Capítulo

Estrategias de Seguridad a través de Grupos

En este capítulo trataremos:

- Planificara una estrategia de grupos
- Entenderá la importancia de una estrategia de grupos
- Aprenderá a crear grupos de usuarios
- Identificara los grupos predefinidos
- Aprenderá a establecer derechos de usuario

Introducción:

Controlar el acceso a los recursos es una de las tareas más significativas de la administración de la red. Por lo que deberá entender qué técnicas son empleadas para simplificar la concesión de permisos.

Introduccion a Grupos

Un grupo es un conjunto de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una sola unidad. Los usuarios y los equipos que pertenecen a un grupo determinado se denominan miembros del grupo.

Los grupos de los Servicios de dominio de Active Directory (AD DS) son objetos de directorio que residen en un dominio y en objetos contenedores Unidad organizativa (OU). AD DS proporciona un conjunto de grupos predeterminados cuando se instala y también incluye una opción para crearlos.

Los grupos de AD DS se pueden usar para:

- **Simplificar la administración** al asignar los permisos para un recurso compartido a un grupo en lugar de a usuarios individuales. Cuando se asignan permisos a un grupo, se concede el mismo acceso al recurso a todos los miembros de dicho grupo.
- **Delegar la administración** al asignar derechos de usuario a un grupo una sola vez mediante la directiva de grupo. Después, a ese grupo le puede agregar miembros que desee que tengan los mismos derechos que el grupo.
- **Crear listas de distribución** de correo electrónico.

Los grupos se caracterizan por su **ámbito** y su **tipo**. El ámbito de un grupo determina el alcance del grupo dentro de un dominio o bosque. El tipo de grupo determina si se puede usar un grupo para asignar permisos desde un recurso compartido (para grupos de seguridad) o si se puede usar un grupo sólo para las listas de distribución de correo electrónico (para grupos de distribución).

También existen grupos cuyas pertenencias a grupos no se pueden ver ni modificar. Estos grupos se conocen con el nombre de identidades especiales. Representan a distintos usuarios en distintas ocasiones, en función de las circunstancias. Por ejemplo, el grupo Todos es una identidad especial que representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios.

Grupos predeterminados

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 funciones administrativas específicas 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

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.

Ámbito de grupo

Los grupos se caracterizan por un ámbito que identifica su alcance en el bosque o árbol de dominios. Existen tres ámbitos de grupo: local de dominio, global y universal.

Grupos locales de dominio

Los miembros de los grupos locales de dominio pueden incluir otros grupos y cuentas de dominios de Windows Server 2003, Windows 2000, Windows NT y Windows Server 2008. A los miembros de estos grupos sólo se les pueden asignar permisos dentro de un dominio.

Los **grupos con ámbito Local de dominio** ayudan a definir y administrar el acceso a los recursos dentro de un dominio único. Estos grupos pueden tener los siguientes miembros:

- Grupos con ámbito Global
- Grupos con ámbito Universal
- Cuentas
- Otros grupos con ámbito Local de dominio
- Una combinación de los anteriores

Por ejemplo, para conceder acceso a una impresora determinada a cinco usuarios, puede agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si posteriormente desea que esos cinco usuarios tengan acceso a otra impresora, deberá volver a especificar las cinco cuentas en la lista de permisos para la nueva impresora.

Con un poco de previsión, puede simplificar esta tarea administrativa rutinaria al crear un grupo con ámbito Local de dominio y asignarle permisos de acceso a la impresora. Coloque las cinco cuentas de usuario en un grupo con ámbito Global y agregue este grupo al grupo que tiene ámbito Local de dominio. Cuando desee que los cinco usuarios tengan acceso a una nueva impresora, asigne permisos de acceso a la nueva impresora al grupo con ámbito Local de dominio. Todos los miembros del grupo con ámbito Global recibirán automáticamente el acceso a la nueva impresora.

Grupos globales

Los miembros de los grupos globales pueden incluir sólo otros grupos y cuentas del dominio en el que se encuentra definido el grupo. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque.

Use los grupos con ámbito Global para administrar objetos de directorio que requieran un mantenimiento diario, como las cuentas de usuario y de equipo. Dado que los grupos con ámbito Global no se replican fuera de su propio dominio, las cuentas de un grupo con ámbito Global se pueden cambiar frecuentemente sin generar tráfico de replicación en el catálogo global.

Aunque las asignaciones de derechos y permisos sólo son válidas en el dominio en el que se asignan, al aplicar grupos con ámbito Global de manera uniforme entre los dominios apropiados, es posible consolidar las referencias a cuentas con fines similares. De esta manera se simplifica y se racionaliza la administración de grupos entre dominios. Por ejemplo, en una red que tenga dos dominios, Europe y UnitedStates, si hay un grupo con ámbito Global denominado GLAccounting en el

dominio UnitedStates, debería haber también un grupo denominado GLAccounting en el dominio Europe (a menos que esa función de contabilidad (Accounting) no exista en el dominio Europe).

Importante

Recomendamos encarecidamente que use grupos globales o universales en lugar de grupos locales de dominio cuando especifique permisos para objetos de directorio de dominio que se repliquen en el catálogo global.

Grupos universales

Los miembros de los grupos universales pueden incluir otros grupos y cuentas de cualquier dominio del bosque o del árbol de dominios. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque o del árbol de dominios.

Use los grupos con ámbito Universal para consolidar los grupos que abarquen varios dominios. Para ello, agregue las cuentas a los grupos con ámbito Global y anide estos grupos dentro de los grupos que tienen ámbito Universal. Si usa esta estrategia, los cambios de pertenencias en los grupos que tienen ámbito Global no afectan a los grupos con ámbito Universal.

Por ejemplo, si una red tiene dos dominios, Europe y UnitedStates, y hay un grupo con ámbito Global denominado GLAccounting en cada dominio, cree un grupo con ámbito Universal denominado UAccounting que tenga como miembros los dos grupos GLAccounting, UnitedStates\GLAccounting y Europe\GLAccounting. Después, podrá usar el grupo UAccounting en cualquier lugar de la organización. Los cambios de pertenencia de los grupos GLAccounting individuales no producirá la replicación del grupo UAccounting.

No cambie la pertenencia de un grupo con ámbito Universal frecuentemente. Los cambios de pertenencia de este tipo de grupo hacen que se replique toda la pertenencia del grupo en cada catálogo global del bosque.

Tipos de grupo

Hay dos tipos de grupos en AD DS:

- Grupos de distribución y
- Grupos de seguridad.

