1. Administración de usuarios y grupos

Una correcta gestión y configuración de usuarios puede facilitar en gran medida la administración del sistema operativo y evitar accesos no autorizados al sistema. Una vez terminada esta unidad, debe ser capaz de dar de alta, modificar y eliminar usuarios y grupos del sistema utilizando el entorno gráfico y el entorno de mandatos.

los sistemas Windows tienen un modo básico de funcionamiento: el modo gráfico. Antes de poder trabajar directamente en un sistema Windows -si se encuentra configurado con seguridad- en la pantalla gráfica tendremos que indicar un nombre de usuario (*login*) y una contraseña (*password*); es decir, siempre deberemos identificarnos. A pesar de disponer de este modo gráfico por defecto, podemos encontrarnos en situaciones de administración donde sea necesario abrir desde el entorno gráfico una consola de administración y entrar órdenes desde teclado. De hecho, algunas versiones de Windows disponen de un modo de arranque que da paso a una consola de recuperación que se utiliza cuando las cosas van mal dadas. También puede haber herramientas de recuperación disponibles desde el CDROM/DVD de instalación.

1.1. Usuarios de Windows

En esta unidad aprenderemos a gestionar usuarios locales en el sistema operativo Windows 7 Professional. Debemos tener claro que todos los usuarios y grupos que crearemos en este sistema operativo serán usuarios locales, es decir, su gestión (alta, baja y modificación) únicamente afectará al equipo en el que estamos trabajando.

1.1.1. Introducción a los usuarios locales

> Se entiende por usuario local la configuración personalizada que permite que se inicie una sesión de trabajo y se acceda a los recursos en el equipo local.

Una cuenta de usuario es un conjunto de información que indica en Windows los archivos y directorios a los que se puede acceder, los cambios que se pueden llevar a cabo en el equipo y las preferencias personales como el fondo del escritorio o el protector de pantalla. Las cuentas de usuario permiten que distintas personas compartan el mismo equipo, cada una con sus propios archivos y configuraciones. Cada persona tiene acceso a su cuenta de usuario mediante un nombre y contraseña.

En Windows 7, a diferencia de versiones anteriores como Windows 9X o ME, es necesario que un usuario se valide en el sistema para poder acceder y trabajar. Además, este usuario ha tenido que ser creado por otro perteneciente al grupo de usuarios administradores del sistema.

En toda la familia Windows NT, desde Windows 2000 a Windows 7, una vez instalamos el sistema se crea automáticamente una cuenta de usuario para que una persona pueda acceder al sistema y administrarlo como sea necesario. En este caso, durante el proceso de instalación se crean las credenciales para el usuario administrador del equipo local o usuario principal del sistema (véase la figura 1 .1). Este usuario es el que debe iniciar la sesión por primera vez y el que tendrá los privilegios

Figura 1.1. Creación de usuario inicial administrador

1.1.2. Tipo de cuentas de usuario

En Windows 7, como en la mayoría de sistemas operativos actuales (tanto libres como de propiedad), tenemos diferentes tipos de cuentas de usuario y se pueden utilizar según las necesidades que tengamos en nuestro entorno. En este apartado aprenderá cuáles son las cuentas de usuario más destacadas y qué uso tienen en Windows 7.

Usuario administrador

> El usuario administrador es el usuario que tiene control total sobre el ordenador y puede crear, modificar y eliminar configuraciones del sistema incluyendo usuarios y grupos.

El usuario administrador no debe darse de alta en el sistema, ya que se crea automáticamente. Tampoco podremos eliminarlo pero sí personalizarlo. Este usuario será el que nos permita crear otras cuentas de usuarios, modificarlas, instalar y desinstalar software y también modificar la configuración del sistema.

> La cuenta de usuario administrador se puede renombrar, pero nunca eliminar ni quitar del grupo de usuarios administradores.

Es importante renombrar la cuenta de usuario administrador así como asignar una contraseña especial para proteger el acceso con privilegios al equipo local.

Invitado

Usuario que puede iniciar sesión para utilizar parte del sistema. No puede instalar ni hardware ni software, ni crear, modificar o borrar configuraciones de ningún tipo. Tampoco puede crear ni gestionar ni eliminar usuarios y grupos. La cuenta de invitado es una cuenta especial que permite trabajar con el ordenador con un software específico pero sin poder realizar ninguna modificación.

Usuario inicial

Usuario creado durante la instalación del sistema operativo y que tiene los mismos privilegios que el usuario administrador.

> Una contraseña es un conjunto de caracteres que se utiliza para autenticar, abastecer de identidad o ganar acceso a un recurso.

Para que nuestro sistema sea seguro y podemos evitar que cualquier usuario malintencionado o no autorizado pueda acceder a él, es muy aconsejable proteger todas las cuentas de usuario con una contraseña. Podemos gestionar las contraseñas desde la misma pantalla que utilizamos para modificar información de los usuarios del sistema

Los usuarios del grupo de administradores son los únicos usuarios que pueden ver si el resto de usuarios del sistema tienen una contraseña asignada, modificarla o eliminarla, pero nunca tendrán acceso para verla.

