Lista de seguridad de WhatsApp

ACTIVIST CHECKLIST

Última actualización **22 de octubre de 2026** Toma unos **15 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/whatsapp/

Traducido automáticamente: Esta página se tradujo automáticamente. Hasta ahora solo el 35% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

Mucho activismo ya pasa por WhatsApp, sobre todo en comunidades migrantes. No es la opción más segura ni la más privada, pero a veces es útil para la organización comunitaria porque la gente ya lo usa o porque se necesitan funciones que ofrece WhatsApp (como Comunidades).

Tus mensajes de WhatsApp tienen cifrado de extremo a extremo, así que WhatsApp protege lo que dices mejor que los mensajes de texto normales. Si los polis le piden a tu compañía telefónica tus mensajes de texto normales con una orden judicial, pueden ver el contenido de cada mensaje. Si le piden a Meta tus mensajes de WhatsApp con una orden judicial, no pueden ver el contenido (siempre que no tengas activadas las copias de seguridad de chats).

Piensa en organizar grupos grandes en WhatsApp igual que en las redes sociales: Da por hecho que gente con malas intenciones (el gobierno, la ultraderecha) podría unirse y vigilar cualquier grupo grande sin filtro, igual que podría unirse y vigilar grupos grandes en redes sociales. Da por hecho que también pueden ver quién está en el grupo, igual que podrían ver quién te sigue en redes sociales.

Incluso con las protecciones de esta guía, hay varias cosas que WhatsApp siempre podrá entregarles a los polis:

- Toda tu lista de contactos (si alguna vez le diste a la app acceso a tus contactos, siempre los tendrá, aunque después le quites el permiso)
- Todas las demás personas usuarias de WhatsApp que te tienen A TI en su lista de contactos (fuente[2])
- Los nombres de todos los grupos en los que estás
- Las personas integrantes de todos los grupos en los que estás
- A qué números les escribes y cuándo (incluso pueden obtener esta información en tiempo real[3], algo que la mayoría de las otras empresas tecnológicas no les dan a los polis)
- Si activas las copias de seguridad de chats, a Google o Apple las pueden obligar a entregarlas, y ahí están todos tus mensajes. Consulta Haz copias de seguridad seguras de tus chats de WhatsApp para saber cómo usar las copias de seguridad de forma segura.

¿Nunca has usado WhatsApp? Mira esta guía sobre cómo usar WhatsApp[4].

Protecciones básicas de WhatsApp

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

Si solo tienes 10 minutos, empieza por acá.

Importante Desactiva las copias de seguridad de los chats de WhatsApp (y pídeles a tus contactos que hagan lo mismo)

Las copias de seguridad de WhatsApp no están cifradas por defecto y pueden entregarse por orden judicial.

Las copias de seguridad que WhatsApp crea por defecto en iCloud o Google Drive NO tienen cifrado de extremo a extremo. Eso significa que un tribunal puede obligar a Apple o Google a entregar todo tu historial de chats. Aunque tus mensajes se enviaron de forma segura, la copia de seguridad echa por tierra esa protección al facilitar que se revele todo tu historial de chats.

Desactivar las copias de seguridad también te protege si alguien hackea tu cuenta de iCloud o Google mediante phishing o una contraseña reutilizada.

CÓMO DESACTIVAR LAS COPIAS DE SEGURIDAD POR COMPLETO

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Chats** → **Copia de seguridad** → pon **Copia automática** en **Desactivada**

ANDROID

WhatsApp → ⋮ → **Chats** → **Copia de seguridad** → pon **Copia automática** en **Desactivada**

Avísales a tus amistades: Aunque tus copias de seguridad estén bien protegidas, puede que las personas con las que chateas estén guardando las suyas sin cifrar. Su copia de seguridad incluye tus mensajes. Pídeles a tus contactos que también protejan sus copias de seguridad. Quizá quieras enviarles esta guía.

Si de verdad necesitas hacer copias de seguridad, revisa Cómo respaldar tus chats de WhatsApp de forma segura para hacerlo sin riesgos.

Oculta tu hora de "Última vez y en línea" en WhatsApp

Evita que extraños y miembros de grupos rastreen cuándo usas WhatsApp.

Por defecto, cualquier persona con la que hayas intercambiado mensajes puede ver cuándo estuviste por última vez en WhatsApp. Para quienes hacemos activismo, esa es una forma fácil de que alguien mapee tus patrones de actividad.

CÓMO OCULTAR TU ÚLTIMA VEZ Y TU ESTADO EN LÍNEA

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Privacidad** → **Última vez y en línea** → Selecciona **Nadie**

ANDROID

WhatsApp → ⋮ → **Privacidad** → **Última vez y en línea** → Selecciona **Nadie**

El interruptor de "Configuración estricta de la cuenta" bloquea este ajuste, así que cambia primero Última vez si quieres un valor personalizado.

