Administración de procesos para

Windows

En este tutorial les enseñaremos como se ejecutan los distintos procesos a través de ***Windows.*** También les mostraremos como a acceder al administrador y como ver los distintos procesos que se están ejecutando.

- La **administración de procesos** o **task manager** es una interfaz que nos permite ver y ejecutar procesos u aplicaciones, algo muy importante al momento de poder explotar todas las características de nuestro hardware y sistema operativo.

  Existen dos modos de acceder al administrador de tareas:

1ro Se puede ingresar al administrador de tareas de Windows con la combinación de teclas **Ctrl+Alt+Del**.

2do Puedes acceder a esta a través de Inicio cuando escribas en la opción ejecutar de inicio administrador de tareas o task manager.

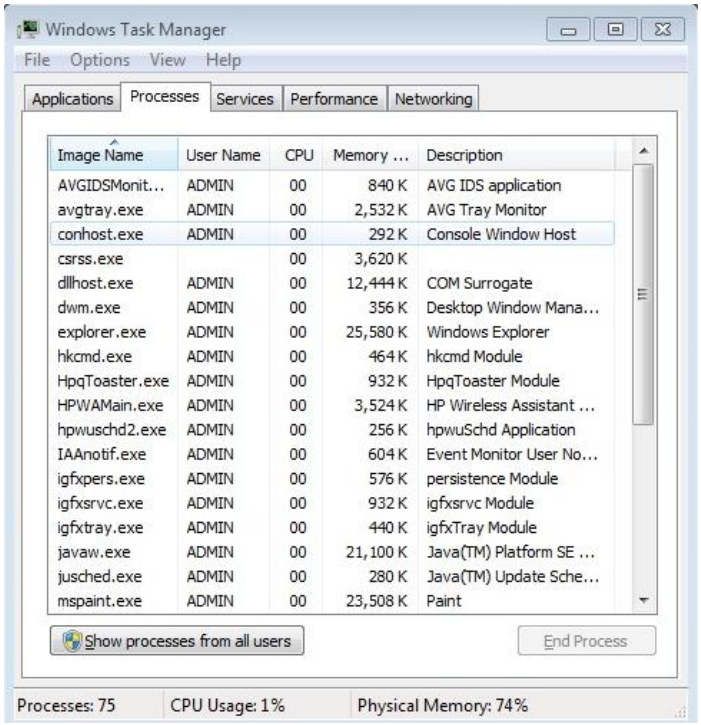
3ro Por último puedes acceder a este presionando la tecla Windows+R para entrar a ejecutar. Desde ahí escribe **taskmgr.exe.**

- El **command Prompt** o **cmd** por otra parte es un interprete de comandos en OS/2 y sistemas basados en Windows NT que también nos permite ver y administrar los distintos procesos de nuestro sistema operativo. Podemos acceder a este y ver los distintos procesos de la siguiente manera:

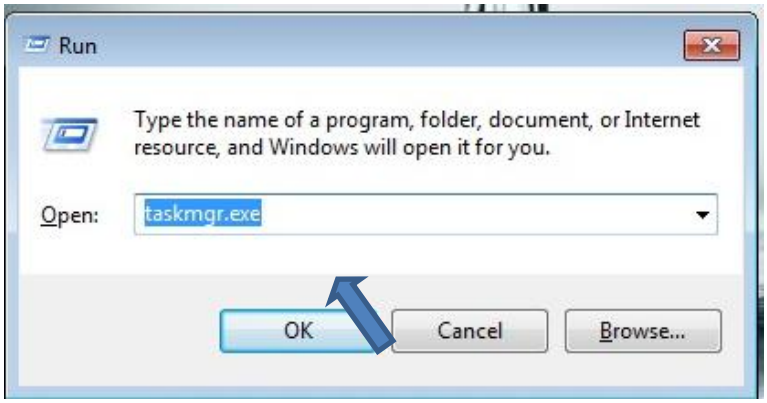
1ro Para acceder a la línea de comandos presionamos las teclas de Windows+R para que salga el cuadro de ejecutar, luego escribimos **cmd.exe** y le damos a OK.

2do También podemos acceder a este directamente buscándolo en menú inicio.

En el administrador de tareas:



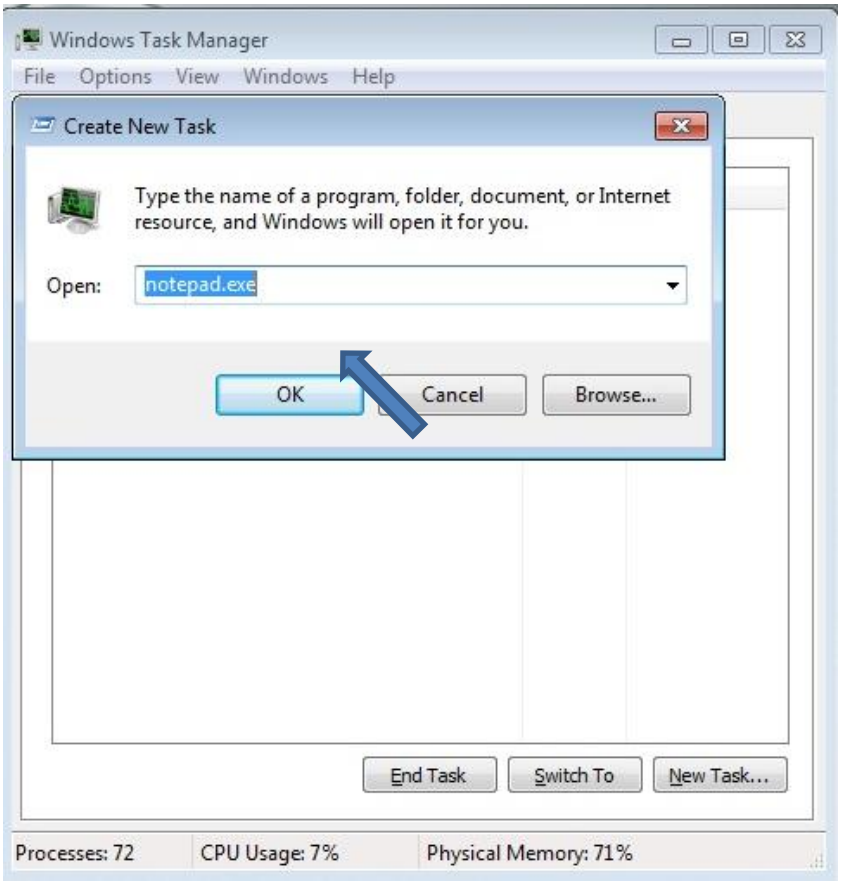
Esta imagen muestra los distintos procesos que se están ejecutando en el sistema operativo.



Le damos a OK para que el administrador de tareas salga automáticamente.

Como ejecutar un proceso

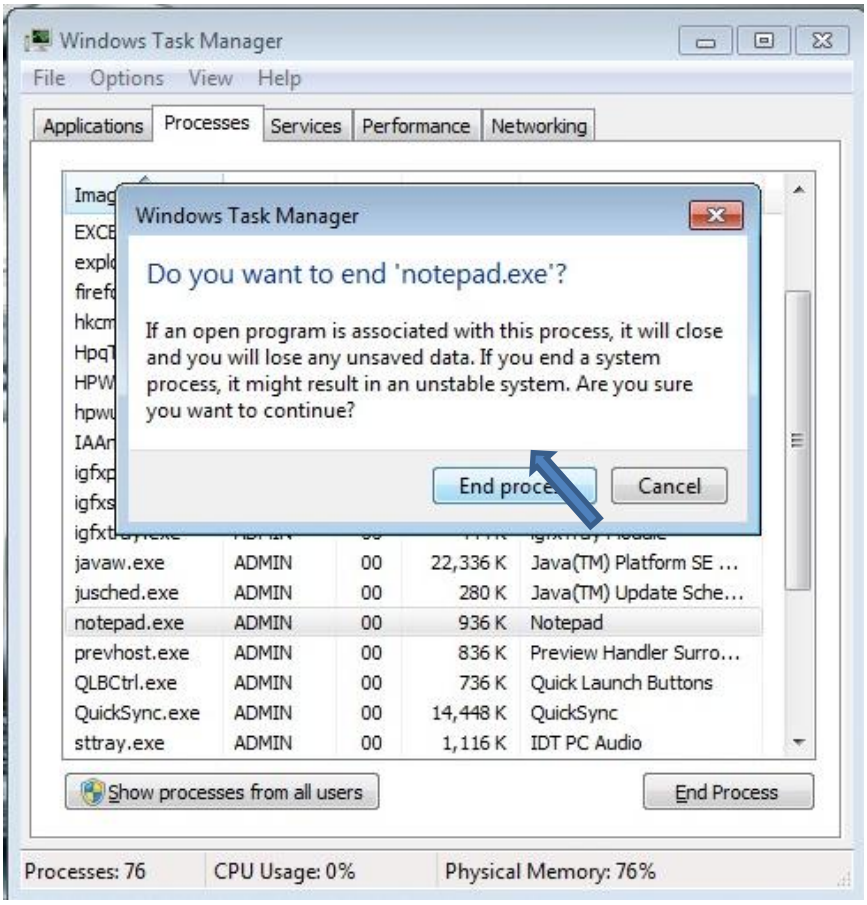
Para abrir el administrador de tareas en línea gráfica se procede a este mediante las teclas **Ctrl+Alt+Delete** o mediante la ejecución de este en inicio. Luego que ya lo tenemos localizado procedemos a abrir la pestaña de aplicaciones, le damos un clic a una tarea nueva y por último escribimos el proceso que queremos ejecutar en nuestro computador.



