Tema 3

GESTIÓN DE USUARIOS, GRUPOS Y EQUIPOS.

Las cuentas de usuario, permiten que varios usuarios utilicen el mismo equipo, y al mismo tiempo mantener separadas las configuraciones de cada uno de ellos: documentos, escritorio, favoritos, etc.

En Windows 7, existen dos tipos de cuentas de usuario, en función de los privilegios que se quieran otorgar al usuario en concreto:

- Usuario estándar o usuario limitado: Estos usuarios, pueden utilizar el software instalado en el equipo, así como cambiar la configuración del equipo que no afecte a otros usuarios ni a la seguridad del equipo. No pueden instalar ni desinstalar software, crear cuentas de usuario, ...
- Usuario Administrador: Los usuarios administradores tienen acceso total al equipo y pueden realizar los cambios que deseen.

La gestión de las cuentas de usuario, puedes llevarla a cabo en el apartado: "Cuentas de usuario y protección infantil" del panel de control, utilizando Administrar del menú contextual de Equipo, Usuarios locales y grupos.

Los grupos se utilizan para agregar a los usuarios de forma que se puedan asignar privilegios más fácilmente a dichos usuarios y hacer más sencilla su administración. Por tanto, se puede incorporar un usuario a uno o a varios grupos teniendo, en cada uno de ellos, unos permisos determinados que le permitirán realizar distintas funciones.

Windows 7, también te permite establecer un control parental sobre las cuentas de usuario, orientado principalmente a la protección de los menores sobre el acceso a determinados contenidos, programas, etc.

En primer lugar, para proceder a la gestión de las cuentas de usuario de un equipo, debes contar con los privilegios de Usuario Administrador, es decir, es necesario crearlas utilizando la cuenta de un usuario que sea administrador, o bien conocer la contraseña de algún usuario de tipo Administrador.

Cuando se crea una nueva cuenta de usuario, se genera lo que se denomina un nuevo perfil para ese usuario. El perfil de usuario, contiene las configuraciones específicas para ese usuario concreto: documentos, favoritos, escritorio, etc. Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo, y aquellos usuarios que acceden a varias estaciones pueden tener un perfil en cada una de ellas. Este perfil se denomina perfil local porque sólo es accesible desde la estación que se ha creado.

Los archivos y configuraciones de cada usuario, se almacenan en su perfil, que permanece almacenado en la Carpeta Usuarios (C:\Usuarios\nombre_usuario).

Si elimina una cuenta de usuario, toda la información almacenada en el perfil de ese usuario, tal como, documentos, imágenes, escritorio, etc. y que se almacena en la ruta: C:\Usuarios\nombre_usuario, puede ser eliminada, o por el contrario, Windows 7 te permite mantenerla, por si es necesario recuperar información.

Control parental de W7.

Este complemento, te ofrece la posibilidad de restringir el acceso de un usuario Estándar del equipo (usuario limitado) al uso del mismo. Se puede limitar el uso del equipo desde varios frentes:

1.- Límites de tiempo: Podemos restringir las horas de uso del mismo a ese usuario.

2.- Juegos: Podemos bloquear la utilización de juegos instalados en el equipo, utilizando una clasificación por edades.

3.- Permitir y bloquear programas específicos: Podemos permitir el uso solamente de los programas especificados.

Este complemento también dispone de complementos adicionales, como filtrado web, para restringir el uso de Internet que es necesario instalarlos.

Esta característica, en un principio está ideada con el fin de controlar el acceso a contenidos por parte de menores de edad, pero también puede ser de utilidad en entornos laborales, especialmente las restricciones de tiempo, y la limitación de uso de programas.

Permisos NTFS

Con los permisos NTFS indicamos que usuarios y grupos tienen acceso a determinados archivos y carpetas. Su principal cometido es dar seguridad a los datos almacenados en los dispositivos de almacenamiento.

Los permisos NTFS se instrumentan en unas marcas que se realizan en los ficheros y carpetas y que se traducen en una **lista de control de acceso** (ACL) para ese fichero o carpeta en cuestión. Cuando iniciamos el sistema operativo, el kernel lee estas marcas y aplica las restricciones.

Para administrar los permisos en una carpeta o fichero, accedemos a sus propiedades y a la pestaña *seguridad*, agregamos los grupos y los usuarios a la ACL y administramos sus permisos. Podemos usar los permisos especiales con el botón *avanzada*.

Por defecto, cuando se crea un fichero o una carpeta hereda los atributos de seguridad de la carpeta inmediatamente superior. El problema está en que la más alta es el disco y este por defecto se configura con permisos para el grupo *todos* con *control total*. Esta configuración debe ser cambiada a otra que incluya *usuarios autentificados* con permiso de *modificar* y solo el grupo *administradores* debe tener *control total*.

La ACL de los archivos incluye los siguientes permisos:

- **Leer**: Se puede leer el archivo y ver sus permisos, atributos y quién es su propietario.
- **Escribir**: Es posible sobrescribir en el archivo. Ver al propietario y los permisos del archivo. Modificar sus atributos.
- **Lectura y Ejecución**: Se pueden ejecutar aplicaciones e incluye el permiso Escribir obligatoriamente.
- **Modificar**: Se puede modificar o eliminar el archivo, e incluye los permisos Escribir, y Lectura y ejecución.
- **Control Total**: Puedes tomar la propiedad y modificar los permisos, e incluye todos los permisos anteriores.

La ACL de las carpetas incluyen los siguientes permisos:

Leer: Permite ver archivos y subcarpetas dentro de la carpeta, ver los permisos y atributos de carpeta y saber quien es el propietario.

- **Escribir**: Permite crear archivos y subcarpetas en la carpeta, modificar atributos de carpeta, ver el propietario y los permisos.
- **Listar el Contenido de la Carpeta**: Ver los nombre de archivos y subcarpetas en la carpeta.
- **Lectura y Ejecución**: Te puedes mover por las carpetas para llegar a leer otros archivos y carpetas donde en principio no tendrías permisos, además incluye los permisos de Leer y Listar el contenido de la carpeta.
- **Modificar**: Puedes eliminar la carpeta e incluye los permiso de Escribir y Lectura y ejecución.
- **Control Total**: Puedes modificar los permisos, tomar la propiedad, eliminar subcarpetas y archivos, y además tienes todos los permisos anteriores.

Los permisos especiales permiten una mayor granularidad a la hora de aplicar restricciones. En realidad, lo permisos antes descritos son conjuntos de estos permisos.

La herencia de permisos

Bloqueo de herencia desde la carpeta hija:

Los permisos se heredan desde la carpeta padre a las subcarpetas y archivos hijos, si bien este comportamiento se puede modificar. En la pestaña *seguridad* existe una opción para bloquear la herencia entre la carpeta padre y la que estamos administrando:

Si desmarcamos esta opción bloqueamos la herencia, siempre desde el punto de vista de la carpeta hija:

Forzar la herencia desde la carpeta padre:

Si desde la pestaña *seguridad* hacemos clic en *avanzada* podemos modificar el comportamiento desde la carpeta padre para que obligue a todas sus hijas a heredar sus permisos:

A pesar de haber bloqueado la herencia en la carpeta hija, marcando esta opción en la carpeta padre sobrescribe la ACL de la carpeta hija.

Bloquear la herencia desde la carpeta padre:

Por último, para administrar un permiso en la carpeta padre y que este no se herede a las carpetas hijas configuradas para heredar, vamos a la pestaña en la que se administran los permisos especiales y marcamos la siguiente:

Así los permisos que apliquemos en esta ventana a la carpeta padre no se heredarán a las carpetas hijas aunque estas estén configuradas para heredar. Es decir, bloqueamos la herencia desde la carpeta padre.

Las Leyes de los permisos NTFS

1. Lo que no está explícitamente permitido, está implícitamente denegado.
2. Los permisos NTFS se suman por pertenencia a grupos. Esto quiere decir que si por la pertenencia a un grupo tenemos permiso de lectura y por pertenencia a otro lo tenemos de escritura, se sumarán y obtendremos lectura y escritura.
3. Denegar prevalece. Siempre prevalece denegar. Si una cuenta tiene privilegios de lectura por pertenencia a un grupo y de denegar leer por pertenencia a otro, prevalece denegar. No se recomienda usar denegar por la dificultad que entraña el posterior rastreo de permisos.
4. Prevalecen los permisos de fichero sobre los de carpeta: Si sobre una carpeta no tenemos permisos pero sobre un fichero que hay dentro de ella si, podremos acceder a él usando file:// y la ruta al fichero desde ejecutar.

Tomar posesión

Por defecto el usuario que crea una carpeta o un fichero pertenece al grupo CREATOR OWNER de esa carpeta o fichero. Este grupo tiene permisos de control total sobre los recursos que crea. Puede ocurrir que un usuario administre la ACL de un recurso, deniegue a todos los usuarios el acceso y sea necesario reestablecer los permisos. Un administrador siempre puede hacerse con la posesión de una carpeta o fichero del que no es propietario.

En la pestaña *seguridad* hacemos clic en *avanzada* y vamos a la pestaña *propietario*. En ella encontramos la lista de los usuarios y grupos que pueden hacerse con la posesión de la carpeta o fichero. Como se observa podemos elegir reemplazar también el propietario en las carpetas hijas y ficheros de la carpeta que estamos administrando.

