INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES 15 &SEGURIDAD

ADMINISTRACIÓN DE WINDOWS SERVER

En esta clase presentaremos las características y ventajas del sistema para servidores ofrecido por Microsoft. Analizaremos las opciones de Active Directory y puntualizaremos cómo administrar las directivas de grupo en forma avanzada.

- WINDOWS SERVER
- DERECHOS Y RESTRICCIONES
- EDICIONES DE WINDOWS SERVER
- COMUNICACIÓN LINUX - WINDOWS
- TIPOS DE MALWARE

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Características y ediciones de Windows Server, así como también la forma correcta de realizar su administración, asignar restricciones y administrar las Directivas de Grupo.

En la clase anterior nos dedicamos a repasar las características del hardware de un servidor de red. Conocimos cada uno de los componentes que lo integran y consideramos sus particularidades. Vimos qué es la tecnología RAID y presentamos el procedimiento detallado para montar una matriz de este tipo. Analizamos el BIOS Setup de un servidor y detallamos las ventajas que nos ofrece la tecnología UEFI. Finalmente dimos consejos de seguridad para los servidores de red y describimos las tecnologías del hardware management. En esta clase conoceremos las principales características de las diversas ediciones de Windows Server y revisaremos los conceptos asociados con la asignación de derechos y las restricciones. Veremos qué es Active Directory y aprenderemos a administrar las Directivas de Grupo en forma avanzada. También explicaremos cómo comunicar servidores Linux con clientes Windows y viceversa, y, para terminar, listaremos los distintos tipos de malware existentes.

15

8
Active Directory

14
Distintas ediciones de Windows Server

20
Administración de Directivas de Grupo

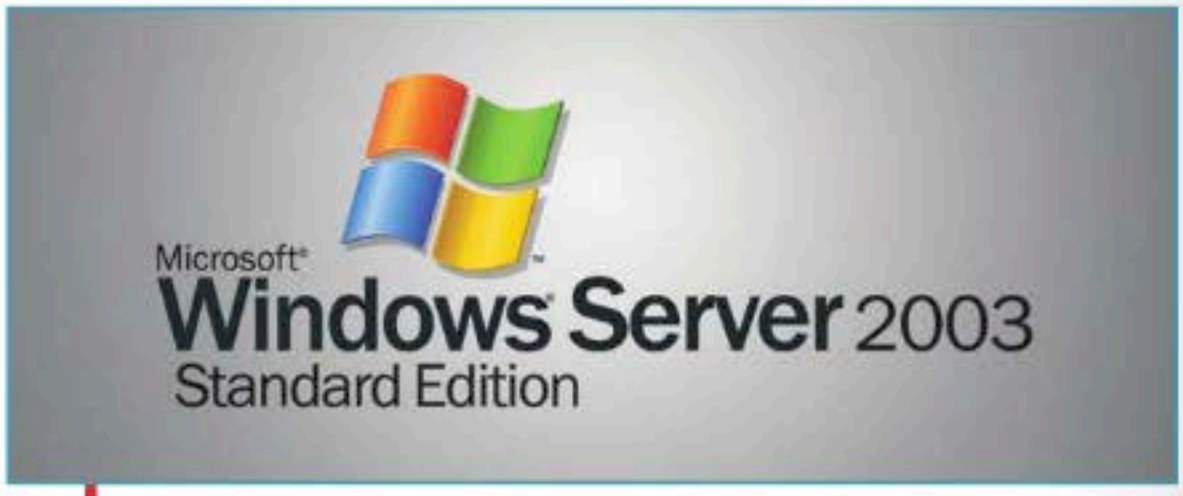
22
Tipos de malware

Windows Server: características

Microsoft ofrece, entre sus sistemas operativos, aquellos dedicados a la gestión y administración de servidores bajo un amigable entorno gráfico.

Dentro del amplio abanico de sistemas operativos que podemos instalar en nuestros equipos, encontramos que existen diferentes versiones y características asociadas a ellos. Entre las distintas empresas desarrolladoras, hay familias de sistemas operativos dedicados a diversas tareas, principalmente hogareñas y empresariales.

Casi el 90% de los equipos hogareños de escritorio cuentan con sistemas operativos de la empresa Microsoft, de la familia Windows. A lo largo de los años, estos fueron modificados según las necesidades de los diversos clientes, y hoy, una de las ramas principales son los sistemas dedicados a servidores (empresas y redes informáticas grandes), conocidos como Windows Server.



Windows Server presenta diversas alternativas para sus versiones de sistemas operativos adaptados a cada necesidad.

Windows Server

Se puede considerar que las diversas versiones de Windows Server corresponden a los sistemas operativos comerciales destinados al consumidor promedio, pero centrados en aplicaciones y rendimiento para empresas y organizaciones. La primera versión de ellos destinada a las organizaciones fue Windows NT (que, a partir de entonces, fue conocido como Windows NT 3.5, 3.51, 4.0), que se correspondía con Windows 95, y así sucesivamente para Windows 2000 (Windows NT 2000), Windows XP (se integraron muchos programas, procesos y aplicaciones, y se conoció el nuevo Windows Server 2003, que salió a la venta casi dos años después que XP), Windows Vista (con su versión dedicada a servidores Windows Server 2008), Windows 7 (se actualizó la versión Windows Server 2008 R2), hasta la última versión disponible de Windows 8 con su administrador de servidores Windows Server 2012. Los Windows Server están basados en las tecnología NT y, a diferencia de sus homólogos para computadoras de escritorio, están optimizados para labores empresariales porque deshabilitan funciones con el fin de mejorar el rendimiento (la interfaz gráfica, por ejemplo, se encuentra desactivada para lograr una disminución en el uso de memoria).

Características

Entre las características principales que encontramos a partir del lanzamiento de la familia de productos Windows Server por parte de la empresa Microsoft, se incluyen las que mencionaremos en detalle, a continuación:

- Establece cuentas de usuario gestionadas, organizadas y también personalizadas. Cada usuario puede ser identificado, y se le hace corresponder un perfil con permisos y delegaciones. De esta forma, los datos, redes, servidores y cuentas de usuario quedan protegidos.
- Se establece el sistema de archivos NTFS, que permite establecer cuotas, ampliar la capacidad de almacenamiento y cifrar información. Se habilita la compresión de archivos y se permite el montaje de unidades de almacenamiento sobre sistemas de archivos de otros dispositivos.
- Gestiona el almacenamiento de modo que los archivos menos utilizados son desplazados a unidades de almacenamiento más lentas o menos frecuentadas y, de esta manera, el disco las busca solo cuando las precisa.
- Se implementa Windows Driver Model, que según los dispositivos más utilizados,

estandariza determinadas características, así los fabricantes de hardware solo especifican algunas especiales en sus dispositivos.

- Se gestiona la seguridad de manera centralizada localmente gracias al uso de Active Directory, que relaciona distintos componentes de la red tales como usuarios, grupos de usuarios y políticas de seguridad, entre otros. Utiliza protocolos tales como DNS, DHC y LDAP.
- Emplea autenticación Kerberos basada en la identificación de los terminales cliente-servidor, donde ambos se identifican mutuamente y, luego, la transferencia de información es encriptada y genera conexiones seguras.

Los servidores que podemos manejar gracias a Windows 2003 son:

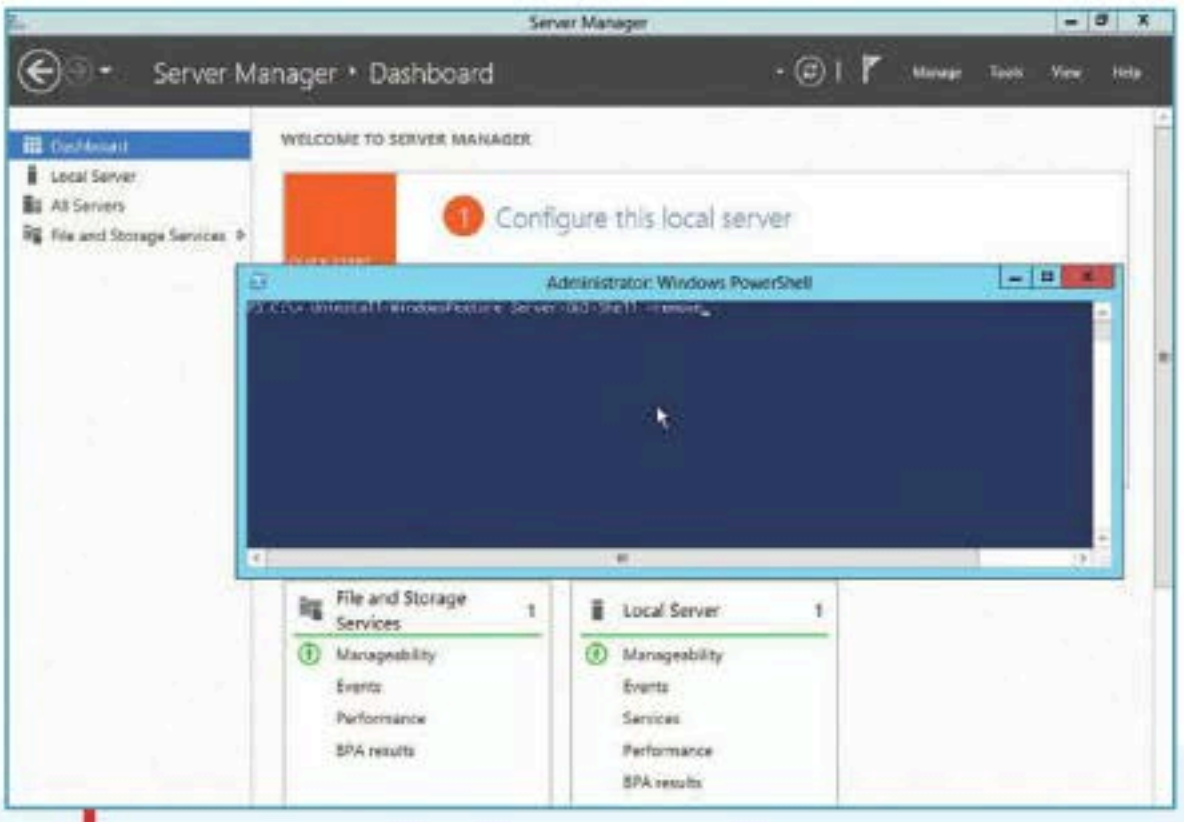
- Servidor de archivos
- Servidor de impresiones e impresoras
- Servidor de aplicaciones de red
- Servidor de correo (SMTP/POP)
- Servidor de terminal
- Servidor de redes privadas virtuales (VPN)
- Controlador de dominios
- Servidor DNS y servidor DHCP
- Servidor WINS
- Servidor RIS (Remote Installation Services, servicios de instalación remota)

Características adicionales

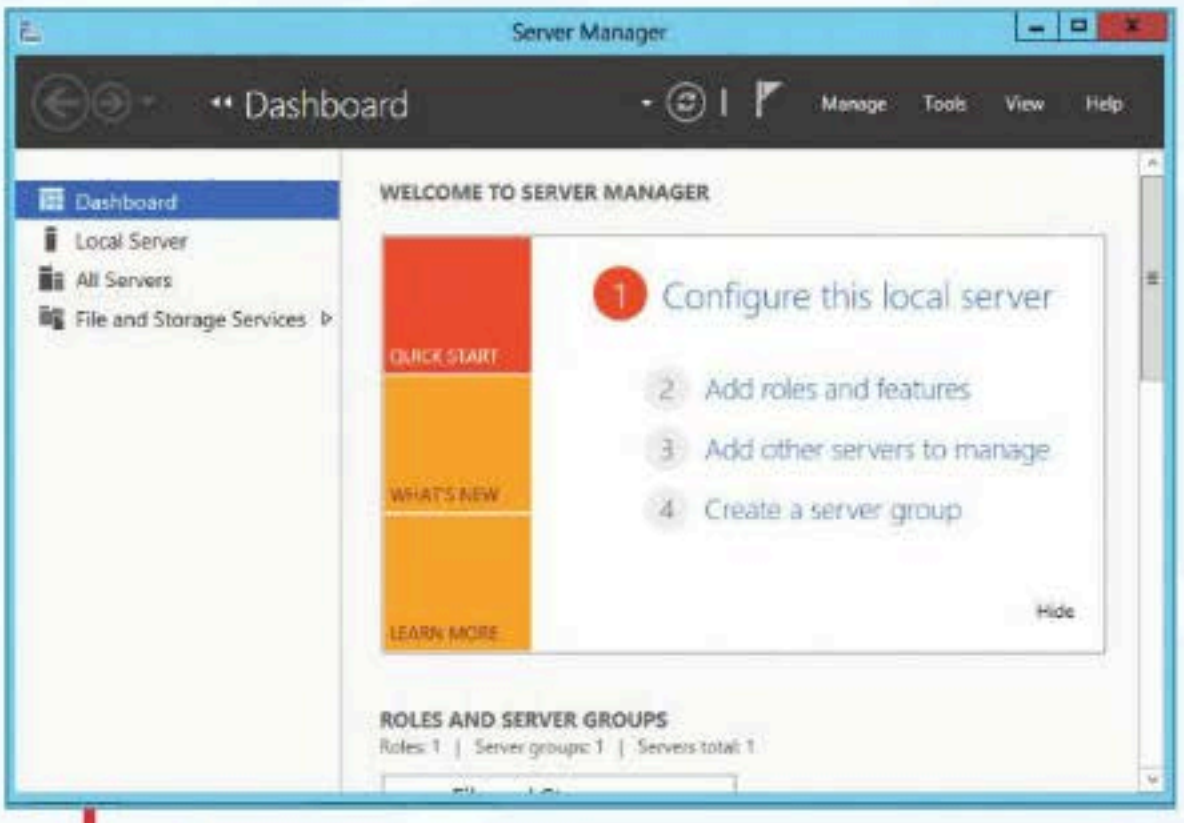
Algunas de las características adicionales se dividen según la versión del sistema operativo. Comercialmente salieron las versiones Web Edition (destinada a servicios y hospedaje web), Standard Edition (cumple con la mayoría de los requerimientos de servicios para servidores), Enterprise Edition (destinada a empresas grandes con numerosos terminales), Data Center Edition (para servidores con grandes flujos de datos) y Small Business Edition (creada para redes con no más de 25 estaciones de trabajo). Al tratarse de sistemas dedicados a funcionar como servidores o como clientes, en los que la seguridad es primordial y las conexiones deben autenticarse permanentemente, las vulnerabilidades tienen que reducirse, indefectiblemente, al mínimo nivel que sea posible.

Integración

En líneas generales, la implementación de Windows Server permite una fácil integración con otros sistemas operativos. Es simple de implementar, administrar y usar, genera una infraestructura de datos segura, con información confiable y de fácil acceso; y ofrece fiabilidad, disponibilidad, escalabilidad y rendimiento. Entre las herramientas de administración disponibles está presente la consola por líneas de comando, cuyo fin es gestionar las cuentas más ágilmente que usando la interfaz gráfica. El soporte del sistema está respaldado por el gigante informático: Microsoft. ■



Dentro de Windows Server, podemos utilizar la consola de comandos para realizar numerosas actividades importantes.



Windows Server 2012 presenta muchas mejoras con respecto al rendimiento, la gestión y la apariencia gráfica.

