Lista de seguridad de Signal

ACTIVIST CHECKLIST

Última actualización **3 de abril 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/signal/

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

Esta guía te ayuda a tomar el control de tus conversaciones privadas en Signal[2]. Aunque Signal ya cifra todo lo que envías, estos pasos extra hacen que tus chats sigan siendo privados, incluso si pierdes tu teléfono, te lo quitan o lo hackean. Vas a aprender formas sencillas de proteger tus mensajes, notificaciones e identidad.

¿Eres nuevo en Signal? Echa un vistazo a esta guía para principiantes sobre cómo usar Signal[3].

Tip: Configurar Signal funciona muy bien como una sesión en grupo con amigues[4]. La mayoría de los pasos toman de 5 a 10 minutos una vez que te sientas a hacerlos.

Oculta tu identidad en Signal

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

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[5] y los policías[6].

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[7] 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.

Activa el nombre de usuario y oculta tu número de teléfono

Si quieres tener la opción de ser anónime en Signal, proteger tu número de teléfono ayuda a proteger tu identidad.

Si instalaste Signal antes de marzo de 2024, cuando introdujeron los nombres de usuario[8], puede que tu número de teléfono siga siendo visible para otras personas.

CÓMO ACTIVAR LOS NOMBRES DE USUARIO Y OCULTAR TU NÚMERO DE TELÉFONO

1. Asegúrate primero de cambiar el nombre que se muestra en tu perfil (ve el punto anterior). Si el nombre que se muestra en tu perfil de Signal es tu nombre completo, ocultar tu número de teléfono solo te ayudará un poco.
2. **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 sin relación** con tu identidad, ni con nombres de usuario que hayas usado antes en otros lugares. Debe terminar en al menos 2 números.
3. **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**.
    1. Opcionalmente, puedes cambiar "Quién puede encontrarme por número". Pero esto significará que ninguno de tus contactos actuales sabrá que ya estás en Signal a menos que tú les escribas primero. Solo cambia esto a "Nadie" si necesitas niveles muy altos de privacidad.
4. **Comparte tu nombre de usuario en lugar de tu número de teléfono:** Si te estás conectando con alguien nuevo por motivos políticos, comparte tu nombre de usuario. Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → **Código QR o enlace** → comparte el código QR o el enlace con la persona con la que quieres estar en contacto. O más sencillo aún, solo dile cuál es tu nombre de usuario.

Desactiva las vistas previas de enlaces

Puede protegerte de que se revele tu ubicación aproximada

Esto te protege de ciertos ataques. Pero asegúrate de revisar bien la URL a la que te están enviando para ver si es de un sitio que te sientes cómode abriendo.

CÓMO DESACTIVAR LAS VISTAS PREVIAS DE ENLACES

Abre Signal → Toca tu foto de perfil → **Ajustes** → **Chats** → **Desactiva Generar vistas previas de enlaces**

Contexto técnico: En 2025 se publicó[9] un ataque que le permite a quien lo usa estimar tu ubicación con un margen de unas 250 millas.

Activa "Retransmitir siempre las llamadas"

Por defecto, las llamadas de Signal se conectan directamente entre tú y la otra persona. Esto significa que el dispositivo de la otra persona puede ver tu dirección IP. Con una orden judicial dirigida a tu proveedor de internet, tu dirección IP puede usarse para identificarte específicamente.

Activar "Retransmitir siempre las llamadas" hace que tus llamadas pasen por los servidores de Signal, ocultando tu dirección IP a la otra persona. (Si ya usas una VPN[10], tu dirección IP ya está oculta.)

CÓMO ACTIVAR RETRANSMITIR SIEMPRE LAS LLAMADAS

Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Avanzado** → Activa **Retransmitir siempre las llamadas**

Protege tus mensajes y llamadas

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

- [ ] 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[11] 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.

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

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

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

1. Pueden ver las notificaciones en tu pantalla de inicio sin desbloquear el teléfono.
2. Si usan herramientas de hacking, pueden acceder al registro de notificaciones que ha recibido tu teléfono. (Ejemplo del caso Prairieland[12].)

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

CÓMO DESACTIVAR LAS NOTIFICACIONES DE SIGNAL

EN IPHONE

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

EN ANDROID

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

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

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

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

Activa "Screen Lock" y "Hide in App Switcher"

Si le pasas tu teléfono a alguien, Screen Lock es una capa extra de seguridad.