Los **permisos SHARE (compartir)** se aplican cuando accedemos por red a una carpeta. Son más sencillos que los permisos NTFS y solo son tres: Control Total, Cambiar y Leer. Estos permisos se pueden aplicar incluso si no tenemos una partición NTFS en el sistema.

Los permisos SHARE se administran en las propiedades del fichero, en la pestaña *compartir* haciendo clic en *permisos.*

Al mezclar los permisos NTFS con los SHARE prevalece siempre el más restrictivo de los dos:

EFECTIVO POR RED	NTFS	SHARE
Leer	Leer	Cambiar
Leer	Modificar	Leer
Leer	Control Total	Leer
Denegado todo	Sin entrada en ACL	Leer
Denegado todo	Denegar leer	Control Total
Modificar	Modificar	Control Total

La correcta administración de los permisos pasa por utilizar permisos mas restrictivos en NTFS y mas relajados en SHARE. Así conseguimos por red los mismos resultados, pero protegemos también localmente ante un eventual acceso local no autorizado.

Para modificar los permisos desde la consola usa el comando icacls.

Las directivas locales.

En Windows, los derechos se han agrupado en un conjunto de reglas de seguridad y se han incorporado en unas consolas de administración denominadas directivas de seguridad que definen el comportamiento del sistema en temas de seguridad. Entre ellas se encuentra la Directiva de seguridad local que es la que se debe utilizar si se desea modificar la configuración de seguridad y el equipo de una estación de trabajo.

desde dicha herramienta de administración se pueden establecer, entre otras, las siguientes directivas:

- **Directivas de cuentas**: en este apartado se pueden establecer cuál es la política de cuentas o de contraseñas que se seguirá. Dentro de este apartado se pueden distinguir reglas en dos grupos: Contraseñas y Bloqueo. Entre ellas, hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión.

- **Directiva local**: en este apartado se encuentran la auditoría del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador y los derechos y privilegios que pueden tener los usuarios en el equipo.
- **Directivas de clave pública**: en este apartado se pueden administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

En Herramientas administrativas del panel de control, Directivas de seguridad local.

Al igual que ocurre con las Directivas de seguridad de un Directorio activo, en Windows 7 podemos ajustar un buen número de directivas locales. Si accedemos a la ventana de Herramientas administrativas en la ruta Inicio/Panel de control/Sistema y seguridad/Herramientas administrativas, podremos pinchar sobre el icono de Directiva de seguridad local. Enseguida, se abrirá una ventana donde, repartidas en diferentes apartados, encontraremos infinidad de opciones para ajustar la seguridad y comportamiento del equipo.

Así, por ejemplo, bajo Directivas de cuenta podremos crear una directiva acerca de la calidad de la contraseña u otra que bloquee la cuenta tras una serie de intentos fallidos de acceso. Bajo el apartado de Directivas locales localizamos el grueso de las opciones, hasta el punto de controlar el cambio de hora, uso de archivo de paginación o quién puede apagar la máquina.

Inicio -> Buscar -> "gpedit.msc

Recursos compartidos.

Compartir recursos, significa que usuarios de otro equipo, situado físicamente en otro lugar, pero conectado a través de una red, pueda utilizar determinados recursos de nuestro equipo. En este apartado, verás cómo compartir los recursos de nuestro equipo, para que puedan ser utilizados por otros usuarios de la red, así como regular el uso de los recursos, estableciendo políticas de seguridad, de forma que podamos determinar qué usuarios son los que pueden tener acceso a un determinado recurso de nuestro equipo, como puede ser una determinada carpeta, o una impresora, así como el nivel de control, que van a tener sobre ese recurso.

Nosotros somos los que decidimos cuáles son los recursos que queremos compartir y con quién.

Nombre del equipo y grupo de trabajo.

Si vas a utilizar tu equipo en una red, en primer lugar, deberás comprobar que está configurado adecuadamente el dispositivo de red (tarjeta de red) del equipo, que te proporciona conexión a la red. La Dirección IP: estática o dinámica, puerta de enlace y servidor o servidores DNS. Suponemos que el dispositivo de red está correctamente configurado, y tenemos conexión a nivel físico con los demás equipos de la red.

En primer lugar, vamos a cambiar el nombre del equipo, así como del grupo de trabajo poniendo un nombre, que te permita identificarle en la red de una forma clara. Por ejemplo, vas a utilizar el nombre: equipo-casa.

Para ello, dirígete a las propiedades del equipo (clic con el botón derecho sobre el icono equipo), y en el menú contextual, haz clic en propiedades.

En el apartado: "Configuración de nombre, dominio y grupo de trabajo del equipo", haz clic en "Cambiar configuración.

En la cuál debes hacer clic, en el botón cambiar. Aquí pon el nombre del equipo que hemos determinado ("Equipo-casa"), y al grupo de trabajo le vas a denominar "CASA".

Acepta los cambios, y es necesario reiniciar el equipo para que se apliquen los mismos.

El nombre de equipo que hemos aplicado, será el que nos permita identificar a nuestro equipo dentro de la red, en la que se pueden mostrar varios equipos, y de esta forma, sabemos con seguridad cuál es el nuestro.

PARA SABER MÁS

En el siguiente enlace puedes ver dos vídeos: un vídeo que ilustra de forma gráfica cómo configurar el adaptador de red (tarjeta de red) en Windows 7 y en Windows XP con una IP estática, establecida de forma manual y otro vídeo en el que se muestra como configurar el adaptador de red en las máquinas Virtuales VMWare y Virtual Box para establecer una red interna, que permita establecer una red entre varias máquinas virtuales.

URL: http://www.youtube.com/watch?v=QvR7hhtFGB0
URL: http://www.youtube.com/watch?v=JOSnITFNlww

Centro de Redes y recursos compartidos.

A continuación, vamos a configurar las opciones necesarias para compartir los recursos de nuestro equipo en la red. Para ello utilizarás el "Centro de redes y de recursos compartidos", en el apartado correspondiente del panel de control: Panel de control →Redes e Internet → Centro de Redes y recursos compartidos.

Las diferencias entre las diferentes ubicaciones de red son las siguientes.

- **Red doméstica**: Elegirás esta ubicación para redes domésticas o cuando conozcas y confíes en los usuarios y dispositivos de la red. Los equipos de una red doméstica pueden pertenecer a un grupo en el hogar. (verás más delante lo que son los grupos en el hogar). La detección de redes está activada para las redes domésticas, lo que permite ver otros equipos y dispositivos de la red y que otros usuarios de la red vean el equipo.
- **Red de trabajo**: Elegirás esta ubicación para oficinas pequeñas u otras redes del lugar de trabajo. La detección de redes, que permite ver otros equipos y dispositivos de la red y que otros usuarios de la red vean tu equipo, está activada de forma predeterminada, pero no podrás crear un grupo en el hogar ni unirte a él.
- **Red pública**: Elegirás esta ubicación para las redes de lugares públicos (por ejemplo, cafeterías o aeropuertos). Esta ubicación se ha diseñado para evitar que tu equipo sea visible para otros equipos y te ayudará a proteger el equipo de software malintencionado de Internet. Grupo Hogar no está disponible en redes públicas, y la detección de redes está desactivada. También debes elegir esta opción si estas conectados directamente a Internet sin usar un enrutador, o si tienes una conexión de banda ancha móvil.

Las ubicaciones de red, lo que hacen es establecer automáticamente un determinado perfil de red, es decir, unas configuraciones predeterminadas de la red que se adecuan en cuanto a seguridad y funcionalidad según el tipo de ubicación elegida.

Sin embargo, puedes también personalizar el perfil de red predeterminado para cada tipo de ubicación.

Para hacerlo, puedes utilizar la configuración de uso compartido avanzado. Vamos a estudiar detalladamente los apartados de esta configuración, entendiendo las funciones de cada apartado.

Para acceder a la configuración avanzada en el panel izquierdo del "Centro de Redes y recursos compartidos", haz clic en "Cambiar configuración de uso compartido avanzado".

En esta pantalla, si contraemos las opciones, haciendo clic en la pestaña para contraer, observamos que tenemos dos perfiles de red: Uno para casa o trabajo, que es el que aplicarás a las ubicaciones de red: Red doméstica y Red de trabajo, y el otro perfil, que es para las redes públicas, correspondiente a la ubicación de "Red pública".

Desplegamos el perfil de red "Casa o trabajo", que es el perfil que tenemos aplicado actualmente, y se muestran las siguientes opciones de configuración:

- **Detección de redes**: Activada. Esta opción permite que nuestro equipo sea visible en la red, así como ver otros equipos. Si desactivas esta opción, no tendrás acceso a la red.
- **Compartir Archivos e impresoras**: Activada. Esta opción como su nombre indica permite compartir archivos, carpetas e impresoras de nuestro equipo en la red. Si está opción está desactivada, los demás usuarios de la red, no podrán tener acceso a los recursos de nuestro equipo. (archivos e impresoras)
- **Uso compartido de la carpeta pública**. La carpeta pública, es una carpeta a la que tienen acceso total (lectura y escritura) todos los usuarios del sistema, bien sean Usuarios estándar o usuarios administradores. La ubicación de esta carpeta es: C:\Usuarios\Acceso público. Si activas el uso compartido de esta carpeta, además de los usuarios del equipo, también tendrán acceso a esta carpeta todos los usuarios de la red.

