



CFGS ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

IMPLANTACIÓN DE SISTEMAS OPERATIVOS



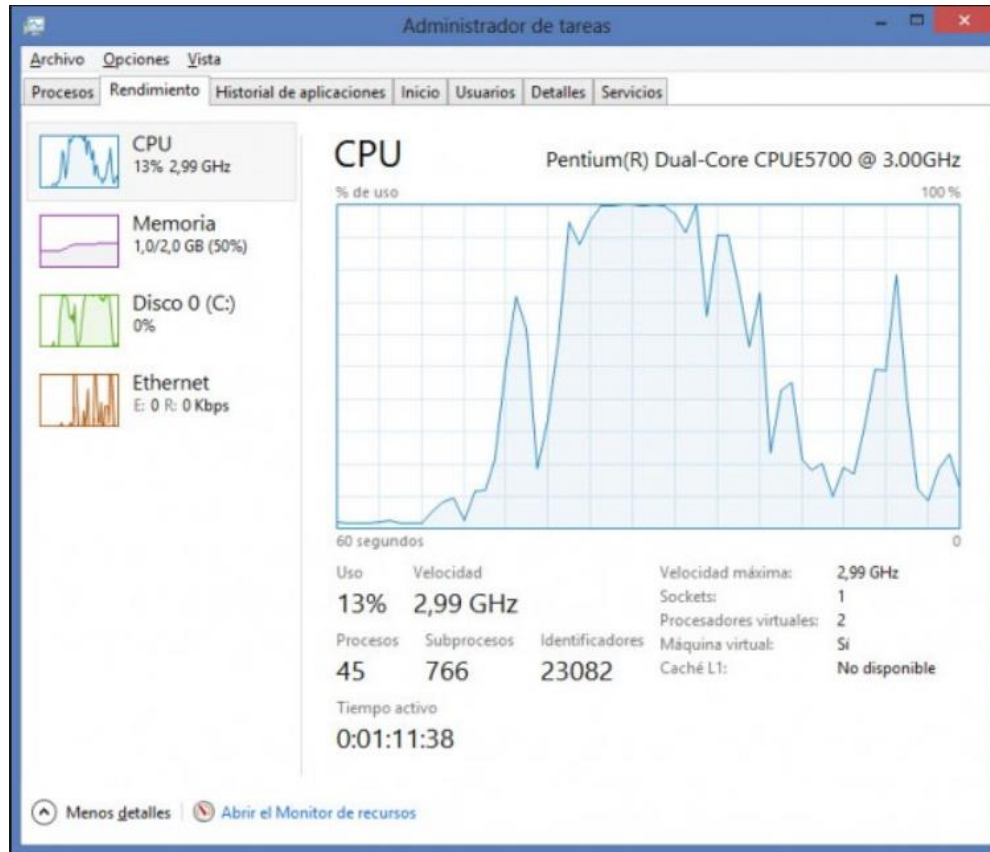
Ud9.- Administración de procesos y servicios.

Índice

- 1.- Introducción a los procesos
- 2.- Administrador de tareas.
- 3.- Introducción a los servicios.
- 4.- Administrador de servicios.



1.- Introducción





1.- Introducción

Podemos definir **un proceso** como una unidad elemental de ejecución de un programa.

Un Proceso en primer plano tiene el control del teclado y el ratón.

Un proceso en segundo plano es un proceso que no recibe ninguna señal por lo general, se ejecuta en silencio sin necesidad de interacción.



2.- Administrador de tareas

Herramienta que permite controlar la actividad del sistema y su rendimiento en tiempo real.