Luego que le demos clic a OK el notepad o el bloc de notas abrirá automáticamente.

Teminar Un Proceso:

Para terminar un proceso por línea gráfica lo primero que tenemos que hacer es abrir el administrador de tareas luego abrimos la pestaña que dice procesos y le damos clic al proceso que queremos terminar, le damos un clic derecho a este y seleccionamos terminar proceso, mas adelante aparecerá una pequeño cuadro de advertencia del administrador de tareas. Si queremos que el proceso termine le damos a aceptar y si queremos cancelar la operación le damos a cancelar.



Si el proceso no funciona lo que debemos hacer es terminar con el mismo, que se encuentran gastando valiosos recursos pero que no se va a ejecutar.

Como cambiarle la prioridad a un proceso

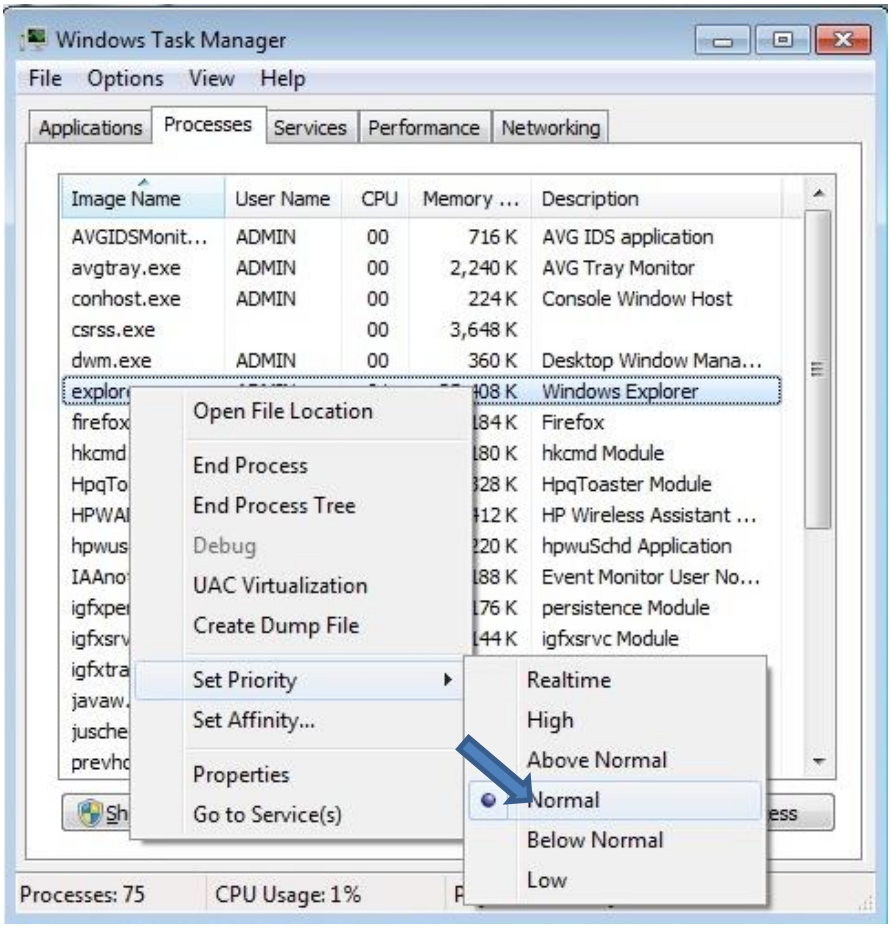
Es común trabajar con varias aplicaciones simultáneamente en su ordenador. Algunos requieren una gran cantidad de recursos para su buen funcionamiento y otros no lo requieren a lo mínimo. De forma predeterminada, el sistema operativo le da a cada nivel la misma prioridad, el nivel normal. Cuando se habla de la prioridad nos referimos a que el procesador le da a cada uno de los procesos al momento el compartimiento con el resto de la energía que proveen. Por ende si es conveniente cambiarle la prioridad al proceso, pues cámbiele el nivel que desee.

Al ejecutar distintas aplicaciones simultáneas en Windows el sistema asigna una serie de prioridades que, a menos que se especifique lo contrario, son iguales para todos. En condiciones normales, todos los procesos que se ejecutan en Windows tienen la misma prioridad, pero si estamos utilizando una aplicación que creemos que necesita más recursos o que es más lenta de la cuenta, podemos modificar su prioridad.

Vamos a ver cómo se puede cambiar de forma individual el nivel de prioridad de una aplicación en ejecución. Al abrir el administrador de tareas podrá cambiarle la prioridad al proceso, luego le damos clic derecho sobre el proceso que queremos cambiar y le damos a **poner prioridad** o **set priority**.

Niveles de proceso:

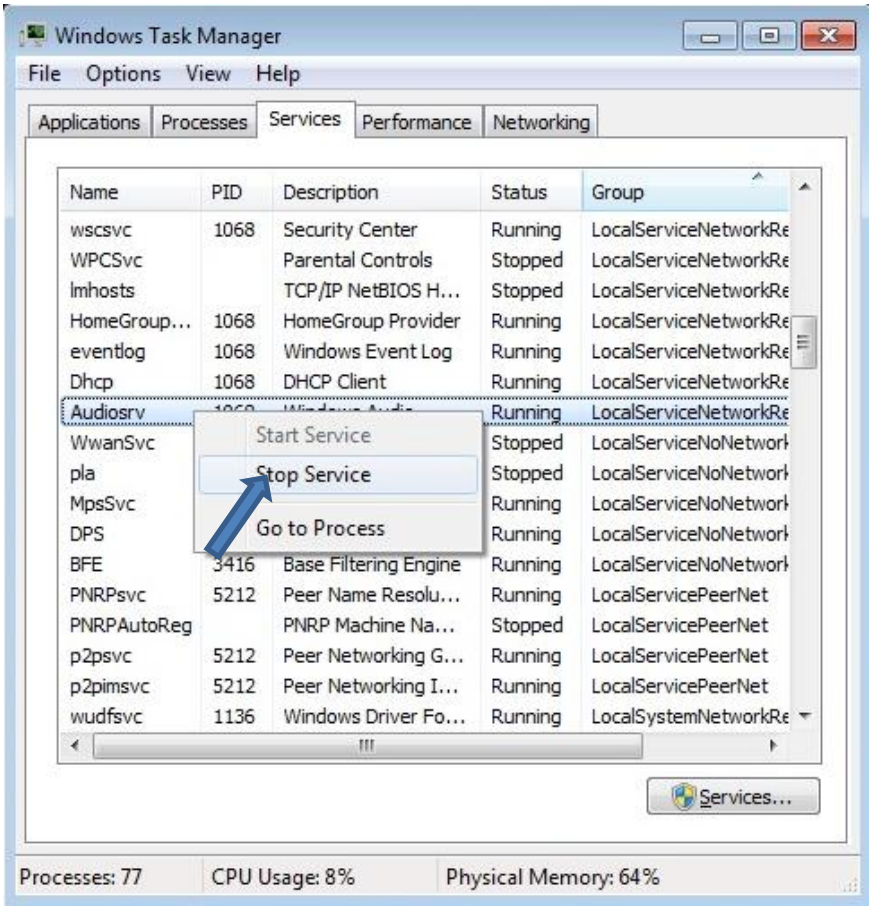
- Tiempo real o Real Time
- Alta o High
- Arriba de lo normal o Above Normal
- Normal
- Debajo de lo normal o Below Normal
- Baja o Low



De esta forma podemos otorgarle a un proceso la prioridad que deseemos.

