Seguridad móvil

Comparte estrategias y tácticas para que podamos utilizar nuestros celulares de manera más segura. Recomendamos **enfáticamente** optar por alguna Ruta de Aprendizaje donde se incluyen actividades de diferentes niveles de profundidad que ayudan a las participantes a obtener una mayor perspectiva sobre los temas abordados.

Introducción y objetivos de aprendizaje

seguridad-movil.png

Image not found or type unknown

En este módulo, compartimos estrategias y tácticas para que podamos utilizar nuestros celulares de manera más segura en los contextos y situaciones que vivimos.

El módulo contiene guías para facilitar conversaciones sobre cómo las activistas de derechos de mujeres y derechos sexuales viven de distintas maneras el acceso a la tecnología celular y la comunicación digital debido a su orientación de género e identidad sexual. Hablaremos sobre cómo usamos nuestros celulares, tanto para nuestra comunicación personal y privada, como para comunicarnos públicamente y en nuestras redes activistas, además de las estrategias y herramientas que utilizamos para gestionar una comunicación celular más segura.

Este módulo incluye: actividades grupales para evaluar el uso que damos a los celulares y cómo se relaciona con nuestra orientación de género e identidad sexual; actividades prácticas para explorar y comprender cómo funcionan nuestros dispositivos y la comunicación celular; actividades grupales para compartir y practicar estrategias y tácticas más seguras en nuestro día a día; guías de facilitación para interrelacionar temas de seguridad feminista y seguridad técnica.

Preguntas frecuentes que escuchamos e intentamos abordar en este módulo:

- ¿Qué sucede cuando otra persona tiene mi celular? ¿Qué información está almacenada en mi celular? ¿Cómo me afecta a mí, a mis colegas y a mis redes activistas?
- ¿Cómo sé si mi pareja, ex, familiares o el gobierno me están vigilando?
- ¿Cómo utilizo mi celular de manera más segura?
- ¿Cómo puedo usar mi celular para organizarme políticamente?

Objetivos de aprendizaje

Al finalizar este módulo, las participantes:

- entenderán cómo el acceso a los celulares y la comunicación es algo íntimo y depende de la identidad de género;
- se familiarizarán con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para la vida personal-privada como para la esfera pública y a nivel de

nuestras redes activistas;
- obtendrán una noción de los conceptos básicos de cómo funciona la comunicación celular y los riesgos implicados;
- adquirirán y practicarán estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en sus vidas y las de sus compañeras y redes activistas;

image-1605452256072.png
Image not found or type unknown

Actividades y rutas de aprendizaje y lecturas complementarias

Esta página te guiará para entender y utilizar este módulo apropiadamente. Estas Rutas de Aprendizaje se componen de actividades de diferentes niveles de profundidad y permiten tener un mejor entendido de los temas relacionados.

Rutas de aprendizaje

Para las facilitadoras/entrenadoras que están interesadas en una actividad determinada, pueden usar una actividad suelta o combinar varias. **Recomendamos empezar por una Actividad Inicial para abrir la discusión y compartir experiencias sobre el uso que dan a los celulares y cómo el género, sexualidad, raza, clase y capacitismo entra en juego.**

Algunas recomendaciones específicas: para grupos que están considerando usar celulares para **documentar casos de violencia,** recomendamos la Actividad de Profundización Documentar casos de violencia para dar pie al debate y discusión sobre los desafíos y oportunidades a la hora de documentar casos de violencia y la Actividad Táctica Usar celulares para documentar casos de violencia: Planeación y práctica

Para los grupos que quieren **usar celulares para comunicarse, organizar y realizar acciones políticas,** sugerimos las Actividades Tácticas, en particular Planear nuestra comunicación celular para organizarnos y actuar y ¡Respalda! ¡Bloquea! ¡Elimina!

Para **quienes usen apps para citas y sexting**, echa un vistazo a la Actividad Inicial Celulares recolectores y las Actividades Tácticas Reinicia tu seguridad para citas en línea y Sexting más seguro.

Actividades de aprendizaje

Actividades iniciales

image-1605640724450.png
Image not found or type unknown

- Celulares, intimidad, acceso y seguridad según identidades de género
- Crear una línea de tiempo sobre nuestros celulares
- Senderismo en el Himalaya
- Celulares recolectores
- Mi celular y yo

Actividades de profundización

image-1605640735000.png
Image not found or type unknown

- El poder del celular - dispositivo, cuenta, servicio, estado, política
- ¿Qué es un celular? ¿Cómo funciona la comunicación telefónica?
- Debate: Documentar casos de violencia

Actividades tácticas

image-1605640743110.png
Image not found or type unknown

- Planear nuestra comunicación celular para organizarnos y actuar
- ¡Respalda! ¡Bloquea! ¡Elimina! También conocido como alguien tomó mi celular: cruzar fronteras, detenciones, incautación y robo
- Conversación, intro + sesion práctica: Escoger apps celulares
- Usar celulares para documentar casos de violencia: planear y poner en práctica
- Reinicia tu seguridad para citas en línea
- Sexting más seguro

Actividades externas basadas en herramientas

Los módulos que incluyen poner en práctica y utilizar herramientas y software específico están enlazados a recursos externos. Esto lo hacemos por varios motivos: el diseño y las funcionalidades de las herramientas, al igual que los temas de seguridad, cambian con frecuencia y pensamos que lo mejor es vincular a recursos que se actualizan con mayor frecuencia.

Mención especial para la capacitación en seguridad celular

Normalmente las participantes tienen diferentes tipos de celulares. Sugerimos formar grupos para las sesiones prácticas según el tipo de celular que tienen (iPhone, diferentes versiones de Android, celulares básicos).

Materiales | Enlaces | Lectura complementaria

en español (en proceso)

- https://ciberseguras.org/
- https://cyber-women.com/es/
- https://es.gendersec.train.tacticaltech.org/
- https://labekka.red/
- https://securityinabox.org/es
- Autoprotección digital contra la vigilancia de EFF: : https://ssd.eff.org/es

en inglés

- Guías de Video for Change: https://video4change.org/resource-categories/
- Guías de Witness: https://witness.org/resources/
- Security in a Box: https://securityinabox.org/en/
- Recursos de My Shadow: https://myshadow.org/ [Los materiales de capacitación y facilitación ya no están disponibles, pero aún hay una guía sobre cómo controlar tus propios datos.]

image-1605452256072.png
Image not found or type unknown

Celulares, intimidad, acceso y seguridad según identidades de género [actividad inicial]

activ-iniciales_200px-con-texto.png
Image not found or type unknown

Esta actividad es **una conversación inicial** sobre las maneras en que las participantes usan sus dispositivos celulares.

Quienes estén facilitando la actividad pueden introducir conceptos como:

- el acceso a celulares según nuestras identidades de género
- cómo manifestamos muchas de nuestras identidades a través de nuestros celulares
- los posibles riesgos de usar celulares según nuestras identidades de género

Recomendamos esta actividad como punto de partida para un taller más largo sobre seguridad celular/móvil.

Esta actividad tiene 3 etapas:

- Compartir en parejas
- Puesta en común
- Síntesis de elementos comunes (dirigida por facilitadoras)

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género.

¿Para quién es esta actividad?

Para cualquier persona que usa un celular.

Tiempo requerido

Aproximadamente **30 minutos.**

Materiales requeridos

- pizarrón o papel grande (en caso de anotar las aportaciones del grupo)

Mecánica

Nuestros celulares son espacios de interacciones íntimas. Conectamos con seres queridos, amantes, amistades; compartimos llamadas, mensajes, imágenes, videos, conversaciones e imágenes privadas. Por ello, sabemos que nuestros celulares son objetos personales íntimos; pero también forman parte de un contexto general donde estos objetos están vinculados a proveedores de telefonía, regulados por políticas gubernamentales, sujetos a la expropiación y a la vigilancia sin nuestro consentimiento.

El acceso a celulares varía según nuestro género. El hecho que mujeres utilicen celulares implica desafiar al poder - hay personas que pueden ejercer violencia contra mujeres por usar celulares; mientras que, en otros contextos, las mujeres usan celulares para reportar casos de abuso.

Discusión en parejas - 15 minutos

Las participantes se dividen en parejas y comparten sus experiencias. Toman turnos en hablar, mientras la otra escucha. Intercambian roles. Cada persona tiene entre 5 y 7 minutos para hablar.

