**ADMINISTRACIÓN DE SISTEMAS OPERATIVOS**

**Creación de Grupos en un Dominio**

**AUTOR**: Ana María Herrero Francisco

**FECHA**: 09/2024

**TABLA DE CONTENIDOS**

[1. GRUPOS DE USUARIOS. 3](#_Toc180862694)

[1.1 GRUPOS INTEGRADOS EN ACTIVE DIRECTORY 4](#_Toc180862695)

[1.2 GRUPOS INTEGRADOS DEL CONTENEDOR BUILTIN 4](#_Toc180862696)

[1.3 GRUPOS INTEGRADOS DEL CONTENEDOR USERS 7](#_Toc180862697)

[2. TIPOS DE GRUPOS. 8](#_Toc180862698)

[3. ÁMBITO DE LOS GRUPOS 10](#_Toc180862699)

[4. CUANDO USAR LOS TIPOS DE GRUPOS DE SEGURIDAD 12](#_Toc180862700)

[5. ADMINISTRACIÓN DE CUENTAS DE GRUPO 14](#_Toc180862701)

[5.1 DESDE LA INTERFAZ GRÁFICA 14](#_Toc180862702)

[5.2 CREACIÓN DE CUENTAS DE GRUPOS 14](#_Toc180862703)

[5.3 PARA CREAR GRUPOS 15](#_Toc180862704)

[5.4 PROPIEDADES DE LAS CUENTAS DE GRUPOS 15](#_Toc180862705)

[5.5 ADICIÓN DE MIEMBROS A UN GRUPO 16](#_Toc180862706)

[5.6 ELIMINACIÓN DE MIEMBROS DE UN GRUPO 18](#_Toc180862707)

[5.7 ADICIÓN DE UN GRUPO COMO MIEMBRO DE OTRO GRUPO 19](#_Toc180862708)

[5.8 ELIMINACIÓNDE UN GRUPOO COMO MIEMBRO DE OTRO GRUPO 20](#_Toc180862709)

[5.9 ELIMINACIÓN DE CUENTAS DE GRUPO 21](#_Toc180862710)

[6. CUANDO UTILIZAR CADA TIPO DE GRUPO 22](#_Toc180862711)

[7. CREACIÓN DE GRUPOS CON DSADD 25](#_Toc180862712)

1. GRUPOS DE USUARIOS.

Igual que creamos usuarios del dominio, también podemos crear grupos de usuarios del dominio.

Un grupo es una colección de cuentas de usuario. Los grupos simplifican la administración permitiendo asignar los permisos y derechos a un grupo de usuarios en lugar de tener que asignar los permisos a cada cuenta de usuario individual. Los usuarios pueden ser miembros de más de un grupo.

Los grupos en Active Directory son **conjuntos de objetos del dominio** que se administran como una única entidad. Los grupos pueden contener cuentas de usuario, cuentas de equipo, contactos y otros grupos. Cuando una cuenta de usuario o de equipo está incluida en un grupo se dice que es miembro del grupo.

Podemos utilizar los grupos para facilitar algunas tareas, como:

* **Simplificar la administración**: Podemos asignar permisos al grupo y éstos afectarán a todos sus miembros.
* **Delegar la administración**: Podemos utilizar la directiva de grupo para asignar derechos de usuario una sola vez y, más tarde, agregar los usuarios a los que queramos delegar esos derechos.
* Crear **listas de distribución de correo electrónico:** sólo se utilizan con los **grupos de distribución.**

La manera de identificar un grupo del dominio con su nombre completo consiste en utilizar su nombre, seguido de una arroba como separador y el nombre del dominio**.** Por ejemplo, para el grupo smr dentro del dominio rlopezs30.local, el nombre completo del grupo será**:** [**smr@rlopezs30.local.**](mailto:smr@rlopezs30.local)

Cuando se asignan permisos, se da a los usuarios la capacidad de acceder a recursos específicos y se define el tipo de acceso que tienen. Por ejemplo, si varios usuarios necesitaran leer el mismo archivo, se añadirían sus cuentas de usuario a un grupo. Entonces se dará a ese grupo el permiso de leer el archivo.

Además de las cuentas de usuario se pueden añadir contactos, equipos y otros grupos a un grupo. Cuando se añaden equipos a un grupo se puede simplificar el proceso de conceder una tarea de sistema para que un equipo acceda a un recurso de otro equipo.

* 1. GRUPOS INTEGRADOS EN ACTIVE DIRECTORY

**Active Directory proporciona un conjunto de grupos integrados que dan a los usuarios derechos y permisos adecuados para realizar tareas específicas**. Los derechos de usuario determinan las tareas del sistema que puede realizar un usuario o un miembro del grupo integrado. Estos grupos permiten simplificar la asignación de derechos y permisos a otras cuentas o grupos. Los grupos integrados son locales, globales y universales.

Los grupos predeterminados del contenedor **Builtin** tienen el ámbito de grupo Integrado local. No se puede cambiar ni el ámbito del grupo ni su tipo.

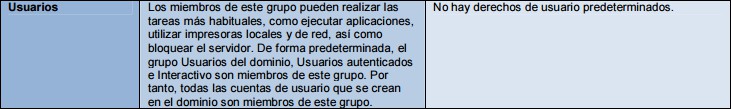
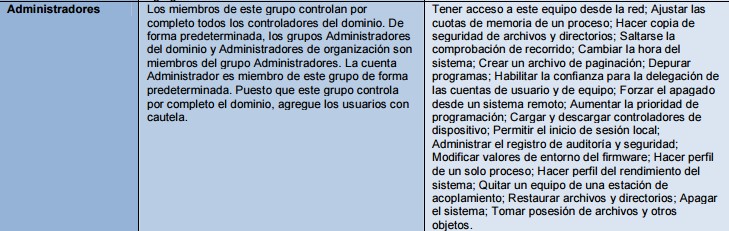
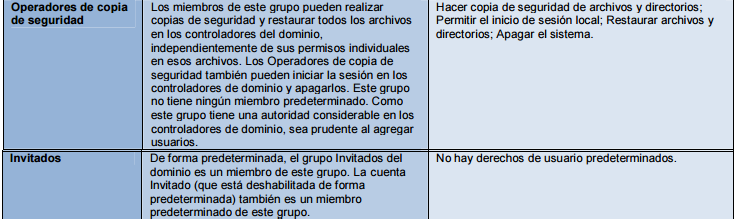
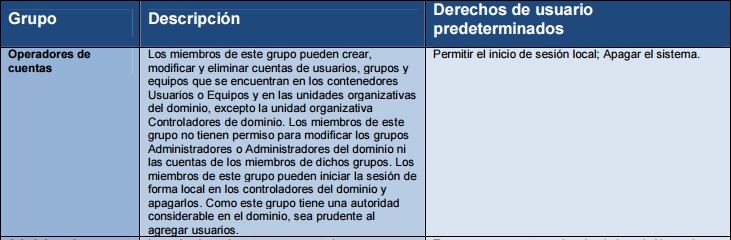
Los grupos predeterminados del contenedor **Users** incluyen grupos definidos con ámbito Global y ámbito Local de dominio.

