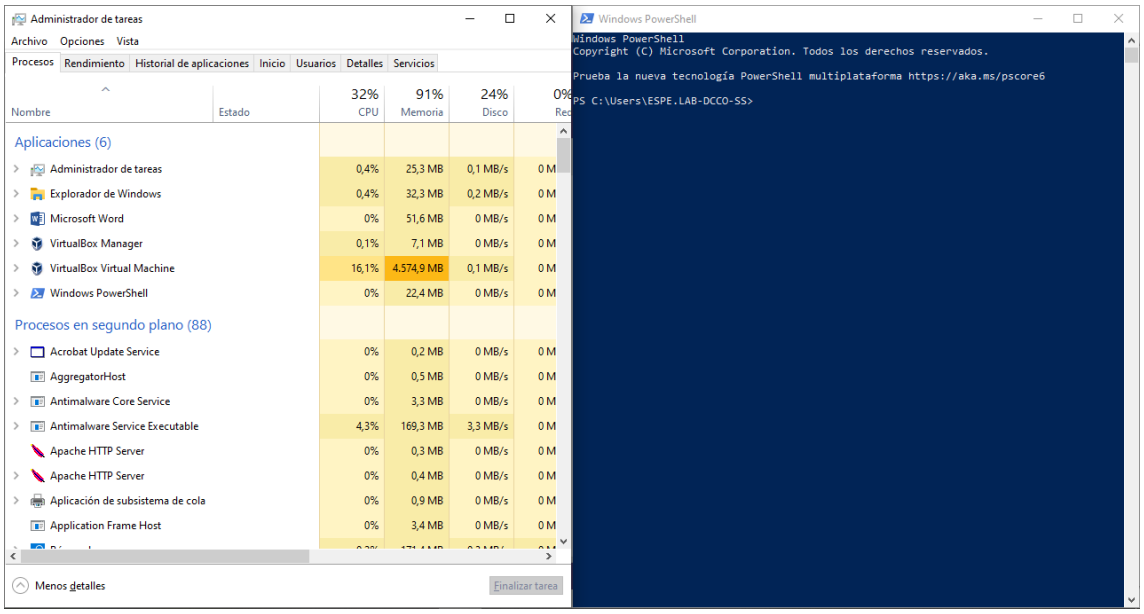
Taller #3

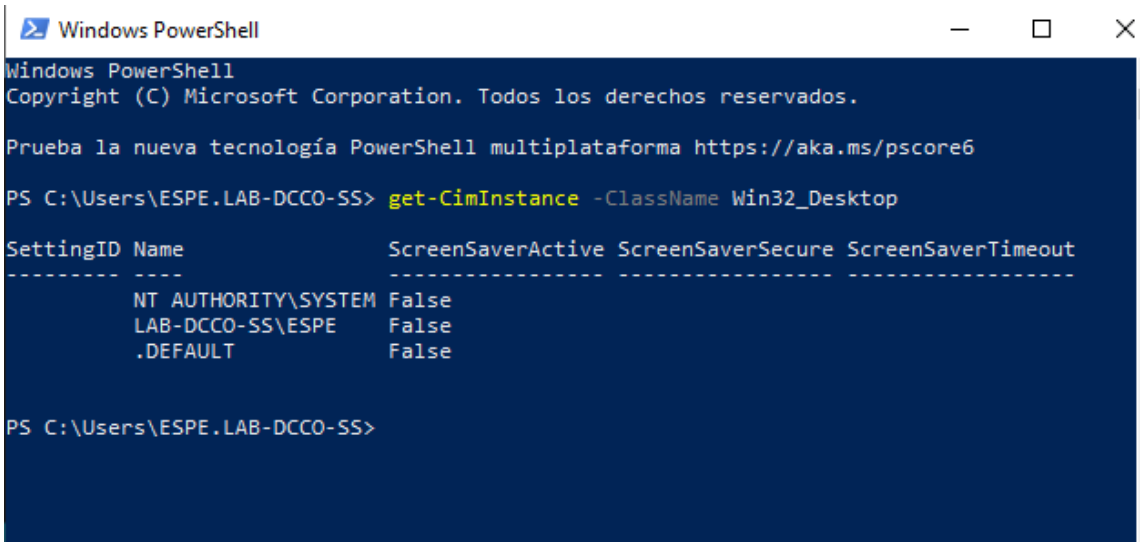
Nombre: Hugo Armijos

Fecha: 16/05/2024

Abrimos PoweShell



Obtener la configuración del escritorio



Obtener configuración Bios

```
PS C:\Users\ESPE.LAB-DCCO-SS> get-CimInstance -ClassName Win32_BIOS


SMBIOSBIOSVersion : N22 Ver. 02.17
Manufacturer      : HP
Name              : N22 Ver. 02.17
SerialNumber      : MXL70218JV
Version           : HPQOEM - 0



PS C:\Users\ESPE.LAB-DCCO-SS>
```

