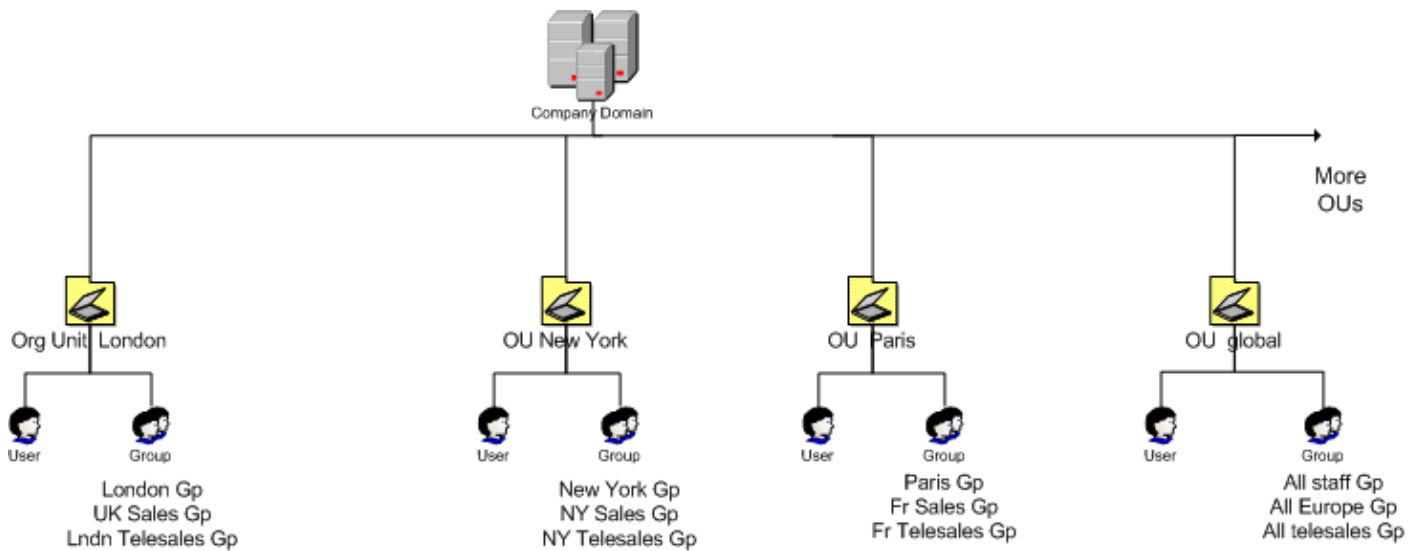


# Sistemas Informáticos

## Tema 12. Windows Server. Usuarios y grupos



# Índice

1. Objetivos .....	3
2. Usuarios.....	3
2.1. Cuentas de usuario predefinidas o integradas .....	3
2.2. Creación de usuarios en modo gráfico .....	4
2.3. Creación de usuarios desde la línea de comandos .....	6
2.4. Eliminación y deshabilitación de cuentas de usuario .....	9
2.5. Configuración de la cuenta de usuario.....	11
2.6. Configuración de inicio de sesión .....	11
3. Grupos en Active Directory .....	13
3.1. Grupos Predefinidos o integrados .....	14
3.2. Creación de grupos mediante la interfaz gráfica .....	15
3.3. Creación de grupos mediante la línea de comandos.....	18
3.4. Eliminación de grupos.....	18
4. Unidades Organizativas .....	19
4.1. Creación de UO .....	19
4.2. Eliminación de UO .....	20
5. Caso Práctico: Creación de la estructura de una organización mediante la línea de comandos .....	22
5.1. Creación de los grupos .....	23
5.2. Creación de las unidades organizativas .....	24
5.3. Creación de usuarios .....	25
6. Consultas sobre objetos del dominio: dsquery .....	29
7. Bibliografía .....	30

## 1. Objetivos

- Crear y configurar usuarios tanto por la interfaz gráfica como por línea de comandos.
- Crear y configurar grupos tanto por la interfaz gráfica como por línea de comandos.
- Crear y administrar Unidades Organizativas.

## 2. Usuarios

Una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:

- Permite **autenticar la identidad de un usuario**, porque sólo podrán iniciar una sesión aquellos usuarios que dispongan de una cuenta en el sistema asociada a una determinada contraseña.
- Permite **autorizar, o denegar, el acceso a los recursos del dominio**, porque, una vez que el usuario haya iniciado su sesión sólo tendrá acceso a los recursos para los que haya recibido los permisos correspondientes.

Cuando creamos una cuenta de usuario nueva, se le asigna un **Identificador de Seguridad (SID, Security IDentifier)** que es único en el dominio. De hecho, el único valor imprescindible para que la cuenta mantenga su identidad es su SID (todos los demás datos o configuraciones de la cuenta los podemos modificar sin problemas). De esta forma, aunque eliminemos una cuenta y volvamos a crear otra con el mismo nombre, ésta será diferente, porque su SID también lo es, lo que significa que no coincidirán ni sus certificados de seguridad, ni sus permisos ni su pertenencia a determinados grupos.

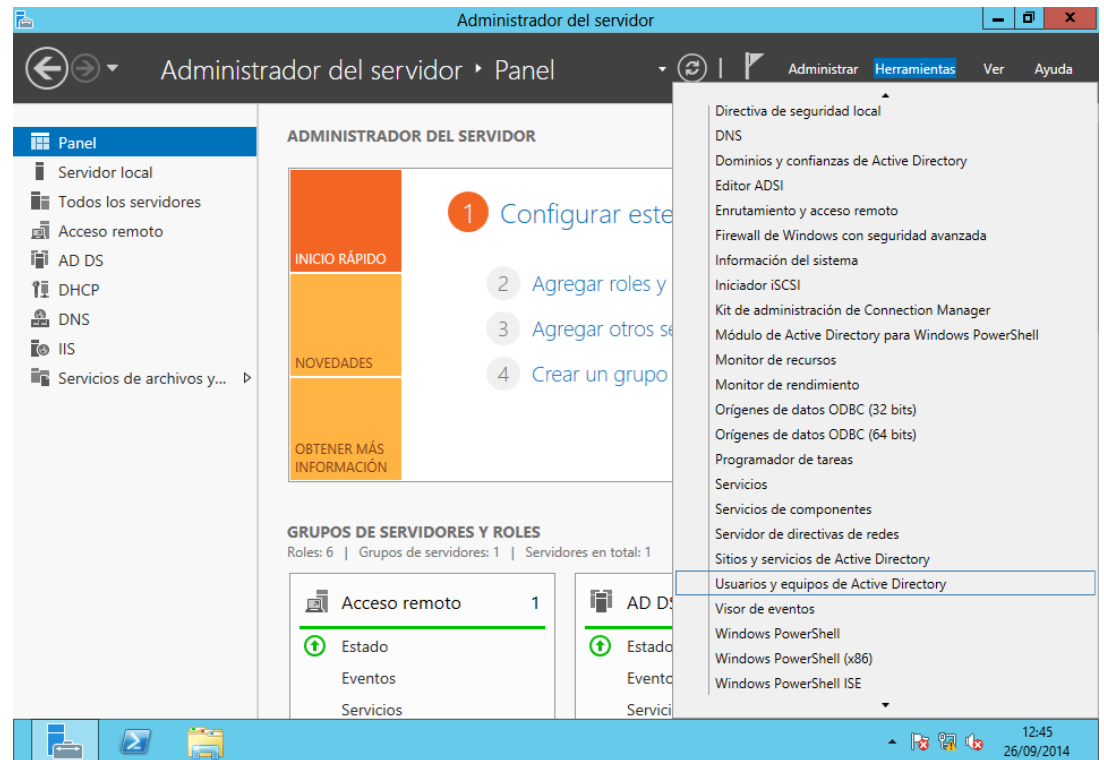
### 2.1. Cuentas de usuario predefinidas o integradas

Cuando se crea el dominio, se crean también dos nuevas cuentas: Administrador e Invitado:

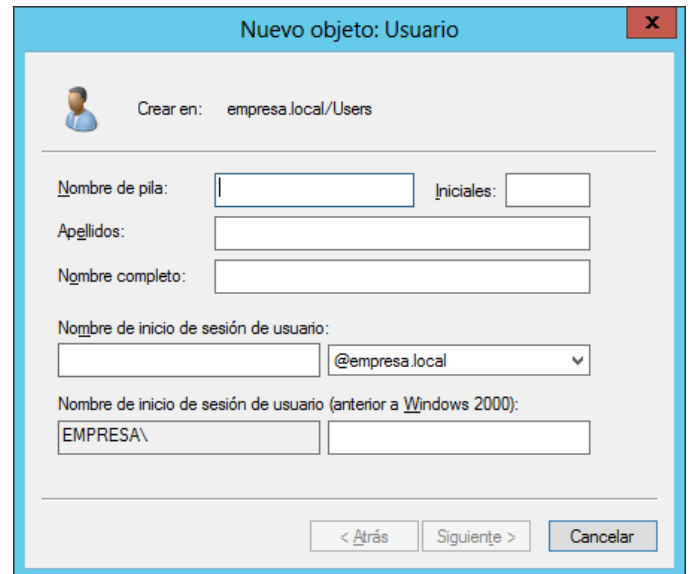
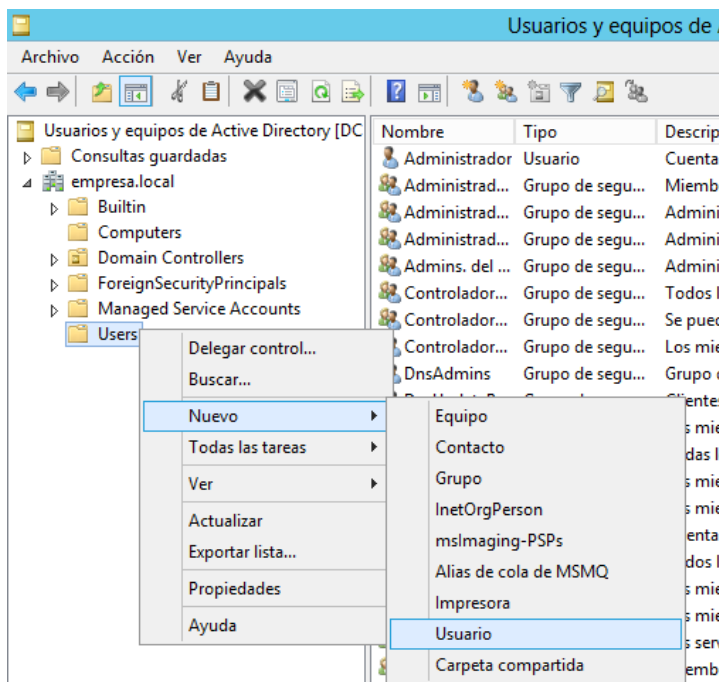
- Administrador: Tiene control total sobre el dominio y no se podrá eliminar ni retirar del grupo Administradores (aunque sí podemos cambiarle el nombre o deshabilitarla).
- Invitado: Está deshabilitada de forma predeterminada y, aunque no se recomienda, puede habilitarse, por ejemplo, para permitir el acceso a los usuarios que aún no tienen cuenta en el sistema o que la tienen deshabilitada. De forma predeterminada no requiere contraseña, aunque esta característica, como cualquier otra, puede ser modificada por el administrador.

## 2.2. Creación de usuarios en modo gráfico

Los usuarios del dominio deben tener una cuenta para poder acceder a los recursos del mismo tras su autenticación frente al controlador de dominio. Para crear una cuenta de usuario mediante la interfaz gráfica accederemos a la herramienta 'Usuarios y equipos de Active Directory' desde 'Herramientas del Administrador del servidor'.



Una vez abierto el administrador de



'Usuarios y equipos de Active Directory', se hace clic con el botón derecho sobre 'Users' y en el menú que aparece, se selecciona 'Nuevo' y a continuación 'Usuario'.

Como normas generales al crear un nombre de usuario hay que observar que:

- Las cuentas de usuario deben ser únicas.
- Los nombres de inicio de sesión se pueden formar con una combinación de letras, mayúsculas o minúsculas, y caracteres alfanuméricos. No se aceptan los caracteres: / \ | [ ] : ; = < > + \* " @ ?
- La cuenta de usuario puede tener hasta 20 caracteres.

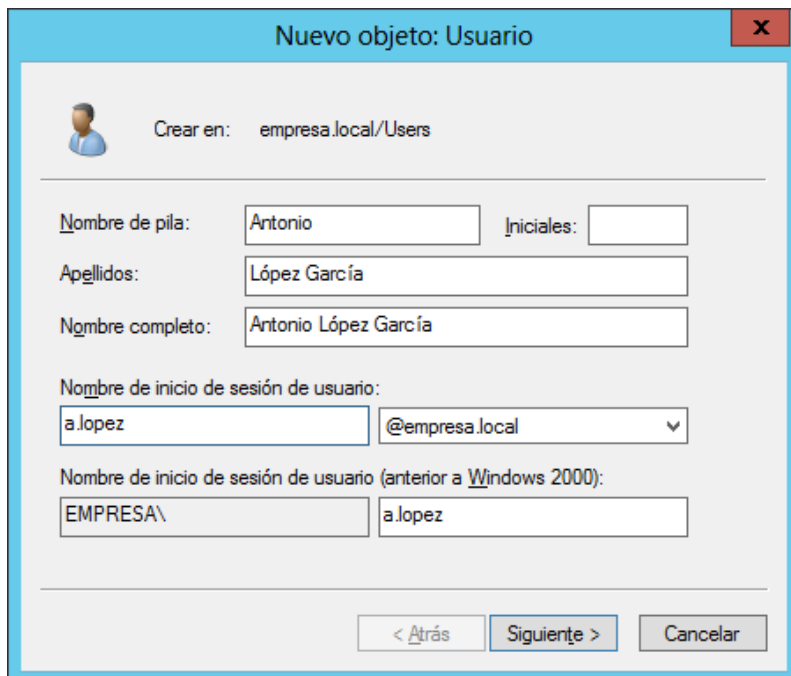
En el cuadro de diálogo de creación de un nuevo usuario se puede introducir el nombre, la(s) inicial(es) del segundo nombre y los apellidos del usuario. Hasta aquí toda esta información es meramente informativa, podría haber, por ejemplo, dos usuarios cuyo nombre completo fuera "Antonio López García".

