TUP: Arquitectura y Sistemas Operativos

Alumno: Hotchkyss, Gersom Tomás

Actividad Práctica 2A: Procesos

Considerando que un proceso es un programa en ejecución, que reside en memoria y consume recursos, podemos analizarlos de diferentes maneras: identificarlos, controlarlos, terminarlos.

Utilizar las consolas: powershell, cmd y Linux

CMD:

1. Listar los procesos del sistema y describir la información suministrada.

Información que suministra: Nombre de imagen, identificador de proceso, uso de memoria, sesión.

```
C:\Users\Usuario>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        144 KB
Registry                        108 Services                   0    127.868 KB
smss.exe                        392 Services                   0      1.232 KB
csrss.exe                       592 Services                   0      6.028 KB
wininit.exe                     856 Services                   0      6.936 KB
csrss.exe                       864 Console                    1      6.096 KB
winlogon.exe                    964 Console                    1     11.668 KB
services.exe                    984 Services                   0     11.832 KB
lsass.exe                        68 Services                   0     24.944 KB
svchost.exe                     728 Services                   0     29.652 KB
fontdrvhost.exe                 764 Services                   0      6.824 KB
fontdrvhost.exe                 760 Console                    1     16.020 KB
WUDFHost.exe                    784 Services                   0      8.972 KB
svchost.exe                    1064 Services                   0     18.516 KB
svchost.exe                    1128 Services                   0     10.928 KB
svchost.exe                    1212 Services                   0     12.296 KB
svchost.exe                    1228 Services                   0      5.516 KB
svchost.exe                    1328 Services                   0     12.704 KB
svchost.exe                    1336 Services                   0     10.012 KB
svchost.exe                    1412 Services                   0     22.196 KB
dwm.exe                        1428 Console                    1     63.188 KB
svchost.exe                    1552 Services                   0      6.584 KB
svchost.exe                    1636 Services                   0      8.808 KB
svchost.exe                    1652 Services                   0     17.744 KB
svchost.exe                    1692 Services                   0     12.336 KB
svchost.exe                    1712 Services                   0      7.692 KB
svchost.exe                    1780 Services                   0      6.300 KB
WUDFHost.exe                   1896 Services                   0      8.824 KB
NVDisplay.Container.exe        1948 Services                   0     19.056 KB
svchost.exe                    1972 Services                   0     10.184 KB
svchost.exe                    2000 Services                   0     12.380 KB
wsc_proxy.exe                  1680 Services                   0     12.640 KB
svchost.exe                    1820 Services                   0      7.964 KB
svchost.exe                    1816 Services                   0      8.076 KB
svchost.exe                    1856 Services                   0     14.236 KB
```

```
C:\Users\Usuario>tasklist > procesos.txt
```

3. Iniciar una instancia de alguna aplicación, por ejemplo Word o cualquier editor de nota. Identificar los datos del proceso que se inicia con esta acción.

Datos mostrados:

- Name (Nombre del proceso): notepad
- Id o PID: Número de identificador de proceso
- CPU: Uso del procesador
- Memory: Uso de Memoria RAM

```
C:\Users\Usuario>start notepad

C:\Users\Usuario>tasklist | findstr notepad
notepad.exe                  8928 Console                    1    14.996 KB
```

