Ciclo: Administración de Sistemas Informáticos en Red

Módulo: IMPLANTACIÓN DE SISTEMAS OPERATIVOS

Grupo: 1º ASIR

PR0302: Introducción a Powershell (II)

Nombre/s: Luis Eduardo Escobar Alegría

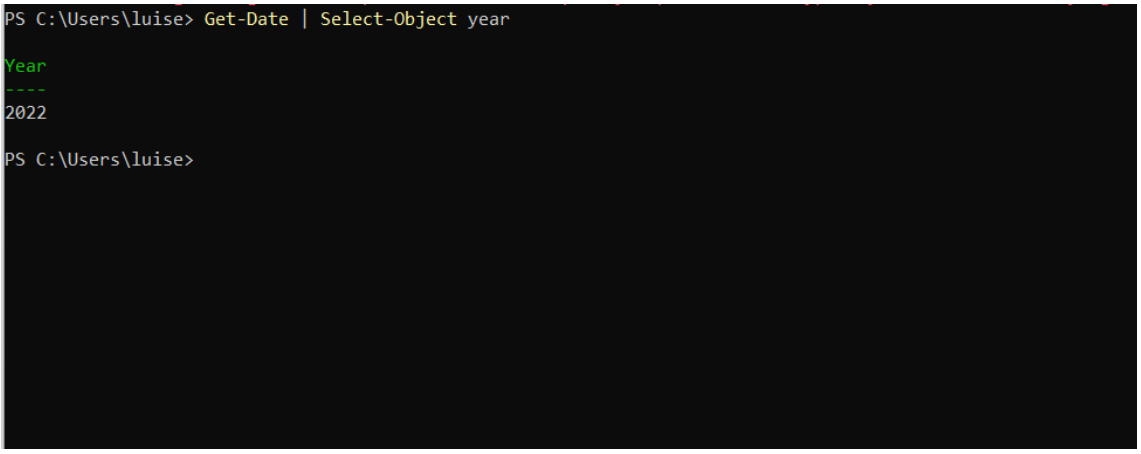
Tienes que contestar las preguntas en este mismo fichero después de cada pregunta. No te olvides de poner tu nombre en el recuadro superior.

Cuando hayas acabado todas las prácticas renombras el fichero para que se llame **{Apellido1} {Apellido2}, {Nombre} – PR0302**. En el nombre y apellidos la primera mayúscula y el resto en minúsculas. El fichero tiene que estar en formato PDF. **Cualquier fichero que no siga esta nomenclatura o no esté en PDF no será corregido**. El fichero final lo tienes que subir a la plataforma.

Ejercicio 1: Powershell

Realiza las siguientes tareas que se te piden utilizando Powershell. Para contestar lo mejor es que hagas una captura de pantalla donde se vea el comando que has introducido y las primeras líneas de la salida de este.

1.- El comando **Get-Date** muestra la fecha y hora actual. Muestra por pantalla únicamente el año en que estamos.



2.- Uno de los requisitos de Windows 11 es que es procesador tenga TPM habilitado. Powershell dispone del comando **Get-TPM** que nos muestra información sobre este módulo. Muestra por pantalla, en formato tabla, las propiedades **TpmPresent**, **TpmReady**, **TpmEnabled** y **TpmActivated**.

En los siguientes ejercicios trabajaremos con los ficheros devueltos por el comando **Get-ChildItem C:\Windows\System32**.

```
PS C:\Users\luise> Get-Tpm | Select-Object | Format-Table TpmPresent, TpmReady, TpmEnabled, TpmActivated

TpmPresent TpmReady TpmEnabled TpmActivated
---------- -------- ---------- ------------
      True     True       True         True

PS C:\Users\luise>
```

3.- Muestra por pantalla el número de ficheros y directorios que hay en ese directorio.

```
PS C:\Users\luise> Get-ChildItem  C:/Windows\System32 | Measure-Object

Count             : 4510
Average           :
Sum               :
Maximum           :
Minimum           :
StandardDeviation :
Property          :
```

