Prepárate para una protesta

ACTIVIST CHECKLIST

Última actualización **18 de marzo de 2026** Toma unos **30 minutos**

Esta copia se hizo el 14 de noviembre de 2026. Actualizamos nuestras guías seguido, a medida que cambian las amenazas y surgen mejores formas de protegerte. Para ver la versión más reciente, visita activistchecklist.org/es/protest/

Traducido automáticamente: Esta página se tradujo automáticamente. Hasta ahora solo el 15% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

Cuando los cops acceden al teléfono de una persona, pueden mapear redes enteras de activistas (tus contactos, tus chats de Signal, tu historial de ubicación y más). Los pasos aquí están pensados para ayudar a protegerte no solo a ti, sino también a las redes conectadas contigo.

Para quién es esta lista: Cualquier persona que asista a protestas, protestas de mayor riesgo, manifestaciones o eventos donde se espera presencia de los cops. Tenemos una guía aparte sobre seguridad digital para vigilar a ICE[2].

¿Piensas arriesgarte a que te arresten? Si vas a participar en una acción planificada donde podrían arrestarte (como un plantón o un bloqueo), mejor sigue nuestra guía de seguridad digital para acciones con riesgo de arresto[3]. Ahí hablamos de los acuerdos sobre teléfonos para tu grupo y de entregarle tu teléfono a una persona de apoyo antes de entrar.

¿Por qué importa esto?

Sabemos que los movimientos sociales han sido vigilados, infiltrados, desacreditados y obstaculizados por agentes del gobierno (cops locales, FBI, CIA, NSA, etc.) durante décadas. El auge de la tecnología significa que a todes nos están rastreando y perfilando (incluso si nunca te han arrestado).

¡Pero hay acciones que podemos tomar para proteger nuestros movimientos! Esta guía ofrece algunas cosas sencillas que podemos hacer antes y durante una protesta/acción para mantenernos a salvo, especialmente a las personas más vulnerables de nuestros movimientos.

Amenazas a considerar

- **Confiscación y registro del teléfono** - Si te arrestan, los cops pueden intentar entrar a tu teléfono para acceder a tus mensajes, fotos y otra información privada y usarla como evidencia
- **Monitoreo de comunicaciones** - Los cops pueden interceptar mensajes de texto y llamadas comunes para recopilar información sobre los planes y participantes de la protesta
- **Rastreo de ubicación** - Tu teléfono emite señales constantemente que pueden revelar tu ubicación y probar que estuviste en una protesta
- **Mapeo de redes activistas** - Al obtener datos del teléfono de una sola persona, los cops pueden identificar comunidades enteras de activistas y organizadores conectados con esa persona

Hay muchas más, pero estas son algunas de las principales.

¿Necesitas tu teléfono?

El teléfono más seguro es no llevar teléfono.

Si puedes, **mejor no lleves tu teléfono**. Esta es la opción más segura para tus datos y tu privacidad.

Dicho esto, muchas veces necesitamos comunicarnos durante las acciones. Si puedes invertir tiempo y dinero, un teléfono secundario[4] es la mejor opción intermedia, porque contiene menos datos.

Sabemos que conseguir un teléfono secundario no funciona para todo el mundo. Si necesitas llevar tu teléfono principal, la lista de abajo te ayudará a hacerlo más seguro.

Protecciones básicas para tu teléfono

TODO EL MUNDO Esta sección es para cualquiera que asista a una protesta de bajo riesgo (No Kings, etc.). Quienes coordinan eventos y participantes con mayor riesgo también deberían seguir las secciones de abajo.

Importante Apaga completamente tu teléfono si tu riesgo de arresto está aumentando

Tus datos están más protegidos cuando tu teléfono está apagado (no solo bloqueado)

Cuando tu teléfono está completamente apagado, es más difícil que la policía te extraiga los datos. Los datos están cifrados hasta que ingresas tu código de acceso por primera vez.

Por eso, lo más importante que puedes hacer para proteger tus datos es apagar tu teléfono apenas creas que tu riesgo de arresto está aumentando.

CÓMO APAGAR TU TELÉFONO

1. IPHONE
   Presiona el botón de bloqueo de pantalla en el lateral **5 veces** para abrir rápidamente la opción **Apagar**

   ANDROID
   Mantén presionado el botón de encendido hasta que aparezca el menú de encendido → toca **Apagar**
2. **Practica** esto varias veces para que puedas hacerlo rápido.
3. Durante la situación de alto riesgo, **recuérdale a la gente cerca de ti** que también apague sus teléfonos.

Contrapesos: Reconocemos que hay contrapesos al apagar tu teléfono. A veces es más importante filmar a la policía o coordinar con nuestros aliades. Piensa bien cuál es tu prioridad. Si necesitas filmar, considera llevar un teléfono secundario[4] para tener menos datos sensibles en él.

