

# **ASO UT 1. Tarea1. Administrar procesos.**

3/10/2024

Creado por: Pedro José Riquelme Guerrero



---

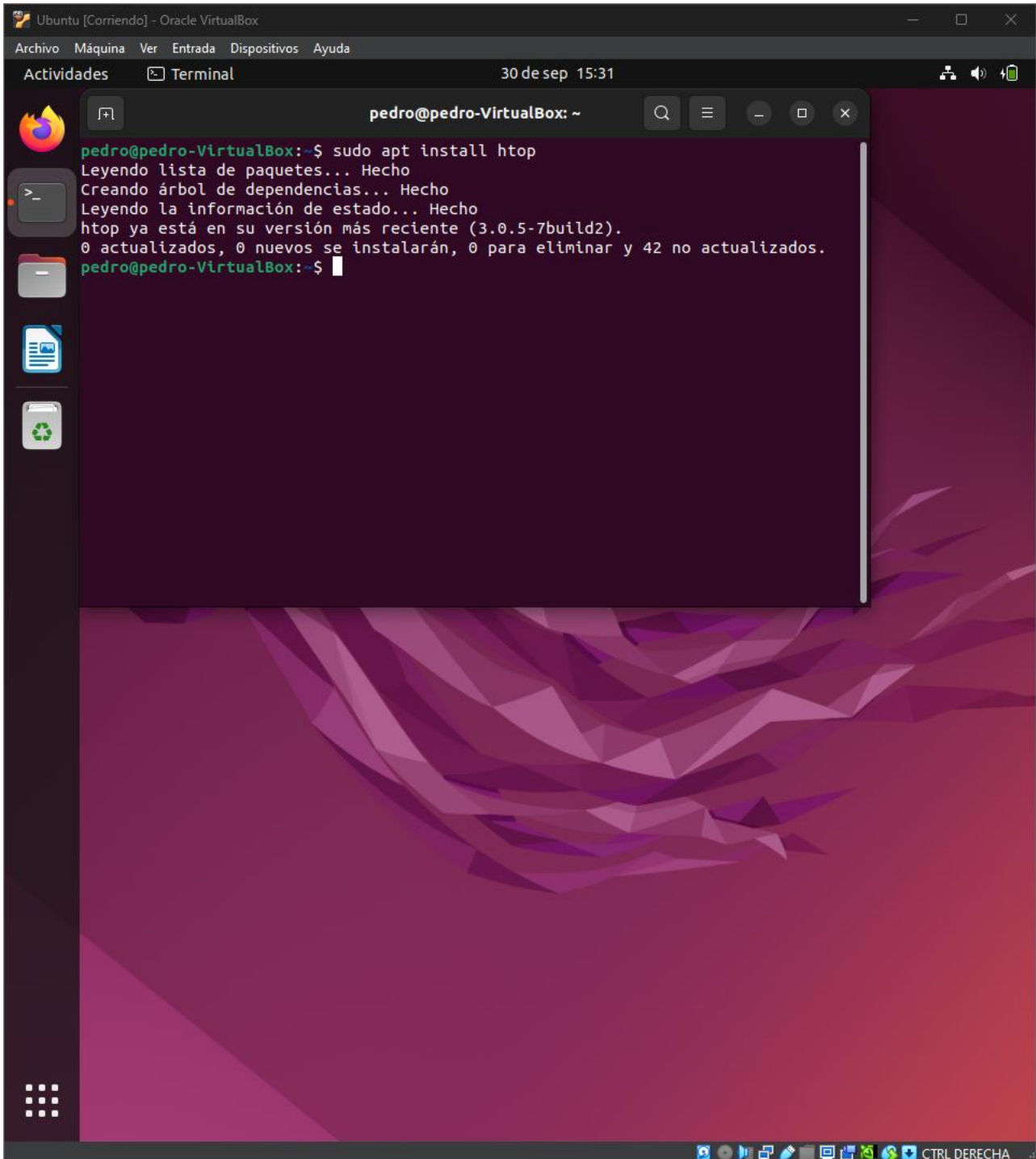
# INDICE

Linux:.....	3
Apartado B.....	9
Apartado C y D .....	11
Windows: .....	12
Apartado A.....	12
Apartado B.....	13
Apartado C:.....	18
Apartado A.....	21
Apartado B.....	23
Apartado C.....	24
Apartado B.....	25
Apartado C:.....	26
Apartado D:.....	28
Apartado B) C) D).....	29
Apartado E) F) .....	32
Apartado E: .....	33
Apartado F: .....	34
Apartado G:.....	35

## Linux:

Lo primero será instalar la herramienta de htop con el siguiente comando:

**“sudo apt install htop”**



The screenshot shows a terminal window titled "pedro@pedro-VirtualBox: ~" within an Ubuntu desktop environment. The terminal output displays the command "sudo apt install htop" and its execution details: "Leyendo lista de paquetes... Hecho", "Creando árbol de dependencias... Hecho", and "Leyendo la información de estado... Hecho". It confirms that htop is already at the latest version (3.0.5-7build2) and that no new packages will be installed. The desktop background is a purple and red geometric pattern, and the system clock shows "30 de sep 15:31".

```
pedro@pedro-VirtualBox:~$ sudo apt install htop
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
htop ya está en su versión más reciente (3.0.5-7build2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 42 no actualizados.
pedro@pedro-VirtualBox:~$
```

```

0[||||| 4.1% Tasks: 116, 276 thr; 1 running
1[||||| 8.4% Load average: 0.14 0.25 0.14
2[||||| 4.7% Uptime: 00:05:34
3[||||| 10.4%
Mem[||||| 893M/4.41G
Swp[||||| 0K/3.18G

  PID USER   PRI  NI  VIRT   RES   SHR  S  CPU% MEM%   TIME+  Command
1777 pedro    20    0 5057M  374M  139M  S  48.9  8.3   0:37.83 /usr/bin/gnome-shell
1795 pedro    20    0 5057M  374M  139M  S  8.4  8.3   0:06.25 /usr/bin/gnome-shell
1934 pedro    20    0  382M  12264  7168  S  0.0  0.3   0:00.24 /usr/bin/ibus-daemon --panel dis
1792 pedro    20    0 5057M  374M  139M  S  10.5  8.3   0:06.01 /usr/bin/gnome-shell
1794 pedro    20    0 5057M  374M  139M  S  7.0  8.3   0:05.95 /usr/bin/gnome-shell
2712 pedro    20    0  547M  55612  42512 S  1.4  1.2   0:00.46 /usr/libexec/gnome-terminal-serv
2730 pedro    20    0  14080  5120  3584  R  0.7  0.1   0:00.20 htop
   1 root     20    0  164M  12884  8148  S  0.0  0.3   0:02.39 /sbin/init splash
 243 root     19   -1 48484  19072  17664 S  0.0  0.4   0:00.76 /lib/systemd/systemd-journald
 296 root     20    0  27060  6912  4608  S  0.0  0.1   0:00.40 /lib/systemd/systemd-udevd
 534 systemd-o 20    0  14836  6784  6016  S  1.4  0.1   0:00.71 /lib/systemd/systemd-oomd
 537 systemd-r 20    0  25540  13624  9472  S  0.0  0.3   0:00.35 /lib/systemd/systemd-resolved
 569 systemd-t 20    0  89388  7296  6528  S  0.0  0.2   0:00.16 /lib/systemd/systemd-timesyncd
 606 systemd-t 20    0  89388  7296  6528  S  0.0  0.2   0:00.00 /lib/systemd/systemd-timesyncd
 627 root     20    0  237M  8004  7108  S  0.0  0.2   0:00.29 /usr/libexec/accounts-daemon
 629 root     20    0  2816  1920  1792  S  0.0  0.0   0:00.05 /usr/sbin/acpid
 631 root     20    0  10992  2560  2432  S  0.0  0.1   0:00.00 /usr/sbin/anacron -d -q -s
 634 avahi     20    0  7632  4096  3712  S  0.0  0.1   0:00.21 avahi-daemon: running [pedro-Vir
 635 root     20    0  12112  2816  2688  S  0.0  0.1   0:00.00 /usr/sbin/cron -f -P
 636 messagebu 20    0  11072  6400  3968  S  0.0  0.1   0:01.49 @dbus-daemon --system --address=
 639 root     20    0  258M  19376  16304 S  0.0  0.4   0:00.88 /usr/sbin/NetworkManager --no-da
 648 root     20    0  82700  3840  3584  S  0.0  0.1   0:00.04 /usr/sbin/irqbalance --foregroun
 649 root     20    0  43660  21120  11776 S  0.0  0.5   0:00.47 /usr/bin/python3 /usr/bin/networ
 651 root     20    0  240M  11652  7996  S  0.0  0.3   0:01.82 /usr/libexec/polkitd --no-debug
 655 root     20    0  237M  7552  7040  S  0.0  0.2   0:00.06 /usr/libexec/power-profiles-daem
 657 syslog    20    0  217M  5888  4480  S  0.0  0.1   0:00.29 /usr/sbin/rsyslogd -n -iNONE
 658 root     20    0  82700  3840  3584  S  0.0  0.1   0:00.00 /usr/sbin/irqbalance --foregroun
 659 root     20    0  240M  11652  7996  S  0.0  0.3   0:00.00 /usr/libexec/polkitd --no-debug
 660 root     20    0  237M  8004  7108  S  0.0  0.2   0:00.06 /usr/libexec/accounts-daemon
 673 root     20    0  237M  7552  7040  S  0.0  0.2   0:00.00 /usr/libexec/power-profiles-daem
 674 root     20    0  1433M  36440  20224 S  0.0  0.8   0:04.42 /usr/lib/snapd/snapd
 679 root     20    0  233M  7040  6400  S  0.0  0.2   0:00.06 /usr/libexec/switcheroo-control
 682 root     20    0  23644  7992  6912  S  0.0  0.2   0:00.46 /lib/systemd/systemd-logind
 684 root     20    0  383M  12780  10348 S  0.0  0.3   0:00.40 /usr/libexec/udisks2/udisksd
 691 root     20    0  16504  6272  5632  S  0.0  0.1   0:00.07 /sbin/wpa_supplicant -u -s -o /r
 697 root     20    0  237M  7552  7040  S  0.0  0.2   0:00.00 /usr/libexec/power-profiles-daem
 698 root     20    0  240M  11652  7996  S  0.0  0.3   0:00.52 /usr/libexec/polkitd --no-debug
 699 root     20    0  383M  12780  10348 S  0.0  0.3   0:00.00 /usr/libexec/udisks2/udisksd
 702 root     20    0  237M  8004  7108  S  0.0  0.2   0:00.02 /usr/libexec/accounts-daemon
 703 avahi     20    0  7444  1408  1152  S  0.0  0.0   0:00.00 avahi-daemon: chroot helper
 704 syslog    20    0  217M  5888  4480  S  0.0  0.1   0:00.12 /usr/sbin/rsyslogd -n -iNONE
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit

```

Una vez instalada y ejecutada la herramienta, podemos observar que es un monitor de procesos más avanzado que el predeterminado del sistema, ya que permite visualizar los núcleos, la memoria de nuestro equipo y el espacio SWP (SWAP), que es el área del disco utilizado cuando la memoria está saturada.

Debajo de esta información, se muestran los procesos, donde el PID (Process ID) es un identificador único asignado a cada proceso en el sistema. La columna "User" indica el usuario al que pertenece el proceso. PRI (Prioridad) es la prioridad asignada a los procesos por el sistema, donde los números más altos indican menor prioridad y los más bajos, incluyendo valores negativos, corresponden a mayor prioridad. También está NI (Nice), que es la prioridad que puede ser modificada por el usuario.

A la derecha, se encuentran los términos VIRT (Virtual memory), RES (Resident memory) y SHR (Shared memory). VIRT es la cantidad de memoria virtual asignada al proceso, mientras que RES representa la memoria física que está utilizando, y SHR es la memoria que comparte con otros procesos.

**S (Status) refleja el estado actual del proceso, con los siguientes posibles estados:**

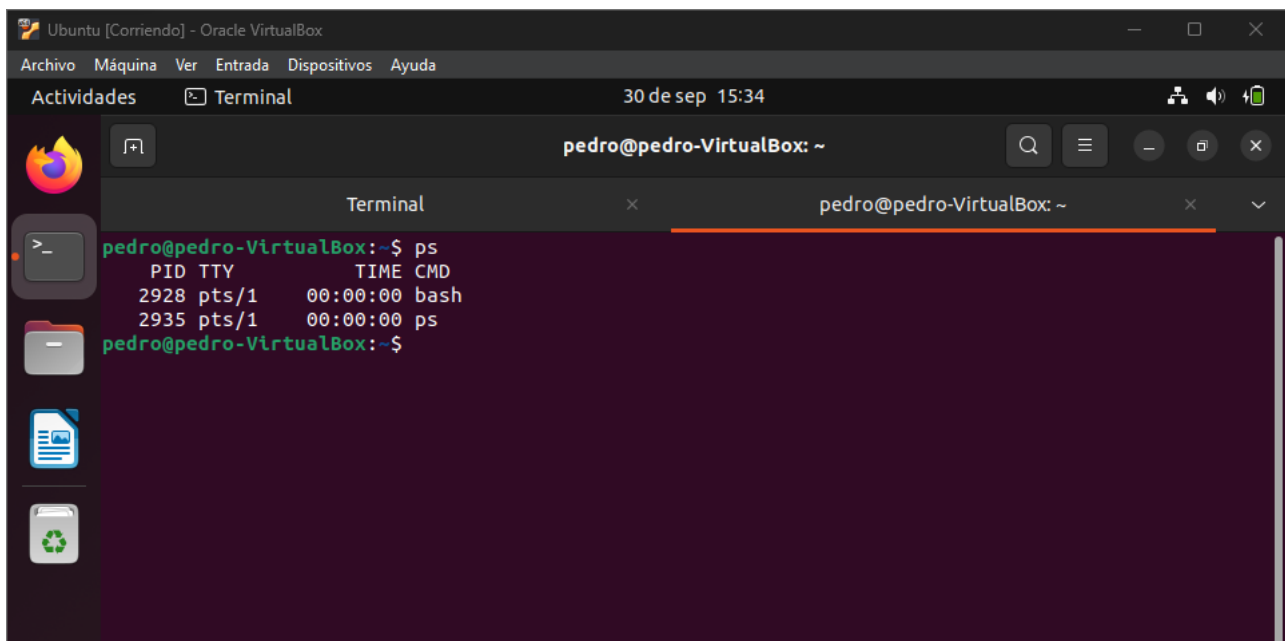
- R: En ejecución (Running).
- S: En espera, aguardando un evento (Sleeping).
- D: En espera ininterrumpible (Uninterruptible Sleep).
- T: Detenido (Stopped).
- Z: Proceso zombie (Zombie).

Las columnas CPU% y MEM% indican el porcentaje de CPU y memoria que está utilizando el proceso, TIME+ muestra la duración del proceso en ejecución, y Command indica el nombre del proceso.

En resumen, htop organiza y presenta la información de manera visual y detallada, ofreciendo opciones adicionales sin necesidad de introducir comandos manuales.

A continuación, compararemos con las herramientas incluidas en el sistema para la gestión de procesos, comenzando con el comando:

**“ps”**

A screenshot of a terminal window titled "Ubuntu [Corriendo] - Oracle VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar is a toolbar with "Actividades" and "Terminal". The terminal itself shows the prompt "pedro@pedro-VirtualBox: ~" and the command "ps" being executed. The output of the command is a table with four columns: "PID", "TTY", "TIME", and "CMD". The table lists two processes: "bash" (PID 2928) and "ps" (PID 2935).

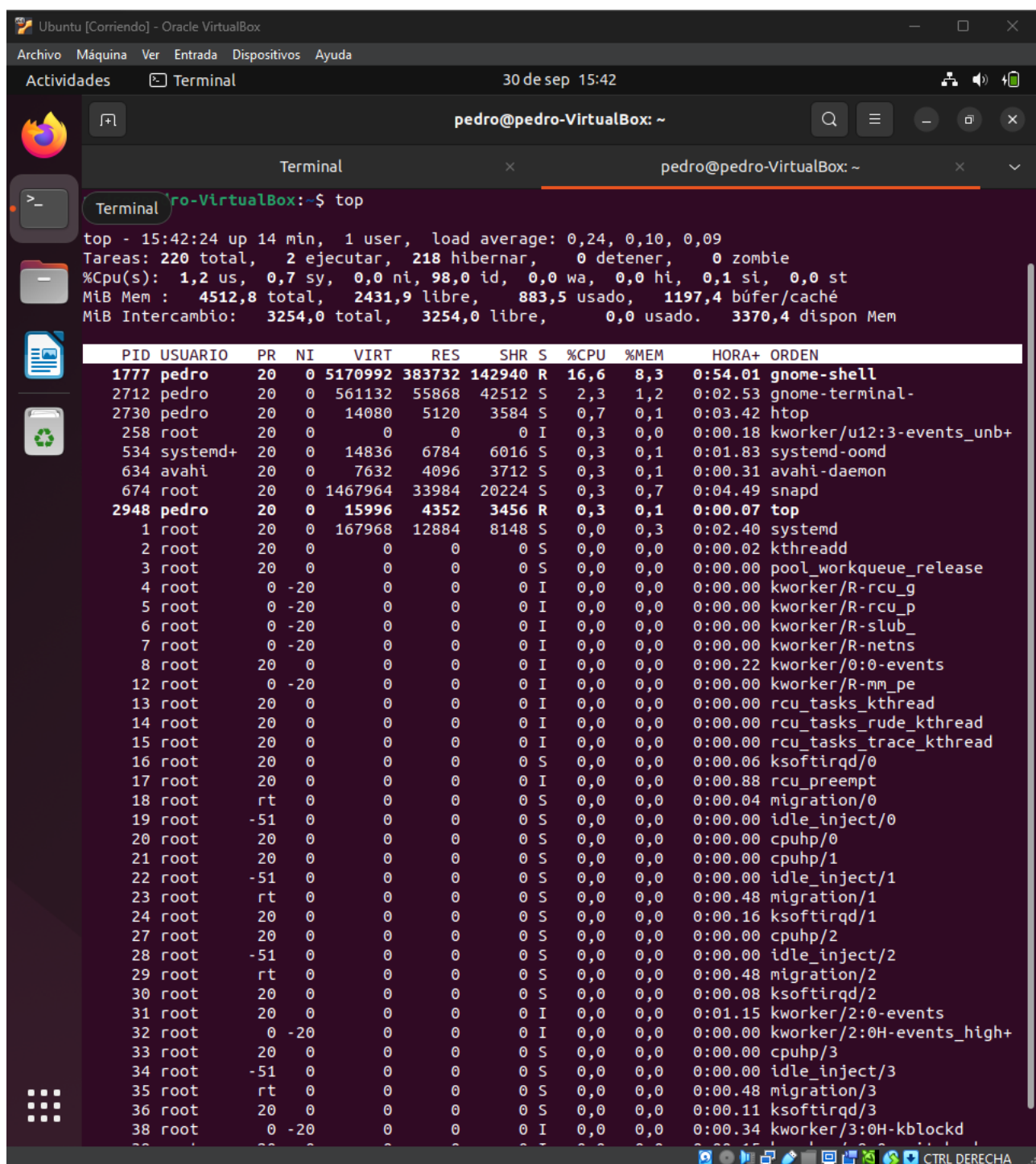
```
pedro@pedro-VirtualBox:~$ ps
  PID TTY          TIME CMD
 2928 pts/1        00:00:00 bash
 2935 pts/1        00:00:00 ps
pedro@pedro-VirtualBox:~$
```



Esta herramienta únicamente muestra los procesos iniciados por el usuario activo. En mi caso, se observan dos consolas: una donde estoy actualizando Linux y otra en la que he ejecutado el comando PS.