Preguntas

Las preguntas se anotarán en un lugar visible para todas las participantes o en trozo de papel a repartir entre las parejas.

- **¿Cómo utilizas tu celular? ¿Cuándo lo utilizas?** *¿Cómo cambia según sean amistades, familiares, compañeras, personas desconocidas?*
- **¿Y para tu activismo y organización política?**
- **¿Cuándo sientes inseguridad a la hora de usar tu celular?** ¿Qué haces en estas situaciones? *Anima a las participantes a centrarse en casos de vigilancia por parte de compañerxs de casa, parejas, familiares, policía...*

Puesta en común - 15 minutos

Las facilitadoras toman nota y sintetizan los puntos. ¿Hay alguna estrategia o situación en particular que quieras abordar?

image-1605451879726.png
Image not found or type unknown

Crear una línea de tiempo sobre nuestros celulares [actividad inicial]

activ-iniciales_200px-con-texto.png
Image not found or type unknown

Actividad introductoria para compartir experiencias personales sobre celulares a través de mover el cuerpo y narrar historias. Hablaremos y escucharemos sobre las diferentes actitudes y conductas que tenemos con nuestros celulares y compartiremos las maneras significativas y personales en que utilizamos y accedemos a estos dispositivos.

Al igual que la actividad Muro de mujeres: Las primeras veces en internet, compartiremos nuestras experiencias sobre tecnologías celulares y las relacionaremos entre sí para plasmar en una línea de tiempo. A través de esta actividad, nos familiarizaremos con las experiencias y relaciones que tenemos con nuestros celulares.

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género.

¿Para quién es esta actividad?

Para cualquier persona que usa un celular.

Tiempo requerido

Aproximadamente 30 minutos.

Materiales requeridos

Etiquetas para marcar segmentos de 5 años (de 1990 a la actualidad) en la línea de tiempo. Pueden anotar las fechas en papeles y colocarlas sobre el suelo (ej. 1990, 1995, 2000... etc).

Mecánica

Prepara una línea de tiempo en el espacio. Las participantes se colocan a lo largo de la línea de tiempo en fechas determinadas. Según cada pregunta, se mueven a alguna fecha de la línea de tiempo. Antes de empezar, indica la fecha de inicio y fin de la línea de tiempo. Si muchas personas se colocan en una misma fecha como respuesta a alguna pregunta, sondea un poco.

Según el tamaño del grupo y cuánto tiempo tienen, puedes hacer 2 o más preguntas.

Pide a 1 ó 2 participantes compartir alguna aportación sobre las preguntas. Por ejemplo, "¿cómo te sentiste?".

Preguntas

- **¿Cuándo fue la primera vez que tuviste un celular?** ¿Cómo era? ¿Lo compartías? ¿Qué edad tenías? ¿Para qué lo utilizabas?
- **¿Cuándo tuviste tu primer teléfono inteligente?** ¿Qué significó para ti? ¿Lo compartías? ¿Cuál es tu aplicativo favorito? ¿Por qué?
- **¿Cuándo fue la primera vez que te conectaste a internet a través de tu celular?** ¿Qué página web viste primero? ¿Por qué?
- **¿Cuándo fue la primera vez que "jubilaste"(desechaste) un celular?** ¿Qué guardaste (por ej. imágenes, historiales de chat, hardware)? ¿Por qué?

Puesta en común - 5 a 10 minutos

Compartan comentarios y observaciones. Las facilitadoras hacen un resumen y relacionan las aportaciones con temas de intimidad y acceso según nuestras identidades de género - toma en cuenta lo que se ha compartido sobre las distintas actitudes y usos que le damos a los celulares.

> **Indicador de interseccionalidad:** ¿Cómo varía el acceso y privacidad celular según el género, la sexualidad, la raza y la clase?

image-1605451259399.png
Image not found or type unknown

Senderismo en el Himalaya [actividad inicial]

activ-iniciales_200px-con-texto.png
Image not found or type unknown

Actividad inicial para sensibilizar en temas de seguridad celular y evaluar (tanto participantes como facilitadoras) los tipos de medidas de seguridad que las participantes están tomando y qué vulnerabilidades deberían abordar primero. Recomendamos hacer esta actividad al inicio del taller sobre seguridad celular.

Objetivos de aprendizaje

- adquirir y poner en práctica estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas.

¿Para quién es esta actividad?

Para cualquier persona que usa un celular.

Tiempo requerido

Aproximadamente **30 minutos**.

Mecánica

Nos ponemos de pie, hombro a hombro. Respondemos a preguntas sobre seguridad celular. Si la respuesta es "sí", damos un paso hacia adelante; si es un "no", damos un paso para atrás.

Ejemplos de preguntas

- ¿Usas bloqueo de pantalla?

- ¿Bloqueas el acceso a tus aplicativos?
- ¿Tienes una tarjeta SIM sin registrar?
- ¿Tienes una cuenta de correo alternativa (no la que siempre usas) asociada a tu celular?
- ¿Tienes activada alguna función de acceso remoto (por ej, Buscar mi iPhone) en tu celular?
- ¿Tienes habilitados los servicios de ubicación en tu celular?
- ¿Tienes un respaldo de tu celular (fotos, mensajes, videos, etc)?
- ¿Utilizas algún anti-virus en tu celular?

Puesta en común - 5 a 10 minutos

Comparte comentarios y observaciones. Las personas facilitando hacen un resumen y relacionan las aportaciones de las participantes con la agenda del día o la serie de sesiones que se van a realizar conjuntamente.

image-1605452256072.png
Image not found or type unknown

Celulares recolectores [actividad inicial]

activ-iniciales_200px-con-texto.png
Image not found or type unknown

Actividad inicial para compartir las diferentes sensaciones que generan nuestros celulares, incluyendo cuando otras personas acceden a nuestros dispositivos y contenidos.

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género;
- entender la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como para la esfera pública y para nuestras redes activistas.

¿Para quién es esta actividad?

Esta actividad funciona particularmente bien porque la mayoría de las participantes pueden identificarse con estas experiencias y situaciones. Recomendamos este ejercicio particularmente si a alguna participante le han expropiado o tomado su celular y quiere compartir los impactos que ha tenido para ella y cuáles han sido sus respuestas emocionales.

> **Indicación sobre cuidados:** recomendamos llevar esta sesión con **mucho cuidado**. Asegúrate de obtener el **consentimiento** claro y explícito de todas las participantes. Esta actividad funciona mejor cuando ya existe un **nivel profundo de confianza** en el grupo.

> **Indicación sobre rutas de aprendizaje:** esta actividad inicial ayuda a preparar discusiones y actividades más prácticas a la hora de abordar situaciones de alto riesgo donde pueden expropiar nuestros dispositivos o los podemos perder.

Tiempo requerido

Aproximadamente **30 minutos.**

Mecánica

Actividad: Recolectar los celulares de las participantes + conversación - 15 minutos

Recolecta los celulares de todas las participantes al inicio de la actividad: pide su consentimiento claro y explícito, pero no expliques por qué los estás tomando.

Discusión

Pregunta:

- ¿Cómo te sientes ahora que no tienes tu celular en tus manos?
- ¿Cuáles son las sensaciones más inmediatas que te vienen?

Actividad: Regresar los celulares + puesta en común - 5 a 10 minutos

Devuelve los celulares a las participantes.

Discusión

Pregunta:

- ¿Cómo te sentiste al entregar tu teléfono? ¿Por qué?
- ¿Y ahora cómo te sientes al recibirlo de vuelta? ¿Por qué?
- ¿Hay situaciones en las que toman tu celular? ¿Quién(es) lo toman? ¿En qué contextos? ¿Por qué?
- ¿Por qué es importante para ti tu celular? ¿A qué te da acceso? *Anima a las participantes a ser específicas sobre cómo se relacionan con sus celulares: ¿a qué logran acceder? ¿qué importancia tiene en sus vidas?*

image-1605451879726.png
Image not found or type unknown

Mi celular y yo [actividad inicial]

activ-iniciales_200px-con-texto.png
Image not found or type unknown

Esta conversación inicial esta diseñada para reflexionar sobre cómo usamos nuestros celulares de maneras íntimas, además de compartir prácticas e inquietudes sobre la vigilancia y la privacidad.

