Windows Monitoring & Diagnostics Cheatsheet

> **Tema:** Monitoreo de recursos, diagnóstico técnico y herramientas avanzadas en Windows **Incluye:** Tabla resumen, kit de diagnóstico ideal y comandos de terminal (PowerShell + WSL)

Introducción

Windows ofrece un poderoso ecosistema de herramientas para:

- Diagnosticar fallos de aplicaciones
- Identificar cuellos de botella de CPU, RAM, disco y red
- Revisar eventos y errores del sistema
- Analizar comportamientos sospechosos o malware
- Monitorear hardware y rendimiento

Este cheatsheet resume las mejores herramientas —gráficas, terminal y Sysinternals— para que trabajes como un **técnico profesional**.

Tabla Resumen de Herramientas de Monitoreo

Herramienta	Tipo	Nivel	Qué monitorea	Cuándo usar
Task Manager	GUI	Básico	CPU, RAM, GPU, disco	Diagnósticos rápidos
Resource Monitor	GUI	Intermedio	RAM, disco, red por proceso	Cuellos de botella
Performance Monitor (PerfMon)	GUI	Avanzado	Métricas profundas, logging	Análisis profesional
Event Viewer	GUI	Avanzado	Logs del sistema	Crash debugging
Reliability Monitor	GUI	Básico	Historial de fallos	Ver “cuándo empezó”
Windows Memory Diagnostic	GUI/Boot	Medio	Pruebas de RAM	SOS de hardware
Sysinternals Process Explorer	GUI	Avanzado	Procesos, DLL, hilos	Malware / debugging
Sysinternals ProcMon	GUI	Experto	Syscalls, registros, archivos	Apps que fallan
TCPView	GUI	Intermedio	Puertos y conexiones	Actividad de red

Herramienta	Tipo	Nivel	Qué monitorea	Cuándo usar
Autoruns	GUI	Avanzado	Inicio del sistema	Optimización / malware
CrystalDiskInfo	GUI	Medio	S.M.A.R.T. del disco	Diagnóstico de HDD/SSD
HWiNFO	GUI	Avanzado	Sensores y temperaturas	Sobrecalentamiento

🧰 Kit de Diagnóstico Ideal para Técnicos

Un set diseñado para técnicos, programadores y soporte profesional.

🔹 Diagnóstico de rendimiento

- **Task Manager**
- **Resource Monitor**
- **Performance Monitor (PerfMon)**

Ideal para: ✔ Lentitud general ✔ Cuellos de disco ✔ Altos consumos de CPU

🔹 Diagnóstico profundo de procesos

- **Process Explorer**
- **Process Monitor (ProcMon)**

Para: ✔ Malware ✔ Procesos ocultos ✔ Apps que se cierran sin error

🔹 Diagnóstico de red

- **TCPView**
- **PowerShell:** `Get-NetTCPConnection`

Usos: ✔ Chequear puertos abiertos ✔ Ver tráfico sospechoso ✔ Determinar qué aplicación usa la red

🔹 Diagnóstico de disco

- **CrystalDiskInfo**
- **PowerShell:** `Get-PhysicalDisk`, `Get-Volume`
- **CHKDSK**

Usos: ✔ Ver salud del disco ✔ S.M.A.R.T. ✔ Latencias de disco que causan cuelgues

🔹 Diagnóstico de memoria

- **memtest86** (el mejor)
- **Windows Memory Diagnostic**

Usos: ✔ Pantallazos azules ✔ Cuelgues aleatorios ✔ Archivos corruptos

---

🔹 Arranque y malware

- **Autoruns**
- **Process Explorer**
- **Defender Offline Scan**

Para: ✔ PC muy lenta al iniciar ✔ Eliminación de malware persistente

---

🔹 Sysinternals Toolkit (Obligatorio)

Kit portátil de Microsoft:

- Process Explorer
- ProcMon
- Autoruns
- TCPView
- PsTools
- DiskTools

Más de 60 herramientas profesionales, sin instalación.

🔧 PowerShell & Terminal para Monitorear Windows

> 💡 **PowerShell es el estándar profesional** para automatizar diagnósticos. 💡 WSL es útil para desarrollo, pero **no monitorea el kernel de Windows**, por lo que sirve sólo para scripts, no para métricas del sistema.

💻 PowerShell — Comandos útiles

🔹 CPU – procesos que más consumen

```
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10
```

🔹 RAM – procesos pesados

```
Get-Process | Sort-Object WorkingSet -Descending | Select-Object -First 10
```

🔹 Disco – info del hardware

```
Get-Disk
Get-PhysicalDisk
Get-Volume
```

🔹 Red – conexiones activas por proceso

```
Get-NetTCPConnection | Select-Object LocalAddress,LocalPort,RemoteAddress,State
```

🔹 Información general del sistema

```
Get-ComputerInfo
```

🔹 Últimos 50 errores del sistema

```
Get-EventLog -LogName System -Newest 50
```

 PerfMon desde PowerShell

Captura datos de rendimiento igual que Performance Monitor pero desde consola:

```
Get-Counter '\Processor(_Total)\% Processor Time'
```

Crear un log automático en CSV:

```
logman create counter MyCPUlog -c "\Processor(_Total)\% Processor Time" -f csv -o
"cpu_log.csv"
```

🐧 WSL – Herramientas útiles (solo para entorno Linux)

> ⚠ **WSL no puede monitorear Windows**, pero te sirve para herramientas Linux adicionales.

- `htop` – monitor de procesos
- `iotop` – uso de disco
- `iftop` – uso de red
- `dstat` – rendimiento general

🎯 Conclusión

✔ Windows tiene herramientas muy potentes para diagnóstico avanzado ✔ PowerShell es la vía profesional para automatizar análisis ✔ Sysinternals es el kit esencial de cualquier técnico ✔ WSL sirve para scripting, pero no para monitorear Windows

---