1.2.1. Creación de contraseñas seguras

Podemos seguir varias reglas para asegurarnos de que nuestra contraseña es segura frente a los intentos de acceso no autorizado al sistema. A modo de resumen podemos mencionar una serie de normas recomendables a la hora de elegir una contraseña:

1. Utilice, al menos, ocho caracteres. Ejemplo: **password** .
2. Utilice tanto letras minúsculas como mayúsculas. Ejemplo: ***P*** **assword** .
3. Utilice algún valor numérico. Ejemplo: **Passw *o*** **rd** .
4. Añada algún carácter especial. Ejemplo: **P @ ssword** .

De esta forma se obtiene una contraseña bastante más segura que la propuesta inicialmente.

1.2.2. Ataques principales contra las contraseñas

Entre los distintos ataques que podemos sufrir contra las contraseñas podemos destacar los siguientes:

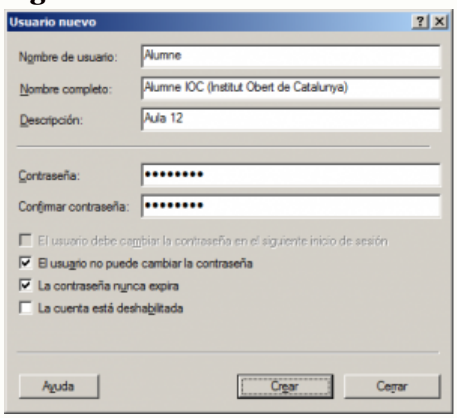
1. **Fuerza sucia** . Razón principal por la que se aconsejan contraseñas largas con números y otros caracteres. Se trata de intentar recuperar su contraseña probando una a una todas las combinaciones posibles de caracteres hasta encontrar la que permite el acceso.
2. **Ataque de diccionario** . Consiste en intentar utilizar las palabras de un diccionario como posible contraseña, así como las contraseñas más utilizadas estadísticamente.

1.2.3. Contraseñas en Windows 7

A la hora de asignar o modificar una contraseña en Windows 7, tenemos varias opciones:

1. **El usuario debe modificar la contraseña al inicio siguiente de sesión.** La primera vez que el usuario se conecte al sistema, éste le obligará a modificar su contraseña tanto si hemos configurado una o no. Cuando el usuario intente acceder al equipo, éste solicitará la contraseña antigua (que debemos comunicar previamente al usuario) y dos veces su nueva contraseña.
2. **El usuario no puede modificar su contraseña.** El usuario podrá acceder al sistema mediante una contraseña (o no) pero nunca podrá modificarla. En este caso, el administrador sí conocerá la contraseña, puesto que, tanto si ha sido asignada como no, él será el que la habrá configurado previamente en el equipo.
3. **La contraseña nunca expira.** Toda contraseña introducida tendrá validez hasta que el administrador lo decida. Si no activamos esta opción, la contraseña caducará en cuarenta y dos días. Esta configuración podrá modificarse.
4. **Cuenta deshabilitada.** Esta opción se utiliza para denegar el acceso a un usuario concreto, durante un tiempo determinado, sin necesidad de eliminar las credenciales del ordenador al que no queremos permitir el inicio de sesión. Sin esta opción deberíamos eliminar la cuenta

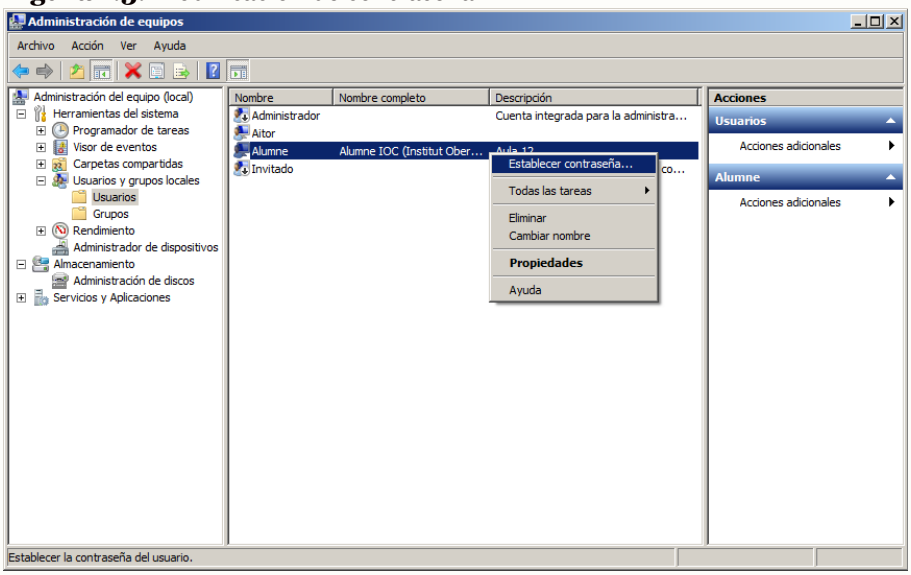
Figura 1.2. Creación de usuario



1.2.4. Modificación de la contraseña

Una de las acciones que puede realizar el administrador del sistema con los usuarios creados es modificar su contraseña (véase la figura 1 .3). Es importante tener claro que como administradores nunca podrá ver la contraseña de los usuarios del sistema pero sí modificarla o, simplemente, saber si un usuario en concreto tiene una contraseña o no para acceder al sistema. Por tanto, siempre podrá asignar nuevas contraseñas pero nunca recuperar las antiguas en caso de pérdida.