Recomendamos realizar esta actividad al inicio de un taller de seguridad celular.

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género.

¿Para quién es esta actividad?

Para cualquier persona que usa un celular.

Tiempo requerido

Aproximadamente **30 minutos**.

Materiales requeridos

- pizarrón o papel grande (en caso de anotar las aportaciones del grupo)

Mecánica

Discusión en parejas - 15 minutos

Las participantes se dividen en parejas y comparten sus experiencias. Toman turnos en hablar, mientras la otra escucha. Intercambian roles. Cada persona tiene entre 5 y 7 minutos para hablar.

Pregunta 1: ¿cuáles son las cosas más personales y privadas que haces con tu celular?

Pregunta 2: ¿qué tipos de cuidados tomas en estas interacciones?

Las personas que están facilitando pueden dar uno o varios ejemplos antes de empezar. Por ejemplo, algo personal o privado que hago en mi celular es tomar fotos de mí desnuda como autoexploración placentera y forma de expresarme. También hago sexting y mantengo conversaciones íntimas con otras personas.

> **Indicador de interseccionalidad:** ¿Cómo varía el acceso y privacidad celular según el género, la sexualidad, la raza, la clase y las capacidades que tiene mi cuerpo?

Puesta en común - 15 minutos

Compartan observaciones y sensaciones de la actividad. Las facilitadoras toman nota y hacen resumen de los puntos. Subrayan y dibujan los puntos en común que van saliendo. ¿Cómo usamos nuestros celulares y en qué medida son aspectos íntimos de nuestras vidas? ¿Cómo se relacionan nuestras identidades de género con el acceso que tenemos a nuestros dispositivos y nuestra privacidad? ¿Qué cuidados tomamos en nuestras interacciones íntimas y en cómo gestionamos los archivos en nuestros celulares? ¿Cuáles son nuestras inquietudes y cómo se relacionan con la privacidad, el género, la sexualidad, la raza, la clase, las capacidades de nuestro cuerpo, nuestra edad, etc?

image_1605451879726.png
Image not found or type unknown

El poder del celular - dispositivo, cuenta, servicio, estado, política [actividad de profundización]

activ-profund_200px-con-texto.png
Image not found or type unknown

Se trata de una **actividad de mapeo colaborativo.** A través de una conversación guiada, el grupo discute cómo se relacionan sus dispositivos celulares, cuentas de diferentes servicios, proveedores de telefonía celular y cómo las políticas corporativas y gubernamentales entran en juego.

Recomendamos realizar esta actividad al inicio del taller de seguridad celular.

Objetivos de aprendizaje

- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como para la esfera pública y nuestras redes activistas;
- obtener una noción de los conceptos básicos sobre cómo funciona la comunicación celular y los riesgos implicados.

¿Para quién es esta actividad?

Para cualquier persona que usa un celular.

Tiempo requerido

Aproximadamente **45 minutos** Si quieres realizar una versión corta de esta actividad, puedes hacer menos preguntas y mostrar una presentación con diapositivas o un ejemplo de mapeo en vez de crear uno en la actividad con las participantes.

Materiales requeridos

- Papeles grandes o rotafolios
- Marcadores

Mecánica

Haz preguntas y mapea las respuestas sobre papel. El objetivo es visualizar las maneras en que nos relacionamos con nuestros celulares. Se discutirá sobre el poder, control y agencia de los celulares y cómo se relaciona con **nuestros dispositivos**, **los diferentes servicios donde estamos registradas**, **los proveedores de telefonía celular** y **las políticas de corporaciones y gobiernos.**

Sugerencias para preparar esta actividad

- Investiga sobre los proveedores locales de telefonía celular;
- Investiga las relaciones entre estos proveedores locales y el Estado. Por ejemplo, ¿se tratan de empresas del Estado?
- Prepara algunos ejemplos locales sobre las maneras en que las activistas feministas usan sus celulares y cómo esto se relaciona con el poder; también sobre cómo la corporaciones y/o el Estado reacciona/regula estos temas;

Dibuja el mapeo en grande en un espacio visible para que se pueda ver mientras se van respondiendo a las preguntas.

- indica los puntos en que las participantes hablan de elecciones y decisiones que tomaron. Por ejemplo, cómo escogieron su celular, proveedor de telefonía y plan de datos; cómo decidieron a quién dar acceso; quién tiene acceso a sus planes de celular...

Ejemplo de mapa. Haz clic para ver más en grande.

PoderCelularesEsquema.png
Image not found or type unknown

Preguntas

- **Sobre los dispositivos**: ¿qué tipo de celular utilizas? ¿Cómo lo conseguiste? ¿Lo compartes? ¿Cómo? ¿Con quiénes?
- **Sobre tu servicio celular**: ¿cómo elegiste tu proveedor telefónico? ¿Compartes tu plan o contrato? ¿Administras tu propio plan/contrato? En caso negativo, ¿quién? ¿Escogiste tu plan/contrato? ¿Cómo?

Pregunta/discute

La relación que tenemos con los proveedores de telefonía celular. ¿Firmaste un término de servicios? ¿Qué condiciones aceptaste cuando firmaste tu contrato? ¿A qué se comprometió tu proveedor?

Nota para facilitadoras: si conoces asuntos particulares sobre proveedores locales, intenta buscar y compartir ejemplos de términos de servicios y/o casos prácticos en los que personas/clientes han discutido temas de seguridad con proveedores de telefonía celular.

Pregunta/discute

La relación entre proveedores de telefonía celular y el Estado. ¿Se tratan de empresas del Estado? ¿Son empresas internacionales, locales o regionales?

Nota para facilitadoras: quizás quieras investigar de antemano sobre regulaciones estatales o cómo han influenciado estos proveedores a nivel local/regional/nacional. ¿Existen casos de cortes recientes del servicio de telefonía por parte del Estado? ¿Conocen casos donde cortaron el servicio de alguien en particular? ¿La policía u otras fuerzas de seguridad confiscan dispositivos?

Materiales complementarios

Casos prácticos: *en la medida que el Programa de Mujeres vaya utilizando esta actividad, agrega enlaces a casos prácticos relevantes aquí.*

- https://www.animalpolitico.com/elsabueso/padron-de-usuarios-telefonia-enciende-alertas-sobre-tus-datos-biometricos/
- Artículo de Wikipedia sobre los principales proveedores en Latinoamérica https://es.wikipedia.org/wiki/Anexo:Empresas_de_telefon%C3%ADa_m%C3%B3vil_de_Latinoam%C3%A9rica
- 101: Registro de tarjetas SIM (en inglés) : https://privacyinternational.org/explainer/2654/101-sim-card-registration

image_1605451259399.png
Image not found or type unknown

¿Qué es un celular? ¿Cómo funciona la comunicación telefónica? [actividad de profundización]

activ-profund_200px-con-texto.png
Image not found or type unknown

El objetivo de esta actividad es profundizar en cómo funciona la comunicación telefónica para poder evaluar y planear los potenciales riesgos. Se recomienda, en cualquier taller sobre celulares, verificar si las participantes cuentan con esta información de base y, en caso contrario, incluir este ejercicio. Se trata de un punto de partida fundamental para poder evaluar riesgos técnicos relacionados con los celulares.

Esta actividad tiene 2 etapas:

- Sesión práctica: desmontar celulares
- Introducción: los datos generados en la comunicación telefónica y consideraciones sobre riesgos.

Objetivos de aprendizaje

- obtener una noción de los conceptos básicos de cómo funciona la comunicación telefónica y de los posibles impactos implicados.

¿Para quién es esta actividad?

Esta actividad es para cualquier persona que participa en un taller sobre celulares.

Tiempo requerido

Aproximadamente **45 minutos.**

Materiales requeridos

- algunos celulares para desmontar e investigar
- un pizarrón, diapositivas o material impreso con apuntes de los contenido

Mecánica

Menciona o discute más en profundidad (según el tiempo disponible) que en esta sesión estarán abordando tecnologías móviles - considerando que son dispositivos fácilmente portables (en nuestras manos o en nuestros bolsillos) y nos permiten comunicarnos (a través de llamadas de voz, sms, navegación web). Esta sesión también aplica a tablets.

