

Usuarios e Grupos en Windows Server



Sistemas Operativos en Rede

Curso 2022-23

Usuarios e Grupos en Windows Server

1.- Conceptos básicos.....	3
1.1.- Conta de usuario.....	3
1.2.- Contas integradas.....	3
1.3.- Conta de equipo.....	4
1.4.- Conta de grupo.....	4
1.4.1.-Ámbito dos grupos.....	5
1.4.2.-Tipos de grupos.....	5
1.4.3.-Grupos integrados.....	6
2.- Crear unha Conta de Usuario.....	20
3.- Propiedades das contas de usuarios.....	24
3.1.- Pestanas General e Dirección.....	26
3.2.- Pestana Cuenta.....	27
3.3.- Pestana Miembro de.....	31
3.4.- Pestana Perfil.....	32
4.- Operacións frecuentes con contas de usuario.....	33
4.1.- Recuperar contrasinais.....	33
4.2.- Deshabilitar unha conta de usuario.....	34
4.3.- Eliminar unha conta de usuario.....	36
4.4.- Copiar unha conta de usuario.....	37
4.5.- Cambiar as propiedades dun grupo de contas.....	42
5.- Crear unha Conta de Grupo.....	44
5.1.- Introducción.....	44
5.2.- Creación de grupos.....	44
6.- Unidades Organizativas.....	47
6.1.- Introducción.....	47
6.2.- Crear unha unidade organizativa.....	49
6.3.- Eliminar unha Unidade Organizativa.....	55

Contidos baixo unha licenza Creative Commons Recoñecemento
- Non Comercial - Sen Obra Derivada 3.0

Emilio Domarco Cid - 2021



1.- Conceptos básicos

Un dos elementos fundamentais na administración dunha rede, é o control dos usuarios, grupos e equipos. Por iso, debemos aprender como crealos, modificalos, organizalos e, se chega o caso, eliminalos.

Ademais, deberemos asignar privilexios para cada un deles, de modo que podamos establecer en que medida e baixo que condicións poderán beneficiarse dos recursos da rede.

1.1.- Conta de usuario

Unha das primeiras ideas que deben quedar claras cando falamos de contas de usuario é que non sempre representan a persoas concretas, senón que tamén poden ser utilizadas como mecanismos de acceso para determinados servizos ou aplicacións da máquina local ou, mesmo, dun equipo remoto.

En definitiva, unha conta de usuario é un obxecto que posibilita o acceso aos recursos do dominio de dous modos diferentes:

- ✓ Permite **autenticar a identidade** dun usuario, porque só poderán iniciar unha sesión aqueles usuarios que dispoñan dunha conta no sistema asociada a un determinado contrasinal.
- ✓ Permite **autorizar, ou denegar**, o acceso aos recursos do dominio, porque, unha vez que o usuario iniciase a súa sesión só terá acceso aos recursos para os que recibise os permisos correspondentes.

Cada conta de usuario dispón dun identificador de seguridade (SID, Security IDentifier) que é único no dominio.

1.2.- Contas integradas

Cando se crea o dominio, créanse tamén dúas novas contas: Administrador e Convidado. Posteriormente, cando é necesario, créase tamén a conta Asistente de axuda.

Estas son as denominadas contas integradas e dispoñen dunha serie de dereitos e permisos predefinidos:

- ✓ **Administrador:** Ten control total sobre o dominio e non se poderá eliminar nin retirar do grupo Administradores (aínda que si podemos cambiarlle o nome ou deshabilitarla).
- ✓ **Convidado:** Está deshabilitada de forma predeterminada e, aínda que non se recomenda, pode habilitarse, por exemplo, para permitir o acceso aos usuarios que aínda non teñen conta no sistema ou que a teñen deshabilitada. De forma predeterminada non require contrasinal, aínda que esta característica, como calquera outra, pode ser modificada polo administrador.

- ✓ **Asistente de axuda:** utilízase para iniciar sesións de Asistencia remota e ten acceso limitado ao equipo. Créase automaticamente cando se solicita unha sesión de asistencia remota e elimínase cando deixan de existir solicitudes de asistencia pendentes de satisfacer.

Por último, é importante ter en conta que, aínda que a conta Administrador estea deshabilitada, poderá seguir usándose para acceder ao controlador de dominio en modo seguro.

1.3.- Conta de equipo

Como ocurría coas contas de usuario, unha conta de equipo serve para autenticar aos diferentes equipos que se conectan ao dominio, permitindo ou denegando o seu acceso aos diferentes recursos do dominio.

Como xa ocurría coas contas de usuario, as contas deben ser únicas no dominio.

Aínda que unha conta de equipo pódese crear de forma manual, tamén se pode crear no momento no que o equipo se une ao dominio, como vimos anteriormente.

1.4.- Conta de grupo

Un grupo é un conxunto de obxectos do dominio que poden administrarse como un todo.

Pode estar formado por contas de usuario, contas de equipo, contactos e outros grupos.

Podemos utilizar os grupos para simplificar algunhas tarefas, como:

- ✓ **Simplificar a administración:** Podemos asignar permisos ao grupo e estes afectarán a todos os seus membros.
- ✓ **Delegar a administración:** Podemos utilizar a directiva de grupo para asignar dereitos de usuario unha soa vez e, máis tarde, agregar os usuarios aos que queiramos delegar eses dereitos.
- ✓ **Crear listas de distribución de correo electrónico:** Só se utilizan cos grupos de distribución que comentaremos máis abaixo.

O Directorio Activo proporciona un conxunto de grupos predefinidos que poden utilizarse tanto para facilitar o control de acceso aos recursos como para delegar determinados roles administrativos.

Por exemplo, o grupo Operadores de copia de seguridade permite aos seus membros realizar copias de seguridade de todos os controladores de dominio, no dominio ao que pertencen.

1.4.1.- Ámbito dos grupos

O ámbito dun grupo establece o seu alcance, é dicir, en que partes da rede pode utilizarse, e o tipo de contas que poden formar parte del.

Ámbito local: Entre os seus membros poden atoparse un ou varios dos seguintes tipos de obxectos:

- ✓ Contas de usuario ou equipo.
- ✓ Outros grupos de ámbito local.
- ✓ Grupos de ámbito global.
- ✓ Grupos de ámbito universal.

As contas ou grupos contidos terán necesidades de acceso similares dentro do propio dominio. Por exemplo, os que necesiten acceder a unha determinada impresora.

Ámbito global: Só poden incluír outros grupos e contas que pertencen ao dominio no que estea definido o propio grupo.

Os membros deste tipo de grupos poden ter permisos sobre os recursos de calquera dominio dentro do bosque. Con todo, estes grupos non se replican fóra do seu propio dominio, de modo que, a asignación de dereitos e permisos que alberguen, non serán válidas noutros dominios do bosque.

Ámbito universal: Entre os seus membros poden atoparse contas ou grupos de calquera dominio do bosque, aos que se lles poden asignar permisos sobre os recursos de calquera dominio do bosque.

1.4.2.- Tipos de grupos

Existen dous tipos de grupos en Active Directory:

Grupos de distribución: Utilízanse en combinación con programas como Microsoft Exchange Server, para crear listas de distribución de correo electrónico.

Estes grupos non dispoñen de características de seguridade, polo que non poden aparecer nas listas de control de acceso discrecional (DACL, Discretionary Access Control Lists).

Grupos de seguridade: Permiten asignar permisos ás contas de usuario, de equipo e grupos sobre os recursos compartidos. Cos grupos de seguridade podemos:

- ✓ Asignar dereitos de usuario aos grupos de seguridade do Directorio Activo. Desta forma, podemos establecer que accións poden levar a cabo os seus membros dentro do dominio (ou do bosque). Como veremos despois, durante a instalación do Directorio Activo, créanse grupos de seguridade predeterminados que facilitan ao administrador a delegación de certos aspectos da administración (como, por exemplo, as copias de seguridade) noutros usuarios do sistema.

- ✓ Asignar permisos para recursos aos grupos de seguridade. O que nos permite definir quen accede a cada recurso e baixo que condicións (control total, só lectura, etc.) Tamén se establecen permisos de forma predeterminada sobre diferentes obxectos do dominio para ofrecer distintos niveis de acceso.

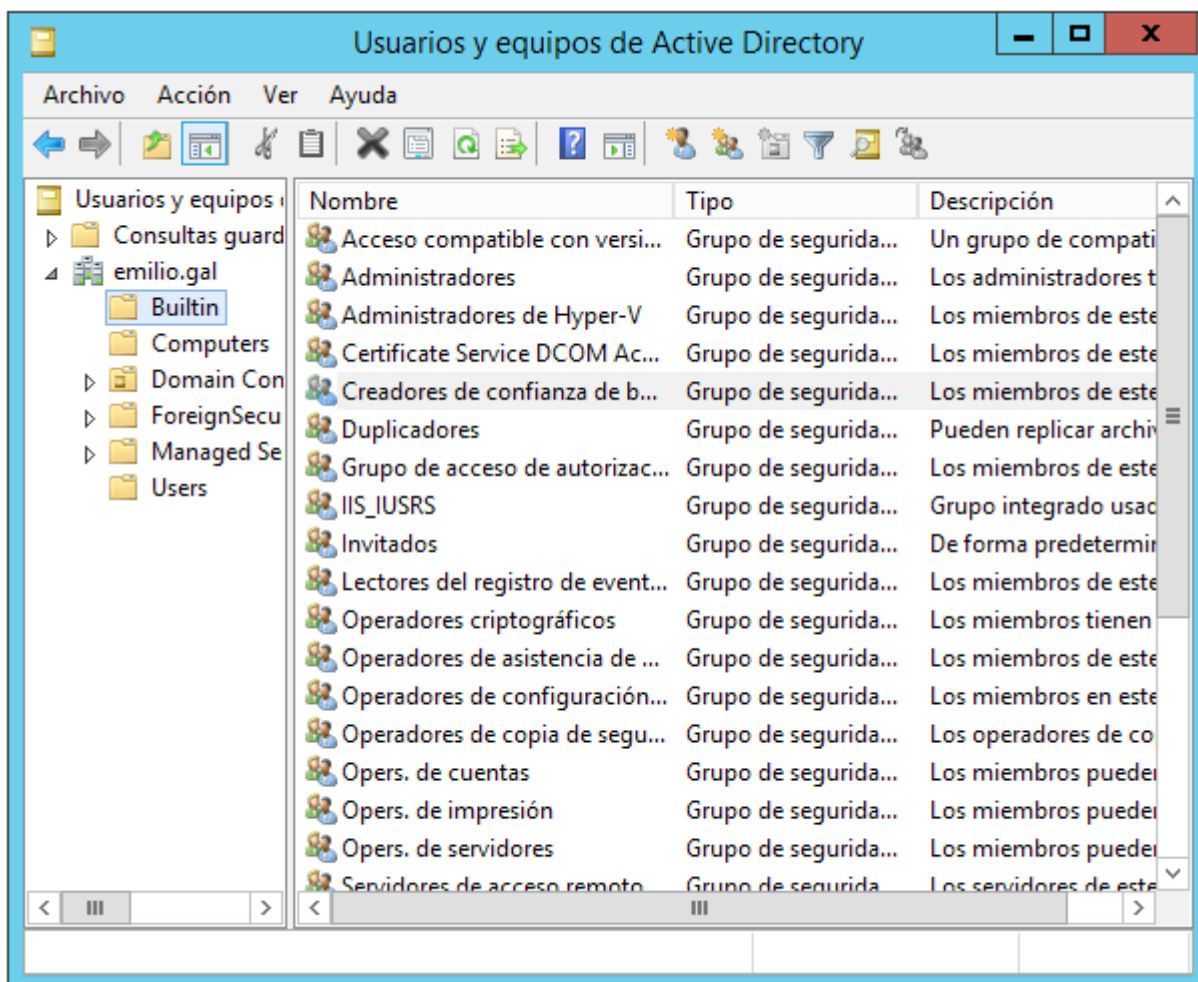
1.4.3.- Grupos integrados

Como mencionamos antes, durante a instalación do Directorio Activo créanse unha serie de grupos que poderemos utilizar para simplificar a asignación de dereitos e permisos a outras contas ou grupos.

Como veremos máis abaixo, os grupos adminístranse co complemento Usuarios e equipos de Active Directory. Cando executemos esta ferramenta, atoparemos os grupos predeterminados en dous colectores:

GRUPOS DO CONTEADOR BUILTIN

Os grupos predeterminados incluídos no colector **Builtin** teñen un ámbito local.



A continuación descríbense os grupos predeterminados situados no colector Integrados e indícanse os dereitos de usuario asignados a cada grupo.

Operadores de contas (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo poden crear, modificar e eliminar contas de usuarios, grupos e equipos que se atopan nos colectores Usuarios ou Equipos e nas unidades organizativas do dominio, excepto a unidade organizativa Controladores de dominio.

Os membros deste grupo non teñen permiso para modificar os grupos Administradores ou Administradores do dominio nin as contas dos membros dos devanditos grupos. Os membros deste grupo poden iniciar a sesión de forma local nos controladores do dominio e apagalos.

Como este grupo ten unha autoridade considerable no dominio, sexa prudente ao agregar usuarios.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Permitir o inicio de sesión local.
- ✓ Apagar o sistema.

Administradores (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo controlan por completo todos os controladores do dominio.

De forma predeterminada, os grupos Administradores do dominio e Administradores de organización son membros do grupo Administradores.

A conta Administrador é membro deste grupo de forma predeterminada. Posto que este grupo controla por completo o dominio, os usuarios serán agregados a el con cautela.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Ter acceso a este equipo desde a rede.
- ✓ Axustar as cotas de memoria dun proceso.
- ✓ Facer copia de seguridade de arquivos e directorios.
- ✓ Saltarse a comprobación de percorrido.
- ✓ Cambiar a hora do sistema.
- ✓ Crear un arquivo de paginación.
- ✓ Depurar programas.
- ✓ Habilitar a confianza para a delegación das contas de usuario e de equipo.
- ✓ Forzar o apagado desde un sistema remoto.
- ✓ Aumentar a prioridade de programación.
- ✓ Cargar e descargar controladores de dispositivo.
- ✓ Permitir o inicio de sesión local.
- ✓ Administrar o rexistro de auditoría e seguridade.
- ✓ Modificar valores de contorna do firmware.
- ✓ Facer perfil dun só proceso.

- ✓ Facer perfil do rendemento do sistema.
- ✓ Quitar un equipo dunha estación de axuste.
- ✓ Restaurar arquivos e directorios.
- ✓ Apagar o sistema.
- ✓ Tomar posesión de arquivos e outros obxectos.

Os usuarios e grupos que integran o grupo Administradores son:

- ✓ Administrador.
- ✓ Administradores da empresa (grupo de seguridade universal).
- ✓ Administradores do dominio (grupo de seguridade global).

Operadores de copia de seguridade (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo poden realizar copias de seguridade e restaurar todos os arquivos nos controladores do dominio, independentemente dos seus permisos individuais neses arquivos. Os Operadores de copia de seguridade tamén poden iniciar a sesión nos controladores de dominio e apagalos. Este grupo non ten ningún membro predeterminado. Como este grupo ten unha autoridade considerable nos controladores de dominio, ao agregar usuarios a este grupo hai que ser prudente.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Facer copia de seguridade de arquivos e directorios.
- ✓ Permitir o inicio de sesión local.
- ✓ Restaurar arquivos e directorios.
- ✓ Apagar o sistema.

Convidados (Grupo de seguridade e grupo local de dominio).

De forma predeterminada, os invitados teñen o mesmo acceso que os membros do grupo Usuarios, agás que a conta de invitado ten máis restricións aínda.

Este grupo non ten dereitos de usuario predeterminados.

Os usuarios e grupos que integran o grupo Convidados son o grupo **Convidados do dominio** (grupo de seguridade global) e a conta **Convidado** (que está deshabilitada de forma predeterminada).

Creadores de confianza de bosque de entrada (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden crear confianza de bosque de entrada unidireccionales no dominio raíz do bosque. Por exemplo, os membros deste grupo que residen no Bosque A poden crear unha confianza de bosque de entrada unidireccional desde o Bosque B.

Esta confianza de bosque de entrada unidireccional permite aos usuarios do Bosque A ter acceso a recursos situados no Bosque B.

Os membros deste grupo dispoñen do permiso Crear confianza de bosque de entrada no dominio raíz do bosque.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Operadores de configuración de rede (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden modificar a configuración TCP/IP, así como renovar e liberar as direccións TCP/IP nos controladores do dominio.

Este grupo non ten ningún membro predeterminado.

Este grupo non ten dereitos de usuario predeterminados.

Usuarios do Monitor de sistema (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden supervisar os contadores de rendemento nos controladores do dominio, tanto de forma local como desde clientes remotos, sen ser membros dos grupos Administradores ou Usuarios do rexistro de rendemento.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Usuarios do rexistro de rendemento (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden administrar os contadores de rendemento, os rexistros e as alertas dos controladores do dominio, tanto de forma local como desde clientes remotos, sen ser membros do grupo Administradores.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Acceso compatible con versiones anteriores a Windows 2000 (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo teñen acceso de lectura en todos os usuarios e grupos do dominio. Este grupo proporciónase para garantir a compatibilidade con versións anteriores nos equipos con Windows NT 4.0 e anteriores.

De forma predeterminada, **a identidade especial Todos** é membro deste grupo. Agregaranse usuarios a este grupo unicamente se se executan en Windows NT 4.0 ou versións anteriores.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Ter acceso a este equipo desde a rede.
- ✓ Saltarse a comprobación de percorrido.

Este grupo intégrano:

- ✓ Usuarios autenticados.

Operadores de impresión (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden administrar, crear, compartir e eliminar impresoras que están conectadas aos controladores do dominio.

Tamén poden administrar obxectos de impresora de Active Directory no dominio. Os membros deste grupo poden iniciar a sesión de forma local nos controladores do dominio e apagalos.

Posto que os membros deste grupo poden cargar e descargar controladores de dispositivos en todos os controladores do dominio, os usuarios agregaranse con cautela.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Permitir o inicio de sesión local.
- ✓ Apagar o sistema.

Este grupo non ten ningún membro predeterminado.

Usuarios de escritorio remoto (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden iniciar a sesión nos controladores do dominio de forma remota.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Duplicadores (Grupo de seguridade e grupo local de dominio).

Este grupo admite funcións de replicación de directorio e o Servizo de replicación de arquivos utilízao nos controladores do dominio.

Este grupo non ten ningún membro predeterminado. Non agregar usuarios a este grupo.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Operadores de servidores (Grupo de seguridade e grupo local de dominio).

Nos controladores de dominio, os membros deste grupo poden iniciar sesións interactivas, crear e eliminar recursos compartidos, iniciar e deter varios servizos, facer copias de seguridade e restaurar arquivos, formatear o disco duro e apagar o equipo.

Dado que este grupo ten moita importancia para os controladores de dominio, os usuarios serán agregados con cautela.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Facer copia de seguridade de arquivos e directorios.
- ✓ Cambiar a hora do sistema.
- ✓ Forzar o apagado desde un sistema remoto.
- ✓ Permitir o inicio de sesión local.
- ✓ Restaurar arquivos e directorios.
- ✓ Apagar o sistema.

Este grupo non ten ningún membro predeterminado.

Usuarios (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo poden realizar as tarefas máis habituais, como executar aplicacións, utilizar impresoras locais e de rede, así como bloquear o servidor.

Todas as contas de usuario que se crean no dominio son membros deste grupo.

Este grupo non ten dereitos de usuario predeterminados.

Os usuarios e grupos que integran o grupo Usuarios son:

- ✓ O grupo Usuarios do dominio (grupo de seguridade global).
- ✓ Usuarios autenticados.
- ✓ Interactivo (INTERACTIVE).

Administradores de Hyper-V (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo teñen acceso completo e sen restricións a todas as características de Hyper-V.

- ✓ Este grupo non ten ningún membro predeterminado.

Certificate Service DCOM Access (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo pódense conectar a entidades de certificación na empresa.

- ✓ Este grupo non ten ningún membro predeterminado.

Grupo de acceso de autorización de Windows (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo teñen acceso ao atributo Token Groups Global And Universal calculado en obxectos de usuario.

- ✓ Este grupo ten como membro ao usuario Enterprise Domain Controllers.

ISS_IUSRS (Grupo de seguridad e grupo local de dominio).

Grupo integrado por Internet Information Services (Servizos de información de internet).

- ✓ Este grupo ten como membro ao usuario IUSR.

Lectores de rexistro de eventos (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden ler rexistros de eventos do equipo local.

- ✓ Este grupo non ten ningún membro predeterminado.

Operadores criptográficos (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo teñen autorización para realizar operacións criptográficas.

- ✓ Este grupo non ten ningún membro predeterminado.

Operadores de asistencia de control de acceso (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden consultar de forma remota os atributos de autorización e os permisos para os recursos deste equipo.

- ✓ Este grupo non ten ningún membro predeterminado.

Servidores de acceso remoto RDS (Grupo de seguridad e grupo local de dominio).

Os servidores deste grupo permiten aos usuarios de programas Remote App e escritorios virtuales persoais obter acceso a estes recursos.

En implementacións con conexión a Internet, estes servidores adóitanse implementar nunha rede perimentral.

Este grupo debe encherse en servidores que executen o Axente de conexión a Escritorio Remoto. Os servidores de Porta de ligazón de Escritorio remoto e de Acceso Web de Escritorio remoto usados na implementación deben formar parte deste grupo.

- ✓ Este grupo non ten ningún membro predeterminado.

Servidores de administración RDS (Grupo de seguridad e grupo local de dominio).

Os servidores deste grupo poden realizar accións administrativas rutinarias en servidores que executen Servizos de Escritorio Remoto.

Este grupo debe encherse en todos os servidores dunha implementación de Servizos de Escritorio Remoto. Os servidores que executen o servizo de Administración central de RDS deben incluírse neste grupo.

- ✓ Este grupo non ten ningún membro predeterminado.

Servidores de extremo RDS (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo executan máquinas virtuales e hospedan sesións onde se executan os programas Remote App e os escritorios virtuais persoais dos usuarios.

Este grupo debe encherse nos servidores que executen o Axente de conexión a Escritorio remoto.

Os servidores hosts de sesión de Escritorio remoto e de virtualización de Escritorio Remoto usados na implementación deben formar parte deste grupo.

- ✓ Este grupo non ten ningún membro predeterminado.

Servidores de licenzas de Terminal Server (Grupo de seguridad e grupo local de dominio).

Os membros deste grupo poden actualizar as contas de usuario en Active Directory con información sobre a emisión de licenzas con fins de seguimento e informes de uso de licenzas CAL por usuario do TS.

- ✓ Este grupo non ten ningún membro predeterminado.

Usuarios COM distribuídos (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo poden iniciar, activar e usar obxectos de COM distribuído neste equipo.

- ✓ Este grupo non ten ningún membro predeterminado.

Usuarios de administración remota (Grupo de seguridade e grupo local de dominio).

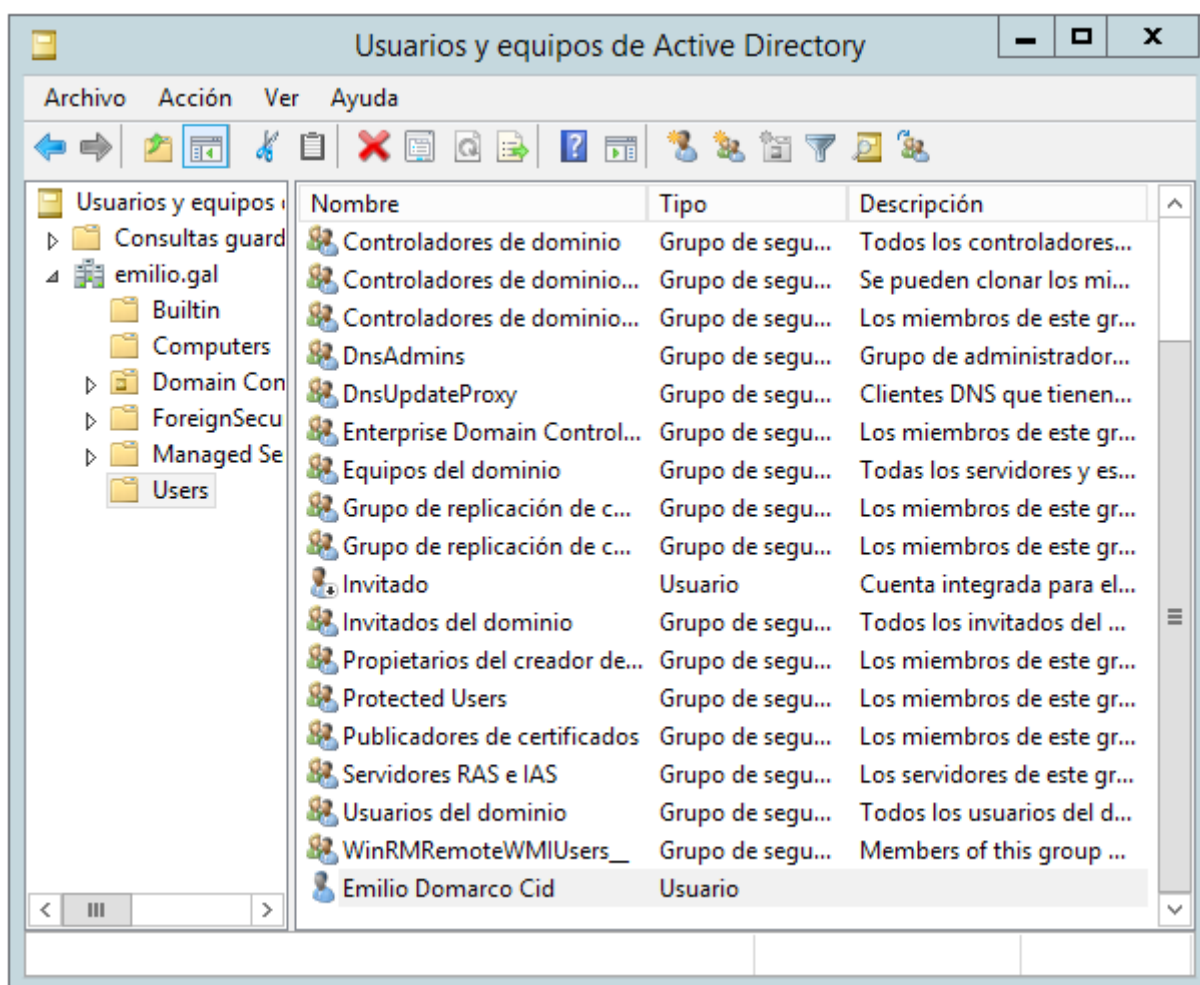
Os membros deste grupo poden acceder aos recursos de WMI mediante protocolos de administración (como WS-Management a través do servizo de Administración remota de Windows). Isto aplícase só ao espazo de nomes de WMI que conceden acceso ao usuario.

