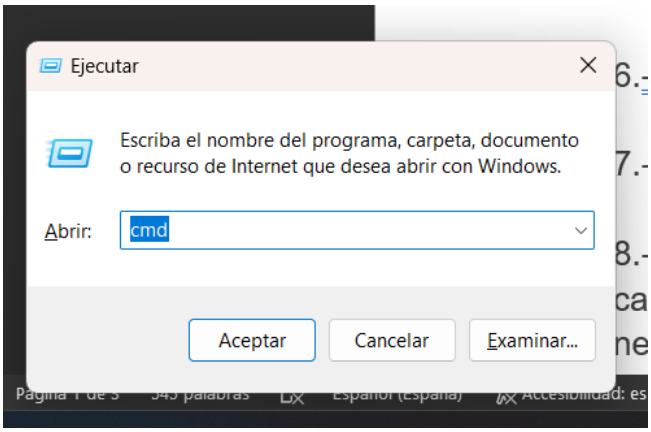
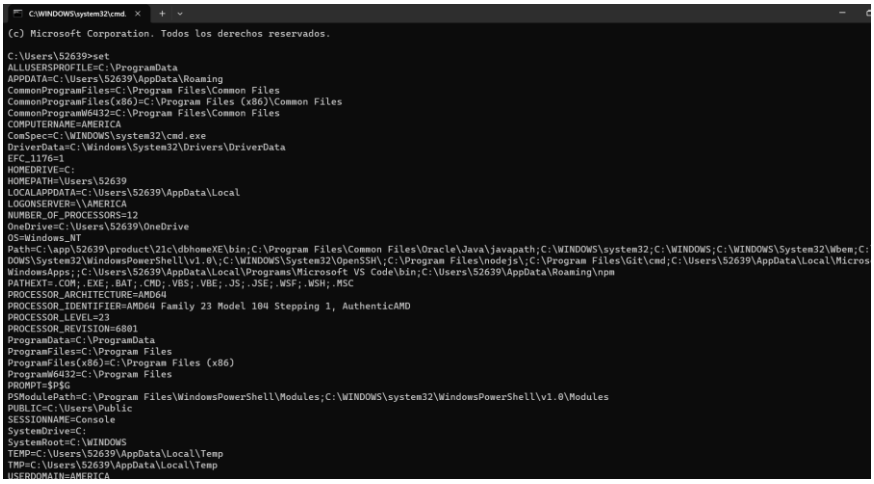
1 .- Ejecute cmd como Administrador de Sistema Operativo

Win + R - cmd



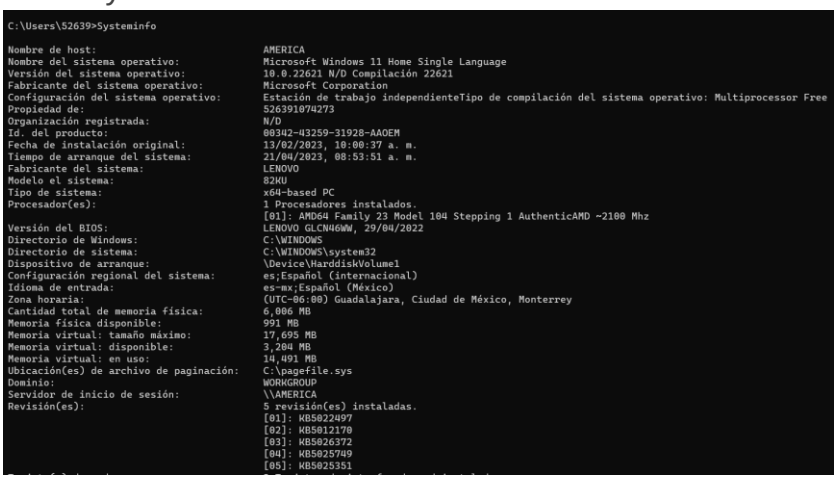
2.- Muestre las Variables del Sistema Operativo