Tanto los grupos del contenedor Builtin, como los del contenedor Users, pueden cambiarse libremente de contenedor, siempre que se mantengan dentro del mismo dominio.

* 1. GRUPOS INTEGRADOS DEL CONTENEDOR BUILTIN

Los grupos predeterminados se encuentran en el contenedor Builtin y en el contenedor Users. Los grupos predeterminados del contenedor Builtin tienen el ámbito de grupo Integrado local. Su ámbito de grupo y tipo de grupo no se pueden cambiar. El contenedor Users incluye grupos definidos con ámbito Global y grupos definidos con ámbito Local de dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas del dominio, pero no se pueden mover a otros dominios.

La siguiente tabla muestra algunos de los grupos integrados del contenedor Builtin.



* 1. GRUPOS INTEGRADOS DEL CONTENEDOR USERS

La siguiente tabla muestra algunos de los grupos integrados del contenedor Users.

Tabla

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza baja

Los grupos predeterminados, como es el caso del grupo Administradores del dominio, son grupos de seguridad que se crean automáticamente cuando se crea un dominio de Active Directory. Estos grupos predefinidos pueden usarse para ayudar a controlar el acceso a los recursos compartidos y para delegar roles administrativos específicos en todo el dominio.

A muchos grupos predeterminados se les asigna automáticamente un conjunto de derechos de usuario que autorizan a los miembros del grupo a realizar acciones específicas en un dominio, como iniciar sesión en un sistema local o realizar copias de seguridad de archivos y carpetas. Por ejemplo, un miembro del grupo Operadores de copia de seguridad puede realizar operaciones de copia de seguridad para todos los controladores de dominio del dominio.

Cuando se agrega un usuario a un grupo, ese usuario recibe:

* Todos los derechos de usuario asignados al grupo
* Todos los permisos asignados al grupo para los recursos compartidos

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

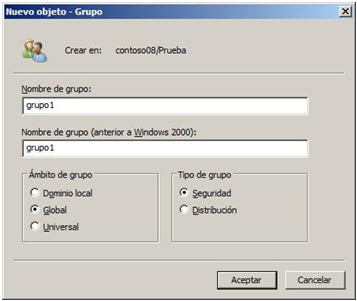
1. TIPOS DE GRUPOS.

Existen dos tipos de grupos en Active Directory:

* **Grupos de distribución**: se utilizan junto con programas como Microsoft Exchange Server, para crear listas de distribución de correo electrónico, y permiten el envío de mensajes a un conjunto de usuarios.. Están orientados a agrupar a diferentes usuarios para que cuando el grupo recibe un mail automáticamente se envíe una copia de este a todos los usuarios que pertenecen al grupo de distribución.

No tienen un SID establecido, por lo que no pueden ser usados para incluirlos en ACL Estos grupos no disponen de características de seguridad, por lo que no pueden aparecer en las listas de control de acceso discrecional (DACL, Discretionary Access Control Lists).

* **Grupos de seguridad**: permiten asignar permisos a las cuentas de usuario, de equipo y grupos sobre los recursos compartidos. Los grupos de Seguridad son los que utilizaremos para controlar a los usuarios, es decir para asignar derechos y establecer restricciones de acceso a los diferentes recursos que se encuentran en la red. A través de los grupos de seguridad podemos:
* **Asignar derechos de usuario**: podemos establecer qué acciones pueden llevar a cabo sus miembros dentro del dominio (o del bosque).
* **Asignar permisos para recursos**: nos permite definir quién accede a cada recurso y en qué condiciones (control total, sólo lectura, etc.). Es posible establecer permisos de forma predeterminada sobre diferentes objetos del dominio para ofrecer distintos niveles de acceso.



1. ÁMBITO DE LOS GRUPOS

El ámbito de un grupo establece su alcance en el bosque o árbol de dominios, es decir, en qué partes de la red puede utilizarse, el tipo de cuentas que pueden formar parte de él y dónde se pueden conceder permisos de red para el grupo. En ese sentido, pueden pertenecer a una de las siguientes categorías:

* **Ámbito local**: entre sus miembros pueden encontrarse uno o varios de los siguientes tipos de objetos:
  + cuentas de usuario o equipo de cualquier dominio.
  + Otros grupos de ámbito local del mismo dominio.
  + Grupos de ámbito global (Globales) de cualquier dominio.
  + Grupos de ámbito universal (Universales) de cualquier dominio.

Los permisos asignados a los grupos locales son efectivos únicamente para los recursos del dominio en el que se crea el grupo y su replicación se limita a ese dominio. Quedan fuera de su ámbito pues otros dominios del árbol, o del bosque. Son empleados para asignar derechos de usuario y permisos a recursos sólo del mismo dominio donde pertenece el grupo dominio local.

Este tipo de grupos solo será visible en el propio dominio donde se ha creado o al que pertenece.

* **Ámbito global**: sólo pueden incluir:
  + cuentas que pertenezcan al mismo dominio en el que esté definido el propio grupo
  + grupos globales del mismo dominio.

Los grupos globales se definen en un dominio, pero no se replican a otros controladores de dominio. Los permisos asignados a los grupos globales tienen validez en cualquier dominio dentro del bosque al que pertenecen.

* **Ámbito universal**: entre sus miembros pueden encontrarse:
  + Usuarios y grupos Globales y Universales de cualquier dominio dentro del bosque donde resida el grupo universal.

Los grupos universales se definen en un dominio, pero se replican a los dominios del bosque, lo que puede generar un mayor tráfico de replicación. Por lo tanto, se recomienda su uso en redes con múltiples dominios donde sea necesario compartir recursos y permisos en todo el bosque. Los permisos asignados a los grupos universales se aplican en cualquier dominio del bosque.

Como bien indica su nombre estos pueden contener objetos de cualquiera de los dominios del bosque y puede utilizarse para asignar permisos y derechos en cualquier dominio del bosque.

Este tipo de grupos será visible desde cualquiera de los dominios del bosque. Utilizad grupos universales para anidar grupos globales, de modo que podáis asignar permisos a recursos relacionados en múltiples dominios. Y recordad que el nivel de funcionalidad del dominio ha de ser Nativo o superior para usar grupos universales.

Escala de tiempo

Descripción generada automáticamente

**Cuando se crea un grupo se debe seleccionar un tipo de grupo y un ámbito del grupo**.

El ámbito de un grupo determina dónde se puede utilizar el grupo en la red. Los tres ámbitos de los grupos son dominio local, global y universal.  
Para verlo más claro, vamos a incluir aquí una tabla resumen sobre los distintos tipos de grupos:

Tabla

Descripción generada automáticamente

1. CUANDO USAR LOS TIPOS DE GRUPOS DE SEGURIDAD

La elección del tipo de grupo adecuado depende del alcance necesario y las necesidades específicas de administración de permisos y accesos en tu entorno. Al seleccionar el tipo de grupo correcto, se logra un mejor rendimiento y eficiencia en la administración del Directorio Activo, asegurando que los usuarios adecuados tengan acceso a los recursos necesarios dentro del dominio.

