# Seguridad digital para acciones con riesgo de arresto

ACTIVIST CHECKLIST

Última actualización **30 de octubre de 2026** Toma unos **20 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/action/

**Traducido automáticamente**: Esta página se tradujo automáticamente. Hasta ahora solo el 3% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

Esta guía trata sobre la seguridad digital si necesitas llevar tu celular a una acción no violenta de desobediencia civil (también llamada acción directa) en la que algunas personas planean arriesgarse a que las arresten. Es una parte de mantener a salvo a tu grupo. Tu acción también debe planear la seguridad física, tener un equipo de seguridad y asegurarse de que todo el mundo conozca sus derechos. Nuestra lista de seguridad para quienes organizan acciones[2] te puede ayudar con todo esto.

**Evalúa tu nivel de riesgo**: Esta guía es para acciones donde corres un riesgo legal relativamente bajo (por ejemplo: un plantón o encadenarte a una puerta). Si estás planeando algo en lo que buscas el anonimato o donde las consecuencias legales son mucho más graves, deberías tomar muchas más precauciones de las que ofrece esta guía.

Esta guía está escrita para la siguiente situación:

- Es una acción organizada de forma lo suficientemente central como para establecer acuerdos de seguridad digital que todes seguirán.
- Animaste a la mayoría de las personas que van a la acción a **no llevar su teléfono**
- Algunas personas todavía necesitan su teléfono para coordinar el despliegue (por ejemplo: coordinación táctica, médicos, equipo de desescalada, etc.)
- El riesgo de arresto es alto, o planeas arriesgarte a que te arresten.
- Crees que los policías podrían intentar usar herramientas para hackear celulares para acceder a los datos de los celulares que confisquen.
- No te preocupa la vigilancia hacia y desde la acción.

Si algo de esto no aplica a tu acción, quizás necesites tomar más precauciones. Revisa la sección de seguridad reforzada del celular para protestas[3] o considera llevar un celular secundario[4] (a veces llamado "celular desechable").

**Tip para organizadores:** En los días previos a la acción, considera organizar una fiesta de seguridad[5] para que tu crew haga estos pasos en conjunto antes del día de la acción.

---

## ¿Por qué importa esto?

Sabemos que los movimientos sociales han sido vigilados, infiltrados, desacreditados y obstruidos por agentes del gobierno (cops locales, FBI, CIA, NSA, etc.) durante décadas. El avance de la tecnología significa que a todes nos rastrean y nos crean perfiles (aunque nunca te hayan arrestado).

Incluso cuando ejercemos nuestro derecho legal a la libertad de expresión y de reunión, hay muchas fuerzas del gobierno que buscan aplastar la disidencia y criminalizar a quienes hacemos activismo. (Mira el caso de los 15 de Minnesota[6])

**¡Pero hay cosas que podemos hacer para proteger nuestros movimientos!** Esta guía ofrece algunas acciones simples que todes podemos tomar antes y durante una protesta/acción para mantenernos a nosotres y a las personas más vulnerables de nuestros movimientos más segures. Tomar estas precauciones ayuda a proteger a todas las personas con las que te organizas (no solo a ti y a tus datos). No es señal ni admisión de haber hecho nada malo.

## Amenazas a considerar

- **Confiscación y revisión 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
- **Vigilancia de las comunicaciones** - Los cops pueden interceptar mensajes SMS y llamadas comunes para obtener información sobre los planes y participantes de la protesta
- **Citación judicial de los datos de tu cuenta o de tu compañía telefónica** - Los policías pueden conseguir una orden judicial para acceder a tus cuentas en línea (como Google o Apple) o a tus datos de comunicación y ubicación a través de tu compañía telefónica.
- **Informantes y agentes encubiertos**: personas en tus reuniones o chats grupales podrían estar pasándole a la policía lo que ven y leen
- **Mapeo de redes activistas** - Al obtener datos del teléfono de una persona, los cops pueden identificar comunidades enteras de activistas y organizadores conectades con esa persona

# Para todas las personas que participan en la acción

- [ ] Importante **Pónganse de acuerdo como grupo: quien se arriesgue a ser arrestade debe darle su teléfono a una persona de apoyo (o dejarlo en casa)**

  Los celulares apagados y con menos riesgo de ser confiscados nos protegen a todes.