Obtener información del procesador

```
PS C:\Users\ESPE.LAB-DCCO-SS> get-CimInstance -ClassName Win32_PROCESSOR

DeviceID Name                                Caption                         MaxClockSpeed SocketDesignation Manufacturer
-------- ----                                -------                         ------------- ----------------- ------------
CPU0     Intel(R) Core(TM) i7-6700T CPU @ 2.80GHz Intel64 Family 6 Model 94 Stepping 3 2808          U3E1              GenuineIntel
```

Obtener procesos del equipo

Windows PowerShell

```
PS C:\Users\ESPE.LAB-DCCO-SS> Get-PROCESS

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     98       5     1412       4644                6680   0 AggregatorHost
    252      15     5876      24468       0,20  10448   1 ApplicationFrameHost
    133       8     1588       5912             4144   0 armsvc
     99       7     2900       4444             5720   0 cmd
     99       7     2896       4392             5728   0 cmd
    100       6     2616       4376             7240   0 cmd
    100       6     2620       4376             7248   0 cmd
    139       9     6548       6736             5496   0 conhost
    141       9     6540       6720             5748   0 conhost
    141       9     6548       6732             5756   0 conhost
    133       9     6560       6724             5948   0 conhost
    273      14     6416      18672       0,91  11000   1 conhost
    214      13     2740       9024             6044   0 cscript
    214      13     2756       9036             6052   0 cscript
    793      28     2072       4408              680   0 csrss
    462      20     2296       5036              772   1 csrss
    492      17     5048      20952       2,72   8240   1 ctfmon
    268      16     3844      13100       0,41   2604   1 dllhost
    199      17     3560      10604             7048   0 dllhost
   1173      40    47092      45040             1204   1 dwm
   2432      89    74608      94824      24,67   2204   1 explorer
    184      14     3676      16912       0,11  12144   1 FileCoAuth
     36       7     4592       8784              608   1 fontdrvhost
     36       5     1488       2444              704   0 fontdrvhost
    174      21     8076       7740             4068   0 httpd
    290      30    10912       7240             6632   0 httpd
     96       6     1044       4364             4100   0 ibtsiva
      0       0       60          8                0   0 Idle
    178      10     1844       8500             2804   0 igfxCUIService
    216      14     3820      13328       0,31   6040   1 igfxEM
    146       8     1344       6808             1540   0 IntelCpHDCPSvc
    143       7     1508       6552             1856   0 IntelCpHeciSvc
    424      26  2277956      11240             7272   0 java
    424      24   364404      16728             7276   0 java
    697     124    14772      17716             8548   0 klnagent
     52       6     1076       3224              924   0 LsaIso
   1711      33     9012      22576              932   0 lsass
      0       0     1224     116544             2736   0 Memory Compression
    317      22   324596      23648             4456   0 mongod
    395      18    10368      21388             3940   0 MoUsoCoreWorker
    520      17    11716      18028             8808   0 MpDefenderCoreService
    142       9     2032       7424       0,02   4040   1 msedge
```

Obtener proceso en especifico

```
PS C:\Users\ESPE.LAB-DCCO-SS> Get-PROCESS -ID 10448

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    252      15     5908      22636       0,20  10448   1 ApplicationFrameHost
```