El único término adicional que aparece aquí es TTY, que según lo que he investigado, indica si el terminal es físico o virtual. En este caso, es virtual, ya que está abierto en un entorno gráfico.

La segunda herramienta que viene con el sistema es el comando:  
“top”



The screenshot shows a terminal window titled "Terminal" with the prompt "pedro@pedro-VirtualBox: ~". The output of the "top" command is displayed, showing system statistics and a list of running processes. The system statistics include: top - 15:42:24 up 14 min, 1 user, load average: 0,24, 0,10, 0,09; Tareas: 220 total, 2 ejecutar, 218 hibernar, 0 detener, 0 zombie; %Cpu(s): 1,2 us, 0,7 sy, 0,0 ni, 98,0 id, 0,0 wa, 0,0 hi, 0,1 si, 0,0 st; MiB Mem: 4512,8 total, 2431,9 libre, 883,5 usado, 1197,4 búfer/caché; MiB Intercambio: 3254,0 total, 3254,0 libre, 0,0 usado, 3370,4 dispon Mem.

PID	USUARIO	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	HORA+	ORDEN
1777	pedro	20	0	5170992	383732	142940	R	16,6	8,3	0:54.01	gnome-shell
2712	pedro	20	0	561132	55868	42512	S	2,3	1,2	0:02.53	gnome-terminal-
2730	pedro	20	0	14080	5120	3584	S	0,7	0,1	0:03.42	htop
258	root	20	0	0	0	0	I	0,3	0,0	0:00.18	kworker/u12:3-events_unb+
534	systemd+	20	0	14836	6784	6016	S	0,3	0,1	0:01.83	systemd-oomd
634	avahi	20	0	7632	4096	3712	S	0,3	0,1	0:00.31	avahi-daemon
674	root	20	0	1467964	33984	20224	S	0,3	0,7	0:04.49	snappd
2948	pedro	20	0	15996	4352	3456	R	0,3	0,1	0:00.07	top
1	root	20	0	167968	12884	8148	S	0,0	0,3	0:02.40	systemd
2	root	20	0	0	0	0	S	0,0	0,0	0:00.02	kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:00.00	pool_workqueue_release
4	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/R-rcu_g
5	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/R-rcu_p
6	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/R-slub_
7	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/R-netns
8	root	20	0	0	0	0	I	0,0	0,0	0:00.22	kworker/0:0-events
12	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/R-mm_pe
13	root	20	0	0	0	0	I	0,0	0,0	0:00.00	rcu_tasks_kthread
14	root	20	0	0	0	0	I	0,0	0,0	0:00.00	rcu_tasks_rude_kthread
15	root	20	0	0	0	0	I	0,0	0,0	0:00.00	rcu_tasks_trace_kthread
16	root	20	0	0	0	0	S	0,0	0,0	0:00.06	ksoftirqd/0
17	root	20	0	0	0	0	I	0,0	0,0	0:00.88	rcu_preempt
18	root	rt	0	0	0	0	S	0,0	0,0	0:00.04	migration/0
19	root	-51	0	0	0	0	S	0,0	0,0	0:00.00	idle_inject/0
20	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/0
21	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/1
22	root	-51	0	0	0	0	S	0,0	0,0	0:00.00	idle_inject/1
23	root	rt	0	0	0	0	S	0,0	0,0	0:00.48	migration/1
24	root	20	0	0	0	0	S	0,0	0,0	0:00.16	ksoftirqd/1
27	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/2
28	root	-51	0	0	0	0	S	0,0	0,0	0:00.00	idle_inject/2
29	root	rt	0	0	0	0	S	0,0	0,0	0:00.48	migration/2
30	root	20	0	0	0	0	S	0,0	0,0	0:00.08	ksoftirqd/2
31	root	20	0	0	0	0	I	0,0	0,0	0:01.15	kworker/2:0-events
32	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/2:0H-events_high+
33	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/3
34	root	-51	0	0	0	0	S	0,0	0,0	0:00.00	idle_inject/3
35	root	rt	0	0	0	0	S	0,0	0,0	0:00.48	migration/3
36	root	20	0	0	0	0	S	0,0	0,0	0:00.11	ksoftirqd/3
38	root	0	-20	0	0	0	I	0,0	0,0	0:00.34	kworker/3:0H-kblockd

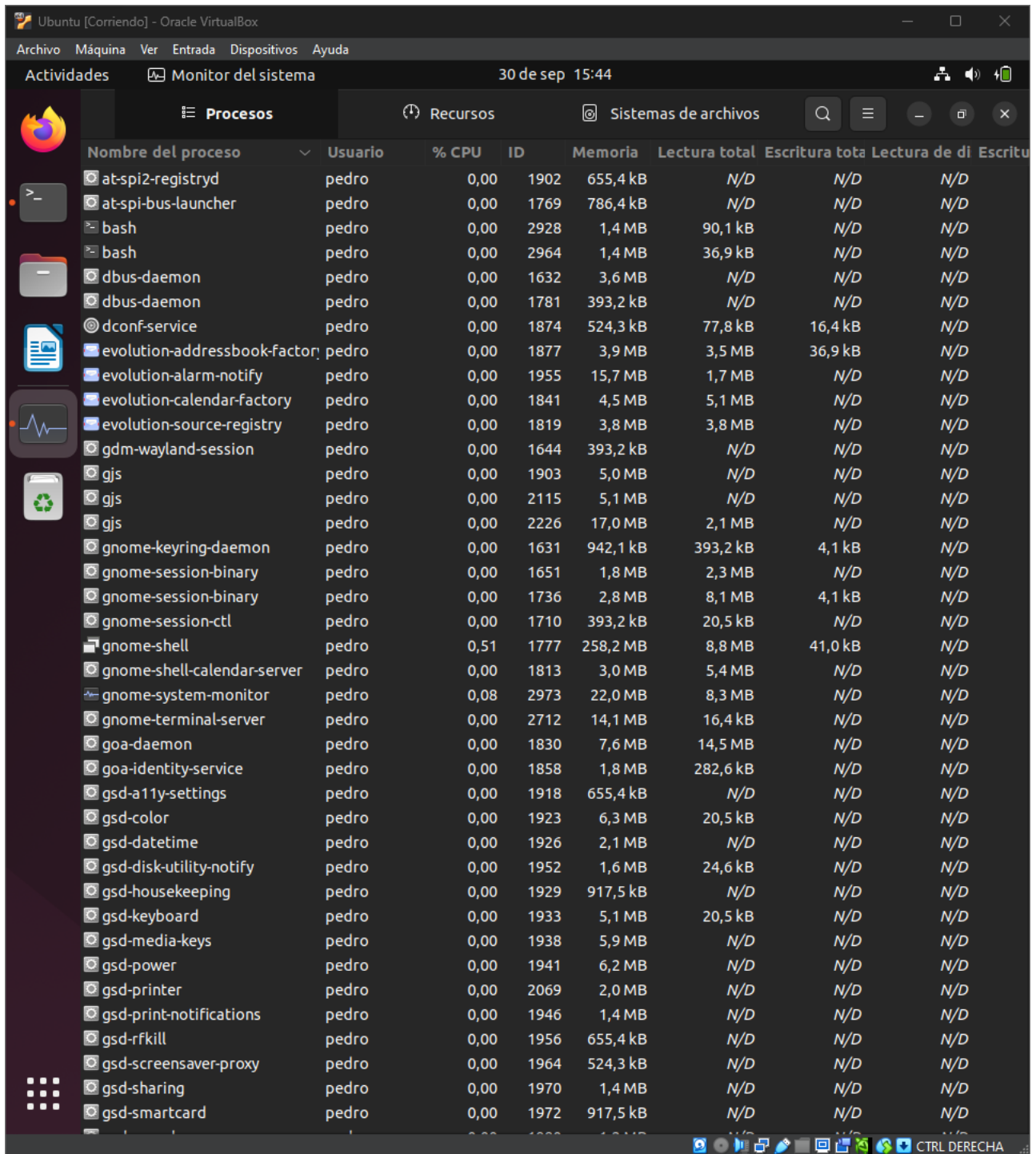
Se parece mucho a la herramienta de htop pero sin la facilidades que nos ofrece como por ejemplo los colores o cambios sin necesidad de usar “comandos”  
El orden podemos observar que es igual que el del htop sin tener los porcentajes usados por cada núcleo y en la memoria que usa en total y sin poder ver como se diferencia por colores.

La tercera herramienta usaremos el comando:  
“pstree”

```
pedro@pedro-VirtualBox:~$ pstree
systemd--ModemManager--2*[{ModemManager}]
systemd--NetworkManager--2*[{NetworkManager}]
systemd--VBoxDRMClient--5*[{VBoxDRMClient}]
systemd--VBoxService--8*[{VBoxService}]
systemd--accounts-daemon--2*[{accounts-daemon}]
systemd--acpid
systemd--avahi-daemon--avahi-daemon
systemd--colord--2*[{colord}]
systemd--cron
systemd--cups-browsed--2*[{cups-browsed}]
systemd--cupsd
systemd--dbus-daemon
systemd--gdm3--gdm-session-wor--gdm-wayland-ses--gnome-session-b--2*[{gnome-session-b}]
systemd--gdm3--gdm-session-wor--gdm-wayland-ses--2*[{gdm-wayland-ses}]
systemd--gdm3--2*[{gdm3}]
systemd--gnome-keyring-d--3*[{gnome-keyring-d}]
systemd--irqbalance--{irqbalance}
systemd--2*[{kerneloops}]
systemd--networkd-dispat
systemd--packagekitd--2*[{packagekitd}]
systemd--polkitd--2*[{polkitd}]
systemd--power-profiles--2*[{power-profiles-}]
systemd--rsyslogd--3*[{rsyslogd}]
systemd--rtkit-daemon--2*[{rtkit-daemon}]
systemd--snapd--10*[{snapd}]
systemd--switcheroo-cont--2*[{switcheroo-cont}]
systemd--(sd-pam)
systemd--VBoxClient--VBoxClient--3*[{VBoxClient}]
systemd--VBoxClient--VBoxClient--2*[{VBoxClient}]
systemd--at-spi2-registr--2*[{at-spi2-registr}]
systemd--dbus-daemon
systemd--dconf-service--2*[{dconf-service}]
systemd--evolution-addre--5*[{evolution-addre}]
systemd--evolution-calen--8*[{evolution-calen}]
systemd--evolution-sourc--3*[{evolution-sourc}]
systemd--2*[{gjs}--6*[{gjs}]]
systemd--gnome-session-b--at-spi-bus-laun--dbus-daemon
systemd--gnome-session-b--at-spi-bus-laun--3*[{at-spi-bus-laun}]
systemd--gnome-session-b--at-spi-bus-laun--evolution-alarm--5*[{evolution-alarm}]
systemd--gnome-session-b--at-spi-bus-laun--gsd-disk-utilit--2*[{gsd-disk-utilit}]
systemd--gnome-session-b--at-spi-bus-laun--update-notifier--3*[{update-notifier}]
systemd--gnome-session-b--at-spi-bus-laun--3*[{gnome-session-b}]
systemd--gnome-session-c--{gnome-session-c}
systemd--gnome-shell--Xwayland
systemd--gnome-shell--gjs--7*[{gjs}]
systemd--gnome-shell--18*[{gnome-shell}]
systemd--gnome-shell-cal--5*[{gnome-shell-cal}]
```

Con esta herramienta nos enseña los procesos como si fuera un árbol jerárquico donde se pude ver cuál es la raíz principal.

Por último, con el monitor de sistema que nos ofrece Ubuntu predeterminado sin tener que instalar nada:



Ubuntu [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Monitor del sistema 30 de sep 15:44

Procesos Recursos Sistemas de archivos

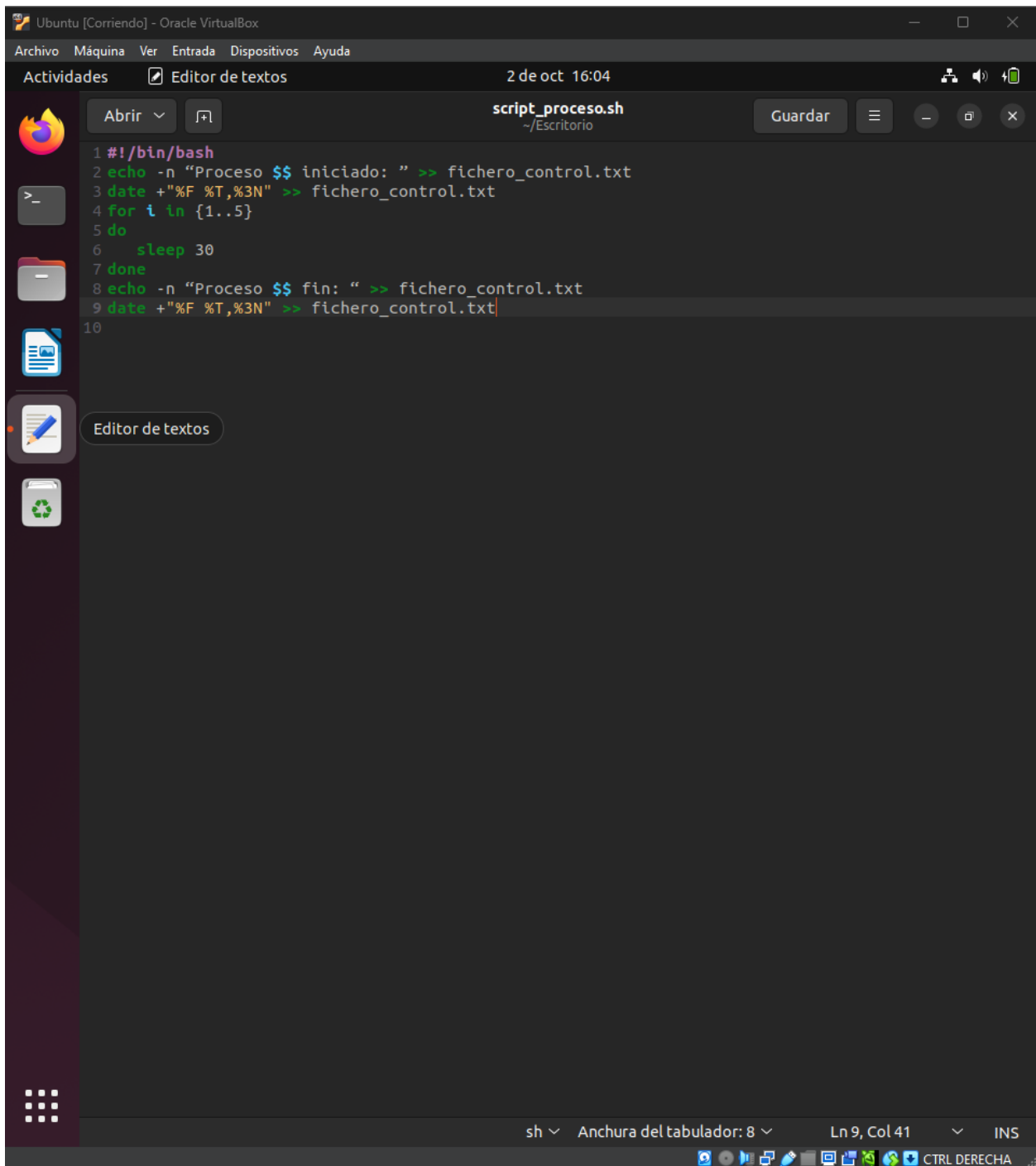
Nombre del proceso	Usuario	% CPU	ID	Memoria	Lectura total	Escritura total	Lectura de di	Escritu
at-spi2-registryd	pedro	0,00	1902	655,4 kB	N/D	N/D	N/D	
at-spi-bus-launcher	pedro	0,00	1769	786,4 kB	N/D	N/D	N/D	
bash	pedro	0,00	2928	1,4 MB	90,1 kB	N/D	N/D	
bash	pedro	0,00	2964	1,4 MB	36,9 kB	N/D	N/D	
dbus-daemon	pedro	0,00	1632	3,6 MB	N/D	N/D	N/D	
dbus-daemon	pedro	0,00	1781	393,2 kB	N/D	N/D	N/D	
dconf-service	pedro	0,00	1874	524,3 kB	77,8 kB	16,4 kB	N/D	
evolution-addressbook-factor	pedro	0,00	1877	3,9 MB	3,5 MB	36,9 kB	N/D	
evolution-alarm-notify	pedro	0,00	1955	15,7 MB	1,7 MB	N/D	N/D	
evolution-calendar-factory	pedro	0,00	1841	4,5 MB	5,1 MB	N/D	N/D	
evolution-source-registry	pedro	0,00	1819	3,8 MB	3,8 MB	N/D	N/D	
gdm-wayland-session	pedro	0,00	1644	393,2 kB	N/D	N/D	N/D	
gjs	pedro	0,00	1903	5,0 MB	N/D	N/D	N/D	
gjs	pedro	0,00	2115	5,1 MB	N/D	N/D	N/D	
gjs	pedro	0,00	2226	17,0 MB	2,1 MB	N/D	N/D	
gnome-keyring-daemon	pedro	0,00	1631	942,1 kB	393,2 kB	4,1 kB	N/D	
gnome-session-binary	pedro	0,00	1651	1,8 MB	2,3 MB	N/D	N/D	
gnome-session-binary	pedro	0,00	1736	2,8 MB	8,1 MB	4,1 kB	N/D	
gnome-session-ctl	pedro	0,00	1710	393,2 kB	20,5 kB	N/D	N/D	
gnome-shell	pedro	0,51	1777	258,2 MB	8,8 MB	41,0 kB	N/D	
gnome-shell-calendar-server	pedro	0,00	1813	3,0 MB	5,4 MB	N/D	N/D	
gnome-system-monitor	pedro	0,08	2973	22,0 MB	8,3 MB	N/D	N/D	
gnome-terminal-server	pedro	0,00	2712	14,1 MB	16,4 kB	N/D	N/D	
goa-daemon	pedro	0,00	1830	7,6 MB	14,5 MB	N/D	N/D	
goa-identity-service	pedro	0,00	1858	1,8 MB	282,6 kB	N/D	N/D	
gsd-a11y-settings	pedro	0,00	1918	655,4 kB	N/D	N/D	N/D	
gsd-color	pedro	0,00	1923	6,3 MB	20,5 kB	N/D	N/D	
gsd-datetime	pedro	0,00	1926	2,1 MB	N/D	N/D	N/D	
gsd-disk-utility-notify	pedro	0,00	1952	1,6 MB	24,6 kB	N/D	N/D	
gsd-housekeeping	pedro	0,00	1929	917,5 kB	N/D	N/D	N/D	
gsd-keyboard	pedro	0,00	1933	5,1 MB	20,5 kB	N/D	N/D	
gsd-media-keys	pedro	0,00	1938	5,9 MB	N/D	N/D	N/D	
gsd-power	pedro	0,00	1941	6,2 MB	N/D	N/D	N/D	
gsd-printer	pedro	0,00	2069	2,0 MB	N/D	N/D	N/D	
gsd-print-notifications	pedro	0,00	1946	1,4 MB	N/D	N/D	N/D	
gsd-rfkill	pedro	0,00	1956	655,4 kB	N/D	N/D	N/D	
gsd-screensaver-proxy	pedro	0,00	1964	524,3 kB	N/D	N/D	N/D	
gsd-sharing	pedro	0,00	1970	1,4 MB	N/D	N/D	N/D	
gsd-smartcard	pedro	0,00	1972	917,5 kB	N/D	N/D	N/D	

Como podemos observar si nos damos cuenta se parece mucho a el administrador de tareas de Windows, completo y con interfaz gráfica. Las opciones que nos da son, matar procesos, cambiar de prioridad, etc. Y todo eso sin necesidad de comandos y solo usando un ratón.