- **Screen Lock:** Si le pasas tu teléfono a alguien mientras está desbloqueado, esto hace que tengan que volver a usar el rostro, huella o PIN para abrir Signal.
- **Hide in App Switcher:** Esto oculta tus mensajes cuando cambias entre aplicaciones.

CÓMO OCULTAR LA PANTALLA EN EL SELECTOR DE APPS

IPHONE

Abre Signal → Toca tu foto de perfil → **Settings** → **Privacy** → Activa **Screen Lock** y luego activa **Hide Screen in App Switcher**

ANDROID

Abre Signal → Toca tu foto de perfil para abrir **Settings** → **Privacy** → Activa **Screen lock** y luego activa **Screen Security**

Desactiva "Show Calls in Recents" (solo iPhone)

Esto evita que la policía vea tu historial de llamadas de Signal si te confiscan el teléfono.

CÓMO DESACTIVAR "SHOW CALLS IN RECENTS"

Esta opción solo existe en los iPhone: Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Llamadas** → Desactiva **Mostrar llamadas en Recientes**

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

Activa el PIN de Signal y el bloqueo de registro

Te protege de ataques avanzados en los que alguien "roba" tu número de teléfono y lo registra en Signal

Si alguien con mucho interés en atacarte logra averiguar tu número de teléfono, puede intentar robártelo con algo llamado " SIM Swapping" o llamando a tu compañía telefónica para pedir una "portabilidad" de tu número a otra compañía. Luego podrían usar tu número de teléfono para registrar una cuenta de Signal y empezar a recibir mensajes dirigidos a ti.

Estos son ataques avanzados que no le pasan a la mayoría de la gente. Aun así, es fácil proteger tu cuenta de Signal.

Puedes protegerte activando el **bloqueo de registro** en Signal. Evita que alguien secuestre tu cuenta, incluso si te roban el número de teléfono. Nadie podrá registrar una nueva cuenta de Signal con tu número hasta que tu cuenta haya estado inactiva por 7 días.

Si olvidas tu PIN, tendrás que esperar 7 días antes de poder crear una cuenta nueva (y tus contactos no se recuperarán). Más sobre los PIN y el bloqueo de registro[14].

CÓMO ACTIVAR EL PIN DE SIGNAL Y EL BLOQUEO DE REGISTRO

Activa el bloqueo de registro: Abre Signal → Toca tu foto de perfil → **Ajustes** → **Cuenta** → Activa **Bloqueo de registro**

Mejora tu PIN: Tuviste que configurar un PIN de Signal durante la instalación. Si no lo recuerdas o quieres usar un PIN más fuerte, así es como puedes hacerlo:

1. **Genera un PIN fuerte:** Para máxima seguridad, usa un PIN de 8 o 10 dígitos y asegúrate de que sea generado por computadora. Aquí tienes un generador de PIN aleatorios[15] que puedes usar.
2. **Configura un PIN de Signal:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Cuenta** → **Crear/Cambiar PIN** (Si aún no sabes cuál es tu PIN).
3. **Guarda tu PIN o activa los recordatorios de PIN:** Si tienes un gestor de contraseñas[16] que usas con regularidad, guarda tu PIN ahí. Si crees que podrías olvidar dónde guardaste tu PIN, deja activados los "recordatorios de PIN".

Activa un teclado privado para Signal (solo en Android)

En Android, el teclado predeterminado puede registrar lo que escribes.

CÓMO ASEGURARTE DE TENER UN TECLADO PRIVADO EN ANDROID

Nota: Esto es solo para teléfonos Android. Los teclados de los iPhones ya son privados, a menos que hayas instalado un teclado personalizado.

OPCIÓN 1 (más fácil) - Activa un teclado de incógnito
Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Seguridad de la aplicación** → Activa **Teclado de incógnito**

OPCIÓN 2 (más privada) - Reemplaza el teclado integrado en todo el sistema

- La opción anterior simplemente "le pide" al proveedor del teclado (Google) que no registre lo que escribes. No hay garantía de que cumpla. Lo más seguro es instalar un teclado personalizado.
- FlorisBoard[17] es una buena opción. Primero debes instalar F-Droid[18], que es una tienda de apps más privada.

Desactiva los resúmenes de notificaciones con IA

Google y Apple no han dejado claro cuándo sus herramientas de IA envían nuestra información privada (como los mensajes de Signal) fuera de nuestro dispositivo a sus servicios. Si se envían a sus servidores, corren el riesgo de ser accedidos mediante una orden judicial del gobierno.