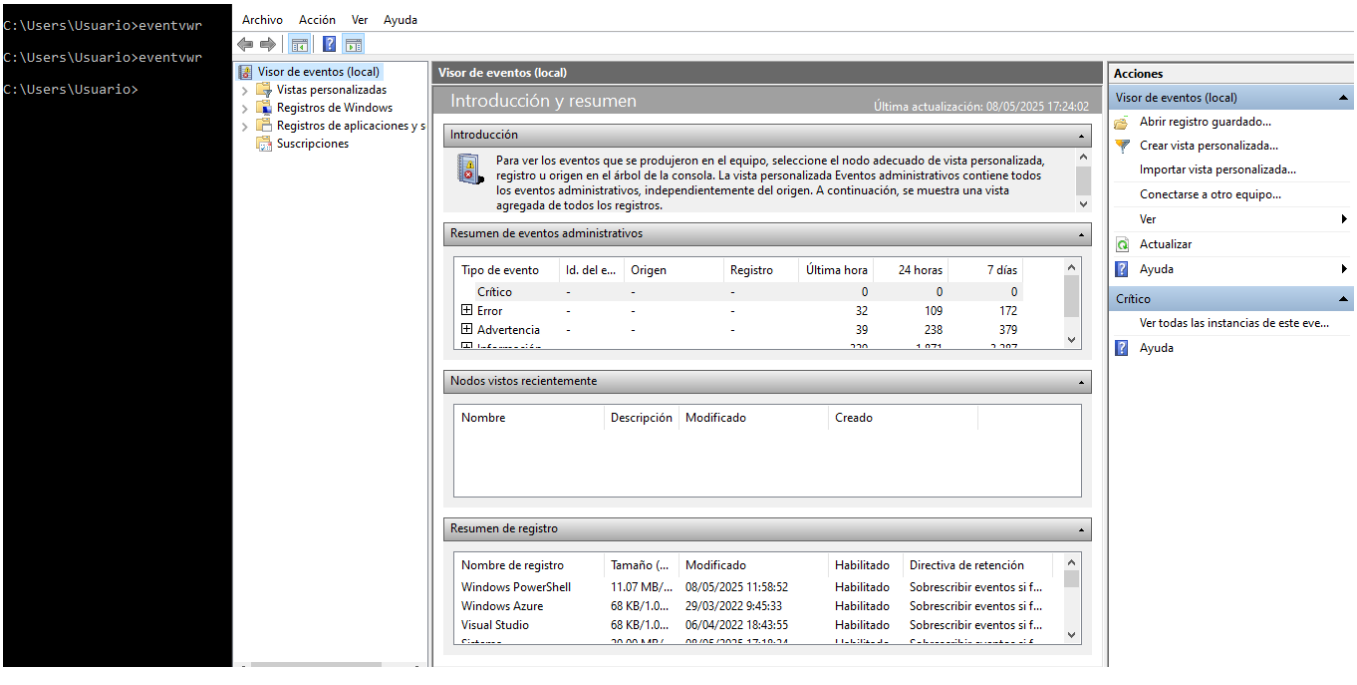
4. Mostar solo el proceso del punto 2.

```
C:\Users\Usuario>tasklist | findstr notepad procesos.txt
```

5. Cerrar la aplicación, “matando” el proceso de la misma.

```
C:\Users\Usuario>taskkill /IM notepad.exe /F
Correcto: se terminó el proceso "notepad.exe" con PID 8928.
```

6. Consulto los log del sistema operativo y analice si se registraron estas acciones



Varios

7. Cuál es el comando para reiniciar el sistema (PC o servidor)?

```
C:\Users\Usuario>shutdown /r /t 0
```

8. Cuál es el comando para apagar el sistema (PC o servidor)?.

```
C:\Users\Usuario>shutdown /s /t 0
```

9. Qué es un archivo de log. Cuál es el formato más común?.

Un archivo log es un archivo de texto donde el sistema o una aplicación registra eventos importantes, errores, accesos, etc.

Formato más común: 2025-05-08 10:32:45 ERROR: Servicio X ha fallado

10. Consultar la fecha y hora del sistema. Por qué es importante tener la fecha y hora del sistema de manera correcta?.

```
C:\Users\Usuario>time
La hora actual es: 17:34:01.54
Escriba una nueva hora: 14
El cliente no dispone de un privilegio requerido.
```

Es importante tener la fecha y hora del sistema de manera correcta para poder sincronizar archivos y tareas, auditorías y logs y evitar errores en certificados, servidores y redes.