## Apartado B

Para crear el script podemos abrir el editor de textos y poner el siguiente script:



The screenshot shows a text editor window titled 'script\_proceso.sh' in a virtual machine environment. The script content is as follows:

```
1 #!/bin/bash
2 echo -n "Proceso $$ iniciado: " >> fichero_control.txt
3 date +%F %T,%3N >> fichero_control.txt
4 for i in {1..5}
5 do
6     sleep 30
7 done
8 echo -n "Proceso $$ fin: " >> fichero_control.txt
9 date +%F %T,%3N >> fichero_control.txt
10
```

The editor interface includes a menu bar with 'Archivo', 'Máquina', 'Ver', 'Entrada', 'Dispositivos', and 'Ayuda'. The status bar at the bottom indicates 'sh', 'Anchura del tabulador: 8', 'Ln 9, Col 41', and 'INS'.

Al intentar ejecutar el script, la consola me devuelve "permiso denegado", y al intentar hacerlo como superusuario tampoco funciona. Esto se debe a que el script no tiene permisos de ejecución. Para verificarlo, utilizamos el comando ``ls -l nombrescript.sh``, que muestra ``-rw-rw-r--``, lo que indica la falta de permisos de ejecución.

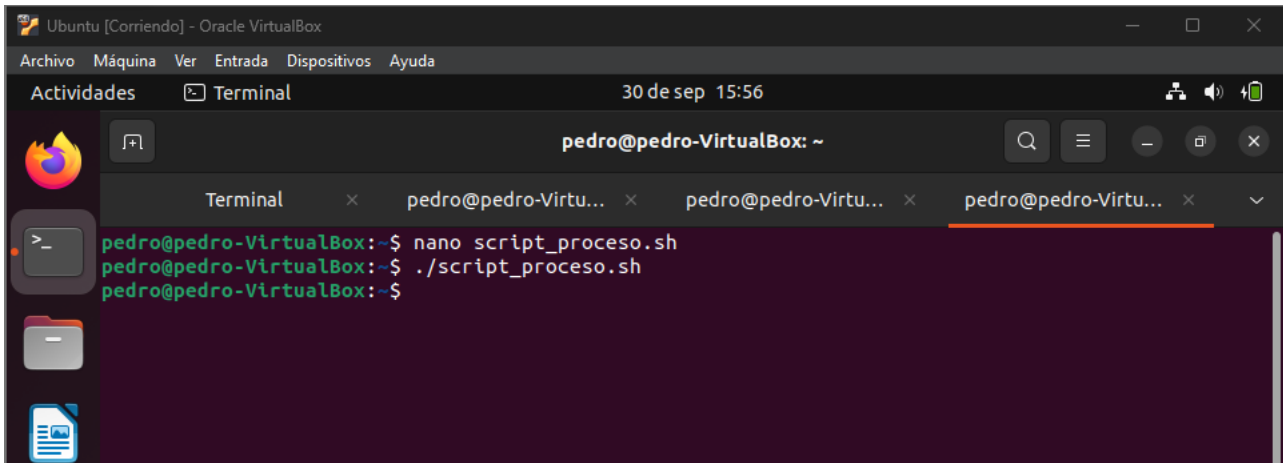
Para corregirlo, utilizamos el comando `chmod +x script\_proceso.sh` para otorgar los permisos necesarios. Al verificar nuevamente los permisos del archivo, confirmamos que ya es ejecutable.

Finalmente, ejecutamos el script con `./script\_proceso.sh` en la consola.

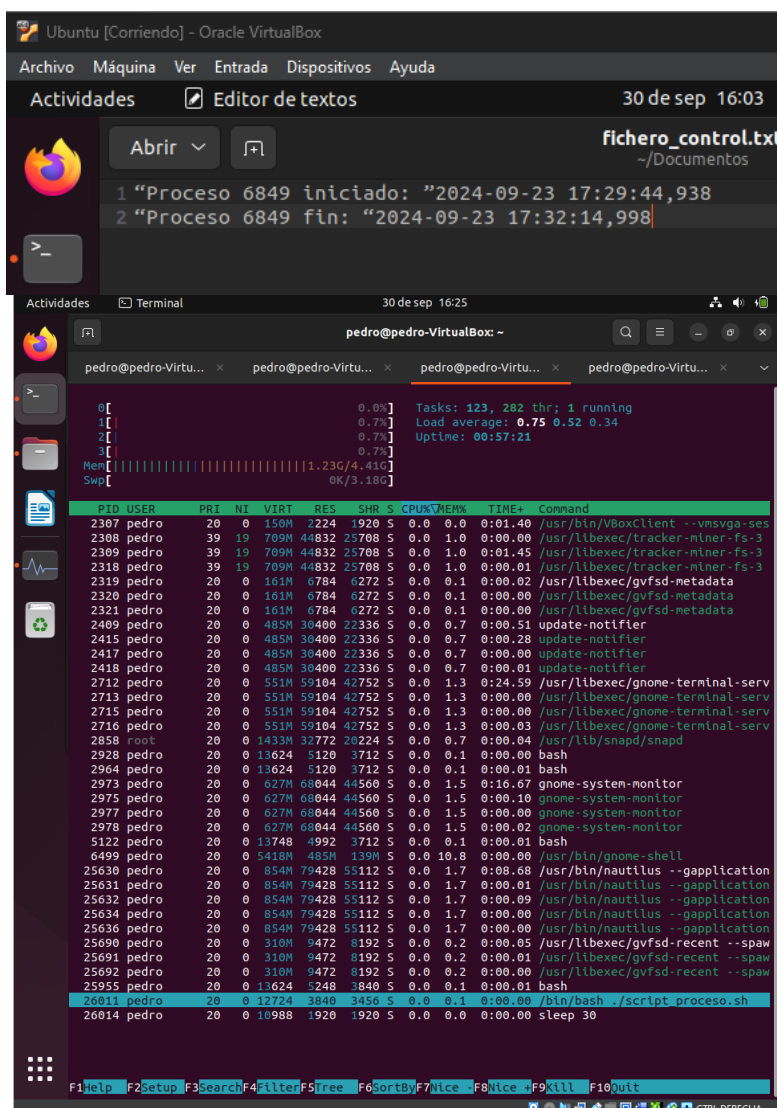
Al ejecutar se nos creara un archivo llamado `fichero_control.txt`, en mi caso contiene

"Proceso 6849 iniciado: "2024-09-23 17:29:44,938

"Proceso 6849 fin: "2024-09-23 17:32:14,998



```
Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de sep 15:56
pedro@pedro-VirtualBox: ~
Terminal x pedro@pedro-Virtu... x pedro@pedro-Virtu... x pedro@pedro-Virtu... x
pedro@pedro-VirtualBox:~$ nano script_proceso.sh
pedro@pedro-VirtualBox:~$ ./script_proceso.sh
pedro@pedro-VirtualBox:~$
```



```
Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Editor de textos 30 de sep 16:03
fichero_control.txt
~/Documentos
1 "Proceso 6849 iniciado: "2024-09-23 17:29:44,938
2 "Proceso 6849 fin: "2024-09-23 17:32:14,998

Actividades Terminal 30 de sep 16:25
pedro@pedro-VirtualBox: ~
pedro@pedro-Virtu... x pedro@pedro-Virtu... x pedro@pedro-Virtu... x pedro@pedro-Virtu... x
Tasks: 123, 282 thr: 1 running
Load average: 0.75 0.52 0.34
Uptime: 00:57:21
Mem[|||||] 1.23G/4.41G
Swp[ ] 0K/3.18G

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
2387 pedro 20 0 158M 2224 1920 S 0.0 0.0 0:01.40 /usr/bin/VBoxClient --vmsvga-se
2388 pedro 39 19 709M 44832 25708 S 0.0 1.0 0:00.00 /usr/libexec/tracker-miner-fs-3
2389 pedro 39 19 709M 44832 25708 S 0.0 1.0 0:01.45 /usr/libexec/tracker-miner-fs-3
2318 pedro 39 19 709M 44832 25708 S 0.0 1.0 0:00.01 /usr/libexec/tracker-miner-fs-3
2319 pedro 20 0 161M 6784 6272 S 0.0 0.1 0:00.02 /usr/libexec/gvfsd-metadata
2320 pedro 20 0 161M 6784 6272 S 0.0 0.1 0:00.00 /usr/libexec/gvfsd-metadata
2321 pedro 20 0 161M 6784 6272 S 0.0 0.1 0:00.00 /usr/libexec/gvfsd-metadata
2409 pedro 20 0 485M 30400 22336 S 0.0 0.7 0:00.51 update-notifier
2415 pedro 20 0 485M 30400 22336 S 0.0 0.7 0:00.28 update-notifier
2417 pedro 20 0 485M 30400 22336 S 0.0 0.7 0:00.00 update-notifier
2418 pedro 20 0 485M 30400 22336 S 0.0 0.7 0:00.01 update-notifier
2712 pedro 20 0 551M 59104 42752 S 0.0 1.3 0:24.59 /usr/libexec/gnome-terminal-serv
2713 pedro 20 0 551M 59104 42752 S 0.0 1.3 0:00.00 /usr/libexec/gnome-terminal-serv
2715 pedro 20 0 551M 59104 42752 S 0.0 1.3 0:00.00 /usr/libexec/gnome-terminal-serv
2716 pedro 20 0 551M 59104 42752 S 0.0 1.3 0:00.03 /usr/libexec/gnome-terminal-serv
2858 root 20 0 1433M 32772 20224 S 0.0 0.7 0:00.04 /usr/lib/snapd/snapd
2928 pedro 20 0 13624 5120 3712 S 0.0 0.1 0:00.00 bash
2964 pedro 20 0 13624 5120 3712 S 0.0 0.1 0:00.01 bash
2973 pedro 20 0 627M 68044 44560 S 0.0 1.5 0:16.67 gnome-system-monitor
2975 pedro 20 0 627M 68044 44560 S 0.0 1.5 0:00.10 gnome-system-monitor
2977 pedro 20 0 627M 68044 44560 S 0.0 1.5 0:00.00 gnome-system-monitor
2978 pedro 20 0 627M 68044 44560 S 0.0 1.5 0:00.02 gnome-system-monitor
5122 pedro 20 0 13748 4992 3712 S 0.0 0.1 0:00.01 bash
6499 pedro 20 0 5418M 485M 139M S 0.0 10.8 0:00.00 /usr/bin/gnome-shell
25630 pedro 20 0 854M 79428 55112 S 0.0 1.7 0:00.68 /usr/bin/nautilus --gapplication
25631 pedro 20 0 854M 79428 55112 S 0.0 1.7 0:00.01 /usr/bin/nautilus --gapplication
25632 pedro 20 0 854M 79428 55112 S 0.0 1.7 0:00.09 /usr/bin/nautilus --gapplication
25634 pedro 20 0 854M 79428 55112 S 0.0 1.7 0:00.00 /usr/bin/nautilus --gapplication
25636 pedro 20 0 854M 79428 55112 S 0.0 1.7 0:00.00 /usr/bin/nautilus --gapplication
25690 pedro 20 0 310M 9472 8192 S 0.0 0.2 0:00.05 /usr/libexec/gvfsd-recent --spaw
25691 pedro 20 0 310M 9472 8192 S 0.0 0.2 0:00.01 /usr/libexec/gvfsd-recent --spaw
25692 pedro 20 0 310M 9472 8192 S 0.0 0.2 0:00.00 /usr/libexec/gvfsd-recent --spaw
25955 pedro 20 0 13624 5248 3840 S 0.0 0.1 0:00.01 bash
26011 pedro 20 0 12724 3840 3456 S 0.0 0.1 0:00.00 /bin/bash ./script_proceso.sh
26014 pedro 20 0 10988 1920 1920 S 0.0 0.0 0:00.00 sleep 30

F1 Help F2 Setup F3 Search F4 Filter F5 Tree F6 Sort By F7 Nice F8 Nice F9 Kill F10 Quit
CTRL DERECHA
```

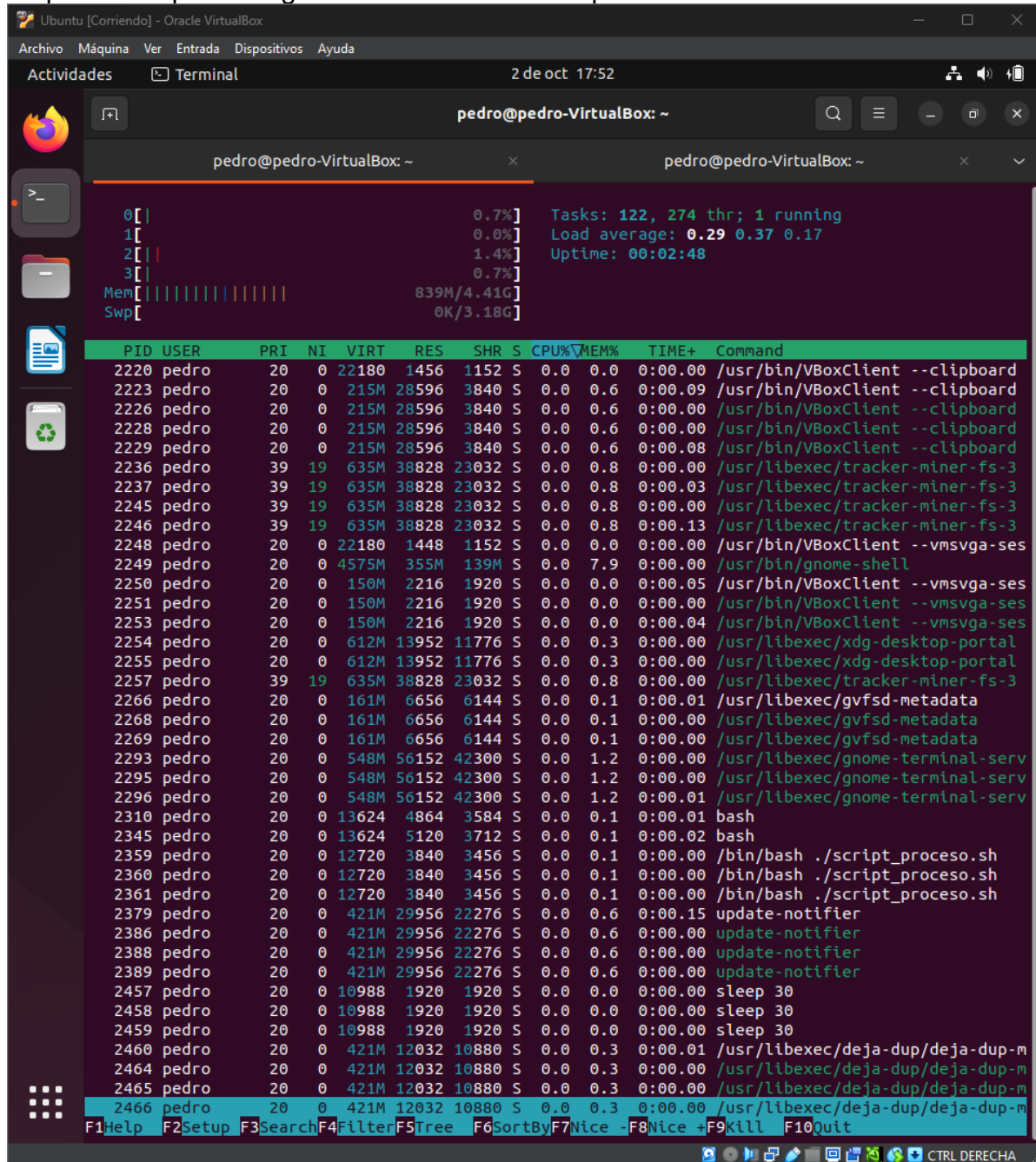
## Apartado C y D

En htop vemos el proceso abierto por el comando al abrir varios al mismo tiempo vemos que abre el mismo proceso tres veces cada uno con un id propio.

