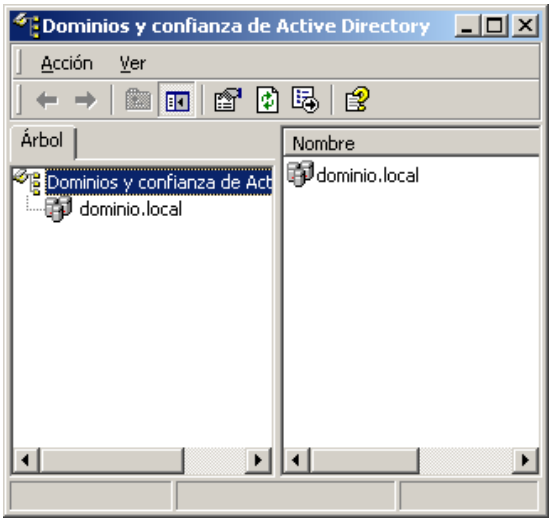
1. Dominios y confianzas de Active Directory

Dominios y confianzas de Active Directory ayuda a administrar las relaciones de confianza entre dominios. Estos dominios pueden ser de Windows 2000 en el mismo bosque, dominios de Windows 2000 en bosques diferentes, dominios de sistemas operativos anteriores a Windows 2000 e, incluso, territorios de Kerberos V5.



Con Dominios y confianzas de Active Directory se puede:

- Proporcionar interoperabilidad con otros dominios, tales como dominios de sistemas operativos anteriores a Windows 2000 y dominios de otros bosques de Windows 2000, mediante la administración de las confianzas.
- Cambiar el modo de funcionamiento de un dominio de Windows 2000 del modo mixto al modo nativo.
- Agregar y quitar sufijos UPN alternativos usados para crear nombres de inicio de sesión de usuario.
- Transferir la función maestro de operaciones de nombres de dominio de un controlador de dominio a otro.

Active Directory es el servicio de directorio utilizado en Windows 2000 Server. Constituye la base de las redes distribuidas de Windows 2000. Podemos utilizar Dominios y confianzas de Active Directory para administrar confianzas de dominios, modos y sufijos de nombres principales de usuarios. Podemos administrar Active Directory de forma remota mediante las Herramientas de administración de Windows 2000.

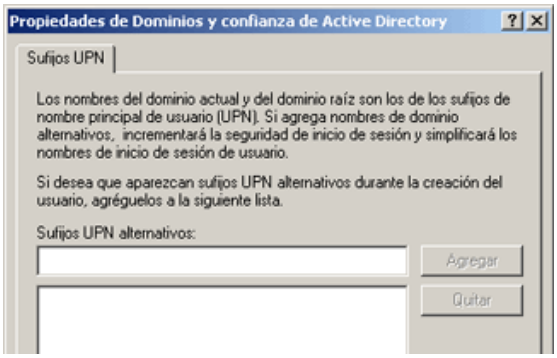
Con las Herramientas de administración de Windows 2000, incluidas en los discos compactos de Windows 2000 Server y Windows 2000 Advanced Server, podemos administrar un servidor remotamente desde cualquier equipo que ejecute Windows 2000. Las Herramientas de administración de Windows 2000 contienen complementos de Microsoft Management Console y otras herramientas administrativas utilizadas para administrar equipos que ejecutan Windows 2000 Server, que no se suministran con Windows 2000 Professional.

Una vez instaladas las Herramientas de administración de Windows 2000 en un equipo, el administrador puede abrir las herramientas administrativas del servidor y comenzar a administrar un servidor remoto desde ese equipo.

Para abrir Dominios y confianzas de Active Directory, hacemos clic en Inicio, seleccionamos Programas, Herramientas administrativas y, a continuación, hacemos clic en Dominios y confianzas de Active Directory.

2. Propiedades de Dominios y confianza de Active Directory

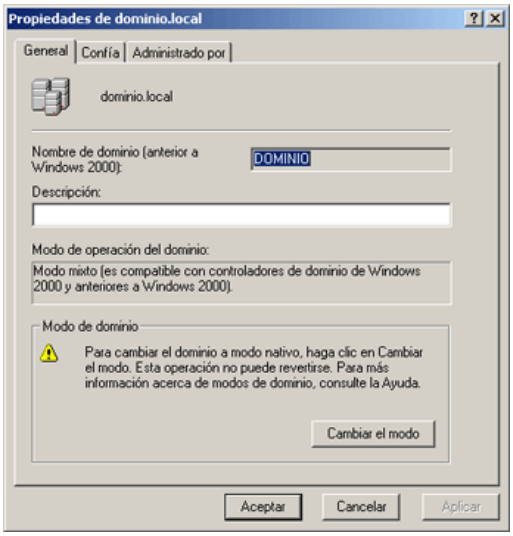
Si pulsamos **la raíz** de Dominios y confianza de Active Directory, desde el menú **Ver** podemos acceder a Propiedades donde podemos especificar los sufijos UPN con los que podemos acceder iniciar sesión. Un UPN es un nombre simplificado que los usuarios pueden proporcionar cuando inician sesión en Active Directory.



El nombre utiliza el formato estándar de direcciones de correo electrónico que consiste en un nombre de usuario prefijo y un nombre de dominio sufijo, separados por un signo @, como se define en la RFC 822 (por ejemplo, usuario@dominio.com). Los UPNs proporcionan a los usuarios de la red un formato de nombre de inicio de sesión unificado que los aísla de la jerarquía de dominios de Active Directory y de la necesidad de especificar el complejo nombre LDAP para sus objetos usuario cuando inician sesión.

De forma predeterminada, el sufijo del UPN de los usuarios de un bosque en particular es el nombre del primer dominio creado en el primer árbol del bosque, también llamado el hombre DNS del bosque. Por medio del Administrador de Dominios y confianzas de Active Directory se pueden especificar sufijos UPN adicionales que los usuarios pueden emplear en lugar del hombre DNS del bosque cuando inicien sesión. Para hacer esto, hay que seleccionar el objeto raíz en el árbol de la consola de la pantalla principal de Dominios y confianzas de Active Directory, y escoger Propiedades en el menú Acción. En la pestaña Sufijos UPN, hay que pulsar el botón Agregar para especificar sufijos adicionales. Estos sufijos se aplican en todo el bosque y están disponibles para cualquier usuario de cualquier dominio de cualquier árbol de ese bosque, siempre que se cree la cuenta de dicho usuario posteriormente a la creación del sufijo UPN.

