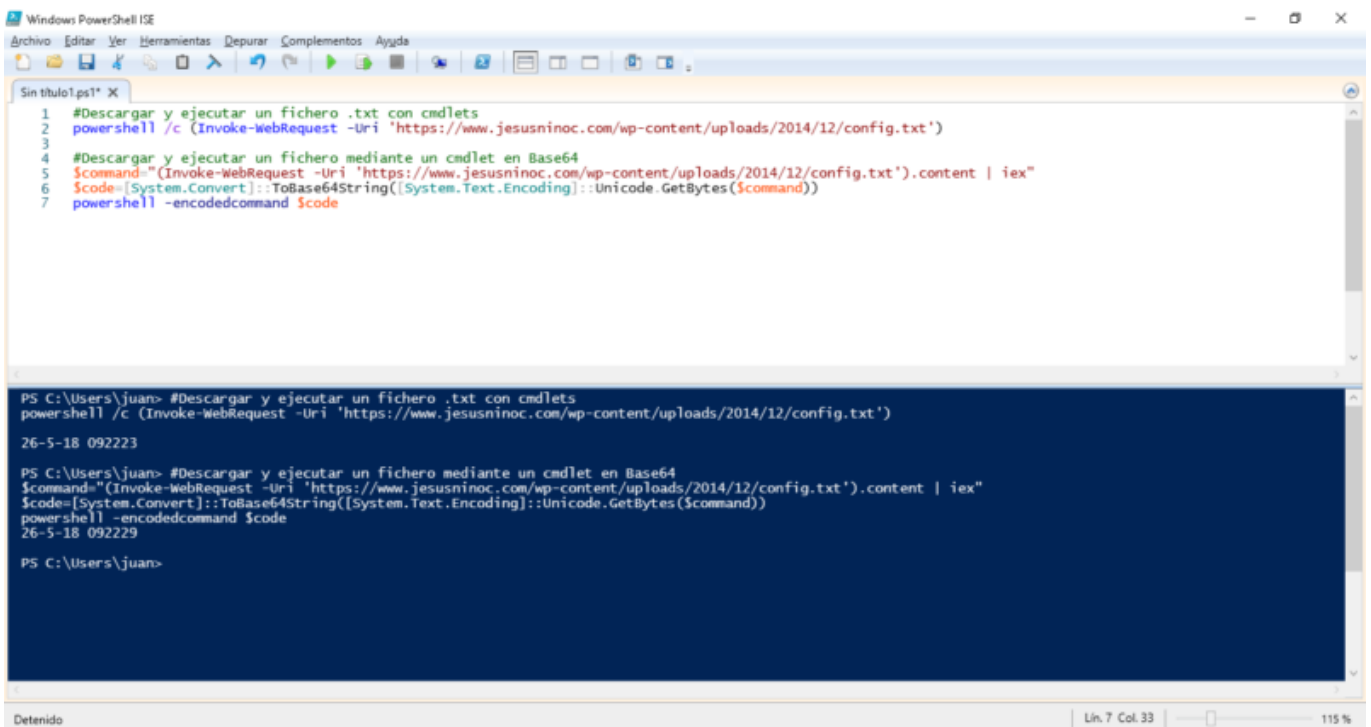


Formas de descargar y ejecutar ficheros desde un servidor en PowerShell utilizando Invoke-WebRequest

[crayon-6a9d79497d79a627395099/]



The screenshot shows a Windows PowerShell ISE window with a menu bar (Archivo, Editar, Ver, Herramientas, Depurar, Complementos, Ayuda) and a toolbar. The editor pane contains a script with two methods to download and execute a file. The console pane shows the output of the first method.

```
Sin título1.ps1 X
1 #Descargar y ejecutar un fichero .txt con cmdlets
2 powershell /c (Invoke-WebRequest -Uri 'https://www.jesusninoc.com/wp-content/uploads/2014/12/config.txt')
3
4 #Descargar y ejecutar un fichero mediante un cmdlet en Base64
5 $command="(Invoke-WebRequest -Uri 'https://www.jesusninoc.com/wp-content/uploads/2014/12/config.txt').content | iex"
6 $code=[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($command))
7 powershell -encodedcommand $code
```

```
PS C:\Users\juan> #Descargar y ejecutar un fichero .txt con cmdlets
powershell /c (Invoke-WebRequest -Uri 'https://www.jesusninoc.com/wp-content/uploads/2014/12/config.txt')
26-5-18 092223

PS C:\Users\juan> #Descargar y ejecutar un fichero mediante un cmdlet en Base64
$command="(Invoke-WebRequest -Uri 'https://www.jesusninoc.com/wp-content/uploads/2014/12/config.txt').content | iex"
$code=[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($command))
powershell -encodedcommand $code
26-5-18 092229

PS C:\Users\juan>
```

Detenido | Lin. 7 Col. 33 | 115 %