Los **grupos de distribución** se usan para crear listas de distribución de correo electrónico y los grupos de seguridad se usan para asignar permisos para los recursos compartidos.

Los grupos de distribución sólo se pueden usar con aplicaciones de correo electrónico (como Microsoft Exchange Server 2007) para enviar mensajes a conjuntos de usuarios. Los grupos de distribución no tienen seguridad habilitada, lo que significa que no pueden aparecer en las listas de control de acceso discrecional (DACL). Si necesita un grupo para controlar el acceso a los recursos compartidos, cree un grupo de seguridad.

Si se usan con cuidado, los grupos de seguridad son eficaces para conceder acceso a los recursos de la red. Con los grupos de seguridad se puede:

- Asignar derechos de usuario a los grupos de seguridad de AD DS

Se asignan **derechos de usuario** a un grupo de seguridad para determinar lo que pueden hacer los miembros de ese grupo en el ámbito de un dominio (o bosque). A algunos grupos de seguridad se les asignan derechos de usuario automáticamente cuando se instala AD DS para ayudar a los administradores a definir la función administrativa de una persona en el dominio. Por ejemplo, si se agrega un usuario al grupo Operadores de copia de seguridad de Active Directory, éste puede realizar operaciones de copia de seguridad y restauración de archivos y directorios en cada controlador de dominio del dominio.

- Asignar permisos para recursos a los grupos de seguridad

Los permisos y los derechos de usuario no son lo mismo.

Los **permisos** determinan quién puede obtener acceso a un recurso compartido y el nivel de acceso, como Control total. Los grupos de seguridad se pueden usar para administrar el acceso y los permisos en un recurso compartido. Algunos permisos que se establecen en objetos de dominio se asignan automáticamente para proporcionar varios niveles de acceso a los grupos de seguridad predeterminados, como el grupo Operadores de cuentas o el grupo Administradores del dominio.

Como sucede con los grupos de distribución, los grupos de seguridad también se pueden usar como entidades de correo electrónico. Al enviar un mensaje de correo electrónico al grupo, se envía a todos sus miembros.

Identidades especiales

Además de los grupos de los contenedores Users y Builtin, los servidores en los que se ejecuta Windows Server 2008 o Windows Server 2003 incluyen varias identidades especiales.

Por comodidad se las suele llamar grupos. Estos grupos especiales no tienen pertenencias específicas que se puedan modificar.

Sin embargo, pueden representar a distintos usuarios en distintas ocasiones, en función de las circunstancias. Los grupos siguientes son identidades especiales:

Identidad Especial	Descripción
Inicio de sesión anónimo	Este grupo representa a los usuarios y servicios que obtienen acceso a un equipo y sus recursos a través de la red sin usar un nombre de cuenta, contraseña o nombre de dominio. En los equipos con Windows NT y versiones anteriores, el grupo Inicio de sesión anónimo es un miembro predeterminado del grupo Todos. En los equipos con Windows Server 2008 o Windows Server 2003, el grupo Inicio de sesión anónimo no es miembro del grupo Todos de manera predeterminada.
Todos	Este grupo representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios. Cuando un usuario inicia sesión en la red, se agrega automáticamente al grupo Todos.
Red	Este grupo representa a los usuarios que obtienen acceso en ese momento a un recurso dado a través de la red, frente a los usuarios que obtienen acceso a un recurso mediante un inicio de sesión local en el equipo en el que reside el recurso.

	Cuando un usuario obtiene acceso a un recurso dado a través de la red, se agrega automáticamente al grupo Red.
Interactivo	Este grupo representa a todos los usuarios que disponen de una sesión iniciada en un equipo determinado y que están obteniendo acceso a un recurso ubicado en ese equipo, frente a los usuarios que obtienen acceso al recurso a través de la red. Cuando un usuario obtiene acceso a un recurso dado en el equipo en el que ha iniciado sesión, se agrega automáticamente al grupo Interactivo.

Aunque a las identidades especiales se les puede conceder derechos y permisos para los recursos, sus pertenencias no se pueden ver ni modificar. Las identidades especiales no tienen ámbitos de grupo. Los usuarios son asignados automáticamente a ellas cuando inician sesión u obtienen acceso a un recurso concreto.

Información sobre creación de grupos

En AD DS, los grupos se crean en los dominios. Para crear grupos se utiliza Usuarios y equipos de Active Directory. Con los permisos necesarios, se pueden crear grupos en el dominio raíz del bosque, en cualquier otro dominio del bosque o en una unidad organizativa.

Además de por el dominio en el que se crea, un grupo también se caracteriza por su ámbito. El ámbito de un grupo determina lo siguiente:

- El dominio desde el que se pueden agregar miembros
- El dominio en el que son válidos los derechos y permisos asignados al grupo

Elija el dominio o la unidad organizativa donde va a crear un grupo en función de las tareas de administración que requiera el grupo. Por ejemplo, si un directorio tiene varias unidades organizativas y cada una tiene un administrador diferente, puede crear grupos con ámbito Global dentro de esas unidades organizativas para que los administradores administren la pertenencia a grupos de los usuarios de las unidades organizativas que les correspondan. Si se necesitan grupos para controlar el acceso fuera de la unidad organizativa, puede anidar los grupos de la unidad organizativa dentro de grupos con ámbito Universal (u otros grupos con ámbito Global) que puede utilizar en otros lugares del bosque.

Nota

Es posible mover grupos dentro de un dominio, pero sólo los grupos con ámbito Global se pueden mover entre dominios diferentes. Los derechos y permisos que se asignan a un grupo con ámbito Universal se pierden cuando el grupo se mueve a otro dominio y deben realizarse nuevas asignaciones.