La pestaña General de **Propiedades de Dominios** y confianzas de Active Directory muestra el nombre NetBIOS con el cual conocen los clientes de nivel inferior al dominio y permite especificar una descripción para ese dominio. Esta pestaña también muestra el modo de operación actual del dominio y permite cambiarlo.

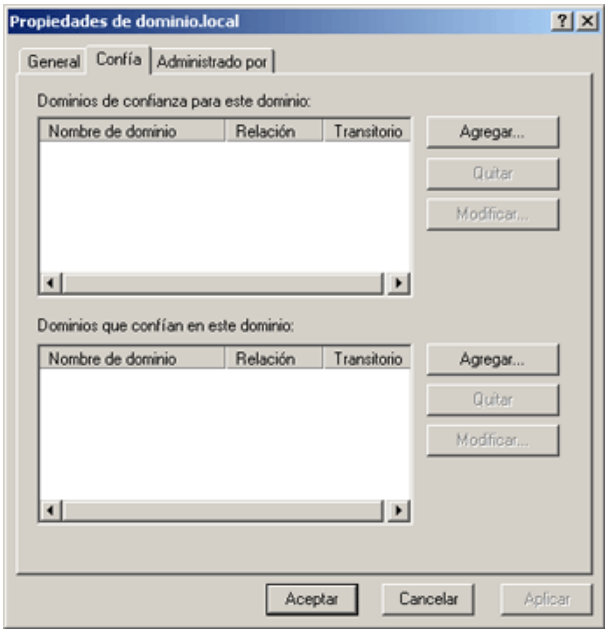


La pestaña Confía de **Propiedades de Dominios** y confianzas de Active Directory se encarga de gestionar las relaciones de confianza del dominio. Cuando se establece una relación de confianza entre dos dominios, los usuarios de un dominio pueden acceder a recursos ubicados en otro dominio en que se confíe. Un árbol de dominios Active Directory es una colección de dominios que no sólo comparten el mismo esquema, la configuración y el espacio de nombres, sino que también están conectados por medio de relaciones de confianza.

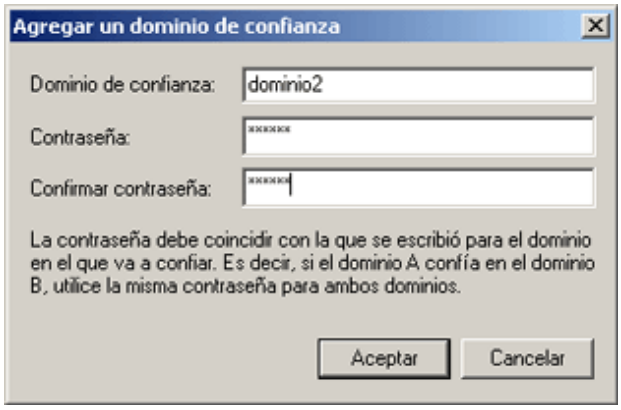
Windows 2000 soporta dos tipos de relaciones de confianza: las confianzas explicitas y de un sentido utilizadas por Windows NT, y las confianzas transitivas y jerárquicas proporcionadas por el protocolo de seguridad Kerberos en los dominios Active Directory. Las relaciones de confianza de Windows NT sólo funcionan en un sentido. Un administrador debe crear explícitamente las confianzas en ambos sentidos para lograr una relación mutua entre los dominios.

Active Directory crea automáticamente relaciones de confianza Kerberos en todos los dominios de un árbol; estas se aplican en ambos sentidos y son transitivas. Una relación de confianza transitiva es aquella que se propaga a través de la jerarquía del árbol. La creación de cada nuevo dominio en un árbol incluye el establecimiento de las relaciones de confianza con el resto de dominios del árbol, lo que permite a los usuarios acceder a recursos en cualquiera de los dominios del árbol (asumiendo que tienen los permisos apropiados) sin que un administrador tenga que configurarlo manualmente.

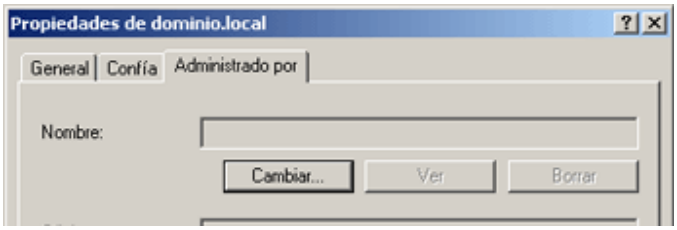
Para proporcionar acceso al dominio a usuarios de otro árbol o para conceder acceso a otro árbol a los usuarios del dominio, se pueden establecer relaciones de confianza manualmente pulsando uno de los botones Agregar de la pestaña Confía y especificando el nombre NetBIOS de un dominio. Estas relaciones son en un solo sentido; hay que establecer una confianza para cada dominio para crear una confianza bidireccional. Dependiendo de la naturaleza del dominio que confía o en el que se confía, la relación podrá o no ser transitiva. Se puede establecer una relación de confianza transitiva con dominios Windows 2000 en otro árbol, pero las relaciones con dominios Windows NT no pueden ser transitivas.



Para establecer una relación de confianza con otro dominio, hay que especificar el nombre del dominio en el cuadro de diálogo Agregar un dominio de confianza y proporcionar una contraseña. Para completar el proceso, un administrador del otro dominio debe especificar el nombre de este dominio en el cuadro de diálogo Agregar un dominio que confía y proporcionar la misma contraseña. Ambos dominios deben dar su aprobación antes de que los sistemas puedan establecer la relación de confianza.



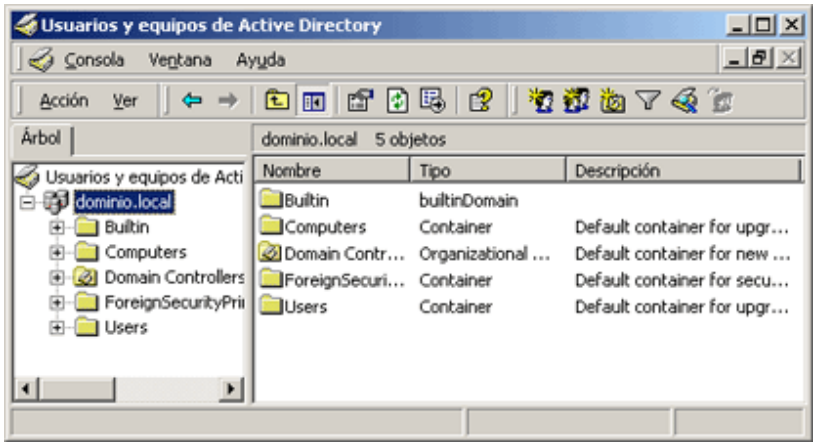
La tercera pestaña **Administrador por** de la ventana **Propiedades de un dominio**, identifica al individuo que es el administrador designado para el dominio. Esta pestaña proporciona información de contacto sobre el administrador derivada de la cuenta de usuario asociada en Active Directory.
Se puede cambiar el administrador pulsando el botón Cambiar y seleccionando otra cuenta de usuario desde la pantalla de Active Directory que se muestra.