Permisos en Windows Server

Con Active Directory funcionando sobre Windows Server, tenemos las herramientas que necesitamos para implementar una solución segura y estable para el control de nuestra red.

Una vez implementado el dominio Active Directory, ¿cómo configuramos nuestro dominio de manera que cada usuario posea los permisos para realizar solo las tareas que necesita y se eliminen los riesgos de efectuar acciones no deseadas? Antes de adentrarnos en las opciones de seguridad del dominio Active Directory, es necesario conocer, desde el punto de vista de la seguridad, los distintos tipos de objetos que utilizaremos.

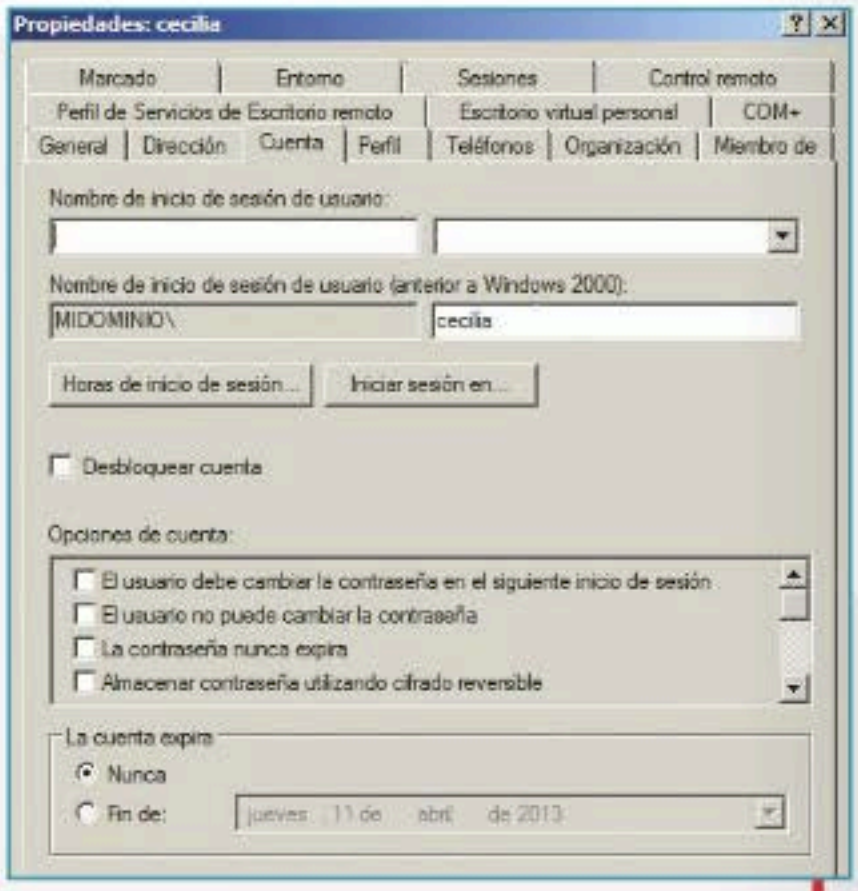
Usuarios

Este tipo de objetos representa a una persona que emplea algún servicio en los equipos del dominio. Siempre tenemos que tratar de que cada persona que ingrese en alguno de ellos tenga su propio usuario, ya que esto facilita la asignación de políticas personalizadas y el seguimiento de las acciones de cada uno. Los usuarios de un dominio Active Directory se administran mediante el complemento Usuarios y Equipos de Active Directory, desde donde podemos realizar todas las tareas relacionadas con los objetos de tipo usuario, como crear, modificar y borrar cuentas, así como también cambiar las contraseñas en caso de que alguna persona olvide sus datos de ingreso.

DEBEMOS TRATAR DE QUE CADA PERSONA TENGA UNA CUENTA DE USUARIO DISTINTA; MÁS IMPORTANTE AÚN ES SI SE TRATA DE LOS ADMINISTRADORES.

Grupos

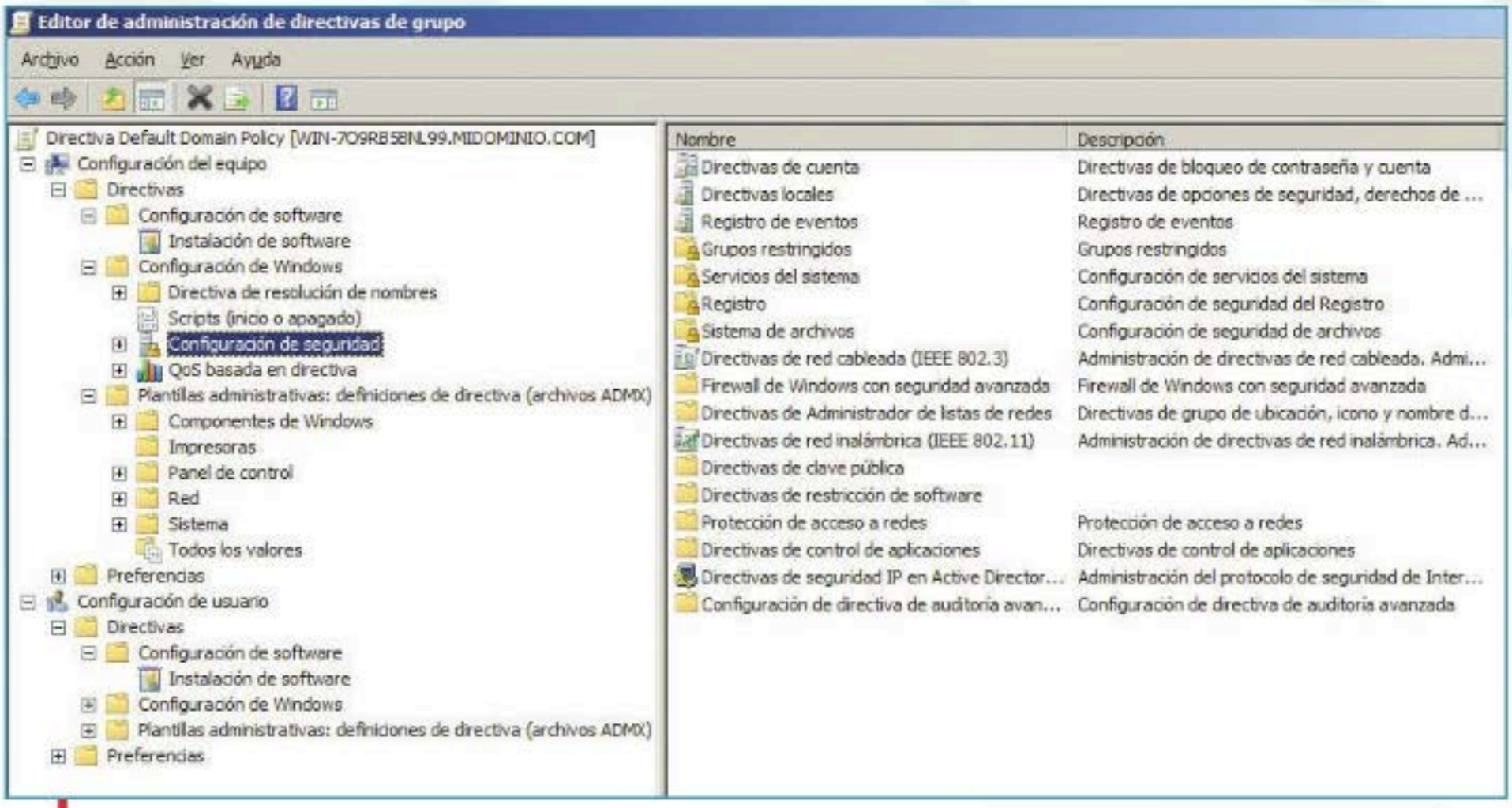
Si bien tenemos que asignar una cuenta de usuario a cada persona para poder establecer políticas personalizadas, esto no quiere decir que las opciones del dominio vayan a asignarse a cada uno de manera individual. Los grupos permiten asignar políticas o permisos a un conjunto de usuarios; de este modo, evitamos problemas en muchas situaciones. Un ejemplo sería cuando un usuario cambia de sector en una empresa; si tenemos los permisos y políticas definidos por usuario, deberemos modificar, en la cuenta de la persona, los permisos y políticas para que concuerden con su nuevo rol. Si organizamos nuestra política de seguridad utilizando grupos, bastará con cambiar el usuario al grupo que representa el sector al que fue asignado. Los grupos se administran desde el complemento Usuarios y Equipos de Active Directory, donde podremos cambiar los parámetros de los objetos del tipo grupo, como nombre, miembros y subgrupos.



En el dominio Active Directory hay parámetros para establecer en los objetos de tipo Usuario.

Equipos

Para que una PC o servidor forme parte de nuestro dominio Active Directory, debe existir un canal seguro mediante el cual



Las políticas de grupo permiten gestionar las opciones de configuración de los equipos que forman parte del dominio.

se realicen las tareas relacionadas con la gestión centralizada de la seguridad, como la autenticación de usuarios o la autorización de acceso a un recurso que está compartido en la red.

Con el fin de establecer el mencionado canal seguro, tenemos que "unir" los equipos al dominio. Esta acción se realiza mediante un usuario del dominio Active Directory que posea los privilegios apropiados, y tiene como finalidad delegar la gestión de la seguridad en el dominio. Una vez unidos los equipos al dominio, se crea una cuenta especial que identifica a cada PC o servidor; esta cuenta es un objeto del tipo Equipo. Las cuentas de equipo se administran del mismo modo que las de usuario, desde el complemento Usuarios y Equipos de Active Directory.

Unidades organizativas

Las unidades organizativas son contenedores que nos permiten organizar el resto de los objetos (por ejemplo, usuarios, grupos y equipos) y, a la vez, vincularlos a las políticas de grupo, a fin de modificar las opciones de configuración que creamos necesarias, incluidas las referidas a la seguridad. Al igual que los usuarios, grupos y equipos, las unidades organizativas se administran mediante el uso del complemento Usuarios y Equipos, presente en Active Directory.

Políticas de grupo

Existe una gran cantidad de opciones relacionadas con los usuarios y equipos de nuestro dominio Active Directory; en este caso, nos interesan las que se refieren a la seguridad. Las opciones de los usuarios y equipos se gestionan mediante la herramienta Políticas de Grupo. A través del uso de políticas de grupo, administraremos de forma centralizada, eficiente y escalable los parámetros de los miembros de nuestro dominio Active Directory.

Clasificación

El número de opciones de configuración que podemos administrar mediante

Sitios de interés

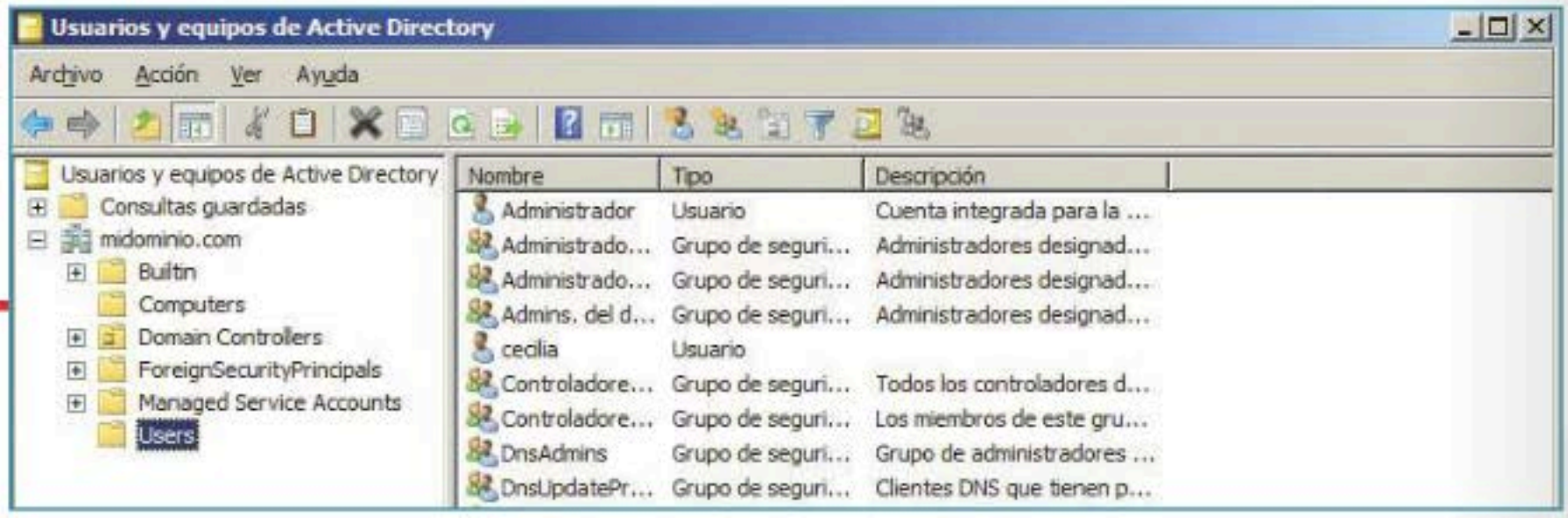
Las políticas de grupo abarcan una infinidad de parámetros de seguridad y de aplicación general, a la vez que van evolucionando de la mano de los sistemas operativos Windows. Resulta indispensable tener una lista de sitios de referencia. Uno de los más importantes es, sin lugar a dudas, el sitio de Microsoft TechNet (http://technet.microsoft.com**) y otro es el de** GroupPolicy Central **(www.grouppolicy.biz).**

políticas de grupo es enorme. A medida que evoluciona la plataforma Windows, se incorporan otras funcionalidades que aprovechan las características de las nuevas versiones de Windows, tanto en las cliente (Windows XP, Windows Vista, Windows 7 y Windows 8) como en las servidor (Windows Server 2000, 2003, 2008 y 2012). Como vemos a continuación, existen 18 categorías de políticas de grupo:

- **Plantillas administrativas:** son directivas que tienen el objetivo de configurar el Registro de Windows, donde se almacenan las opciones de funcionamiento de una gran cantidad de aplicaciones, servicios y componentes.
- **Opciones de seguridad:** abarcan las destinadas a establecer los parámetros de seguridad de los equipos y usuarios miembros del dominio; por ejemplo, mediante una política de seguridad de esta categoría, podemos establecer el máximo número de intentos que un usuario puede hacer para ingresar incorrectamente la contraseña, luego de los cuales la cuenta se bloquea.
- **Configuración de red cableada:** abarca las opciones que se relacionan con las redes cableadas, por ejemplo, los parámetros que están vinculados a la protección de acceso por red (NAP).
- **Configuración de red inalámbrica:** en esta categoría se encuentran las opciones referidas a las redes inalámbricas, por ejemplo, los tipos de encriptación soportados (WPA, WPA2 etc.).
- **Scripts:** mediante políticas de grupo, podemos establecer pequeños programas para que se ejecuten en algún instante específico, por ejemplo, cuando un usuario ingrese a un equipo mediante su usuario y contraseña.
- **Políticas de grupo de instalación de software:** permiten la instalación de software en las PCs o servidores desde los controladores de dominio.
- **Redirección de carpetas:** es posible redireccionar carpetas de los perfiles de los usuarios a los fines de cambiar su ubicación original. Una finalidad de este tipo de políticas es centralizar las carpetas `Mis documentos` de los usuarios en un servidor central.
- **Cuotas de disco:** existen políticas que regulan el uso en las carpetas que consideremos críticas; de este modo, controlamos el uso del espacio en disco.
- **Opciones del sistema de archivos encriptado:** permiten establecer los parámetros en caso de que necesitemos encriptar alguna partición en los servidores o PCs de nuestro dominio.
- **Mantenimiento de Internet Explorer:** dado que muchas de las amenazas de seguridad informática provienen de Internet, conviene centralizar las opciones de configuración de Internet Explorer.
- **Políticas de restricción de software:** por medio de estas políticas, controlamos los paquetes que pueden ejecutarse en los equipos de nuestro dominio.
- **Calidad de servicio basado en políticas:** se encarga de configurar la prioridad de los servicios a nivel de red.
- **Políticas IPSec:** permiten establecer parámetros relacionados con la red segura por Internet.
- **Búsqueda de Windows:** cambian opciones vinculadas a la búsqueda dentro de las PCs y servidores de nuestro dominio.
- **Distribución de conexiones a impresoras:** distribuye a los clientes del dominio las conexiones a las impresoras; estas políticas son especialmente útiles en redes donde existen muchos dispositivos de impresión.
- **Archivos sin conexión:** especifican los parámetros para la sincronización de archivos para los clientes que en algún momento se desconectan del dominio para funcionar en redes distintas. Un ejemplo de la aplicación de estas políticas son los equipos portátiles.