Niveles de Funcionamiento

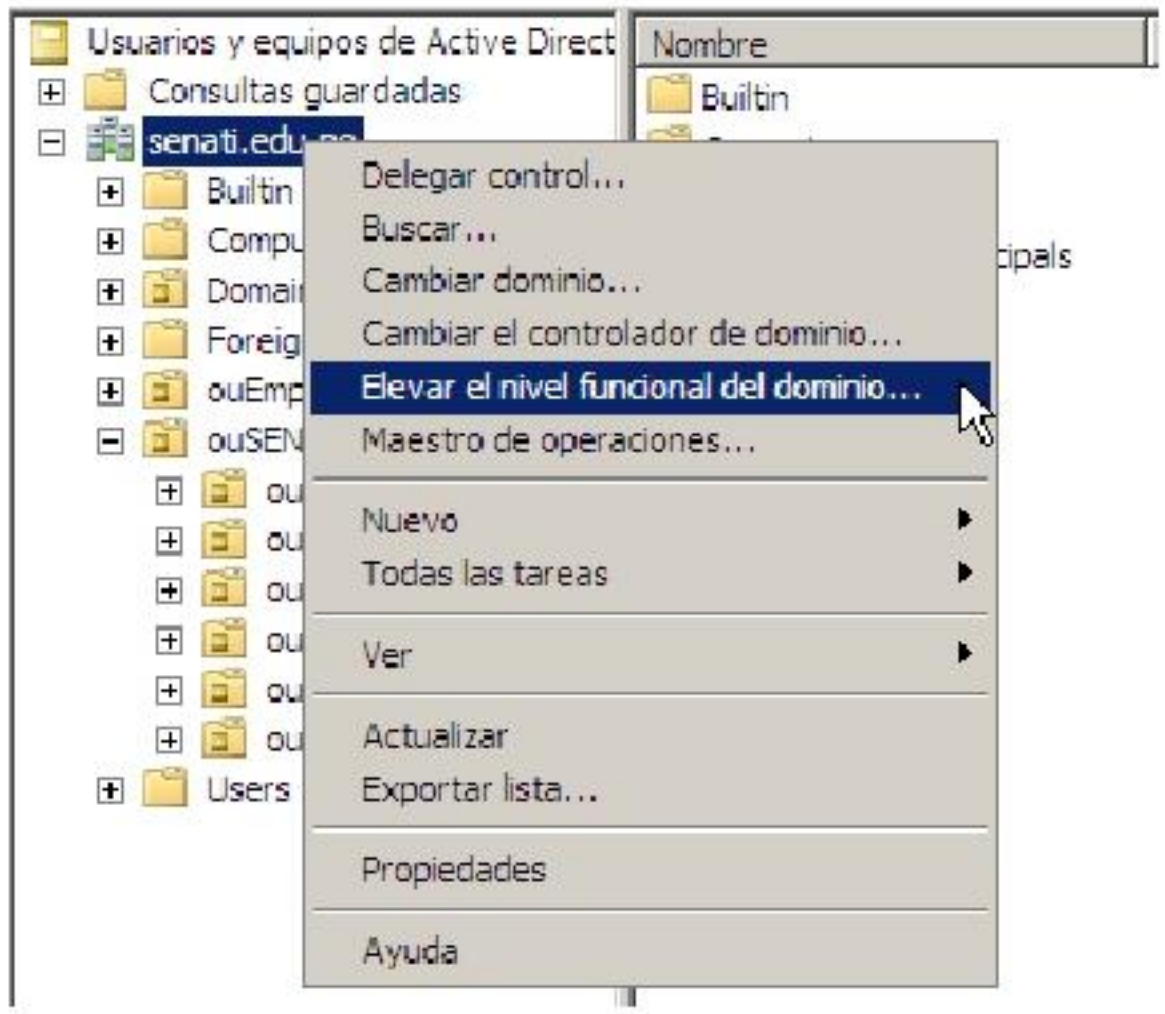
El nivel funcional determina cómo se comportarán los grupos dentro del bosque y a la vez determina qué clase de características estarán disponibles, como por ejemplo la capacidad de unir bosques.

Si el nivel funcional del dominio se encuentra definido como nativo de Windows 2000 o superior, el dominio contiene una jerarquía de unidades organizativas y la administración se delega a los administradores de cada unidad organizativa, puede que sea más eficaz anidar los grupos con ámbito Global. Por ejemplo, si OU1

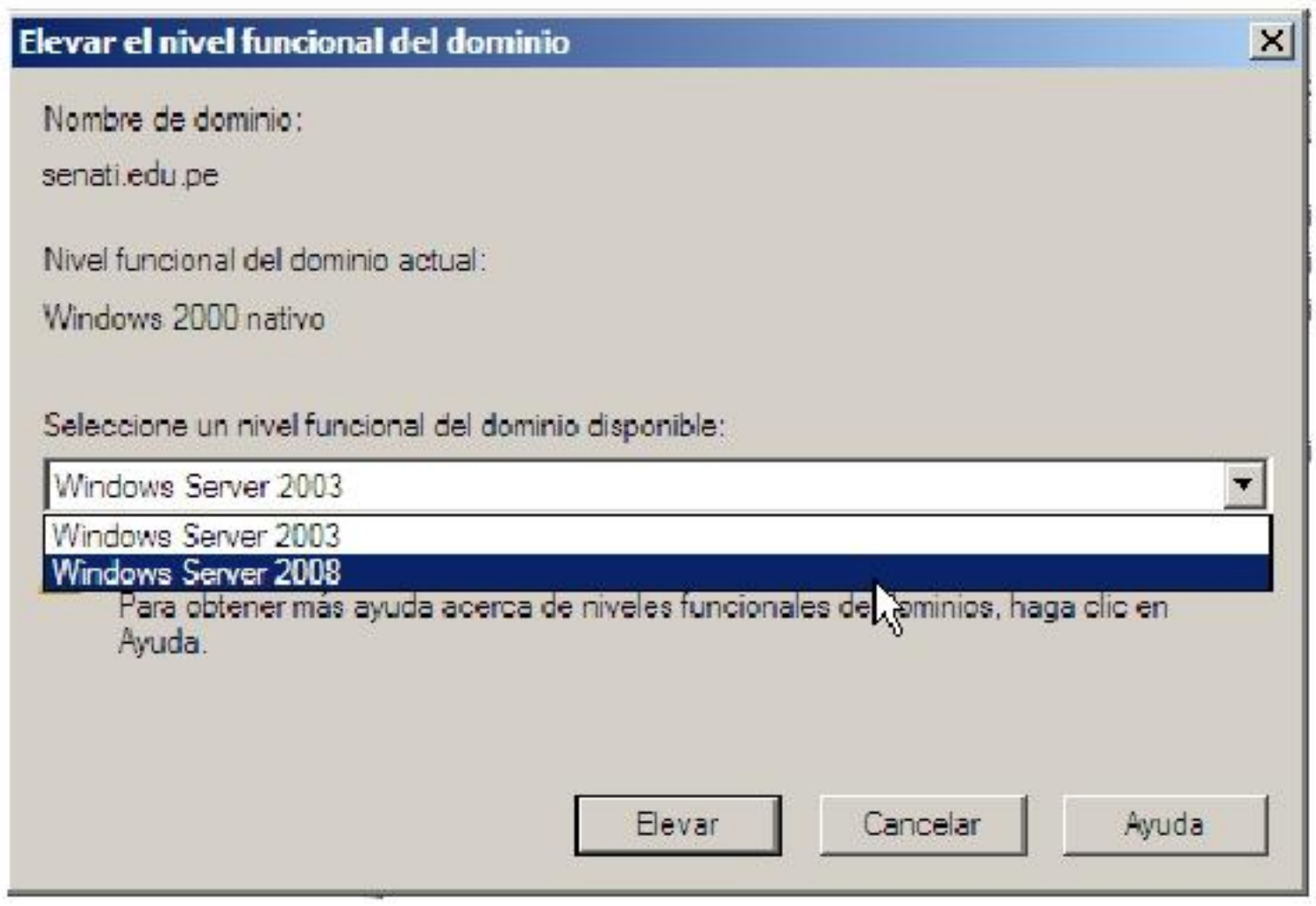
contiene a OU2 y OU3, un grupo con ámbito Global en OU1 puede tener como miembros a los grupos con ámbito Global en OU2 y OU3. En OU1, el administrador puede agregar o quitar miembros de grupo de OU1 y los administradores de OU2 y OU3 pueden agregar o quitar miembros de grupo para las cuentas de sus propias OU sin tener derechos administrativos para el grupo con ámbito Global en OU1.