Activa la configuración estricta de cuenta en WhatsApp

Activa en un solo paso la verificación en dos pasos, las notificaciones de seguridad, el bloqueo de remitentes desconocidos, la desactivación de vistas previas de enlaces y el silenciado de llamadas desconocidas.

Activar la configuración estricta de cuenta activa varias protecciones a la vez. Es una buena opción por defecto para cualquier persona que haga activismo.

CÓMO ACTIVAR LA CONFIGURACIÓN ESTRICTA DE CUENTA

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Privacidad** → **Avanzado** → **Configuración estricta de cuenta** → **Siguiente** → **Activar**

ANDROID

WhatsApp → ⋮ → **Privacidad** → **Avanzado** → **Configuración estricta de cuenta** → **Siguiente** → **Activar**

Si prefieres activar cada ajuste manualmente en lugar de usar Configuración estricta de la cuenta, estos son los pasos

Solo necesitas esto si prefieres elegir ajustes individuales en vez de usar el botón de Configuración estricta de la cuenta de arriba. Si ya activaste Configuración estricta de la cuenta, puedes saltarte esta parte.

- [ ] **Verificación en dos pasos.** WhatsApp → **Privacidad** → **Avanzado** → **Verificación en dos pasos** → establece un PIN
- [ ] **Notificaciones de seguridad.** WhatsApp → **Privacidad** → **Avanzado** → **Notificaciones de seguridad** → activa
- [ ] **Bloquear medios de remitentes desconocidos.** WhatsApp → **Privacidad** → **Avanzado** → **Bloquear medios de contactos desconocidos** → activa
- [ ] **Desactivar vistas previas de enlaces.** WhatsApp → **Privacidad** → **Avanzado** → **Desactivar vistas previas de enlaces** → activa
- [ ] **Silenciar llamadas de desconocidos.** WhatsApp → **Privacidad** → **Llamadas** → **Silenciar llamadas de desconocidos** → activa
- [ ] **Limita la visibilidad de tu perfil solo a contactos** (hora de última vez, info, foto de perfil, estado). WhatsApp → **Privacidad** → configura cada uno en **Mis contactos** o **Nadie**

Acuérdate de guardar tu PIN de verificación en dos pasos en un lugar seguro, como tu password manager[5]. Si lo pierdes, puedes quedarte bloqueade fuera de tu cuenta.

Activa los mensajes temporales por defecto en WhatsApp

Te protege a ti y a tus contactos si algún teléfono es confiscado o vulnerado.

Activar los mensajes temporales por defecto te mantiene a ti y a tus contactos más seguros si un teléfono llega a ser confiscado o vulnerado. No sabemos a quién le van a quitar el teléfono los cops. Aunque creas que estás hablando de cosas totalmente legales, el gobierno puede encontrar formas de tergiversar tus palabras.

Las opciones de WhatsApp son 24 horas, 7 días o 90 días. 7 días es una buena opción por defecto, y luego puedes establecer manualmente un tiempo más corto para conversaciones más sensibles.

CÓMO ACTIVAR LOS MENSAJES TEMPORALES POR DEFECTO

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Privacidad** → **Tiempo predeterminado de los mensajes** → elige la duración

ANDROID

WhatsApp → ⋮ → **Privacidad** → **Tiempo predeterminado de los mensajes** → elige la duración

El tiempo predeterminado solo se aplica a los **nuevos chats que tú inicies**. Si alguien más inicia una conversación contigo, el temporizador no se aplica. Para activarlo en una conversación existente, abre el chat > toca el nombre en la parte superior > **Mensajes temporales**.

Prácticas de seguridad continuas en WhatsApp

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

No compartas nada en WhatsApp que no publicarías también en redes sociales

WhatsApp sirve para movilizar a mucha gente, pero no para planificar cosas de mayor riesgo

DO: Usa WhatsApp para movilizaciones masivas (de forma parecida a como usarías las redes sociales)

DO NOT: Organizar turnos de ICE watch, defensa electoral o acciones directas en WhatsApp

Ten en cuenta que las discusiones sobre temas políticos o estratégicos pueden ser vigiladas por actores de extrema derecha, sobre todo en grupos o canales usados para comunicación o movilización masiva donde no controlas del todo quién entra.

Evita decir cualquier cosa en WhatsApp que no publicarías abiertamente en redes sociales.

Si estás planeando acciones sensibles con gente de confianza, usa Signal[6].

No "chatees" con Meta AI en WhatsApp

Todo lo que le preguntes a Meta AI sobre tu organización, tus contactos o tus planes queda guardado y podría terminar en manos de la policía.

Para quienes hacemos activismo, Meta AI es una herramienta de recolección de datos disfrazada de asistente útil. Todo lo que le preguntes sobre tu organización, tus contactos, tus ubicaciones o tus planes queda guardado, se usa para armar tu perfil y podría terminar en manos de la policía.

