

RA2: Administra procesos del sistema describiendo y aplicando criterios de seguridad y eficiencia.

Concepto de proceso del sistema, tipos, estado y ciclo de vida.

Podemos definir el **proceso del sistema** como una ejecución diferenciada de uno de los programas del sistema. Por ejemplo, si nombramos el proceso del sistema explorer.exe, nos estamos refiriendo a esta instancia del programa en funcionamiento.



Explorador de Windows	0%	32,9 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
-----------------------	----	---------	--------	--------	----------	----------

El **programa** explorer.exe es un objeto pasivo mientras no lo estamos procesando, de ahí la distinción. También surge a menudo el término **servicio**, que se caracteriza por trabajar en segundo plano.

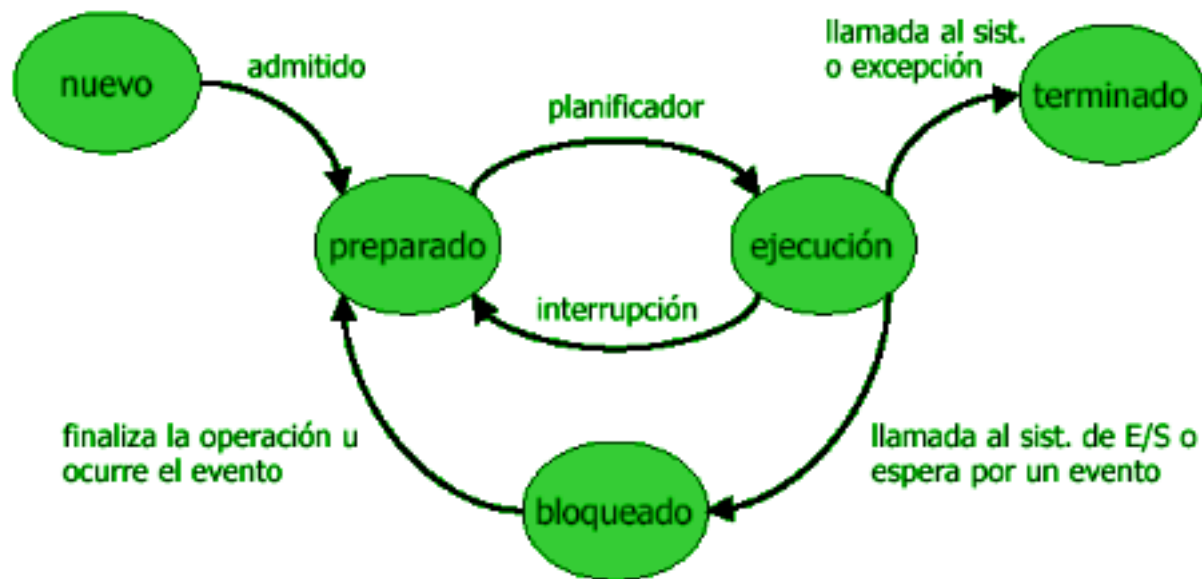
Podemos distinguir entre dos tipos de procesos, los **procesos en primer plano** y los **procesos en segundo plano**. Mientras que los usuarios pueden interactuar con los procesos en primer plano, los procesos en segundo plano son aquellos que realizan su función con independencia del usuario, que no interactúa con ellos. Otra manera de referirse a ellos es **procesos interactivos** para los primeros y **demonios** para los segundos..

Un proceso puede tener **3 estados**: Preparado, en ejecución y bloqueado. Otras clasificaciones incluyen también nuevo y terminado.

- **Preparado:** El proceso está listo para lanzarse, a la espera de que el gestor de procesos le asigne CPU y pase a estado de ejecución o bien se finalice por acción de otra instrucción.
- **En ejecución:** El proceso ejecuta órdenes mientras disponga de tiempo de ejecución, hasta terminar sus instrucciones o algo lo bloquee. Por ejemplo, un proceso puede quedar a medias si supera el tiempo que se le ha asignado de ejecución.
- **Bloqueado:** De manera similar al estado preparado, el proceso bloqueado está a la espera de que el gestor de procesos le asigne tiempo de ejecución o que otra

instrucción lo finalice. Se diferencia del estado preparado en que ya ha sido iniciado anteriormente.

Definimos el ciclo de vida de un proceso como los cambios que experimenta desde que sea crea hasta que se finaliza.



Podemos ver que los únicos apartados lineales del ciclo son la creación y la finalización. Durante su ciclo de vida, un proceso puede estar sujeto a muchos cambios en función de la gestión de procesos, interrupciones...

Eventos internos del procesador: Interrupciones y excepciones

Una **interrupción** es un evento interno del procesador que interrumpe un proceso que estaba en ejecución, suspendiendo temporalmente la misma. Hoy en día, los dispositivos son los encargados de solicitar la interrupción de los procesos.

Pongamos un ejemplo de **interrupción mediante hardware**. Tenemos un dispositivo de entrada/salida, por ejemplo una impresora, que ha encontrado un problema para imprimir un documento porque no le queda papel. La impresora 'avisa' al procesador del problema, que interrumpe el proceso que origina esa impresión. En nuestro ejemplo teórico, al restablecer el

suministro de papel, la impresora enviará una nueva señal y el procesador reanudará el proceso.

La **interrupción mediante software**, por otra parte, tiene su origen en el propio código. Por ejemplo, cuando los programas se vendían con varios discos de instalación, los procesos de instalación se interrumpían a sí mismos y quedaban a la espera hasta que se introducía el siguiente disco de instalación. Cuando el disco era insertado, se podía reanudar el proceso de instalación.



Ejemplo de instalación con interrupción de software.

Finalmente, las **excepciones** son un tipo de interrupción causada por una condición de error en un programa, como puede ser un acceso no válido a la memoria o una división entre cero. El usuario pierde el control temporalmente mientras el sistema operativo intenta subsanar el error,

ofreciendo al usuario una pantalla informativa.



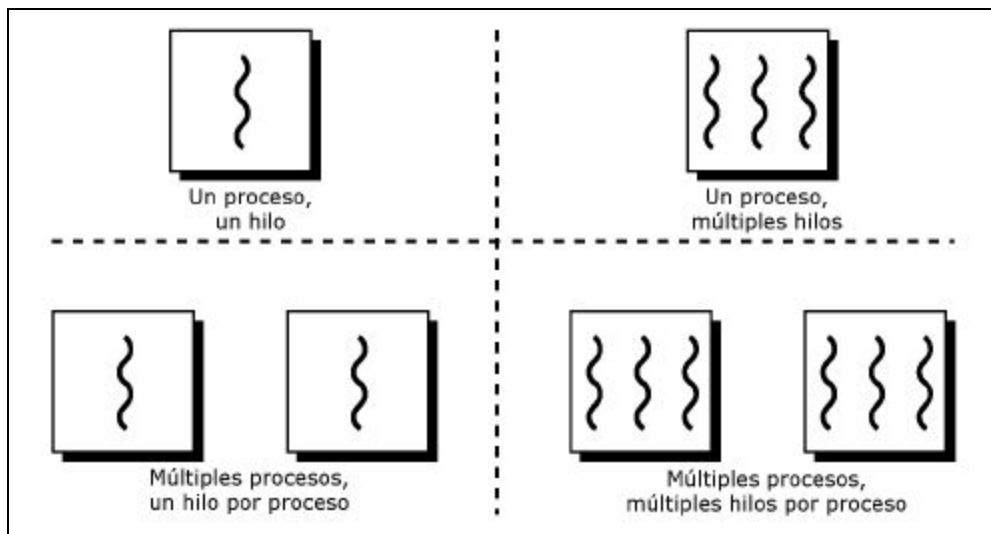
Blue Screen Of Death, la pantalla mostrada a los usuarios en sistemas Windows.

Diferencias y similitudes entre procesos e hilos. El concepto de trabajo en contexto.

Mientras que un **proceso** se ejecuta de manera independiente y no se puede comunicar con otros procesos salvo que se usen mecanismos de comunicación entre procesos. Todo proceso integra, al menos, un hilo.

No obstante, los **hilos** nos confieren mayor flexibilidad. Tienen una serie de semejanzas con los **procesos**, a saber:

- Pueden estar en uno o varios estados: listo, bloqueado, en ejecución o terminado.
- Comparten la CPU.
- Un hilo dentro de un proceso se ejecuta secuencialmente.
- Cada hilo tiene su propia pila y contador de programa.
- Pueden crear sus propios hilos hijos.



A pesar de sus parecidos, hay una **diferencia fundamental**. Los hilos pueden compartir sus órdenes y leer o modificar la pila de otros hilos. Ello conlleva una serie de **ventajas**:

- La creación de un nuevo hilo en un proceso existente es más rápida que crear un nuevo proceso.
- De igual forma, terminar un hilo es más rápido que terminar un proceso
- La conmutación entre hilos de un mismo proceso es más ágil que un salto entre procesos.
- Los hilos hacen más rápida la comunicación entre procesos, ya que al compartir memoria y recursos, se pueden comunicar entre sí sin invocar el núcleo del SO.

Sobre el concepto de **trabajo**, tenemos que diferenciar entre dos tipos de hilos. Hay un **hilo jefe** encargado de repartir la carga de trabajo entre **hilos trabajadores**. Eso no impide que se de un hilo jefe que a la vez sea hilo trabajador, solo que tiene esa tarea jerárquica.

