

**MÓDULO:**

Sistemas informáticos

**UT4\_2\_Configuración del sistema  
operativo**

## ÍNDICE DE CONTENIDO

1	Usuarios y grupos .....	2
1.1	Asistente para cuentas de usuario desde Panel de Control .....	2
1.2	Gestión de cuentas de usuario y grupos locales mediante consola .....	3
1.2.1	Gestión de usuarios .....	3
1.2.2	Gestión de grupos .....	6
1.3	Gestión de cuentas de usuario mediante consola especial .....	6
1.4	Gestión de cuentas de usuario desde la interfaz de línea de comandos (CLI) .....	7
2	Gestión de las contraseñas .....	8
3	Número de identificación de seguridad (SID) .....	9
4	Listas de control de acceso (ACL) .....	11
4.1	Ver la lista de control de acceso (ACL) de una carpeta o archivo .....	11
4.2	Herencia de permisos .....	11
5	Administrando el equipo .....	12
5.1	Herramientas del sistema .....	13
5.1.1	Programador de tareas .....	13
5.1.2	Visor de eventos .....	13
5.1.3	Carpetas compartidas .....	14
5.1.4	Usuarios y grupos locales .....	14
5.1.5	Rendimiento .....	14
5.1.6	Administrador de dispositivos .....	15
5.2	Almacenamiento .....	15
5.2.1	Administración de discos .....	15
5.3	Servicios y Aplicaciones .....	15
6	Editor de directivas de grupo local .....	16

## 1 Usuarios y grupos

Las cuentas de usuario representan a una persona y se utilizan para iniciar sesiones distintas y tener acceso a los recursos. Por tanto, una cuenta de usuario se utiliza para:

- Autenticar la identidad del usuario.
- Autorizar o denegar el acceso a los recursos.
- Administrar la seguridad.
- Auditar las acciones realizadas con la cuenta de usuario.

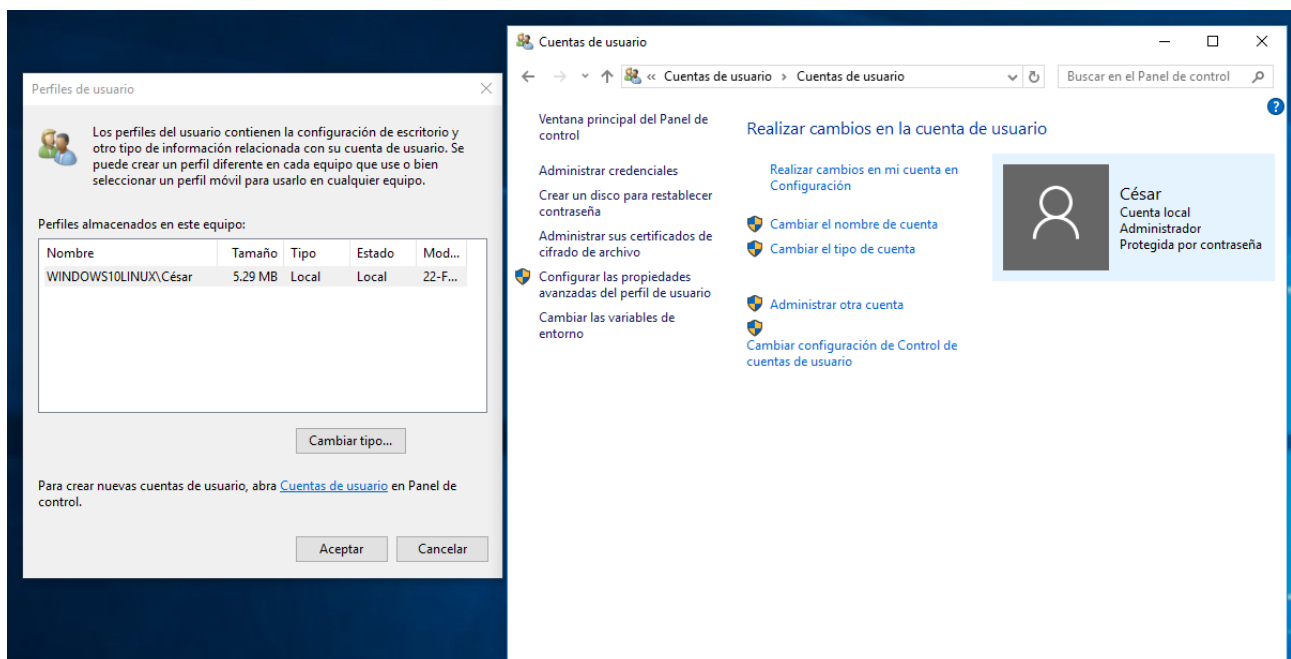
Se pueden crear, borrar y modificar cuentas de usuario en Windows usando varias técnicas distintas:

- Asistente para cuentas de usuario desde Panel de Control.
- Gestión de cuentas de usuario y grupos locales mediante consola.
- Gestión de cuentas de usuario mediante consola especial.
- Gestión de cuentas de usuario desde la interfaz de línea de comandos (CLI).

### 1.1 Asistente para cuentas de usuario desde Panel de Control

Para abrir la herramienta Cuentas de usuario, hay que abrir el **Panel de control** desde el menú Inicio y, a continuación, **Cuentas de usuario**.

Desde aquí se pueden crear cuentas nuevas, cambiar el nombre, cambiar el tipo de cuenta, acceder a los **perfiles de usuario**, etc.



Esta es la opción más sencilla para crear cuentas de usuario, es fácil de usar, pero muy poco potente. Aunque con distintas prestaciones, básicamente esta aplicación es igual a versiones anteriores de sistemas operativos Windows.

#### 🌈 Diferencia entre cuenta de usuario y perfil de usuario:

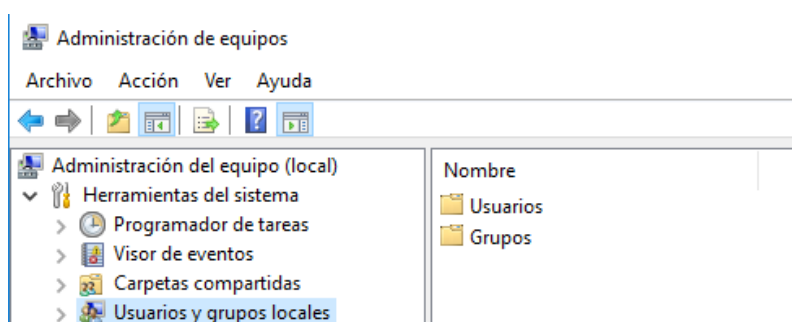
- Cuenta de usuario ➔ Aquella que le da a una persona acceso al equipo y a los programas que este contiene.
- Perfil de usuario ➔ Contiene la configuración de escritorio y otro tipo de información relacionada con la cuenta de usuario  
La información del perfil se encuentra en **C:\Users\NombreUsuario**.