PARA FORMAR PARTE DEL DOMINIO, DEBE EXISTIR UN CANAL SEGURO ENTRE LOS CONTROLADORES Y LOS MIEMBROS.

- **Preferencias - Extensiones de Políticas de grupo:** a partir de Windows 7 y Windows Server 2003, se incluye una serie de preferencias que nos permiten afinar al detalle la configuración de los equipos que son miembros de nuestro dominio.



Mediante el administrador de usuarios y equipos de Active Directory, se gestionan los grupos, las cuentas de Usuario y las de Equipo.

Cada equipo que está formando parte del dominio Active Directory se encuentra representado por una cuenta de Equipo.

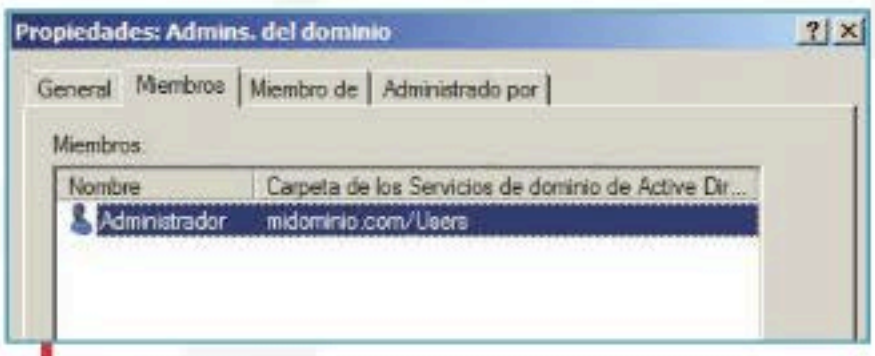
- **Aceleradores de Internet Explorer**: estas políticas permiten establecer los parámetros de los aceleradores de Internet Explorer, una característica introducida a partir de Windows 7.

Descripción

Cada política de grupo tiene dos nodos o partes: la parte relacionada al usuario y la parte relacionada al equipo. Ambas abarcan las opciones que afectan a los objetos de tipo Usuario y de tipo Equipo, respectivamente, los cuales deben estar contenidos en la Unidad Organizativa a la que se vincula la política de grupo. Las políticas de grupo pueden establecerse a nivel local (en cada equipo), a nivel de sitio, a nivel de dominio o a nivel de unidad organizativa.

Administración de políticas de grupo

Utilizaremos la herramienta `gpedit.msc` para editar las políticas de grupo a nivel local en cada equipo, mientras que, para trabajar con las políticas de grupo a nivel de dominio, recurriremos a la herramienta **Consola de Administración de Políticas de Grupo** (**GPMC**). Mediante la Consola GPMC podremos crear, modificar y borrar políticas de grupo, así como también vincularlas a las unidades organizativas, sitios y dominios.



Los objetos del tipo Grupo nos permiten organizar y administrar el dominio en forma eficiente.

SMB

En el caso de una implementación del sistema operativo SMB (Small Business Server), la asignación de derechos y restricciones puede realizarse gracias a la consola de administración incorporada en el sistema operativo. Esta consola de administración funciona como un práctico panel de control en el cual se nos presentan en forma gráfica todas las opciones que necesitamos para administrar un servidor para el hogar o la pequeña empresa.

Aplicación

Según el nivel en el que establecemos las políticas de grupo, será la prioridad de ejecución. Como es lógico, las políticas que definamos a nivel local son las que tienen menos prioridad de ejecución, ya que la finalidad del dominio es que los equipos deleguen la gestión de la seguridad en los controladores de dominio. El orden en el que se aplicarán las políticas de grupo es el siguiente: primero se aplican las vinculadas a nivel de sitio, luego se cargan las que están vinculadas al dominio, después las relacionadas a la unidad organizativa a la que pertenezca el usuario o el equipo y, finalmente, las políticas de grupo definidas de manera local. Si existen conflictos entre dos o más políticas de grupo, tendrán precedencia aquellas vinculadas al nivel de mayor prioridad. Por ejemplo, ante un conflicto en una opción definida en una política de grupo vinculada a nivel de dominio y otra vinculada a nivel de unidad organizativa, tendrá precedencia la opción configurada en la política de grupo vinculada a nivel de dominio.

Herencia

Las políticas de grupo se heredan desde un contenedor hacia los elementos que contiene. Por ejemplo, si definimos una OU con nombre Sistemas y, dentro de ella, definimos otra OU llamada Desarrollo, las políticas de grupo vinculadas a la OU Sistemas serán heredadas por la OU Desarrollo, ya que la primera contiene a la segunda. La herencia puede bloquearse mediante los parámetros de configuración de las políticas de grupo.

Recomendaciones de seguridad

Algunos conceptos que debemos tener en cuenta, y que tienen un impacto positivo importante en el nivel de seguridad de nuestro dominio Active Directory, son los siguientes:

- **Evitar cuentas genéricas**: debemos tratar de que cada persona tenga una cuenta de usuario distinta de los demás.
- **Revisar los registros que genera Active Directory**: es importante que revisemos periódicamente los mensajes que genera Active Directory en el registro de eventos y también los que generan reportes automáticos. Una alternativa para este fin es la herramienta de Microsoft llamada logparser. ■

Active Directory

Es la solución comercial de Microsoft para un servicio de directorio dentro de una red distribuida de computadoras. Aquí conoceremos sus características y los detalles de su funcionamiento.

Active Directory es el nombre comercial que utiliza la empresa de desarrollo Microsoft para referirse a su solución informática o implementación propia de un servicio de directorio para una red distribuida de computadoras. Un servicio de directorio es un componente importante dentro de una red. Los usuarios y administradores, con frecuencia, no saben el nombre exacto de los objetos en los que están interesados. Quizá conozcan uno o más atributos de los objetos y, de esta manera, puedan consultar al servicio de directorio para obtener una lista de aquellos que concuerden con los atributos conocidos. Un servicio de directorio permite que un usuario encuentre cualquier objeto sabiendo solo uno de sus atributos, lo que ahorra tiempo en tareas cotidianas, como acceder a los recursos que se encuentran compartidos en la red de computadoras.

Protocolos y estructura

Este producto utiliza un conjunto de protocolos diferentes, entre los que podemos resaltar **LDAP** (*Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios), **DNS** (*Domain Name System*, sistema de nombres de dominio), **DHCP** (*Dynamic Host Configuration Protocol*, protocolo de configuración dinámica de host; entendiendo como host al nodo huésped o computadora local que consume el servicio) y **Kerberos** (protocolo de autenticación de nodos de una red). Suele referirse a Active Directory con el diminutivo **AD**. Posee una estructura jerárquica que nos permite mantener un conjunto de objetos relacionados con componentes de una red. Cuando mencionamos componentes, queremos decir usuarios, grupos, permisos, y asignación de recursos y políticas de acceso. Como administradores, con Active Directory podemos definir políticas a nivel de empresa, ejecutar programas en una serie de computadoras e implementar actualizaciones para toda una organización. AD posee una base de datos centralizada en donde se almacenan, desde directorios con cientos de objetos, hasta directorios con millones de ellos.

Los servidores de Active Directory pueden procesar los inicios de sesión de los usuarios que se conectan.

LOS OBJETOS DE ACTIVE DIRECTORY SE PUEDEN CLASIFICAR EN TRES CATEGORÍAS: RECURSOS, SERVICIOS Y USUARIOS.

Arquitectura

Estructuralmente hablando, **AD** está conformado por un conjunto de dominios y subdominios (en organizaciones pequeñas, por lo general, los objetos se aglutinan en un único dominio), que se definen a través del protocolo **DNS**. Es por eso que para utilizar Active Directory necesitamos uno o más servidores DNS en línea dentro de la red. Active Directory se encuentra basado en un conjunto de estándares denominados X.500.

Los dominios y subdominios están dispuestos en una estructura jerárquica en forma de árbol. Si un usuario pertenece a un dominio particular, este será reconocido por los subdominios que descienden de él, sin necesidad de definirlo para cada uno de ellos. Además, distintos árboles (no comparten el nombre de zona DNS) pueden agruparse para conformar un bosque y establecer una relación de confianza (trust) entre ellos, de manera tal que los usuarios y los recursos de los distintos árboles sean visibles entre sí. AD es el que mantiene cada estructura de árbol en forma individual.

Active Directory, como mencionamos con anterioridad, utiliza un sistema común de resolución de nombres (**DNS**) y un catálogo común que contiene una réplica completa de todos

los objetos del directorio del dominio en que se aloja, además de una réplica parcial de todos los objetos del directorio de cada dominio del bosque. Podemos clasificar dichos objetos en tres grandes categorías: recursos (por ejemplo, impresoras), servicios (como correo electrónico) y usuarios (por ejemplo, cuentas y grupos). Gracias a que los objetos se encuentran catalogados, AD puede brindar información sobre ellos, organizarlos, controlar su acceso y establecer la seguridad. Los objetos se encuentran dentro de los directorios que poseen un dominio o subdominio.
Cada objeto es una representación abstracta de una entidad única e indivisible (que puede ser un usuario, un nodo de la red, un recurso como una impresora, una aplicación o una fuente compartida de datos). Esta representación contiene todos los atributos de la entidad. Los objetos pueden contener otros objetos. Cada uno de los atributos, que son la estructura interna básica de un objeto, se define por un objeto esquema o metadato, que también define la clase de objetos que se pueden almacenar en un directorio. Cada atributo se puede utilizar en diferentes esquemas de clase de objeto. Cada objeto esquema se utiliza para definir los atributos de un conjunto de objetos y, por lo tanto, se integra con ellos.
Esto quiere decir que modificar o eliminar un objeto esquema puede volverse una acción tediosa y compleja, ya que la modificación o eliminación se propagará a través de todos los objetos con los que se encuentre efectivamente integrado.

Funcionamiento

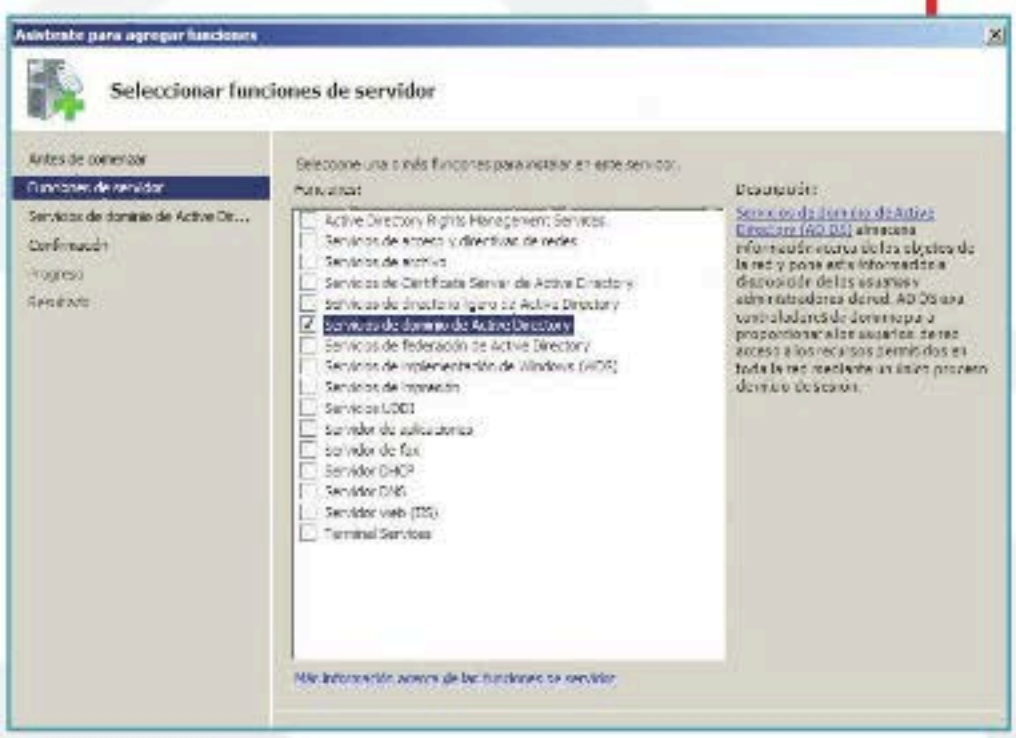
Active Directory posee una base de datos centralizada que almacena la información relacionada a un dominio de autenticación.
La sincronización entre los distintos servidores de autenticación del dominio es un punto fuerte de esta implementación.
Cada objeto posee atributos que lo identifican de forma unívoca (por ejemplo, un usuario puede tener los campos **<<Nombre>>**, **<<E-mail>>**, etc.; y una impresora puede incluir los campos **<<Nombre>>**, **<<Fabricante>>**, **<<Modelo>>**, **<<Usuarios Autorizados>>**, etc.). Toda esta información se encuentra centralizada y se replica de manera automática entre todos los servidores que controlan el acceso al dominio.
De esta manera, es factible crear recursos (como carpetas compartidas, impresoras de red, etc.) y conceder autorización de acceso a ellos a usuarios, con la ventaja de que todos estos objetos se encuentran memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito. Para decirlo en otras palabras, Active Directory es una implementación de servicio de directorio centralizado en una red distribuida, que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).
Las relaciones de confianza entre dominios (*trust* en inglés) permiten que usuarios de un dominio particular accedan y consuman recursos presentes en otro dominio diferente del primero. Estas relaciones son creadas en forma automática cuando se crean nuevos dominios. Los límites de las relaciones de confianza no son marcados por el dominio sino por el bosque al cual pertenecen los dominios implicados. Existen diferentes tipos de relaciones de confianza:

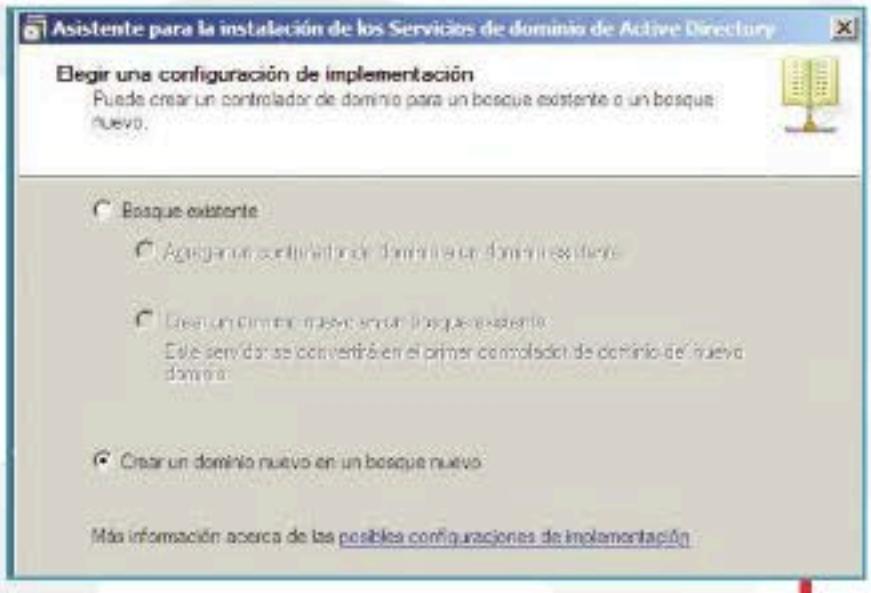
- **Confianza transitiva:** estas relaciones son automáticas y de dos sentidos (ida y vuelta) entre dominios que se encuentran gestionados por Active Directory.
- **Confianza explícita:** son aquellas relaciones que se establecen de forma manual para especificar una ruta de acceso con propósitos de autenticación. Este tipo de relación puede ser de uno o dos sentidos (de ida y/o de vuelta), dependiendo de la aplicación. Se utiliza con frecuencia para acceder sin dificultades a dominios compuestos por computadoras con Windows NT 4.0.