En acciones de menor riesgo donde puede haber arrestos, lo mejor es que todes A) dejen su teléfono en casa o B) **apaguen sus teléfonos** y se los dejen a una persona de apoyo. Muchas veces es alguien que hace apoyo carcelario. Esta persona no debería ir a la acción o, si va, debería quedarse en un lugar de muy bajo riesgo, bien en las orillas de la acción.

CÓMO HACER UN ACUERDO SOBRE CELULARES PARA TU ACCIÓN

1. **Decidan qué roles de verdad necesitan celular.** Normalmente son pocas personas, como quien coordina la táctica, quien hace de enlace con la policía o les médiques. Todes les demás dejan sus celulares con la persona de apoyo. Nadie en un rol con alto riesgo de arresto debería llevar celular. (O debería entregarlo en cuanto empiece la acción).
2. **Antes de empezar la acción, la persona de apoyo junta la mayoría de los celulares.**
3. **Hagan un plan para devolverle los celulares a la gente cuando la suelten**. Normalmente, la persona de apoyo carcelario les lleva los celulares cuando salen.
4. **Compartan el acuerdo con tiempo y repítanlo** en los talleres y en la reunión informativa antes de la acción.

**Consejo**: si hay muchos celulares y necesitas confirmar que cada persona es la verdadera dueña del que señala en la pila, puedes pedirle que lo desbloquee frente a ti.

## 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[7] (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[8] 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[9] para instrucciones detalladas sobre cómo configurar Signal de la forma más segura posible.

## Importante Cambia tu configuración predeterminada para que todos los nuevos chats de Signal tengan los mensajes que desaparecen activados

Esto nos mantiene a todes más seguros si le confiscan o hackean el teléfono a alguien.

La mejor mejora que cualquiera puede hacer al usar Signal es asegurarse de que los mensajes que desaparecen[10] estén activados ***por defecto***. La mayoría de activistas con quienes hablamos no lo tienen activado por defecto. (Y la mayoría de la gente se olvida de activarlo manualmente en cada nuevo chat.)

Esto te mantiene a ti y a otras personas a salvo. No sabemos a quién le van a incautar el teléfono los cops. Aunque creamos que estamos hablando de cosas totalmente legales, el gobierno puede encontrar formas de tergiversar nuestras palabras para intentar armarnos un caso por disentir

Hay dos cosas que hay que tener en cuenta sobre los mensajes que desaparecen:

1. **Primero, cambia tu configuración predeterminada** para que cualquier chat que crees tenga esta función activada.
2. **Segundo, asegúrate de que esté activado en los chats que otras personas inician:** si alguien más inicia el chat, puede que no tenga los mensajes que desaparecen activados. Puede que necesites activarlo.

CÓMO ACTIVAR LOS MENSAJES QUE DESAPARECEN

1. **Para cambiar la configuración predeterminada:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Mensajes que desaparecen** → configura el tiempo que quieras (más largo o más corto según tu tolerancia al riesgo).
2. **(Solo Android) Cambia tu límite de retención de mensajes:** Esto borrará los mensajes incluso en chats que no tengan activados los mensajes que desaparecen. (Solo se borrarán en tu dispositivo.) Abre Signal → Toca tu foto de perfil → **Ajustes** → **Datos y almacenamiento** → **Administrar almacenamiento** → **Conservar mensajes** → configura el tiempo máximo que quieras. Regresa una pantalla y activa **Aplicar límites a dispositivos vinculados**.
3. **Para cambiar chats existentes:** Signal → Abre el chat que quieres cambiar → Toca el nombre de la persona (o del grupo) en la parte superior de la pantalla → **Mensajes que desaparecen** → configura el tiempo que quieras.
4. **Borra los mensajes/chats antiguos:** Los mensajes que desaparecen NO se aplican de forma retroactiva. Así que puede que quieras borrar los chats antiguos de tu teléfono. Lamentablemente, esto no los borrará en los teléfonos de otras personas. Así que si es algo muy sensible, quizá tengas que pedirles que también borren el chat manualmente. (Y ya que estás, ¡anímales a activar los mensajes que desaparecen por defecto!)