En el cuadro de texto 'Nombre de inicio de sesión de usuario' se introduce el nombre de usuario siguiendo la estructura que haya predefinido el administrador del sistema (como se ha indicado anteriormente, este nombre **debe** ser único en todo el dominio).

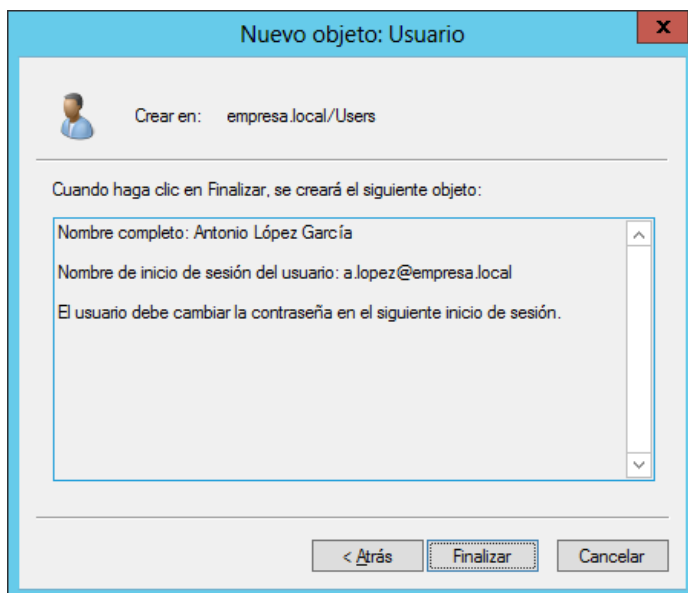
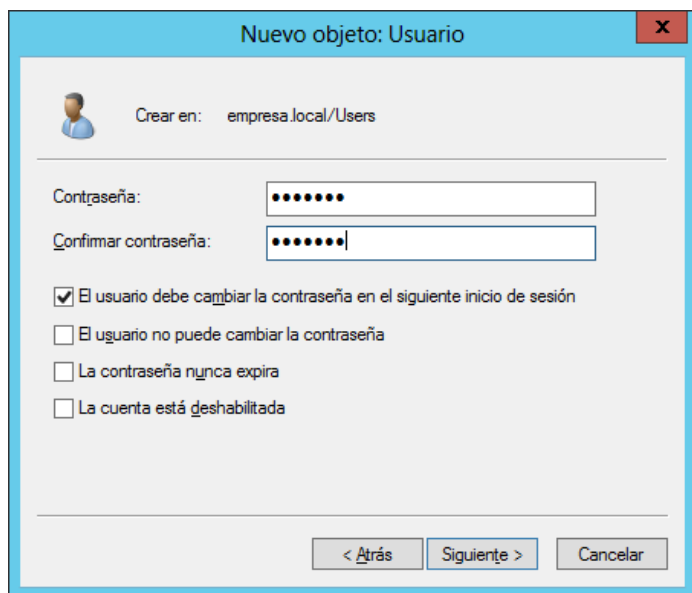
Algunos ejemplos de criterios para la creación del nombre de usuario podrían ser los siguientes:

- Dos primeras letras del nombre y apellidos. El nombre de inicio de sesión del usuario Antonio López García sería: anloga.
- Inicial del primer nombre y primer apellido completo. El nombre de inicio de sesión del ejemplo anterior sería: alopez.
- Diferentes caracteres para separar la inicial del primer nombre y el apellido completo: a.lopez, a-lopez, etc.
- Primer nombre completo y primer apellido completo separados por un punto: antonio.lopez.

Adoptando el tercero de los criterios anteriores obtendríamos algo como lo que se muestra en la imagen.



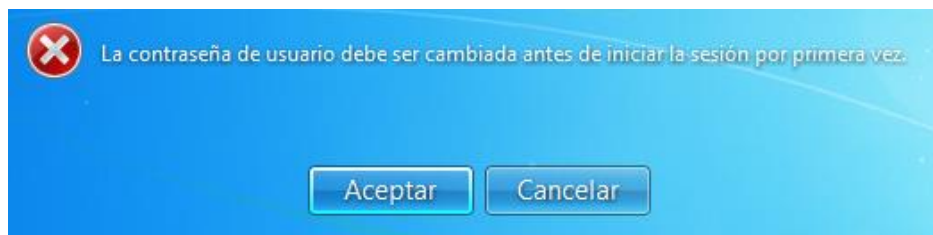
A continuación se solicitará que se introduzca la contraseña del usuario. Esta debe cumplir con los criterios de complejidad establecidos. Además aparecen una serie de opciones para configurar las propiedades de la contraseña:



En la imagen aparecen cuatro opciones para la contraseña:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca expira.
- La cuenta está deshabilitada.

La primera de las opciones es útil para que el administrador cree el nuevo usuario con una contraseña convencional. El usuario cuando se autentifique por primera vez en el sistema entrará con la contraseña que le ha proporcionado el administrador, pero automáticamente, el sistema le indicará que debe ser cambiada. De esta manera, el administrador ya no conocerá la contraseña del usuario, garantizándose la privacidad de esta.



El segundo de los casos ('El usuario no puede cambiar la contraseña') está pensado para crear usuarios genéricos, supongamos que creamos una cuenta de usuario para utilizar un ordenador conectado a un escáner, y queremos que los usuarios que deseen utilizar ese escáner, siempre entren con la misma cuenta al equipo asociado al escáner. Podríamos pensar en utilizar un usuario genérico del tipo:

- login: escaner
- pass: escaner

En un caso así, no querríamos que accidentalmente, o como acto de vandalismo, la contraseña fuera cambiada, invalidando cualquier posible acceso de otras personas a esa cuenta.

La inhabilitación del tercer caso ('La contraseña nunca expira'), tiene por objetivo evitar que el sistema pida al usuario que cambie la contraseña periódicamente. Resulta interesante mantener esta opción, aunque pueda resultar incómodo cambiar la contraseña cada, por ejemplo, seis meses. De esta manera estamos protegiéndonos de posibles accesos indebidos por parte de alguien que haya averiguado la contraseña de alguna manera.

Finalmente, la cuarta opción ('La cuenta está deshabilitada') sirve para bloquear usuarios que no queremos que tengan acceso al sistema, pero tampoco queremos eliminarlos, ya que se invalidarían los permisos referidos a este usuario. También puede servir para crear usuarios que no queremos que estén operativos hasta un momento determinado.

## 2.3. Creación de usuarios desde la línea de comandos

### 2.3.1. Opción 1: net user

Existen varias posibilidades para crear cuentas de usuario del dominio. La opción más sencilla, pero solamente válida en entornos en los que haya un único dominio, sería la siguiente:

```
>>net user a.lopez contraseña /add
```

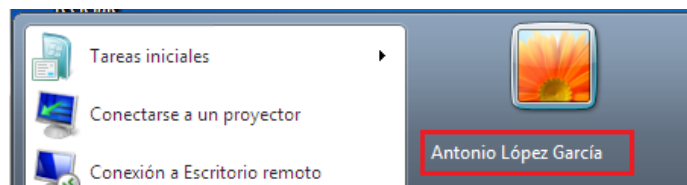
De esta manera creamos una cuenta de usuario del dominio con los mínimos atributos posibles: nombre de usuario y contraseña.

Fijémonos con un poco más de detalle en la sintaxis. El comando utilizado es `net user`, a continuación indicamos el nombre de usuario, luego la contraseña, y finalmente introducimos `/add` que sirve para crear la cuenta. Si no indicáramos nada, estaríamos modificando una cuenta existente, y si indicamos `/del` (sin la contraseña) estaremos borrando la cuenta.

Para hacerlo de una manera más completa, podemos incluir también en la cuenta de usuario el nombre completo del mismo con el modificador `/fullname:`

```
>>net user a.lopez contraseña /fullname:"Antonio López García" /add
```

Así cuando el usuario se identifique en el sistema, no aparecerá como a.lopez sino que aparecerá el nombre completo: Antonio López García.



Además podemos implementar una política de seguridad/privacidad que consiste en que el usuario tenga permiso para cambiar la contraseña, de manera que él sea el único conocedor de la misma, ya que el administrador, le habrá asignado una contraseña, digamos, inicial. Para ello utilizamos el modificador `/passwordchg`, que habilita al usuario para modificar o no la contraseña:

```
>>net user a.lopez contraseña /fullname:"Antonio López García" /passwordchg:yes /add
```

Si queremos que el usuario no sucumba a la tentación de quitar la contraseña para que el acceso sea más sencillo (y más peligroso), podemos añadir otra opción más al comando para crear la cuenta de usuario: `/passwordreq`. Si el valor de este modificador es `yes`, siempre deberá haber contraseña, si el valor es `no`, podrá no haber contraseña.

```
>>net user a.lopez contraseña /fullname:"Antonio López García" /passwordchg:yes /passwordreq:yes /add
```

Finalmente, añadir una reseña respecto a la longitud de las contraseñas. Mediante el comando `net accounts /minpwlen` podemos imponer un límite inferior a la longitud de la contraseña de las cuentas de usuario del dominio. Por ejemplo:

```
>>net accounts /minpwlen:8
```

hará que no sean válidas las contraseñas de menos de 8 caracteres.

### 2.3.2. Opción 2: dsadd user

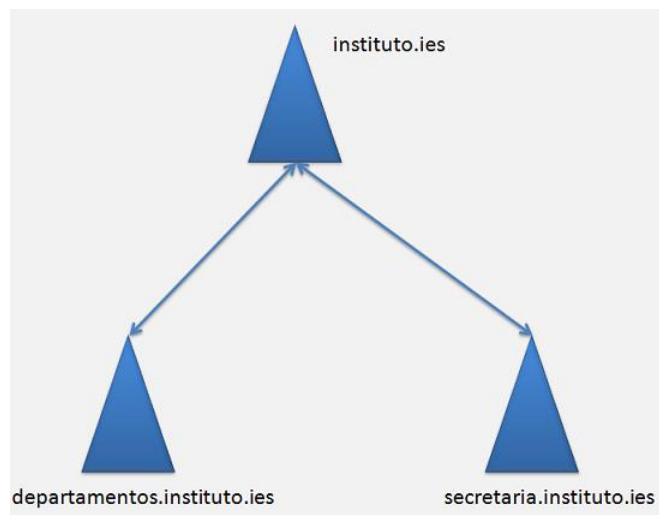
La opción **más correcta** para crear usuarios del dominio es mediante el comando `dsadd user`. Este comando nos va a permitir definir la ubicación en la que se creará el usuario en lo referente a:

- Dominio o subdominio.
- Unidad Organizativa.

Supongamos que tenemos una estructura de red con varios dominios un dominio raíz y varios subdominios), como la que se muestra en la imagen.

Si desde el controlador del dominio `instituto.ies` quisiéramos crear un usuario en el dominio `departamentos.instituto.ies` el comando `net user` no nos serviría, ya que crearía el usuario en el dominio raíz.

Para crear desde el controlador del dominio raíz, el usuario `jgomez` del dominio `departamentos.instituto.ies` deberíamos ejecutar el siguiente comando:



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

La salida de la ejecución del comando sería:

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

Comprobemos que efectivamente se ha creado el usuario jgomez en el subdominio.

Usuarios y equipos de Active Direct		Nombre	Tipo	Descripción
+ Consultas guardadas		Administrador	Usuario	Cuenta integrada para la ...
+ departamentos.instituto.ies		Admins. del d...	Grupo de seguri...	Administradores designad...
+ Builtin		Controladore...	Grupo de seguri...	Todos los controladores d...
+ Computers		Controladore...	Grupo de seguri...	Los miembros de este gru...
+ Domain Controllers		DnsAdmins	Grupo de seguri...	Grupo de administradores ...
+ ForeignSecurityPrincipals		DnsUpdatePr...	Grupo de seguri...	Clientes DNS que tienen p...
+ Managed Service Accounts		Equipos del d...	Grupo de seguri...	Todas los servidores y est...
+ Users		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...
		jgomez	Usuario	
		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...

Es importante que los distintos controladores de dominio estén sincronizados, ya que en caso contrario la creación de los usuarios dará error.



Podríamos utilizar un comando algo más complejo para configurar más detalladamente la cuenta de un nuevo usuario:

```
>>dsadd user "CN=rperez, CN=Users, DC=departamentos, DC=instituto, DC=ies" -pwd Hol@hola -disabled no -ln "Pérez García" -fn Roberto -mustchpwd yes -canchpwd yes -memberof "CN=Alumnos, CN=Users, DC=departamentos, DC=instituto, DC=ies"
```

Algunas de las opciones utilizadas son:

- -ln: apellidos del usuario.
- -fn: nombre del usuario.
- -mustchpwd: obligación de cambiar la contraseña en el primer inicio de sesión.
- -canchpwd: el usuario puede cambiar la contraseña.
- -memberof: grupo del que es miembro el usuario.

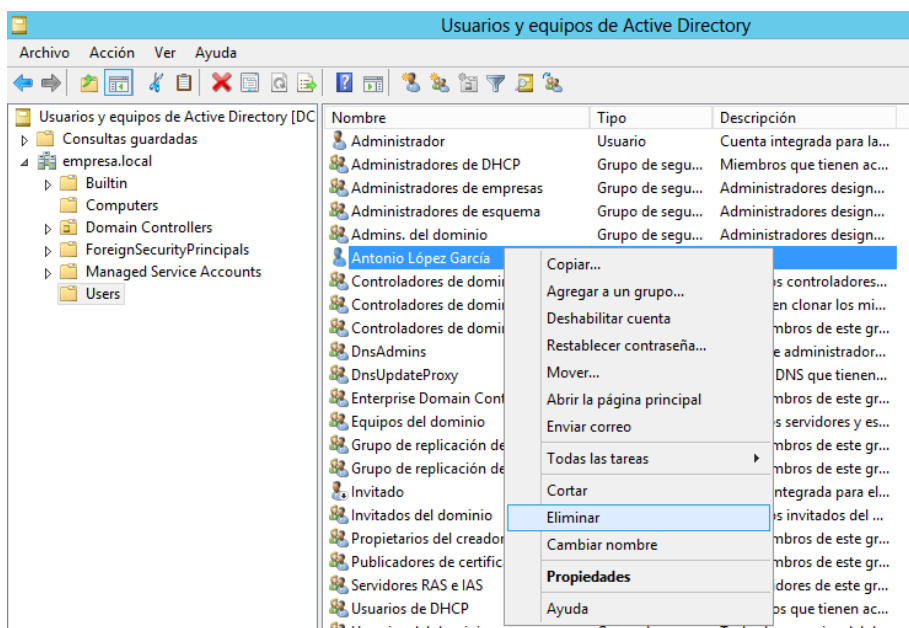
En los siguientes enlaces se muestran un par de referencias acerca de las distintas opciones que posee el comando dsadd.