Conexiones de uso compartido de archivos: Esta opción se utiliza para que los datos que viajan a través de la red vayan encriptadas (cifradas), y puedes elegir entre cifrado de 128 bits, (mayor seguridad), o cifrados de 40 o 56 bits.

Uso compartido con protección con contraseña: Desactivado. Si se activa esta opción, únicamente pueden acceder a los recursos compartidos, usuarios de este equipo, o sea, que tengan una cuenta de usuario creada en el equipo, ya que para acceder a los recursos compartidos del equipo, es necesario especificar el nombre de usuario y la contraseña de un usuario que tenga una cuenta en el equipo que comparte los recursos. Es una opción de seguridad interesante, para gestionar el acceso a los recursos compartidos.

Carpetas compartidas.

Los permisos que se pueden establecer, sobre una carpeta compartida, pueden ser:

- **Lectura**: Únicamente permite a los usuarios ver y leer archivos, no permite realizar modificaciones en los mismos, borrarlos o guardar archivos en la carpeta.
- **Lectura y escritura**. Permite a los usuarios realizar cambios en los archivos, borrar archivos, modificar archivos, así como copiar archivos a la carpeta y crear nuevas carpetas.

Para compartir una carpeta en la red, para que todos los usuarios de la red, puedan tener acceso total a la carpeta. Tendrán derechos de lectura y escritura.

Para ello, haz clic, con el botón derecho sobre la carpeta creada. Y en el menú contextual, selecciona la opción propiedades. En la nueva ventana, pincha en la pestaña compartir. A continuación, en la pestaña compartir, haz clic en el botón Uso compartido avanzado. En la ventana de uso compartido avanzado, marca la casilla: "Compartir esta carpeta", y a continuación, haz clic en el botón permisos. En la ventana permisos, en el primer panel: Nombres de grupos o usuarios, aparecen "Todos", lo cuál indica que vas a compartir esta carpeta con todos los usuarios.

En el panel inferior, establece los permisos de acceso a la carpeta para los usuarios. Puesto que hemos dicho que deben tener acceso total, marca la casilla, "Control total (lectura y escritura)".

Una vez compartida, la carpeta en la red para que todos los usuarios tengan acceso total a la misma, puedes comprobar su visibilidad en la red.

Para ello, abre el explorador de Windows 7, y pincha en el icono red. A continuación, se muestran los equipos de la red, y también aparece nuestro propio equipo. Haz doble clic en nuestro equipo, y se muestran los recursos compartidos de nuestro equipo.

Unidades de red

Una vez que has compartido una carpeta en la red, y puedes tener acceso a la misma desde otro equipo de la red, es muy habitual en entornos laborales y domésticos, la creación de las denominadas unidades de red.

Una unidad de red consiste en crear en nuestro equipo una nueva unidad de almacenamiento como si de un nuevo disco duro se tratase. Puedes comprobar que en realidad, lo que almacenamos en ese nuevo disco o unidad, se almacena directamente en una determinada carpeta compartida de otro equipo que forma parte de la red. La información almacenada el la unidad de red, se encuentra físicamente en otro equipo.

Las unidades de red, son de gran utilidad para agilizar el trabajo en la red, ya que por ejemplo, en una oficina, si el administrativo, cada vez que acaba un documento, que debe traspasar al equipo de su jefe, tiene que abrir el explorador de archivos, seleccionar el icono red, esperar a que se muestren todos los equipos de la red, buscar el equipo de su jefe, entrar en él y buscar la carpeta compartida donde debe guardar el documento ,¡esto supone una gran perdida de tiempo!

Sin embargo, utilizando una unidad de red, puede guardar directamente el documento desde la aplicación con la que lo ha creado, exactamente igual que si lo guardase en una carpeta de su disco duro, ya que la unidad de red, es una unidad de almacenamiento más.

Si al crear la unidad de red, marcas la opción conectar de nuevo al iniciar sesión, la unidad se vuelve a crear automáticamente cada vez que el usuario inicia sesión. Hay que tener en cuenta, que si el equipo al que está conectada la unidad de red no está encendido, mostrará un error al conectar la unidad de red.

CASO PRÁCTICO

CARMINFO S. L. ha incorporado a dos nuevos trabajadores, Alberto y Marisa, que ayudarán a llevar a cabo los proyectos para los que es contratada la pequeña empresa.
La dueña de CARMINFO S. L. y la empleada más antigua, Laura, ya llevan un tiempo organizando la red de la empresa utilizando Active Directory.
Desde el principio, uno de sus objetivos fue que cada integrante de la organización pudiera iniciar sesión en Active Directory individualmente: cada persona con su propia cuenta de usuario. Por lo tanto, tendrán que crear, al menos cuatro cuentas de usuario.
Por otro lado, Carmen ha repartido las funciones entre sus empleados y empleadas, de modo que no todos tienen que utilizar los recursos de la empresa (impresoras, carpetas, espacio en disco, etc.) de la misma forma, por lo que sería interesante agrupar de alguna forma esas cuentas de usuario, en función del tipo de acceso a los recursos que necesitan.
Por todo ello, en CARMINFO S. L. tienen que:

- Crear cuentas de usuario.
- Agruparlas si tienen funciones similares.
- Repartir la administración de estas cuentas.
- Realizar todas estas funciones de una forma eficiente y profesional.

Cuentas de usuario de Active Directory.

CASO PRÁCTICO

Carmen quiere lograr un objetivo: que cada persona inicie sesión con su cuenta de usuario y que a cada persona se le puedan asignar permisos y derechos en el dominio.
Carmen considera la lista de personas que trabajan en la empresa: Carmen Martínez (ella misma), Laura García, Alberto Gómez y Marisa Fernández.
Piensa que sería conveniente que los nombres de las cuentas de usuario identifiquen claramente a sus propietarios, para evitar confusiones. Por eso, en función de sus nombres y apellidos, decide que creará cuentas de usuario con los siguientes nombres: *cmartinez*, *lgarcia*, *agomez* y *mfernandez* (primera letra del nombre y el apellido). Así, todos saben quién es quién.

Antes de empezar a gestionar cuentas de usuario, es recomendable que adquieras unos conocimientos sólidos sobre el tipo de objeto que estás manejando. En un entorno de Active Directory, existen los siguientes **tipos de cuentas de usuario.**

Clasificación de los usuarios.

En Active Directory podrás crear diferentes tipos de cuentas de usuario. Puedes probar esto abriendo la herramienta **Usuarios y Equipos de Active Directory** e intentando crear un usuario. No obstante, un poco más adelante te enseñaremos a crear cuentas de usuario. De momento, fíjate en la clasificación que aquí se hace.

1) **Usuario**: En AD (Active Directory – Directorio Activo) se manejan cuentas de usuario ***locales*** y cuentas de usuario *de* ***dominio***. Las locales son las que se utilizan en equipos que no están incorporados a un dominio. Por ejemplo, si acabas de instalar Windows 7 y aún no has hecho al equipo miembro de un dominio, al iniciar sesión en el equipo estás utilizando un cuenta de usuario local. Las cuentas de usuario local residen en el equipo al que pertenecen. No se puede iniciar sesión en el equipo PC-Laura con una cuenta de usuario local perteneciente al equipo PC-Carmen.

Si el equipo pertenece a un dominio, sigue siendo posible utilizar sus cuentas de usuario locales, pero aparece la posibilidad de iniciar sesión con las cuentas de usuario de dominio. Las cuentas de usuario de dominio residen en la base de datos de AD y son comunes para todos los equipos que pertenecen al dominio. Por ejemplo, si se crea la cuenta *cmartinez* en AD, esta cuenta sirve para iniciar sesión en todos los equipos del dominio.

2) **InetOrgPerson**: Éste es un tipo de usuario introducido en Windows Server 2003. Se utiliza para aportar compatibilidad con otros servicios de directorio diferentes a Active Directory pero que soporten el protocolo LDAP (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorio). También sirve para iniciar sesión en el dominio y se le pueden asignar permisos y privilegios, al igual que a las cuentas de tipo "usuario". Si alguna vez realizas una migración desde un servicio de directorio basado en LDAP a Active Directory, tendrás que manejar cuentas de este tipo.

3) **Contacto**: A veces puede ser interesante crear un cuenta para utilizarla únicamente como una cuenta de correo electrónico. Para ello, se crearía una cuenta de tipo "contacto". Este tipo de cuentas no se pueden utilizar para iniciar sesión en el dominio, ni se les pueden asignar permisos ni derechos. Es decir, no tienen información de seguridad asociada. Sin embargo, sí pueden pertenecer a grupos de distribución, como verás más adelante.

4) **Usuarios predeterminados**: Estas cuentas son creadas automáticamente cuando se configura un dominio en Active Directory. Si quieres ver cuáles son, basta con que en un controlador de dominio abras la herramienta "**Usuarios y equipos de Active Directory"** y examines el contenedor "Users". En el siguiente apartado profundizaremos en este tipo de cuentas.

Usuarios predeterminados.

