Usuarios, grupos y equipos. Conceptos básicos

Uno de los elementos fundamentales en la administración de una red, es el control de los usuarios, grupos y equipos. Por ello, debemos aprender cómo crearlos, modificarlos, organizarlos y, si llega el caso, eliminarlos. Además, deberemos asignar privilegios para cada uno de ellos, de modo que podamos establecer en qué medida y bajo qué condiciones podrán beneficiarse de los recursos de la red. Este objetivo lo cubriremos, en parte durante el presente capítulo, pero seguiremos completándolo en el siguiente.

Cuenta de usuario

Las cuentas de usuario también suelen identificarse como entidades de seguridad.

Como ya comentábamos en el capítulo anterior, una de las primeras ideas que deben quedar claras cuando hablamos de cuentas de usuario es que no siempre representan a personas concretas, sino que también pueden ser utilizadas como mecanismos de acceso para determinados servicios o aplicaciones de la máquina local o, incluso, de un equipo remoto. En definitiva, una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:

- Por razones de seguridad, debes evitar que varios usuarios utilicen la misma cuenta para iniciar sesión en el dominio.

  Permite **autenticar la identidad** de un usuario, porque sólo podrán iniciar una sesión aquellos usuarios que dispongan de una cuenta en el sistema asociada a una determinada contraseña.

- Permite **autorizar**, **o denegar**, el acceso a los recursos del dominio, porque, una vez que el usuario haya iniciado su sesión sólo tendrá acceso a los recursos para los que haya recibido los permisos correspondientes.

Cada cuenta de usuario dispone de un identificador de seguridad (*SID*, *Security IDentifier*) que es único en el dominio.

Cuentas integradas

Cuando se crea el dominio, se crean también dos nuevas cuentas: *Administrador* e *Invitado*. Posteriormente, cuando es necesario, se crea también la cuenta *Asistente de ayuda*. Estas son las denominadas *cuentas integradas* y disponen de una serie de derechos y permisos predefinidos:

Desde el punto de vista de la seguridad, puede ser interesante cambiar el nombre de la cuenta Administrador.

- **Administrador**: Tiene control total sobre el dominio y no se podrá eliminar ni retirar del grupo *Administradores* (aunque sí podemos cambiarle el nombre o deshabilitarla).
- **Invitado**: Está deshabilitada de forma predeterminada y, aunque no se recomienda, puede habilitarse, por ejemplo, para permitir el acceso a los usuarios que aún no tienen cuenta en el sistema o que la tienen deshabilitada. De forma predeterminada no requiere contraseña, aunque esta característica, como cualquier otra, puede ser modificada por el administrador.
- **Asistente de ayuda**: se utiliza para iniciar sesiones de *Asistencia remota* y tiene acceso limitado al equipo. Se crea automáticamente cuando se solicita una sesión de asistencia remota y se elimina cuando dejan de existir solicitudes de asistencia pendientes de satisfacer.

Por último, es importante tener en cuenta que, aunque la cuenta *Administrador* esté deshabilitada, podrá seguir usándose para acceder al controlador de dominio en *modo seguro*.

Cuenta de equipo

Como ocurría con las cuentas de usuario, una cuenta de equipo sirve para autenticar a los diferentes equipos que se conectan al dominio, permitiendo o denegando su acceso a los diferentes recursos del dominio. Del mismo modo que con las cuentas de usuario, las cuentas de equipo deben ser únicas en el dominio. Aunque una cuenta de equipo se puede crear de forma manual (como veremos más adelante), también se puede crear en el momento en el que el equipo se une al dominio.

Cuenta de grupo

Cuando una cuenta de usuario o de equipo está incluida en un grupo se dice que es *miembro del grupo*.

Un grupo es un conjunto de objetos del dominio que pueden administrarse como un todo. Puede estar formado por cuentas de usuario, cuentas de equipo, contactos y otros grupos. Podemos utilizar los grupos para simplificar 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 que comentaremos más abajo.