Kerberos

Kerberos es un protocolo de autenticación que se utiliza en redes de computadoras. Fue creado por Gerard Kominek y permite que dos computadoras presentes en una red insegura demuestren su identidad de modo seguro. En sus comienzos utilizaba una arquitectura de cliente-servidor que permite a ambos verificar la identidad del otro. Se basa en criptografía de clave simétrica y requiere de un tercero de confianza. Consideremos que, en la actualidad, existen extensiones que hacen posible el uso de claves asimétricas.

Los servicios de Active Directory deben ser instalados en el servidor. No se encuentran activos por defecto.





Para poder consumir los servicios ofrecidos por Active Directory podemos crear un nuevo dominio.

En una red de computadoras que implementan Active Directory es necesaria la presencia de uno o más servidores DNS.

- **Confianza de acceso directo**: es una relación de confianza explícita que crea accesos directos entre dos dominios en la estructura de dominios. Este tipo de relaciones permite incrementar la conectividad entre dos dominios, y así, reduce las consultas y los tiempos de espera para la autenticación.
- **Confianza entre bosques**: estas relaciones permiten la interconexión entre bosques de dominios, creando relaciones transitivas de doble sentido. En Windows 2000, las relaciones de confianza entre bosques son del tipo explícito, a diferencia de lo que sucede en Microsoft Windows Server 2003.

Para conectarse a otros bosques o dominios que no son de Active Directory, AD usa el protocolo Kerberos en su versión 5, aunque también soporta **NTLM** y usuarios web mediante autentificación **SSL/TLS**. Los direccionamientos a recursos están definidos por los estándares **UNC** (convención universal de nombramiento), URL (localizador uniforme de recursos) y las definiciones de direcciones establecidas en el protocolo LDAP.
Cada objeto que forma parte de la red posee un nombre distintivo o **DN** (*Distinguished Name*). Así, por ejemplo, una impresora denominada **Imprimir**, que se encuentra dentro de una unidad organizativa u **OU** (*Organizational Unit*) llamada **Administración**, perteneciente al dominio **organizacion.org**, puede especificarse de dos modos:

- En notación DN, CN=Imprimir, OU=Administración, DC=organización, DC=org; donde CN (Common Name) es el nombre común y DC (Domain Class Object) hace referencia a la clase de objeto de dominio.
- En forma canónica podemos especificar la dirección como **organización.org/Administración/Imprimir**.

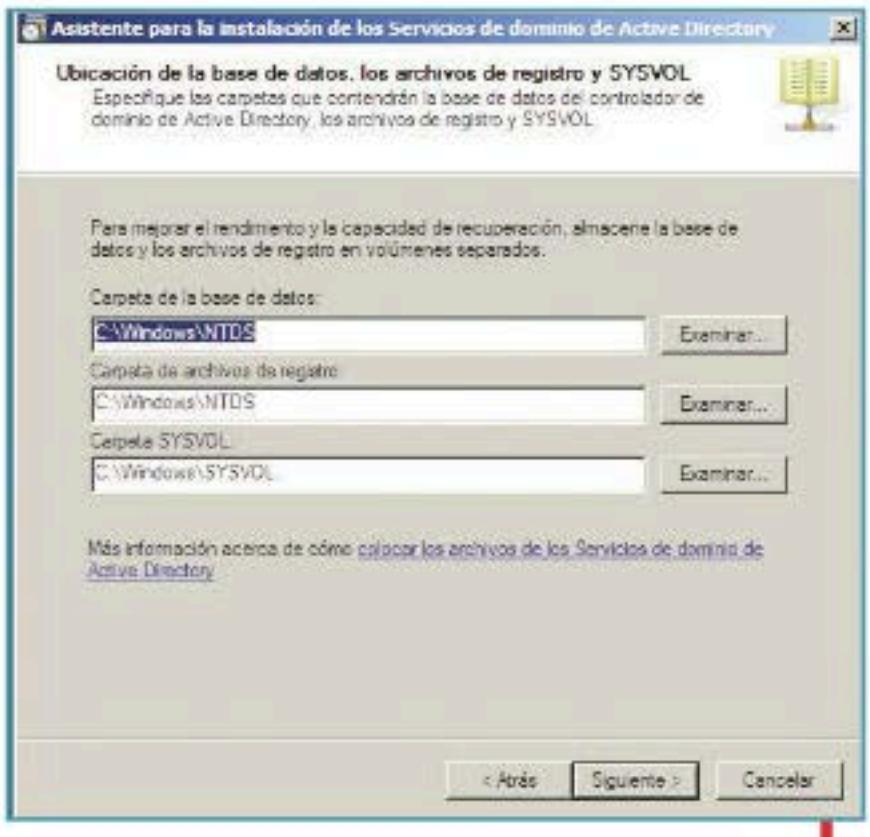
También podemos emplear métodos para individualizar un recurso en forma local:

- Empleando una distinción de mombre relativo o **RDN** (*Relative Distinguished Name*), que se caracteriza por buscar un recurso a través del nombre común (CN) solamente.
- Empleando un identificador global único o **GUID** (*Globally Unique Identifier*), que genera una cadena de caracteres de 128 bits de la cual se vale AD para buscar y replicar información.

Algunos tipos de objetos poseen un nombre de usuario principal o **UPN** (*User Principal Name*) que posibilita el acceso de forma abreviada a un recurso o directorio dentro de una red de computadoras. La notación es **nombredeobjeto@dominio**.
Active Directory, a diferencia de Windows NT Server, permite crear estructuras jerárquicas conformadas por dominios y subdominios, una manera más sencilla y ágil de representar los recursos de una red según su ubicación o función dentro de una organización o empresa. Además, se basa en estándares como X.500 y LDAP para acceder a la información.

Personalización

Otra característica peculiar que ofrece Active Directory son las interfaces de servicio o **ADSI** (*Active Directory Service Interface*), que brindan a los programadores la posibilidad orientada a objetos de crear programas que interactúen con



Active Directory posee una base de datos centralizada en donde se guarda la información de los objetos que pertenecen a un dominio.

AD, y aprovechen sus capacidades, mediante lenguajes de desarrollo de alto nivel, como Visual Basic, sin tener que lidiar con los diferentes espacios de nombres.
Es posible desarrollar software que realice un acceso único a diferentes recursos de la red sin importar si están basados en LDAP o en algún otro protocolo. También es posible generar ciertas secuencias de comandos que puedan ser ejecutadas por los administradores de la red.

Requisitos para la instalación

Antes de instalar Active Directory, debemos asegurarnos de que la computadora que va a ser configurada como controlador de dominio (*Domain Controller*) cumple con cada uno de los requisitos de hardware y de sistema operativo necesarios para su correcto funcionamiento.
Además, el controlador de dominio debe tener acceso al servidor DNS, y el software de este debe soportar la integración con Active Directory. Por lo general, se realiza la instalación de la solución DNS proporcionada por Microsoft.

- Se debe contar con cualquier versión de servidor de Windows instalado, como Windows 2000 Server, Windows 2003 Server en sus diferentes versiones o Microsoft Windows 2008. Por otra parte, para instalat Microsoft Windows 2003 Server es necesario tener instalado el Service Pack 1.
- Se requiere la instalación del protocolo TCP/IP configurado de forma manual en lo que se refiere a los parámetros de la interfaz o placa de red, es decir, que dichos parámetros no sean asignados de manera dinámica por un servidor DHCP.
- Tiene que haber uno o más servidores DNS dentro de la red donde se desea implementar AD, para resolver la dirección de los distintos recursos presentes en los dominios.
- Se necesita un mínimo de 250 MB de espacio en disco, 200 MB para la base de datos de Active Directory y 50 MB para los archivos logs de transacciones de Active Directory. Los requisitos del tamaño del archivo para la base de Active Directory y los archivos log dependen del número y del tipo de objetos en el dominio. Se requiere espacio de disco adicional si el controlador de dominio es un servidor de catálogo global.
- Se precisa una partición o un volumen con formato NTFS como sistema de archivos. La partición NTFS se requiere para la carpeta denominada SYSVOL.

Soluciones alternativas

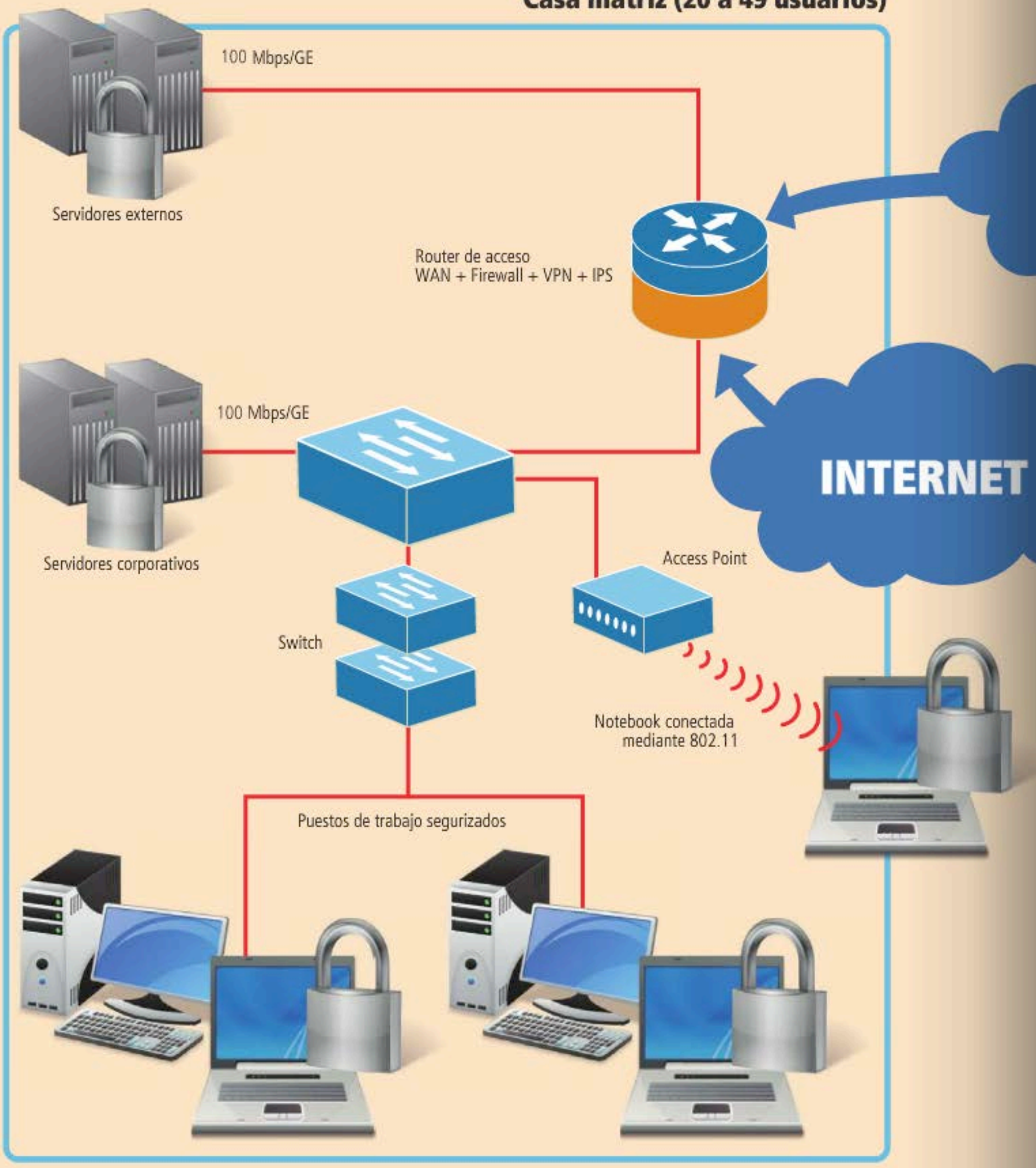
Existen diferentes alternativas que es necesario considerar; a continuación, veremos las más importantes:

- **Samba**: software de código abierto que se ejecuta sobre sistemas Linux. Posee un controlador de dominios compatible con Windows NT 4.0. Sitio web: **www.samba.org**.
- **Mandriva Directory Server**: aplicación también de código abierto que ofrece una interfaz web de gestión para administrar el controlador de dominios Samba y el protocolo LDAP. Sitio web: **http://mds.mandriva.org**.
- **Novell eDirectory**: solución que soporta sistemas operativos como Linux, UNIX, AIX, Solaris y Novell Netware. Sitio web: **www.novell.com/developer/develop_to_edirectory.html**.
- **Oracle Directory Server Enterprise Edition**: solución basada en Java y desarrollada por Oracle (dueña de Sun Microsystems). Sitio web: **www.oracle.com/technetwork/testcontent/index-085178.html**.
- **OpenDS**: implementación de servicio de directorios de código abierto, desarrollada en Java. Sitio web: **http://opends.java.net**. ■