1. **Grupos locales de dominio:**

* **Uso recomendado**: los grupos locales de dominio son ideales cuando se necesitan asignar permisos y controlar el acceso a los recursos del dominio que están ubicados en el mismo dominio en el que se creó el grupo local del dominio.
* **Alcance limitado**: estos grupos solo se aplican al dominio específico en el que se crean y su replicación se limita a ese dominio.
* **Ejemplo de uso**: si tenemos un recurso específico en un dominio y queremos conceder permisos a un grupo de usuarios dentro de ese dominio, podemos utilizar un grupo local de dominio. De esta forma, para cada recurso compartido (impresora, directorio compartido, etc.) se crean tantos grupos locales como configuraciones de permisos se necesiten. Por ejemplo, control total sobre un directorio o de solo lectura: GL\_ControlTotalDocumentos y GL\_LecturaDocumentos. Se configuran los permisos con estos dos grupos locales y, por último, tan solo tendremos que añadir los grupos globales o usuarios del dominio individuales a cada uno de los grupos en función de los permisos que queramos darles.

1. **Grupos globales**:

* **Uso recomendado**: Se utilizan para organizar a los usuarios que comparten requisitos de acceso a la red similares. Los grupos globales se pueden utilizar para asignar permisos para obtener acceso a los recursos que se encuentran en cualquier dominio dentro del mismo bosque.
* **Alcance extendido**: los permisos asignados a los grupos globales se aplican a cualquier dominio dentro del bosque al que pertenecen.
* **Ejemplo de uso**: podemos agrupar usuarios con una función similar y otorgar permiso para acceder a un recurso, como una impresora o una carpeta compartida y archivos, que está disponible en el dominio local o en otro dominio del mismo bosque.

1. **Grupos universales:**

* **Uso recomendado**: los grupos universales sirven para agrupar elementos de diferentes dominios en un mismo grupo. Además, se recomienda el uso de grupos universales cuando un mismo conjunto de usuarios pertenecientes a varios dominios deben recibir acceso a recursos situados en dominios distintos.
* **Alcance amplio**: los permisos asignados a los grupos universales se aplican a cualquier dominio dentro del bosque y su replicación abarca todo el árbol del bosque.
* **Ejemplo de uso**: si tenemos varios dominios en un bosque y necesitamos otorgar permisos, a usuarios de diferentes dominios, para acceder a recursos en todo el bosque, puedes utilizar un grupo universal para gestionar esos permisos.

1. ADMINISTRACIÓN DE CUENTAS DE GRUPO

Los grupos nos permiten administrar objetos del dominio de forma conjunta. Un grupo puede estar formado por cuentas de usuario, de equipo, contactos o, incluso, otros grupos.

La idea principal consiste en asignar permisos a un grupo. Después bastará con hacer a un usuario miembro de ese grupo para que obtenga sus permisos. De este modo, sólo tendremos que asignar permisos una vez al grupo, en lugar de hacerlo para cada una de las cuentas de usuario de manera individual.

Las acciones más frecuentes que podemos realizar con cuentas de grupo son: crearlas, modificar sus valores, añadir miembros a un grupo, eliminar miembros de un grupo, convertir a un grupo en miembro de otro grupo, conseguir que un grupo deje de ser miembro de otro y eliminar grupos.

* 1. DESDE LA INTERFAZ GRÁFICA

Para administrar grupos en el Directorio Activo desde la interfaz gráfica podemos utilizar la herramienta “Usuarios y Equipos de Active Directory” desde la ventana de “Administrador del Servidor”. En el contenedor Users podemos crear grupos en el dominio.

* 1. CREACIÓN DE CUENTAS DE GRUPOS

Para crear grupos debemos tener claro la infraestructura de la empresa, los usuarios y grupos que van a ser miembros del grupo creado e incluso los grupos a los cuales el que estamos creando pertenecerá.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* 1. PARA CREAR GRUPOS

Desde Inicio/**Herramientas administrativas/Usuarios y equipos de Active Directory** Sobre el contenedor en el que queramos crear el grupo, menú contextual, **Nuevo, Grupo**.

Se introducen los campos:

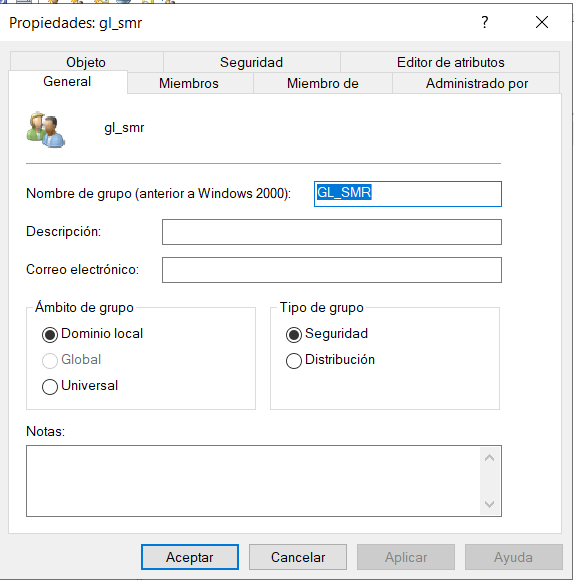
* **Nombre del grupo**: nombre del grupo con el que quedará reconocido en el sistema. El

S.O. le asigna un **SID** (*Security IDentifiers*) al grupo para gestionarlo de forma interna, transparente al usuario. **El nombre del grupo tiene ser único en el dominio o dentro de cada equipo local, pudiendo**

* 1. PROPIEDADES DE LAS CUENTAS DE GRUPOS

Para modificar un grupo tenemos que seleccionar el grupo y con el botón derecho del ratón hacer clic sobre Propiedades.

Desde aquí disponemos de las características de la cuenta del grupo organizada en seis pestañas diferentes.



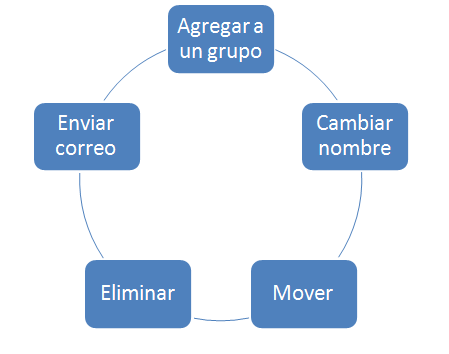
En la pestaña **General**, además de poder cambiar el Nombre del grupo (anterior a Windows 2000), la Descripción y el correo electrónico donde se recibirán las incidencias relacionadas con el grupo, también podemos modificar el Ámbito del grupo y el Tipo de grupo. Desde la pestaña **miembros**, elegiremos los usuarios, equipos o grupos que son miembros del grupo que estamos editando.

La pestaña **Miembro de**, nos permite que este grupo sea, a su vez, miembro de un grupo distinto.