El *Directorio Activo* proporciona un conjunto de grupos predefinidos que pueden utilizarse tanto para facilitar el control de acceso a los recursos como para delegar determinados roles administrativos. Por ejemplo, el grupo *Operadores de copia de seguridad* permite a sus miembros realizar copias de seguridad de todos los controladores de dominio, en el dominio al que pertenecen.

Ámbito de los grupos

El ámbito de un grupo establece su alcance, es decir, en qué partes de la red puede utilizarse, y el tipo de cuentas que pueden formar parte de él. 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.
    - Otros grupos de ámbito local.
    - Grupos de ámbito global.
    - Grupos de ámbito universal.

  Las cuentas o grupos contenidos tendrán necesidades de acceso similares dentro del propio dominio. Por ejemplo, los que necesiten acceder a una determinada impresora.

- Los grupos de ámbito global son perfectos para contener objetos que se modifique con frecuencia, debido a que, como no se replican fuera del dominio, no generan tráfico en la red para la actualización del catálogo global.

Ámbito global: Sólo pueden incluir otros grupos y cuentas que pertenezcan al dominio en el que esté definido el propio grupo. Los miembros de este tipo de grupos pueden tener permisos sobre los recursos de cualquier dominio dentro del bosque. Sin embargo, estos grupos no se replican fuera de su propio dominio, de modo que, la asignación de derechos y permisos que alberguen, no serán válidas en otros dominios del bosque.

- Ámbito universal: Entre sus miembros pueden encontrarse cuentas o grupos de cualquier dominio del bosque, a los que se les pueden asignar permisos sobre los recursos de cualquier dominio del bosque.

Tipos de grupos

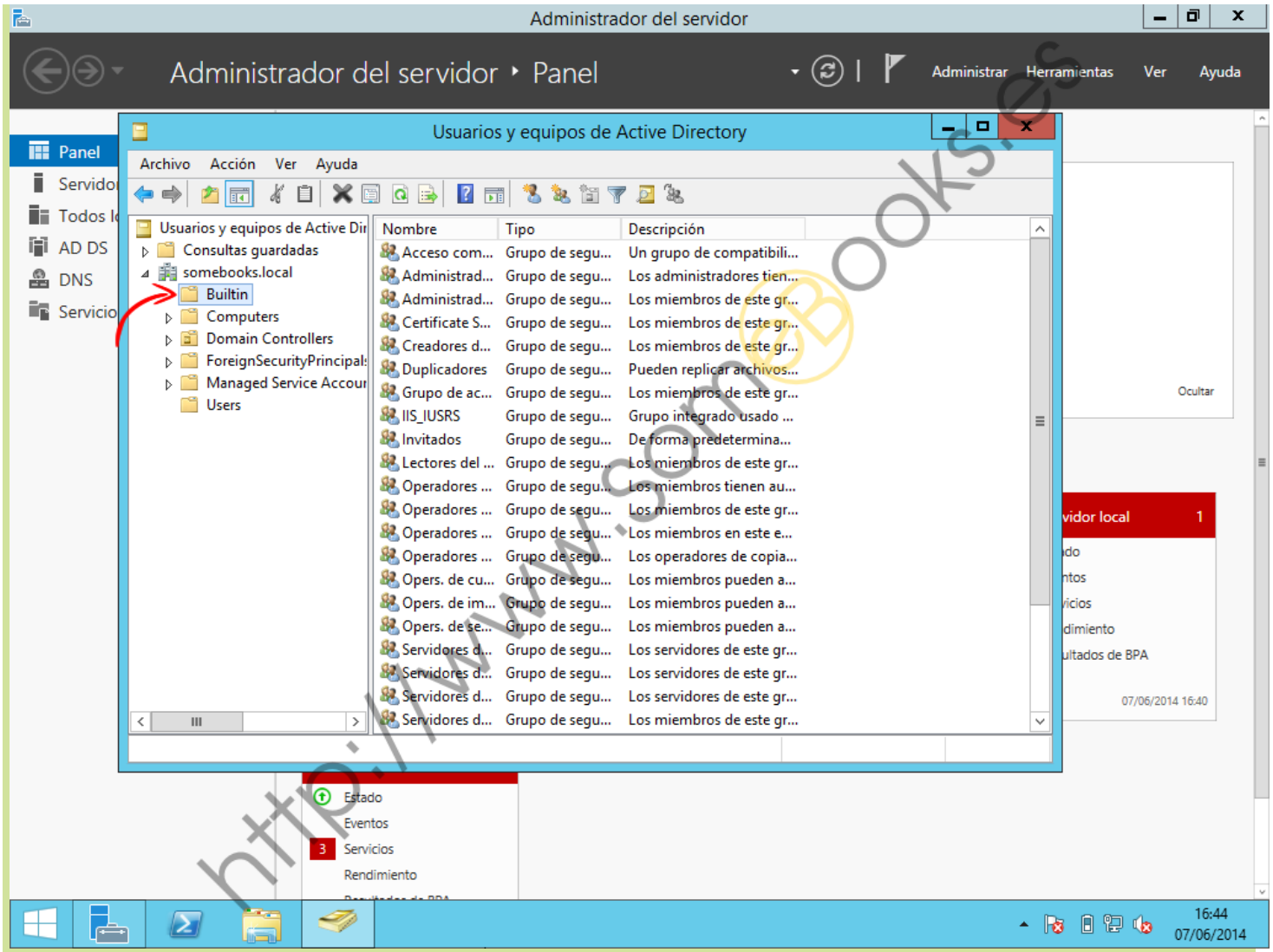
Existen dos tipos de grupos en *Active Directory*:

- Grupos de distribución: Se utilizan en combinación con programas como *Microsoft Exchange Server*, para crear listas de distribución de correo electrónico. 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. Con los grupos de seguridad podemos:
    - *Asignar derechos de usuario* a los grupos de seguridad del Directorio Activo. De esta forma, podemos establecer qué acciones pueden llevar a cabo sus miembros dentro del dominio (o del bosque). Como veremos después, durante la instalación del Directorio Activo, se crean grupos de seguridad predeterminados que facilitan al administrador la delegación de ciertos aspectos de la administración (como, por ejemplo, las copias de seguridad) en otros usuarios del sistema.
    - *Asignar permisos para recursos* a los grupos de seguridad. Lo que nos permite definir quién accede a cada recurso y bajo qué condiciones (control total, sólo lectura, etc.) También se establecen permisos de forma predeterminada sobre diferentes objetos del dominio para ofrecer distintos niveles de acceso.

Grupos integrados

Como hemos mencionado antes, durante la instalación del *Directorio Activo* se crean una serie de grupos que podremos utilizar para simplificar la asignación de derechos y permisos a otras cuentas o grupos. Como veremos más abajo, los grupos se administran con el complemento *Usuarios y equipos de Active Directory*. Cuando ejecutemos esta herramienta, encontraremos los grupos predeterminados en dos contenedores:

Los grupos predeterminados incluidos en el contenedor *Builtin* tienen un ámbito local.



En el contenedor *Users* podemos encontrar grupos predeterminados que tienen tanto ámbito local como global.

