Seguridad digital para monitoreo de ICE

ACTIVIST CHECKLIST

Última actualización **2 de febrero de 2026** Toma unos **20 minutos - 2 horas**

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/ice/**

Traducido automáticamente: Esta página se tradujo automáticamente. Hasta ahora solo el 6% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

Para quién es esto: Cualquier persona que observe las actividades de ICE para exigirles cuentas: filmando, patrullas a pie, adopta-una-esquina o respuesta rápida. Esto incluye a ICE/DHS/CBP y cualquier agencia que colabore con ellos. (Nota: el trabajo de acompañamiento y el apoyo mutuo implican otros riesgos: muchas cosas de esta guía pueden servir en esas situaciones, pero no se diseñó específicamente para esas necesidades.)

Alcance: Esta guía busca ayudarte a reducir el riesgo de que tus datos privados queden expuestos al Estado o a actores de derecha. Incluye pasos para proteger tu identidad, ubicación, comunicaciones, planes de organización y dirección de tu casa.

Nota: Esta guía no aborda directamente la seguridad física, la seguridad operativa ni los riesgos legales relacionados con la observación de ICE. Aunque encontrarás prácticas que tocan esos temas, el objetivo de esta guía es ayudarte a manejar los riesgos digitales.

Riesgos: Las actividades principales de ICE giran en torno a la detención y la deportación. Pero la infraestructura digital es clave en cómo operan y en cómo intentan vigilar, reprimir y castigar los esfuerzos por exigir cuentas. Por ejemplo, sabemos que ICE está intentando rastrear a cualquiera que los filme[2]. Los agentes usan reconocimiento facial[3] y vigilan redes sociales, siguen hasta su casa a quienes los observan[4] y rastrean la ubicación[5] de la gente sin orden judicial. El gobierno federal ha intentado armar casos contra activistas por ejercer sus derechos de la primera enmienda. También sabemos que adversarios de derecha están infiltrando[6] hilos de Signal y doxeando[7] a activistas.

¡Pero podemos hacer mucho para protegernos! Puede sonar a mucho, pero el gobierno federal no es todopoderoso (aunque quiera hacerte creer que sí). Hay muchos pasos que podemos dar para hacerles más difícil la vigilancia digital y para cuidarnos unes a otres frente a tácticas represivas.

Nos cuidamos entre todes: Tu teléfono no solo tiene *tus* datos. Tiene tus grupos de Signal, tus contactos, fotos de personas de tu comunidad, hilos con otres organizadores, etc. Si te lo confiscan, tu red de organización puede quedar expuesta y en riesgo. Esta guía ofrece pasos para ayudarte a mantenerte a salvo a ti y a tu comunidad.

Contexto: Esta guía se creó en respuesta a la invasión de ICE en Minneapolis (a principios de 2026) y se hizo en consulta con organizadores de monitoreo de ICE de ahí y de todo el país.

Háganlo en crew. La seguridad del monitoreo de ICE funciona mejor cuando todo tu equipo está en la misma página. Consideren organizar una fiesta de seguridad[8] con tu patrulla, equipo de respuesta rápida o crew de filmación para que todes se configuren juntes.

Prácticas para todas las personas que observan a ICE

TODO EL MUNDO Esta sección es para todes quienes participan en el trabajo de exigir cuentas sobre las actividades de

ICE, incluyendo patrullas, filmar a ICE, hacer sonar silbatos, acompañamiento, etc.

Si solo tienes 15-20 minutos, empieza con estos puntos.

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[9] 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.

Usa Signal para mensajes y llamadas cifradas, especialmente para tu activismo y conversaciones políticas

Las llamadas y mensajes normales no son privados y los cops pueden vigilarlos fácilmente y obtenerlos

DO: Usa Signal

DO NOT: Usar Facebook Messenger, Telegram, mensajes de texto normales, etc. (Evita WhatsApp si es posible)

La mayoría de los mensajes y llamadas normales pueden ser vistos por tu compañía telefónica y el gobierno. Telegram es increíblemente inseguro[10]. (Más abajo te contamos lo que pensamos sobre WhatsApp.)

Signal es la mejor opción para mantener tus mensajes seguros y para que con quién hablas se mantenga privado.

CÓMO CONFIGURAR SIGNAL

1. Instala Signal[11] en tu teléfono.
2. Ya puedes enviar mensajes a tus contactos usando su número de teléfono (también deben tener Signal instalado). Si le vas a escribir a alguien nuevo con quien aún no tienes confianza, cuando sea posible intercambien nombres de usuario[12] en lugar de números de teléfono.
3. Para iniciar un mensaje nuevo: toca el ícono "Crear" en la esquina superior derecha de Signal y luego escribe el número de teléfono o el nombre de usuario de la persona
4. Activa los mensajes que desaparecen por defecto: Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Mensajes que desaparecen** → elige el tiempo que prefieras.
5. Sigue la Lista de Seguridad de Signal[13] para asegurarte de tener la mayor seguridad y privacidad

Cuándo usar Signal

Algunos ejemplos de cuándo te conviene especialmente usar Signal

- Hablar de una protesta o acción que no es pública
- Organizar una protesta o acción que es pública, pero quienes la organizan quieren proteger su privacidad
- Criticar al gobierno o a otras personas con poder

> **¡Sigue alzando la voz en público!** Pasar algunas conversaciones a Signal por seguridad no se trata de quedarse en silencio: se trata de organizarse de forma segura sin dejar de criticar abiertamente a quienes tienen el poder. No obedezcas de antemano[14].

¿Y qué pasa con WhatsApp? (Evítalo si puedes, úsalo si no te queda de otra)

Los mensajes de WhatsApp están protegidos con el método de cifrado desarrollado por Signal, así que el contenido de tus mensajes está seguro. Sin embargo, Meta recopila mucha información sobre con quién hablas, con qué frecuencia y en qué grupos estás. Solo en 2024, entregaron datos del 78% de las solicitudes del gobierno[15]. Tus mensajes están seguros, pero con quién te comunicas no lo está. Es una opción a considerar si es poco probable que la comunidad con la que trabajas se cambie a Signal. Es más seguro que los mensajes normales, Telegram, etc. Si usas WhatsApp, sigue nuestra lista de seguridad para WhatsApp[16] para activar la configuración estricta de la cuenta y reforzar tu configuración de privacidad.

- [ ] 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[17] 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.