- ✓ Este grupo non ten ningún membro predeterminado.

GRUPOS DO COLECTOR USERS

A continuación descríbense os grupos predeterminados situados nos colector Usuarios e indícanse os dereitos de usuario asignados a cada grupo.

No colector Users podemos atopar grupos predeterminados que teñen tanto ámbito local como global.



Publicadores de certificados (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo teñen permitida a publicación de certificados para usuarios e equipos.

Este grupo non ten ningún membro predeterminado, pero se é membro do grupo de replicación de contrasinal RODC denegada (Grupo de seguridade e do domino local).

- ✓ Este grupo non ten dereitos de usuario predeterminados.

DnsAdmins (Grupo de seguridade e grupo local de dominio).

Este grupo instálase xunto ao servizo DNS. Os membros deste grupo teñen acceso administrativo ao Servidor DNS.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

DnsUpdateProxy (Grupo de seguridade e grupo global).

Este grupo instálase xunto ao servizo DNS. Os membros deste grupo son clientes DNS que poden realizar actualizacións dinámicas en lugar doutros clientes, como os servidores DHCP.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Administradores de dominio (Grupo de seguridade e grupo global).

Os membros deste grupo controlan o dominio por completo. De forma predeterminada, este grupo pasa a ser membro do grupo Administradores (Grupo de seguridade local do colector Built-in) en todos os controladores, estacións de traballo e servidores membros do dominio no momento en que se une ao dominio e do grupo de replicación de contrasinal RODC denegada.

De forma predeterminada, a conta Administrador é membro deste grupo. Posto que o grupo controla o dominio por completo, débense agregar os usuarios con cautela.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Ter acceso a este equipo desde a rede.
- ✓ Axustar as cotas de memoria dun proceso.
- ✓ Facer copia de seguridade de arquivos e directorios.
- ✓ Saltarse a comprobación de percorrido.
- ✓ Cambiar a hora do sistema.
- ✓ Crear un arquivo de paginación.

- ✓ Depurar programas.
- ✓ Habilitar a confianza para a delegación das contas de usuario e de equipo.
- ✓ Forzar o apagado desde un sistema remoto.
- ✓ Aumentar a prioridade de programación.
- ✓ Cargar e descargar controladores de dispositivo.
- ✓ Permitir o inicio de sesión local.
- ✓ Administrar o rexistro de auditoría e seguridade.
- ✓ Modificar valores de contorna do firmware.
- ✓ Facer perfil dun só proceso.
- ✓ Facer perfil do rendemento do sistema.
- ✓ Quitar un equipo dunha estación de axuste.
- ✓ Restaurar arquivos e directorios.
- ✓ Apagar o sistema.
- ✓ Tomar posesión de arquivos e outros obxectos.

Equipos do dominio (Grupo de seguridade e grupo global).

Este grupo contén todas as estacións de traballo e os servidores unidos ao dominio. De forma predeterminada, todas as contas de equipo creadas pasan a ser membros deste grupo automaticamente.

- ✓ Este grupo non ten dereitos de usuario predeterminados.

Controladores de dominio (Grupo de seguridade e grupo global).

Este grupo contén todos os controladores do dominio. Este grupo intégrase como membro no grupo de replicación de contrasinal RODC denegada.

- ✓ Este grupo non ten dereitos de usuario predeterminados.

Invitados do dominio (Grupo de seguridade e grupo global).

Este grupo contén todos os invitados do dominio.

- ✓ Neste grupo intégrase a conta de invitado, inicialmente deshabilitada.
- ✓ O grupo Convidados do Dominio pasa a se membro do grupo Convidados (grupo de seguridade local do colector Builtin).

Usuarios do dominio (Grupo de seguridade e grupo global).

Este grupo contén todos os usuarios do dominio. De forma predeterminada, todas as contas de usuario creadas no dominio pasan a ser membros deste grupo

automaticamente.

Este grupo pódese utilizar para representar todos os usuarios do dominio.

Por exemplo, se se desexa que todos os usuarios do dominio teñan acceso a unha impresora, pódense asignar permisos para a impresora a este grupo (ou se pode agregar o grupo Usuarios do dominio nun grupo local do servidor de impresoras que dispoña dos permisos para utilizala).

- ✓ Este grupo intégrase no grupo Convidados (Grupo de seguridade local do colector Builtin).
- ✓ Este grupo non ten dereitos de usuario predeterminados.

Administradores de empresas (Grupo de seguridade e grupo universal).

Os membros deste grupo controlan por completo todos os dominios do bosque. De forma predeterminada, este grupo é un membro do grupo Administradores (Grupo de seguridade local do colector Builtin) en todos os controladores de dominio do bosque e do grupo de replicación de contrasinal RODC denegada.

De forma predeterminada, a conta Administrador é membro deste grupo. Dado que este grupo controla o bosque por completo, débense agregar os usuarios con cautela.

Os dereitos dos usuarios predeterminados neste grupo son:

- ✓ Ter acceso a este equipo desde a rede.
- ✓ Axustar as cotas de memoria dun proceso.
- ✓ Facer copia de seguridade de arquivos e directorios.
- ✓ Saltarse a comprobación de percorrido.
- ✓ Cambiar a hora do sistema.
- ✓ Crear un arquivo de paginación.
- ✓ Depurar programas.
- ✓ Habilitar a confianza para a delegación das contas de usuario e de equipo.
- ✓ Forzar o apagado desde un sistema remoto.
- ✓ Aumentar a prioridade de programación.
- ✓ Cargar e descargar controladores de dispositivo.
- ✓ Permitir o inicio de sesión local.
- ✓ Administrar o rexistro de auditoría e seguridade.
- ✓ Modificar valores de contorna do firmware.
- ✓ Facer perfil dun só proceso.
- ✓ Facer perfil do rendemento do sistema.
- ✓ Quitar un equipo dunha estación de axuste.
- ✓ Restaurar arquivos e directorios.
- ✓ Apagar o sistema.
- ✓ Tomar posesión de arquivos ou outros obxectos.

Propietarios do creador de directiva de grupo (Grupo de seguridade e grupo global).

Os membros deste grupo poden modificar a Directiva de grupo no dominio. De forma predeterminada, a conta Administrador é membro deste grupo.

Como este grupo ten unha autoridade considerable no dominio, débese ser prudente ao agregar usuarios. Este grupo agrégase ao grupo de replicación de contrasinal RODC denegada.

- ✓ Este grupo non ten dereitos de usuario predeterminados.

Servidores NIVEIS e IAS (Grupo de seguridade e grupo local de dominio).

Os servidores deste grupo teñen permitido o acceso ás propiedades de acceso remoto dos usuarios.

- ✓ Este grupo non ten dereitos de usuario predeterminados.

Administradores de esquema (Grupo de seguridade e grupo universal).

Os membros deste grupo poden modificar o esquema de Active Directory. Este grupo intégrase no grupo de replicación de contrasinal RODC denegada.

De forma predeterminada, a conta Administrador é membro deste grupo. Como este grupo ten unha autoridade considerable no bosque, débese ser prudente ao agregar usuarios.

- ✓ Este grupo non ten dereitos de usuario predeterminados.

Enterprise Domain Controllers de só lectura (Grupo de seguridade e grupo universal).

Os membros deste grupo son controladores de dominio de só lectura na empresa.

- ✓ Este grupo non ten ningún membro predeterminado.

Controladores de dominio clonables (Grupo de seguridade e grupo local).

Pódense clonar os membros do grupo que sexan controladores de dominio.

- ✓ Este grupo non ten ningún membro predeterminado.

Controladores de dominio de só lectura (Grupo de seguridade e grupo global).

Os membros deste grupo son controladores de dominio de só lectura no dominio.

- ✓ Este grupo non ten ningún membro predeterminado.
- ✓ Este grupo intégrase no grupo de replicación de contrasinal RODC denegada.

Protected Users (Grupo de seguridade e grupo global).

Os membros deste grupo teñen proteccións adicionais contra a seguridade de autenticación.

- ✓ Este grupo non ten ningún membro predeterminado.

Grupo de replicación de contrasinal RODC denegada (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo non poden replicar os contrasinais a ningún controlador de dominio de só lectura no dominio.

Este grupo ten como membros predeterminados:

- ✓ Administradores de empresa.
- ✓ Administradores de esquema.
- ✓ Administradores do dominio.
- ✓ Controladores de dominio.
- ✓ Controladores de dominio de só lectura.
- ✓ Propietarios do creador de directivas de grupo.
- ✓ Publicadores de certificados.

Grupo de replicación de contrasinal RODC permitida (Grupo de seguridade e grupo local de dominio).

Os membros deste grupo poden replicar os contrasinais a todos os controladores de dominio de só lectura no propio dominio.

- ✓ Este grupo non ten ningún membro predeterminado.

WinRMRemoteWMIUsers_ (Grupo de seguridade e grupo local de dominio).

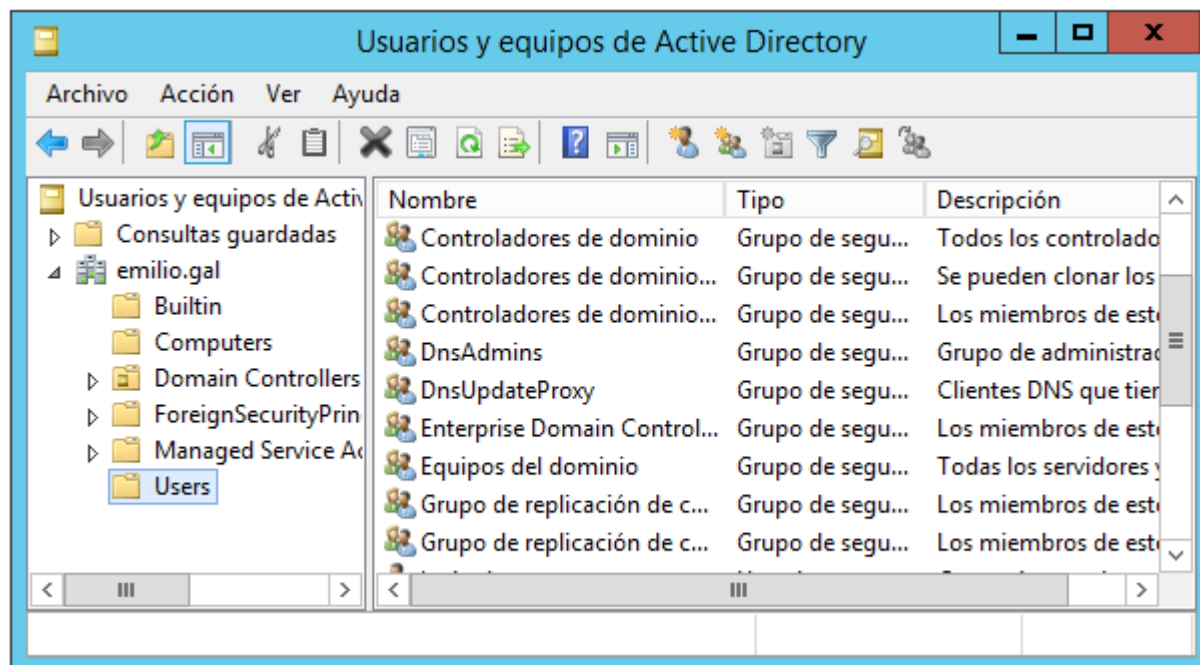
Os membros deste grupo poden acceder aos recursos de WMI cos protocolos d xestión (como WS-Management a través do servizo de administración remota de Windows).

Isto aplícase só aos espazos de nomes WMI que conceden acceso ao usuario.

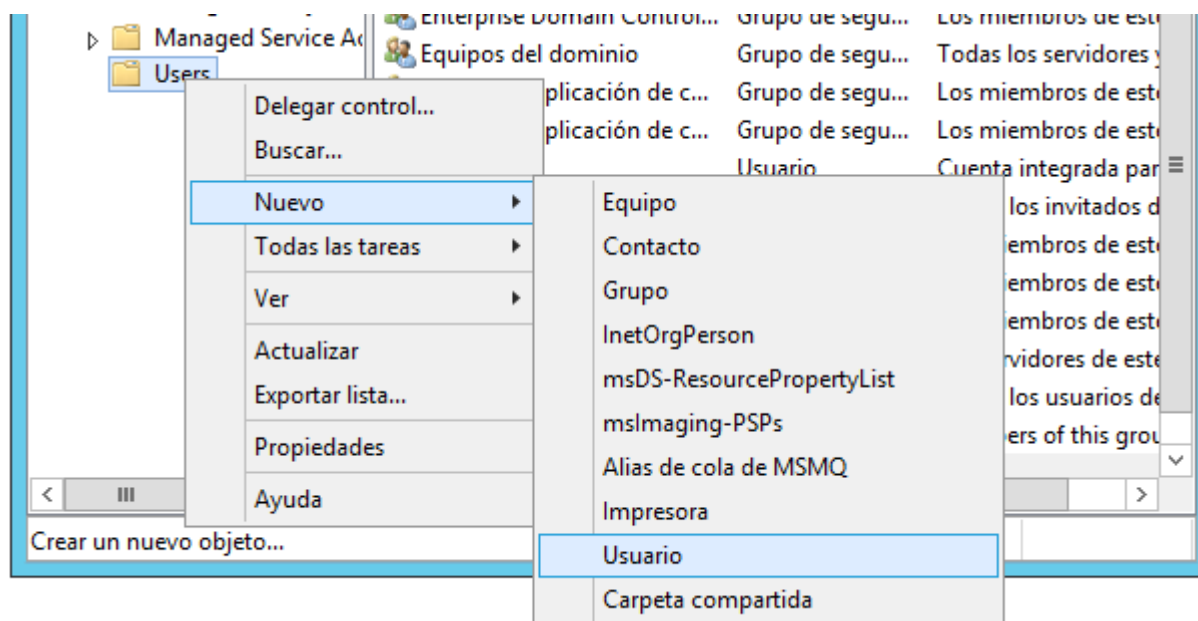
- ✓ Este grupo non ten ningún membro predeterminado.

2.- Crear unha Conta de Usuario

Para crear un usuario novo do dominio o primeiro que teremos que facer será entrar abrir o menú de “Herramientas” -> “Usuarios y equipos de Active Directory” e no noso dominio ir ó apartado de Users.



Faremos clic co botón dereito sobre Users e aparece o seguinte menú onde elixiemos **Nuevo** e, a continuación **Usuario**



Veremos que aparece a ventana **Nuevo objeto: Usuario**, que é o asistente de creación de usuarios.

No primeiro paso, teremos que encher os datos do usuario: O seu Nome, Apelidos e Iniciais. Con eles formarase o campo Nome completo

A continuación, escribiremos o Nome de inicio de sesión de usuario que, en realidade, componse de dous partes: o nome propiamente devandito e o sufijo, que o eliximos dunha lista desplegable. Se dispomos de varios dominios na rede, na lista aparecerá unha entrada por cada un deles.

Por último, o campo Nome de inicio de sesión de usuario (anterior a Windows 2000) ten como obxecto permitir que se conecten ao dominio clientes que executen Windows 95, Windows 98 ou Windows NT.

Cuando rematemos de encher tódolos datos pulsaremos no botón **Siguiete**.

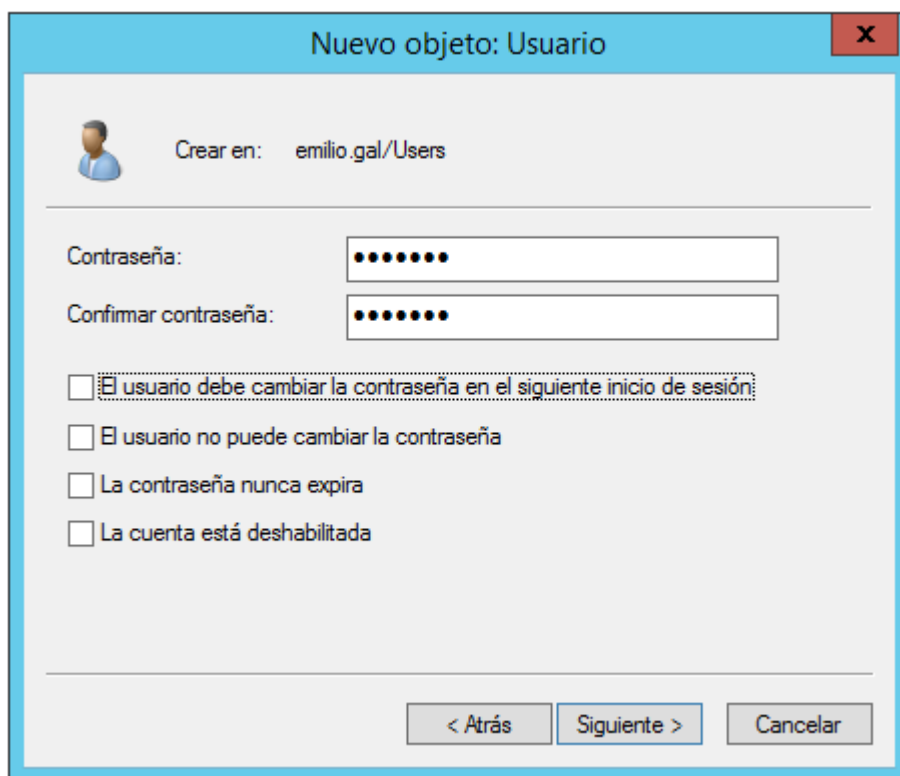
A continuación, teremos que escribir un contrasinal para o usuario, que deberá cumprir cos requirimentos de seguridade do sistema operativo.

É dicir, que de forma predeterminada deberá ter un mínimo de seis caracteres de longo e conter caracteres de, polo menos, tres do catro conxuntos seguintes:

- ✓ Maiúsculas do alfabeto inglés.
- ✓ Minúsculas do alfabeto inglés.
- ✓ Díxitos decimais (do 0 ao 9).
- ✓ Caracteres non alfanuméricos.

Ademais, na parte inferior da ventana dispomos de catro opcións:

- ✓ **O usuario debe cambiar o contrasinal no seguinte inicio de sesión:** Se o marcamos (opción por defecto), obrigaremos ao usuario a cambiar o contrasinal que estamos a escribir a próxima vez que inicie sesión no dominio. Desta forma, o usuario estará seguro de que ninguén máis coñece o seu contrasinal.
- ✓ **O usuario non pode cambiar o contrasinal:** Ao contrario que a anterior, esta opción impide que o usuario poida cambiar o seu contrasinal en ningún momento. Esta opción pode resultar interesante para que o administrador manteña o control total sobre algunha conta temporal ou de invitado.
- ✓ **O contrasinal nunca expira:** fai que o contrasinal non expire no prazo que estableza o sistema operativo. Microsoft recomenda que as contas de servizo teñan esta opción habilitada e usen contrasinais seguros
- ✓ **A conta está deshabilitada:** Mentres esta opción estea habilitada, o usuario non poderá iniciar sesión no sistema.



Nuevo objeto: Usuario

Crear en: emilio.gal/Users

Contraseña: [masked]

Confirmar contraseña: [masked]

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ El usuario no puede cambiar la contraseña

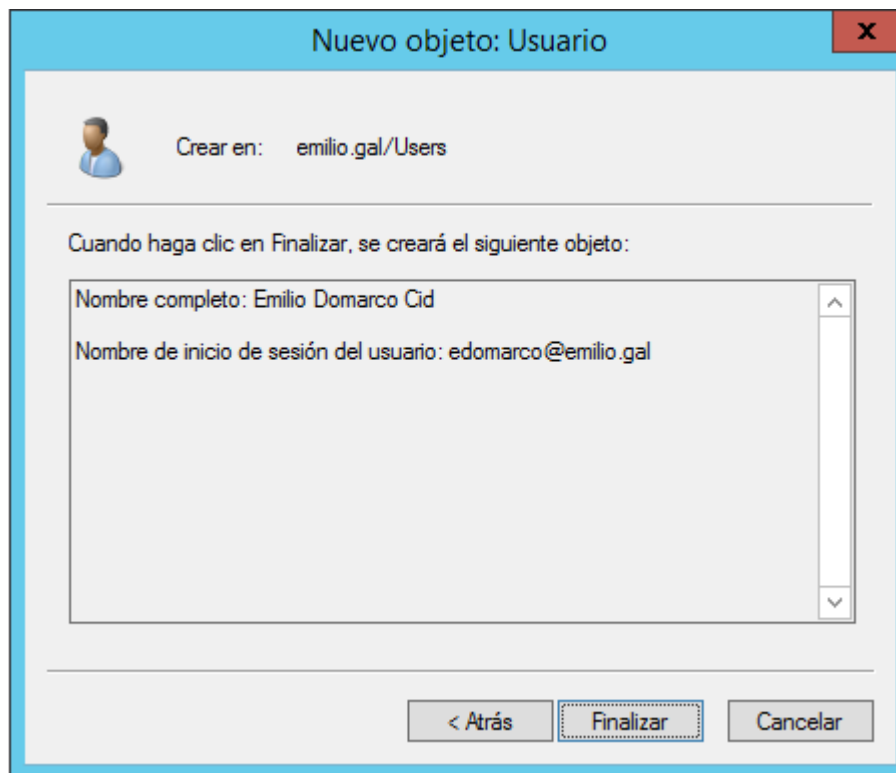
☐ La contraseña nunca expira

☐ La cuenta está deshabilitada

< Atrás Siguiente > Cancelar

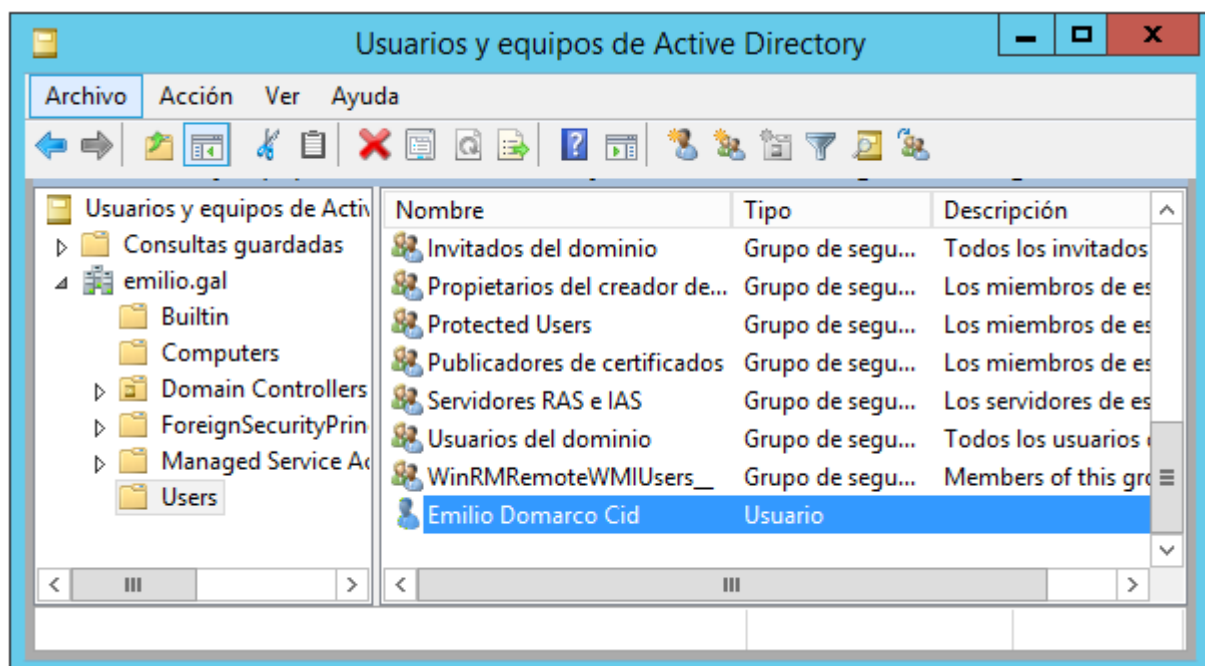
Cando completemos os datos necesarios neste paso, faremos clic sobre o botón **Seguiente**.

Como é habitual en todas as ferramentas de configuración de Windows Server 2012 R2, o asistente móstranos un resumo dos datos introducidos antes de crear a conta de maneira efectiva.