- [Technet](#)
- [Blog redesw2003](#)

## 2.4. Eliminación y deshabilitación de cuentas de usuario

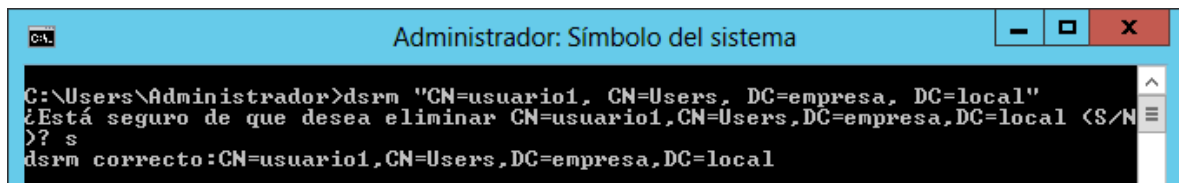
Como hemos comentado anteriormente, cada cuenta de usuario creada en un dominio tiene un **identificador de seguridad (SID)** único. Si eliminamos una cuenta de usuario y después volvemos a crearla exactamente igual, el identificador SID será diferente. Esto se traduce en que *no se podrán recuperar los permisos y privilegios de la cuenta eliminada*.

Si finalmente decidimos eliminar la cuenta, accederemos a 'Usuarios y equipos de Active Directory', seleccionaremos el usuario a eliminar, haremos clic con el botón derecho y luego 'Eliminar'.



Para eliminar una cuenta de usuario mediante la línea de comandos utilizaremos el comando dsrm. En el ejemplo siguiente eliminaríamos la cuenta del usuario usuario1 del dominio empresa.local.

```
>>dsrm "CN=usuario1, CN=Users, DC=empresa, DC=local"
```

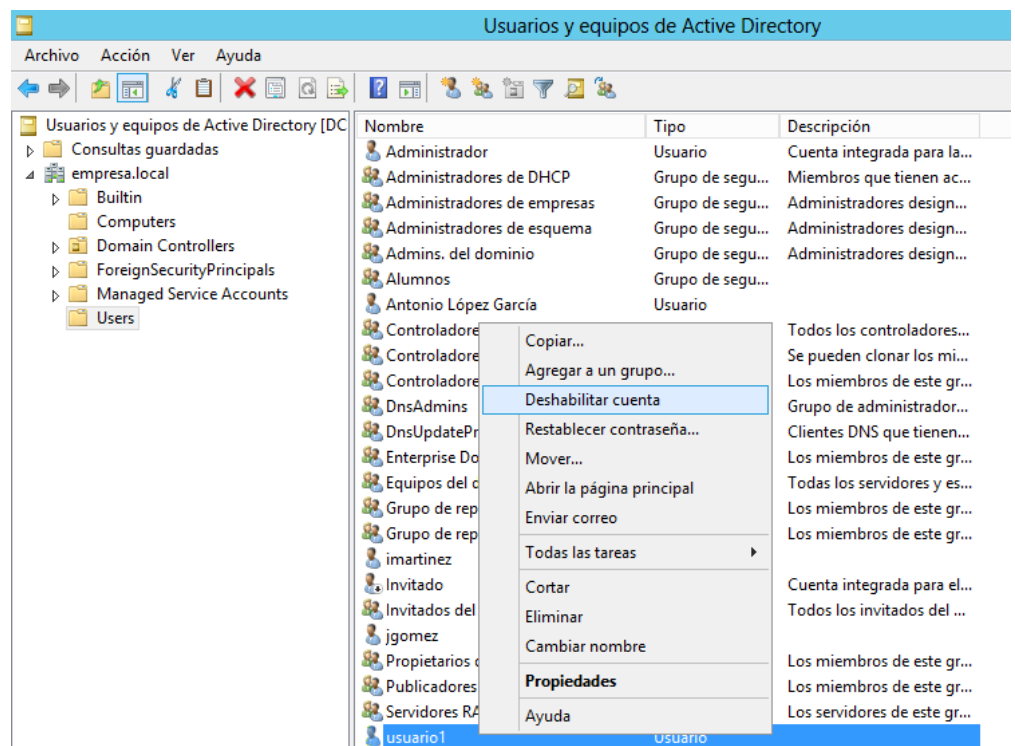


Para evitar posibles problemas con la eliminación de cuentas, el cual es un proceso definitivo, se suele optar por la **deshabilitación de cuentas**.

Supongamos una empresa en la que un trabajador va a cesar su actividad. El administrador de sistemas deshabilitará su cuenta en la fecha en la que el trabajador vaya a dejar de prestar sus servicios. De esta manera el trabajador cesado ya no podrá iniciar sesión en el dominio, pero si pasado un tiempo hiciera falta volver a iniciar sesión, bastaría con habilitar de nuevo la cuenta.

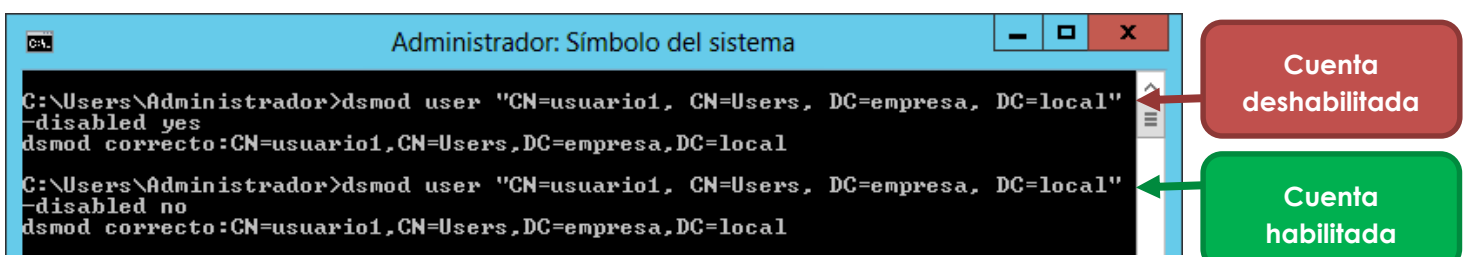
Otro ejemplo real podría ser una universidad, en la que cada alumno tiene una cuenta de usuario. Cuando finaliza sus estudios, la cuenta es deshabilitada, pero si posteriormente cursa otros estudios, la cuenta volvería a habilitarse.

Como antes, accederemos a 'Usuarios y equipos de Active Directory' y haciendo clic con el botón secundario sobre el usuario a bloquear, seleccionaremos la opción 'Deshabilitar la cuenta'.



Para deshabilitar una cuenta de usuario mediante la línea de comandos utilizaremos el comando `dsmod` con el modificador `-disabled` con valor `yes`:

```
>>dsmod user "CN=usuario1, CN=Users, DC=empresa, DC=local" -disabled yes
```



## 2.5. Configuración de la cuenta de usuario

Las cuentas de usuarios creadas en el dominio se pueden configurar de una manera detallada en la ventana 'Propiedades de la cuenta', para ello se hace clic con el botón derecho del ratón sobre la cuenta de usuario que se desea editar.

Las propiedades de la cuenta de usuario que más utilizaremos durante este curso serán:

- **General:** Se puede modificar el Nombre, Apellido, etc. y además modificar información administrativa como la descripción, oficina, teléfono, email y página web.
- **Cuenta:** Se puede configurar algunas características de la contraseña de usuario, las horas de inicio de sesión, la caducidad de la cuenta, **desbloquear** la cuenta, etc.
- **Perfil:** En esta ficha se pueden editar aspectos importantes como son la ubicación física del perfil del usuario y el fichero de comandos de inicio de sesión.
- **Miembro de:** Se muestra el listado de grupos a los que el usuario pertenece.

The screenshot shows the 'Propiedades: Antonio López García' window with the 'General' tab selected. The window has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with tabs: 'Marcado', 'Entorno', 'Sesiones', 'Control remoto', 'Perfil de Servicios de Escritorio remoto', and 'COM+'. The 'General' tab is active, showing fields for 'Nombre de pila' (Antonio), 'Apellidos' (López García), 'Nombre para mostrar' (Antonio López García), 'Descripción', 'Oficina', 'Número de teléfono', 'Correo electrónico', and 'Página web'. There are also buttons for 'Otros...' next to the phone and email fields. At the bottom are buttons for 'Aceptar', 'Cancelar', 'Aplicar', and 'Ayuda'.

## 2.6. Configuración de inicio de sesión

Windows Server 2019 permite configurar los horarios en los que se puede iniciar sesión. Esta funcionalidad puede ser útil para controlar accesos al sistema a horas 'anómalas', o para evitar que usuarios de, por ejemplo, el turno de tarde, puedan acceder al sistema con la cuenta de un usuario del turno de mañana.

Para establecer los horarios en los que se puede iniciar sesión se seguirán los siguientes pasos.

- En 'Usuarios y Equipos de Active Directory' se selecciona el usuario buscado, y haciendo clic con el botón derecho se accede a 'Propiedades'.
- Se abre el cuadro de diálogo 'Propiedades' de la cuenta seleccionada. Se hace clic en la ficha 'Cuenta' y después se hace clic en el botón 'Horas de inicio de sesión'.

The screenshot shows the 'Propiedades: Antonio López García' window with the 'Cuenta' tab selected. The window has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with tabs: 'Marcado', 'Entorno', 'Sesiones', 'Control remoto', 'Perfil de Servicios de Escritorio remoto', and 'COM+'. The 'Cuenta' tab is active, showing fields for 'Nombre de inicio de sesión de usuario' (a.lopez) and 'Nombre de inicio de sesión de usuario (anterior a Windows 2000):' (EMPRESA\). There are buttons for 'Horas de inicio de sesión...' and 'Iniciar sesión en...'. Below these are checkboxes for 'Desbloquear cuenta' and 'Opciones de cuenta'. The 'Opciones de cuenta' section has checkboxes for 'El usuario debe cambiar la contraseña en el siguiente inicio de sesión', 'El usuario no puede cambiar la contraseña', 'La contraseña nunca expira', and 'Almacenar contraseña utilizando cifrado reversible'. At the bottom are buttons for 'Aceptar', 'Cancelar', 'Aplicar', and 'Ayuda'.

En color azul se muestran las horas de inicio permitidas. Para denegar el acceso basta con seleccionar las horas a las que se desea limitar el acceso y se marca la opción 'Inicio de sesión denegado'.

### Horas de inicio de sesión para Antonio López García

0 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 0

Todo	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
lunes																								
martes																								
miércoles																								
jueves																								
viernes																								
sábado																								
domingo																								

○ Inicio de sesión permitido

● Inicio de sesión denegado

De sábado a domingo de 0:00 a 0:00 horas

A todo esto hay que añadir que se puede configurar el inicio de sesión en determinados equipos. Para ello basta con hacer clic en el botón 'Iniciar sesión en...'. Se puede seleccionar si el usuario puede iniciar sesión en 'Todos los equipos' o solo en algunos equipos determinados.

### Estaciones de trabajo de inicio de sesión

?
X

En Nombre de equipo, escriba el nombre NetBIOS o DNS (Sistema de nombres de dominio) del equipo.

Este usuario puede iniciar sesión en:

☐ Todos los equipos

☒ Los siguientes equipos

Nombre de equipo:

win7

### 3. Grupos en Active Directory

Los grupos son un tipo de contenedor que permiten definir conjuntos de usuarios y definir permisos basándonos en esa pertenencia al grupo, en lugar de hacerlo de modo individual, usuario por usuario. Eso no sólo facilita la administración del dominio sino que también permite trabajar de un modo menos propenso a errores. Como pauta general, la agrupación de objetos suele facilitar las tareas de administración reduciendo las posibilidades de error.

Existen dos grandes tipos de grupos en el Directorio Activo de Windows:

- **Grupos de seguridad:** este tipo de grupos permite definir permisos para recursos del dominio. Son los utilizados en las listas de control de accesos (ACLs) que se estudiarán más adelante. Este tipo de grupos son los que se utilizarán en la administración de la red.
- **Grupos de distribución:** no poseen características de seguridad, únicamente son un listado de usuarios para mensajería.

Dentro de los grupos de seguridad existen a su vez tres ámbitos:

- **Grupo Universal:** es un grupo cuyos permisos se extienden a diversos dominios. Además este tipo de grupos puede estar formado por usuarios o grupos de usuarios de diferentes dominios.
- **Grupo Global:** es muy similar a los grupos universales, es decir pueden permitir el acceso a recursos de cualquiera de los dominios del árbol del Directorio Activo, pero con la salvedad de que todos los miembros del grupo deben pertenecer **al mismo dominio**.
- **Grupo Local del Dominio:** es un grupo creado en un dominio con miembros que pueden provenir de otros dominios y que únicamente puede tener acceso a recursos dentro de su dominio.

#### ¿En qué casos utilizar un ámbito u otro de grupo?

Los grupos universales suelen tener su utilidad en grandes empresas en las que se ha definido un bosque de dominios asignando dominios a cada uno de sus departamentos o divisiones. En este tipo de estructuras, cuando se realiza una modificación en el grupo, esta debe replicarse en todos los controladores de domino que estén configurados como catálogo global.

