Administración de usuarios y grupos

En Windows

**Usuarios locales**

La configuración personalizada que permite que se inicie una sesión de trabajo y acceda a los recursos en el equipo local.

Cuando se dan de alta usuarios en un sistema, las cuentas que se generan únicamente permiten el acceso local pero no el acceso a sistemas remotos.

Una ***cuenta de usuario*** es un conjunto de información que indica al Windows los archivos y directorios a 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 diferentes 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 una contraseña.

En Windows 7 y superiores, es necesario que un usuario se valide en el sistema para poder acceder y trabajar.

Una **cuenta de usuario tiene que ser creada** por otro usuario que pertenezca al grupo de usuarios administradores del sistema.

En toda la familia Windows NT, desde el Windows 2000 a Windows 10, 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

**Tipo de cuentas de usuario**

**usuario administrador**

Tiene control total sobre el sistema y puede crear, modificar y eliminar configuraciones del sistema incluyendo los usuarios y los grupos.

El usuario administrador no debe darse de alta en el sistema, ya que se crea automáticamente.

Tampoco lo podremos eliminar pero sí personalizarlo.

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

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

**invitado**

Usuario que puede iniciar la 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 llevar a cabo ninguna modificación.

**usuario inicial**

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

**Gestión de contraseñas**

Una contraseña es un conjunto de caracteres que se utiliza para autenticar, proveer 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, 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 los usuarios del sistema, tienen una contraseña asignada, modificarla o eliminarla, pero nunca tendrán acceso para verla.

**Creación de contraseñas seguras**

Podemos seguir varias reglas para asegurarnos de que nuestra contraseña es segura ante 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, como mínimo, ocho caracteres. Ejemplo: **password** .
2. Utilice tanto letras minúsculas como mayúsculas. Ejemplo: ***P*assword** .
3. Utilice algún valor numérico. Ejemplo: **Passw*0*rd** .
4. Agregue algún carácter especial. Ejemplo: **P*@*ssw0rd**.

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

**Ataques principales contra las contraseñas**

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

1. **Fuerza bruta**. Razón principal por la que se aconsejan contraseñas largas con números y otros caracteres. Se trata de intentar recuperar la 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 como las contraseñas más utilizadas estadísticamente.

**Contraseñas en el Windows**

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

1. **El usuario debe cambiar la contraseña al inicio siguiente de sesión.**

1. **El usuario no puede modificar la contraseña.**

.

1. **La contraseña no expira nunca.**

1. **Cuenta deshabilitada.**

**Modificación de la contraseña**

El administrador nunca podrá ver la contraseña de los usuarios del sistema pero sí modificarla.

También puede asignar nuevas contraseñas.

**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.

En el directorio raíz de la instalación del S.O. (generalmente C: \) hay 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, salvapantallas, programas instalados, etc.

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

Otro de los directorios dignas de mención es ***Default***, que por defecto se encontrará **oculto** en el mismo directorio Usuarios (antes Default User). Contiene la configuración por defecto de cualquier nuevo usuario que creamos en el sistema, es decir, cualquier nuevo usuario que creamos cogerá inicialmente el contenido y las configuraciones que hay en este directorio. El directorio *Default* y todo su contenido se copiarán con su nombre, y cualquier modificación que este usuario haga sólo le afectará a él mismo.

Si se borrara el directorio de un usuario determinado, en el inicio siguiente de sesión se volvería a hacer 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** el cual almacena los datos específicos de los programas.
* **Cookies**. Almacena información sobre las preferencias del usuario.
* **Entorno de red**. Guardar 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**. Guardar los accesos directos a los elementos de la carpeta impresoras.
* **Menú inicio**. Se guardan los accesos directos que encontrará en el menú inicio de nuestro equipo.
* **Mis documentos**. Guardar todos los documentos del usuario.
* **Mis imágenes**. Guardar 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 utilizados recientemente.
* **SendTo**. Guardar los accesos directos de las utilidades de control de los documentos.