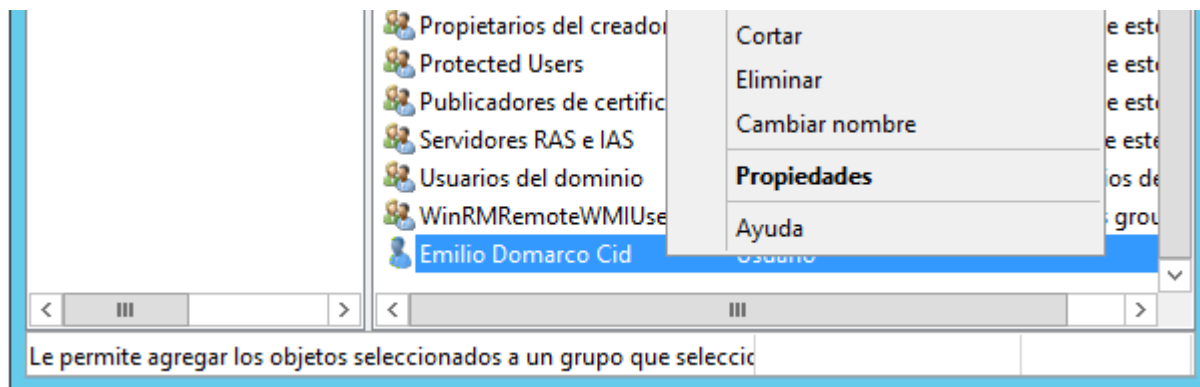
Se todo é correcto, faremos clic sobre o botón **Finalizar**.

Se todo é correcto, a ventana **Nuevo objeto: Usuario** pecharase e volveremos ver a ventana Usuarios y equipos de Active Directory onde poderemos ver a conta que acabamos de crear.

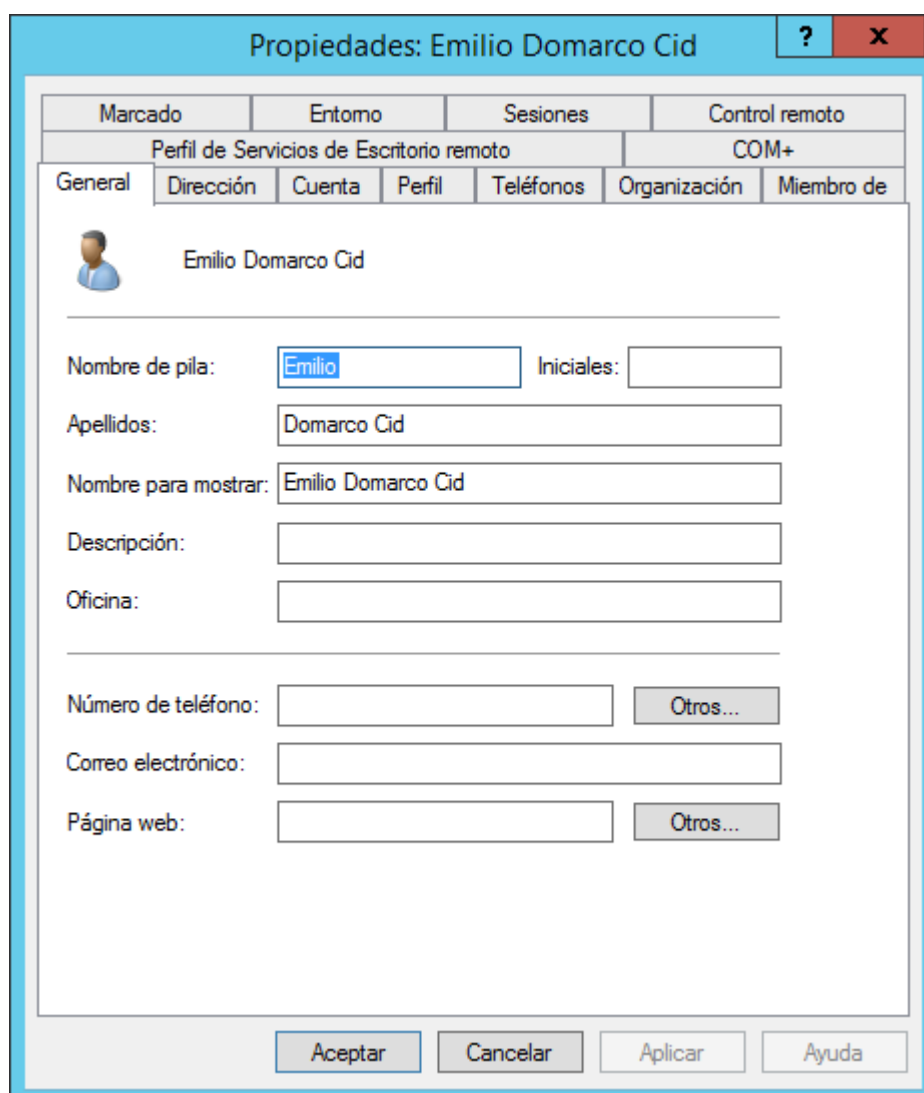


3.- Propiedades das contas de usuarios

Para acceder ás propiedades dun usuario e configuralas debemos facer clic co botón dereito do rato sobre o usuario e picar en **Propiedades**



o que nos mostra a ventá de Propiedades do usuario, que podemos ver na seguinte imaxe...



Nesta ventá temos diferentes pestanas con varios atributos cada unha que podemos configurar do usuario:

- ✓ **Pestana Conta**: nesta pestana temos os atributos de Conta. Estas propiedades inclúen os nomes de logon, o contrasinal e diferentes parámetros de configuración da conta de usuario.
- ✓ **Pestanas Xeneral, Dirección, Teléfonos e Organización**.
 - ✓ **A pestana General** permite especificar a información persoal do usuario como nome, dirección, teléfono, etc.
 - ✓ **As pestanas Dirección e Teléfonos** permiten incluír información detallada de contacto.
 - ✓ **A pestana Organización** a información do usuario na empresa como o departamento, o nome de empresa, etc.
- ✓ **Pestana Perfil**. Nesta pestana podemos configurar o path de traballo por defecto do usuario así como asignarlle un script de inicio de sesión, unha carpeta persoal e unha unidade de rede que apunte a este ou outro servidor.
- ✓ **Pestana Membro de**: nesta pestana indicamos a que grupos de seguridade pertence o usuario e comprobamos a cuales pertence xa. A pertenza a grupos é importante xa que se utiliza para dar permisos aos usuarios aos recursos de rede en vez de asignar permisos directamente aos usuarios.
- ✓ **Pestanas Perfil de Escritorio Remoto, Ámbito, Control Remoto e Sesións**. Todas estas pestanas son relativas á configuración de acceso remoto do usuario vía Terminal Service.
- ✓ **Pestana Marcado**: nesta pestana podemos habilitar un usuario para que acceda remotamente á rede a través dunha tecnoloxía de acceso remoto como o marcado por MODEM e VPN e configuramos como se conectará.
- ✓ **Pestana COM+**: aquí podemos habilitar un usuario para usar COM+

A maioría destas propiedades deben modificarse de xeito individual para cada usuario polo que se temos que modificar un gran número de usuarios non temos outro remedio que ir un a un.

Non obstante hai unha serie de propiedades que admiten a selección múltiple de usuarios para modificalas nun só paso en todos os usuarios seleccionados.

Para facelo, seleccionamos todos os usuarios que desexemos e sobre un deles picamos co botón dereito do rato e picamos en Propiedades para abrir as propiedades dos usuarios.

Ao ter varios usuarios seleccionados só teremos habilitadas para cambiar as propiedades que admiten a selección múltiple.

Estas propiedades son:

- ✓ **Pestana Xeral**: Descrición, Oficina, Número de Teléfono, Fax, Páxina Web, Correo Electrónico.
- ✓ **Pestana Conta**: Sufixo UPN, Horas de Logon, Restricións de máquina (máquinas nas que un usuario pode iniciar sesión), todas as opcións de conta, Data de Expiración da conta.
- ✓ **Pestana Dirección**: Rúa, Cidade, Provincia, Código Postal, País
- ✓ **Pestana Perfil**: Ruta de perfil, Script de Inicio de sesión e Carpeta persoal
- ✓ **Pestana Organización**: Nome de empresa, Departamento, Compañía, Administrador.

A continuación imos comentar as pestanas máis importantes:

3.1.- Pestanas General e Dirección.

Nestas pestanas imos ir cubrindo os datos persoais do usuario, que aínda que pareza que non teñen importancia valeranos nunha organización grande para poder buscar un usuario en concreto.

Propiedades: Emilio Domarco Cid

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

Emilio Domarco Cid

Nombre de pila: Emilio Iniciales:

Apellidos: Domarco Cid

Nombre para mostrar: Emilio Domarco Cid

Descripción: Conta de usuario normal de Emilio

Oficina: IES A Sangriña

Número de teléfono: 986 1112233 Otros...

Correo electrónico: emilio.domarco.cid@gmail.com

Página web: www.emilio.com Otros...

Propiedades: Emilio Domarco Cid

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

Calle: Rúa Nova

Apartado postal: 12345

Ciudad: Allariz

Estado o provincia: Ourense

Código postal: 32660

País o región: España

3.2.- Pestana Cuenta

Propiedades: Emilio Domarco Cid

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:
edomarco @emilio.gal

Nombre de inicio de sesión de usuario (anterior a Windows 2000):
EMILIO\ edomarco

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

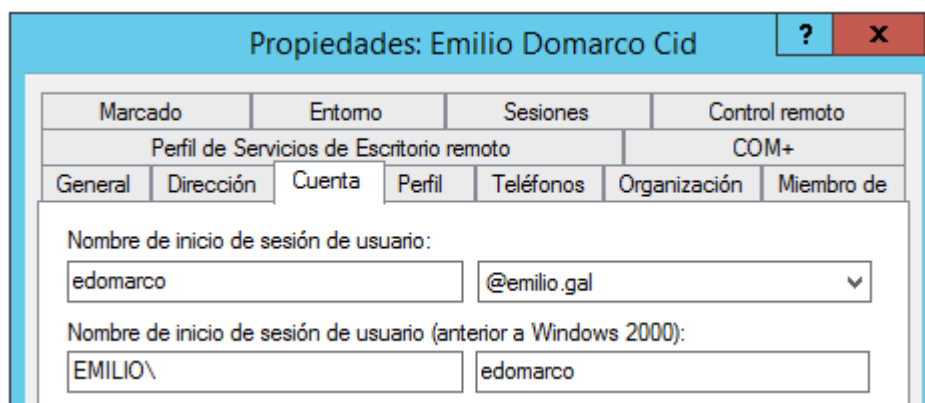
☐ Fin de: lunes , 2 de noviembre de 2015

NOME DE INICIO DE SESIÓN

É o nome co que o usuario iniciará sesión nun dominio de active Directory.

A lista da dereita mostra os sufixos do nome principal de usuario (UPN) que se poden empregar para crear o nome de inicio de sesión de usuario.

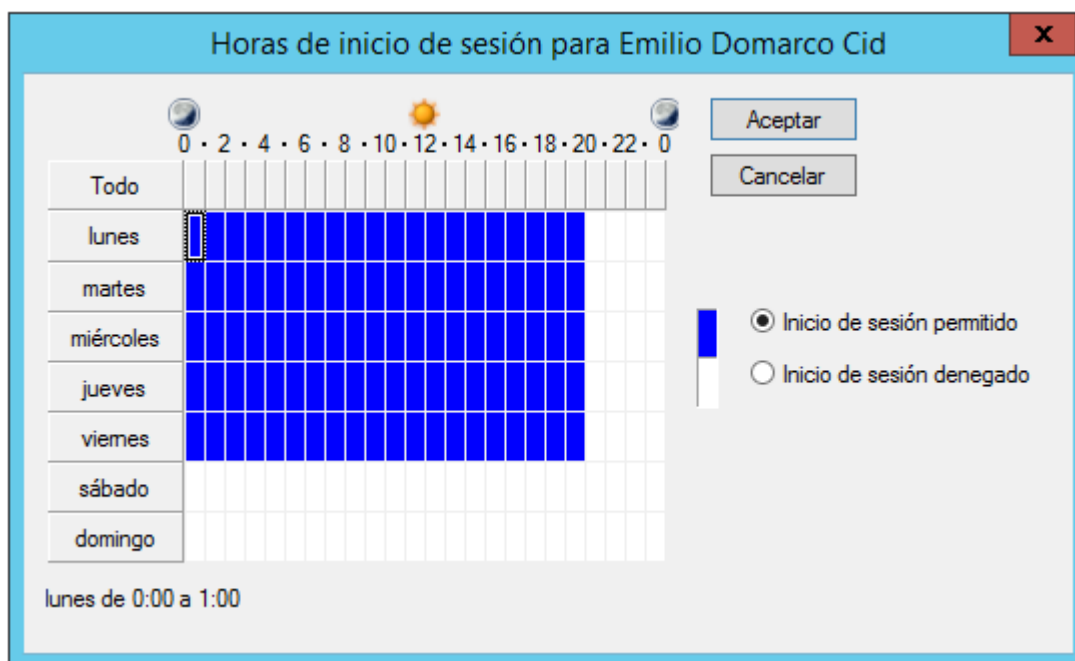
A lista contén o nome completo do Sistema de nomes de dominio (DNS) do dominio actual, o nome DNS completo do dominio raíz do bosque actual.



HORAS DE INICIO DE SESIÓN

Faremos clic neste botón para cambiar as horas durante as cuales o usuario pode iniciar sesión no dominio. De xeito predeterminado o inicio de sesión no dominio permítese as 24 horas do día durante os 7 días da semana.

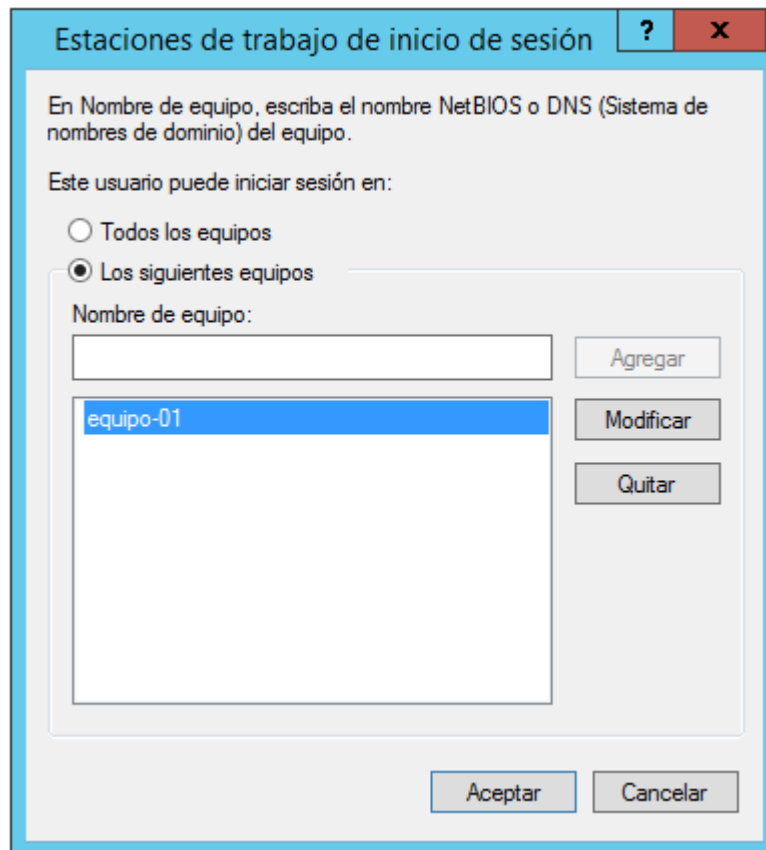
Simplemente iremos marcando as horas de inicio de sesión permitidas (en azul) e as horas de inicio de sesión denegadas (en branco)



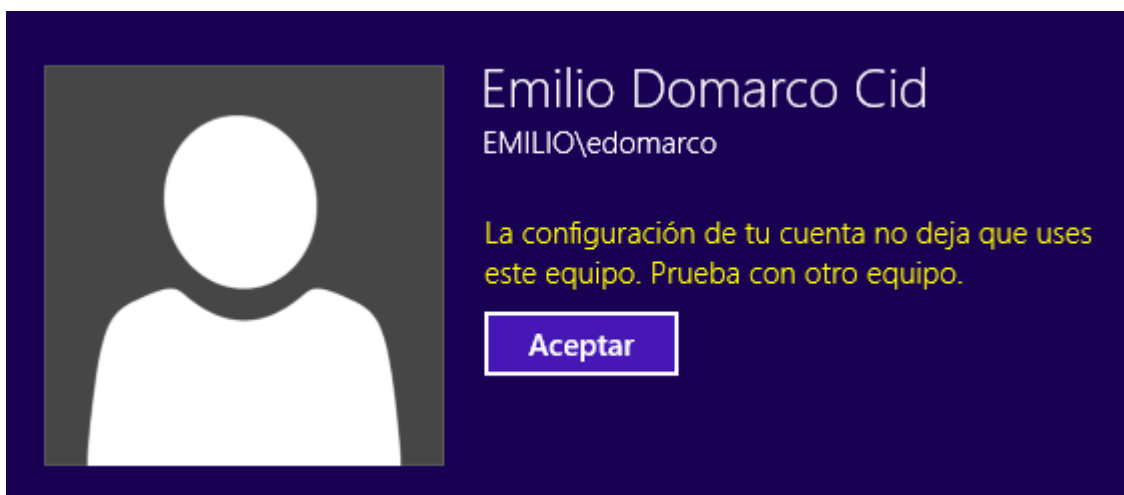
INICIAR SESIÓN EN

De xeito predeterminado un usuario pode iniciar sesión en calquera ordenador que esté engadido ó dominio.

Marcando a opción de **Los siguientes equipos** poderemos seleccionar os equipos onde este usuario pode iniciar sesión, non sendo posible iniciala noutros que non estén na lista.

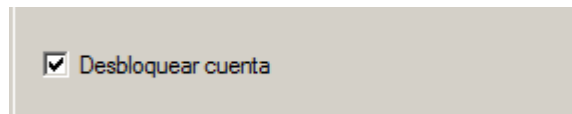


Se o intentamos noutro equipo (neste caso en equipo-02) que non estea na lista daranos o seguinte erro:



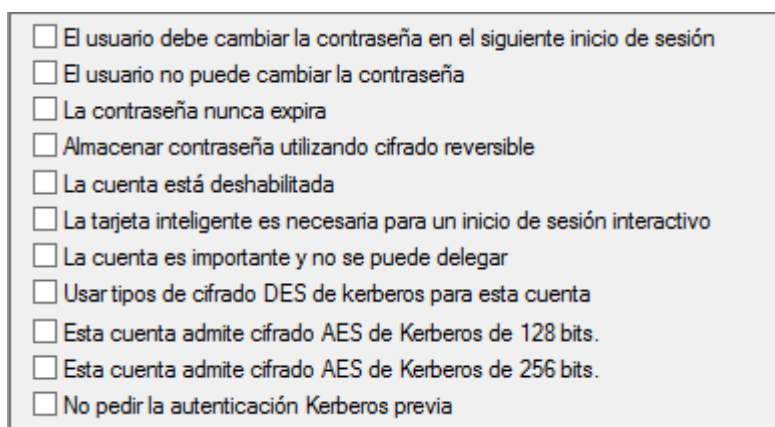
DESBLOQUEAR CUENTA

Permite desbloquear contas de usuario bloqueadas porque se produciron demasiados erros ó intentar iniciar a sesión.

A screenshot of a Windows Server management console showing a single checkbox labeled 'Desbloquear cuenta' which is checked.

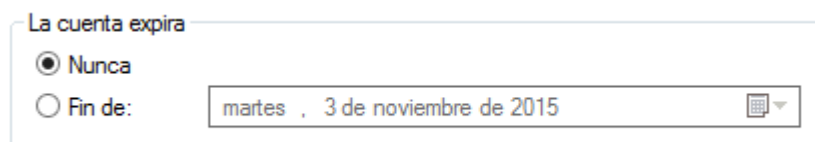
OPCIONES DE CUENTA

Poderemos seleccionar unha serie de opcións referentes á conta de usuario, aparte das 4 primeiras xa vistas no momento da creación, como son:

A screenshot of a list of account options in Windows Server. The options are: '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 tarjeta inteligente es necesaria para un inicio de sesión interactivo', 'La cuenta es importante y no se puede delegar', 'Usar tipos de cifrado DES de Kerberos para esta cuenta', 'Esta cuenta admite cifrado AES de Kerberos de 128 bits.', 'Esta cuenta admite cifrado AES de Kerberos de 256 bits.', and 'No pedir la autenticación Kerberos previa'. All checkboxes are currently unchecked.

LA CUENTA EXPIRA

Establece a directiva de expiración da conta de usuario. Esta opción é interesante para usuarios ou empregados temporais, xa que deste xeito aseguramos que pasado un tempo non poidan entrar no sistema.

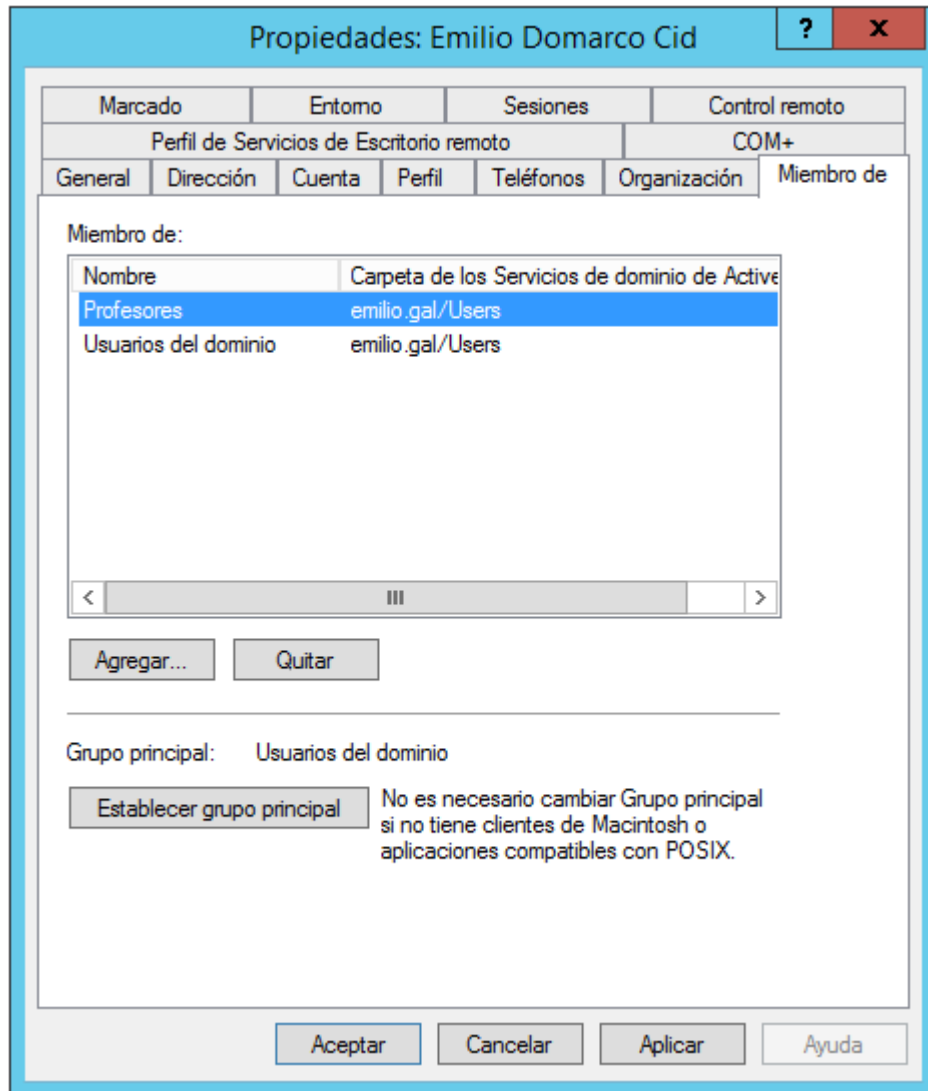
A screenshot of the 'La cuenta expira' (Account Expires) settings in Windows Server. It shows two radio buttons: 'Nunca' (Never) which is selected, and 'Fin de:' (Expires on:). The 'Fin de:' option has a text box next to it containing 'martes , 3 de noviembre de 2015' and a calendar icon.

Posteriormente mediante as Directivas de Grupo poderemos ir “afinando” un pouco máis as opcións da conta de usuario.

3.3.- Pestana Miembro de

Nesta solapa lle diremos o grupo ou grupos ós que pertence a conta de usuario. Iremos engadindo os grupos ós que queremos que pertenza o usuario.

Por exemplo, se temos creado un grupo chamado Profesores, poderíamos asignar a este usuario ó grupo:



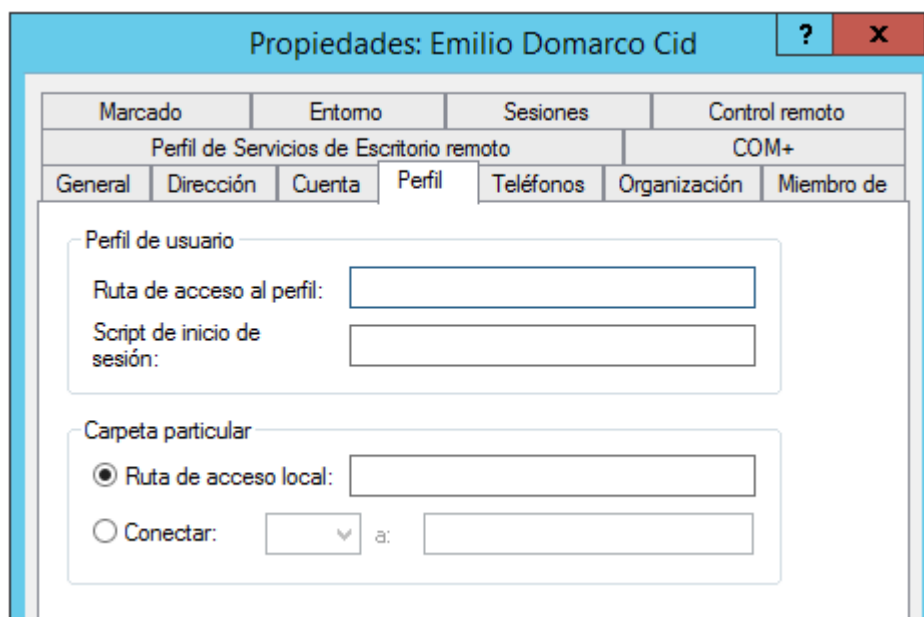
Neste caso lle dicimos que pertenza ó grupo Profesores ademáis de Usuarios del dominio.