Desactiva la ubicación en todo tu teléfono antes de hacer actividades de mayor riesgo

Importante para actividades de mayor riesgo como protestas o monitoreo de ICE.

DO: Desactiva los servicios de ubicación en todo tu teléfono cuando hagas actividades de mayor riesgo

Las apps de tu celular recopilan tu ubicación exacta y la venden a corredores de datos. Los polis compran estos datos sin orden judicial y usan herramientas como Webloc[5] para ver qué teléfonos estuvieron en una zona, incluso en una protesta. El historial de ubicaciones que guardan Google o Apple también puede ser solicitado con una citación judicial.

Si desactivas la ubicación en todo tu teléfono, las apps no pueden recopilar tu ubicación GPS, así que no se puede vender a corredores de datos ni Google/Apple pueden acceder a ella.

Desactivar la ubicación no oculta dónde estás a tu compañía telefónica. Mientras tu teléfono esté encendido y tenga señal, tu compañía puede saber más o menos dónde estás por las antenas a las que te conectas, y los polis pueden conseguir esos datos. De más a menos protección:

1. Deja tu teléfono en casa.
2. Apaga tu teléfono. Una bolsa de Faraday te da todavía más protección.
3. Activa el modo avión **y** desactiva la ubicación.
4. Desactiva solo la ubicación.

El modo avión por sí solo no apaga el GPS. Las apps pueden seguir registrando tu ubicación y subirla cuando te vuelvas a conectar.

CÓMO DESACTIVAR LOS SERVICIOS DE UBICACIÓN

IPHONE

Ajustes → Privacidad y seguridad → Desactivar Localización

(Atajo más rápido: dile a Siri "Desactivar localización")

ANDROID

Ajustes → Ubicación → Desactivar Usar ubicación

Otros consejos:

- Puede que quieras **imprimir mapas** o **guardar mapas sin conexión** para orientarte.
- Si tienes smartwatches o rastreadores bluetooth tipo "perdí mis llaves/cartera", asegúrate de dejarlos en casa o de desactivar también su rastreo.

Revoca los permisos de ubicación a las apps que no los necesitan (que son la mayoría)

Protégete de las apps con acceso a tu ubicación que le dan al gobierno o a los corredores de datos un registro detallado de tus movimientos

DO: Desactiva el rastreo de ubicación en la mayoría de apps

DO NOT: Dejar que cada app sepa dónde estás

CÓMO REVISAR LOS PERMISOS DE UBICACIÓN EN IPHONE

1. Ve a **Ajustes → Privacidad y seguridad → Localización**
2. Revisa cada app y configúrala en una de estas opciones:
   - **Nunca: la mejor opción para la mayoría de las apps**
   - Preguntar la próxima vez o cuando comparta: útil para apps que rara vez necesitan tu ubicación
   - Al usar la app: solo para apps de navegación esenciales
   - Siempre: casi ninguna app debería tener este permiso
3. Asegúrate de configurar la app **Cámara** en "**Nunca**" para no arriesgarte a revelar tu ubicación cuando compartas o subas fotos.
4. Entra a la sección **Servicios del sistema → Desactivar Ubicaciones importantes**

CÓMO REVISAR LOS PERMISOS DE UBICACIÓN EN ANDROID

1. Ve a **Ajustes** → **Privacidad** → **Administrador de permisos** → **Ubicación**
2. Revisa cada app y configúrala en una de estas opciones:
   - **No permitir: la mejor opción para la mayoría de las apps**
   - Preguntar siempre: útil para apps que rara vez necesitan tu ubicación
   - Permitir solo mientras se usa la app: solo para apps de navegación esenciales
   - Permitir todo el tiempo: casi ninguna app debería tener este permiso

Es especialmente importante desactivar el rastreo de ubicación en tu app de cámara/fotos

Estas apps tal vez sí necesitan tu ubicación mientras las usas:

- Navegación (Apple Maps, Magic Earth, CoMaps)
- Apps para pedir transporte (pero solo mientras las usas activamente)

Algunas apps pueden necesitar permiso temporal:

- Las apps de entrega de comida solo necesitan tu ubicación cuando estás haciendo un pedido

Apps que definitivamente NO necesitan acceso a tu ubicación:

- Apps de fotos
- Apps de redes sociales
- Juegos
- La mayoría de las apps de compras
- Apps de banca
- Apps de noticias
- La mayoría de las apps de productividad

Recuerda: cada app con acceso a tu ubicación es una posible fuga de privacidad. Cuando tengas dudas, desactiva la ubicación y vuelve a activarla solo si descubres que realmente la necesitas.

Desactiva el desbloqueo facial/por huella digital (biométrico)

Tienes mayor protección legal[6] con un código de acceso que con el desbloqueo biométrico. Los cops pueden intentar obligarte a desbloquear con datos biométricos.