POWERSHELL:

1- Información que suministra: Nombre del proceso, id (PID), uso de CPU, memoria, tiempo de inicio.

```
PS C:\Users\Usuario> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    328      16     3944      14948       0.19    8200   1 ADPClientService
    431      27    55060     137384       4.14   12440   1 AdskAccessCore
    287      16    16204      35504       0.31   13292   1 AdskAccessService
    387      17    10768      28580              4584   0 AdskAccessServiceHost
    364      25    45136      91036       0.81    6872   1 AdskAccessUIHost
    340      20    13720      49168       0.06    7104   1 AdskAccessUIHost
    404      21    39460      53400       0.17   12752   1 AdskAccessUIHost
    210      18    15360      50560       0.05   13108   1 AdskAccessUIHost
    929      43    71344      90220       0.89   13144   1 AdskAccessUIHost
    460      25     6224      21408       1.53   12540   1 AdskIdentityManager
    126      11    20176      18752              4524   0 AdskLicensingService
    567      38    41460      56976       1.91   12672   1 AdSSO
    115       7     2280       7308              9724   0 AggregatorHost
    434      24    17512      33364       0.19   14024   1 ApplicationFrameHost
    337      25     4424      17144              8912   0 ApplicationWebServer
    492      28    48528      75912              4400   0 aswEngSrv
   1020      28    28672      46220              8444   0 aswidsagent
   1574      38    47368      77844              3868   0 aswToolsSvc
    161      12     7528       8752              4476   0 atkexComSvc
   5263     120    81808     138736              3712   0 AvastSvc
   2229      45    28380      57148       2.16   3916   1 AvastUI
    972      38     5892      18196              1872   0 AvEmUpdate
    413      19     5464      26256       0.20    668   1 backgroundTaskHost
    305      31     9124      28564       0.09   1124   1 backgroundTaskHost
    530      25     6992      30672       0.31   1464   1 backgroundTaskHost
    419      33    13536      39256       0.91   1620   1 backgroundTaskHost
    350      33    16224      42844       0.58   3552   1 backgroundTaskHost
    361      22     5824      30272       0.20   5040   1 backgroundTaskHost
    109       7     6472      10560              3372   0 conhost
    168      10     6720      13372              5124   0 conhost
    111       7     6388      10568       0.02   8340   1 conhost
    278      14     4672      16504       0.27   12856  1 conhost
    125       8     1312       6124              5768   0 CptService
    954      30     2364       6212               592   0 csrss
    637      22     2636       5768               800   1 csrss
    447      17     4300      21028       0.70   10296  1 ctfmon
    118      10    17956      10648              6120   0 dispatcher
    266      28     6940      14976       0.14   12316  1 dllhost
   1164      46    59244      59844              1392   1 dwm
    127      10     1508       6696              4544   0 EwServer
   2207      84   116024     135100       8.63   10556  1 explorer
    201      11     2136       7504              3776   0 fdhost
     79       6     1000       4772              5324   0 fdlauncher
    207      15     2532      10732              4576   0 FNPLicensingService
    171      11     2920       8812              4592   0 FNPLicensingService64
     50       7     4052       6732               684   0 fontdrvhost
```

2-

```
PS C:\Users\Usuario> Get-Process | Out-File "procesos.txt"
```

3-

Datos mostrados:

- Name (Nombre del proceso): notepad
- Id o PID: Número de identificador de proceso
- CPU: Uso del procesador
- Memory: Uso de Memoria RAM

```
PS C:\Users\Usuario> start notepad
PS C:\Users\Usuario> Get-Process notepad

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    247      14     3284      14840       0.09   12564   1 notepad
```

4-

```
PS C:\Users\Usuario> Select-String -Path "procesos.txt" -Pattern "notepad"
```