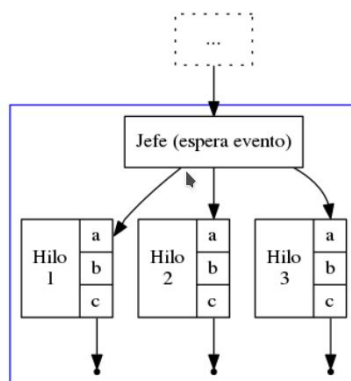
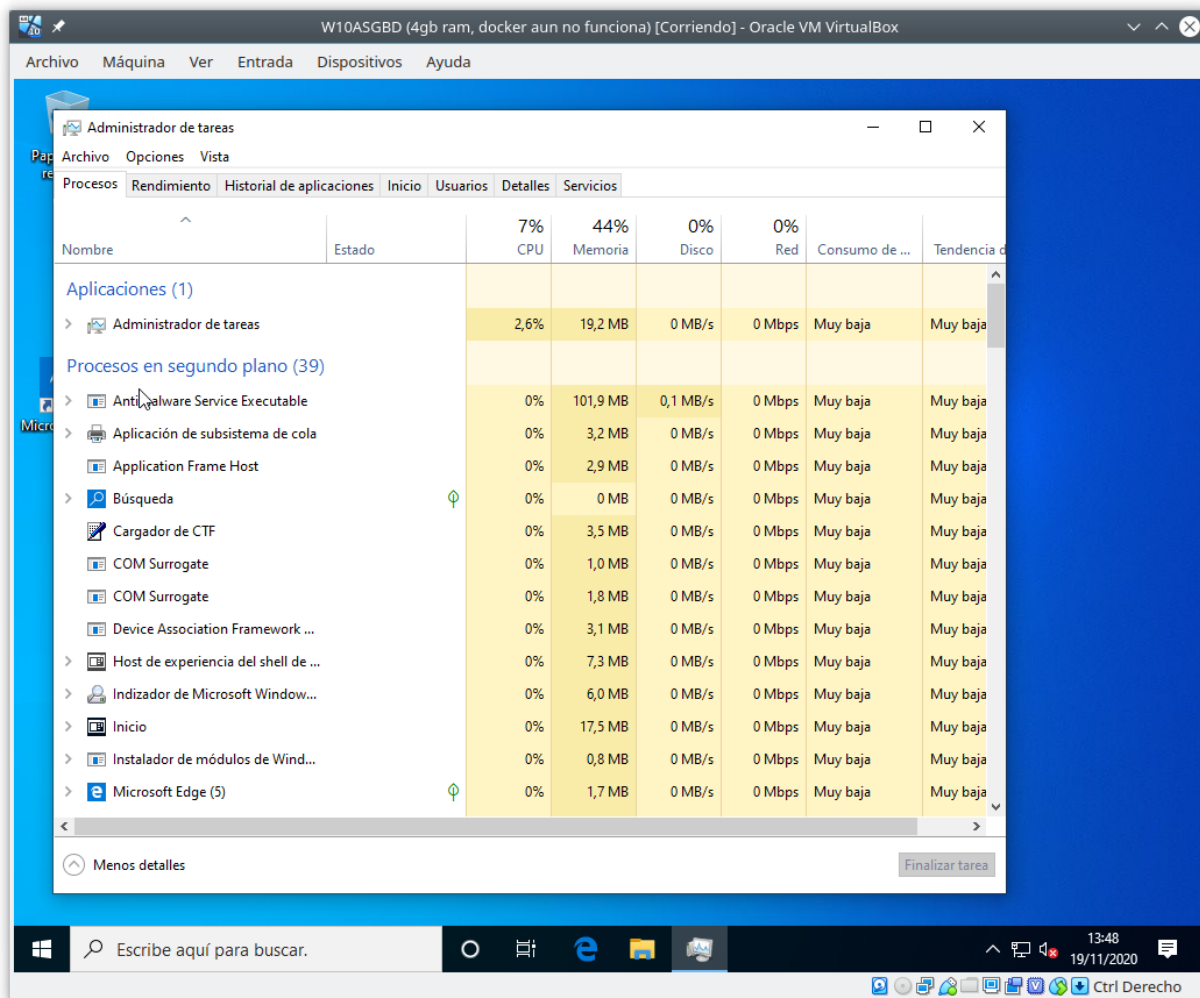


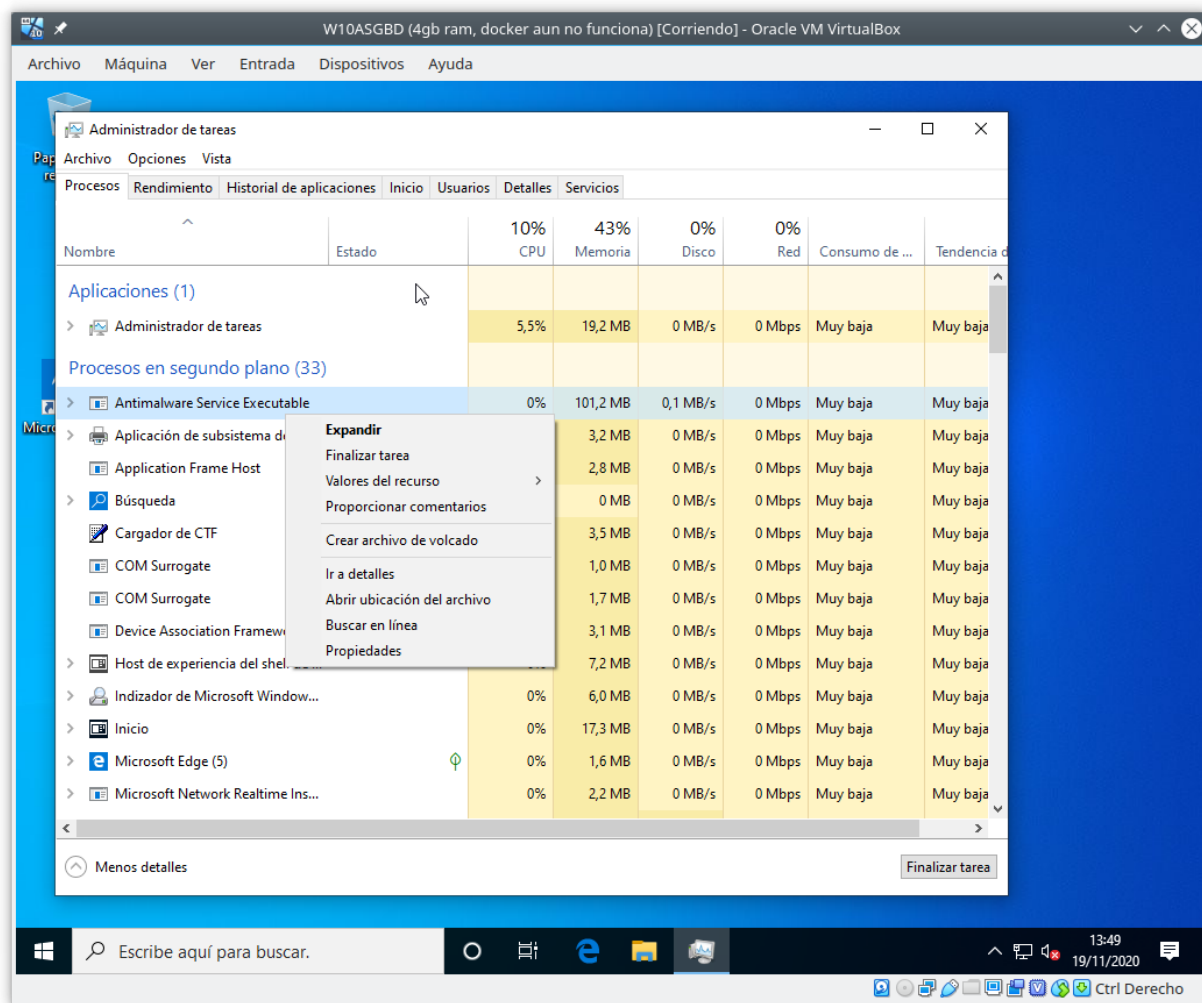
Figura: Patrón de hilos jefe/trabajador

Tareas de identificación, creación, manipulación y terminación de procesos mediante administrador de tareas.

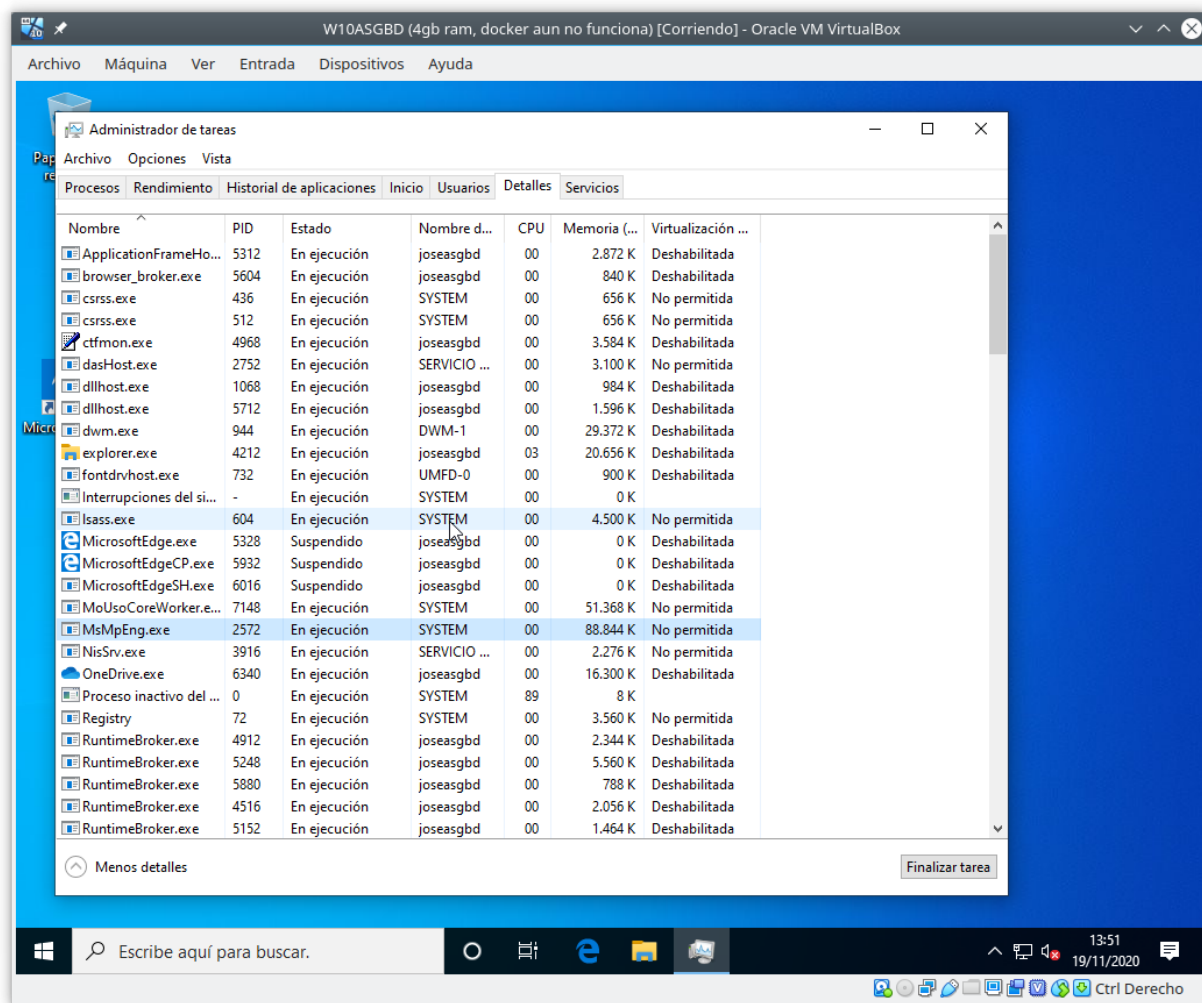
Accedemos al administrador de tareas con el buscador de la barra de tareas o con el atajo de teclado **control+shift+esc.** Una vez allí nos dirigimos a la pestaña 'Procesos'