## 1.2 Gestión de cuentas de usuario y grupos locales mediante consola

Otra opción que tenemos para gestionar cuentas de usuario, es la consola de usuarios locales y grupos. Podemos llegar a dicha consola de varias formas, aunque la más rápida es invocándola directamente desde Inicio – Ejecutar (tecla Windows + R) y escribir: **lusrmgr.msc**.



Esta consola lusrmgr.msc es la forma típica de gestionar usuarios y grupos en Windows. También podemos llegar a ella pinchando botón derecho sobre Mi PC (o Equipo), seleccionando Administrar y luego Usuarios y grupos locales.



Veremos que tenemos dos carpetas, una para los usuarios y otra para los grupos. Podemos crear usuarios nuevos accediendo a las propiedades de la carpeta usuarios (botón derecho sobre ella) y seleccionando la opción de Usuario nuevo. Podemos modificar un usuario accediendo a sus propiedades (botón derecho sobre el usuario y escogiendo propiedades, o directamente realizando doble clic sobre el usuario).

Del mismo modo que trabajamos con usuarios, podemos hacerlo con los grupos, creando grupos nuevos o modificando los ya existentes. Un usuario puede pertenecer a todos los grupos que deseemos, y un grupo puede contener tantos usuarios como necesitemos.

### 1.2.1 Gestión de usuarios

Podemos crear todas las cuentas de usuario que queramos, pero aparte de estas cuentas normales, existen dos cuentas de usuario especiales en Windows, ya creadas y que no deben ser modificadas o eliminadas: administrador e invitado.

La cuenta del Administrador del sistema (**Administrador**). Todos los sistemas Windows tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitadas para que solo puedan ser ejecutadas por el Administrador. Es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador (integrándolas como miembros del grupo Administradores) aunque Administrador solo puede haber uno. Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema (aunque se crea normalmente sin contraseña). Normalmente esta cuenta no dispone de contraseña por defecto y está deshabilitada para que no pueda ser usada.

La cuenta de **Invitado**. Es la contraria a la cuenta de Administrador, está totalmente limitada, no cuenta apenas con ningún permiso o derecho, pero permite que cualquier usuario pueda entrar en nuestro sistema sin contraseña (lo que se denomina acceso anónimo) y darse un “paseo” por el mismo. Por defecto esta cuenta está desactivada. Es altamente recomendable nunca activar dicha cuenta a menos que sea indispensable, ya que representa un riesgo altísimo de seguridad.

Si accedemos a las propiedades de un usuario, veremos cómo tenemos tres pestañas con las que trabajar:



- a) **General**. Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta.
  - El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.
  - El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.
  - La contraseña nunca expira. En Windows las contraseñas se consideran material fungible, es decir, que tras un cierto tiempo de uso el sistema obligará a cambiar dichas contraseñas. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque nunca.
  - La cuenta está deshabilitada. No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.
  - La cuenta está bloqueada. Mediante determinados mecanismos de seguridad se puede llegar a bloquear una cuenta, impidiendo su uso.
- b) **Miembro de**. Desde esta pestaña podemos añadir al usuario a grupos. Los grupos se usan para dar permisos y derechos a los usuarios fácilmente, sin tener que ir usuario por usuario. Así, por ejemplo, si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos los permisos del grupo Administradores.

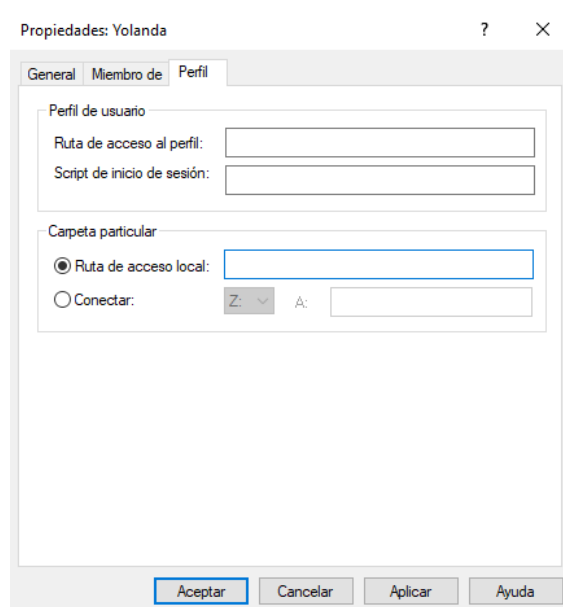
En la pestaña “miembro de” veremos todos los grupos a los que el usuario pertenece actualmente. Si le damos al botón agregar podremos escribir directamente el nombre de un grupo donde agregarlo. Si queremos escoger dicho grupo de una lista de los grupos posibles, hay que escoger la opción Avanzada y luego Buscar ahora, que nos mostrará una lista de todos los grupos del sistema. Basta con seleccionar el que queramos (o los que queramos) y pulsar aceptar.

- c) **Perfil**. Nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario.

Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo, y aquellos usuarios que acceden a varias estaciones pueden tener un perfil en cada una de ellas. Este perfil se denomina **perfil local** porque solo es accesible desde la estación en que está creado.

Además, existe un **perfil temporal** que se crea cuando se produce un error en la carga del perfil del usuario. Éste se elimina al final de la sesión y no se almacenan los cambios realizados por el usuario en la configuración del *Escritorio* y los archivos.

Para asignar un perfil de usuario, un script de inicio de sesión o una carpeta particular para la cuenta de usuario, se utiliza la ficha **Perfil** de la pantalla de **Propiedades** de cada usuario.



