

# GUÍA

Esta guía es para personas migrantes y refugiadas que se encuentran movilizándose o en un nuevo espacio y proporciona herramientas para disminuir los impactos de la violencia de género digital en sus vidas.

# PARA MOVERSE SEGURAS Y SEGUROS





# GUÍA

## PARA MOVERSE SEGURAS Y SEGUROS



Realizado con el apoyo de la Agencia de la ONU para los  
Refugiados (ACNUR) y apoyo del Gran Ducado de Luxemburgo

# GUÍA PARA MOVERSE SEGURAS Y SEGUROS

Si te han amenazado o extorsionado a través de redes sociales o correo electrónico, divulgado tus datos personales o información íntima, o has sentido incomodidad y acoso en chats de redes sociales o mensajería instantánea, entonces conoces la *violencia de género digital*.

Es toda forma de discriminación, acoso, explotación, abuso y agresión que se produce a través del uso de redes sociales, correo electrónico, celulares y cualquier medio dentro de las tecnologías de la información y comunicación (TICS), que conlleva diferentes afectaciones a nivel físico, psicológico, sexual y económico

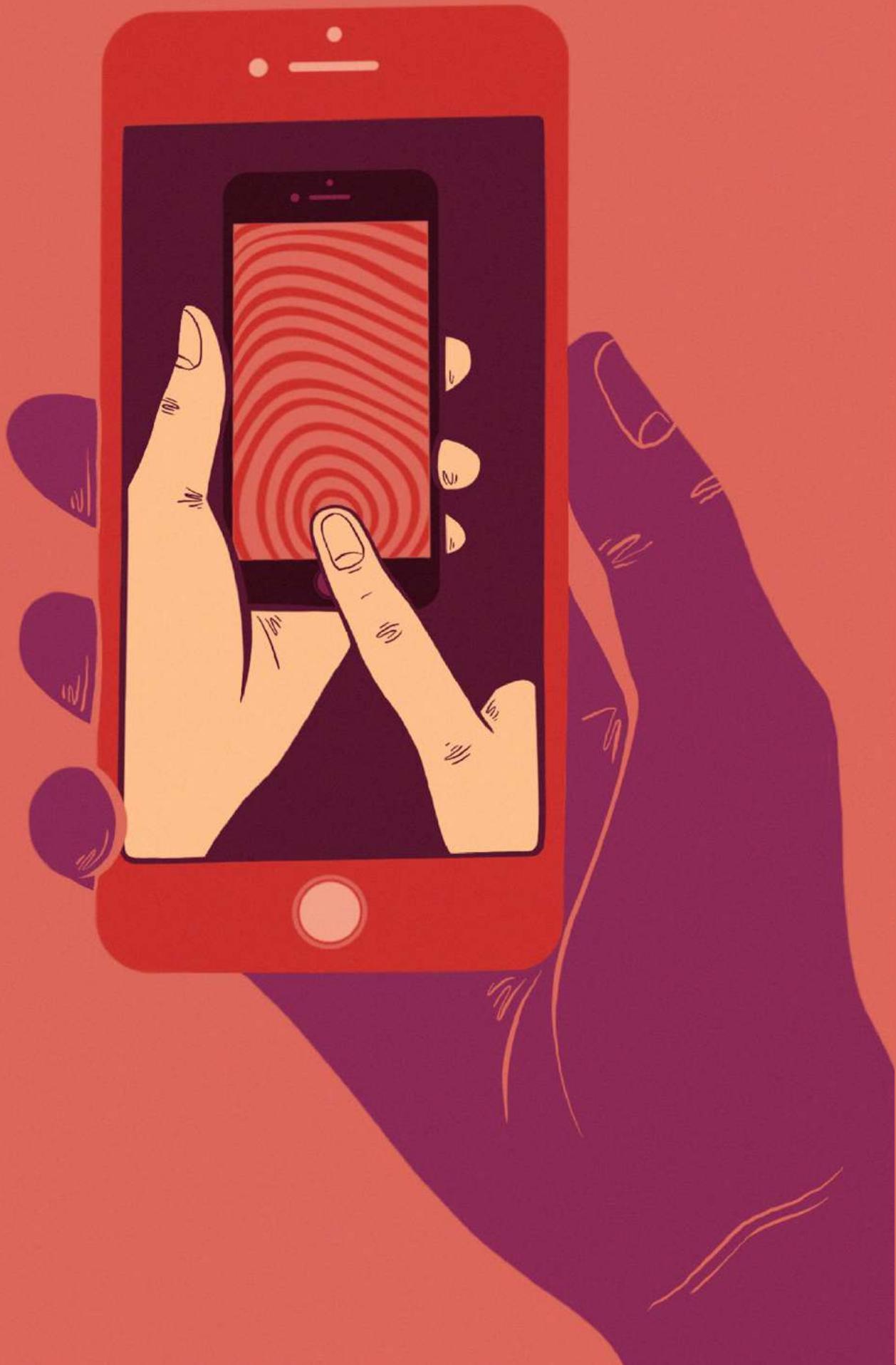
La mejor manera de protegerse es conociendo mejor como funciona la internet y tus dispositivos, celulares, tablets, y computadoras.