Si etiquetas a @MetaAI en un chat grupal, los mensajes de alrededor terminan en los sistemas de Meta, aunque solo quisieras hacer una pregunta rápida. Una vez que Meta AI entra en la conversación, ese historial ya no queda solo entre las personas del chat.

No puedes desactivar Meta AI por completo en WhatsApp. La mejor protección es no usarlo nunca y no etiquetar nunca a **@MetaAI** en un chat grupal.

Para mantener a Meta AI fuera de chats y grupos específicos, activa también la privacidad avanzada del chat en esos chats.

Nunca ingreses un código de vinculación ni escanees un código QR en "Dispositivos vinculados"

Los atacantes te engañan para que vincules su navegador a tu cuenta, dándoles acceso total a tus chats.

DO: Escanea un código QR de WhatsApp solo cuando TÚ mismo hayas abierto WhatsApp Web o Desktop

DO NOT: Ingresar un código de vinculación o escanear un código QR porque un sitio web o una persona te lo pide

¿Qué son los "Dispositivos vinculados"? WhatsApp te permite usar tu cuenta en otros dispositivos (una computadora, una tablet, un segundo teléfono) vinculándolos con un código QR o un código de vinculación. La mayoría de la gente nunca usa esta función. Mira la explicación oficial[7] de WhatsApp si quieres más contexto.

Los atacantes se dieron cuenta de que pueden engañarte para que vincules *su* dispositivo a tu cuenta. Si un sitio web o alguien desconocido te guía para "verificar" ingresando un código en WhatsApp, eso no es verificación. Eso es darles acceso completo a tus chats. El mismo truco funciona con códigos QR.

Entonces: **nunca ingreses un código de vinculación ni escanees un código QR de WhatsApp porque un sitio web o una persona te lo pidió.** Solo escanea un código QR de WhatsApp cuando **tú mismo** acabas de abrir WhatsApp Web o Desktop.

Puedes revisar tu cuenta en cualquier momento. Mira Revisa los dispositivos vinculados con regularidad.

Nunca le envíes a nadie tu PIN de WhatsApp ni tu código de verificación de 6 dígitos

Ni siquiera a alguien que dice ser de "WhatsApp Support". Así es como se roban las cuentas.

Tu PIN de WhatsApp y el código de verificación de 6 dígitos que WhatsApp te envía por mensaje son las llaves de tu cuenta. Cualquiera que los consiga puede apoderarse de ella.

Nunca compartas estos códigos con nadie, por ningún motivo. Esto aplica incluso si la persona dice ser de "WhatsApp Support" o "WhatsApp Security". WhatsApp nunca te va a enviar un DM, llamar ni mandar un mensaje pidiéndote tu PIN o código de verificación. Si alguien te los pide, es un intento de phishing.

Han aumentado los mensajes falsos que dicen ser de "WhatsApp Support" y que intentan robarte la cuenta de esta forma. Si no estás segure de que un mensaje sea legítimo, no respondas, no toques ningún enlace y no ingreses ningún código. En vez de eso, contacta a WhatsApp desde la sección de **Ayuda** dentro de la app.

Protecciones avanzadas de WhatsApp

AMENAZA MEDIA Esta sección es para ti si tienes un rol de liderazgo o haces un activismo que tiene más chance de ser atacado por el Estado o tu oposición.

Activa el Chat restringido en los chats y grupos de WhatsApp sensibles

Bloquea Meta AI, la exportación del chat, el guardado automático de archivos en la galería y el acceso desde dispositivos vinculados como WhatsApp Web en ese chat.

El Chat restringido se activa chat por chat. Cuando está activado, nadie en ese chat puede:

- Exportar el chat
- Guardar automáticamente en su galería las fotos y videos del chat
- Usar las funciones de Meta AI en el chat
- Abrir el chat en un dispositivo vinculado, como WhatsApp Web, WhatsApp Desktop o una tablet

> **Un chat restringido no aparece en tu computadora.** Una vez activado, tú y todas las demás personas del chat solo pueden leer y enviar mensajes desde su teléfono principal. Nadie en el chat podrá verlo en WhatsApp Desktop, WhatsApp Web ni en una tablet.

La idea es mantener a los agentes de IA y las apps no oficiales de WhatsApp fuera de tus chats. Estas herramientas se conectan a la cuenta de WhatsApp de alguien como un dispositivo vinculado. Si alguien en tu grupo conectó una, puede leer todos los chats de su cuenta, incluido el de tu grupo. Al activar el Chat restringido, ya no pueden leer ese chat. También ayuda si alguien engaña a una persona del chat para que vincule el dispositivo del atacante a su cuenta (mira Revisa con regularidad la lista de Dispositivos vinculados de WhatsApp).

Tienes que activarlo en cada chat sensible. No se puede activar automáticamente para todos los chats, y solo puedes cambiarlo desde tu teléfono principal.