Set



3.- Muestre la información del Sistema Operativo

Systeminfo



5.- Cambiese a c: y luego vaya a Documents

cd \ & CD %HOMEPATH%\Documents

```
C:\Users\52639\Documents>
```

6.- Obtenga el nombre de la PC

echo %COMPUTERNAME%

```
C:\>echo %COMPUTERNAME%
AMERICA
```

7.- Obtenga el nombre del usuario

echo %USERNAME%

```
C:\>echo %USERNAME%
52639
```

8.- Determine cuántas unidades de red tienes su equipo ,así mismo comparta una carpeta en el equipo del compañero y conectela en la de usted, con el comando net use

```
C:\>net use
Se registrarán las nuevas conexiones.

No hay entradas en la lista.
```

9.-Determine qué servicios están corriendo listelos y realice un bat que reinicie el servicio

net stop

net start

```
C:\>net stop "OracleServiceXE"
El servicio de OracleServiceXE está deteniéndose...
El servicio de OracleServiceXE se detuvo correctamente.


C:\>net start "OracleServiceXE"
El servicio de OracleServiceXE está iniciándose......
El servicio de OracleServiceXE se ha iniciado correctamente.
```

10.- Determine la información que tiene el usuario con el comando net user [usuario]

```
Cuentas de usuario de \\AMERICA

-------------------------------------------------------------------------------
52639                    Administrador            DefaultAccount
Invitado                 WDAGUtilityAccount
Se ha completado el comando correctamente.
```

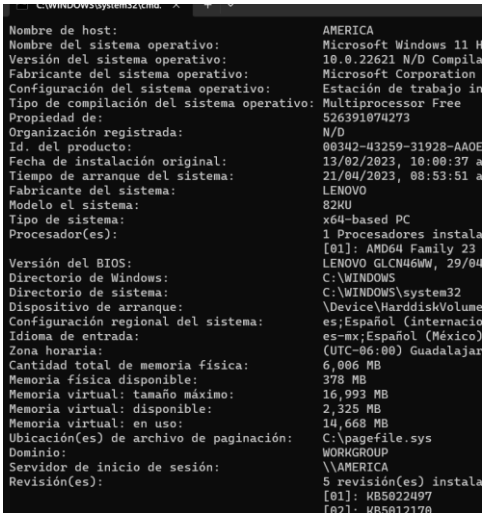
11.- Cómo leer datos de un archivo para crear “n” usuarios en mi equipo (analice)

```
$usuarios = Get-Content -Path "C:\ruta\usuarios.txt"

foreach ($usuario in $usuarios) {
    $datosUsuario = $usuario.Split(",")
    $nombreUsuario = $datosUsuario[0]
    $contrasena = $datosUsuario[1]

    $objUsuario = New-Object -TypeName
System.Management.Automation.PSCredential -ArgumentList $nombreUsuario,
(ConvertTo-SecureString -String $contrasena -AsPlainText -Force)
    New-LocalUser -Name $nombreUsuario -Password $objUsuario.Password -
PasswordNeverExpires $true
}
```

12.-Cree un archivo zip o rar que contenga todos los archivos de word y los mande a la carpeta compartida de su compañero. así mismo realice un log de cuando inicio y cuando termino la tarea esto en una tarea programada (comando at) que se ejecute a las 8:10 am

```
powershell -command "Compress-Archive -Path *.docx -DestinationPath
Ruta\Archivo.zip"

Ruta\Archivo.rar \\nombre_equipo\nombre_compartido

Tarea iniciada: [Fecha y hora actual]

Tarea finalizada: [Fecha y hora actual]

at 08:10 /interactive cmd /c "Ruta\script.bat"
```

13.-Encuentre en el systeminfo el nombre de la pc.



14.-Determine el comando que está realizando:

forfiles /S /C "cmd /c if @fsize GEQ 4000000000 echo @PATH" > salida.tx

EQU - igual NEQ - no igual LSS - menor que LEQ - menor que o igual GTR - mayor que GEQ - mayor que o igual

El comando forfiles está siendo utilizado para buscar archivos en una estructura de directorios y realizar una acción en base a ciertos criterios. A continuación, se describe el significado y uso de los parámetros y comandos adicionales presentes en el comando:

- /S: Este parámetro indica que se debe buscar en todos los subdirectorios de la ubicación especificada.

