Seguridad digital para trabajadores federales

ACTIVIST CHECKLIST

Última actualización **24 de febrero de 2025** Toma unos **1 hora**

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/federal/

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].

Esta guía tiene más de **1 año**. Puede que algunos de sus consejos ya no estén al día.

¿Estás usando un dispositivo del gobierno ahora mismo? Si estás visitando esta página desde un teléfono o computadora del gobierno, o conectado al Wi-Fi del gobierno, por favor cierra el sitio y vuelve más tarde. Tu tráfico puede ser monitoreado fácilmente desde los sistemas del gobierno.

Para quién es esta lista: Cualquier trabajador federal que esté resistiendo la toma del gobierno por Trump/Musk/DOGE.

La guía a continuación te ofrece algunos consejos para minimizar el rastro digital de tu resistencia y mantenerte más protegido contra represalias. Ninguna seguridad digital te puede mantener perfectamente anónimo y protegido, pero cada paso a continuación agrega una capa importante.

¡Nos cuidamos entre todes! La seguridad se trata de los pasos que damos para *cuidarnos mutuamente*, no solo a nosotros mismos. Comparte esta guía con tus colegas y ayuda a quienes te rodean a pensar en su seguridad digital. ¡Ahora eres embajador!

Aún mejor: organiza una fiesta de seguridad[2] y trabajen juntos en esta lista durante el almuerzo o después del trabajo. Mucho más efectivo que reenviar un enlace.

Pasos básicos de seguridad

☐ Habla de resistencia y críticas solo lejos de los dispositivos del gobierno (teléfonos/laptops)

Asume que todos los dispositivos del gobierno están registrando lo que tecleas y lo que dices cerca de sus micrófonos

Es razonable actuar como si todos los dispositivos del gobierno te estuvieran vigilando. Esta vigilancia puede no estar activa, pero podría ser fácil para ellos encontrar el rastro de tus actividades.

❌ **No hables de tu resistencia ni de tus objeciones...**

- mientras escribes en un **teléfono del gobierno**
- mientras escribes en una **computadora del gobierno**
- mientras estés conectade al **Wi-Fi del gobierno**, incluso si usas tu teléfono/computadora personal
- mientras estés cerca de un teléfono o computadora del gobierno que tenga **micrófono** (aunque no sea un dispositivo que te hayan dado a ti)
- mientras estés en una **videollamada alojada por el gobierno** (incluso si es con gente de confianza)

✅ **Qué hacer en su lugar**

- ¡Busca colegas de confianza con quienes organizarte!
- Tantea el terreno primero. Construye confianza con el tiempo si aún no la tienes.
- Habla en persona, lejos de dispositivos del gobierno con micrófonos y fuera de los edificios del gobierno.
- Envía mensajes o llama a esas personas de confianza usando la app Signal, que está cifrada (mira el siguiente punto de la lista)

Por ejemplo: Está genial y es importante usar Signal (en tu teléfono personal) para hablar de tu disidencia, críticas, frustraciones y planes. Pero si lo haces justo al lado de tu laptop del gobierno, es posible que tu conversación sea vigilada. Aunque sea poco probable, vale la pena moverte a otro cuarto.

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[3]. (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[4] 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[5] 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[6] 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[7].

¿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[8]. 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[9] para activar la configuración estricta de la cuenta y reforzar tu configuración de privacidad.

No uses tu nombre real ni tu foto en tu perfil de Signal

Te ayuda a protegerte de los policías o atacantes que quieren desanonimizarte. Es muy útil si estás en grupos de Signal sin verificar.

Mucho del trabajo de organización comunitaria pasa en grupos de Signal sin verificar, donde no sabes cuánto puedes confiar en cada quien. Estos grupos pueden ser infiltrados por adversarios de derecha[10] y los policías[11].

Usar un nombre falso evita que alguien encuentre tu identidad real con una búsqueda en Google.

Usar una foto que no sea tu cara evita que alguien encuentre tus perfiles en redes sociales por coincidencia de imagen o reconocimiento facial.

Ambos pasos te ayudan a defenderte del doxxing[12] y del acoso en línea.