Para engadir un novo grupo de pertenza do usuario, simplemente lle daremos a “agregar” e introducimos o grupo ó que queremos que pertenza.



3.4.- Pestana Perfil

Se ben este apartado o veremos con máis detalle máis adiante, esta opción é das máis importantes á hora de configurar unha conta de usuario.



RUTA DE ACCESO Ó PERFIL

Aquí lle diremos a ruta de acceso ó perfil, sexa do tipo que sexa (móbil ou obrigatorio).

SCRIPT DE INICIO DE SESIÓN

Lle diremos onde atopar o script que queremos que se execute ó iniciar unha sesión.

RUTA DE ACCESO LOCAL

Especificaremos que a carpeta particular se encontra nunha ruta de acceso local. Escribiremos a ruta da carpeta particular.

CONECTAR

Seleccionaremos esta opción para elixir unha ruta de acceso de rede para a conexión a unha carpeta particular.

Faremos clic na flecha da lista despregable e a continuación seleccionaremos unha letra de unidade.

No cadro poderemos especificar que a carpeta particular se encontra nunha rede. Para especificar unha ruta de acceso de rede para a carpeta particular, deberemos primeiro crear o recurso compartido e establecer permisos que concedan acceso ó usuario. Para elo se poden empregar carpetas compartidas doutro equipo.

4.- Operacións frecuentes con contas de usuario

A continuación, imos incluír algunhas das operacións que se realizan máis a miúdo sobre as contas de usuario, como parte das tarefas comúns de administración.

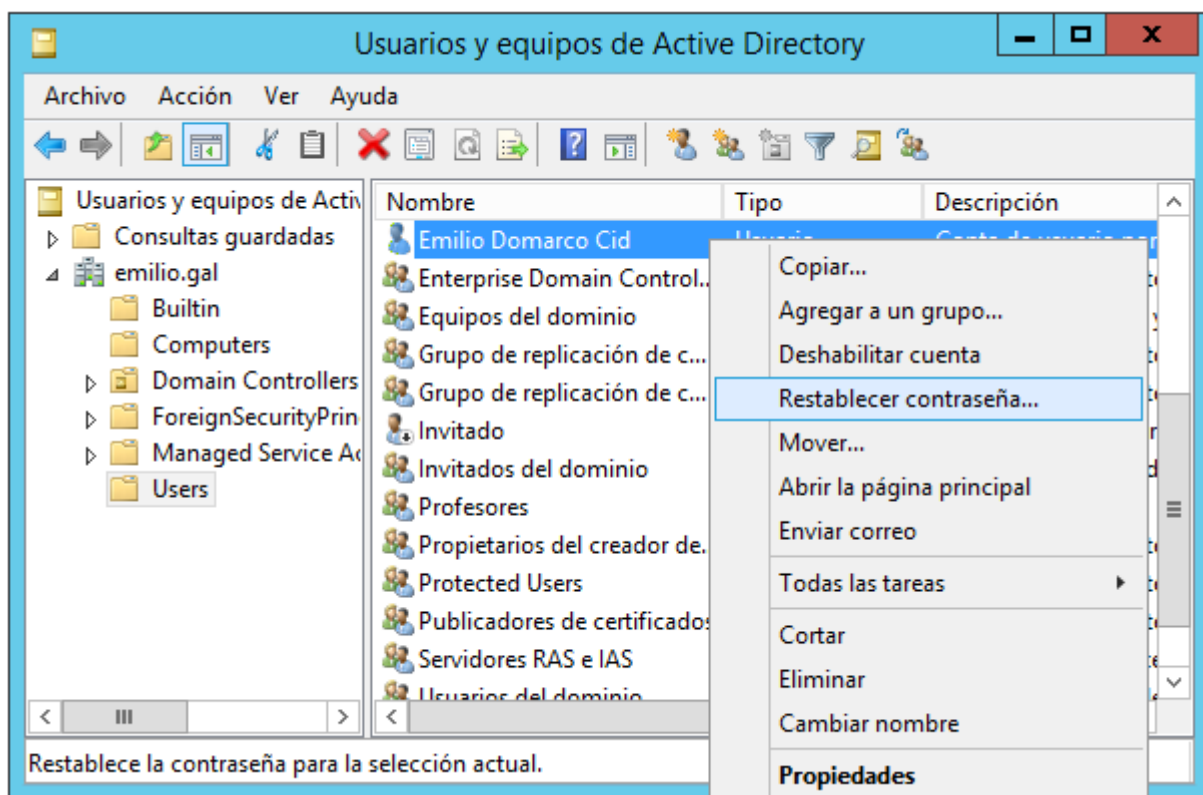
4.1.- Recuperar contrasinais

En ocasións, un usuario esquece o seu contrasinal (por un simple descoido, porque a política de seguridade da empresa obriga a cambiar os contrasinais con frecuencia, porque o usuario leva tempo sen entrar no sistema, etc.).

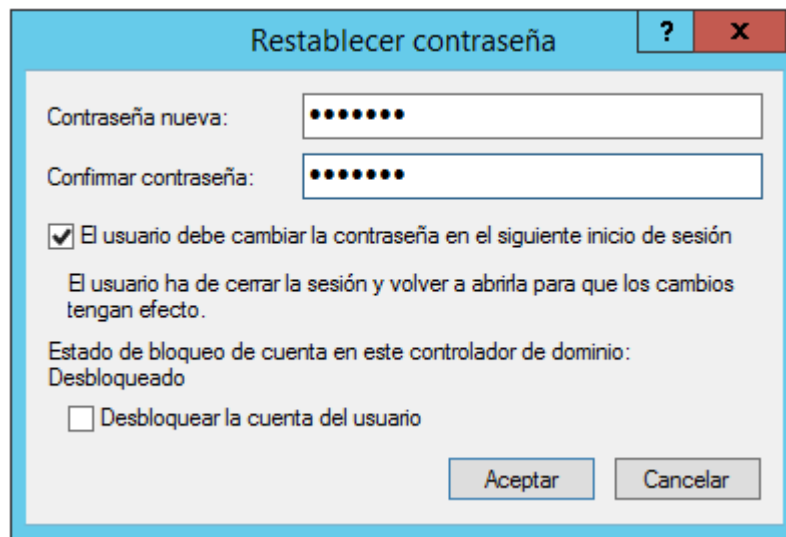
Por cuestións de seguridade, Windows Server 2012 R2 non permite que ninguén, nin sequera o administrador, poida ver o contrasinal dun usuario. Con todo, unha operación que si podemos facer como administradores é asignar un contrasinal novo, comunicala por un medio seguro ao usuario, e obrigarlle a que este a cambie no seu primeiro inicio de sesión. Desta forma, o contrasinal resultante volverá ser coñecida só polo usuario implicado.

Como nos apartados anteriores, usaremos o menú **Herramientas** do Administrador do Servidor. No seu interior, faremos clic sobre Usuarios e equipos de Active Directory (ou ben, utilizaremos a consola **Ferramentas de Emilio** que creamos anteriormente).

Unha vez aberta a ventana, facemos clic co botón dereito do rato sobre o usuario que queremos modificar e no menú de contexto que aparece eliximos **Restablecer contraseña**.



Ábrese a ventana Restablecer contraseña onde escribiremos o contrasinal por duplicado e poderemos seleccionar a opción El usuario debe cambiar la contraseña en el siguiente inicio de sesión, se así ó considereamos necesario.



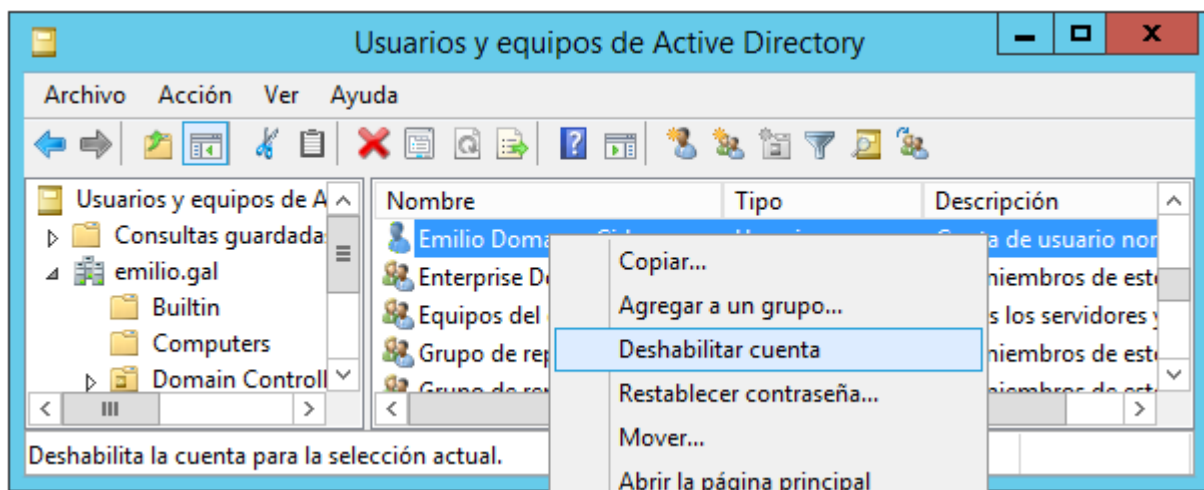
4.2.- Deshabilitar unha conta de usuario

Pode ser recomendable deshabilitar a conta dun usuario que estará ausente durante un determinado período de tempo.

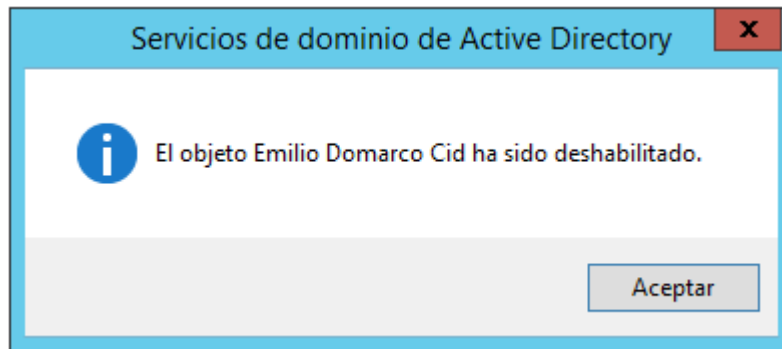
Noutras ocasións, pode resultar interesante dispor dunha conta de usuario ficticia, con todos os parámetros necesarios preconfigurados e utilízala como molde para crear, de forma rápida, novas contas no futuro (veremos como facer isto máis abaixo). Neste caso, tamén é recomendable, por razóns de seguridade, que esta conta ficticia atópese deshabilitada.

Para deshabilitar unha conta, teremos que recorrer de novo á ferramenta **Usuarios y equipos de Active Directory** (xa vimos en apartados anteriores como abrila).

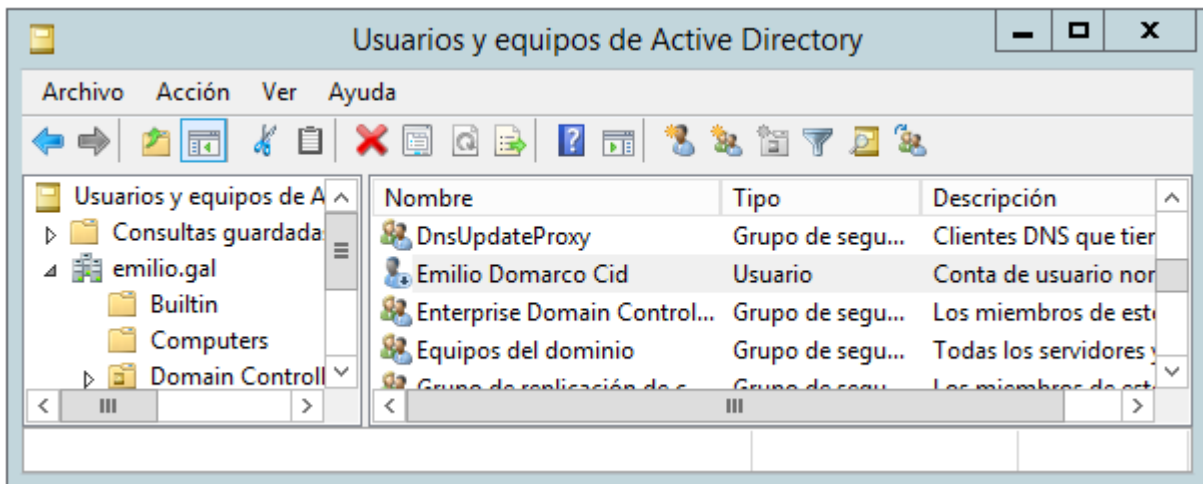
Unha vez aberta a ventana, facemos clic co botón dereito do rato sobre o usuario que queremos modificar e no menú que aparece, eliximos a opción **Deshabilitar cuenta**



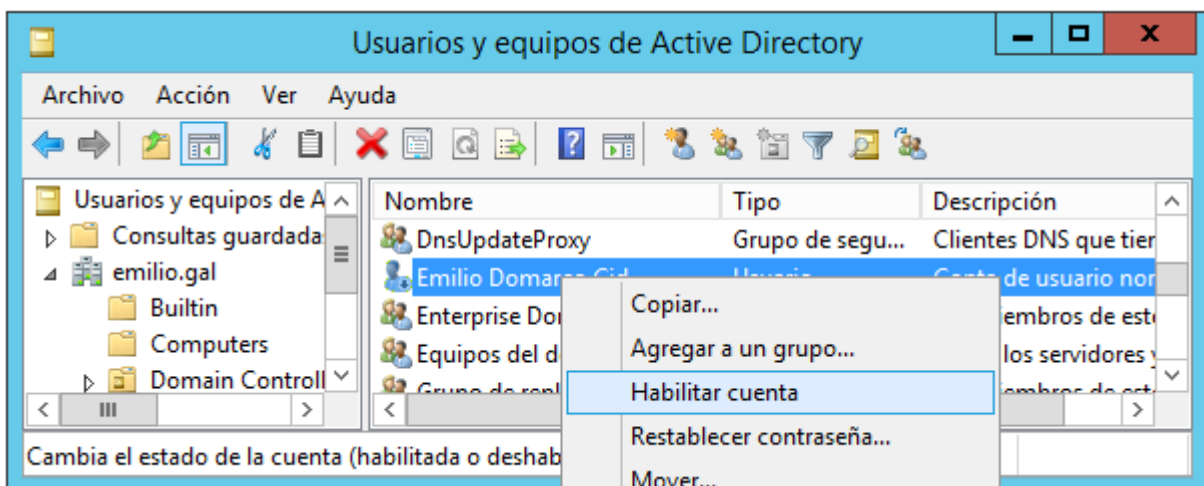
Aparecerá unha ventna informando de que a conta foi deshabilitada.



Observa que a icona dunha conta de usuario deshabilitada na ferramenta **Usuarios y equipos de Active Directory** contén á súa dereita unha frecha negra que apunta cara abaixo (👤)



Cando necesitemos volver habilitala, só temos que volver facer clic co botón dereito do rato sobre o nome da conta e pulsaresmos en **Habilitar cuenta**.

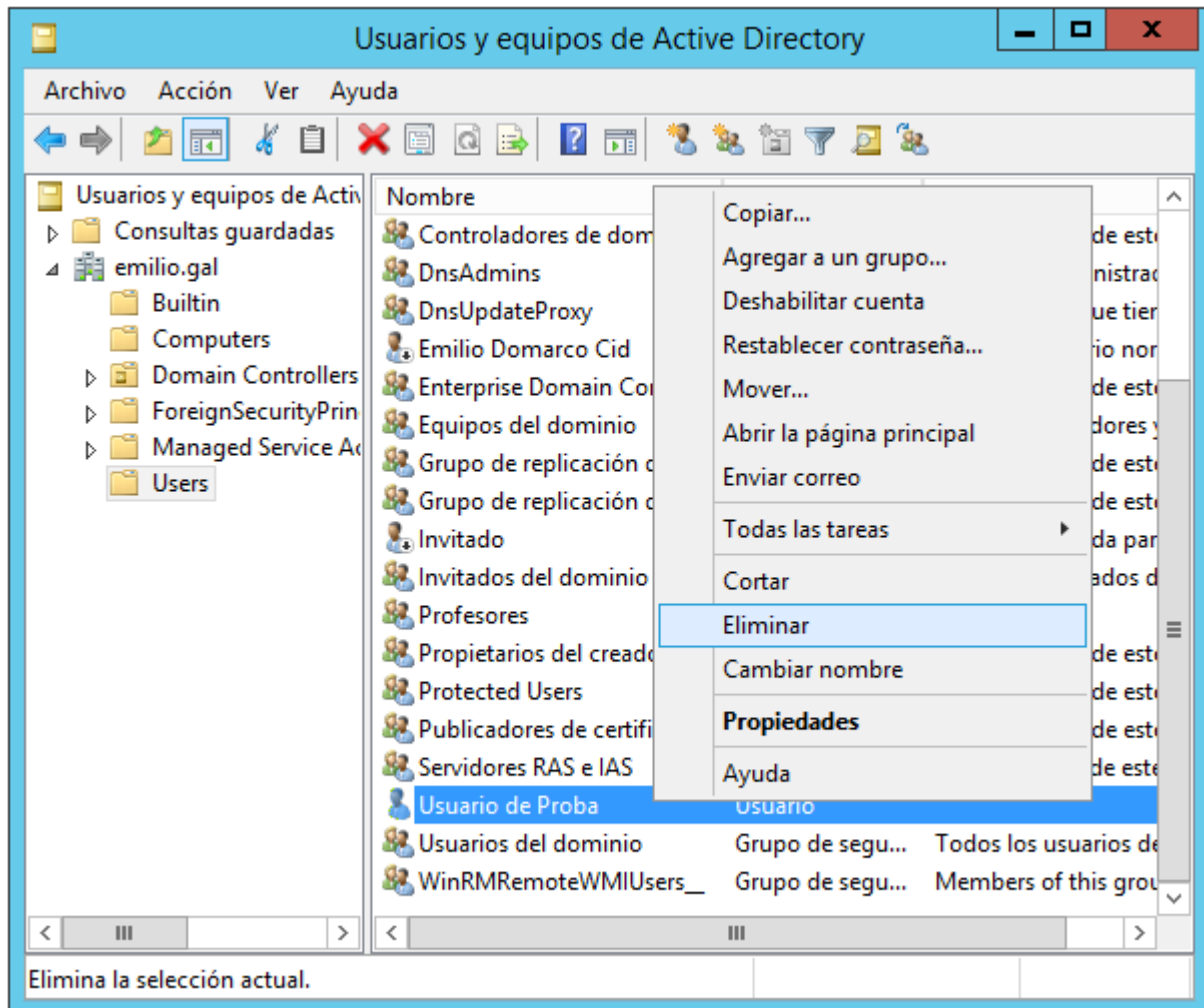


4.3.- Eliminar unha conta de usuario

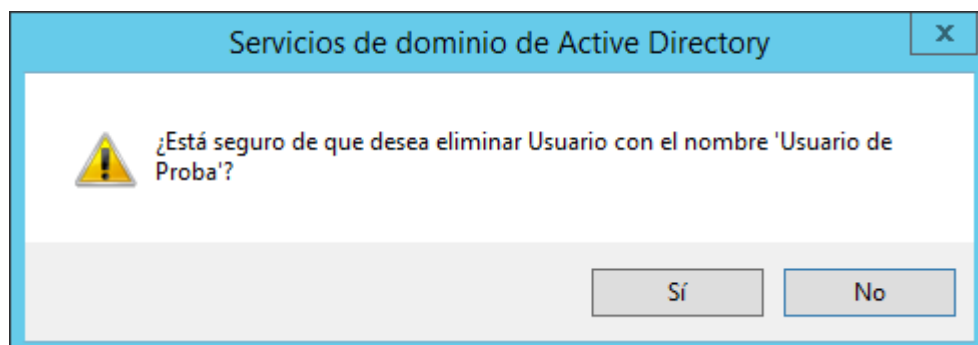
Aínda que non sexa a operación máis frecuente, nalgúns ocasións, é necesario eliminar algunhas das contas do sistema.

Como de costume, o primeiro será abrir a ferramenta **Usuarios y equipos de Active Directory** (igual que fixemos en apartados anteriores). A continuación, buscaremos a conta que pretendemos eliminar e facemos clic co botón dereito do rato sobre ela.

No menú de contexto que aparece, facemos clic sobre **Eliminar**



Ábrese un cadro de diálogo que nos avisa de que imos a eliminar a conta de usuario.



4.4.- Copiar unha conta de usuario

Á hora de crear a estrutura do dominio e os usuarios do mesmo, ímonos encontrar con que a maioría das características dos usuarios do mesmo son iguais, e dicir, que os usuarios que creemos terán todos as mesmas propiedades, excepto o nome.

Neste caso sería tedioso ir cubrindo os datos de cada usuario un a un, e para poder solucionar isto podemos crear un usuario “modelo” a partir do cal iremos creando os novos usuarios, o cal nos facilitará moito a tarefa de dar de alta ós novos membros o dominio.

Crearemos un novo usuario ó que lle poderemos chamar “**_plantilla**”. Podemos observar que leva un guión diante que só nos vai servir para que na lista de usuarios nolo coloque de primeiro e en caso de ter moitos usuarios no dominio non perder tempo buscándoo.

Creamos o novo usuario:

The screenshot shows the 'Nuevo objeto: Usuario' dialog box. At the top, it says 'Crear en: emilio.gal/Users'. Below this, there are several input fields: 'Nombre de pila:' with the value '_plantilla', 'Iniciales:' (empty), 'Apellidos:' (empty), 'Nombre completo:' with the value '_plantilla', 'Nombre de inicio de sesión de usuario:' with the value 'plantilla' and a dropdown menu showing '@emilio.gal', and 'Nombre de inicio de sesión de usuario (anterior a Windows 2000):' with the value 'EMILIO\' and 'plantilla'. At the bottom, there are three buttons: '< Atrás', 'Siguiete >', and 'Cancelar'. The 'Siguiete >' button is highlighted in blue.

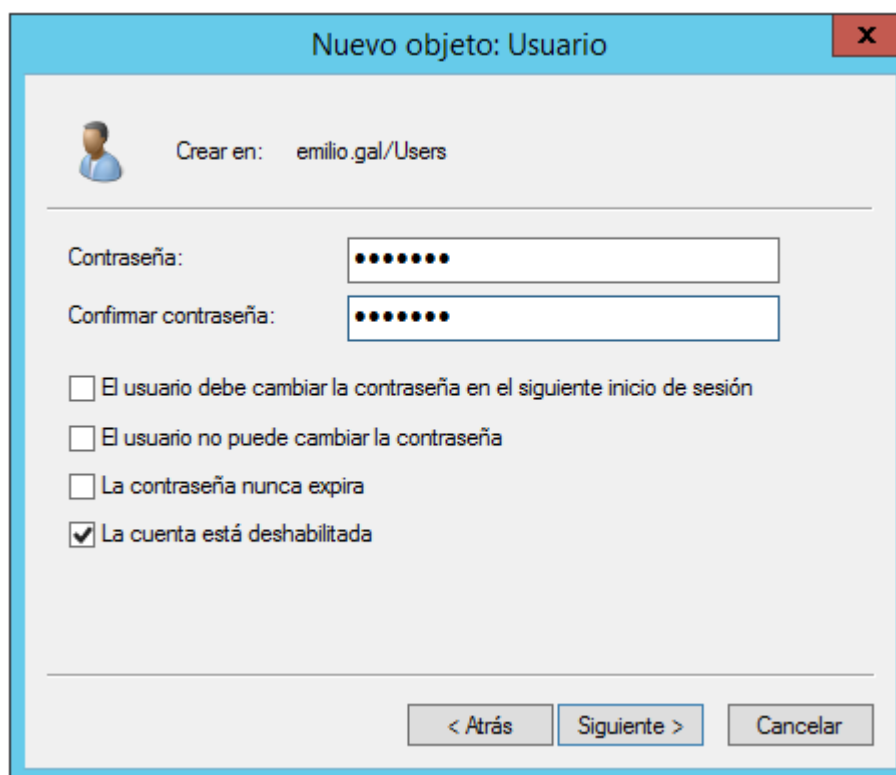
No seguinte paso, deberemos escribir un contrasinal que cumpra coas políticas de seguridade do sistema (xa falamos desta cuestión con anterioridade).

Tamén poderemos obrigar ao usuario a que cambie o contrasinal no seu primeiro inicio de sesión aínda que nós non o faremos.

Por último, lembra que a conta que utilizamos como modelo está deshabilitada, polo que a conta que estamos a crear a partir dela tamén o estará.