CÓMO DESACTIVAR EL DESBLOQUEO FACIAL/POR HUELLA

IPHONE

Configuración → **Face ID y código** → Desactiva **Usar Face ID para desbloquear el iPhone**

(Puedes dejar el resto activado.)

ANDROID

Ajustes → **Pantalla de bloqueo** (o **Seguridad**) → **Datos biométricos y seguridad** → **Desactiva tanto Reconocimiento facial como Desbloqueo con huella** para desbloquear tu teléfono

Advertencia: El desbloqueo facial y por huella digital te permiten usar contraseñas más fuertes sin tener que escribirlas todo el tiempo. Si tienes que elegir, es mejor tener un código de acceso más largo que desactivar el desbloqueo facial/por huella digital. Si dejas la biometría activada, asegúrate de saber cómo desactivarla rápido si vas a entrar en una situación de alto

riesgo (mira los tips abajo).

- **Apagar tu teléfono por completo es la mejor manera de desactivar temporalmente la biometría**, porque además cifra tus datos. El próximo desbloqueo requerirá tu código de acceso.
- **Truco para bloquear el iPhone:** Si dejas activado el desbloqueo facial/por huella digital, puedes forzar que se use tu código de acceso en el próximo desbloqueo **presionando el botón lateral 5 veces**.
- **Truco para la cámara del iPhone:** Puedes tomar fotos sin desbloquear tu teléfono **deslizando hacia la izquierda** en tu pantalla de inicio. (Por si te arrestan mientras estás grabando.)
- **Tip para la cámara de Android:** En muchos teléfonos Android, puedes abrir la cámara sin desbloquearlo **presionando dos veces el botón lateral o de encendido**.

Mantén tu teléfono (y laptop) actualizados con la última versión del sistema operativo

Te protege de hackers, spyware y las herramientas que usa la policía para hackear teléfonos.

DO: Instala las actualizaciones apenas te lo pidan

DO NOT: Seguir presionando el botón de "actualizar más tarde"

Cada vez que sale una nueva actualización del sistema operativo, se están corrigiendo fallas de seguridad. Cada actualización que no has instalado representa una lista más larga de formas en que la policía puede hackear tu dispositivo. Piénsalo como un edificio grande con cada vez más puertas sin llave.

Si tu sistema operativo no está actualizado, muchas de las otras recomendaciones de esta guía no protegerán tus datos.

Empieza por tu teléfono. Si estás haciendo algo de mayor riesgo, asegúrate de actualizar todos tus dispositivos.

CÓMO HACER LAS ACTUALIZACIONES

Como las actualizaciones de seguridad son tan importantes, **diseñamos una herramienta que te guía paso a paso**.

Revisa las actualizaciones de tu teléfono y computadora →

CÓMO HACER LAS ACTUALIZACIONES MANUALMENTE

Si prefieres hacer las actualizaciones manualmente, aquí te explicamos cómo hacerlo en cada dispositivo:

Haz clic para ver los pasos manuales

iPhone

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu iPhone aún tiene soporte[7]
2. **Sistema operativo:** Ajustes → **General** → **Actualización de software**
3. Las **apps** están configuradas para actualizarse automáticamente por defecto. Para verificarlo, ve a **Ajustes** → **Apps** → **App Store** y asegúrate de que **Actualizaciones de apps** esté activado.

Mac

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu Mac aún tiene soporte[7]
2. **Sistema operativo:** Menú Apple → **Ajustes del Sistema** → **General** → **Actualización de software**
3. **Apps instaladas desde la Mac App Store:** Estas apps están configuradas para actualizarse automáticamente por defecto. Para verificarlo, abre la **App Store**, ve a **App Store** → **Ajustes** y asegúrate de que **Actualizaciones automáticas** esté activado.
4. **Otras apps:** Busca actualizaciones desde la barra de menú superior → Haz clic en el nombre de la app → Haz clic en **Buscar actualizaciones** o **Acerca de [NOMBRE DE LA APP]**, o revisa en **Ajustes...**. Si no ves la opción de actualizar, puede que esté configurada para actualizarse automáticamente en segundo plano.

Android

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu Android aún tiene soporte[7]
2. **Sistema operativo:** Ajustes → **Sistema** → **Actualización del sistema** (puede variar según el fabricante)
3. Las **apps** de Google Play Store están configuradas para actualizarse automáticamente por defecto. Para verificarlo, abre **Play Store**, toca el ícono de tu perfil y ve a **Ajustes** → **Preferencias de red** → **Actualizar apps automáticamente**.

Windows

1. **Actualiza tu sistema:** Inicio → **Configuración** → **Actualización y seguridad** → **Windows Update**
2. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu equipo con Windows aún tiene soporte[7]
3. **Apps de la Microsoft Store:** Asegúrate de activar las actualizaciones automáticas[8] (activadas por defecto).
4. **Otras apps:** Busca actualizaciones en la barra de menú → **Ayuda** → **Buscar actualizaciones**, o busca **Actualizaciones** o **Acerca de** en la configuración de la app.