Figura 1.3. Modificación de contraseña



Es importante tener en cuenta que, si realizamos esta acción, será necesario informar al usuario sobre este cambio para que pueda volver a iniciar la sesión en nuestro sistema.

1.3. Perfiles de usuarios locales

Cada vez que se genera un nuevo usuario y éste accede al sistema por primera vez, el mismo sistema genera una configuración personal y específica para el usuario. Entre estas configuraciones podemos destacar el escritorio, el panel de control y las aplicaciones.

Dentro del directorio raíz de la instalación del sistema operativo (generalmente c:\) existe una carpeta llamada *Usuarios* (anteriormente, *Documents and Settings*), que contiene las carpetas personales de los usuarios. Cada una de ellas incluye numerosos archivos y carpetas.

Cada una de estas carpetas contiene información sobre el inicio de sesión personalizada del usuario como, por ejemplo: accesos directos del escritorio, fondos de pantalla, protector de pantalla, programas instalados, etc. De esta forma, todas las modificaciones que los usuarios realicen en su

Todas estas carpetas, archivos y documentos no podrán ser eliminados ni modificados por ningún usuario que no sea su propio propietario. Únicamente el administrador del sistema o un usuario con privilegios suficientes podría modificarlos.

Otro de los directorios dignos de mención es *Default* , que por defecto se encontrará oculto en el mismo directorio Usuarios. Este directorio, denominado anteriormente *Default User* , contiene la configuración por defecto de cualquier nuevo usuario que creamos en el sistema, es decir, cualquier nuevo usuario que creamos tomará inicialmente el contenido y las configuraciones existentes en este directorio. El directorio *Default* y todo su contenido se copiarán con su nombre, y cualquier modificación que este usuario realice sólo le afectará a sí mismo.

Si por el motivo que fuera, se borrara accidentalmente el directorio de un usuario determinado, en el inicio siguiente de sesión se volvería a realizar una copia del directorio *Default* .

En cada uno de los perfiles podemos encontrar diferentes directorios, algunos de ellos se describen a continuación:

- **Datos de programa** que almacena los datos específicos de los programas.
- **Cookies** . Almacena información sobre las preferencias del usuario.
- **Entorno de red** . Guarda los accesos directos a opciones de “Mis sitios de red”.
- **Escritorio** . En el que se guardan los iconos que aparecen en el escritorio del usuario incluyendo archivos, directorios y accesos directos.
- **Favoritos** . En este directorio se guardan los accesos directos a los programas y aplicaciones favoritas y sus ubicaciones.
- **Configuración local** . Almacena los archivos de datos de programas, historial y archivos temporales.
- **Impresoras** . Guarda los accesos directos a los elementos de la carpeta impresoras.
- **Menú inicio** . Se guardan los accesos directos que puede encontrar en el menú inicio de nuestro equipo.
- **Mis documentos** . Guarda todos los documentos del usuario.
- **Mis imágenes** . Guarda los elementos de imagen del usuario.
- **Plantillas** . Contiene los accesos directos a las plantillas creadas por el usuario.
- **Reciente** . En este directorio se almacenan los accesos directos recientemente utilizados.
- **SendTo** . Guarda los accesos directos de las utilidades de control de los documentos.

Las carpetas Configuración local, Datos de programa, Entorno de red, Impresoras, Plantillas, Recent y SentTo están ocultas y no son visibles a menos que lo indique expresamente, marcando “ *Mostrar todos los archivos y carpetas ocultas* ” en la ficha “ *Ver* ” de *Opciones de carpeta* en el menú *Herramientas* .

Asimismo, podemos encontrar también hasta tres archivos llamados NTuser.dat, que contiene datos del registro del usuario, NTuser.dat.LOG, que es un archivo en el que se guardarán los cambios anteriores a la última modificación del registro y poder resolver posibles problemas a la hora de producirse y NTuser.man el cual contiene los datos del registro del usuario pero es un archivo de sólo lectura y, por tanto, no se guardan los cambios.

1.4. Grupos de usuarios

Se entiende por *grupo local* la entidad administrativa que es capaz de incluir un conjunto de usuarios o incluso de otros grupos de tal forma que todos los

debe pertenecer necesariamente a un grupo para estar identificado en el sistema.

Todos los usuarios que damos de alta en nuestro sistema deben pertenecer de forma predeterminada a un grupo concreto. Por tanto, siempre que en nuestro sistema queramos modificar los privilegios de uno o más usuarios, lo podemos hacer directamente sobre los usuarios o sobre un grupo que, normalmente, contendrá más de un usuario.