4.- Los objetos devueltos por el comando anterior tienen una propiedad denominada **Extension**, que indica la extensión del archivo. Calcula el número de ficheros en el directorio que tienen la extensión **.dll**.

```
PS C:\Users\luise> Get-ChildItem * .D11 | measure

Count             : 0
Average           :
Sum               :
Maximum           :
Minimum           :
StandardDeviation :
Property          :


PS C:\Users\luise>
```

5.- Muestra los ficheros del directorio con extensión **.exe** que tengan un tamaño superior a 50000 bytes.

```
PS C:\Users\luise> Get-ChildItem  C:/Windows\System32 | Where-Object Extension -eq .exe | Where-Object Length -gt 50000

    Directory: C:\Windows\System32

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---          01/08/2022    14:30         286720 AggregatorHost.exe
-a---          05/06/2021    14:05        3231744 aitstatic.exe
-a---          01/08/2022    14:29         110592 alg.exe
-a---          01/08/2022    14:29         143360 AppHostRegistrationVerifier.exe
-a---          17/09/2022    17:22         163840 appidpolicyconverter.exe
-a---          05/06/2021    14:05          95376 ApplicationFrameHost.exe
-a---          14/10/2022    12:26        1414560 ApplyTrustOffline.exe
-a---          13/09/2021    17:33         253952 ApproveChildRequest.exe
```

6.- Muestra los ficheros de este directorio que tengan extensión **.dll**, ordenados por fecha de creación y mostrando únicamente las propiedades de fecha de creación (*CreationTime*), último acceso (*LastAccessTime*) y nombre (*Name*).

```
PS C:\Users\luise> Get-ChildItem  C:/Windows\System32 | Where-Object Extension -eq .dll | Select-Object CreationTime, LastAccessTime, Name | Sort-Object CreationTime

CreationTime        LastAccessTime      Name
------------        --------------      ----
01/02/2002 18:02:02 15/10/2022 13:14:55 msvcp140_codecvt_ids.dll
01/02/2002 18:02:02 18/10/2022 11:57:31 vcruntime140.dll
01/02/2002 18:02:02 18/10/2022 11:57:31 vcruntime140_1.dll
01/02/2002 18:02:02 15/10/2022 13:14:55 msvcp140_atomic_wait.dll
01/02/2002 18:02:02 15/10/2022 13:14:55 msvcp140_2.dll
01/02/2002 18:02:02 15/10/2022 13:14:55 msvcp140_1.dll
01/02/2002 18:02:02 18/10/2022 11:57:32 vccorlib140.dll
01/02/2002 18:02:02 16/10/2022 23:16:00 concrt140.dll
01/02/2002 18:02:02 18/10/2022 11:57:31 msvcp140.dll
02/02/2002 4:02:02  15/10/2022 13:14:54 msvcp100.dll
02/02/2002 4:02:02  17/10/2022 14:12:40 msvcr100.dll
20/02/2011 7:51:56  15/10/2022 13:14:54 atl100.dll
20/02/2011 7:51:56  15/10/2022 13:14:54 mfc100u.dll
20/02/2011 7:51:56  15/10/2022 13:14:54 mfc100.dll
20/02/2011 7:51:56  15/10/2022 13:14:54 mfcm100u.dll
20/02/2011 7:51:56  15/10/2022 13:14:54 mfcm100.dll
05/10/2013 9:58:24  15/10/2022 13:14:54 vccorlib120.dll
05/10/2013 9:58:24  18/10/2022 9:46:43  msvcr120.dll
05/10/2013 9:58:24  15/10/2022 13:14:54 msvcp120.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfc140.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfc140chs.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfc140cht.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfcm140u.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfcm140.dll
10/06/2016 8:53:14  15/10/2022 13:14:55 mfc140deu.dll
```

