Detectar apps nocivas en el teléfono

Un teléfono con una app maliciosa avisa: se calienta sin usarlo, la batería no dura, los datos se acaban solos y aparecen anuncios donde no debería haberlos. Esta guía enseña a revisar el comportamiento del equipo y a encontrar la app responsable.

Señales de alerta

- La batería se agota mucho más rápido que antes, sin cambiar de uso.
- El teléfono se calienta estando en reposo o con la pantalla apagada.
- Los datos móviles se disparan aunque no veas videos ni descargues nada.
- Aparecen anuncios en la pantalla de inicio o fuera de las apps.
- Hay aplicaciones instaladas que no recuerdas haber instalado.
- El teléfono se pone lento de repente o se reinicia solo.
- Una app pide permisos que no tienen sentido (una linterna pidiendo tus contactos).

Revisión paso a paso

1. **Revisa las apps instaladas**
   Ajustes → Aplicaciones. Recorre la lista completa. Si ves una app que no conoces o que no recuerdas instalar, anota su nombre: es la primera sospechosa.

2. **Revisa la batería por app**
   Ajustes → Batería → Uso de la batería. La app que más gasta sin que la uses es sospechosa: una app maliciosa trabaja en segundo plano todo el día.

3. **Revisa los datos por app**
   Ajustes → Conexiones → Uso de datos → Uso de datos móviles. Una app que consume muchos datos sin abrirla puede estar enviando información.

Revisión paso a paso (continuación)

4. **Pasa Play Protect**
   Abre Play Store → tu perfil → Play Protect → Analizar. Es el escáner de Google: marca las apps dañinas que conoce.

5. **Revisa los administradores del dispositivo**
   Ajustes → Seguridad → Administradores del dispositivo. Una app nociva se pone ahí para que no la puedas desinstalar. Si hay una app rara activada, desactívala primero.

6. **Prueba el modo seguro**
   Mantén Encendido, mantén pulsado «Apagar» y elige «Reiniciar en modo seguro». En modo seguro solo corren las apps del sistema: si el problema desaparece, la culpable es una app que instalaste.

Limpieza

Desinstala la app sospechosa desde Ajustes → Aplicaciones. Si no te deja desinstalarla, quítale primero el permiso de administrador del dispositivo (paso 5) y luego desinstálala. Borra también su caché y sus datos. Si el problema persiste después de quitarla, haz respaldo y restablece el equipo de fábrica: es la única forma segura de sacar una app que se esconde en el sistema.

Prevención

- Instala apps solo de Play Store o de fuentes oficiales del fabricante.
- No instales APK que lleguen por WhatsApp, Telegram o enlaces de internet.
- Revisa los permisos antes de aceptar: una app debe pedir solo lo que necesita para funcionar.
- Mantén el sistema y las apps actualizados, y Play Protect activado.

> **Advertencia**
> Un antivirus no sustituye la revisión: muchas apps nocivas no son virus, son apps normales con permisos abusivos o con publicidad escondida. El mejor detector es revisar el comportamiento del equipo y los permisos de cada app.