CÓMO ACTIVAR EL CHAT RESTRINGIDO

En un chat individual (cualquiera de las dos personas puede activarlo):

IPHONE

Abre el chat → toca el nombre del contacto arriba → **Chat restringido** → actívalo

ANDROID

Abre el chat → ⋮ → **Ver contacto** → **Chat restringido** → actívalo

En un grupo (solo quienes administran el grupo pueden activarlo):

Abre el grupo → toca el nombre del grupo arriba → **Chat restringido** → actívalo

Si no eres admin, pídele a alguien que administre el grupo que lo active.

SI YA ACTIVASTE LA PRIVACIDAD AVANZADA DEL CHAT

El chat restringido reemplaza una configuración anterior llamada Privacidad avanzada del chat. Los chats donde activaste la Privacidad avanzada del chat **no cambian automáticamente a chat restringido**, y todavía se pueden abrir en dispositivos vinculados hasta que los actualices.

Abre el chat → toca el nombre del chat arriba → **Privacidad avanzada del chat** → **Actualizar** → **Continuar**

El chat restringido solo funciona por completo si todas las personas del chat tienen la versión más reciente de WhatsApp. Alguien con una versión anterior todavía podría leer el chat en un dispositivo vinculado, una app no oficial o un agente de IA, y WhatsApp no te va a avisar. Pídeles a todas las personas en grupos sensibles que mantengan WhatsApp actualizado. Además, no impide que alguien tome capturas de pantalla o reenvíe mensajes individuales.

Evita que WhatsApp guarde fotos y videos automáticamente en tu galería

Mantén las imágenes sensibles fuera de las copias de seguridad de iCloud o Google Photos, donde pueden ser solicitadas por orden judicial.

Las fotos y videos que recibes en WhatsApp pueden terminar en más lugares de los que crees. Por defecto, WhatsApp puede guardarlos directamente en tu galería, y iCloud o Google Photos los respaldarán en la nube automáticamente.

Eso significa que imágenes sensibles (videos de protestas, fotos de organizadores, cualquier cosa que pueda exponer a tu comunidad) y sus metadatos (como el lugar y la hora en que se tomó la foto) pueden quedarse en una cuenta de Google o Apple donde los cops las pueden pedir con una orden judicial. Borrar después cada copia se vuelve mucho más difícil.

CÓMO DESACTIVAR EL GUARDADO AUTOMÁTICO PARA TODOS LOS CHATS

IPHONE

WhatsApp → **Configuración** → **Chats** → desactiva **Guardar en Carrete**

ANDROID

WhatsApp → **Ajustes** → **Chats** → desactiva **Visibilidad de archivos**

CÓMO DESACTIVAR EL GUARDADO AUTOMÁTICO PARA UN CHAT O GRUPO ESPECÍFICO

IPHONE

Abre el chat → toca el nombre del chat arriba → **Guardar en Carrete** → elige **Predeterminado**, **Siempre** o **Nunca**

ANDROID

Abre el chat → toca el nombre del chat arriba → **Visibilidad de archivos** → elige **Predeterminado**, **Sí** o **No**

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

Te ayuda a protegerte de la policía o de atacantes que quieran revelar tu identidad. Es especialmente útil si estás en grupos de WhatsApp donde no se ha verificado a quienes participan.

Mucha de la organización comunitaria pasa en grupos de WhatsApp sin verificar, donde no sabes qué tanto puedes confiar en todas las personas del grupo. Estos grupos pueden ser infiltrados por adversarios de derecha[8] y por la policía[9].

Usar un nombre falso o solo tu primer nombre evita que alguien descubra tu identidad real con una búsqueda en Google. Usar una foto que no muestre tu cara evita que alguien encuentre tus redes sociales con una búsqueda por imagen o con reconocimiento facial. Ambos pasos te ayudan a protegerte del doxxing[10] y del acoso en línea.

> Es muy difícil tener anonimato total en WhatsApp, porque tu número de teléfono lo puede ver cualquier persona a la que le escribas y cualquiera que esté en un grupo contigo. Si en un grupo hay alguien con malas intenciones, puede usar fácilmente tu número de teléfono para descubrir tu identidad[10]. Si configuras un nombre de usuario de WhatsApp, tu número queda oculto para quienes todavía no lo tienen.

CÓMO CAMBIAR EL NOMBRE DE TU PERFIL

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → Toca tu nombre → Vuelve a tocar tu nombre → Cambia tu nombre por uno falso o solo tu primer nombre → Toca **Guardar**

ANDROID

WhatsApp → ⋮ → **Ajustes** → Toca tu nombre arriba → Vuelve a tocar tu nombre → Cambia tu nombre por uno falso o solo tu primer nombre → Toca **Guardar**

CÓMO CAMBIAR TU FOTO DE PERFIL

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → Toca tu foto de perfil → Toca **Editar** debajo de la foto de perfil → Sube una foto genérica que hayas encontrado en internet y que no tenga relación con tu identidad, tus gustos, tus intereses ni tu ubicación

ANDROID

WhatsApp → ⋮ → **Ajustes** → Toca tu foto de perfil → Toca **Editar** debajo de la foto de perfil → Sube una foto genérica que hayas encontrado en internet y que no tenga relación con tu identidad, tus gustos, tus intereses ni tu ubicación

Recuérdales a las personas de tus grupos que también lo hagan. La seguridad es cosa de todes.