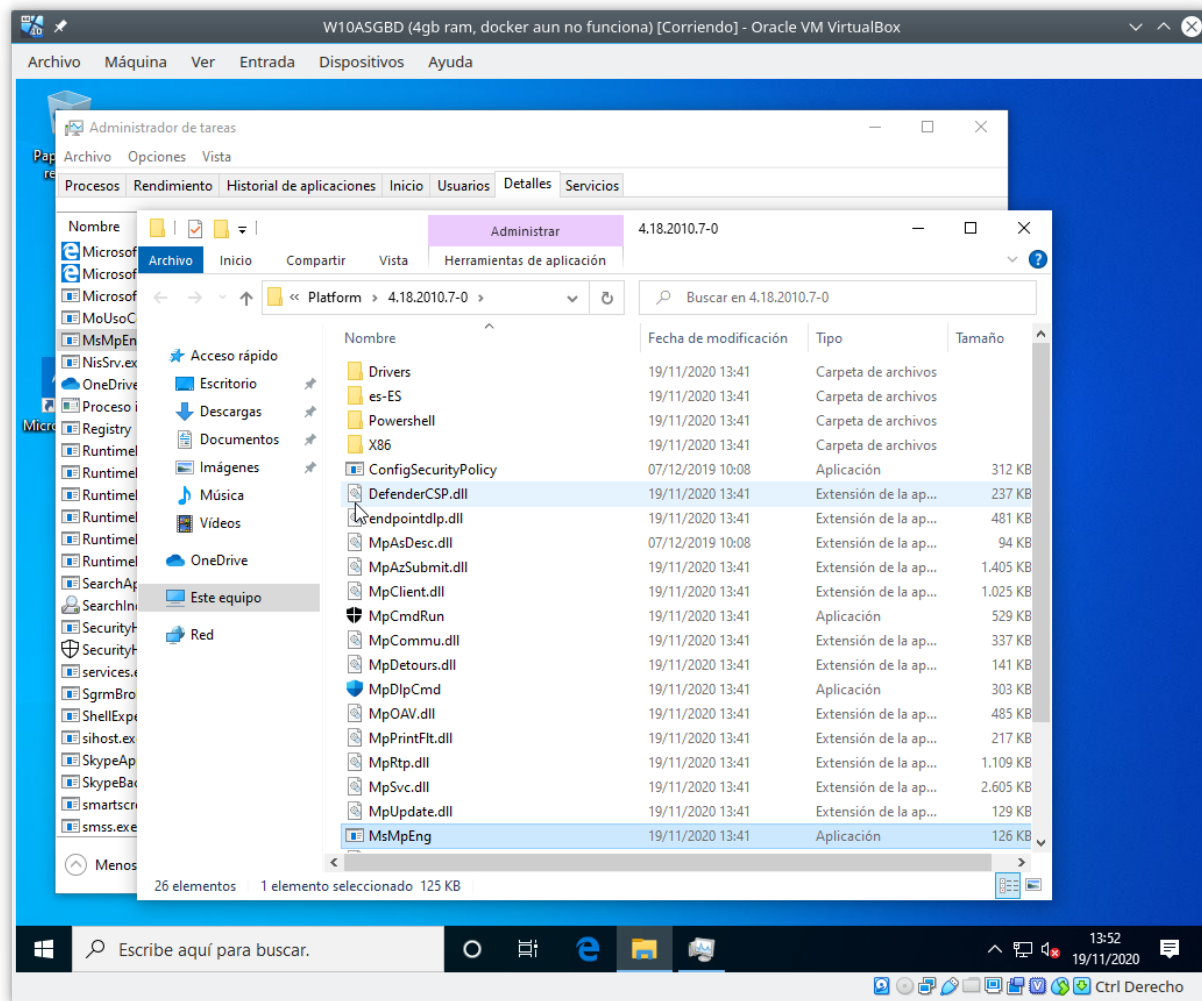
Aquí podemos observar los diferentes procesos y datos sobre los mismos.



Haciendo click derecho en un proceso, se nos presentan diferentes opciones. Podemos empezar por ir a detalles para obtener más información.

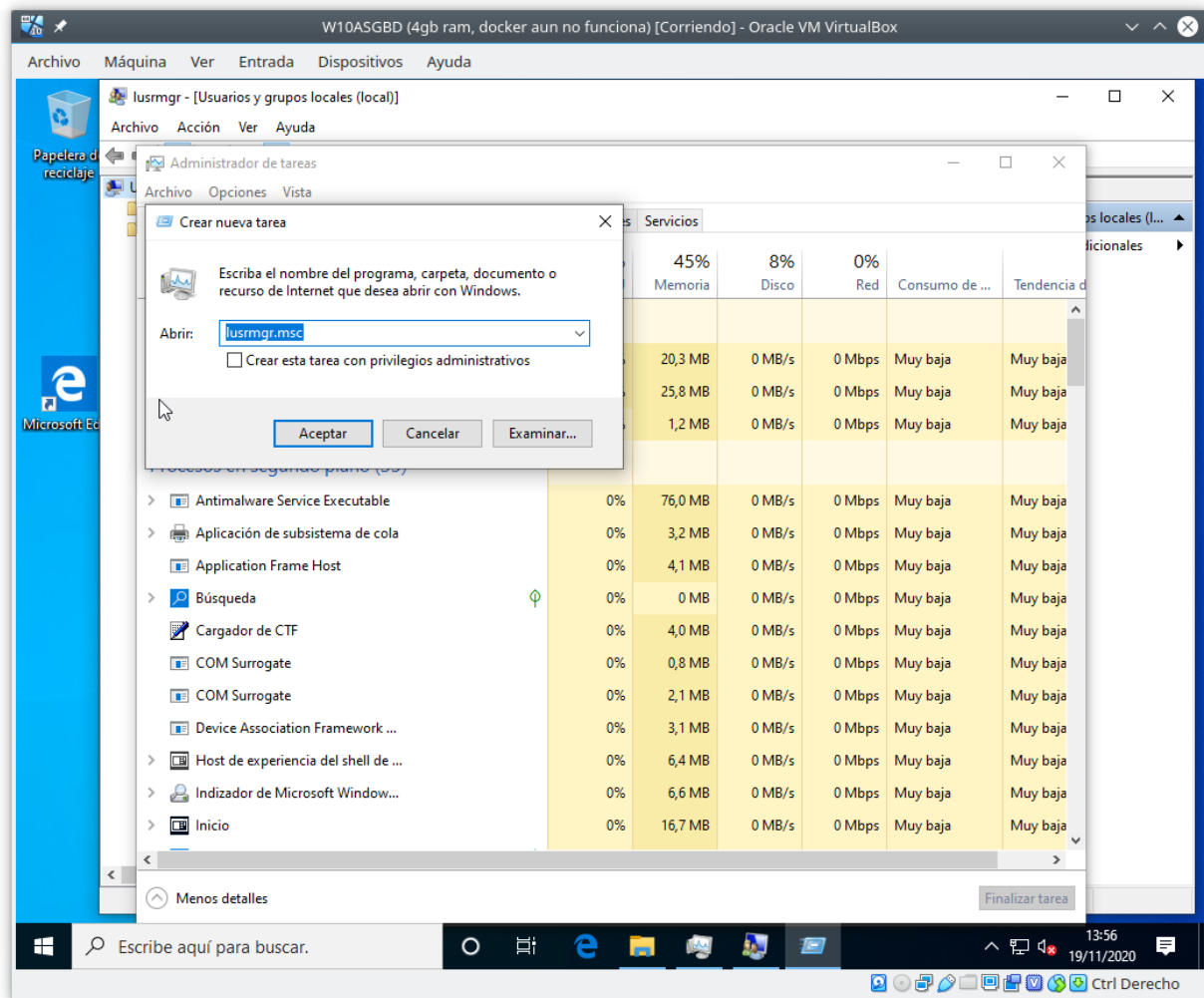


En esta vista podemos ver el nombre completo de proceso, útil para buscar documentación sobre el mismo. Vemos su ID de proceso, el estado actual, el usuario que lo está ejecutando y el uso que hace de los recursos hardware.