Las carpetas Configuración local, Datos de programa, Entorno de red, Impresoras, Plantillas, Reciente y SendTo, 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:

**NTuser. Dat**, que contiene datos del registro del usuario.

**NTuser. Dat. LOG**, que es un archivo donde se guardarán los cambios anteriores a la última modificación del registro y poder resolver posibles problemas a la hora de producirse.

**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.

**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 manera que todos los permisos o privilegios concedidos a este grupo, se heredarán directamente por todos los usuarios o grupos que pertenezcan. Todo usuario de nuestro equipo 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 lugar 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 manera predeterminada, 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 este 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 hacer copias de seguridad o restaurar archivos.
6. **Usuarios.**Los usuarios que pertenecen a este grupo no pueden hacer cambios accidentales o intencionados en el sistema, pero pueden ejecutar la mayoría de aplicaciones.
7. **Usuarios avanzados.**Estos usuarios tienen derechos administrativos limitados.
8. **Usuarios de escritorio remoto.**A los miembros de este grupo se permite 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 COM 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 manera 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.

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 la UAC, cualquier aplicación se debe ejecutar con permisos de usuario no administrador salvo que el mismo usuario permita la ejecución con permisos administrativos.

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

Un *token* es un conjunto de bytes que expresa el nivel de privilegio que tiene un usuario concreto.

Cuando un usuario accede al sistema, el sistema operativo crea un testigo (*token*) de acceso para él. Este testimonio contiene información sobre el nivel de acceso que tiene, e incluye identificadores de seguridad específicos (SID) y privilegios de Windows. Siempre que un administrador accede al sistema, éste crea dos testigos de acceso totalmente independientes, uno concede acceso de usuario estándar, y el otro acceso de administrador. El testimonio de usuario estándar contiene exactamente la misma información específica de usuario que el testigo con acceso administrador, pero se han eliminado los privilegios de Windows administrativos y los SID. El testigo de acceso de usuario estándar se utiliza para iniciar aplicaciones que no hacen tareas administrativas o aplicaciones de usuario estándar.

Cuando un usuario que pertenece al grupo de administradores locales debe ejecutar alguna aplicación que lleva a cabo tareas administrativas (aplicaciones de administrador), Windows 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 denomina *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. 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.

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, el 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:

* Ir a Inicio y en el cuadro de búsqueda y escribimos: cmd. Esto hace que en la lista de programas aparezca el icono de la consola de comandos.
* Btn Dcho "Abrir ubicación de archivo”
* Desde el archivo, Btn Dcho 🡪 Crear acceso directo
* Copiar el acceso directo creado en el escritorio
* Para dar más privilegios de administrador a esta consola, nos situamos encima del acceso directo y escogemos "Propiedades". En las "Opciones avanzadas" marcamos la casilla "Ejecutar como administrador".

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

**Tabla. 1**

|  |  |
| --- | --- |
| **orden** | **Descripción** |
| DATE | Mostrar fecha. También permite modificarla. |
| TIME | Muestra hora. También permite modificarla. |
| DIR | Mostrar 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 fitxer.cmd | Programa externo que permite la creación de un fichero, en este caso un fichero de órdenes. |
| . \ Fitxer.cmd | Llama a un fichero de órdenes, ejecutando las líneas de este una después de la otra. |
| TYPE archivo.txt | Muestra el contenido de su archivo. |
| 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. |

Dominios, grupos de trabajo y grupos domésticos

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

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

Generalmente, 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.

En un grupo de trabajo

* Todos los equipos se encuentran en el mismo nivel, no hay 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.
* Un grupo de trabajo no está protegido con contraseña.
* Todos los equipos deben encontrarse en la misma red local o subred.

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 sólo es necesario escribir la contraseña una vez, al agregar el equipo al grupo en el hogar.

En un dominio

* Uno o más equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y los permisos de todos los equipos del dominio. Así resulta más sencillo efectuar cambios, ya que estos 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 este equipo.
* Habitualmente sólo se pueden hacer cambios limitados a la configuración de un equipo para que 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 diferentes redes locales.

navegación

La navegación es el proceso de buscar otros ordenadores o recursos compartidos en la red Windows.