Crea un nombre de usuario en WhatsApp para ocultar tu número de teléfono

Quienes no tengan tu número verán tu nombre de usuario en su lugar. Útil en grupos de organización grandes o donde no conoces bien a todes.

Ahora WhatsApp te deja elegir un nombre de usuario. Cuando tu nombre de usuario esté activo, quienes no tengan tu número guardado verán tu nombre de usuario en vez de tu número. También puedes darle a alguien tu nombre de usuario en vez de tu número cuando quieras conectar.

Esto importa sobre todo en grupos de organización grandes o donde no conoces bien a todes, porque pueden infiltrarse personas con malas intenciones. Tu número de teléfono es una de las formas más fáciles de averiguar quién eres[10].

WhatsApp está activando los nombres de usuario país por país. Si todavía no están activos donde vives, igual puedes reservar uno ahora para tenerlo listo cuando lleguen.

CÓMO CREAR UN NOMBRE DE USUARIO

WhatsApp → **Ajustes** → **Cuenta** → **Nombre de usuario** → elige un nombre de usuario

Elige un nombre de usuario que no uses en ningún otro lado y que no incluya tu nombre real. Si reutilizas un usuario de Instagram, X u otro sitio, cualquiera puede vincular tu cuenta de WhatsApp con ese perfil.

Opcional: agrega una clave de nombre de usuario. **Nombre de usuario** → **Clave de nombre de usuario**. Es un código extra que la gente necesita, además de tu nombre de usuario, para escribirte por primera vez. Así, desconocides no pueden simplemente adivinar tu nombre de usuario y contactarte. Si empiezas a recibir mensajes no deseados, cambia tu clave.

Tener un nombre de usuario no te hace anónime.

- Igual necesitas un número de teléfono para usar WhatsApp, y Meta todavía puede entregárselo a la policía.
- Quienes ya tengan tu número guardado, y cualquier persona con la que ya hayas chateado por número, todavía pueden verlo.
- Meta sigue sabiendo con quién hablas y en qué grupos estás.

Revisa que no estés compartiendo tu ubicación en tiempo real en ningún chat de WhatsApp

Es fácil dejar la ubicación en tiempo real activada sin darte cuenta. Revísala de vez en cuando para no estar transmitiendo tus movimientos a un chat.

WhatsApp te permite compartir tu ubicación en tiempo real con una persona o grupo por un tiempo determinado. Es fácil activarla y olvidarte de ella, sobre todo si empezaste a compartirla con alguien hace horas.

Para activistas, una ubicación en tiempo real activa es un mapa directo de tus movimientos que cualquiera en el chat puede ver.

CÓMO REVISAR Y DETENER EL USO COMPARTIDO DE LA UBICACIÓN EN TIEMPO REAL

IPHONE

WhatsApp → **Ajustes** → **Privacidad** → **Ubicación en tiempo real** → revisa la lista y toca **Dejar de compartir** en lo que ya no necesites

ANDROID

WhatsApp → ⋮ → **Ajustes** → **Privacidad** → **Ubicación en tiempo real** → revisa la lista y toca **Dejar de compartir** en lo que ya no necesites

Respalda tus chats de WhatsApp de forma segura (solo si realmente necesitas respaldos)

Si realmente necesitas respaldos, activa el respaldo cifrado de extremo a extremo de WhatsApp para que Google o Apple no puedan entregarlos.

La opción más segura es dejar los respaldos completamente desactivados (ver Desactivar los respaldos de chats de WhatsApp). Activa los respaldos solo si realmente los necesitas, por ejemplo si vas a cambiar de dispositivo o cruzar una frontera y necesitas borrar WhatsApp temporalmente.

Si necesitas respaldos, activa el respaldo cifrado de extremo a extremo que WhatsApp trae incorporado. Sin esto, se puede obligar a Google o Apple a entregarle todo tu historial de chats a los cops.

CÓMO ACTIVAR LOS RESPALDOS CIFRADOS

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Chats** → **Copia de seguridad** → **Copia de seguridad cifrada de extremo a extremo** → configura una passkey o contraseña

ANDROID

WhatsApp → ⋮ → **Chats** → **Copia de seguridad** → **Copia de seguridad cifrada de extremo a extremo** → configura una passkey o contraseña

Guarda la contraseña en un gestor de contraseñas[5]. WhatsApp no puede recuperarla por ti.