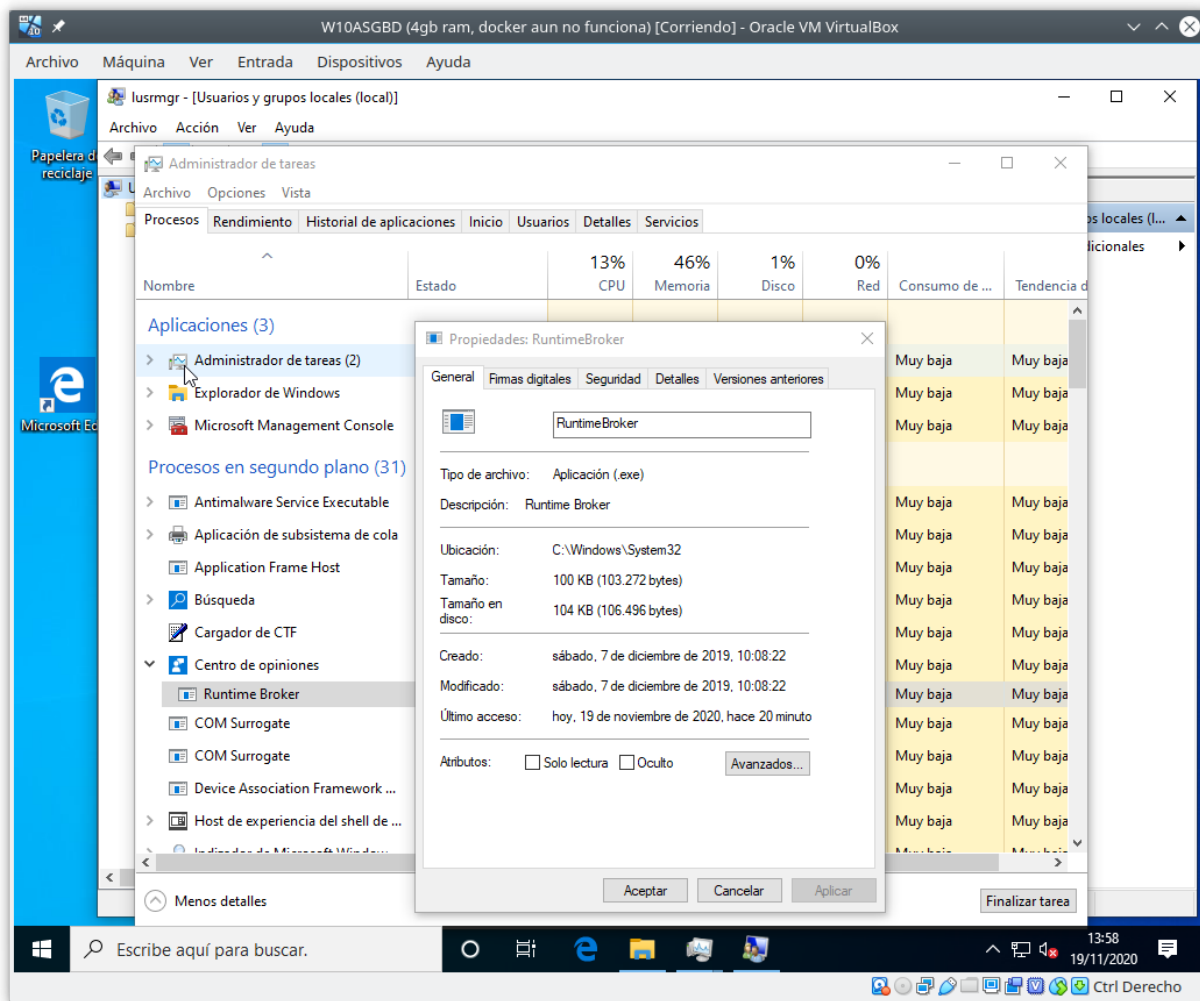


Haciendo click derecho sobre el proceso podemos ver la ubicación del archivo. Otras opciones son buscar información en línea o ir al servicio, cambiando a la pestaña servicios.

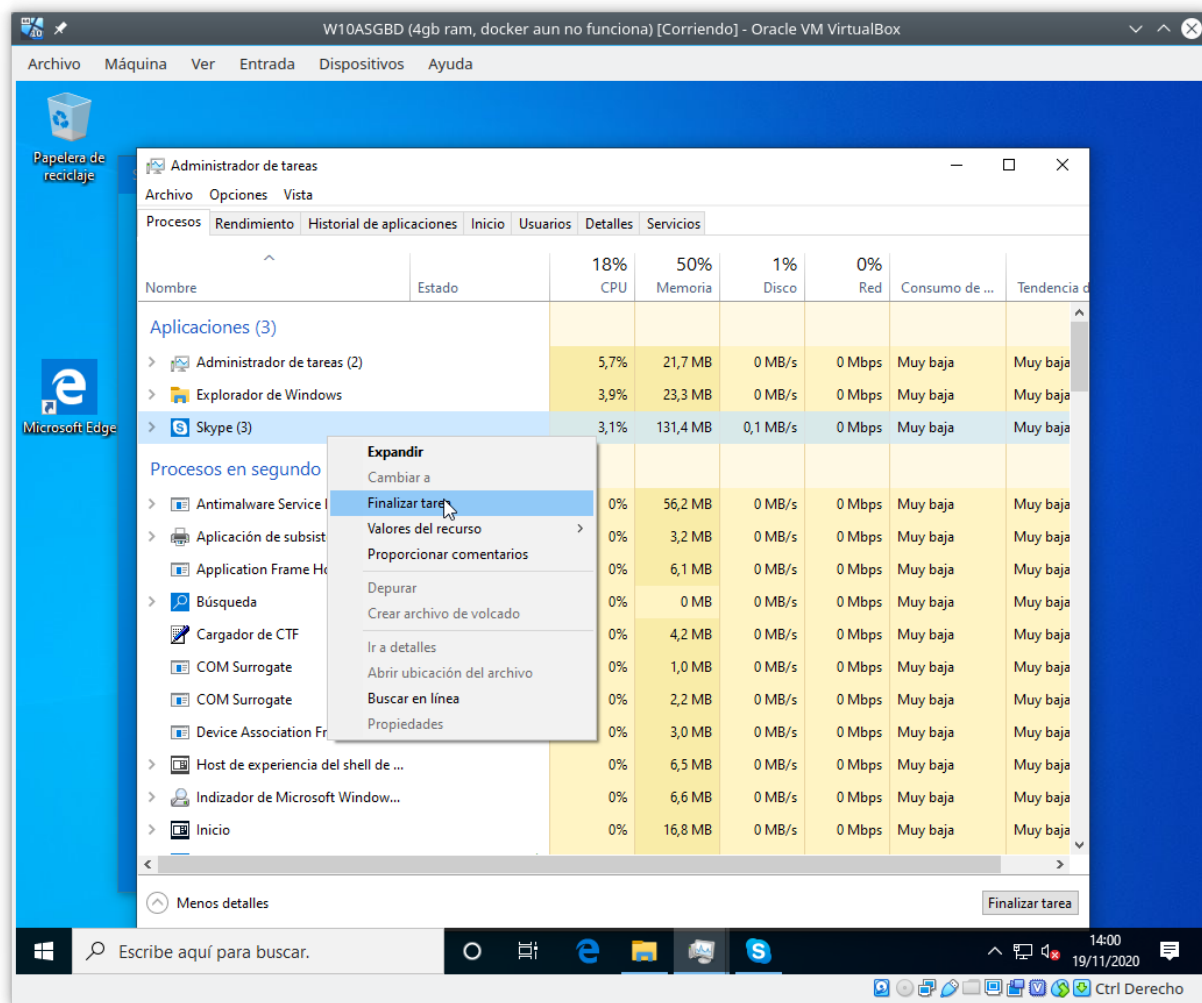
Para iniciar un proceso desde el administrador de tareas tan solo tenemos que pulsar en 'archivo' y 'crear nueva tarea'



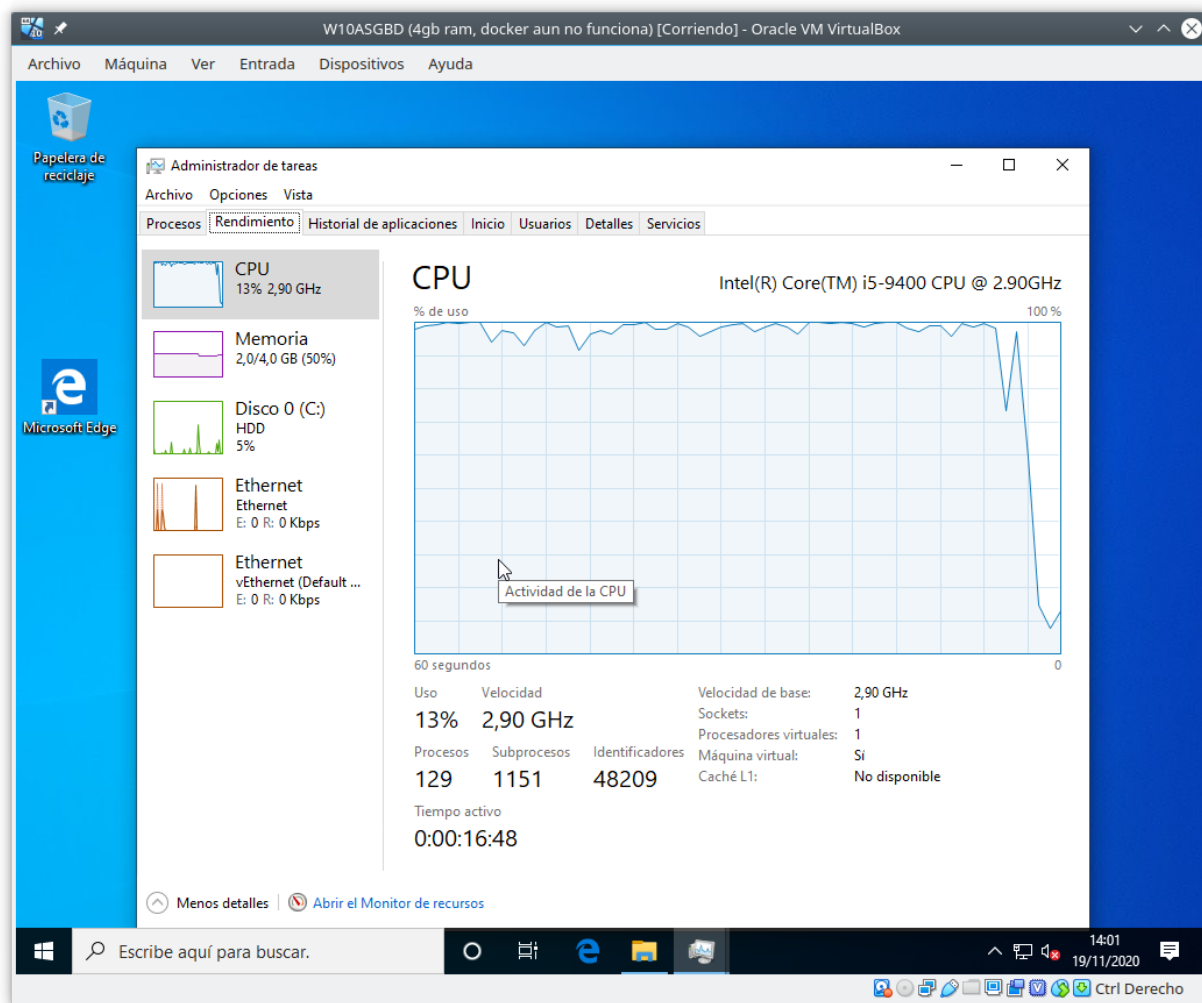
En la imagen hemos accedido a los usuarios y grupos locales como ejemplo.