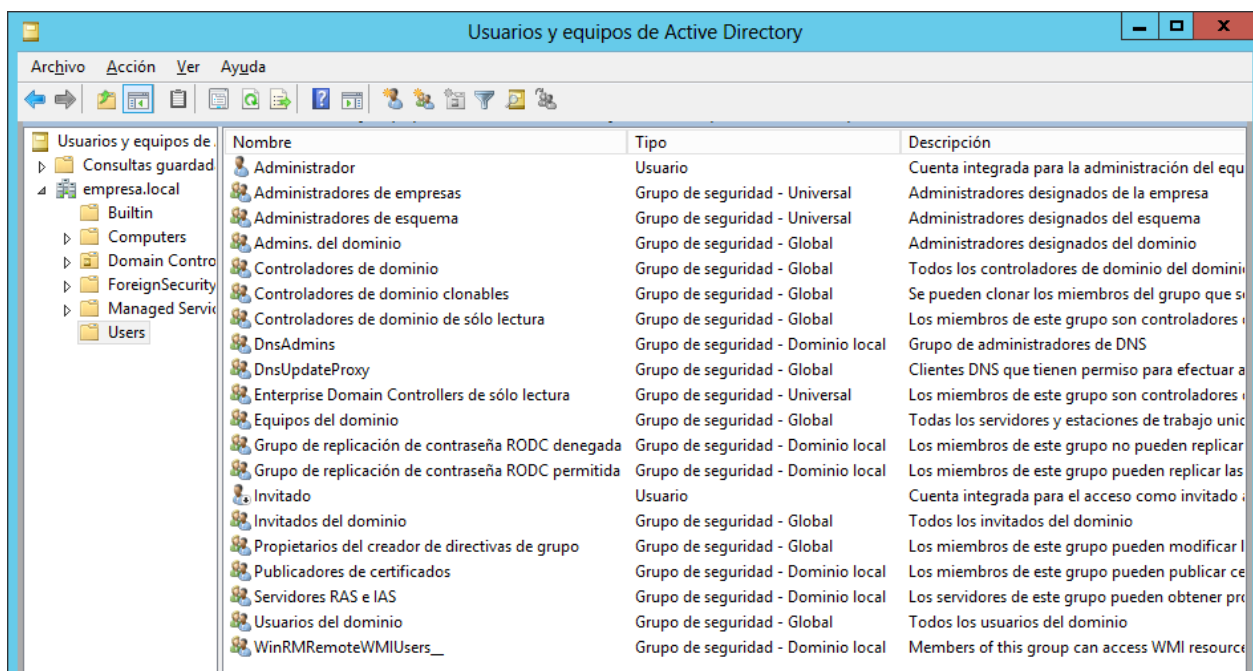
En redes de dominio único se pueden aplicar grupos globales que tendrán mayor sentido cuando se defina un segundo dominio, lo que puede ocurrir en el momento en el que haya una ampliación de la organización.

Como pautas generales para la administración de redes tendremos en cuenta las siguientes consideraciones:

1. No se debe asignar un ámbito más amplio del necesario.
2. Los grupos locales de dominio no se pueden procesar en otros dominios.
3. Un grupo global no se replica fuera del dominio ya que no forma parte del plan de replicación del catálogo global.
4. Los grupos universales se replican por toda la red generando tráfico que puede tener una cierta incidencia en el rendimiento de esta (aunque este aspecto se ha optimizado en Windows Server 2008 y posteriores frente a ediciones anteriores).
5. Si un grupo universal está compuesto por grupos globales y se producen cambios dentro de los grupos globales, no se produce un cambio en el catálogo global, y por tanto esa modificación no conlleva una replicación en todos los controladores de domino del bosque.

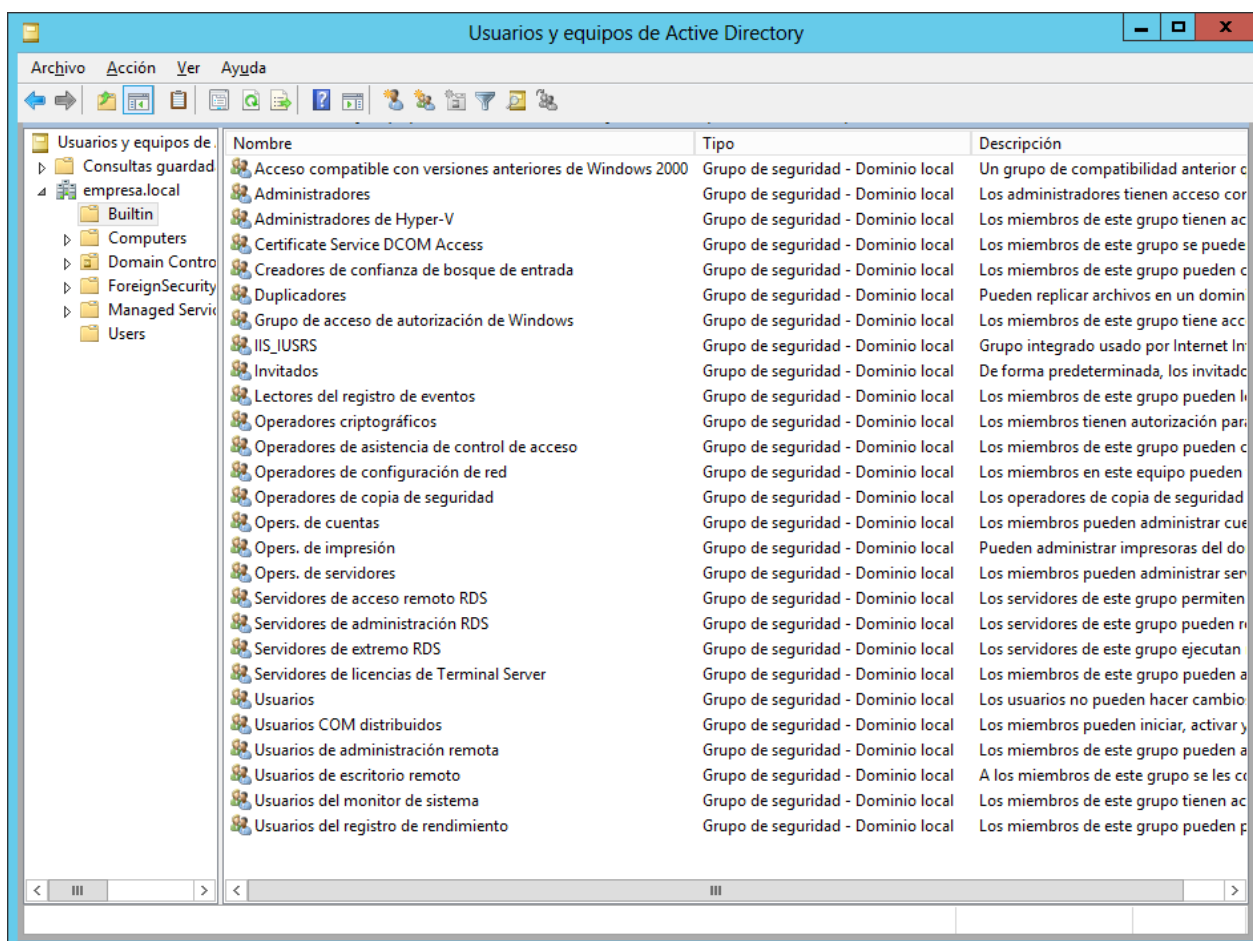
### 3.1. Grupos Predefinidos o integrados

Al instalar el Directorio Activo podemos comprobar que se han generado automáticamente una serie de grupos predefinidos con unos permisos acorde a sus funciones asignadas.



Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la administración del equ
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 s
Controladores de dominio de sólo lectura	Grupo de seguridad - Global	Los miembros de este grupo son controladores
DnsAdmins	Grupo de seguridad - Dominio local	Grupo de administradores de DNS
DnsUpdateProxy	Grupo de seguridad - Global	Cientes DNS que tienen permiso para efectuar a
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de este grupo son controladores
Equipos del dominio	Grupo de seguridad - Global	Todas los servidores y estaciones de trabajo unio
Grupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local	Los miembros de este grupo no pueden replicar
Grupo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden replicar las
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 l
Publicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden publicar ce
Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden obtener pro
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 resource

Usuarios y grupos creados automáticamente al instalar el Directorio Activo.



Nombre	Tipo	Descripción
Acceso compatible con versiones anteriores de Windows 2000	Grupo de seguridad - Dominio local	Un grupo de compatibilidad anterior c
Administradores	Grupo de seguridad - Dominio local	Los administradores tienen acceso cor
Administradores de Hyper-V	Grupo de seguridad - Dominio local	Los miembros de este grupo tienen ac
Certificate Service DCOM Access	Grupo de seguridad - Dominio local	Los miembros de este grupo se puede
Creadores de confianza de bosque de entrada	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden c
Duplicadores	Grupo de seguridad - Dominio local	Pueden replicar archivos en un domin
Grupo de acceso de autorización de Windows	Grupo de seguridad - Dominio local	Los miembros de este grupo tiene acc
IIS_IUSRS	Grupo de seguridad - Dominio local	Grupo integrado usado por Internet In
Invitados	Grupo de seguridad - Dominio local	De forma predeterminada, los invitado
Lectores del registro de eventos	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden l
Operadores criptográficos	Grupo de seguridad - Dominio local	Los miembros tienen autorización par
Operadores de asistencia de control de acceso	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden c
Operadores de configuración de red	Grupo de seguridad - Dominio local	Los miembros en este equipo pueden
Operadores de copia de seguridad	Grupo de seguridad - Dominio local	Los operadores de copia de seguridad
Opsrs. de cuentas	Grupo de seguridad - Dominio local	Los miembros pueden administrar cue
Opsrs. de impresión	Grupo de seguridad - Dominio local	Pueden administrar impresoras del do
Opsrs. de servidores	Grupo de seguridad - Dominio local	Los miembros pueden administrar ser
Servidores de acceso remoto RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo permiten
Servidores de administración RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden n
Servidores de extremo RDS	Grupo de seguridad - Dominio local	Los servidores de este grupo ejecutan
Servidores de licencias de Terminal Server	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden a
Usuarios	Grupo de seguridad - Dominio local	Los usuarios no pueden hacer cambio
Usuarios COM distribuidos	Grupo de seguridad - Dominio local	Los miembros pueden iniciar, activar y
Usuarios de administración remota	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden a
Usuarios de escritorio remoto	Grupo de seguridad - Dominio local	A los miembros de este grupo se les co
Usuarios del monitor de sistema	Grupo de seguridad - Dominio local	Los miembros de este grupo tienen ac
Usuarios del registro de rendimiento	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden p

Grupos integrados denominados Builtin.



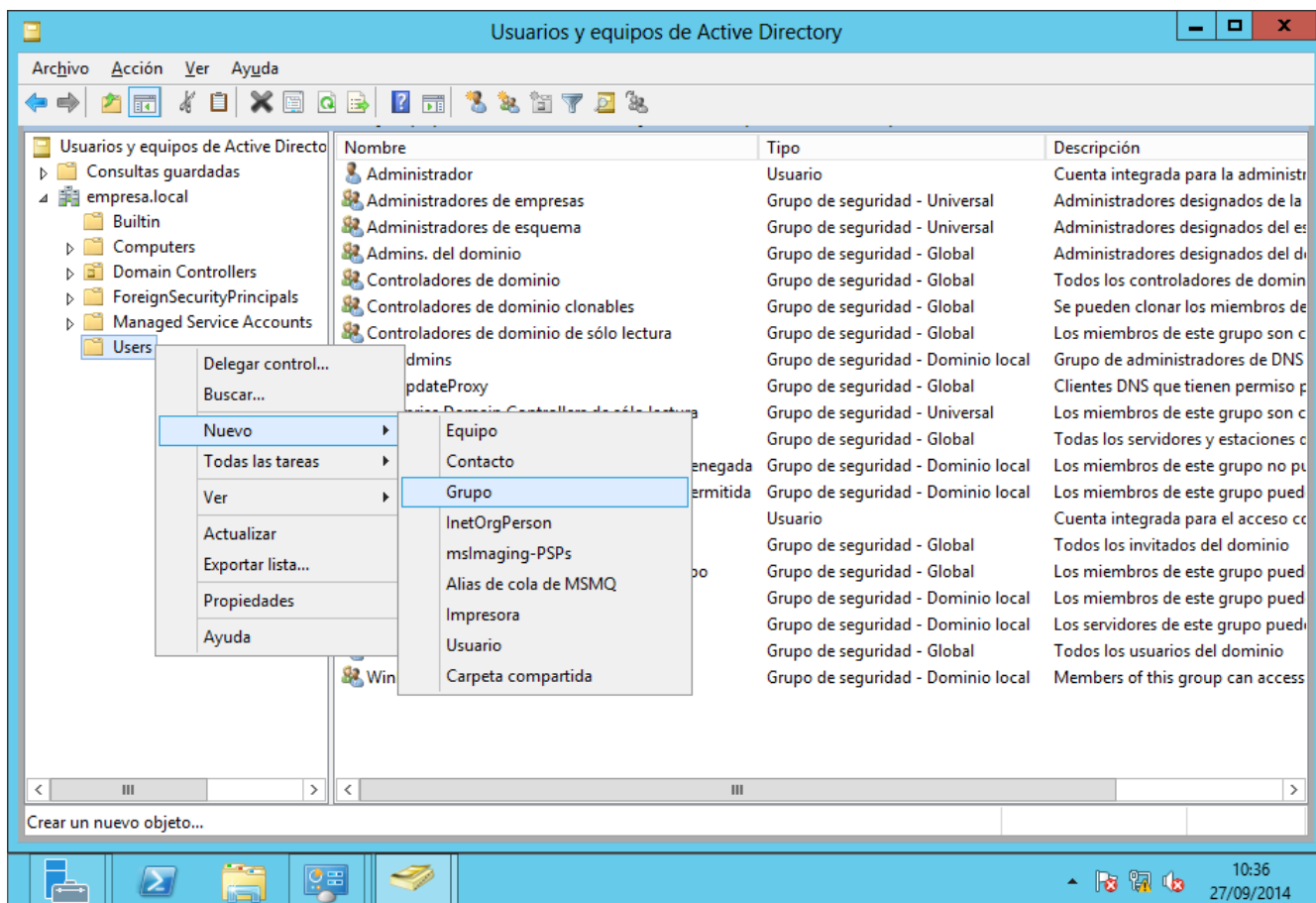
Examinemos las funciones de algunos de los grupos más utilizados:

- **Usuarios del dominio:** grupo global que contiene **todas** las cuentas de usuarios el dominio.
- **Administradores del dominio:** grupo global que permite a sus miembros realizar tareas de administración del dominio.
- **Administradores de empresa:** grupo universal que permite a sus miembros realizar tareas de administración en **todos los dominios de la red**.
- **Administradores de esquema:** grupo universal que permite a sus miembros modificar la estructura de los objetos del Directorio Activo.
- **Administradores:** grupo local que permite a sus miembros realizar tareas de administración en el controlador de dominio.
- **Operadores de copias de seguridad:** grupo local que permite a sus miembros realizar copias de seguridad o restaurar archivos dentro del dominio.
- **Operadores de cuenta:** grupo local que permite a sus miembros crear, editar y eliminar cuentas de usuario y grupos.
- **Operadores de impresión:** grupo local que permite a sus miembros configurar y administrar el uso de impresoras de red.
- **Operadores de servidor:** grupo local que permite a sus miembros crear carpetas compartidas en el servidor y realizar copias de seguridad o restaurar archivos en el controlador de dominio.
- **Usuarios:** grupo local que limita las posibilidades de que un usuario haga un cambio accidental en el sistema pero sí permite ejecutar la mayoría de las aplicaciones.