Solo iPhone: Para protección extra además del respaldo cifrado de WhatsApp, también puedes activar la **Protección de datos avanzada para iCloud** de Apple. Es una opción aparte, que aplica a todo iCloud y cifra de extremo a extremo casi todo lo que tienes en tu cuenta de iCloud.

Para quienes organizan o administran grupos

AMENAZA MEDIA Esta sección es para ti si tienes un rol de liderazgo o haces un activismo que tiene más chance de ser atacado por el Estado o tu oposición.

Si estás a cargo de un grupo de organización, la configuración del grupo importa tanto como tu configuración personal.

Protege tus grupos de organización en WhatsApp

La privacidad de un grupo depende de su integrante menos seguro.

Si administras un grupo de organización, la configuración del grupo importa tanto como tu configuración personal.

La privacidad de un chat grupal depende de su integrante menos seguro. Si una persona es infiltrada o tiene un dispositivo comprometido, todo lo que hay en el chat puede quedar expuesto. Apoya a tu grupo para que sigan juntes las normas acordadas.

CÓMO PROTEGER LA CONFIGURACIÓN DE TU GRUPO

Configuración recomendada para el grupo:

- [ ] **Activa los mensajes temporales en el grupo desde el principio.** Elige el plazo más corto que el grupo pueda aguantar.
- [ ] **Activa el chat restringido** en el grupo (solo quienes administran el grupo pueden hacerlo). Esto desactiva la exportación del chat, evita que los archivos se descarguen automáticamente en la galería de todes, deja a Meta AI fuera del chat y bloquea los dispositivos vinculados para que los agentes de IA y las apps no oficiales no puedan entrar. Avísales a les integrantes que el grupo solo funcionará en sus celulares, no en WhatsApp Desktop ni en WhatsApp Web. Si antes activaste la opción anterior de privacidad avanzada del chat, cámbiala a chat restringido, porque no se actualiza sola.
- [ ] **Haz que el grupo sea solo por invitación.** Abre el chat del grupo → toca el nombre del grupo → **Permisos del grupo** → limita quién puede editar la info, añadir participantes y enviar mensajes.
- [ ] **Pónganse de acuerdo sobre las normas del grupo desde el principio:** nada de copias de seguridad en la nube, nada de hablar de acciones de alto riesgo por WhatsApp y no agregar gente nueva sin aprobación. Asegúrate de que todes les integrantes nueves acepten estas normas y recuérdaselas de vez en cuando a quienes ya están en el grupo.
- [ ] **Define una forma de verificar a la gente que se ajuste a sus necesidades y al nivel de riesgo que pueden asumir.** Los grupos más grandes son más fáciles de infiltrar.

- [ ] **Usa las Comunidades de WhatsApp para mantener privados los números de teléfono de los miembros del grupo**

  Las Comunidades ocultan los números de teléfono entre los miembros, lo cual ayuda cuando organizas grupos grandes o que no han sido completamente verificados.

WhatsApp tiene una función más reciente llamada **Comunidades** que te permite crear un grupo principal con varios subgrupos.

El beneficio para quienes organizan es que las Comunidades tienen una función de "privacidad del número de teléfono" para que los demás miembros no puedan ver los números de teléfono entre sí.

> La privacidad del número de teléfono en las Comunidades tiene límites: les admins del grupo todavía pueden ver tu número, y también cualquiera que ya lo tenga guardado en su libreta de contactos.

Si manejas un grupo grande de organización en WhatsApp, considera migrar a una Comunidad para reducir el riesgo de que otros miembros o infiltrades hagan doxxing[10] a la gente del grupo.

Protecciones para activistas de mayor riesgo

AMENAZA ALTA Esta sección es para ti si ocupas un rol de alto perfil o tu activismo implica trabajo de alto riesgo que podría traer consecuencias graves o represalias.

Los puntos de esta sección te ayudarán a proteger tus datos si los polis te quitan el dispositivo.

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**[11] y en Android se llama **Programa de Protección Avanzada**[12]. (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[13]. 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.

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[14]
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[14]
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[14]
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[14]
3. **Apps de la Microsoft Store:** Asegúrate de activar las actualizaciones automáticas[15] (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.

Desactiva el desbloqueo facial/por huella digital (biométrico)

Tienes mayor protección legal[16] 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**.

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[17] 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[17]. (¡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[17].

☐ Dale acceso a WhatsApp solo a fotos específicas de tu biblioteca

Evita que WhatsApp pueda ver todas las imágenes de tu biblioteca, por si la empresa cambia cómo usa esos datos.

Meta lanzó hace poco una función[18] en la app de Facebook que envía todas las imágenes de tu biblioteca de fotos a sus servidores para procesarlas. Esto es una violación grave de la privacidad y puede representar un riesgo legal para activistas.