También podemos manipular estos procesos, haciendo click derecho y entrando en el menú de propiedades. Es importante que sepamos lo que estamos haciendo y nos documentemos antes de empezar a manipular estas opciones.



También podremos finalizar una tarea desde el administrador. En la imagen podemos ver cómo finalizamos un proceso que suele consumir muchos recursos.



Finalmente podemos abrir la pestaña rendimiento para comprobar el número de procesos activos y los recursos que están usando. La gráfica muestra el consumo de Skype en nuestra máquina virtual y el cambio tras finalizar su proceso.

Tareas de identificación, creación, manipulación y terminación de procesos mediante PowerShell.

PowerShell es una herramienta poderosa que emplea los comandos del símbolo del sistema y sus propios comandos orientados a objetos. Es importante tener una buena documentación a mano y por suerte la podemos encontrar en docs de Microsoft.

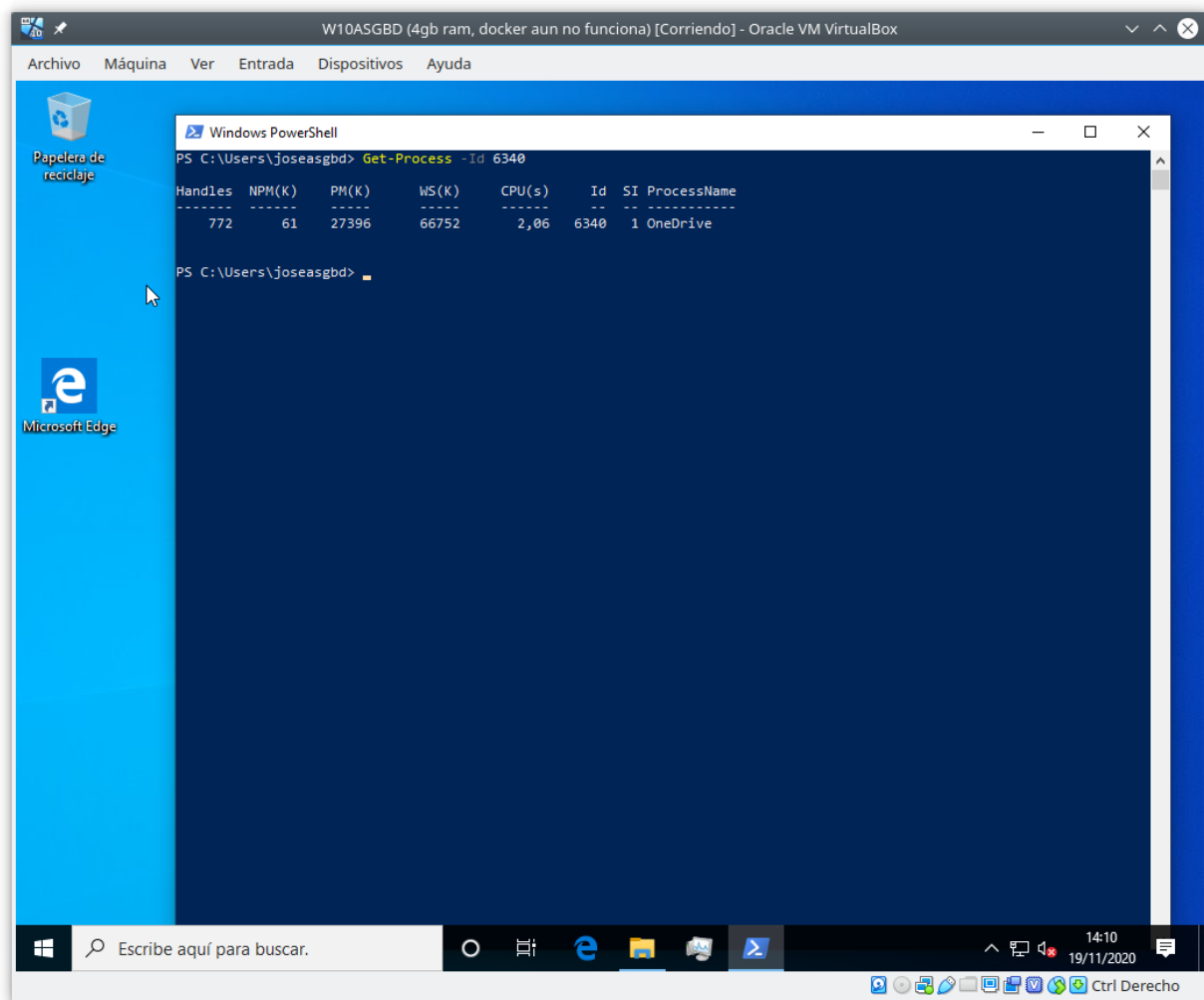
<https://docs.microsoft.com/es-es/powershell/scripting/samples/sample-scripts-for-administration?view=powershell-7.1>

Para identificar procesos nos interesan las siguientes instrucciones:

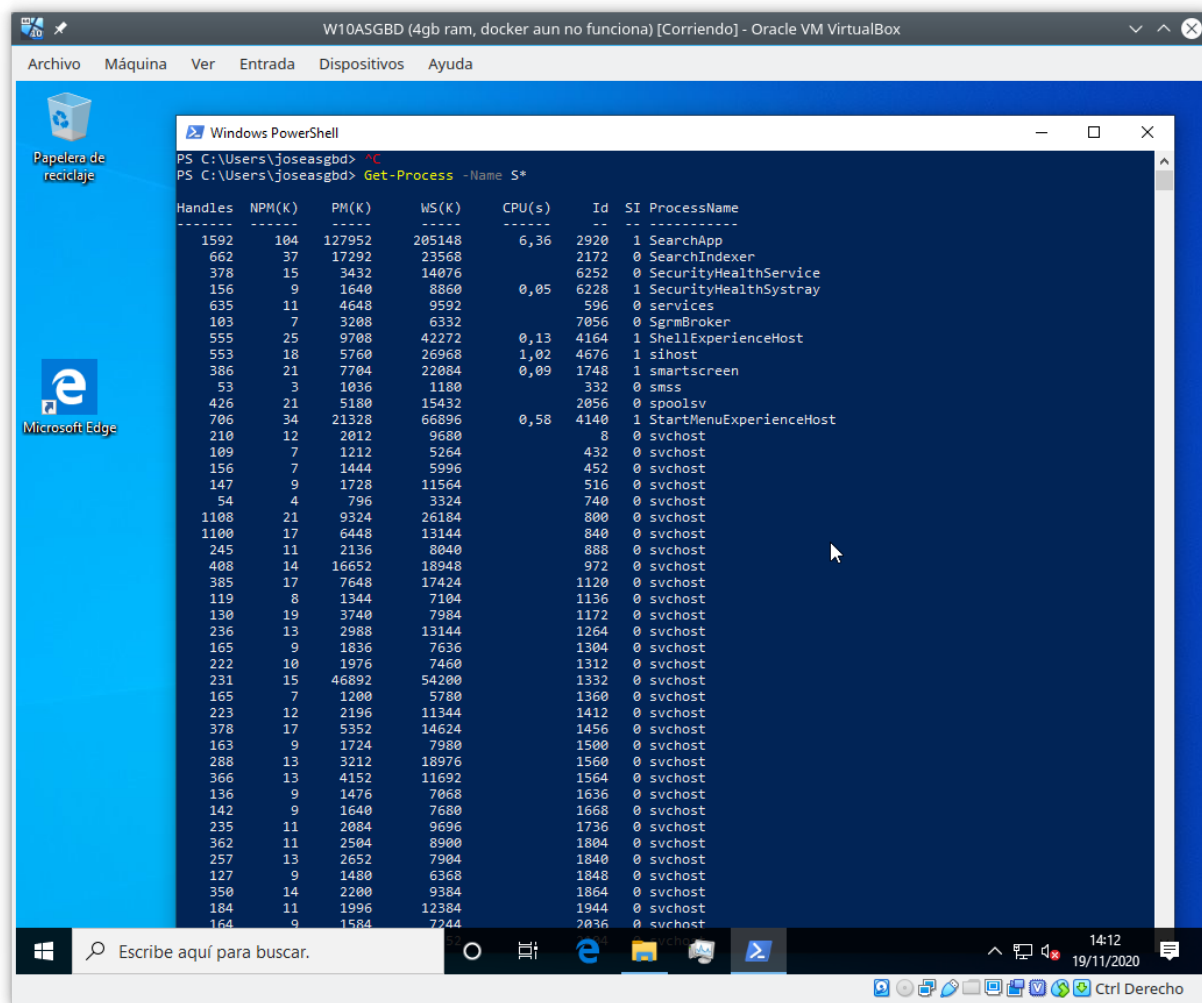
The screenshot shows a Windows VM window titled "W10ASGBD (4gb ram, docker aun no funciona) [Corriendo] - Oracle VM VirtualBox". Inside the VM, a Windows PowerShell window is open, displaying the output of the `Get-Process` command. The output is a table with columns: Handles, NPM(K), PM(K), WS(K), CPU(s), Id, SI, and ProcessName. The list includes various system and user processes such as ApplicationFrameHost, browser_broker, conhost, csrss, csrss, ctfmon, dasHost, dllhost, dwm, explorer, fontdrvhost, Idle, lsass, Memory Compression, MicrosoftEdge, MicrosoftEdgeCP, MicrosoftEdgeSH, MoUsoCoreWorker, MsMpEng, NisSrv, OneDrive, powershell, Registry, RuntimeBroker, SearchApp, SearchIndexer, SecurityHealthService, SecurityHealthSystray, services, SgrmBroker, ShellExperienceHost, sihost, and smartscreen.

