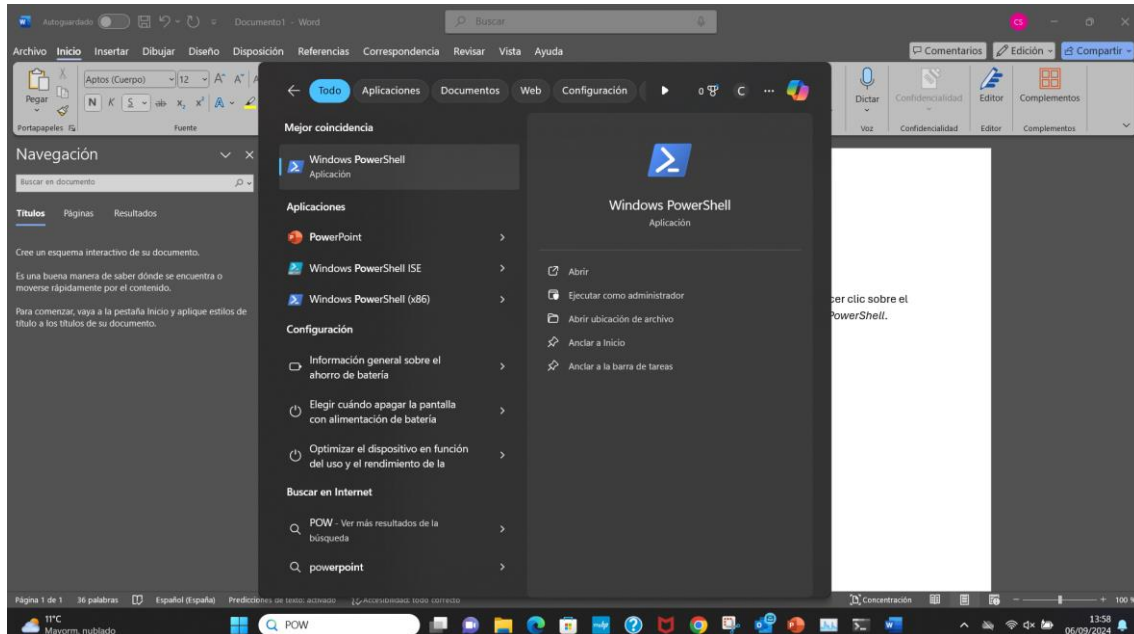


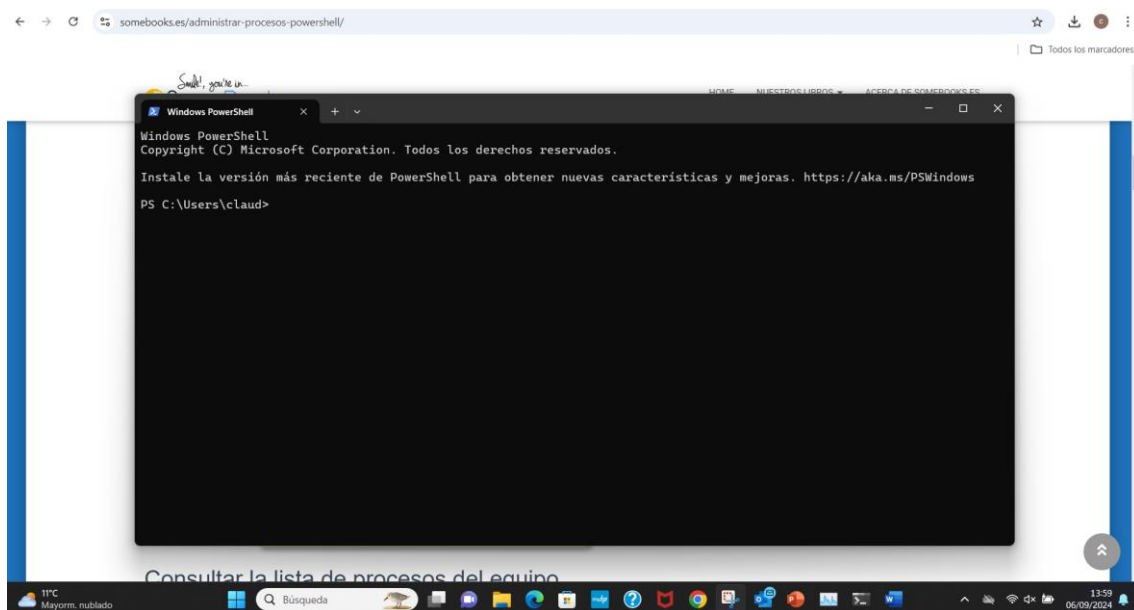
GESTIÓN DE PROCESOS CON POWERSHELL

1. Iniciar la ejecución de PowerShell

Para abrir una nueva ventana de *PowerShell*, comenzaremos por hacer clic sobre el botón *Inicio* y desplazarnos por el menú hasta la carpeta *Windows PowerShell*.



Al poco aparecerá una ventana, lista para comenzar a escribir nuestras órdenes:



2. Consultar la lista de procesos del equipo

Para obtener la lista con todos los procesos que se están ejecutando en ese momento en el equipo, basta con utilizar el comando **Get-Process** sin argumentos:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\c\aud> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
498	26	49568	44292	0,02	14484	2	AccountsControlHost
176	11	4340	9736		6492	0	AggregatorHost
221	18	26152	21256	0,33	8124	2	ai
310	18	22800	37408	0,02	9744	2	ai
221	18	22516	18428	0,16	15944	2	ai
423	18	6724	18968		10896	0	AppHelperCap
627	32	22332	38524	2,06	10556	2	ApplicationFrameHost
182	10	2056	9064	0,02	15108	2	AppVShNotify
323	19	4692	1624	0,09	4404	2	backgroundTaskHost
577	26	6324	1556	0,11	7756	2	backgroundTaskHost
184	11	2660	12208	0,02	20496	2	backgroundTaskHost
348	24	40044	80572	0,91	360	2	chrome
405	26	56456	108632	1,86	1888	2	chrome
490	11	2172	7264	0,08	2104	2	chrome
435	26	63588	105804	1,95	2396	2	chrome
411	26	62604	117616	1,31	4072	2	chrome
415	26	52312	105292	0,45	5348	2	chrome