Antes de la existencia del navegador, los usuarios tenían que conocer el nombre del ordenador al que se querían conectar, luego tenían que 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 la siguiente:

\ ServidorIOC \ apuntes

ó

\ 192.168.1.1 \ recursos

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

Controlador de dominio

Un controlador de dominio en un dominio Windows mantiene 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 principalmente centradas 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.

Incluyen usuarios, grupos, ordenadores y procesos.

Los SIDs se escriben normalmente en un formulario *ASCII* como campos separados por guiones, tal como se muestra en el siguiente ejemplo:

S-1-5-21-1638239387-7675610646-9254035128-545

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

Autenticación

Cuando un usuario teclea 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, la cual incluye el nombre de usuario, el grupo y los permisos que el usuario posee en el dominio. En este 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 él 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 consigue 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 de romper que la seguridad que proporcionan los grupos de trabajo.

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 ponerlas a disposición de los administradores y de los 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 alrededor de LDAP, y el servicio de nombres lo suministra un servidor DNS en lugar de un servidor WINS. Los dominios en Active Directory se pueden organizar en una estructura jerárquica en árbol, en la que, cada controlador de dominio es fijo, no hay distinción entre controlador primario y secundario, como ocurría en los dominios Windows NT.

Active Directory no hace 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 de 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 los datos también son conocidas 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 usuarios representan a una persona y se denominan **principales de seguridad** dentro del Directorio Activo, ya 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 con una identidad que 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 lo 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 (otras cuentas de usuario).
* 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 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 sacada del grupo local de Administradores. Es recomendable cambiar el nombre 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 mantener 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.

**Los perfiles de usuario**

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

Se pueden especificar el aspecto del escritorio, la barra de tareas, el contenido de menú Inicio (incluyendo los programas o aplicaciones), etc.

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 denomina **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 este servidor. De este modo, se puede acceder al perfil independientemente de la estación de trabajo en la que se está en línea. Este perfil se denomina **Perfil de red** ya que se puede acceder a él desde cualquier estación de trabajo que esté conectada a la red.

Hay 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 lo tanto, podrá ser modificado por el usuario, pero todos los cambios que éste realice en configuración, se perderán una vez finalice la sesión. Únicamente podrá ser modificado (y guardados los cambios) para usuarios que pertenezcan al grupo de administradores.

**Los perfiles móviles**

Como ya se ha visto anteriormente, este tipo de perfiles son asignados a cada usuario, pueden ser modificados por ellos mismos y los cambios producidos permanecerán tal como estén cuando 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, estos 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 se 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 , 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 lograr esto, 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, estos no se guardarán en el archivo al finalizar la sesión, de este modo, 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 donde 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 manera, si envía un mensaje de correo electrónico a este 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 distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Microsoft Exchange) para enviar correo electrónico a los grupos de los usuarios.

Un grupo de seguridad puede convertirse en un grupo de distribución (y al contrario) en cualquier momento. Cada grupo de seguridad y de 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 les 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 se los 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 se pueden utilizar 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 los podemos 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 aquel 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.

Windows 10

El Control de cuentas de usuario en Windows es una función de seguridad que **ayuda a evitar cambios no autorizados en el sistema operativo**. Una parte de usuarios lo deshabilita y es un error.

Cuando se implementó en [Windows Vista](https://support.microsoft.com/es-co/help/922708/how-to-use-user-account-control-uac-in-windows-vista), el Control de cuentas de usuario (también conocido como UAC) fue una de las características más criticadas, seguramente al no ser bien explicada/entendida y ante la gran cantidad de avisos que los usuarios percibieron más como un molestia que ralentizaba su trabajo que como una mejora de su seguridad.