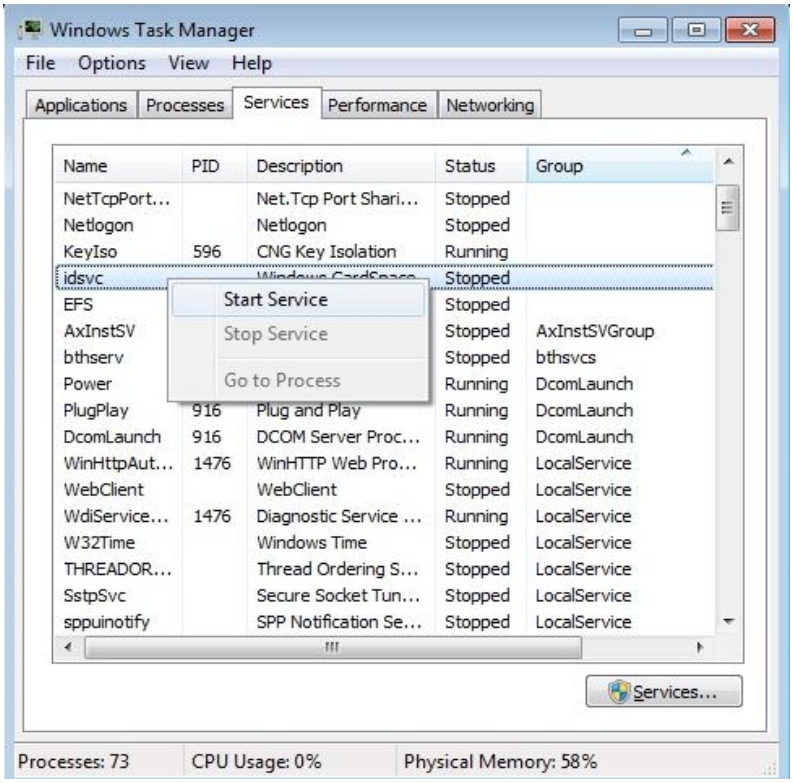
Como suspender un proceso

Para suspender un proceso por línea gráfica abrimos el administrador de tareas, luego abrimos la pestaña de servicios, le damos clic derecho al servicio que queremos suspender y por ultimo le damos a **detener el proceso** o **stop service**.



Como reanudar un servicio

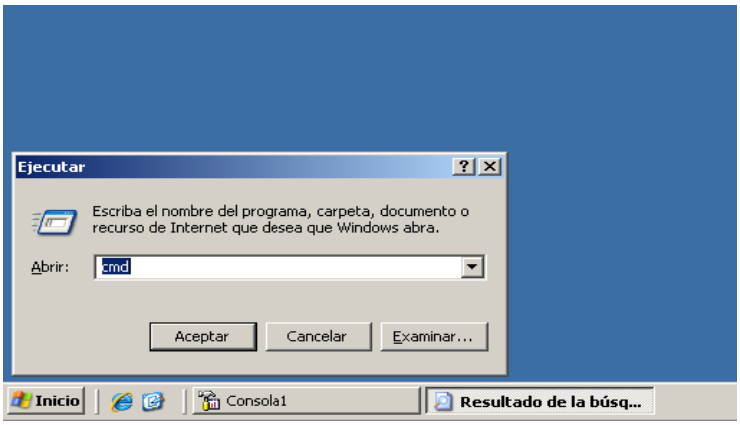
Para reanudar un proceso se procede a abrir el administrador de tareas, le damos a servicios y seleccionamos el servicio que queremos reanudar dándole clic a **start Service.**

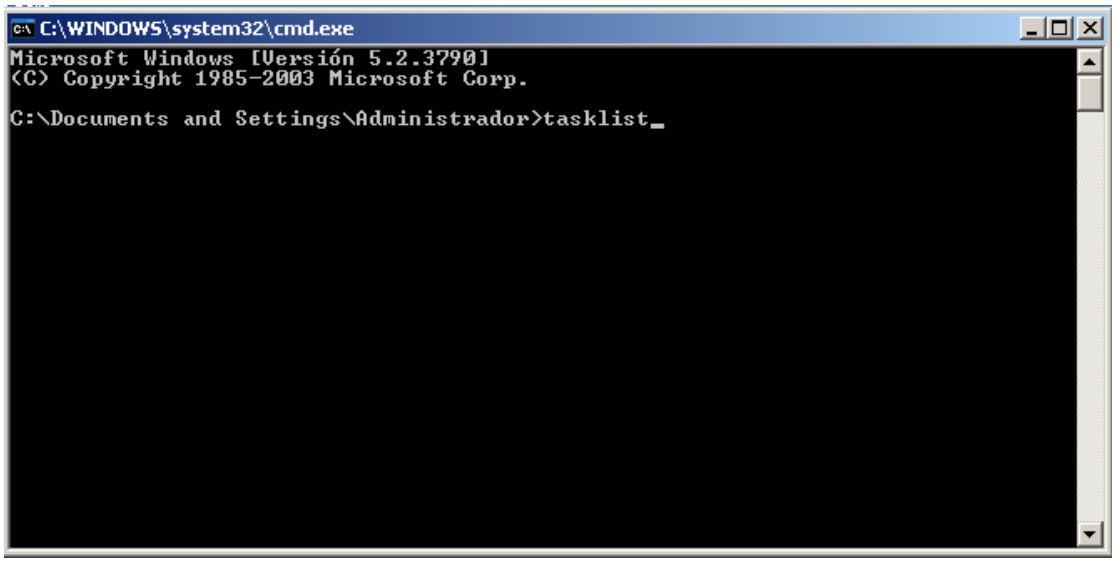


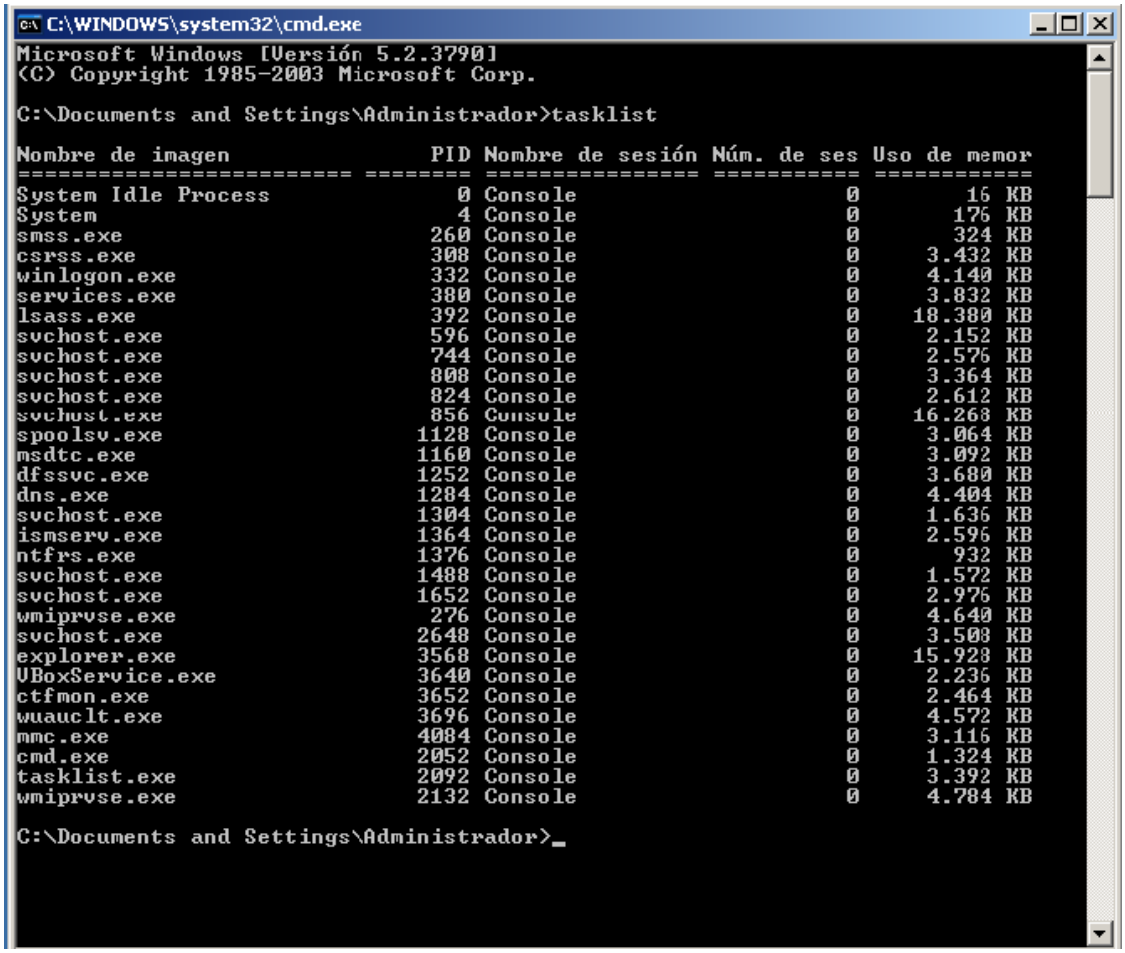
De esta forma reanudamos el proceso que fue detenido anteriormente.