5-

```
PS C:\Users\Usuario> Stop-Process -Name "notepad"
```

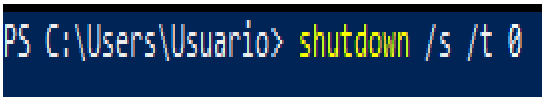
6-

```
PS C:\Users\Usuario> Get-EventLog -LogName System -Newest 50

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   94574 may. 08 17:41 Information BROWSER                3221233504 El servicio Examinador no puede recuperar la li...
   94573 may. 08 17:40 Warning     DCOM                         10016 No se encontró la descripción del id. de evento...
   94572 may. 08 17:40 Information Service Control M...   1073748864 El tipo de inicio del servicio Servicio de tran...
   94571 may. 08 17:40 Information Microsoft-Windows...         158 El proveedor de hora 'VMICTimeProvider' ha indi...
   94570 may. 08 17:40 Error       Service Control M...   3221232495 El servicio Agente de supervisión en tiempo de ...
   94569 may. 08 17:40 Error       Service Control M...   3221232472 El servicio Google Update Servicio (gupdate) no...
   94568 may. 08 17:40 Error       Service Control M...   3221232481 Se agotó el tiempo de espera (30000 ms) para la...
   94567 may. 08 17:40 Warning     BROWSER                2147491669 El servicio explorador no puede recuperar una l...
   94566 may. 08 17:38 Information Service Control M...   3221232498 El siguiente controlador de inicio del sistema ...
   94565 may. 08 17:38 Information Service Control M...   1073748864 El tipo de inicio del servicio BITS se cambió d...
   94564 may. 08 17:38 Information Microsoft-Windows...         7001 Notificación de inicio de sesión de usuario par...
   94563 may. 08 17:38 Information WAS                    1073747035 El servicio de activación de procesos de Window...
   94562 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'bindflt' (10.0, ...
   94561 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'storqosflt' (10....
   94560 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'CldFlt' (10.0, 2...
   94559 may. 08 17:38 Information Microsoft-Windows...            1 Filtro de sistema de archivos 'CldFlt' (Versión...
   94558 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'CldFlt' (10.0, 2...
   94557 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'luafv' (10.0, 20...
   94556 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'wcifs' (10.0, 20...
   94555 may. 08 17:38 Information Microsoft-Windows...        51046 Servicio de cliente DHCPv6 iniciado
   94554 may. 08 17:38 Information Microsoft-Windows...        50103 El cliente DHCPv4 registró una la notificación ...
   94553 may. 08 17:38 Information Microsoft-Windows...        50036 Servicio cliente DHCPv4 iniciado
   94552 may. 08 17:38 Information Microsoft-Windows...        16983 El administrador de cuentas de seguridad está r...
   94551 may. 08 17:38 Information Microsoft-Windows...        16977 El dominio está configurado con las siguientes ...
   94550 may. 08 17:38 Information Microsoft-Windows...        16962 Se están restringiendo las llamadas remotas a 1...
   94549 may. 08 17:38 Information Microsoft-Windows...           14 Configuración de Credential Guard: 0, 0
   94548 may. 08 17:38 Error       VBoxNetLwf             3221487628 El controlador detectó un error interno del con...
   94547 may. 08 17:38 Information Microsoft-Windows...           55 El procesador lógico Hyper-V 3 expone las sigui...
   94546 may. 08 17:38 Information Microsoft-Windows...           55 El procesador lógico Hyper-V 2 expone las sigui...
   94545 may. 08 17:38 Information Microsoft-Windows...           55 El procesador lógico Hyper-V 1 expone las sigui...
   94544 may. 08 17:38 Information Microsoft-Windows...           55 El procesador lógico Hyper-V 0 expone las sigui...
   94543 may. 08 17:38 Information MEIx64                 1074200578 Intel(R) Management Engine Interface driver has...
   94542 may. 08 17:38 Warning     Microsoft-Windows...         219 No se pudo cargar el controlador \Driver\WudfRd...
   94541 may. 08 17:38 Information Microsoft-Windows...        10118 El reflector UMDF no se puede conectar al Admin...
   94540 may. 08 17:38 Warning     Microsoft-Windows...         219 No se pudo cargar el controlador \Driver\WudfRd...
   94539 may. 08 17:38 Information Microsoft-Windows...        10118 El reflector UMDF no se puede conectar al Admin...
   94538 may. 08 17:38 Information Microsoft-Windows...           24 No se encontró la descripción del id. de evento...
   94537 may. 08 17:38 Information Microsoft-Windows...          172 No se encontró la descripción del id. de evento...
   94536 may. 08 17:38 Information Microsoft-Windows...           98 No se encontró la descripción del id. de evento...
   94535 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'npsvctrig' (10.0...
   94534 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'UCPD' (10.0, 205...
   94533 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'aswMonFlt' (10.0...
   94532 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'FileCrypt' (10.0...
   94531 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'aswSnx' (10.0, 2...
   94530 may. 08 17:38 Information Microsoft-Windows...            6 Filtro de sistema de archivos 'aswSP' (10.0, 20...
   94529 may. 08 17:38 Information Microsoft-Windows...           98 No se encontró la descripción del id. de evento...
```