Los grupos de usuarios se gestionan desde el mismo sitio donde se gestionan las cuentas de usuarios. A continuación se muestran los grupos que podemos encontrar por defecto en Windows 7:

1. **Administradores.** Usuarios con acceso completo y sin ningún tipo de restricción en el sistema. A este grupo pertenecen el usuario administrador y todos los usuarios autorizados para administrar casi todo el ordenador local.
2. **Duplicadores.** Usuarios que pueden replicar archivos en un dominio.
3. **Invitados.** De forma predefinida, los usuarios del grupo "Invitados" tienen el mismo acceso que los miembros del grupo "Usuarios" excepto la cuenta del usuario "Invitado" que tiene más restricciones.
4. **Operadores de configuración de red.** Los miembros de ese grupo pueden tener ciertos privilegios para administrar la configuración de las características de red.
5. **Operadores de copia de seguridad.** Los miembros de este grupo pueden invalidar restricciones de seguridad con el único propósito de realizar copias de seguridad o restaurar archivos.
6. **Usuarios.** Los usuarios que pertenecen a este grupo no pueden realizar cambios accidentales o intencionados en el sistema, pero pueden ejecutar la mayoría de aplicaciones.
7. **Usuarios avanzados.** Estos usuarios tienen limitados derechos administrativos.
8. **Usuarios de escritorio remoto.** Los miembros de este grupo permiten el inicio de sesión remoto.
9. **Lectores del registro de eventos.** Los miembros de este grupo pueden leer los registros de eventos del equipo local.
10. **Operadores criptográficos.** Los usuarios que pertenecen a este grupo están autorizados a realizar operaciones criptográficas.
11. **Usuarios CÓMO distribuidos.** Los miembros de este grupo pueden iniciar, activar y utilizar objetos de COM distribuidos en el equipo.
12. **Usuarios del monitor de sistema.** Los miembros de este grupo tienen acceso a los datos del contador de rendimientos de forma local y remota.
13. **Usuarios del registro de rendimiento.** Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar proveedores de seguimiento y recopilar seguimientos de eventos localmente y mediante el acceso remoto a este equipo.

1.5. Control de cuentas de usuario (UAC)

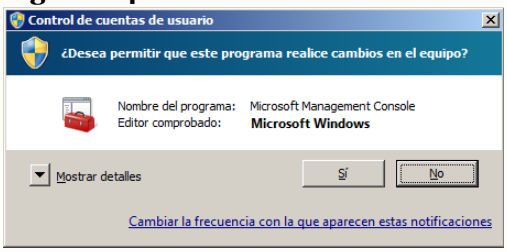
El control de cuentas de usuario (UAC, del inglés *user account control*) es un nuevo conjunto de tecnologías introducido en Windows Vista que tiene como objetivo evitar que programas maliciosos (*malware*) puedan causar problemas en el sistema operativo. Con el UAC, cualquier aplicación debe ejecutarse con permisos de usuario no administrador a menos que el propio usuario permita la ejecución con permisos administrativos.

En esta versión de Windows, y gracias al UAC, los usuarios estándar y los usuarios administradores, ejecutan aplicaciones en el contexto de seguridad de los usuarios estándar.

Cuando un usuario accede al sistema, el sistema operativo crea un testimonio (*token*) de acceso para él. Este testimonio contiene información sobre su nivel de acceso, e incluye identificadores de seguridad específicos (SID) y privilegios de Windows. Siempre que un

estándar contiene exactamente la misma información específica de usuario que el testimonio con acceso administrador, pero se han eliminado los privilegios de Windows administrativos y SID. El testimonio de acceso de usuario estándar se utiliza para iniciar aplicaciones que no realizan tareas administrativas o aplicaciones de usuario estándar.

Figura 1.4. UAC Usuario administrador

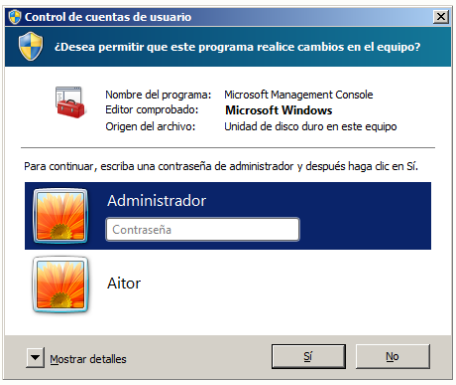


Cuando un usuario que pertenece al grupo de administradores locales debe ejecutar alguna aplicación que lleva a cabo tareas administrativas (aplicaciones de administrador), Windows 7 pide a estos usuarios que cambien o eleven su contexto de seguridad de usuario estándar a usuario administrador. Esta experiencia de usuario de administrador predeterminado se llama *modo de aprobación de administrador* . En este modo, las aplicaciones requieren un permiso específico para ejecutarse como aplicaciones de administrador.

Cuando se ha iniciado una aplicación de administrador, aparece un mensaje de control de cuentas de usuario de forma predeterminada (vea la figura 1 .4). Si el usuario es un administrador, el mensaje da la opción de permitir o evitar que se inicie la aplicación.

Si el usuario es un usuario estándar y no pertenece al grupo de administradores, puede especificar el nombre de usuario y la contraseña de un usuario que sea miembro del grupo de administradores locales. (Ver la figura 1 .5).

Figura 1.5. UAC, usuario no administrador



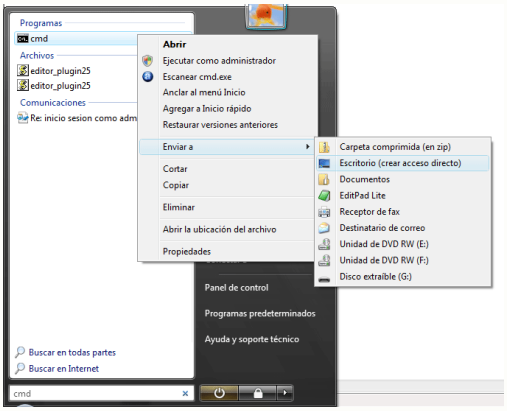
Al diseñar una aplicación para Windows 7, los programadores de software deben identificar su aplicación como aplicación de administrador o aplicación de usuario estándar. Si una aplicación no se ha identificado como aplicación de administrador, Windows 7 la tratará como una aplicación de usuario estándar. Sin embargo, los administradores también pueden marcar una aplicación para que se trate como aplicación de administrador.