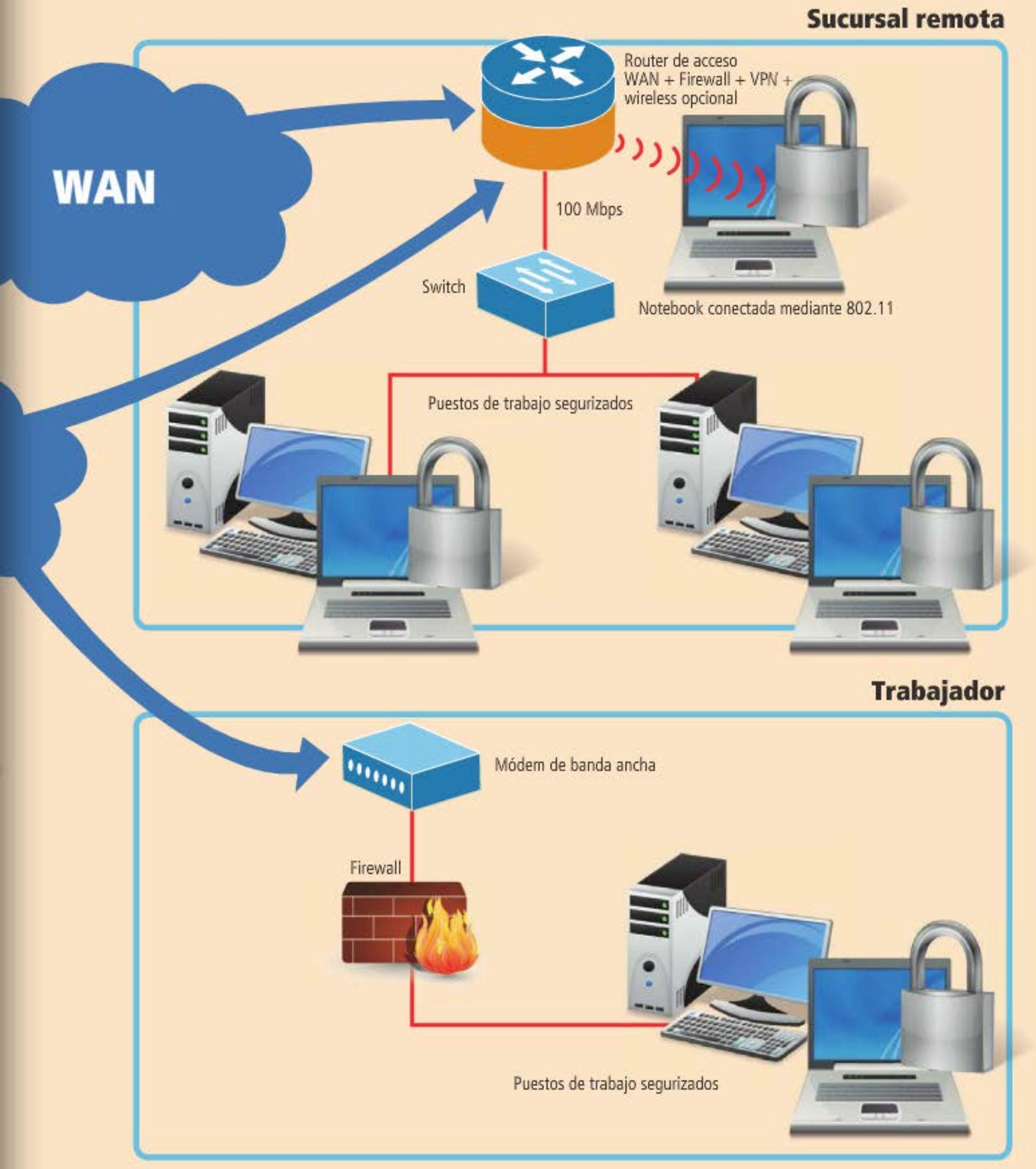
Protocolo de archivos compartidos

Samba es una implementación de código abierto del protocolo de archivos compartidos de Windows, renombrado como sistema de archivos común de Internet o **CIFS** (*Common Internet File System*) en la actualidad, para sistemas operativos de la familia UNIX. Samba es un sistema que hace posible que computadoras Linux, Mac OS X o UNIX, servidores o clientes, actúen como computadoras Windows dentro de una red.

Seguridad en red SMB



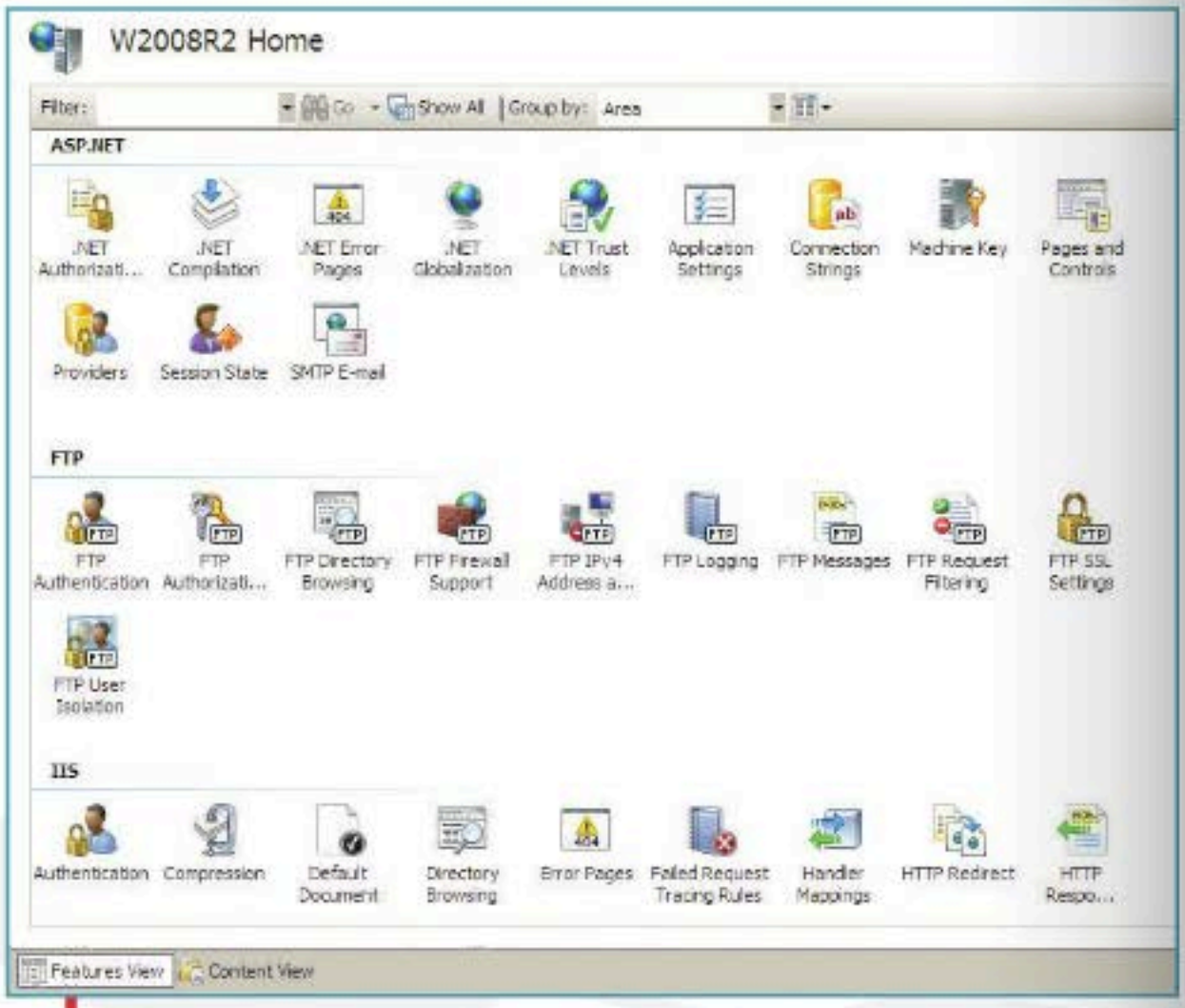
EN ESTAS PÁGINAS CONOCEREMOS UNA TÍPICA IMPLEMENTACIÓN DE SEGURIDAD EN UNA RED SMB.



Distintas ediciones de Windows Server

Analizaremos en detalle las distintas características, ventajas y desventajas de los sistemas operativos desarrollados para servidores.

Para identificar las distintas mejoras que se han realizado a través de los años en los sistemas operativos orientados a servidores, haremos un listado cronológico en el que especificaremos qué modificaciones se fueron haciendo. Cuando se lanzó el primer sistema operativo, se fueron detectando falencias, desventajas y, principalmente, se fue adaptando a los cambios. En los tiempos en que las redes informáticas no eran del tamaño que hoy representan, los sistemas operativos convenciones cumplían y abarcaban todas las necesidades. Pero a medida que fueron creciendo, surgieron nuevos requerimientos y se realizaron mejoras para satisfacer los requerimientosde los administradores, como condiciones de seguridad, protección y manejo de la información, velocidad de conexión y administración de perfiles. Los nuevos sistemas operativos han sido diseñados para abastecer las necesidades actuales y futuras. A continuación, veremos en detalle sus principales características.



Una de las herramientas principales que encontramos es el **IIS** para el manejo de **Web Services**.

Service Pack

Si bien todos los sistemas operativos tienen sus versiones destinadas a clientes específicos, su uso requirió mejoras o servicios adicionales. Cada una de las versiones de los S.O. estuvo acompañada de numerosos Service Packs que introdujeron aplicaciones nuevas, parches de seguridad y funciones que extendieron la vida útil de cada sistema, en algunos casos, durante décadas. Como estos sistemas estaban orientados a la seguridad, fue indispensable efectuar mejoras continuas.

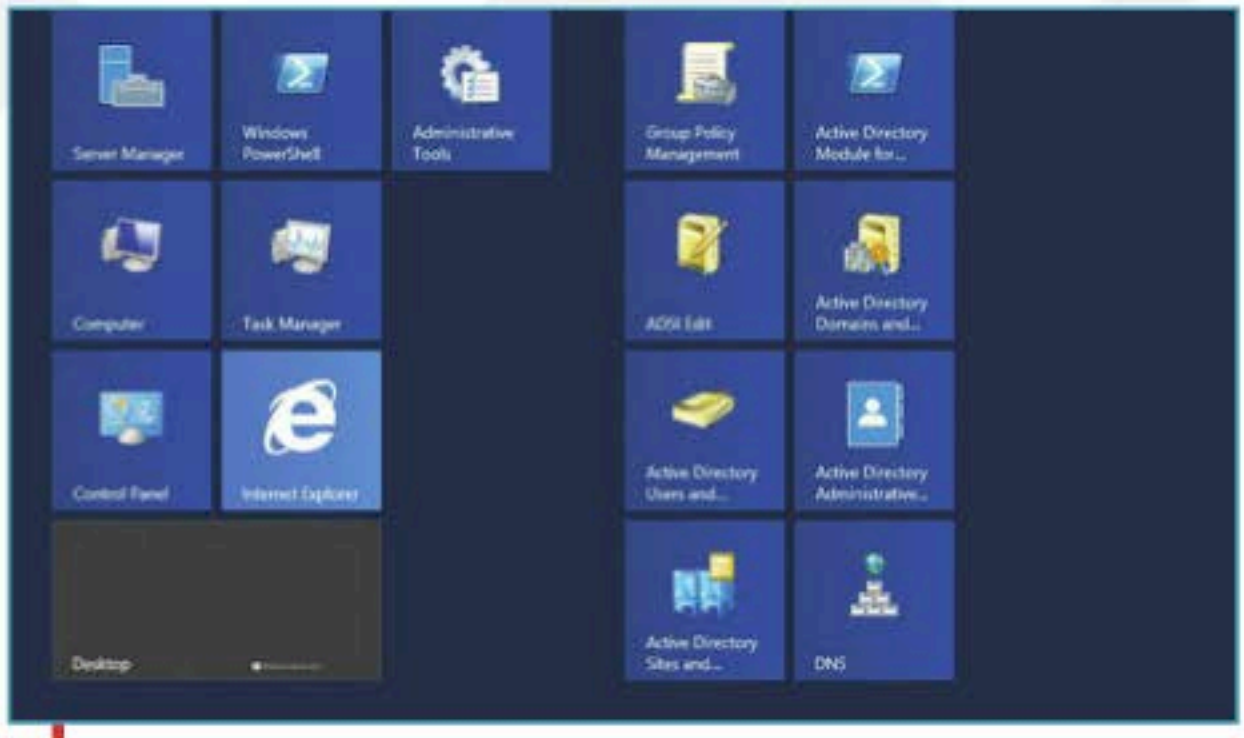
Windows 2000

Fue el primero en combinar y unificar los sistemas operativos que, hasta ese entonces, eran diferentes (**Windows 98** y **Windows NT**). A partir de eso, los sistemas que surgieron unificaron servicios pero de manera distinta, habilitando o deshabilitando funciones para optimizar el rendimiento según su uso.
Las principales tareas relacionadas con el sistema operativo son crear cuentas de usuario, asignar privilegios, asignaciones y delegaciones, asignar DNS, actuar como **servidor WEB**, resolver los nombres de dominio, y actuar como servidor de impresión, de archivos y DHCP, entre otros servicios provenientes de la familia NT.

Windows Server 2003

La versión 2003 siguió la línea característica de la familia de sistemas operativos orientados a servidores.
Su núcleo estaba basado en la tecnología NT en su versión 5.2. En comparación, era muy similar al sistema operativo **Windows XP**, pero con características especiales orientadas a servidores y rendimiento; algunas funciones eran desactivadas para llevar a cabo esta tarea.
Algunas de las características principales son las que mencionamos a continuación:

- Servicios de información de Internet (IIS, *Internet Information Services*) v6.0, que ofrece un servidor web.
- *Manage Your Server*, herramienta que permite al administrador escoger que funcionalidad debe ser utilizada.
- Se mejora Active Directory, que permite desactivar clases de un determinado esquema, o correr diversas instancias de servidores de directorio (ADAM).
- Aplica una mejora en las políticas de grupo, donde se optimizan la administración de los permisos.
- Se implementa un sistema de backup para la recuperación de archivos.
- Se mejora el administrador de discos, con la posibilidad de realizar backup de los archivos almacenados o abiertos.
- Se mejora la encriptación de la información, al igual que las herramientas de consola ofrecidas junto a esta versión del sistema operativo.



En **Windows Server 2012** se realiza un cambio íntegro en los servicios e interfaz gráfica, orientado a mejorar la gestión de servidores.

Windows Server 2008

Es el sucesor directo de Windows Server 2003 y se comporta como el hermano de **Windows 7**. Utiliza el núcleo NT 6.1.
Las principales novedades se refieren a mejoras en Active Directory, mejores presentaciones de virtualización, actualización a **IIS 7.5** y soporte para más de 256 procesadores. Se mejora la gestión del hardware para hacerla más efectiva, el control remoto del sistema es menos complejo, y las políticas de seguridad se reestructuraron.
Existen nuevas funciones tales como un proceso de reparación de archivos NTFS (se realiza en segundo plano), la creación de cuentas de usuario en paralelo, facilidad de cierre de los servicios, implementación del sistema de archivos SMB2 (mejora el acceso a los servidores multimedia), introducción del *Address Space Load Randomization* (**ASLR**, que genera una protección contra la carga de controladores en memoria) y de *Windows Hardware Error Architecture* (**WHEA**, protocolo mejorado de reporte de errores), mejora el rendimiento de la virtualización, inclusión de una consola mejorada para administración y renovación del núcleo del sistema. Sus versiones son las siguientes: Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y especializado en Itanium.