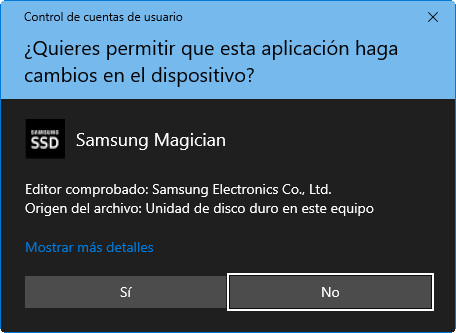
Microsoft lo ha ido mejorando en cada versión posterior de sus sistemas y **recomendamos mantenerlo activado,** aunque sea en su opción mínima.

**Qué es y cómo se activa UAC**

Como decíamos, UAC es una capa de seguridad añadida en Windows que previene de cambios no autorizados en el sistema operativo que puedan afectar a la seguridad o a la configuración de otras personas que usen un mismo equipo.

Estos cambios pueden ser realizados por usuarios sin permisos suficientes, aplicaciones, controladores y, lo peor, por cualquiera forma de malware que se haya introducido o pretenda introducirse en el equipo. El Control de cuentas de usuario se asegura de que **ciertos cambios se realicen solo con la aprobación del administrador**. Si los cambios no son aprobados por él no se ejecutan y el sistema permanece sin cambios.

Su funcionamiento del lado del usuario es simple. Cuando ejecutas un archivo, una aplicación o algún elemento de la configuración que esté a punto de realizar cambios importantes en el sistema, la función mostrará una notificación similar a la siguiente. Para el ejemplo, el software de gestión de las SSD de Samsung en Windows 10 y desde una cuenta de administración:

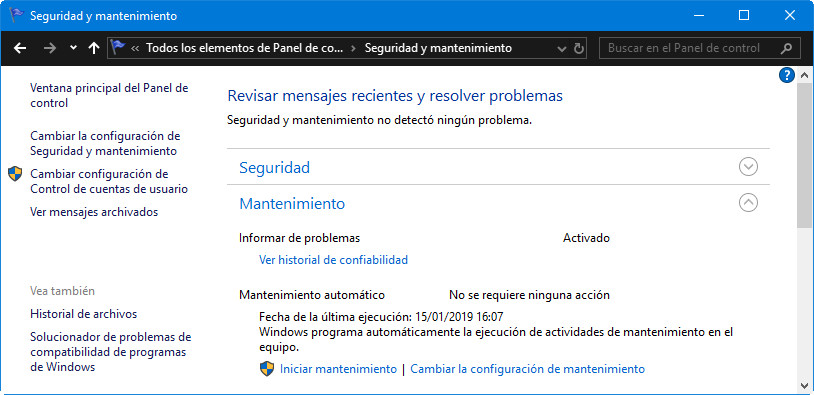
[](https://www.muycomputer.com/wp-content/uploads/2019/01/Control_cuentas_usuario_4.jpg)

La solicitud de la UAC muestra el nombre del programa que está a punto de realizar un cambio de sistema que requiere la aprobación de un administrador. También muestra el editor del programa y el origen del archivo ejecutable. Un enlace a «más detalles» informa del certificado del editor y el acceso a la gestión de estas notificaciones que veremos después. Si la aplicación es de confianza y se ejecuta desde una cuenta de administración **solo es necesario autorizar la petición**.

Si el acceso se ha realizado desde una cuenta sin privilegios de administración la notificación será diferente y, siguiendo el ejemplo de [Windows 10](https://www.muycomputer.com/?s=windows+10), la solicitud del UAC solicita el PIN del administrador (si está establecido) o la contraseña. En otros sistemas como Windows 7 y Windows 8.1, el indicador de UAC siempre solicita la contraseña del administrador.

**Conocer los programas** que activarán el control de cuentas es muy sencillo porque tienen un símbolo de UAC en la esquina inferior derecha del icono en el escritorio y también en el mismo ejecutable que puedes ver en el explorador de archivos.