Configura Signal para que sea lo más seguro y privado posible

Oculta tu nombre real, tu foto real, las vistas previas de mensajes, y crea un nombre de usuario

Los pasos a continuación te ayudan a protegerte si los cops te confiscan el dispositivo, o si alguien hostil (cops o de derecha) en un grupo de Signal intenta descubrir tu identidad.

La lista de abajo reúne los pasos más importantes. Para instrucciones más detalladas y pasos avanzados, lee nuestra Lista de Seguridad de Signal completa →[13]

CÓMO CONFIGURAR SIGNAL PARA QUE SEA MÁS SEGURO Y PRIVADO

Cambia estos ajustes de Signal:

- [ ] **Activa los mensajes que desaparecen por defecto:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Mensajes que desaparecen** → Configura el tiempo que quieras (Esto solo afectará a los chats que tú inicies.)

- [ ] **Cambia tu nombre visible para que no sea tu nombre real:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono en la parte superior → Toca el primer elemento con la silueta de una persona → Edita el nombre visible de tu perfil

- [ ] **Cambia tu foto de perfil para que no sea tu cara:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono en la parte superior → **Editar foto** → sube una foto genérica que hayas encontrado en internet que no tenga relación con tu identidad, trabajo, ubicación o intereses.

- [ ] **Crea un nombre de usuario y compártelo en vez de tu número de teléfono:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono en la parte superior → Toca el símbolo **@** → **Editar nombre de usuario** → elige un nombre de usuario que no tenga ninguna relación con tu identidad ni que hayas usado antes en otro lugar. Debe terminar en al menos 2 números. (Herramienta: Generador de nombres de usuario aleatorios[18]). Da este nombre de usuario[19] en vez de tu número de teléfono para aumentar tu privacidad.
  Ejemplo: `@CarefreeMoose.22`

- [ ] **Oculta las vistas previas de mensajes en las notificaciones:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → **Notificaciones** → **Contenido de la notificación** → Selecciona **Sin nombre ni contenido**

- [ ] **Oculta tu número de teléfono:**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Número de teléfono** → En **Quién puede ver mi número** → Selecciona **Nadie**

- [ ] **Activa el teclado incógnito (solo Android):**
  Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Seguridad de la app** → Activa **Teclado incógnito**

Prácticas continuas en Signal:

- Si alguien más inicia un nuevo chat (o grupo), puede que no tenga los mensajes que desaparecen activados. Asegúrate de activar los mensajes que desaparecen en ese chat específico si no lo hicieron.
- Comparte tu nombre de usuario de Signal en vez de tu número de teléfono real.

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.

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 por completo el desbloqueo facial/por huella (biometría)

Te protege si la policía intenta forzarte a desbloquear tu teléfono.

La policía puede intentar forzarte a desbloquear tu teléfono con tu cara/huella[23] (aunque se supone que esto requiere una orden judicial, eso no significa que siempre pase así).

Tienes mayor protección legal[24] con un código de acceso que con el desbloqueo biométrico.

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 el reconocimiento facial como el desbloqueo por huella** para desbloquear tu teléfono

Ten en cuenta: el desbloqueo facial/por huella puede facilitar usar un código de acceso fuerte sin tener que escribirlo cada vez. Si sientes que tienes que elegir entre un código de acceso largo y desactivar la biometría, te recomendamos un código de acceso más largo.

Tip para bloquear el iPhone: Para forzar tu código de acceso en el siguiente desbloqueo, presiona el botón lateral 5 veces seguidas, o mantén presionado el botón lateral junto con cualquiera de los botones de volumen por unos segundos.

Pruébalo primero: dependiendo de tu configuración, estos gestos también pueden iniciar una cuenta regresiva para llamar a servicios de emergencia. Puedes cambiar eso[25].

Nota: Hacer esto no protege tus datos de las herramientas de hackeo de teléfonos que usa la policía. La única forma de hacerlo es apagar completamente tu dispositivo.

Tip para bloquear Android: En la mayoría de los teléfonos Android, puedes desactivar temporalmente el desbloqueo facial/por huella manteniendo presionado el botón de encendido y tocando "Bloqueo" en el menú que aparece.

Tip 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 la mayoría de los teléfonos Android, puedes abrir la cámara sin desbloquear tu teléfono presionando dos veces el botón de encendido.

Filmar de forma segura

TODO EL MUNDO Esta sección es para cualquiera que filme a ICE u otros agentes del gobierno.

El objetivo de filmar a los cops es doble:

1. **Disuasión** - Sabemos que filmar no evita el daño, pero a veces reduce la posibilidad de que ocurra.
2. **Documentación/rendición de cuentas** - Si alguien resulta herido, tenemos la documentación para mostrar a los tribunales y al público.

Es completamente legal y está protegido por la Constitución filmar a los cops[26]. Mira este video de capacitación de la ACLU[27].

☐ Graba videos sin desbloquear tu teléfono (¡solo desliza a la izquierda!)

Protege tus datos si te confiscan el teléfono mientras estás grabando

Si te confiscan el teléfono mientras estás grabando o tomando fotos, la policía puede acceder a todo.

Tu teléfono te permite tomar fotos sin desbloquearlo primero, así tus datos quedan más seguros.

CÓMO GRABAR SIN DESBLOQUEAR TU TELÉFONO

Primero, asegúrate de tener el desbloqueo facial desactivado[28]. Si lo tienes activado, tu teléfono podría desbloquearse automáticamente aunque sigas en la pantalla de bloqueo.

IPHONE

Desliza a la izquierda en la pantalla de bloqueo. (O mantén presionado el ícono de la cámara.)

ANDROID

Desliza a la izquierda en la pantalla de bloqueo, o presiona dos veces el botón de encendido (si está activado en **Ajustes** → **Sistema** → **Gestos** → **Abrir cámara rápidamente**).

Comparte videos de encuentros con ICE con cuidado (no los publiques en internet de inmediato)

En algunas situaciones, publicarlos puede poner a otrxs activistas en riesgo legal

DO: Coordina con tu red activista antes de compartir o publicar

DO NOT: Publicar en internet apenas termines de grabar

Los videos de interacciones con los cops son muy importantes en nuestro trabajo. Y también pueden generar riesgo legal para activistas u otras personas.

Antes de publicar, consulta con tu red activista y/o con abogadxs alineadxs con el movimiento.

CÓMO COMPARTIR VIDEOS E IMÁGENES DE FORMA SEGURA

- **Consulta a la comunidad activista:** Las personas de tu red son las más indicadas para saber cómo usar los videos de forma que proteja a nuestras comunidades y a la vez responsabilice a quienes nos atacan
- **Consulta a abogadxs alineadxs con el movimiento:** Pregunta en tu comunidad si hay abogadxs locales que estén alineadxs con tu causa. Si no sabes con quién hablar, contacta a CLDC[29] (línea de respuesta rápida: 541-603-6891) o al NLG[30].