346	24	46144	67636	20,94	5716	2	chrome
351	24	33708	67272	0,61	6256	2	chrome
393	25	53476	93324	1,53	7936	2	chrome
494	29	41144	81132	3,34	8860	2	chrome

Aunque, si la salida es demasiado larga y no cabe en la ventana, siempre puedes hacer una pausa procesándola con el comando **more**:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\c\aud> Get-Process | more
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
498	26	49568	44292	0,02	14484	2	AccountsControlHost
176	11	4340	9736		6492	0	AggregatorHost
221	18	26152	21256	0,33	8124	2	ai
310	18	22800	37408	0,02	9744	2	ai
221	18	22516	18428	0,16	15944	2	ai
427	19	6804	19008		10896	0	AppHelperCap
634	32	21568	38444	2,08	10556	2	ApplicationFrameHost
182	10	2056	9064	0,02	15108	2	AppVShNotify
323	19	4692	1624	0,09	4404	2	backgroundTaskHost
577	26	6324	1556	0,11	7756	2	backgroundTaskHost
348	24	40044	80572	0,91	360	2	chrome
405	26	56456	108628	1,86	1888	2	chrome
476	11	2172	7264	0,08	2104	2	chrome
435	26	64616	105828	1,95	2396	2	chrome
411	26	59196	114528	1,31	4072	2	chrome
415	26	52312	105284	0,45	5348	2	chrome
346	24	46144	67636	20,94	5716	2	chrome
351	24	33708	67272	0,61	6256	2	chrome
393	25	53476	93324	1,53	7936	2	chrome
494	29	41144	81132	3,34	8860	2	chrome
306	22	20936	46708	0,31	9252	2	chrome
365	26	46976	88732	1,73	9356	2	chrome
312	23	24864	58676	0,25	9764	2	chrome
641	28	77724	126736	3,78	10020	2	chrome
366	25	64072	72492	3,98	10396	2	chrome
480	27	81024	121580	21,95	10520	2	chrome