En ella se distinguen los siguientes apartados:

1. **Ruta de acceso al perfil.** Se utiliza para indicar la ruta de acceso para el perfil móvil u obligatorio de un usuario. Si es un perfil local, no es preciso rellenarlo.
2. **Los archivos de comandos de inicio de sesión.** En Windows 10, se denomina **script de inicio de sesión**. Se utiliza para indicar el nombre de un archivo de proceso por lotes que se ejecuta automáticamente cuando el usuario inicia sesión. Estos archivos tienen que tener **BAT** como extensión, aunque también se puede utilizar cualquier programa ejecutable.
3. **La ruta de acceso local.** Indica el directorio local privado de cada usuario donde puede almacenar sus archivos y programas. Así mismo, es el directorio predeterminado que se utilizará en el *Símbolo del sistema* y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

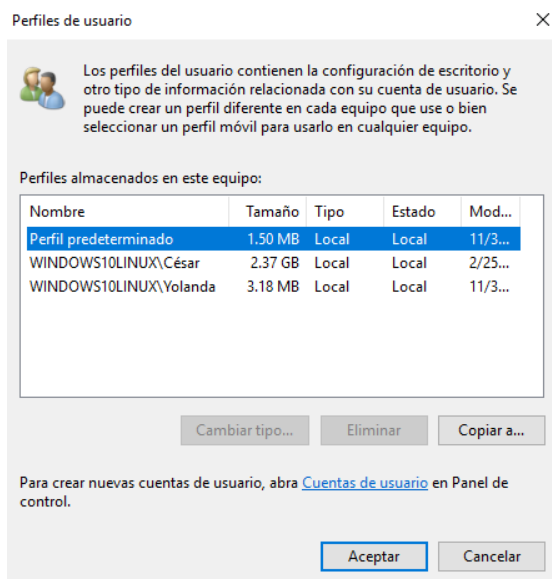
Se debe crear antes de especificar su ruta y su utilización es incompatible con **Conectar**.

4. **Conectar a una unidad de red.** Indica la letra deseada que estará conectada al directorio de red, es decir, un directorio compartido, privado de cada usuario, donde puede almacenar sus archivos y programas.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Se debe crear antes de especificar su ruta y su utilización es incompatible con **Ruta de acceso local**.

Se especifica con el formato *\\nombre del servidor\nombre compartido del subdirectorio privado\nombre del usuario*.



### Cómo ver el tipo de perfil de un usuario.

Panel de control → Sistema y seguridad → Sistema → Configuración avanzada del sistema → Configuración, del bloque Perfiles de usuario.

## 1.2.2 Gestión de grupos

Si nos vamos a la gestión de grupos, veremos cómo Windows ya incluye por defecto unos cuantos grupos creados:

El grupo más importante es el de **Administradores**, ya que cualquier usuario al que hagamos miembro de dicho grupo pasará a tener los permisos de un Administrador.

Otro grupo interesante es **Invitados**, ya que cualquier usuario al que hagamos miembro de dicho grupo pasará a tener todas las limitaciones del grupo Invitados.

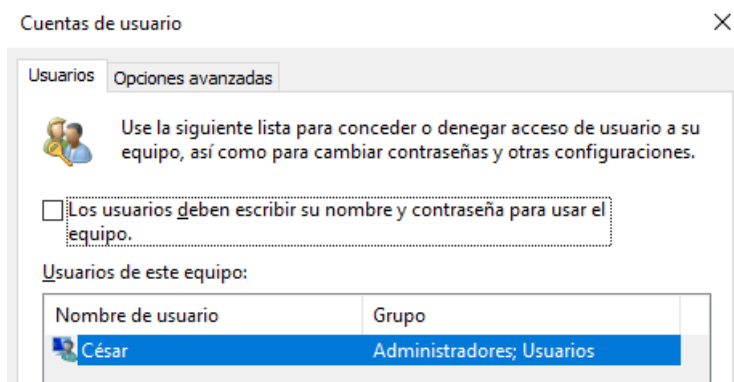
Podemos crear todos los grupos que queramos, sin ningún tipo de limitación y hacer miembros de los mismos a los usuarios que deseemos.

## 1.3 Gestión de cuentas de usuario mediante consola especial

Podemos también gestionar las cuentas de usuario mediante una consola especial, normalmente oculta. Para acceder a dicha consola, hay que ejecutar la orden:

### control userpasswords2

Con este gestor de cuentas de usuario tenemos un control especial sobre los usuarios, permitiéndonos realizar algunas acciones que no son accesibles desde ningún otro sitio.



Desde la pantalla que nos muestra (**Usuarios**), al pulsar el botón “propiedades” (previa activación del checkbox) podemos incluir al usuario en algún grupo de usuarios, bien uno de los dos incluidos en el gestor (Usuario estándar o Administrador) o bien seleccionando otro grupo.

Además, el checkbox que indica que *Los usuarios deben escribir su nombre y contraseña para usar el equipo* es el que permite que se muestre o no el menú de usuarios cuando se inicia Windows. Si está desactivado, se iniciará Windows con el usuario por defecto. En este [enlace](#) se puede consultar cómo especificar qué usuario se va a usar por defecto.

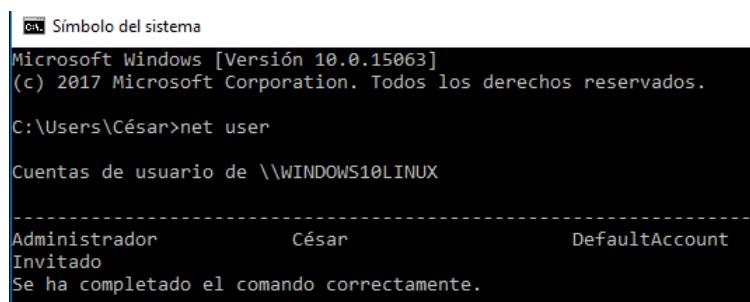
Una opción que puede resultar interesante, aunque también peligrosa es la de poder restablecer la contraseña de cualquier usuario, incluido el usuario administrador. Para hacerlo, basta con que nos hayamos autenticado con una cuenta de usuario que pertenezca al grupo Administradores. Esta opción ha sido incluida, ya que a veces los usuarios olvidan con el tiempo la contraseña que le asignaron a la cuenta de Administrador en el momento de la instalación del equipo, y es a su vez, la causante de que Microsoft oculte esta consola para que no sea ejecutada por los usuarios normales.

En la pestaña “**Opciones avanzadas**” de este gestor podemos ver opciones muy interesantes, como la administración de nuestras contraseñas, un botón que nos lleva a `lusrmgr.msc` u obligar a utilizar el inicio de sesión seguro (`Ctrl+Alt+Supr`).

#### 1.4 Gestión de cuentas de usuario desde la interfaz de línea de comandos (CLI)

La última opción para gestionar las cuentas de usuario es hacerlo directamente desde el símbolo del sistema o interfaz de línea de comandos (CLI) o Shell de texto (Windows + R y ejecutar `cmd`). Esta opción puede parecer la más engorrosa, pero resulta ser la más práctica y potente en muchísimas ocasiones, sobre todo si sabemos cómo hacer scripts de sistema.