Comparte videos/fotos de forma segura (vía Signal, etc.)

DO: Envía fotos usando canales cifrados: Signal, Proton Drive u OnionShare

DO NOT: Usar un sistema de almacenamiento en la nube como Google Photos o iCloud

Si compartes videos/fotos sensibles con activistas o abogados de confianza, conviene hacerlo por canales seguros. Proveedores de nube como Apple o Google podrían entregarle tus datos a la policía con una orden judicial.

CÓMO COMPARTIR VIDEOS DE FORMA SEGURA

- Signal[11]: Compartir archivos por Signal es lo más fácil y seguro. También elimina automáticamente los "metadatos" (como la ubicación). Pero ten en cuenta que si tu video es largo, se reducirá la calidad.

  Calidad: Asegúrate de activar el envío de archivos en "alta calidad" en la configuración de Signal. Abre Signal → Toca tu foto de perfil → **Settings** → **Data and storage** → **Media quality** → **Sent media quality** → Selecciona **High**

- Proton Drive[31]: Puedes almacenar archivos hasta 5GB con una cuenta gratuita.
- OnionShare[32]: Lo mejor si necesitas enviar muchos archivos grandes. Cifrado de extremo a extremo. Quien lo reciba tendrá que usar Tor Browser[33].

Avanzado: ¿Quieres guardar tus videos con un nivel extra de seguridad/cifrado? Échale un ojo a Tella[34]. ¿Quieres agregar metadatos verificables que demuestren que tomaste el video en un momento determinado y que no ha sido alterado? Échale un ojo a Proofmode[35].

Considera usar una cámara "normal" para filmar (si es posible)

La mayoría de los consejos de seguridad digital de esta página tienen que ver con que te confisquen o vigilen el teléfono.

Si puedes arreglártelas sin tu teléfono y consigues una cámara "normal", eso te da aún más protección.

Si tienes el teléfono completamente apagado, está mucho más protegido de la vigilancia o de las herramientas de "hackeo de teléfonos" que usan los cops.

CÓMO USAR UNA "CÁMARA NORMAL" PARA FILMAR

Opción 1: Sin el teléfono contigo. Lo más seguro es no llevarlo encima mientras filmas, por si te arrestan, pero muches lo necesitamos.

Opción 2: El teléfono contigo pero completamente apagado. Asegúrate de que tenga un código de acceso fuerte y el sistema operativo más reciente.

Cámaras a considerar:

- Cámara de acción (GoPro, Akaso, Crosstour, etc.)
- Body cam o cámara corporal (BOBLOV, etc.)
- Consigue una cámara compacta
- O simplemente lleva un teléfono secundario

Elimina la info oculta de las fotos (ubicación, etc.) antes de publicarlas o compartirlas

Las fotos que compartes pueden revelar tu ubicación o identidad si no eliminas esos datos antes

Por defecto, las fotos y videos de tu celular incluyen datos ocultos ("metadatos") que revelan tu ubicación GPS exacta, la fecha y hora, y el modelo de tu celular.

Si publicamos la foto en internet, los cops o adversarios de derecha pueden usar estos metadatos para rastrearte e identificarte.

Cuándo conservar los metadatos: Si estás documentando abusos o violencia (de los cops, actores de derecha, etc.), guarda un original con los metadatos por si llega a servir como prueba legal. Pero sí elimina los metadatos cuando vayas a compartir algo públicamente.

CÓMO ELIMINAR LA INFO OCULTA DE LAS FOTOS ANTES DE COMPARTIRLAS

Nuestra recomendación: Envíalas por Signal

A cualquier foto o video que envíes por Signal se le eliminan automáticamente todos los metadatos.

Si quieres compartirla en internet, puedes enviarte la foto a ti misme, volver a guardarla desde Signal y borrar la original.

Otras opciones seguras

- La app web Image Scrubber[36] te ayuda a eliminar los metadatos, pero solo de imágenes.
- ExifCleaner[37] - App de escritorio (Mac, Windows)
- ImageOptim[38] - App para Mac

Prácticas para observadores frecuentes de ICE

AMENAZA MEDIA Esta sección es para cualquiera que haga trabajo frecuente para exigir cuentas a ICE. Mejorar tu seguridad es importante porque estás asumiendo más riesgo.

Importante Considera tener un teléfono secundario para ICE watch y respuesta rápida

Protégete a ti y a tu comunidad: si te confiscan el teléfono, habrá menos datos expuestos

El trabajo de ICE watch y respuesta rápida implica un mayor riesgo de arresto. La mejor forma de protegerte a ti y a tu comunidad es tener ***la menor cantidad posible de datos*** en el teléfono que puedan confiscarte. Y la forma más fácil de lograrlo es llevar contigo solo un teléfono secundario cuando hagas trabajo de mayor riesgo.

Conseguir un teléfono extra no está al alcance de todes, pero te animamos a pedir apoyo en tu red—mucha gente tiene teléfonos viejos guardados que aún funcionan.

No dejes que la falta de un teléfono secundario te impida hacer este trabajo.

Qué debería tener un teléfono secundario:

- Números de teléfono de cualquier persona con quien necesites estar en contacto (amistades, familia, hijes, etc.)
- Hilos de Signal solo del trabajo de ese día (sal de todos los demás hilos de Signal, borra todos los DMs)
- Una app de mapas privada como Magic Earth
- Fotos/videos documentando a ICE (borra todo lo que no sea de hoy después de guardarlo en un lugar seguro)
- ... ¡Y casi nada más!

Opción 1: El enfoque más anónimo

CÓMO CONSEGUIR UN TELÉFONO SECUNDARIO MÁS ANÓNIMO

- Sigue nuestra guía detallada del teléfono secundario[39] si quieres más anonimato. Esto te ayudará si crees que podrías ser blanco de vigilancia estatal (que rastreen la ubicación de tu teléfono por tu trabajo político). Esta guía toma varias horas para completarse.

Opción 2: El enfoque más fácil

CÓMO CONSEGUIR UN TELÉFONO SECUNDARIO MENOS ANÓNIMO

No todes necesitan el anonimato extra de la Opción 1. Este enfoque más fácil está vinculado a tu identidad—la meta principal es simplemente minimizar los datos en tu teléfono para no poner en riesgo a la gente con la que organizas si te lo confiscan.