-- Más --

Y cuando necesitamos sólo algunos de los procesos, siempre podemos establecer un filtro. Por ejemplo, por su nombre:

```
PS C:\Users\claud> Get-Process -Name a*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
498	26	49568	44292	0,02	14484	2	AccountsControlHost
176	11	4340	9536		6492	0	AggregatorHost
221	18	26152	20972	0,33	8124	2	ai
310	18	22872	37496	0,02	9744	2	ai
221	18	22516	18176	0,16	15944	2	ai
423	18	6760	18904		10896	0	AppHelperCap
640	33	20756	38792	2,11	10556	2	ApplicationFrameHost
182	10	2056	8716	0,02	15108	2	AppVShNotify

Por ejemplo, por ID:

```
PS C:\Users\claud> Get-Process -id 18856
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
722	34	57256	68200	0,31	18856	1	Notepad

Por otro lado, si lo que necesitamos es una información detallada sobre un proceso, o un grupo de procesos, podemos enviar la salida de **Get-Process** a **Format-List**, que se encarga de formatear la salida de las propiedades de un objeto de modo que cada una aparezca en una nueva línea.

```
PS C:\Users\claud> Get-Process -Name explorer | Format-List *
```

```
Name                : explorer
Id                  : 9780
PriorityClass       : Normal
FileVersion        : 10.0.22621.4168 (WinBuild.160101.0800)
HandleCount        : 7100
WorkingSet         : 312496128
PagedMemorySize    : 377860096
PrivateMemorySize  : 377860096
VirtualMemorySize  : 1450520576
TotalProcessorTime : 00:02:20.8750000
SI                 : 2
Handles            : 7100
VM                 : 2204768743424
WS                 : 312496128
PM                 : 377860096
NPM                : 192648
Path               : C:\WINDOWS\Explorer.EXE
Company            : Microsoft Corporation
CPU                : 140,875
ProductVersion     : 10.0.22621.4168
Description        : Explorador de Windows
Product            : Sistema operativo Microsoft® Windows®
_ NounName         : Process
BasePriority        : 8
ExitCode           :
HasExited          : False
ExitTime           :
Handle             : 3296
SafeHandle          : Microsoft.Win32.SafeHandles.SafeProcessHandle
MachineName        : .
```

3. Detener un proceso por nombre

Cuando necesitamos forzar la detención de un proceso que está ejecutándose, podemos recurrir al *cmdlet* **Stop-Process**. Por ejemplo, podríamos escribir la siguiente orden para detener el navegador (necesario abrir primero el navegador para que cargue el proceso):

Stop-Process -name chrome*

Si lo prefieres, podrías utilizar el argumento *-id* y utilizar el número de proceso. Por ejemplo, si abrimos el Bloc de notas, vemos que el ID asociado es 22032

```
PS C:\Users\claud> Get-Process -Name n*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
234	15	3508	12048		18168	0	NetworkCap
627	33	67240	106868	0,03	22032	2	Notepad

Si ejecutamos el comando vemos que se ha borrado el proceso:

```
PS C:\Users\claud> Stop-Process -id 22032
PS C:\Users\claud> Get-Process -Name n*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
234	15	3508	12048		18168	0	NetworkCap

Incluso podemos hacer que el *cmdlet* nos pida confirmación antes de parar el proceso. Para ello, basta con utilizar el argumento *-Confirm*. Por ejemplo, abrir la calculadora y ver que está activo el proceso asociado:

```
PS C:\Users\claud> Get-Process -Name c*
```