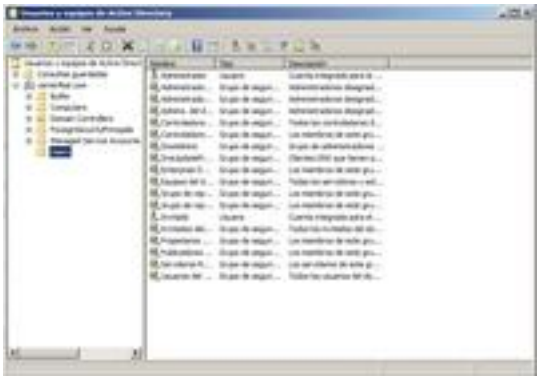
Como viste en anteriores apartados, las cuentas de usuario predeterminadas son aquellas que vienen “de serie”, es decir, que se crean cuando instalas el sistema. Las más importantes son:

Administrador: Es la cuenta que tiene todos los privilegios sobre el dominio. Puede asignar derechos y permisos a los usuarios del dominio. Debes utilizar esta cuenta únicamente para tareas que requieran privilegios administrativos. En otras palabras: cuando no te quede más remedio. Si te acostumbras a utilizar la cuenta de Administrador para trabajos normales, no administrativos, corres el riesgo de realizar alguna acción involuntaria que estropee algo. O peor aún, que un programa (o virus), corriendo en tu sesión, provoque daños importantes. Si normalmente trabajas con una cuenta no administrativa, no podrás causar daños graves, porque tu cuenta no tiene derechos o permisos suficientes.

Por defecto, la cuenta de Administrador es miembro de los siguientes grupos: Administradores, Admins. del dominio, Administradores de empresa (sólo si el dominio es el dominio raíz del bosque), Creadores y propietarios de Políticas de Grupo, Administradores de esquema y Usuarios del dominio. Todos estos son grupos predeterminados del dominio, de los que hablaremos en la sección.

La cuenta Administrador es la primera que se crea cuando configuras un nuevo dominio.

Si la cuenta de Administrador se deshabilita, todavía se puede iniciar sesión con ella en Modo Seguro.

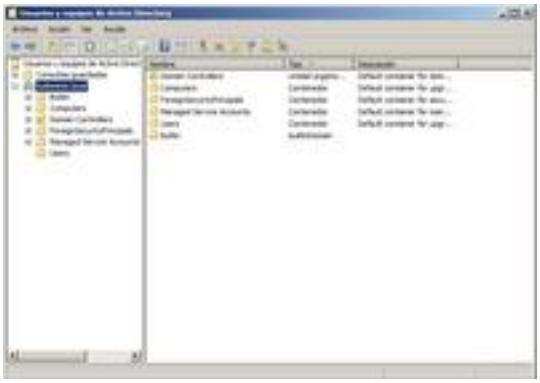


Invitado: Está pensada para que la utilicen las personas que no tienen una cuenta de usuario en el dominio. Está deshabilitada por defecto, ya que no es buena idea conceder acceso a personas ajenas a la organización. Por ello, sólo debe habilitarse en casos justificados. Para utilizarla no es necesario escribir una contraseña. A esta cuenta se le pueden conceder permisos y derechos como a cualquier otra cuenta. Por defecto, esta cuenta pertenece a los grupos Invitados e Invitados del Dominio.

Creación y eliminación de usuarios.

Crear un usuario es una operación muy sencilla. En un controlador de dominio, debes abrir la herramienta "Usuarios y Equipos de Active Directory", que se encuentra en "**Herramientas Administrativas**", dentro del "Panel de control".

Se abrirá un programa como el de esta imagen:



- Debes **elegir un contenedor** en el que crear los usuarios. Un poco más adelante aprenderás a crear tus propios contenedores, pero por ahora puedes elegir el contenedor "Users".

- Una vez elegido el contenedor, en el menú **"Acción"** eliges **"Nuevo"** y en el desplegable que aparece eliges "Usuario". En lugar del menú, también puedes utilizar el botón correspondiente en la barra de herramientas.

- Debes completar los campos que pide: nombre de pila, apellidos y nombre de inicio de sesión. El campo *Iniciales* sirve para indicar la inicial del segundo nombre. No es habitual utilizarlo en idioma castellano. De toda esta información, el nombre de inicio de sesión es el que identificará al usuario en el sistema. En la pantalla siguiente tendrás que especificar la contraseña y las opciones de usuario que desees.

En el siguiente vídeo puedes ver un ejemplo de creación de un usuario.

URL: SOR03_CONT_R06_CreacionUsuario.flv

Cuando el número de usuarios que hay que crear es muy grande, este proceso puede hacerse muy pesado. En esta unidad aprenderás una técnica para agilizar el trabajo: la utilización de plantillas.

Es conveniente que planifiques adecuadamente cómo vas a nombrar los usuarios. Las organizaciones crecen y cambian, y conviene tener un "esquema de nomenclatura", para que los nombres de usuario no se asignen aleatoriamente (lo que podría llevar a confusiones y repeticiones).

En las organizaciones pequeñas se suele utilizar el nombre y la inicial del primer apellido. Por ejemplo, Carmen Martínez sería *carmenm*. También se suele utilizar la inicial del nombre y el primer apellido completo (*cmartinez)*. En organizaciones más grandes, utilizarían el nombre completo (*carmenmartinez*). Incluso, se pueden utilizar puntos como separadores (*carmen.martinez*). Si existen varias personas con el mismo nombre, puede incluirse números (*carmen.martinez.01, carmen.martinez.02*). Lo importante es que el esquema sea coherente y adaptable.

Otra recomendación sobre nomenclatura es identificar las cuentas de usuario pertenecientes a trabajadores y trabajadoras temporales, mediante algún **prefijo**, por ejemplo, *tmp_jose.gonzalez*. De este modo, cuando el trabajador o la trabajadora ya no pertenezca a la empresa, es sencillo localizar la cuenta de usuario para inhabilitarla.

Para **eliminar un usuario**, lo único que debes hacer es seleccionar el usuario y pulsar "Supr", o elegir "eliminar" en el menú contextual.

Los nombres de usuario para cuentas de dominio deben ser únicas en Active Directory. Los nombres de inicio de sesión de usuario deben ser únicos en el bosque en el que se crea la cuenta de usuario.

Opciones de las cuentas de usuario.

A veces, necesitarás controlar el tipo de acceso al dominio que tendrá una cuenta de usuario. Para ello, utilizarás las opciones de las cuentas de usuario. Con estas opciones puedes, por ejemplo, configurar las horas en las que una persona puede iniciar sesión en el dominio, en qué equipos, durante cuánto tiempo estará activa su cuenta, etc.

Para acceder a las opciones de una cuenta determinada, debes hacer doble clic sobre ella en "Usuarios y Equipos de Active Directory". En lugar de doble clic, también puedes abrir el menú contextual (normalmente con el botón secundario del ratón) y elegir "**Propiedades**". A continuación puedes ver las opciones más relevantes y su significado.

Horas de inicio de sesión: Permite establecer los períodos de tiempo durante los cuales está permitido iniciar sesión.

Iniciar sesión en: Permite establecer en qué equipos del dominio está permitido iniciar sesión.

La cuenta está bloqueada: A veces, un usuario introduce su contraseña de forma errónea en varios intentos. Esto provoca el bloqueo de su cuenta. En este caso, esta casilla aparecerá habilitada. Para desbloquear la cuenta, un Administrador debe desmarcar esta casilla.

El usuario debe cambiar la contraseña en el próximo inicio de sesión: Si esta casilla está marcada, el sistema obligará al usuario a cambiar la contraseña la próxima vez que inicie sesión. Esto es muy útil para obligar a los usuarios y usuarias a cambiar la contraseña de vez en cuando, o a establecer una contraseña propia, desconocida para el administrador, la primera vez que utilizan el sistema.

El usuario no puede cambiar la contraseña: Si se marca, el usuario no puede cambiar su propia contraseña.

La contraseña nunca caduca: Hace que, para esta cuenta de usuario, no se tenga en cuenta el tiempo de caducidad de la contraseña. Si no está marcada esta opción, el usuario o la usuaria estará obligado a cambiar la contraseña cada cierto tiempo.

Almacenar la contraseña utilizando cifrado reversible: Algunos sistemas operativos, como por ejemplo los de Apple, pueden almacenar las contraseñas en texto plano. En caso de tener ese tipo de sistemas en nuestro dominio, activaríamos esta opción.

La cuenta expira: Si se establece una fecha de expiración, la cuenta se deshabilitará automáticamente llegado ese día. Útil para limitar la duración de las cuentas de los empleados y empleadas temporales.

REFLEXIONA

¿Qué crees que es mejor, que el administrador o administradora conozca las contraseñas de los usuarios y usuarias o que no las conozca? Si tu respuesta es la segunda opción, estás en lo cierto. El administrador o administradora siempre podrá cambiar las contraseñas de los usuarios y usuarias, pero no debe conocerlas. Imagina que una persona tiene la misma contraseña en el dominio y en su cuenta de Facebook. ¿Te parece adecuado que el administrador o administradora del dominio pueda "probar suerte" a ver si por casualidad puede entrar en la cuenta de Facebook de esa persona? Por eso, al crear un usuario, es importante marcar la opción "el usuario debe cambiar la contraseña en el próximo inicio de sesión".