Por Líneas de Comandos

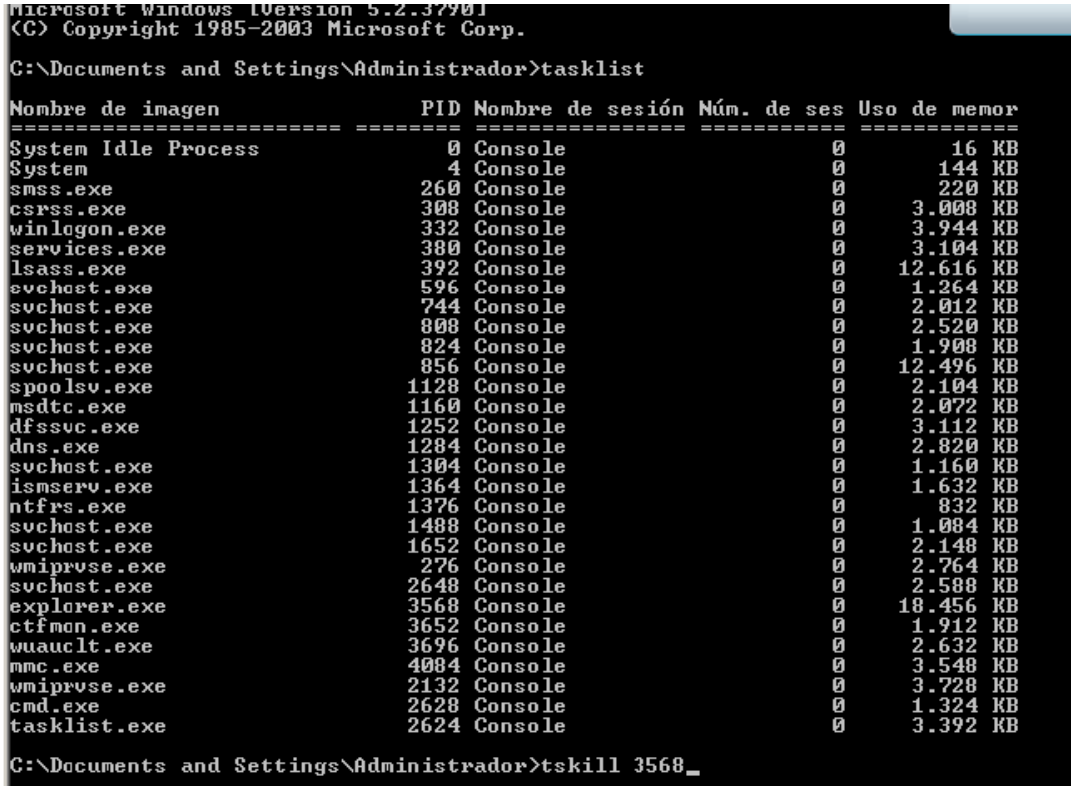
Para administrar procesos por CLI simplemente de click en inicio/ejecutar y escriba CMD y le abrirá la línea de comandos, en esta escriba tasklist y le mostrara una lista con todos los procesos, parecida a la 3ra imagen;



