

266 - WINDOWS

Quién intenta entrar en tu PC: Visor de eventos

Aprende a revisar los registros de Windows para ver inicios de sesión fallidos, como hace un auditor de seguridad.



NIVEL
Medio

TIEMPO
20 min

CATEGORÍA
Windows

WEB
soporteinformatico360.com

Windows apunta en un registro cada vez que alguien inicia sesión o falla la contraseña. Mirar ese registro de vez en cuando te ayuda a detectar intentos raros en tu propio equipo, igual que hacen los equipos de seguridad.

■ Qué necesitas

- ✓ Tu PC con Windows 11
- ✓ Una cuenta de administrador
- ✓ Unos minutos sin prisa
- ✓ Papel o un archivo para anotar lo que veas

■ Paso a paso

01

Abre el Visor de eventos

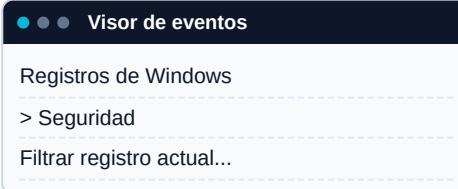
Pulsa Win + R, escribe eventvwr.msc y pulsa Intro. Acepta el aviso de permisos si aparece.

Win + R

02

Ve al registro de Seguridad

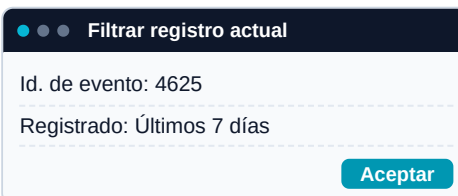
En el panel izquierdo abre Registros de Windows y haz clic en Seguridad. Ahí están los inicios de sesión.



03

Filtra los intentos fallidos

Pulsa Filtrar registro actual y escribe 4625 en el campo de ID de evento. Cada resultado es una contraseña equivocada.



04

Míralo también por comandos

Abre Terminal como administrador y lista los últimos fallos. El 4624 muestra los inicios correctos.

Terminal

```
$ Get-WinEvent -FilterHashtable @{LogName='Security';Id=4625} -MaxEvents 10  
$ █
```

05

Interpreta lo que ves

Un fallo suelto suele ser un despiste tuyo. Muchos seguidos, de madrugada o desde otra IP de tu red, merecen revisión.

06

Comprueba el bloqueo de cuenta

Escribe net accounts para ver tras cuántos intentos fallidos se bloquea la cuenta. Un valor de 10 o menos es razonable.

Terminal

```
$ net accounts  
$ █
```

■ Consejos

CONSEJO 1

Revisa el registro una vez al mes y anota si algo cambia.

CONSEJO 2

Usa contraseñas largas o PIN con Windows Hello para frenar intentos.

CONSEJO 3

Si ves muchos fallos que no son tuyos, cambia la contraseña y pide ayuda a un técnico.



Importante: Practica solo en tus propios equipos o con permiso del dueño. Acceder o intentar acceder a sistemas ajenos sin permiso es delito. No borres el registro de Seguridad: es la prueba si algo pasa.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112