Por lo que entendemos, estas funciones de IA ***por ahora*** solo resumen las notificaciones. Pero por cómo van las cosas, podrían volverse más invasivas.

Lee nuestro artículo sobre ¿Apple Intelligence está leyendo mis mensajes de Signal?[19]

OPCIÓN A: CÓMO DESACTIVAR LOS RESÚMENES DE NOTIFICACIONES CON IA SOLO PARA SIGNAL

Opción A: Desactiva los resúmenes de notificaciones con IA solo para Signal

IPHONE

Abre la app **Ajustes** → **Notificaciones** → **Resumir notificaciones** → Desactiva **Signal**

ANDROID

Ajustes → **Notificaciones** → **Resúmenes de notificaciones** → **Administrar apps** (en **No incluir estas apps**) → Desactiva **Signal**

CÓMO DESACTIVAR POR COMPLETO LOS RESÚMENES DE NOTIFICACIONES CON IA

Opción B: Desactiva por completo los resúmenes de notificaciones con IA

IPHONE

Abre la app **Ajustes** → **Apple Intelligence y Siri** → Desactiva **Apple Intelligence**

ANDROID

Abre **Ajustes** → **Notificaciones** → Desactiva **Usar resúmenes de notificaciones** (o **Resúmenes de notificaciones**)

MAC

> **Ajustes del Sistema** → **Apple Intelligence y Siri** → Desactiva **Apple Intelligence** → **Confirmar**

(Para Mac se necesita una computadora Apple con procesador M1 o más reciente.)

Mantente alerta ante mensajes falsos de "Signal Support" que intentan obtener tu PIN de Signal o tu código de verificación

Protege tu cuenta y no entregues tu código de verificación ni tu PIN

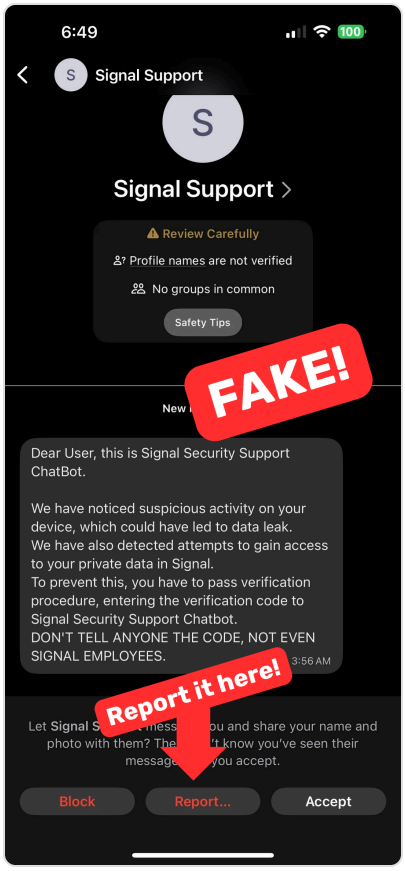
Cada vez hay más mensajes falsos de "Signal Support"[20] que intentan secuestrar tu cuenta.

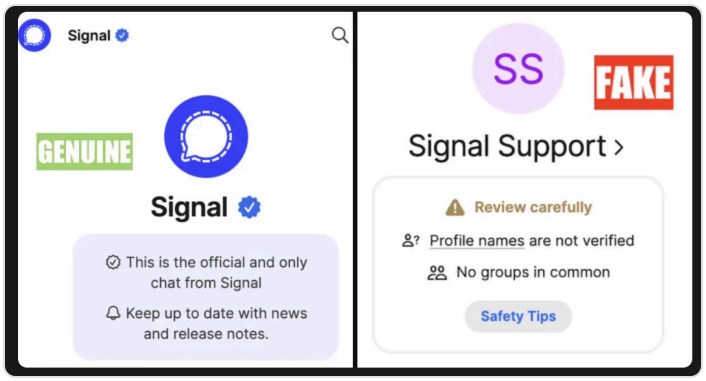
Usa estos ejemplos para estar atente a mensajes falsos de Signal.

Recuerda: Signal nunca te va a pedir que les envíes tu PIN ni tu código de verificación. Solo te lo pedirá cuando estés instalando la app por primera vez en un dispositivo.

Lee más sobre estafas y phishing en Signal.[21]

Aquí van algunos ejemplos de mensajes de estafa:





Asegura tu teléfono

Signal es tan seguro como el teléfono donde lo uses. Si te confiscan o hackean tu dispositivo, la policía tiene herramientas forenses que pueden descifrar códigos de acceso débiles y sacar tus mensajes directamente de tu dispositivo. Estos pasos protegen tus mensajes de Signal a nivel del dispositivo.