CÓMO CAMBIAR TU PERFIL

1. **Cambia el nombre que muestra tu perfil:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → Toca la primera opción con la silueta de una persona → Edita el nombre que muestra tu perfil
2. **Cambia tu foto de perfil:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → **Editar foto** → sube una foto genérica que hayas encontrado en internet y que no tenga relación con tu identidad/preferencias/intereses/ubicación.

Lo mismo aplica con aún más fuerza en redes sociales. Si tu perfil de Instagram, Facebook o LinkedIn muestra tu nombre real completo junto con una foto clara de tu cara, quienes te ataquen pueden identificarte fácilmente aunque el resto de tu perfil sea privado. Mira Asegura tus redes sociales para más info.

Recuérdales a las personas de tus grupos que hagan esto también. La seguridad es un trabajo de equipo.

Considera configurar tu perfil de LinkedIn y otras redes sociales para que sean más privados

Protégete de ser identificado como objetivo por el contenido de tus redes sociales

Hemos visto varios informes de DOGE usando referencias a "DEI" en LinkedIn y otros perfiles de redes sociales

CÓMO CONFIGURAR TU PERFIL DE REDES SOCIALES PARA QUE SEA PRIVADO

LinkedIn:

- **Visibilidad del perfil público:** LinkedIn → **Editar perfil**[13] → **Editar visibilidad** → desactívala por completo o selecciona los elementos que quieras desactivar para proteger tu privacidad e historial.
- **Hiberna tu perfil por completo:** Si te sientes cómode hibernando tu perfil por completo[14] para todo el mundo (incluyendo quienes están en tu red) durante un tiempo, esa es la opción más segura. Quizás quieras ponerte un recordatorio para reactivarlo más adelante.
- **Ajusta otras configuraciones de visibilidad:** LinkedIn → **Ícono de perfil** → **Configuración** → **Privacidad** → **Visibilidad** → ajusta cada opción para que sea más privada.
- **Feed de actividad de LinkedIn:** Tus contactos actuales en LinkedIn aún podrán ver tu feed. Si quieres evitar ser identificado como objetivo, te conviene revisar tu historial y borrar publicaciones[15].

X/Twitter: Sigue estas instrucciones[16] para ocultar tus publicaciones.

Usa un navegador enfocado en privacidad para tu navegación diaria (en vez de Chrome)

Reduce el rastreo, así dejas menos rastro digital.

DO: Usa Brave[17] (lo más fácil) o Firefox[18] (requiere más configuración)

DO NOT: Usar Google Chrome, Microsoft Edge, etc.

Recomendamos **Brave** porque ofrece la mayor privacidad sin necesidad de configuración adicional, que es nuestro objetivo en este sitio.

Tips extra para configurar Brave:

- Instala Privacy Badger[19] para tener protección adicional.
- También puedes instalar la app de Brave para iPhone[20] o Android[21].

Otras opciones de navegador:

CÓMO CONFIGURAR BRAVE

Brave es un navegador enfocado en privacidad que te permite instalar extensiones de Google Chrome.

1. **Instala Brave**[22] en tu computadora (o celular[22]).
2. Sigue los pasos después de abrirlo para importar tu configuración desde Chrome u otro navegador[23]. (Mira la advertencia más abajo sobre cómo los plugins te hacen más identificable.)
3. **Configura los ajustes de privacidad:** En el navegador de escritorio, ve a Brave → **Configuración** → **Shields** y selecciona lo siguiente: (La aplicación móvil no tendrá todos estos ajustes)
   - Selecciona **Agresivo** en "Bloqueo de rastreadores y anuncios"
   - Selecciona **Estricto** en "Actualizar conexiones a HTTPS"
   - Desmarca todo en **Bloqueo de redes sociales**
   - (Opcional) Activa **Olvídame cuando cierre este sitio.** (En la app móvil, esta opción se llama "Borrar datos del sitio") El sitio no podrá guardar nada sobre ti después de que reinicies tu navegador.

     Esto hará más difícil que los sitios te rastreen por internet. Es bueno para la privacidad, pero querrás desactivarlo manualmente para sitios específicos. Entra al sitio → Haz clic en el logo de Brave (el león) en la barra de URL → **Controles avanzados** → **Desactiva Olvídame cuando cierre este sitio**

Opcional:

1. Desactiva la molesta página de nueva pestaña: Brave → **Configuración** → **Empezar** → **Página de nueva pestaña** → Selecciona **Página en blanco** en el menú desplegable
2. Desactiva los elementos de la barra de herramientas: Brave → **Configuración** → **Apariencia** → **Barra de herramientas** → Desactiva todos los botones de la barra que no quieras (Brave Rewards, VPN, Wallet, Leo AI, etc.)