Usa Signal para comunicarte (mensajes/llamadas) en protestas/acciones

Los mensajes con cifrado de extremo a extremo protegen tu privacidad frente a la vigilancia, mientras que los mensajes de texto comunes pueden ser interceptados y leídos.

DO: Instala y usa Signal[9] (gratis) para tu activismo y trabajo político

DO NOT: Usar WhatsApp, Telegram, iMessage o mensajes de texto comunes (para tu activismo)

CÓMO INSTALAR Y USAR SIGNAL

1. Instala Signal[10] en tu teléfono
2. Envía mensajes o llama a tus contactos usando su número de teléfono, o pídele a alguien su nombre de usuario de Signal. Esa persona también debe tener Signal instalado.

Mira nuestra Signal Checklist[11] para instrucciones detalladas sobre cómo configurar Signal de la forma más segura posible.

Desactiva las vistas previas en las notificaciones de Signal

Si te confiscan el celular (y está encendido), los cops pueden leer los mensajes en tu pantalla de inicio sin desbloquearlo.

CÓMO DESACTIVAR LAS VISTAS PREVIAS DE LAS NOTIFICACIONES DE SIGNAL

Abre Signal → Toca tu foto de perfil → **Ajustes** → **Notificaciones** → **Contenido de las notificaciones** → Selecciona **Sin nombre ni contenido**

Mantén tu teléfono en modo avión siempre que sea posible en una protesta

Protege los datos de tu ubicación desactivando las conexiones inalámbricas. Esto mantiene tus actividades en la protesta privadas y seguras.

El modo avión no desactiva el rastreo de ubicación por GPS. Debes desactivar los servicios de ubicación.

Si llevas tu teléfono, puede que lo necesites para comunicarte. Ten en cuenta que cada vez que tengas cobertura celular, tu ubicación puede ser aproximada según las torres celulares a las que estés conectado/a.

Configura el código de acceso de tu teléfono con 8 a 10 dígitos aleatorios

A los cops les toma años descifrar un código de acceso aleatorio de 8 dígitos. Probablemente pueden adivinar tu código de acceso actual en menos de 5 minutos con herramientas automatizadas.

DO: Usa un generador de códigos de acceso aleatorios[12] para crear un código de 8 a 10 dígitos

DO NOT: Uses cualquier código de acceso que se te haya ocurrido a ti (fechas, patrones en el teclado, etc.). Uses códigos de acceso de 6 dígitos si puedes evitarlo.

CÓMO CAMBIAR TU CÓDIGO DE ACCESO

1. Genera un código de acceso aleatorio de 8 a 10 dígitos usando este generador de códigos de acceso aleatorios[12]. (¡No lo inventes tú—las personas somos malas eligiendo al azar!)
2. Cambia tu código de acceso:

   IPHONE

   Ajustes → **Face ID y código** → **Cambiar código** → **Opciones de código** → **Código numérico personalizado**

   ANDROID

   Ajustes → **Seguridad** → **Bloqueo de pantalla** → Ingresa el bloqueo actual → **PIN/Contraseña** → Ingresa un código de acceso
3. **Practica el nuevo código de acceso** al menos 10 veces seguidas ahora mismo para que sea más probable que lo recuerdes. (Desactivar la biometría obligará a pedir el código de acceso cada vez que bloquees el teléfono.)
4. Escribe tu nuevo código de acceso en papel y guárdalo en un lugar seguro en casa hasta que lo memorices. Luego destrúyelo después de 2 a 3 semanas. Poner un recordatorio en tu teléfono puede ayudar.

¿Cuánto tarda en descifrarse un código de acceso?

TIPO	TIEMPO QUE TOMA DESCIFRARLO (PROMEDIO)	EJEMPLO
Patrón de 6 dígitos *fácil de adivinar*	**Menos de 24 horas** para descifrarlo	*333666 (patrón común)* o *110585 (patrón de fecha para el 5 de noviembre de 1982)*
Código *aleatorio* de 6 dígitos	**200 días** para descifrarlo	*238253*
Código *aleatorio* de 8 dígitos	**Más de 40 años** para descifrarlo	*34780026*

Nota: Estos tiempos solo aplican a teléfonos. Las computadoras se pueden descifrar mucho más rápido y necesitan contraseñas mucho más fuertes.

Fuentes: Las estimaciones en la tabla de arriba asumen los intentos por segundo observados en el mundo real con las herramientas forenses de hackeo que usan los cops. Si necesitas más seguridad, usa un código de acceso de 10 dígitos, que te protegerá incluso en los peores escenarios posibles de descifrado. Mira las fuentes enlazadas en las preguntas frecuentes sobre códigos de acceso aquí[12].