Nos da información de:

Procesos /Aplicaciones

Rendimiento

Historial de aplicaciones

Inicio

Usuarios

Detalles

Servicios

Algunas formas de abrirlo:

1. Pulse Ctrl+Shift+Esc

2. Pulse Ctrl+Alt+Del y seleccione Administrador de tareas

3. Haga clic con el botón derecho en la barra de tareas y seleccione Administrador de tareas

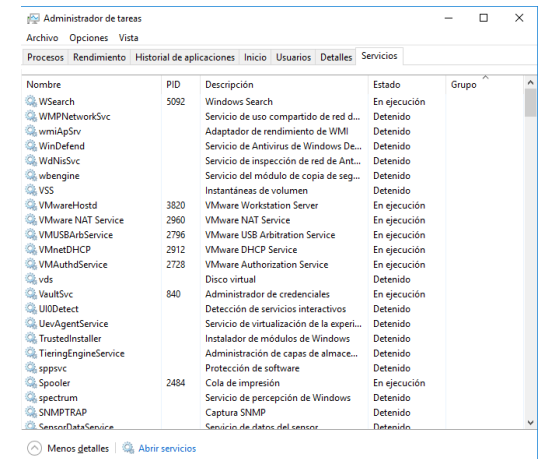
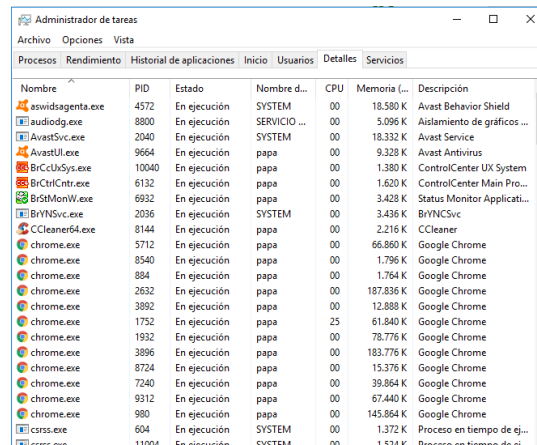
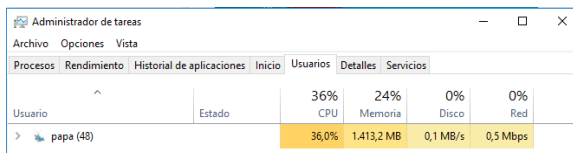
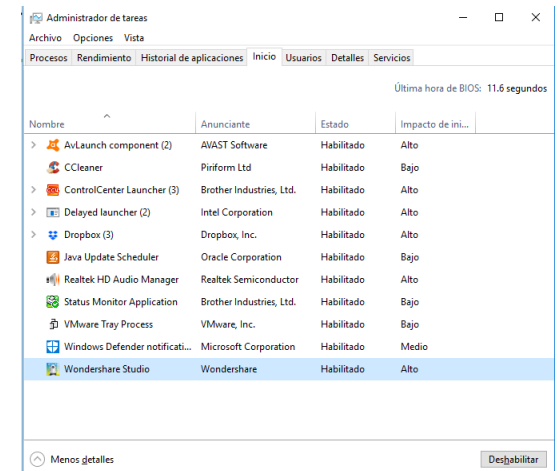
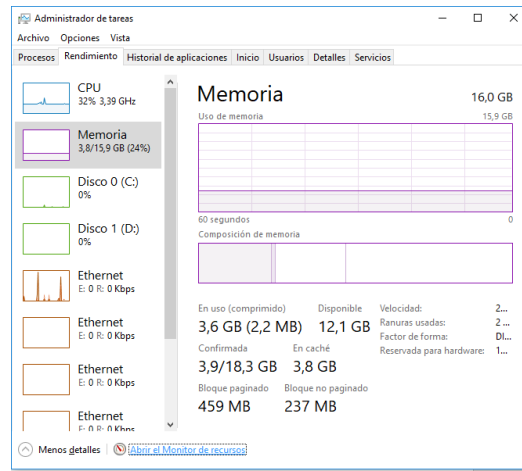
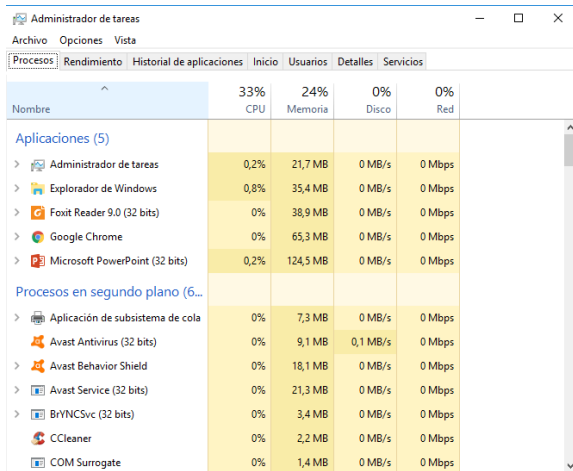