7-

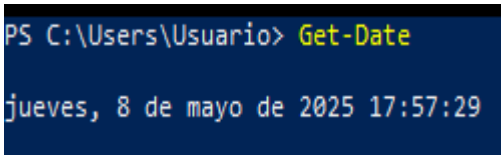
8-



9- Un archivo log es un archivo de texto donde el sistema o una aplicación registra eventos importantes, errores, accesos, etc.

Formato más común: 2025-05-08 10:32:45 ERROR: Servicio X ha fallado

10-



Es importante tener la fecha y hora del sistema de manera correcta para poder sincronizar archivos y tareas, auditorías y logs y evitar errores en certificados, servidores y redes.

LINUX:

1- Información que suministra: Usuario, PID, uso de CPU, y memoria, tiempo de ejecución, nombre del proceso.

```
usuario@ai1-pc095:~$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  0.1 167148 12088 ?        Ss   15:00   0:01 /sbin/init sp
root           2  0.0  0.0      0     0 ?        S    15:00   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    15:00   0:00 [pool_workque
root           4  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/R-rc
root           5  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/R-rc
root           6  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/R-sl
root           7  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/R-ne
root           8  0.0  0.0      0     0 ?        I    15:00   0:00 [kworker/0:0-
root           9  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/0:0H
root          10  0.0  0.0      0     0 ?        I    15:00   0:00 [kworker/0:1-
root          11  0.1  0.0      0     0 ?        I    15:00   0:00 [kworker/u8:0
root          12  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/R-mm
root          13  0.0  0.0      0     0 ?        I    15:00   0:00 [rcu_tasks_kt
root          14  0.0  0.0      0     0 ?        I    15:00   0:00 [rcu_tasks_ru
root          15  0.0  0.0      0     0 ?        I    15:00   0:00 [rcu_tasks_tr
root          16  0.0  0.0      0     0 ?        S    15:00   0:00 [ksoftirqd/0]
root          17  0.1  0.0      0     0 ?        I    15:00   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    15:00   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    15:00   0:00 [idle_inject/
root          20  0.0  0.0      0     0 ?        S    15:00   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    15:00   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    15:00   0:00 [idle_inject/
root          23  0.0  0.0      0     0 ?        S    15:00   0:00 [migration/1]
root          24  0.0  0.0      0     0 ?        S    15:00   0:00 [ksoftirqd/1]
root          25  0.0  0.0      0     0 ?        I    15:00   0:00 [kworker/1:0-
root          26  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/1:0H
root          27  0.0  0.0      0     0 ?        S    15:00   0:00 [cpuhp/2]
root          28  0.0  0.0      0     0 ?        S    15:00   0:00 [idle_inject/
root          29  0.0  0.0      0     0 ?        S    15:00   0:00 [migration/2]
root          30  0.0  0.0      0     0 ?        S    15:00   0:00 [ksoftirqd/2]
root          31  0.0  0.0      0     0 ?        I    15:00   0:00 [kworker/2:0-
root          32  0.0  0.0      0     0 ?        I<   15:00   0:00 [kworker/2:0H
root          33  0.0  0.0      0     0 ?        S    15:00   0:00 [cpuhp/3]
root          34  0.0  0.0      0     0 ?        S    15:00   0:00 [idle_inject/
root          35  0.0  0.0      0     0 ?        S    15:00   0:00 [migration/3]
root          36  0.0  0.0      0     0 ?        S    15:00   0:00 [ksoftirqd/3]
```