## PROTECCIÓN DIGITAL

Es la búsqueda de estrategias y herramientas para cuidar la información personal y laboral que se guarda en dispositivos y en la internet mejorando la capacidad de asegurar nuestras comunicaciones.

Constantemente en el espacio digital recibimos información falsa, acoso digital y sexual. Proteger la información que se encuentra pública en redes sociales y en nuestros dispositivos es la manera de prevenir agresiones físicas y digitales.





# ¿QUÉ ES LA PROTECCIÓN DIGITAL?

1. *Haz una lista del número de cuentas en redes sociales, correo electrónico y aplicaciones que tienes: ¿Uso todas? ¿Hace cuánto no la uso? ¿necesito todas estas cuentas?*
2. *Elimina las cuentas que no utilizas, ¿cómo lo haces?*  
Todas las redes sociales y correo electrónico tienen un opción de configuración, entra y busca "Eliminar cuenta".
3. *¿Cuándo fue la última vez que cambiaste la contraseña de tus cuentas, correo electrónico, dispositivos y redes sociales?*
  - Cada cuenta debe tener otra contraseña diferente, nunca REPITAS.
  - Es importante que si te encuentras en movimiento cambies estas contraseñas cada 3 a 6 meses.
  - Utilizar frases u oraciones fácil de recordar (cómo nombre de una película, libro, frase de una canción).
  - Debe tener al menos 12 caracteres, incluir espacios en blanco y/o caracteres especiales (%&/\$ • %).
  - Evitar el uso de datos personales como fechas de nacimiento, nombres de hijos/as, etc.

# ELIMINA TU RASTRO

Entender como no dejar rastro de nuestros datos personas en las redes y en las aplicaciones es fundamental para que no puedan ver nuestra ubicación e información privada.

## ¿ME COMUNICO POR MENSAJERÍA INSTANTÁNEA? ¿USO CANALES SEGUROS?

Lamentablemente WhatsApp y Facebook Messenger NO son canales seguros.

Existen otras opciones que son aplicaciones igualmente vinculadas a nuestros números de teléfono que permiten tener mayor seguridad principalmente, porque no guardan los datos personales.