Protecciones avanzadas para tu teléfono

AMENAZA MEDIA **Esta sección es para ti si:**

→ **Eres organizador/a o líder** en espacios de movimientos sociales.
→ **Es probable que los cops te vigilen** por identidades que tienes (raza, sexualidad, estatus migratorio, etc.).
→ **Tienes vínculos cercanos** con muchas personas en riesgo.

Si estás en mayor riesgo, te recomendamos configurar un teléfono secundario[4] para protestas y activismo, si puedes. Hacerlo te protegerá a ti y a tu red mucho más de lo posible con tu teléfono principal.

Configura los mensajes que desaparecen de Signal entre 5 y 15 minutos en todas las conversaciones activas durante la protesta o acción

Tus mensajes que desaparecen se borrarán aunque te confisquen el teléfono (pero solo si ya los leíste).

CÓMO ACTIVAR LOS MENSAJES QUE DESAPARECEN

Abre Signal → Abre cada conversación (una a la vez) → Toca el nombre del contacto o grupo → Selecciona **Mensajes que desaparecen** → Configura el temporizador en **5-15 minutos**.

Puedes ajustarlo a un tiempo más largo después de la acción.

Importante: Los mensajes solo desaparecen después de haber sido LEÍDOS, así que los mensajes nuevos quedarán en un teléfono confiscado y los cops podrán acceder a ellos. Si sabes a quién arrestaron, sácalx del grupo.

Te recomendamos también configurar los mensajes que desaparecen para todas las conversaciones nuevas en Abre Signal → Toca tu foto de perfil → **Ajustes** → **Mensajes que desaparecen** → **1 semana**.

Oculta la vista previa del mensaje y el nombre del remitente en las notificaciones de Signal

Si te confiscan el teléfono, los cops pueden acceder a tu historial de notificaciones.

Si te confiscan el teléfono, hay dos formas en que los cops pueden acceder a tu historial de notificaciones:

1. Pueden ver las notificaciones en tu pantalla de inicio sin desbloquear el teléfono.
2. Si usan herramientas de hacking, pueden acceder al registro de notificaciones que ha recibido tu teléfono. (Ejemplo del caso Prairieland[13].)

Esto solo aplica a los mensajes entrantes. Y es un riesgo incluso después de que el mensaje haya desaparecido de Signal (si tienes activados los mensajes que desaparecen).

CÓMO DESACTIVAR LAS NOTIFICACIONES DE SIGNAL

EN IPHONE

Abre Signal → Toca tu foto de perfil → Ajustes → Notificaciones → Contenido de las notificaciones → **Selecciona "Sin nombre ni contenido"**

EN ANDROID

Abre Signal → Toca tu foto de perfil para abrir Ajustes → Notificaciones → Mostrar → **Selecciona "Sin nombre ni mensaje"**

Si desactivas las notificaciones de Signal a nivel del sistema operativo del teléfono, no te avisará de las llamadas entrantes de Signal.

Si usas Signal Desktop, asegúrate de desactivar también las notificaciones allí.

Para que sepas: Si quieres borrar el registro de notificaciones que iOS ya guardó, la única forma es restablecer tu teléfono de fábrica y configurarlo como uno nuevo — no desde una copia de seguridad, ya que estas incluyen el historial de notificaciones.

Sigue nuestra lista de seguridad de Signal

CÓMO ASEGURAR SIGNAL

Completa todos los pasos de nuestra Lista de Signal[11] para que Signal sea más seguro y privado.

Lista de seguridad de Signal →

Desactiva el Advertising ID (que puede permitir que los cops rastreen tu ubicación)

Los cops usan herramientas que dependen de tu advertising ID para rastrearte

Sabemos que ICE y otras agencias policiales están usando herramientas de rastreo de ubicación[5] que dependen en parte del "ID de publicidad" que tu teléfono proporciona. Estas herramientas suelen usarse para reprimir movimientos sociales.

Los advertising IDs también se han usado para elegir blancos de spyware[14] que se entrega a través de anuncios.

En los iPhones, esta función está desactivada por defecto. En Android, viene activada por defecto y hay que desactivarla.

CÓMO DESACTIVAR EL ID DE PUBLICIDAD

IPHONE

Ajustes → **Privacidad y seguridad** → **Seguimiento** → **Desactivar el seguimiento de apps**

Por defecto, los iPhones ya tienen esta opción desactivada. Pero puedes revisarlo para asegurarte.

ANDROID

Ajustes → Toca el ícono de búsqueda y busca "anuncios" o "publicidad" → Toca **Eliminar ID de publicidad**

Esta opción aparece en lugares distintos según el teléfono, así que lo más fácil es buscarla.

Desactiva los asistentes de voz cuando tu teléfono esté bloqueado (Siri o Google Assistant)

Protégete de que la cana use tu teléfono para ejecutar comandos básicos incluso cuando esté bloqueado.