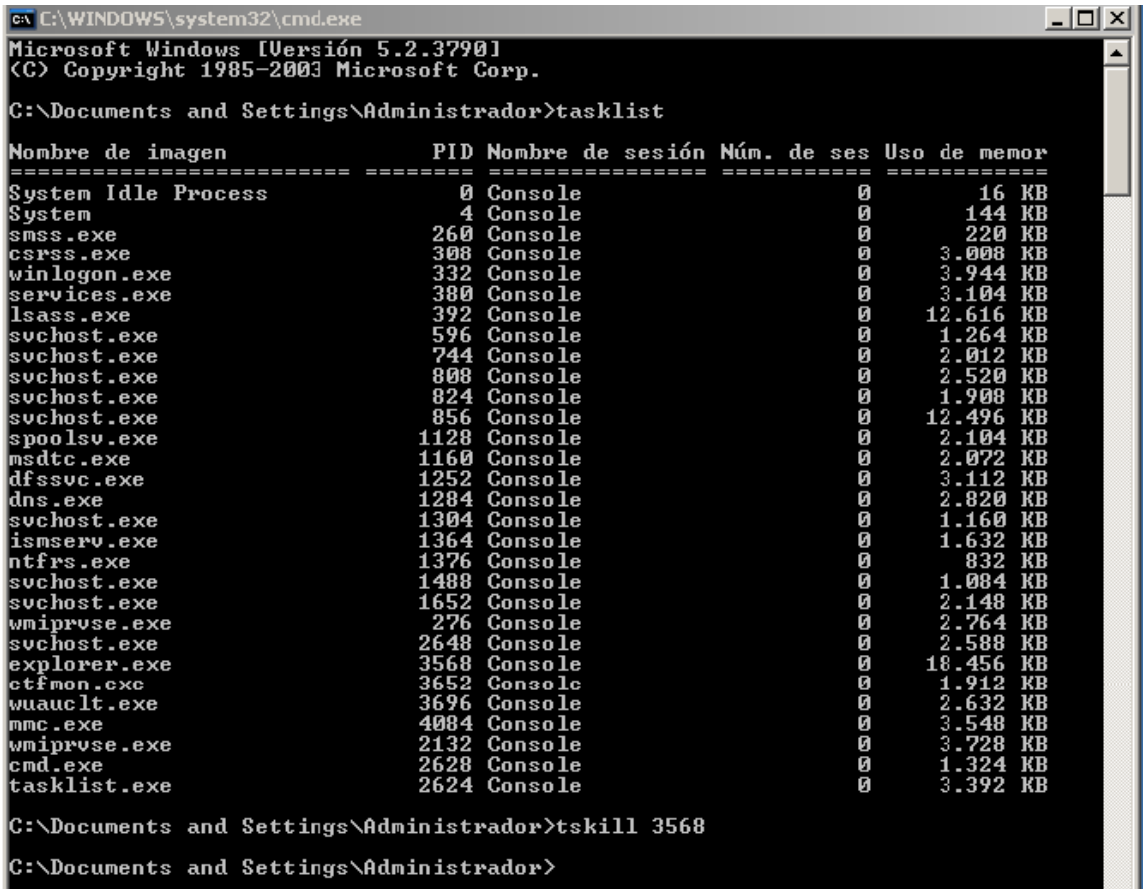




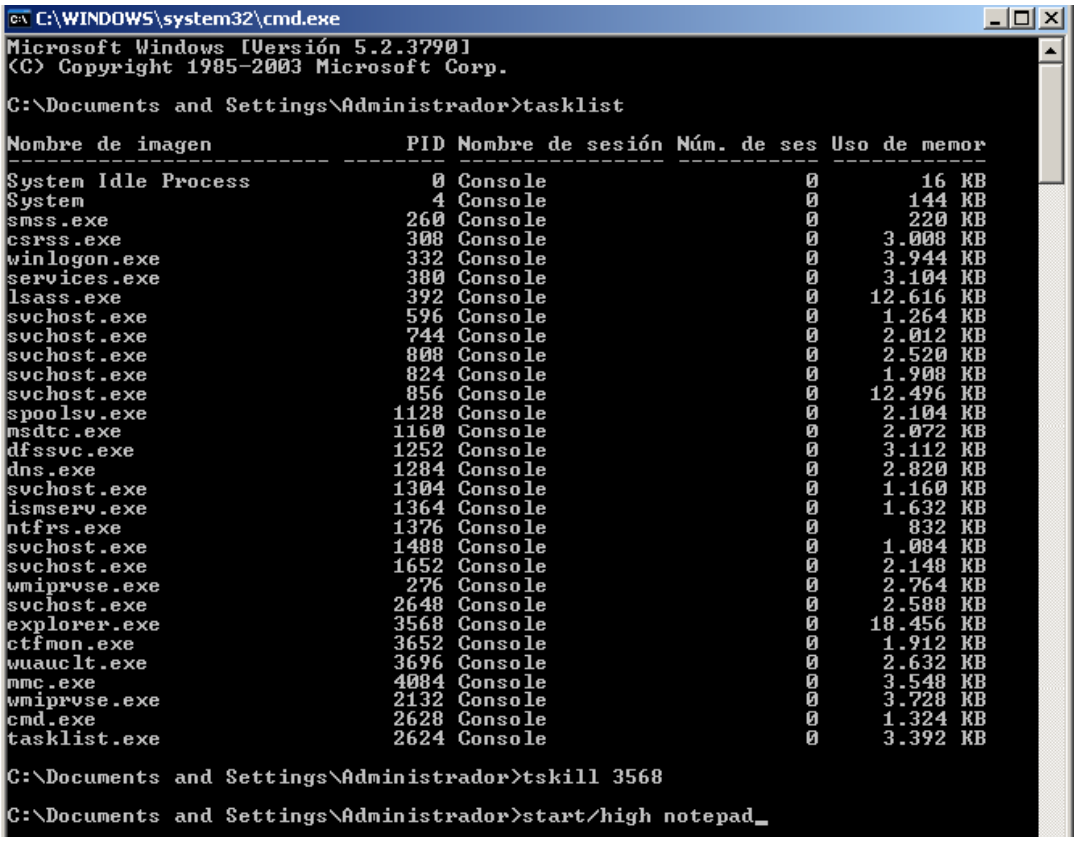
Para terminar con un proceso simplemente escriba “tskill y el numero de PID, como en el ejemplo de abajo

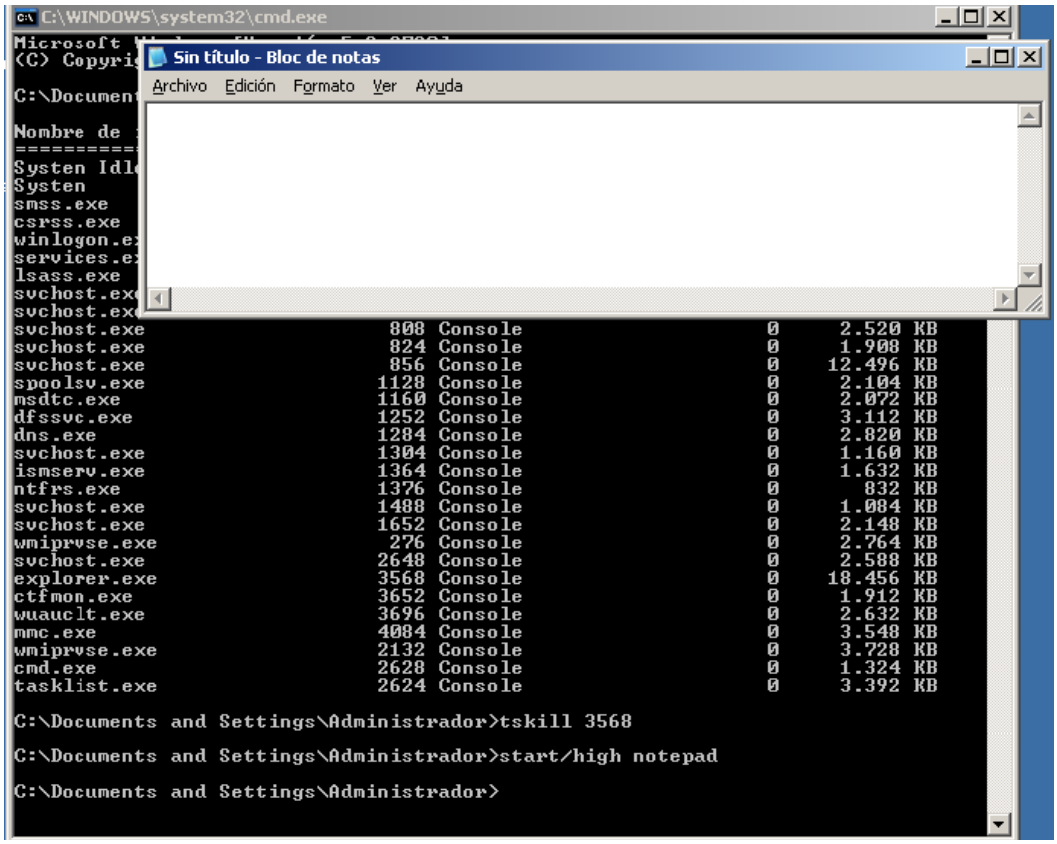


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrador>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process               0 Console                    0         16 KB
System                            4 Console                    0        144 KB
smss.exe                        260 Console                    0        220 KB
csrss.exe                       308 Console                    0      3.008 KB
winlogon.exe                    332 Console                    0      3.944 KB
services.exe                    380 Console                    0      3.104 KB
lsass.exe                       392 Console                    0     12.616 KB
svchost.exe                     596 Console                    0      1.264 KB
svchost.exe                     744 Console                    0      2.012 KB
svchost.exe                     808 Console                    0      2.520 KB
svchost.exe                     824 Console                    0      1.908 KB
svchost.exe                     856 Console                    0     12.496 KB
spoolsv.exe                    1128 Console                    0      2.104 KB
msdtc.exe                      1160 Console                    0      2.072 KB
dfssvc.exe                     1252 Console                    0      3.112 KB
dns.exe                        1284 Console                    0      2.820 KB
svchost.exe                    1304 Console                    0      1.160 KB
ismserv.exe                    1364 Console                    0      1.632 KB
ntfrs.exe                      1376 Console                    0        832 KB
svchost.exe                    1488 Console                    0      1.084 KB
svchost.exe                    1652 Console                    0      2.148 KB
wmiprvse.exe                    276 Console                    0      2.764 KB
svchost.exe                    2648 Console                    0      2.588 KB
explorer.exe                   3568 Console                    0     18.456 KB
ctfmon.exe                     3652 Console                    0      1.912 KB
wuauclt.exe                    3696 Console                    0      2.632 KB
mmc.exe                        4084 Console                    0      3.548 KB
wmiprvse.exe                   2132 Console                    0      3.728 KB
cmd.exe                        2628 Console                    0      1.324 KB
tasklist.exe                   2624 Console                    0      3.392 KB