Es importante darse cuenta del considerable ahorro de tiempo para el administrador que permite la existencia de grupos predefinidos para tareas muy concretas.

### 3.2. Creación de grupos mediante la interfaz gráfica

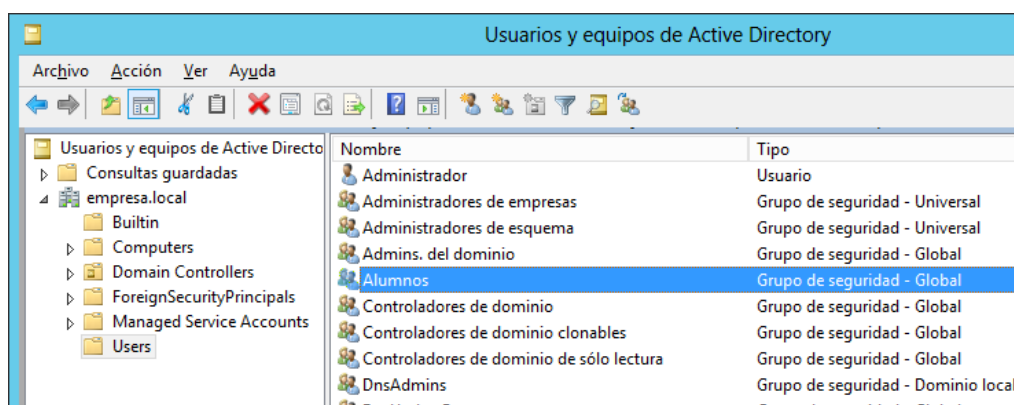
Los grupos se crean de manera muy similar a como se creaban los usuarios en el Directorio Activo.



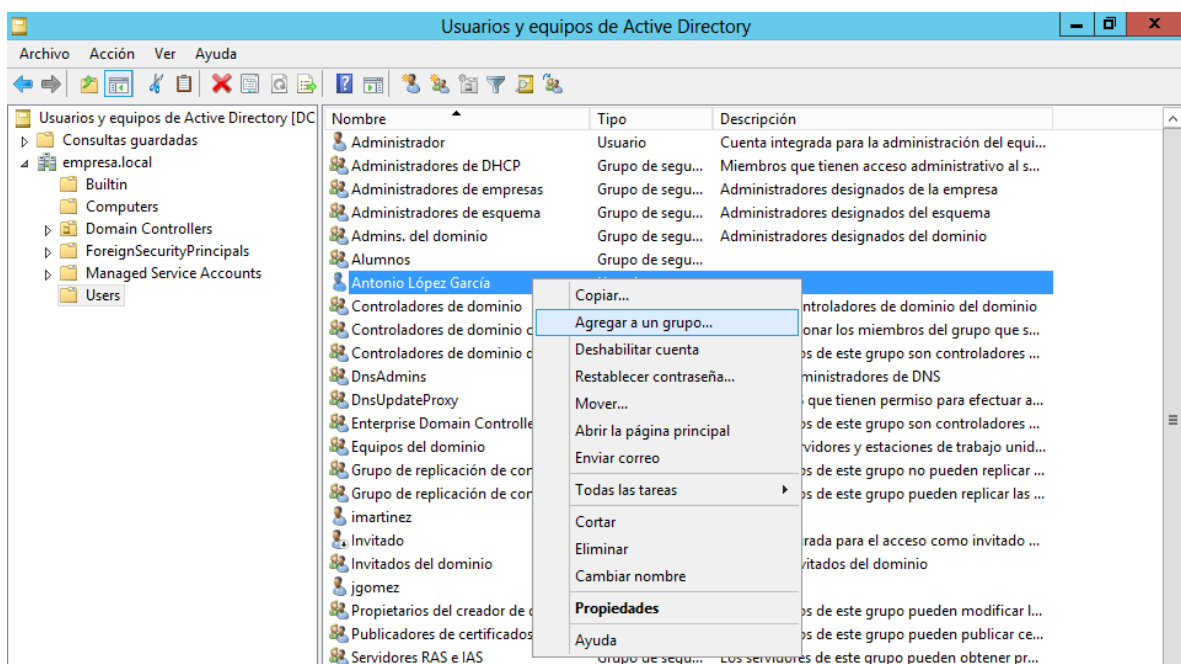
Se abrirá un cuadro de diálogo que nos permitirá introducir el nombre del grupo, así como su ámbito y tipo.



Por defecto se nos indica que el ámbito del grupo será 'Global' y el tipo de grupo será de 'Seguridad'. En principio, si no tenemos unas necesidades que justifiquen lo contrario, crearemos los grupos con esas propiedades. Tras pulsar 'Aceptar' nos aparecerá el nuevo grupo en el listado de 'Usuarios y equipos de Active Directory'.



Si queremos añadir usuarios en el grupo basta con seleccionar el usuario y en el menú que se abrirá al hacer clic con el botón derecho, acceder a la opción 'Agregar a un grupo'.





Se abrirá un cuadro en el que podremos indicar/buscar el grupo al que queremos añadir el usuario.

**Selección de Grupos**

Seleccionar este tipo de objeto:

Desde esta ubicación:

Escriba los nombres de objeto que desea seleccionar (ejemplos):

Tras aceptar, aparecerá un mensaje indicando que la operación se ha realizado con éxito y podremos comprobar en las propiedades del usuario que efectivamente es miembro del grupo 'Alumnos'.

**Servicios de dominio de Active Directory**

Se ha completado con éxito la operación Agregar a grupo.

**Usuarios y equipos de Active Directory**

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory [DC]

- Consultas guardadas
- empresa.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

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...	Administradores desig
Admins. del dominio	Grupo de segu...	Ad
Alumnos	Grupo de segu...	
Antonio López García	Usuario	
Controladores de dominio		Copiar...
Controladores de dominio clon		Agregar a un grupo...
Controladores de dominio de s		Deshabilitar cuenta
DnsAdmins		Restablecer contraseñ
DnsUpdateProxy		Mover...
Enterprise Domain Controllers		Abrir la página princip
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		
jgomez		
Propietarios del creador de dire		
Publicadores de certificados		
Servidores RAS e IAS		

**Propiedades**

**Propiedades: Antonio López García**

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

Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active Dir..
Alumnos	empresa.local/Users
Usuarios del dominio	empresa.local/Users

Grupo principal: Usuarios del dominio

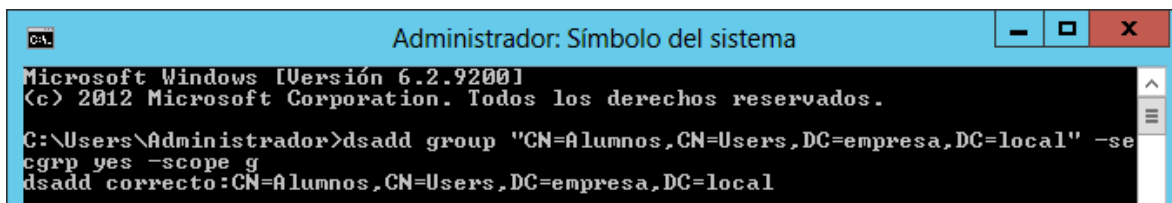
No es necesario cambiar Grupo principal si no tiene clientes de Macintosh o aplicaciones compatibles con POSIX.

### 3.3. Creación de grupos mediante la línea de comandos

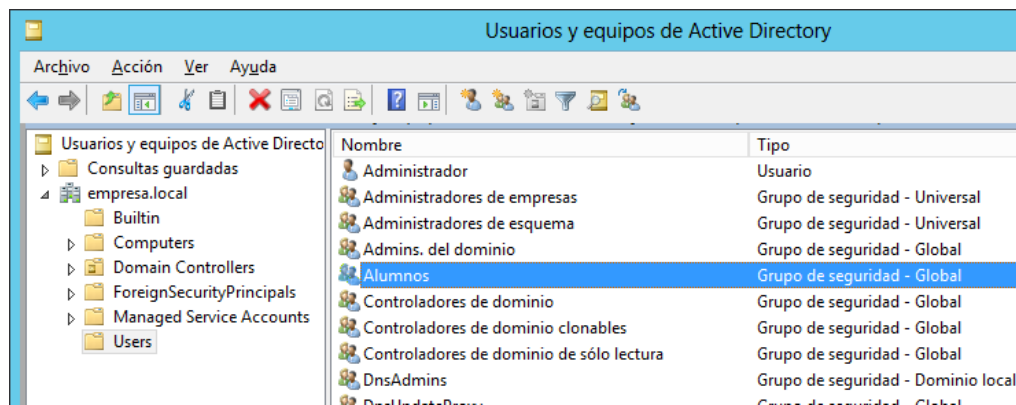
Para crear un grupo desde la consola, el comando utilizado es: `dsadd group`. Para especificar si el grupo es de seguridad o de distribución se utiliza la opción: `-secgrp yes` ( o `-secgrp no` si se trata de un grupo de distribución). Para especificar el ámbito del grupo como universal, global o local se utiliza `-scope` seguido de `u`, `g` o `l`, respectivamente.

Si queremos crear el grupo 'Alumnos' como en el caso anterior escribiríamos el siguiente comando:

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



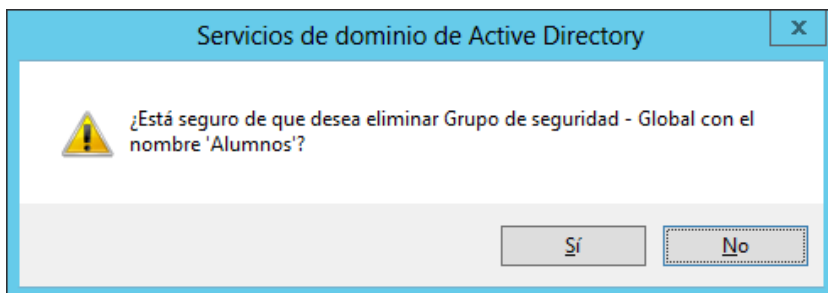
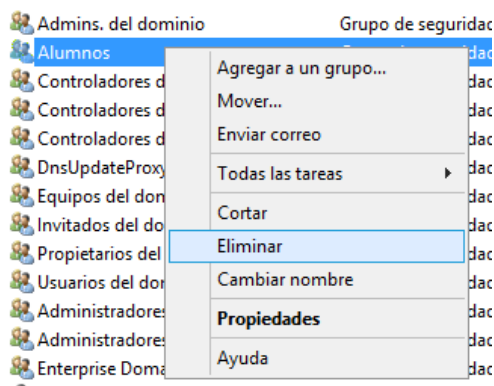
Si observamos el administrador de 'Usuarios y Equipos de Active Directory', vemos que el grupo se ha creado correctamente.



Se puede obtener más información acerca de la administración de los grupos por la línea de comandos en el [siguiente enlace del Technet de Microsoft](#).

### 3.4. Eliminación de grupos

Haciendo clic con el botón derecho sobre el grupo elegimos la opción "eliminar".



## 4. Unidades Organizativas

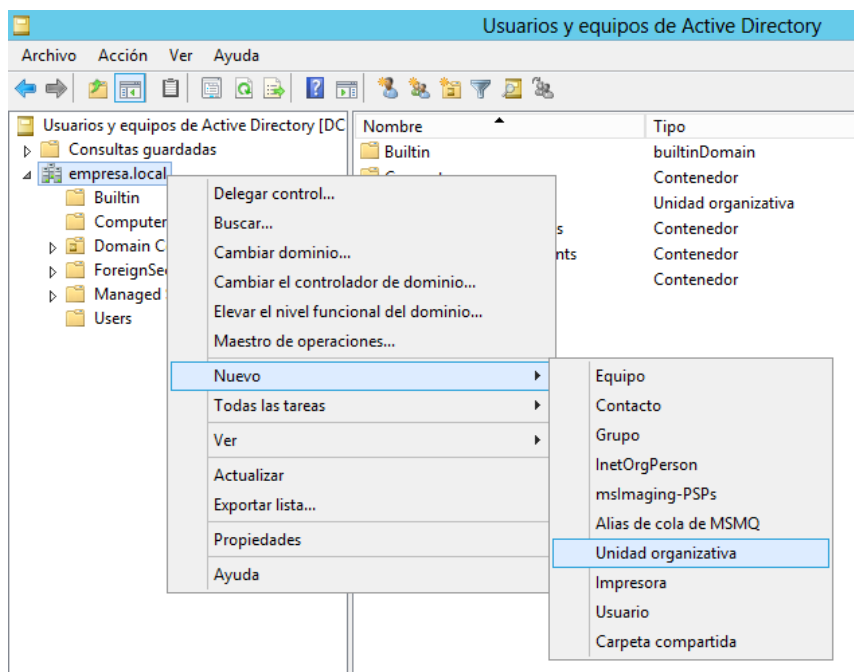
Una unidad organizativa es un contenedor de objetos (usuarios, grupos, equipos, otras unidades organizativas, etc.) pertenecientes a un **mismo** dominio. Son especialmente útiles para reproducir la estructura de la empresa donde se halle el dominio. Es decir, si por ejemplo, una empresa está dividida en tres departamentos (dirección, ventas y producción), podemos crear tres unidades organizativas correspondientes a estos tres departamentos, donde incluyamos todos los objetos del dominio correspondientes a cada una de las áreas de la empresa.

Su utilidad radica en dos aspectos fundamentales:

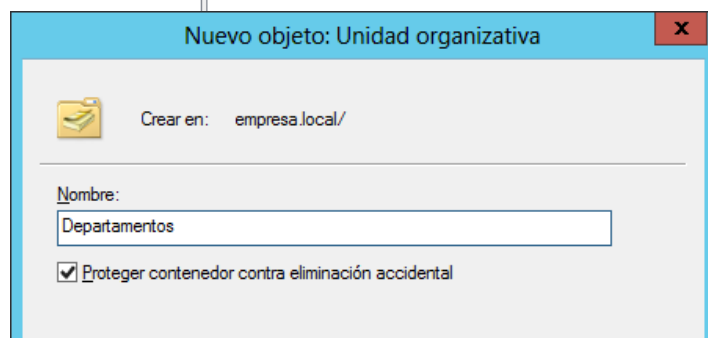
1. De esta manera es muy sencillo establecer directivas de seguridad (las veremos en el tema 5) que se apliquen a todos los objetos de cada departamento.
2. Como dentro de la unidad organizativa, se pueden introducir otras unidades organizativas, se puede replicar la estructura jerárquica de la empresa sin necesidad de crear más dominios o subdominios.