1. **Consigue un teléfono:** Cualquier teléfono sirve—pregunta por ahí si alguien tiene uno viejo. Pide a alguien con conocimientos técnicos que revise si está "desbloqueado" (que acepte cualquier SIM).
2. **Consigue servicio:** Compra una SIM prepagada (Tracfone, Mint Mobile) en Costco, Walmart o una tienda de barrio. O agrega una línea a tu plan actual.
3. **Crea una cuenta nueva de Apple/Google:** No inicies sesión con tu cuenta normal—tus datos se sincronizarían y eso arruina el propósito.
4. **Deja tu teléfono principal en casa:** Lleva solo el teléfono secundario para el trabajo de alto riesgo. Avísale a tus contactos cercanos que pueden localizarte ahí en caso de emergencia.
5. **Mantén los datos al mínimo:** No conviertas este en tu teléfono para todo el activismo—si te lo confiscan, igual tendría datos riesgosos. Únete solo al hilo de Signal del día, sáltate los canales generales de coordinación y sal de los hilos cuando termine tu turno.

Nota: Si tienes que llevar tu teléfono principal contigo para emergencias, asegúrate de que 1) esté apagado, 2) tenga el sistema operativo actualizado y 3) tenga un código de acceso de 8 dígitos verdaderamente aleatorio. Esos tres elementos juntos harán que sea difícil para los cops descifrarlo.

Usa una app de mapas/navegación que respete tu privacidad (Apple Maps o Magic Earth)

Protégete de que Google entregue tus datos a los cops

DO: Usa Apple Maps[40] (solo iPhone) o Magic Earth[41] (gratis)

DO NOT: Usar Google Maps

Tu historial de ubicación revela mucho sobre tus intereses, tus amistades y tu actividad política. También pueden usarlo en tu contra en un juicio.

Tu teléfono siempre le revela tu ubicación aproximada a tu compañía celular, porque sabe a qué torre celular estás conectade. Pero cualquier app a la que le des tu ubicación GPS exacta tiene mucho más detalle.

Puedes protegerte usando una app de mapas que cuide más tu privacidad.

Apple Maps (solo iPhone) ofrece protecciones de privacidad[42] más fuertes de lo que podrías esperar y es mucho más privado que Google. Sin embargo, al ser una gran empresa de tecnología, es mejor para el uso cotidiano y no tanto para organización sensible. Lo recomendamos porque tiene funciones de tráfico en vivo y transporte público que las alternativas centradas en la privacidad no tienen.

CÓMO CONFIGURAR APPLE MAPS (SOLO IPHONE)

1. Apple Maps[40] viene instalado por defecto (puedes reinstalarlo si lo eliminaste).
2. Ve a **Ajustes** → **Privacidad y seguridad** → **Localización** → **Servicios del sistema**, y desactiva **Análisis del iPhone**, **Rutas y tráfico** e **Mejorar Mapas**.

Magic Earth[41] (iPhone o Android; gratis) ofrece una privacidad sólida. Es mucho más fácil de usar que nuestra otra sugerencia multiplataforma (CoMaps). Eso sí, algunas funciones solo están disponibles en la versión de paga.

CÓMO CONFIGURAR MAGIC EARTH (IPHONE O ANDROID)

1. Instala Magic Earth[41] (gratis; de paga para tráfico en vivo)
2. ¡Funciona prácticamente igual que Google Maps o Apple Maps!

CoMaps[43] (iPhone o Android; gratis) es menos fácil de usar que Magic Earth o Apple Maps, pero tiene las promesas de privacidad más fuertes. Puedes usarlo completamente sin conexión, lo cual es muy útil para activistas que hacen trabajo sensible. Dicho esto, no tiene datos de tráfico en vivo ni rutas de transporte público, lo que dificulta usarlo como tu app principal de navegación.

Activa el Modo Aislamiento (iPhone) o Protección Avanzada (Google y Android)

El spyware es un tipo de ataque avanzado que aprovecha vulnerabilidades sofisticadas en nuestros dispositivos. En respuesta, Apple y Google han creado un modo de seguridad avanzado que ofrece mayor protección contra el spyware.

En los iPhone se llama **Modo Aislamiento**[44] y en Android se llama **Programa de Protección Avanzada**[45]. (También puedes activar el Programa de Protección Avanzada solo en tu cuenta de Google aunque no tengas un teléfono Android.)

No tenemos reportes de nadie que se haya infectado con spyware teniendo activado el Modo Aislamiento de Apple. La Protección Avanzada de Android es más reciente y todavía no se ha podido comprobar qué tan efectiva es.

Compromisos de uso: Ambas funciones implican sacrificar algunas funcionalidades. Mira la lista completa de compromisos[46]. Si te topas con problemas que no te funcionan, siempre puedes desactivar la función después.

CÓMO ACTIVAR EL MODO AISLAMIENTO EN IPHONE

IPHONE

Ajustes → **Privacidad y seguridad** → **Modo Aislamiento** → **Activar**

Esta función está disponible para iOS 16 en adelante.

CÓMO ACTIVAR LA PROTECCIÓN AVANZADA EN ANDROID

ANDROID

Ajustes → **Seguridad y privacidad** → en **Otros ajustes** toca **Protección Avanzada**

Nota: La ubicación de este ajuste puede variar entre dispositivos Android, así que te recomendamos buscar 'Protección Avanzada' en la barra de búsqueda de Ajustes.

Esta función está disponible para Android 16 en adelante.

Importante Elimina tu información de los sitios de "búsqueda de personas" usando un servicio automatizado (como EasyOptOuts)

Usar una herramienta para eliminar tu información automáticamente de todos estos sitios te ahorra mucho tiempo.

DO: Regístrate en EasyOptOuts[47] ($20/año) — o en Optery Ultimate[48] ($249/año) para mayor cobertura

DO NOT: No recomendamos DeleteMe porque es menos efectivo que EasyOptOuts

Los **sitios de "búsqueda de personas"** son un tipo de "data broker". Recopilan información de registros públicos y privados para armar un "perfil" de prácticamente cualquier persona. Si alguna vez has tenido un número de teléfono, usado una tarjeta de crédito o votado, probablemente estés en alguno de estos sitios.

Pruébalo: Busca tu nombre o número de teléfono en este sitio[49] (lo usamos como ejemplo porque muestra los resultados al instante, sin pedirte que te registres). A la mayoría de la gente le sorprende cuánta información está disponible fácilmente. Otros sitios importantes de esta categoría son Whitepages, Spokeo, BeenVerified, y un número creciente de herramientas de búsqueda con IA.