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
339	20	8732	28916	0,34	5312	1	ApplicationFrameHost
135	9	1552	8632	0,02	4284	1	browser_broker
264	14	4116	17820	0,13	3208	1	conhost
483	21	1548	5092		436	0	csrss
363	17	1620	4944		512	1	csrss
454	17	5116	21728	0,75	4968	1	ctfmon
368	18	3624	13428		2752	0	dasHost
138	9	1892	12348	0,08	1068	1	dllhost
297	34	7444	15444	0,16	5712	1	dllhost
982	57	43476	73020		944	1	dwm
2123	83	36396	112724	7,81	4212	1	explorer
32	6	1648	4676		724	1	fontdrvhost
32	5	1272	3332		732	0	fontdrvhost
0	0	60	8		0	0	Idle
1256	25	6628	18528		604	0	lsass
0	0	196	21868		1484	0	Memory Compression
970	51	21672	65632	0,34	960	1	MicrosoftEdge
1066	132	163980	201824	2,75	848	1	MicrosoftEdgeCP
274	14	4464	15940	0,39	6260	1	MicrosoftEdgeSH
261	22	101480	114796		7148	0	MoUsoCoreWorker
661	66	169328	113808		2572	0	MsMpEng
198	11	3588	10148		3916	0	NisSrv
772	61	27396	66748	2,06	6340	1	OneDrive
684	44	54748	74256	2,61	1896	1	powershell
0	7	4236	72928		72	0	Registry
334	18	4304	22396	0,23	4516	1	RuntimeBroker
283	16	5504	23628	1,13	4912	1	RuntimeBroker
583	28	10676	39192	0,67	5248	1	RuntimeBroker
264	14	3352	17676	0,27	5880	1	RuntimeBroker
199	11	2388	16156	0,08	6620	1	RuntimeBroker
1592	104	127952	205304	6,36	2920	1	SearchApp
670	37	17504	23636		2172	0	SearchIndexer
378	15	3460	14088		6252	0	SecurityHealthService
156	9	1640	8860	0,05	6228	1	SecurityHealthSystray
660	12	4860	9680		596	0	services
103	7	3324	6412		7056	0	SgrmBroker
555	25	9708	42260	0,11	4164	1	ShellExperienceHost
581	18	5952	28096	1,02	4676	1	sihost
411	22	7936	22228	0,09	1748	1	smartscreen

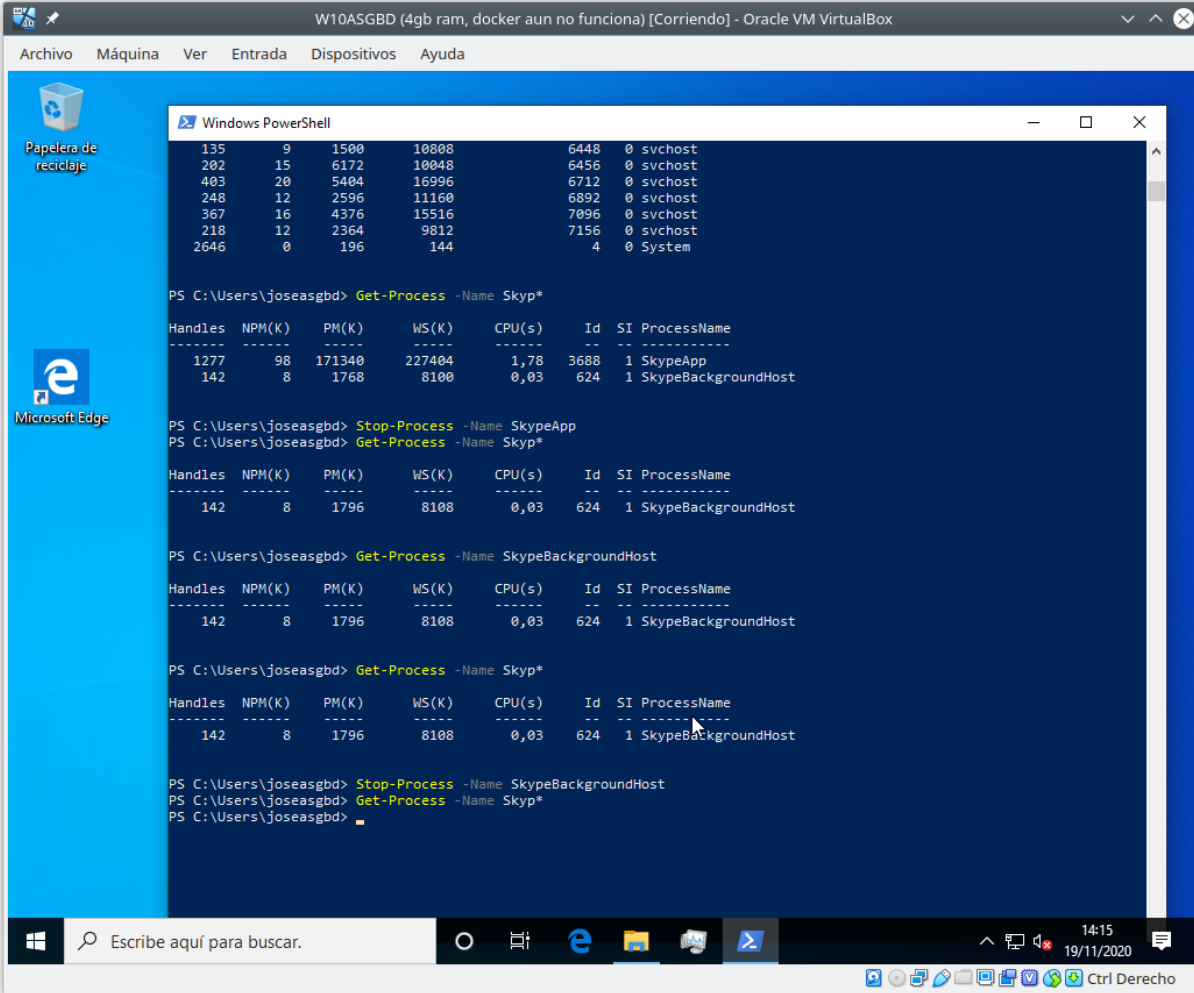
`Get-Process` nos entrega una detallada lista de los procesos en ejecución. Podemos limitar la lista si añadimos una ID como parámetro.



También podemos buscar por nombre de proceso. En el siguiente ejemplo, buscamos todos los procesos que empiezan por S para asegurarnos de que Skype se ha cerrado correctamente.



El comando "Stop-Process -Name nombre_del_proceso" nos permite terminar un proceso. Para ponerlo en práctica, hemos vuelto a lanzar Skype para localizarlo y destruirlo.