CÓMO DESACTIVAR LOS ASISTENTES DE VOZ

IPHONE

Ajustes → **Siri** → Desactiva **Permitir Siri con el bloqueo**

ANDROID

Ajustes → **Google** → **Ajustes de las apps de Google** → **Búsqueda, Assistant y Voz** → **Google Assistant** → Desactiva **Pantalla de bloqueo**

No compartas fotos ni videos con caras, tatuajes u otros rasgos que permitan identificar a alguien

Ten cuidado al compartir fotos donde se vean las caras de las personas. Pueden usarse como prueba en su contra si los arrestan.

Tomar fotos es arriesgado, pero también importante. Documentar nuestras acciones suele ser clave para contar nuestra historia y sumar gente a la causa. Pero no queremos crear pruebas que el Estado pueda usar para rastrear y procesar a activistas.

CÓMO TOMAR FOTOS PROTEGIENDO IDENTIDADES

- Cuando sea posible, trata de no captar caras desde el principio.
- Desactiva la subida automática a la nube en Google Photos, iCloud Photos, etc., para que las fotos no se suban antes de que puedas revisarlas y difuminarlas.
- Si captas una foto con una cara, usa la herramienta de difuminado[15] de Signal antes de enviarla a cualquier lado. Difumina también rasgos únicos, como tatuajes o ropa llamativa.
- Ten mucho cuidado con las fotos que publicas en redes sociales. Los polis vigilan y revisan estas plataformas todo el tiempo para rastrear a activistas.
- Si te estás organizando con un grupo conocido, hablen con anticipación sobre los acuerdos para documentar y compartir.

Imprime indicaciones o usa mapas sin conexión

Tu historial de Google Maps muestra todos los lugares donde has estado, y la policía puede obtener estos datos con una orden judicial.

DO: Usa indicaciones impresas o mapas sin conexión de Magic Earth[16] o mapas sin conexión de Apple Maps

DO NOT: Usar Google Maps

Puedes protegerte de las “órdenes de geocercado” que la policía usa para rastrear a cualquier persona en una zona determinada.

CÓMO USAR NAVEGACIÓN PRIVADA

- **Desactiva los servicios de ubicación** antes de salir hacia la acción/protesta.
- Mantén tu teléfono en **modo avión** tanto como puedas, para que tu operador tampoco sepa dónde estás.
- Usa **indicaciones impresas** a la antigua si puedes. Imprímelas desde Open Street Map[17] para mantener tu búsqueda más privada. (Accede a Open Street Maps usando Tor Browser[18] para aún más privacidad.)
- Usa una app que permita mapas y direcciones privadas sin conexión. Los mapas de Magic Earth[16] son los mejores (Android e iPhone), pero Apple Maps también te permite descargar mapas sin conexión y funciona muy bien. Encuentra la función dentro de la app para descargar una zona con anticipación, luego mantén tu teléfono en modo avión todo el tiempo. Las funciones de navegación automática no funcionarán, así que tendrás que ir siguiendo las indicaciones manualmente.

Desactiva el Bluetooth y el Wi-Fi

Los cops pueden usar herramientas de rastreo[19] para identificar quién está en una zona según las señales de Bluetooth y Wi-Fi que emite tu teléfono.

Si vas a llevar tu teléfono, suponemos que lo usarás para comunicarte y que necesitas conexión celular, así que activar el modo avión probablemente no te sirva. Por eso, lo mejor es **desactivar el Bluetooth y el Wi-Fi** para reducir el rastreo.

Aviso para iPhone: Deslizar hacia abajo y usar el "**centro de control**" para desactivar Bluetooth/Wi-Fi en realidad no los apaga. Solo te desconecta de las redes actuales, pero el teléfono sigue transmitiendo señales que pueden ser rastreadas. Para apagarlos por completo, sigue las instrucciones de abajo.

CÓMO DESACTIVAR EL BLUETOOTH Y EL WI-FI

IPHONE
Ajustes → **Bluetooth** → **Desactivar Bluetooth**

IPHONE
Ajustes → **Wi-Fi** → **Desactivar Wi-Fi**

ANDROID
Ajustes → **Bluetooth** → **Avanzado** (o el menú de tres puntos) → **Desactivar Bluetooth** y **desactivar el escaneo por Bluetooth**

ANDROID
Ajustes → **Wi-Fi** → **Avanzado** (o el menú de tres puntos) → **Desactivar Wi-Fi** y **desactivar Escaneo** o **Escaneo de Wi-Fi**

Sal de los grupos de Signal que podrían poner a otras personas en riesgo

Esto ayuda a proteger a tu red si te confiscan el teléfono.

Si los cops te confiscan el teléfono, uno de los mayores riesgos es exponer a toda tu red. Aunque la gente no use su nombre real en su cuenta de Signal, sigue existiendo un ID único detrás de cada nombre de usuario de Signal. Y los cops pueden usar esto para correlacionar la identidad de alguien entre varios dispositivos incautados.

