

# Las cuentas de usuario

Distinguiremos entre las cuentas predefinidas y las cuentas interactivas, que permiten a los usuarios abrir una sesión en el equipo. Las cuentas predefinidas de tipo Administrador o Invitado permiten sacar provecho de ciertas funcionalidades del sistema operativo. Este tipo de cuenta no corresponde directamente a un usuario real. Por el contrario, una cuenta de usuario interactiva corresponde a una persona física. El sistema le asigna una imagen, llamada perfil, que se almacena en esta ubicación: C:\Usuarios\

Cada usuario pertenece a un grupo genérico (predefinido). Al igual que es posible crear usuarios, se pueden crear nuevos grupos.

A cada grupo le corresponde un juego de permisos y restricciones. Por ejemplo, si el grupo de administradores tiene todos los permisos, el de los invitados trabaja en una especie de libertad vigilada.

Se puede acceder a la gestión de las cuentas de usuario desde el **Panel de control, Cuentas de usuario y protección infantil**. También puede utilizar la consola de gestión avanzada de usuarios introduciendo el comando **netplwiz** en la zona de búsqueda del menú **Inicio**.

Si desea reiniciar la contraseña de una cuenta desde la consola de gestión avanzada de los usuarios, haga clic en el botón **Restablecer contraseña**. Para acceder a las propiedades de un usuario y visualizar el grupo al que pertenece, haga clic en el botón **Propiedades**.

Seleccione la pestaña **Opciones avanzadas** y, en la sección **Administración avanzada de usuarios**, haga clic en el botón **Opciones avanzadas**. Se muestra la consola de administración de usuarios. Se puede acceder igualmente a esta consola introduciendo el comando **lusrmgr.msc** en la zona de búsqueda del menú **Inicio**.

Durante la instalación de Windows 8, hemos visto que es posible configurar una cuenta de usuario de tipo Cuenta Microsoft para integrar las funcionalidades de Cloud ofrecidas por el nuevo sistema operativo de Microsoft, como el correo, los contactos o SkyDrive. La gestión de este tipo de cuenta es idéntica a las cuentas de usuario locales del ordenador.

## 1. Funcionamiento de los perfiles de usuario

Al arrancar el ordenador, se le pedirá que inicie sesión. Cada nombre de sesión corresponde a un usuario. La primera vez que inicia sesión en un sistema acabado de instalar, se utiliza un perfil de usuario predeterminado. Este perfil depende de este árbol de Registro: HKEY\_USERS. En adelante, a medida que realice modificaciones en su entorno de trabajo, se guardarán cada una de sus preferencias. De hecho, con el tiempo, su perfil de usuario se pulirá.

En los sistemas NT, también utilizamos perfiles itinerantes (más conocidos como perfiles móviles): en un entorno en el que el usuario utilice diferentes equipos, éste podrá encontrar el mismo entorno de trabajo sea cual sea el ordenador en el que abra sesión.

Por otra parte, es posible asignar un perfil obligatorio para un usuario o grupo de usuarios, o modificar el perfil predeterminado que afectará a cada nuevo usuario creado. Dicho de otro modo, podrá copiar un perfil de usuario de una cuenta a otra de la misma manera que se fabrican figuras utilizando un molde.

## 2. Los grupos predefinidos

Existen algunos grupos de usuarios que están configurados de manera predeterminada en el sistema. Nos limitaremos a hablar de los más conocidos.

## a. Los principios de seguridad integrados

**ANONYMOUS LOGON:** representa los usuarios y servicios que acceden a un ordenador sin utilizar un nombre de cuenta, contraseña ni nombre de dominio.

**CREADOR PROPIETARIO:** representa el usuario que ha creado o tomado posesión de un objeto.

**INTERACTIVE:** representa todos los usuarios conectados a un equipo en ese momento y que acceden a un recurso determinado de ese ordenador (en contraste con los usuarios que acceden al recurso mediante una red). Cada vez que un usuario accede a un recurso específico en el ordenador en el que está conectado en ese momento, se le añade de manera automática al grupo interactivo.

**DIALUP:** representa cualquier usuario que se conecta al ordenador mediante una conexión de acceso remoto.

**REMOTE INTERACTIVE LOGON:** representa cualquier usuario que se conecta al equipo mediante una conexión de Escritorio remoto.

**NETWORK:** recoge a los usuarios que acceden en ese momento a un recurso determinado mediante una red (en contraste con los usuarios que acceden a un recurso abriendo una sesión local en el ordenador que contiene dicho recurso). Cada vez que un usuario accede a un recurso determinado mediante la red, se le añade de manera automática al grupo Network.

**Todos:** agrupa todos los usuarios de la red actual, incluyendo los invitados y usuarios de otros dominios. Cada vez que un usuario abre una sesión en la red, se le añade de manera automática al grupo Todos.

**USUARIO DE TERMINAL SERVER:** representa cualquier usuario que accede al equipo mediante una conexión Escritorio remoto.

**Usuarios autenticados:** este grupo comprende todos los usuarios que tienen una cuenta y contraseña en la máquina local o en Active Directory.

**Todos los paquetes de aplicación:** esta entidad administra los permisos de acceso a los recursos del sistema para aplicaciones Windows Store.