### 4.1. Creación de UO

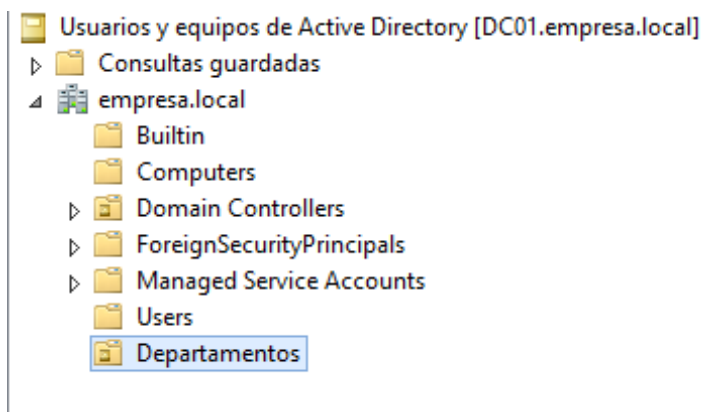
Para crear una unidad organizativa abriremos la ventana 'Usuarios y Equipos de Active Directory' (menú de 'Inicio', 'Herramientas Administrativas'). A continuación, nos situamos sobre el dominio y haciendo clic con el botón secundario seleccionamos 'Nuevo' y 'Unidad Organizativa'.



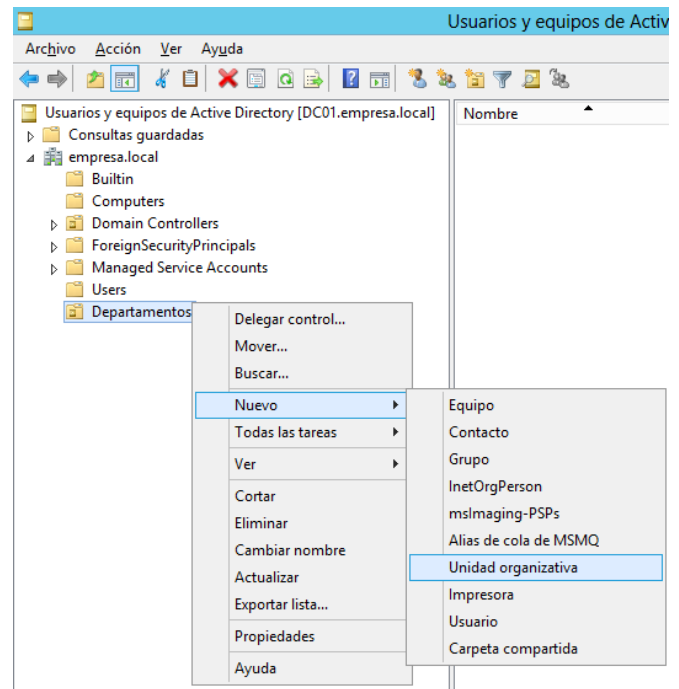
A continuación se abrirá el diálogo que nos permite indicar el nombre del nuevo objeto.



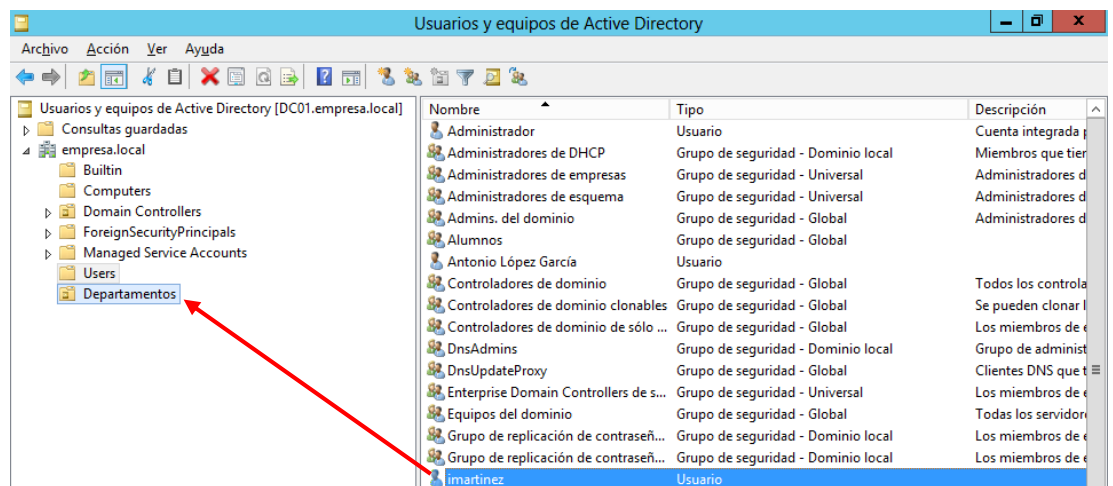
Tras pulsar 'Aceptar', podemos comprobar que efectivamente se ha creado la unidad organizativa dentro del dominio.



Haciendo clic con el botón secundario sobre la unidad organizativa creada, podemos comprobar los elementos que podemos incluir dentro de esta.

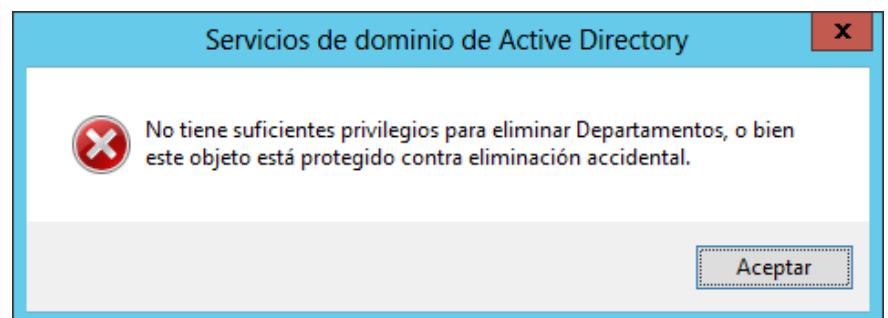


Para agregar objetos a una unidad organizativa, bastará con seleccionarlos y arrastrarlos hasta la unidad organizativa en la que queremos que estén incluidos.

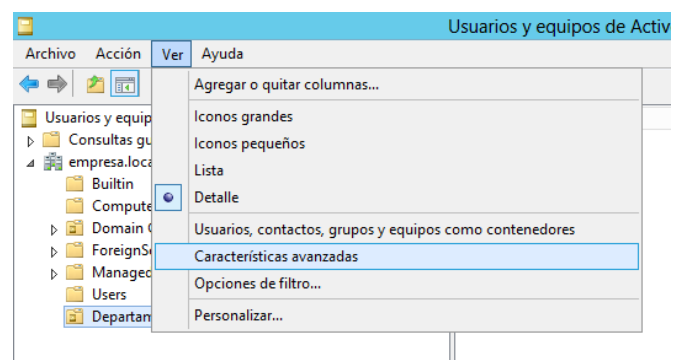


## 4.2. Eliminación de UO

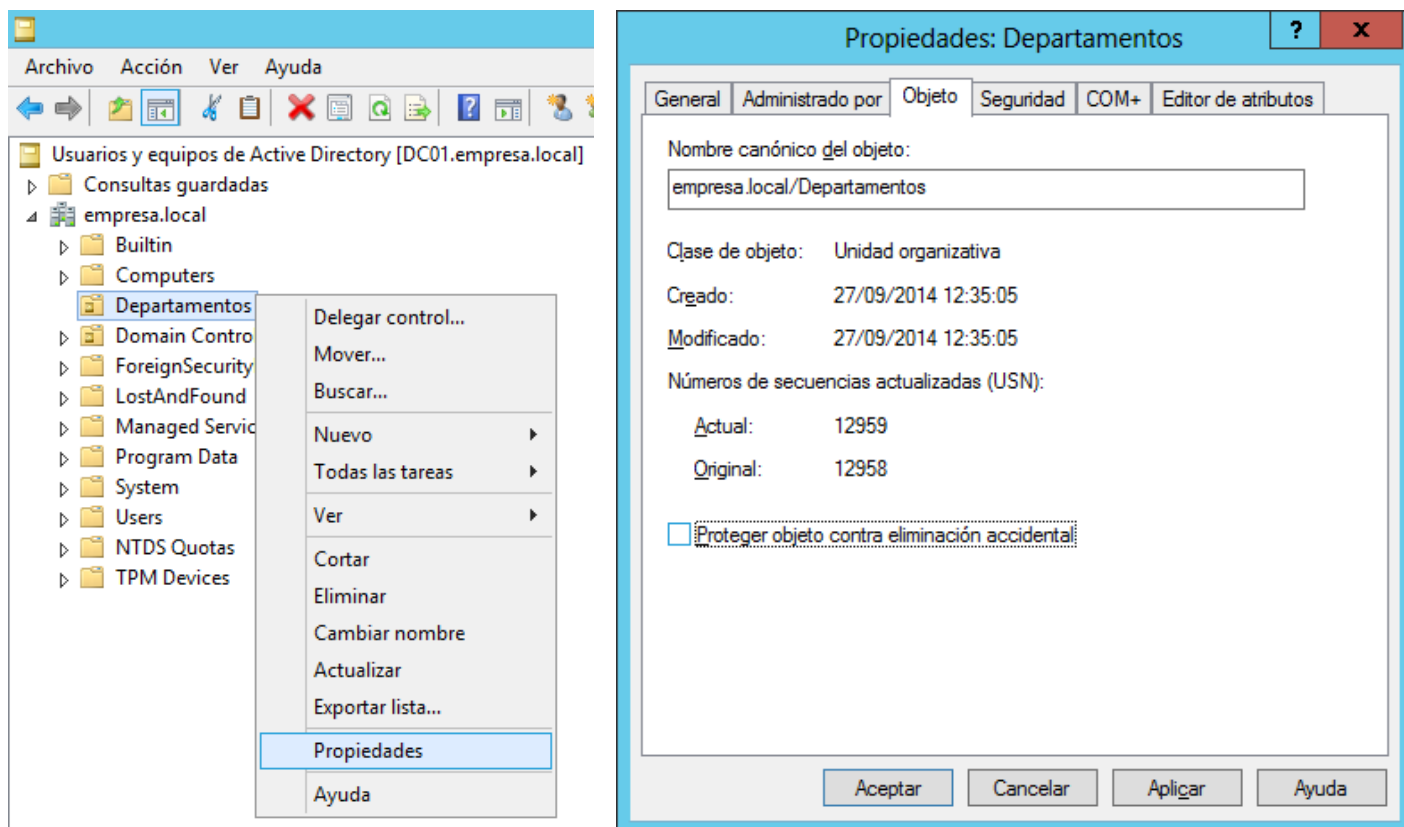
Si tratamos de borrar una unidad organizativa, al estar protegidas contra eliminaciones accidentales, nos aparecerá el siguiente mensaje.



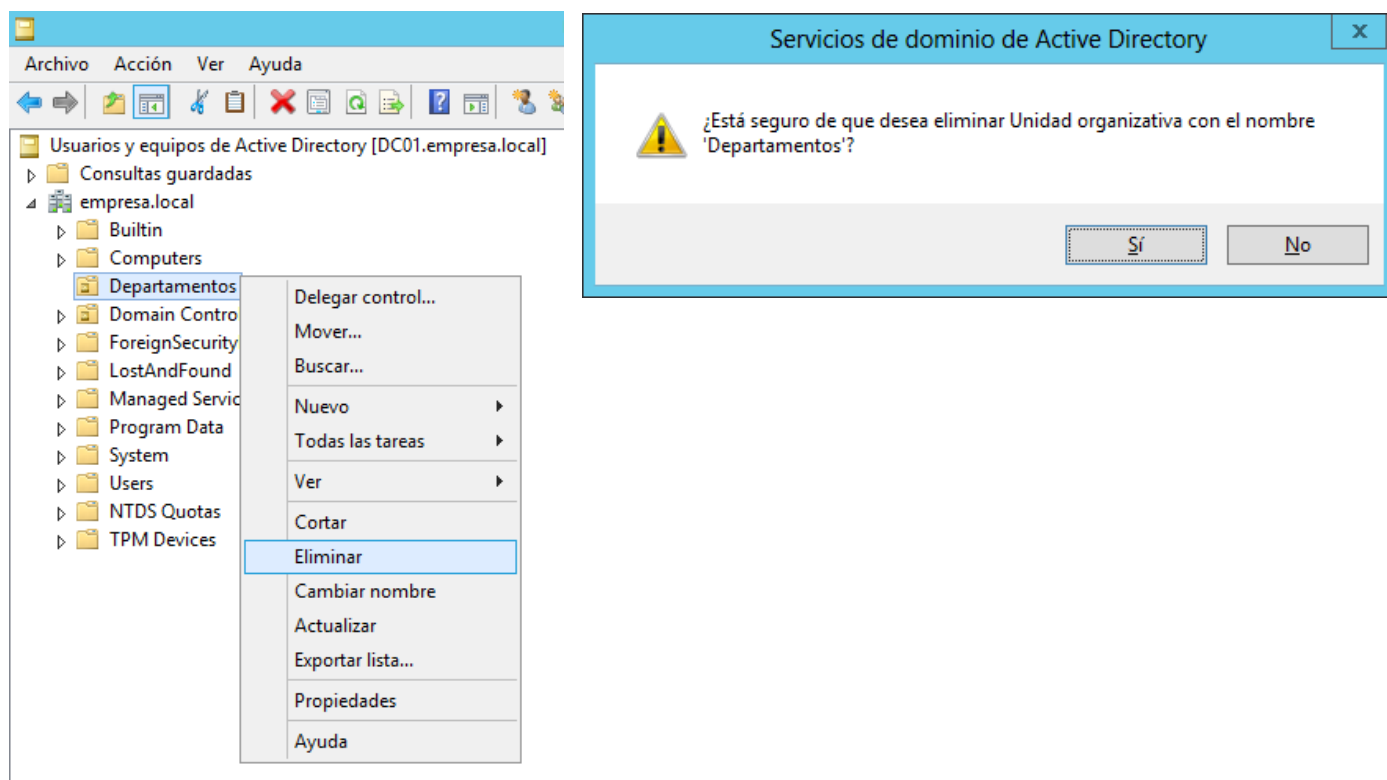
Para eliminar las unidades organizativas, en primer lugar deberemos activar las 'características avanzadas' seleccionando en el menú 'Ver' la opción 'Características Avanzadas'.