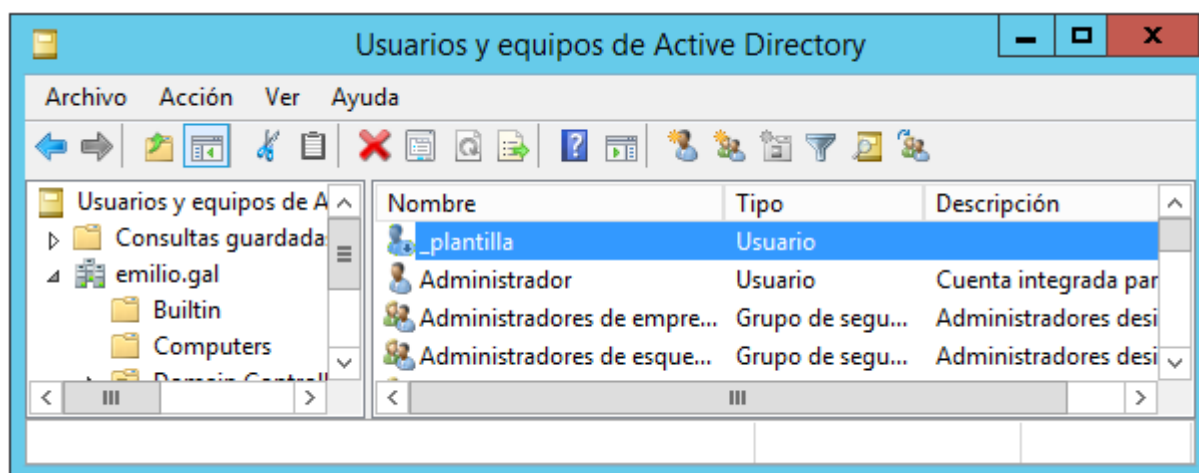
Por tanto, debes lembrar desmarcar a opción La cuenta está deshabilitada, ou habilitala máis tarde, para que o usuario poida utilizala.

Introducimos a contraseña e lle dicimos que a conta está deshabilitada para que ninguén poda loguearse con esta conta.

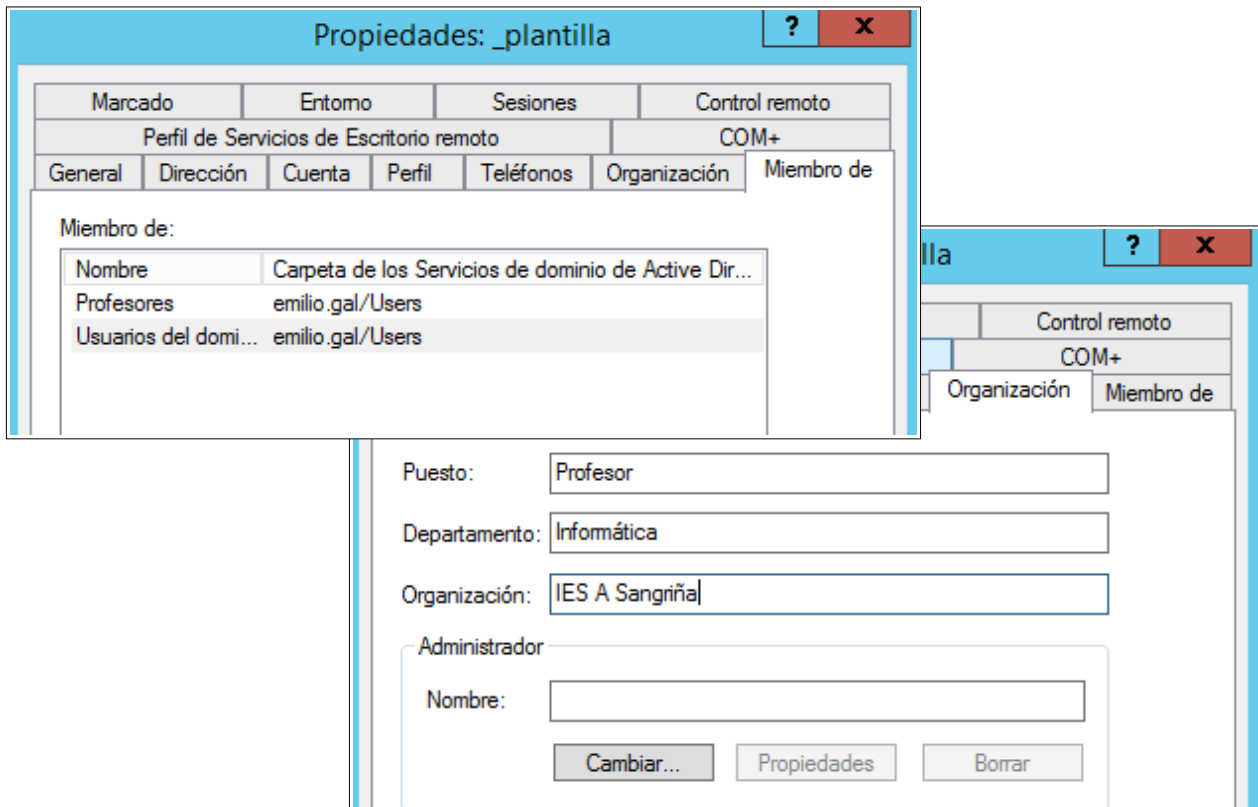


Observamos que a conta xa está creada e nola pon de primeira xa que tivemos a precaución de porlle o (_) antes do nome.

Tamén podemos observar que a conta está deshabilitada (Frecha negra cara abaixo diante do usuario)

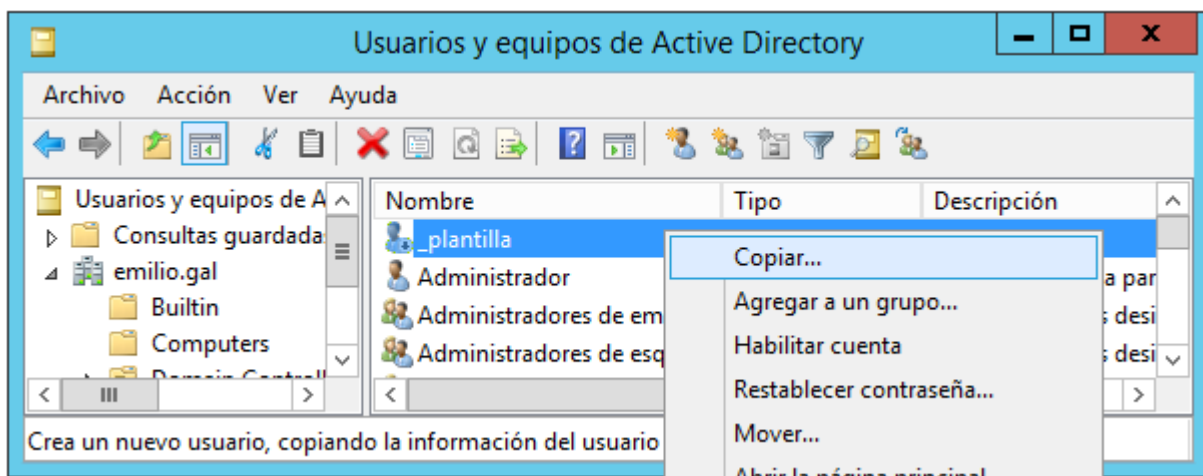


Agora lle configuramos a pertenza a grupos, rutas do perfil, scripts de inicio de sesión e todos aqueles parámetros que sexan comúns as contas que se queiran crear.

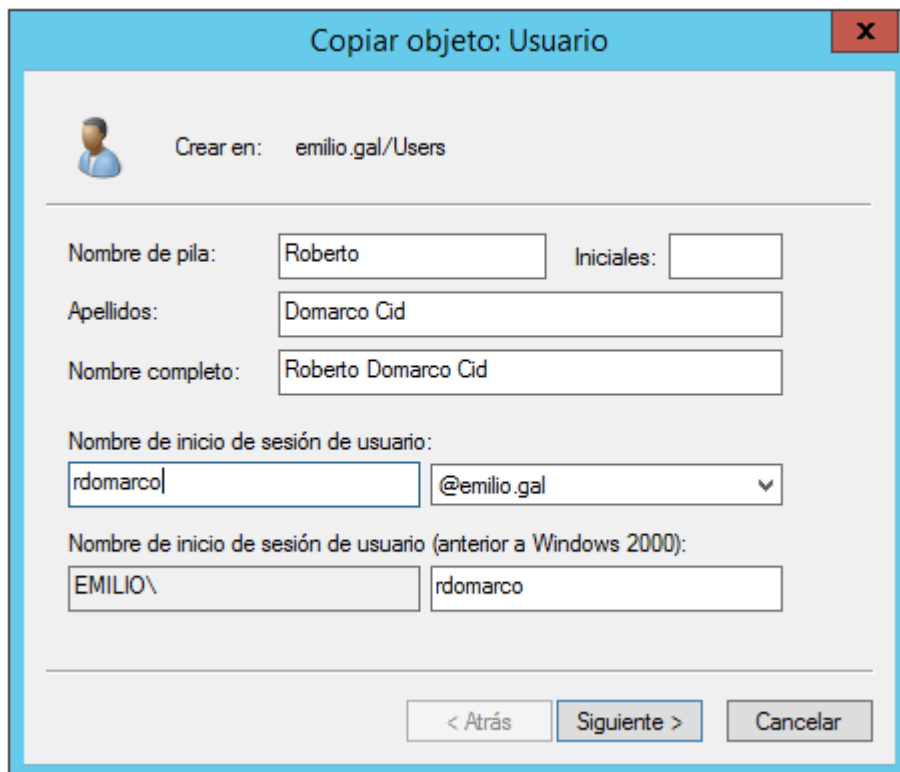


Deste xeito xa temos creada a plantilla cos datos comúns e agora só queda ir creando novos usuarios a partires deste usuario modelo.

Para crear novos usuarios a partir desta plantilla pulsaremos o botón dereito encima da súa conta (vemos que ó odenar aparece de primeira debido ó guión que lle puxemos diante) e iremos á opción “copiar”:



Vemos que nos sae a plantilla para introducir o nome do novo usuario como sempre que damos de alta un usuario onde introduciremos os datos, neste caso Roberto Domarco Cid.



Copiar objeto: Usuario

Crear en: emilio.gal/Users

Nombre de pila: Roberto Iniciales:

Apellidos: Domarco Cid

Nombre completo: Roberto Domarco Cid

Nombre de inicio de sesión de usuario:

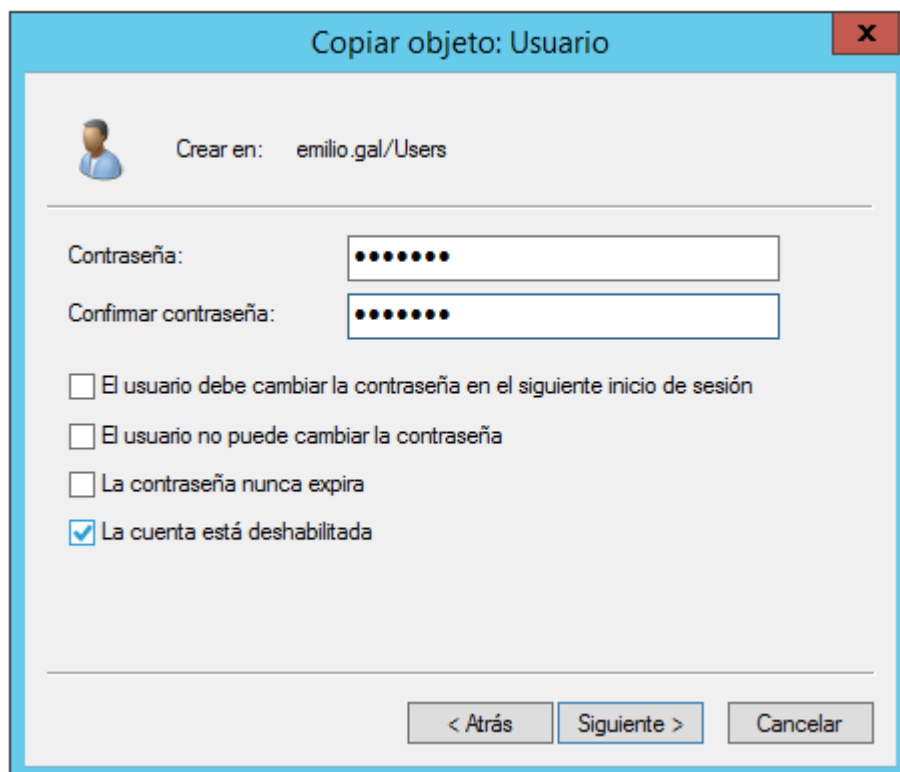
rdomarco @emilio.gal

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

EMILIO\'\' rdomarco

< Atrás Siguiete > Cancelar

Dámoslle a **Siguiete** e introducimos a contraseña e teremos a precaución de **desmarcar a casilla de Cuenta deshabilitada** que marcáramos na plantilla.



Copiar objeto: Usuario

Crear en: emilio.gal/Users

Contraseña:

Confirmar contraseña:

☐ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

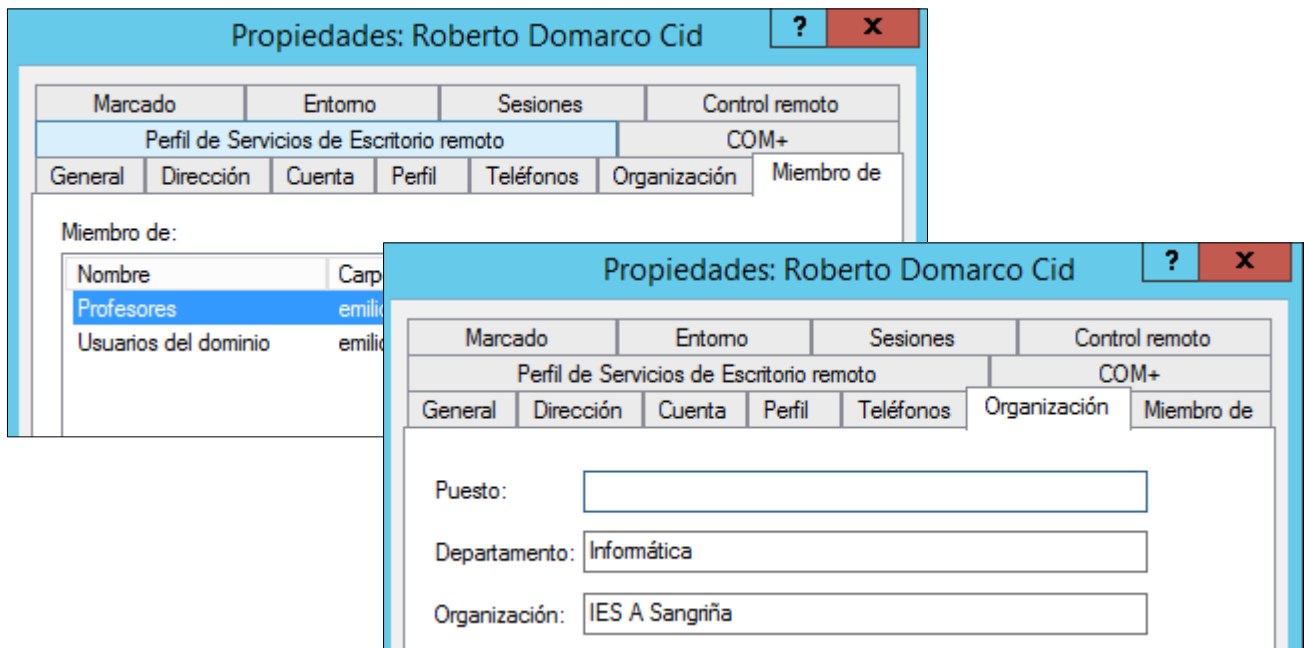
☐ El usuario no puede cambiar la contraseña

☐ La contraseña nunca expira

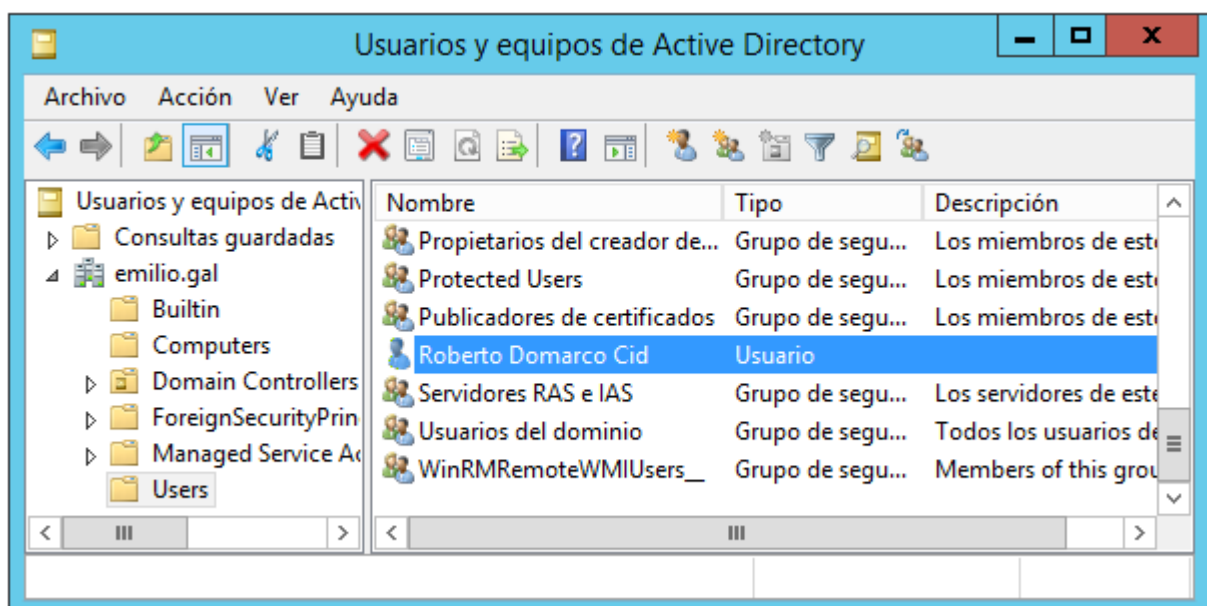
☒ La cuenta está deshabilitada

< Atrás Siguiete > Cancelar

Se agora imos as propiedades do usuario creado poderemos observar que tería as mesmas propiedades que o usuario plantilla:



E xa temos o usuario Roberto creado:

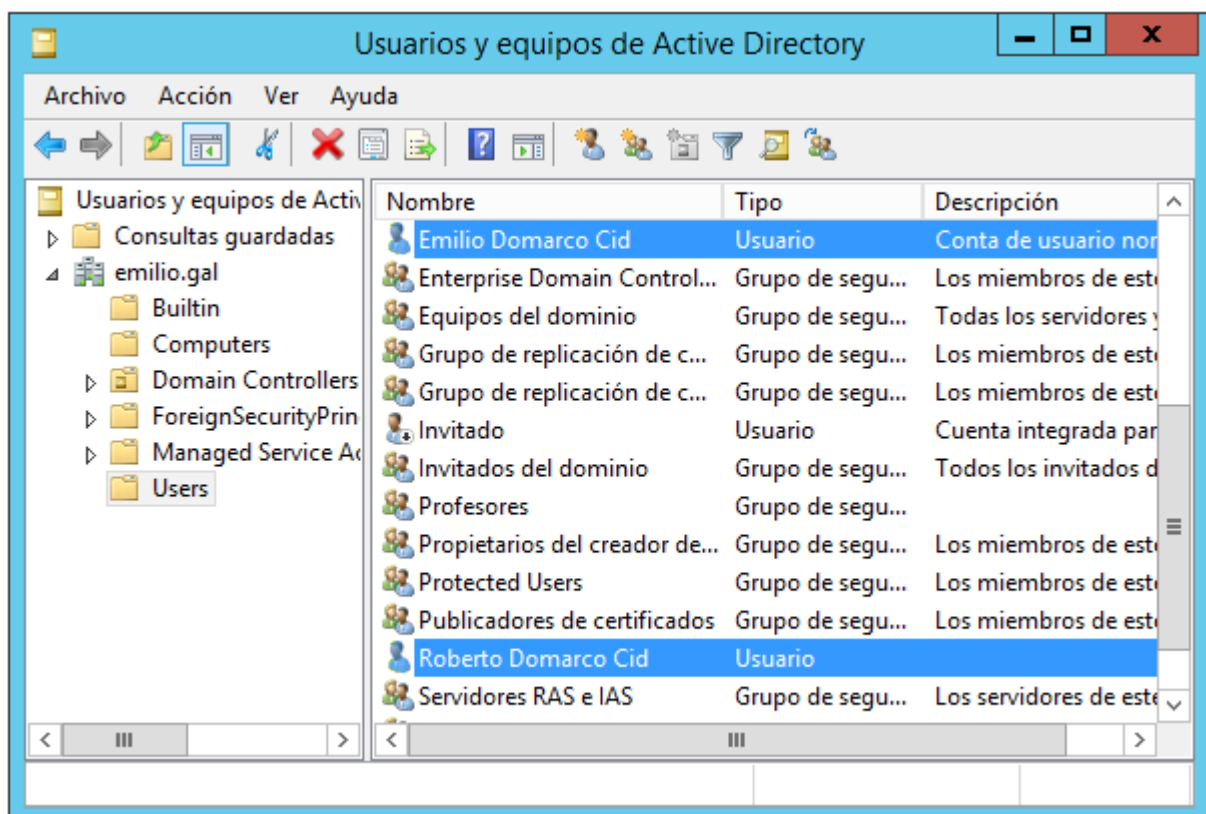


4.5.- Cambiar as propiedades dun grupo de contas

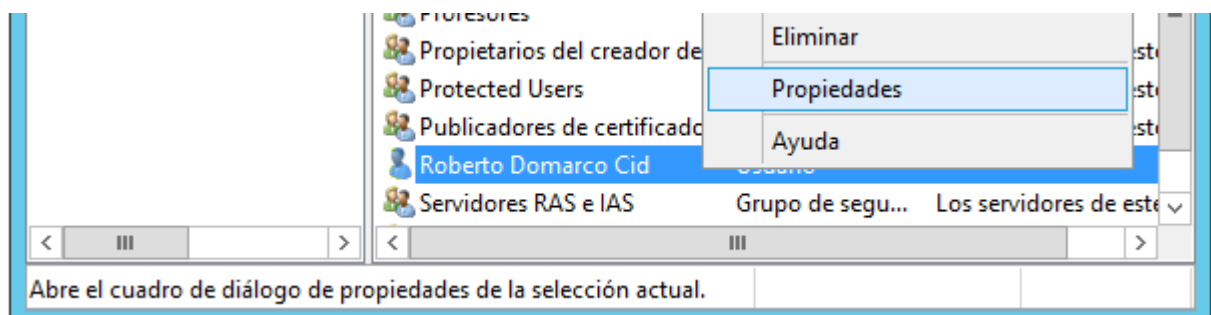
Como dicíamos ó principio do tema a maioría das propiedades dos usuarios deben modificarse de xeito individual pero haberá veces que deberemos cambiar as propiedades dun grupo de usuarios e esta tarefa, se se fixese un a un, sería tediosa e levaríanos moito tempo.

De ahí que o sistema nos permita cambiar de xeito conxunto unha serie de propiedades comúns ás contas de usuario tal e como vimos ó principio, que é o que se coñece como **propiedades con selección múltiple**.