2.- Administrador de tareas

Administrador de tareas				
Archivo Opciones Vista				
Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios				
Nombre	32% CPU	24% Memoria	0% Disco	0% Red
Aplicaciones (6)				
> Administrador de tareas	0%	12,8 MB	0 MB/s	0 Mbps
> Explorador de Windows	0,9%	36,1 MB	0 MB/s	0 Mbps
> Foxit Reader 9.0 (32 bits)	0%	38,9 MB	0 MB/s	0 Mbps
> Google Chrome	0%	64,1 MB	0 MB/s	0,1 Mbps
> Microsoft PowerPoint (32 bits)	0%	120,4 MB	0 MB/s	0 Mbps
> Recortes	0,2%	2,9 MB	0,1 MB/s	0 Mbps
Procesos en segundo plano (6...)				
Aislamiento de gráficos de disp...	0%	5,3 MB	0 MB/s	0 Mbps
> Aplicación de subsistema de cola	0%	7,3 MB	0 MB/s	0 Mbps
> Avast Antivirus (32 bits)	0%	9,1 MB	0 MB/s	0 Mbps
> Avast Behavior Shield	0%	18,1 MB	0 MB/s	0 Mbps
> Avast Service (32 bits)	0%	18,7 MB	0 MB/s	0 Mbps
> BrYNCSvc (32 bits)	0%	3,4 MB	0 MB/s	0 Mbps



2.- Administrador de tareas





2.- Administrador de tareas

Ejercicio: Aplicaciones en segundo plano

1.- Visualizar los procesos/aplicaciones en segundo plano.



Privacidad
Ubicación, cámara

Al final de las opciones podemos encontrarnos con:



Aplicaciones en segundo plano

Aplicaciones en segundo plano

Aplicaciones en segundo plano

Permitir que las aplicaciones se ejecuten en segundo plano

☒ Activado

[Declaración de privacidad](#)

Elige qué aplicaciones se pueden ejecutar en segundo plano

Elige las aplicaciones que pueden recibir información, enviar notificaciones y mantenerse actualizadas, incluso cuando no las estés usando. Desactivar las aplicaciones en segundo plano puede ayudar a ahorrar energía.



3D Builder

☒ Activado



Adobe Photoshop Express

☒ Activado



Alarms y reloj

☒ Activado



Calculadora

☒ Activado



Calendario

☒ Activado

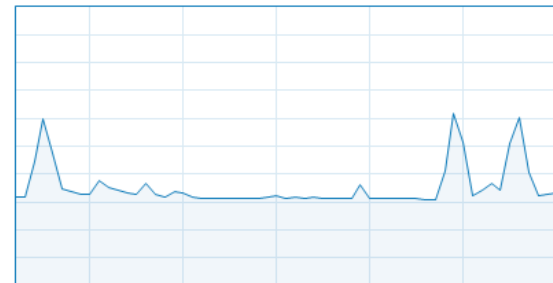
2.- Elimina las que considere innecesarias y visualiza el uso de la CPU.

CPU

Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz

% de uso

100 %



60 segundos

0



2.- Administrador de tareas

Ejercicio: Procesos peligrosos

¿Cómo sabemos si un proceso es peligroso?.