Adentro de nuestros celulares - 5 minutos

¡Ahora toca desmontar nuestros teléfonos! Los celulares son como computadoras pequeñas. Ubiquemos las diferentes partes de nuestros dispositivos:

- Las partes que escuchan y proyectan sonido: micrófonos, altavoces/bocinas
- Las partes que ven y muestran visuales: cámaras, pantallas
- Las partes que envían y reciben información de otras fuentes: GPS, antena, WiFi
- Partes de la computadora, hardware: batería, circuitos
- Memoria: tarjeta SD, otras memorias integradas en las ranuras
- SIM del teléfono

Identidad de la tarjeta SIM + identidad del teléfono - 5 minutos

Tu teléfono se compone de todas estas piezas y tiene varios rasgos identificativos; aparte de la marca, modelo y sistema operativo, también tiene dos nombres: un identificador de dispositivo y un identificador de tarjeta SIM. Es importante conocerlos porque nuestros celulares comunican esta información hacia fuera a menudo, especialmente el identificador SIM (IMSI) y nos pueden identificar a través de estas características.

- **IMEI**: nombre del dispositivo.

Identidad internacional de equipo móvil (IMEI): https://es.wikipedia.org/wiki/IMEI

- **IMSI**: nombre de tu tarjeta SIM

Identidad Internacional de Suscripción al Servicio Móvil (IMSI): https://es.wikipedia.org/wiki/IMSI

Nuestros celulares comunican - 35 minutos

Utilizamos nuestros teléfonos para comunicarnos con personas: SMS, mensajes, plataformas de redes sociales, aplicativos, llamadas. Nuestros celulares también comparten información sobre nuestros teléfonos y nosotras mismas - no sólo nuestros mensajes, pero también metadatos como nuestra ubicación, etc. Estos metadatos pueden vincularse a más información sobre nosotras como nuestras redes sociales, nuestras redes activistas/organizativas y nuestros lugares de trabajo.

Es relevante tomar esto en cuenta, sobre todo para entender que nuestros celulares pueden ser dispositivos de rastreo en tiempo real y almacenar un registro de nuestras actividades.

1. A nuestros celulares les gusta hablar

Nuestros teléfonos intentan hablar con diferentes tipos de redes a su alrededor para anunciar que está cerca, para ver si se puede conectar a alguna red y para averiguar si alguien se quiere conectar al dispositivo.

Empresas de telefonía

Hay torres y antenas con las que se comunica tu celular. Cada antena tiene un cierto alcance. Tu celular se comunica con cualquier torre que queda cerca y comparte, **como mínimo, tu IMSI** (para informar qué empresa de teléfono estás utilizando) y tu número (para que puedas recibir mensajes, llamadas y otros tipo de comunicación en tu dispositivo). Cada vez que estás cerca de una torre es como si estuvieras colocando un marcador indicando dónde estás en cada momento y qué estás haciendo según el uso que das a tu celular.

GPS

Cuando está activado, tu celular se comunica con satélites GPS, también informando dónde estás en cada momento.

Wifi

Si está habilitado, en la medida que pases cerca de alguna red WiFi, tu dispositivo puede intentar conectarse a ella y dejar un rastro de que estuviste ahí (tanto en la red como en tu celular).

Bluetooth/NFC

Cuando está activado, otros dispositivos que usan Bluetooth y NFC pueden comunicarse con tu dispositivo, intentar conectarse y compartir archivos.

Discusión grupal: ¿qué funciones necesitas activar en cada momento? ¿Tener registros de dónde has estado implica un riesgo para ti?

2. A ti te gusta hablar

Utilizamos nuestros celulares para comunicarnos. Los diferentes tipos de comunicación aparecen de manera diferente:

SMS

Mensajes de texto y metadatos - aparecen en texto plano a la hora de enviarse y almacenarse en tu dispositivo y en la infraestructura de las empresas de telefonía. Una analogía útil es pensar que los SMS son como cartas postales. Si alguien la intercepta, puede ver todo su contenido y sus metadatos (por ej, quien lo envía y lo recibe, fecha).

MMS

Contenidos multimedia y metadatos - si alguien intenta interceptar tu comunicación, podrá verla o no según los mensajes estén cifrados o no. Al enviar estos mensajes MMS, tu proveedor de telefonía celular y los proveedores de las personas con las que te estás comunicando guardan un registro de los contenidos y metadatos (quién envía/recibe, fecha).

Llamadas

Contenido de llamadas y metadatos - supuestamente las llamadas deberían estar cifradas, pero tu proveedor de telefonía y los proveedores de las personas con las que te estás comunicando almacenan metadatos sobre la llamada (por ej, quien envía/recibe, fecha). Si alguien accede a estas empresas de telefonía, pueden llegar a esuchar y grabar llamadas.

Para más información sobre Apps y Mensajería, véase:

- Conversación, intro + sesion práctica: Escoger apps celulares

Comentario sobre vigilancia estatal: varía según el país. En algunos lugares, los gobiernos tienen acceso a cualquer dato gestionado por las empresas de telefonía -- en estos casos, considera que todos los contenidos y metadatos que se envían y guardan en servicios sin cifrar pueden ser accedidos por gobiernos, tanto en tiempo real como a posteriori durante una investigación.

Tu mejor mecanismo de defensa contra la vigilancia es usar cifrado de extremo a extremo.

3. Un teléfono es una computadora pequeña

Bug de software - un teléfono es una computadora y puede estar infectada de malware igual que una compu de escritorio o laptop. Tanto personas como gobiernos utilizan este tipo de software para meterse en los dispositivos de otras personas. El malware suele utilizar partes del teléfono para funcionar como un "bug" o dispositivo de rastreo para escuchar a través del micrófono o datos de ubicación.

4. La nube es un archivero

Nuestros celulares también acceden a datos que están en la "nube", es decir, en "internet", o más bien, en un dispositivo que está conectado a internet. Tus apps pueden estar accediendo a datos que están en la nube y no en tu dispositivo.

Consideraciones: ¿los datos enviados entre mi celular y mis servicios están cifrados? ¿están cifrados cuando están almacenados? ¿Conozco casos en los que personas o grupos adversarios pueden tener acceso a esta información? ¿Cuándo? ¿Cómo?

Nota de facilitación: mientras hablas, las participantes pueden hacer preguntas sobre partes de sus celulares o los riesgos asociados a los métodos de comunicación que compartes. Toma tiempo en responder a las pregutnas. Si puedes, toma nota en un pizarrón o un papel grande sobre los temas que van saliendo, incluyendo los que no se van a poder cubrir en el taller, pero que puedas dar seguimiento después para mandar más información.

Materiales complementarios

- Materiales sobre celulares en el portal ciberfeminista Ciberseguras: https://ciberseguras.org/?s=celular
- Cibermujeres Módulo Celulares más seguros https://cyber-women.com/es/celulares-m%C3%A1s-seguros/
- 7 maneras de encontrar tu número IMEI o MEID en tu celular (inglés): http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- Identidad internacional de equipo móvil (IMEI): https://es.wikipedia.org/wiki/IMEI
- Identidad Internacional de Suscripción al Servicio Móvil (IMSI): https://es.wikipedia.org/wiki/IMSI

El sitio de Yo y Mi Sombra de Tactical Tech contiene muchas guías sobre tecnología celular.

- Materiales descargables de Yo y Mi Sombra: https://myshadow.org/materials
- Sitio de Yo y mi Sombra: https://myshadow.org/es

image-1605452256072.png
Image not found or type unknown

Debate: Documentar casos de violencia [actividad de profundización]

activ-profund_200px-con-texto.png
Image not found or type unknown

Actividad de profundización para facilitar una conversación y compartir ejemplos sobre el uso de celulares para documentar casos de violencia y debatir posibles impactos como perpetuar indirectamente o directamente la violencia. Este ejercicio se puede utilizar para hablar específicamente de casos donde ciertos medios y canales han tomado documentación de medios activistas y han tergiversado la información para perpetuar la violencia.

Objetivos de aprendizaje

- entender la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas.

¿Para quién es esta actividad?

Grupos que están o planean documentar casos de violencia con sus celulares

Tiempo requerido

Aproximadamente **60 minutos.**

Materiales requeridos

- Información impresa sobre casos prácticos o proyectar esta información en la pared.