Para lanzar el proceso varias veces lo haremos de la siguiente manera:

**“./script\_proceso.sh & ./script\_proceso.sh & ./script\_proceso.sh &”**

La prioridad que le asigna el sistema a nuestro proceso es de 20.



```
0[ ] 0.7%] Tasks: 122, 274 thr; 1 running
1[ ] 0.0%] Load average: 0.29 0.37 0.17
2[ ] 1.4%] Uptime: 00:02:48
3[ ] 0.7%]
Mem[ ] 839M/4.41G
Swp[ ] 0K/3.18G
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
2220	pedro	20	0	22180	1456	1152	S	0.0	0.0	0:00.00	/usr/bin/VBoxClient --clipboard
2223	pedro	20	0	215M	28596	3840	S	0.0	0.6	0:00.09	/usr/bin/VBoxClient --clipboard
2226	pedro	20	0	215M	28596	3840	S	0.0	0.6	0:00.00	/usr/bin/VBoxClient --clipboard
2228	pedro	20	0	215M	28596	3840	S	0.0	0.6	0:00.00	/usr/bin/VBoxClient --clipboard
2229	pedro	20	0	215M	28596	3840	S	0.0	0.6	0:00.08	/usr/bin/VBoxClient --clipboard
2236	pedro	39	19	635M	38828	23032	S	0.0	0.8	0:00.00	/usr/libexec/tracker-miner-fs-3
2237	pedro	39	19	635M	38828	23032	S	0.0	0.8	0:00.03	/usr/libexec/tracker-miner-fs-3
2245	pedro	39	19	635M	38828	23032	S	0.0	0.8	0:00.00	/usr/libexec/tracker-miner-fs-3
2246	pedro	39	19	635M	38828	23032	S	0.0	0.8	0:00.13	/usr/libexec/tracker-miner-fs-3
2248	pedro	20	0	22180	1448	1152	S	0.0	0.0	0:00.00	/usr/bin/VBoxClient --vmsvga-ses
2249	pedro	20	0	4575M	355M	139M	S	0.0	7.9	0:00.00	/usr/bin/gnome-shell
2250	pedro	20	0	150M	2216	1920	S	0.0	0.0	0:00.05	/usr/bin/VBoxClient --vmsvga-ses
2251	pedro	20	0	150M	2216	1920	S	0.0	0.0	0:00.00	/usr/bin/VBoxClient --vmsvga-ses
2253	pedro	20	0	150M	2216	1920	S	0.0	0.0	0:00.04	/usr/bin/VBoxClient --vmsvga-ses
2254	pedro	20	0	612M	13952	11776	S	0.0	0.3	0:00.00	/usr/libexec/xdg-desktop-portal
2255	pedro	20	0	612M	13952	11776	S	0.0	0.3	0:00.00	/usr/libexec/xdg-desktop-portal
2257	pedro	39	19	635M	38828	23032	S	0.0	0.8	0:00.00	/usr/libexec/tracker-miner-fs-3
2266	pedro	20	0	161M	6656	6144	S	0.0	0.1	0:00.01	/usr/libexec/gvfsd-metadata
2268	pedro	20	0	161M	6656	6144	S	0.0	0.1	0:00.00	/usr/libexec/gvfsd-metadata
2269	pedro	20	0	161M	6656	6144	S	0.0	0.1	0:00.00	/usr/libexec/gvfsd-metadata
2293	pedro	20	0	548M	56152	42300	S	0.0	1.2	0:00.00	/usr/libexec/gnome-terminal-serv
2295	pedro	20	0	548M	56152	42300	S	0.0	1.2	0:00.00	/usr/libexec/gnome-terminal-serv
2296	pedro	20	0	548M	56152	42300	S	0.0	1.2	0:00.01	/usr/libexec/gnome-terminal-serv
2310	pedro	20	0	13624	4864	3584	S	0.0	0.1	0:00.01	bash
2345	pedro	20	0	13624	5120	3712	S	0.0	0.1	0:00.02	bash
2359	pedro	20	0	12720	3840	3456	S	0.0	0.1	0:00.00	/bin/bash ./script_proceso.sh
2360	pedro	20	0	12720	3840	3456	S	0.0	0.1	0:00.00	/bin/bash ./script_proceso.sh
2361	pedro	20	0	12720	3840	3456	S	0.0	0.1	0:00.00	/bin/bash ./script_proceso.sh
2379	pedro	20	0	421M	29956	22276	S	0.0	0.6	0:00.15	update-notifier
2386	pedro	20	0	421M	29956	22276	S	0.0	0.6	0:00.00	update-notifier
2388	pedro	20	0	421M	29956	22276	S	0.0	0.6	0:00.00	update-notifier
2389	pedro	20	0	421M	29956	22276	S	0.0	0.6	0:00.00	update-notifier
2457	pedro	20	0	10988	1920	1920	S	0.0	0.0	0:00.00	sleep 30
2458	pedro	20	0	10988	1920	1920	S	0.0	0.0	0:00.00	sleep 30
2459	pedro	20	0	10988	1920	1920	S	0.0	0.0	0:00.00	sleep 30
2460	pedro	20	0	421M	12032	10880	S	0.0	0.3	0:00.01	/usr/libexec/deja-dup/deja-dup-m
2464	pedro	20	0	421M	12032	10880	S	0.0	0.3	0:00.00	/usr/libexec/deja-dup/deja-dup-m
2465	pedro	20	0	421M	12032	10880	S	0.0	0.3	0:00.00	/usr/libexec/deja-dup/deja-dup-m
2466	pedro	20	0	421M	12032	10880	S	0.0	0.3	0:00.00	/usr/libexec/deja-dup/deja-dup-m

```
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice +F9Kill F10Quit
```

## Windows:

### Apartado A

Cuando nos metemos a el administrador de tareas de Windows nos vamos a el apartado de detalles y hacemos click derecho sobre el nombre de la columna y filtramos por prioridad de base.

The screenshot shows the Windows Task Manager application in the 'Detalles' (Details) tab. A right-click context menu is open over the 'Nombre' (Name) column header. The menu options include 'Memoria (espacio de trabajo privado activo)', 'Memoria (espacio de trabajo privado)', 'Memoria (espacio de trabajo compartido)', 'Tamaño de asignación', 'Bloque paginado', 'Bloque no paginado', 'Errores de página', 'Diferencia de errores de página', 'Prioridad base' (which is selected), 'Identificadores', and 'Subprocesos'. The task list below shows various system processes, including ApplicationFrameHost.exe, csrss.exe, explorer.exe, and svchost.exe. The taskbar at the bottom shows the date 30/09/2024 and the time 16:57.

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
ApplicationFrameHo...	1704	En ejecución	Pedro José...	00	6.300 K	Deshabilitada
audiodg.exe			SERVICIO ...	00	3.736 K	No permitida
BraveCrash			SYSTEM	00	276 K	No permitida
BraveCrash			SYSTEM	00	408 K	No permitida
csrss.exe			SYSTEM	00	916 K	No permitida
csrss.exe			SYSTEM	00	860 K	No permitida
ctfmon.exe			Pedro José...	00	3.412 K	Deshabilitada
dasHost.exe			SERVICIO ...	00	2.908 K	No permitida
dllhost.exe			Pedro José...	00	3.168 K	Deshabilitada
dwm.exe			DWM-1	00	33.600 K	Deshabilitada
explorer.exe			Pedro José...	00	29.428 K	Deshabilitada
fontdrvhost			UMFD-0	00	932 K	Deshabilitada
Interrupcio			SYSTEM	00	0 K	
lsass.exe			SYSTEM	00	5.492 K	No permitida
MicrosoftEn			SYSTEM	00	520 K	No permitida
MsMpEng			SYSTEM	00	96.664 K	No permitida
NisSrv.exe			SERVICIO ...	00	2.324 K	No permitida
OneDrive.e			Pedro José...	00	36.960 K	Deshabilitada
Proceso inactivo del ...	0	En ejecución	SYSTEM	99	8 K	
Registry	156	En ejecución	SYSTEM	00	5.248 K	No permitida
RuntimeBroker.exe	1944	En ejecución	Pedro José...	00	2.140 K	Deshabilitada
RuntimeBroker.exe	6848	En ejecución	Pedro José...	00	3.056 K	Deshabilitada
RuntimeBroker.exe	7248	En ejecución	Pedro José...	00	7.316 K	Deshabilitada
RuntimeBroker.exe	7544	En ejecución	Pedro José...	00	1.456 K	Deshabilitada
RuntimeBroker.exe	7800	En ejecución	Pedro José...	00	1.428 K	Deshabilitada
RuntimeBroker.exe	10112	En ejecución	Pedro José...	00	1.736 K	Deshabilitada
SearchApp.exe	7000	Suspendido	Pedro José...	00	0 K	Deshabilitada
SearchIndexer.exe	5264	En ejecución	SYSTEM	00	12.548 K	No permitida
SecurityHealthServic...	8300	En ejecución	SYSTEM	00	2.224 K	No permitida
SecurityHealthSysra...	8260	En ejecución	Pedro José...	00	980 K	Deshabilitada
services.exe	768	En ejecución	SYSTEM	00	4.148 K	No permitida
SgrmBroker.exe	7584	En ejecución	SYSTEM	00	3.872 K	No permitida
sihost.exe	5820	En ejecución	Pedro José...	00	4.304 K	Deshabilitada
SkypeApp.exe	3120	Suspendido	Pedro José...	00	0 K	Deshabilitada
smartscreen.exe	6676	En ejecución	Pedro José...	00	9.856 K	Deshabilitada
smss.exe	440	En ejecución	SYSTEM	00	264 K	No permitida
spoolsv.exe	3032	En ejecución	SYSTEM	00	4.140 K	No permitida
StartMenuExperienc...	6152	En ejecución	Pedro José...	00	21.884 K	Deshabilitada
svchost.exe	904	En ejecución	SYSTEM	00	8.816 K	No permitida
svchost.exe	96	En ejecución	Servicio de...	00	6.940 K	No permitida
svchost.exe	572	En ejecución	SYSTEM	00	1.416 K	No permitida
svchost.exe	1036	En ejecución	SYSTEM	00	960 K	No permitida
svchost.exe	1092	En ejecución	SERVICIO ...	00	852 K	No permitida

## Apartado B

El comando **Tasklist** es un comando que es similar a el comando **Top** en Linux, tasklist muestra lo siguiente:

```
Windows [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
C:\Users\Pedro José Riquelme>tasklist

Nombre de imagen          PID Nombre de sesión Núm. de ses Uso de memor
-----
System Idle Process       0 Services          0          8 KB
System                    4 Services          0        152 KB
Registry                 156 Services        0       72.692 KB
smss.exe                 440 Services        0        1.224 KB
csrss.exe                548 Services        0        5.660 KB
wininit.exe              624 Services        0        7.332 KB
csrss.exe                632 Console         1        5.576 KB
winlogon.exe             696 Console         1       12.172 KB
services.exe             768 Services        0       10.328 KB
lsass.exe                788 Services        0       20.436 KB
svchost.exe              904 Services        0       32.508 KB
fontdrvhost.exe          928 Services        0        3.480 KB
fontdrvhost.exe          936 Console         1        4.716 KB
svchost.exe              96 Services         0       15.900 KB
svchost.exe              572 Services        0        7.920 KB
dwm.exe                  764 Console         1       72.320 KB
svchost.exe             1036 Services        0        8.064 KB
svchost.exe             1092 Services        0        5.676 KB
svchost.exe             1100 Services        0       10.460 KB
svchost.exe             1112 Services        0       12.412 KB
svchost.exe             1288 Services        0       18.672 KB
svchost.exe             1308 Services        0       15.528 KB
svchost.exe             1380 Services        0       19.892 KB
svchost.exe             1420 Services        0        6.360 KB
svchost.exe             1512 Services        0       20.684 KB
svchost.exe             1560 Services        0        8.720 KB
svchost.exe             1600 Services        0        7.928 KB
VBoxService.exe         1732 Services        0        7.292 KB
svchost.exe             1752 Services        0       11.668 KB
svchost.exe             1836 Services        0       56.376 KB
svchost.exe             1848 Services        0        8.020 KB
svchost.exe             1872 Services        0        6.148 KB
svchost.exe             1972 Services        0       10.040 KB
svchost.exe             2028 Services        0        8.404 KB
Memory Compression       1236 Services        0        3.228 KB
svchost.exe             1740 Services        0        8.192 KB
svchost.exe             1856 Services        0        7.812 KB
svchost.exe             2072 Services        0        7.568 KB
svchost.exe             2188 Services        0        7.664 KB
svchost.exe             2268 Services        0        8.192 KB
svchost.exe             2312 Services        0        9.848 KB
svchost.exe             2576 Services        0       18.236 KB
svchost.exe             2596 Services        0       13.176 KB
svchost.exe             2656 Services        0        7.612 KB
svchost.exe             2828 Services        0        6.800 KB
svchost.exe             2836 Services        0       10.316 KB
svchost.exe             2864 Services        0       10.244 KB
svchost.exe             2904 Services        0       28.572 KB
svchost.exe             2924 Services        0       12.936 KB
spoolsv.exe              3032 Services        0       20.244 KB
svchost.exe             3068 Services        0       19.192 KB
svchost.exe             2688 Services        0        8.520 KB
svchost.exe             3224 Services        0        6.628 KB
svchost.exe             3264 Services        0       10.924 KB
```



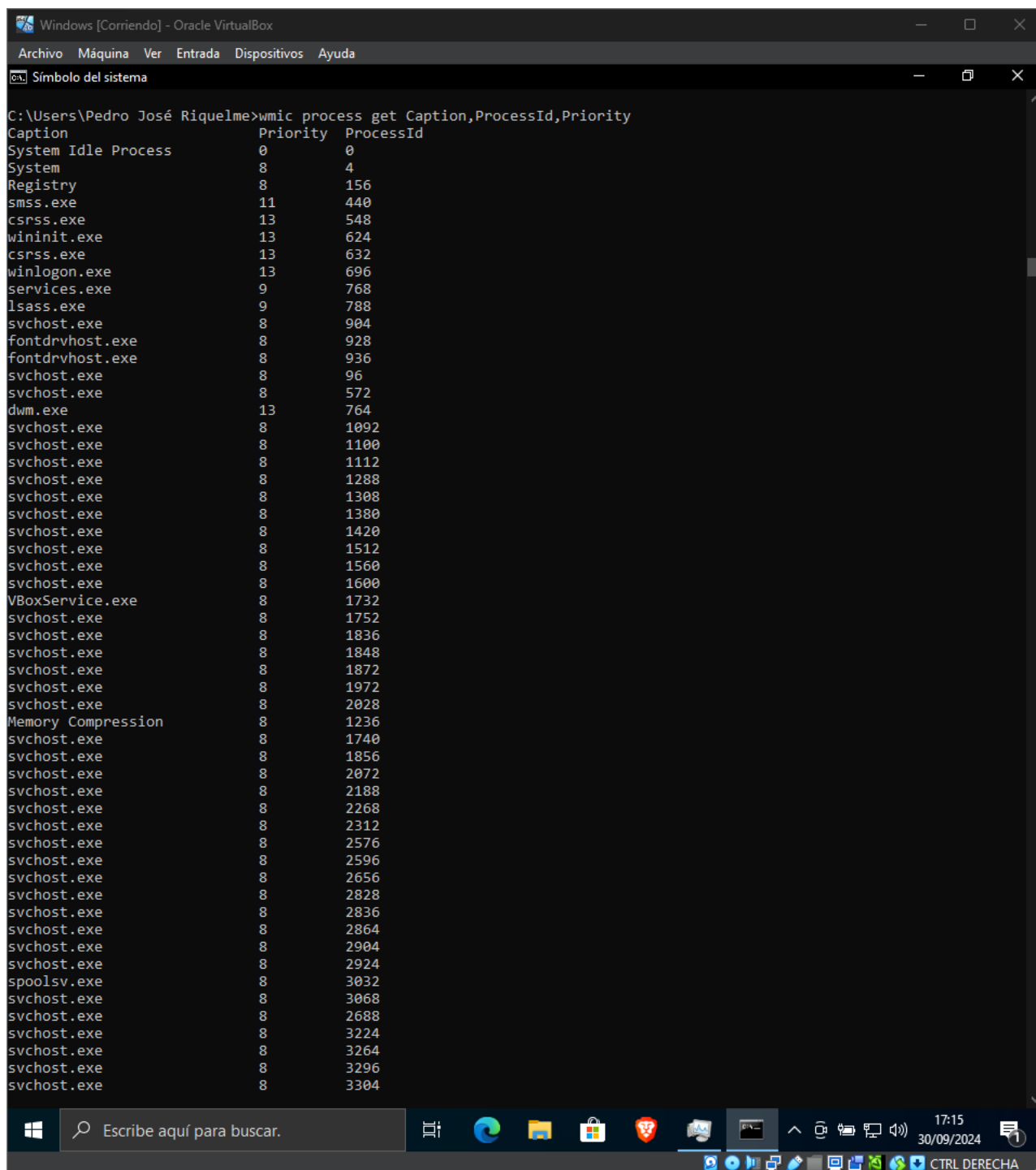
Veremos en orden el nombre del proceso, el ID proceso, nombre de sesión referente a la proveniencia del proceso, numero de sesiones y uso de memoria.

**Wmic process** nos dice el nombre del proceso el PID, el uso de CPU, el uso de memoria y el usuario que inició el proceso:

```
Windows [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
C:\> Símbolo del sistema
C:\Users\Pedro José Riquelme>wmic process
Caption
CommandLine
CreationClassName CreationDate
ExecutablePath
ExecutionState Handle HandleCount InstallDate Ke
rnelModeTime MaximumWorkingSetSize MinimumWorkingSetSize Name
OSCreationClassName OSNam
OtherOperationCount OtherTransferCount PageFaults Pag
eFileUsage ParentProcessId PeakPageFileUsage PeakVirtualSize PeakWorkingSetSize Priority PrivatePageCount Proc
essId QuotaNonPagedPoolUsage QuotaPagedPoolUsage QuotaPeakNonPagedPoolUsage QuotaPeakPagedPoolUsage ReadOperatio
nCount ReadTransferCount SessionId Status TerminationDate ThreadCount UserModeTime VirtualSize WindowsVersi
on WorkingSetSize WriteOperationCount WriteTransferCount
System Idle Process
Win32_Process 20240930165155.65104
4+120 Win32_ComputerSystem DESKTOP-51HC711 System Idle Process
0 0 Win32_OperatingSystem Micro
407812500
soft Windows 10 Pro|C:\Windows\Device\Harddisk0\Partition2 0 0 9 60
0 60 8192 12 0 61440 0
1 0 0 1 10 0 8192 10.0.19045
8192 0 0 0
System
Win32_Process 20240930165155.65104
4+120 Win32_ComputerSystem DESKTOP-51HC711 System
4 2677 Win32_OperatingSystem Micro
7656250
soft Windows 10 Pro|C:\Windows\Device\Harddisk0\Partition2 34053 158350 2704 196
0 0 216 14868480 868
1 0 0 1 200 0 4001792 134 4
193732 346 0 55286242
155648
Registry
Win32_Process 20240930165146.91478
2+120 Win32_ComputerSystem DESKTOP-51HC711 Registry
156 0 Win32_OperatingSystem Micro
281250
soft Windows 10 Pro|C:\Windows\Device\Harddisk0\Partition2 189 3755 30471 628
8 4 7744 113098752 105724
10 156 13 220 8 6438912 4 156
2048 0 4 79200256 10.0.19045
74444800 392 12345344
smss.exe
Win32_Process 20240930165155.68024
9+120 Win32_ComputerSystem DESKTOP-51HC711 smss.exe
440 53 Win32_OperatingSystem Micro
781250
soft Windows 10 Pro|C:\Windows\Device\Harddisk0\Partition2 511 37982 969 107
2 4 1136 2203367919616 1272
4 13 8 11 1097728 22 440
13220 0 2 0 2203359780864 10.0.19045
1253376 12 908
csrss.exe
Win32_Process 20240930165208.50380
3+120 Win32_ComputerSystem DESKTOP-51HC711 csrss.exe
548 498 Win32_OperatingSystem Micro
031250
soft Windows 10 Pro|C:\Windows\Device\Harddisk0\Partition2 5205 99604 2534 193
```

Este comando puede mostrar la prioridad, pero para hacerlo necesitamos ejecutar:  
**`wmic process get Caption,ProcessId,Priority`**.

"Caption" nos proporciona el nombre del proceso, "ProcessId" el identificador del proceso, y "Priority" indica la prioridad del mismo. En Windows, la prioridad va de 0 a 31, siendo el número más alto el que tiene mayor prioridad.