Cambiar el nivel funcional del dominio

- En la herramienta Usuarios y equipos de Active Directory, haga clic derecho en el dominio, y seleccione **Elevar el nivel funcional del dominio**.



- Observará el siguiente cuadro de diálogo, con el cual podrá observar el nivel funcional actual, y además, cambiar a un nivel superior.



Planificacion de estrategias de grupo

En Active Directory, se crearán un gran número de grupos de distribución y seguridad. Las siguientes convenciones de nomenclatura pueden ayudar a administrar estos grupos. Las organizaciones establecen sus propias convenciones de nomenclatura para los grupos de distribución y de seguridad.

Un nombre de grupo debería identificar su ámbito, tipo, la finalidad de su creación y los permisos que puede tener.

Determinacion de los nombres de grupo

Grupos de Seguridad

Tenga en cuenta los siguientes puntos al definir una convención de nomenclatura para los grupos de seguridad:

Ámbito de los grupos de seguridad

Aunque el tipo y ámbito de grupo se muestra como tipo de grupo en Usuarios y equipos de Active Directory, las organizaciones suelen incorporar el ámbito en la convención de nomenclatura del nombre de grupo.

Por ejemplo, para identificar el ámbito de los grupos de seguridad, Northwind Traders añade una letra al principio del nombre de grupo:

- G IT Admins

  G para grupos globales

- U All IT Admins

  U para grupos universales

- DL IT Admins Full Control

  DL para grupos locales de dominio

Posesión del grupo de seguridad

El nombre de un grupo de seguridad de dominio, ya sea universal, global o local de dominio, debe identificar de forma clara al propietario del grupo e incluir el nombre del departamento o equipo al que pertenece.

A continuación, se muestra un ejemplo de convención de nomenclatura que podría utilizar Northwind Traders para identificar al propietario del grupo:

- G Marketing Managers
- DL IT Admins Full Control

Nombre de dominio

El nombre de dominio o su abreviatura se coloca al principio del nombre de grupo a petición del cliente. Por ejemplo:

- G NWTraders Marketing
- DL S.N.MSFT IT Admins Read

Finalidad del grupo de seguridad

Por último, se pude incluir en el nombre la finalidad empresarial del grupo y los permisos máximos que debería tener el grupo en la red. Esta convención de nomenclatura se suele aplicar a los grupos locales o grupos locales de dominio.

A continuación, se muestra un ejemplo de convención de nomenclatura que podría utilizar Northwind Traders para identificar la finalidad del grupo de seguridad: Northwind Traders utiliza un descriptor para identificar los permisos máximos que debería tener el grupo en la red. Por ejemplo:

- DL IT London OU Admins
- DL IT Admins Full Control

Grupos de distribución

Como los grupos de seguridad se utilizan sobre todo para la administración de la red, sólo el personal encargado de esta tarea debe utilizar la convención de nomenclatura. Los usuarios finales utilizan grupos de distribución; por lo tanto, debe interesarles la convención de nomenclatura que sigue.

Al definir una convención de nomenclatura para los grupos de distribución, tenga en cuenta los siguientes puntos:

Nombres de correo electrónico

- **Longitud**. Utilice un alias corto. Para respetar las normas actuales de datos descendentes, la longitud mínima de este campo es de tres caracteres y la longitud máxima, de ocho.
- **Palabras ofensivas**. No cree grupos de distribución con palabras que puedan considerarse ofensivas. Si no está seguro, no utilice la palabra.
- **Permitidos**. Puede utilizar cualquier carácter ASCII. Los únicos caracteres especiales permitidos son el guión (-) y el carácter de subrayado (_).
- **Designaciones especiales**. No utilice las siguientes combinaciones de caracteres para los grupos de distribución:
  - Un carácter de subrayado (_) al principio del nombre de grupo del alias.
  - Un nombre o una combinación de nombre y apellidos que pueda confundirse fácilmente con un nombre de cuenta de usuario.

Nombres para mostrar

- **Alias de usuario**. Con el fin de estandarizar los nombres, no incluya un alias como parte del nombre para mostrar (por ejemplo, Informes directos de Sfeli). Incluya el nombre completo (por ejemplo, Informes directos de Susana Félix).
- **Palabras ofensivas**. No cree grupos de distribución con palabras que puedan considerarse ofensivas.
- **Discusiones sociales**. No debería permitirse la utilización de grupos de distribución para discusiones sociales, porque el área de carpetas públicas es un medio más eficaz para transmitir y almacenar un gran número de comunicaciones relacionadas con discusiones sociales. Ya que un mensaje puede ser visto por varios usuarios, se minimiza el tráfico de red y el almacenamiento de datos si se utilizan las carpetas públicas en lugar de los grupos de distribución.
- **Longitud**. La longitud máxima de este campo es de 40 caracteres. Se aceptan abreviaturas, siempre que su significado no sea confuso.
- **Estilo.** No ponga en mayúsculas toda la descripción, pero sí la primera letra del nombre para mostrar. Utilice ortografía y puntuación correctas.
- **Parte superior de la libreta de direcciones**. No utilice la palabra Un/a, números, caracteres especiales (sobre todo, comillas) o un espacio en blanco al inicio de la descripción. Esto hace que aparezca en la parte superior de la libreta de direcciones. La libreta de direcciones debería comenzar por nombres de usuario individuales que empiecen por A.