Puedes encontrar este mismo tipo de símbolos en algunos elementos de configuración del sistema o en las herramientas del panel de control. Así sabrás de antemano que esos elementos necesitarán la aprobación del administrador cuando los ejecutes.



**Cómo funciona UAC**

En Windows, al contrario de como sucede de forma general en otros sistemas como Linux, **las aplicaciones se ejecutan de forma predeterminada sin ningún permiso administrativo**. Tienen los mismos permisos de una cuenta de usuario estándar, no pueden realizar ningún cambio en el sistema operativo, sus archivos de sistema o la configuración del registro. Además, no pueden cambiar nada que sea propiedad de otras cuentas de usuario. Las aplicaciones solo pueden cambiar archivos propios y en el registro los exc, los relativos al usuario  y la configuración del registro o los archivos del usuario y la configuración del registro.

Cuando una aplicación requiere cambios que afecten a otras cuentas de usuario, modificaciones a los archivos y carpetas del sistema de Windows o instalación de nuevo software, se muestra un indicador de UAC, que solicita el permiso. Si el usuario niega la autorización el cambio no se llevará a cabo. Si el usuario lo autoriza (e ingresa la contraseña del administrador cuando se requiera), la aplicación recibe permisos administrativos y puede hacer los cambios del sistema que desee.

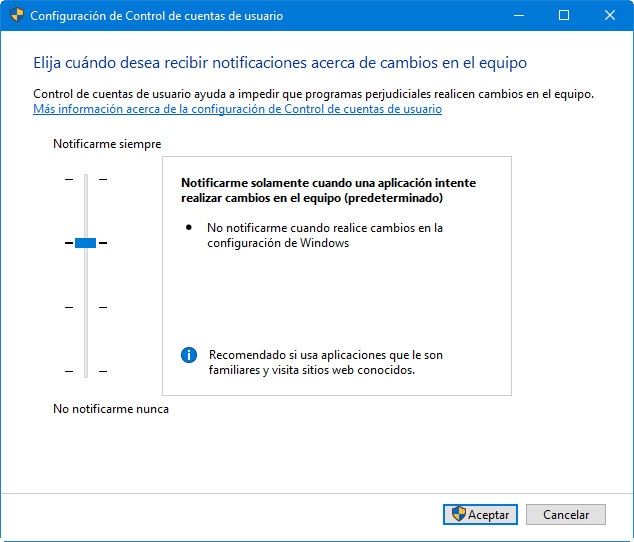
Estos permisos se otorgan **solo hasta que la aplicación deja de ejecutarse o el usuario la cierra**. Lo mismo ocurre con los archivos que activan una solicitud de UAC. Hay muchos cambios que requieren privilegios administrativos en Windows, dependiendo de cómo esté configurado el UAC en tu computadora puede activarse en muchas acciones:

* Ejecutando una aplicación como administrador.
* Cambios en la configuración del sistema, archivos en las carpetas de Windows o Archivos de programa.
* Instalar y desinstalar controladores y aplicaciones.
* Ver o cambiar las carpetas y archivos de otro usuario.
* Agregar o eliminar cuentas de usuario.
* Configurando la actualización de Windows.
* Cambiar la configuración del Firewall de Windows.
* Cambiar la configuración de la misma UAC.
* Cambiar el tipo de cuenta de un usuario.
* Ejecutando el Programador de Tareas.
* Restaurando archivos de sistema respaldados.
* Cambiando la fecha y hora del sistema.
* Configuración de controles parentales o seguridad.
* Instalación de controles ActiveX (en Internet Explorer).
* Etc.