Para ellos disponemos de una orden que nos permite gestionar las cuentas de usuario:  
**net user**



```

C:\Símbolo del sistema
Microsoft Windows [Versión 10.0.15063]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.

C:\Users\César>net user

Cuentas de usuario de \\WINDOWS10LINUX

-----
Administrador      César      DefaultAccount
Invitado
Se ha completado el comando correctamente.

```

Este comando nos permite consultar, agregar o modificar cuentas de usuario. Algunos de los parámetros principales de esta orden pueden ser los siguientes:

**Nombredeusuario.** Especifica el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o consultar. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

**Contraseña.** Asigna o cambia una contraseña para la cuenta de usuario. Escribimos un asterisco (\*) si deseamos que se nos pida la contraseña. Los caracteres de la contraseña no se muestran en la pantalla a medida que los escribimos, así que hay que tener cuidado.

**/add.** Agrega el usuario al sistema.

**/delete.** Borra el usuario del sistema.

**/help.** Argumento para lanzar la ayuda de net user.

Si al ejecutar la orden desde la línea de comandos (CMD) obtenemos el *error de sistema 5 (acceso denegado)*, es porque estamos ejecutando una línea de comandos sin ser administrador.



Para evitar esto se puede hacer un acceso directo a CMD en el escritorio y lanzarlo con el botón derecho – Ejecutar como Administrador.

También podemos escribir CMD en el botón inicio (Windows – escribir CMD) y en lugar de pulsar INTRO pulsamos CONTROL – SHIFT – INTRO con lo que conseguiremos que lo que ejecutemos se ejecute como Administrador.

En la siguiente dirección podemos ver algunas opciones más de esta potente orden podemos consultar el siguiente [enlace](#).

La mayor potencia de la interfaz de línea de comandos aparece cuando usamos scripts o procesos por lotes. Estos scripts son pequeños programas que podemos realizar con un editor de texto y que se ejecutan directamente en nuestro sistema operativo.

## 2 Gestión de las contraseñas

Windows es un sistema operativo muy configurable por parte del usuario, aunque algunas de las configuraciones más potentes suelen estar algo ocultas para que no sean accesibles por los usuarios normales y sólo puedan ser accedidas por usuarios avanzados.

En concreto, desde la consola de configuración de directivas de seguridad local, podemos gestionar varios aspectos sobre las contraseñas. Esta consola se denomina **secpol.msc**, y para gestionar las contraseñas debemos entrar en Configuración de Seguridad → Directivas de cuenta → Directiva de contraseñas.

Las configuraciones más útiles que se pueden gestionar aquí son:

- **Exigir historial de contraseñas.** Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente. El valor numérico indica cuántas contraseñas recordará.
- **La contraseña debe cumplir los requerimientos de complejidad.** Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas y minúsculas junto con números, no parecerse al nombre de la cuenta, etc.
- **Longitud mínima de la contraseña.** Indica cuántos caracteres debe tener la contraseña como mínimo. Un valor 0 en este campo indica que pueden dejarse las contraseñas en blanco.
- **Vigencia máxima de la contraseña.** Las contraseñas de los usuarios caducan y dejan de ser válidas después del número de días indicado en esta configuración. El sistema obligará al usuario a cambiarla (recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
- **Vigencia mínima de la contraseña.** Indica cuánto tiempo debe transcurrir desde que un usuario cambia la contraseña hasta que puede volver a cambiarla.

Desde la consola de configuración de seguridad local (**secpol.msc**) también podemos gestionar el comportamiento del sistema cuando un usuario intenta abrir sesión y se equivoca repetidamente con la contraseña. Podemos indicar que una cuenta de usuario quede bloqueada si alguien intenta abrir sesión con dicha cuenta y se equivoca un número determinado de veces. Esta configuración la encontramos en Configuración de seguridad → Directivas de cuenta → Directivas de bloqueo de cuenta.

Se puede configurar:

- **Duración del bloqueo de cuenta.** Durante cuánto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor 0 indicará que la cuenta se bloqueará hasta que un administrador la desbloquee.
- **Restablecer el bloqueo de cuenta después de.** Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero.
- **Umbral de bloqueo de cuenta.** Indica cuántos intentos erróneos se permiten antes de bloquear la cuenta. Evidentemente, para que los dos valores anteriores sean aplicables, la cuenta debe poder bloquearse.

### 3 Número de identificación de seguridad (SID)

Para referirse a las cuentas de usuario internamente, el sistema operativo no usa el nombre de ésta y su contraseña, esos son los datos que usamos nosotros, al igual que nos llamamos entre nosotros con nuestro nombre, pero la administración nos conoce por nuestro DNI. El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID (Security Identifier o Identificador de Seguridad).

Desde Windows es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden **whoami.exe**. Si ejecutamos la siguiente orden en el símbolo del sistema: **whoami /user**, nos muestra el nombre de nuestro usuario actual y su SID.

```
C:\Users\César>whoami /user

INFORMACIÓN DE USUARIO
-----

Nombre de usuario      SID
=====
windows10linux\césar S-1-5-21-2808957090-3584531727-2581535050-1000

C:\Users\César>whoami.exe
windows10linux\césar

C:\Users\César>
```

El último número, en este caso 1000, se conoce como **RID (identificador relativo del usuario)** y todo lo que está delante del mismo identifica el dominio al que pertenece ese usuario. En concreto, esos tres grandes números que se observan (2808957090-3584531727-2581535050) se generan automáticamente y al azar cada vez que instalamos un sistema operativo Windows, y aparecerán en todas las cuentas que creemos en dicho sistema. El RID del administrador siempre es el 500. Los RID de usuarios suelen comenzar en el 1000.

La parte del SID nos da información sobre el objeto con el que estamos trabajando. Así, por ejemplo, si hablamos de algunos grupos o usuarios especiales tenemos:

- S-1-1-0 → es el SID del grupo Todos (Everyone).
- S-1-2-0 → es el SID del grupo Usuarios locales.
- S-1-3-1 → es el SID de Creator – Owner.
- S-1-5 → este inicio de SID nos indica que estamos trabajando con un usuario o grupo normal.