Perfiles de usuario.

CASO PRÁCTICO

En CARMINFO S. L. se han creado los usuarios *cmartinez, lgarcia*, *agomez* y *mfernandez*. Gracias a eso, los cuatro integrantes de la empresa (Carmen, Laura, Alberto y Marisa) pueden iniciar sesión en todos los equipos utilizando siempre su nombre de inicio de sesión y su contraseña.
Sin embargo, han observado que si cambian el fondo de escritorio, o los iconos del menú inicio, estos cambios sólo quedan almacenados en el equipo donde los han efectuado. Si al día siguiente utilizan otro equipo, tendrán diferente fondo de escritorio y diferente configuración del menú inicio.
A todos les gustaría poder contar con la misma configuración de escritorio y de menú inicio, independientemente del equipo en el que inicien sesión.
Otro problema con el que se encuentran es que cuando guardan archivos en las carpetas locales, no pueden acceder a ellas si se sientan en otro equipo.

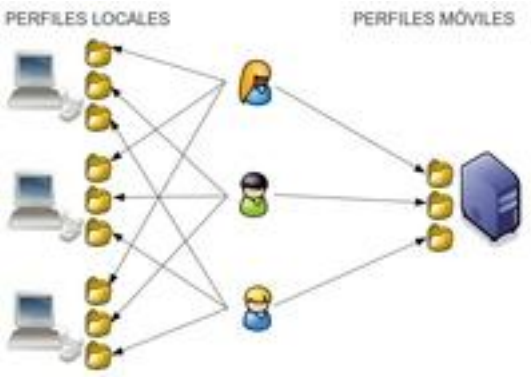
El **perfil** de un usuario contiene opciones globales e información de configuración, normalmente referidos al escritorio, la barra de tareas y el menú inicio. Cuando un usuario cambia el aspecto, comportamiento, etc. de alguno de estos elementos, esos cambios se almacenan en su perfil.
En los siguientes apartados aprenderás a establecer diferentes tipos de perfiles para los usuarios.

Características de los perfiles.

Probablemente, hasta ahora no te lo habías planteado, pero cada vez que inicias sesión en tu equipo con tu cuenta de usuario, se carga tu configuración, tu perfil, de forma que cada vez que accedes al sistema, éste te ofrece un aspecto y comportamiento idéntico. El perfil se crea la primera vez que un usuario inicia sesión (por eso, la primera vez que un usuario inicia sesión en un equipo, el proceso es bastante lento).
Cada usuario tiene su propio perfil, de forma que el aspecto del escritorio, barra de tareas y menú inicio es distinto para cada usuario. Existen tres tipos de perfiles:

- Por defecto, los perfiles se almacenan de forma **local**. Esto significa que el perfil se crea y almacena en el equipo en el que el usuario inicia sesión. Los cambios que realice quedan almacenados en dicho equipo y no estarán disponibles cuando se inicie sesión en un equipo diferente. Es lo que les pasa a los integrantes de CARMINFO S. L. en el caso práctico. Una clara desventaja es que los usuarios no tienen acceso a su configuración habitual si cambian de equipo. Otra es que se crean varios perfiles para cada usuario: uno en cada equipo en el que el usuario haya iniciado sesión. Esto ocupa espacio de almacenamiento.

- Cuando se trabaja en un dominio, es muy habitual configurar **perfiles móviles**. Estos se almacenan en una carpeta compartida en red, de forma que están disponibles desde cualquier equipo del dominio. Esto presenta varias ventajas:
    1. Sólo existe un perfil para cada usuario: el que está en la carpeta compartida.
    2. Los cambios que el usuario realiza en su perfil están disponibles independientemente del equipo en el que inicie sesión.



Tanto el perfil local como el perfil móvil pueden convertirse en **perfil obligatorio**. Este perfil no permite realizar cambios o, mejor dicho, no los almacena. Si un usuario con perfil obligatorio cambia el fondo de escritorio, por ejemplo, este cambio no quedará guardado. En el siguiente inicio de sesión, encontrará el mismo fondo de escritorio de siempre.

Cómo crear un perfil móvil y conectar con una unidad de red.

En el siguiente vídeo puedes ver el proceso completo para crear un perfil móvil y para que el usuario tenga acceso automático a una unidad de red. Es recomendable que veas el vídeo, después leas el apartado y después vuelvas a ver el vídeo para corroborar lo que se te explica.

Texto enlace: Establecimiento de un perfil móvil.
URL: SOR03_CONT_R10_PerfilMovil.flv

Para crear un **perfil móvil** lo primero que hay que hacer es crear una carpeta compartida en la que ubicarlo. Lo normal es que en el dominio exista un servidor de archivos con al menos una carpeta dedicada a almacenar los perfiles de todos los usuarios. La estructura sería como la reflejada en la figura.

No es necesario crear cada carpeta individual. Windows Server las creará automáticamente. Sólo es necesario crear la carpeta PERFILES (puede tener cualquier otro nombre) y compartirla en red. Ojo, hay que dar permiso de Lectura y Escritura al grupo "Usuarios del dominio" y de control total a Admins. del dominio.

Una vez hecho esto, accedemos a las propiedades del usuario y pulsamos en la pestaña "Perfil". En ella, tenemos varios cuadros de texto. Para nuestro propósito, modificaremos los siguientes:

- **Ruta de acceso al perfil**: En este cuadro de texto pondremos la ruta de red de la carpeta que compartirá el perfil. Supón que el equipo en el que se encuentra la carpeta PERFILES se llama *servidorficheros.carminfosl.com*. Imagina también que el nombre compartido de la carpeta PERFILES es su nombre compartido por defecto, es decir, PERFILES. Ahora, imagina que establecemos la ruta de acceso al perfil para el usuario *cmartinez*. Entonces, la ruta completa de acceso al perfil sería:

\\servidorficheros.carminfosl.com\PERFILES\cmartinez

Siendo, por lo tanto, una subcarpeta de la carpeta compartida PERFILES. Con esto, ya has configurado un *perfil móvil*, ya que cada vez que este usuario inicie y cierre sesión, utilizará el perfil que se almacena en la carpeta de red, por lo que estará accesible desde cualquier ordenador del dominio.

- **Conectar... a**: Esta característica es muy útil para que los usuarios puedan ubicar sus datos cómodamente en un recurso de red. Lo que se suele hacer es lo siguiente: En un servidor de ficheros, se crea una carpeta compartida para almacenar los archivos de los usuarios. La estructura sería como la de la figura, en la que se ha creado una carpeta llamada DATOS (puede tener cualquier nombre) y se ha compartido en red.

Una vez hecho esto, en el cuadro de texto "Conectar… a" se escribe la ruta de red de la subcarpeta del usuario. Si se trata del usuario *cmartinez*, y el equipo se llama *servidorficheros.carminfosl.com*, tendrás que escribir:

\\servidorficheros.carminfosl.com\DATOS\cmartinez

Además, en el cuadro desplegable podrás seleccionar la letra de unidad que desees. **Por defecto, la Z:** Con esta acción, lograrás que cuando el usuario inicie sesión en cualquier equipo del dominio, en "Mi PC" o "Equipo" aparezca una unidad (Z: o la letra que hayas elegido) que apunta directamente a la ruta de red especificada. Todo lo que el usuario guarde en esa unidad se estará guardando en la ubicación de red, por lo que estará disponible desde cualquier equipo del dominio.

Es aconsejable orientar a los usuarios del dominio para que guarden su información importante en dicha unidad, de forma que resida en el servidor de ficheros y no en cada equipo localmente. Es mucho más fácil programar copias de seguridad para un solo equipo (el servidor de ficheros) que para todos los discos duros de todos los equipos del dominio.

Cómo convertir un perfil en obligatorio.

Si no quieres que los usuarios puedan realizar cambios en su escritorio, debes convertir el perfil en obligatorio. Se trata de un proceso sumamente sencillo: consiste simplemente en cambiar el nombre de un fichero. La única complicación consiste en tomar posesión de la carpeta del perfil. En la siguiente animación puedes encontrar el proceso detallado.

Texto enlace: Establecimiento de un perfil obligatorio.
URL: SOR03_CONT_R13_PerfilObligatorio.odp

Esta configuración es útil en entornos controlados, en los que el usuario está muy limitado. Como cualquier cosa, el uso de perfiles obligatorios tiene ventajas e inconvenientes.

Ventajas:

- Como el perfil obligatorio es de sólo-lectura, puedes utilizar el mismo perfil obligatorio para un gran número de usuarios, con lo que ahorras espacio de almacenamiento y haces la gestión del perfil mucho más simple.
- Los usuarios no pueden contaminar el entorno de escritorio. Al iniciar sesión, todo vuelve a estar limpio y ordenado, como al principio.
- Como los perfiles obligatorios no contienen datos específicos de usuario, su tamaño es reducido. Esto hace que el proceso de inicio de sesión, durante el que se trasmiten los datos de perfil por la red, sea mucho más corto que si se trata de perfiles móviles con muchos datos (por ejemplo, con archivos grandes en el Escritorio).