La pestaña **Administrado por**, nos permite delegar la administración de este grupo en otro usuario diferente.

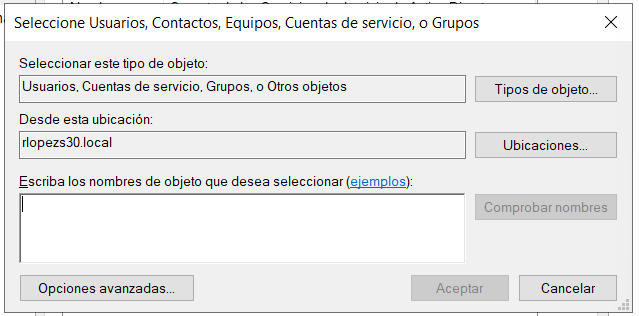
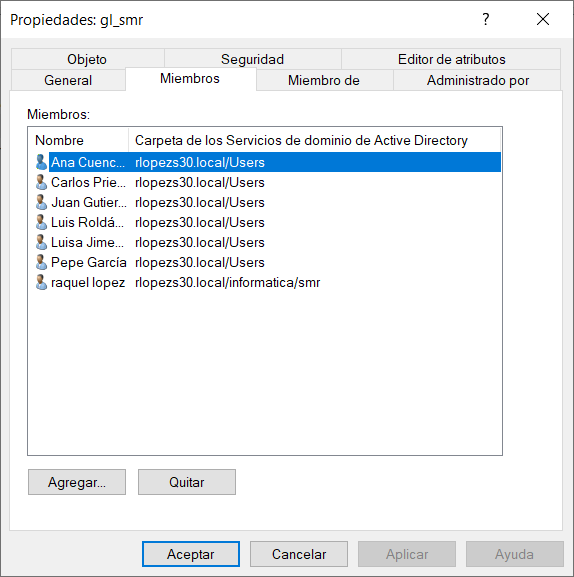
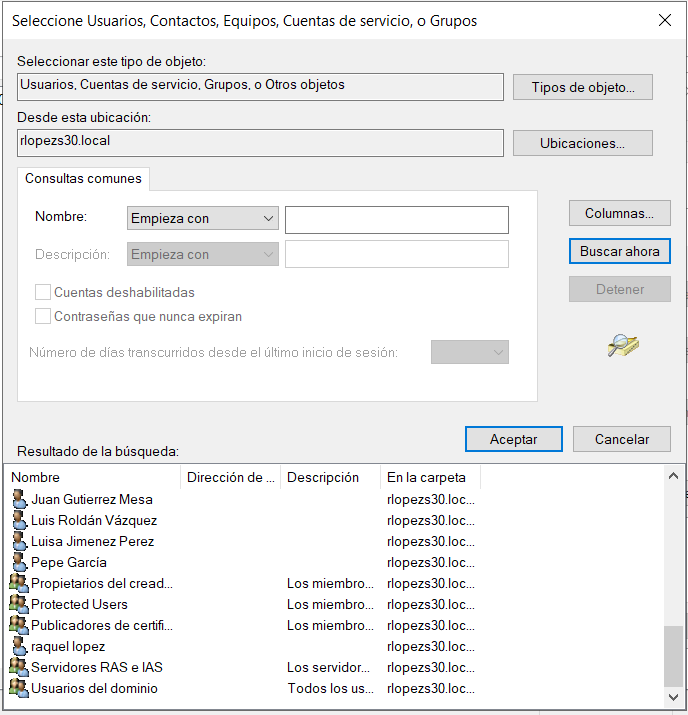
La pestaña **Objeto** nos muestra el *nombre canónico* del grupo. El nombre canónico se refiere al nombre completo y único de un objeto dentro del directorio. Este nombre incluye la ruta completa desde el nivel del dominio hasta el objeto específico.

La pestaña **Seguridad** nos permite especificar permisos a grupos o usuarios. La pestaña **Editor de atributos**, nos permite ver y editar los atributos del grupo.



* 1. ADICIÓN DE MIEMBROS A UN GRUPO

Para añadir un nuevo miembro a un grupo debemos abrir la ventana **Propiedades** de dicho grupo y elegir la solapa **Miembros**. Si conocemos los nombres de las cuentas que vamos a incluir, sólo tendremos que escribirlos en el cuadro titulado **Escriba los nombres de objeto que desea seleccionar**. Sin embargo, también podemos elegirlos de una lista haciendo clic sobre **Opciones avanzadas**.



Si sabemos los primeros caracteres que tienen las cuentas de usuario que estamos buscando, podemos escribirlos a continuación de **Empieza con**. Lo más sencillo es dejarlo todo en blanco y hacer clic sobre **Buscar ahora**. En el cuadro Resultado de la búsqueda aparecen todos los elementos que podemos seleccionar.

Sólo queda elegir los objetos que queremos añadir como miembros del grupo. Es posible utilizar las teclas Mayúsculas (Shift) y Control (Ctrl) combinadas con el clic del ratón para realizar selecciones múltiples.

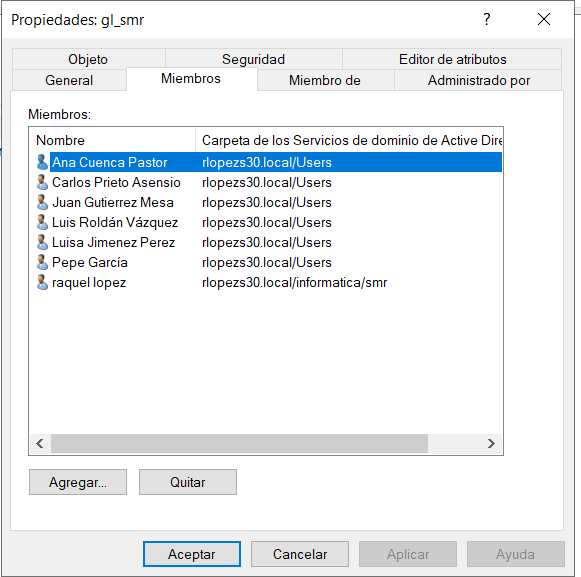
La ventana Seleccione Usuarios, Contactos, Equipos, Cuentas de servicio o Grupos vuelve a su aspecto normal y muestra los nombres de las cuentas que hemos elegido. De vuelta a la ventana propiedades, veremos que ya aparecen los nuevos miembros.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

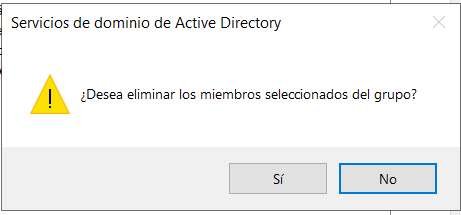
Descripción generada automáticamente

* 1. ELIMINACIÓN DE MIEMBROS DE UN GRUPO

Para eliminar a cualquiera de los miembros de un grupo, basta con volver a la ventana **Propiedades** de dicho grupo y elegir, de nuevo, la pestaña **Miembros**. A continuación, elegiremos el usuario que queremos que deje de ser miembro del grupo.