**Cómo elegir el tiempo de tus mensajes que desaparecen:** El tiempo que configures depende de qué tan sensibles sean tus mensajes. Una pregunta que puedes hacerte es: "si le incautaran o hackearan el dispositivo a alguien, ¿qué tan importante es que estos mensajes no sean accesibles?"

- Para chatear sobre cosas de bajo riesgo con amigues, puedes elegir 4 semanas.
- Para organizing político común, puedes elegir 1 semana.
- Para acciones de mayor riesgo, puedes ponerlo en 1 día, 1 hora o 5 minutos, para que los mensajes desaparezcan antes de que empiece la acción.

**Nota:** Los mensajes solo desaparecen después de que se hayan leído. Así que si quien recibe el mensaje no lo lee en 2 semanas, y tienes los mensajes que desaparecen configurados en 4 semanas, en realidad desaparecerá 6 semanas después de que lo enviaste.

## Usa Proton Docs para colaborar (en lugar de Google Docs)

Protege los datos de tu grupo para que Google no rastree cada documento que ves

DO: Usa Proton Docs (o CryptPad) para organizarte

DO NOT: Usar Google Docs para organizarte

Google rastrea toda la actividad de sus usuarios, incluyendo qué documentos abres, compartes y consultas. La policía puede conseguir estos datos con citaciones/órdenes judiciales, y se sabe que a veces los comparten sin la autorización necesaria. Organizarnos fuera de Google Docs nos ayuda a cuidarnos entre todes.

**Proton Docs**[11] es una alternativa de buena calidad a Google Docs. Tus documentos tienen cifrado de extremo a extremo, lo que significa que aunque las autoridades accedieran a los servidores de Proton, no podrían ver lo que contienen tus documentos.

**¡Proton Docs no te hace anónime por defecto!** Si estás organizando actividades de mayor riesgo, asegúrate de conocer las limitaciones de Proton y cómo usarlo de forma segura[12].

CÓMO USAR PROTON DOCS

1. Crea una cuenta de Proton[13] si aún no tienes una — elige el plan gratuito
2. Entra a Proton Drive[14] → Haz clic en el botón **New** → Selecciona **New Document**
3. Cuando tu documento esté listo para compartir, puedes hacer clic en el botón "Share" y compartirlo con otras cuentas de Proton, o activar "Create public link" para compartirlo con personas que no tengan una cuenta de Proton. ¡Ten cuidado dónde compartes el enlace, porque será menos seguro! Te recomendamos usar una contraseña si activas el modo "cualquier persona con el enlace puede ver".

Anima a las personas con quienes te organizas a abrir una cuenta de Proton para que todes puedan avanzar hacia una mayor seguridad.

**¿Buscas formularios?** Proton no tiene algo como Google Forms. Puedes probar los formularios de CryptPad[15] o Jotform[16] con la opción de cifrado de extremo a extremo activada.

## No escribas nada que no quieras que te lean en voz alta en un juicio

Los chats, documentos y notas pueden terminar en manos de la policía.

DO: Habla de los detalles delicados en persona, con los teléfonos guardados

DO NOT: Poner en chats grupales o documentos compartidos quién se arriesga a ser arrestade o los detalles del plan

Vivimos una época en la que el gobierno federal vigila y persigue a activistas con una intensidad que no veíamos desde hace décadas.

Cuando organizamos a gran escala, siempre buscamos un equilibrio entre la seguridad y la necesidad de hacer crecer nuestros movimientos y construir poder.

Una forma de reducir riesgos innecesarios es tener cuidado con lo que ponemos por escrito. Lo que escribimos muchas veces termina usándose en nuestra contra en un juicio, incluso si usamos herramientas cifradas como Signal.

En cualquier trabajo de organización que implique riesgo de arresto (o que esté muy en la mira, como la vigilancia comunitaria de ICE[17] o la solidaridad con Palestina), es importante tener acuerdos sobre lo que no se va a poner por escrito.

