

Introducción a Active Directory

1. ¿QUÉ ES ACTIVE DIRECTORY?

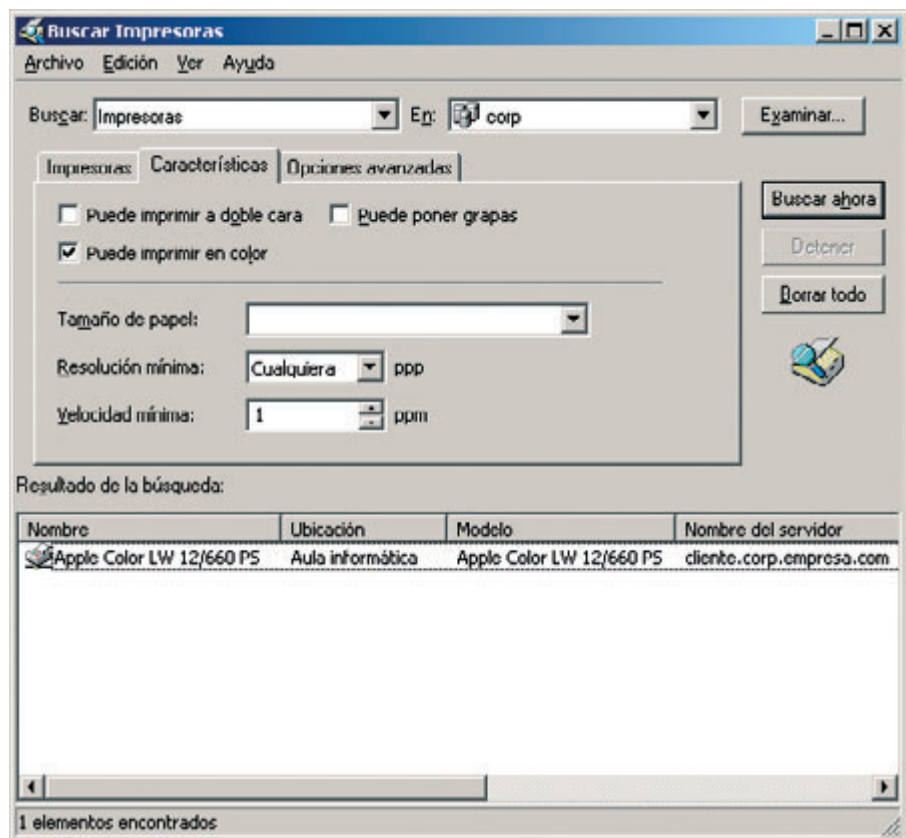
Active Directory es el servicio de directorio que proporciona Windows 2003. Un directorio es un lugar donde se acude cuando buscamos algún recurso en la red.

El servicio de directorio funciona de forma similar a las páginas amarillas. Por ejemplo, usted puede buscar fontaneros, peluqueros, médicos, etc. en las páginas amarillas.

De la misma forma podremos utilizar Active Directory para, por ejemplo, localizar las impresoras de la red que pueden imprimir en color.

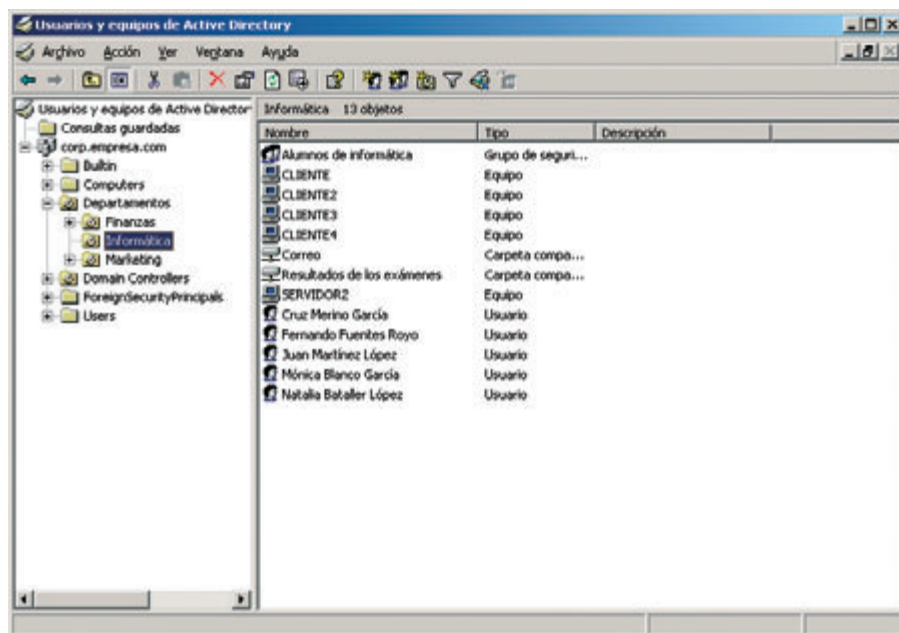
Active Directory actúa como el centro de información de la red:

- Para los **clientes** de la red, Active Directory proporciona un lugar y una forma de buscar recursos: personas, impresoras, máquinas de fax, aplicaciones, bases de datos, etc.



- Para los **administradores** de la red, Active Directory es la herramienta y el medio que permite controlar la seguridad en la red.

En un dominio, el directorio reside en los ordenadores que actúan como controladores de dominio. Cada uno de ellos tiene una copia del mismo.



Active Directory proporciona un lugar (el directorio) donde almacenar toda la información que necesita el administrador, facilitándole, en gran medida, su trabajo.

En un dominio, el directorio reside en los ordenadores que actúan como controladores de dominio. Es importante entender que puede haber más de un controlador de dominio en un dominio, sobre todo si el número de ordenadores es grande. En estos casos, todos los controladores tienen la misma copia del directorio.

De hecho, cuando se realiza alguna modificación en un controlador de dominio, se transmite a los restantes controladores de dominio en un proceso que se conoce como “**replicar el directorio**”.

2. OBJETOS DE ACTIVE DIRECTORY

Es necesario introducir una serie de conceptos antes de estudiar cómo utilizar Active Directory en una red Windows 2003.

Así, el concepto fundamental en Active Directory es el de **objeto**. Un objeto es cualquier elemento o recurso que se puede encontrar en la red y que interesa administrar.

Para Active Directory, un usuario, impresora, grupo, carpeta compartida o aplicación es un objeto.

Los objetos se caracterizan por tener propiedades, que son conocidas en Active Directory con el nombre de **atributos**.

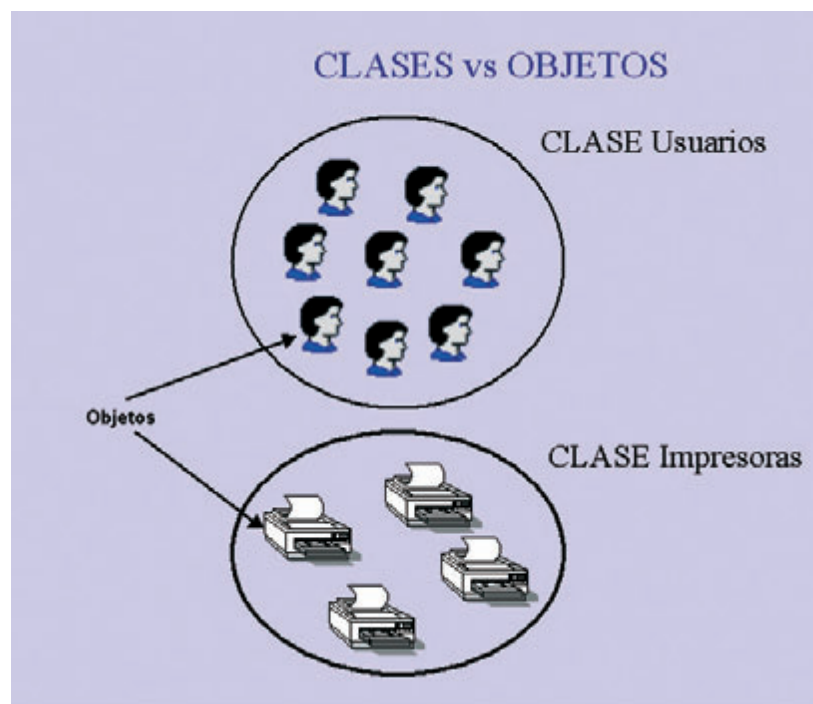
Por ejemplo, en el caso de una impresora, podríamos tener como atributos su velocidad de impresión, si puede imprimir en color, etc. En el caso de una cuenta de usuario, podríamos tener su nombre, apellidos, dirección de correo electrónico, etc.



Al manejar los recursos de la red como objetos, Active Directory permite realizar búsquedas utilizando sus atributos.