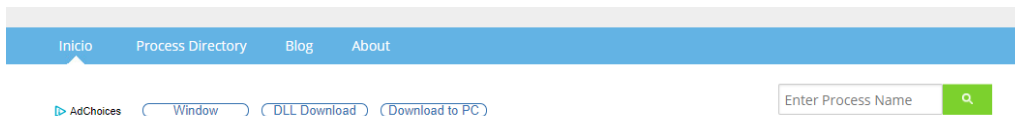
1.- Accedemos al Adm de tareas y a la solapa Detalles.

2.- Nos encontramos dos procesos sospechosos:

explorer.exe, csrss.exe

3.- Accedemos a la página: <http://www.processlibrary.com/es/>

4.- Escribimos el nombre del proceso.

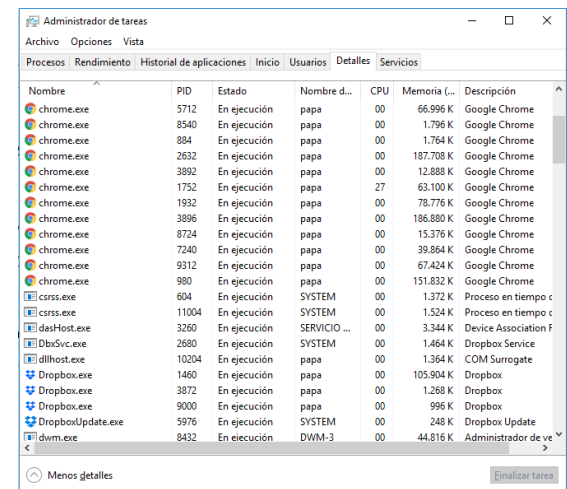


www.processlibrary.com

www.neuber.com/taskmanager/process/

<http://www.file.net/process/>

¿Necesitas spyware Terminator?





2.- Administrador de tareas

Ejercicio: Procesos peligrosos

csrss.exe

■ Nivel de seguridad inseguro

el csrss.exe es un process que se coloca como Trojan. el Este Trojan permite que los atacantes tengan acceso a su ordenador de las posiciones ...

<http://www.processlibrary.com/es/directory/files/csrss/26095>

csrss.exe

■ Nivel de seguridad seguro

csrss.exe es la cañería ejecutable para el Microsoft Client/Server Runtime Server Subsystem. que este proceso maneja la mayoría de los comandos gráficos en Windows ...

<http://www.processlibrary.com/es/directory/files/csrss/26031>

Cualquiera que te diga que el proceso alojado en system32 puede ser un virus, te está tomando el pelo o tiene alguna intención oculta.

El servicio en esta carpeta es un archivo funcional del sistema, y en caso de ser eliminado, modificado o alterado generaría problemas en el sistema y cierta inestabilidad. Además, ya de por sí los permisos que tiene no permiten cambiarlo.

¿Es un virus csrss.exe?

Puedes encontrarte con una o varias instancias de este proceso siempre funcionando en segundo plano en el sistema. Siempre la única legítima del sistema se va a encontrar en C:\Windows\System32, y puedes hacer click derecho sobre el proceso y darle a abrir ubicación del archivo para comprobar su origen.



2.- Administrador de tareas

Ejercicio: Procesos y aplicaciones asociadas.

1.- Abre las siguientes aplicaciones y minimízalas.

Bloc de notas, calculadora, Paint y IE.

2.- Abre el administrador de tareas. Localiza las aplicaciones y los procesos asociados.

Por ejemplo:

a) Buscamos la calculadora en la solapa procesos.

b) Una vez localizada. Botón dcho: ir a Detalle.

3.- Procede, desde la solapa Detalles a eliminar o Finalizar la tarea.

4.- Finaliza el proceso explorer.exe ¿Qué ha pasado?

5.- ¿Puedes recuperar el sistema sin reiniciar? → Accede Adm Tarea: Archivo_Ejecutar



3.- Introducción a los servicios.

¿Cómo sabe nuestro ordenador portátil qué redes inalámbricas hay disponibles en cada momento y cómo detecta el sistema que hemos conectado una unidad de memoria USB?