Mecánica

Plenaria - 10 minutos

Compartimos las maneras en que usamos nuestros celulares para documentar casos de violencia.

> **Consideraciones sobre cuidados:** pueden compartirse incidentes que son disparadores psicológicos. A la hora de invitar a las participantes a compartir sus experiencias, toma en cuenta los acuerdos que se han tomado previamente. Puedes avisar al inicio de la sesión que se va a hablar de violencia e invitar a cada una y al grupo a buscar qué necesitan para cuidarse y no sobrepasar sus capacidades y límites.

Preguntas:

- ¿Cuáles son algunos ejemplos de generar y compartir documentación sobre casos de violencia que han tenido un impacto positivo en tu trabajo, activismo y tus comunidades?
- ¿Qué estabas documentando?
- ¿Qué pasó?
- ¿Cómo la compartiste?
- ¿Con quiénes compartiste y cómo escogiste a estas personas?
- ¿Cuáles fueron las respuestas y reacciones?

Las personas que están facilitando pueden preparar ejemplos recientes y locales de grupos activistas que usan sus celulares para documentar casos de violencia. Estos ejemplos pueden, entre otros temas, incluir: documentar violencia ejercida por el Estado, re-enviar/re-publicar videos o transmitir en vivo actos violentos, y las implicaciones de tener este tipo de contenidos en tus dispositivos.

Incluimos más ejemplos en la sección de "Materiales complementarios” más adelante. Puedes utilizarlos para tus sesiones o utilizar casos más actuales y apropiados para tu grupo.

Grupos pequeños - casos prácticos - 20 minutos

Entrega a cada grupo un caso práctico para leer y discutir. Puedes encontrar ejemplos de casos prácticos en la sección de “Materiales complementarios”. Escoge algún caso (situaciones hipotéticas, publicaciones de blog, artículos de noticias) y modíficalo a tu medida o escribe tus propios ejemplos más relevantes a los contextos de las participantes.

- ¿Cuál es el ejemplo?
- ¿Cuáles son los argumentos/razones por las que estás usando un celular para documentar este caso de violencia o no hacerlo?
- ¿De qué maneras puedes reducir los impactos negativos de este tipo de documentación?

Escenarios

Ejemplos de cómo escribir tus propios relatos para los talleres que vayas a facilitar. Crear varias situaciones ayuda a abordar diferentes temas en el grupo. Los ejemplos incluidos están diseñados para provocar conversaciones sobre la documentación, el activismo, el consentimiento y la perpetuación de la violencia.

Escenario 1

Tu comunidad está enfrentando situaciones de violencia y acoso. Junto con otras personas, se han organizando para documentar casos y compartirlos en plataformas de redes sociales con subtítulos y texto para explicar los incidentes y el contexto actual de violencia. Vinculas esta documentación a materiales que incluyen una lista de demandas por parte de tu comunidad y materiales de apoyo para personas que viven situaciones de violencia similares.

Escenario 2

Observas una situación de violencia en la calle y empiezas a transmitirla en vivo desde tu canal de red social donde tienes miles de seguidoras. No conoces las personas que estás grabando ni el contexto de lo que está pasando.

Escenario 3

Tu comunidad y tú han estado transmitiendo en vivo protestas para visibilizar su importancia y para documentar incidentes de violencia que suceden en estos eventos. Te enteras que la policía local y grupos adversarios están utilizando este material para fichar a personas y para hacer montajes tergiversantes que después publican en redes sociales.

En plenaria - puesta en común - 30 minutos

La puesta en común es una oportunidad para que cada grupo comparta su caso práctico y que se discutan entre todas los desafíos actuales sobre documentar casos de violencia y compartirla en línea. Deja tiempo para que los grupos puedan compartir e interactuar.

- ¿Cuál es el ejemplo?
- ¿Qué argumentos/razones surgieron para no usar celulares para documentar determinados casos de violencia?

- ¿Qué temas suscitan para las demás personas? ¿Coinciden con tus inquietudes? ¿Cómo estás reflexionando sobre estos temas? ¿Qué estrategias estás siguiendo para lograr el mejor impacto posible y reducir la probabilidad de los impactos negativos?

Dibujen los temas comunes conforme vayan saliendo en la discusión. ¿Cuáles son los preocupaciones principales de las participantes en el ámbito de su trabajo? - algunos temas que pueden surgir y que puedes abordar en las sesiones pueden incluir aspectos prácticos: por ej, cómo documentar, almacenar y compartir información; cómo verificar medios y noticias falsas; cómo se usan contenidos para incitar a la violencia y qué formas de compartir documentación pueden perpetuar más violencia y daño.

Materiales complementarios

Casos prácticos y publicaciones en blogs sobre los impactos de documentar casos de violencia

Ejemplos de cómo las personas están usando celulares para organizarse políticamente - sugerimos recopilar ejemplos actuales y relevantes sobre cómo activistas usan celulares. También puedes pedir ejemplos a las participantes y organizadoras.

- Trabajadoras migrantes documentando casos de abuso
  - OFW-SOS del Centro de Defensa a las Migrantes (Centre for Migrant Advocacy)

Caso práctico sobre transmisión en vivo de acciones violentas: los desafíos éticos de transmisión en vivo | Irie Crenshaw y Justin Pehoski (Live streaming violent acts Case Study: The Ethical Challenges of Live Internet Broadcasting, Irie Crenshaw and Justin Pehoski)
https://mediaengagement.org/research/matters-of-facebook-live-or-death/

- Australia

El mundo está volviéndose en contra de la transmisión en vivo como consecuencia del tiroteo en Christchurch. Australia dirige la demanda contra videos explícitos sin filtrar | Casey Newton, 4 de Abril, 2019 (The world is turning against live streaming, In the aftermath of the Christchurch shooting, Australia is leading the charge against raw, unfiltered video, Casey Newton, April 4, 2019) https://www.theverge.com/interface/2019/4/4/18294951/australia-live-streaming-law-facebook-twitter-periscope

- Ejemplos en Brasil

"Informe de Brasil: si te mata la policia, ¿eres culpable por defecto al menos que haya una prueba en video?" de Priscila Neri (Dispatch from Brazil: If killed by police, guilty by default unless there's video?, Priscila Neri) https://lab.witness.org/dispatch-from-brazil-if-killed-by-police-guilty-by-default-unless-theres-video/

- Whatsapp y violencia en la India

"WhatsApp limitará drásticamente el re-envío de mensajes en todo el mundo para detener la propagación de noticias falsas a raíz de los casos de violencia en la India y Myanmar" | Kurt Wagner, 19 de Julio, 2018 (WhatsApp will drastically limit forwarding across the globe to stop the spread of fake news, following violence in India and Myanmar, Kurt Wagner Jul 19, 2018)
https://www.vox.com/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar

- Ejemplos en los Estados Unidos

Momento de video viral de C-SPAN | Integrantes del congreso de Estados Unidos transmiten en vivo una protesta para exigir una legislación sobre regulación de armas, Hadas Gold, 22 de Junio de 2016 (C-SPAN's viral video moment, Hadas Gold, 6/22/2016)
https://www.politico.com/story/2016/06/cspan-house-sitin-democrats-224696 US Congress members livestream a sit-in demanding a vote on gun-control legislation.

image-1605451879726.png
Image not found or type unknown

Planear nuestra comunicación celular para organizarnos y actuar [actividad táctica]

activ-tacticas_200px-con-texto.png
Image not found or type unknown

A continuación, compartimos unas consideraciones orientativas para grupos que están organizando y/o participando en acciones políticas y usan apps de mensajería/chat.

Puedes usar esta guía para facilitar conversaciones que apoyen a los grupos activistas a considerar los tipos de comunicación que utilizan y diseñar colectivamente protocolos más seguros sobre la gestión y la comunicación en el grupo.

Esta actividad tiene 3 etapas:

- Mapear formas de comunicación y evaluación de riesgos
- Planear: grupos y escenarios.
- Instalar apps (opcional)
- Implementar (opcional)

Si el grupo no ha optado por un aplicativo de chat aún, puede realizar la actividad Conversación, intro + sesiones prácticas: Escoger apps para el celular.

Objetivos de aprendizaje

- adquirir y poner en práctica estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Para participantes con diferentes niveles de experiencia utilizando celulares.