3. Administración de los dominios

El complemento Dominios y confianzas de Active Directory también proporciona acceso al complemento **Usuarios y equipos de Active Directory** que se utiliza para consultar y modificar los objetos de un dominio y sus propiedades.

Cuando se selecciona un dominio en el árbol de la consola de la pantalla principal y se escoge **Administrar** en el **menú Acción**, la MMC abre el complemento Usuarios y equipos de Active Directory con el foco en el dominio seleccionado.



El complemento Usuarios y equipos de Active Directory es la principal herramienta de los administradores de Active Directory, y es la herramienta que se utilizará más a menudo para el mantenimiento diario del directorio.

Usuarios y equipos de Active Directory muestra todos los objetos de un dominio por medio de una pantalla con un árbol expandible al estilo del Explorador de Windows.

Los cuadros de diálogo de cada objeto proporcionan acceso a las propiedades del objeto, que se pueden modificar para actualizar la información del usuario y las restricciones de la cuenta.

También se utiliza Usuarios y equipos de Active Directory para crear nuevos objetos y modelar la jerarquía del árbol creando y poblando objetos contenedores.

Usuarios y equipos de Active Directory, como la mayoría de las herramientas de administración de Active Directory, es un complemento de la MMC. El archivo del complemento se llama DSA.MSC, y se puede ejecutar el administrador de una de estas tres formas.

1. Seleccionando Usuarios y equipos de Active Directory desde el grupo Herramientas administrativas en el grupo Programas del menú inicio.
2. Resaltando un dominio en el árbol de la consola del complemento Dominios y confianzas de Active Directory y escoger Administrar en el menú Acción. Esto abre un nuevo cuadro de dialogo de la MMC llamado Usuarios y equipos de Active Directory dejando la ventana Dominios y confianzas de Active Directory intacta.
3. Abriendo el cuadro de dialogo Ejecutar desde el menú Inicio y ejecutar el archivo de complemento DSA.MSC.

Para realizar muchas de las funciones que proporciona el complemento Usuarios y equipos de Active Directory es necesario iniciar sesión en el dominio utilizando una cuenta que tenga privilegios administrativos. Se puede utilizar el Asistente para delegación de control para delegar tareas administrativas sobre objetos específicos a otros usuarios sin concederles acceso administrativo completo al dominio.

4. Objetos de Active Directory

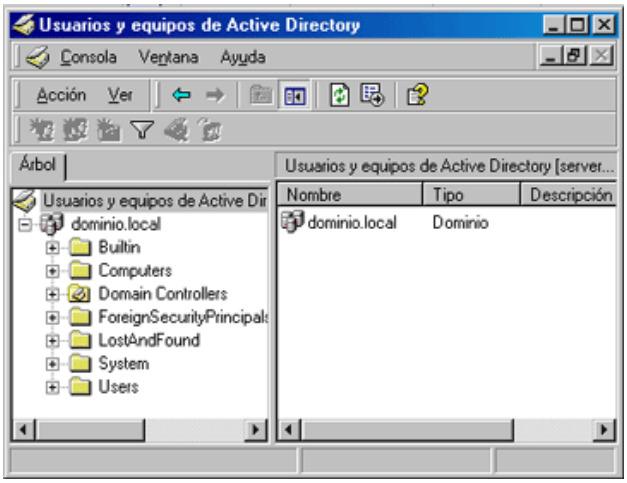
El cuadro de diálogo principal de Usuarios **y equipos de Active Directory** contiene muchos de los elementos estándar de las pantallas de la MMC. El árbol de la consola (a la izquierda) muestra un dominio Active Directory y los objetos contenedor dentro de una pantalla expandible. El panel de resultados (a la derecha) muestra los objetos del contenedor resaltado. El administrador incluye una barra de herramientas especializada que proporciona acceso instantáneo a las funciones más comúnmente utilizadas y una barra de descripción que proporciona información sobre el estado del administrador o sobre el objeto resaltado actualmente. El programa muestra las acciones que se pueden realizar sobre cada objeto en el menú Acción una vez que se han pulsado los objetos.

Los objetos de la pantalla Usuarios y equipos de Active Directory representan tanto entidades físicas (equipos y usuarios), como las entidades lógicas (grupos y unidades organizativas).

Modo normal y modo avanzado

De forma predeterminada, Usuarios y equipos de Active Directory opera en modo normal. El modo normal sólo muestra los objetos a los que los administradores accederán con mayor probabilidad durante una sesión de mantenimiento de Active Directory típica. Esto incluye las unidades organizativas que contienen los usuarios y grupos predefinidos creados durante la instalación de Active Directory y todos los objetos creados por los administradores después de la instalación. El modo normal también oculta ciertas pestañas de la ventana Propiedades de un objeto, incluyendo la pestaña Objeto y la pestaña Seguridad que se pueden utilizar para establecer permisos para el objeto.

Sin embargo, cuando se escoge **Características avanzadas** en el menú **Ver** del administrador, la pantalla cambia para incluir todos los objetos Active Directory del sistema que representan directivas, registros DNS y otros elementos del servicio de directorio, además del contenedor LostAndFound. Desde esta interfaz se puede consultar información sobre los objetos del sistema y controlar el acceso a ellos modificando los permisos asociados. Como el acceso a estos objetos no se requiere con frecuencia, se puede impedir que aparezcan dejando el administrador en modo normal. Sin embargo, cuando haya que modificar los permisos de los objetos estándar como unidades organizativas, usuarios y grupos, habrá que activar las Características avanzadas para acceder a la pestaña Seguridad de la ventana Propiedades de un objeto.



En estos formularios veremos una serie de iconos, que son los siguientes:

	**Dominio:** Objeto raíz de la pantalla Usuarios y equipos de Active Directory; identifica el dominio que está administrando actualmente el administrador.
	**Unidad organizativa:** Objeto contenedor utilizado para crear agrupaciones lógicas de objetos equipo, usuario y grupo.
	**Usuario:** Representa un usuario de la red y funciona como un almacén de información de identificación y autenticación.
	**Equipo:** Representa un equipo de la red y proporciona la cuenta de máquina necesaria para que el sistema inicie sesión en el dominio.
	**Contacto:** Representa un usuario externo al dominio para propósitos específicos como envío de correo electrónico; no proporciona las credenciales necesarias para iniciar sesión en el dominio.