La respuesta es que hay servicios ejecutándose en segundo plano que se encargan de estas tareas, explorando las señales de radio y el estado del bus USB, respectivamente.



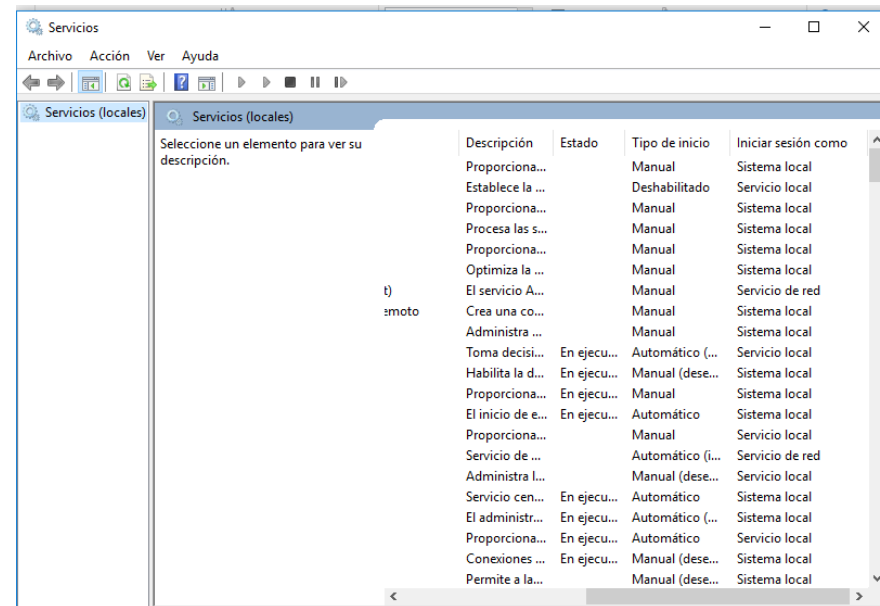


4.- Administración de servicios.

Un **servicio** no es más que un programa que se ejecuta en el ordenador.

Se suele ejecutar de forma automática al inicio del sistema operativo.

Los servicios normalmente no cuentan con interfaz de usuario, ni siquiera un icono de notificación en la barra de tareas.





4.- Administración de servicios.

Descripción	Estado	Tipo de inicio	Iniciar sesión como
-------------	--------	----------------	---------------------

Nombre

Descripción

Estado

(detenido, iniciado, deteniéndose, iniciándose y blanco: el servicio no está funcionando)

Tipo de inicio

Iniciar sesión (recoge la cuenta que usa el servicio para iniciar sesión en el sistema).

Tipo de inicio:

Automático (inicio retrasado): el servicio se ejecutará de forma automática una vez que Windows haya terminado de iniciarse.

Automático: el servicio se inicia al mismo tiempo que Windows, durante el proceso de arranque.

Manual: El servicio se iniciará solo cuando Windows lo considere necesario o bien a demanda del usuario del sistema.

Deshabilitado: El servicio no se iniciará en ningún caso, ni siquiera cuando Windows considere que sería necesario.



4.- Administración de servicios.

Descripción	Estado	Tipo de inicio	Iniciar sesión como
-------------	--------	----------------	---------------------

Iniciar sesión:

La mayoría de los servicios se ponen en marcha antes de que el usuario haya iniciado la sesión en el sistema. Precisan saber **qué cuenta** es la que se deben utilizar para ejecutarse, información que se establece en la página Iniciar sesión:

Sistema local: Permite el acceso completo al sistema sin ninguna restricción.

Servicio local: es una cuenta que otorga al servicio el mismo nivel de acceso a recursos que los miembros del grupo usuarios, es decir, que cualquier usuario corriente. Está limitado a recursos de red.

Servicio de red: Prácticamente es idéntica a la anterior, salvo por el hecho de que para acceder a comunicaciones por red el servicio se identifica utilizando como credenciales la cuenta del propio ordenador.