- /C: Especifica el comando que se ejecutará para cada archivo encontrado.

Dentro del comando /C, se utiliza cmd /c para ejecutar un comando de CMD.

- if @fsize GEQ 4000000000: Es una expresión condicional que verifica si el tamaño del archivo (@fsize) es mayor o igual (GEQ) a 4,000,000,000 bytes (aproximadamente 4 GB). Es decir, verifica si el tamaño del archivo es igual o superior a 4 GB.

- echo @PATH: Si la expresión condicional anterior es verdadera, se utiliza el comando echo para imprimir la ruta del archivo (@PATH).

- > salida.txt: Redirige la salida de la consola al archivo "salida.txt", es decir, el resultado de la ejecución del comando se guarda en ese archivo.

En resumen, el comando forfiles se utiliza para buscar archivos en la estructura de directorios y, en este caso, se busca archivos con un tamaño igual o superior a 4 GB. Si se encuentra un archivo que cumple ese criterio, se imprimirá su ruta en el archivo "salida.txt".

15.- Determine el espacio libre de sus unidades y mande la información a un archivo

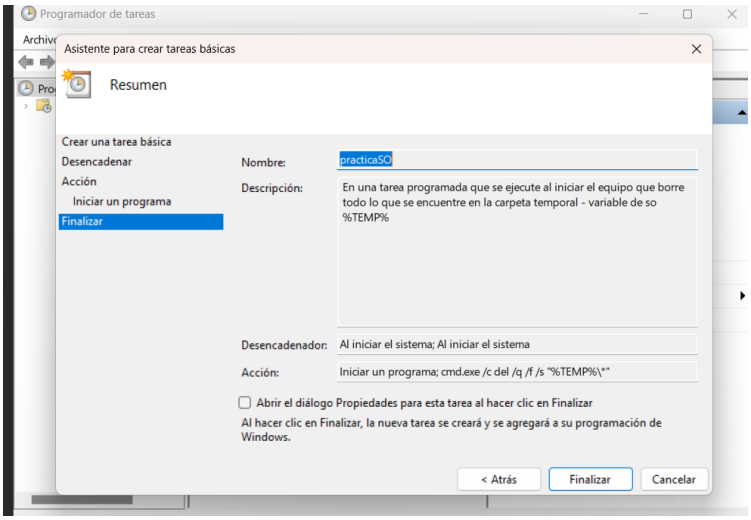
```
C:\Users\52639>wmic logicaldisk get caption, freespace > espacio_libre.txt

C:\Users\52639>type espacio_libre.txt
Caption  FreeSpace
C:       57537896448
D:       967503921152
```

16.-Busca y enlista las carpetas que contienen archivos de word

FOR /D /r %a in (*) do @if exist %a*.docx (echo %a)

```
C:\>FOR /D /r %a in (*) do @if exist %a\*.docx (echo %a)
C:\Program Files\erwin\Data Modeler r9\MetaIntegration\conf\MIRModelBridgeTemplate\SapBw
C:\Program Files\Microsoft Office\root\vfs\Windows\SHELLNEW
C:\Users\52639\AppData\Local\Temp
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\TempState
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\shared\transfers\2023_11
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\shared\transfers\2023_18
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\shared\transfers\2023_19
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\shared\transfers\2023_6
C:\Users\52639\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\shared\transfers\2023_9

C:\>
```

17.-En una tarea programada que se ejecute al iniciar el equipo que borre todo lo que se encuentre en la carpeta temporal - variable de so %TEMP%