Obtener servicios

```
PS C:\Users\ESPE.LAB-DCCO-SS> Get-SERVICE

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_c32ef       Agent Activation Runtime_c32ef
Running  AdobeARMservice    Adobe Acrobat Update Service
Stopped  AJRouter           Servicio de enrutador de AllJoyn
Stopped  ALG                Servicio de puerta de enlace de niv...
Running  Apache2.4          Apache2.4
Running  AppHostSvc         Asistente de host para aplicaciones
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
Running  AppXSvc            Servicio de implementación de AppX ...
Stopped  aspnet_state       ASP.NET State Service
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)
Running  AzureAttestService AzureAttestService
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 inteligen...
Stopped  BluetoothUserSe... Servicio de soporte técnico de usua...
Running  BrokerInfrastru... Servicio de infraestructura de tare...
Stopped  Browser            Examinador de equipos
Stopped  BTAGService        Servicio de puerta de enlace de aud...
Stopped  BthAvctpSvc        Servicio AVCTP
Stopped  bthserv            Servicio de compatibilidad con Blue...
Stopped  camsvc             Servicio Administrador de funcional...
Stopped  CaptureService_... CaptureService_c32ef
Running  cbdhsvc_c32ef      Servicio de usuario del portapapele...
Running  CDPSvc             Servicio de plataforma de dispositi...
Running  CDPUserSvc_c32ef   Servicio de usuario de plataforma d...
Stopped  CertPropSvc        Propagación de certificados
Running  ClipSVC            Servicio de licencia de cliente (Cl...
Stopped  cloudidsvc         Servicio de identidad en la nube de...
Stopped  com.docker.service Docker Desktop Service
Stopped  COMSysApp          Aplicación del sistema COM+
Stopped  ConsentUxUserSv... ConsentUX_c32ef
Running  CoreMessagingRe... CoreMessaging
```

Activar el Windows update

```
PS C:\Users\ESPE.LAB-DCCO-SS> Start-Service -Name wuauserv
PS C:\Users\ESPE.LAB-DCCO-SS>
```

Detener el Windows update

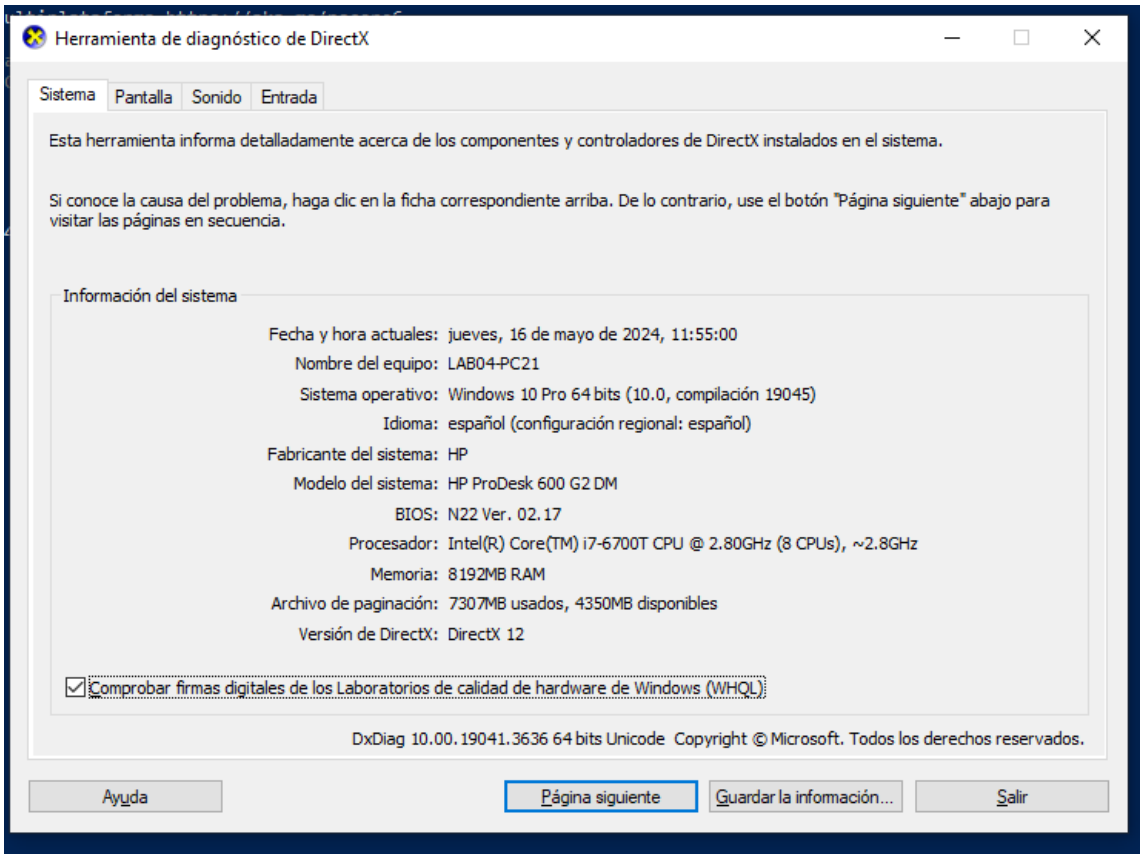
```
PS C:\Windows\system32> Stop-Service -Name wuauserv
PS C:\Windows\system32>
```