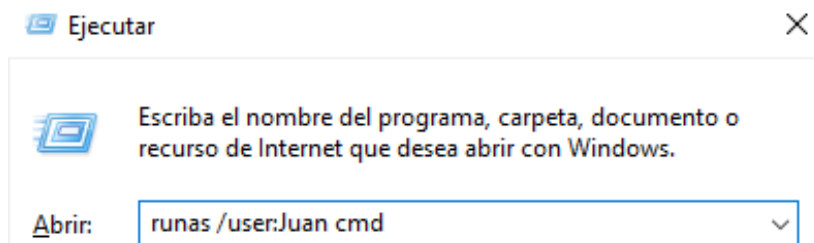
Si queremos ver no solo el SID que se le ha otorgado a nuestro usuario, sino el SID de todos los grupos a los que pertenece nuestro usuario, usaremos la orden con el parámetro **/groups**.

```
C:\Windows\system32>whoami /user /groups

INFORMACIÓN DE USUARIO
-----
Nombre de usuario      SID
=====
windows10linux\césar S-1-5-21-2808957090-3584531727-2581535050-1000

INFORMACIÓN DE GRUPO
-----
Nombre de grupo                                     Tipo      SID      Atributos
=====
Todos                                              Grupo conocido S-1-1-0   Grupo obliga
NT AUTHORITY\Cuenta local y miembro del grupo de administradores Grupo conocido S-1-5-114 Grupo obliga
BUILTIN\Administradores                          Alias      S-1-5-32-544 Grupo obliga
BUILTIN\Usuarios                                Alias      S-1-5-32-545 Grupo obliga
NT AUTHORITY\INTERACTIVE                          Grupo conocido S-1-5-4   Grupo obliga
INICIO DE SESIÓN EN LA CONSOLA                    Grupo conocido S-1-2-1   Grupo obliga
NT AUTHORITY\Usuarios autenticados                 Grupo conocido S-1-5-11  Grupo obliga
NT AUTHORITY\Esta compañía                         Grupo conocido S-1-5-15  Grupo obliga
NT AUTHORITY\Cuenta local                          Grupo conocido S-1-5-113 Grupo obliga
LOCAL                                              Grupo conocido S-1-2-0   Grupo obliga
NT AUTHORITY\Autenticación NTLM                    Grupo conocido S-1-5-64-10 Grupo obliga
Etiqueta obligatoria\Nivel obligatorio alto        Etiqueta    S-1-16-12288
```

El comando **whoami** solo nos muestra información sobre el usuario actual, así que, si queremos ver los SID de distintos usuarios, tendremos que ejecutar dicha orden como dichos usuarios. Con la orden **runas** podremos ejecutar un Shell (sesión de texto) como otro usuario (ejecutar como...).



Con esto conseguiremos abrir una nueva shell en la que seremos el usuario que estamos suplantando, por lo que si ejecutamos en dicha ventana **whoami** nos responderá con el nuevo usuario.

## 4 Listas de control de acceso (ACL)

Un recurso local es cualquier elemento del sistema que permite ser usado por los usuarios. Así, una impresora, una carpeta, un fichero o una conexión de red son recursos. Por cada recurso el sistema cuenta con una lista donde anota los usuarios que pueden usar dicho recurso y de qué forma pueden usarlo. Si un usuario no está en esta lista, el sistema le impedirá usar el recurso.

Ya hemos visto que el sistema no ve nombres de usuarios y grupos, realmente ve identificadores de seguridad (SID), de modo que lo que dicha lista realmente tiene en su interior es una serie de SIDs y los permisos que cada uno de esos SIDs tiene sobre el recurso. Esta lista con la que cuenta cada recurso se conoce como **ACL (Access Control List o Lista de Control de Acceso)**.

Cuando un usuario intenta acceder a un recurso el sistema comprobará si en la ACL de dicho recurso aparece el SID del usuario, y en caso contrario comprobará si aparece el SID de algún grupo al que pertenezca el usuario. Si no aparece en la ACL ningún SID del usuario o de algún grupo del que sea miembro, el sistema niega el acceso al usuario a dicho recurso.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) está permitida para ese SID en la ACL. Si lo está, le autoriza para hacerlo, en caso contrario se lo impide.

Puede ocurrir que un usuario tenga permisos contradictorios. Imaginemos que en la ACL de la carpeta DATOS aparece que el SID del usuario usu1 puede escribir en la carpeta, pero usu1 pertenece al grupo Alumnos, que aparece en el ACL de DATOS como que no tiene derecho a escribir. Bien, en este caso se aplica la siguiente regla:

**Lo que más pesa en cualquier ACL es la denegación implícita de permisos. Si un permiso está denegado, no se sigue mirando, se deniega inmediatamente.**

### 4.1 Ver la lista de control de acceso (ACL) de una carpeta o archivo

Una ACL contiene una **ACE (Access Control Entry o Entrada de Control de Acceso)**, que indica qué permisos tiene cada usuario, es decir, una ACE para cada usuario o grupo. Los permisos se asignan en forma de permisos positivos (permite) y negativos (deniega). En una ACL primero están situados los permisos denegados y a continuación los permitidos. ¿Cómo podemos observar esto visualmente?

Si hacemos clic derecho sobre una carpeta o archivo y elegimos *Propiedades* y luego la pestaña “*Seguridad*”, veremos que nos aparecen los distintos usuarios y los permisos que tienen sobre dicha carpeta o archivo.

### 4.2 Herencia de permisos

Cualquier recurso que se crea hereda automáticamente la ACL de su recurso padre, si es que existe. Si asignamos unos permisos a un directorio y creamos otro directorio dentro de éste, el nuevo directorio hereda los permisos del directorio padre o contenedor.