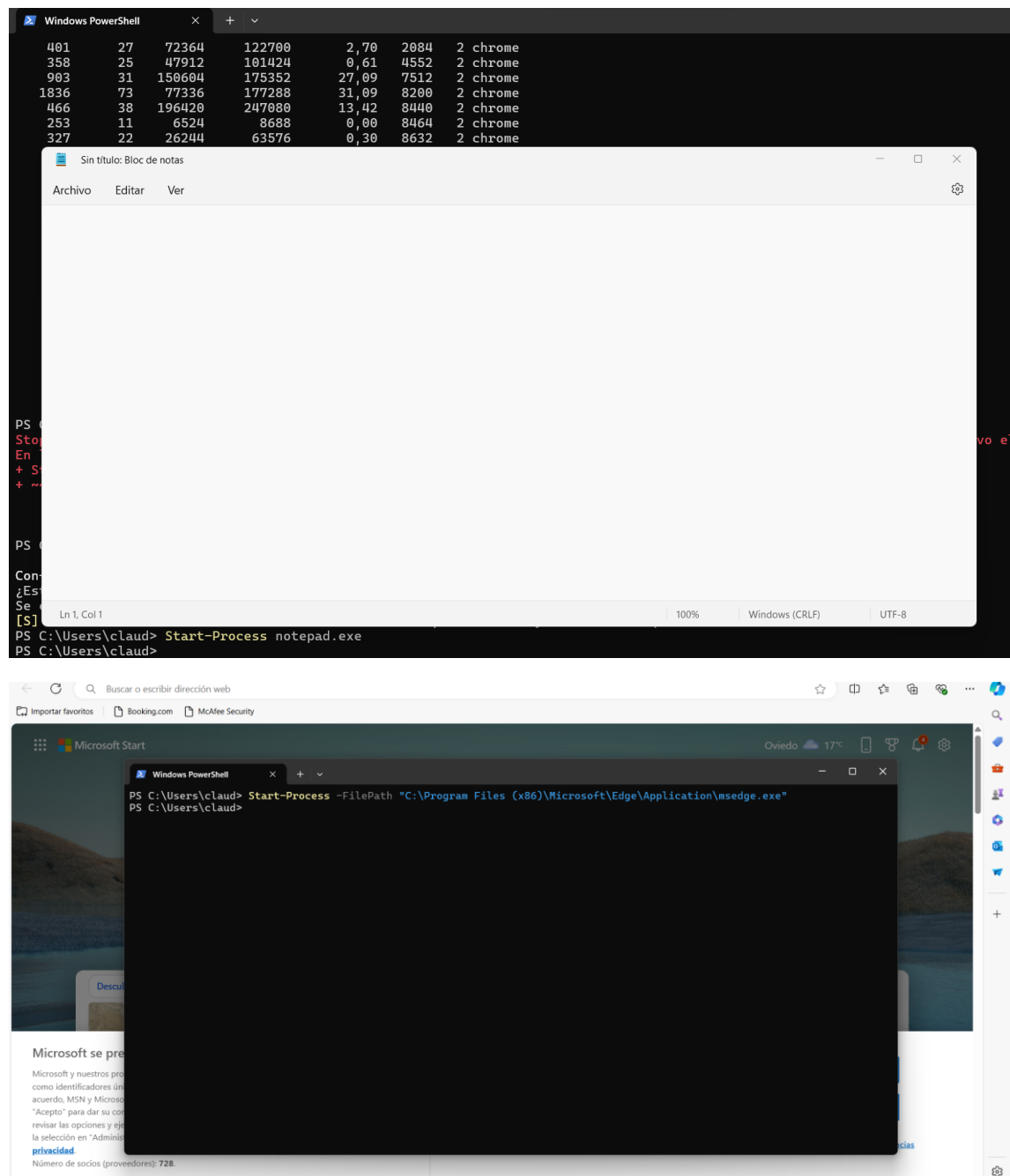
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
646	47	66648	110112	0,11	7004	2	CalculatorApp
401	27	72364	122700	2,70	2084	2	chrome
358	25	47912	101424	0,61	4552	2	chrome
903	31	150604	175352	27,09	7512	2	chrome
1836	73	77336	177288	31,09	8200	2	chrome
466	38	196420	247080	13,42	8440	2	chrome
253	11	6524	8688	0,00	8464	2	chrome

```
PS C:\Users\claud> Stop-Process -name CalculatorApp -Confirm

Confirm
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "Stop-Process" en el destino "CalculatorApp (7004)".
[S] Sí [0] Sí a todo [N] No [T] No a todo [U] Suspendir [?] Ayuda (el valor predeterminado es "S"):
```