2-

```
usuario@ai1-pc095:~$ ps aux > procesos.txt
```

3- Datos mostrados:

User: Usuario que ejecuta el proceso

PID: Identificador de procesos

%CPU, %MEM: Uso de CPU y memoria

START: Hora de inicio

COMMAND: Nombre del programa

```
usuario@ai1-pc095:~$ gedit &
[1] 22194
usuario@ai1-pc095:~$ ps aux | grep gedit
usuario    22194  3.2  0.8 569044 67956 pts/0    Sl   15:15   0:00 gedit
usuario    22223  0.0  0.0  11716  2560 pts/0    S+   15:15   0:00 grep --color=auto gedit
usuario@ai1-pc095:~$
```

4-

```
usuario@ai1-pc095:~$ grep gedit procesos.txt
usuario@ai1-pc095:~$
```

5-

```
usuario@ai1-pc095:~$ pkill gedit
usuario@ai1-pc095:~$
```

6-

```
gersom@gersom-VirtualBox:~$ journalctl -xe
may 09 19:26:06 gersom-VirtualBox sudo[4592]:   gersom : TTY=pts/0 ; PWD=/home/gersom ; USER=root ; COMMAND=/usr/bin/jo>
may 09 19:26:06 gersom-VirtualBox sudo[4592]: pam_unix(sudo:session): session opened for user root(uid=0) by gersom(uid>
may 09 19:26:10 gersom-VirtualBox dbus-daemon[1893]: [session uid=1000 pid=1893] Activating service name='org.gnome.Dej>
may 09 19:26:10 gersom-VirtualBox dbus-daemon[1893]: [session uid=1000 pid=1893] Successfully activated service 'org.gn>
may 09 19:26:11 gersom-VirtualBox sudo[4592]: pam_unix(sudo:session): session closed for user root
may 09 19:26:13 gersom-VirtualBox dbus-daemon[1893]: [session uid=1000 pid=1893] Activating via systemd: service name='>
may 09 19:26:13 gersom-VirtualBox systemd[1861]: Starting gnome-terminal-server.service - GNOME Terminal Server...
   Subject: A start job for unit UNIT has begun execution
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

   A start job for unit UNIT has begun execution.

   The job identifier is 810.
may 09 19:26:13 gersom-VirtualBox dbus-daemon[1893]: [session uid=1000 pid=1893] Successfully activated service 'org.gn>
may 09 19:26:13 gersom-VirtualBox systemd[1861]: Started gnome-terminal-server.service - GNOME Terminal Server.
   Subject: A start job for unit UNIT has finished successfully
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

   A start job for unit UNIT has finished successfully.

   The job identifier is 810.
may 09 19:26:13 gersom-VirtualBox systemd[1861]: Started vte-spawn-8c3c6c19-e263-4e0a-96cd-f9c832730e32.scope - VTE chi>
   Subject: A start job for unit UNIT has finished successfully
   Defined-By: systemd
   Support: http://www.ubuntu.com/support

   A start job for unit UNIT has finished successfully.

   The job identifier is 837.
```

7-

```
usuario@ai1-pc095:~$ sudo reboot
```

8-

```
usuario@ai1-pc095:~$ sudo poweroff
```

9- Un archivo log es un archivo de texto donde el sistema o una aplicación registra eventos importantes, errores, accesos, etc.

Formato más común: 2025-05-08 10:32:45 ERROR: Servicio X ha fallado

10-

Es importante tener la fecha y hora del sistema de manera correcta para poder sincronizar archivos y tareas, auditorías y logs y evitar errores en certificados, servidores y redes.