Informacion

```
PS C:\Windows\system32> get-WmiObject -Class Win32_OperatingSystem


SystemDirectory : C:\Windows\system32
Organization    :
BuildNumber     : 19045
RegisteredUser  : epcamino
SerialNumber    : 00331-20210-18697-AA343
Version         : 10.0.19045
```

Usar dxDiag en win+r para obtener info de la maquina



Test de conexión

```
PS C:\Windows\system32> Test-Connection 8.8.8.8

Source        Destination     IPV4Address      IPV6Address                              Bytes    Time(ms)
------        -----------     -----------      -----------                              -----    --------
LAB04-PC21    8.8.8.8         8.8.8.8                                                   32       78
LAB04-PC21    8.8.8.8         8.8.8.8                                                   32       78
Test-Connection : Error de prueba de conexión con el equipo '8.8.8.8': Error debido a falta de recursos
En línea: 1 Carácter: 1
+ Test-Connection 8.8.8.8
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (8.8.8.8:String) [Test-Connection], PingException
    + FullyQualifiedErrorId : TestConnectionException,Microsoft.PowerShell.Commands.TestConnectionCommand

LAB04-PC21    8.8.8.8         8.8.8.8                                                   32       78
```

Obtener info ip

```
PS C:\Windows\system32> ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 10.3.10.22
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.3.10.1

Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::e497:1f13:c654:6a52%22
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet vEthernet (Default Switch):

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::e32f:5e08:f2ee:494%37
   Dirección IPv4. . . . . . . . . . . . . . : 172.23.64.1
   Máscara de subred . . . . . . . . . . . . : 255.255.240.0
   Puerta de enlace predeterminada . . . . . :
PS C:\Windows\system32>
```

Test de conexión por IP

```
PS C:\Windows\system32> Test-Connection 10.3.10.22

Source        Destination     IPV4Address      IPV6Address                              Bytes    Time(ms)
------        -----------     -----------      -----------                              -----    --------
LAB04-PC21    10.3.10.22      192.168.56.1     fe80::e497:1f13:c654:6a52%22             32       0
LAB04-PC21    10.3.10.22      192.168.56.1     fe80::e497:1f13:c654:6a52%22             32       0
LAB04-PC21    10.3.10.22      192.168.56.1     fe80::e497:1f13:c654:6a52%22             32       0
LAB04-PC21    10.3.10.22      192.168.56.1     fe80::e497:1f13:c654:6a52%22             32       0
```

Obtener info de las cuentas

```
PS C:\Windows\system32> Get-LocalUser

Name               Enabled Description
----               ------- -----------
Administrador      False   Cuenta integrada para la administración del equipo o dominio
DefaultAccount     False   Cuenta de usuario administrada por el sistema.
ESPE               True    ESPE
Invitado           False   Cuenta integrada para el acceso como invitado al equipo o dominio
postgres           True    PostgreSQL service account
WDAGUtilityAccount False   Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.
```