Vamos a ver un ejemplo creando un acceso directo a la consola y dando privilegios de administrador:

Hasta ahora ha visto que la gestión de usuarios en los sistemas Windows puede hacerse fácilmente por medio de herramientas gráficas. ES interesante, sin embargo, disponer de una consola que nos permita introducir órdenes. Esta gestión conviene realizarla con privilegios de administrador.

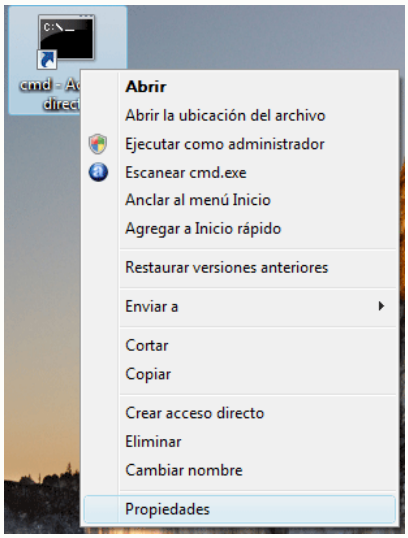
Una vez que haya accedido al entorno gráfico, para iniciar una consola se le recomienda seguir los siguientes pasos:

Figura 1.6. Lista de programas con el icono de consola



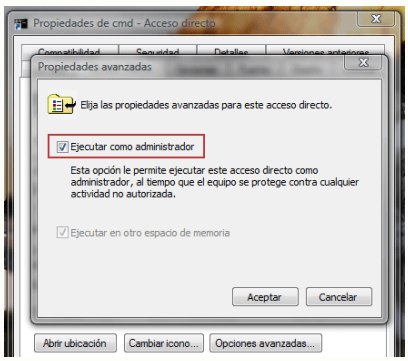
- Para hacer más fácil el acceso posterior a la aplicación puede situarnos con el ratón sobre el icono y crear un acceso directo al escritorio eligiendo “Enviar al escritorio (crear acceso directo)” (figura 1 .7).

Figura 1.7. Propiedades del acceso directo a consola



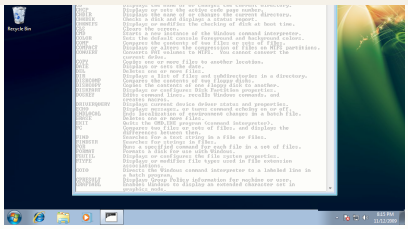
- Para dar más privilegios de administrador a esta consola, nos situamos sobre el acceso directo y escogemos “Propiedades”. En las “Opciones avanzadas” marcamos la casilla “Ejecutar como administrador” y aceptamos. Cerramos las ventanas y ya tenemos un acceso directo a una consola de administración (figura 1 .8).

Figura 1.8. Propiedades del acceso directo a consola



Dentro de esta ventana (figura 1 .9), ya puede introducir las órdenes. La primera orden que puede probar es la de la ayuda: HELP

Figura 1.9. La consola



En la tabla 1 .1 dispone de una lista de órdenes básicas para utilizar en la consola de Windows. En Internet dispone de sitios web que amplían esta lista y otros que describen cada orden.

Tabla 1.1. Órdenes básicas de la consola

Orden	Descripción
DATE	Muestra fecha. También permite modificarla.
TIME	Muestra hora. También permite modificarla.
DECIR	Muestra todos los archivos de la ruta donde nos encontramos.
CD	Permite cambiar de carpeta.
MD carpeta	Crea una carpeta con el nombre 'carpeta'.
RMDIR carpeta	Elimina la carpeta 'carpeta'.
TREE	Muestra la estructura de carpetas.
NOTEPAD archivo.cmd	Programa externo que permite la creación de un archivo, en este caso un archivo de mandatos.
.\archivo.cmd	Llamamiento a un archivo de mandatos, ejecutando las líneas de éste una después de otra.
TYPE archivo.txt	Muestra el contenido del archivo especificado.
DEL archivo.txt	Elimina el archivo especificado.
ATTRIB	Muestra y permite cambiar atributos de archivos.
SHUTDOWN	Permite apagar el sistema.
SYSTEMINFO	Muestra información diversa del sistema.

En el sitio web **CommandWindows.com** (bit.ly/2OY1eJN) tiene una extensa lista de órdenes con su descripción.

1.6. Dominios, grupos de trabajo y grupos domésticos

Los dominios, grupos de trabajo y grupos domésticos representan diferentes formas de organizar equipos en las redes. La principal diferencia entre ellos es la forma de administrar los equipos y otros recursos de las redes.

Todos los equipos que ejecuten Windows en una red, deben ser parte de un grupo de trabajo o de un dominio. Los equipos que ejecuten Windows en redes domésticas también pueden ser parte de un grupo en el hogar (o grupo doméstico), pero no es un requisito.