```
C:\Users\Pedro José Riquelme>wmic process get Caption,ProcessId,Priority
Caption                Priority ProcessId
System Idle Process    0      0
System                 8      4
Registry               8      156
smss.exe               11     440
csrss.exe              13     548
wininit.exe            13     624
csrss.exe              13     632
winlogon.exe           13     696
services.exe           9      768
lsass.exe              9      788
svchost.exe            8      904
fontdrvhost.exe        8      928
fontdrvhost.exe        8      936
svchost.exe            8      96
svchost.exe            8      572
dwm.exe               13     764
svchost.exe            8     1092
svchost.exe            8     1100
svchost.exe            8     1112
svchost.exe            8     1288
svchost.exe            8     1308
svchost.exe            8     1380
svchost.exe            8     1420
svchost.exe            8     1512
svchost.exe            8     1560
svchost.exe            8     1600
VBoxService.exe        8     1732
svchost.exe            8     1752
svchost.exe            8     1836
svchost.exe            8     1848
svchost.exe            8     1872
svchost.exe            8     1972
svchost.exe            8     2028
Memory Compression     8     1236
svchost.exe            8     1740
svchost.exe            8     1856
svchost.exe            8     2072
svchost.exe            8     2188
svchost.exe            8     2268
svchost.exe            8     2312
svchost.exe            8     2576
svchost.exe            8     2596
svchost.exe            8     2656
svchost.exe            8     2828
svchost.exe            8     2836
svchost.exe            8     2864
svchost.exe            8     2904
svchost.exe            8     2924
spoolsv.exe            8     3032
svchost.exe            8     3068
svchost.exe            8     2688
svchost.exe            8     3224
svchost.exe            8     3264
svchost.exe            8     3296
svchost.exe            8     3304
```

**Get process** nos dice la siguiente información: Nombre del proceso, PID, Uso de la CPU, Uso de memoria, Usuario que inició el proceso y Tiempo de ejecución.

```

Windows [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

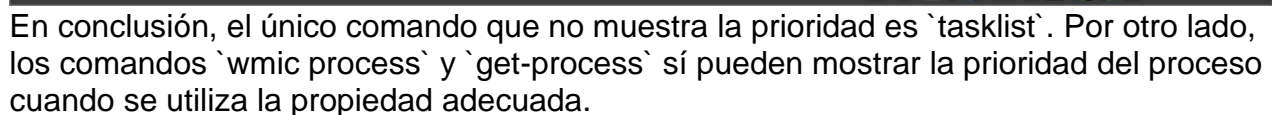
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\Pedro José Riquelme> Get-process

Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI ProcessName
-----  -
478      27     16676  35536  2,22    1704  1 ApplicationFrameHost
183      11     1756   368    0,05    6884  0 BraveCrashHandler
167      9      1884   384    0,05    6980  0 BraveCrashHandler64
73       5      2236   4500    0,05    7488  1 cmd
265      14     8456   24212  2,73    3764  1 conhost
267      14     4324   18920  0,20    6320  1 conhost
492      20     1932   5632   0,05    548   0 csrss
382      18     1904   5556   0,05    632   1 csrss
438      17     4180   20876  2,31    5992  1 ctfdmon
359      18     3568   13580  0,42    3544  0 dasHost
276      26     6480   16008  0,42    7300  1 dllhost
1047     50     41540  76504  0,42    764   1 dwm
2203     80     62336  122152  27,53   6300  1 explorer
36       5      1272   3488   0,05    928   0 fontdrvhost
36       6      1628   4704   0,05    936   1 fontdrvhost
0        0       60     8       0       0     0 Idle
1310     25     7392   20460  0,05    788   0 lsass
0        0       72     640    0,05   1236  0 Memory Compression
211      13     2096   3832   0,05    6196  0 MicrosoftEdgeUpdate
592      66    166112  133088  0,05    3320  0 MsMpEng
178      20     4072   9400   0,05    4420  0 NlsSrv
743     106    47336  90664  2,52    8476  1 OneDrive
689      44    84204  98992  3,73    4008  1 powershell
0        0      2056   68196  0,05    156   0 Registry
120       8     1520   8088   0,13    3048  1 RuntimeBroker
288      17     6388   25584  4,17    6848  1 RuntimeBroker
576      29    11816  42888  6,92    7248  1 RuntimeBroker
228      13     2960   14276  3,97    7544  1 RuntimeBroker
151       9     2156   12424  0,17    7800  1 RuntimeBroker
216      11     2540   12960  0,16   10112  1 RuntimeBroker
1541    123    167784  254576  30,97   7000  1 SearchApp
716      44    24180  36056  0,05    5264  0 SearchIndexer
397      16     3964   15020  0,05    8300  0 SecurityHealthService
160       9     1908   9508   0,14    8260  1 SecurityHealthSystray
622      11     5068   10400  0,05    768   0 services
105       7     4500   6852   0,05    7584  0 SgrmBroker
559      18     6312   26788  3,59    5820  1 silhost
419      36    11260  1236   0,72    3120  1 SkypeApp
435      24     8232   23772  0,23   10072  1 smartscreen
53       3      1072   1224   0,05    440   0 smss
479      23     6104   20244  0,05    3032  0 spoolsv
750      35    26164  78100  8,48    6152  1 StartMenuExperienceHost
1110     20     8108   16592  0,05    96   0 svchost
258      10     2264   7988   0,05    572   0 svchost
1384     23    11476  32728  0,05    904   0 svchost
112       7     1276   5640   0,05   1092  0 svchost
213      12     2436   10444  0,05   1100  0 svchost
259       9     1976   12244  0,05   1112  0 svchost
736      77    62212  27564  0,05   1160  0 svchost
391      14    16148  18732  0,05   1288  0 svchost
390      17     5760   15540  0,05   1308  0 svchost
326      18     4128   19840  0,05   1380  0 svchost
160       7     1468   6348   0,05   1420  0 svchost
297      13     3392   18928  0,05   1512  0 svchost
136      19     4296   8708   0,05   1560  0 svchost
219      10     2172   7936   0,05   1600  0 svchost
172      11     8368   18676  0,05   1672  0 svchost
179       9     1728   8168   0,05   1740  0 svchost

```

## “Get-Process | Select-Object Name, Id, PriorityClass”



## Apartado C:

La herramienta que necesitamos para el ejercicio la podemos descargar a través de este [enlace](#) (aunque salga aviso de virus es el zip que sale en la pagina web oficial de Microsoft así que no te asustes)

Una vez descargada la herramienta y ejecutada nos saldrá lo siguiente donde podremos ver una interfaz mucho mas bonita y clara para poder entenderla y nos enseña los procesos padres e hijos en forma de árbol jerárquico. Para cambiar la prioridad se hace dando click derecho como en el administrador de tareas

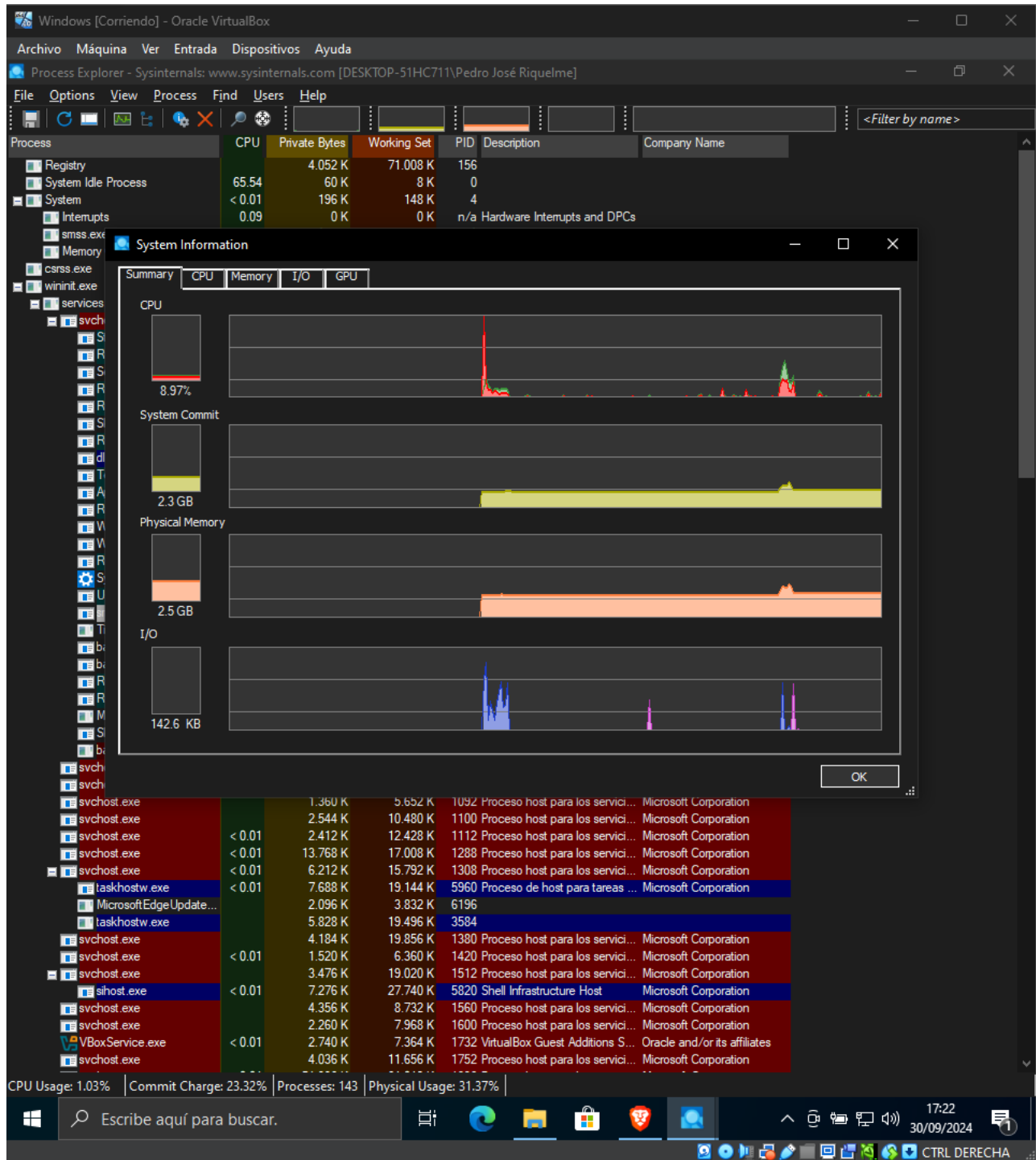
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		3.580 K	70.632 K	156		
System Idle Process	100.00	60 K	8 K	0		
System	0.17	196 K	148 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1.072 K	1.224 K	440		
Memory Compression		72 K	396 K	1236		
csrss.exe		2.004 K	5.680 K	548		
wininit.exe		1.440 K	7.296 K	624		
services.exe		5.848 K	11.028 K	768		
svchost.exe		11.404 K	32.732 K	904	Proceso host para los servi...	Microsoft Corporation
StartMenuExperience...		25.896 K	77.928 K	6152		
RuntimeBroker.exe		6.252 K	25.536 K	6848	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	167.784 K	254.348 K	7000	Search application	Microsoft Corporation
RuntimeBroker.exe		11.424 K	41.796 K	7248	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2.820 K	14.244 K	7544	Runtime Broker	Microsoft Corporation
SkypeApp.exe	Susp...	11.260 K	1.460 K	3120	SkypeApp	Microsoft Corporation
RuntimeBroker.exe		2.156 K	12.424 K	7800	Runtime Broker	Microsoft Corporation
dllhost.exe		6.372 K	15.956 K	7300	COM Surrogate	Microsoft Corporation
TextInputHost.exe		8.880 K	39.908 K	1240		Microsoft Corporation
ApplicationFrameHost...		16.768 K	35.592 K	1704	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		2.608 K	12.976 K	10112	Runtime Broker	Microsoft Corporation
WWAHost.exe	Susp...	37.780 K	83.240 K	7848	Host de Microsoft WWA	Microsoft Corporation
WinStore.App.exe	Susp...	15.224 K	1.732 K	8532	Store	Microsoft Corporation
RuntimeBroker.exe		1.520 K	8.088 K	3048	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	20.380 K	5.640 K	780	Configuración	Microsoft Corporation
UserOOBEBroker.exe		2.112 K	9.968 K	9200	User OOBEBroker	Microsoft Corporation
smartscreen.exe		9.692 K	27.128 K	10072	SmartScreen de Windows D...	Microsoft Corporation
WmiPrvSE.exe		3.216 K	10.824 K	4252		
svchost.exe		8.132 K	16.600 K	96	Proceso host para los servi...	Microsoft Corporation
svchost.exe	< 0.01	2.416 K	8.004 K	572	Proceso host para los servi...	Microsoft Corporation
svchost.exe		1.276 K	5.640 K	1092	Proceso host para los servi...	Microsoft Corporation
svchost.exe		2.436 K	10.444 K	1100	Proceso host para los servi...	Microsoft Corporation
svchost.exe		1.976 K	12.244 K	1112	Proceso host para los servi...	Microsoft Corporation
svchost.exe		16.192 K	18.884 K	1288	Proceso host para los servi...	Microsoft Corporation
svchost.exe		5.968 K	15.672 K	1308	Proceso host para los servi...	Microsoft Corporation
taskhostw.exe		6.868 K	17.288 K	5960	Proceso de host para tareas ...	Microsoft Corporation
MicrosoftEdgeUpdate...		2.096 K	3.832 K	6196		





En el apartado de opciones, existe la posibilidad de cambiar el color de los procesos y consultar su significado.

En la sección View, se encuentra la opción "system information", donde podemos ver gráficas con más detalles sobre la CPU, la memoria, y otros aspectos del sistema.



## Apartado A

La forma más sencilla de gestionar las aplicaciones de arranque es desde el Administrador de Tareas, donde se puede buscar a la izquierda el ícono de "Aplicaciones de arranque". Aquí se muestran las aplicaciones que se inician al encender el PC, junto con su estado y el impacto en el arranque.

The screenshot shows the Windows Task Manager application running in Oracle VM VirtualBox. The 'Inicio' (Startup) tab is selected, displaying a list of applications that start with Windows. The list includes Microsoft Edge, Microsoft OneDrive, VirtualBox Guest Additions Tools, and Windows Security notifications. Each entry shows the application name, publisher, status (Habilitado), and startup impact (No medido, Alto, or Bajo). The 'Último tiempo de BIOS' is 0.0 segundos.

Nombre	Anunciante	Estado	Impacto de ini...
Microsoft Edge	Microsoft Corporation	Habilitado	No medido
Microsoft OneDrive	Microsoft Corporation	Habilitado	Alto
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Habilitado	Bajo
Windows Security notificati...	Microsoft Corporation	Habilitado	Bajo

Menos detalles

Deshabilitar

17:24 30/09/2024

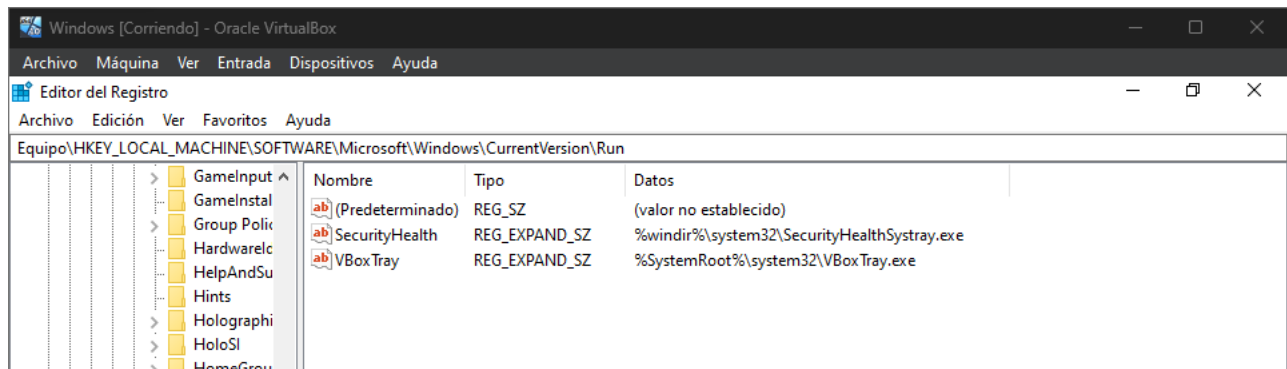
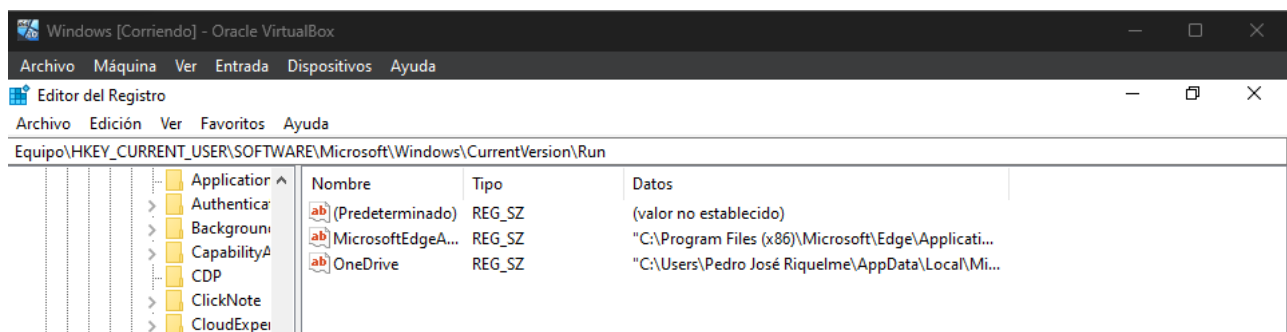
CTRL DERECHA

Además de esta opción, también es posible ver estos procesos de arranque mediante el Editor de Registro, PowerShell o directamente en la carpeta donde se almacena la configuración de las aplicaciones de inicio.

El registro HKCU (HKEY\_CURRENT\_USER) guarda configuraciones específicas del usuario, lo que significa que los programas listados en esta sección solo se ejecutan cuando ese usuario inicia sesión. Por otro lado, el registro HKLM (HKEY\_LOCAL\_MACHINE) contiene configuraciones que afectan a todos los usuarios del sistema, por lo que los programas allí listados se ejecutan cuando cualquier usuario inicia sesión.

En el Editor de Registro, las ubicaciones clave para ver estos programas son:

- `HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

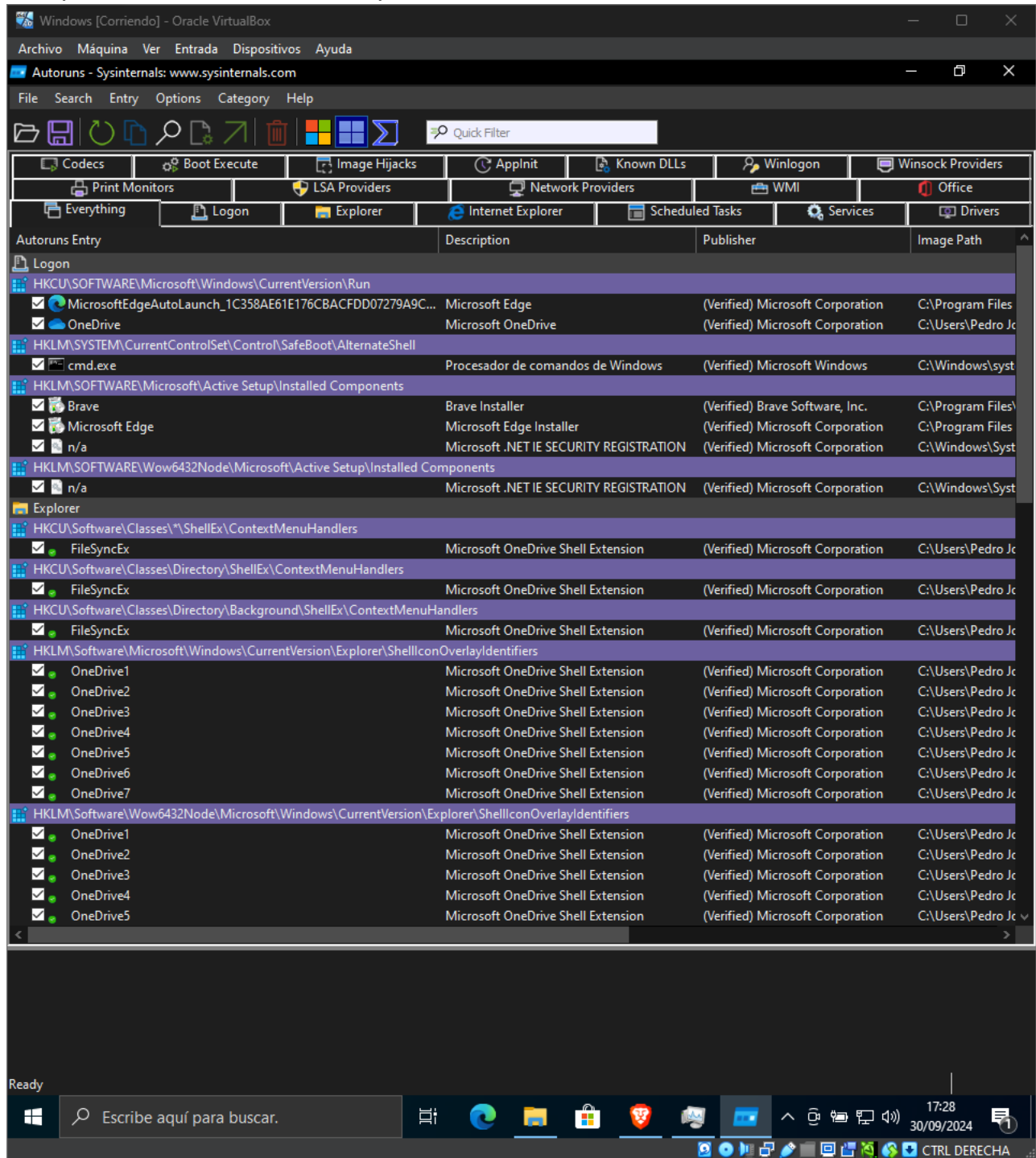


## Apartado B

Sysinternals Autoruns, descargamos la herramienta [aquí](#).

Después de descargar abrimos el zip y ejecutamos el exec.

Como se ve los procesos son los mismos que los que encontré en el editor de registro excepto el de brave, el cual no aparecía.





## Apartado C

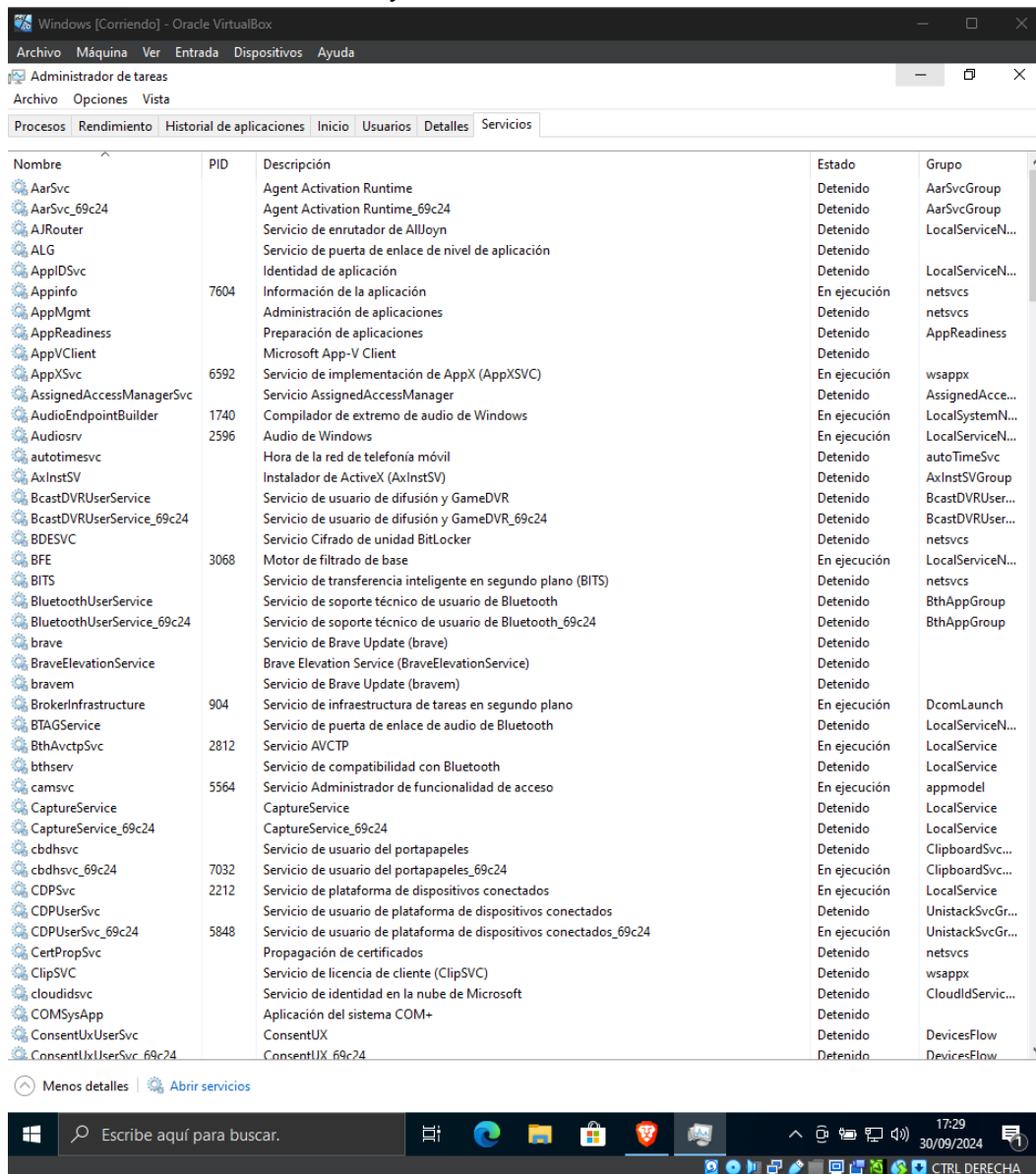
Para identificar procesos maliciosos, es importante observar el uso de recursos del proceso, como un consumo excesivo de CPU, GPU o memoria.

También es clave prestar atención al nombre del proceso y verificar su firma digital. Además, las conexiones que el proceso establece con la red son otro aspecto importante a tener en cuenta para detectar actividad sospechosa.

## 4) Windows: Servicios en windows.

### Apartado A:

Cuando nos metemos a los servicios nos salen todos los servicios que tenemos instalados en el ordenador y nos dicen su estado.



Nombre	PID	Descripción	Estado	Grupo
AarSvc		Agent Activation Runtime	Detenido	AarSvcGroup
AarSvc_69c24		Agent Activation Runtime_69c24	Detenido	AarSvcGroup
AJRouter		Servicio de enrutador de AllJoyn	Detenido	LocalServiceN...
ALG		Servicio de puerta de enlace de nivel de aplicación	Detenido	
ApplDSvc		Identidad de aplicación	Detenido	LocalServiceN...
AppInfo	7604	Información de la aplicación	En ejecución	netsvcs
AppMgmt		Administración de aplicaciones	Detenido	netsvcs
AppReadiness		Preparación de aplicaciones	Detenido	AppReadiness
AppVClient		Microsoft App-V Client	Detenido	
AppXSvc	6592	Servicio de implementación de AppX (AppXSVC)	En ejecución	wsappx
AssignedAccessManagerSvc		Servicio AssignedAccessManager	Detenido	AssignedAcce...
AudioEndpointBuilder	1740	Compilador de extremo de audio de Windows	En ejecución	LocalSystemN...
AudioSrv	2596	Audio de Windows	En ejecución	LocalServiceN...
autotimesvc		Hora de la red de telefonía móvil	Detenido	autoTimeSvc
AxInstSV		Instalador de ActiveX (AxInstSV)	Detenido	AxInstSVGroup
BcastDVRUserService		Servicio de usuario de difusión y GameDVR	Detenido	BcastDVRUser...
BcastDVRUserService_69c24		Servicio de usuario de difusión y GameDVR_69c24	Detenido	BcastDVRUser...
BDESVC		Servicio Cifrado de unidad BitLocker	Detenido	netsvcs
BFE	3068	Motor de filtrado de base	En ejecución	LocalServiceN...
BITS		Servicio de transferencia inteligente en segundo plano (BITS)	Detenido	netsvcs
BluetoothUserService		Servicio de soporte técnico de usuario de Bluetooth	Detenido	BthAppGroup
BluetoothUserService_69c24		Servicio de soporte técnico de usuario de Bluetooth_69c24	Detenido	BthAppGroup
brave		Servicio de Brave Update (brave)	Detenido	
BraveElevationService		Brave Elevation Service (BraveElevationService)	Detenido	
bravem		Servicio de Brave Update (bravem)	Detenido	
BrokerInfrastructure	904	Servicio de infraestructura de tareas en segundo plano	En ejecución	DcomLaunch
BTAGService		Servicio de puerta de enlace de audio de Bluetooth	Detenido	LocalServiceN...
BthAvctpSvc	2812	Servicio AVCTP	En ejecución	LocalService
bthserv		Servicio de compatibilidad con Bluetooth	Detenido	LocalService
camsv	5564	Servicio Administrador de funcionalidad de acceso	En ejecución	appmodel
CaptureService		CaptureService	Detenido	LocalService
CaptureService_69c24		CaptureService_69c24	Detenido	LocalService
cbdhsvc		Servicio de usuario del portapapeles	Detenido	ClipboardSvc...
cbdhsvc_69c24	7032	Servicio de usuario del portapapeles_69c24	En ejecución	ClipboardSvc...
CDPSvc	2212	Servicio de plataforma de dispositivos conectados	En ejecución	LocalService
CDPUserService		Servicio de usuario de plataforma de dispositivos conectados	Detenido	UnistackSvcGr...
CDPUserService_69c24	5848	Servicio de usuario de plataforma de dispositivos conectados_69c24	En ejecución	UnistackSvcGr...
CertPropSvc		Propagación de certificados	Detenido	netsvcs
ClipSvc		Servicio de licencia de cliente (ClipSvc)	Detenido	wsappx
cloudidsvc		Servicio de identidad en la nube de Microsoft	Detenido	CloudIdServic...
COMSysApp		Aplicación del sistema COM+	Detenido	
ConsentUxUserSvc		ConsentUX	Detenido	DevicesFlow
ConsentUxUserSvc_69c24		ConsentUX_69c24	Detenido	DevicesFlow

## Apartado B

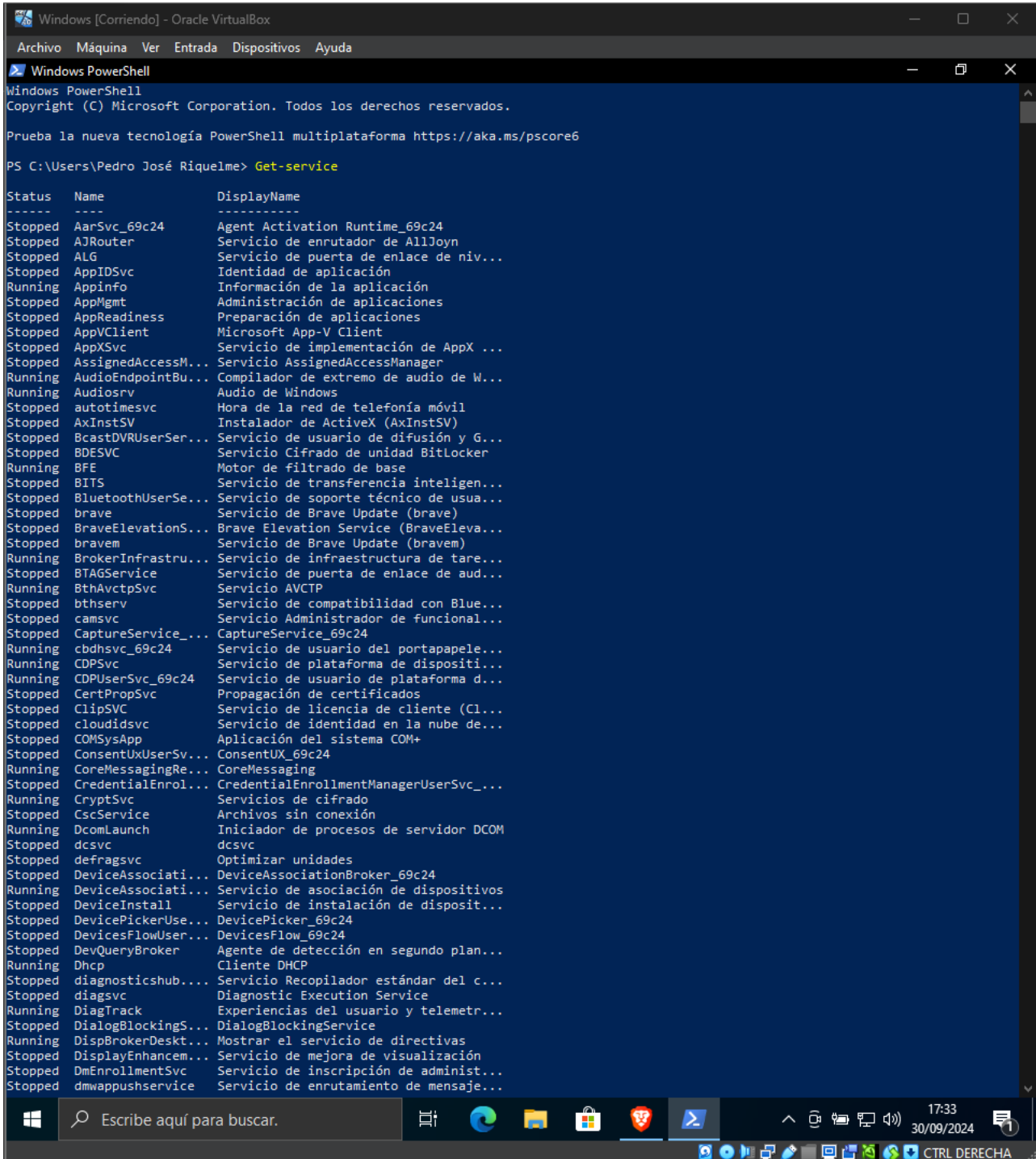
Aquí se muestra el nombre del servicio, una breve descripción, su estado actual, el tipo de inicio, y si el servicio es local o de red.

La diferencia entre inicio manual y automático es clara: el inicio manual requiere que el usuario lo active, mientras que el automático se ejecuta al iniciar el sistema. Esto es útil para programas que no necesitas en todas las sesiones, como Discord o Steam, lo que ayuda a ahorrar recursos.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
Acceso a datos de usuarios...	Proporciona...	En ejecu...	Manual	Sistema local
Actualizador de zona horari...	Establece la ...		Deshabilitado	Servicio local
Adaptador de rendimiento ...	Proporciona...		Manual	Sistema local
Administración de aplicacio...	Procesa las s...		Manual	Sistema local
Administración de autentic...	Proporciona...		Manual	Sistema local
Administración de capas de...	Optimiza la ...		Manual	Sistema local
Administración remota de ...	El servicio A...		Manual	Servicio de red
Administrador de conexio...	Crea una co...		Manual	Sistema local
Administrador de conexio...	Administra ...	En ejecu...	Automático	Sistema local
Administrador de conexio...	Toma decisi...	En ejecu...	Automático (...)	Servicio local
Administrador de configura...	Habilita la d...		Manual (dese...	Sistema local
Administrador de credencia...	Proporciona...	En ejecu...	Manual	Sistema local
Administrador de cuentas d...	El inicio de e...	En ejecu...	Automático	Sistema local
Administrador de cuentas ...	El Administr...	En ejecu...	Manual	Sistema local
Administrador de identidad...	Proporciona...		Manual	Servicio local
Administrador de mapas de...	Servicio de ...		Automático (i...	Servicio de red
Administrador de pagos y ...	Administra l...	En ejecu...	Manual (dese...	Servicio local
Administrador de sesión local	Servicio cen...	En ejecu...	Automático	Sistema local
Administrador de usuarios	El administr...	En ejecu...	Automático (...)	Sistema local
Adquisición de imágenes d...	Proporciona...		Manual (dese...	Servicio local
Agent Activation Runtime...	Runtime for ...		Manual	Sistema local
Agente de conexión de red	Conexiones ...	En ejecu...	Manual (dese...	Sistema local
Agente de detección en seg...	Permite a la...		Manual (dese...	Sistema local
Agente de directiva IPsec	El protocolo...		Manual (dese...	Servicio de red
Agente de eventos de tiempo	Coordina la ...	En ejecu...	Manual (dese...	Servicio local
Agente de eventos del siste...	Coordina la ...	En ejecu...	Automático (...)	Sistema local
Agente de supervisión en ti...	Supervisa y ...	En ejecu...	Automático (i...	Sistema local
Agrupación de red del mis...	Permite la c...		Manual	Servicio local
Aislamiento de claves CNG	El servicio Ai...	En ejecu...	Manual (dese...	Sistema local
Almacenamiento de datos ...	Controla el ...	En ejecu...	Manual	Sistema local
Aplicación auxiliar de NetBl...	Proporciona...	En ejecu...	Manual (dese...	Servicio local
Aplicación auxiliar IP	Proporciona...	En ejecu...	Automático	Sistema local
Aplicación del sistema CO...	Administra l...		Manual	Sistema local
Archivos sin conexión	El servicio d...		Manual (dese...	Sistema local
Asignador de detección de ...	Crea un ma...		Manual	Servicio local
Asignador de extremos de ...	Resuelve ide...	En ejecu...	Automático	Servicio de red
Asistente para la conectivid...	Proporciona...		Manual (dese...	Sistema local
Audio de Windows	Administra ...	En ejecu...	Automático	Servicio local
Autenticación natural	Servicio de a...		Manual (dese...	Sistema local
Ayudante para el inicio de s...	Permite al u...		Manual (dese...	Sistema local
BranchCache	Este servicio...		Manual	Servicio de red
Brave Elevation Service (Bra...			Manual	Sistema local

## Apartado C:

Get-service muestra el status del proceso, que es el estado actual de este, el nombre interno del proceso, y el DisplayName que es un nombre descriptivo del proceso.



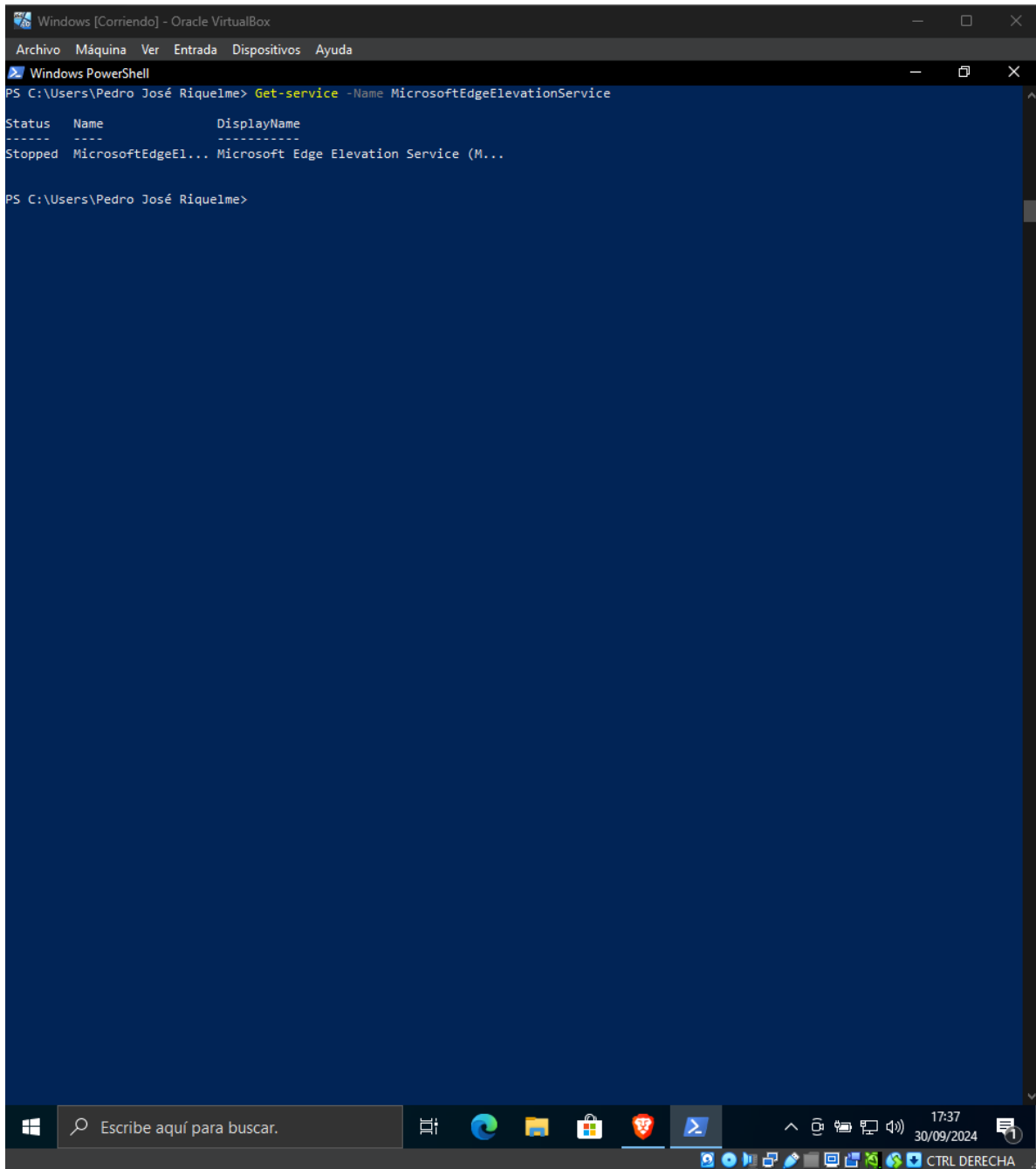
```
Windows [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