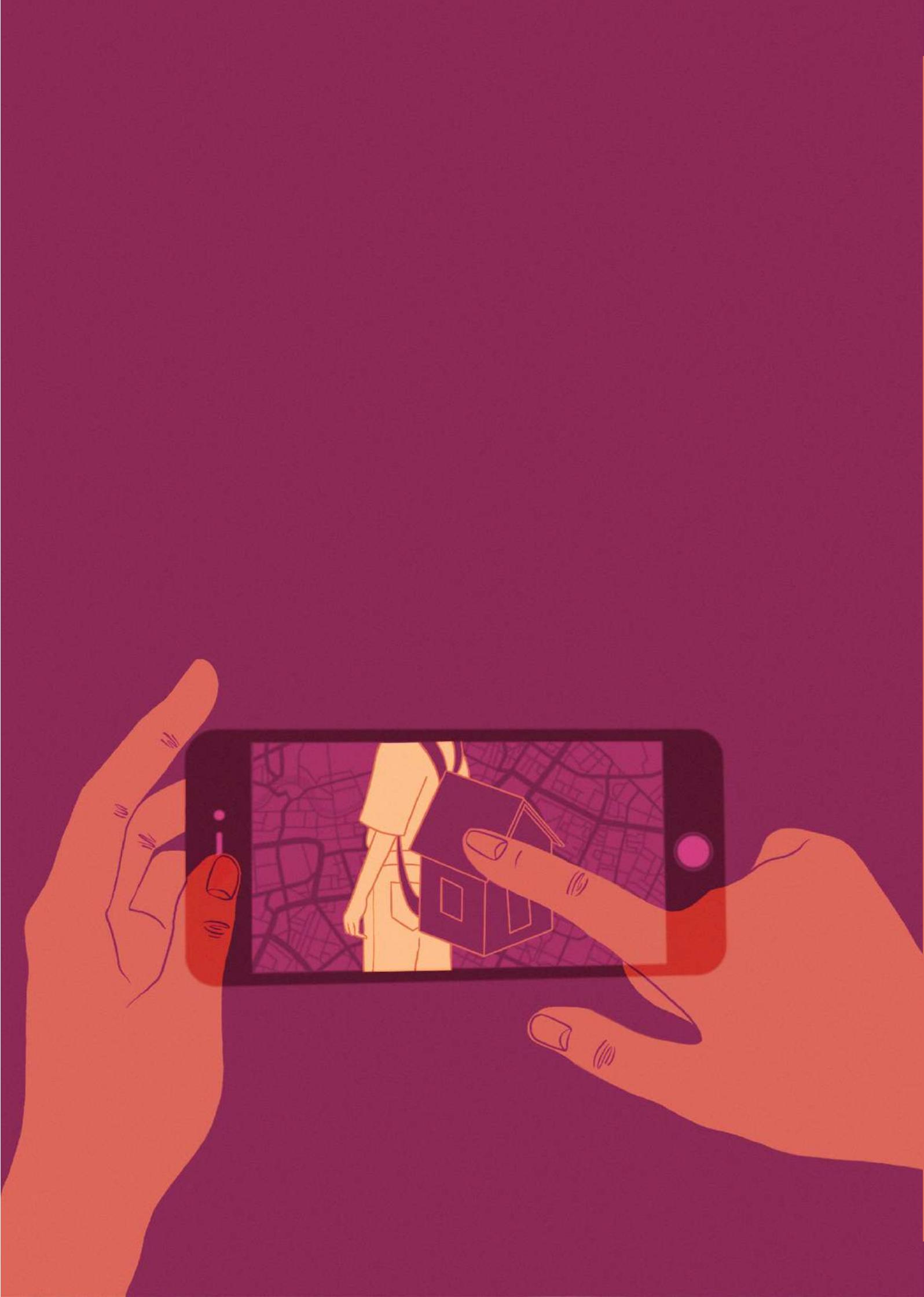
## ESTAS OPCIONES SON SIGNAL Y WIRE

Te permiten comunicarte por llamadas, videollamadas, mensajes y sobre todo, configurar la opción "Desaparecer mensajes" en un determinado tiempo.

## MANTÉN TU UBICACIÓN SEGURA Y PRIVADA:

- Asegúrate que cualquier tipo de reconocimiento geográfico, GPS, esté apagado en tus aplicaciones y tus aparatos.
- No hagas publicaciones en tiempo real.
- Si planeas publicar fotos con alguien más, asegúrate de recibir su autorización
- No envíes fotos donde se pueda ver tu ubicación.





# REDES SOCIALES

*Evita interactuar con cuentas desconocidas en redes sociales, te puedes poner en riesgo y ser vulnerable al acoso digital y al doxxing (enviar y exponer tu información públicamente por el internet).*

Revisa cuales son las políticas de privacidad y seguridad de tu cuenta de redes sociales. Intenta configurarla de manera que tu mantegas el mayor control posible sobre tu información.

## USA LA AUTENTICACIÓN DE DOS FACTORES EN CADA CUENTA QUE LO OFREZCA

*“Autenticación de Dos factores” se asegura de confirmar tu identidad después de que hayas ingresado tu contraseña, usualmente mandando un texto a tu teléfono con un código para que puedas acceder a un sitio web o utilizar una aplicación.*

Facebook, Twitter, y muchos servicios de correo electrónico ofrecen autenticación de dos factores.

Recuerda: nunca publiques tu número de teléfono, dirección u otra información privada en redes sociales.

# CONOCE TU CELULAR

Tú celular es un dispositivo que necesita constante limpieza de información y revisión, de manera que pueda ser una herramienta segura:

- Revisa la memoria de almacenamiento, borra todo lo que ya no necesites en > administración de archivos.
- Revisa que cuenta de correo electrónico se encuentra vinculada a tu celular, actualízala.
- Realiza respaldos y formatea una vez al año tu celular, le dará más tiempo de vida.
- Revisa las aplicaciones, si hay alguna que ya no uses elimínala.
- Cada aplicación tiene ciertos permisos, entra a cada una y revisa que tipo de permisos le estas concediendo como:
  - Ubicación > desactívalo para todas las aplicaciones.
  - Micrófono > desactívalo en apps que no utilices para hablar.
  - Cámara > desactívalo en apps que no utilices para hacer fotos.
  - ¿Qué modelo de celular es? ¿Cuánta memoria RAM y de almacenamiento tiene?

## BUSCAR TRABAJO POR INTERNET

La información que se encuentra disponible en internet no siempre es de confianza, por eso te damos algunos tips a continuación:

- Fijate que pongan nombre de la empresa o negocio, dirección o algún dato que te permita verificar su existencia.
- Comprueba buscando en redes sociales la existencia del negocio o trabajo.
- Para solicitar información sobre el trabajo envía un correo electrónico de preferencia, y sino, pregunta por redes, no uses tu número directamente.
- Nunca entregues tus datos personales como dirección de vivienda o número de pasaporte.





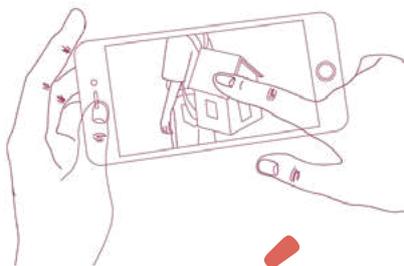
## AVISO

Si necesitas más información, conoces o has sufrido violencia de género por redes sociales, a través de tu celular o vía internet, repórtalo, nosotras te acompañamos.

E-mail seguro: [reportalaviolenciadigital@riseup.net](mailto:reportalaviolenciadigital@riseup.net)

**\*SE GUARDARÁ LA CONFIDENCIALIDAD DEBIDA DEL CASO.**

Más información en  
<https://www.navegandolibres.org/>



# GUÍA

PARA MOVERSE  
SEGURAS Y SEGUROS