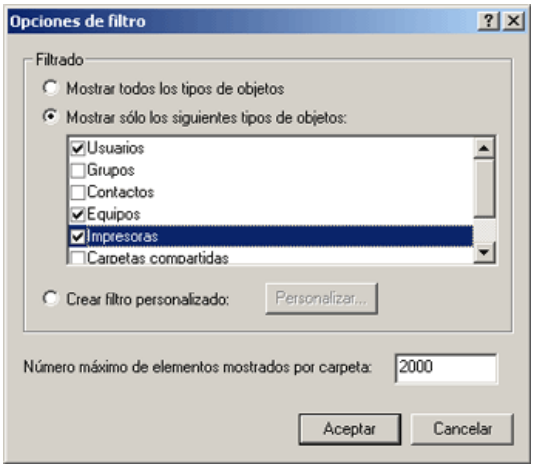
	Grupo: Objeto contenedor que representa una agrupación lógica de usuarios, equipos u otros grupos (o los tres) que es independiente de la estructura del árbol de Active Directory. Los grupos pueden contener objetos de diferentes unidades organizativas y dominios.
	Carpeta compartida: Proporciona acceso de red, basado en Active Directory, a una carpeta compartida en un sistema Windows 2000.
	Impresora compartida: Proporciona acceso de red, basado en Active Directory, a una impresora compartida en un sistema Windows 2000.

Se puede utilizar el complemento Usuarios y equipos de Active Directory para administrar cualquier dominio de la red. Para cambiar el dominio que se muestra en el administrador, hay que resaltar la raíz o el objeto dominio en el árbol de la consola y escoger Conectar con el dominio en el menú Acción. Esto muestra el cuadro de diálogo Conectar con el dominio, donde se puede introducir el nombre del dominio o buscar otro dominio.

En el menú Acción también se puede escoger Conectar con el controlador de dominio para acceder al dominio seleccionado utilizando un controlador de dominio específico de la red. A menos que los controladores de dominio no estén sincronizados, la información debería ser la misma en todas las replicas, pero algunas veces puede ser útil seleccionar un controlador de dominio en una ubicación diferente para evitar una lenta o cara conexión WAN.

Cuando se empieza a poblar Active Directory con nuevos objetos, puede crecer rápidamente a un tamaño difícil de manejar. Un elevado número de objetos en la pantalla puede dificultar la localización del objeto específico que se necesita. Para evitar que se muestren temporalmente los objetos que no es necesario ver, se puede aplicar un filtro al complemento Usuarios y equipos de Active Directory basándose en los tipos de objetos o basándose en el contenido de atributos de objetos específicos.

Cuando se escoge **Opciones de filtro desde el menú Ver**, aparece el cuadro de diálogo Opciones de filtro. Aquí se puede optar por mostrar todos los tipos de objetos, seleccionar tipos de objetos específicos a mostrar o crear un filtro personalizado basándose en los atributos de los objetos.



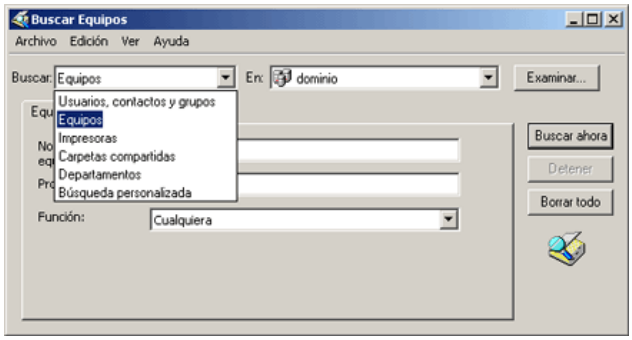
Cuando se selecciona la opción Crear filtro personalizado y se pulsa el botón Personalizar, se muestra un cuadro de diálogo Buscar Búsqueda personalizada. En este cuadro de diálogo se puede seleccionar un tipo de objeto, escoger un atributo de ese objeto y especificar un valor completo o parcial para ese atributo.

También se pueden **buscar** objetos específicos en todo Active Directory sin modificar lo que muestra el administrador.

Si se selecciona el objeto dominio y se escoge **Buscar en el menú Acción**, se muestra el cuadro de diálogo Buscar Usuarios, contactos y grupos, en el cual se puede especificar el tipo de objeto que se desea localizar, un dominio específico o todo el directorio y el nombre y descripción del objeto.

El programa busca entonces en el CG que se creó automáticamente en el primer controlador del dominio para localizar el objeto deseado. El CG es un subconjunto de todo Active Directory que sólo contiene los atributos más comúnmente utilizados, lo que facilita la búsqueda de un objeto específico. Sin el CG, la tarea de buscar en una instalación Active Directory que incluye controladores de dominio en ubicaciones remotas podría requerir un extenso tráfico WAN que es tan lento como caro.

La pestaña Opciones avanzadas del cuadro de dialogo Buscar Usuarios, contactos y grupos utiliza la misma interfaz que la característica Filtro personalizado. De la misma forma, se pueden buscar objetos basándose en sus atributos. Si un atributo que se selecciona no es parte del CG, la búsqueda procederá inspeccionando el contenido real de los controladores de dominio de la red. En algunos casos, esto puede ralentizar considerablemente el proceso de búsqueda.



4.1. Objetos predeterminados de Active Directory

Un dominio Active Directory recién creado contiene objetos unidades organizativas, equipos, usuarios y grupos que crea de forma predeterminada el Asistente para instalación de Active Directory. Estos objetos proporcionan acceso al sistema a varios niveles e incluyen grupos que permiten a los administradores delegar tareas de mantenimiento de la red específicas a otros. Incluso si no se espera utilizar esos objetos en el futuro, hay que utilizarlos para crear otros objetos con los permisos apropiados para la red.

Por ejemplo, aun si no se desea tener ningún usuario único con el control completo concedido a la cuenta de administrador, hay que iniciar sesión como administrador para poder crear los nuevos objetos usuario con los derechos y permisos deseados. Con Active Directory se pueden dejar partes de la estructura del directorio «huérfanas» si se modifica, se borra o se desactiva la cuenta de administrador sin haber creado primero otros objetos usuario o haberles concedido permisos equivalentes para las distintas partes del directorio.