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

PS C:\Users\Pedro José Riquelme> Get-Service

Status Name DisplayName
-----
Stopped AarSvc_69c24 Agent Activation Runtime_69c24
Stopped AJRouter Servicio de enrutador de AllJoyn
Stopped ALG Servicio de puerta de enlace de niv...
Stopped AppIDSvc Identidad de aplicación
Running AppInfo Información de la aplicación
Stopped AppMgmt Administración de aplicaciones
Stopped AppReadiness Preparación de aplicaciones
Stopped AppVClient Microsoft App-V Client
Stopped AppXSvc Servicio de implementación de AppX ...
Stopped AssignedAccessM... Servicio AssignedAccessManager
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)
Stopped BcastDVRUserSer... Servicio de usuario de difusión y G...
Stopped BDESVC Servicio Cifrado de unidad BitLocker
Running BFE Motor de filtrado de base
Stopped BITS Servicio de transferencia intelligen...
Stopped BluetoothUserSe... Servicio de soporte técnico de usua...
Stopped brave Servicio de Brave Update (brave)
Stopped BraveElevationS... Brave Elevation Service (BraveEleva...
Stopped bravem Servicio de Brave Update (bravem)
Running BrokerInfrastru... Servicio de infraestructura de tare...
Stopped BTAGService Servicio de puerta de enlace de aud...
Running BthAvctpSvc Servicio AVCTP
Stopped bthserv Servicio de compatibilidad con Blue...
Stopped camsvc Servicio Administrador de funcional...
Stopped CaptureService_... CaptureService_69c24
Running cbdhsvc_69c24 Servicio de usuario del portapapele...
Running CDPSvc Servicio de plataforma de dispositi...
Running CDPUserSvc_69c24 Servicio de usuario de plataforma d...
Stopped CertPropSvc Propagación de certificados
Stopped ClipSvc Servicio de licencia de cliente (Cl...
Stopped cloudidsvc Servicio de identidad en la nube de...
Stopped COMSysApp Aplicación del sistema COM+
Stopped ConsentUxUserSv... ConsentUX_69c24
Running CoreMessagingRe... CoreMessaging
Stopped CredentialEnrol... CredentialEnrollmentManagerUserSvc_...
Running CryptSvc Servicios de cifrado
Stopped CscService Archivos sin conexión
Running DcomLaunch Iniciador de procesos de servidor DCOM
Stopped dcsvc dcsvc
Stopped defragsvc Optimizar unidades
Stopped DeviceAssociati... DeviceAssociationBroker_69c24
Running DeviceAssociati... Servicio de asociación de dispositivos
Stopped DeviceInstall Servicio de instalación de disposit...
Stopped DevicePickerUse... DevicePicker_69c24
Stopped DevicesFlowUser... DevicesFlow_69c24
Stopped DevQueryBroker Agente de detección en segundo plan...
Running Dhcp Cliente DHCP
Stopped diagnosticshub... Servicio Recopilador estándar del c...
Stopped diagsvc Diagnostic Execution Service
Running DiagTrack Experiencias del usuario y telemetr...
Stopped DialogBlockingS... DialogBlockingService
Running DispBrokerDesk... Mostrar el servicio de directivas
Stopped DisplayEnhancem... Servicio de mejora de visualización
Stopped DmEnrollmentSvc Servicio de inscripción de administ...
Stopped dmwappushservice Servicio de enrutamiento de mensaje...
```

Si queremos que me muestre la información de un servicio en particular utilizaremos la propiedad -Name con el nombre del servicio deseado.



```
Windows [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Windows PowerShell
PS C:\Users\Pedro José Riquelme> Get-Service -Name MicrosoftEdgeElevationService

Status  Name                DisplayName
-----  ----                -
Stopped MicrosoftEdgeEl... Microsoft Edge Elevation Service (M...

PS C:\Users\Pedro José Riquelme>
```

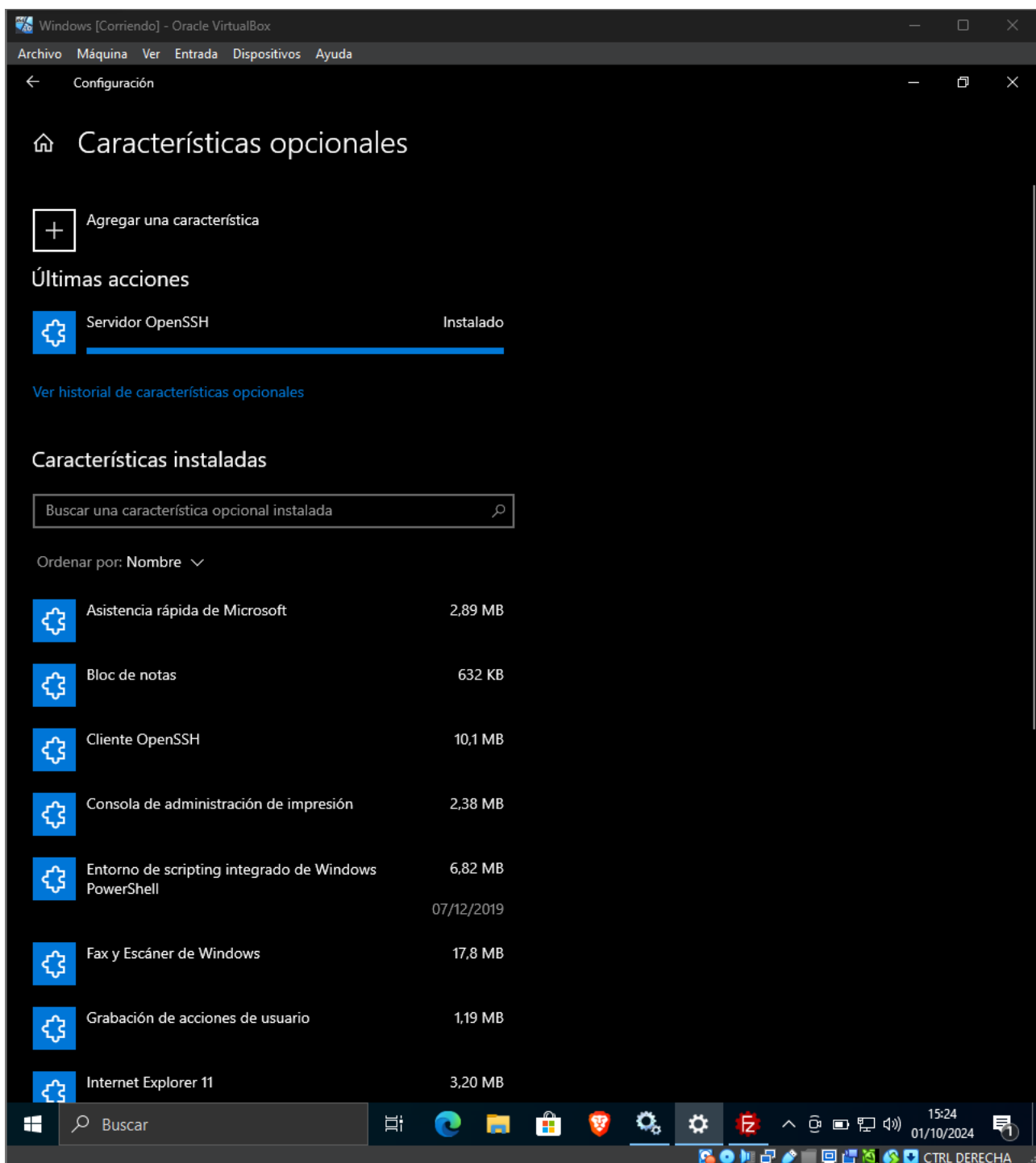
Aquí he elegido el servicio de MicrosoftEdgeElevationService, si quisiéramos parar o iniciar un servicio lo haríamos de la siguiente manera:

**Get-Service -Name MicrosoftEdgeElevationService**  
**Stop-Service -Name MicrosoftEdgeElevationService**

## Apartado D:

Yo he elegido instalar el servicio de OpenSSH.Server, como por powershell no me dejaba instalarlo pasé a instalarlo mediante los ajustes. Nos vamos a el apartado de características opcionales -> Agregar una característica y buscamos el servicio de “Servidor OpenSSH” e instalamos el servicio, sino sería con el siguiente comando:

**“Add-WindowsCapability -Online -Name OpenSSH.Server”**

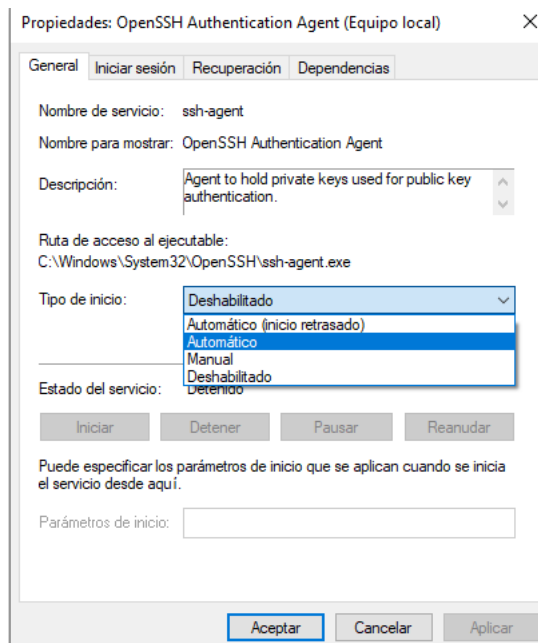
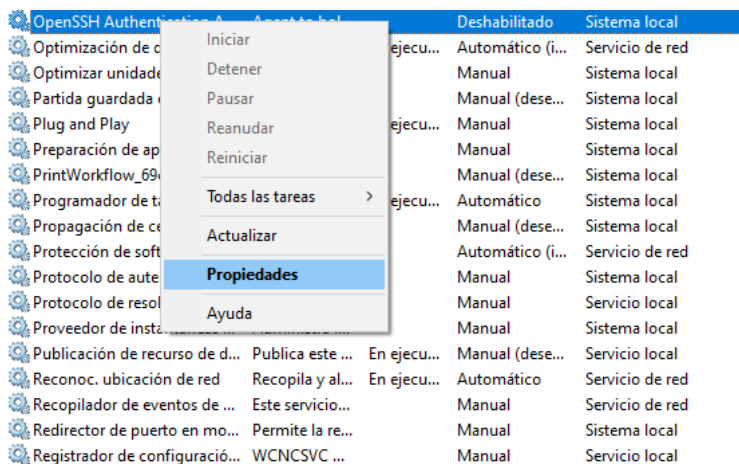




## Apartado B) C) D)

Una vez instalado, podemos abrir los servicios desde PowerShell utilizando el comando ``services.msc`` o, alternativamente, desde el buscador de Windows escribiendo "servicios".

Como se puede observar, el servicio está configurado para iniciar de manera manual, lo que significa que no se activará con el arranque del sistema. Para cambiar esto y permitir que se inicie automáticamente, simplemente hacemos doble clic en el servicio o clic derecho y seleccionamos "Propiedades". Luego, en la opción de tipo de inicio, cambiamos de "Manual" a "Automático", aplicamos los cambios y hacemos clic en "Aceptar".



Ahora abrimos powershell en modo administrador, si no dara error, y escribimos lo siguiente:

Para ver el estado del servicio: **Get-Service -Name sshd**

Para iniciar el servicio: **Start-Service -Name sshd**

Para pararlo: **Stop-Service -Name sshd**

```
Windows [Corriendo] - Oracle VirtualBox
Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Service -Name sshd

Status      Name      DisplayName
-----
Stopped     sshd      OpenSSH SSH Server

PS C:\Windows\system32> Start-Service -Name sshd
PS C:\Windows\system32> Get-Service -Name sshd

