

La iniciativa DefiendeMesoamérica tiene por objetivo respaldar a las personas y comunidades que cuidan los bosques mesoamericanos y a las personas que trabajan en su protección.

Escanea para conocer más de la iniciativa



www.defiendemesoamerica.org

info@defiendemesoamerica.org

CONTACTO

CONSEJOS PARA APPS DE MENSajería



DefiendeMesoamérica
Iniciativa Mesoamericana para la Defensa Integral de Personas Cuidadoras de los Bosques

Herramientas de cuidado digital

Si te quitan el celular, lo pierdes o te lo revisan sin tu permiso, no solo se llevan un aparato: pueden acceder a tus conversaciones, contactos, fotos y mucha información importante sobre tu comunidad o tu trabajo de defensa del territorio. Por eso es importante tomar medidas simples, pero efectivas, para cuidar lo que compartimos y con quién hablamos, sobre todo si trabajamos en la defensa de la tierra, el agua, los bosques, o los derechos humanos.

Este material está pensado justo para eso: ayudarte a proteger tus mensajes en aplicaciones como WhatsApp y Signal. Aquí encontrarás recomendaciones fáciles de aplicar, como bloquear el acceso a tus chats, ocultar conversaciones, usar mensajes temporales y activar opciones de seguridad que ya vienen incluidas en las apps. No necesitas instalar nada extra ni ser experta o experto en tecnología.



La idea no es complicarte, sino prevenir. Porque aunque no podamos controlar todo lo que pasa, sí podemos reducir los riesgos. Y cuando cuidamos nuestra información, también estamos cuidando a las personas con las que nos organizamos y a las luchas que defendemos por la tierra, el agua y la vida.

Tómate unos minutos para aplicar estos consejos y compártelos con tu gente. En estos tiempos, la seguridad digital también es parte de nuestra defensa colectiva.

Tips para usar en WhatsApp

#1 Bloquea el acceso a la app con datos biométricos

Bloqueando el acceso a WhatsApp agrega seguridad a todos tus chats. Si tu teléfono es robado o lo pierdes, no podrán abrir la aplicación, manteniendo tus mensajes inaccesibles. Utiliza datos biométricos.

iOS: Ajustes > Privacidad > Bloqueo de aplicación > Requerir Face ID

Android: Ajustes > Privacidad > Bloqueo de aplicación > Desbloquear con rasgos

#2 Bloquea y oculta tus chats

Bloquear y ocultar chats agrega una capa seguridad, incluso si han accedido físicamente a tu celular. Los "chats restringidos" aparecen en la parte superior de tu lista de chats y necesitan autenticación biométrica o a través de PIN para acceder a ellos.

Para mayor privacidad puedes ocultarlos de tu lista de chats para que no aparezcan listados. Necesitarás escribir un PIN o contraseña en el buscador de WhatsApp para encontrarlos.

Restringir Chat:

iOS: Mantener presionado chat > Restringir chat

Android: Mantener presionado chat > Seleccionar 3 puntitos > Restringir chat

Ocultar chats restringidos:

Android/iOS: Chats restringidos > Ajustes > Ocultar Chats restringidos

#3 Deshabilita la visibilidad de las fotos en la galería

Las imágenes y videos descargados son visibles en la galería de tu teléfono, incluidos memes, pantallazos, y fotos de grupos que ni siquiera aún revisas.

iOS: Ajustes > Chats > Apaga "Guardar en Fotos"

Android: Ajustes > Chats > Apaga "Visibilidad de Archivos"

MANTEN TUS CHATS SEGUROS

#4 Usa mensajes temporales

Borrar el historial de mensajes automáticamente protege tu privacidad si alguien tiene acceso a tu teléfono o de otra persona con la que conversas. Además disminuye tu huella digital.

iOS: En el chat > Click en el nombre del chat > Mensajes temporales

Android: En el chat > Seleccionar 3 puntitos > Mensajes temporales

#5 Activa Doble Autenticación

Usando el doble factor de autenticación (2FA) no será tan fácil obtener control de tu cuenta de WhatsApp, ya que no solo se requiere acceso a tu celular o número sino que también se necesitará un código o PIN de 6 dígitos creado por tí.

Android/iOS: Ajustes > Cuenta > Verificación en dos pasos > Activar

#6 Encripta tus respaldos

Si decides guardar respaldos de tus chats en Google Drive o iCloud estos datos no estarán encriptados, esto permite que cualquiera que acceda a ellos puede leerlos, para evitar esto puedes activar la encriptación de tus respaldos.

iAndroid/iOS: Ajustes > Chats > Copia de seguridad > Copia de seguridad cifrada de extremo a extremo



Tips para usar en Signal

#1 Usa un alias, no tu número

No es necesario que compartas tu número telefónico a tus contactos de Signal, tanto ellos como tu puedes usar sus "alias", funciona igual que un número, manteniendo esa información privada.

Android/iOS: Ajustes > Click sobre tu nombre > @ Alias

#2 Usa Bloqueo de registro

Esta función te ayuda a evitar secuestros de tu cuenta. Esto evita que personas no autorizadas puedan acceder a tu cuenta, incluso si obtienen acceso a tu número de teléfono o al código de verificación. Si alguien da de alta tu cuenta en otro dispositivo, necesitará del código PIN.

Android/iOS: Ajustes > Cuenta > Bloqueo de registro

#3 Bloquea el acceso a la app

Bloqueando el acceso a Signal agrega seguridad a todos tus chats. Si tu teléfono es robado o lo pierdes, no podrán abrir la aplicación, manteniendo tus mensajes inaccesibles. Utiliza datos biométricos o PIN.

Android/iOS: Ajustes > Privacidad > Bloqueo de pantalla

#4 Usa mensajes temporales

Borrar el historial de mensajes automáticamente protege tu privacidad si alguien tiene acceso a tu teléfono o de otra persona con la que conversas. Además disminuye tu huella digital.

iOS: En el chat > Click en el nombre del chat > Mensajes temporales

Android: En el chat > Ajustes del chat > Mensajes temporales