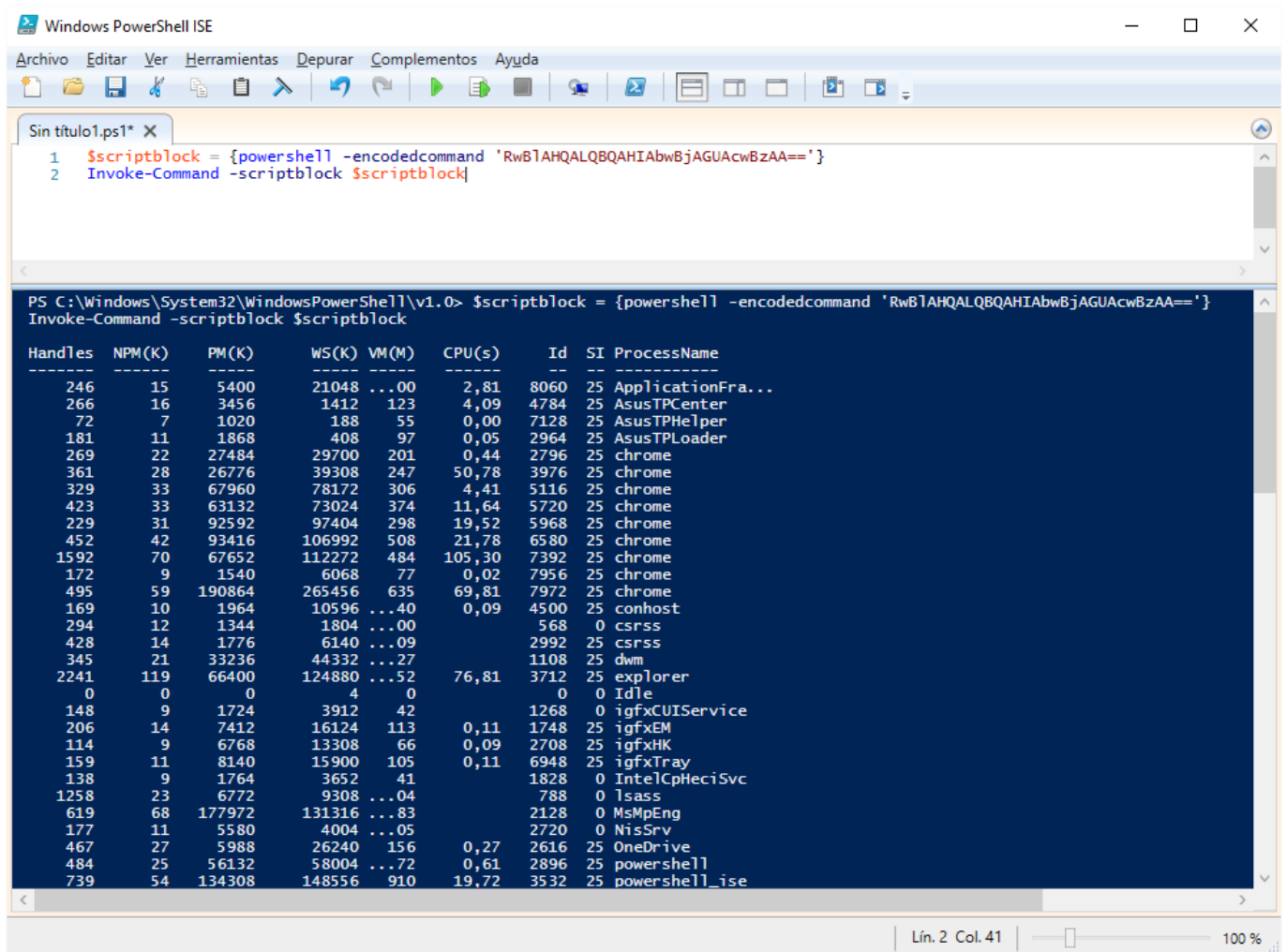


Invocar expresiones con cmdlets codificados en Base64 (Invoke-Command)

[crayon-6a9d829e23521700676436/]



The screenshot shows the Windows PowerShell ISE interface. The script editor at the top contains two lines of code:

```
1 $scriptblock = {powershell -encodedcommand 'RwB1AHQALQBQAHIAbwBjAGUAcwBzAA=='}  
2 Invoke-Command -scriptblock $scriptblock
```

The console window below shows the execution of the script. The command prompt is `PS C:\Windows\System32\WindowsPowerShell\v1.0>`. The output is a table of system processes:

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	SI	ProcessName
246	15	5400	21048	...00	2,81	8060	25	ApplicationFra...
266	16	3456	1412	123	4,09	4784	25	AsusTPCenter
72	7	1020	188	55	0,00	7128	25	AsusTPHelper
181	11	1868	408	97	0,05	2964	25	AsusTPLoader
269	22	27484	29700	201	0,44	2796	25	chrome
361	28	26776	39308	247	50,78	3976	25	chrome
329	33	67960	78172	306	4,41	5116	25	chrome
423	33	63132	73024	374	11,64	5720	25	chrome
229	31	92592	97404	298	19,52	5968	25	chrome
452	42	93416	106992	508	21,78	6580	25	chrome
1592	70	67652	112272	484	105,30	7392	25	chrome
172	9	1540	6068	77	0,02	7956	25	chrome
495	59	190864	265456	635	69,81	7972	25	chrome
169	10	1964	10596	...40	0,09	4500	25	conhost
294	12	1344	1804	...00		568	0	csrss
428	14	1776	6140	...09		2992	25	csrss
345	21	33236	44332	...27		1108	25	dwm
2241	119	66400	124880	...52	76,81	3712	25	explorer
0	0	0	4	0		0	0	Idle
148	9	1724	3912	42		1268	0	igfxCUIService
206	14	7412	16124	113	0,11	1748	25	igfxEM
114	9	6768	13308	66	0,09	2708	25	igfxHK
159	11	8140	15900	105	0,11	6948	25	igfxTray
138	9	1764	3652	41		1828	0	IntelCpHeciSvc
1258	23	6772	9308	...04		788	0	lsass
619	68	177972	131316	...83		2128	0	MsMpEng
177	11	5580	4004	...05		2720	0	NisSrv
467	27	5988	26240	156	0,27	2616	25	OneDrive
484	25	56132	58004	...72	0,61	2896	25	powershell
739	54	134308	148556	910	19,72	3532	25	powershell_ise