Así, podemos buscar impresoras que impriman en color o usuarios cuyo nombre empiece por la letra E.

En Active Directory, los objetos se organizan en clases. Ejemplos de clases son usuarios, impresoras, equipos, etc.



En Active Directory, toda la información sobre los objetos se almacena en el directorio.

Debe saber diferenciar entre lo que es una clase y lo que es un objeto. Así, la clase representa la idea que tenemos de los objetos, mientras que los objetos son casos concretos de las clases.

Por ejemplo, podemos tener la clase **Usuarios** y el objeto **Juan Martínez López**.

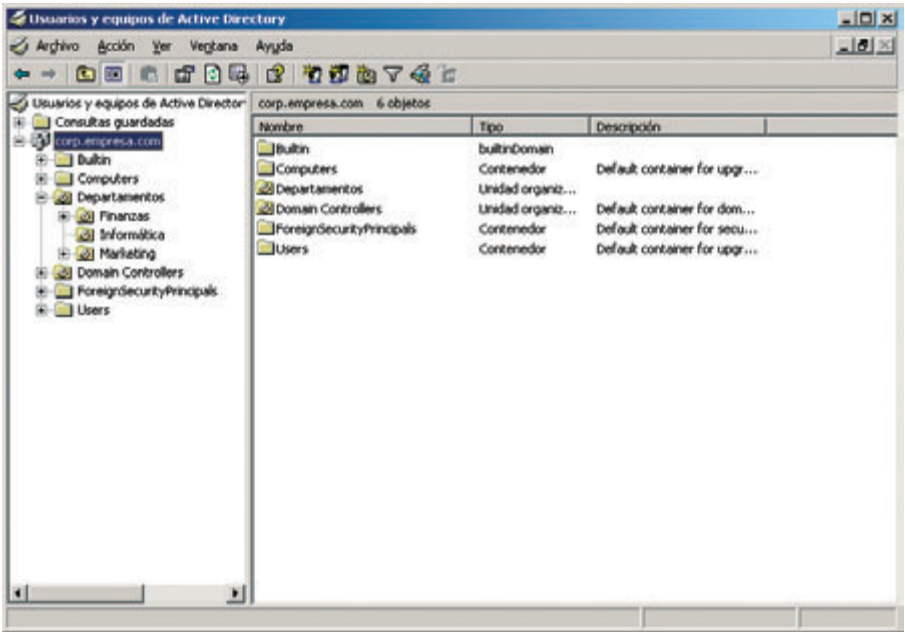
Así, la clase viene definida por los atributos que conforman a los objetos: nombre, apellidos, dirección, etc.; mientras que un objeto se diferencia de otro por el valor que tienen dichos atributos: Juan Martínez López, C/ Legazpi, 19, jmartinez@empresa.com, etc.

3. ESTRUCTURA DEL DIRECTORIO


Active Directory permite representar la estructura de la empresa en el directorio. Para ello, utiliza los conceptos de **dominio** y **unidad organizativa (UO)**.

Para trabajar con la estructura del dominio, utilizará la herramienta administrativa **Usuarios y equipos de Active Directory**.

Así, observe en la figura adjunta cómo tenemos el dominio **corp.empresa.com** en la parte superior del directorio, del que cuelga el resto de objetos.