Objetos creados de forma predeterminada en un dominio Active Directory			
Nombre del objeto	**Tipo de objeto**	**ubicación**	**Función**
Builtin	builtinDomain	Dominio raíz	Contenedor predeterminado para los grupos que proporcionan acceso a las funciones de administración del servidor.
Computers	Contenedor	Dominio raíz	Contenedor predeterminado para cuentas de equipo actualizadas.
Users	Contenedor	Dominio raíz	Contenedor predeterminado para cuentas de usuario actualizadas.
Domain controllers	Unidad organizativa	Dominio raíz	Contenedor predeterminado para los nuevos controladores de dominio Windows 2000.
Opers. de cuentas	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar las cuentas de usuario y de grupo del dominio.
Administradores	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar completamente el equipo/dominio.
Operadores de copia	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden saltarse la seguridad de los archivos para hacer copia de seguridad de ellos.

Invitados	Grupo de seguridad. Integración local	Builtin	Usuarios que tienen concedido acceso de invitado al equipo/dominio.
Opers. de impresión	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar las impresoras del dominio.
Duplicadores	Grupo de seguridad. Integración local	Builtin	Soporta la replica de archivos en un dominio.
Opers. de servidores	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar. servidores de dominio.
Usuarios	Grupo de seguridad. Integración local	Builtin	Usuarios corrientes.
Usuarios DHCP	Grupo de seguridad. Dominio local	Contenedor Users	Sus miembros sólo tienen acceso de lectura al Servidor DHCP
DnsAdmins	Grupo de seguridad. Dominio local	Contenedor Users	Administradores del DNS.
Servidores RAS e IAS	Grupo de seguridad. Dominio local	Contenedor Users	Servidores Ras e IAS.
Usuarios WINS	Grupo de seguridad. Dominio local	Contenedor Users	Sus miembros solo tienen acceso de lectura a WINS.
Publicadores de certificados	Grupo de seguridad. Global	Contenedor Users	Agentes de certificación de la empresa y de renovación.
DnsUpdateProxy	Grupo de seguridad. Global	Contenedor Users	Clientes de DNS a los que se permite realizar actualizaciones dinámicas en nombre de algunos otros clientes (como servidores DHCP).
Admins. del dominio	Grupo de seguridad. Global	Contenedor Users	Administradores designados del dominio.
Equipos del dominio	Grupo de seguridad. Global	Contenedor Users	Todas las estaciones de trabajo y servido res unidos al dominio.
Controladores de dominio	Grupo de seguridad. Global	Contenedor Users	Todos los controladores de dominio del dominio.
Invitados del dominio	Grupo de seguridad. Global	Contenedor Users	Todos los in vitados del dominio.
Usuarios del dominio	Grupo de seguridad. Global	Contenedor Users	Todos los usuarios del dominio.
Administración de empresas	Grupo de seguridad.	Contenedor Users	Administradores designados de la empresa.

	Global		
Administradores de esquema	Grupo de seguridad. Global	Contenedor Users	Administradores designados del esquema.
Administrador	Usuario	Contenedor Users	Cuenta predefinida para administrar el equipo/dominio.
Invitado	Usuario	Contenedor Users	Cuenta predefinida para el acceso en calidad de invitado al equipo/dominio.
IUSR_xxx	Usuario	Contenedor Users	Cuenta predefinida para el acceso anónimo a los Servicios de Internet información Server (IIS).
IWAM_xxx	Usuario	Contenedor Users	Cuenta predefinida para el acceso anónimo a aplicaciones IIS sin proceso.
Krbtgt	Usuario	Contenedor Users	Cuenta del servicio Centro de distribución de claves.

5. Creación de unidades organizativas

El esquema del servicio de directorio establece qué objetos se pueden crear en un dominio Active Directory, dónde se pueden ubicar y qué atributos se permite que tengan. Usuarios y equipos de Active Directory solo permite crear objetos en las ubicaciones apropiadas para el tipo de objeto. Por ejemplo, no se puede crear un objeto unidad organizativa (OU) subordinada a un objeto usuario, pero un objeto usuario puede subordinarse a un objeto OU.

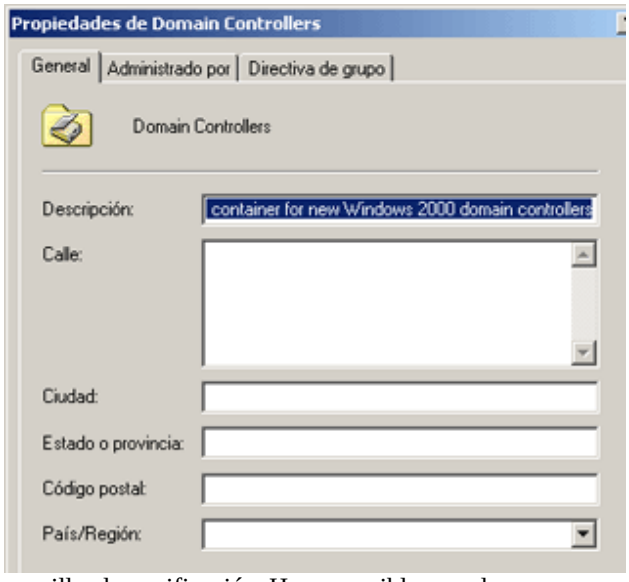
Sin embargo, las OU se pueden subordinar unas a otras y el número de capas de OU que se pueden crear en el dominio Active Directory es ilimitado. Para crear una OU hay que pulsar el objeto dominio u otra OU en el panel de ámbito o en el de resultados de Usuarios y equipos de Active Directory y escoger Nuevo en el menú Acción y seleccionar Unidad organizativa. también se puede pulsar el botón Crear un nuevo departamento en la barra de herramientas de Usuarios y equipos de Active Directory para conseguir el mismo efecto. después de especificar un nombre para el nuevo objeto en el cuadro de diálogo Nuevo objeto, el administrador crea un icono con el nombre apropiado y lo inserta en la pantalla de Usuarios y equipos de Active Directory.

Una vez que se ha creado una OU es posible poblarla con otros objetos, como usuarios, equipos, grupos y otras OU, o se pueden modificar sus atributos abriendo la ventana Propiedades desde el menú Acción.