Por lo general, los equipos de redes domésticas forman parte de un grupo de trabajo y, probablemente, de un grupo en el hogar, y los equipos de redes del puesto de trabajo forman parte de un dominio.

1.6.1. En un grupo de trabajo

- Todos los equipos se encuentran en el mismo nivel, no existe ningún equipo que tenga el control sobre otro.
- Cada equipo dispone de un conjunto de cuentas de usuario. Para iniciar sesión en cualquier equipo del grupo de trabajo, debe disponer de una cuenta en el equipo.
- Normalmente, no hay más de veinte equipos.

1.6.2. En un grupo doméstico

- Los equipos de una red doméstica pueden pertenecer a un grupo de trabajo, pero también pueden pertenecer a un grupo doméstico. Un grupo doméstico permite compartir fácilmente imágenes, música, vídeos, documentos e impresoras con otras personas de una red doméstica.
- El grupo en el hogar está protegido con contraseña, pero solo es necesario escribir la contraseña una vez, al agregar el equipo al grupo en el hogar.

1.6.3. En un dominio

- Uno o más equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y permisos de todos los equipos del dominio. Así resulta más sencillo efectuar cambios, ya que éstos se aplican automáticamente a todos los equipos. Los usuarios de dominio deben proporcionar una contraseña o algún otro tipo de credencial cada vez que accedan al dominio.
- Si se dispone de una cuenta de usuario en el dominio, se puede iniciar sesión en cualquier equipo del dominio sin necesidad de disponer de una cuenta en ese equipo.
- Habitualmente sólo se pueden realizar cambios limitados a la configuración de un equipo porque los administradores de red con frecuencia desean garantizar un nivel de homogeneidad entre los equipos.
- Un dominio puede incluir miles de equipos.
- Los equipos pueden encontrarse en distintas redes locales.

1.6.4. Navegación

La navegación es el proceso de buscar otros ordenadores o recursos compartidos en la red Windows. Debe tener en cuenta que es lo mismo que utilizar un navegador web, aparte de la idea general de buscar e intentar descubrir lo que podemos encontrar. Por otra parte, navegar por la red de Windows es parecido a hacerlo por la web, puesto que todos los recursos a los que podemos acceder pueden ser modificados sin previo aviso.

Antes de la existencia del navegador, los usuarios debían conocer el nombre del ordenador al que querían conectarse, después debían teclear manualmente una dirección UNC en el gestor de archivos o la aplicación implicada para poder acceder al recurso. Un ejemplo de dirección UNC puede ser `\servidorIOC\apunts`, o también `\192.168.1.1\recursos`.

La navegación es mucho más sencilla, ya que permite examinar los contenidos de la red utilizando una interfaz del entorno de red de los clientes Windows.

1.6.5. Controlador de dominio

Un controlador de dominio en un dominio Windows funciona de forma muy similar a un servidor NIS en una red Unix, manteniendo una base de datos del dominio que contiene la información de los usuarios y grupos, así como sus servicios asociados. Las responsabilidades de un controlador de dominio están centradas principalmente en la seguridad, incluyendo la autenticación o la tarea de permitir o denegar el acceso a los recursos del dominio a un determinado usuario. Esto se realiza normalmente gracias al uso de un nombre de usuario y una clave. El servicio que mantiene la base de datos en los controladores de dominio se denomina *Security Account Manager (SAM)*.

El modelo de seguridad de Windows gira en torno a los identificadores de seguridad (SIDs) y las listas de control de acceso (ACLs). Los identificadores de seguridad son utilizados para representar objetos en un dominio, que incluyen (pero no limitan) a los usuarios, grupos, ordenadores y procesos. Los SIDs se escriben normalmente en un formulario *ASCII* como campos separados por guiones, tal y como se muestra en el siguiente ejemplo:

Un SID comienza con el carácter “S”, seguido de un guión. El número inmediatamente posterior al primer guión se denomina identificador relativo (RID) y es un número único dentro del dominio que identifica a un usuario, grupo, ordenador o cualquier otro objeto. El número RID es análogo al identificador de usuario (UID) o al identificador de grupo (GID) en un sistema Unix o dentro de un dominio NIS.

Las ACLs (listas de control de acceso) proveen la misma funcionalidad que los permisos de los archivos comunes en los sistemas Unix (rwx). Sin embargo, las ACLs son más versátiles. Los permisos de los archivos Unix sólo pueden establecer permisos para el propietario del recurso, el grupo al que este archivo pertenece, y “otros”, es decir, cualquier otro usuario. Las ACLs de Windows permiten establecer permisos individuales para cualquier número arbitrario de usuarios y/o grupos. Las ACLs están constituidas por una o más entradas de control de acceso (ACE - Access Control Entries), cada una de las cuales contienen un SID y derechos de acceso asociados a ellos.

1.6.6. Autenticación

Cuando un usuario teclea a su usuario y clave para ingresar en un dominio Windows, se invoca un “desafío de seguridad” y un protocolo de respuesta entre el ordenador cliente y el controlador de dominio para verificar que el usuario y la clave son válidos. Seguidamente el controlador de dominio envía el SID de nuevo al cliente, quien lo utilizará para crear un token de seguridad (SAT – Security Access Token) que es válido únicamente para este sistema, que será utilizado para autenticaciones posteriores. Esta señal de acceso contiene la información sobre el usuario codificada en su interior, que incluye el nombre de usuario, el grupo y los permisos que el usuario posee en el dominio. En ese momento, el usuario está autenticado en el dominio.