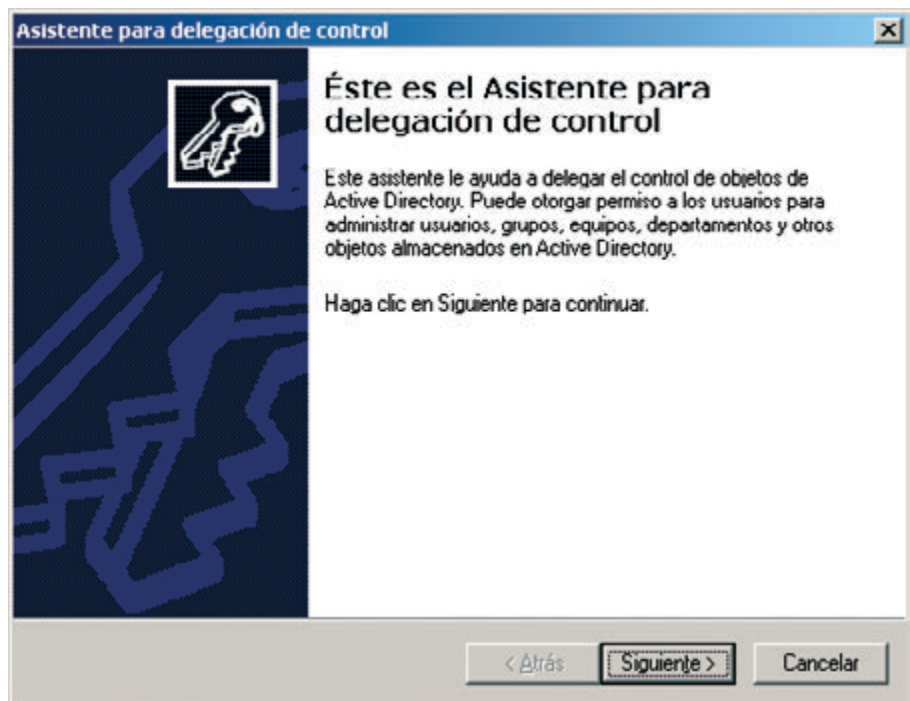


Bien, debe saber que en Active Directory, el **dominio** representa los límites de todo aquello que nos interesa en la red y que se almacena en el directorio.

Como el dominio puede ser demasiado general y no adaptarse exactamente a la estructura administrativa u organizativa de su empresa, Windows 2003 introduce el concepto de **unidad organizativa** .

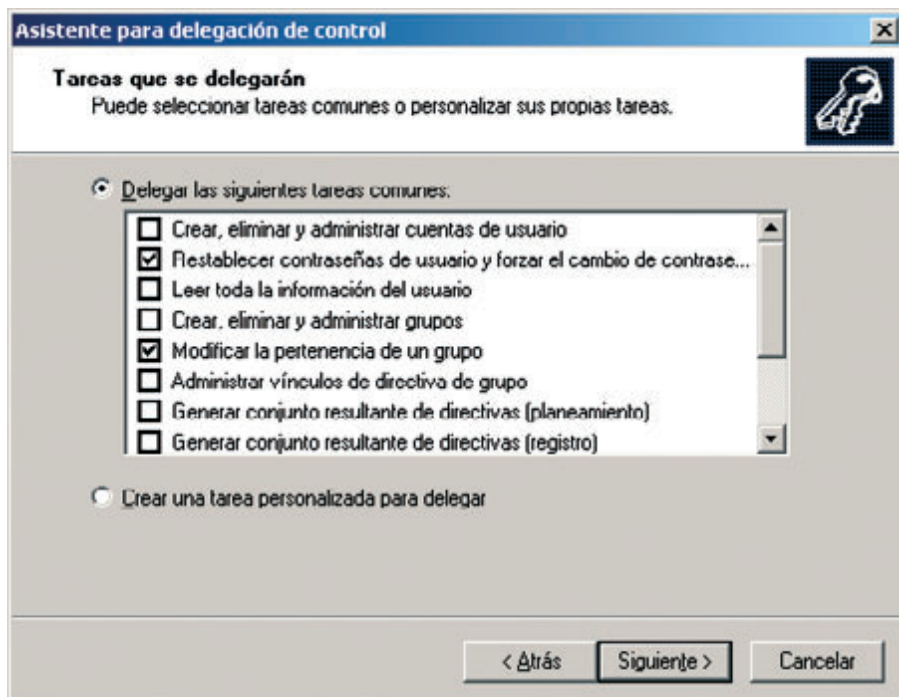
Usted puede utilizar este concepto para plasmar, por ejemplo, la organización en departamentos de su empresa: Marketing, Finanzas, Informática, etc. Y lo que es mejor, puede utilizar el concepto de unidad organizativa para **delegar** la administración de dichos departamentos.

Para ello, haga clic con el botón derecho del ratón en una unidad organizativa y elija **Delegar control**. Se iniciará un asistente.



Por ejemplo, imagínese que decide delegar funciones del Administrador de red en un usuario del departamento de Finanzas, de forma que no sea necesaria su intervención para ciertas tareas administrativas. Esto lo podrá hacer delegando esa responsabilidad en una unidad organizativa.

En el asistente se le solicita que indique el usuario o usuarios sobre los que delegará y qué tareas podrán realizar.



Si la red es lo suficientemente grande, delegar responsabilidades de administración puede mejorar significativamente el servicio que se dé a los usuarios, siempre que las personas en las que se delega realicen correctamente su trabajo.