5.1. Configuración de los objetos OU

La ventana **Propiedades** de una OU consta de tres pestañas. La pestaña General y la pestaña Administrado por permiten especificar información sobre la OU como una frase descriptiva y una dirección para la ubicación del objeto, además de la identidad de la persona responsable de administrar la OU. La información que se incluye en estas pestañas depende del criterio utilizado para diseñar el Active Directory. Una OU puede estar asociada a un departamento particular dentro de una organización, una ubicación física como una habitación, una planta o un edificio, o incluso una sucursal en una ciudad o país particular.

La pestaña **Directiva de grupo** es donde se crean y administran los vínculos a los objetos directiva de grupo de Active Directory. Los objetos directiva de grupo son colecciones de parámetros del sistema que controlan la apariencia y la funcionalidad de los clientes de la red. Cuando se aplican directivas de grupo a OU, dominios y sitios, todos los objetos contenidos en esas entidades heredan los parámetros del sistema.



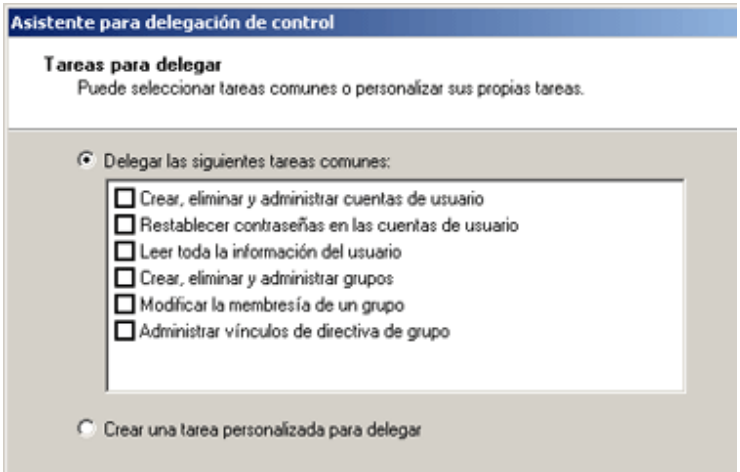
Las OU se pueden enlazar a múltiples objetos directiva de grupo en esta pestaña y, se pueden controlar las prioridades con que se aplican las directivas. Cuando se utilice el botón Modificar de la pestaña directiva de grupo para modificar un objeto directiva de grupo, Usuarios y equipos de Active Directory ejecuta el complemento MMC directiva de grupo.

Cuando se activan las **Características avanzadas** en el menú Ver de Usuarios y equipos de Active Directory, la ventana Propiedades de la OU también muestra la pestaña Objeto y la pestaña Seguridad. La pestaña Objeto muestra la ruta de acceso completa al objeto en la jerarquía del dominio, las fechas y horas de su creación y última modificación y los números de secuencia de actualización de la creación y la última modificación.

La pestaña Seguridad permite controlar el acceso al objeto asignando permisos a usuarios y grupos. Con la casilla de verificación Hacer posible que los permisos heredables se propaguen, también se puede controlar si el objeto hereda los permisos que han sido asignados a su objeto primario.

El botón Avanzada de la pestaña Seguridad proporciona acceso al cuadro de diálogo Configuración de control de acceso desde el que se puede controlar el acceso al objeto con un detalle mucho mayor. En el cuadro de diálogo Seguridad, se puede especificar si usuarios y grupos específicos tienen permiso para crear y eliminar objetos secundarios en la OU, pero esta pantalla permite especificar que tipos de objetos se pueden crear y eliminar.

5.2.Delegación del control de los objetos



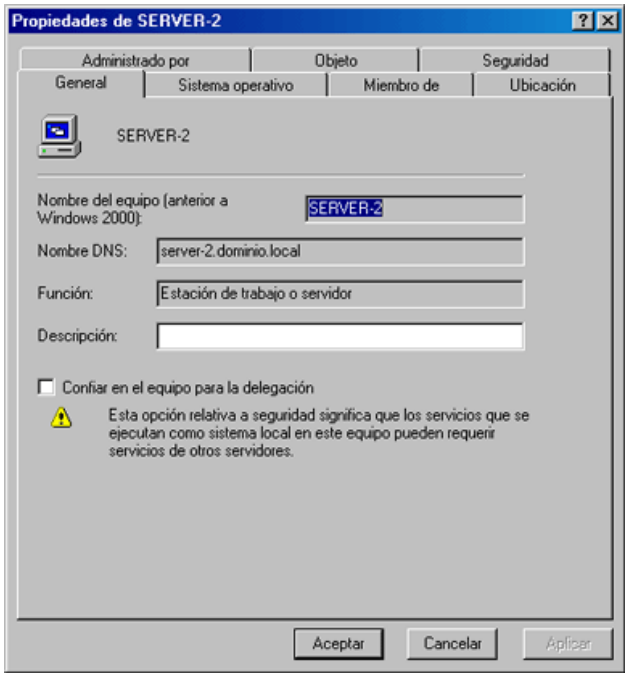
Active Directory esta diseñado para soportar redes empresariales mucho más grandes que la que soportan los dominios Windows NT, y las redes mas grandes requieren, naturalmente, más atención y mantenimiento por parte de los Administradores. Active Directory permite a los administradores delegar el control sobre objetos contenedor específicos a otros usuarios sin otorgarles acceso completo al dominio. Para hacer esto, hay que ejecutar el Asistente para delegación de control escogiendo **Delegar control** desde el menú **Acción** de un dominio o **unidad organizativa**.

El asistente pide primero que se especifique el objeto contenedor sobre el que se desea delegar el control y los usuarios o grupos (o ambos) a los que se desea delegar el control. Una vez que se haya hecho esto, el asistente muestra la pantalla Tipo de objeto de Active Directory, que se puede utilizar para especificar que tipos de objetos del contenedor podrán controlar los usuarios/grupos seleccionados. Se puede, por ejemplo, conceder a un usuario o grupo especifico control sobre los objetos usuario solo en el contenedor, permitiéndoles actualizar información de usuario pero impidiéndoles la modificación de otros tipos de objetos.

En el cuadro de diálogo Permisos, se especifica el grado de control que se desea que tengan los usuarios/grupos seleccionados sobre los objetos seleccionados. El cuadro Mostrar estos permisos permite seleccionar si se desea trabajar con los permisos generales que conciernen a todo el objeto o los permisos de la propiedad que controlan el acceso a los atributos individuales del objeto. Con este tipo de permisos se puede conceder a los usuarios la capacidad de modificar algunas de las propiedades del objeto al mismo tiempo que se protegen otras. De esta forma, cabe la posibilidad de permitir a los Administradores del departamento realizar modificaciones sencillas en los objetos usuario, como cambiar las direcciones y los números de teléfono, sin poner en peligro otras propiedades del objeto.