7.- Muestra el tamaño (*Length*) y nombre completo (*FullName*) de todos los ficheros del directorio ordenados por tamaño en sentido descendente.

```
PS C:\Windows\System32> Get-ChildItem |Select-Object Length, FullName | Sort-Object -descending

Length    FullName
------    --------
          C:\Windows\System32\0409
630784    C:\Windows\System32\RMActivate_isv.exe
524288    C:\Windows\System32\RMActivate_ssp_isv.exe
524288    C:\Windows\System32\RMActivate_ssp.exe
598016    C:\Windows\System32\RMActivate.exe
192512    C:\Windows\System32\RMapi.dll
244152    C:\Windows\System32\rmclient.dll
36864     C:\Windows\System32\RmClient.exe
126976    C:\Windows\System32\RMSRoamingSecurity.dll
147456    C:\Windows\System32\rmttpmvscmgrsvr.exe
20992     C:\Windows\System32\rnr20.dll
73728     C:\Windows\System32\RoamingSecurity.dll
200704    C:\Windows\System32\Robocopy.exe
234456    C:\Windows\System32\rometadata.dll
3468      C:\Windows\System32\rootporterr.mof
73728     C:\Windows\System32\RotMgr.dll
45056     C:\Windows\System32\ROUTE.EXE
106496    C:\Windows\System32\RpcEpMap.dll
1145480   C:\Windows\System32\RtCOM64.dll
294912    C:\Windows\System32\rstrui.exe
233472    C:\Windows\System32\RstrtMgr.dll
27616     C:\Windows\System32\RstMwEventLogMsg.dll
```

8.- Muestra el tamaño y nombre completo de todos los ficheros del directorio que tengan un tamaño superior a 10MB (10000000 bytes) ordenados por tamaño.

```
PS C:\Windows\System32> Get-ChildItem  |Select-Object Length, FullName | Where-Object Length -gt 10000000 | Sort-Object -descending @{ Expression='length'; Descending='True'}

   Length FullName
   ------ --------
147398024 C:\Windows\System32\MRT.exe
 32903496 C:\Windows\System32\WindowsCodecsRaw.dll
 27896648 C:\Windows\System32\mfxplugin64_hw.dll
 27197440 C:\Windows\System32\edgehtml.dll
 25104384 C:\Windows\System32\Hydrogen.dll
 23633920 C:\Windows\System32\mshtml.dll
 19406848 C:\Windows\System32\HolographicWorld.dll
 18898944 C:\Windows\System32\Windows.UI.Xaml.dll
 14787936 C:\Windows\System32\vmms.exe
 11744608 C:\Windows\System32\ntoskrnl.exe
 11677696 C:\Windows\System32\wmp.dll
 11052416 C:\Windows\System32\ntkrla57.exe
 10504968 C:\Windows\System32\Windows.Media.Protection.PlayReady.dll
```

9.- Muestra el tamaño y nombre completo de todos los ficheros del directorio que tengan un tamaño superior a 10MB y extensión .exe ordenados por tamaño.

```
PS C:\Windows\System32> Get-ChildItem C:\Windows\System32 | Where-Object Length -gt 10000000 | Where-Object Extension -eq .exe | Select-Object Length, FullName | Sort-Object -descending

   Length FullName
   ------ --------
147398024 C:\Windows\System32\MRT.exe
 11052416 C:\Windows\System32\ntkrla57.exe
 11744608 C:\Windows\System32\ntoskrnl.exe
 14787936 C:\Windows\System32\vmms.exe
```

Hemos visto cómo usar el comando Where-Object para filtrar objetos con propiedades de tipo texto o numérico (por ejemplo, Where-Object CPU -gt 1 o Where-Object Name -eq “Notepad”, sin embargo, hay propiedades que pueden tener otro tipo de datos. Dos de estos datos son los booleanos y los de tipo fecha.