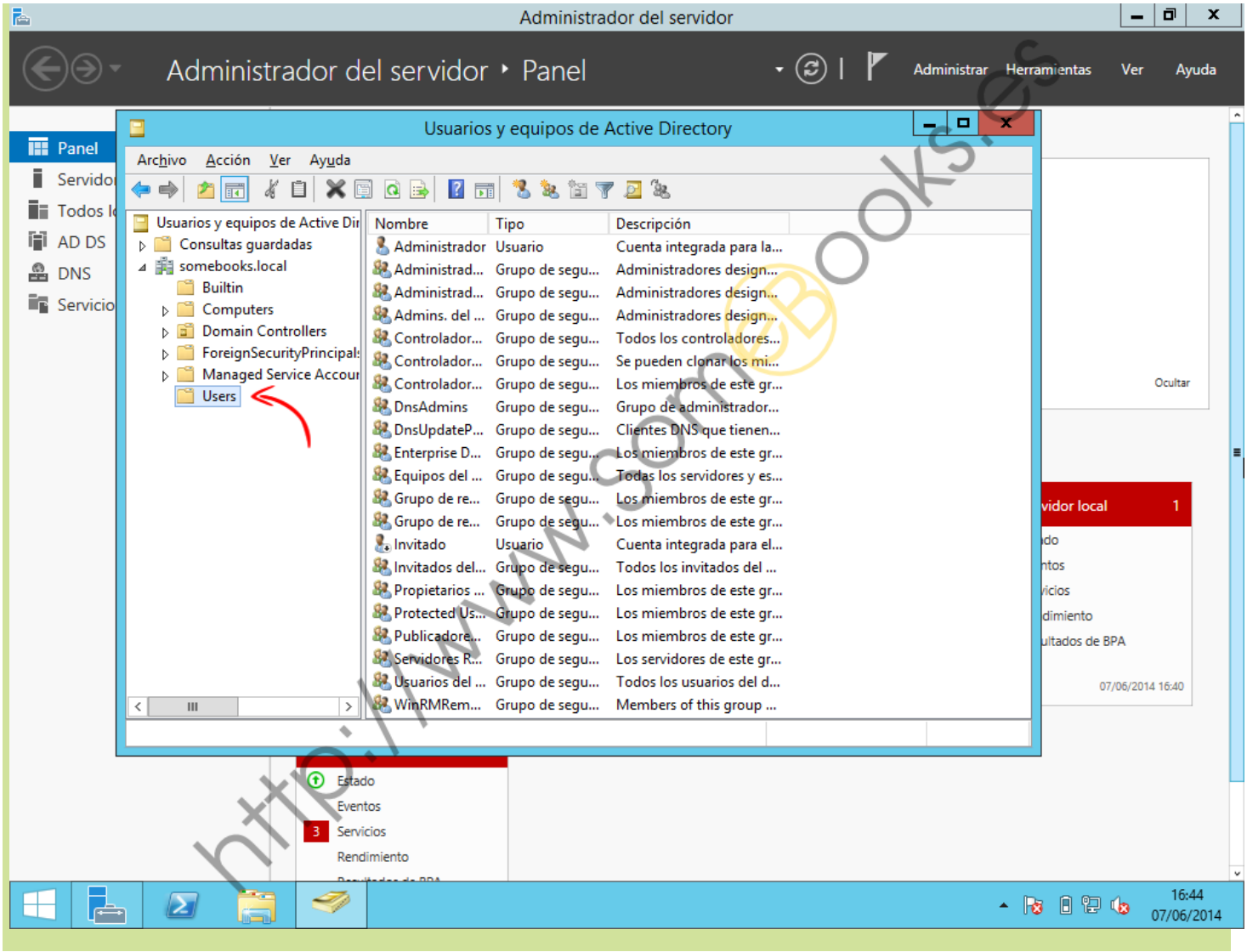
Puedes ver un pequeño resumen de todos ellos en la siguiente tabla:

Grupo	Descripción	Derechos de sus miembros
Operadores de cuentas	Sus miembros pueden crear, modificar y eliminar grupos y cuentas de usuario y equipo dentro de cualquier contenedor salvo en la unidad organizativa *Controladores de dominio*. Tampoco pueden modificar los grupos *Administradores* o *Administradores del dominio* (ni sus miembros). Sus miembros pueden iniciar y cerrar sesión de forma local en el controlador del dominio.	Permitir el inicio de sesión local Apagar el sistema