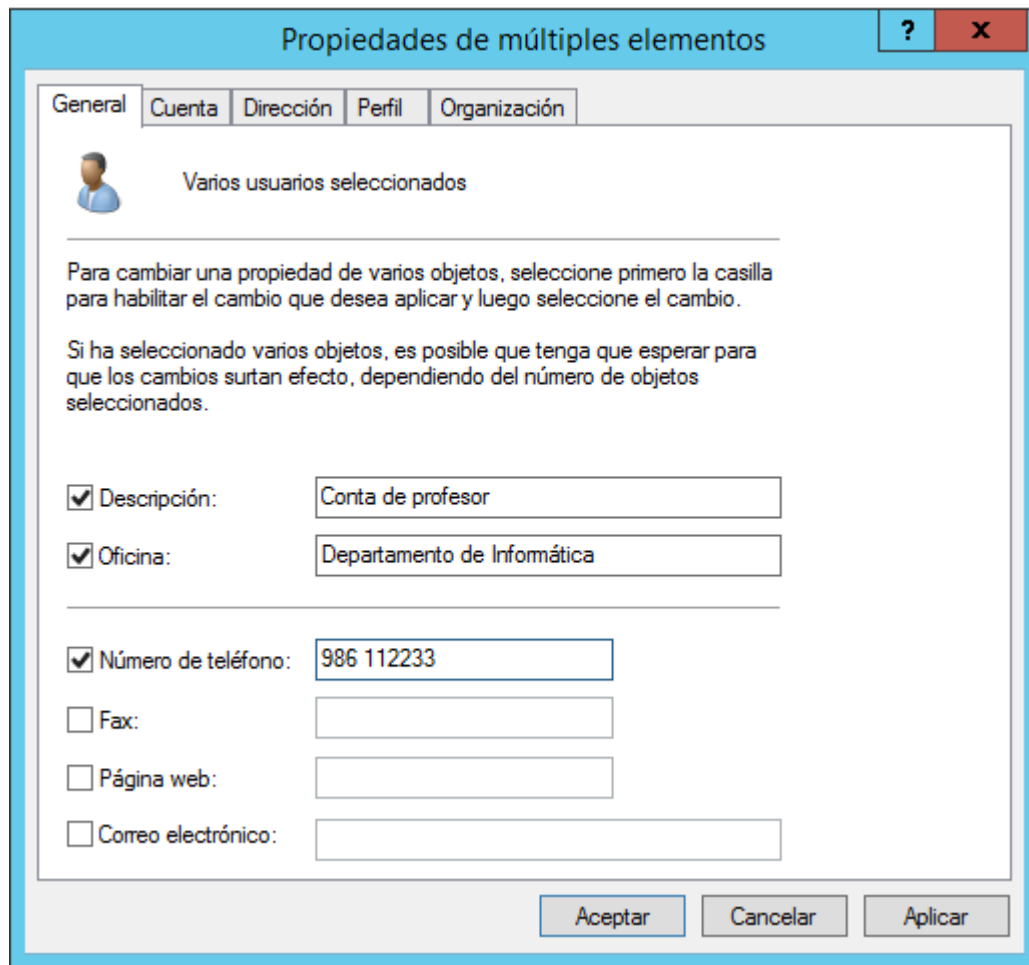
Para facelo, seleccionamos todos os usuarios que desexemos seleccionándoos coa tecla Control pulsada:



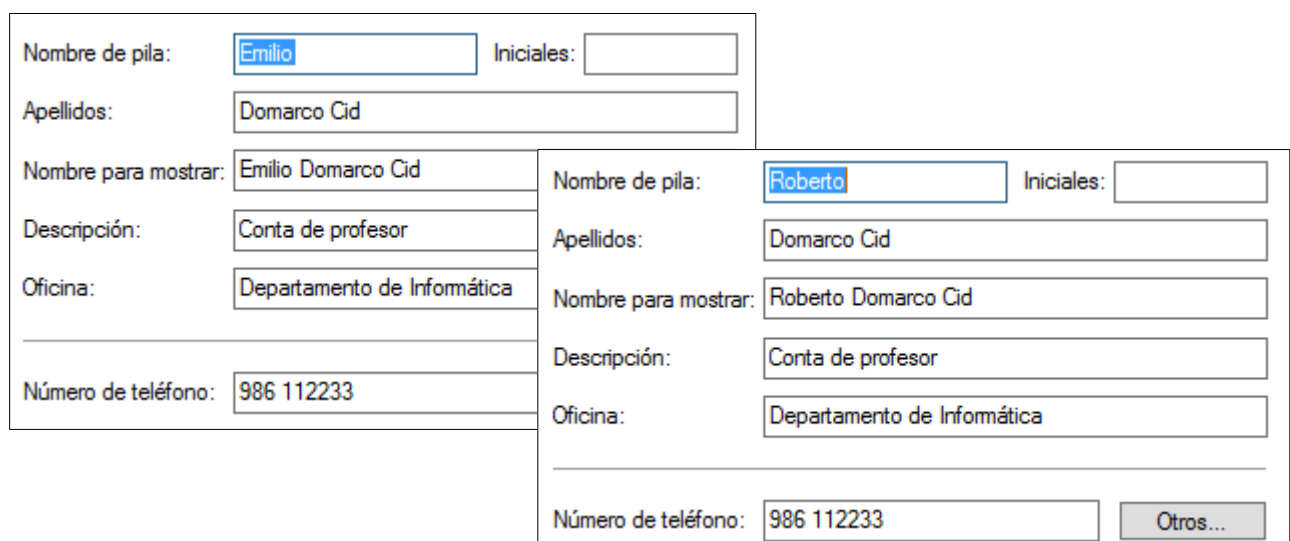
Sobre un deles picamos co botón dereito do rato e picamos en Propiedades para abrir as propiedades dos usuarios.



Ábrenos a seguinte ventana onde vemos as 5 pestanas de propiedades que se poden cambiar de xeito conxunto:



Se agora vemos as propiedades dos usuarios observamos que se cambiaron para os dous usuarios que tiñamos seleccionados:



5.- Crear unha Conta de Grupo

5.1.- Introducción

Nunha empresa normal as tarefas a realizar basicamente serán sempre as mesmas, aínda que é moi probable que ao longo do tempo cambien as persoas que as realizan.

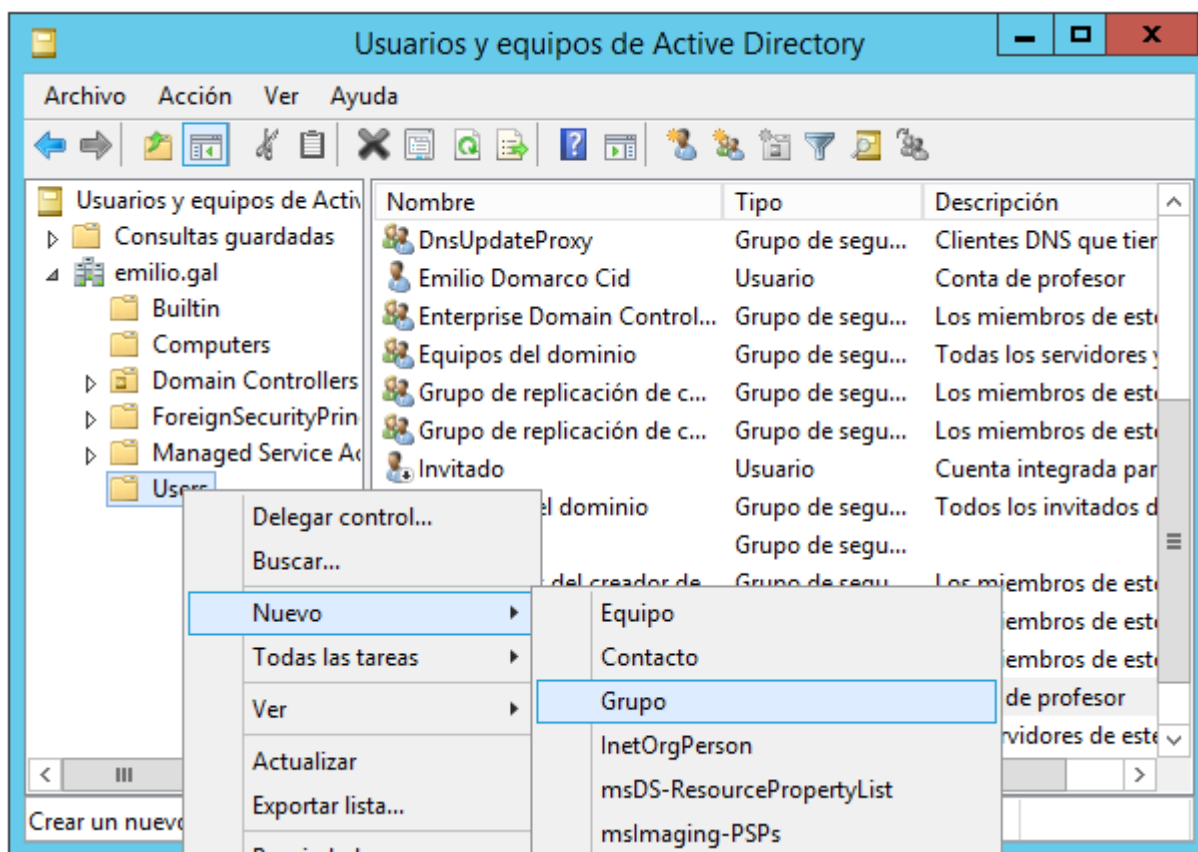
Sobre a base deste principio, nun dominio Active Directory é moito máis útil asignar as tarefas e os permisos para realízalas aos grupos en lugar da un usuario individual. Polo tanto imos ver como utilizar os grupos para identificar tarefas administrativas, filtrar Directivas de grupo, asignar directivas de contrasinais únicas, asignar permisos, etc.

De forma básica, un grupo serve para unificar nunha soa entidade unha cantidade indeterminada de entidades individuais (obxectos de Active Directory) como usuarios, máquinas, outros grupos, etc.

Se temos que asignar un permiso determinado a unha carpeta de arquivos a un elevado número de usuarios teríamos que incluír nos permisos da carpeta a todos os usuarios. Non obstante se facemos a todos os usuarios membros dun grupo e damos o permiso ao grupo só temos que facelo unha vez.

5.2.- Creación de grupos

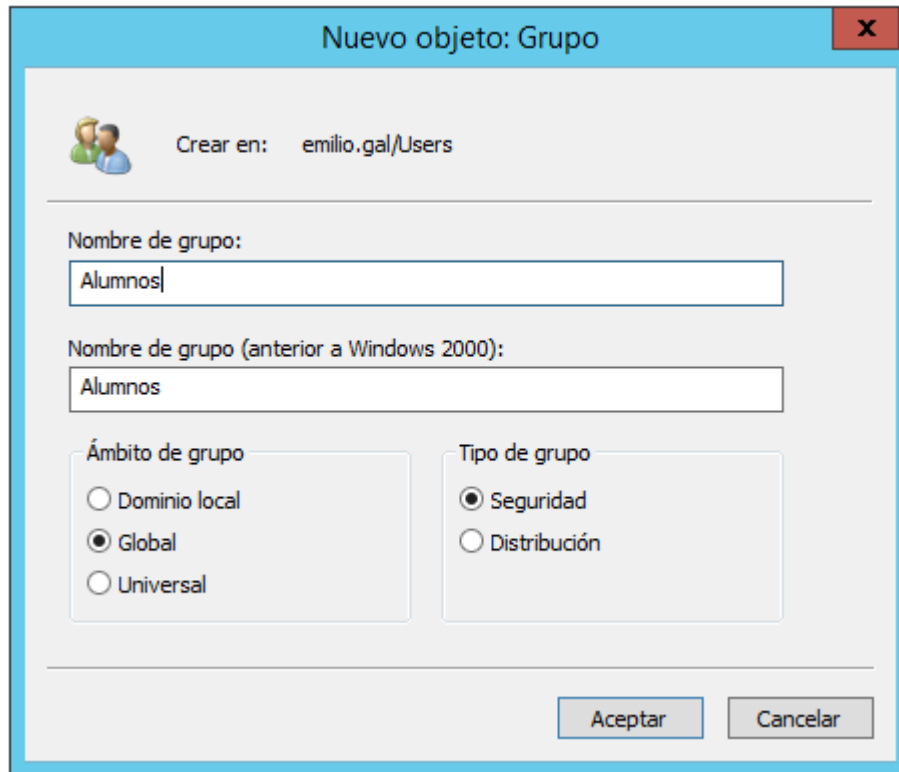
Dentro de **Usuarios y equipos de Active Directory** pulsamos o botón dereito e imos a opción de “nuevo” e despois “grupo”:



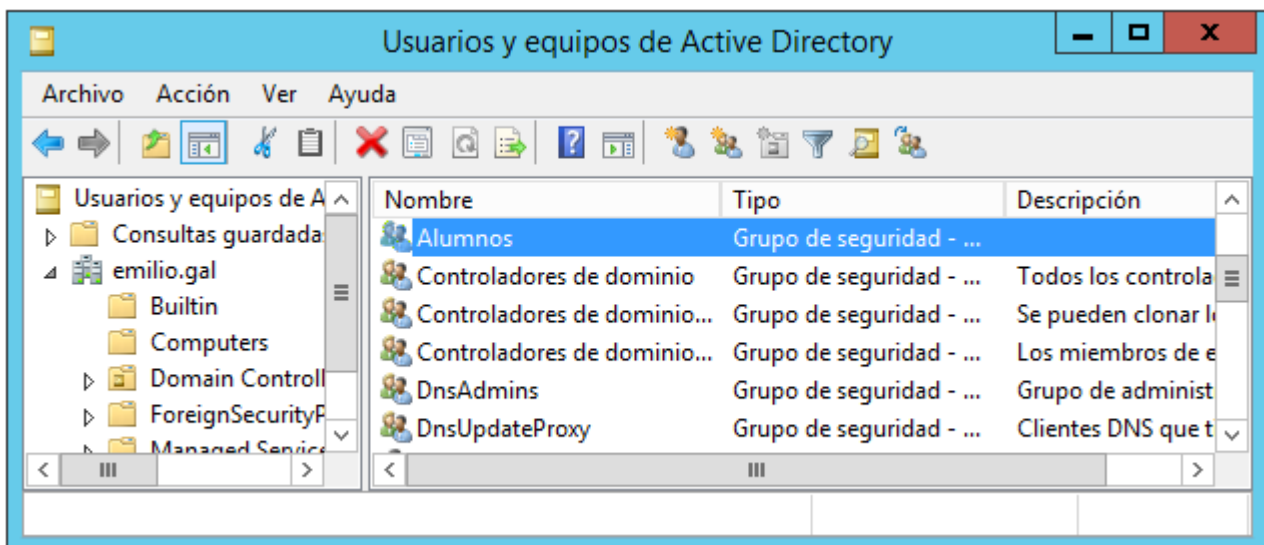
Na ventá que nos abre temos que elixir xa unha serie de propiedades.

A primeira é o nome do grupo que debería indicar a funcionalidade do grupo e mesmo os permisos que ten para que nos axude á administración, aínda que se pode poñer calquera nome.

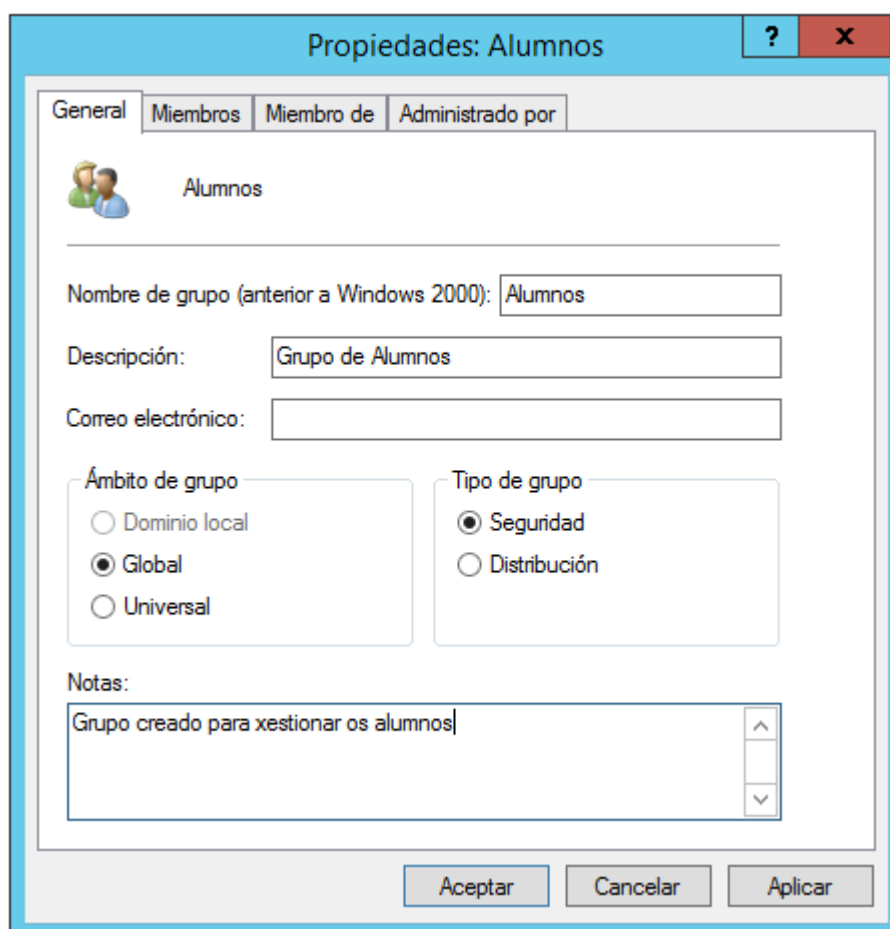
Imos crear o grupo Alumnos:



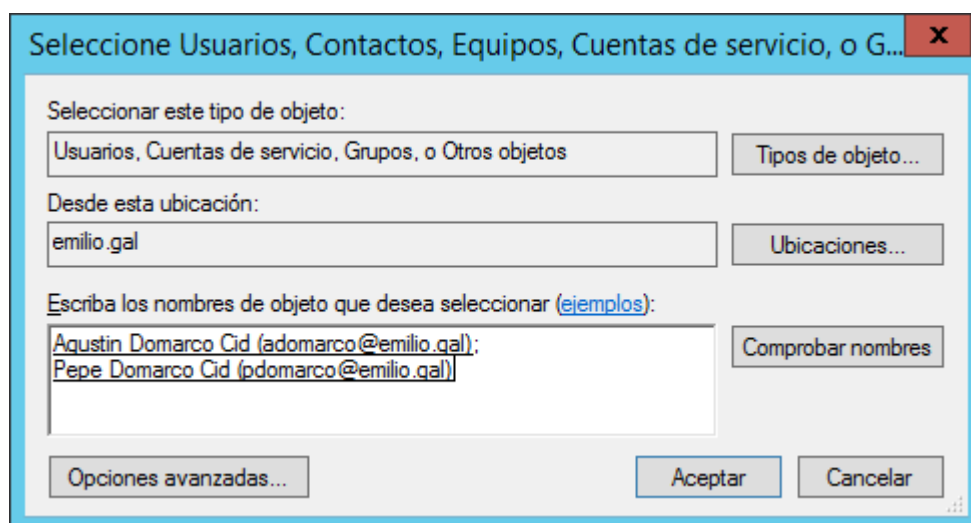
E xa vemos que se creou o grupo:



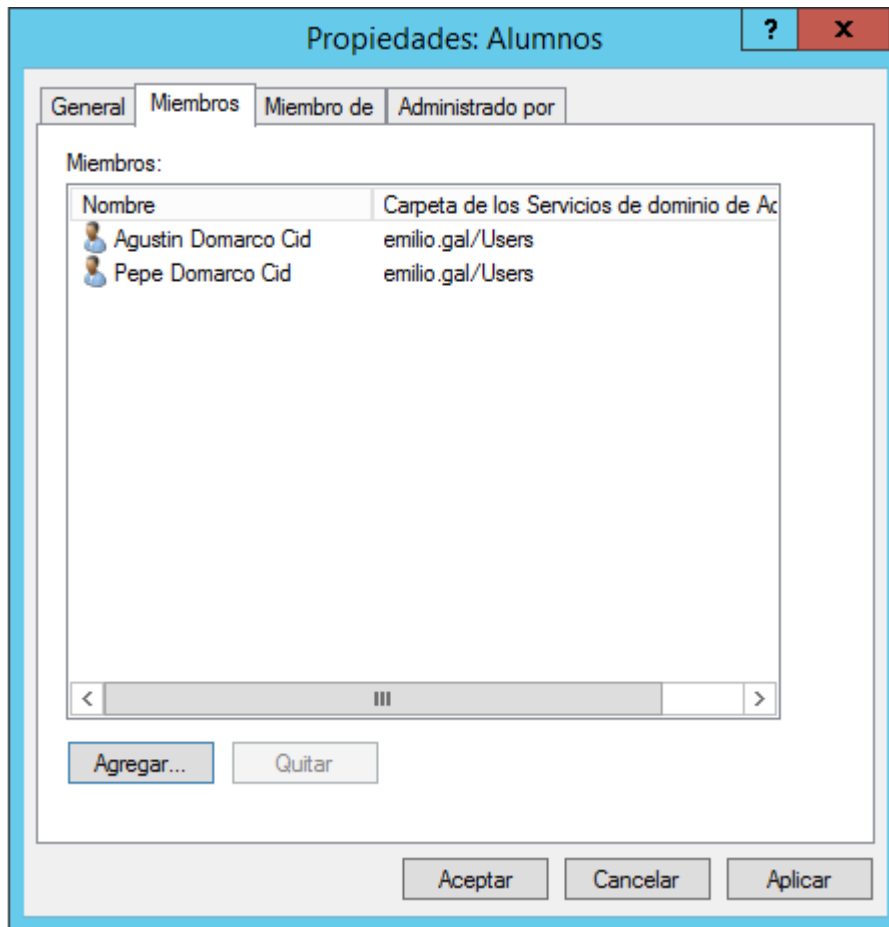
Ahora podemos ver las propiedades del grupo Alumnos haciendo doble clic en el nombre del grupo:



Na pestana “miembros” veremos os usuarios que pertencen a este grupo ou ben os podemos engadir neste momento:



Vemos xa os usuarios engadidos ó grupo:



6.- Unidades Organizativas

6.1.- Introducción

Unha Unidade Organizativa (Organizational Unit, OU) é un obxecto do Directorio Activo que pode conter a outros obxectos do directorio. É dicir, é un colector de outros obxectos, de forma análoga a unha carpeta ou directorio nun sistema de arquivos tradicional.

En concreto, dentro dunha unidade deste tipo poden crearse contas de usuario, de grupo, de equipo, de recurso compartido, de impresora compartida, etc., ademais doutras unidades organizativas. É dicir, mediante unidades organizativas podemos crear unha xerarquía de obxectos no directorio (o cal se asemella outra vez a un sistema de arquivos típico de Windows).

Os obxectos situados dentro dunha unidade organizativa poden moverse máis tarde a outra, se fose necesario.

Sen embargo, un obxecto non pode copiarse: cada obxecto é único no directorio, e a súa existencia é independente da unidade organizativa á que pertence.

Polo tanto, o obxectivo das unidades organizativas é estruturar ou organizar o conxunto dos obxectos do directorio, agrupándoos de foma coherente.

No Directorio Activo, as unidades organizativas permiten:

✓ **Delegar a administración**

Cada unidade organizativa pode administrarse de forma independente.

En concreto, pódese outorgar a administración total ou parcial dunha unidade organizativa a un usuario ou grupo de usuarios calquera.

Isto permite delegar a administración de subconxuntos estancos do dominio a certos usuarios que posúan o nivel de responsabilidade axeitada.

✓ **Establecer de forma centralizada comportamentos distintos a usuarios e equipos.**

A cada unidade organizativa poden vincularse políticas de grupo, que aplican comportamentos (xeralmente en forma de restricións) aos usuarios e equipos cuxas contas se sitúan na devandita unidade.

Desta forma, podemos aplicar restricións distintas a subconxuntos de usuarios e equipos do dominio, en función exclusivamente da unidade organizativa onde se sitúan.

Por exemplo, podemos limitar os usuarios do departamento de contabilidade para que só poidan utilizar certas aplicacións, pero que isto non se aplique a os usuarios do departamento de informática.

En moitos sentidos, o concepto de unidade organizativa pódese utilizar en Windows 2012 da mesma forma que se entendía o concepto de dominio en versións anteriores de Windows, é dicir, conxunto de usuarios, equipos e recursos administrados independentemente.

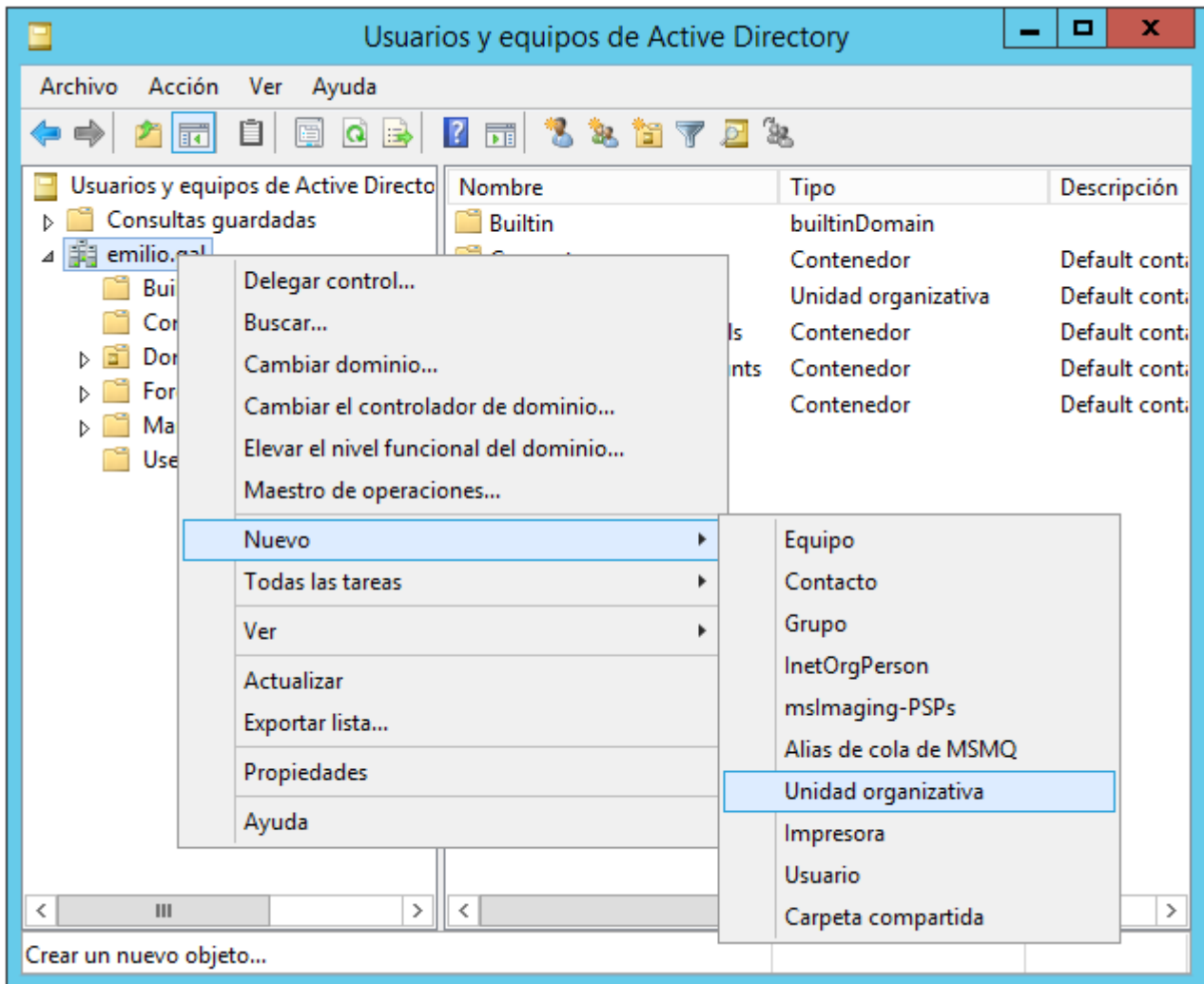
En realidade, en Windows 2012 o concepto de dominio vén máis ben asociado á distribución dos sitios (topoloxía de rede) e a a implementación de DNS que exista (ou queira crearse) na empresa.