Desventajas:

- A todo el mundo le gusta personalizar su ambiente de trabajo de alguna forma: cambiando el fondo de pantalla o el tema de Windows. Como ya hemos comentado, los perfiles obligatorios eliminan esta posibilidad. Esto sólo es una desventaja si no es lo que se pretende, claro está.
- Algunas aplicaciones (muy pocas, eso sí) no funcionan correctamente con perfiles obligatorios, por lo que hay que probar todo el software que se va a utilizar.
- Si dejas algo "mal" en el perfil obligatorio (por ejemplo, si no pones un acceso directo en el escritorio a un programa que los usuarios o usuarias utilizan mucho), te molestarán hasta que lo arregles. Y eso te llevará tiempo y trabajo.

Por lo tanto, antes de establecer una política de perfiles obligatorios, tienes que **valorar los pros** y los **contras**, y tomar la decisión más adecuada. Recuerda que no tienes que hacer cosas sólo porque sepas hacerlas.

Grupos en Active Directory.

CASO PRÁCTICO

En CARMINFO S. L. se han creado los usuarios *cmartinez*, *lgarcia*, *agomez* y *mfernandez*. Ahora, Carmen se da cuenta de que existen ciertos datos (en concreto el tema de contabilidad y gestión económica) a los que sólo deben tener acceso Laura y ella, pero no Alberto y Marisa. Además, quiere ser la única que pueda crear y eliminar cuentas de usuario en el dominio.

Meditando sobre este asunto, se da cuenta de que puede agrupar a los cuatro integrantes de la empresa de la siguiente forma, según sus funciones en la empresa y acceso a recursos:

- Alberto y Marisa: acceso básico a ciertos datos y sin tareas administrativas en el dominio.
- Carmen y Laura: acceso total a ciertos datos.
- Sólo Carmen: acceso total a las tareas administrativas del dominio.

Carmen charla con Laura sobre este asunto:
-Laura, cada vez vamos siendo más personas en esta empresa. La idea de instalar Active Directory iba bien encaminada, ¿no te parece?
-Sí. Al principio yo no lo veía muy claro, pero es evidente que ha sido buena idea. Ya tenemos la infraestructura preparada para la incorporación de nuevas personas.
-Vamos a crear cuentas de usuario para Alberto y Marisa, para que puedan iniciar sesión en el dominio. Y también vamos a crear grupos, porque no todos usaremos los recursos del mismo modo.
-Es lo lógico.

Los grupos en Active Directory son objetos que pueden contener: otros grupos, usuarios, equipos y otros recursos, como archivos, directorios y listas de distribución de correo electrónico, entre otros.

Para que puedas planificar correctamente los grupos de una red, tienes que comprender adecuadamente sus dos características principales: el **tipo** y el **ámbito**.

Clasificación de los grupos.

Es importante que entiendas bien la clasificación de los grupos. ¿Por qué? Porque si comprendes bien las características de cada grupo, sabrás elegir qué tipo o ámbito de grupo debes usar en cada momento. Y saber hacer esa elección correctamente es propio de un buen administrador de Active Directory.

En lo referente al **tipo**, existen dos posibilidades:

- **Grupos de seguridad**: se utilizan para controlar el acceso a los recursos. Es el tipo de grupo que utilizarás habitualmente. Además, son "parecidos" a los grupos locales, que son los que probablemente ya habrás utilizado en sistemas operativos monopuesto, como Windows 7. Se llaman "de seguridad" porque se utilizan para controlar el acceso a los recursos. Por ejemplo, puedes decidir que un grupo de seguridad de tu red, *recursoshumanos*, pueda imprimir en la impresora *laser*, pero no administrar trabajos de impresión.
- **Grupos de distribución**: este tipo de grupos nada tiene que ver con el control de acceso a los recursos. Se trata de listas de distribución de correo electrónico. Son útiles para integrarlos con un servidor de correo: por ejemplo, Microsoft Exchange.

En este módulo aprenderás a manejar los grupos de seguridad, por lo que en los próximos apartados nos centraremos exclusivamente en ellos.

En lo relativo al **ámbito**, existen tres posibilidades:

- **Grupos locales de dominio.**
- **Grupos globales.**
- **Grupos universales.**

En los subsiguientes apartados profundizaremos en estos tres ámbitos de grupos. También hablaremos de los **grupos predeterminados**, que son aquellos que "vienen de serie", es decir, que se crean automáticamente al instalar el sistema. Estos grupos predeterminados que vas a conocer son de seguridad, no de distribución, y los encontrarás de varios ámbitos diferentes.

Grupos locales de dominio.

Antes de decirte qué características tiene esta clase de grupos, debes aprender algo mucho más importante:

Utiliza grupos locales de dominio para conceder permisos de acceso a los recursos del dominio en el que estás creando dichos grupos.

Seguro que lo entiendes mejor con un ejemplo: piensa en la impresora láser de CARMINFO S. L. Dicha impresora pertenece al dominio *carminfosl.com*, y su nombre es *laser*, por lo que su **FQDN** (Fully Qualified Domain Name - Nombre cualificado completo de dominio) es ***laser.carminfosl.com*.**

Ahora supón que se desea que algunos usuarios de *carminfosl.com* (aún no nos importa cuáles) puedan imprimir y administrar trabajos de impresión y que otros sólo puedan imprimir. Aquí es donde entran en juego los grupos locales de dominio. En un ejemplo como éste, lo primero que has de hacer es crear dos grupos locales de dominio. A uno de ellos lo llamarás, por ejemplo, *Impresores*, y al otro *Adminslaser*.

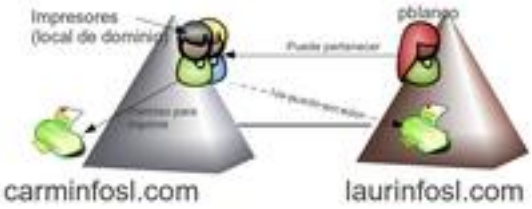
Después, concederás permisos de impresión a ambos grupos y permisos para administrar los trabajos de impresión exclusivamente a *Adminslaser*.
Más adelante, manejando la pertenencia a grupos, harás que las personas que deban administrar trabajos pertenezcan a *Adminslaser* y las personas que sólo puedan imprimir pertenezcan a *Impresores*.

El modo de asignar permisos correctamente lo aprenderás en la siguiente unidad, pero de momento, debes saber que los grupos locales de dominio se utilizan para conceder permisos sobre los recursos locales del dominio.

Ahora piensa una cosa: ¿qué pasa si queremos que a un recurso local puedan acceder usuarios de otros dominios del bosque? Ningún problema: seguiremos la misma estrategia: los permisos se los daremos **solamente** a los grupos locales de dominio. Lo bueno de estos grupos es que pueden contener **miembros de cualquier dominio del bosque.**

Un grupo local de dominio puede contener miembros de cualquier dominio del bosque y se le pueden asignar permisos sólo sobre recursos de su propio dominio.

Imagina el bosque formado por *carminfosl.com* y *laurinfosl.com*. Si quieres que el usuario *pblanco@laurinfosl.com* imprima sobre *laser.carminfosl.com*, harás que *pblanco* pertenezca al grupo *Impresores* de *carminfosl.com*. Siendo estrictos, no debes hacer pertenecer directamente a *pblanco*, sino a un grupo global al que pertenezca ese usuario. Te hablaremos de esto en el siguiente apartado.



Por otro lado, sería imposible conceder al grupo local de dominio *Impresores*, perteneciente a *carminfosl.com*, algún tipo de permiso sobre un recurso de *laurinfosl.com*.

Grupos globales.

Para esta clase de grupos, también tenemos una frase importante:

Utiliza grupos globales para agrupar usuarios o recursos de forma similar a como están agrupados en la organización.

Por ejemplo, si en la organización a la que pertenece el dominio existe un departamento de Ventas y otro de Desarrollo, es muy recomendable que crees sendos grupos globales con esos nombres: *Ventas* y *Desarrollo,* y hagas pertenecer a ellos a los usuarios del dominio pertenecientes a cada departamento.

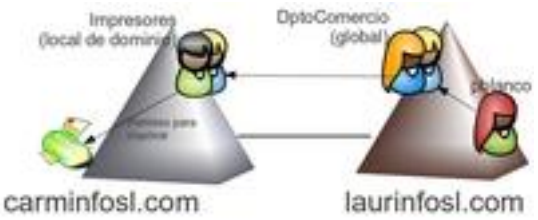
De esta manera, podrás administrar necesidades comunes que surgen en las organizaciones. Es muy posible que los miembros del departamento de Ventas necesiten acceder a ciertas carpetas a las que no deben tener acceso los de Desarrollo y viceversa. Por eso es lógico agrupar a la gente que pertenece al Departamento de Ventas, por un lado, y por otro lado, a la gente que pertenece al Departamento de Desarrollo.

Un grupo global puede contener usuarios y equipos que sean sólo de su propio dominio y se le pueden asignar permisos sobre recursos de cualquier dominio del bosque.

¿Para qué utilizar los grupos globales? Los utilizarás en combinación con los grupos locales de dominio. Piensa en el ejemplo del apartado anterior, con el árbol formado por *carminfos.com* y *laurinfosl.com*.