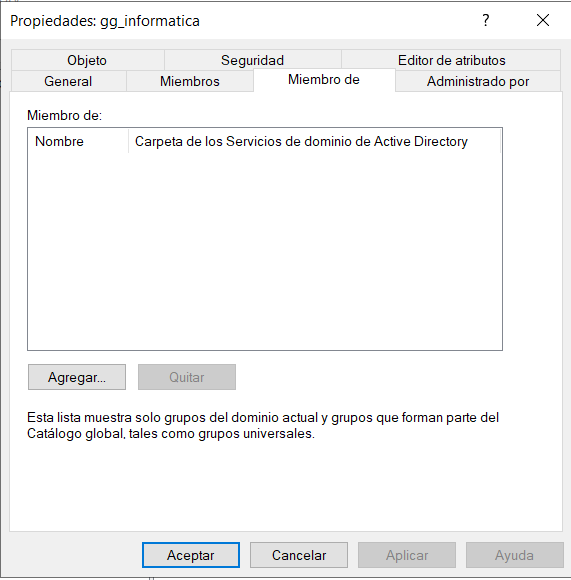
También podemos utilizar las teclas Mayúsculas (Shift) y Control (Ctrl) combinadas con el clic del ratón para poder elegir varias cuentas de usuario y eliminarlas todas al mismo tiempo.

Después de hacerlo, aparecerá un mensaje para confirmar que estamos seguros de la eliminación.

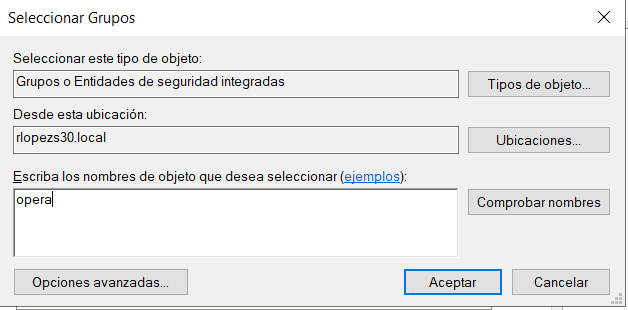
**Al eliminar una cuenta de la lista de miembros de un grupo, no estamos borrando dicha cuenta, sólo le estamos quitando los permisos heredados de dicho grupo**.

* 1. ADICIÓN DE UN GRUPO COMO MIEMBRO DE OTRO GRUPO

La opción **Miembro de** permite visualizar y administrar las relaciones de pertenencia entre los grupos. Al convertir a un grupo en miembro de otro grupo, éste heredará todos sus permisos. Y, por lo tanto, también sus miembros. De este modo, podemos crear una estructura jerárquica de grupos, evitando repetir en unos grupos la asignación de permisos que hayamos configurado en otros.



Para que un grupo sea miembro de otro grupo, desde la ventana **Propiedades** de dicho grupo, elegiremos la pestaña **Miembro de**. Esto hará que se muestre la ventana **Seleccionar Grupos**, casi idéntica a la ventana Seleccione Usuarios, Contactos, Equipos, Cuentas de servicio o Grupos.



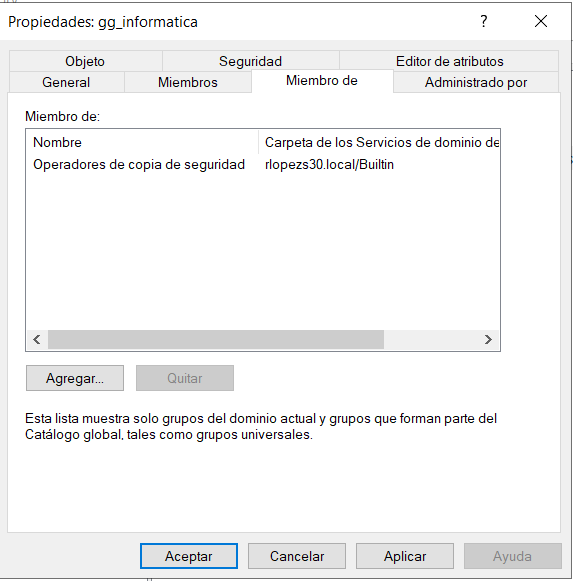
De la misma manera, podemos hacer clic, directamente, sobre el botón **Opciones avanzadas** y hacer una búsqueda o elegir el grupo de la lista completa.

Sin embargo, si sabemos cómo empieza el nombre del grupo que buscamos, podemos escribirlo en el cuadro de texto **Escriba los nombres de objeto que desea seleccionar**. Si existe más de un nombre de grupo que comienza por los mismos caracteres, se mostrará una ventana titulada **Nombres múltiples encontrados**. Seleccionamos el grupo y aceptamos. En la ventana **Seleccionar Grupos**, comprobamos que ya aparece el grupo elegido.

Interfaz de usuario gráfica, Texto, Aplicación

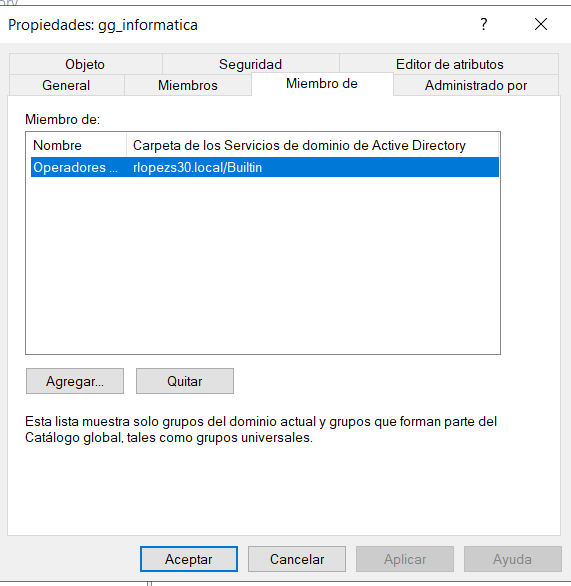
Descripción generada automáticamente

Para completar la selección hacemos clic sobre el botón **Aceptar**. De esta forma, hemos conseguido que el grupo elegido aparezca en la lista **Miembro de**. Hacemos clic sobre Aceptar y completamos el proceso.



* 1. ELIMINACIÓNDE UN GRUPOO COMO MIEMBRO DE OTRO GRUPO

Es la operación contraria a la anterior, es decir, lograr que un grupo deje de ser miembro de otro grupo, sólo hay que volver a la ventana **Propiedades** de dicho grupo y elegir la pestaña **Miembro de**. Una vez ahí, elegimos el grupo que queremos eliminar, y hacemos clic sobre el botón **Quitar**. Al hacerlo,aparecerá un mensaje para confirmar que estamos seguros de la eliminación.



Al volver a la ventana de propiedades,

comprobaremos que el grupo ya no aparece.