Por qué pagar por servicios de eliminación automática: Puedes hacer este proceso de "exclusión" manualmente, pero toma una cantidad enorme de tiempo, y tienes que repetirlo cada pocos meses cuando los sitios de corredores de datos cambian. Es ridículo que tengamos que pagar para proteger nuestra privacidad, pero nos ahorra mucho tiempo para enfocarnos en nuestra organización.

¿Qué herramienta de eliminación automática debería usar?

- **EasyOptOuts**[47] **(recomendado)** - $20/año - Es de los más efectivos[50] y el más barato.
- **Optery Ultimate**[48] - $250/año - Un poco más efectivo si puedes pagar la inversión adicional. Pueden tomar una copia de tu identificación (con el número de ID borrado) y excluirte de los sitios que requieren una identificación.
- **¿Y qué hay de DeleteMe? -** Es la opción más conocida, pero solo fue 27% efectiva eliminando perfiles, comparada con EasyOptOuts (65%) y Optery Ultimate (68%). (Fuente[51]).

CÓMO ELIMINAR TU INFORMACIÓN DE LOS SITIOS DE "BÚSQUEDA DE PERSONAS" USANDO EASYOPTOUTS

Tiempo requerido: 5–15 minutos

1. **Regístrate en EasyOptOuts**[47] ($20/año)
2. **Ingresa tu información personal:** Sigue las indicaciones. Lo más importante es incluir tu información **actual** (dirección, teléfono, correo). Si no logras encontrar todas tus direcciones anteriores, no pasa nada.

   > **Advertencia:** NO ingreses **alias** ni **números de teléfonos desechables** que uses exclusivamente para el activismo y que ya estén completamente separados de tu identidad real. No querrías que queden vinculados dentro de este sistema.

3. Continúa con el siguiente punto de la lista para hacer **exclusiones manuales** en los sitios que EasyOptOuts no puede manejar.
4. Considera pedirle a cualquier persona que viva en tu casa que también se registre. Si alguien descubre que viven juntes, podría buscar a esa persona con la misma facilidad y luego atacarte a ti.

Tiempos: Las primeras eliminaciones pueden tardar unos días en completarse, y a veces hasta un par de meses para ciertos sitios.

Para tu información: No recibimos comisiones por ninguno de los servicios pagos a los que enlazamos. Los recomendamos porque son los más efectivos que hemos encontrado.

Privacidad de EasyOptOuts: A algunas personas les preocupa ingresar toda su información en un sitio así. Aunque ningún sitio está libre de filtraciones de datos, confiamos en este sitio por su historial y reputación. Y la información es necesaria para hacer las eliminaciones.

Herramienta alternativa: Kanary[52] es una app gratuita que busca tu información personal en Google y te guía para eliminarla manualmente. Aun así requiere mucho tiempo y es probable que la gente la abandone antes de terminar todas las eliminaciones.

Sal de Clearview AI para ponerle más difícil a la policía el reconocimiento facial

Ayuda a que sea más difícil para la policía criminalizarte por tu protesta legal

ICE está usando Clearview AI[53] para atacar a manifestantes y observadores. Muchas agencias policiales también usan esta plataforma para hacer vigilancia sin orden judicial.

Puedes protegerte excluyendo tus datos de Clearview AI. (Para que sepas - ICE está invirtiendo en otras herramientas de reconocimiento facial[54] de las que no te puedes excluir.)

CÓMO EXCLUIR TUS DATOS DEL RECONOCIMIENTO FACIAL DE CLEARVIEW AI

Envía un formulario de exclusión para Clearview AI[55] - Requiere enviar una foto tuya.

Lamentablemente, la exclusión solo es posible en estados que han aprobado leyes de privacidad.

Instala una app de VPN confiable con bloqueo de anuncios para dificultarle a los cops la vigilancia sin orden judicial

Una VPN hace que sea más difícil que los sitios web te rastreen y evita que tu proveedor de internet registre tu tráfico.

DO: Instala una app de VPN confiable en tu(s) dispositivo(s) y déjala encendida. Recomendamos IVPN[56] ($6/mes).

DO NOT: Usar cualquier VPN que encuentres por ahí en internet. Nord VPN, Surfshark, ExpressVPN, etc., son populares pero no tan confiables.

Cada vez que te conectas a internet (desde el teléfono o la computadora), tu proveedor de internet le está revelando tu ubicación aproximada a cada sitio o app que usas.

Sabemos que las agencias policiales están usando herramientas para rastrear tu ubicación[5] con datos recopilados de las apps que tienes y los anuncios que ves. Usar una VPN con el bloqueo de anuncios activado hace mucho más difícil que te rastreen. Además, una VPN verificada no rastreará tu navegación; los cops pueden conseguir una citación (subpoena) para acceder a tu tráfico de internet que rastrea tu proveedor de internet.

Una VPN ayuda a ocultar tu ubicación y hace que sea un poco más difícil identificarte.

Tener una VPN con bloqueo de anuncios activado en tu teléfono puede ayudar a evitar el rastreo de ubicación sin orden judicial (a través de redes publicitarias).

Revisa nuestra página dedicada a VPN[57] para más info sobre cuándo una VPN es realmente útil y cuándo no.

Una VPN no te hace totalmente anónime. Para navegación sensible que requiera mayor anonimato, considera usar Tor Browser[58] como segundo navegador junto al que usas a diario.

Opciones: Estas son las VPN que recomendamos para la mayoría de activistas (ve nuestra lista completa de VPN verificadas[57]):

- **IVPN**[59] **(recomendación principal)**: Fácil de usar y se renueva automáticamente.
- **Proton VPN**[60] tiene un plan gratuito sólido, pero solo sirve para 1 dispositivo. Para obtener bloqueo de anuncios, necesitas un plan pagado. (Si usas Proton, revisa nuestra guía para usar Proton de forma segura[61].)