4. Iniciar un nuevo proceso

Podemos utilizar el comando `Start-Process` incluyendo a continuación el nombre de un programa o de un script.



5. Detener un proceso por ID

Cuando necesitamos forzar la detención de un proceso que está ejecutándose, podemos recurrir al *cmdlet* **Stop-Process**. Por ejemplo, podríamos escribir la siguiente orden para detener Notepad (necesario abrir primero el navegador para que cargue el proceso):

Stop-Process -id numero

Primero buscamos el ID del proceso que queremos detener. En este caso tenemos dos procesos abiertos de Notepad.

```
PS C:\Users\claud> Get-Process -Name notepad*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
216	13	2924	13700	0,38	1904	1	Notepad
722	34	57252	104980	0,31	18856	1	Notepad

A continuación, ejecutamos el comando con el ID correspondiente para detener uno de los procesos:

```
PS C:\Users\claud> Stop-Process -id 1904
PS C:\Users\claud> Get-Process -Name notepad*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
722	34	57252	104980	0,31	18856	1	Notepad

6. Obtener Información de Uso de Recursos

Para mostrar el uso de CPU por los diferentes procesos en orden descendente se usa el siguiente comando `Get-Process | Sort-Object -Property CPU -Descending`

```
Windows PowerShell
PS C:\Users\claud> Get-Process | Sort-Object -Property CPU -Descending
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
2380	66	634944	316696	2.558,00	16944	1	chrome
1992	140	260668	177760	1.056,48	19040	1	OmenCommandCenterBackground
2173	51	288128	161388	991,92	968	1	msedge
3515	96	189044	265048	884,50	4796	1	chrome
51440	257	513292	378240	765,94	10440	1	explorer
898	30	684940	287172	424,78	24404	1	msedge
425	28	112920	16484	411,08	13524	1	msedge
503	29	134260	101536	383,69	14752	1	chrome
2494	531	123908	206512	311,67	16148	1	msedge
4189	68	101336	130916	307,28	15216	1	OneDrive
461	31	363192	103092	164,88	25048	1	chrome
805	35	34960	45968	142,92	5200	1	HPSYSTEMEVENTUTILITYBACKGROUND
494	35	78168	63456	141,03	8592	1	chrome
2598	82	283216	354984	109,31	5076	1	POWERPNT
644	21	11732	29736	99,00	13740	1	ctfmon
519	29	169804	16	71,88	10484	1	msedgeview2
417	29	204364	257080	66,47	18476	1	chrome
2833	82	286272	422912	58,33	9720	1	WINWORD
764	23	7884	35064	47,78	9360	1	sihost
176	11	2028	7880	45,80	8816	1	ipf_helper
430	28	21792	42148	45,44	8712	1	msedge
1223	127	1431852	1047152	43,38	22840	1	eclipse
400	27	63912	71752	42,06	19880	1	chrome
487	26	17424	24152	37,11	8832	1	uihost
494	49	412272	85096	31,45	17176	1	msedgeview2
3656	88	216792	224744	29,91	2120	1	OUTLOOK

7. Consultar la lista de servicios del equipo

Para obtener la lista con todos los procesos que se están ejecutando en ese momento en el equipo, basta con utilizar el comando **Get-Service** sin argumentos:

```
Windows PowerShell
PS C:\Users\cloud> Get-Service

Status  Name                DisplayName
-----
Stopped AarSvc_d7dbf        Agent Activation Runtime_d7dbf
Stopped AJRouter        Servicio de enrutador de AllJoyn
Stopped ALG            Servicio de puerta de enlace de niv...
Running AppIDSvc        Identidad de aplicación
Running AppInfo        Información de la aplicación
Stopped AppReadiness    Preparación de aplicaciones
Stopped AppXSvc        Servicio de implementación de AppX ...
Running AudioEndpointBu...  Compilador de extremo de audio de W...
Running Audiosrv        Audio de Windows
Stopped autotimesvc      Hora de la red de telefonía móvil
Stopped AxInstSV        Instalador de ActiveX (AxInstSV)
Running BcastDVRUserSer...  Servicio de usuario de difusión y G...
Running BDESVC          Servicio Cifrado de unidad BitLocker
Running BFE            Motor de filtrado de base
Running BITS            Servicio de transferencia inteligen...
Running BluetoothUserSe...  Servicio de soporte técnico de usua...
Running BrokerInfrastru...  Servicio de infraestructura de tare...
Stopped BTAGService      Servicio de puerta de enlace de aud...
Stopped BthAvctpSvc      Servicio AVCTP
Running bthserv         Servicio de compatibilidad con Blue...
Running camsvc          Servicio Administrador de funcional...
Stopped CaptureService_...  CaptureService_d7dbf
Running cbdhsvc_d7dbf     Servicio de usuario del portapapele...
Running CDPSvc          Servicio de plataforma de dispositi...
Running CDPUserSvc_d7dbf  Servicio de usuario de plataforma d...
Stopped CertPropSvc      Propagación de certificados
```

Aunque, si la salida es demasiado larga y no cabe en la ventana, siempre puedes hacer una pausa procesándola con el comando **more**:

```

PS C:\Users\claud> Get-Service | more

Status      Name                DisplayName
-----
Stopped     AarSvc_d7dbf        Agent Activation Runtime_d7dbf
Stopped     AJRouter            Servicio de enrutador de AllJoyn
Stopped     ALG                 Servicio de puerta de enlace de niv...
Running     AppIDSvc            Identidad de aplicación
Running     AppInfo             Información de la aplicación
Stopped     AppReadiness        Preparación de aplicaciones
Running     AppXSvc             Servicio de implementación de AppX ...
Running     AudioEndpointBu...  Compilador de extremo de audio de W...
Running     Audiosrv            Audio de Windows
Stopped     autotimesvc         Hora de la red de telefonía móvil
Stopped     AxInstSV            Instalador de ActiveX (AxInstSV)
Running     BcastDVRUserSer... Servicio de usuario de difusión y G...
Running     BDESVC              Servicio Cifrado de unidad BitLocker
Running     BFE                 Motor de filtrado de base
Running     BITS                Servicio de transferencia inteligen...
Stopped     BluetoothUserSe... Servicio de soporte técnico de usua...
Running     BrokerInfrastru... Servicio de infraestructura de tare...
Stopped     BTAGService         Servicio de puerta de enlace de aud...
Stopped     BthAvctpSvc         Servicio AVCTP
Running     bthserv             Servicio de compatibilidad con Blue...
Running     camsvc              Servicio Administrador de funcional...
Stopped     CaptureService_...  CaptureService_d7dbf
Running     cbdhsvc_d7dbf       Servicio de usuario del portapapele...
Running     CDPSvc              Servicio de plataforma de dispositi...
Running     CDPUserSvc_d7dbf    Servicio de usuario de plataforma d...
Stopped     CertPropSvc         Propagación de certificados
-- Más --
    
```

Y cuando necesitamos sólo algunos de los procesos, siempre podemos establecer un filtro. Por ejemplo, por su nombre:

```

PS C:\Users\claud> Get-Service -name appinfo

Status      Name                DisplayName
-----
Running     appinfo             Información de la aplicación
    
```

8. Iniciar o detener un servicio

```

powershell

Start-Service -Name "wuauserv"
Stop-Service -Name "wuauserv"
    
```