Meta (la empresa matriz que también es dueña de WhatsApp) ha dicho que este tipo de función no existe en WhatsApp. Aun así, vale la pena desactivar el acceso amplio a las fotos en WhatsApp, ya que la empresa lanzó exactamente esa función en Facebook.

CÓMO DARLE A WHATSAPP ACCESO LIMITADO A TU BIBLIOTECA DE FOTOS

El acceso limitado agrega uno o dos pasos cuando quieras compartir una foto nueva, pero es sencillo.

IPHONE

app **Ajustes** → **Apps** → **WhatsApp** → **Fotos** → selecciona **Acceso limitado**

ANDROID

app **Ajustes** → **Apps** → **WhatsApp** → **Permisos** → **Fotos y videos** → selecciona **Seleccionar fotos y videos cada vez** (o **Preguntar siempre**, según tu dispositivo)

Oculta el contenido de las notificaciones de WhatsApp en la pantalla de bloqueo

Evita que las vistas previas de mensajes y los nombres de quien envía aparezcan si te confiscan el teléfono.

Si te confiscan el teléfono, tu historial de notificaciones puede revelar el contenido de los mensajes y los nombres de quienes los envían, incluso después de que los mensajes mismos hayan desaparecido. Mira el caso de Prairieland[19] para entender por qué esto importa.

Apple solucionó el problema que hacía que las notificaciones entrantes de Signal se guardaran incluso después de desactivar los mensajes, en iOS/iPadOS 26.4.2 (y en la rama de mantenimiento anterior 18.7.8). Aunque solucionaron ese problema, no está claro si los teléfonos Android siguen teniendo la misma debilidad, así que vale la pena ocultar las vistas previas en cualquiera de las dos plataformas.

CÓMO OCULTAR EL CONTENIDO DE LAS NOTIFICACIONES DE WHATSAPP

IPHONE

app **Ajustes** → **Notificaciones** → **WhatsApp** → pon **Mostrar previsualizaciones** en **Nunca**

ANDROID

app **Ajustes** → **Aplicaciones** → **WhatsApp** → **Notificaciones** → desactiva **Mostrar contenido de notificaciones en la pantalla de bloqueo**

Desactiva los resúmenes de notificaciones con IA para WhatsApp

Apple Intelligence y los resúmenes de notificaciones de Android pueden enviar partes de tus notificaciones a servidores en la nube.

Apple Intelligence y los resúmenes de notificaciones de Android pueden enviar partes de tus notificaciones a servidores en la nube. No queda del todo claro qué se envía ni a dónde, y esos datos podrían ser exigidos mediante una solicitud del gobierno.

Tenemos un artículo sobre este tema relacionado con Signal. El mismo razonamiento aplica para WhatsApp: ¿Apple Intelligence está leyendo mis mensajes de Signal?[20]

CÓMO DESACTIVAR LOS RESÚMENES DE NOTIFICACIONES CON IA PARA WHATSAPP

IPHONE

app **Ajustes** → **Notificaciones** → **Resumir notificaciones** → desactiva **WhatsApp**

ANDROID

app **Ajustes** → **Notificaciones** → **Resúmenes de notificaciones** → agrega **WhatsApp** a la lista de excluidas

- [ ] **Revisa seguido la lista de dispositivos vinculados de WhatsApp**

  Puedes evitar que te roben tu cuenta si revisas de vez en cuando tus dispositivos vinculados.

La función multidispositivo de WhatsApp es una de las principales vías para que alguien se apodere de tu cuenta. Los atacantes te engañan para que escanees un código QR o ingreses un código de vinculación, y así su computadora empieza a ver todos los mensajes que envías y recibes.

Esa misma infraestructura multidispositivo también la han usado empresas de spyware mercenario para atacar a periodistas y organizadores. Consulta nuestra página sobre spyware[21] para saber más.

CÓMO REVISAR TUS DISPOSITIVOS VINCULADOS

IPHONE

WhatsApp → Toca **Tú** en la barra inferior → **Dispositivos vinculados**

ANDROID

WhatsApp → ⋮ → **Dispositivos vinculados**

Cierra la sesión de cualquier dispositivo que no reconozcas. Si no usas WhatsApp Web ni la app de escritorio, cierra la sesión en todos.

Para tus chats y grupos más sensibles, activa la privacidad avanzada del chat: así esos chats no aparecen en ningún dispositivo vinculado y, si alguien se apodera de uno, no podrá leerlos.

Otros recursos

- Guía de cómo usar WhatsApp[4] — Electronic Frontier Foundation
- Mejorar la seguridad de WhatsApp[22] — Freedom of the Press Foundation

Preguntas frecuentes

¿Qué es esa opción de "verificar el código de cifrado" que veo en cada chat?