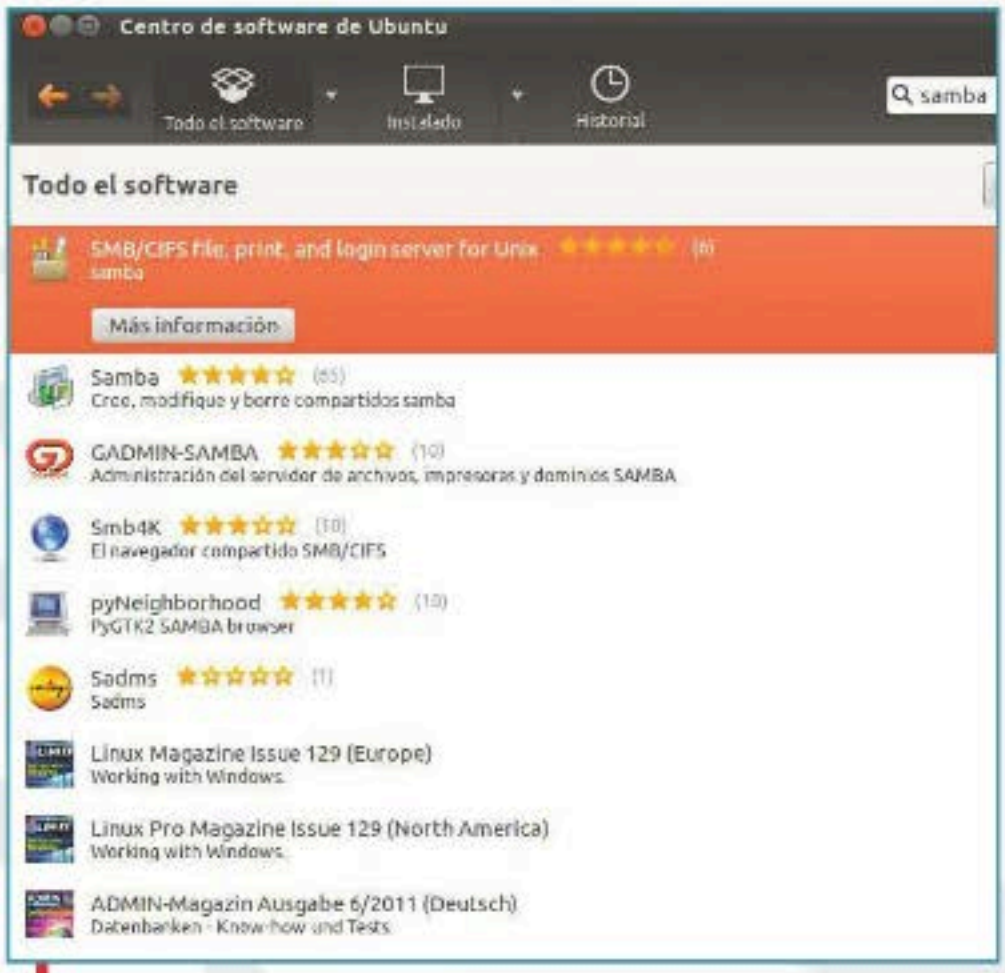
Windows Server 2012

Es la versión más renovada de **Windows Server** a la fecha, y representa a Windows 8 para servidores. Es el sucedor de Windows Server 2008 R2. Tiene menos cantidad de versiones, ya que las ha readaptado para brindar más funcionalidades a menos grupos; cuenta con solo cuatro y no tiene soporte para procesadores con tecnología Intel Itanium. Entre sus cambios, podemos mencionar: actualización de Hyper-V, rol de administración de IPs, renovada versión de Task Manager y un nuevo sistema de archivos conocido como ReFS.
Toda la interfaz fue mejorada para optimizar la gestión de múltiples servidores. El PowerShell incluye más de 2300 comandos nuevos y tiene la función de autocompletar.
El administrador de tareas se renueva para darle prioridad a la identificación de procesos que consumen muchos recursos.
Se mejora Active Directory, se actualiza a IIS 8.0, Hyper-V mejora la virtualización y se reduce el consumo de recursos.
Presenta **ReFS**, un sistema de archivos para servidores que mejora a NTFS. Se implementa *IP Address Managment*, que administra IP para búsqueda y auditoría en una red bajo servidores DHCP y DNS.
Soporta 640 procesadores y direcciona 4 TB de memoria física. ■

Comunicar servidores Linux con Windows

¿Cómo hacemos para que dos plataformas aparentemente incompatibles, como Windows y Linux, puedan compartir recursos? La respuesta es el paquete SAMBA.

Son numerosas las razones que llevan a nuestra red a tener un esquema heterogéneo, e indefectiblemente llega el momento en el que necesitamos interactuar entre las plataformas. Por suerte existe SAMBA, un paquete capaz de comunicar servidores basados en Linux con clientes Windows, y viceversa. En sus inicios, su nombre fue SMB (*Server Message Block*), utilizado por Microsoft para compartir recursos entre equipos de la plataforma Windows. Está desarrollado por una amplia comunidad de programadores a lo largo y ancho del planeta, y se basa tanto en la documentación de los protocolos como en la observación del funcionamiento de estos, ardua tarea que realiza la comunidad encargada de desarrollar el paquete. Esta maravilla del software libre nos brinda la posibilidad de compartir recursos en una red con equipos que tienen sistemas operativos tan disímiles como Windows y Linux. Según la cantidad de equipos presentes en nuestra red, pueden presentarse distintos escenarios; la principal diferencia es el modo en el que se gestiona la seguridad.



En caso de tener el modo gráfico instalado, podemos utilizar el gestor de software para instalar el paquete SAMBA.

Solución a medida

En una red con pocos equipos, la seguridad se gestiona en cada PC o servidor en forma aislada; este tipo de red se denomina red entre iguales. En este caso, tenemos que configurar los permisos y credenciales de los usuarios en cada lugar en donde se utilizan; por ejemplo, hay que crear los usuarios de la red en cada uno de los servidores que posean carpetas o impresoras compartidas, así como también asignar los permisos correspondientes en cada servidor de manera individual.

A medida que aumenta la cantidad de servidores y PCs en una red, surgen problemas relacionados con la reducida escalabilidad de la gestión aislada de la seguridad. Un ejemplo claro es que, al tener una gran cantidad de servidores con recursos compartidos, resulta impráctico tener que crear un usuario en cada uno de los servidores cuando una persona ingresa en la red.

La solución a los problemas de escalabilidad de las redes entre iguales es la centralización de la gestión de la seguridad en un grupo de servidores dedicados a este fin. Este tipo de red recibe el nombre de dominio, y los servidores a los que les asignamos el rol de gestores de la seguridad se llaman Controladores de dominio.

Active Directory

Una vez que la red está funcionando como un dominio, los servidores a los que les asignamos la función de Controladores de dominio toman un rol crucial. De ellos depende la gestión de la seguridad dentro de la red; cuando no estén disponibles, la red perderá las capacidades de autenticar, autorizar y registrar los accesos de los usuarios. Microsoft le dio el nombre de Active Directory al grupo de servicios que permiten gestionar de forma

centralizada la seguridad de una red configurada como dominio. Entre los servicios más importantes, podemos destacar el de resolución de nombres (DNS), que permite identificar a los distintos equipos que forman parte del dominio.
Otro servicio relevante es LDAP, destinado a realizar consultas a los controladores, como en el caso de que un servidor necesite consultar cuáles son los miembros de un grupo.
Por otra parte, no podemos dejar de mencionar a Kerberos, que es, sin lugar a dudas, el servicio más importante del dominio, porque se encarga de implementar la autenticación de los usuarios de forma completamente segura y centralizada.

INDEFECTIBLEMENTE, LLEGA EL MOMENTO EN EL QUE NECESITAMOS INTERACTUAR ENTRE LAS PLATAFORMAS; POR SUERTE, EXISTE SAMBA.

Instalación de SAMBA

El primer paso que tenemos que dar es instalar el paquete SAMBA; si decidimos hacerlo desde la consola en modo texto, el comando puede variar de una distribución a otra: por ejemplo, `apt-getinstall samba` en Debian/Ubuntu, o `yuminstall samba` en Fedora. También podemos instalar SAMBA desde la aplicación **Yast** en **SuSE** o desde el gestor de software en caso de que nuestra distribución tenga el modo gráfico instalado.

Paquetes adicionales

Para instalar SAMBA como controlador de dominio Active Directory, necesitamos también los paquetes que permitan a nuestro servidor llevar a cabo los roles de servidor DNS, servidor Kerberos y servidor NTP (este último es opcional pero altamente recomendable, ya que permite sincronizar la hora de los equipos que forman parte del dominio, algo imprescindible para el funcionamiento del servicio Kerberos).
Los nombres de los paquetes pueden variar de una distribución a otra. A modo de ejemplo, los comandos de instalación en Debian 6 son: `apt-getinstall krb5-admin-server krb5-user` para el servicio Kerberos, `apt-getinstallntp` para el servicio NTP y `apt-getinstall bind9 bind9utils` para implementar el rol de servidor DNS.

Para configurar el funcionamiento de SAMBA, tendremos que acceder y editar los archivos de texto adecuados.

Configurar SAMBA

SAMBA, como la mayoría de los servicios en Linux, se configura mediante archivos de texto. Si bien existen interfaces de escritorio y web que nos permiten realizar la configuración gráficamente generando los parámetros por nosotros de manera interactiva, mediante la edición de los archivos de configuración, nos aseguramos de tener a nuestro alcance las opciones que se pueden parametrizar.
El principal archivo de configuración es `smb.conf` y lo podemos encontrar en la carpeta `/etc/samba`, donde se guardan los archivos relacionados con los parámetros del servicio SAMBA. Los archivos de configuración por defecto están extensamente comentados, y la documentación del paquete es realmente completa, por lo que pondremos énfasis solo en las opciones principales. Para configurarlo podemos utilizar un editor de texto como Vi u otro incluido en la distribución.

Recursos adicionales

Un sitio que no podemos dejar de visitar es el que mantiene la comunidad desarrolladora del proyecto SAMBA, el cual se encuentra en la dirección **www.samba.org**. En él encontraremos ejemplos de configuración de los distintos roles, noticias acerca de nuevas versiones y funcionalidades, recomendaciones sobre seguridad al configurar el paquete y una gran cantidad de recursos adicionales. Algo para tener en cuenta es que en el sitio del proyecto SAMBA es donde primero se publican las actualizaciones del paquete.

SAMBA como cliente o servidor

En este caso, tenemos que configurar el equipo para que sea capaz de llevar a cabo el rol de cliente o servidor en una red entre iguales, interactuando con equipos que poseen sistemas operativos de la familia Windows. A continuación, revisaremos las principales opciones para configurar dentro del archivo **smb.conf**:

```
1. [global]
2. workgroup = MIRED
3. netbiosname = MISERVIDOR
4. server string = Servidor de Archivos
(Samba-Linux)
5. log file = /var/log/samba/samba.log
```

En la línea número 1 se especifica que las opciones siguientes forman parte de la sección Global; en la segunda línea indicamos el nombre de nuestra red entre iguales, en este caso, es MIRED.
La línea número 3 nos permite indicar el nombre con el que se identifica al equipo que estamos configurando, independientemente de su rol de servidor o de cliente. Este es el nombre con el que los demás equipos nos solicitarán los recursos que compartamos, por ejemplo, mediante el entorno de red de Windows.

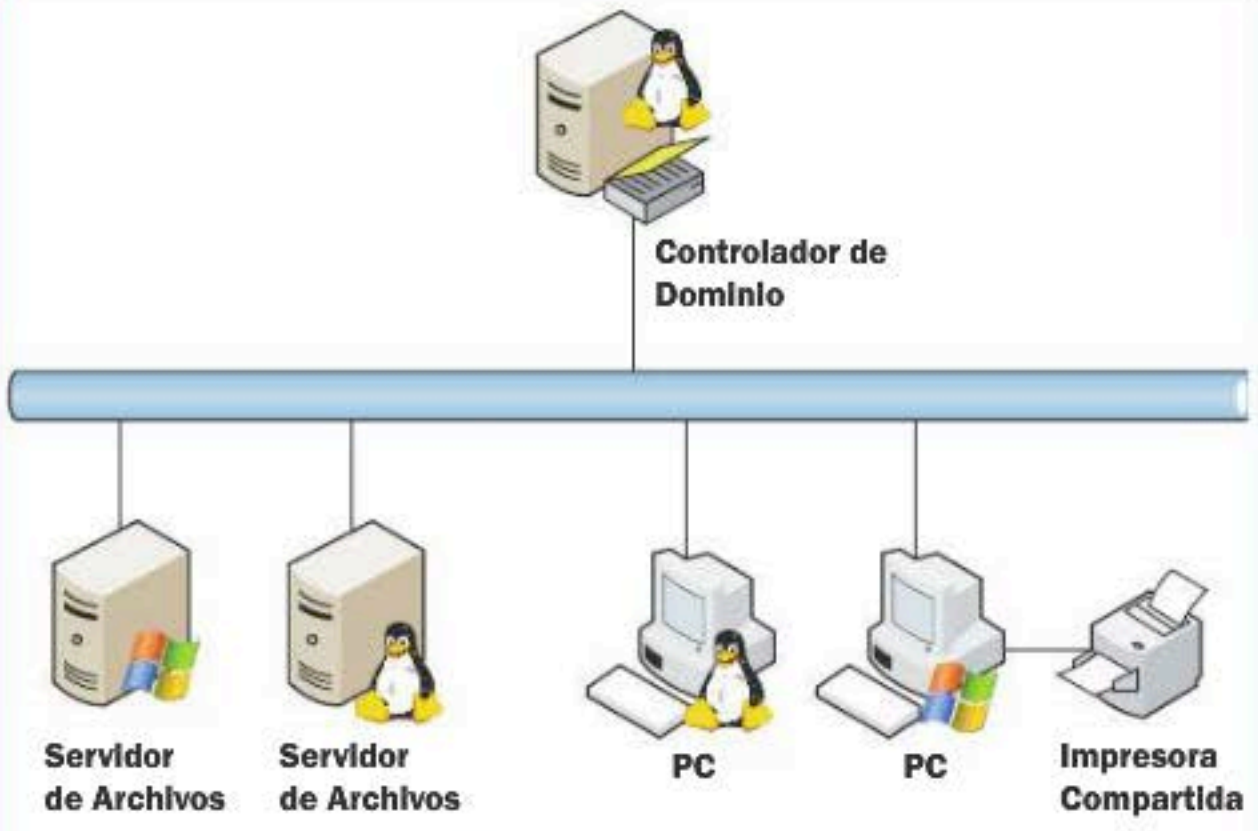
```
root@linux: ~
root@linux:~# service smbd restart
smbd start/running, process 3406
root@linux:~#
```

Una vez finalizada la instalación y la configuración del paquete SAMBA, es necesario iniciar el servicio correspondiente.

