

294 - MAC

Qué escucha y se conecta en tu Mac: audítalo con lsof

Aprende a ver los puertos abiertos y las conexiones de tu propio Mac para detectar servicios que sobran o apps sospechosas.



NIVEL
Medio

TIEMPO
25 min

CATEGORÍA
Mac

WEB
soporteinformatico360.com

Cada servicio que escucha en un puerto es una puerta que alguien podría tocar. Con la Terminal de tu Mac puedes ver qué puertas hay abiertas y qué apps hablan con Internet. Es la primera revisión que haría un auditor de seguridad.

■ Qué necesitas

- ✓ Un Mac con macOS actualizado
- ✓ La app Terminal (en Aplicaciones > Utilidades)
- ✓ Tu contraseña de administrador
- ✓ Hacerlo solo en tu propio equipo

■ Paso a paso

01

Abre la Terminal

Pulsa Cmd + Espacio, escribe «Terminal» y pulsa Intro.

Cmd + Espacio

02

Mira qué puertos escuchan

Este comando lista los programas que esperan conexiones TCP. Fíjate en la columna COMMAND y en el número de puerto tras los dos puntos.

```
Terminal
$ sudo lsof -iTCP -sTCP:LISTEN -n -
P
$
```

03

Distingue local de abierto

Si pone 127.0.0.1 o [::1], solo escucha dentro del Mac. Si pone un asterisco (*), acepta conexiones desde la red y merece más atención.

04

Revisa las conexiones activas

Este otro comando muestra con quién habla cada app ahora mismo. Pulsa Ctrl + C para salir de nettop.

```
Terminal
$ lsof -i -n -P | grep ESTABLISHED
$ nettop -m tcp
$
```

05

Apaga lo que no uses

En Ajustes del Sistema, General, Compartir, desactiva servicios que no necesites, como Compartir pantalla o Sesión remota.

```
Ajustes del Sistema
General > Compartir
Compartir pantalla: desactivado
Sesión remota: desactivado
```

06

Investiga lo que no conozcas

Si un nombre te resulta raro, búscalo en Monitor de Actividad, pestaña Red. Si no sabes qué es, no lo borres a ciegas: consúltalo antes.



■ Consejos

CONSEJO 1

Anota el resultado de hoy para compararlo dentro de unas semanas.

CONSEJO 2

Mantén activado el cortafuegos de macOS para bloquear conexiones entrantes no deseadas.

CONSEJO 3

Repite la revisión tras instalar apps nuevas o de origen poco conocido.



Importante: Usa estas técnicas solo en tus propios equipos o con permiso por escrito: auditar o atacar sistemas ajenos sin autorización es delito. Si encuentras algo que no sabes explicar, pide ayuda a un técnico antes de tocar nada.

¿Prefieres que lo hagamos por ti?

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

910 117 112

soporte@soporteinformatico360.com
soporteinformatico360.com