Advertencia sobre plugins: Cada plugin que instalas hace que tu navegador se distinga de "la multitud" y te vuelve más identificable, reduciendo la efectividad de las funciones de privacidad que vienen integradas en Brave.

- **Firefox** puede ofrecer aún más privacidad si te tomas el tiempo de instalar los plugins correctos y configurarlo bien[24].
- Usa **Tor Browser**[25] para navegación muy sensible que sea realmente anónima

Cuando estés en un edificio federal

Ya sea que trabajes regularmente en la oficina o solo la visites en algún momento, estos pasos ayudarán a agregar capas de protección.

☐ Evita llevar tu teléfono o laptop personal a edificios federales (si puedes)

Si es posible, no llevar teléfono ni laptop es lo más seguro

La opción más segura es no llevar tu teléfono ni tu laptop.

Dicho esto, no siempre podemos dejar el teléfono personal en casa, ya que podemos ser el contacto de emergencia de alguien (por ejemplo).

Si vas a llevar tus dispositivos, sigue los pasos del siguiente punto de la checklist.

☐ Si vas a llevar un dispositivo personal, sigue estos pasos para mantenerlo más seguro

Mantenlo apagado siempre que puedas. No te conectes al Wi-Fi del gobierno. Si te conectas al Wi-Fi, usa una VPN confiable[26].

Debemos asumir que cualquier red o dispositivo del gobierno puede vigilar todo lo que hacemos, incluso si es en nuestro dispositivo personal.

Recomendaciones:

1. No lleves tus dispositivos personales si es posible
2. Si tienes que llevar tu dispositivo, déjalo apagado el mayor tiempo posible
3. Si tienes que encenderlo, no te conectes al Wi-Fi (ni al ethernet) del gobierno
4. Si tienes que conectarte al Wi-Fi, asegúrate de hacerlo únicamente con una VPN de confianza activa para proteger tu actividad. Asegúrate de instalar una VPN[27] con anticipación.

Si llevas dispositivos del gobierno a casa

Hay pasos que puedes tomar para protegerte en casa, incluso cuando tienes dispositivos del gobierno en la vivienda

☐ Apaga tu teléfono y laptop y guárdalos cuando termines de trabajar (y antes de hablar de disidencia)

DO: Apaga tus dispositivos y guárdalos en un cajón o clóset	DO NOT: Dejar tus dispositivos encendidos y cerca de donde hablas

Si tu teléfono o laptop del gobierno está cerca de ti, asume que el micrófono puede escuchar tus conversaciones.

CÓMO HACERLO

1. **Asegúrate de que los dispositivos estén apagados** al final del día y cada vez que hables de disidencia en tu casa
2. **Asegúrate de que los dispositivos estén guardados** en un cajón, un clóset o un cuarto con la puerta cerrada. Esto asegura que, si el micrófono de alguna manera siguiera encendido, no se escuchen tus conversaciones. (Esto puede ser poco probable para muchas de nosotres, pero es una precaución que solo toma un minuto.)

Separa tus redes Wi-Fi de casa: activa una "red de invitados" para los dispositivos del gobierno

DO: Conecta tus dispositivos del gobierno solo a la "red de invitados" de tu router

DO NOT: Conectes tus dispositivos personales

Esto no es la mayor prioridad, pero es buena idea.

Activar una "red de invitados" en tu router Wi-Fi hace que tus dispositivos del gobierno no tengan acceso a los dispositivos personales de tu red.

CÓMO ACTIVAR Y USAR UNA RED DE INVITADOS

1. Revisa tu router Wi-Fi para ver el modelo o, al menos, la marca
2. Usa Brave Search[28] (en lugar de Google) para buscar `cómo activar la red de invitados en [MODELO O MARCA AQUÍ]`
3. Sigue las instrucciones que encuentres y configura una red Wi-Fi con un nombre distinto al de tu red principal.
4. En tu teléfono y laptop del gobierno, busca la opción "Olvidar esta red" para tu Wi-Fi principal. Luego vuelve a conectarlos a la nueva red Wi-Fi de invitados.