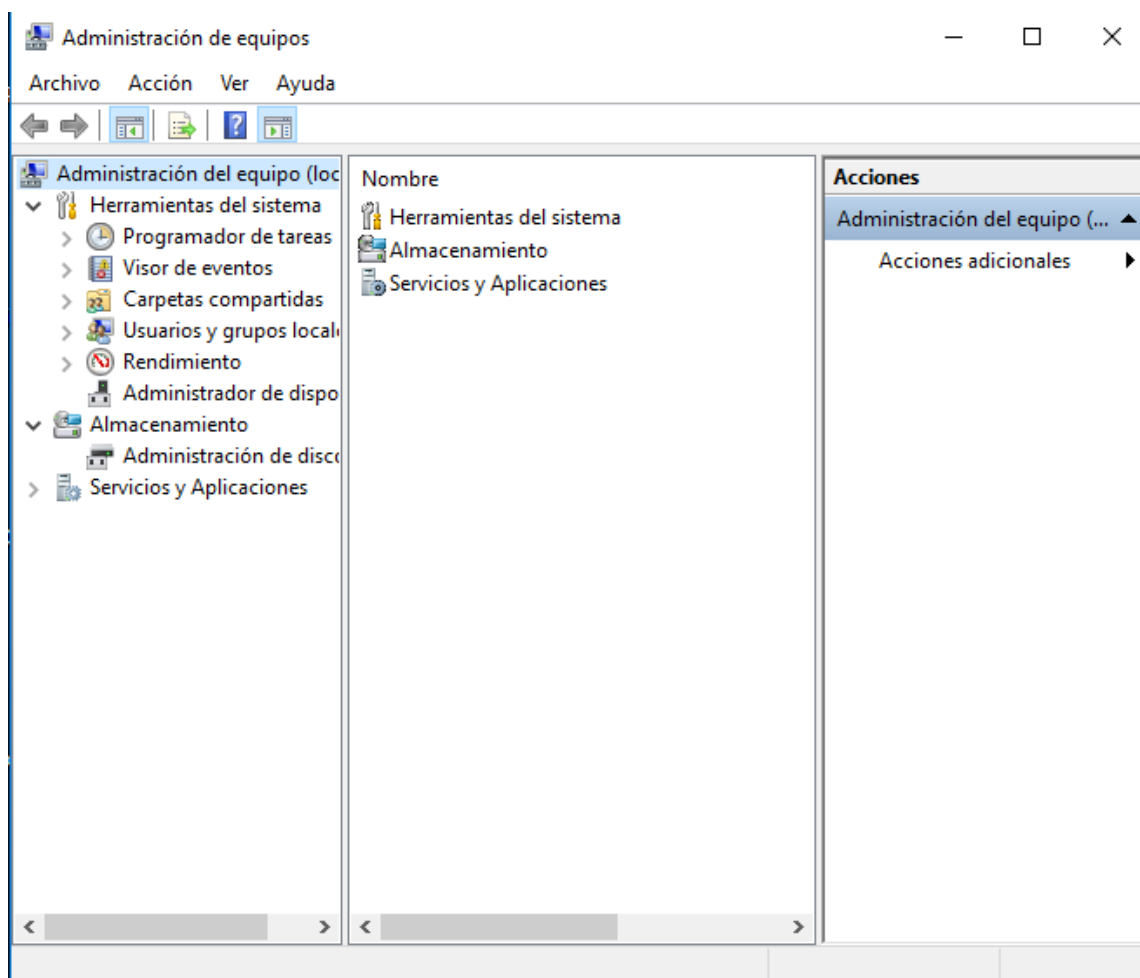
No obstante, podemos hacer que se rompa esa herencia si es que deseamos modificar los permisos al nuevo directorio y que no herede los de su padre o contenedor. Para ello, accedemos al botón de **Opciones avanzadas**, que está en la pestaña “*Seguridad*”.

En la primera pestaña, **Permisos**, nos muestra los permisos que existen sobre ese elemento, y tenemos el botón **Deshabilitar herencia**. Si hacemos clic en él, nos muestra un mensaje de advertencia explicándonos la acción importante que vamos a llevar a cabo y ofreciéndonos dos alternativas: “*Convertir los permisos heredados en permisos explícitos en este objeto*” o “*Quitar todos los permisos heredados de este objeto*”.

## 5 Administrando el equipo

Administración de equipos es un conjunto de herramientas administrativas de Windows que se pueden utilizar para administrar un equipo local o remoto. Las herramientas están organizadas en una única consola, que facilita la presentación de las propiedades administrativas y el acceso a las herramientas necesarias para realizar las tareas de administración de equipos.

Para acceder al administrador de equipos es: Panel de control → Sistema y seguridad → Herramientas administrativas → Administración de equipos. O también, de igual forma que se indicó anteriormente (apartado 1.2), podemos llegar a ella pinchando botón derecho sobre Mi PC (o Equipo) y seleccionando Administrar.



La consola Administración de equipos consta de una ventana dividida en dos paneles. En el panel izquierdo aparece el árbol de consola y el derecho muestra los detalles. Al hacer clic en un elemento del árbol de consola, la información acerca del elemento se muestra en el panel de detalles. La información que se muestra es específica del elemento seleccionado.

Las herramientas administrativas de Administración de equipos se agrupan en las tres categorías siguientes en el árbol de consola:

- Herramientas del sistema.
- Almacenamiento.
- Servicios y Aplicaciones.

Cada categoría incluye varias herramientas o servicios.