En este capítulo hemos estudiado cómo se estructura el directorio:

- Se utiliza el concepto de **dominio** como límite de todo aquello que nos interesa de la red. Recuerde que este concepto está ligado al uso del sistema de nombres DNS.
- Se utiliza el concepto de **unidad organizativa** (UO) para dividir la información referente a un dominio y como estructura para delegar responsabilidades de administración.

Todo esto, con el objetivo de reflejar la estructura de su empresa en Active Directory.

4. MODOS DE DOMINIO Y DE BOSQUE

En Windows 2003 obtenemos algunas novedades en Active Directory que no están disponibles en versiones anteriores.

El concepto de dominio apareció junto al sistema operativo Windows NT Server. Sin embargo, la incorporación de **Active Directory** en Windows 2000 Server aportó muchas características nuevas.

Ahora con Windows 2003 obtenemos otras novedades en Active Directory no disponibles en las versiones anteriores. Sin embargo, en muchos casos nos vamos a encontrar con la necesidad de mantener equipos con Windows NT o Windows 2000.

Por lo tanto, nos podemos encontrar en tres situaciones:

- Que todos los controladores de dominio ejecuten Windows 2003 --> **Modo Windows 2003**.
- Que convivan controladores de dominio con Windows 2003 y Windows 2000 --> **Modo Windows 2000 nativo**.
- Que convivan controladores de dominio con Windows 2003, Windows 2000 y Windows NT. ---> **Modo Windows 2000 mixto**.

Fíjese que sólo nos referimos a los equipos que actúan como controladores de dominio. Esto no afecta en nada a los restantes equipos de la red: servidores miembro o clientes.

Dependiendo de la situación de nuestra red, dispondremos de unas u otras opciones en Active Directory. Esto se conoce como el **nivel funcional del dominio**.

No se puede volver a un nivel funcional inferior de dominio o bosque sin volver a crear el dominio o bosque.

Podemos comprobar el modo en el que está funcionando el dominio a través de sus propiedades, en la herramienta **Usuarios y equipos de Active Directory**. Por otra parte, en su mismo menú contextual aparece el comando **Elevar el nivel funcional del dominio**, que sirve para cambiar el modo actual.

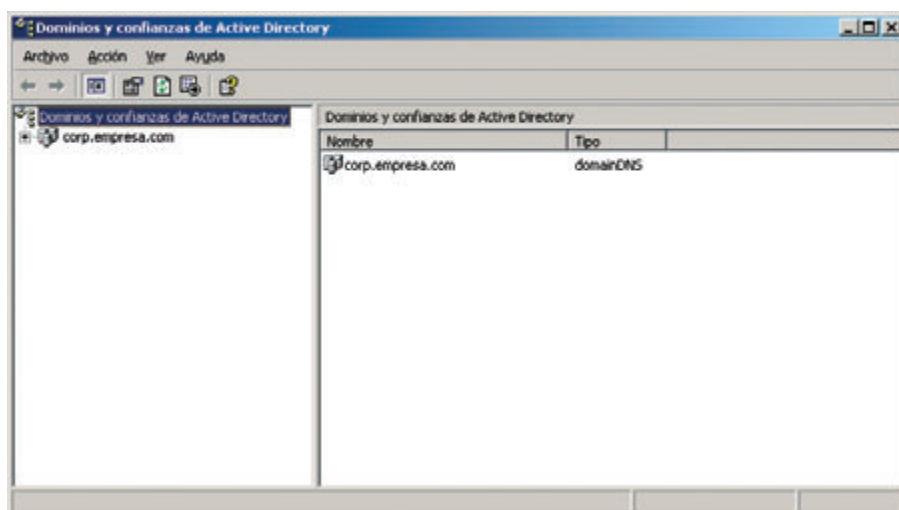
Esta operación es muy importante, ya que al elevar el dominio al nivel funcional Windows Server 2003, dispondremos de todas las características de Active Directory, pero también estaremos obligados a configurar todos los controladores de dominio con este sistema operativo.

En el apéndice de este manual tiene más información sobre la estructura de bosques.

Recuerde que todos los controladores tienen la misma copia del directorio, por lo que debe propagarse cualquier cambio que se realice a todos los restantes. Esto, lógicamente, incluye el cambio a un nivel funcional superior del dominio.

Del mismo modo podemos elevar el nivel funcional del bosque. Es la misma idea, pero respecto de los dominios del bosque.