Necesitas salir Y borrar el grupo:

- Si solo sales del grupo, los mensajes antiguos quedan en tu teléfono, junto con el historial de quiénes estaban en el grupo.
- Si solo borras el grupo, los nuevos mensajes seguirán llegando y la conversación vuelve a aparecer.

CÓMO SALIR Y BORRAR UN GRUPO DE SIGNAL

1. **Haz un plan para volver a unirte después:** Cuando vayas a una situación con posibilidad de arresto, haz una lista en papel, en casa o en un lugar seguro, de todos los grupos y de a quién necesitas escribirle para que te vuelva a agregar después de la acción o del cruce de frontera.
2. **Para salir del grupo:** Signal → [Grupo] → Toca el ícono del grupo arriba → **Salir del grupo**
   - Si eres la única persona admin, tienes que sacar a todos los miembros o asignar a otra persona como admin.
3. **Para borrar el grupo de tu teléfono:** Signal → Pantalla principal → Desliza la conversación hacia la izquierda → **Eliminar**
   - Esto no lo borrará para nadie más.

Consejos de higiene de seguridad:

- Pon un recordatorio recurrente para limpiar tus conversaciones de Signal cada 3 meses.
- Asegúrate de anotar de qué grupos estás saliendo y a quién le puedes pedir que te vuelva a agregar después de la acción.

Nota: Si este proceso te parece muy molesto y engorroso (¡porque lo es!), esa es otra buena razón para usar un teléfono secundario[4] para las acciones. Ese teléfono solo estaría en uno o dos grupos necesarios para llevar a cabo la acción ese día.

Haz una copia de seguridad de tu teléfono

Por si te confiscan el teléfono y necesitas uno nuevo.

Te recomendamos respaldar tu teléfono en una computadora en vez de la nube para mayor seguridad. La policía puede conseguir una orden judicial para acceder a tus respaldos de iCloud/Google, fotos en línea, documentos en línea, etc.

CÓMO HACER UNA COPIA DE SEGURIDAD DE TU TELÉFONO EN TU COMPUTADORA

Para iPhone: Conéctalo a la computadora con un cable USB, abre iTunes/Finder, selecciona tu dispositivo, haz clic en "Back Up Now" en la sección de copia de seguridad manual y asegúrate de que "Encrypt local backup" esté seleccionado para proteger tus datos. (Guarda tu contraseña)

Para Android: Conecta el teléfono a la computadora con un cable USB, elige el modo "File Transfer" cuando se te indique y luego copia manualmente las carpetas que quieras (DCIM, Downloads, etc.) al disco duro de tu computadora.

Usa una bolsa de Faraday para bloquear todas las señales rastreables de tu teléfono

Una bolsa de Faraday bloquea todas las señales (GPS, celular, Wi-Fi, Bluetooth, etc.) que entran y salen de tu teléfono.

En teoría, apagar tu teléfono debería lograr lo mismo. Aunque no es común, hay formas[20] de hackear un teléfono para que se conecte a la red incluso si está apagado[20]. Una bolsa de Faraday te da un nivel extra de seguridad.

Algunas opciones de dónde comprar bolsas de Faraday:

- Bolsa de Faraday de Mic Lock[21] ($13) - la más barata, pero puede dejar pasar un poco de señal
- Bolsa de Faraday de MOS Equipment[22] ($23)
- Bolsa de Faraday de SLNT[23] ($30)

Otros consejos de seguridad para protestas

TODO EL MUNDO Esta sección es para cualquier persona que haga trabajo de activismo o incidencia.

Elige un número de teléfono al que llamar si te arrestan. Escríbelo en tu cuerpo con un sharpie.

Este es el número al que vas a llamar si te arrestan, alguien que pueda apoyarte desde afuera. Esto aplica para situaciones de mayor riesgo.

CÓMO ELEGIR UN NÚMERO DE TELÉFONO AL QUE LLAMAR SI TE ARRESTAN

1. **Decide a quién llamar si te arrestan:**
   - Si no sabes si hay una línea activa de apoyo carcelario en tu zona, elige a alguien como tu contacto de emergencia y usa su número de teléfono. Puede ser una amistad o compañere de confianza que pueda ayudarte a conseguir apoyo legal. Asegúrate de pedirle permiso con anticipación.
   - Si vas a participar en una acción de mayor riesgo, es posible que quienes la organizan ya hayan establecido un número específico de línea legal para que uses.
   - Si estás en una ciudad grande, puede haber una línea directa de jail support del National Lawyers Guild con gente lista para apoyar a activistas. Revisa la lista de números de líneas de jail support del NLG aquí[24]. Solo recomendamos usar una línea directa si llenaste un formulario de jail support con anticipación, así pueden llamar a tus contactos por ti mientras te dan apoyo al mismo tiempo.
2. **Escribe el número de la línea legal en tu cuerpo con sharpie** en un lugar donde no se borre fácilmente (brazo, pierna, torso). Llama a ese número si te arrestan y te dan una llamada telefónica.