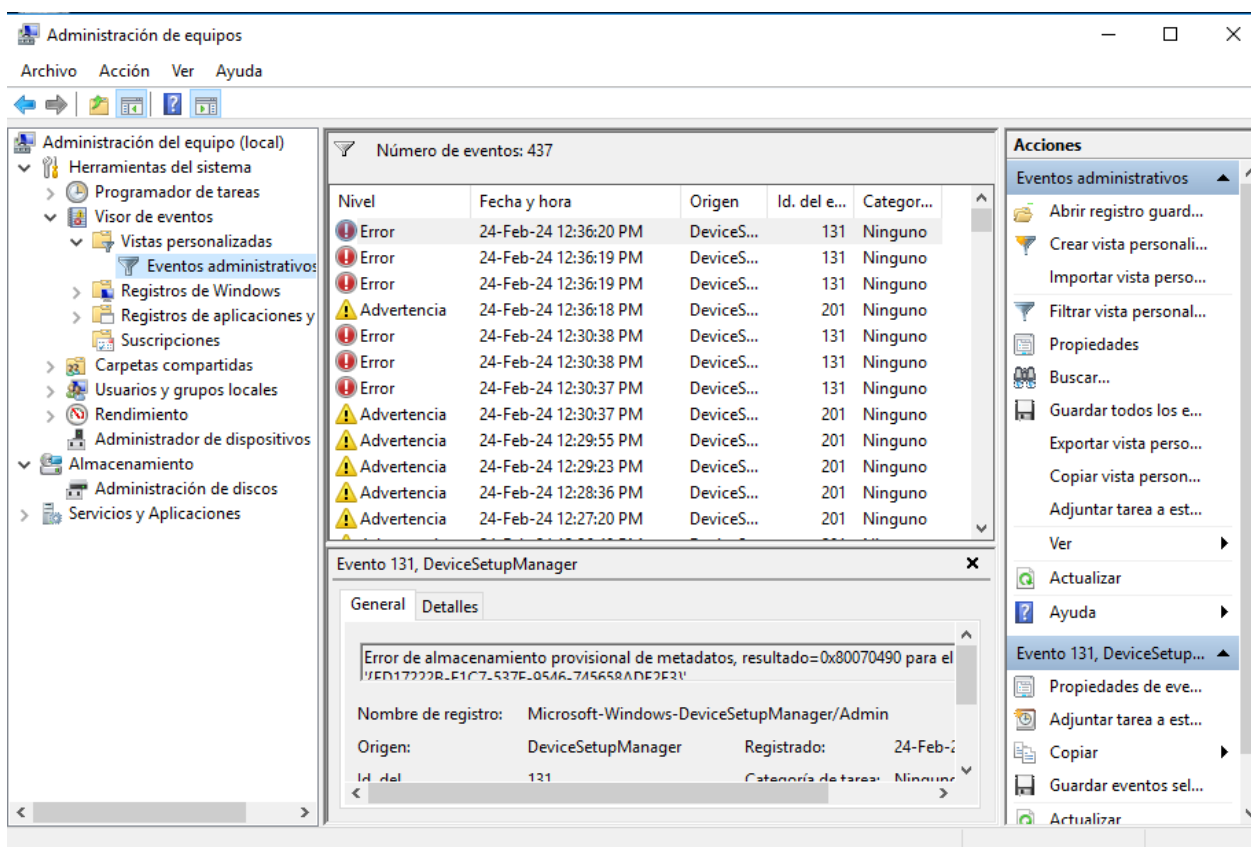
## 5.1 Herramientas del sistema

### 5.1.1 Programador de tareas

Permite programar para determinadas horas la ejecución de tareas.

### 5.1.2 Visor de eventos

El **visor de eventos** es la herramienta que permite examinar y administrar los eventos ocurridos en el equipo. Un **evento** o **suceso** es un acontecimiento significativo del sistema o de una aplicación que requiere una notificación al usuario. Ejemplos de eventos son actualizaciones automáticas, cierres inesperados de programas, incidencias con el hardware, eventos de los controladores de dispositivos, errores o fallos en la ejecución de los mismos, servicios que se arrancan o detienen, eventos de seguridad del sistema, información de accesos, etc.



Se puede observar que el visor de eventos se organiza como un árbol de directorios del que cuelgan subcarpetas:

- Vistas personalizadas con Eventos administrativos.
- Registros de Windows, divididos en Aplicación, Seguridad, Instalación, Sistema y Eventos reenviados.
- Registros de aplicaciones y servicios, los cuales incluyen eventos de software y de hardware.
- Suscripciones.

En la parte central de la ventana del visor de eventos puedes acceder a los eventos particulares y en el panel Acciones de la derecha tienes disponibles todas las acciones que de manera contextual puedes realizar con los elementos seleccionados.

Por ejemplo, cuando una aplicación o dispositivo no te funcione correctamente, puedes acudir al visor de eventos y recabar información. Quizá te ayude a solucionar el problema y a refinar el funcionamiento de tu equipo.

**Campos del visor de eventos**

- **Nivel del evento.** Icono que indica la importancia del evento.
- **Fecha y hora.** La fecha y hora en que se produjo el evento.
- **Origen.** Es el software que ha registrado el suceso. Puede tratarse de una aplicación o de un componente del sistema, por ejemplo, un controlador.
- **Identificador del evento.** El número de identificación del evento.
- **Categoría.** La categoría en la que esté clasificado el evento.
- **Usuario.** El usuario que ha generado el suceso.
- **Equipo.** El ordenador en el que se ha generado el suceso.

**Tipos de sucesos del visor de sucesos**- **Error**

Se refiere a un problema importante. Ejemplo: una aplicación que falla al cargarse.

- **Advertencia**

Suceso que no es importante necesariamente, pero que indica la posibilidad de problemas en el futuro. Ejemplo: si queda poco espacio de disco, se registrará una advertencia.

- **Información**

Describe el funcionamiento correcto de una aplicación, un controlador o un servicio. Ejemplo: cuando se carga correctamente un controlador de red, se registrará un suceso de información.

- **Acceso correcto auditado**

Se refiere a un intento de acceso de seguridad correcto auditado. Ejemplo: un intento correcto de inicio de sesión en el sistema de un usuario, se registrará como un suceso de acceso correcto auditado.

- **Acceso erróneo auditado**

Se refiere a un intento de acceso de seguridad erróneo auditado. Ejemplo: si un usuario intenta tener acceso a una unidad de red y no lo consigue, se registrará como un suceso de acceso erróneo auditado.

**5.1.3 Carpetas compartidas**

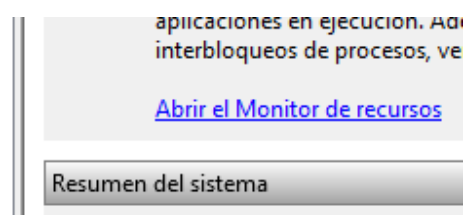
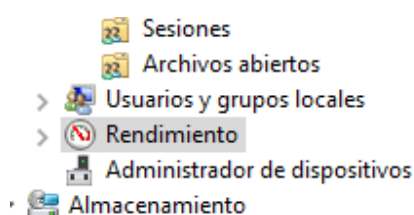
Utiliza esta herramienta para ver las conexiones y los recursos que hay en uso en el equipo. Es posible crear, ver y administrar recursos compartidos, ver las sesiones y los archivos abiertos, y cerrar archivos y desconectar sesiones.

**5.1.4 Usuarios y grupos locales**

Utiliza esta herramienta para crear y administrar las cuentas de usuarios locales y grupos.