Una vez que se le ha proporcionado al asistente la información apropiada, se configura el objeto seleccionado con los permisos adecuados. Si se comprueba la pestaña Seguridad de la ventana Propiedades del objeto, se podrán observar los permisos que ha asignado el asistente a los usuarios o grupos seleccionados.

6. Configuración de los objetos equipo



Una vez que Usuarios y equipos de Active Directory crea el objeto equipo, se pueden configurar sus atributos utilizando las siguientes siete propiedades: General, Sistema operativo, Miembro de, ubicación, Administrado por, Objeto y Seguridad. Casi todas las pestañas tienen el mismo propósito que las de otros objetos. Las dos que son únicas para el objeto Equipo son Sistema operativo y ubicación.

La pestaña Sistema operativo identifica el sistema operativo que se esta ejecutando en el equipo, la versión y el service pack instalado actualmente. Estos campos no son modificables; están en blanco cuando se crea manualmente un objeto equipo y se rellenan cuando el equipo se une a un dominio. La pestaña ubicación permite especificar que ubicaciones sirve el sitio en la configuración del directorio.

Usuarios y equipos de Active Directory proporciona acceso administrativo a **equipos remotos** representados por objetos en Active Directory. Cuando se pulsa un objeto equipo y se escoge Administrar en el menú Acción, el administrador abre el complemento MMC Administración de equipos con el equipo como foco. Con esta característica, se pueden leer los registros de sucesos del sistema remoto, manipular sus servicios y realizar cualquiera del resto de las tareas que proporciona el complemento administración de equipos.

7. Publicación de carpetas compartidas

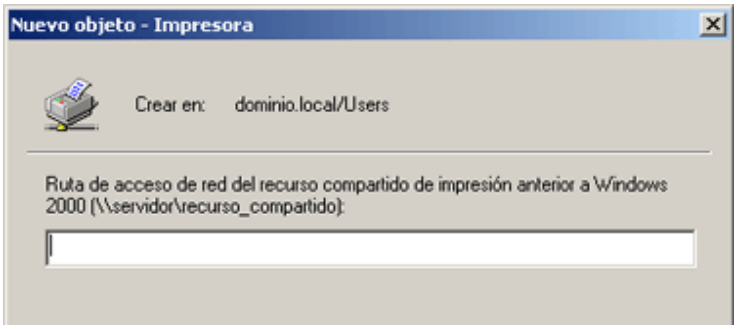
Los objetos carpeta compartida permiten publicar directorios de red compartidos en Active Directory, lo que permite a los usuarios acceder a ellos directamente explorando el Entorno de red del objeto. Esto elimina la necesidad de que los usuarios conozcan la ubicación exacta de la carpeta compartida. La creación de un objeto carpeta compartida no crea realmente el recurso compartido; hay que hacer esto manualmente en la pestaña Compartir de la ventana Propiedades de la unidad de disco o de la carpeta en la ventana del Explorador de Windows o en la ventana Mi PC. También se pueden crear objetos carpeta compartida para carpetas del Sistema de archivos distribuidos (DFS, Distributed File Sytem).

Para crear un objeto carpeta compartida, hay que pulsar un objeto contenedor en **Usuarios y equipos de Active Directory**, escoger **Nuevo** en el menú Acción y seleccionar **Carpeta compartida**. En el cuadro de dialogo Nuevo objeto, hay que especificar un nombre para el nuevo objeto a introducir la ruta de acceso UNC al recurso compartido. Después de que el administrador cree el objeto, es posible configurarlo utilizando las pestañas de la ventana Propiedades del objeto.

Los permisos que se establecen en la pestaña Seguridad de la ventana Propiedades de la carpeta compartida no controlan el acceso a la propia carpeta compartida, solo al objeto carpeta compartida. Para acceder a la carpeta por medio de Active Directory, un usuario debe tener permiso para acceder tanto al recurso compartido como al objeto. Lo mismo es cierto para un objeto impresora.

8. Publicación de impresoras

La creación de objetos impresora permite a los usuarios acceder a las impresoras a través de Active Directory prácticamente de la misma forma en que acceden a las carpetas compartidas. Un objeto impresora se crea como se haría con un objeto carpeta compartida, seleccionando un contenedor y escogiendo Nuevo\Impresora en el menú Acción y especificando la ruta de acceso UNC a la impresora compartida. El administrador crea entonces el objeto, combinando el nombre del sistema anfitrión y el del recurso compartido para formar el nombre del objeto.



9. Traslado, cambio de nombre y eliminación de objetos

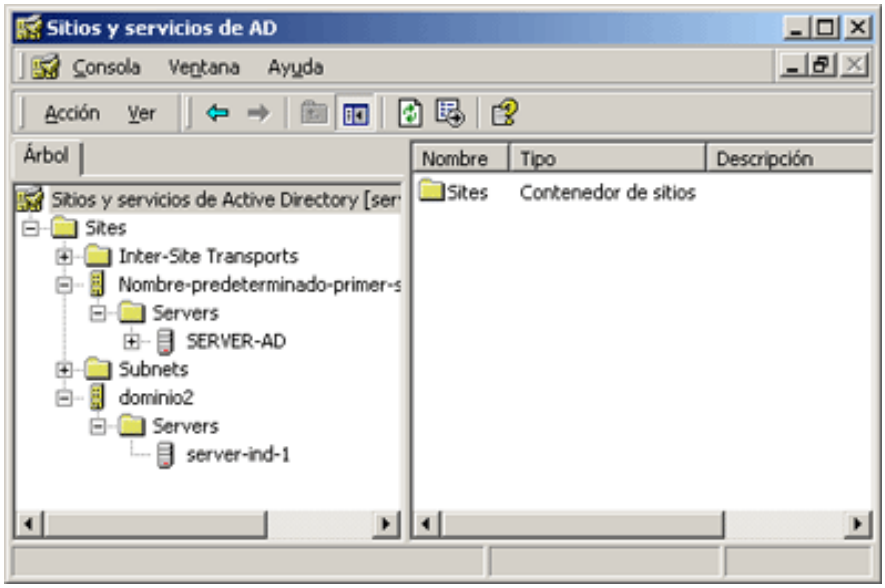
Una vez que se han creado objetos en Active Directory, se puede utilizar Usuarios y equipos de Active Directory para remodelar el árbol en cualquier momento trasladando objetos a diferentes contenedores, cambiándoles el nombre y eliminándolos. El **menú Acción** de casi cualquier objeto Active Directory contiene un comando **Mover**, que abre un cuadro de diálogo en el que se puede buscar un contenedor donde situar el objeto. También se pueden seleccionar varios objetos manteniendo presionada la tecla CTRL mientras se pulsa en ellos con el ratón y moviéndolos conjuntamente al mismo contenedor.