Interfaz de usuario gráfica, Texto, Aplicación

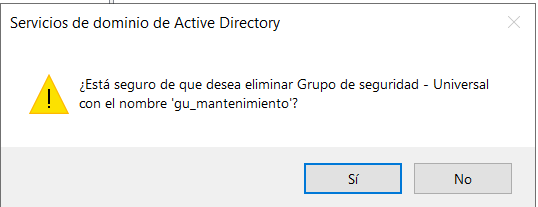
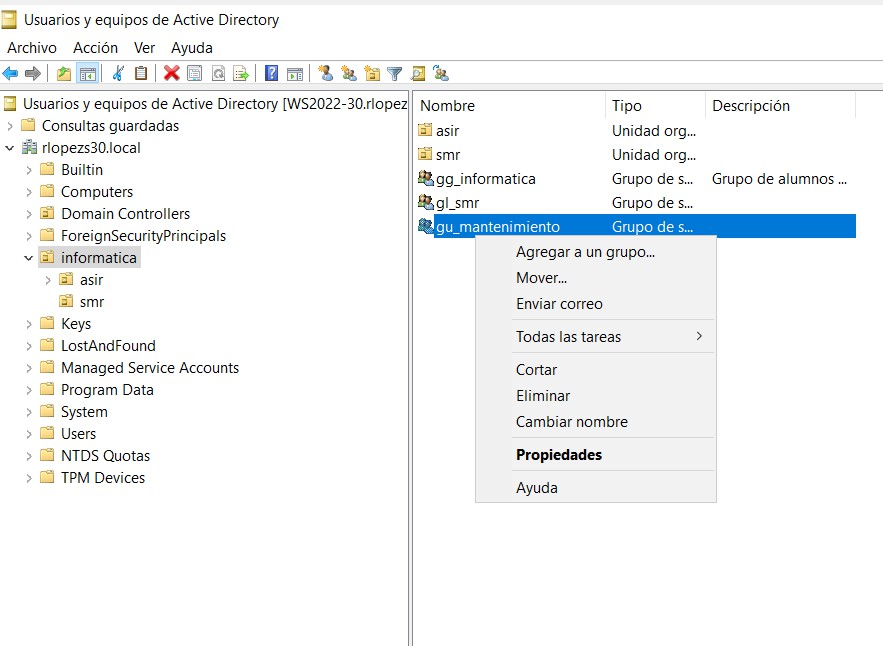
Descripción generada automáticamente

* 1. ELIMINACIÓN DE CUENTAS DE GRUPO

No es frecuente que se eliminen grupos en un dominio. Sin embargo, en ocasiones podremos necesitar reestructurar el esquema de nuestra red y puede resultar interesante distribuir las cuentas de una forma diferente a como lo habíamos hecho hasta ese momento. En ese escenario, será muy útil crear nuevos grupos y eliminar los que ya teníamos.

Eliminar un grupo no significa eliminar todas sus cuentas miembro, pero sí perderemos los privilegios asignados al propio grupo.

Desde Usuarios y Equipos de Active Directory, hacemos con el botón derecho sobre el grupo que queremos eliminar…



Aparecerá un mensaje para confirmar que estamos seguros de la eliminación. Si estamos conformes, hacemos clic sobre el botón **Sí**.

1. CUANDO UTILIZAR CADA TIPO DE GRUPO

Los grupos con ámbito local de dominio nos ayudan a definir y administrar el acceso a los recursos en un solo dominio. Por ejemplo, para conceder a cinco usuarios acceso a una impresora determinada, podemos agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si más tarde deseamos dar a esos cinco usuarios acceso a una nueva impresora, debemos especificar nuevamente las cinco cuentas en la lista de permisos de la nueva impresora.

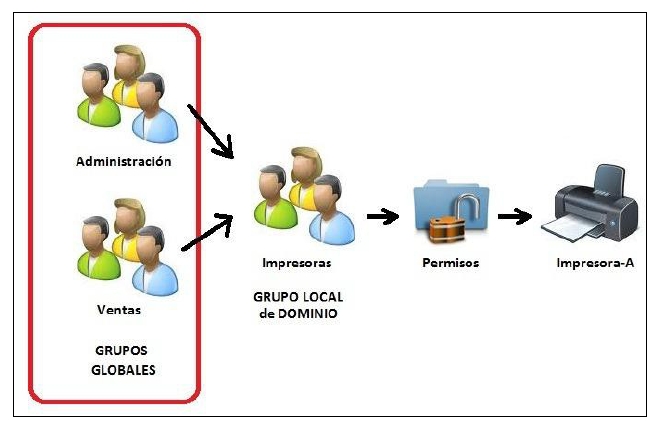
Si planeamos antes los grupos, podemos simplificar esta tarea administrativa rutinaria. Para hacerlo, deberemos crear un grupo de seguridad con ámbito local de dominio y asignarle los permisos necesarios para tener acceso a la impresora. Ahora añadimos a los 5 usuarios como miembros del nuevo grupo con lo cual podrán acceder a la impresora.

Si ahora deseamos dar a esos 5 usuarios acceso a una nueva impresora, basta con añadir a la lista de permisos de esa impresora el grupo local anteriormente creado (1 operación) y no añadir manualmente a los 5 usuarios (5 operaciones).

Además, si queremos que un usuario deje de poder usar las impresoras, bastará con sacar a dicho usuario del grupo, con lo que habremos conseguido que no pueda usar dichos recursos. Si no usamos grupos, no nos quedaría más remedio que ir impresora por impresora e ir quitándole los permisos al usuario por cada una de ellas.

Pero, ¿y si necesitamos que estos 5 usuarios impriman en una impresora situada en otro domino del bosque?

Para ello, en lugar de añadir los usuarios a un grupo local de dominio, lo conveniente es colocar las cinco cuentas de usuario en un grupo con ámbito global y agregar este grupo global como miembro del grupo local de dominio que da permisos sobre las impresoras. De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque.



Imaginemos que tenemos 5 usuarios de nuestro sistema, que tienen unas necesidades similares, pongamos por ejemplo que necesitan imprimir en plotters de gran tamaño.

Si tenemos un plotter de este tipo, podríamos añadir a la ACL del plotter a los 5 usuarios, pero es mucho más cómodo incluir a los 5 usuarios en un grupo (NEC\_PLOTTER por ejemplo) e indicar al plotter que dicho grupo tiene permiso para usarlo.

¿Y este grupo, de que tipo debería ser?

Si lo asignamos como Dominio Local, podremos usar el plotter siempre que esté dentro de nuestro dominio local. Sin embargo, si en otro dominio del bosque se instala un nuevo plotter, ellos no podrán ver el grupo NEC\_PLOTTER puesto que dicho grupo “no sale” de nuestro dominio de ninguna forma.

Si lo asignamos como Global, el grupo NEC\_PLOTTER si sería visible en los otros dominios, pero pongamos que de repente nos avisan que el usuario LUISJOSE (que no es de nuestro dominio, sino de otro dominio del bosque) necesita permisos para usar nuestro plotter… no podremos incluir al usuario LUISJOSE en el grupo NEC\_PLOTTER, ya que un grupo Global solo permite que introduzcamos a usuarios de nuestro propio dominio.