Si va a delegar la responsabilidad de administrar grupos de chat a algunas personas del grupo, planea implementar un diseño y protocolo en el taller.

Tiempo requerido

Aproximadamente **60 minutos** para mapear/visualizar y diseñar y hasta **3 horas** si vas a instalar aplicativos de chat, mapear/visualizar, diseñar e implementar.

Materiales requeridos

- Papel para dibujar y visualizar/mapear.

Mecánica

Mapear formas de comunicación y evaluación de riesgos

Consideraciones: Privacidad

Toma en cuenta que podemos comunicar diferentes tipos de mensajes por signal y algunos mensajes pueden ser más públicos que otros. Mapea los diferentes tipos de comunicación y diseña grupos acorde a vuestras consideraciones de privacidad.

¿Qué tipos de comunicación estableces y qué consideraciones tomas en cada caso?

Puede haber diferentes clases de información -- por ejemplo, información confidencial entre dos personas o sólo debe conocer una persona y documentar sin compartir.

QUIÉN	EJEMPLOS DE TIPO DE COMUNICACIÓN
1 entre un grupo pequeño de personas que se conocen	*ubicación de responsables de la organización/actividad*

2 importante que colaboradoras/voluntarias conozcan o para grupos pequeños coordinarse entre sí	*cambios en la ubicación de la multitud*
3 puede compartirse abiertamente	*hora de inicio de manifestación, grupos que apoyan la acción públicamente*

PLANEAR: Grupos y escenarios

Crea grupos según los diferentes tipos de comunicación.

Sugerimos basarse en las preguntas a continuación. Incluimos recomendaciones para gestionar grupos de comunicación y ejemplos de situaciones para cada tipo. Plantea qué funciona para tu grupo y lo que no, qué cambios puedes realizar.

Membresía/pertenencia

- QUIÉN - ¿quién puede formar parte de este grupo?
- CÓMO - ¿cómo se une alguien al grupo? ¿Cuál es el procedimiento? ¿Necesita haber algun tipo de revisión, presentación o registro?
- CONFIRMACIÓN Y NOTIFICACIÓN - ¿Cómo se avisa al grupo cuando alguien entra? ¿Qué relevancia tiene hacerlo?
- SEGUIR ACUERDOS - ¿Qué se hace si alguien entra al grupo sin seguir el procedimiento?
- INFORMACIÓN PERSONAL - ¿qué tipo de servicio de mensajería/chat están utilizando? ¿las participantes del grupo pueden ver los números de todas? En caso de que alguien quiera/necesite mantener su número privado, hay que tomar esto en cuenta a la hora de formar parte de grupos más grandes.

Saber con quién estás hablando - VERIFICACIÓN

Para cualquier tipo de comunicación ¿cómo verificas con quién estás hablando?

- CARA-A-CARA - ¿es necesario conocerse cara a cara antes de formar parte del grupo? ¿puede entrar sin este contacto si tiene el aval de alguna integrante del grupo?
- SEGURIDAD- VERIFICA que tus mensajes están llegando a los dispositivos correctos. Si estás usando Signal o Whatsapp, VERIFICA LOS NÚMEROS DE SEGURIDAD.
- PALABRAS DE SEGURIDAD - VERIFICA que tus llamadas están llegando a donde tienen que llegar. Si estás usando Signal para llamadas, UTILIZA PALABRAS CLAVES DE SEGURIDAD. Si utilizas otro aplicativo, ¿quieres seguir algún protocolo para verificar, al inicio de la llamada, que la persona con la que te estás comunicando es la cierta y puedes hablar libremente?

Seguridad de mensajes - configuraciones

Discutan, basándose en el nivel de confidencialidad de la información que se está comunicando, ¿qué acuerdos quieren pactar sobre la configuración de mensajes?

- BORRAR Mensajes - ¿Cuánto tiempo se mantienen los historiales de chat en los dispositivos?
- AUTODESTRUCCIÓN de mensajes - En Signal, puedes programar la desaparición de mensajes automáticamente. ¿Quieres utilizar esta funcionalidad? ¿Cómo y por qué?
- ESCONDE mensajes en tu pantalla de inicio - configura tus apps de chat para que no muestren mensajes en la pantalla. De esta manera, en caso de perder el control de tu dispositivo (lo pierdes, te lo roban o confiscan, etc.), no pueden ver tus mensajes.
- CÓDIGOS - Para información muy confidencial, sugerimos establecer palabras código antes de planear y actuar. Por ejemplo, decir "¡Listxs para tomar un café!" en vez de "¡Listxs para la marcha!".

Planilla para organizar grupos de comunicación

1. Grupos pequeños para información confidencial [se siguen protocolos estrictos de verificación]

> Consideraciones/riesgos: el riesgo de personas desconocidas o que no has conocido en persona entrando en el grupo implica que tendrán acceso a información que no quieres que se vuelva pública y potencialmente podrán compartirla.

- Si tienes información confidencial que debe ser compartido sólo entre personas conocidas.
- Grupo muy pequeño (8 personas o menos). Todo el mundo se conoce y se han visto presencialmente;
- Sólo agregan participantes cuando están cara a cara.
- VERIFICAR identidad (en SIgnal, verificar números de seguridad) en persona;
- Si el número de seguridad de alguien cambia, hace falta verificarla de nuevo.
- No compartes más de lo que necesites. Evita tomar riesgos innecesarios.
- ELIMINAR

2. Nodos - grupos pequeños

> Consideraciones/riesgos: que personas se unan al grupo y envíen información que no es útil o intencionadamente incorrecta.

- Riesgo de "spamming": interferir en el grupo y hacerlo inservible.
- Entre 2-20 personas. Evitar temas que no son relevantes para el grupo.
- Un grupo grande puede componerse de múltiples nodos con el fin de mantener el enfoque y gestión.

- Los nodos se conectan entre sí para asegurar un flujo de información.
- Puede haber personas de enlace en cada nodo para pasar información al resto del grupo;

3. Grupo abierto / información pública

La información en este grupo será pública y en tiempo real.

A diferencia del resto de los grupos dnde la información se puede filtrar o compartir fuera del grupo sin consentimiento, en este grupo toda la información es pública por defecto.

Seguridad de dispositivos

Si toman tu dispositivo (robo, extravío, confiscación, etc.), evita que otras personas se hagan pasar por tí y lean tus mensajes, contactos, correo, etc. Para más información sobre seguridad de dispositivos, véase la actividad: ¡Respalda! ¡Bloquea! ¡Elimina! También conocido como alguien tomó mi celular: cruzar fronteras, detenciones, incautación y robo

- Configura el bloqueo
- Establece una contraseña robusta y segura
- Cifra tu celular
- Cifra tu tarjeta SIM

Batería y red

¿Qué pasas si alguien no puede usar Signal o el aplicativo que ha escogido el grupo? ¿O no tiene acceso a su dispositivo o internet por algun fallo o corte de red? ¿Tienes un plan B para conectarte a internet? por ej, algún router portable (pero atención, si ocupa la misma red celular y hay un fallo a este nivel, entonces no servirá) ¿Tienen algun plan/protocolo/procedimiento fuera de internet? ¿Tienen cargadores USB o alguna forma de cargar baterías?

Materiales complementarios

- Cómo realizar verificaciones de seguridad y usar palabras clave de seguridad (inglés) - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/
- https://ssd.eff.org/es
- https://ciberseguras.org/?s=celular

image_1605452256072.png
Image not found or type unknown

¡Respalda! ¡Bloquea! ¡Elimina! También conocido como alguien tomó mi celular: cruzar fronteras, detenciones, incautación y robo [actividad táctica]

activ-tacticas_200px-con-texto.png
Image not found or type unknown

En esta actividad, planearemos y realizaremos los preparativos para situaciones donde nuestros celulares pueden estar bajo riesgo físico. Algunas situaciones pueden incluir:

- Temas de seguridad a la hora de participar en protestas y marchas
- Temas de seguridad a la hora de cruzar fronteras
- Temas de seguridad cuando hay riesgo de detención y incautación
- Temas de seguridad cuando hay riesgo de robo y acoso

Esta actividad consiste en 4 etapas con la opción de una parte más práctica dedicada a instalar y configurar dispositivos.