☐ Vístete para pasar desapercibide, considera cubrirte la cara si quieres más privacidad

Los cops pueden usar tecnología de reconocimiento facial[25] para identificarte a partir de grabaciones de cámaras de seguridad. Nuestros adversarios suelen usar herramientas de "búsqueda inversa de imágenes" para encontrarte y acosarte en línea.

CÓMO PASAR DESAPERCIBIDE

- **Usa ropa neutra** que sea difícil de identificar (evita patrones o colores muy llamativos).
- **Cubre los tatuajes** o cualquier cosa identificable que te haga destacar en fotos o videos.
- **Usa una mascarilla KN-95** tanto para protegerte del COVID como para tener más anonimato.

☐ Planea tu viaje teniendo en cuenta la vigilancia

Piensa en el nivel de riesgo que estás asumiendo y considera cuánto esfuerzo quieres poner en evitar la vigilancia.

Algunos tipos de rastreo que debes tener en cuenta:

- **Lectores automáticos de placas:** Están por todas partes, pero sobre todo en casetas de peaje y puentes.
- **Cámaras de vigilancia**[26]: Hay cámaras dentro y fuera de la mayoría de negocios, tiendas, etc., y en el transporte público. También piensa en las cámaras de consumo que están en cosas como timbres inteligentes.
- **Tarjeta de transporte**: Si usas el transporte público con una tarjeta de transporte, esto deja un rastro digital. Considera pagar en efectivo o comprar una tarjeta de un solo uso cuando vayas a una protesta. (Además: Casi todo el transporte público siempre tiene muchas cámaras de vigilancia.)
- **Tarjeta de crédito**: Si usas tu tarjeta de crédito o pagas con "tap", estás creando un rastro digital que te ubica en cierto lugar a una hora específica. Considera usar efectivo cuando sea posible para tener más privacidad.
- **Apps de viajes compartidos (Uber/Lyft):** Usar una app de viajes compartidos para llegar a la protesta dejará un registro claro de tus movimientos y ubicación.

Más información

Consejo: Antes de tu próxima acción, considera hacer esta lista como sesión grupal[27] con las personas con quienes vas. Es más divertido y así todes van a terminar realmente los pasos.

- Electronic Frontier Foundation - Guía para asistir a una protesta[6] (actualizado en 2024)
- CLDC - Espera lo inesperado: Asegura tu teléfono contra la confiscación o pérdida[28] (2021)
- Freedom of the Press Foundation - Qué hacer si los cops te confiscan el teléfono[29] (2016)
- Freedom of the Press Foundation - Consejos de seguridad móvil: Nueve pasos para preparar tu teléfono antes de una acción[30] (2020)
- Freedom of the Press Foundation - Tu smartphone y tú: Un manual de mantenimiento móvil moderno[31] (2024)
- The Markup - ¿Cómo preparo mi teléfono para una protesta?[32] (2024)

Sigue aprendiendo con estas guías relacionadas

Fundamentos de seguridad

Prácticas básicas de seguridad que toda persona activista debería seguir.

Seguridad en Signal

Asegura la app de mensajería Signal para tener comunicaciones más seguras.

Seguridad en viajes y vuelos

Prácticas de seguridad digital para activistas que viajan.

Enlaces

1. activistchecklist.org/es/contribute/
2. activistchecklist.org/es/ice/
3. activistchecklist.org/es/action/
4. activistchecklist.org/es/secondary/
5. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
6. ssd.eff.org/module/attending-protest
7. activistchecklist.org/es/updates/
8. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
9. signal.org
10. signal.org/download/
11. activistchecklist.org/es/signal/
12. strongphrase.net/passcode
13. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
14. activistchecklist.org/es/spyware/
15. signal.org/blog/blur-tools/
16. magicearth.com
17. openstreetmap.org
18. activistchecklist.org/es/research/
19. unwall.app/www.wired.com/story/dnc-hidden-signal-hunt/
20. theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data
21. mic-lock.com/products/signal-blocking-faraday-bag
22. mosequipment.com/collections/all-products/products/mission-darkness-non-window-faraday-bag-for-phones
23. slnt.com/collections/faraday-phone-sleeves/products/faraday-bags?variant=48508947005734
24. nlg.org/chapters-2/
25. sls.eff.org/technologies/face-recognition
26. sls.eff.org/technologies/surveillance-camera-networks
27. activistchecklist.org/es/party/
28. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
29. freedom.press/training/mobile-security-for-activists-and-journalists/
30. freedom.press/training/mobile-security-protest-preparation-tips-activists/
31. freedom.press/training/your-smartphone-and-you-handbook-modern-mobile-maintenance/
32. themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024