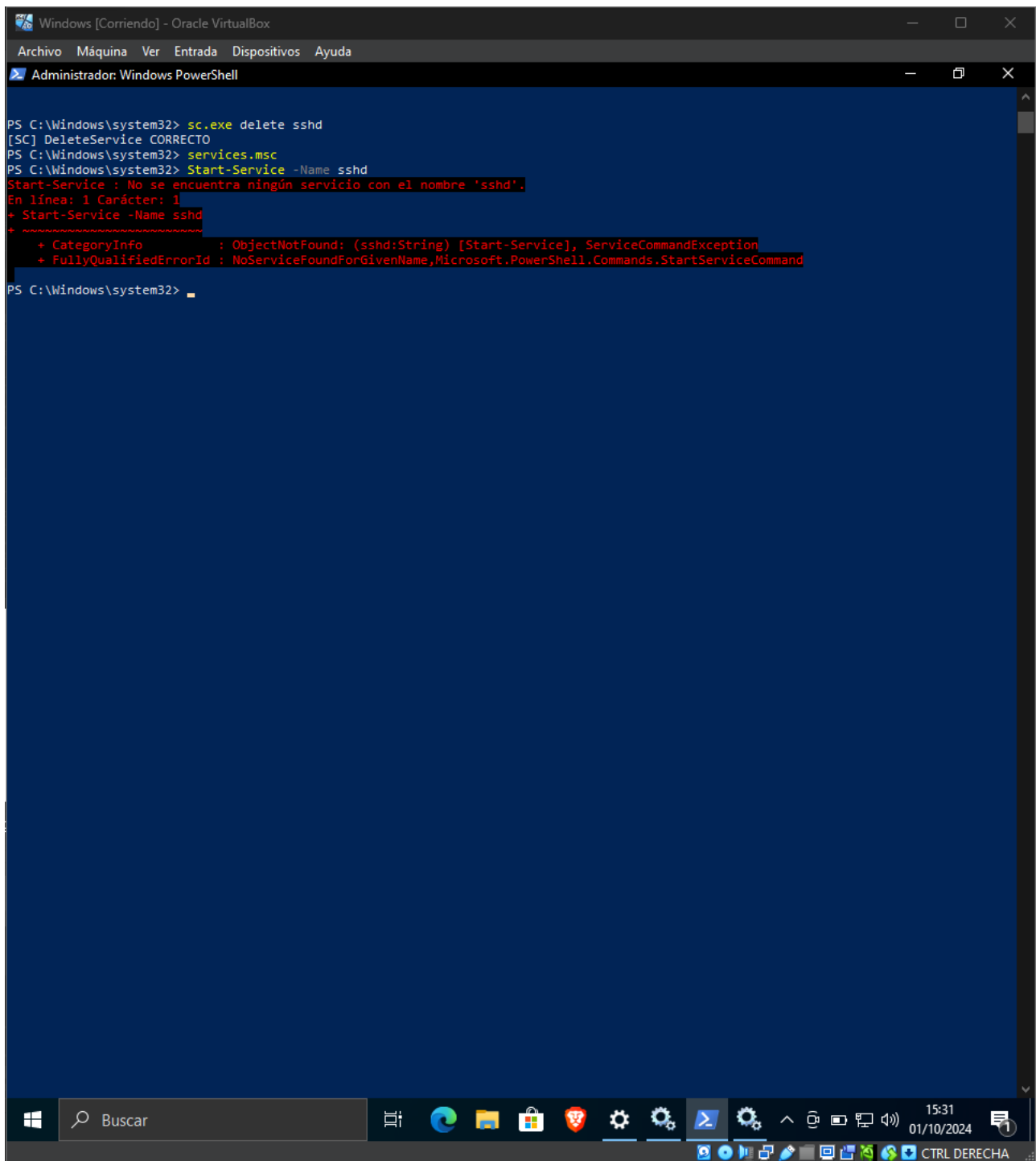
Status      Name      DisplayName
-----
Running     sshd      OpenSSH SSH Server

PS C:\Windows\system32> Stop-Service -Name sshd
PS C:\Windows\system32> Get-Service -Name sshd

Status      Name      DisplayName
-----
Stopped     sshd      OpenSSH SSH Server

PS C:\Windows\system32>
```

Para eliminar el servicio volveremos a powershell y escribiremos lo siguiente:  
“**sc.exe delete sshd**”

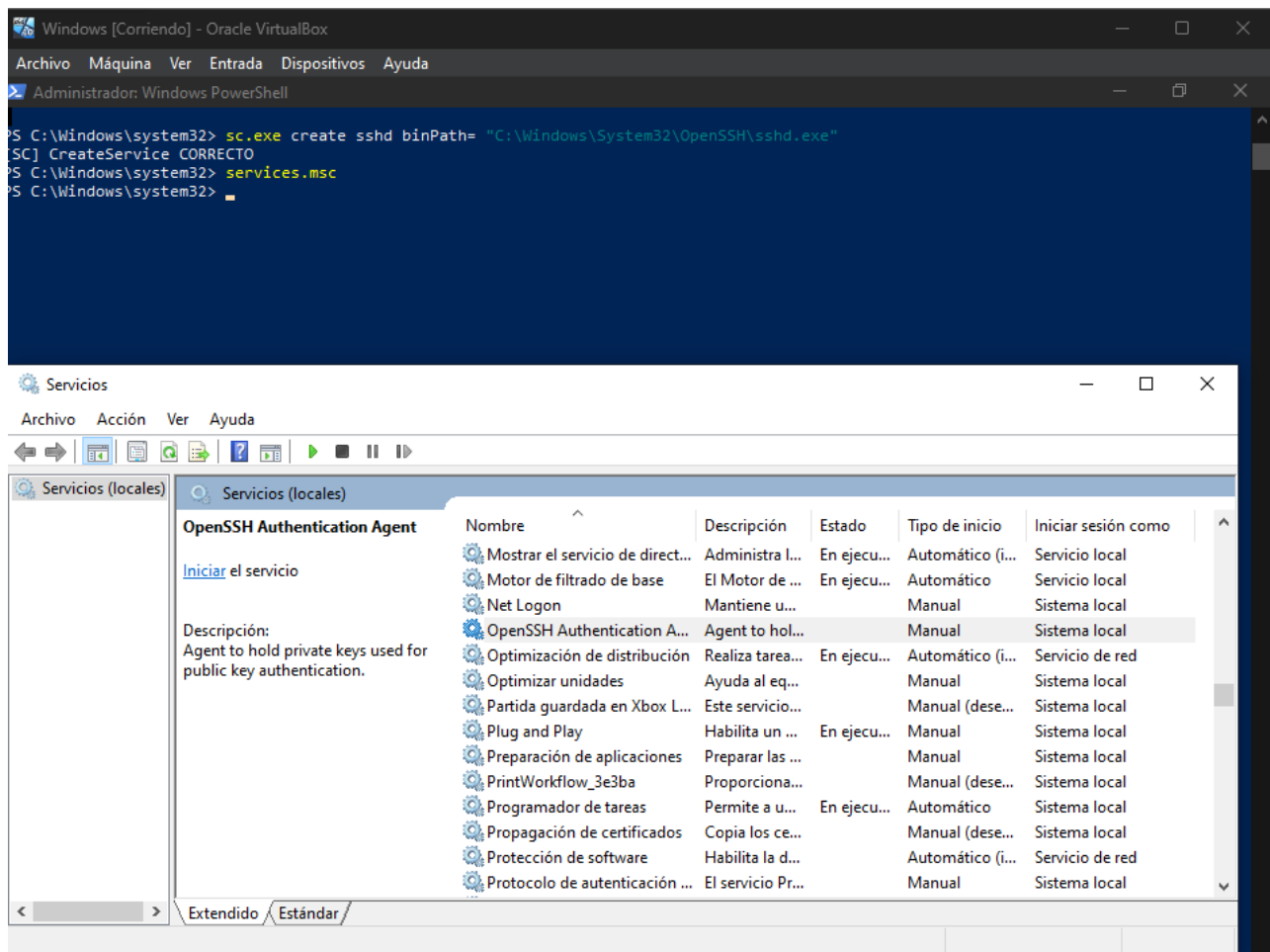


```
Windows [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Administrador: Windows PowerShell

PS C:\Windows\system32> sc.exe delete sshd
[SC] DeleteService CORRECTO
PS C:\Windows\system32> services.msc
PS C:\Windows\system32> Start-Service -Name sshd
Start-Service : No se encuentra ningún servicio con el nombre 'sshd'.
En línea: 1 Carácter: 1
+ Start-Service -Name sshd
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (sshd:String) [Start-Service], ServiceCommandException
+ FullyQualifiedErrorId : NoServiceFoundForGivenName,Microsoft.PowerShell.Commands.StartServiceCommand

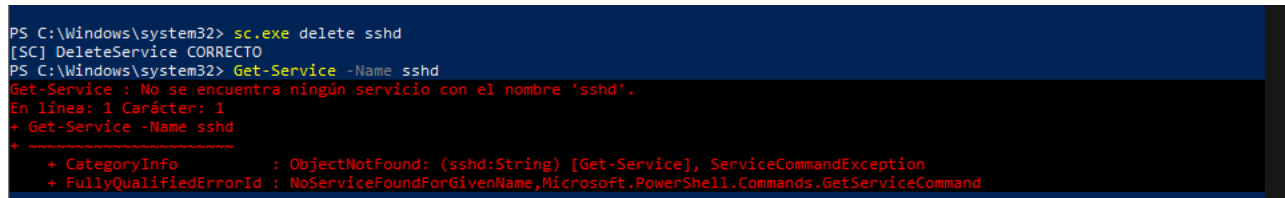
PS C:\Windows\system32>
```

## Apartado E) F)



Ahora, al observar la lista, notamos que el servicio ya no aparece, lo que indica que lo hemos eliminado. En consecuencia, intentaremos iniciarlo utilizando los comandos que hemos visto anteriormente para la gestión de servicios.

Sin embargo, al intentar iniciarlo con el comando `Start-Service`, recibimos un error, ya que el servicio ha sido eliminado previamente. Para volver a iniciar el servicio, será necesario ejecutarlo desde el archivo `.exe` correspondiente o registrarlo manualmente nuevamente en el sistema.



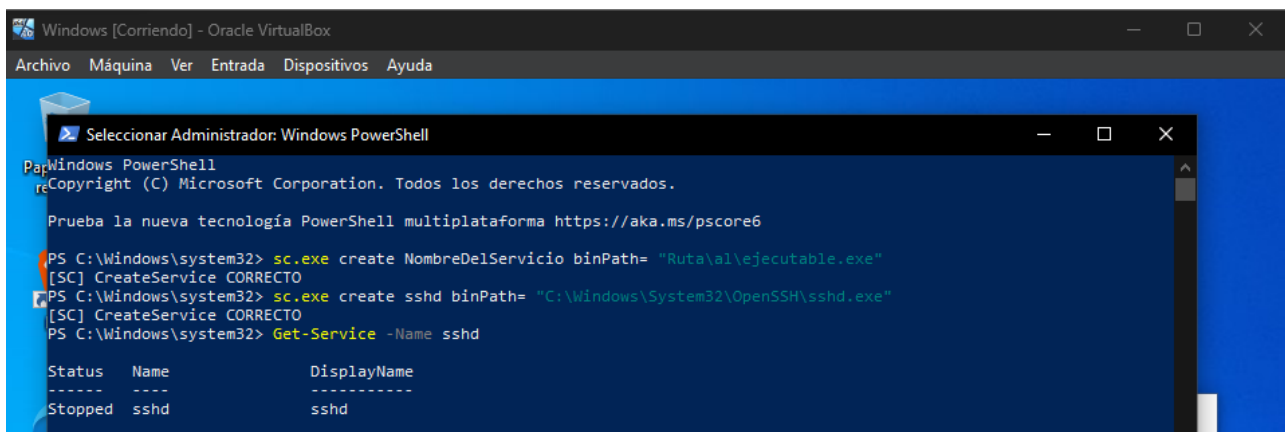
## Apartado E:

Para crear un servicio, debemos usar en PowerShell el siguiente comando. En este caso, volveremos a registrar el servicio **sshd**:

```
sc.exe create NombreDelServicio binPath= "Ruta\al\ejecutable.exe"
```

Para nuestro caso específico, el comando será:

```
sc.exe create sshd binPath= "C:\Windows\System32\OpenSSH\sshd.exe"
```



```
Windows [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

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

PS C:\Windows\system32> sc.exe create NombreDelServicio binPath= "Ruta\al\ejecutable.exe"
[SC] CreateService CORRECTO
PS C:\Windows\system32> sc.exe create sshd binPath= "C:\Windows\System32\OpenSSH\sshd.exe"
[SC] CreateService CORRECTO
PS C:\Windows\system32> Get-Service -Name sshd

Status  Name      DisplayName
-----  -
Stopped sshd      sshd
```

---

## **Apartado F:**

El árbol de registro de Windows es un espacio donde cada servicio se representa mediante una subclave. En estas subclaves se almacena información como el nombre del servicio, el tipo de inicio, el ejecutable asociado y otros parámetros de configuración.

Dentro de cada subclave, se pueden encontrar valores que determinan el comportamiento del servicio. Por ejemplo, es posible especificar si un servicio debe ejecutarse al inicio del sistema y el tipo de cuenta bajo la cual se ejecuta, entre otros detalles.

La ruta para acceder a los servicios en el registro es:

**“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services”**

Por otro lado, la ruta para los servicios del usuario es:

**“HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall”**



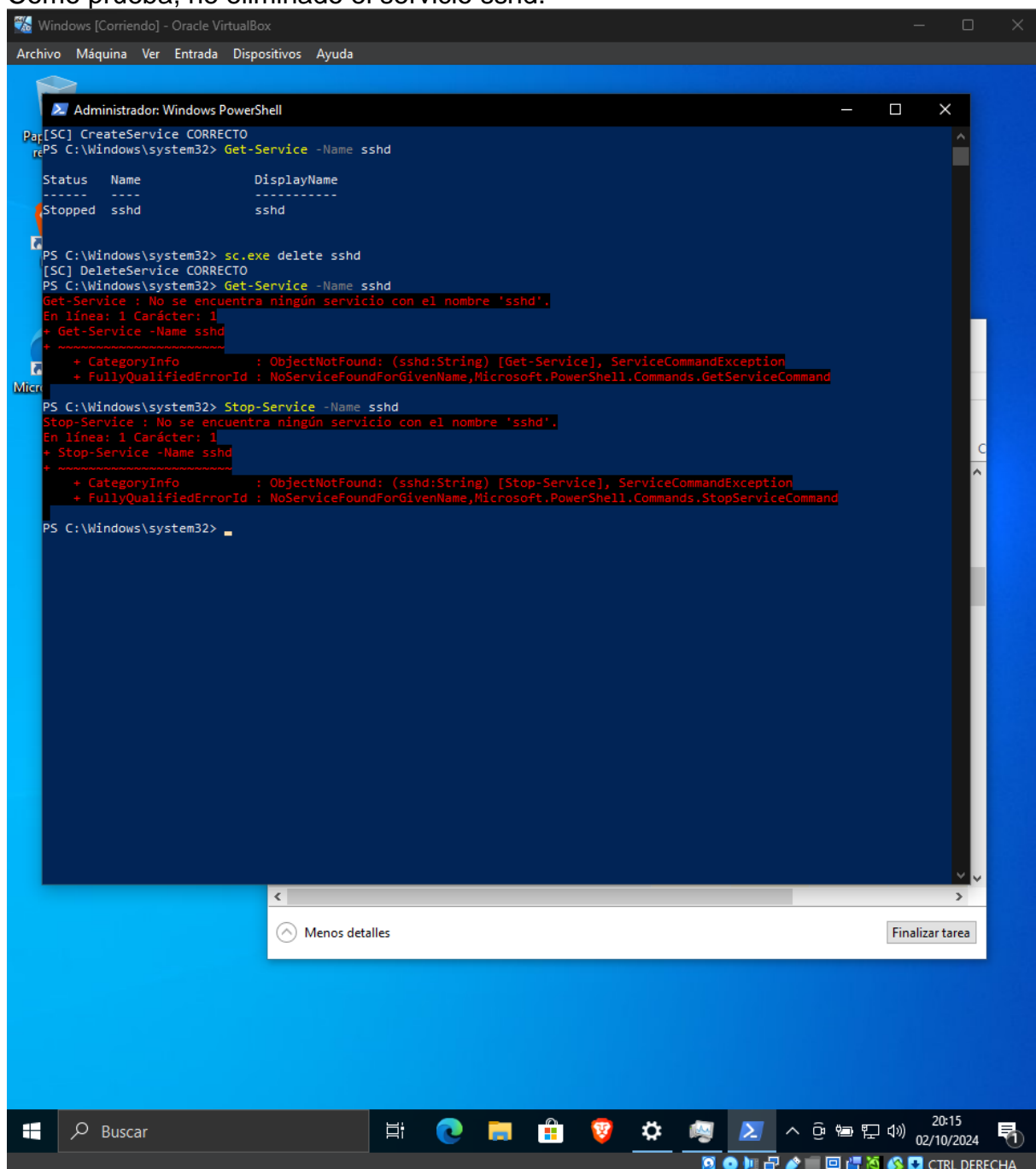
## Apartado G:

Podemos desinstalar un servicio utilizando el siguiente comando:

**“sc.exe delete NombreDelServicio”**

Sin embargo, es importante tener en cuenta que desinstalar servicios no es recomendable, ya que puede causar inestabilidad en el equipo y generar problemas de dependencias.

Como prueba, he eliminado el servicio sshd.



```
Windows [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Service -Name sshd

Status      Name      DisplayName
-----
Stopped     sshd      sshd

PS C:\Windows\system32> sc.exe delete sshd
[SC] DeleteService CORRECTO
PS C:\Windows\system32> Get-Service -Name sshd
Get-Service : No se encuentra ningún servicio con el nombre 'sshd'.
En línea: 1 Carácter: 1
+ Get-Service -Name sshd
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (sshd:String) [Get-Service], ServiceCommandException
+ FullyQualifiedErrorId : NoServiceFoundForGivenName,Microsoft.PowerShell.Commands.GetServiceCommand

PS C:\Windows\system32> Stop-Service -Name sshd
Stop-Service : No se encuentra ningún servicio con el nombre 'sshd'.
En línea: 1 Carácter: 1
+ Stop-Service -Name sshd
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (sshd:String) [Stop-Service], ServiceCommandException
+ FullyQualifiedErrorId : NoServiceFoundForGivenName,Microsoft.PowerShell.Commands.StopServiceCommand

PS C:\Windows\system32>
```

Menos detalles Finalizar tarea