- Las propiedades **booleanas** son las que pueden tener un valor de Verdadero o Falso, por ejemplo, la propiedad Exists del comando Get-ChildItem.

```
DirectoryName                 Property        string DirectoryName {get
Exists                        Property        bool Exists {get;}
Extension                     Property        string Extension {get;}
```

  Cuando queremos filtrar por estas propiedades y queremos poner que un valor es verdadero o falso, no podemos poner directamente True o False, ya que el sistema las interpretará como cadenas de texto en lugar de hacerlo como valores booleanos. En estos casos, es necesario utilizar dos variables del sistema que representaremos de la forma **$True** y **$False**.
- Otro tipo de propiedades muy común son las de fecha y hora, que podemos encontrar por ejemplo en la fecha de creación de un fichero.

```
PS C:\Users\victor> Get-ChildItem | Get-Member CreationTime

   TypeName: System.IO.DirectoryInfo

Name         MemberType Definition
----         ---------- ----------
CreationTime Property   datetime CreationTime {get;set;}
```

- Aquí encontramos el mismo problema que en el caso anterior ya que si ponemos la fecha directamente la interpretará como una cadena. En este caso, hay que utilizar el comando **Get-Date** con el parámetro **-date** que convierte una fecha en modo texto a un objeto de tipo datetime que almacena dicha fecha.

```
PS C:\Users\victor> get-date -date "2 de noviembre de 2021"

martes, 2 de noviembre de 2021 0:00:00
```

Pero ahora hay otro problema, ¿cómo hacemos para incluir el valor devuelto por este comando en el parámetro de otro comando? En este caso tenemos que recurrir a los paréntesis de la siguiente forma:

```
PS C:\Users\victor> Get-ChildItem | Where-Object CreationTime -gt (Get-Date -date "1 de octubre de 2021")
```

Los **paréntesis** hacen que en primer lugar se ejecute el comando que hay en su interior y, el valor devuelto por dicho comando reemplazará todo lo que hay entre paréntesis.
Hay diversas formas de indicar la fecha que se le pasa al comando Get-Date, tanto con fecha y hora como solo fecha. Algunos ejemplos son:

- “2 de noviembre de 2021 10:05:00”
- “02/11/2021”
- “02/11/21 10:10:30”
- “2021-02-11”

Teniendo en cuenta lo anterior, realiza los siguientes ejercicios:

10.- Muestra todos los procesos que tienen el estado Respond puesto a False, es decir, todos los procesos del sistema que se hayan colgado.

```
PS C:\Windows\System32> Get-Process | Where-Object Responding -eq $False

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
     61    51,69       1,48       2,19    9524   8 SystemSettings
```

11.- Muestra todos los ficheros de C:\Windows que hayan sido creados con fecha posterior al 15 de octubre.

```
PS C:\Windows\System32> Get-ChildItem C:\Windows | Where-Object CreationTime -gt "15/10/2022 01:00:00".date

    Directory: C:\Windows

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----          05/06/2021    15:16                addins
d----          04/08/2022    16:11                appcompat
d----          14/10/2022    12:31                apppatch
d----          18/10/2022    11:58                AppReadiness
d-r--          16/08/2022    16:30                assembly
d----          14/10/2022    12:31                bcastdvr
d----          05/06/2021    14:10                Boot
d----          05/06/2021    14:10                Branding
d----          14/10/2022    12:31                BrowserCore
d----          25/01/2022     3:00                ca-ES
d----          14/10/2022    12:30                CbsTemp
d----          05/06/2021    14:10                Containers
d----          05/06/2021    14:10                Cursors
d----          01/08/2022    14:01                debug
d----          05/06/2021    14:10                diagnostics
d----          01/08/2022    16:15                DiagTrack
d----          05/06/2021    15:09                DigitalLocker
d---s          05/06/2021    14:10                Downloaded Program Files
d----          08/10/2021    17:16                en-US
d----          08/10/2021    17:39                es-ES
d----          25/01/2022     3:00                eu-ES
d-r-s          01/08/2022    16:15                Fonts
d----          05/06/2021    14:10                GameBarPresenceWriter
d----          25/01/2022     3:00                gl-ES
```