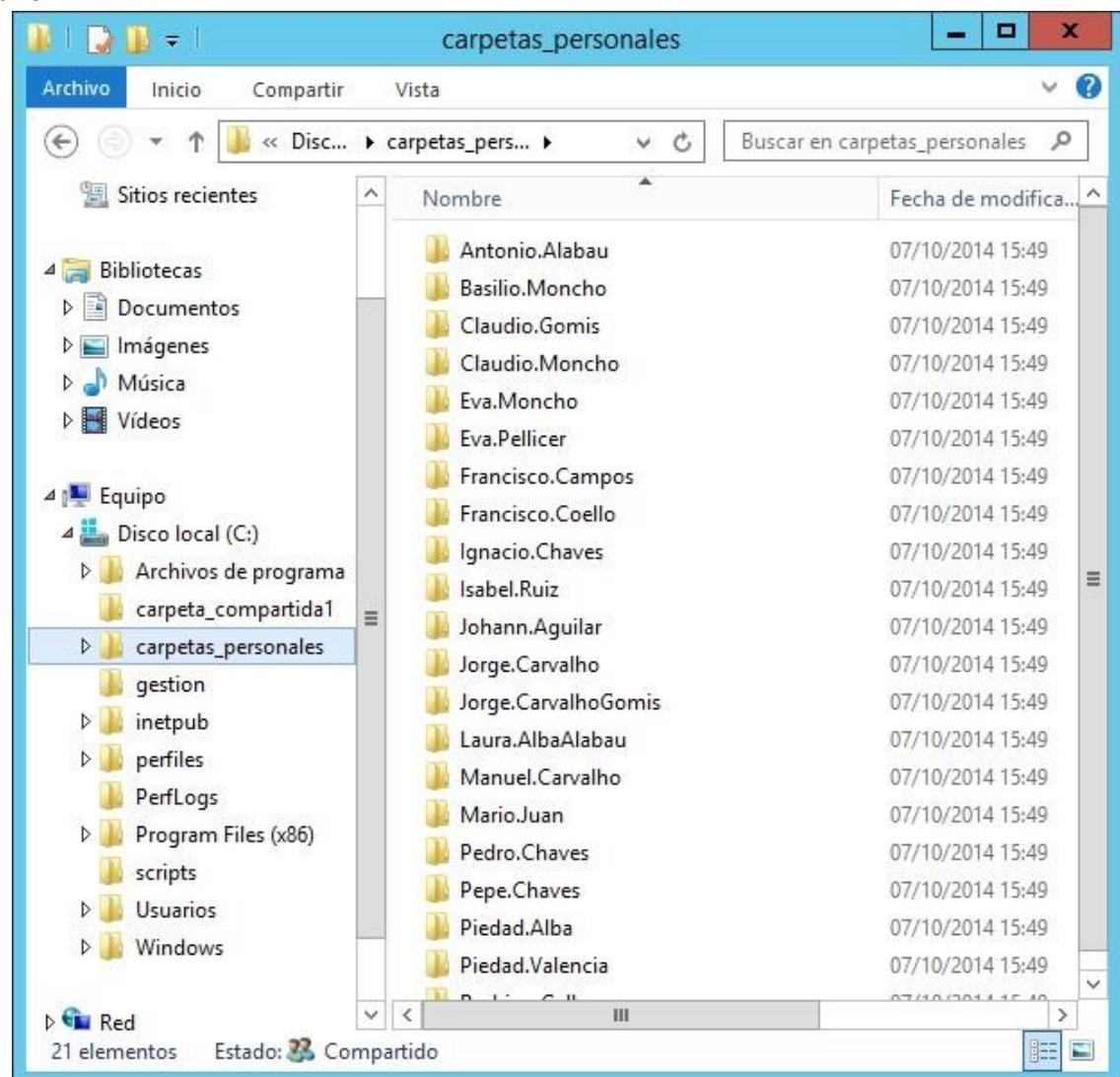
Per a no haver de afegir manualment la carpeta personal usuari per usuari utilitzarem de nou la variable %username% seleccionant a tots els usuaris i modificant la fitxa perfil.



D'aquesta manera es crearà automàticament en el controlador de domini una carpeta amb el nom de cada usuari a la qual únicament ell tindrà accés, i que tindrà disponible (en aquest cas) en la unitat R:

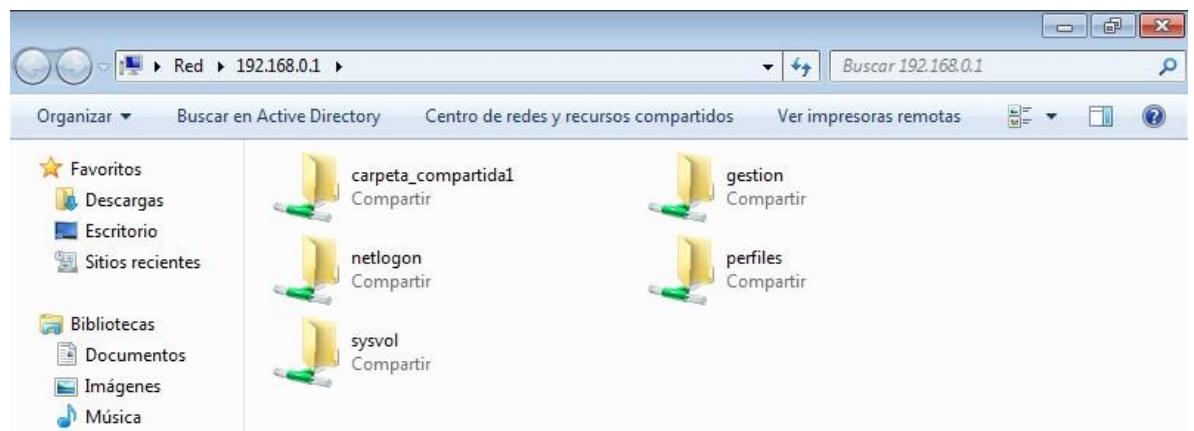


Si examinem el costat del servidor, veiem que s'han creat automàticament les carpetes de tots els usuaris.



La direcció de la unitat muntada és \\192.168.0.1\carpetes\_personals\$\%username%. En primer cal destacar que s'ha optat per posar l'adreça IP del controlador de domini en lloc del nom de l'equip perquè d'aquesta manera es redueix el trànsit en la xarxa que suposaria fer la consulta al servidor DNS.

D'altra banda , en crear la carpeta compartida se li ha assignat com a nom carpetes\_personals\$. El símbol \$ fa que les carpetes compartides es troben 'ocultes' en la xarxa, en definitiva, si no es busca pel seu nom, no apareixen en el llistat de recursos compartits accessibles via xarxa com es va veure anteriorment.



## 7. Bibliografia

- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curs Cefire Windows Server 2012.
- Somebooks.es (2014). Sistemes Operatius en Xarxa. Disponible en <http://somebooks.es/?p=4787>
- Wikipedia. Sistema Operatiu de xarxa. Disponible en [http://es.wikipedia.org/wiki/sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/sistema_operativo_de_red)
- Blog de SoporteTI. Disponible en: <http://blog.soporteti.net/>
- Elaboració pròpria