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

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[15] 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[15]. (¡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[15].

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[22]
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[22]
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[22]
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[22]
3. **Apps de la Microsoft Store:** Asegúrate de activar las actualizaciones automáticas[23] (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[24] 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**.

Protección más alta

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 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**[25] y en Android se llama **Programa de Protección Avanzada**[26]. (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[27]. 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.

Verifica los números de seguridad con tus contactos importantes

Confirma que nadie está interceptando en secreto tus mensajes entre tú y la otra persona

Signal cifra tus mensajes para que solo tú y la otra persona puedan leerlos. Pero en teoría, un atacante sofisticado podría colocarse entre tú y tu contacto, interceptando los mensajes antes de pasarlos. Esto se conoce como un ataque de "intermediario" o "man-in-the-middle". Los **números de seguridad** te permiten confirmar que tu conexión cifrada va directo a tu contacto, sin que nadie se meta en el medio.

La mayoría de la gente no necesita hacer esto. Si estás chateando con amistades sobre organización del día a día, el cifrado de Signal ya está haciendo su trabajo. Pero si estás comunicándote sobre algo de alto riesgo (acciones directas, asuntos legales delicados, periodistas hablando con una fuente), verificar los números de seguridad vale la pena el paso extra.

Piénsalo como un sello de cera en un sobre. El cifrado es el sello, pero un atacante sofisticado podría romperlo, leer el contenido y volver a sellarlo con su propia cera. Verificar los números de seguridad es la forma de confirmar que nadie cambió el sello.

CÓMO VERIFICAR LOS NÚMEROS DE SEGURIDAD

1. **Abre la conversación** con la persona que quieres verificar → **Toca su nombre** en la parte de arriba → **Ver número de seguridad**.
2. **Compara los números con tu contacto:**
   - **En persona (lo mejor):** Toca "Escanear código" y escanea su código QR. Si coincide, verás un mensaje de éxito.
   - **A distancia:** Léanse los números mutuamente en una llamada o videollamada donde estés seguro de que estás hablando con la persona correcta. No lo verifiques por Signal mismo.
3. **Marca como verificado:** Si los números coinciden, toca la marca de verificación.

Solo necesitas hacer esto una vez por contacto, a menos que sus números de seguridad cambien (por ejemplo, si consigue un teléfono nuevo). Si eso pasa, Signal te avisará. Verifica de nuevo antes de compartir algo sensible.

¿Hackearon Signal? ¿Es seguro? ¿Es confiable?

Cada par de meses vemos circular publicaciones que aseguran que Signal no es seguro o que lo hackearon.

¿Hackearon Signal? Casi seguro que no[28].

Para una explicación más completa sobre la seguridad de Signal, incluyendo su propiedad sin fines de lucro, cifrado, código abierto, rumores sobre financiamiento y riesgos del dispositivo, lee nuestro artículo: ¿Es seguro Signal?[29].

Hay riesgos al usar Signal, pero generalmente tienen que ver con usarlo de forma segura, no con la tecnología en sí.

Por ejemplo, si alguien se infiltra en un grupo privado de Signal, podría tomar capturas de pantalla de todos los mensajes y publicarlos en línea.

También es posible que los cops confisquen tu teléfono y logren entrar si tienes un passcode débil. Pero eso no es una falla de Signal. Todos tus mensajes están disponibles para cualquiera que tenga acceso físico a tu teléfono y pueda desbloquearlo. Por eso recomendamos tener un passcode fuerte[16] y mantener siempre actualizado el sistema operativo de tu dispositivo[16].

Otros recursos

- ¿Es seguro Signal?[29] — cómo funciona Signal, qué datos puede compartir y mitos comunes sobre su seguridad.
- Aquí tienes una excelente guía sobre cómo usar los grupos de Signal para el activismo[30].
- Asegurando Signal[31] — Freedom of the Press Foundation

Preguntas frecuentes

¿Signal es realmente seguro?

Sí. Signal es el mensajero más seguro de uso masivo disponible. Los mensajes y las llamadas tienen cifrado de extremo a extremo, el código es open source, y Signal lo administra una organización sin fines de lucro que no guarda el contenido de los mensajes. Los mayores riesgos suelen estar en cómo se usa Signal, no en la tecnología en sí: un código de acceso débil, un grupo con alguien infiltrado, o alguien tomando capturas de pantalla.