Cómo llegan los datos a un juicio:

- **Le quitan el teléfono a alguien.** Si arrestan a alguien del chat y la policía logra entrar a su teléfono, puede leer todos los mensajes y documentos que haya ahí.
- **Una empresa entrega tu cuenta.** Servicios como Google Docs no tienen cifrado de extremo a extremo, así que la empresa puede ver tus documentos y dárselos a la policía si esta consigue una citación judicial u orden judicial. En 2025, Google le entregó a ICE la información de la cuenta de une estudiante de posgrado en respuesta a una citación judicial, sin avisarle antes[18].
- **Alguien del grupo es informante o policía encubierto.** En el caso federal de 2026 contra les Minnesota 15, agentes encubiertos se unieron a chats grupales de Signal de activistas[6] y compartieron lo que leían, que luego la fiscalía usó en el juicio.

CÓMO MANTENER TUS PLANES FUERA DEL REGISTRO ESCRITO

Evita poner por escrito las cosas más riesgosas, ya sea en mensajes, documentos o incluso notas en papel.

**Antes de escribir algo, pregúntate: "¿Me parecería bien escuchar esto leído en voz alta en un juicio contra mí?"** Si no, guárdalo para una conversación en persona (idealmente con todos los teléfonos y dispositivos en otro cuarto).

Cosas que quizás prefieras no poner por escrito:

- Que planeas hacer algo que implica riesgo de arresto (incluso una sentada muy tranquila normalmente viola alguna ley de allanamiento)
- Quién participa en el grupo o la acción
- Quién está a cargo
- En el caso de acciones: el lugar, las tácticas y datos que identifiquen a las personas involucradas
- Otros grupos involucrados
- Chistes, desahogos o sarcasmos que podrían leerse como una amenaza o intención real.

Último paso: crea hábitos para **borrar o destruir lo que sí pusiste por escrito en cuanto ya no lo necesites**. Esto se suele olvidar, así que ayuda tener formas de rendir cuentas.

**Trata los grupos grandes o abiertos como si alguien adentro fuera informante.** Por lo general, no puedes saber quién es informante. Y no es buena idea ponerse a "buscar al soplón" dentro de un grupo. Entre más personas haya en un grupo, más difícil es conocer a todo el mundo. Deja las conversaciones más delicadas para grupos pequeños de personas que conoces y en las que confías.

## 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[19]. 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.

# Protege tu teléfono (para quienes lleven teléfono)

Si eres de las personas que van a llevar teléfono y tienes datos muy sensibles en tu teléfono principal o corres un alto riesgo de que los policías te tengan en la mira, te recomendamos seguir todos los pasos de esta guía con un teléfono secundario[4] que tenga menos datos.

- [ ] **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[20]
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[20]
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[20]
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[20]
3. **Apps de la Microsoft Store:** Asegúrate de activar las actualizaciones automáticas[21] (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.

## 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[22] 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[22]. (¡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[22].

## Desactiva el desbloqueo facial/por huella digital (biométrico)

Tienes mayor protección legal[23] 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**.

## ☐ 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.

# Durante la acción (si llevaste teléfono)

### 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.

### Dale tu teléfono a alguien que no se arriesgue a ser arrestade

No tener tu celular contigo cuando te detienen es la mejor forma de proteger tus datos y al movimiento. Apagarlo por completo es la segunda mejor opción.

CÓMO DARLE TU TELÉFONO A ALGUIEN QUE NO SE ARRIESGUE A SER ARRESTADE

- **Si planeas arriesgarte a que te arresten**: apaga tu teléfono y dáselo a tu persona de apoyo designada antes de empezar la acción.
- **Si necesitas un teléfono durante la acción**: Quienes tienen un rol de apoyo (táctico, primeros auxilios, desescalada, etc.) pueden necesitar un teléfono durante la acción. Dependiendo de cómo esté diseñada la acción y de lo impredecibles que sean los policías, puede que puedan irse o no cuando aumente el riesgo de arresto.
  - Si el diseño de tu acción lo permite y necesitas tu teléfono hasta el último momento, entrégaselo a alguien.
  - Si necesitas tu teléfono y no puedes entregárselo a nadie, asegúrate de apagarlo por completo antes del arresto.