CÓMO CONFIGURAR IVPN

1. **Genera tu cuenta:** Ve a IVPN y haz clic en Generate IVPN Account[62] ($6/mes o $60/año). En **Standard Plan** haz clic en **Select** (elige el **Pro Plan** si tienes más de 2 dispositivos).
2. **Anota tu Account ID:** Guárdalo en un lugar seguro, como tu gestor de contraseñas. No hay opción de "olvidé mi contraseña", así que si lo pierdes, nadie podrá recuperarlo por ti.
3. **Paga:** Selecciona mensual o anual, marca la casilla **Automatic renewal**, ingresa tus datos de pago y haz clic en **Make Payment**.
   - En lugar de una tarjeta de crédito, también puedes pedir una tarjeta de voucher para IVPN[63] para proteger aún más tu identidad.
4. **Instala la app de escritorio** (Mac[64], Windows[65]) e inicia sesión con tu Account ID.
5. **Activa la conexión automática:** Busca IVPN en tu barra de herramientas → **Show IVPN** → ⚙️ **Ícono de engranaje** → **Settings** → **General** y activa **Launch at login**, **Autoconnect on launch** y **Allow background daemon to manage autoconnect**.
6. **Activa el bloqueo de anuncios:** Enciende **AntiTracker** en la pantalla principal de la app de IVPN para bloquear anuncios (esto ayuda a mantener tu ubicación privada, sobre todo en tu teléfono).
7. **Instala la app móvil** (iPhone[66], Android[67]) e inicia sesión con el mismo Account ID, luego activa las mismas opciones mencionadas arriba. (En iPhone, la conexión automática no es una opción porque viene activada por defecto.)

Recomendamos mantener tu VPN encendida todo el tiempo, salvo que tengas problemas para conectarte a algún sitio (ve nuestra lista de desventajas de usar una VPN[57]).

Por qué ya no recomendamos Mullvad: Mullvad solía ser la VPN #1 más recomendada por activistas y personas en riesgo. Su tecnología VPN sigue siendo la mejor que existe, pero uno de sus cofundadores arruinó recientemente su excelente reputación al donar cientos de miles de dólares[68] a un partido político de extrema derecha en Suecia. Así que ya no podemos recomendarla.

Prácticas para coordinadores de grupo

AMENAZA ALTA **Esta sección es para:**

→ Cualquiera que asuma un rol de **coordinación** dentro de las redes de monitoreo de ICE.

→ Cualquiera que asuma un rol intencionalmente **público**

Asegúrate de hacer también todo lo de las secciones anteriores.

☐ Usa Proton Docs y Proton Mail para el activismo en lugar de Google Docs y Gmail

Protégete a ti y a tu comunidad de las solicitudes de datos del gobierno de las que no te enteras.

DO: Usa Proton Docs[69] y Proton Mail[70]

DO NOT: Usar Google Docs y Gmail para comunicaciones de activismo

Las empresas de tecnología (como Google) a menudo reciben solicitudes del gobierno[71] para entregar todos los datos de la cuenta[72] de una persona activista. Esto suele incluir una "orden de silencio", lo que significa que la empresa no puede avisarle a la persona usuaria hasta meses o años después.

Las herramientas en la nube cifradas como Proton Mail[70], Drive[73], Docs[69] y Sheets[74] hacen que la empresa no tenga copias legibles de tus datos que pueda entregar. Si el gobierno los quiere, tendría que pedírtelos a ti, dándote aviso y la oportunidad de impugnarlo con apoyo legal.

Límites del correo cifrado: Proton cifra todo en sus servidores. Pero el cifrado solo protege ambos extremos si quien recibe también usa correo cifrado. Si le envías un correo a alguien que usa Gmail, Google tiene una copia que puede entregar.

Para comunicación sensible, siempre usa Signal con los mensajes que desaparecen activados.

CÓMO CONFIGURAR Y USAR PROTON DOCS Y PROTON MAIL

Crea una cuenta de Proton

Sugerencia: Elige un nombre de usuario aleatorio[18] y un nombre para mostrar aleatorio[75]. así tienes la opción de no revelar que compartes esta dirección de correo.

1. **Regístrate** para obtener una cuenta gratuita de Proton[76].
2. **Verifica:** Cuando te pidan verificar que eres humano, elige la opción "CAPTCHA" en vez de la opción "email", para que no vincules tu identidad real.
3. Cuando te pidan poner tu número de teléfono o correo como método de recuperación, elige **Quizás más tarde.**

Usa Proton Drive/Docs/Sheets

- **Crea y edita** documentos de forma colaborativa, parecido a Google Docs. La otra persona necesita tener una cuenta de Proton para compartirlos directamente.
- **Comparte de forma segura:** Solo usa "compartir por enlace" cuando sea necesario, ponle contraseña al documento y configura el "enlace público" con fecha de vencimiento.

Usa Proton Mail

- **Usa Proton Mail para:** cuentas de sitios web, boletines, comunicaciones públicas que necesiten anonimato y trabajo de organización no sensible.
- **No uses ningún correo para:** comunicaciones realmente sensibles que puedan poner a alguien en riesgo legal.
- **Qué se cifra y qué no:** Los mensajes entre personas que usan Proton Mail se cifran de extremo a extremo automáticamente. Los mensajes a personas que usan otro proveedor de correo no estarán cifrados, pero puedes enviar un correo protegido con contraseña[77].

CryptPad[78] es otra opción popular de documentos cifrados, pero es muy difícil de usar. Si tiene las funciones que necesitas, logra el mismo resultado.

Usando Proton de forma segura: Proton es una gran mejora frente a Gmail/Google Docs, pero tiene limitaciones reales que debes conocer. Consulta nuestra guía para usar Proton de forma segura[61] para saber qué está cifrado, qué no, y cómo evitar errores comunes.

Excluye tus datos de los sitios de "búsqueda facial"

Protégete para que una foto tuya no se use para descubrir tu identidad.

Puedes protegerte excluyendo tus datos de los sitios de "búsqueda inversa de fotos". Esto hace más difícil que alguien use tu foto de perfil en línea para averiguar tu nombre legal, lo cual podría llevarles a encontrarte en los sitios de búsqueda de personas mencionados arriba.

CÓMO ELIMINARTE DE LOS SITIOS DE "BÚSQUEDA FACIAL"

Cada uno de estos sitios (irónicamente) te pedirá que subas una foto de tu rostro. Es un mal necesario si quieres que te eliminen. Tienes que decidir si el riesgo de darles más datos vale la pena para lograr la exclusión.

> **Nota sobre subir tu identificación oficial**: Algunos de estos sitios son terribles y te piden subir una foto de tu identificación oficial o pasaporte con la información sensible oculta. Lo más fácil es poner cinta adhesiva sobre todo lo que aparece en tu identificación, excepto tu nombre y foto, y luego tomar la foto.