4.- Administración de servicios.

Ejercicio: Servicios

1.- ¿Qué servicios se inician automáticamente?

Servicios (locales)					
Administrador de conexiones de Windows Detener el servicio Reiniciar el servicio Descripción: Toma decisiones de conexión/desconexión automáticas en función de las opciones de conectividad de red disponibles actualmente para el equipo y permite administrar la conectividad de red	Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
	Administrador de cuentas de seguridad	El inicio de e...	En ejecu...	Automático	Sistema local
	Administrador de sesión local	Servicio cen...	En ejecu...	Automático	Sistema local
	Adquisición de imágenes de Windows (WIA)	Proporciona...	En ejecu...	Automático	Servicio local
	Aplicación auxiliar IP	Proporciona...	En ejecu...	Automático	Sistema local
	Asignador de extremos de RPC	Resuelve ide...	En ejecu...	Automático	Servicio de red
	Audio de Windows	Administra ...	En ejecu...	Automático	Servicio local
	Avast Antivirus	Gestiona e i...	En ejecu...	Automático	Sistema local
	Cliente de seguimiento de vínculos distribuidos	Mantiene lo...	En ejecu...	Automático	Sistema local
	Cliente DHCP	Registra y ac...	En ejecu...	Automático	Servicio local
	Cola de impresión	Este servicio...	En ejecu...	Automático	Sistema local

2.- ¿En estado se encuentra el servicio Windows Update?

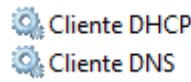


4.- Administración de servicios.

Ejercicio: Servicios: Cliente DHCP

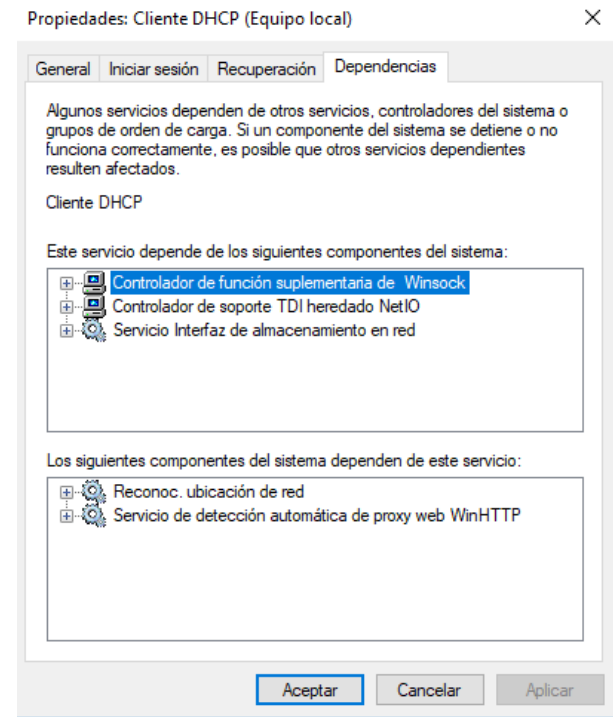
Este servicio busca un servidor DHCP válido que se encuentre presente en nuestra red y obtiene la IP y los parámetros de configuración de red necesarios para una correcta conexión.

1.- Localízalo.



2.- ¿De qué servicios depende y a quién da servicio?

3.- Intenta detenerlo. ¿Te deja detenerlo?