Deste modo, en moitas organizacións de pequeno ou medio tamaño resulta máis axeitado implementar un modelo de dominio único con múltiples unidades organizativas que un modelo de múltiples dominios.

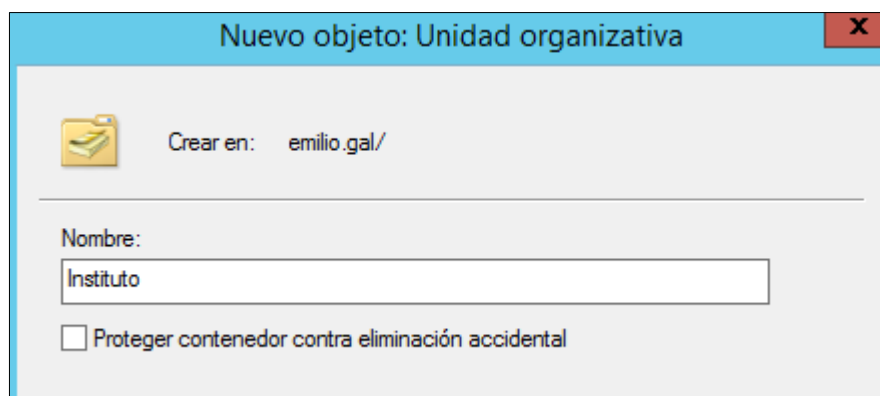
Se é necesario, cada unidade pode administrarse independentemente, cun ou varios administradores delegados e comportamentos (políticas) diferentes.

6.2.- Crear unha unidade organizativa

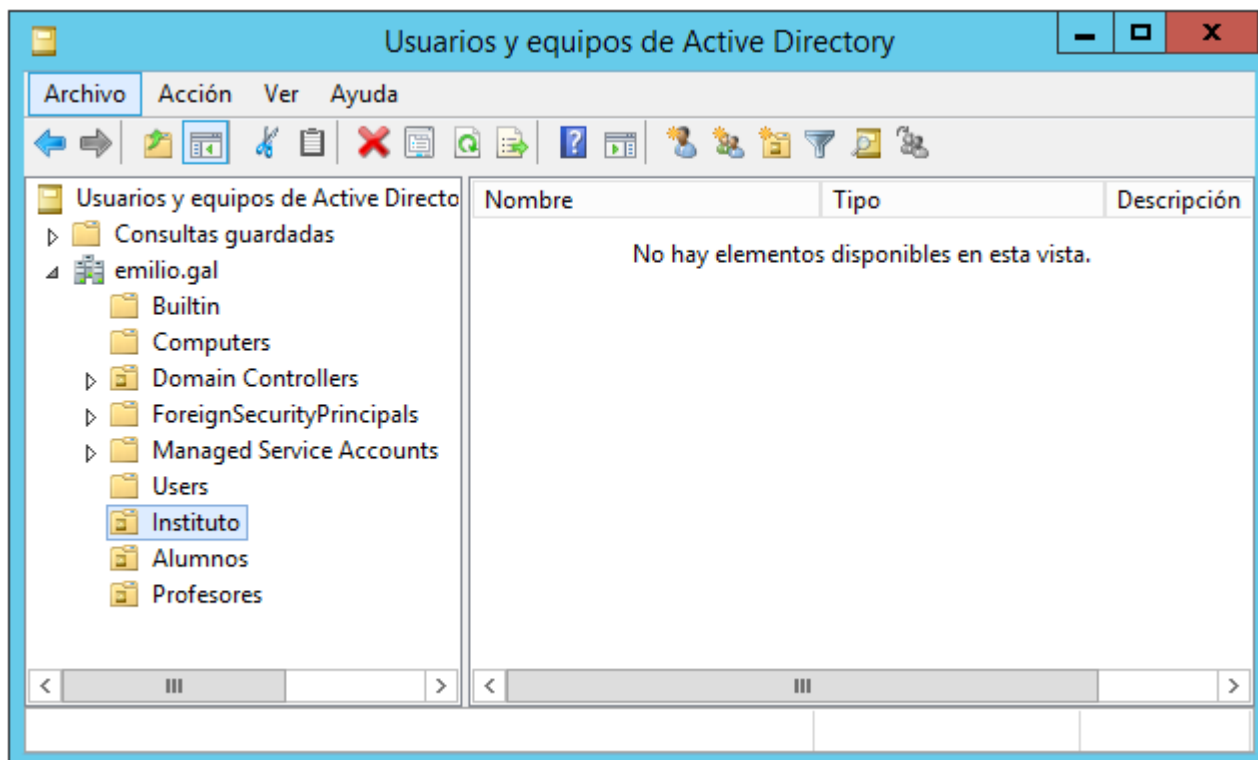
Primeiramente temos que abrir o complemento **Usuarios y equipos do Active Directory** e expandimos o nodo do dominio, neste caso **emilio.gal** seguidamente pulsamos co botón dereito e seleccionamos **Nuevo** → **Unidad Organizativa**:



E lle damos o nome que desexemos conforme á estrutura que queramos crear da nosa empresa ou institución, no noso caso **Instituto**, **Alumnos** e **Profesores** tendo a precaución de desactivar a casilla de **Proteger contenedor contra eliminación accidental**.

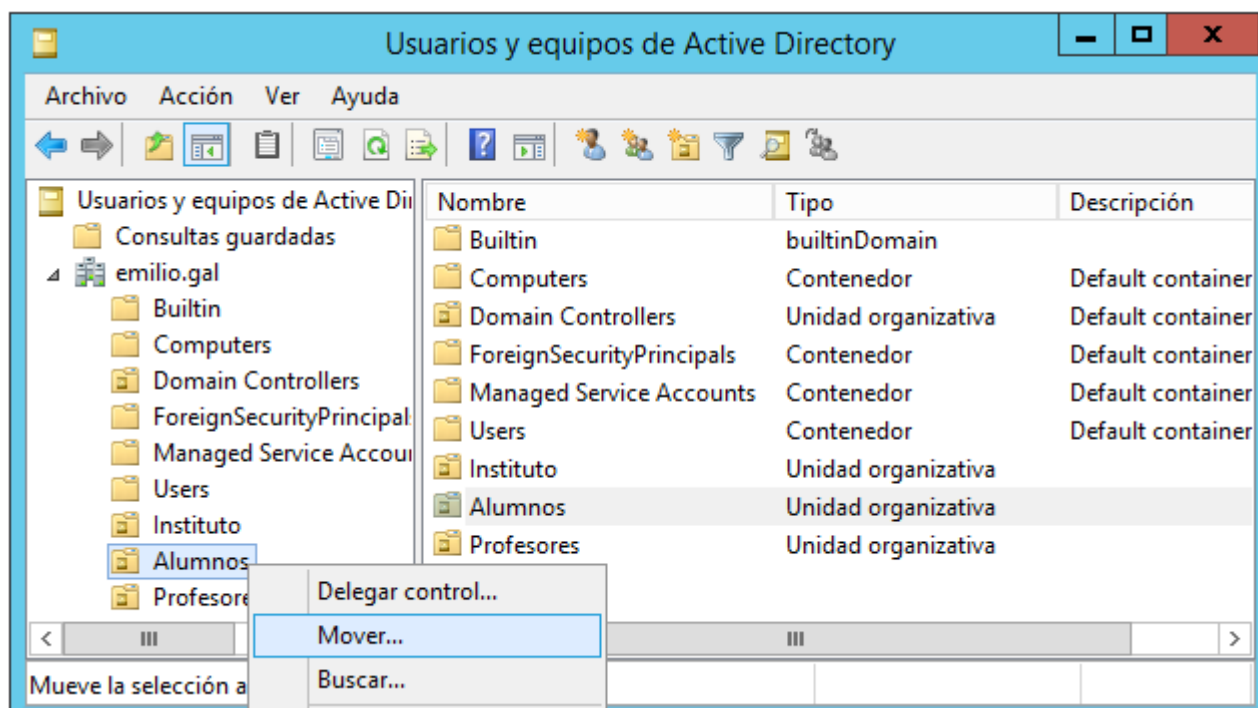


Aquí xa observamos as unidades organizativas creadas .

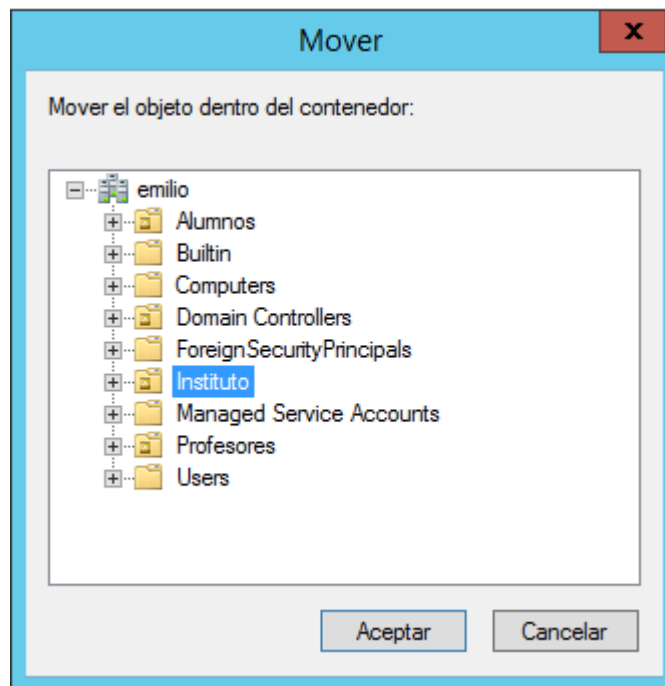


Para organizar mellor a nosa estrutura podemos copiar as unidades de Profesores e Alumnos dentro da unidade do Instituto, co cal posteriormente lle poderemos aplicar directivas a todos.

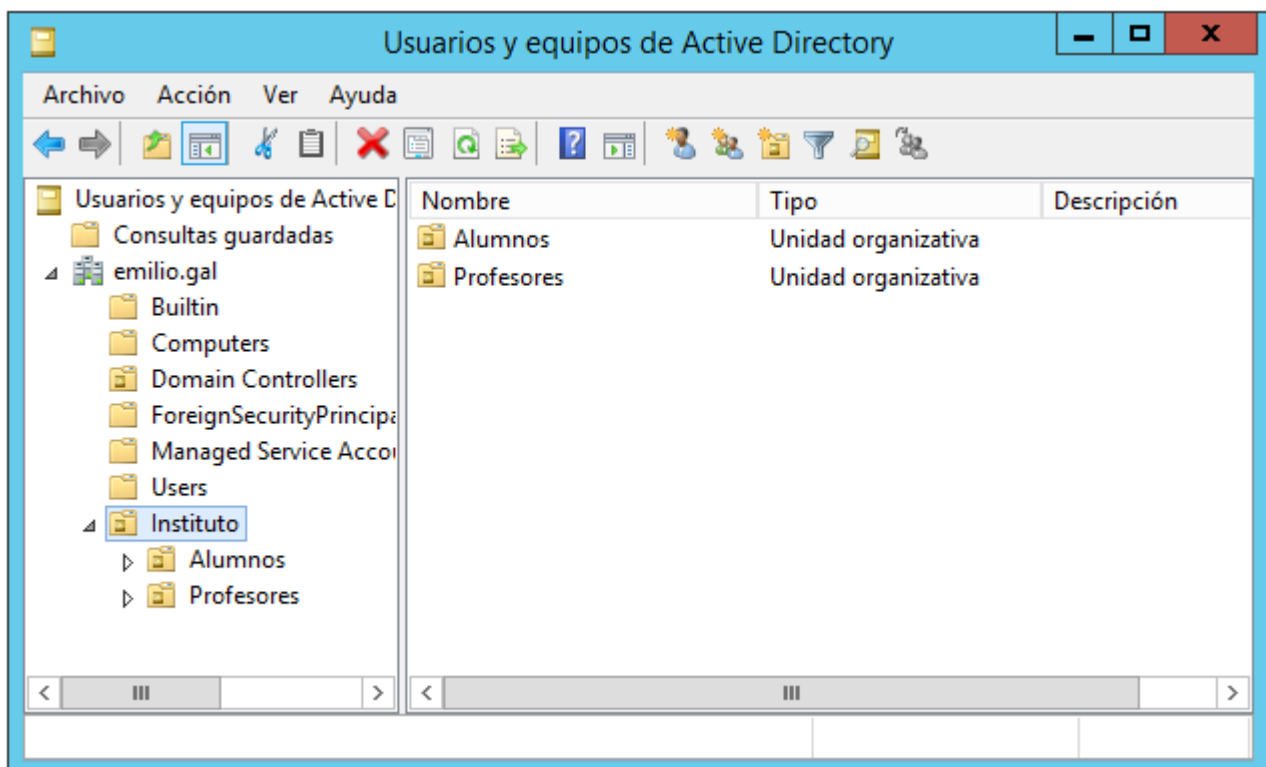
Para elo simplemente teremos que arrastrar a Unidade desexada dentro da unidade de destino ou picar co botón dereito encima da unidade a mover e seleccionr a opción “mover”:



Aparécenos o seguinte cadro de diálogo onde lle diremos a onde a queremos mover:

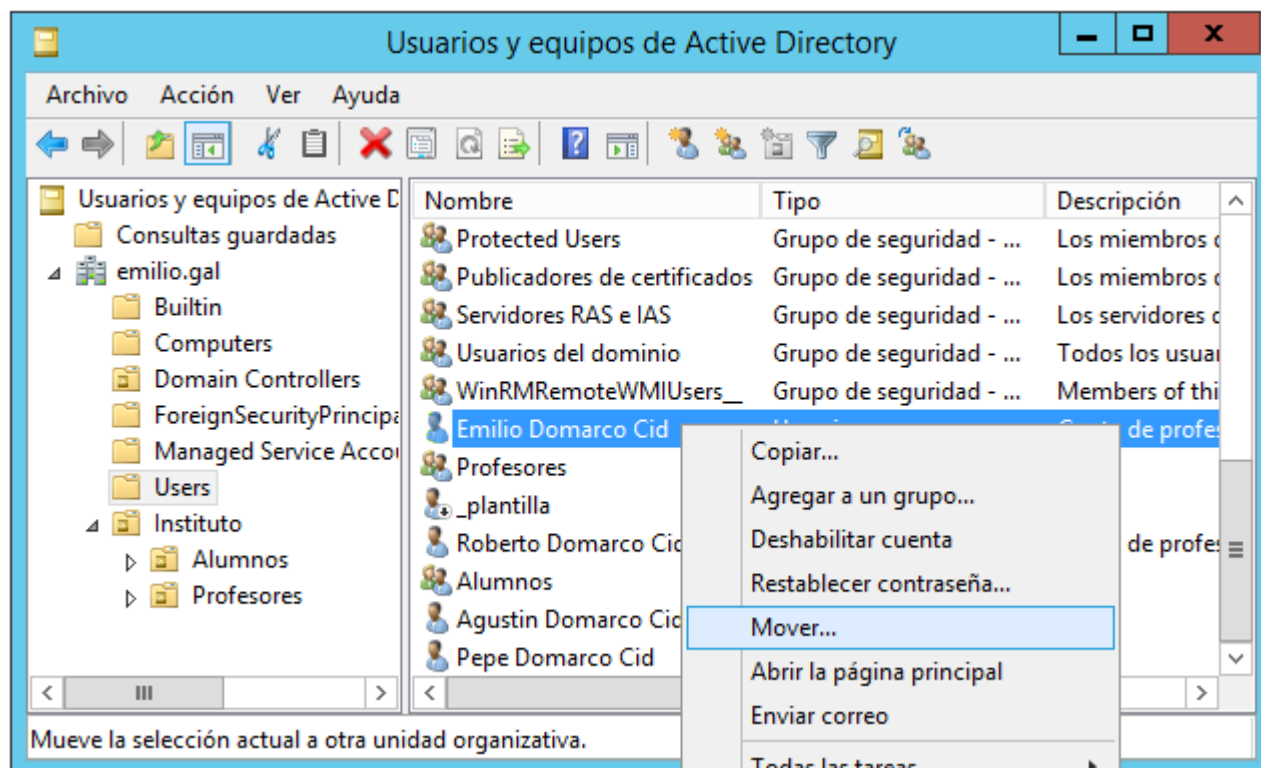


Repetimos o proceso coa UO de Profesores e xa vemos como nos quedou a estrutura de Unidades Organizativas:

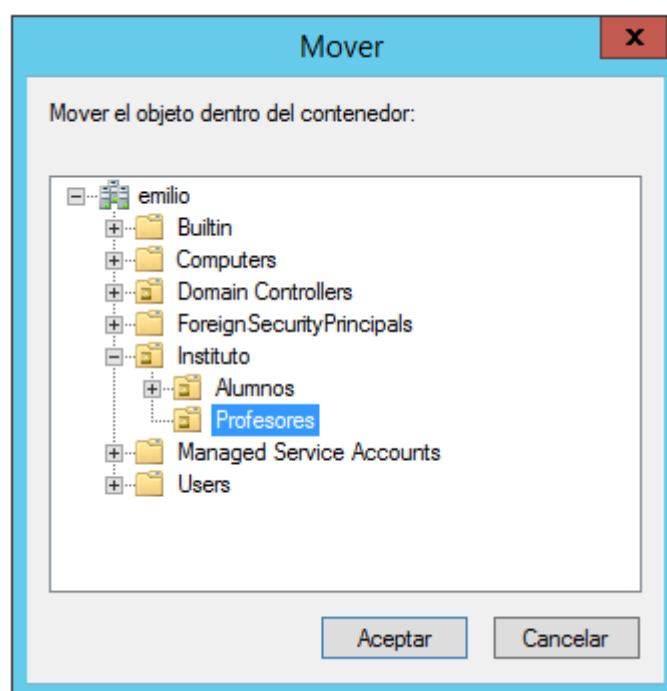


Agora só quedaría ir movendo os usuarios e equipos desexados dentro das unidades organizativas ata conseguir a estrutura planificada.

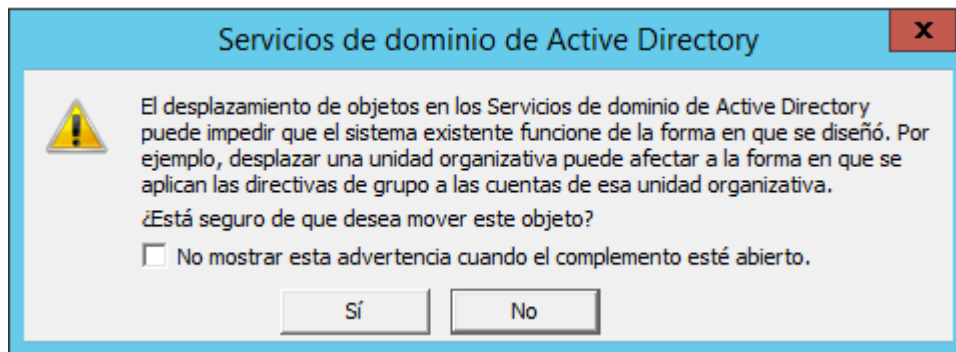
Por exemplo meteremos o usuario Emilio e Roberto dentro de Profesores ben arrastrándoo ou ben co botón dereito no usuario e a opción mover.



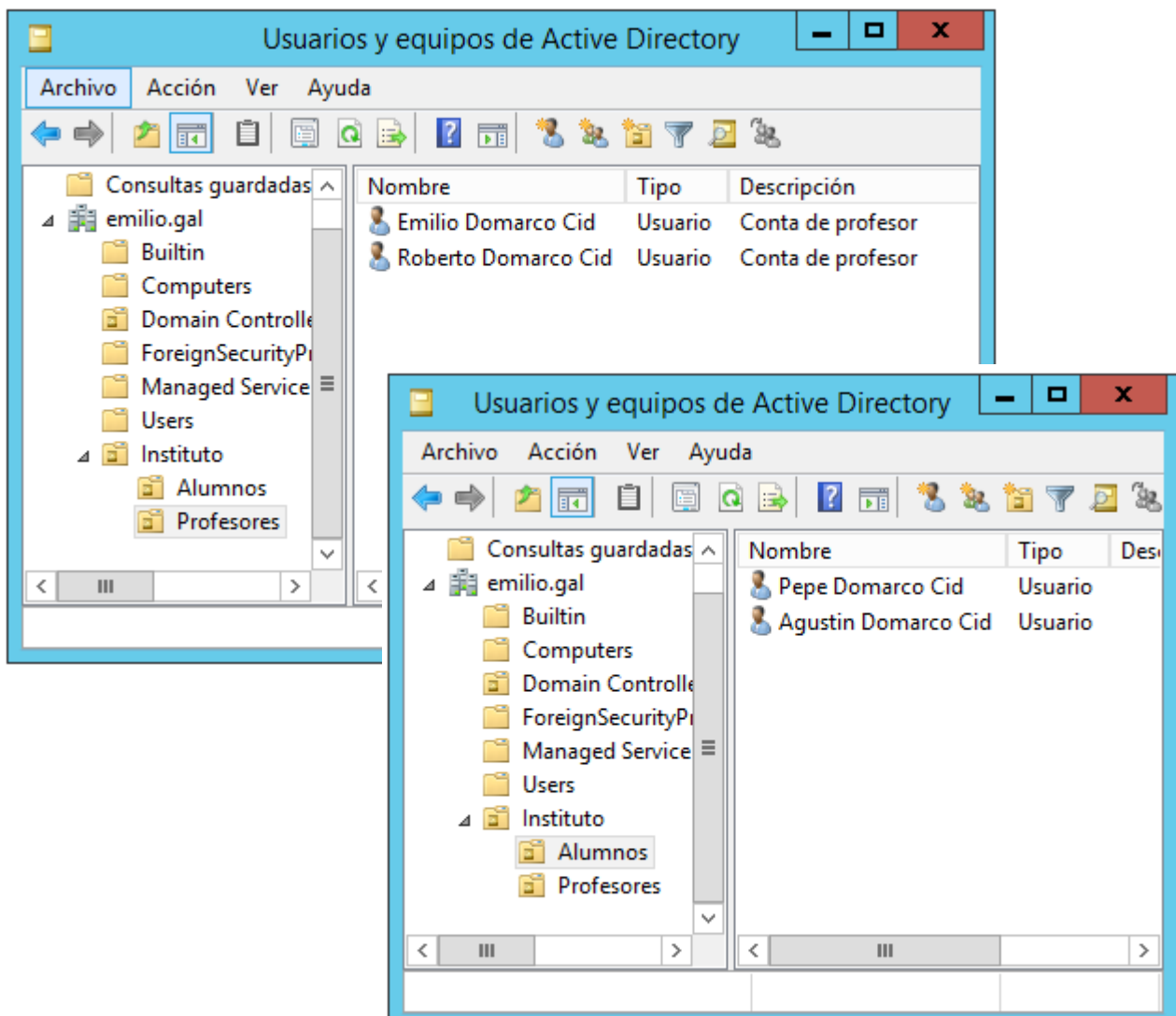
Indicámoslle a Unidade Organizativa a onde o queremos mover:



Se o proceso de engadir un usuario o facemos arrastrándoo, como agora con Roberto, cando o fagamos saíranos o seguinte aviso

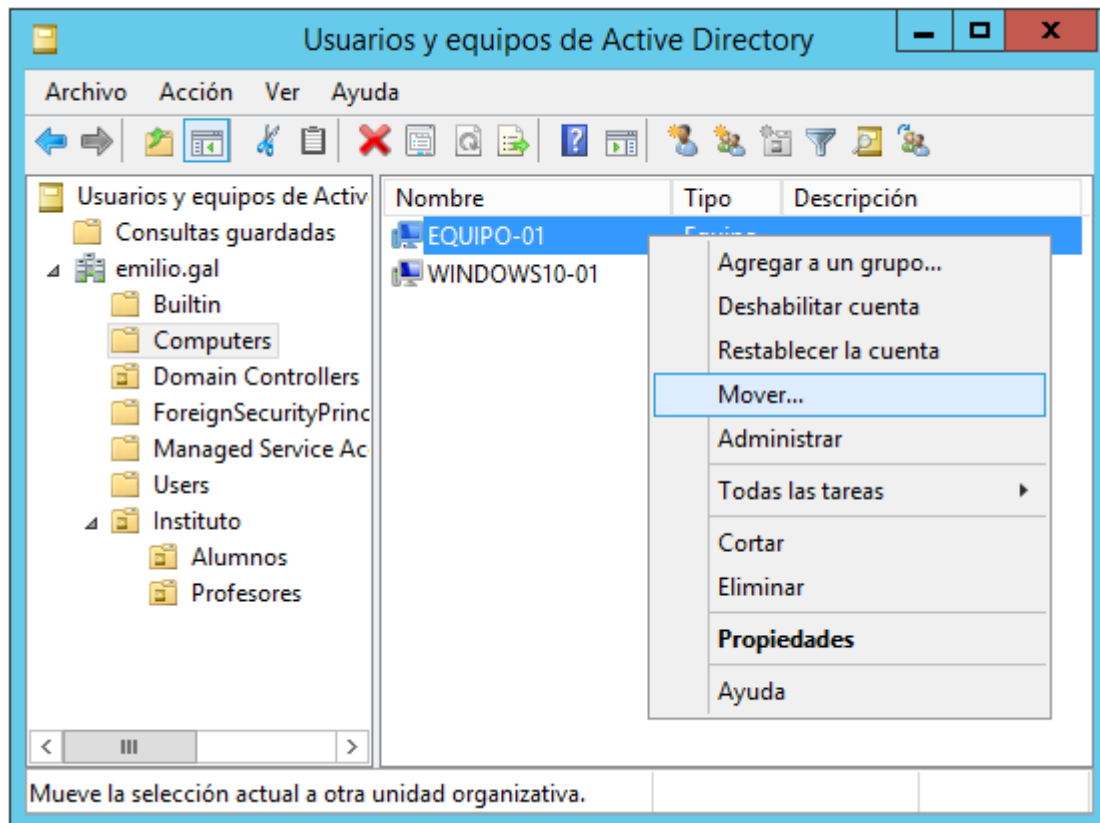


Repetimos a operación cos alumnos Pepe e Agustín arrastrándooos á Unidade Organizativa Alumnos e vemos xa como queda a estrutura:

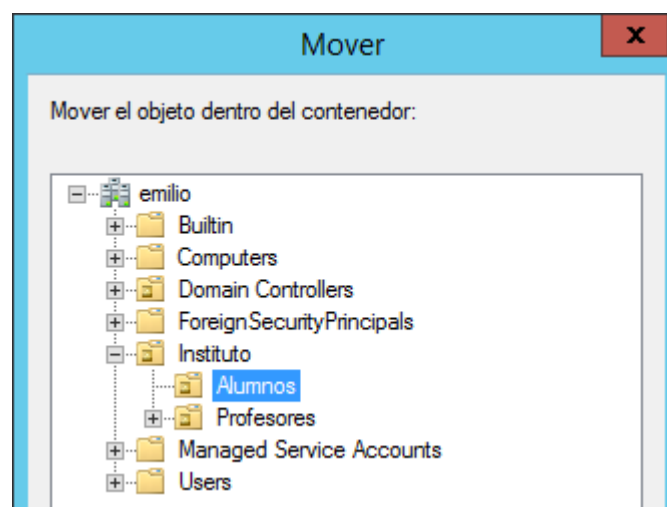


Asimesmo tamén poderemos engadir os ordenadores dentro da unidade organizativa que nos interesa. Por exemplo poderíamos introducir o ordenador EQUIPO-01 dentro dos Alumnos do instituto xa que imos supor que ese ordenador é duha aula na que traballan os alumnos.