Si todos los dominios del bosque están funcionando en modo Windows Server 2003, lo lógico es que elevemos el bosque a dicho nivel funcional. Para ello, utilizaremos la herramienta administrativa **Dominios y confianzas de Active Directory**.



Para elevar el nivel del bosque, haga clic con el botón derecho del ratón en Dominios y confianzas de Active Directory y elija **Elevar nivel funcional del bosque**.

Este capítulo sólo pretende explicarle cómo cambiar el nivel funcional de un dominio o de todo un bosque. Las características adicionales que obtenemos al elevarlo a uno u otro nivel puede encontrarlas en la ayuda de Windows 2003.

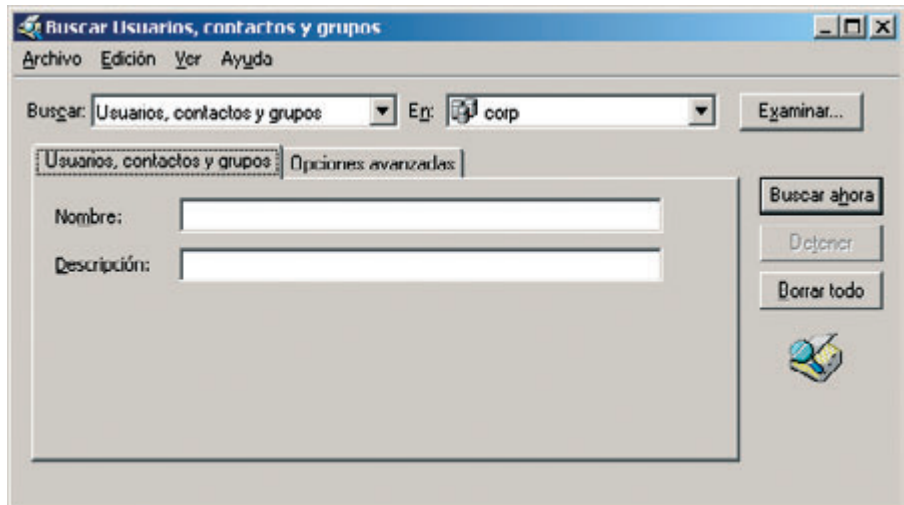
En muchos casos son características que difícilmente va a utilizar, por lo que si necesita mantener equipos con sistemas operativos anteriores a Windows 2003 para que actúen como controladores de dominio, no necesita elevar el nivel funcional de los dominios o de los bosques.

Por ejemplo, sólo se puede renombrar un dominio si el bosque está funcionando en el nivel superior, es decir, Windows Server 2003.

5. EXPLORAR EL DIRECTORIO

Windows 2003 proporciona la información del directorio de dos formas: realizando búsquedas o a través de la exploración, como si fuera una parte más del sistema de ficheros.

Desde la herramienta **Usuarios y equipos de Active Directory**, podremos realizar búsquedas a través del comando **Buscar** del menú contextual del dominio o de algún otro objeto contenedor, como una unidad organizativa.



Tenga en cuenta que para ello no es necesario disponer de privilegios administrativos. Cualquier usuario que pueda ejecutar esta herramienta administrativa (desde el controlador o desde otro equipo), podrá realizar búsquedas, otra cosa es que pueda modificar la información almacenada en el directorio.

Desde Windows 2003 podremos realizar búsquedas en el directorio si accedemos a la opción **Buscar** del menú Inicio y elegimos **Otras opciones de búsqueda** en la parte izquierda del cuadro de diálogo. Una de esas opciones es buscar impresoras, equipos o personas.

En esta opción se puede decir que se busque en el directorio.



La información que se proporciona al explorar el directorio es menor que la que puede encontrar a través de la herramienta **Usuarios y equipos de Active Directory**.

Es normal: una cosa es explorar el directorio con el objetivo de obtener información descriptiva y otra es utilizar una herramienta para realizar tareas administrativas.

En **Windows XP** puede acceder a **Mis sitios de red** y activar el hipervínculo **Buscar en Active Directory**. Este hipervínculo sólo aparecerá si el equipo pertenece a un dominio.

Para el usuario, el directorio es como un centro de información y de recursos donde puede acudir cuando necesite alguna cosa.

Para el administrador, es la herramienta que le permite organizar y gestionar los recursos de la red.

Esta lección le ha mostrado una visión general del directorio y del servicio Active Directory. A partir de ahora veremos cómo crear los objetos y cómo administrarlos.