C:\Documents and Settings\Administrador>tskill 3568_
```

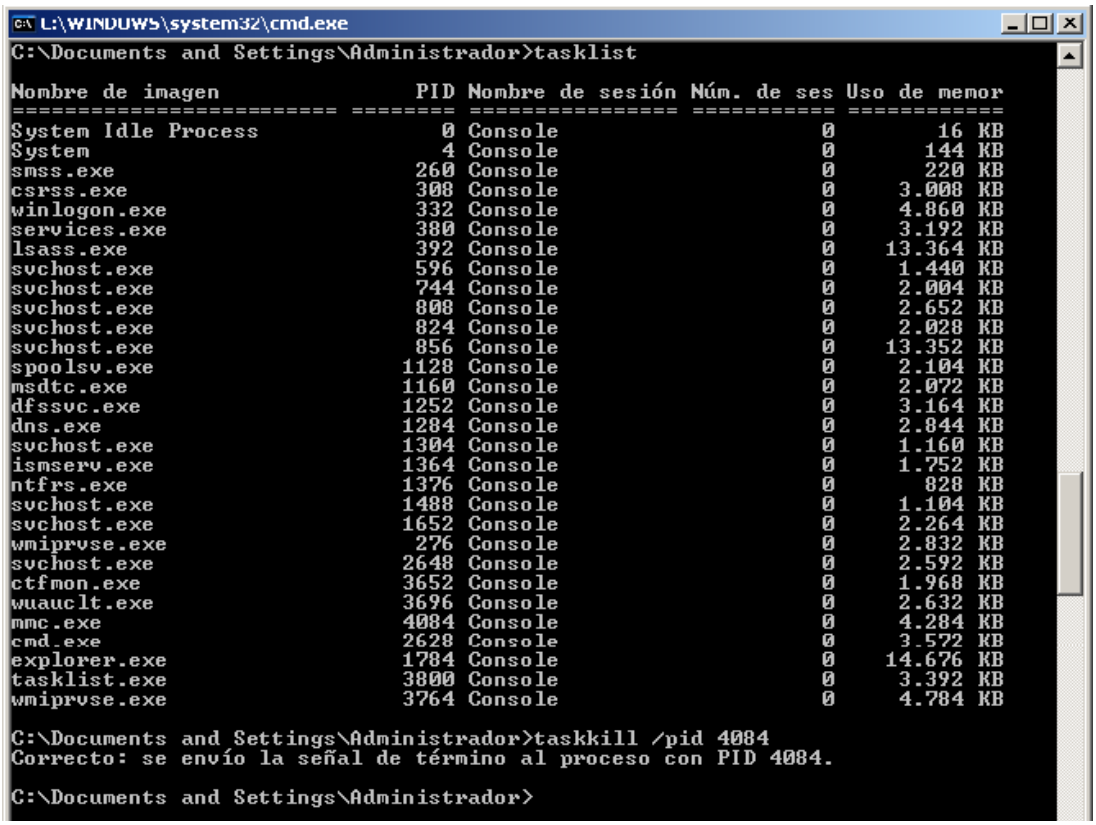


Luego para iniciar una tarea con una prioridad especifica escriba “start/(high, above normal,below,normal,low)” vea el ejemplo en la imagen de abajo.

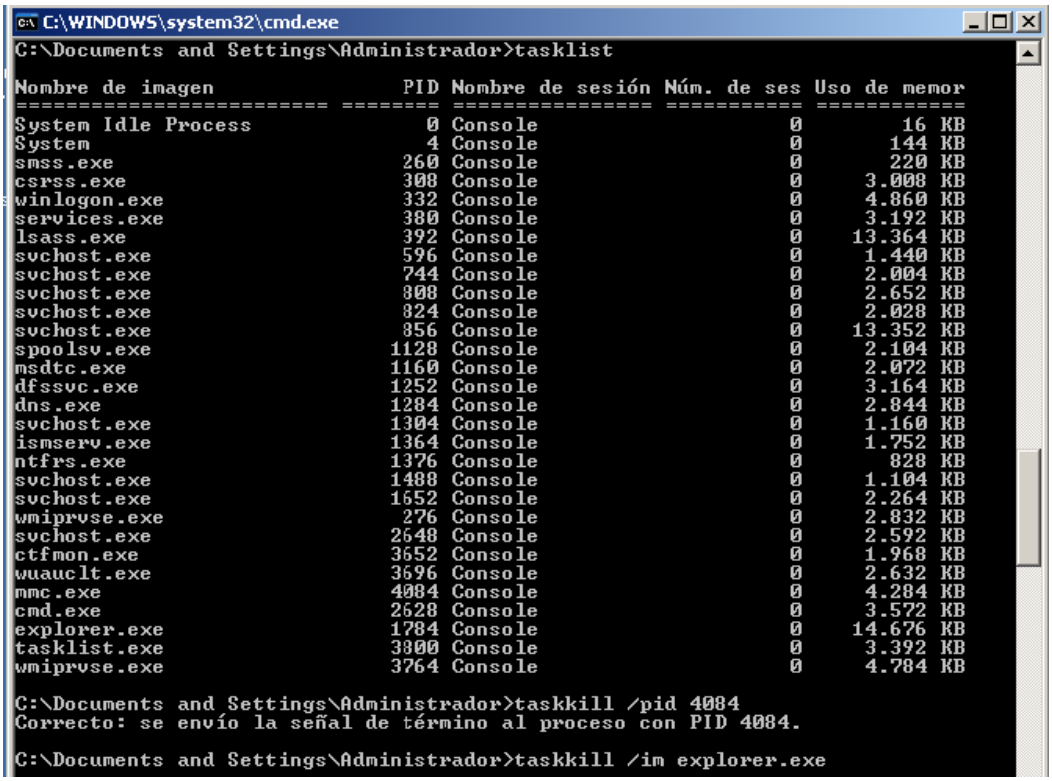

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrador>tasklist
Nombre de imagen PID Nombre de sesión Núm. de ses Uso de memor
System Idle Process 0 Console 0 16 KB
System 4 Console 0 144 KB
smss.exe 260 Console 0 220 KB
csrss.exe 308 Console 0 3.008 KB
winlogon.exe 332 Console 0 3.944 KB
services.exe 380 Console 0 3.104 KB
lsass.exe 392 Console 0 12.616 KB
svchost.exe 596 Console 0 1.264 KB
svchost.exe 744 Console 0 2.012 KB
svchost.exe 808 Console 0 2.520 KB
svchost.exe 824 Console 0 1.908 KB
svchost.exe 856 Console 0 12.496 KB
spoolsv.exe 1128 Console 0 2.104 KB
msdtc.exe 1160 Console 0 2.072 KB
dfssvc.exe 1252 Console 0 3.112 KB
dns.exe 1284 Console 0 2.820 KB
svchost.exe 1304 Console 0 1.160 KB
ismserv.exe 1364 Console 0 1.632 KB
ntfrs.exe 1376 Console 0 832 KB
svchost.exe 1488 Console 0 1.084 KB
svchost.exe 1652 Console 0 2.148 KB
wmiprvse.exe 276 Console 0 2.764 KB
svchost.exe 2648 Console 0 2.588 KB
explorer.exe 3568 Console 0 18.456 KB
ctfmon.exe 3652 Console 0 1.912 KB
wuauclt.exe 3696 Console 0 2.632 KB
mmc.exe 4084 Console 0 3.548 KB
wmiprvse.exe 2132 Console 0 3.728 KB
cmd.exe 2628 Console 0 1.324 KB
tasklist.exe 2624 Console 0 3.392 KB
C:\Documents and Settings\Administrador>tskill 3568
C:\Documents and Settings\Administrador>start/high notepad


C:\WINDOWS\system32\cmd.exe
Sin título - Bloc de notas
Archivo Edición Formato Ver Ayuda
svchost.exe 808 Console 0 2.520 KB
svchost.exe 824 Console 0 1.908 KB
svchost.exe 856 Console 0 12.496 KB
spoolsv.exe 1128 Console 0 2.104 KB
msdtc.exe 1160 Console 0 2.072 KB
dfssvc.exe 1252 Console 0 3.112 KB
dns.exe 1284 Console 0 2.820 KB
svchost.exe 1304 Console 0 1.160 KB
ismserv.exe 1364 Console 0 1.632 KB
ntfrs.exe 1376 Console 0 832 KB
svchost.exe 1488 Console 0 1.084 KB
svchost.exe 1652 Console 0 2.148 KB
wmiprvse.exe 276 Console 0 2.764 KB
svchost.exe 2648 Console 0 2.588 KB
explorer.exe 3568 Console 0 18.456 KB
ctfmon.exe 3652 Console 0 1.912 KB
wuauclt.exe 3696 Console 0 2.632 KB
mmc.exe 4084 Console 0 3.548 KB
wmiprvse.exe 2132 Console 0 3.728 KB
cmd.exe 2628 Console 0 1.324 KB
tasklist.exe 2624 Console 0 3.392 KB
C:\Documents and Settings\Administrador>tskill 3568
C:\Documents and Settings\Administrador>start/high notepad
C:\Documents and Settings\Administrador>

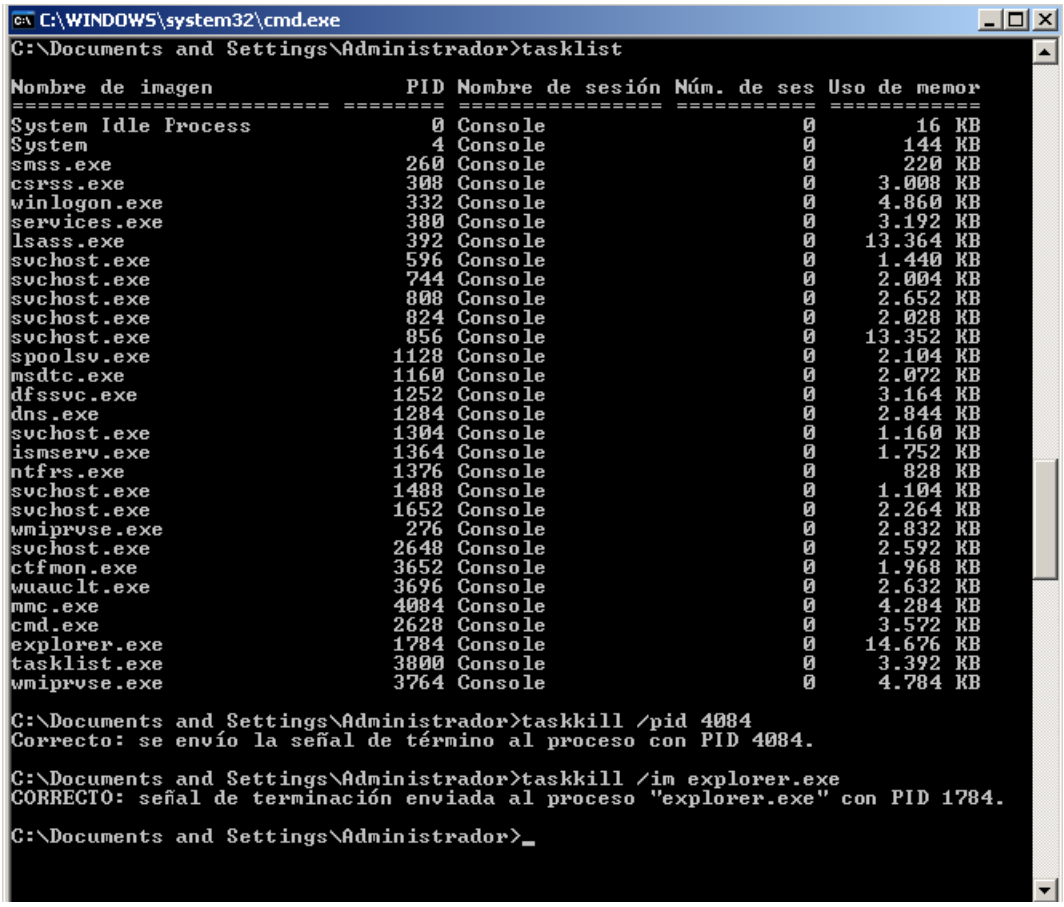
Vea otra imagen de cómo matar o terminar un proceso;



Y aquí vea otra forma de cómo terminar un proceso, escriba taskkill /im “nombre del proceso.exe”

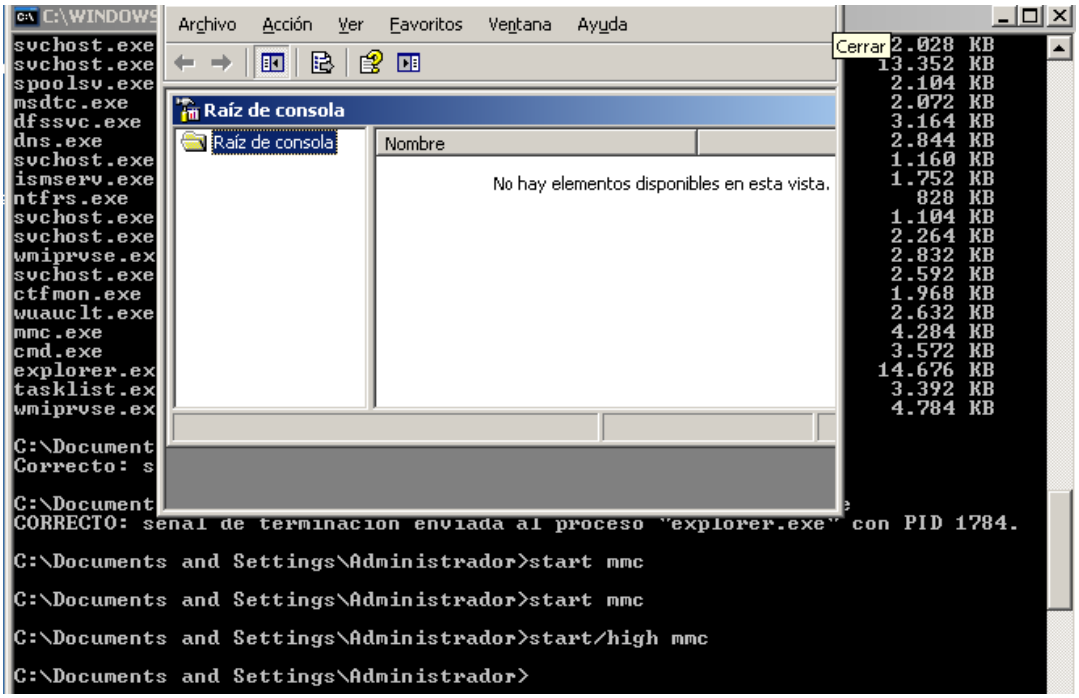


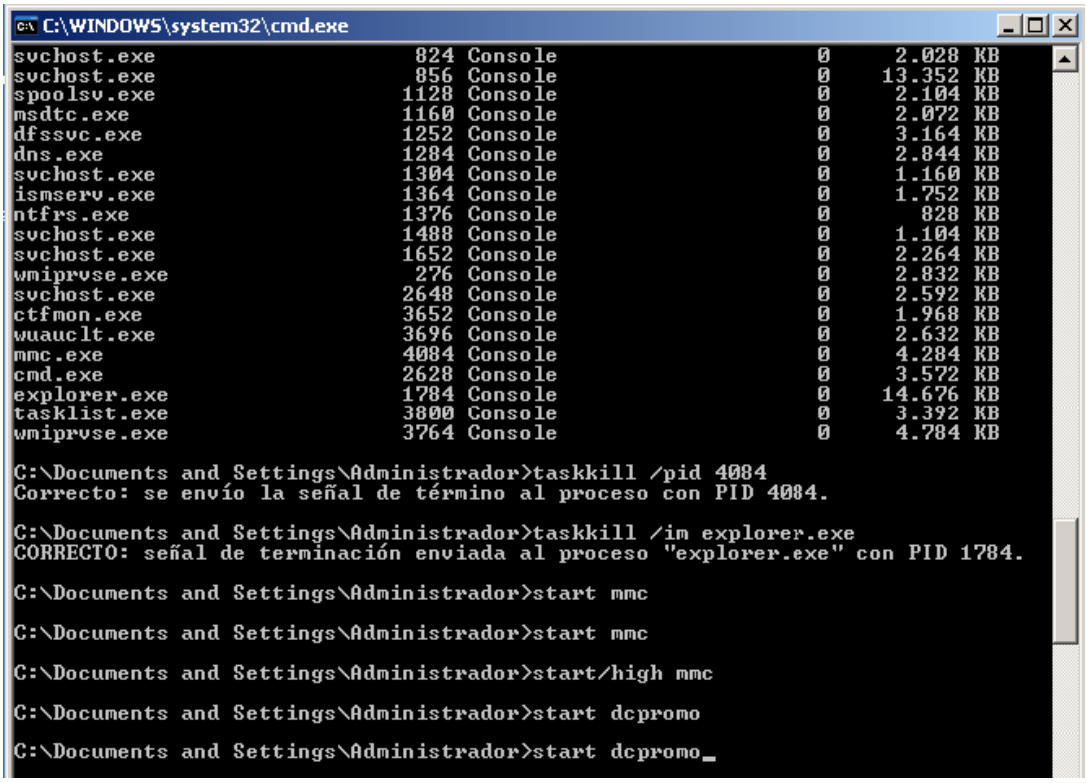
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process               0 Console                    0         16 KB
System                            4 Console                    0        144 KB
smss.exe                        260 Console                    0        220 KB
csrss.exe                       308 Console                    0      3.008 KB
winlogon.exe                    332 Console                    0      4.860 KB
services.exe                    380 Console                    0      3.192 KB
lsass.exe                       392 Console                    0     13.364 KB
svchost.exe                     596 Console                    0      1.440 KB
svchost.exe                     744 Console                    0      2.004 KB
svchost.exe                     808 Console                    0      2.652 KB
svchost.exe                     824 Console                    0      2.028 KB
svchost.exe                     856 Console                    0     13.352 KB
spoolsv.exe                    1128 Console                    0      2.104 KB
msdtc.exe                      1160 Console                    0      2.072 KB
dfssvc.exe                     1252 Console                    0      3.164 KB
dns.exe                        1284 Console                    0      2.844 KB
svchost.exe                    1304 Console                    0      1.160 KB
ismserv.exe                    1364 Console                    0      1.752 KB
ntfrs.exe                      1376 Console                    0        828 KB
svchost.exe                    1488 Console                    0      1.104 KB
svchost.exe                    1652 Console                    0      2.264 KB
wmiprvse.exe                    276 Console                    0      2.832 KB
svchost.exe                    2648 Console                    0      2.592 KB
ctfmon.exe                     3652 Console                    0      1.968 KB
wuauclt.exe                    3696 Console                    0      2.632 KB
mmc.exe                        4084 Console                    0      4.284 KB
cmd.exe                        2628 Console                    0      3.572 KB
explorer.exe                   1784 Console                    0     14.676 KB
tasklist.exe                   3800 Console                    0      3.392 KB
wmiprvse.exe                   3764 Console                    0      4.784 KB

C:\Documents and Settings\Administrador>taskkill /pid 4084
Correcto: se envío la señal de término al proceso con PID 4084.

C:\Documents and Settings\Administrador>taskkill /im explorer.exe
```