- Prácticas actuales de cuidado
- Planear y configurar nuestros dispositivos
- Presentación - Opcional

Si quieren, terminen esta actividad con una parte más práctica para aplicar estrategias y tácticas.

Objetivos de aprendizaje

- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas;
- obtener una noción básica de cómo funciona la comunicación celular y de los riesgos implicados;
- adquirir y practicar estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Para participantes con diferentes niveles de experiencia utilizando celulares para poner en práctica la seguridad táctica con especial enfoque en los cuidados y dispositivos.

Tiempo requerido

Aproximadamente **80 minutos**.

Materiales requeridos

- Papeles grandes/rotafolios/pizarrón + marcadores

Mecánica

Este ejercicio está diseñado para apoyar a activistas que tienen la intención de interactuar en situaciones arriesgadas con sus celulares. Como resultado de esta actividad, tendrán un mapa de herramientas y tácticas que pueden utilizar.

Prácticas actuales de cuidado digital - 20 minutos

> **Consideraciones de cuidados:** *en esta actividad táctica planeamos y nos preparamos para usar nuestros celulares en situaciones donde, tanto nosotras como nuestros dispositivos, se exponen*

Empieza recalcando que prepararse para una situación arriesgada implica considerar primero cómo nos cuidamos antes, durante y después de la acción.

A través de una discusión grupal, comparte qué diferentes maneras tienen de cuidarse en situaciones de mucho riesgo. A nivel individual, responde a las siguientes preguntas:

- Entre las situaciones en las que participas, ¿en qué casos necesitas considerar tu seguridad física y la de tu dispositivo?
- ¿Qué estás haciendo ya para cuidarte - antes, durante y después - en estas experiencias?

Divide el papel en 3 secciones: antes, durante y después. Se verá algo así como:

Ejemplo		
· · · · · ANTES · · · · ·	**· · · · · DURANTE · · · · ·**	**· · · · · DESPUÉS · · · · ·**

Una vez contestada las preguntas, compartan en el grupo sus respuestas, tanto prácticas que realizan por su cuenta como las que hacen con otras personas. Anota en un pizarrón o papel grande palabras clave que salen de las aportaciones. Deja visible esta constelación de palabras.

Las participantes seguirán utilizando este método sencillo para organizar la siguiente parte del taller.

Planear y configurar nuestros dispositivos - 45 minutos

Si estás trabajando con participantes que están organizando un evento, realiza el ejercicio basado en eso. En caso contrario, estos escenarios descritos a continuación pueden servir. Son ejemplos y te invitamos a apropiarte de ellos, modificarlos e inventar tus propias situaciones.

Escenario 1: Temas de seguridad a la hora de participar en protestas y marchas

Vas a participar en una marcha/protesta masiva. Necesitas poder mantener segura la información almacenada en tu celular y evitar que te rastreen en la protesta/marcha, pero también necesitas utilizar tu celular para contactar con aliadas en caso de emergencias. También estás pensando en utilizar tu celular para documentar la marcha/protesta y cualquier posible violación a los derechos humanos que pueda pasar.

Escenario 2: Temas de seguridad a la hora de cruzar fronteras (inseguras)

Estás viajando y vas a cruzar la frontera hacia una ubicación insegura. Quieres utilizar tu celular para mantenerte en contacto con aliadas sin que otras personas ajenas te rastreen. Pregunta a las demás qué estrategias tienen cuando saben que quizás alguien tenga acceso a su dispositivo. Algunos ejemplos de situaciones pueden incluir cruzar la frontera, subirse a un avión, ir a una protesta/marcha.

Escenario 3: Temas de seguridad cuando hay riesgo de detención y incautación

Te has enterado, a través de un contacto de confianza, que te están fichando por parte del Estado y pretenden detenerte y confiscar tus dispostivos debido a tu activismo.

Escenario 4: Temas de seguridad cuando hay riesgo de robo y acoso

Te preocupa que alguien pueda robarte el celular y utilizar el contenido almacenado para acosarte.

Pide a las participantes documentar sus discusiones sobre papeles que tengan 3 secciones: antes, durante y después. Se verá algo así como:

EJEMPLO		
· · · · · ANTES · · · · ·	**· · · · · DURANTE · · · · ·**	**· · · · · DESPUÉS· · · · ·**

En grupos pequeños, deja tiempo para discutir las siguientes preguntas:

¿Qué riesgos e impactos viven las personas (en este escenario o en el evento que está planeando el grupo)? ¿Quiénes viven estos impactos? Toma en cuento a ti, a las personas que están en tu celular de alguna manera (es decir, información sobre ella), tus actividades (temas y eventos en los que estás trabajando), etc.

Puedes basarte en las siguientes preguntas como orientación para reducir los impactos desde una perspectiva táctica.

Antes: piensa en qué harás para preparar tu celular para este escenario.

- ¿Qué archivos vas a eliminar? ¿Por qué?
- ¿Qué aplicativos vas a instalar? ¿Por qué?
- ¿Vas a avisar a gente sobre tus planes?
- ¿Vas a acordar, entre un grupito de personas, un protocolo de seguimiento para saber cómo está cada quien antes y después de la actividad si es posible?
- ¿Qué formas de comunicación segura vas a utilizar con las demás personas?
- ¿Qué otros tipos de estrategias vas a implementar con tus aliadas para mantenerse seguras durante la actividad?

Durante: piensa cómo vas a utilizar tu celular en este escenario.

- Fuente de electricidad: ¿es un tema que hay que considerar?
- ¿Cómo vas a asegurar que las personas puedan cargar sus celulares?
- Servicio: ¿es un tema que hay que considerar?
- ¿Qué vas a hacer si alguien no puede usar/acceder a su servicio telefónico, aplicativos o datos?
- ¿Tienen algún plan/protocolo/procedimiento fuera de internet?
- ¿Con quién(es) quieres comunicarte en esta situación? ¿Cómo lo harás?
- ¿Estás documentando la protesta/marcha? En caso afirmativo, ¿estás utilizando algún aplicativo en particular?
- ¿Quién podrá contactarte a través del celular?
- ¿Y con quién(es) vas a contactar?
- Si vas a utilizar otra tarjeta SIM, ¿cómo vas a escoger un proveedor telefónico?
- ¿Sabes si algunos son más seguros que otros?
- ¿Quién(es) podrán contactar contigo?
- ¿Con quién(es) te vas a contactar?

Después: piensa qué vas a hacer después de este escenario.

- Archivos multimedia: si aplica, ¿qué vas a hacer con las grabaciones, fotos, audios y otros archivos multimedia que recopilaste?
- Metadatos y registros que tu celular genera: ¿qué medidas necesitas tomar sobre los datos que tu celular genera en este contexto (tomando en cuenta los metadatos, los historiales y las ubicaciones dispositivo)?
- En caso de incautación: ¿cómo sabes si tu celular no tiene spy-ware?
- En caso de robo o incautación: ¿qué vas a hacer para restaurar la integridad y seguridad de tu celular?

Deja entre 30 y 45 minutos para que los grupos puedan pensar en planes, estrategias y tácticas. Después comparte en plenaria las diferentes respuestas. Utiliza estas respuestas para planear una sesión práctica de seguridad celular.

Presentación (opcional) - 15 minutos

Anotaciones para facilitar la sesión: según tu forma de trabajar y cómo son tus participantes, quizás quieras profundizar y complementar con alguna presentación. A continuación incluimos anotaciones que creemos que pueden ser útiles para planear la sesión.