A veces los routers Wi-Fi pueden ser difíciles de configurar. Si necesitas ayuda, pídele a alguien de confianza que sepa de tecnología.

Si alguna vez tuviste herramientas de gestión de dispositivos móviles instaladas en tu dispositivo personal, quítalas

Las apps de gestión de dispositivos móviles son programas que ayudan al gobierno o a las empresas a administrar dispositivos de forma remota para mantenerlos seguros. Si alguna vez te exigieron instalar una de estas apps en tu dispositivo **personal**, asegúrate de quitarla si tienes permiso para hacerlo. Esto suele pasar cuando ya no trabajas para el gobierno.

Apps de MDM comunes:

- Microsoft Intune
- IBM MaaS360
- VMware Workspace ONE (antes AirWatch)
- MobileIron
- BlackBerry UEM
- Master Data Management de Civica

CÓMO QUITAR LAS APPS DE GESTIÓN DE DISPOSITIVOS MÓVILES

1. Haz una copia de seguridad de tu dispositivo (iPhone[29], Android[30])
2. Restablece tu dispositivo a los valores de fábrica (iPhone[31], Android[32])
3. Restaura desde la copia de seguridad (iPhone[33], Android[30])

Cuando estés organizando

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[34] 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[35].

CÓMO USAR PROTON DOCS

1. Crea una cuenta de Proton[36] si aún no tienes una — elige el plan gratuito
2. Entra a Proton Drive[37] → 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[38] o Jotform[39] con la opción de cifrado de extremo a extremo activada.

- [ ] **Sigue nuestra lista de Security Essentials para más protección**

  La lista de Security Essentials te guiará para asegurar tus cuentas y proteger tu privacidad

GUÍA DE SECURITY ESSENTIALS

Sigue nuestra lista de Security Essentials[40] para asegurarte de que tus dispositivos personales estén lo más seguros posible.

Preguntas frecuentes

¿Es riesgoso abrir mi correo personal en un dispositivo del gobierno?

Una solicitud FOIA[41] buscará productos escritos creados con recursos del gobierno. No es una orden de registro. Cualquier cosa producida en un dispositivo del gobierno estaría sujeta a FOIA (documentos, correos, mensajes, etc.).

(Fuente: Un exempleado de FOIA. Esto no es asesoramiento legal.)

¿Es riesgoso abrir un correo/chat del gobierno en un dispositivo personal?

Cualquier cosa creada en una app del gobierno en un dispositivo personal (Outlook, Teams, etc.) estaría sujeta a FOIA. Una solicitud FOIA no abriría tu dispositivo personal a una búsqueda amplia de tus datos personales. Las solicitudes tienen que ser muy específicas y la búsqueda de información usaría palabras clave especificadas en la solicitud. Cambia la redacción (nombres, etc.) en los mensajes y productos escritos del gobierno si no quieres que se incluyan.

(Fuente: Un exempleado de FOIA. Esto no es asesoramiento legal.)

¿Otras preguntas?

Por favor contáctanos[42] si tienes otras preguntas que no estén respondidas aquí.

Comparte esta lista con otros trabajadores federales

Mientras más seamos los que practicamos seguridad digital, más seguros estaremos todes. Considera enviarle esto a tus colegas —**y asegúrate de enviarlo por Signal**:

> Aquí hay una lista para trabajadores federales que quieren proteger su seguridad digital. Me pareció útil y quería compartirla. **Lista de seguridad digital:** https://activistchecklist.org/federal[43] **Consejos clave:**
>
> - No uses tu teléfono/computadora del gobierno para hablar de tu disidencia.
> - No hables de tu disidencia cerca de ningún dispositivo del gobierno que tenga micrófono
> - No te conectes al Wi-Fi del gobierno con tus dispositivos personales (o usa una VPN como IVPN.net o Proton VPN si no te queda otra opción)
> - No accedas a correo/chat/mensajes personales en un dispositivo del gobierno (te expone a FOIA)
> - Habla de tu disidencia únicamente usando la app de Signal en tu teléfono personal (no por mensajes/llamadas normales ni por correo, ni en dispositivos del gobierno). Encuentra a los colegas en quienes confías y conéctense por Signal.