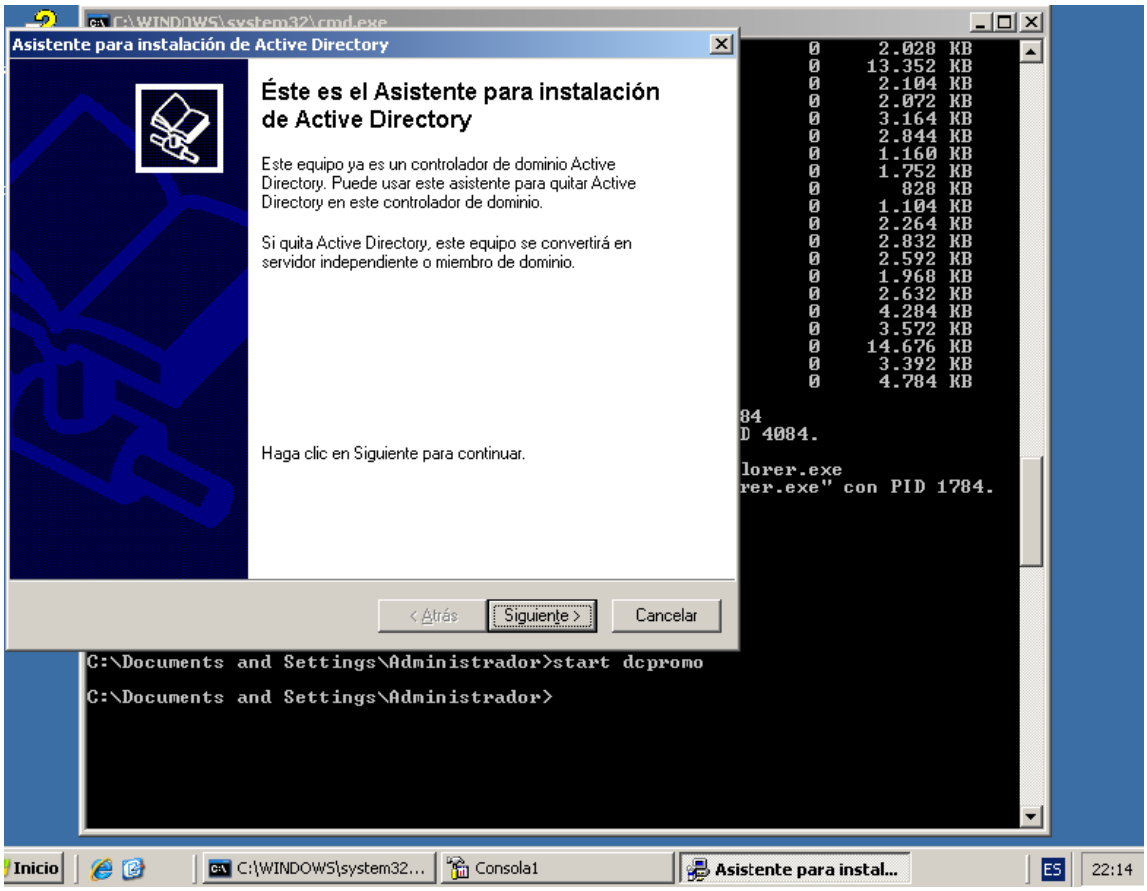
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process               0 Console                    0         16 KB
System                            4 Console                    0        144 KB
smss.exe                        260 Console                    0        220 KB
csrss.exe                       308 Console                    0      3.008 KB
winlogon.exe                    332 Console                    0      4.860 KB
services.exe                    380 Console                    0      3.192 KB
lsass.exe                       392 Console                    0     13.364 KB
svchost.exe                     596 Console                    0      1.440 KB
svchost.exe                     744 Console                    0      2.004 KB
svchost.exe                     808 Console                    0      2.652 KB
svchost.exe                     824 Console                    0      2.028 KB
svchost.exe                     856 Console                    0     13.352 KB
spoolsv.exe                    1128 Console                    0      2.104 KB
msdtc.exe                      1160 Console                    0      2.072 KB
dfssvc.exe                     1252 Console                    0      3.164 KB
dns.exe                        1284 Console                    0      2.844 KB
svchost.exe                    1304 Console                    0      1.160 KB
ismserv.exe                    1364 Console                    0      1.752 KB
ntfrs.exe                      1376 Console                    0        828 KB
svchost.exe                    1488 Console                    0      1.104 KB
svchost.exe                    1652 Console                    0      2.264 KB
wmiprvse.exe                    276 Console                    0      2.832 KB
svchost.exe                    2648 Console                    0      2.592 KB
ctfmon.exe                     3652 Console                    0      1.968 KB
wuauclt.exe                    3696 Console                    0      2.632 KB
mmc.exe                        4084 Console                    0      4.284 KB
cmd.exe                        2628 Console                    0      3.572 KB
explorer.exe                   1784 Console                    0     14.676 KB
tasklist.exe                   3800 Console                    0      3.392 KB
wmiprvse.exe                   3764 Console                    0      4.784 KB