- **Caracteres especiales**. Las barras diagonales (/) se aceptan en los nombres para mostrar, pero no al inicio de los nombres de servidor. No utilice más de un apóstrofe (') y ninguno de los siguientes caracteres especiales: " * @ # $ % | [ ] ; < > =

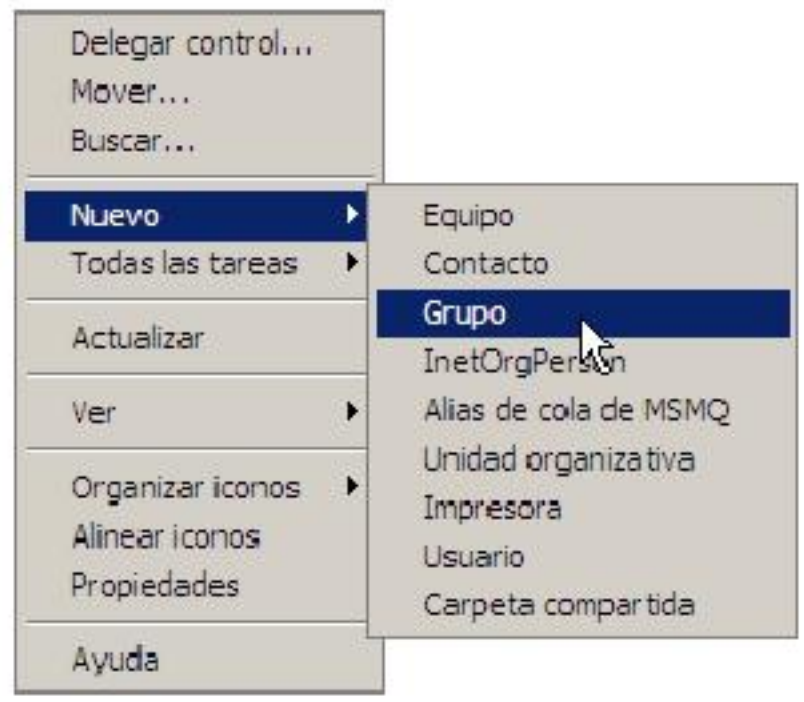
Posesión

Un único grupo de distribución puede tener un máximo de cinco copropietarios.

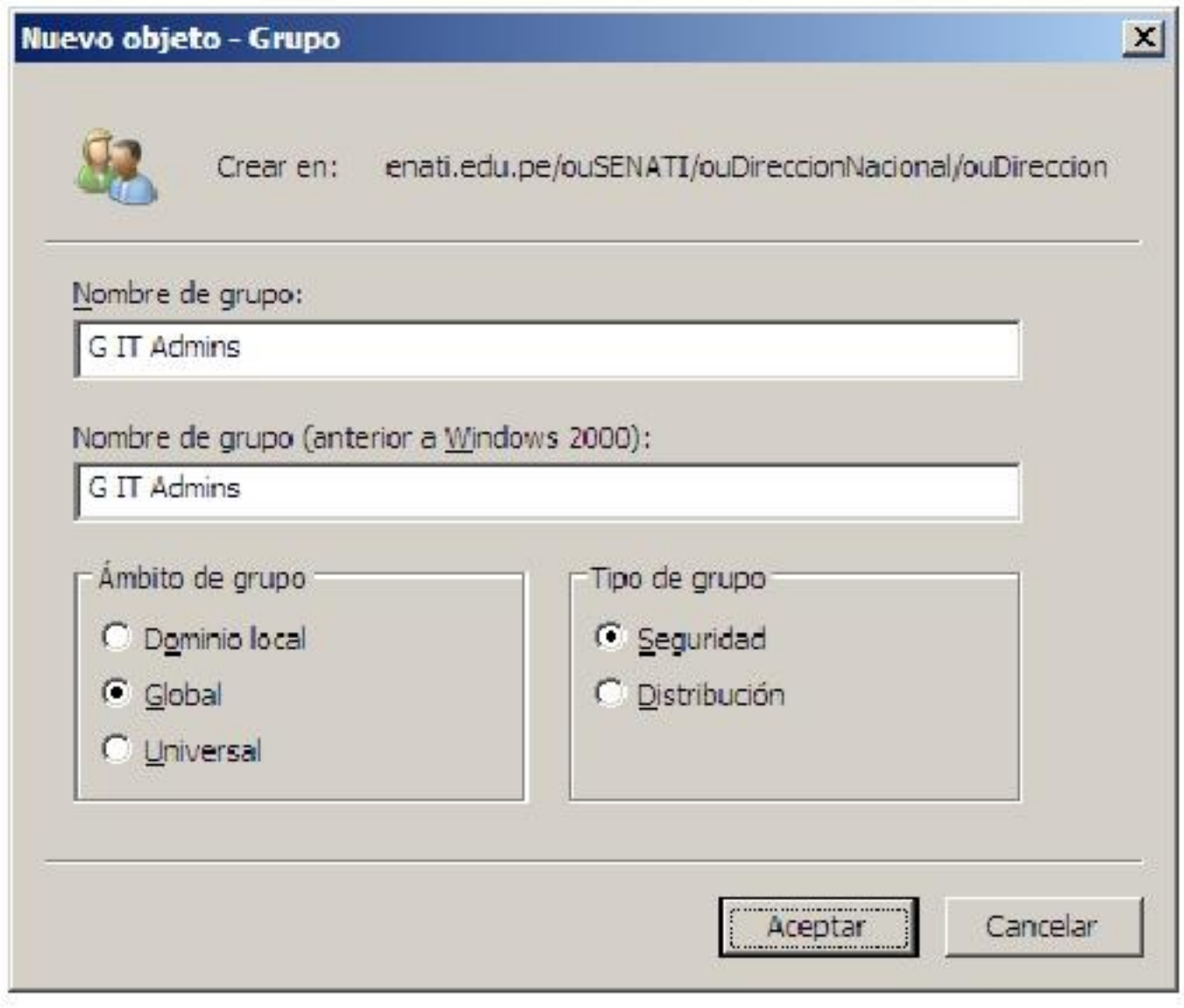
Implementación de Grupos

Creacion de grupos

1. Haga clic derecho en una unidad organizativa o en una zona libre del área de trabajo.
2. Luego señale **Nuevo** y haga clic en **Grupo**.