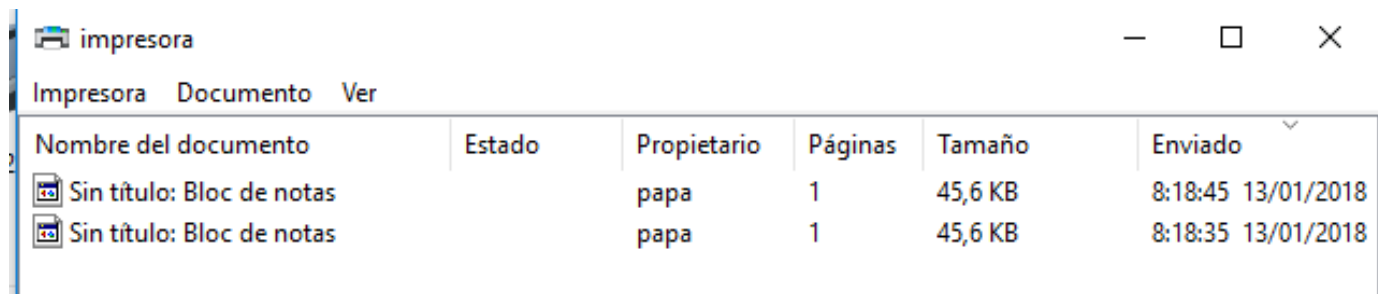






4.- Administración de servicios.

Ejercicio: Servicios: Cola de impresión

- 1.- Localiza el servicio y su estado. Si no se está ejecutándose. Actívalo.
- 2.- Instala una impresora local (ficticia) en Windows.
- 3.- Manda un par de archivos a la impresora.
- 4.- Observa la cola de impresión.



impresora						
Impresora Documento Ver						
Nombre del documento	Estado	Propietario	Páginas	Tamaño	Enviado	
 Sin título: Bloc de notas		papa	1	45,6 KB	8:18:45	13/01/2018
 Sin título: Bloc de notas		papa	1	45,6 KB	8:18:35	13/01/2018



4.- Administración de servicios.











Ejercicio: Servicios: Cola de impresión

5.- Imagínate que la impresora se ha quedado bloqueada y no responde.

6.- Vamos a liberar los archivos de la cola:

- Detenemos el servicio de cola de impresión. Ahora no tendrás acceso temporal a las impresoras. No te preocupes.
- Borramos los archivos de la cola:
- Reanudamos el servicio.
- Observa la cola de impresión.

Disco local (C:) > Windows > System32 > spool > PRINTERS

Nombre	Fecha de modifica...	Tipo	Tamaño
 00005.SHD	13/01/2018 8:18	Archivo SHD	3 KB
 00005.SPL	13/01/2018 8:18	Shockwave Flash ...	46 KB
 00006.SHD	13/01/2018 8:18	Archivo SHD	3 KB
 00006.SPL	13/01/2018 8:18	Shockwave Flash ...	46 KB
 FP00002.SHD	13/01/2018 8:22	Archivo SHD	3 KB
 FP00002.SPL	09/12/2017 18:23	Shockwave Flash ...	13 KB
 FP00007.SHD	08/01/2018 9:24	Archivo SHD	3 KB
 FP00007.SPL	08/01/2018 9:24	Shockwave Flash ...	13 KB
 FP00008.SHD	08/01/2018 9:24	Archivo SHD	3 KB
 FP00008.SPL	08/01/2018 9:24	Shockwave Flash ...	13 KB



5.- Administración desde la línea de comandos

5.1.- Comandos CMD

Procesos:

tasklist → Muestra información de los procesos.

tasklist /v → Información detallada.

tasklist /svc → servicios asociados a los procesos.

Taskkill → Matar procesos

Ejemplos:

```
TASKKILL /IM notepad.exe  
TASKKILL /PID 1230 /PID 1241 /PID 1253
```

Servicios:

Sc query |more → Listamos los servicios.

net start → Listamos los servicios.

Net stat servicio → Iniciar un servicio.

Net stop servicio → Parar un servicio.



5.- Administración desde la línea de comandos

5.2.- Comandos cmdlet

Procesos:

Get-Process → Muestra información de los procesos.

Stop-Process → Detener un proceso.

Start-Process → Iniciar un proceso.

Ejercicio: ¿Sabes qué hace este comando?

```
Get-Process | Out-GridView
```

Servicios:

Get-service → Listamos los servicios.

Stop-Service → Para un servicio.

Start-Service → Inicia el servicio.



Sugerencias/mejoras del tema



Sugerencias /mejoras del tema