**5.1.5 Rendimiento**

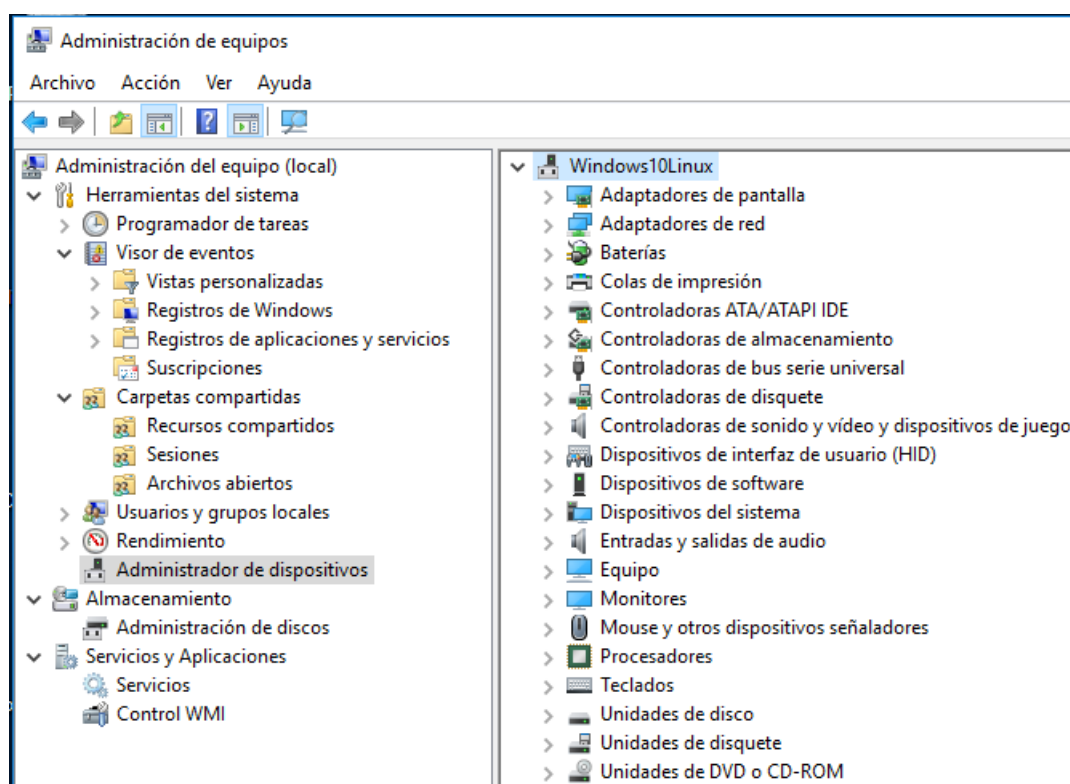
Su principal característica es que da acceso al **Monitor de recursos** para revisar datos de rendimiento de dispositivos del sistema, como CPU, discos duros, tráfico de red o uso de la memoria.





### 5.1.6 Administrador de dispositivos

Utiliza esta herramienta para ver los dispositivos hardware instalados en el equipo, actualizar los controladores de dispositivo, modificar la configuración de hardware y solucionar conflictos con los dispositivos.



## 5.2 Almacenamiento

### 5.2.1 Administración de discos

Muestra los **volúmenes** junto a su información, como el tipo de sistema de archivos (NTFS, FAT32, etc.), su estado (partición de recuperación, partición primaria, de arranque, etc.) Utiliza la herramienta de administración de discos para realizar tareas relacionadas con el disco.

También se puede acceder al administrador de discos directamente con el comando **diskmgmt.msc**.

## 5.3 Servicios y Aplicaciones

Un **servicio** es un tipo de aplicación que normalmente se ejecuta en segundo plano. Los servicios proporcionan a los usuarios aplicaciones que incorporan diversas formas de poder utilizar los recursos del sistema operativo, multiusuario la mayoría de las veces.

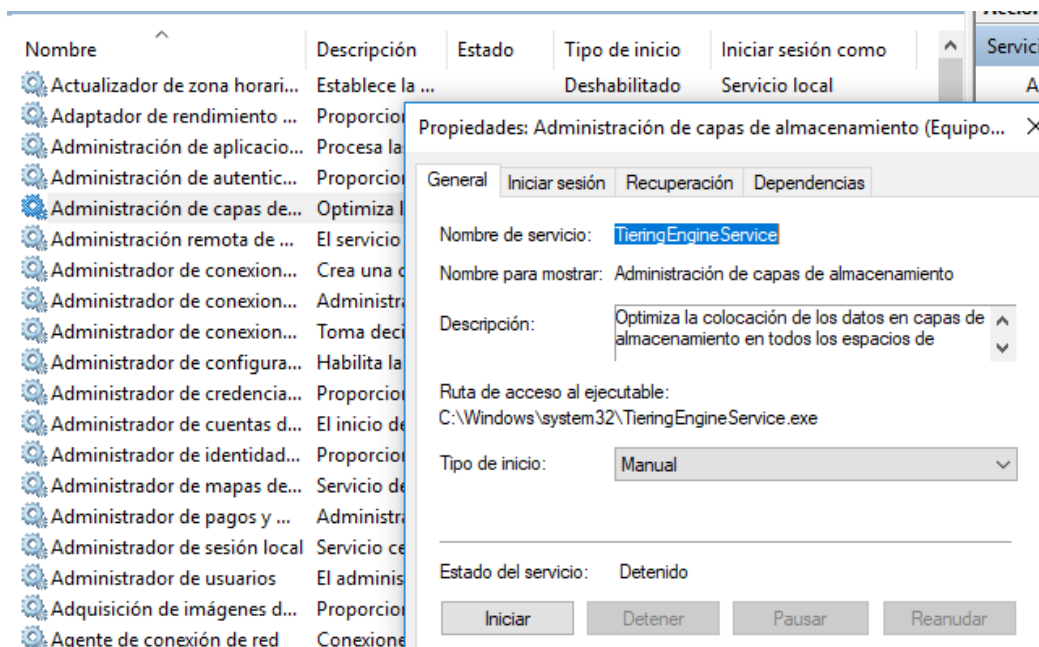
Algunos de los servicios lanzados por los sistemas operativos son aplicaciones del tipo cliente-servidor, servidores web, servidores de bases de datos y otras aplicaciones basadas en servidores, tanto de forma local como a través de una red.

En general, los servicios se utilizan para **iniciar, detener, pausar-reanudar o deshabilitar** programas y aplicaciones (que a su vez pueden ser servicios) en equipos locales y remotos. La mayoría de los servicios se instalan en un sistema informático al instalar el propio sistema operativo. Muchas aplicaciones, especialmente aquellas que utilizan servicios de red, acceso a bases remotas de datos y otras muchas, instalan sus propios servicios, que se añaden a los que ya instaló en su momento el propio sistema operativo.



Estos servicios son esenciales para el funcionamiento de muchas de las aplicaciones y del propio sistema operativo. Si estos programas, o sea, los servicios, no estuvieran ejecutándose, muchas aplicaciones no funcionarían o algo tan común como el acceso a Internet sería imposible.

Desde esta opción del administrador de equipos se pueden consultar los servicios de Windows y ver cuáles están funcionando y cuáles no. También es posible acceder directamente a la consola de servicios mediante la orden **services.msc**.



## 6 Editor de directivas de grupo local

Por último, hay que señalar el editor de directivas de grupo local para llevar a cabo la configuración de las directivas del equipo, además de las directivas de seguridad vistas en el apartado 2. Se muestra mediante la consola **gpedit.msc**