C:\Documents and Settings\Administrador>taskkill /pid 4084
Correcto: se envío la señal de término al proceso con PID 4084.

C:\Documents and Settings\Administrador>taskkill /im explorer.exe
CORRECTO: señal de terminación enviada al proceso "explorer.exe" con PID 1784.

C:\Documents and Settings\Administrador>_
```

Y para iniciar un proceso escriba start y el nombre de el proceso que este ligado al sistema operativo





Y aquí otro ejemplo de cómo crear un proceso, vea como iniciar el asistente para active directory,



Principales procesos que arranca Windows

La gran mayoría de los programas crean procesos que permiten iniciar el sistema operativo con el que estamos trabajando. Los recursos disponibles en un sistema operativo son limitados y entre mas procesos se inicien con el mismo mas largo será el tiempo necesario para el arranque. Además muchos de estos procesos se mantienen residentes después del arranque, gastando memoria y recursos, haciendo que el sistema responda de manera mas lenta y disponga de una cantidad menor de recursos para los programas que realmente deseamos emplear.

Además la mayoría de los programas maliciosos (virus, gusanos de red, adwares, spywares, etc.) también crearán procesos de inicio para iniciarse o reinstalarse en cada arranque del sistema, algo que seria muy perjudicial tanto para el software como para el usuario.

Hay que tener en cuenta que no todos los procesos en Windows son procesos de inicio, es decir, no todos los procesos que se presentan en el administrador de tareas son procesos de Windows.

Para acceder a los principales procesos que inicia Windows se procede a abrir ejecutar (presionando la tecla de Windows+R), escribimos ‘’**msconfig**’’ y le damos a Enter.

Los archivos o procesos de inicio son los siguientes:

NTLDR --> C: (System Partition Root) --> Preinicio e Inicio (preboot y boot)
BOOT.INI --> C: --> Inicio
BOOTSECT.DOS --> C: --> Inicio (opcional)
NTDETECT.COM --> C: --> Inicio
NTBOOTDD.SYS --> C: --> Inicio (opcional)
NTOSKRNL.EXE --> systemrootsystem32 --> Carga del Kernel (núcleo)
HAL.DLL --> systemrootsystem32 --> Carga del Kernel (núcleo)
SYSTEM --> systemrootsystem32 --> Inicialización del Kernel
dispositivos.sys --> systemroorsystem32drivers --> Inicialización del Kernel

Al instalar un sistema operativo (Windows 2000 XP) se modifica o se crea un archivo boot.ini en la partición activa (arrancable) del sistema. El programa NTLDR usará dicha información para mostrarnos la pantalla de inicio desde la cual podremos seleccionar el sistema operativo a cargar.

El archivo boot.ini es un archivo de texto que contiene dos secciones [boot loader] y [operating systems]. NTLDR usará dicha información para construir la pantalla de inicio del sistema.