Si lo asignamos como Universal, no tendríamos ningún problema, ya que este tipo de grupos no tiene prácticamente ningún tipo de limitación, sin embargo, dichos grupos influyen negativamente en el funcionamiento de nuestro dominio, ya que “consumen” muchos recursos de nuestro directorio activo.

Una solución “elegante” sería crear NEC\_PLOTTER como grupo local, y darle permisos sobre nuestro plotter. A continuación, creamos un grupo global NEC\_PLOTTERg y le añadimos como miembro a nuestro grupo local NEC\_PLOTTER. De esta forma, un dominio de nuestro bosque podrá añadir a sus recursos a nuestro grupo NEC\_PLOTTERg y así asignarles permisos a nuestros usuarios. Del mismo modo, si necesito añadir a un usuario LUISJOSE de otro dominio a nuestro plotter, lo puedo introducir en el grupo local NEC\_PLOTTER.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. CREACIÓN DE GRUPOS CON DSADD

Para verlo más claro, vamos a incluir aquí una tabla resumen sobre los distintos tipos de grupos:

Tabla

Descripción generada automáticamente

Podemos gestionar las cuentas de grupos desde el símbolo del sistema con los mismos comandos que usamos para gestionar las cuentas de usuario.

Interfaz de usuario gráfica

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Así, para crear una cuenta de grupo usamos el comando.

Creación de grupos:

**dsadd group GroupDn [atributos]**

Donde “group” es el nombre del grupo que vamos a crear y GroupDn es el nombre distinguido del grupo.

Ya vimos en qué consistía un nombre distinguido así, por ejemplo, para crear un grupo con nombre VIKINGOS usamos el siguiente comando:

*dsadd group “CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM”*

Comprobad desde Usuarios y Equipos de Active Directory que efectivamente el grupo se ha creado correctamente.

Algunas de las opciones que podemos usar con este comando son:

* ***-Secgrp [yes | no]***Especifica si el grupo es de seguridad (yes) o de distribución (no).
* ***-Scope [L | G | U]***Indica si el ámbito es Local (L), Global (G) o Universal (U).
* **-samid Nombre** Especifica el sAMAccountName del grupo. Si no lo especificamos, el nombre del grupo será el especificado en el DN del grupo.
* **-desc descripción** Establece la descripción del grupo
* -**members MenberDn** Añade miembros al nuevo grupo. Los miembros se especifican mediante sus DNs y separados por espacios.
* -**memberof GroupDn** Hace que el nuevo grupo que estamos creando sea miembro de uno o más grupos existentes. Los grupos también se especifican mediante su DN y separados por espacios.

Ahora llegamos a la parte en la que crearemos dos grupos:

Un grupo global en el que incluiremos las cuentas de usuario correspondientes a los miembros del departamento desarrollo.

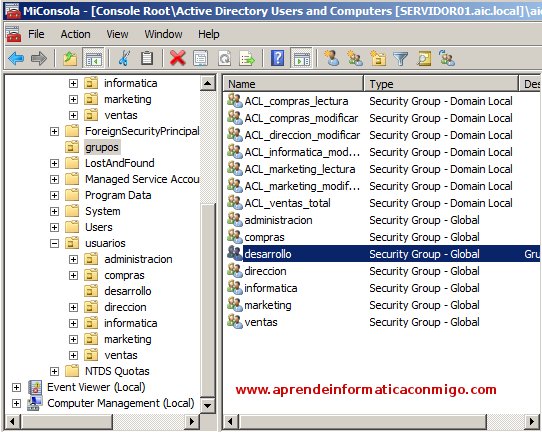
Otro grupo Local de Dominio que llamaremos “**ACL\_desarrollo\_modificar**” en el que incluiremos como miembros a los Grupos Globales de “**direccion**” y “**desarrollo**“.

Para crear el Grupo Global “**desarrollo**” introduciremos el siguiente comando:

**dsadd group “CN=desarrollo,OU=grupos,DC=aic,DC=local” -samid desarrollo -secgrp yes -scope g -desc “Grupo Global de desarrollo” -members “CN=desarrollo01,OU=desarrollo,OU=usuarios,DC=aic,DC=local”**

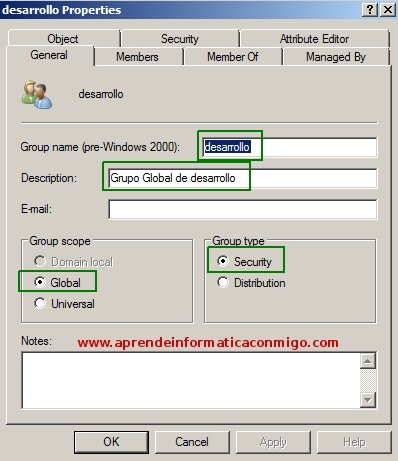
[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-05.jpg)

No hay mucho que decir, simplemente vamos a comprobar que lo ha hecho como nosotros queríamos:

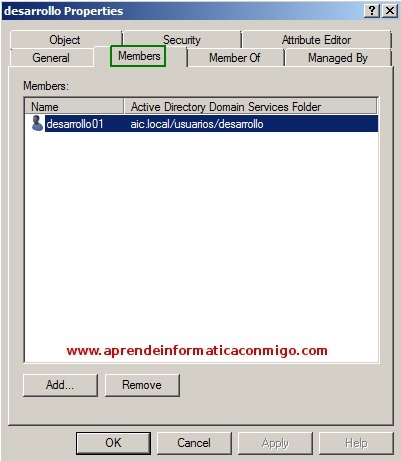
[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-06.jpg)

De momento, el Grupo Global “desarrollo” lo ha creado.

Ahora vamos a ver las propiedades:

[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-07.jpg)

Muy bien, ahora vamos a mirar en la pestaña “**Members**” porque debería de estar el usuario “**desarrollo01**“:

[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-08.jpg)

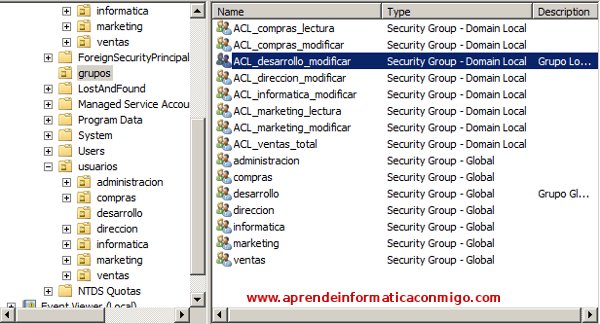
En efecto. Ahí está.

Pasamos a la creación del siguiente grupo, el grupo Local de Dominio “**ACL\_desarrollo\_modificar**” en el que incluiremos como miembros a los Grupos Globales “**desarrollo**” y “**direccion**“.