# Después de la acción

### Después de la acción, borra los documentos de planificación y los grupos de Signal

Los chats y documentos viejos todavía se pueden leer si confiscan un teléfono o si más adelante una cuenta recibe una citación judicial.

Cuando termina la acción, ya no hacen falta los documentos ni los chats que crearon. Mientras más tiempo sigan existiendo, más posibilidades hay de que terminen en manos de la policía por un teléfono confiscado, una citación judicial o un informante dentro del grupo.

**Antes de la acción**, pónganse de acuerdo en un plan de limpieza. Creen un sistema para rendirse cuentas y asegurarse de cumplirlo.

> **Si arrestaron o acusaron a alguien, consulta con tu equipo de apoyo legal o con un abogado o abogada antes de borrar cualquier cosa.** Borrar registros cuando ya sabes que hay una investigación, cargos o una citación judicial, conocida como subpoena, puede considerarse destrucción de pruebas, que es otro delito aparte. Esta es otra razón para activar los mensajes temporales con un temporizador corto antes de la acción, así la mayoría de los mensajes ya habrán desaparecido.

CÓMO HACER LIMPIEZA DESPUÉS DE UNA ACCIÓN

1. **Borra los documentos.** Esto incluye documentos de planificación, documentos de Proton/CryptPad, hojas de cálculo, formularios de apoyo a personas detenidas y cualquier nota escrita. Luego vacía la papelera.
2. **Cierra los grupos de Signal**: los grupos de Signal pueden ser útiles para seguir organizándose, pero la lista de integrantes es un riesgo para todo el mundo si algún día confiscan el teléfono de alguien. En vez de mantener activo ese grupo pequeño, considera pasar a todo el mundo a un grupo más grande solo de anuncios para seguir organizándose.
   - Publica un mensaje avisando que el grupo se va a cerrar y pide a todo el mundo que borre el chat de su teléfono. Elimina tú a cada integrante para asegurarte de que se haga.
   - Borra el chat de tu propio teléfono: Signal → Pantalla principal → Desliza a la izquierda sobre el chat → **Eliminar**. (Esto no elimina el grupo de los teléfonos de las demás personas, solo del tuyo. Pero los mensajes temporales se borrarán automáticamente de los teléfonos de todo el mundo).
3. **Si no eres admin,** sal del grupo Y bórralo, y anima a las demás personas a hacer lo mismo.
4. **Destruye cualquier nota en papel**, mapa o lista.

# Aprende más

- CLDC - Espera lo inesperado: protege tu teléfono contra la confiscación o pérdida[24] (2021)
- Freedom of the Press Foundation - Qué hacer si los cops confiscan tu teléfono[25] (2016)

## Sigue aprendiendo con estas guías relacionadas

### Checklist de seguridad para quienes organizan acciones

Seguridad física, digital y legal para quienes organizan.

### Organiza una security party

Una agenda modelo para recorrer los checklists en grupo.

### Prepárate para una protesta

Seguridad digital para quienes asisten a una protesta.

# Enlaces

1. activistchecklist.org/es/contribute/
2. activistchecklist.org/es/action-safety/
3. activistchecklist.org/es/protest/
4. activistchecklist.org/es/secondary/
5. activistchecklist.org/es/party/
6. unwall.app/www.wired.com/story/ice-is-running-one-of-the-largest-anti-left-surveillance-operations-in-us-history/
7. signal.org
8. signal.org/download/
9. activistchecklist.org/es/signal/
10. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
11. proton.me/drive/docs
12. activistchecklist.org/es/proton/
13. proton.me
14. drive.proton.me
15. cryptpad.fr
16. jotform.com
17. activistchecklist.org/es/ice/
18. eff.org/deeplinks/2026/04/google-broke-its-promise-me-now-ice-has-my-data
19. nlg.org/chapters-2/
20. activistchecklist.org/es/updates/
21. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
22. strongphrase.net/passcode
23. ssd.eff.org/module/attending-protest
24. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
25. freedom.press/training/mobile-security-for-activists-and-journalists/