**Cómo se gestiona el Control de cuentas de usuario en Windows**

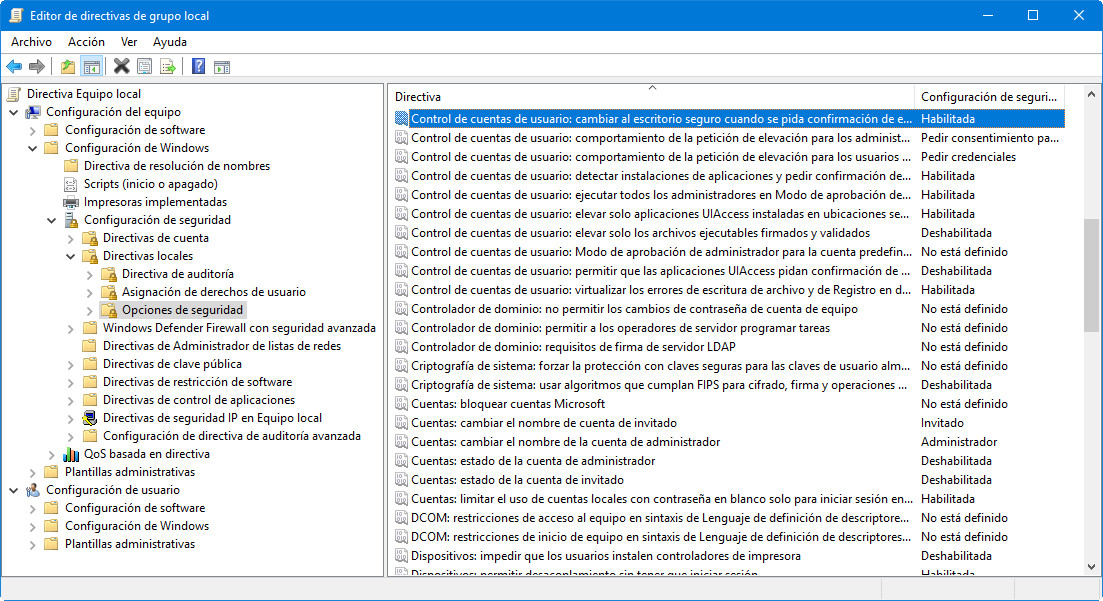
Hay dos maneras básicas de configurar esta función, una **básica** desde la configuración de usuario y otra más **avanzada** mediante políticas de grupo.

La gestión más sencilla se realiza accediendo al UAC desde el «Panel de control > Seguridad y mantenimiento > Cambiar configuración de Control de cuentas de usuarios». También se accede desde «ejecutar > msconfig > herramientas». Más directo es utilizar la búsqueda de Windows. En todos los casos nos encontraremos con la herramienta que ves en la imagen:

[](https://www.muycomputer.com/wp-content/uploads/2019/01/Control_cuentas_usuario_5.jpg)

Frente al original de Windows Vista que solo ofrecía dos niveles, las versiones más recientes de Windows ofrecen **cuatro niveles para elegir según el tipo de usuario y el uso del equipo**. [Cada nivel se explica por sí solo](https://answers.microsoft.com/es-es/windows/forum/windows_10-security/activar-o-desactivar-el-control-de-cuentas-de/46cacd85-b45d-4fbf-bec7-d51dcf14f8a0?auth=1) y va desde el deshabilitado (no recomendado) a la máxima protección donde la UAC pedirá autorización ante cualquier cambio, cuando las aplicaciones intenten instalar software o hacer cambios en el equipo y/o en la configuración de Windows.

Para usuarios avanzados y administradores la gestión más completa se realiza con el editor de políticas de grupo, accesibles desde el «Menú de Inicio > ejecutar > gpedit.msc». Una vez en el editor navega a «Configuración del Equipo > Configuración de Windows > Configuración de seguridad > Opciones de seguridad». Busca las directivas de Control de cuentas de usuario para adecuar su uso a tus necesidades. Hay una decena que puedes gestionar.

[](https://www.muycomputer.com/wp-content/uploads/2019/01/Control_cuentas_usuario_3.jpg)

Resumiendo. El Control de cuentas de usuario en Windows (UAC) es una capa de seguridad añadida en Windows que mejora la protección del equipo ayudando a evitar cambios no autorizados en el sistema operativo. Aunque a veces sus múltiples notificaciones puedan resultar pesadas **recomendamos mantenerlo activado** al menos en sus niveles básicos.