Ver pagina de google html

```
PS C:\Windows\system32> Invoke-WebRequest -Uri "http://www.google.com"

StatusCode        : 200
StatusDescription : OK
Content           : <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="es-419"><head><meta
                    content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta
                    content="/images/branding/googleg/1x...
RawContent        : HTTP/1.1 200 OK
                    Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src
                    'nonce-BNcTbc6S3q995tPD_WFeOg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
                    https: ...
Forms             : {f}
Headers           : {[Content-Security-Policy-Report-Only, object-src 'none';base-uri 'self';script-src
                    'nonce-BNcTbc6S3q995tPD_WFeOg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
                    https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp], [X-XSS-Protection, 0],
                    [X-Frame-Options, SAMEORIGIN], [Cache-Control, private, max-age=0]...}
Images            : {@{innerHTML=; innerText=; outerHTML=<IMG id=hplogo style="PADDING-BOTTOM: 14px; PADDING-TOP:
                    28px; PADDING-LEFT: 0px; PADDING-RIGHT: 0px" alt=Google
                    src="/images/branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png" width=272
                    height=92>; outerText=; tagName=IMG; id=hplogo; style=PADDING-BOTTOM: 14px; PADDING-TOP: 28px;
                    PADDING-LEFT: 0px; PADDING-RIGHT: 0px; alt=Google;
                    src=/images/branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png; width=272;
                    height=92}}
InputFields       : {@{innerHTML=; innerText=; outerHTML=<INPUT type=hidden value=es-419 name=hl>; outerText=;
                    tagName=INPUT; type=hidden; value=es-419; name=hl}, @{innerHTML=; innerText=; outerHTML=<INPUT
                    type=hidden value=hp name=source>; outerText=; tagName=INPUT; type=hidden; value=hp; name=source},
                    @{innerHTML=; innerText=; outerHTML=<INPUT type=hidden name=biw>; outerText=; tagName=INPUT;
                    type=hidden; name=biw}, @{innerHTML=; innerText=; outerHTML=<INPUT type=hidden name=bih>;
                    outerText=; tagName=INPUT; type=hidden; name=bih}...}
Links             : {@{innerHTML=<SPAN class=gbtb2></SPAN><SPAN class=gbts>Búsqueda</SPAN>; innerText=Búsqueda;
                    outerHTML=<A id=gb_1 class="gbzt gbz0l gbp1" href="https://www.google.com.ec/webhp?tab=ww"><SPAN
                    class=gbtb2></SPAN><SPAN class=gbts>Búsqueda</SPAN></A>; outerText=Búsqueda; tagName=A; id=gb_1;
                    class=gbzt gbz0l gbp1; href=https://www.google.com.ec/webhp?tab=ww}, @{innerHTML=<SPAN
                    class=gbtb2></SPAN><SPAN class=gbts>Imágenes</SPAN>; innerText=Imágenes; outerHTML=<A id=gb_2
                    class=gbzt href="https://www.google.com/imghp?hl=es-419&amp;tab=wi"><SPAN class=gbtb2></SPAN><SPAN
                    class=gbts>Imágenes</SPAN></A>; outerText=Imágenes; tagName=A; id=gb_2; class=gbzt;
                    href=https://www.google.com/imghp?hl=es-419&amp;tab=wi}, @{innerHTML=<SPAN
                    class=gbtb2></SPAN><SPAN class=gbts>Maps</SPAN>; innerText=Maps; outerHTML=<A id=gb_8 class=gbzt
                    href="http://maps.google.com.ec/maps?hl=es-419&amp;tab=wl"><SPAN class=gbtb2></SPAN><SPAN
                    class=gbts>Maps</SPAN></A>; outerText=Maps; tagName=A; id=gb_8; class=gbzt;
                    href=http://maps.google.com.ec/maps?hl=es-419&amp;tab=wl}, @{innerHTML=<SPAN
                    class=gbtb2></SPAN><SPAN class=gbts>Play</SPAN>; innerText=Play; outerHTML=<A id=gb_78 class=gbzt
                    href="https://play.google.com/?hl=es-419&amp;tab=w8"><SPAN class=gbtb2></SPAN><SPAN
                    class=gbts>Play</SPAN></A>; outerText=Play; tagName=A; id=gb_78; class=gbzt;
                    href=https://play.google.com/?hl=es-419&amp;tab=w8}...}
ParsedHtml        : System.__ComObject
RawContentLength  : 53316
```

Verificar conexión con pagina

```
PS C:\Windows\system32> Test-Connection -ComputerName "facebook.com"

Source         Destination     IPV4Address      IPV6Address                              Bytes    Time(ms)
------         -----------     -----------      -----------                              -----    --------
DESKTOP-HV... facebook.com     31.13.67.35                                               32       85
DESKTOP-HV... facebook.com     31.13.67.35                                               32       84
DESKTOP-HV... facebook.com     31.13.67.35                                               32       84
DESKTOP-HV... facebook.com     31.13.67.35                                               32       93
```