Cuando se traslada un objeto contenedor a una nueva ubicación, se trasladan automáticamente todos los objetos incluidos en el contenedor al mismo tiempo y también se modifican las referencias a esos objetos en el resto de objetos de Active Directory. Si, por ejemplo, el Usuario X es un miembro del Grupo Y y se traslada la unidad organizativa que contiene el objeto usuario de X a una nueva ubicación, X sigue siendo miembro de Y, y la lista de miembros del Grupo Y se actualiza automáticamente para mostrar a X en su nueva ubicación. De la misma forma, cuando se cambia el nombre de un objeto utilizando el comando Cambiar nombre del menú Acción o pulsando sobre el objeto una vez, todas las referencias a ese objeto a lo largo de Active Directory Cambian para reflejar el nuevo nombre. Cuando se elimina un objeto contenedor, todos los objetos incluidos en el contenedor se eliminan también.

10. Sitios y servicios de Active Directory

Sitios y servicios de Active Directory es un complemento de Microsoft Management Console (MMC) que se utiliza para crear y administrar los sitios que constituyen una red de Microsoft Windows 2000 y para establecer vínculos entre los sitios. Un sitio se define como un grupo de equipos de una o varias subredes de protocolo de Internet (Internet Protocol, IP) que están bien conectadas. Una subred es una red que forma parte de otra red de mayor tamaño.

Bien conectadas significa que los sistemas comparten un transporte de red que proporciona comunicaciones de bajo coste y gran velocidad entre las máquinas y, generalmente, hace referencia a sistemas de una misma ubicación que están conectados mediante LAN. Los sistemas que no están bien conectados son los que utilizan comunicaciones relativamente lentas y caras. Active Directory consta de uno o varios sitios, pero los sitios no forman parte de los espacios de nombres con los que se trabaja al crear la jerarquía de Active Directory.



Los sitios no aparecen como objetos en el espacio de nombres de Active Directory; se hallan apartados completamente de la jerarquía de bosques, árboles y dominios. Un sitio puede contener objetos de diferentes dominios, y los objetos de un dominio pueden estar repartidos entre sitios diferentes. La razón fundamental para dividir la red de una empresa en varios sitios es aprovechar las comunicaciones eficientes entre los sistemas bien conectados y regular el tráfico con las conexiones más lentas y caras. Más concretamente, Active Directory utiliza los sitios durante la autenticación y la réplica.

Cuando se crea el primer controlador de dominio de Windows 2000 de la red, el Asistente para Active Directory crea el primer sitio, lo denomina **Nombre-predeterminado-primer-sitio** y lo asocia con el servidor que se acaba de promover. Se puede dejar este nombre o proporcionar a este sitio un nombre más descriptivo si se desea. Si todos los servidores de Active Directory de la red van a estar ubicados lo bastante cerca unos de otros como para comunicarse mediante conexiones LAN no hace falta ningún sitio más ni el complemento Sitios y Servicios de Active Directory. A medida que se promueve cada servidor de la red a controlador de dominio, Active Directory lo añade al sitio y configura automáticamente la topología de réplica entre los servidores.

Si se van a tener servidores en ubicaciones remotas, sin embargo, se pueden crear otros sitios utilizando Sitios y servicios de Active Directory. Al crear objetos subred y asociarlos con sitios concretos, se ofrece a Active Directory la información que necesita para añadir de manera automática al sitio correspondiente a cada servidor que se promueve a controlador de dominio, de acuerdo con la subred en la que se halla la máquina. Si se desplaza un servidor a una ubicación nueva en un sitio diferente hay que trasladar manualmente el objeto servidor al nuevo objeto sitio.

11. El esquema de Active Directory

El esquema es el sello de Active Directory, lo que indica el tipo de objetos que puede haber en la base de datos y sus atributos. Para personalizar Active Directory para su uso en la red, se puede modificar el esquema para crear nuevos tipos de objetos, añadir nuevos atributos a los tipos de objetos existentes y modificar el tipo de información incluida en un atributo. Para ello hay que utilizar el complemento de MMC denominado Esquema de Active Directory.

La modificación del esquema es una tarea que, por lo general, los administradores no tienen que realizar nunca. Como mucho, se llega a modificar el esquema de manera ocasional o, quizás, solo una vez. Las modificaciones del esquema son objeto de las mismas advertencias que las modificaciones del registro del sistema de Windows 2000, salvo que a mayor escala. Igual que las modificaciones inadecuadas del registro pueden afectar negativamente a un solo sistema, las modificaciones inadecuadas del esquema pueden tener un efecto devastador en toda la red.

12. Funciones de maestros de operaciones

Los controladores de dominios deben manejar cinco funciones de maestros de operaciones en cada bosque de Active Directory. Algunas de las funciones de maestros de operaciones resultan fundamentales para la red y, si la máquina que los facilita falla, se pondrá de manifiesto inmediatamente. Otras pueden no estar disponibles durante mucho tiempo sin que ni el operador ni los usuarios se den cuenta. Las funciones son las siguientes:

- **Emulador del controlador principal de dominio (PDC, Primary Domain Controller):** actúa como el controlador principal de dominio de Windows NT en los dominios que tienen controladores de dominio secundarios de Windows NT o que tienen equipos sin el software cliente de Windows 2000.

- **Maestro de esquema:** Controla todas las actualizaciones y modificaciones del esquema.

- **Maestro de nombres de dominio:** Controla la adición o eliminación de dominios.

- **Maestro de identificadores relativos (RID, Relative Identifier):** Asigna ID relativos a cada controlador de dominio.

- **Maestro de infraestructuras:** Actualiza los cambios en las referencias de grupo a usuario cuando se modifican las pertenencias a los grupos.

Generalmente no hay motivo para interferir en los maestros de operaciones. La transferencia de funciones resulta relativamente trivial. Se realiza una transferencia cuando el titular original de la función está disponible. En circunstancias graves, cuando el controlador que posee la función no esta disponible, se puede tomar una función, pero se trata de una medida drástica y no se debe adoptar a la ligera. En todos los casos, salvo con el emulador PDC, cuando se toma una función de maestro de operaciones (en lugar de transferirla), no se debe reactivar al titular original de la función tomada sin volver a dar formato completo al disco de inicio y reinstalar Windows 2000.