> Nos cuidamos entre todes.

Consejos para la organización comunitaria

Si eres nuevo en la organización política, ¡bienvenide! Este momento requiere que todes encontremos nuestro lugar en el movimiento. Por suerte, hay muchos recursos sobre los cuales construir, así que nadie tiene que reinventar la rueda.

Aquí hay algunos lugares para empezar:

- Organizing: People, Power, Change[44] por Marshall Ganz de la Harvard Kennedy School (libro gratis, PDF)
- The Citizens Handbook[45] (en inglés)
- Community Organizing Basics[46] de Neighborhood Anarchist Collective (enlaces al final sobre facilitación, convocatoria, cultura de seguridad y más)
- Team Building[47] de Activist Handbook
- Organizing 101[48] de Beautiful Trouble
- Por último, busca mentoría con organizadores con experiencia. ¡Hay miles de personas que ya han hecho esto antes y están deseosas de apoyarte!

Hablando con la prensa: Si parte de tu organización incluye compartir tus historias con la prensa, asegúrate de obtener el usuario de Signal (o número de teléfono) del reportero y comunícate solo por Signal. Ten cuidado con poner tu nombre, correo y número de teléfono en un formulario si no estás seguro a dónde irá esa información.

Leer más

- WIRED: DOGE despierta el miedo a la vigilancia en todo el gobierno de EE. UU.[49] (2025, 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.

Ventajas y desventajas del Modo de aislamiento 3 min de lectura [50] Póster "La poli en la puerta" [51]

Enlaces

1. activistchecklist.org/es/contribute/
2. activistchecklist.org/es/party/
3. blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/
4. signal.org
5. support.signal.org/hc/en-us/articles/6829998083994-Phone-Number-Privacy-and-Usernames-Deeper-Dive
6. activistchecklist.org/es/signal/
7. penguinrandomhouse.ca/books/558051/on-tyranny-by-timothy-snyder/9780804190114/excerpt
8. atomicmail.io/blog/is-whatsapp-safe-the-truth-about-your-privacy
9. activistchecklist.org/es/whatsapp/
10. nitter.net/camhigby/status/2015093531526729789
11. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
12. activistchecklist.org/es/doxxing/
13. linkedin.com/public-profile/settings

14. linkedin.com/help/linkedin/answer/a1336653/
15. linkedin.com/help/linkedin/answer/a1342513
16. help.x.com/en/safety-and-security/how-to-make-x-private-and-public
17. brave.com
18. mozilla.org/en-US/firefox/
19. privacybadger.org
20. apps.apple.com/us/app/brave-private-web-browser-vpn/id1052879175
21. play.google.com/store/apps/details?id=com.brave.browser&hl=en
22. brave.com/download/
23. support.brave.com/hc/en-us/articles/360019782291-How-do-I-import-or-export-browsing-data
24. privacyguides.org/en/desktop-browsers/
25. activistchecklist.org/es/research/
26. activistchecklist.org/vpn/
27. activistchecklist.org/es/vpn/
28. search.brave.com
29. support.apple.com/en-us/108366
30. support.google.com/android/answer/2819582?hl=en
31. support.apple.com/en-us/108931
32. support.google.com/android/answer/6088915?hl=en
33. support.apple.com/en-us/118105
34. proton.me/drive/docs
35. activistchecklist.org/es/proton/
36. proton.me
37. drive.proton.me
38. cryptpad.fr
39. jotform.com
40. activistchecklist.org/es/essentials/
41. en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States)
42. activistchecklist.org/es/contact/
43. activistchecklist.org/federal
44. actionnetwork.org/user_files/user_files/000/041/455/original/organizing_people_power_changeadaptedfromMarshallGanz.pdf
45. citizenshandbook.org/toc.html
46. neighborhoodanarchists.org/organizing-guide
47. activisthandbook.org/organising
48. beautifultrouble.org/toolbox/set/organizing-101
49. unwall.app/www.wired.com/story/surveillance-privacy-doge-federal-employees/
50. activistchecklist.org/es/lockdown/
51. activistchecklist.org/es/police/