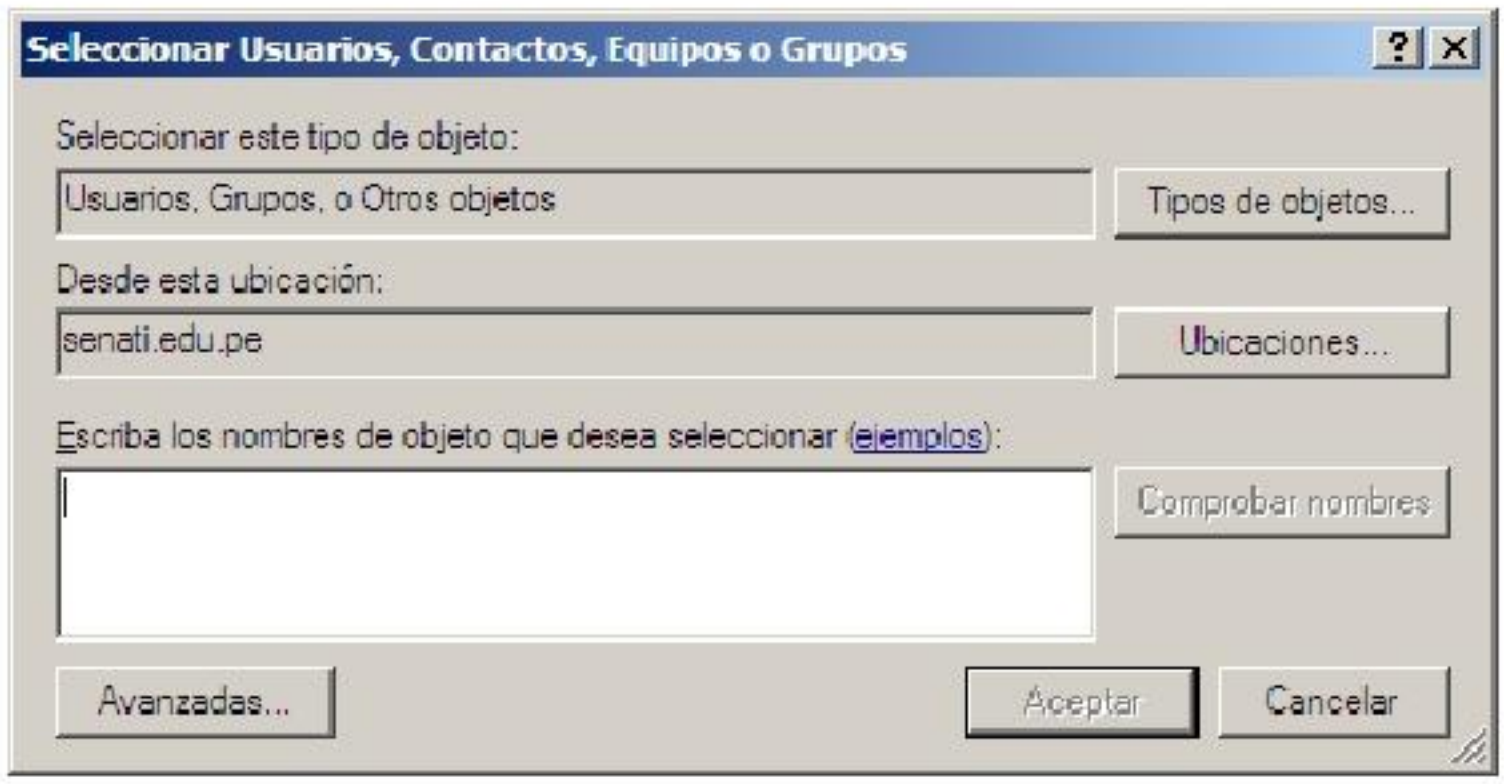
3. Escriba el nombre del grupo y haga clic en Aceptar.



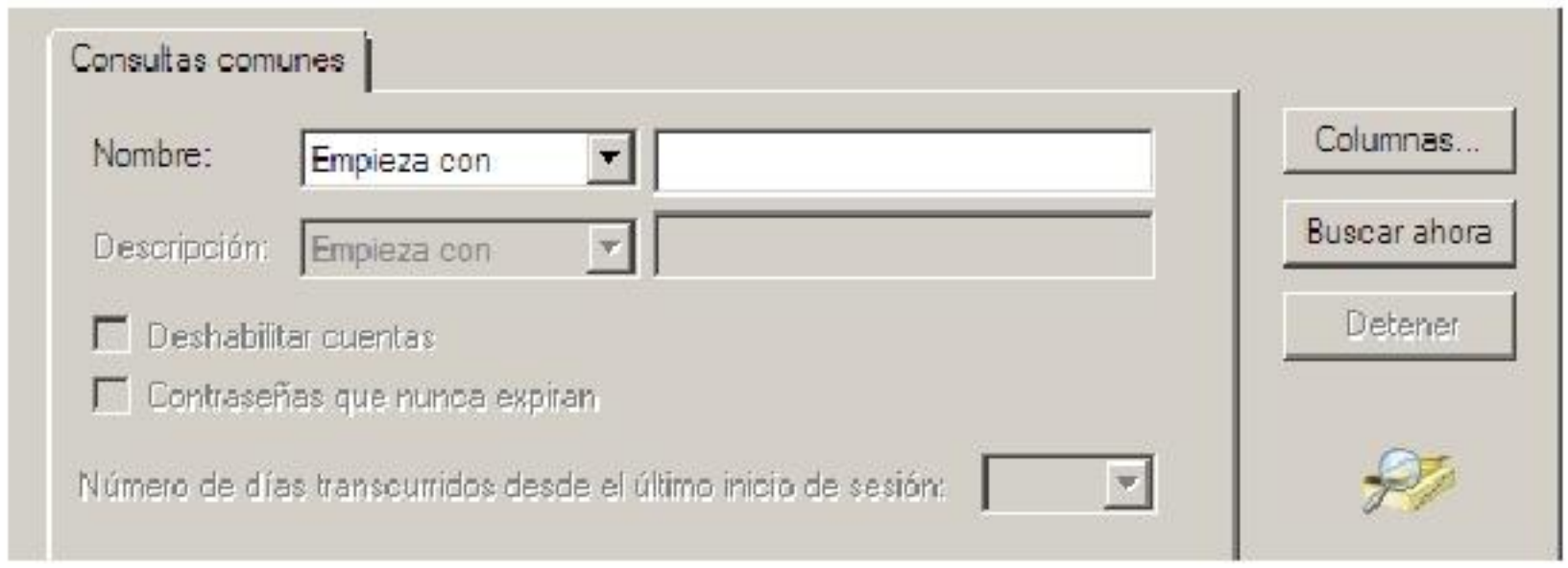
Puede realizar otros tipos de acción sobre un grupo, tales como:

1. Eliminación de grupos.
2. Adición de usuarios a un grupo. (Describiremos este proceso)
   a. Haga clic derecho en el grupo.
   b. Haga clic en **Agregar a un grupo**.
   c. Seleccione la ficha **Miembros**.