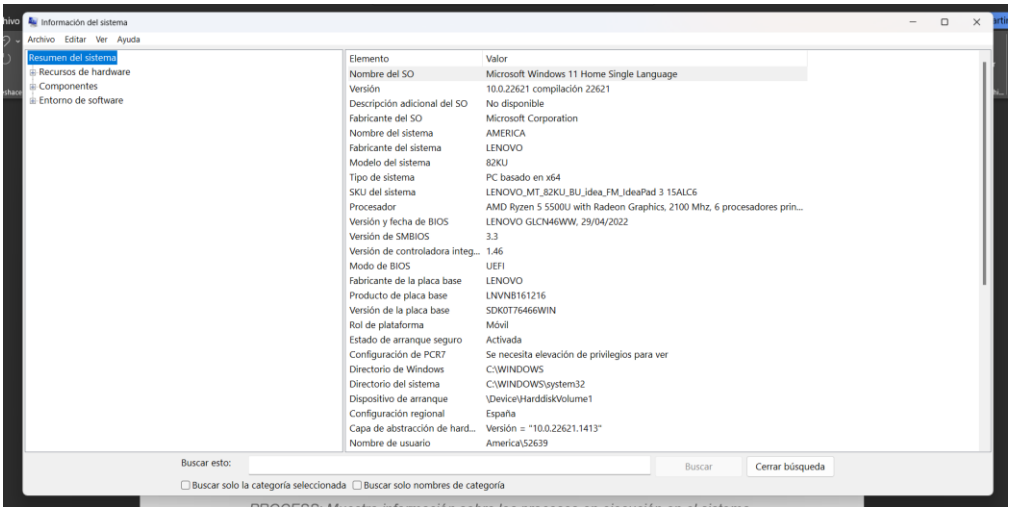
18.- investigar para que nos puede servir el comando msiexec

El comando msiexec en Windows se utiliza para ejecutar y controlar la instalación, desinstalación, reparación y administración de paquetes MSI (Windows Installer). Los paquetes MSI son archivos de instalación utilizados para distribuir aplicaciones en entornos Windows.

19.-Determine cual zona horaria tiene su maquina y cámbiela si no esta correcta tzutil.

```
C:\>tzutil /g
Central Standard Time (Mexico)_dstoff
C:\>
```

21.- Ejecutar msinfo32 y analice los datos.



22.- Determine que realiza :

QUERY { PROCESS | SESSION | TERMSERVER | USER }

El comando QUERY en Windows permite obtener información sobre procesos, sesiones, servidores de terminales y usuarios. Dependiendo del argumento utilizado después de QUERY, el comando proporcionará información específica sobre el elemento especificado. Aquí tienes una descripción de los argumentos comunes:

- PROCESS: Muestra información sobre los procesos en ejecución en el sistema. Esto incluye el ID del proceso, el nombre del proceso, el ID de sesión y el estado actual del proceso.

- SESSION: Muestra información sobre las sesiones activas en el servidor. Esto incluye el ID de sesión, el nombre de inicio de sesión del usuario, el estado de la sesión y el tipo de sesión.

- TERMSERVER: Muestra información sobre los servidores de terminales disponibles en el sistema. Esto incluye el ID de sesión del servidor de terminales, el nombre del servidor y el estado del servidor.
- USER: Muestra información sobre los usuarios que están actualmente conectados al sistema. Esto incluye el nombre de inicio de sesión del usuario, el dominio al que pertenece y la fecha y hora en que se inició la sesión.

23.-Como se debe registrar un dll en windows y donde es encuentran las dlls registradas

```
regsvr32 practicaso.dll
```

24. Tasklist y taskkill

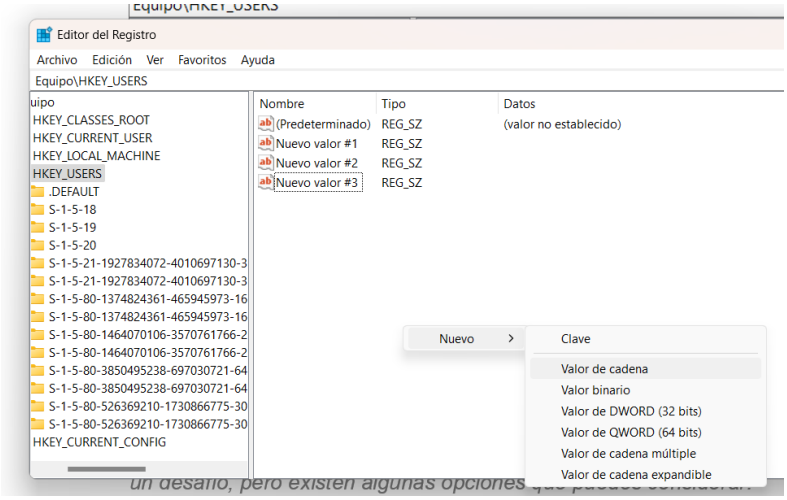
tasklist y taskkill son dos comandos útiles en Windows para administrar y finalizar procesos en la línea de comandos. Aquí te explico brevemente cómo funcionan:

1. tasklist: Este comando muestra una lista de los procesos en ejecución en el sistema, incluyendo su ID de proceso (PID), nombre de imagen, uso de memoria y otros detalles. Para utilizarlo, abre una ventana de comandos y escribe tasklist, luego presiona Enter. Obtendrás una lista de los procesos en ejecución en tu sistema.
2. taskkill: Este comando se utiliza para finalizar o cerrar procesos específicos. Puedes finalizar un proceso según su nombre o PID. El formato básico del comando es taskkill /IM <nombre de proceso> para finalizar por nombre o taskkill /PID <PID> para finalizar por ID de proceso. Por ejemplo, para finalizar el proceso "notepad.exe", puedes ejecutar taskkill /IM notepad.exe. Si conoces el PID del proceso, puedes usar taskkill /PID <PID>.

Ten en cuenta que el uso de taskkill puede ser potencialmente peligroso si se utiliza incorrectamente, ya que terminar un proceso en ejecución puede tener efectos no deseados en el sistema o en las aplicaciones en ejecución. Asegúrate de seleccionar el proceso correcto antes de finalizarlo y ten en cuenta que algunos procesos del sistema son esenciales y no se deben cerrar indiscriminadamente.

Recuerda que para ejecutar tanto tasklist como taskkill, debes tener privilegios de administrador en la cuenta de usuario utilizada en la línea de comandos.

25.- Encuentre cómo agregar una cadena a regedit de la pc y analise sus valores posibles



26.-Caso real : en todo lugar hay gente que le gusta quitar hardware de los equipos, como logra detectar ese cambio dentro de un universo de 200 equipos , para que este sea detectado automáticamente.

Detectar cambios en el hardware de 200 equipos de manera automática puede ser un desafío, pero existen algunas opciones que puedes considerar:

1. Inventariado de hardware: Realiza un inventario de hardware inicial detallado de los 200 equipos, incluyendo información como el número de serie del equipo, componentes clave, etc. Puedes utilizar herramientas de administración de activos o software de gestión de inventario para automatizar este proceso. Después de eso, configura un sistema de monitoreo que compare regularmente el inventario inicial con el estado actual de los equipos para detectar cambios.
2. Soluciones de gestión de configuración: Utiliza herramientas de gestión de configuración como Ansible, Puppet o SCCM para establecer una configuración estándar en los equipos. Estas herramientas pueden monitorear los cambios en la configuración y enviar alertas si se detecta alguna desviación. Esto puede incluir la detección de cambios en los componentes de hardware.
3. Monitoreo remoto de hardware: Considera utilizar herramientas de monitoreo remoto de hardware que proporcionen información en tiempo real sobre el estado y la configuración del hardware. Estas herramientas pueden detectar cambios físicos en los componentes del equipo, como la eliminación de hardware.
4. Etiquetas de seguimiento físico: Coloca etiquetas o sellos de seguimiento en los equipos para indicar que han sido verificados y que no deben ser modificados sin autorización. Esto puede actuar como una medida disuasoria y también ayudar a identificar rápidamente cualquier manipulación no autorizada.

5. Alertas y notificaciones automatizadas: Configura sistemas de alerta y notificación para recibir alertas en tiempo real cuando se detecte un cambio en el hardware de alguno de los equipos. Esto te permitirá tomar medidas inmediatas.

Es importante tener en cuenta que ninguna solución es infalible y es posible que se requiera una combinación de enfoques para garantizar la detección efectiva de cambios en el hardware. Además, asegúrate de contar con políticas y procedimientos claros para abordar cualquier cambio o manipulación no autorizada.