Posteriormente, cuando el cliente intenta acceder a un recurso compartido dentro del dominio, el sistema cliente entra en un desafío de seguridad y un intercambio de respuestas con el servidor del recurso. Seguidamente, el servidor entra en otro desafío de seguridad para comprobar que el cliente es válido. Lo que sucede realmente es que el servidor utiliza la información que ha obtenido del cliente para hacerse pasar por éste y autenticarse a sí mismo ante el controlador de dominio. Si el controlador de dominio, viendo sus credenciales, envía un SID al servidor, éste lo utilizará para crear su propio SAT para el cliente, de esta forma habilita el acceso a sus recursos locales en beneficio del cliente. En este punto, el cliente se encuentra autenticado para los recursos del servidor y se le permite acceder a ellos. El servidor utiliza el SID almacenado en el SAT para determinar que permisos de modificación y uso posee el cliente para el recurso en cuestión, esto lo logra comparándolo con las entradas de las ACLs del recurso.

Aunque este método de autenticación pueda parecer demasiado complicado, permite a los clientes la autenticación sin enviar las claves en texto plano a través de la red, y es mucho más difícil romper que la seguridad que proporcionan los grupos de trabajo.

1.6.7. Dominios Active Directory

> Un directorio es una estructura jerárquica que almacena información sobre los objetos existentes en una red y un servicio de directorio proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores y usuarios de la red.

A partir de Windows 2000, Microsoft introdujo Active Directory (Directorio Activo), un paso más allá de los dominios de Windows NT. Con Active Directory, el modelo de autenticación está centrado en torno a LDAP, y el servicio de nombres lo suministra un servidor DNS en lugar de un servidor

secundario, como ocurría en los dominios Windows NT.

Active Directory no realiza cambios fundamentales en la forma en que funcionan los dominios en Windows de cara a los usuarios finales pero si introduce algunas estructuras de dominio importantes que podrían afectar a la forma de aproximarse al diseño del dominio. Active Directory utiliza dominios como unidades principales de la estructura lógica. Los dominios ayudan a organizar la estructura de la red ajustándose a la organización de la empresa, ya sea política o geográficamente.

El Directorio Activo cuenta con las siguientes características:

- Incorpora un **directorio** que es un almacén de datos para guardar información sobre los objetos (estos objetos incluyen normalmente recursos compartidos como servidores, archivos, impresoras y cuentas de usuario y equipos en red).
- Incorpora un conjunto de reglas (**esquema**) básicas que definen las clases de objetos y los atributos contenidos en el directorio (los atributos y datos también son conocidos como metadatos), las restricciones y los límites en las instancias de estos objetos así como el formato de sus nombres.

Conceptos sobre los usuarios

Las cuentas de usuario representan a una persona y se denominan **principales de seguridad** dentro del Directorio Activo, puesto que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de usuario permite que un usuario inicie sesiones en equipos y dominios cuya identidad se puede autenticar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario única y su contraseña. Por tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario
- Autorizar o denegar el acceso a los recursos del dominio
- Administrar otros principales de seguridad
- Auditar las acciones realizadas por el usuario mediante su cuenta

Los usuarios en Active Directory pueden ser de dos tipos:

- **Usuarios globales** . Estas cuentas se crean en los servidores que sean controladores de dominio y pueden utilizarse para conectarse a los dominios en los que se han creado ya otros dominios en los que se confía (dominios de confianza).
- **Usuarios locales** , Estas cuentas de usuario se crean en estaciones de trabajo o servidores que no sean controladores de dominio y, por tanto, no pueden utilizarse para conectarse a ningún dominio. Un usuario local es una cuenta a la que se pueden asignar permisos y derechos para el equipo local en el que se ha creado.

Por defecto, durante la instalación de un equipo servidor, se crean dos cuentas de usuario que pueden utilizarse para iniciar sesión y tener acceso a los recursos. Estas cuentas son:

- La cuenta del usuario **Administrador** que permite administrar el equipo en el que se ha creado. Esta cuenta puede ser renombrada pero nunca podrá ser eliminada, deshabilitada ni salvo del grupo local de Administradores. Es recomendable renombrar y asignar una contraseña segura a esta cuenta así como crear otras cuentas de usuario administrador para mejorar la seguridad del servidor.
- La cuenta del usuario **Invitado** . Normalmente esta cuenta está deshabilitada (y deberíamos mantenerla de esta manera) pero se podría habilitar si se desea que algún usuario pueda conectarse al equipo o al dominio de esta forma aunque, debe tener en cuenta, que no necesita ninguna contraseña para iniciar sesión. Esta cuenta puede eliminarse y renombrarse.

Los perfiles de usuario

Un perfil de usuario es una de las más potentes herramientas para configurar el entorno de trabajo de los usuarios en red.

Cada usuario puede tener su perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo (así pues, aquellos usuarios que se conectan a diferentes estaciones de trabajo pueden tener un perfil diferente en cada uno de ellas). Este perfil se llama **Perfil local** porque sólo es accesible desde la estación donde ha sido creado.

