

# Seguridad en Móvil Android

Samsung, Xiaomi, Pixel, Motorola...: el móvil es tu diario, ciérralo bien

En el móvil llevamos fotos, conversaciones, ubicación y todas las cuentas abiertas. Además, el acceso físico al móvil es la vía más común de control en pareja y de instalación de apps espía (stalkerware). Los nombres de los menús cambian un poco según la marca; si no encuentras algo, usa la lupa de búsqueda dentro de Ajustes.

¿Dónde están los ajustes? Ajustes (rueda dentada) — usa el buscador de Ajustes si un menú no aparece igual en tu marca. Los nombres pueden variar un poco según la versión de la app o del móvil.

## 10 medidas, paso a paso

### 1 Pon un bloqueo de pantalla de verdad

**Ruta:** Ajustes → Seguridad y privacidad (o Pantalla de bloqueo) → Bloqueo de pantalla → PIN de 6 cifras o contraseña.

Evita el patrón: se adivina mirando las marcas de los dedos en la pantalla. Cambia el código si alguien lo conoce.

### 2 Activa la Protección antirrobo

**Ruta:** Ajustes → Google → Todos los servicios → Protección antirrobo.

Activa «Bloqueo antirrobo» (bloquea el móvil si te lo arrancan de la mano) y «Bloqueo de dispositivos sin conexión».

### 3 Activa «Encontrar mi dispositivo»

**Ruta:** Ajustes → Google → Todos los servicios → Encontrar mi dispositivo.

Si lo pierdes, entra desde cualquier ordenador en [android.com/find](https://android.com/find) para localizarlo, bloquearlo o borrarlo.

### 4 Activa el bloqueo remoto

**Ruta:** Ajustes → Google → Todos los servicios → Protección antirrobo → Bloqueo remoto.

Te permite bloquear el móvil solo con tu número de teléfono desde [android.com/lock](https://android.com/lock).

### 5 Revisa qué apps tienen tus permisos

**Ruta:** Ajustes → Seguridad y privacidad → Privacidad → Gestor de permisos.

Mira quién usa tu Ubicación, Micrófono, Cámara y SMS. Quitá el permiso a cualquier app que no lo necesite.

## 6 Busca apps espía

**Ruta:** Ajustes → Aplicaciones → Ver todas. Y también: Ajustes → Seguridad → Apps de administración de dispositivos y Ajustes → Accesibilidad.

Desconfía de apps con nombres genéricos («System Service», «Sync», «Wi-Fi»), sin icono, o que tengan permisos de accesibilidad o administración sin que tú se los dieras.

## 7 Mantén activado Play Protect

**Ruta:** Abre Google Play → toca tu foto → Play Protect → rueda dentada → activa «Analizar apps con Play Protect».

Pulsa «Analizar» de vez en cuando. Avisa de apps dañinas, incluidas muchas de espionaje.

## 8 No instales apps fuera de Google Play

**Ruta:** Ajustes → Aplicaciones → Acceso especial → Instalar apps desconocidas → desactiva todas.

Las apps espía suelen instalarse así, desde un archivo .apk.

## 9 Oculta el contenido de las notificaciones

**Ruta:** Ajustes → Notificaciones → Notificaciones en pantalla de bloqueo → «Mostrar solo notificaciones sin contenido sensible» o «No mostrar».

Evita que alguien lea tus mensajes con el móvil bloqueado encima de la mesa.

## 10 Mantén el móvil actualizado

**Ruta:** Ajustes → Sistema → Actualización de software (o «Actualización del sistema»).

Las actualizaciones cierran fallos que se usan para espiar.

## Señales de alarma

- La batería se gasta mucho más rápido o el móvil se calienta sin usarlo.
- Alguien sabe dónde has estado o qué has hablado sin que se lo hayas contado.
- Ves una app que no recuerdas haber instalado. Antes de borrarla, si sospechas de control o espionaje, guarda capturas y pide asesoramiento: la propia app puede ser una prueba.

## ¿Te está pasando algo de esto?

No estás solo y no es culpa tuya. En la Asociación Rainbow E Safe acompañamos a personas LGTBIQ+ que sufren violencia digital: te ayudamos a recoger pruebas, a recuperar tus cuentas y a valorar si denunciar.

**presidente@rainbowesafe.com · rainbowesafe.com · @rainbowesafe**

Si estás en peligro, llama al **112**. Si la violencia viene de tu pareja o expareja: **016** (gratuito, 24 h, no deja rastro en la factura). Antes de borrar nada, haz capturas: son tu prueba.