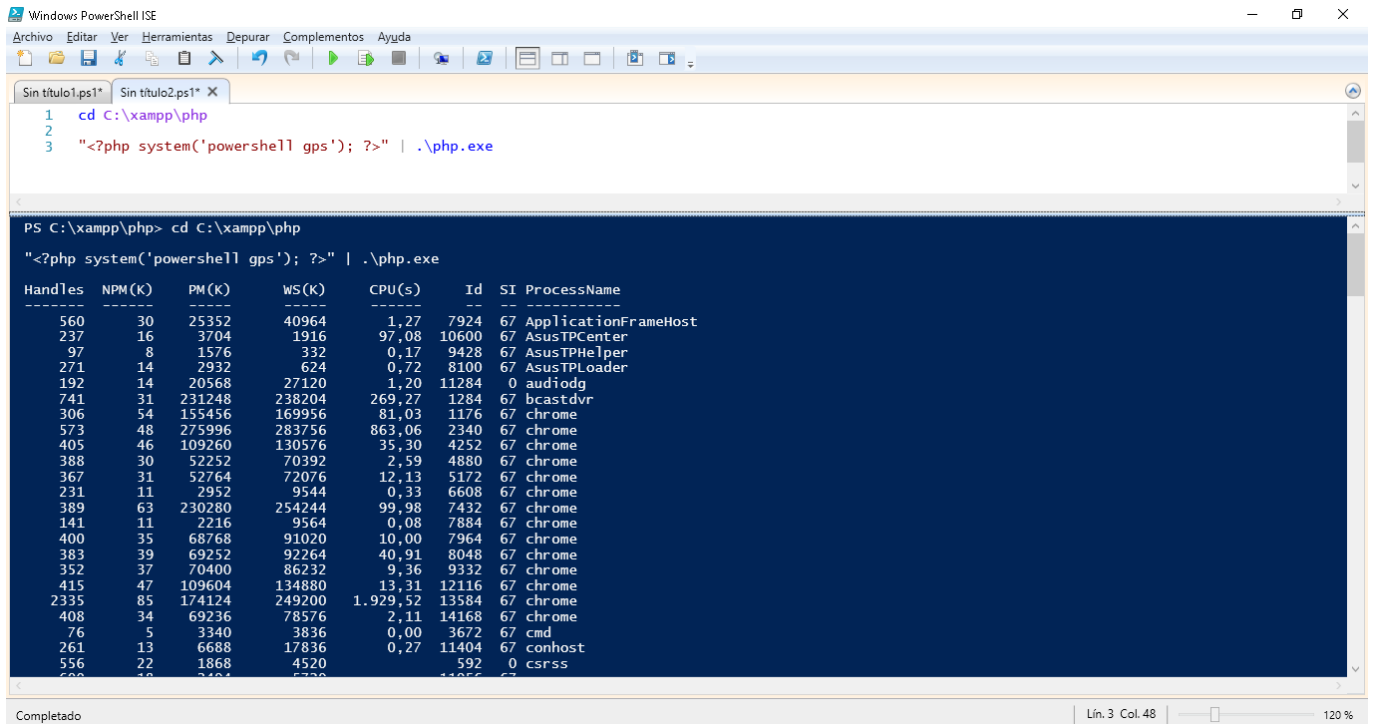


Ejecutar en PHP un cmdlet de PowerShell en Base64

[crayon-6a9d4e577611f432751710/]



The screenshot shows the Windows PowerShell ISE interface. The editor has two tabs: 'Sin título1.ps1*' and 'Sin título2.ps1* X'. The active tab 'Sin título2.ps1*' contains the following code:

```
1 cd C:\xampp\php
2
3 "<?php system('powershell gps'); ?>" | .\php.exe
```

The console output shows the command being executed and the resulting process list:

```
PS C:\xampp\php> cd C:\xampp\php
"<?php system('powershell gps'); ?>" | .\php.exe
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
560	30	25352	40964	1,27	7924	67	ApplicationFrameHost
237	16	3704	1916	97,08	10600	67	AsusTPCenter
97	8	1576	332	0,17	9428	67	AsusTPHelper
271	14	2932	624	0,72	8100	67	AsusTPLoader
192	14	20568	27120	1,20	11284	0	audiodg
741	31	231248	238204	269,27	1284	67	bcastdvr
306	54	155456	169956	81,03	1176	67	chrome
573	48	275996	283756	863,06	2340	67	chrome
405	46	109260	130576	35,30	4252	67	chrome
388	30	52252	70392	2,59	4880	67	chrome
367	31	52764	72076	12,13	5172	67	chrome
231	11	2952	9544	0,33	6608	67	chrome
389	63	230280	254244	99,98	7432	67	chrome
141	11	2216	9564	0,08	7884	67	chrome
400	35	68768	91020	10,00	7964	67	chrome
383	39	69252	92264	40,91	8048	67	chrome
352	37	70400	86232	9,36	9332	67	chrome
415	47	109604	134880	13,31	12116	67	chrome
2335	85	174124	249200	1.929,52	13584	67	chrome
408	34	69236	78576	2,11	14168	67	chrome
76	5	3340	3836	0,00	3672	67	cmd
261	13	6688	17836	0,27	11404	67	conhost
556	22	1868	4520		592	0	csrss
688	18	2484	5728		11856	67	

The status bar at the bottom indicates 'Completado' (Completed) and 'Lin. 3 Col. 48'.