Sitios de los que excluirte:

1. Excluirse de Clearview.ai[55] - Solo requiere una foto, no una identificación oficial. Lamentablemente, la exclusión solo es posible en estados que han aprobado leyes de privacidad. ***Clearview lo usan principalmente las agencias policiales, así que es importante excluirte.***
2. Excluirse de PimEyes[79] - Requiere una foto de tu identificación oficial. (¡Tapa tu número de identificación!)
3. Excluirse de FaceCheck.ID[80] - En lugar de subir una identificación oficial, puedes subir una selfie en la que toques tu barbilla con dos dedos. Además, debes seleccionar manualmente las fotos que quieres que eliminen.

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**

Activa la Protección Avanzada de Datos de iCloud (iPhone) o el Programa de Protección Avanzada de Google

Apple, Google y otros servicios ofrecen funciones de seguridad adicionales para protegerte de ataques dirigidos a tus cuentas y datos. Estas protegen tus cuentas en línea con cada empresa, no el dispositivo en sí.

La Protección de datos avanzada de Apple activa el cifrado de extremo a extremo para la mayor parte de tu contenido.

CÓMO ACTIVAR LA PROTECCIÓN AVANZADA EN TUS CUENTAS DE CORREO/NUBE

Protege tus datos:

- Protección de Datos Avanzada de iCloud[81] - Activa el cifrado de extremo a extremo para casi todos los datos guardados en iCloud, protegiendo tu información frente a órdenes judiciales del gobierno. Asegúrate de guardar la clave de recuperación en un lugar muy seguro (como un gestor de contraseñas[82]).

Protege tu cuenta:

- Programa de Protección Avanzada de Google[83] - Ayuda a proteger tu cuenta contra phishing y accesos no autorizados.
- Account Guard de Microsoft[84]
- Proton Sentinel[85]

☐ Configura Signal para que tu número de teléfono no sea localizable

Aunque tu número de teléfono no es visible en Signal por defecto, la gente todavía puede escribir tu número y encontrarte. Si estás en riesgo de acoso, tal vez prefieras compartir solo tu nombre de usuario de Signal[19] con la gente.

CÓMO HACER QUE TU NÚMERO DE TELÉFONO NO SEA LOCALIZABLE EN SIGNAL

1. **Si quieres cambiar tu nombre de usuario:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → Toca el símbolo **@** → **Editar nombre de usuario** → elige un nombre de usuario **completamente ajeno** a tu identidad, o a cualquier nombre de usuario que hayas usado antes en otros lugares. Debe terminar en al menos 2 números.
2. **Oculta tu número de teléfono:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Número de teléfono** → En **Quién puede ver mi número** → Selecciona **Nadie**.
3. **Haz que tu número de teléfono no sea localizable:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Número de teléfono** → En **Quién puede encontrarme por número** → Selecciona **Nadie**.
4. Dile a la gente tu nombre de usuario en vez de tu número de teléfono cuando quieras conectar con ellos en Signal.

☐ Usa chats grupales pequeños con temporizadores cortos de mensajes que desaparecen

Un chat de 50 personas significa 50 celulares que pueden ser confiscados, perdidos o vulnerados; cualquiera de ellos expone toda la conversación. Aunque a veces necesitamos grupos grandes en Signal, no manejes toda tu organización a través de un solo chat grupal grande. Cuando estés coordinando algo específico —una acción, un proyecto, una decisión delicada— arma un grupo pequeño solo con las personas que necesitan estar ahí, y configura los mensajes para que desaparezcan rápido.

CÓMO MANTENER PEQUEÑOS LOS GRUPOS DE SIGNAL

- **Crea un grupo pequeño** solo con las personas directamente involucradas en un proceso.
- **Configura un temporizador corto para los mensajes que desaparecen** (de 1 hora a 1 día para coordinación activa; máximo 1 semana para trabajo continuo). Los mensajes solo desaparecen después de que la persona los lee, así que en algunos casos puedes ponerlo hasta en 1 hora.
- **Elimina o sal del grupo** cuando termine la coordinación. Haz una limpieza de vez en cuando de los chats viejos que olvidaste eliminar. Recuérdale a las demás personas que salgan y eliminen el grupo.

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[39] para las acciones. Ese teléfono solo estaría en uno o dos grupos necesarios para llevar a cabo la acción ese día.

Limpia tus datos privados en línea y cuentas de redes sociales para defenderte del acoso/doxxing

Protégete del gobierno o de los trolls de derecha que usan datos públicos para atacarte.

El gobierno usa herramientas de rastreo de redes sociales[86] para vigilar a activistas sin una orden judicial. Los adversarios de derecha usan sitios de "búsqueda de personas" y redes sociales para intentar asustarnos y que dejemos de organizarnos.

Puedes limpiar tu información personal para que sea más difícil que te conviertas en blanco de estos ataques.

CÓMO DEFENDERTE DEL DOXXING

Tenemos una guía detallada sobre cómo defenderte del doxxing y el acoso como este.

Lista de Defensa contra el Doxxing →

Aquí van algunos de los pasos más importantes de esa guía:

1. Sal de los sitios de "búsqueda de personas" usando EasyOptOuts[47] ($20/año)
2. Asegura tus cuentas de redes sociales usando Block Party[87] (gratis o $50/año si usas el código promocional JOINTHEPARTY)

Prácticas para activistas de mayor riesgo

AMENAZA ALTA **Esta sección es para:**

→ Activistas inmigrantes (sin importar su estatus migratorio) o cualquier persona cuyo color de piel o apariencia les ponga en mayor riesgo de ser blanco de ICE mientras observa

Asegúrate de completar también las secciones anteriores.

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[39] para tener menos datos sensibles en él.

Crea tu plan de emergencia si te arrestan (o te sientes en peligro en casa)

Planificar con anticipación puede ayudarte a sobrellevar mejor una situación estresante.

Como la disidencia se está criminalizando cada vez más[88], nos conviene prepararnos por si nos arrestan o si nos sentimos amenazades en casa por adversarios.

CÓMO HACER UN PLAN DE EMERGENCIA

Plan de emergencia corto

Si necesitas la "miniversión" de esa guía, aquí tienes algunas preguntas para empezar:

1. **¿Quién forma tu red de apoyo?** Si te arrestaran esta noche, ¿a quién llamarías? ¿Tienes su número memorizado?
2. **¿A quién vas a avisar si sabes que vas a estar en una situación de mayor riesgo?** Un grupo sencillo de Signal funciona bien para esto.
3. **¿Tienen lo que necesitan?** ¿Cuentan con una lista de a quién más contactar, tu info médica y el número de una línea legal de emergencia? ¿Tienen lo necesario para cuidar a tus mascotas, hijes, etc.?
4. **¿A dónde irías si te sintieras en peligro en casa?** Si tuvieras que salir de tu casa esta noche porque te sientes en peligro, ¿dónde te quedarías? ¿Esa persona lo sabe?