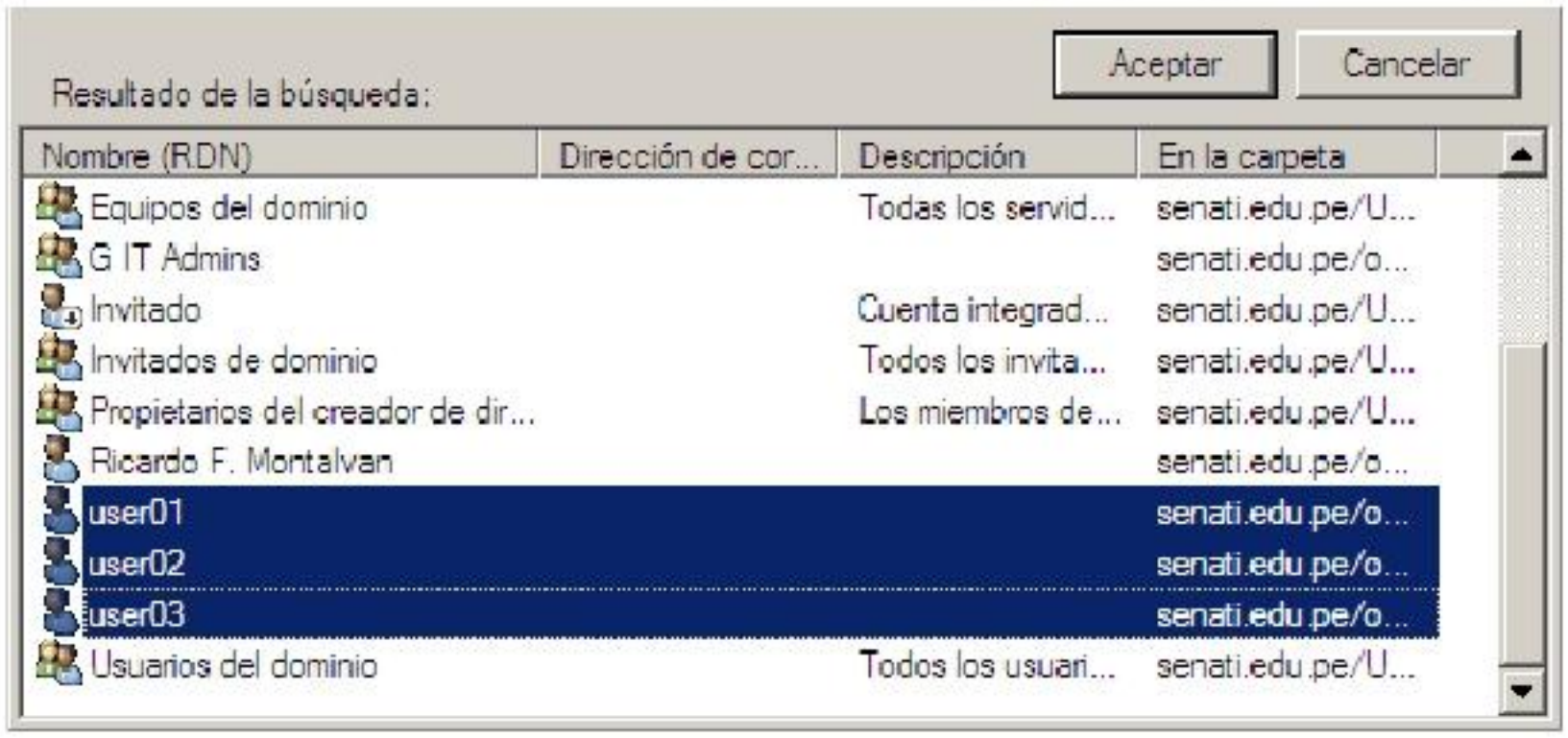
d. **Se mostrará el siguiente cuadro de diálogo, haga clic en el botón Avanzadas….**