The screenshot shows a Windows 10 desktop environment within a VirtualBox VM. A PowerShell window is open, displaying the results of several commands. The desktop background is blue with icons for 'Papelera de reciclaje' and 'Microsoft Edge'. The taskbar at the bottom shows the Start button, a search bar, and several application icons. The system tray on the right shows the time as 14:15 on 19/11/2020.

```
W10ASGBD (4gb ram, docker aun no funciona) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Papelera de reciclaje
Microsoft Edge

Windows PowerShell
135      9      1500      10808      6448      0      svchost
202      15      6172      10848      6456      0      svchost
403      20      5404      16996      6712      0      svchost
248      12      2596      11160      6892      0      svchost
367      16      4376      15516      7096      0      svchost
218      12      2364      9812      7156      0      svchost
2646     0      196      144      4      0      System

PS C:\Users\joseasgbd> Get-Process -Name Skyp*

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
1277     98  171340  227404  1,78  3688  1 SkypeApp
142      8   1768    8100    0,03  624   1 SkypeBackgroundHost

PS C:\Users\joseasgbd> Stop-Process -Name SkypeApp
PS C:\Users\joseasgbd> Get-Process -Name Skyp*

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
142      8   1796    8108    0,03  624   1 SkypeBackgroundHost

PS C:\Users\joseasgbd> Get-Process -Name SkypeBackgroundHost

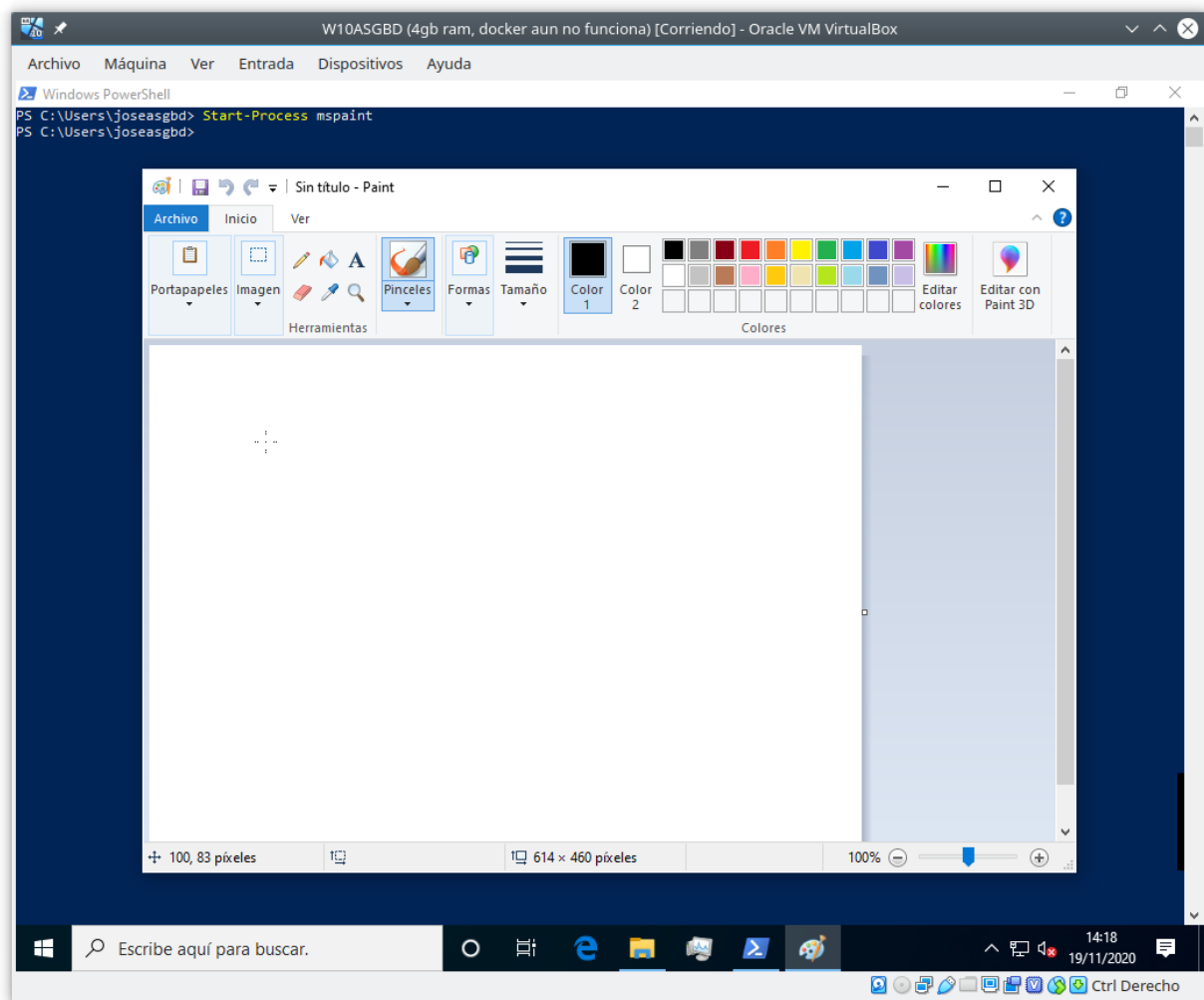
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
142      8   1796    8108    0,03  624   1 SkypeBackgroundHost

PS C:\Users\joseasgbd> Get-Process -Name Skyp*

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
142      8   1796    8108    0,03  624   1 SkypeBackgroundHost

PS C:\Users\joseasgbd> Stop-Process -Name SkypeBackgroundHost
PS C:\Users\joseasgbd> Get-Process -Name Skyp*
PS C:\Users\joseasgbd>
```

En esta secuencia hemos localizado los procesos que derivan de Skype, destruyendo ambos y asegurándonos de que han finalizado.



El comando Start-Process nos permite iniciar un nuevo proceso, tal como muestra la imagen.

En la documentación vemos algunos comandos algo más avanzados como

[Wait-Process](#), [Debug-Process](#) y [Invoke-Command](#)


Subsección I: Comprobación de la secuencia de arranque del sistema, los procesos implicados y la relación entre ellos.


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

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\jpadi> Get-WmiObject win32_process | Sort-Object Processid | Select-Object Processid,Name,CommandLine