Los usuarios que se conectan a un servidor pueden tener, además, perfiles en ese servidor. De esta forma, se puede acceder al perfil independientemente de la estación de trabajo en la que se está conectado. Este perfil se llama **Perfil de red** ya que se puede acceder a él desde cualquier estación de trabajo que esté conectada a la red.

Existen dos tipos de perfiles de red:

- **Perfil móvil** : Este tipo de perfil es asignado a cada usuario por los administradores pero puede ser modificado por el usuario y los cambios efectuados permanecerán una vez haya finalizado la sesión.
- **Perfil obligatorio** : Este tipo de perfil tiene la misma estructura que el **perfil móvil** pero asegura que los usuarios puedan trabajar en un entorno común. Por tanto, podrá ser modificado por el usuario pero todos los cambios que éste realice en la configuración, se perderán una vez haya finalizado la sesión. Únicamente podrá ser modificado (y guardados los cambios) por usuarios que pertenezcan al grupo de administradores.

Los perfiles móviles

Como ya ha visto anteriormente, estos tipos de perfiles son asignados a cada usuario, pueden ser modificados por ellos mismos y los cambios producidos permanecerán uno como haya finalizado la conexión.

Para que esto sea posible, los datos de registro del usuario se guardarán en un archivo llamado NTuser.dat (dentro del subdirectorio de perfiles locales con el nombre del usuario tal y como hemos visto anteriormente). Cuando el usuario se conecta, el contenido de este archivo se copia en la categoría **HKEY_CURRENT_USER** del registro. Cuando el usuario realice cambios en su perfil, éstos se guardarán automáticamente en el archivo NTuser.dat al finalizar la conexión, de esta forma, los cambios producidos por el usuario se mantendrán la próxima vez que éste inicie sesión.

Los perfiles obligatorios

Como ya ha visto anteriormente, este tipo de perfiles, tienen la misma estructura que los perfiles móviles, pero aseguran que los usuarios trabajen en un entorno común. Por tanto, los usuarios pueden modificarlos pero los cambios realizados se pierden al finalizar la conexión y únicamente se mantendrán si estos cambios son realizados por usuarios que tengan permisos de administrador.

Para ello, se guardan los datos del registro de usuario en un archivo llamado NTuser.man. Cuando el usuario se conecta, este archivo se copia en la categoría **HKEY_CURRENT_USER** del registro. Cuando el usuario realice cambios en su perfil, éstos no se guardarán en el archivo al finalizar la sesión, de esta forma, los cambios realizados no se mantendrán la próxima vez que el usuario inicie sesión en el equipo.

Conceptos sobre los grupos

Las cuentas de grupo representan a un grupo y, al igual que los usuarios, se denominan principales de seguridad dentro de Active Directory, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad. Podemos encontrar dos grupos diferenciados:

- **Los grupos de seguridad** : Estos tipos de grupos se muestran dentro de las listas de control de acceso discrecional (DACL) que es el lugar en el que están definidos los permisos sobre los recursos y los objetos. Estos grupos de seguridad se pueden utilizar también como entidades de correo electrónico, de esta forma, si envía un mensaje de correo electrónico a ese grupo, el mensaje será recibido automáticamente para todos los miembros del grupo de seguridad.
- **Los grupos de distribución** : En este tipo de grupos no es posible habilitar la seguridad ya que no aparecen en las listas de control de acceso discrecional (DACL). Los grupos de

Un grupo de seguridad puede convertirse en un grupo de distribución (y por el contrario) en cualquier momento. Cada grupo de seguridad y distribución tiene un ámbito que identifica el alcance de aplicación del grupo. Existen cuatro tipos de grupos diferenciados en función de su alcance de aplicación.

- **Grupos de ámbito universal** : Estos tipos de grupos (que únicamente se pueden crear en equipos servidores que tengan instalado el Directorio Activo) pueden tener como miembros a otros grupos universales, grupos globales y cuentas de cualquier dominio de Windows y se los puede conceder permisos de cualquier dominio. También se pueden denominar **grupos universales** .
- **Grupos de ámbito global** : Estos tipos de grupos (que únicamente se pueden crear en equipos servidores que tengan instalado el Directorio Activo) pueden tener como miembros a grupos globales y cuentas únicamente del dominio en el que se ha definido el grupo y les puede conceder permisos de cualquier dominio. Estos grupos también se pueden denominar **grupos globales** .
- **Grupos de ámbito global de dominio** : Estos tipos de grupos (que únicamente se pueden crear en equipos servidores que tengan instalado el Directorio Activo) pueden tener como miembros a grupos universales, grupos globales, grupos locales de dominio de su propio dominio y cuentas de cualquier dominio de Windows y únicamente pueden utilizarse para conceder permisos en el dominio que contiene el grupo. También pueden ser llamados **grupos de dominio local**
- **Grupos locales** : Estos tipos de grupos únicamente se pueden encontrar en equipos que ejecuten una versión cliente de Windows o que sean servidores miembros (equipos Windows Server pero que no tengan el Directorio Activo instalado). Pueden tener como miembro a cuentas locales del equipo en el que se han creado y, si ese equipo forma parte de un dominio, podrá tener también cuentas y grupos globales del propio dominio y de los dominios de confianza y se pueden utilizar para conceder permisos en el equipo en el que se ha creado este grupo.