Plan de emergencia detallado

Si tienes la capacidad, te recomendamos completar nuestra guía de emergencia completa.

Checklist de plan de emergencia personal →

Otros recursos

- **Empezar un grupo de respuesta rápida o patrulla a pie:**
  - Guía de respuesta rápida del Bay Area[89] y zine[90]
  - Guías de Minneapolis[91]
  - Lecciones de Minneapolis[92]
  - Kit de Charlotte[93] (enlace de Google Docs)
  - Dignity Toolkit[94] - Cómo crear conexiones entre los recursos que ya existen en tu comunidad
- **Seguridad:**
  - Evaluaciones de riesgo y kits de seguridad comunitaria de Vision Change Win[95]
  - Recursos de seguridad de Kala Mendoza[96]
  - Street medic 101[97] (en inglés)
  - Riot Medicine Handbook[98] (en inglés)

Sigue aprendiendo con estas guías relacionadas

Defensa contra doxxing

Protégete del doxxing y del acoso en línea.

Planificación de emergencia

Arma una red de apoyo de emergencia en caso de que te detengan o te amenacen.

Enlaces

1. activistchecklist.org/es/contribute/
2. kenklippenstein.com/p/ice-making-list-of-anyone-who-films
3. unwall.app/www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html
4. apnews.com/article/immigration-protest-arrests-detention-ice-8993bfd5d54b870521ec5b44fc42cd71
5. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
6. xcancel.com/camhigby/status/2015093523733733474
7. aljazeera.com/amp/news/2025/7/11/canary-mission-how-us-uses-a-hate-group-to-target-palestine-advocates
8. activistchecklist.org/es/party/
9. activistchecklist.org/es/spyware/
10. blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/
11. signal.org
12. support.signal.org/hc/en-us/articles/6829998083994-Phone-Number-Privacy-and-Usernames-Deeper-Dive
13. activistchecklist.org/es/signal/
14. penguinrandomhouse.ca/books/558051/on-tyranny-by-timothy-snyder/9780804190114/excerpt
15. atomicmail.io/blog/is-whatsapp-safe-the-truth-about-your-privacy
16. activistchecklist.org/es/whatsapp/
17. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
18. strongphrase.net/username
19. signal.org/blog/phone-number-privacy-usernames/
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. theintercept.com/2026/01/30/washington-post-hannah-natanson-fbi-biometrics-unlock-phone/
24. ssd.eff.org/module/attending-protest
25. support.apple.com/guide/personal-safety/emergency-call-text-iphone-apple-watch-ips4f0cd709b/web
26. nyclu.org/resources/know-your-rights/you-have-right-film-ice
27. youtu.be/4xBUa67XAyM?t=988
28. activistchecklist.org/es/protest/
29. cldc.org
30. nlg.org
31. proton.me/drive
32. onionshare.org
33. torproject.org?noredirect=1
34. tella-app.org
35. proofmode.org
36. everestpipkin.github.io/image-scrubber/
37. exifcleaner.com
38. imageoptim.com/mac
39. activistchecklist.org/es/secondary/
40. apps.apple.com/us/app/apple-maps/id915056765
41. magicearth.com
42. youtu.be/alodEeY6YAM?t=137
43. comaps.app/privacy/
44. support.apple.com/en-us/105120
45. landing.google.com/intl/en_us/advancedprotection/
46. activistchecklist.org/es/lockdown/
47. easyoptouts.com
48. optery.com
49. fastpeoplesearch.com
50. consumerreports.org/electronics/personal-information/services-that-delete-data-from-people-search-sites-review-a2705843415/
51. innovation.consumerreports.org/wp-content/uploads/2024/08/Data-Defense_-Evaluating-People-Search-Site-Removal-Services-.pdf
52. kanary.com
53. forbes.com/sites/thomasbrewster/2025/09/08/ice-to-pay-10-million-for-clearview-facial-recognition-to-investigate-agent-assaults/
54. 404media.co/inside-ices-supercharged-facial-recognition-app-of-200-million-images/
55. clearview.ai/privacy-and-requests
56. ivpn.net
57. activistchecklist.org/es/vpn/
58. activistchecklist.org/research
59. ivpn.net/en/
60. protonvpn.com
61. activistchecklist.org/es/proton/
62. ivpn.net/en/pricing/
63. digitalgoods.proxysto.re/en
64. ivpn.net/en/apps-macos/
65. ivpn.net/en/apps-windows
66. ivpn.net/en/apps-ios
67. ivpn.net/en/apps-android
68. techradar.com/vpn/vpn-privacy-security/i-dont-like-that-he-made-this-donation-mullvad-ceo-reacts-to-co-founders-donation-to-controversial-swedish-populist-party
69. proton.me/drive/docs
70. proton.me/mail
71. theintercept.com/2025/09/16/google-facebook-subpoena-ice-students-gaza/
72. cldc.org/google-is-a-fcking-snitch/
73. proton.me/drive/
74. proton.me/drive/sheets
75. strongphrase.net/identity
76. account.proton.me/signup
77. proton.me/support/password-protected-emails
78. cryptpad.fr
79. pimeyes.com/en/opt-out-request-form
80. facecheck.id/en/RemoveMyPhotos
81. support.apple.com/es-es/108756
82. activistchecklist.org/es/essentials/
83. landing.google.com/advancedprotection/
84. accountguard.microsoft.com
85. proton.me/support/proton-sentinel
86. eff.org/deeplinks/2026/01/ice-going-surveillance-shopping-spree
87. blockpartyapp.com
88. indefenseofmovements.substack.com/p/criminalizing-dissent-in-the-wake
89. crimethinc.com/2026/07/16/protecting-your-neighbors-by-following-ice-vehicles-a-guide-from-the-bay-area
90. cdn.crimethinc.com/assets/articles/2026/07/16/move-ice-get-out-the-bay_print_black_and_white.pdf
91. defend612.com/local-resources/
92. crimethinc.com/2026/01/15/rapid-response-networks-in-the-twin-cities-a-guide-to-an-updated-model
93. docs.google.com/document/d/14xX5K4exAvFLx9nW-SVCaKP5RDM6y4WveLflBFYS7To/edit?tab=t.0
94. dignitytoolkit.org
95. visionchangewin.org/services-and-programs/community-safety/
96. linktr.ee/kalamendoza
97. youtube.com/live/g3KheaiW4hA
98. riotmedicine.net/downloads