**Permisos de propietario:** representa los permisos aplicados al propietario actual de un objeto.

**SYSTEM:** es con esta identidad con la que el corazón del sistema operativo administra el conjunto de componentes esenciales para el funcionamiento del núcleo:

- El proceso csrss.exe (*Client/Server Runtime Subsystem*) administra las ventanas y los elementos gráficos de Windows.
- El proceso Lsass.exe (*Local Security Authority Subsystem Service*) administra los mecanismos de seguridad local y de autenticación de los usuarios a través del servicio WinLogon.
- El proceso Lsm.exe (*Local Session Manager*) administra el inicio de sesión local.
- El proceso wmicprvse.exe (*Windows Management Instrumentation*) administra las herramientas WMI.
- El proceso Wininit.exe administra el inicio de Windows.
- El proceso Winlogon.exe (*Windows Logon Process*) administra el inicio y cierre de sesiones.
- El proceso SearchIndexer administra la indexación de archivo para las funciones de búsqueda.
- El proceso svchost.exe que es un nombre de proceso host genérico para ejecutar servicios a partir de bibliotecas dinámicas (DLL). Verá diversas instancias de este proceso que corresponden a los diferentes servicios Windows arrancados.

**Servicio de red:** esta cuenta la utilizan los servicios que necesitan autenticarse con otros equipos presentes en la red, sin necesidad de tener privilegios demasiado amplios.

**SERVICIO LOCAL:** es el mismo tipo de cuenta con la diferencia de que sólo puede acceder a los recursos de red que permiten un acceso anónimo. Permite especialmente ejecutar los procesos vinculados con el Administrador de dispositivos y algunos servicios relacionados con la red, por ejemplo, la resolución de nombres NetBIOS (LmHosts).

**Restricted:** permite definir una ACE en una ACL que contiene un permiso de tipo "Denegar" para todos los token de acceso restringidos, ya sea porque se le asigna a la entidad un permiso de tipo "Denegar", o porque el permiso acordado es de tipo "Lectura". En cualquiera de los casos, los grupos o los usuarios restringidos no tienen acceso al recurso, ya que las ACE negativas tienen prioridad sobre las positivas. Para las demás entradas, únicamente tendrán un acceso de sólo lectura.

**Trusted Installer:** la tecnología Windows Resource Protection (WRP) actúa como un tipo de autoridad suprema que impide cualquier cambio en los archivos, directorios y claves del Registro que se consideran necesarios para el buen funcionamiento del sistema. En este caso, solo el servicio Trusted Installer puede realizar los cambios en los recursos que están protegidos por este servicio.

## **b. Los grupos de usuarios**

**Administradores:** reúne a los miembros que poseen privilegios de administrador.

**Invitados:** los miembros del grupo Invitados disponen por defecto del mismo acceso que los miembros del grupo Usuarios, con la excepción de que la cuenta de invitado dispone de privilegios restringidos.

**Operadores de configuración de red:** reúne a los miembros que poseen cierto número de privilegios relacionados con la configuración de interfaces de red.

**Operadores de copia de seguridad:** reúne a los miembros que tienen permisos para guardar y restaurar todos los archivos de un ordenador.

**Usuarios:** los miembros de este grupo tienen acceso limitado a los recursos y disponen de un número restringido de privilegios.

**Usuarios avanzados:** los miembros de este grupo pueden realizar cierto número de tareas administrativas sin necesidad de tener un control total del equipo. Este grupo existe por razones de compatibilidad con sistemas anteriores.

**Usuarios de escritorio remoto:** agrupa a los miembros que tienen privilegios para abrir una sesión remota.

**Usuarios del monitor de sistema:** agrupa a los miembros que pueden visualizar los datos de rendimiento en tiempo real en el Monitor de rendimiento.

**Usuarios del registro de rendimiento:** agrupa a los miembros que pueden, además de visualizar datos de rendimiento en tiempo real, crear y modificar conjuntos de datos del Monitor del sistema.

**Usuarios de administración remota:** agrupa a los miembros que acceden a los recursos WMI a través de protocolos de comunicación compatibles.

**Administradores Hyper-V:** agrupa los miembros que tienen privilegios de administrador para las funcionalidades Hyper-V.

**Operador de cifrado:** agrupa los miembros que tienen privilegios de uso de operaciones de cifrado.

### c. Los usuarios predefinidos

**Administrador:** esta cuenta especial le permite liberarse del control de las cuentas de usuario. El token de acceso que se le otorga es único. Por defecto, está desactivado en Windows 7 y Windows 8.

**Invitado:** esta cuenta también está desactivada por defecto en Windows 7 y Windows 8. Resulta útil en los casos en que queremos darle un acceso ocasional a un usuario que no tendrá casi ningún privilegio ni derecho sobre los recursos.

Puede activar estas dos cuentas con el siguiente procedimiento:

- En el cuadro de texto **Iniciar búsqueda** del menú **Iniciar**, introduzca el siguiente comando: `netplwiz`.
- Haga clic en la pestaña **Opciones avanzadas** y en el botón **Opciones avanzadas**.
- Abra la rama **Usuarios** y la cuenta que desea modificar.
- Desmarque la casilla **Cuenta deshabilitada**.