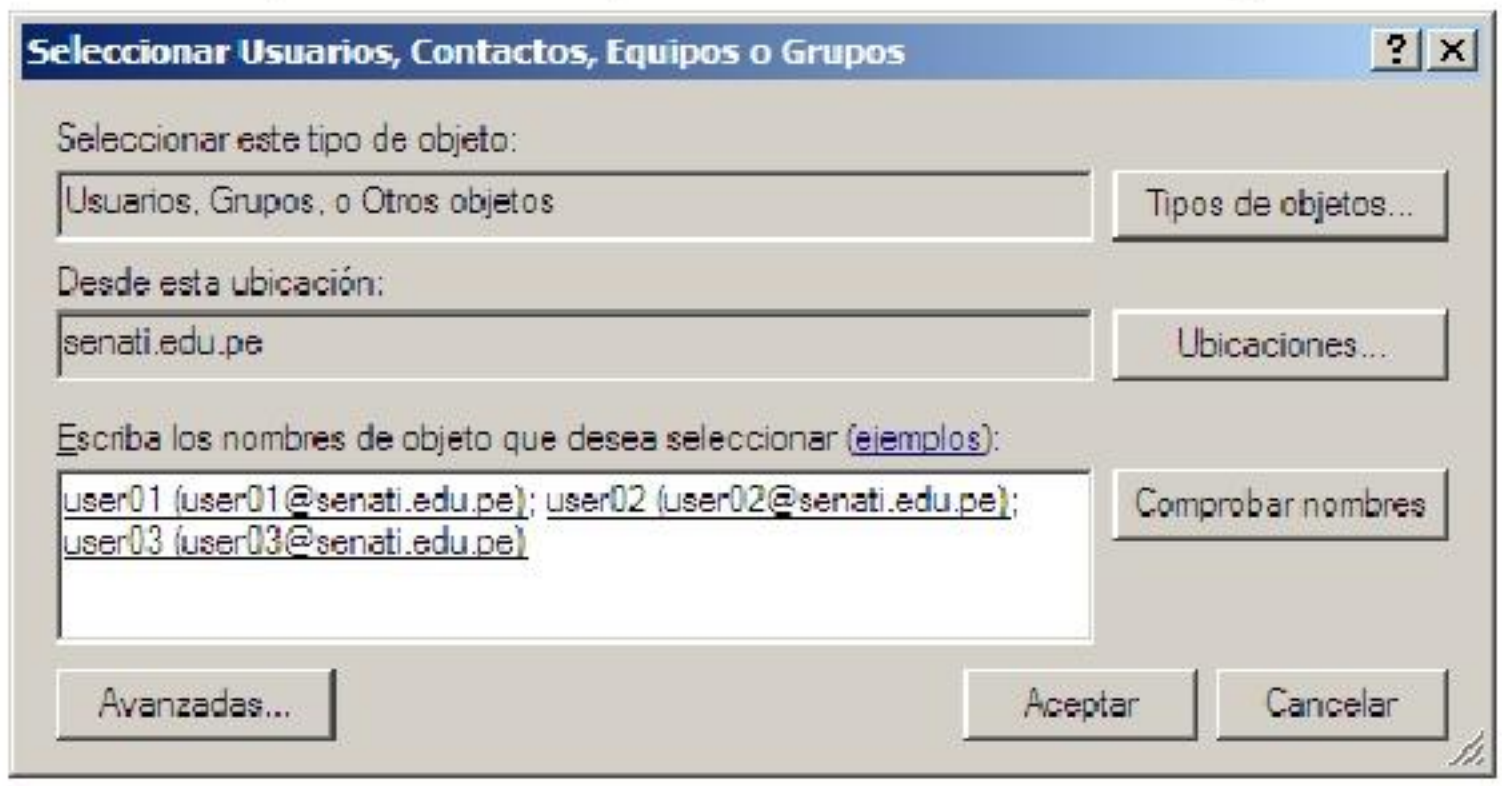
e. **En el cuadro de diálogo siguiente, si desea puede escribir el nombre de usuario que busca o en todo caso haga clic en el botón Buscar ahora.**



f. Seleccione los usuarios que necesita agregar y haga clic en Aceptar.



g. Aparecerán los usuarios seleccionados y comprobados. En esta ventana también puede escribir el nombre de usuario y utilizar el botón Comprobar nombres para verificar su existencia. Haga clic en Aceptar.



h. La lista se agregará a las propiedades del grupo. Haga clic en Aceptar.

Actividad 1

Crear grupos mediante Usuarios y equipos de Active Directory

1. Cree los siguientes grupos globales en la unidad organizativa Locations/NombreEquipo/Grupos:
    a. G NombreEquipo Accounting Managers
    b. G NombreEquipo Accounting Personnel
2. Cree los siguientes grupos locales de dominio en la unidad organizativa Locations/NombreEquipo/Grupos:
    a. DL NombreEquipo Accounting Managers Full Control
    b. DL NombreEquipo Accounting Managers Read
    c. DL NombreEquipo Accounting Personnel Full Control
    d. DL NombreEquipo Accounting Personnel Read

Ejercicio Grupal Práctico (fórmense grupos de 3 personas para analizar la solución)

Tomando en cuenta el ejercicio práctico desarrollado en el capítulo anterior, considere la siguiente configuración existente y a partir de ellos cree los Grupos pertinentes, respetando los patrones y normas estudiados en el presente capítulo.

1. Los siguientes usuarios ya deben existir en su empresa (Sucursal Principal).
    a. Jorge Tafur (Gerente General)
    b. Miguel Millano(Sub Gerente)
    c. Miguel Quispe (Gerente Técnico)
    d. Margot Donaire (Asistente Administrativo de la Gerencia técnica)
    e. Frank Molina (Supervisor Area 1 Turno mañana)
    f. Jorge Muñoz (Supervisor Area 2 Turno mañana)
    g. Victor Mimbela (Supervisor Area 3 Turno mañana)
    h. Marcos Torres (Supervisor Area 1 Turno noche)
    i. Francisco Dominguez (Supervisor Area 2 Turno noche)
    j. Richard Morris (Supervisor Area 3 Turno noche)
    k. Manuel Pacora (Contador)
    l. Susana Frey (Asistente administrativo de Contabilidad)
    m. Jared Yafac (Gerente de RRHH)
    n. Viviana Martinoti (Asistente administrativo de RRHH)
    o. Lizeth Coronado (Gerente de Finanzas)
    p. Mark Romero (Asistente administrativo de Finanzas)
    q. Desire More (Gerente de Marketing)
    r. Raúl Thomas (Asistente administrative de Marketing)
    s. Mónica Suarez(Promotora de Ventas)
    t. Vanesa Farfan (Promotora de Ventas)
    u. Ivan Farías (Promotor de Ventas)
    v. Martha Molina (Promotor de Ventas)
    w. Una cuenta especial para todos los obreros.
2. Se necesitará futuramente configurar diferentes permisos y derechos en carpetas compartidas, impresoras, directivas y otros, por lo que se debe crear grupos tomando en cuenta (Se deja a criterio de los integrantes del grupo)
    a. Crecimiento de la empresa a diferentes sucursales a nivel nacional, con la consecuente adición de servidores y controladores de dominio.
    b. Carpetas compartidas que de acuerdo al grupo que representa, por ejemplo Gerentes necesitarán acceso a los diferentes carpetas de sus áreas con nivel de control total, mientras que otras recursos pueden requerir sólo lectura. De la misma manera, los supervisores quizá necesiten acceso de sólo lectura a todos los recursos de su área.

Preguntas de Repaso

1. Investigación:
    a. Qué proceso se realiza para cambiar el ámbito de un grupo.
2. ¿Cuál es la diferencia entre los grupos: Dominio Local, Global y Universal?
3. ¿Puede un grupo Universal contener a grupos de Dominio Local? ¿Por qué?
4. ¿Puede un grupo Universal contener a grupos Globales? ¿Por qué?
5. ¿Puede un grupo Universal contener a grupos Universales? ¿Por qué?
6. ¿Puede un grupo Global contener a grupos de Dominio Local? ¿Por qué?
7. ¿Puede un grupo Global contener a grupos Globales? ¿Por qué?
8. ¿Puede un usuario pertenecer a varios grupos?