Esta función te da una forma de verificar las claves de cifrado de un chat específico. Se usa en situaciones de riesgo extremadamente alto, donde alguien podría haber intentado meterse en medio de tu conexión la primera vez que te conectaste con otra persona. Si tus chats son tan sensibles que necesitas protegerte de este tipo de amenaza avanzada, deberías estar usando Signal en vez de WhatsApp.

¿Y las demandas de 2026 que dicen que WhatsApp creó una "puerta trasera" para saltarse el cifrado de extremo a extremo?

Dos demandas distintas en 2026 afirman que WhatsApp tiene una forma de que el personal de Meta lea los mensajes de les usuaries, saltándose el cifrado de extremo a extremo. Les expertes en criptografía que han revisado esta afirmación creen que lo más probable es que sea falsa o exagerada. Si resulta ser cierto, sería una violación de la privacidad como nunca hemos visto de parte de una gran empresa tecnológica. Nuestra postura: las afirmaciones extraordinarias requieren pruebas extraordinarias. Aunque para nada creemos que Meta sea una empresa ética, queremos esperar a ver qué sale de las demandas. Como siempre, si te preocupa, usa Signal.

¿WhatsApp es más seguro que los mensajes de texto comunes (SMS)?

En cuanto al contenido de los mensajes, sí. Los mensajes de WhatsApp tienen cifrado de extremo a extremo, así que tu compañía telefónica no puede entregarle el contenido de tus mensajes a los polis, aunque tenga una orden judicial. Los mensajes de texto normales (SMS) no están cifrados y la compañía telefónica ve cada palabra. Aun así, WhatsApp es peor que Signal en cuanto a metadatos: Meta registra a quién le escribes, cuándo y en qué grupos estás, y le entrega esa información a los polis cuando se la piden.

¿Los polis pueden leer mis mensajes de WhatsApp?

No pueden leer el contenido de los mensajes mientras viajan entre tu dispositivo y el de otra persona. Pero sí pueden acceder a tus mensajes si activas las copias de seguridad de los chats sin el cifrado de extremo a extremo. Pueden obligar a Meta a entregar muchos metadatos (tu lista de contactos, a quién le escribes, los grupos en los que estás, tus direcciones IP). También pueden entrar a un teléfono confiscado que tenga un código débil y leer los mensajes directamente.

¿Los nombres de usuario de WhatsApp le ocultan mi número de teléfono a la policía?

No. Los nombres de usuario ocultan tu número de teléfono a otras personas en WhatsApp que todavía no lo tienen. Igual necesitas un número de teléfono para usar WhatsApp, y Meta puede entregárselo a la policía junto con tu lista de contactos, los grupos en los que estás y con quién te escribes.

¿Cuándo debo usar Signal en vez de WhatsApp?

Usa Signal para organizar trabajo político delicado. Signal casi no recopila metadatos y no entrega casi nada cuando la policía se lo pide. Vale la pena configurar WhatsApp si tu comunidad ya lo usa y es poco probable que se cambie, pero intenta llevar las conversaciones de mayor riesgo a Signal.

Sigue aprendiendo con estas guías relacionadas

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

Fundamentos de seguridad
Prácticas básicas de seguridad que toda persona activista debería seguir.

Protección contra spyware
Protégete del spyware y los programas de vigilancia.

Defensa contra doxxing
Protégete del doxxing y del acoso en línea.

- VPNs para activistas 15 min de lectura 23
- Verificador de actualizaciones de seguridad 14
- Cómo usar Proton de forma segura 16 min de lectura 24
- Eliminar rastreo de enlaces 3 min de lectura 25
- ¿Es Signal seguro? 4 min de lectura 26
- ¿Apple Intelligence está leyendo mis mensajes de Signal? 5 min de lectura 20

Enlaces

1. activistchecklist.org/es/contribute/
2. justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/
3. rollingstone.com/politics/politics-features/whatsapp-imessage-facebook-apple-fbi-privacy-1261816/
4. ssd.eff.org/module/how-to-use-whatsapp
5. activistchecklist.org/es/essentials/
6. activistchecklist.org/es/signal/
7. faq.whatsapp.com/1324084875126592/?cms_platform=web
8. nitter.net/camhigby/status/2015093531526729789
9. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
10. activistchecklist.org/es/doxxing/

11. support.apple.com/en-us/105120
12. landing.google.com/intl/en_us/advancedprotection/
13. activistchecklist.org/es/lockdown/
14. activistchecklist.org/es/updates/
15. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
16. ssd.eff.org/module/attending-protest
17. strongphrase.net/passcode
18. redact.dev/blog/meta-camera-roll-ai-sharing-suggestions-2025
19. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
20. activistchecklist.org/es/signal-ai/
21. activistchecklist.org/es/spyware/
22. freedom.press/digisec/blog/upgrading-whatsapp-security/
23. activistchecklist.org/es/vpn/
24. activistchecklist.org/es/proton/
25. activistchecklist.org/es/links/
26. activistchecklist.org/es/signal-secure/