El objetivo final es que *pblanco* pueda imprimir en la impresora del dominio *carminfosl.com*. Ahora bien, lo más lógico es que en su propia organización, LAURINFO S. L., *pblanco* (Paloma Blanco) pertenezca a una división o departamento, por ejemplo, al Departamento de Comercio. En ese caso, lo más habitual es que no sólo Paloma Blanco, sino todo el departamento, pueda imprimir en la impresora de *carminfosl.com* (para enviar copias impresas a CARMINFO S. L.).

¿Cómo organizarías este supuesto? Lo has adivinado: utilizando **grupos globales**. Crearías un grupo global en *laurinfoslo.com* llamado *DptoComercio*, o algo parecido, en *laurinfosl.com*. Todos los usuarios de los trabajadores de ese departamento serían miembros de ese grupo, incluida Paloma Blanco, *pblanco*. Después, en el dominio *carminfosl.com* editarías las propiedades del grupo local de dominio *Impresores* y **harías miembro al grupo *DptoComercio* de *laurinfosl.com* del grupo *Impresores* de *carminfosl.com***.



De esta forma, no sólo Paloma Blanco, sino todo el Departamento de Comercio, puede imprimir en la impresora del dominio *carminfosl.com*.

Este es un esquema habitual para la utilización de grupos globales y grupos locales de dominio. En la siguiente unidad, profundizaremos en la forma de utilizar los grupos para conceder permisos de acceso a los recursos.

Grupos universales.

Con estos grupos debes tener "autocontrol". ¿Por qué? Porque los grupos universales tienen muy pocas restricciones. Eso puede resultar un "atajo" muy tentador para los administradores, porque se pueden utilizar para todo en todos los dominios del bosque. Por ejemplo, se puede hacer miembro de un grupo universal a cualquier usuario de cualquier dominio del bosque, independientemente del dominio al que pertenezca.

Sin embargo, no es nada recomendable que utilices grupos universales como la principal forma de agrupar usuarios, otros grupos y equipos. ¿Por qué? Porque tiene inconvenientes importantes. El principal es que la información sobre los grupos universales se almacena en el **catálogo global**. Bueno, y ¿qué es el catálogo global? Es una porción de la información de la base de datos de Active Directory que es común a todos los dominios del bosque y que, por lo tanto, se replica por todos los dominios. Para ello, algunos controladores de dominio funcionan también como **servidores de catálogo global**.

Entonces, cada vez que se hace un cambio en las propiedades de un grupo universal, este cambio tiene que replicarse por todo el bosque, es decir, este cambio tiene que ser almacenado en todos los servidores de catálogo global. Si el bosque es grande y si abarca diferentes ubicaciones geográficas (con el consecuente retardo en las comunicaciones), este puede ser un proceso muy lento.

En las últimas versiones de Windows Server (en la versión 2008 y en la versión 2008 R2), se ha mejorado el sistema de replicación, por lo que la utilización de grupos universales no es tan desaconsejable como antes. Pero de todos modos, es mejor utilizarlos solamente cuando corresponde.

¿Y en qué casos sí es recomendable utilizarlos? En ejemplos como el de la figura. Se trata del árbol de dominios llamado *garabato.es*. Existen varios dominios que pertenecen a él y, en cada dominio, existe un grupo *global* llamado *DPTODesarrollo*. Los trabajadores y trabajadoras de los departamentos de desarrollo de las diferentes delegaciones (Santander, Sevilla, Valencia...) pertenecen al grupo global *DPTODesarrollo* de su dominio.

Se desea que TODOS los trabajadores y trabajadoras que trabajen en algún departamento de desarrollo de la corporación GARABATO puedan imprimir en la impresora del dominio *santander.garabato.es*. ¿Cómo llevarías a cabo este esquema?

Lo lógico es, como ya hemos visto, crear un grupo *local de dominio* llamado *Impresores* y concederle permisos de impresión. A continuación, podrías hacer miembros del grupo *Impresores* a todos los grupos globales llamados *DPTODesarrollo* de las distintas delegaciones. Sin embargo, es mucho más práctico crear un grupo *universal* llamado, por ejemplo, *Desarrolladores* y hacer miembro de él a todos los grupos *globales* llamados *DPTODesarrollo* de todos los dominios. Después, harías miembro a *Desarrolladores* de *Impresores*.

Grupos predeterminados.

Hemos incluido este apartado para que conozcas qué grupos están disponibles desde el momento en el que se instala Active Directory. Es decir, los grupos predeterminados son aquellos que ya están creados, sin necesidad de que lo hagas tú.

Como ya están creados, puedes verlos en la herramienta "Usuarios y equipos de Active Directory", en los contenedores "Users" y "Builtin", tal y como se ve en la figura.

Los grupos predeterminados más utilizados son:

- **Usuarios del dominio:** Es un grupo global. Sus miembros son, por defecto, todos los usuarios que se van creando en el dominio. No tienen ningún tipo de privilegio administrativo.
- **Administradores**: Es un grupo local de dominio. Los miembros de este grupo controlan por completo todos los controladores del dominio. De forma predeterminada, los grupos Administradores del dominio y Administradores de empresa son miembros del grupo Administradores. La cuenta Administrador es miembro de este grupo de forma predeterminada. Puesto que este grupo controla por completo el dominio, ten cuidado con los usuarios a los que haces miembro de este grupo.
- **Admins. del dominio:** Es un grupo global. Sus miembros tienen máximos privilegios en todo el dominio. Ojo: sobre el dominio, no sobre el árbol ni el bosque. Por defecto, el usuario *Administrador* del dominio pertenece a este grupo. Ten en cuenta que el nombre de este grupo es tal y como está escrito, con la abreviatura "Admins." en lugar de "Administradores".
- **Administradores de empresa:** Es un grupo universal. Reside en el dominio raíz del bosque. Sus miembros tienen los máximos privilegios sobre todos los dominios del bosque, por lo que debes tener mucho cuidado al decidir quién pertenece a ese grupo. Ten en cuenta que también se puede traducir por "Administradores de organización", término que se utiliza en muchos libros y manuales. Por defecto, el usuario *Administrador* del dominio raíz del bosque pertenece a este grupo.

PARA SABER MÁS

Tienes más información sobre grupos predeterminados de Active Directory en el siguiente enlace.

Texto enlace: Grupos predeterminados de Active Directory.
URL: http://technet.microsoft.com/es-es/library/cc756898%28WS.10%29.aspx

Creación y eliminación de grupos.

Ahora que ya sabes todo lo necesario sobre los tipos y ámbitos de los grupos, sólo queda que aprendas a crearlos. En realidad, se trata de un proceso evidente e inmediato. El verdadero reto al que te puedes enfrentar a la hora de organizar grupos en Active Directory es decidir cuántos grupos, de qué ámbito, etc. vas a crear, así como establecer las membresías y los permisos.

En la siguiente presentación encontrarás los pasos necesarios para crear grupos, añadir y quitar miembros y eliminar grupos.

Texto enlace: Gestión de grupos en Active Directory.
URL: SOR03_CONT_R23_PresentacionGrupos.odp

Utilización de plantillas.

CASO PRÁCTICO

No hace mucho tiempo, la corporación GARABATO contrató a CARMINFO S. L. para realizar algunas tareas de administración informática. Ahora, se han vuelto a poner en contacto con la empresa de Carmen. El motivo es que han creado tres departamentos nuevos, con veinte trabajadores cada uno, en su delegación de Santander. Le encargan a CARMINFO S. L. la creación y configuración de las cuentas de usuario en Active Directory para estos nuevos trabajadores. Carmen charla con Alberto sobre el tema.

- Alberto, ¿te ves capacitado para hacerlo tú?
- Sí, Carmen, pero ya estamos hasta arriba de trabajo. Y hay que crear nada menos que sesenta usuarios. Eso me llevará por lo menos cuatro horas.
- No, no tiene por qué llevarte tanto tiempo.
- Es que no es sólo crear el usuario, Carmen. También tenemos que agregarle a diferentes grupos, poner la ruta de acceso al perfil, poner la ruta para conectar la unidad de red... Es todo el rato lo mismo, pero lleva mucho tiempo escribirlo cada vez, incluso utilizando copiar y pegar...
- A ver, Alberto... ¿nunca te han enseñado a utilizar plantillas?

El caso de Alberto es común: tener que crear muchos usuarios puede convertirse en una pesadilla si hay que modificar muchas de sus propiedades, como el nombre, los apellidos, la pertenencia a grupos, las rutas de acceso al perfil y a la unidad de red, etc.

Creación de usuarios mediante plantillas.

Es probable que alguna vez te encuentres en la misma situación que Alberto: tener que crear un montón de cuentas de usuario. Es más, la cosa podría ser aún peor. Podrías tener que crear cientos de cuentas de usuario de golpe. Por ejemplo, si se está implantando un sistema nuevo en una empresa. ¿Cómo lo abordarías?

Para cantidades realmente ingentes de usuarios, lo que un administrador de sistemas debe hacer es utilizar algún lenguaje de **script** (guión) que le permita escribir un programa que tome los datos de algún listado o base de datos y genere los comandos necesarios para crear los usuarios con las propiedades adecuadas.