En la cuarta línea configuramos la descripción del equipo, la que lo describe con mayor detalle. Por último, en la quinta línea indicamos en qué archivo se guardarán los registros que genera el paquete SAMBA; esto puede ser de gran ayuda cuando necesitamos resolver algún inconveniente. De esta forma, tenemos lista la configuración básica del paquete SAMBA en una red de iguales. En caso de que necesitemos compartir un recurso, debemos agregar en el archivo **smb.conf** una sección como la siguiente:

```
1. [documentos]
2. path=/home/cecilia/documentos
3. browseable=yes
4. writeable=yes
5. validusers = Cecilia
```

Al igual que en la configuración global, la primera línea indica el nombre de la sección; en este caso, es también el nombre del recurso compartido.
En la segunda línea configuramos la ruta donde se encuentra la carpeta que deseamos compartir. Las líneas 3 y 4 nos permiten indicar que la carpeta compartida es visible cuando se navega por los recursos compartidos del servidor y que se puede escribir en ella, respectivamente. Por último, la quinta línea especifica que solo podrá acceder el usuario con la cuenta Cecilia. Cabe destacar que tendremos que definir dicho usuario en el sistema operativo y en el paquete SAMBA.



Aquí podemos ver el esquema de una red configurada como dominio Active Directory, con el servidor SAMBA actuando como Controlador de dominio.

Procedimiento para configurar Kerberos

Para que el paquete SAMBA pueda formar parte de un dominio Active Directory o ser un Controlador de dominio, necesitamos configurar el paquete Kerberos.
A continuación, se muestran las principales opciones del archivo de configuración **krb5.conf**, ubicado en la carpeta /etc, la cual almacena los parámetros generales del sistema operativo. La siguiente es la configuración que debemos establecer para configurar al paquete SAMBA como miembro de un dominio Active Directory:

```
1. 'libdefaults'
2. default_realm = DOMINIOAD.NET
3. 'realms'
4. DOMINIOAD.NET = {
5. kdc = controlador.dominioad.net
6. }
7. 'domain_realms'
8. .dominioad.net = DOMINIOAD.NET
```

Las líneas 1, 3 y 7 indican las distintas secciones del archivo de configuración. La línea 2, el dominio Kerberos que se utilizará por defecto. En las siguientes líneas indicamos que el distribuidor de claves del dominio `DOMINIOAD.NET` es el equipo que tiene como dirección DNS `controlador.dominioad.net`, y especificamos que los equipos que forman parte del dominio tienen las direcciones DNS finalizadas en .dominioad.net.

SAMBA como miembro de un dominio

En este caso, tenemos que configurar al paquete SAMBA para implementar un servidor que forme parte de un dominio Active Directory. De este modo, podremos compartir recursos con los equipos que son miembros del dominio, independientemente del sistema operativo que tengan instalado. A continuación, revisaremos las principales opciones del archivo `smb.conf`:

```
[global]
1. realm = DOMINIOAD.NET
serverstring = MiServidor
2. security = ADS
3. encryptpasswords = yes
```

En la línea número 1 definimos el nombre del dominio al cual vamos a unir el equipo; esta opción debe concordar con los parámetros que configuramos en el paquete Kerberos. Luego, en la línea número 2 delegamos en Active Directory la gestión de la seguridad del servidor. En la línea 3 especificamos la obligatoriedad de encriptar las claves, parámetro necesario para comunicarnos con el controlador de dominio.
Para finalizar la configuración, solo nos resta iniciar el servicio Kerberos y el servicio SAMBA y, luego, llamar a la función que realiza la vinculación al dominio Active Directory. La primera acción se lleva a cabo con el comando `kinit administrador@DOMINIOAD.NET`; luego iniciamos SAMBA con el comando correspondiente a la distribución que tengamos instalada. A modo de ejemplo, en Ubuntu Server se inicia el servicio con el comando `servicesmbdstart`.

SAMBA como controlador de dominio

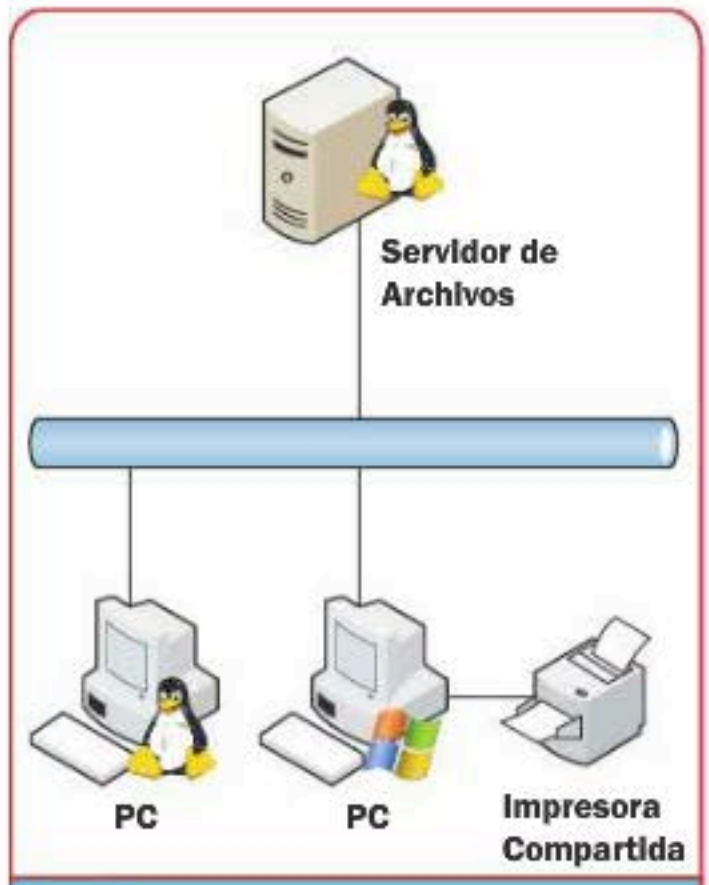
Uno de los lugares desde donde podemos obtener SAMBA es el sitio web oficial **www.samba.org**. Una vez copiado a la carpeta donde se compilará, ejecutamos los comandos:

```
# tar -zxvf samba-4.0.0.tar.gz
# cd samba-4.0.0
samba-4.0.0# ./configure --enable-
debug --enable-selftest
samba-4.0.0# make
samba-4.0.0# makeinstall
```

Ahora ya tenemos el paquete SAMBA compilado e instalado, resta configurarlo para asignarle el rol de Controlador de dominio Active Directory. Afortunadamente, el paquete incluye un script que genera el archivo de configuración `smb.conf`:

```
# /usr/local/samba/bin/
samba-tooldomainprovision
```

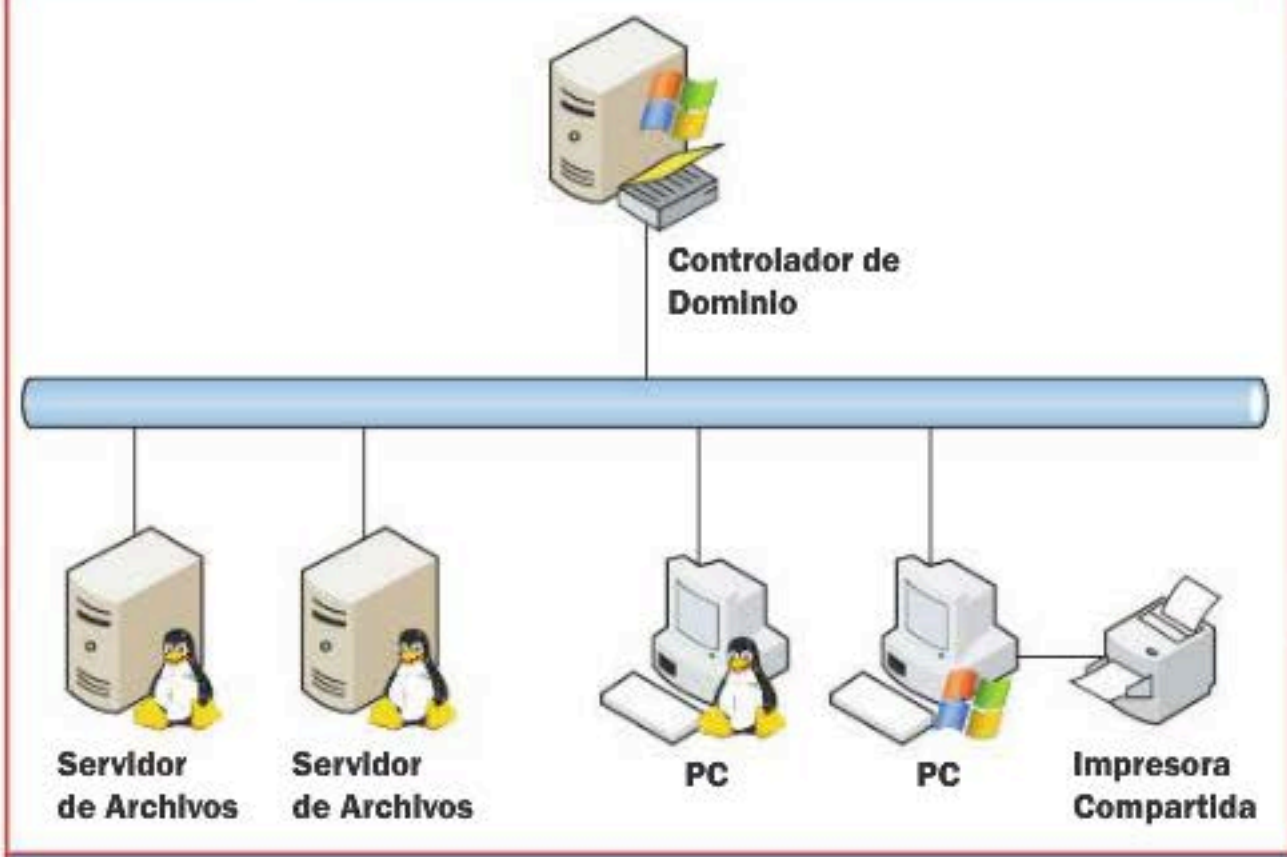
Para concluir la configuración del paquete SAMBA como Controlador de dominio Active Directory, corregimos el archivo krb5.conf, el cual es generado automáticamente al configurar el paquete como Controlador de dominio.



Red entre iguales con equipos Windows y Linux, en ella se comparten los recursos entre ambas plataformas.

Solo tendremos que corregir la opción `${REALM}` con el nombre del dominio que indicamos en la configuración del paquete. Iniciamos Kerberos y arrancamos SAMBA:

```
# kinit administrador@DOMINIOAD.NET
# /usr/local/samba/sbin/samba ■
```



Esquema de una red configurada como Dominio Active Directory, donde vemos a SAMBA actuando como un miembro más del dominio.

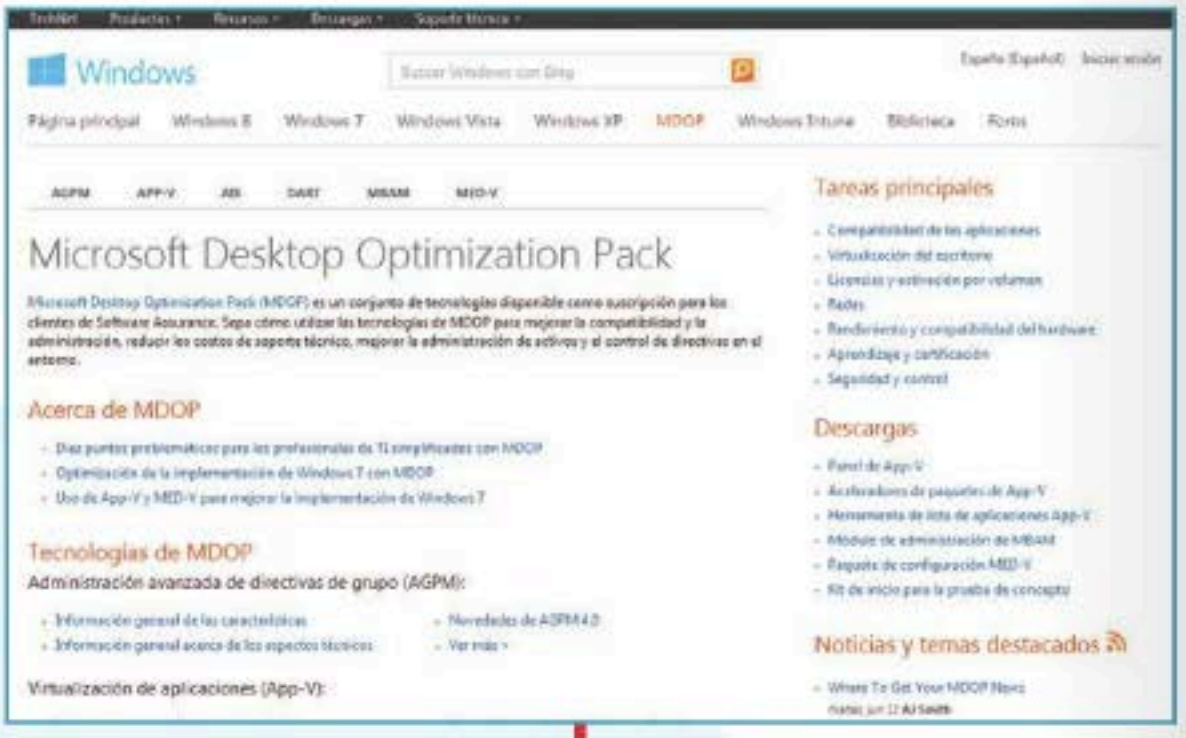
Administración de Directivas de Grupo

Se trata de una aplicación que encontramos dentro del MDOP, la cual nos permite realizar una gestión eficaz de las políticas de grupos, editarlas y delegarlas de manera offline.

Entre todas las herramientas que el sistema operativo nos brinda para controlar y dirigir los permisos dentro de la red, encontramos una que nos permite delegar acciones conteniéndolas en un mismo lugar, y nos permite revisar, editar, aprobar y generar nuevas políticas en un mismo aplicativo. La herramienta que se encarga del control de las políticas de grupo funciona como el manager de estas dentro del sistema operativo.

LA ADMISTRACIÓN AVANZADA DE DIRECTIVAS DE GRUPO PERMITE HACER CAMBIOS SIN CONEXIÓN.

Esta aplicación funciona como cliente/servidor, y permite realizar la administración avanzada de las Directivas de Grupo (**AGPM**, **Advanced Group Policy Managment**), que brinda un control de cambios integral y edición sin conexión. Es un componente principal dentro del paquete de optimización de Microsoft Desktop (**MDOP**, **Microsoft Desktop Optimization Pack**). MDOP ayuda a las organizaciones a reducir el costo de desarrollo de aplicaciones, utilizar aplicaciones como servicios y mejorar la administración de las configuraciones de escritorio.
La aplicación **AGPM** flexibiliza la administración de las políticas de grupos, principalmente, cuando estas se encuentran en entornos de red complejos. Una de las principales características es la posibilidad de realizar cambios en los objetos de las políticas de grupos (**Group Policy Objects**, **GPO**) de manera offline, auditar los cambios y encontrar variaciones entre las distintas versiones de los GPO. Nos otorga informes detallados para controlar cambios en las versiones, capturas en el historial y restauración de versiones antiguas velozmente.



Para Windows 7, Windows 8 y anteriores (en versiones Ultimate), se usa el MDOP para activar AGPM.

Edición offline

Los archivos de AGPM permiten el almacenamiento offline de los GPO, y esto habilita que los cambios realizados en los GPO no afecten el área de trabajo hasta que terminemos su desarrollo. De esta manera, editaremos los objetos libremente, bajo nuestras normativas, sin afectar los procesos que estén funcionando en ese momento. Una vez que finalicemos los cambios, estos GPO sustituirán a los antiguos mediante una sincronización. Si estas actualizaciones no resultan favorables, es posible restituir los cambios realizados.