Ahora ya podemos desmarcar la opción de 'Proteger contra eliminación accidental' en las propiedades de la unidad organizativa.



Ahora, para eliminar la unidad organizativa 'Departamentos', bastará con hacer clic con el botón secundario y seleccionar 'Eliminar'.



En el próximos temas, utilizaremos las unidades organizativas para gestionar de manera eficaz el dominio, aplicando directivas de seguridad específicas a cada unidad organizativa.

## 5. Caso Práctico: Creación de la estructura de una organización mediante la línea de comandos

La administración del dominio es una tarea sencilla mediante la interfaz gráfica, pero puede ser muy tediosa si hay que repetir en innumerables ocasiones secuencias de acciones. Pensemos, por ejemplo, en el caso típico en el que hay que **dar de alta a una cantidad muy grande de usuarios**, creando la estructura completa de la organización. Este tipo de procesos puede facilitarse enormemente mediante la utilización de **scripts**.

Concretamente, en este ejemplo se plantea la creación de las cuentas de usuario de una organización, así como sus grupos y unidades organizativas.

Vamos a suponer que la organización está formada por cinco departamentos:

1. Dirección.
2. Finanzas.
3. Producción.
4. Ventas.
5. Servicios.

Esta empresa está formada por 40 trabajadores, por lo que es complicado darlos a todos de alta mediante la interfaz gráfica correctamente, sin equivocarse en la asignación de grupos, direcciones de correo, etc. Para automatizar el proceso, se podría extraer del sistema ERP (openERP, openBravo, SAP, Navisión, etc.) un fichero de texto, por ejemplo en formato csv. El fichero de texto podría estar estructurado con los siguientes campos:

1. Nombre.
2. Apellidos.
3. Contraseña.
4. Departamento.
5. Cargo.

	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

Además de los grupos asociados a departamentos, se ha decidido crear tres unidades organizativas en el dominio para gestionar las directivas de seguridad (estas las veremos en el tema 5). En estas se incluirán únicamente a usuarios. Las tres unidades organizativas serán:

1. Directores (por ejemplo podrían estar los directores de departamento).
2. Mandos intermedios.
3. Trabajadores.

Como se puede comprobar, la tarea es muy ardua si ha de realizarse manualmente. Para automatizarla, se plantea la **creación de tres scripts**:

1. Creación de los **grupos**.
2. Creación de las **unidades organizativas**.
3. Creación de los **usuarios** del dominio a partir del fichero CSV obtenido del ERP, y configuración de las cuentas, así como su inclusión en grupos y unidades organizativas

A continuación se presentan los tres scripts (ficheros con extensión `.bat`) propuestos para crear la estructura completa de la empresa (crearemos toda esta estructura en el dominio `empresa.local`).

## 5.1. Creación de los grupos

Crearemos los grupos globales para cada departamento con el siguiente script (que os podéis descargar en departamentos.bat).

```
@echo off

for /F %%a in (departamentos.csv) do (

echo Procesando el grupo %%a

dsadd group "CN=%%a,CN=Users,DC=empresa,DC=local" -secgrp yes -scope g

)
```

En este caso, departamentos.csv es un fichero que contiene los departamentos de la empresa. Como únicamente se trata de cinco departamentos, podrían crearse manualmente.

El comando anterior recorre el fichero departamentos.csv con la opción /F. El contenido de cada línea se almacena en la variable %%a. Finalmente para cada línea se ejecuta el comando dsadd que crea el grupo de seguridad de ámbito global (-secgrp yes -scope g) con el nombre contenido en la variable %%a.

Además crearemos manualmente por la línea de comandos un grupo local de dominio extra para incluir a usuarios y grupos que queramos que tengan permisos de acceso especiales a los recursos compartidos. Haremos miembros de este grupo a todos los usuarios del grupo Dirección y a todos los usuarios del grupo Finanzas utilizando la opción -members.

```
>>dsadd group "CN=Acceso_extra,CN=Users,DC=empresa,DC=local" -secgrp yes
-scope l -members "CN=Dirección,CN=Users,DC=empresa,DC=local"
"CN=Finanzas,CN=Users,DC=empresa,DC=local"
```

En las siguientes imágenes se muestra el resultado de la ejecución de los comandos anteriores.

Nombre	Tipo
Acceso_extra	Grupo de seguridad - Dominio local
Administrador	Usuario
Administradores de DHCP	Grupo de seguridad - Dominio local
Administradores de empresas	Grupo de seguridad - Universal
Administradores de esquema	Grupo de seguridad - Universal
Admins. del dominio	Grupo de seguridad - Global
Controladores de dominio	Grupo de seguridad - Global
Controladores de dominio clonables	Grupo de seguridad - Global
Controladores de dominio de sólo ...	Grupo de seguridad - Global
Direccion	Grupo de seguridad - Global
DnsAdmins	Grupo de seguridad - Dominio local
DnsUpdateProxy	Grupo de seguridad - Global
Enterprise Domain Controllers de s...	Grupo de seguridad - Universal
Equipos del dominio	Grupo de seguridad - Global
Finanzas	Grupo de seguridad - Global
Grupo de replicación de contraseñ...	Grupo de seguridad - Dominio local
Grupo de replicación de contraseñ...	Grupo de seguridad - Dominio local
Invitado	Usuario
Invitados del dominio	Grupo de seguridad - Global
krbtgt	Usuario
Produccion	Grupo de seguridad - Global
Propietarios del creador de directiv...	Grupo de seguridad - Global
Publicadores de certificados	Grupo de seguridad - Dominio local
Servicios	Grupo de seguridad - Global
Servidores RAS e IAS	Grupo de seguridad - Dominio local
Usuarios de DHCP	Grupo de seguridad - Dominio local
Usuarios del dominio	Grupo de seguridad - Global
Ventas	Grupo de seguridad - Global

Grupos creados

Propiedades: Acceso\_extra

Objeto	Seguridad	Editor de atributos
General	Miembros	Miembro de Administrado por

Miembros:

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

Agregar... Quitar

Aceptar Cancelar Aplicar Ayuda

Miembros del grupo Acceso\_extra



## 5.2. Creación de las unidades organizativas

Aunque probablemente no valga la pena confeccionar un script para crear las tres unidades organizativas previstas, utilizaremos el mismo patrón del caso anterior para crearlas.

En este caso el script (unidades.bat) sería así:

```
@echo off

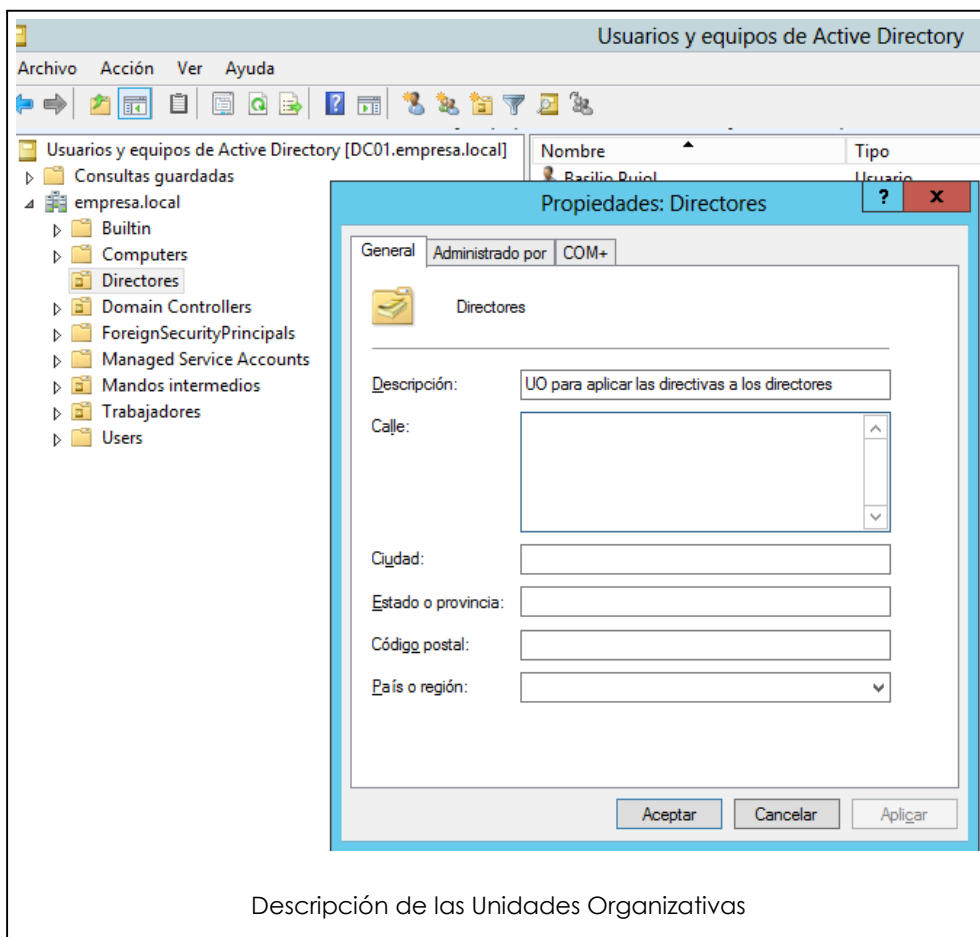
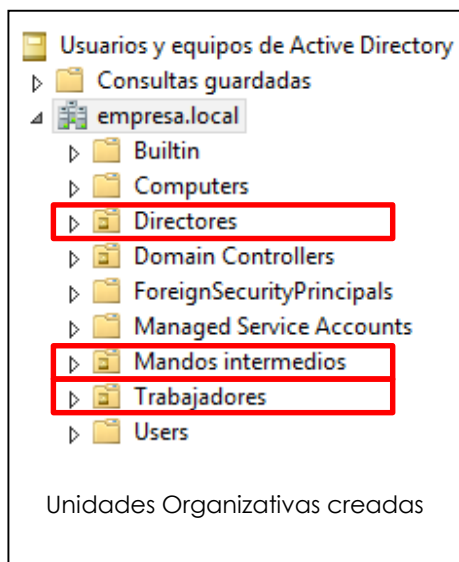
for /F "tokens=1,2 delims=;" %%a in (unidades_org.csv) do (

echo Procesando la unidad organizativa %%a

dsadd ou "OU=%%a,DC=empresa,DC=local" -desc "%%b"

)
```

unidades\_org.csv es el fichero que contiene el nombre de las unidades organizativas planificadas para el dominio, y su descripción, la cual adjuntamos a la unidad organizativa mediante la opción `-desc`