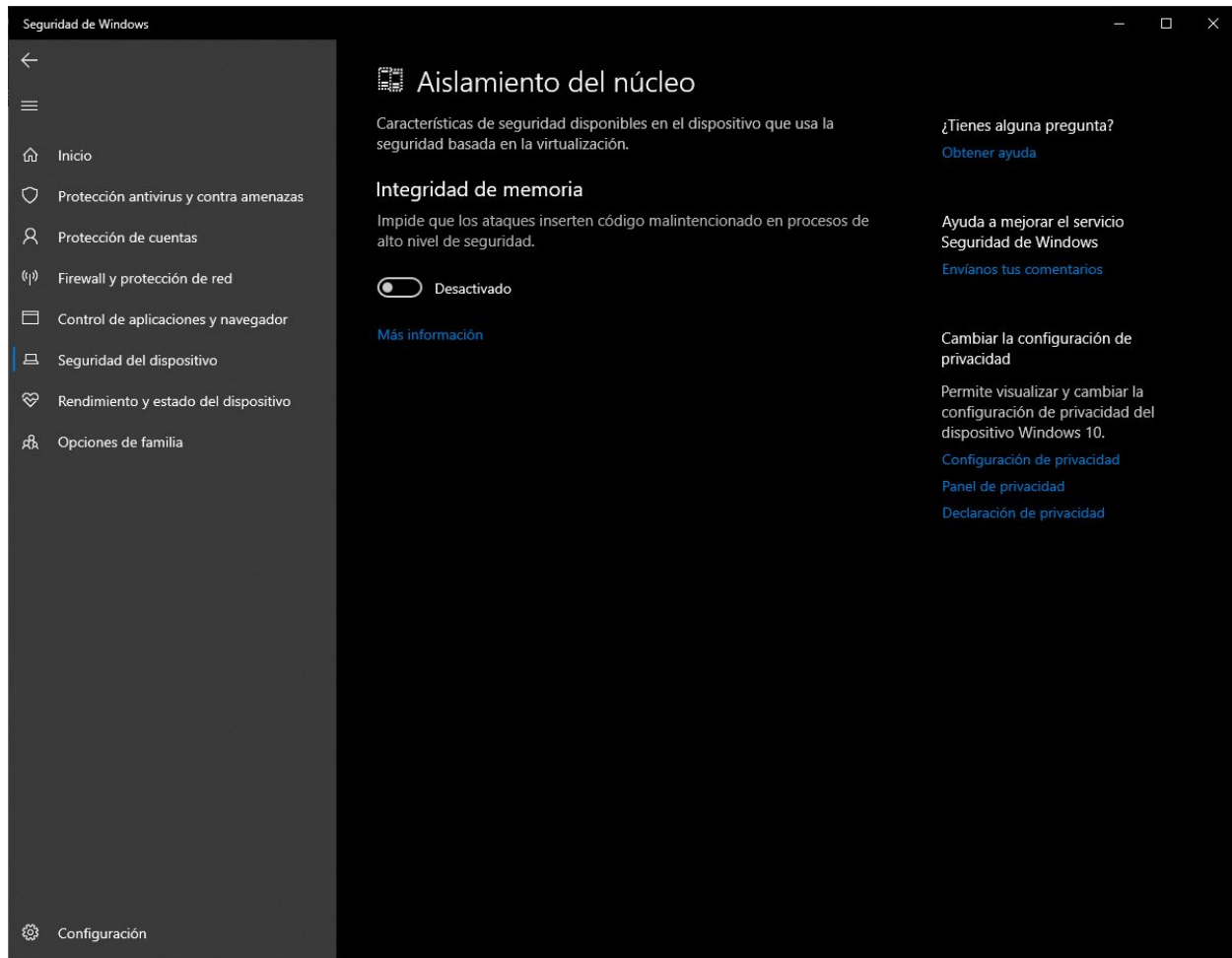
Processid Name                CommandLine
-----
0 System Idle Process
4 System
100 Registry
444 smss.exe
580 svchost.exe
604 svchost.exe
612 csrss.exe
616 fontdrvhost.exe
708 wininit.exe
716 csrss.exe
720 fontdrvhost.exe
812 winlogon.exe
876 svchost.exe
920 services.exe
928 lsass.exe
1004 svchost.exe
1096 dwm.exe
1132 firefox.exe
1192 svchost.exe
1224 svchost.exe
1232 svchost.exe
```



Esta captura nos muestra los procesos relacionados con el arranque, ordenados por ID de proceso. Los procesos implicados se explican en la sección final del trabajo, 'Procesos habituales del sistema'

Subsección II: Medidas de seguridad ante la aparición de procesos no identificados

Windows dispone de varias herramientas para usuario integradas.



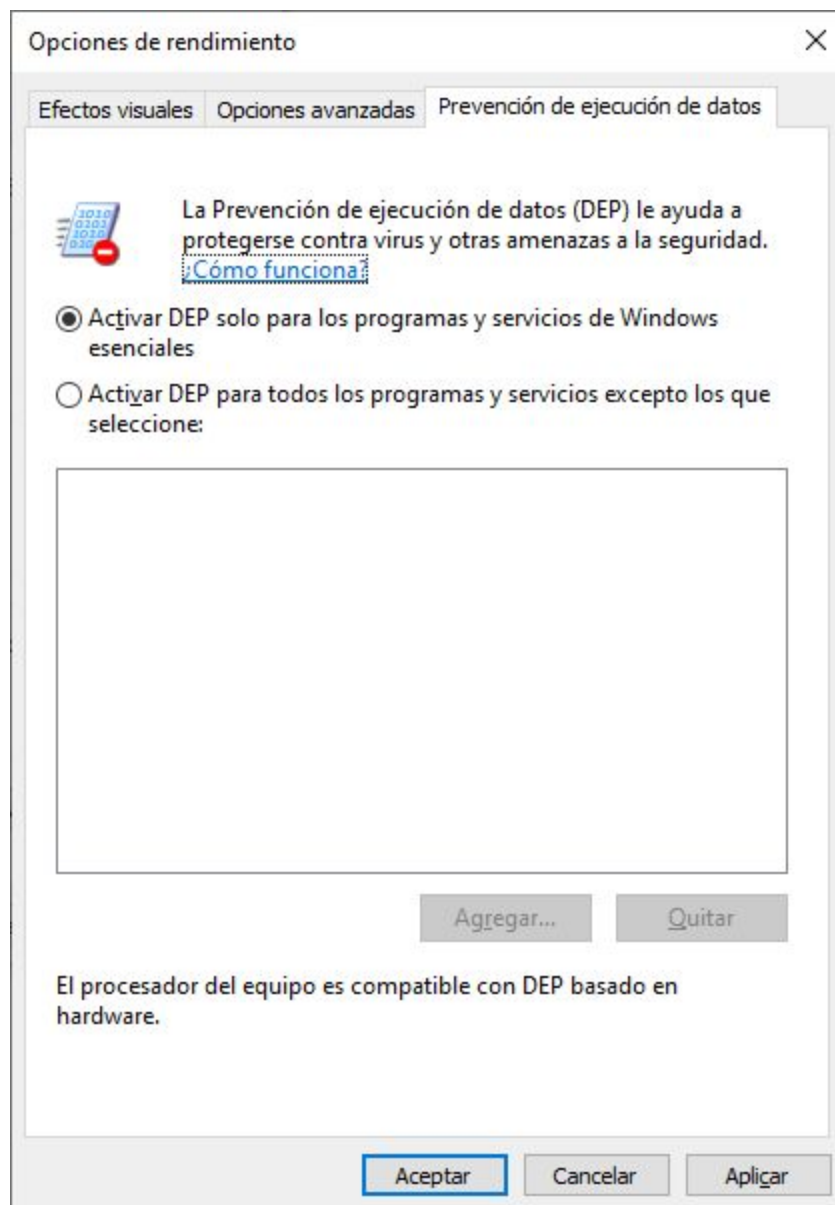
Por ejemplo, se puede activar el aislamiento del núcleo para añadir una capa extra de seguridad para ciertos procesos. Se emplea Hyper-v para ello.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/memory-integrity>

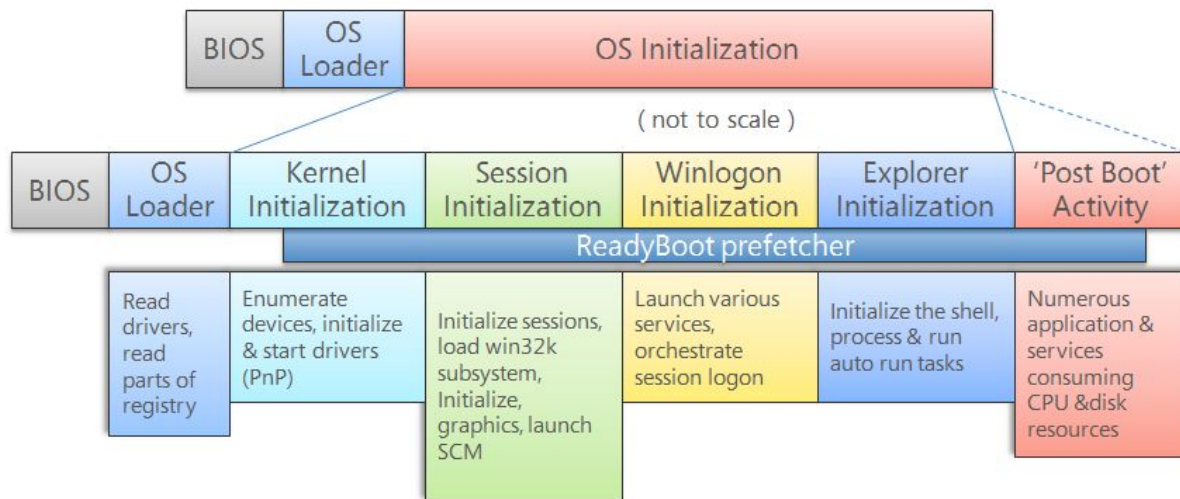
También podemos añadir la columna 'Elevado' a la sección 'Detalles' del administrador de tareas para saber qué se está ejecutando con privilegios de administrador.

Administrador de tareas							
Archivo Opciones Vista							
Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios							
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Elevado	Virtualización ...
CompPkgSvc.exe	4060	En ejecución	jpadi	00	1.108 K	No	Deshabilitada
conhost.exe	10084	En ejecución	jpadi	00	76 K	No	Deshabilitada
csrss.exe	612	En ejecución	SYSTEM	00	560 K	Sí	No permitida
csrss.exe	716	En ejecución	SYSTEM	00	768 K	Sí	No permitida
ctfmon.exe	6284	En ejecución	jpadi	00	5.300 K	No	Deshabilitada
dasHost.exe	3988	En ejecución	SERVICIO ...	00	20 K	Sí	No permitida
Discord.exe	2064	En ejecución	jpadi	00	13.848 K	Sí	No permitida
Discord.exe	4216	En ejecución	jpadi	00	28.664 K	Sí	No permitida
Discord.exe	2332	En ejecución	jpadi	00	3.864 K	Sí	No permitida
Discord.exe	4820	En ejecución	jpadi	00	456 K	Sí	No permitida
Discord.exe	3164	En ejecución	jpadi	05	91.224 K	Sí	No permitida
Discord.exe	7984	En ejecución	jpadi	00	996 K	Sí	No permitida
DiscSoftBusServiceL...	11376	En ejecución	SYSTEM	00	2.828 K	Sí	No permitida
dllhost.exe	9080	En ejecución	SYSTEM	00	264 K	Sí	No permitida
dllhost.exe	12128	En ejecución	jpadi	00	1.680 K	No	Deshabilitada
dllhost.exe	8436	En ejecución	jpadi	00	1.168 K	No	Deshabilitada
DTShellHlp.exe	2412	En ejecución	jpadi	00	1.956 K	No	Deshabilitada
dwm.exe	1096	En ejecución	DWM-1	00	22.912 K	No	Deshabilitada
explorer.exe	6812	En ejecución	jpadi	00	37.548 K	No	Deshabilitada
FastBootService.exe	3712	En ejecución	SYSTEM	00	248 K	Sí	No permitida
firefox.exe	2432	En ejecución	jpadi	00	413.924 K	No	Deshabilitada
firefox.exe	8084	En ejecución	jpadi	00	46.696 K	No	Deshabilitada
firefox.exe	5992	En ejecución	jpadi	00	91.700 K	No	Deshabilitada
firefox.exe	11292	En ejecución	jpadi	00	45.224 K	No	Deshabilitada
firefox.exe	6304	En ejecución	jpadi	00	9.748 K	No	Deshabilitada
firefox.exe	10540	En ejecución	jpadi	00	260.912 K	No	Deshabilitada
firefox.exe	9296	En ejecución	jpadi	01	103.624 K	No	Deshabilitada
firefox.exe	7384	En ejecución	jpadi	00	157.476 K	No	Deshabilitada
firefox.exe	7728	En ejecución	jpadi	00	796 K	No	Deshabilitada
firefox.exe	1132	En ejecución	jpadi	00	121.208 K	No	Deshabilitada
firefox.exe	6316	En ejecución	jpadi	00	50.568 K	No	Deshabilitada
firefox.exe	12260	En ejecución	jpadi	00	101.992 K	No	Deshabilitada

Una medida más que he encontrado en Sistema>Avanzado>Rendimiento es el sistema de prevención de ejecución de datos. Por defecto hace que los procesos de sistema se ejecuten desde partes de la memoria con unos privilegios especiales, pero se puede configurar para incluir otros procesos.



Procesos habituales del sistema. Funciones y relación entre ellos.



Svchost

Este proceso que encontramos listado varias veces en nuestro administrador de tareas es un parche de Windows para ejecutar archivos dll, ya que no se pueden ejecutar directamente en Windows.

Services.exe

Es el proceso que se encarga de controlar los diferentes servicios de Windows.

System

Proceso vital para el sistema. Su principal labor es mantener la comunicación con el kernel y el hardware del PC. No se puede finalizar desde el administrador de tareas, si aparece la opción se trata de una suplantación de malware.

Winlogon

Este proceso aparece en el administrador de tareas como aplicación de inicio de sesión de Windows. Adicionalmente se ocupa de asociar los diferentes cambios en el sistema a un usuario determinado, así como de generar los avisos de seguridad.

Wininit

Wininit aparece en el Administrador de tareas como Aplicación de inicio de sesión de Windows y es uno de los primeros procesos que se inician durante el arranque del sistema y el último que se para durante el apagado. Se encarga de lanzar otros procesos críticos del sistema y además de comprobar que todos los demás se terminen correctamente en el momento de apagar el equipo.

Lsass.exe

Es el servidor de autenticación local de seguridad.

Genera los procesos responsables de la autenticación de usuarios para el proceso Winlogon. Si la autenticación tiene éxito, lsass.exe genera los tokens de acceso para el usuario que son utilizados para lanzar el shell inicial. Los otros procesos que el usuario inicia heredan estos tokens

Csrss

Client Server Runtime Process es responsable de controlar otros procesos que se ejecutan en segundo plano y de conhost.exe, responsable de la Consola de Windows (CMD). Aparece como Proceso en tiempo de ejecución del cliente-servidor.

Smss

Windows Session Manager es un proceso que se ocupa de crear la memoria virtual, llamar a otros procesos críticos y también a comprobar que arrancan sin errores y que están realizando correctamente sus funciones.

Explorador de Windows

Este proceso se ocupa de gestionar gran parte de la interfaz gráfica de usuario. Es el responsable del menú inicio, la barra de tareas, la bandeja del sistema y también todas las ventanas del propio explorador de archivos. En versiones actuales da la opción de reiniciarlo desde el administrador de tareas.