Integración GPMC

El AGPM tiene un componente de cliente/servidor que se instalan de manera independiente. Primero instalamos el componente servidor en un sistema que tenga acceso a las políticas que queremos administrar y, luego, instalamos el componente de cliente en un sistema

Versiones de Windows y compatibilidad con AGPM

Sistema operativo a utilizar	Versión de AGPM que se puede instalar	AGPM 4.0 administra configuraciones de directiva	AGPM 3.0 administra configuraciones de directiva	AGPM 2.5 administra configuraciones de directiva
Windows Server 2008 R2	AGPM 4.0	Sí	Sí, con algunas excepciones	Sí, con algunas excepciones
Windows 7	AGPM 4.0	Sí	Sí, con algunas excepciones	Sí, con algunas excepciones
Windows Server 2008	AGPM 4.0, AGPM 3.0	Sí	Sí	Sí, con algunas excepciones
Windows Vista con SP1	AGPM 4.0, AGPM 3.0	Sí	Sí	Sí, con algunas excepciones
Windows Vista sin Service Packs instalados (64 bits)		Sí	Sí	Sí
Windows Vista sin Service Packs instalados (32 bits)	AGPM 2.5	Sí	Sí	Sí
Windows Server 2003 (64 bits)		Sí	Sí	Sí
Windows Server 2003 (32 bits)	AGPM 2.5	Sí	Sí	Sí
Windows XP		Sí	Sí	Sí
Windows 2000 Server		Sí	Sí	Sí
Windows 2000 Professional		Sí	Sí	Sí

que posea administradores de las políticas de grupo que tengan permitido revisar, editar y desarrollar las GPO. El componente del cliente se entrega con la consola de administración de las políticas de grupo (Group Policy Managment Console, GPMC). Entre sus opciones encontramos la opción de realizar numerosas modificaciones e, incluso, tomar control de los GPO sin dominio (GPO que no estén en archivo). A través de la consola, podremos delegar dominios y roles a los usuarios AGPM.

Control de cambios

El control de cambios nos brinda un detallado listado de la historia de los GPO durante su ciclo de vida y los cambios que han sufrido. La interfaz es amigable con el usuario y con los administradores experimentados con este tipo de herramientas. De esta manera, si los GPO nos presentan errores o no obtenemos los resultados esperados, podemos revisar los puntos clave donde fueron modificados y, así, corregir los posibles incidentes.

Delegaciones basada en roles

Podemos delegar tareas y permisos a administradores y sectores especializados y asignar usuarios que puedan realizar determinadas tareas para que ellos hagan sus propios cambios. Las modificaciones que hagamos en AGPM serán establecidas en un modelo de revisión, aprobación y edición. Un administrador AGPM tiene control completo de los archivos de AGPM, mientras que un Administrador de rol AGPM define tres roles especiales para sostener el modelo de delegación: revisor, que puede ver y comparar los GPO pero no puede editarlos ni desarrollarlos; editor, que puede ver y comprarlos, chequearlos desde archivo, editarlos y levantarlos al archivo, a la vez que solicitar el desarrollo de GPOs nuevos; y aprobador, que aprueba la creación del desarrollo de los GPO.

Búsqueda y filtro

Hay una característica que permite filtrar la lista de los GPO existentes mediante nombres, estado o comentarios; incluso, se puede filtrar la lista para mostrar los GPO que fueron cambiados por un usuario particular en una fecha específica. Los resultados pueden ser precisos o parciales. La versión más reciente de AGPM es la 4.0, y se aplica a Windows 7, Server 2008, Server 2008 R2 y Vista. En estas versiones se incluyen herramientas para un manejo más limpio, que nos permite encontrarlos por medio de atributos específicos. ■

Tipos de malware

Con la masificación de Internet, surgió con fuerza el fenómeno del software malicioso, el cual se encarga de aprovechar las ventajas que brinda la conectividad en red, aunque de manera ilegal.

El término malware, conjunción de las palabras *malicious* (malicioso) y *software*, se utiliza para englobar a los programas o software malintencionados, es decir, es una clasificación. Nos referimos a malware cuando hablamos de virus, spyware, adware, scareware, gusanos, troyanos, exploits y rootkits (puede que existan más tipos de malware, pero optamos por nombrar los más conocidos). Si bien el phishing no es un malware en sí, también constituye una amenaza de carácter malintencionado. La cualidad de malintencionado hace referencia al objetivo del malware, que va desde alterar el normal funcionamiento de un sistema (con la posibilidad de que este deje de funcionar por completo), pasando por robar información sensible (espiar), utilizar la computadora infectada como un zombie para realizar ataques, suplantar identidades, esparcir spam, obligar a los usuarios a comprar software, hasta descargar y mostrar publicidades.

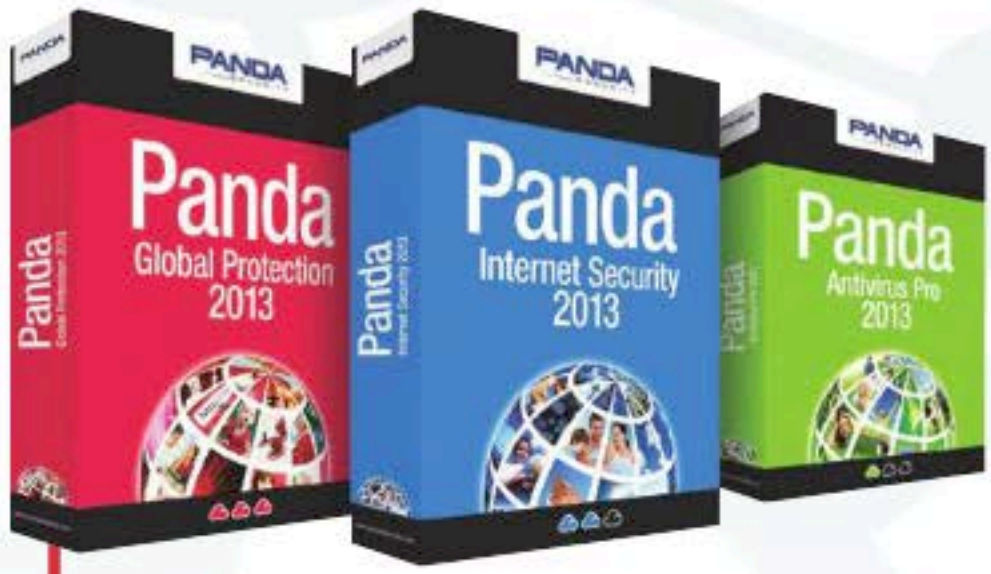
El adware generalmente se utiliza para generar ingresos económicos; en la Red existen diversas soluciones gratuitas.

Este tipo de programas actúan sin el consentimiento de los usuarios. Las amenazas se tipifican sobre la base de particularidades en su comportamiento.
A continuación, vamos a definir los tipos principales de amenazas que acechan a los sistemas.

Virus informático

El objetivo de un **virus informático** es alterar el normal funcionamiento de un sistema, más concretamente, deteriorarlo como lo hace un virus biológico con un ser vivo. Sus efectos pueden incluir la disminución en el rendimiento del sistema (ralentización, por ejemplo, al ejecutar procesos anormales) y la saturación de redes, hasta la corrupción de archivos del sistema (u otros programas), haciendo que la red funcione de forma incorrecta o deje de hacerlo en última instancia. Los más inofensivos solo muestran mensajes por pantalla o reinician el equipo cada cierto período de tiempo.
Debido a que un virus es un archivo ejecutable, es necesario que el usuario lo active para poder infectar un sistema. Una vez que es ejecutado, el código malicioso pasa a residir en la memoria, se apodera de servicios del sistema operativo, se propaga infectando

a otros archivos y a otras computadoras, y comienza a realizar las acciones para las cuales fue programado. Es por eso que no se deben activar archivos ***.EXE** de dudosa procedencia. Al momento de instalar programas, como medida preventiva, conviene descargarlos de las páginas web oficiales de las empresas que los desarrollan. Al igual que los virus biológicos, los virus informáticos mutan. Sus códigos fuente suelen estar accesibles en Internet para la descarga. Los programadores de malware toman dicho código y lo modifican para crear nuevos virus que comparten patrones de comportamiento. Son estos patrones, entre otros elementos, lo que utilizan las herramientas antivirus para detectarlos.



Las soluciones antivirus comparan el comportamiento de las aplicaciones con patrones de comportamiento de virus conocidos para poder detectarlos.

Spyware

El término **spyware** es una conjunción de las palabras *spy* (espiar) y *software*. Este tipo de programa tiene como objetivo espiar información personal atentando contra nuestra privacidad. Recopila información de la computadora infectada y la envía a través de Internet a entidades externas. Si bien trata de pasar inadvertido, puede provocar una disminución del rendimiento del sistema debido a que crea procesos adicionales y genera tráfico de red durante el envío de la información. Se asemeja más a un parásito que a un virus, ya que se instala en la computadora anfitriona pero no infecta a otras. Por lo general, necesita de la intervención del usuario para actuar, porque los sistemas suelen infectarse durante la ejecución de un archivo ***.EXE**, que está infectado. También puede ser introducido por un atacante, luego de instalar troyanos y rootkits; así, el usuario no interviene.

Adware

El término **adware** nace de la conjunción de las palabras *advertisement* (anuncios) y *software*. Abarca a todos aquellos programas que se caracterizan por publicitar servicios y productos. Se descargan y ejecutan sin consentimiento del usuario y muestran o bajan publicidades desde la Web. Esta actividad extra también produce una reducción en el rendimiento del sistema.

Scareware

El término **scareware** proviene de la conjunción de las palabras *scare* (miedo) y *software*. Este tipo de malware, también conocido como Rogue AV, es muy común en este último tiempo. Sobre la base de falsos anuncios de infecciones de un sistema, intenta convencer al usuario, a través del engaño, de comprar el producto que ofrece para solucionarlas. Es una práctica no ética que podría confundirse con una estafa y apela a la ingeniería social (que, básicamente, trata sobre el comportamiento de los usuarios frente a determinadas situaciones) para lograr su objetivo.

MALWARE SE UTILIZA COMO UNA CLASIFICACIÓN PARA ENGLOBAR A LOS PROGRAMAS MALINTENCIONADOS.

Worm

Un **gusano** es un tipo de malware que siempre reside en memoria y se duplica a sí mismo para tratar de alcanzar a los distintos equipos que se encuentran dentro de una red de computadoras. A diferencia de los virus informáticos, un gusano no infecta archivos, trabaja con procesos y se vale de servicios del sistema operativo que a menudo se encuentran ocultos para el usuario. Como los tipos de malware anteriores, perjudica el

Stuxnet

Es un gusano informático que afecta a sistemas Windows y fue descubierto en 2010. Es el primer gusano conocido que espía y reprograma sistemas industriales, como sistemas SCADA de control y monitorización de procesos, afectando infraestructuras críticas como, por ejemplo, la de una central nuclear. Tiene la capacidad de reprogramar controladores lógicos programables y ocultar los cambios realizados. Se sospecha que, debido a su complejidad, pudo haber sido desarrollado por un gobierno.

En 2005 Sony BMG distribuyó CDs que instalaban, fuera de la vista del usuario, un rootkit que limitaba el acceso al contenido del disco.

rendimiento del sistema porque ejecuta procesos adicionales innecesarios en la máquina. No requiere de la intervención del usuario, infecta un sistema, aprovechándose de alguna vulnerabilidad conocida, y se activa en forma automática.

Troyano

El término troyano deriva de la historia del **caballo de Troya**. Los troyanos se presentan al usuario como software legítimo en forma de archivos con la extensión ***.EXE**. Al igual que los virus, necesitan de la intervención del usuario (ejecución) para poder infectar una computadora. Se caracterizan por crear una puerta trasera o backdoor en el sistema, a través de la cual un usuario no autorizado puede administrar el sistema en forma remota. De esta manera, dicho usuario no autorizado puede ejecutar programas, robar información y desestabilizar el sistema, entre otras acciones. A menudo, las redes zombies que existen en la actualidad son creadas por troyanos.

Rootkit

El término **rootkit** es la conjunción de las palabras *root* (raíz), que se utiliza para designar al usuario administrador en entornos UNIX, y *kit* (conjunto de elementos). Se denomina de esta manera a los conjuntos de herramientas que les permiten a sus desarrolladores modificar el comportamiento del sistema operativo para ocultar el accionar de los troyanos u otro malware previamente instalado. Se caracterizan por la necesidad de que exista un backdoor en el sistema, son instalados por el atacante luego de tomar el control de la computadora infectada y no requieren la intervención del usuario. Debido a que los rootkits modifican el comportamiento de un sistema operativo en ejecución, son muy difíciles de detectar. Un método efectivo es apagar el sistema infectado y escanearlo en busca de infecciones a través de otro medio o de otro sistema.

Exploit

El término **exploit** (explotar o aprovechar) hace referencia al aprovechamiento de las vulnerabilidades de un sistema. Consiste en un conjunto de sentencias de programa que tienen como objetivo producir fallas en un sistema, ya sea para que el atacante gane privilegios dentro de él y poder utilizarlo a su antojo, o para desestabilizarlo. No necesita de la intervención del usuario. Cabe destacar que, en la actualidad, las amenazas existentes pueden caer en más de una categoría de las presentadas hasta aquí; es decir, una amenaza particular puede tener características de más de un tipo de malware.

Phishing

Se puede definir como una estafa utilizando medios electrónicos. Generalmente consiste en alojar en un servidor una página web falsa de un sitio conocido, idéntica a la original. El usuario se conecta e ingresa en ella información privada (números de teléfono, de tarjetas de crédito, contraseñas, etc.). El sitio acusa un error y, luego, redirecciona la conexión a la página original para evitar que el usuario detecte el fraude. Entonces, roba información de suma importancia que, después, puede ser vendida o utilizada para beneficio del atacante (**phisher**). Este tipo de amenazas a la seguridad de los usuarios también apela a la obtención de datos mediante diversos procesos fraudulentos, conocidos, en términos generales, con el nombre de ingeniería social. ■

PRÓXIMA ENTREGA

16

ADMINISTRACIÓN DE SISTEMAS LINUX

En el próximo fascículo veremos como configurar y administrar servidores Linux. Conoceremos, además, los comandos más útiles y precauciones de seguridad.

Técnico en REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00015
9 789871 857784

CONTENIDO DE LA OBRA

1 Introducción a las redes informáticas
2 Tipos de redes y topologías
3 Dispositivos de red
4 Instalación de redes cableadas
5 Puesta en marcha de una red cableada
6 Configuración de redes cableadas
7 Instalación de redes inalámbricas
8 Configuración de redes inalámbricas
9 Seguridad en redes cableadas e inalámbricas
10 Configuración avanzada de routers
11 Recursos compartidos y dispositivos multimedia
12 Seguridad física de la red
13 Impresoras de red
14 Hardware de servidores
15 ADMINISTRACIÓN DE WINDOWS SERVER
16 Administración de sistemas Linux
17 Administración y asistencia remota
18 Servidores web y FTP
19 Servidores de mail
20 Servidores de archivos e impresión
21 Servidores adicionales
22 VLAN, VPN y trabajo remoto
23 Telefonía IP
24 Cámaras IP