### 5.3. Creación de usuarios

El siguiente script (usuarios.bat) crea los usuarios asignándolos a su departamento y unidad organizativa.

```
@echo off

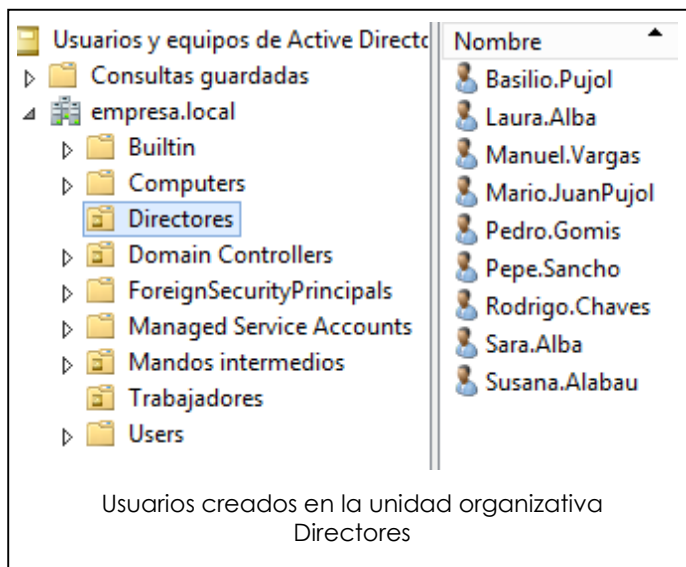
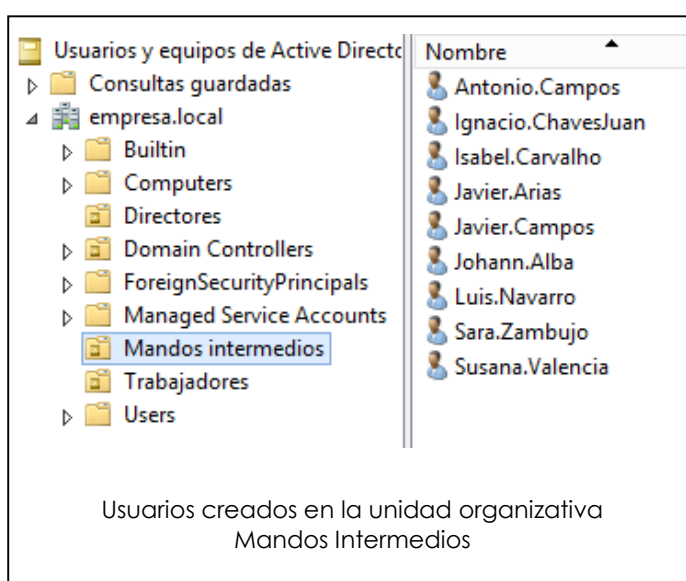
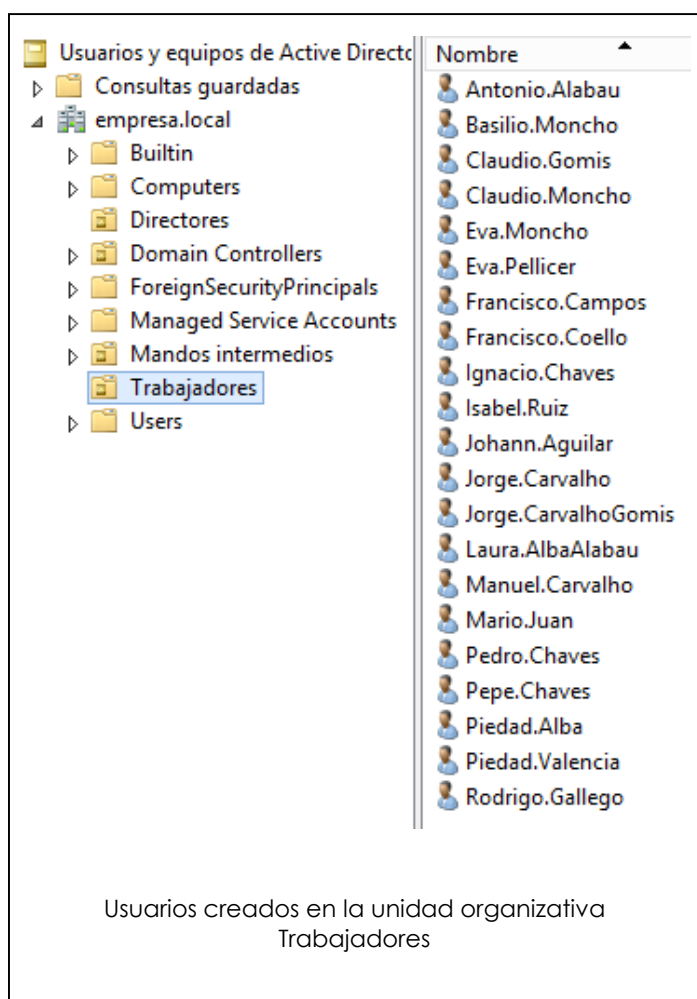
for /F "tokens=1,2,3,4,5,6 delims=; skip=1" %a in (usuarios.csv) do (

echo Procesando el usuario %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 las siguientes imágenes podemos comprobar la creación de los usuarios.



Examinemos detalladamente la sintaxis anterior para poder comprenderla mejor, y así poder modificarla para los casos reales que puedan surgirnos.

Como se ha explicado anteriormente, el bucle `for /F ... do ( ... )` recorre **línea a línea** el fichero que se le pasa como parámetro `in(usuarios.csv)`.

El modificador `tokens=1,2,3,4,5,6` almacena el contenido de las columnas de la 1 a la 6 del fichero en las variables correlativas a la variable `%%a` de la siguiente manera:

- Columna 1 (Nombre): variable `%%a`
- Columna 2 (Primer apellido): variable `%%b`
- Columna 3 (Segundo apellido): variable `%%c`
- Columna 4 (Contraseña): variable `%%d`
- Columna 5 (Departamento): variable `%%e`
- Columna 6 (Cargo): variable `%%f`

En este caso cabe destacar que las columnas están delimitadas con punto y coma (`delims=;`). Modificando la sintaxis anterior, podríamos adaptar el script a cualquier tipo de caracter de separación de columnas. Por otra parte, como la primera fila del fichero son las cabeceras de cada columna, no nos interesa para crear los usuarios, así que la saltamos con `skip=1`. Este modificador sirve para saltar un número determinado de líneas, en este caso 1.

La siguiente línea (`echo ...`) simplemente muestra por la pantalla el usuario que se está procesando en ese instante. Esta línea se puede obviar perfectamente.

A continuación viene la parte más interesante del script, donde utilizamos las variables que hemos creado para introducirlas en el comando `dsadd user`.

- Lo primero que hace el comando es crear el usuario con el *Common Name* definido por las variables `%%a` y `%%b`, unidas por un punto: `"CN=%%a.%%b,`
- Ese usuario se crea en la unidad organizativa asignada al cargo que tenga dentro de la organización ese usuario (Directores, Mandos Intermedios o Trabajadores): `OU=%%f,`
- `DC=empresa, DC=local` indican el dominio dentro del cual se halla la unidad organizativa en la que se creará el usuario.
- `-fn %%a` indica el nombre de pila del usuario.
- `-ln "%%b %%c"` indica los apellidos del usuario.
- `-pwd %%d` indica la contraseña del usuario.
- `-upn %%a.%%b@empresa.local` indica el nombre de sistema del usuario (se sigue el criterio `nombre.primerApellido`).
- `-email %%a.%%b@empresa.local` indica el correo electrónico del usuario, creado con el criterio `Nombre.PrimerApellido@empresa.local`.
- `-mustchpwd yes` obliga al usuario a cambiar la contraseña.
- `-display "%%a %%b %%c"` indica el nombre del usuario que se mostrará ("Nombre Primer Apellido Segundo Apellido").
- `-canchpwd yes` otorga al usuario la posibilidad de cambiar la contraseña.
- `-disabled no` indica que la cuenta está habilitada.
- `-memberof "CN=%%e,CN=Users,DC=empresa,DC=local"` indica el grupo o grupos a los que pertenece el usuario.

Este comando puede enriquecerse mucho más para ceñirse en mayor medida a las necesidades de administración. En las páginas de [Microsoft de Technet](#), se halla una explicación bastante exhaustiva acerca de más opciones de `dsadd`.

En las siguientes imágenes podemos revisar las propiedades con las que ha sido creado cada usuario.

Propiedades: Pedro.Gomis

Marcado Entorno Sesiones Control remoto

Perfil de Servicios de Escritorio remoto COM+

General Dirección Cuenta Perfil Teléfonos Organización Miembro de

Pedro.Gomis

Nombre de pila: Pedro Iniciales:

Apellidos: Gomis Zambujo

Nombre para mostrar: Pedro Gomis Zambujo

Descripción:

Oficina:

Número de teléfono: Otros...

Correo electrónico: Pedro.Gomis@empresa.local

Página web: Otros...

Aceptar Cancelar Aplicar Ayuda

Ficha 'General' de las propiedades del usuario.

Propiedades: Pedro.Gomis

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: Pedro.Gomis @empresa.local

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

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 está deshabilitada

La cuenta expira

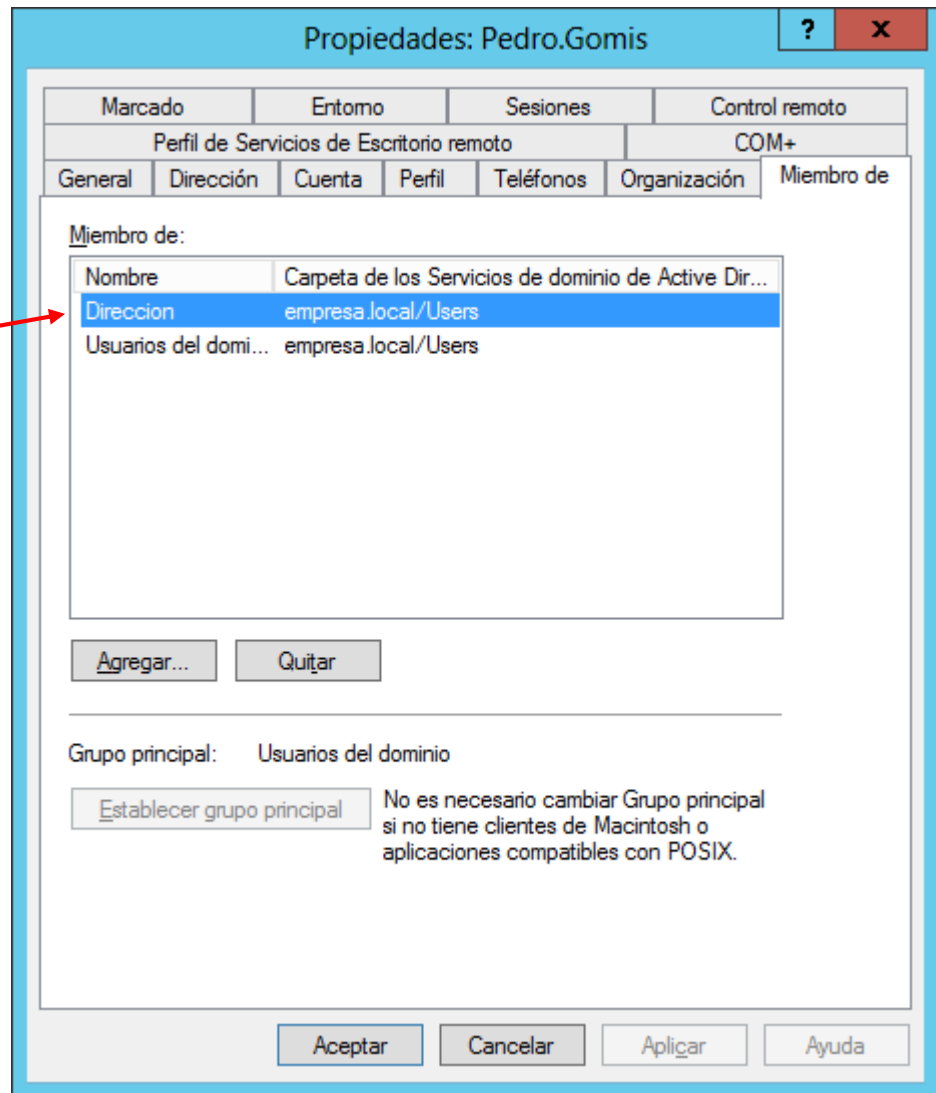
☒ Nunca

☐ Fin de: jueves , 30 de octubre de 2014

Aceptar Cancelar Aplicar Ayuda

Ficha 'Cuenta' de las propiedades del usuario.

-memberof



Ficha 'Miembro de' de las propiedades del usuario.

Si nos fijamos con detenimiento, hay algunos usuarios cuyo nombre y primer apellido coinciden. En ese caso el script anterior **falla** al tratar de crear la segunda cuenta de usuario con el mismo identificador. Si revisamos el fichero usuarios.csv, vemos que esto ocurre con los usuarios:

- Jorge Carvalho Pellicer y Jorge Carvalho Gomis,
- Ignacio Chaves Juan e Ignacio Chaves Vargas,
- Mario Juan Pujol y Mario Juan Valencia, y
- Laura Alba Arias y Laura Alba Alabau.

Debemos establecer un mecanismo de control que detecte esa situación y aporte una alternativa. En este ejemplo se ha optado por controlar si ya existe una cuenta de usuario, y si ya existe se cambia el criterio de creación del identificador de usuario al siguiente:

- Nombre.PrimerApellidoSegundoApellido

Ahora los identificadores de usuario 'duplicados' serán:

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

El siguiente script (usuarios\_v2.bat) resuelve la situación anterior (hay que darse cuenta de que no solo hay que modificar la manera de escribir la cuenta de usuario ("CN=..."), sino también la dirección de correo y el nombre del sistema del usuario -upn y -email.

```
@echo off

for /F "tokens=1,2,3,4,5,6 delims=; skip=1" %%a in (usuarios.csv) do (

echo Procesando el usuario %%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=local" -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"

)
```

La única diferencia con el anterior script radica en el último comando. Hacemos uso del código de estado ERRORLEVEL. Si nos fijamos, en el script, si tratamos de crear con dsadd user un usuario que ya existe, no se creará y devolverá un código de error. En este caso es menor que 0 (podéis comprobarlo manualmente con echo %ERRORLEVEL%).

Al poner como condición NOT ERRORLEVEL 0 en el if, **ejecutamos el comando dsadd user... con las nuevas opciones "CN=%%a.%%b%%c cuando ERRORLEVEL es menor que 0**. Si es igual a 0 significa que no ha habido fallo en la creación del usuario, por lo que no hay que realizar ninguna otra acción.

## 6. Consultas sobre objetos del dominio: dsquery

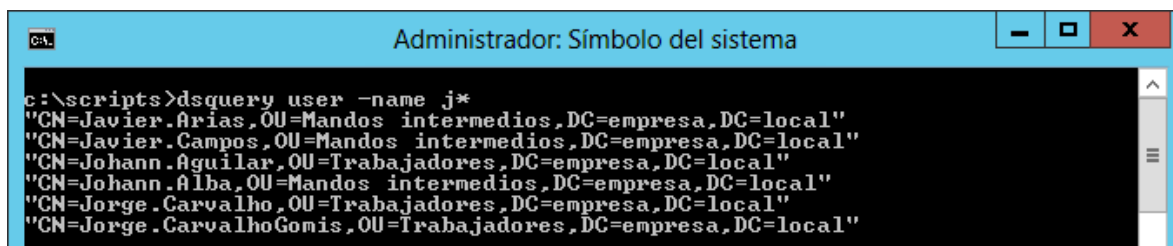
Como hemos visto en algunos ejemplos anteriores, resulta muy tedioso introducir por línea de comandos el nombre completo de un usuario o un grupo. Recordemos el caso de la deshabilitación de la cuenta de un usuario:

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

Tenemos que introducir el nombre completo del usuario para que el comando funcione. Podemos facilitar esta tarea (aunque con ciertos riesgos) mediante el comando dsquery. Entre otras funciones, podemos obtener el nombre completo de un usuario, un grupo, un equipo, etc. a partir de un fragmento del nombre. Para ello escribimos dsquery a continuación user, si buscamos información sobre un usuario, y finalmente un fragmento del nombre:

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

El comando anterior devolverá todos los usuarios cuyo nombre empieza por j.



```
Administrador: Símbolo del sistema

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.CarvalhoGonis,OU=Trabajadores,DC=empresa,DC=local"
```

Si lo que pretendemos es ahorrar tiempo en la escritura de un usuario concreto, podemos introducir el comando de búsqueda en una variable, de manera que esa variable (nombre completo del usuario), podamos utilizarla para configurar su cuenta. En este caso concreto, la deshabilitaremos. En primer lugar introducimos el comando de búsqueda en una variable:

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

Si mostramos el valor de la variable a, veremos que se ha almacenado correctamente el comando anterior:

```
>>echo %a%
```

Para ver el resultado de la ejecución de la variable a escribimos lo siguiente:

```
>>%a%
```

Ahora que ya tenemos el comando de búsqueda y obtención del nombre completo del usuario javier.arias, podemos introducirlo en el comando de deshabilitación de cuentas `dsmod user -disabled yes`. Esto lo realizaremos mediante una tubería (`|`).

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

Comprobemos que efectivamente la cuenta está deshabilitada (ver flecha hacia abajo junto al símbolo de usuario):



Podéis encontrar más información sobre:

- Ficheros por lotes (bat): <http://www.saulo.net/pub/msdos/cap10.htm>
- dsquery: [Technet de Microsoft](http://technet.microsoft.com).

## 7. Bibliografía

- José Ramón Ruiz Rodríguez (2013). Curso Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curso Cefire Windows Server 2012.
- SomeBooks.es (2014). Sistemas Operativos en Red. Disponible en <http://somebooks.es/?p=4787>
- Wikipedia. Sistema Operativo de red. 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/>
- Ficheros por lotes (bat): <http://www.saulo.net/pub/msdos/cap10.htm>