Administradores	Sus miembros tienen un control total sobre los controladores del dominio. Lógicamente, la cuenta *Administrador*es miembro predeterminado de este grupo. Un usuario que sea miembro de este grupo podrá asignarse cualquier privilegio que no ostentara de forma predeterminada.	Acceder al equipo desde la red Ajustar cuotas de memoria a los procesos Realizar backups Eliminar comprobación de recorrido Modificar la hora del sistema Crear un archivo de paginación. Depurar programas. Habilitar la delegación de confianza para cuentas de usuario y equipo. Forzar cierre desde un sistema remoto. Aumentar prioridad de planificación Cargar y descargar controladores de dispositivo Permitir el inicio de sesión local Administrar registro de seguridad y auditoría Modificar valores de entorno del firmware Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Restaurar archivos y directorios Apagar el sistema Tomar posesión de archivos y otros objetos
Operadores de copia de seguridad	Sus miembros pueden hacer backups, y restaurarlos, de todos los datos de los controladores del dominio, aunque no tengan permisos de lectura o escritura sobre ellos. También pueden iniciar sesión en los controladores de dominio y apagarlos.	Hacer backups de archivos y directorios, y restaurarlos. Permitir el inicio de sesión local. Apagar el sistema
Invitados	Por defecto, el grupo *Invitados del dominio* es miembro de este grupo. También lo es la cuenta *Invitado*(deshabilitada de forma predeterminada).	No tiene derechos de usuario predeterminados.
Creadores de confianza de bosque de entrada(sólo aparece en el dominio raíz del bosque)	Sus miembros pueden crear relaciones de confianza a nivel del bosque, siempre que sean unidireccionales al dominio raíz del bosque. Es decir, si nos encontramos en el bosque A, los miembros de este grupo pueden crear una relación de confianza para el bosque B que permita a los usuarios del bosque A acceder a los recursos del bosque B.	No tiene derechos de usuario predeterminados.
Operadores de	Sus miembros pueden cambiar la	No tiene derechos de usuario

configuración de red	configuración TCP/IP y renovar o liberar direcciones TCP/IP en los controladores del dominio. De forma predeterminada, no tiene ningún miembro.	predeterminados.
Usuarios del monitor de sistema	Sus miembros pueden comprobar los valores de rendimiento de los controladores del dominio. Pueden usarse en modo local o desde un cliente.	No tiene derechos de usuario predeterminados.
Usuarios del registro de rendimiento	Sus miembros pueden administrar contadores de rendimiento, registros y alertas en los controladores del dominio. Pueden usarse en modo local o desde un cliente.	No tiene derechos de usuario predeterminados.
Acceso compatible con versiones anteriores a Windows 2000	Sus miembros tienen acceso de lectura a todos los usuarios y grupos del dominio. Ofrece compatibilidad con equipos que ejecuten *Windows NT* 4.0 o anterior. Por defecto, la identidad Todos es miembro de este grupo.	Tener acceso a este equipo desde la red. Omitir comprobación de recorrido
Operadores de impresión	Sus miembros pueden administrar, crear, compartir o eliminar impresoras conectadas a los controladores del dominio. También puede instalar y desinstalar controladores de dispositivo en los controladores del dominio. No tiene miembros predeterminados.	Permitir el inicio de sesión local. Apagar el sistema
Usuarios de escritorio remoto	Sus miembros pueden iniciar una sesión remota en los controladores del dominio. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
Replicador	Alberga funciones de replicación de directorio. El *Servicio de replicación de archivos* lo utiliza en los controladores del dominio. No tiene miembros predeterminados y no debe asignarse ninguno.	No tiene derechos de usuario predeterminados.
Operadores de servidores	Sus miembros pueden iniciar sesión de forma interactiva, crear y eliminar recursos compartidos, iniciar y parar ciertos servicios, realizar backups y recuperarlos, formatear el disco duro y apagar el equipo. No tiene miembros predeterminados.	Hacer backups de archivos y directorios, y restaurarlos. Modificar la hora del sistema. Forzar el cierre desde un equipo remoto. Permitir el inicio de sesión local. Apagar el sistema
Usuarios	Sus miembros pueden realizar las tareas más frecuentes: ejecutar programas, utilizar impresoras (locales o de red), etc. Por defecto, los grupos *Usuarios de dominio*, *Usuarios autenticados* e *Interactivo* son miembros	No tiene derechos de usuario predeterminados.

	de este grupo. Las cuentas de usuario que se crean en el dominio son miembros de este grupo.	