¿Los cops pueden leer mis mensajes de Signal?

Depende. No pueden sacar tus datos de los servidores de Signal. Tus mensajes tienen cifrado de extremo a extremo, así que si la policía le manda una orden judicial a Signal, la empresa solo puede entregar información básica de tu cuenta, como cuándo te registraste y cuándo usaste la app por última vez. Pero si la policía te quita el teléfono, puede obligarte a desbloquearlo con tu cara o tu huella, o usar herramientas forenses para descifrar un código de acceso débil. Una vez que entran, pueden leer todos los mensajes que sigan en el teléfono. Lo mismo pasa con cualquier persona con la que hayas estado chateando. Por eso recomendamos que todes usen un código de acceso fuerte, desactiven el desbloqueo con cara o huella y activen los mensajes temporales.

¿Signal es más seguro que WhatsApp?

Para uso activista, sí. WhatsApp usa el mismo protocolo de cifrado que inventó Signal, pero pertenece a Meta, recopila metadatos detallados sobre quién habla con quién y cuándo, y los comparte con Facebook. Ante pedidos de las autoridades, Meta entrega muchos más datos que Signal.

¿Necesito verificar los números de seguridad?

Para tus contactos más cercanos de organización y cualquier persona con la que hables de planes sensibles, sí. Verificar una vez le dice a Signal que confirmaste que este contacto es quien dice ser. Sin verificación, un atacante sofisticado que controle la red telefónica podría, en teoría, cambiar una llave. Con verificación, te avisarían si eso pasara.

¿Debería usar mi número de teléfono real en Signal?

Si puedes usar un nombre de usuario en lugar de tu número, esa es la opción más privada. Signal ahora te deja poner un nombre de usuario y ocultar tu número de las personas que no lo tengan ya en sus contactos. Activistas que quieran más distancia pueden registrar Signal con un número secundario de MySudo, Google Voice, o una SIM prepagada.

¿Para qué sirve el PIN de registro?

El PIN te permite recuperar tu perfil de Signal, contactos y grupos si pierdes tu celular o configuras Signal en un dispositivo nuevo. También evita que alguien que te robe la SIM pueda registrar Signal como tú en su celular. Elige un PIN largo y guárdalo en tu gestor de contraseñas.

Sigue aprendiendo con estas guías relacionadas

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

Prepárate para una protesta
Seguridad digital para quienes asisten a una protesta.

Seguridad en viajes y vuelos
Prácticas de seguridad digital para activistas que viajan.

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

- VPNs para activistas 15 min de lectura 10
- Verificador de actualizaciones de seguridad 22
- Cómo usar Proton de forma segura 16 min de lectura 32
- Eliminar rastreo de enlaces 3 min de lectura 33
- ¿Apple Intelligence está leyendo mis mensajes de Signal? 5 min de lectura 19

Enlaces

1. activistchecklist.org/es/contribute/
2. signal.org
3. ssd.eff.org/module/how-to-use-signal
4. activistchecklist.org/es/party/
5. nitter.net/camhigby/status/2015093531526729789
6. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
7. activistchecklist.org/es/doxxing/
8. signal.org/blog/phone-number-privacy-usernames/
9. gist.github.com/hackermondev/45a3cdfa52246f1d1201c1e8cdef6117
10. activistchecklist.org/es/vpn/
11. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
12. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
13. activistchecklist.org/es/secondary/
14. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
15. strongphrase.net/passcode
16. activistchecklist.org/es/essentials/
17. florisboard.org
18. f-droid.org/en/
19. activistchecklist.org/es/signal-ai/

20. netzpolitik.org/2026/phishing-attack-numerous-journalists-targeted-in-attack-via-signal-messenger/
21. support.signal.org/hc/en-us/articles/9932566320410-Staying-Safe-from-Phishing-Scams-and-Impersonation
22. activistchecklist.org/es/updates/
23. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
24. ssd.eff.org/module/attending-protest
25. support.apple.com/en-us/105120
26. landing.google.com/intl/en_us/advancedprotection/
27. activistchecklist.org/es/lockdown/
28. hassignalbeenhacked.info
29. activistchecklist.org/es/signal-secure/
30. micahflee.com/using-signal-groups-for-activism/
31. freedom.press/digisec/blog/locking-down-signal/
32. activistchecklist.org/es/proton/
33. activistchecklist.org/es/links/