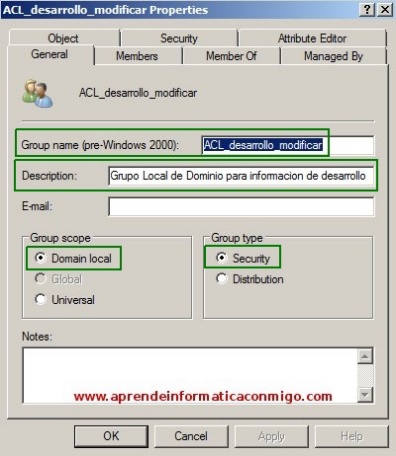
**dsadd group “CN=ACL\_desarrollo\_modificar,OU=grupos,DC=aic,DC=local” -samid ACL\_desarrollo\_modificar -secgrp yes -scope l -desc “Grupo de Dominio Local para informacion sobre desarrollo” -members “CN=desarrollo,OU=grupos,DC=aic,DC=local” “CN=direccion,OU=grupos,DC=aic,DC=local”**

[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-09.jpg) Podemos observar, a parte de que el ámbito (**-scope**) hemos indicado Local, hemos indicado dos grupos como miembros de este nuevo grupo. Los hemos indicado mediante su **DN** y separados por un espacio.

Comprobamos que se ha creado el grupo:

[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-10.jpg)

Bien, ahora revisamos las propiedades del grupo para comprobar que las que le hemos indicado están correctas:

[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-11.jpg)

Parece que en esta pestaña está todo bien.

Pero vamos a ver en la pestaña “**Members**“. Tienen que estar los Grupos Globales “**desarrollo**” y “**direccion**“.

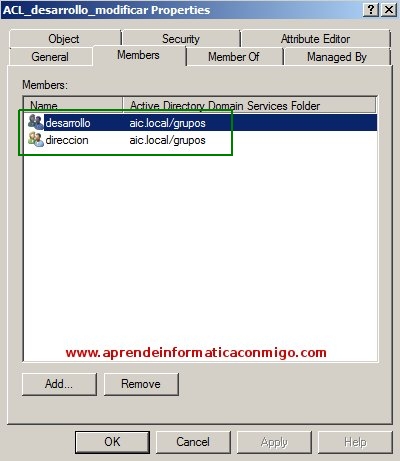
[](http://www.aprendeinformaticaconmigo.com/wp-content/uploads/2010/06/crgrdsadd-12.jpg)

Imagen de la pantalla de un pizarrón blanco

Descripción generada automáticamente con confianza media

Para borrar un grupo, usamos el comando dsrm.

*dsrm “nombre distinguido del grupo”*

Así, para borrar el grupo VIKINGOS anteriormente creado ejecutaríamos el comando:

*dsrm “CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM”*

Texto

Descripción generada automáticamente

Si queremos añadir un usuario a un grupo mediante línea de comandos lo podemos hacer con la orden dsmod.

¿Qué podemos modificar del grupo?

-Añadir Miembros al GRUPO

*dsmod group “nombre distinguido del grupo” –addmbr “nombre distinguido del*

*usuario” “nombre distinguido del usuario” “nombre distinguido del usuario”*

*dsmod group “cn=grupo1,ou=grupos,dc=vallexxx,dc=local” -addmbr “cn=usuario1,ou=usuarios,dc=valleahf,dc=local” “cn=usuario2,ou=usuarios,dc=valleahf,dc=local”*

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Vemos cómo podemos añadir varios miembros a la vez a un grupo, eso sí, siempre usando su nombre distinguido.

Como ejercicio, cread 4 usuarios cualesquiera en USERS, luego crear un grupo llamado NUEVO e introducid como miembros de dicho grupo a los 4 usuarios creados. Todo ello hay que realizarlo desde el símbolo de comandos. Para comprobar que dicho grupo cuenta con los usuarios una vez realizado el ejercicio, podéis acceder a la consola para comprobarlo más cómodamente.

-Quitar Miembros del GRUPO

Otro comando interesante nos permite eliminar la pertenencia de un usuario a un grupo. Esto se consigue con el comando:

*dsmod group “nombre distinguido del grupo” –rmmbr “nombre distinguido del*

*usuario” “nombre distinguido del usuario” “nombre distinguido del usuario” ….*

Como ejercicio, eliminar del grupo NUEVO a dos usuarios de los que se han introducido anteriormente.

Fijaros como simplemente sacamos a los usuarios del grupo, en ningún caso borramos las cuentas de los usuarios.

-Convertir un Grupo en otro tipo de GRUPO

Dsmod group “Nombre distinto del grupo” -secgrp { yes/no }

-scope { L/G/U}

CONSULTAS

MOSTRAR TODOS LOS GRUPOS DEL DOMINIO.

Dsquery group “dc=valleahf,dc=local”

MOSTRAR TODOS LOS GRUPOS DE UNA UO.

Dsquery group “ou=grupos,dc=vallexxx,dc=local”

MOSTRAR TODOS LOS GRUPOS DEL DOMINIO QUE COMIENCEN POR “Grup\*”.

Dsquery group domain root -name grup\*

Nos muestra todos los grupos del dominio que comiencen por Grup.

PARA VER LOS MIEMBROS QUE PERTENECEN A UN GRUPO.

Para ver los miembros de un grupo sin tener que acceder a la consola, podemos usar el comando:

*dsget group “nombre distinguido del grupo” –members*

*dsget group “nombre distinguido del grupo” –members -expand*

*Captura de pantalla de un celular con un texto en blanco y negro

Descripción generada automáticamente con confianza media*

MODIFICAR UN GRUPO YA CREADO.

--añadiendo un conjunto de usuarios, que tenemos creados en otra U.O

Modificar un grupo ya creado añadiendo un conjunto de usuarios que tenemos creados en una unidad organizativa.

Dsquery user “ou=alumnos,dc=valleinclan,dc=local” | dsmod group “cn=Grupo-Alumnos, our=alumnos,dc=valleinclan,dc=local” –addmbr.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

-Modificar un grupo ya creado quitando un conjunto de usuarios que tenemos creados en otra unidad organizativa.

Dsquery user “ou=usuarios,dc=valleahf,dc=local” | dsmod group “cn=fnames,ou=grupos,dc=valleahf,dc=local” -rmbr

MODIFICAR EL NOMBRE DE UN GRUPO POR OTRO NOMBRE

Dsmove “cn=fnames,ou=grupos,dc=valleahf,dc=local” -newname “grupotemp”

MOVER EL GRUPO DE UNA UNIDAD ORGANIZATIVA A OTRA

Dsmove “nombre distinto del grupo a mover” -newparent “unidad organizativa donde lo queremos mover”

Dsmove “cn=grupotemp,ou=grupos,dc=valleahf,dc=local” -newparent “ou=grupox,ou=grupos,dc=valleahf,dc=local”

Pasamos el grupo grupotemp, dentro de la u.o grupox

MOVER EL GRUPO DE UNA UNIDAD ORGANIZATIVA A OTRA y MODIFICAR EL NOMBRE DEL GRUPO.

Dsmove “cn=grupotemp,ou=grupos,dc=valleahf,dc=local” -newname “gruposegundo” -newparent “ou=grupox,ou=grupos,dc=valleahf,dc=local”