PARA SABER MÁS

Si te interesa esta opción, debes informarte sobre la herramienta PowerShell, algo que puedes hacer en el siguiente enlace:

Texto enlace: Creación de usuarios mediante script.
URL: http://geeks.ms/blogs/amazzite/archive/2008/07/13/creaci-243-n-y-modificaci-243-n-de-usuarios-de-active-directory-con-powershell-bulk-users.aspx

No obstante, si la cantidad de usuarios no es enorme, puedes abordar la creación de usuarios de forma manual. La utilización de plantillas te ahorrará mucho trabajo si eliges este método. Una plantilla es, en realidad, un usuario normal y corriente. Lo que harás es crear un usuario del modo habitual y asignarle todas las propiedades que sean comunes a cierto número de usuarios: por ejemplo, a qué grupos pertenece, las rutas de acceso a sus datos, etc.
Una vez configurado este usuario, **se *copia,*** lo que crea automáticamente un usuario con las mismas características, excepto el nombre de usuario y la contraseña.
Para personalizar las rutas de acceso a perfil y datos, es muy útil la utilización de la variable de entorno **%username%,** que se sustituye por el nombre de usuario.
En el siguiente vídeo puedes ver el proceso de creación de una plantilla y cómo se pueden crear varios usuarios a partir de ella.

Texto enlace: Creación de usuarios mediante plantilla.
URL: SOR03_CONT_R26_UtilizacionPlantilla.flv

No olvides desactivar el usuario plantilla cuando hayas acabado. No conviene dejar usuarios disponibles sin asignar a ninguna persona, pues puede representar un agujero de seguridad.

Organización de los elementos en un dominio.

CASO PRÁCTICO

La corporación GARABATO, ha subcontratado por tiempo indefinido a la empresa CARMINFO S. L. para realizar tareas de administración informática en la sede de Santander.
Dicha corporación, cuenta con un bosque en el que se encuentra el dominio *santander.garabato.es*. Los responsables de GARABATO han decidido que los trabajadores de CARMINFO S. L. deben tener ciertos privilegios administrativos en ese dominio, en concreto en todo lo referente a los departamentos de Edición y Comercial, pero no quieren hacerlos pertenecer al grupo *Admins. del dominio*, porque eso significaría que tendrían demasiado poder sobre todos los elementos del dominio.

Aportando ideas para solventar la cuestión, Carmen propone la creación de una unidad organizativa en el dominio, dentro de la cual los miembros de CARMINFO S. L. puedan realizar gestiones, y fuera de la cual no puedan hacer nada.

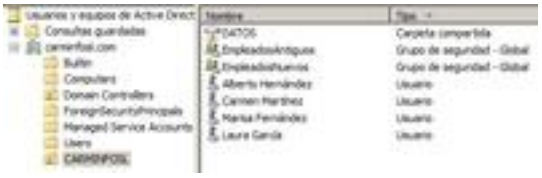
Unidades Organizativas.

Cuando abres la herramienta "Usuarios y equipos de Active Directory", puedes ver que en la parte izquierda se despliega una **estructura de árbol** en la cual se encuentra, como raíz, el dominio. En un nivel jerárquicamente inferior, dentro del dominio, puedes ver varios contenedores. Los más importantes son:

- **Builtin** (en español: predeterminado): en este contenedor se encuentran los grupos predeterminados locales de dominio.
- **Computers** (en español: computadoras): aquí encontrarás los equipos que hayas unido al dominio.
- **Domain controllers** (en español: controladores de dominio): en este contenedor encontrarás los equipos que hayas configurado como controladores de dominio.
- **Users** (En español: usuarios): aquí encontrarás los grupos predeterminados globales y universales, así como los usuarios predeterminados, como por ejemplo, el Administrador.

Cuando se añades elementos al dominio, puedes elegir cualquiera de estos contenedores. Sin embargo, suele ser preferible crear nuestros propios contenedores, porque tienen ventajas añadidas. Estos contenedores que crearás tú se llaman **Unidades Organizativas (UO)**. Para crear una, sitúate en el contenedor que desees, o directamente sobre el dominio y utiliza el menú contextual para seleccionar **Nuevo → Unidad organizativa**. También puedes utilizar el botón correspondiente de la barra de herramientas. Decide un nombre para la misma, y ya está.

Dentro de una unidad organizativa podemos colocar: impresoras, carpetas compartidas, computadoras, usuarios, grupos, otras unidades organizativas, etc. En la figura, tienes un ejemplo de una unidad organizativa que contiene usuarios, grupos y una carpeta compartida.



Aparte de que las utilizarás para tener ordenados los recursos en el dominio, lo realmente bueno de las unidades organizativas es que sirven para ***delegar la administración*.**

En la unidad de la figura, se puede conceder privilegios a un grupo o usuario **sólo** dentro de la unidad organizativa. De esa forma, se puede controlar sobre qué partes del dominio puede un usuario o un grupo tener algún tipo de control. Es decir, se puede hacer que un usuario pueda crear, eliminar y editar usuarios, grupos, equipos, etc. **dentro** de una unidad organizativa y que, sin embargo, no pueda hacer absolutamente nada fuera de ella.

En el siguiente vídeo tienes un ejemplo de cómo se delega la administración sobre una unidad organizativa.

Texto enlace: Delegación de la administración sobre una UO.
URL: SOR03_CONT_R29_DelegacionAdministracionUO.flv

Ejemplo completo de configuración de usuarios, grupos y equipos.

CASO PRÁCTICO

El alcalde de Villapedrusco ha requerido los servicios de CARMINFO S. L. El ayuntamiento está formado por las pedanías de Villapedrusco de Suso y Villapedrusco de Yuso. Para organizar los recursos informáticos del municipio, Carmen propone al alcalde la instalación de un dominio en Active Directory y la incorporación al mismo de los equipos e impresoras de los que dispone el Ayuntamiento. Estos equipos e impresoras se encuentran repartidos entre las pedanías y el edificio del Ayuntamiento.

Marisa, que colabora con Carmen en este proyecto, se informa de todas las personas que deben acceder a los equipos informáticos y le sale la siguiente lista:

- Francisco Pacheco: el Alcalde.
- Susana Rebolledo: Alcaldesa de la pedanía de Villapedrusco de Yuso.
- José Luis Benito: Alcalde pedáneo de Villapedrusco de Suso.
- Rebeca Garrido, Tomás Jiménez, Raquel Heredia y Juan Antonio Sánchez: Concejales.
- Esteban García: Secretario del ayuntamiento.

En principio, se desea que todas estas personas puedan iniciar sesión en el dominio. El Alcalde no ha aclarado aún qué tipo de permisos debe tener cada uno sobre carpetas e impresoras, pero lo indicará pronto. Con toda esta información, Carmen y Marisa se ponen a trabajar.

Resolución del problema.

En este apartado te vamos a plantear una posible configuración del dominio que tienen que instalar Carmen y Marisa. Habría que seguir estos pasos:

1. Elegir un nombre para el dominio. A poder ser, que ese nombre corresponda con un nombre DNS (Domain Name System – Sistema de nombres de dominio) adquirido por la organización. Por ejemplo: *villapedrusco.com.*
2. En un equipo con Windows Server 2008 R2, se ejecuta el asistente *dcpromo* para la instalación de los servicios de Active Directory, instalando, por lo tanto, el dominio *villapedrusco.com*.
3. **UNIDADES ORGANIZATIVAS**: Para organizar mejor los recursos, conviene crear una Unidad Organizativa para almacenar todo lo relacionado con este dominio. La llamarías VILLAPEDRUSCO. Dentro de esta UO y previendo un posible crecimiento de la infraestructura informática, convendría crear dos UOs: YUSO y SUSO.
4. **GRUPOS**: En la UO VILLAPEDRUSCO, también crearíamos los grupos globales *Concejales*, *AlcaldesPedaneos*, *Alcaldes* y *PAS*. Este último grupo representa el personal de administración y servicios (que actualmente se reduce al secretario, pero que podría aumentar. Se hace al grupo *AlcaldesPedaneos* miembro del grupo *Alcaldes*.
5. **USUARIOS**: En la UO VILLAPEDRUSCO, se crearían los usuarios *rebeca.garrido*, *tomas.gimenez*, *raquel.heredia*, *juanantonio.sanchez* y se les haría miembros del grupo *Concejales*. También se crearía el usuario *francisco.pacheco*, y se le haría pertenecer al grupo *Alcaldes*. Por último, se crearía el usuario *esteban.garcia*, y se le haría pertenecer al grupo *PAS*. En cada UO de cada pedanía se crearía el usuario correspondiente a su alcalde pedáneo. Por ejemplo, en la UO YUSO se crearía el usuario *susana.rebolledo*. Todos los usuarios correspondientes a los alcaldes pedáneos pertenecerían al grupo *AlcaldesPedaneos.*
6. **EQUIPOS**: Se incorporarían al dominio los equipos pertenecientes al municipio. Al hacer esto, aparecen en el contenedor *Computers* de la herramienta *Usuarios y Equipos de Active Directory.* Deben moverse a las UOs correspondientes: los que se encuentren en las pedanías a las UOs YUSO o SUSO y los que se encuentren en el Ayuntamiento, a la UO VILLAPEDRUSCO.

Con esto se tendría una configuración básica de la estructura en Active Directory, preparada para la asignación de permisos sobre recursos cuando se definan y **escalable**, es decir, apta para un crecimiento de la organización.