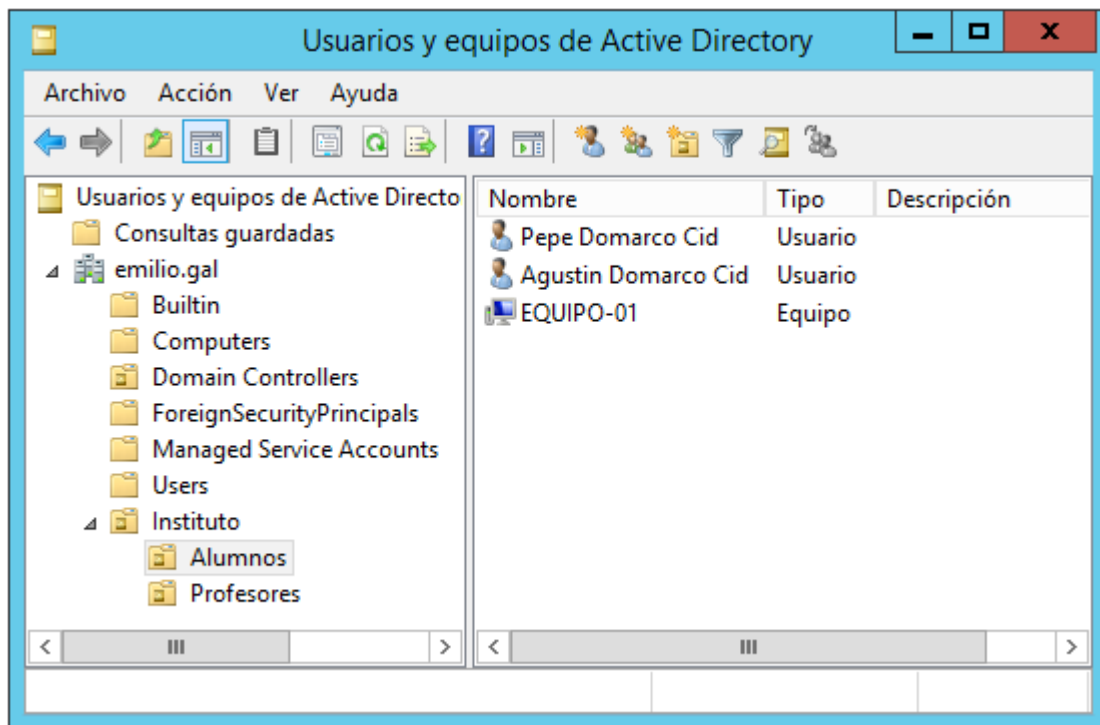
Para elo procederemos de xeito similar a como fixemos antes, e dicir arrastrándoo ou co botón dereito.



E lle dicimos a que Unidade Organizativa o queremos mover:



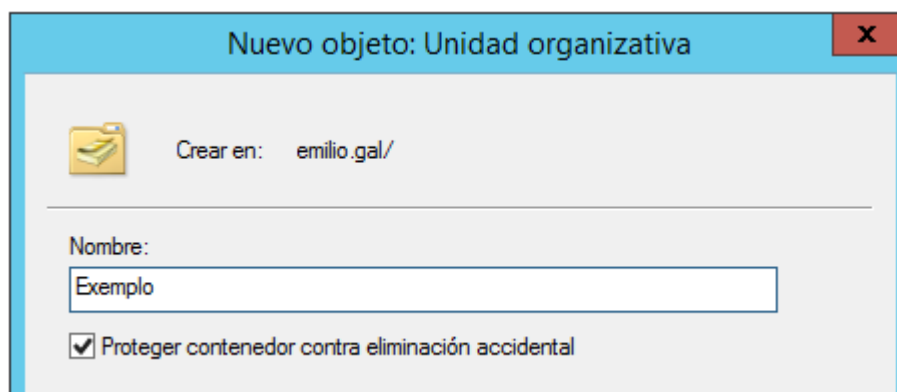
Agora se revisamos a estrutura xa vemos os usuarios e equipos dentro de Alumnos:



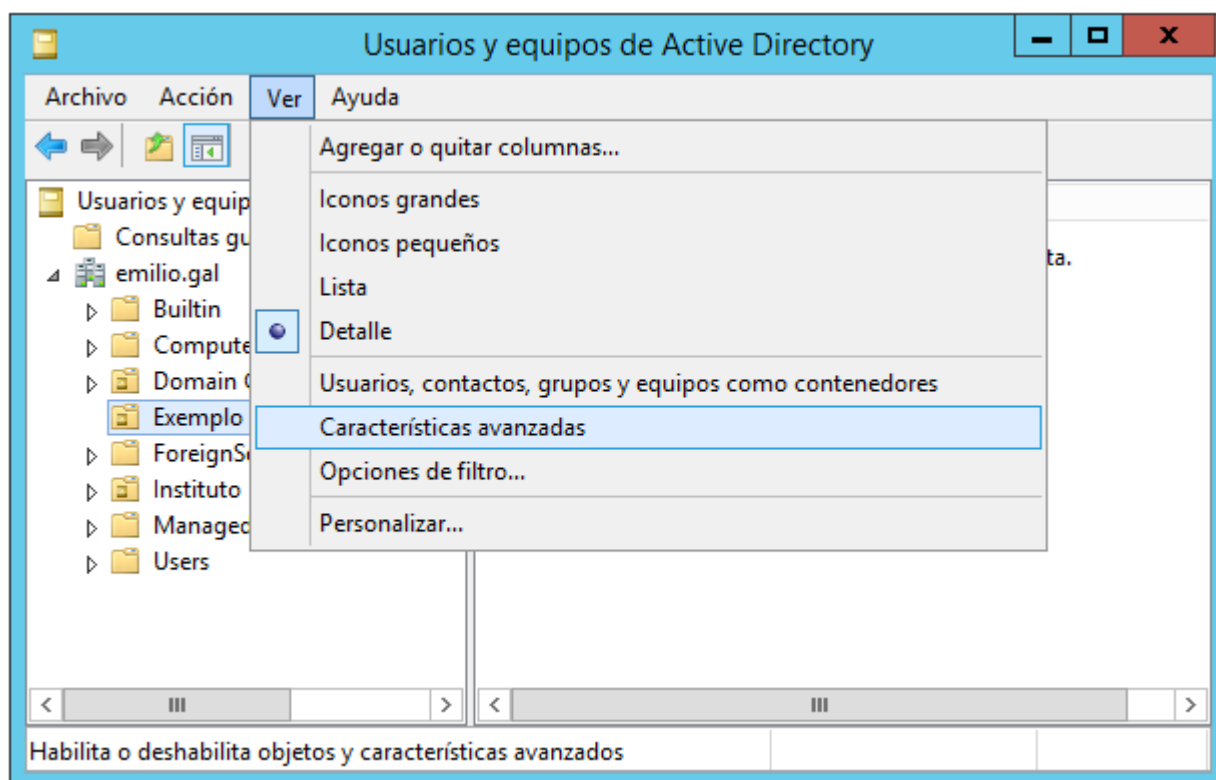
6.3.- Eliminar unha Unidade Organizativa

Para eliminar unha Unidade Organizativa o primeiro que temos que facer e asegurarnos de que está vacía, xa que ó eliminala tamén se eliminarán de xeito permanente os obxectos (usuarios, ordenadores, etc) que estén dentro dela.

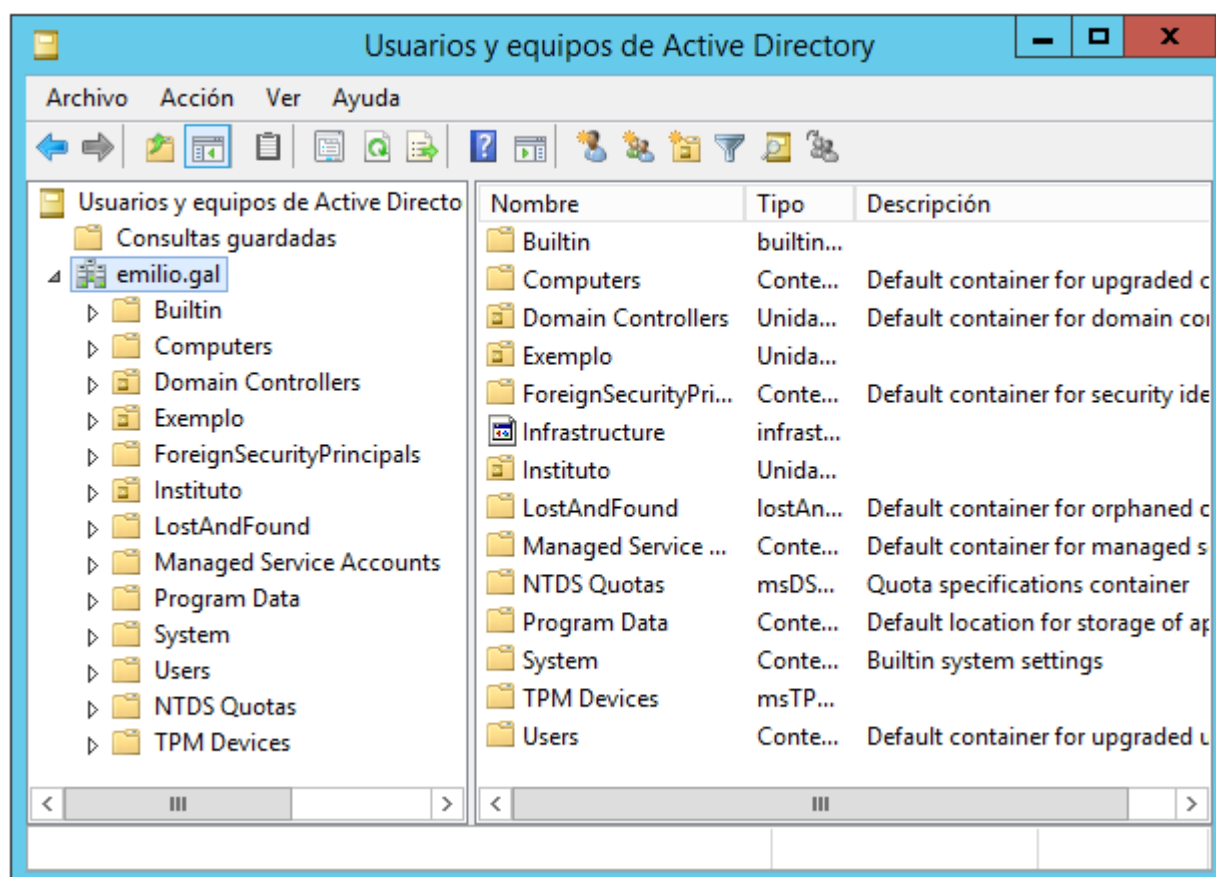
Pode ocorrer que cando queremos eliminar unha Unidade esta estea Protexida contra a eliminación accidental (así é como se crean por defecto, aínda que como vimos antes eliminamos esta protección a efectos didácticos) como se ve na imaxe.



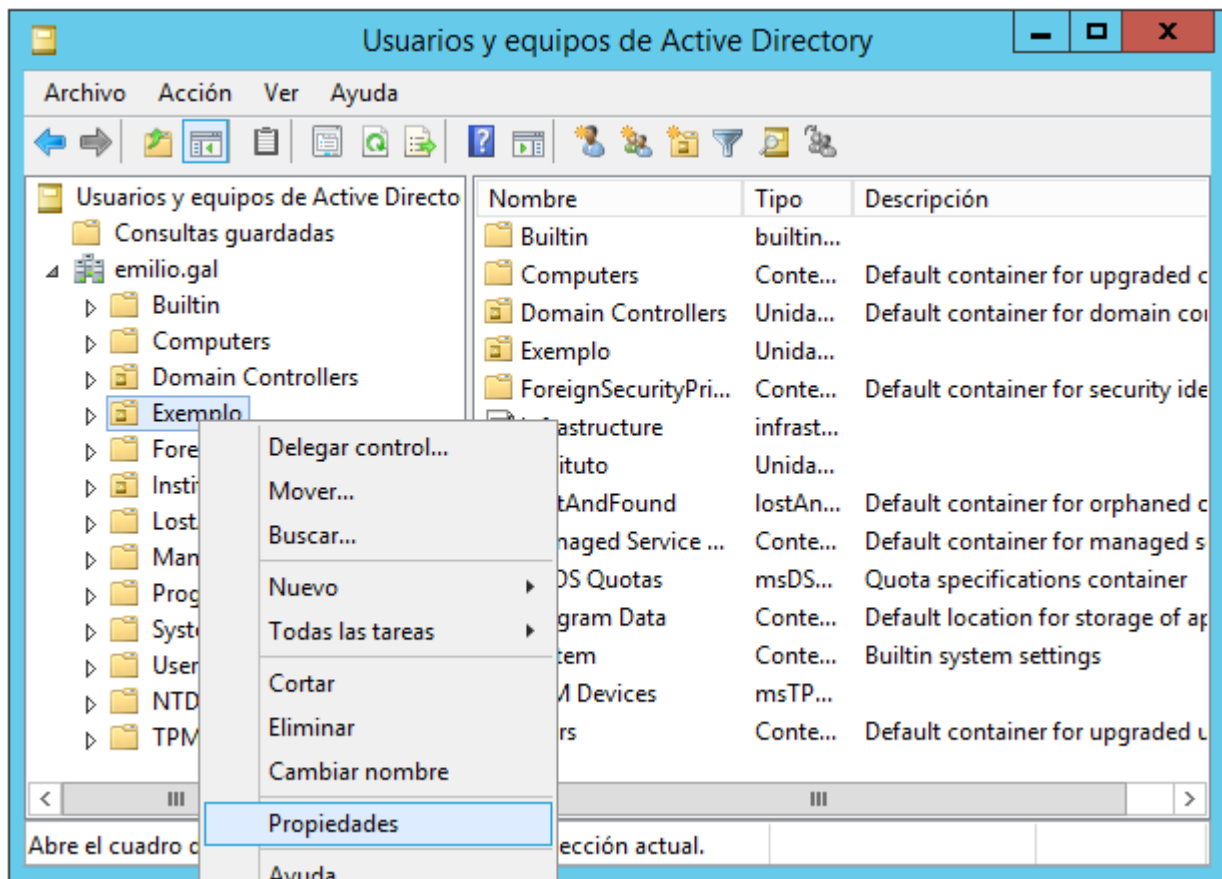
Para poder desprotexela o primeiro que deberemos facer é ir ó menú **Ver** e seleccionar a opción de **Características avanzadas**.



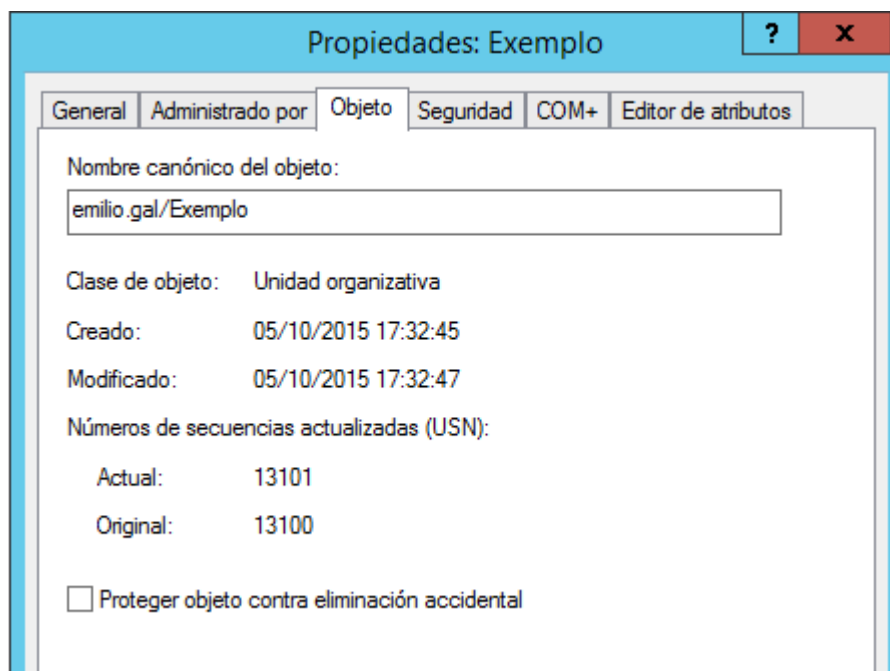
Observamos que xa aparece moita máis información do dominio:



Agora xa podemos pulsar co botón dereito sobre a Unidade Organizativa a borrar (neste caso a de Exemplo) e seleccionar propiedades:

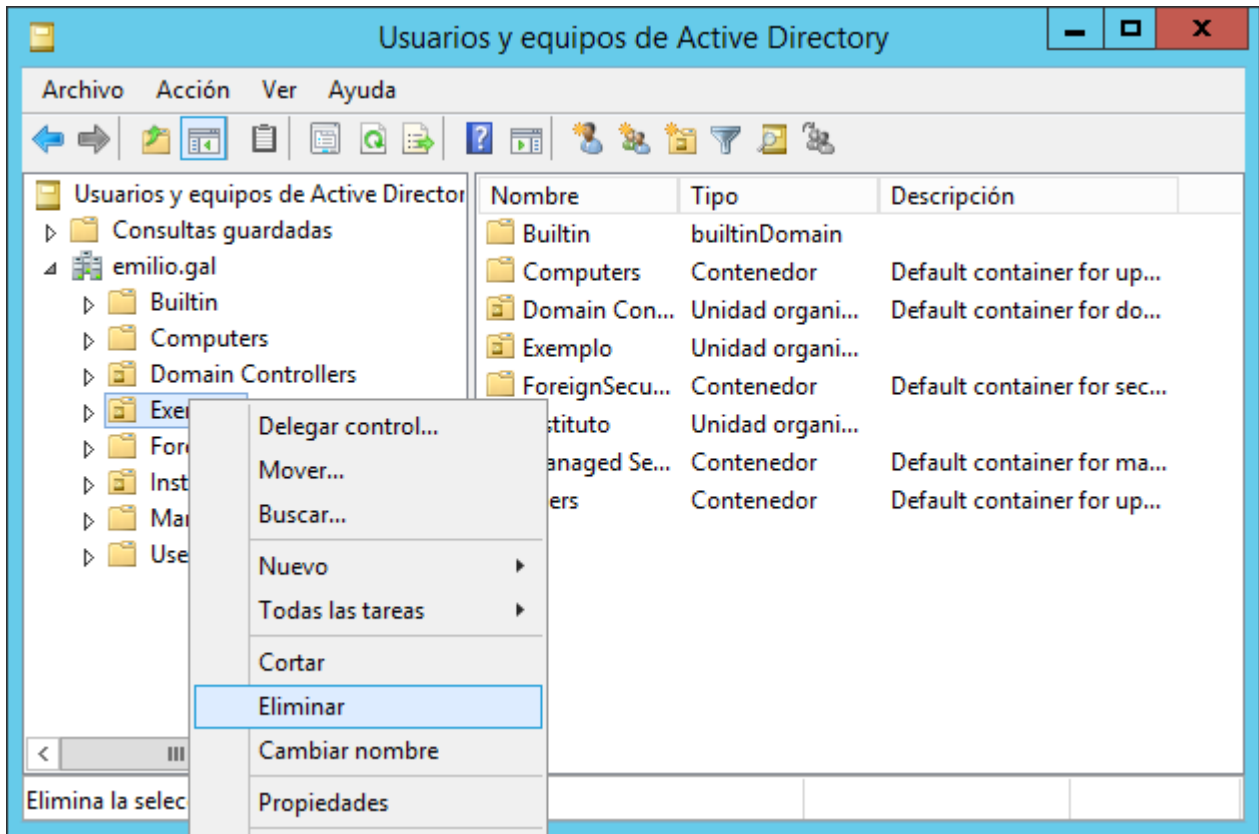


Ó pulsar en Propiedades ábrese a seguinte pantalla, onde iremos á solapa **Objeto** e xa podemos desmarcar a opción de **Proteger objeto contra eliminación accidental**.

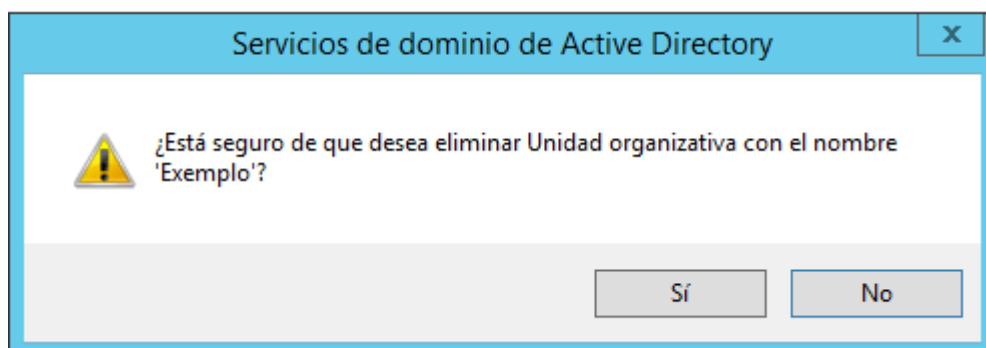


Unha vez desmarcada a opción xa poderíamos eliminar a Unidade Organizativa sempre tendo a precaución de eliminar os obxectos que existan.

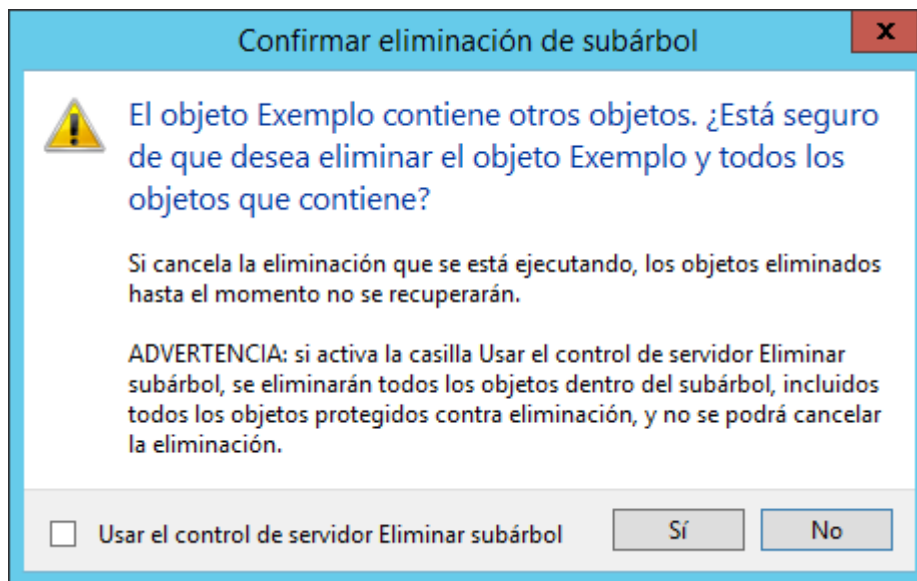
Para eliminar unha Unidade simplemente pulsamos nela co botón dereito e lle damos a Eliminar.



Pregúntanos se estamos seguros de que queremos eliminála, e neste caso lle dicimos que si.



Como dentro da Unidade Organizativa tiñamos un usuario (proba) nos informa de que se eliminarán os obxecto que existan dentro da Unidade, e si cancelamos a eliminación que se está executando os elementos eliminados non se poderán recuperar.



Unha vez rematado o proceso xa observamos que desapareceu a Unidade Exemplo.