También en este caso tienes una tabla con un resumen de sus grupos:

Grupo	Descripción	Derechos de sus miembros
Publicadores de certificados	Sus miembros pueden publicar certificados relativos a usuarios y equipos. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
DnsAdmins (Se instala con el servicio DNS)	Sus miembros pueden administrar el servicio DNS. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
nsUpdateProxy(Se instala con DNS)	Sus miembros son clientes DNS que pueden hacer	No tiene derechos de usuario predeterminados.

http://www.somosBooks.es

	actualizaciones dinámicas en lugar de otros clientes (p. ej. un servidor DHCP) No tiene miembros predeterminados.	
Administradores del dominio	Sus miembros tienen todo el control del dominio. Por defecto, este grupo se hizo miembro del grupo *Administradores* en los controladores del dominio, las estaciones de trabajo del dominio y los servidores miembros del dominio, cuando éstos se unieron al dominio. Lógicamente, la cuenta *Administrador*es miembro predeterminado de este grupo.	Acceder al equipo desde la red Ajustar cuotas de memoria a los procesos Realizar backups y restaurarlos Eliminar comprobación de recorrido Modificar la hora del sistema Crear un archivo de paginación Depurar programas Habilitar la delegación de confianza para cuentas de usuario y equipo. Forzar cierre desde un sistema remoto. Aumentar prioridad de planificación Cargar y descargar controladores de dispositivo Permitir el inicio de sesión local Administrar registro de seguridad y auditoría Modificar valores de entorno del firmware Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Apagar el sistema Tomar posesión de archivos y otros objetos
Equipos del dominio	Contiene todas las estaciones de trabajo y servidores que se han unido al dominio. Por defecto, al crear una cuenta de equipo, se hace miembro de este grupo automáticamente.	No tiene derechos de usuario predeterminados.
Controladores de dominio	Contiene todos los controladores del dominio.	No tiene derechos de usuario predeterminados.
Invitados del dominio	Contiene todos los invitados del dominio.	No tiene derechos de usuario predeterminados.
Usuarios del dominio	Contiene a los usuarios del dominio. Por defecto, las cuentas de usuario pasan a formar parte de este grupo cuando se crean. Así, para asignar permisos sobre un recurso a todos los usuarios (p. ej. una impresora), usaremos este grupo.	No tiene derechos de usuario predeterminados.
Administradores de organización(Sólo aparece en el dominio raíz del bosque)	Sus miembros controlan todos los dominios del bosque. Por defecto, este grupo forma parte del grupo *Administradores* en todos los controladores del bosque. La cuenta *Administrador* es	Acceder al equipo desde la red. Ajustar cuotas de memoria a los procesos. Realizar backups y restaurarlos. Eliminar comprobación de recorrido Modificar la hora del sistema. Crear un archivo de paginación. Depurar programas. Habilitar la

	miembro predeterminado de este grupo.	delegación de confianza para cuentas de usuario y equipo. Forzar cierre desde un sistema remoto. Aumentar prioridad de planificación Cargar y descargar controladores de dispositivo Permitir el inicio de sesión local Administrar registro de seguridad y auditoría Modificar valores de entorno del firmware Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Apagar el sistema Tomar posesión de archivos y otros objetos
Propietarios del creador de directivas de grupo	Sus miembros pueden cambiar la directiva de grupo del dominio. Por defecto, la cuenta *Administrador* es miembro de este grupo.	No tiene derechos de usuario predeterminados.
IIS_WPG(Se instala con IIS)	Este grupo de trabajo para *Internet Information Services* (IIS) 6.0. IIS tiene procesos que ofrecen servicio a ciertos espacios de nombres (p. ej. *www.microsoft.com*)No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
Servidores RAS e IAS	Los servidores incluidos en el grupo pueden acceder a las propiedades de acceso remoto de los usuarios.	No tiene derechos de usuario predeterminados.
Administradores de esquema (aparece únicamente en el dominio raíz del bosque)	Sus miembros pueden modificar el esquema de Active Directory. Por defecto, la cuenta *Administrador* es miembro de este grupo.	No tiene derechos de usuario predeterminados.

Tanto los grupos del contenedor *Builtin* como los del contenedor *Users* pueden cambiarse libremente de contenedor, siempre que se mantengan dentro del mismo dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas (OU) del dominio, pero no se pueden mover a otros dominios.

Debemos conocer los privilegios y derechos que ofrece cada grupo predeterminado a sus miembros antes de asignarle una cuenta de usuario o equipo. Lógicamente, la precaución será mayor cuanto más elevadas sean las capacidades del grupo en cuestión.