Antes

- Recalca que los escenarios planteados son situaciones donde hay una preocupación sobre nosotras mismas y nuestras pertenencias. Realiza planes para verificar con alguien de confianza que todo está bien antes y después de la situación. La frecuencia con la que verificas con esta(s) persona(s) puede variar según el nivel de riesgo de la situación.
- Para situaciones de alto riesgo: recomendamos verificar hasta cada 10 minutos. Por ejemplo, si vas a ir a una protesta/marcha de mucho riesgo o vas a cruzar una frontera peligrosa.
- Para situaciones de riesgo bajo: por ejemplo, estás trabajando con un grupo de trabajadoras sexuales y vas a estar moviéndote a diferentes lugares y participando en diferentes reuniones. Planea verificar con alguien de confianza cada vez que te desplazas al siguiente lugar de reunión y al llegar al destino. Avisa también al empezar y terminar el día con mensajes sencillos como "ya llegué", "voy empezando el día".
- Limpieza: ¿qué tienes en tu dispositivo que quieres mantener privado?
- Cierra sesión: sal de tus sesiones cuando no las estás utilizando. No las mantengas abiertas si no necesitas utilizar el servicio. Si alguien toma tu celular y están abiertas tus sesiones, podrán acceder a tus cuentas, ver qué haces y hacerse pasar por ti.
- Bloquea y cifra: puedes cifrar tu celular, tarjeta SD y tarjeta SIM, cada uno con su propia clave PIN de tal manera que, aunque acedan a tu dispositivo, no pueden acceder a la información. También, en caso de acceder a uno de estos lugares, no pueden acceder a los demás porque tienen claves distintas. *Si estás en una situación donde te están amenazando si no das acceso a tu información, quizás no puedas mantener tus claves y contraseñas privadas. Toma esto en cuenta en tus protocolos de seguridad y habla con otras personas sobre ello.*
- Copia de dispositivos: muchas agencias de policía tienen acceso a equipos que hacen copias digitales de dispositivos como celulares, laptops y discos duros. Si tu dispositivo está cifrado, aunque hagan una copia, no podrán acceder a la información sin la clave. En caso contrario, podrán acceder a los contenidos a través de esta copia.
- Silenciar: deshabilita el sonido y los avisos visuales de tus notificaciones, ponlo en modo silencio.
- Eliminar archivos remotamente: en algunas situaciones, quizás quieras habilitar esta función para asegurar que tú u otros contactos de confianza puedan borrar remotamente el contenido de tu celular en caso de que alguien sin consentimiento consiga acceder a él o en caso de pérdida/extravío.
- Tarjetas SIM y dispositivos: nuestros celulares son dispositivos que crean y comparten mucha información, desde mensajes y llamadas hasta datos de aplicativos y metadatos como ubicación y fechas. Evalúa si quieres llevar tus dispositivos personales encima en situaciones arriesgadas. En caso afirmativo, tus oponentes/adversarios pueden asociarte a tu dispositivo y rastrearte. También puedes dejar tu dispositivo personal en casa o

utilizar algún dispositivo "desechable"("burnout") que planeas utilizar sólo para esta acción o evento, partiendo ya del presupuesto que lo van a asociar a ti, pero que podrás desecharlo después. Toma en cuenta que vas a necesitar tanto un celular como una tarjeta SIM para seguir este método. Y ambos tienen un identificador. Si utilizas tu teléfono y otra tarjeta SIM y después vuelves a meter tu tarjeta SIM, vincularán estas identidades. *Esta estrategia implica una inversión de dinero y energía: evitar que no te rastreen a través del celular y tarjeta SIM implica planear mucho y poder desechar el dispositivo. Si no tienes las condiciones para ello, puedes utilizar un dispositivo alternativo cada vez que participas en una situación arriesgada, pero tomando en cuenta que conforme lo vayas utilizando más y más, será más fácil vincularte a este aparato.*
- Sacar tarjetas SIM: si te encuentras en una situación arriesgada sin haberlo planeado, puedes sacar partes de tu teléfono como tu tarjeta SIM o tarjeta de memoria (en caso de que sea posible). *Observación: en algunas situaciones, esto puede ser utilizado como pretexto por parte de agresores para incrementar el daño que causan.*

Durante

- Eliminar archivos remotamente
- PixelKnot para cifrar mensajes
- Firechat para protestas/marchas y cortes de red

Cuando tu celular ha estado fuera de tu control

- Formatea o sustituye por un dispositivo nuevo: recomendamos restaurar la versión de fábrica. Si puedes permitírtelo económicamente, reemplaza el dispositivo; no resetees tu dispositivo anterior sino déjalo con alguien que pueda analizarlo.
- Tus servicios: cambia las contraseñas de todas tus cuentas.
- Avisa a la gente: si tu celular ha estado fuera de tu control, avisa a tus contactos y las personas con las que has estado manteniendo comunicación e infórmalas sobre las posibles implicaciones.

Materiales complementarios

- EFF Autoprotección Digital Contra La Vigilancia - Cómo cifrar su iPhone - https://ssd.eff.org/es/module/c%C3%B3mo-cifrar-su-iphone
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Signal en iOS - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-ios
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Signal en Android - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-android
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Whatsapp en iOS - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-whatsapp-en-ios

- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Whatsapp en Android - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-whatsapp-en-android

image-1605451259399.png
Image not found or type unknown

Conversación, intro + sesión práctica: Escoger apps celulares [actividad táctica]

activ-tacticas_200px-con-texto.png
Image not found or type unknown

En esta conversación y presentación, nos enfocaremos en apoyar a las participantes a escoger aplicativos celulares por su cuenta, especialmente para que puedan aplicar estos criterios más allá del taller.

Esta actividad tiene 3 etapas:

- Conversación: ¿qué estás usando y por qué?
- Presentación: recomendaciones para escoger apps.
- Actividad práctica: evaluar apps de mensajería **o** Actividad práctica: evaluar apps conocidas

Objetivos de aprendizaje

- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas;
- adquirir y practicar estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Para cualquier persona que ha usado un celular y quiere saber mejor cómo escoger aplicativos.

> **Comentario sobre interseccionalidad:** esta actividad pretende servir de práctica para evaluar la seguridad de aplicativos celulares, en concreto los de mensajería (chat).

Otros tipos de aplicativos que pueden ser más relevantes para las participantes pueden ser:

- apps de menstruación/fertilidad: datos que recolectan y soluciones de control natal que pueden ofrecer
- apps de citas en línea
- apps de mensajería/chat y borrado inmediato (flash apps)
- apps de seguridad, especialmente para mujeres
- apps interactivos y de juegos
- apps de performance y actuación como tiktok

Tiempo requerido

Aproximadamente **60 minutos.**

Materiales requeridos

- papel para que cada grupo pueda anotar
- pizarrón o pap
- algunos celulares con acceso a internet y acceso a las tiendas de apps

Mecánica

Conversación: ¿qué estás usando y por qué? - 10 minutos

Pregunta en plenaria: ¿cuáles son los 5 aplicativos que más utilizas? ¿Para qué los utilizas?

- Enumera los aplicativos que vayan saliendo, sondea quiénes más los utilizan y anota el número de usuarias en cada caso.
- También anota las razones por las que los utilizan.

Después pregunta: ¿cómo escogiste el aplicativo?

- Anota las respuestas.

Haz un resumen y una ronda de reflexiones.

Presentación - recomendaciones para escoger apps - 5 minutos

- ¡Investiga! Aprende qué opciones tienes y qué aplicativos son de confianza. Comparte tus formas de investigar - leer sobre el aplicativo en internet o a través de algún fanzine/panfleto/etc., a través de amistades que les gusta investigar... Lee los comentarios positivos y negativos en la página de descarga del aplicativo.
- ¿Cómo empiezas a averiguar si una app es segura? ¿Quiénes lo desarrollan? ¿Cuál es la política de privacidad? ¿Es de código abierto? ¿Han utilizado la app para acceder a sistemas/dispositivos?
- Comprender los permisos que requiere el aplicativo. Por ejemplo, ¿por qué una app de juegos necesita acceder a tu cámara o libreta de contactos?
- ¿Qué te da seguridad/confianza a la hora de utilizar un aplicativo? ¿Puedes controlar los permisos? ¿Sabes dónde almacena información sobre ti o los datos que produce en general? ¿Sabes dónde está todo eso?
- Si es un aplicativo de redes sociales, ¿cómo quieres interactuar con personas a través de este aplicativo? ¿Qué tanto puedes decidir sobre tu nivel de visibilidad e interacción? ¿Cuál es la configuración por defecto? ¿Qué revela sobre ti? ¿A qué te conecta? ¿Conoces temas de seguridad en relación a esta herramienta? ¿Existen mecanismos para reportar contenidos/personas/páginas? ¿Y mecanismos que pueden ser utilizados en tu contra?

Actividad práctica: Evaluar apps conocidas - 15 minutos

Entra en la tienda de apps/centro de descargas y busca algún aplicativo comúnmente utilizado. Por ejemplo, si vives en una ciudad, una app de taxis o del metro. ¿Cómo optaste por esa herramienta?

Verifica (1) qué permisos pide (2) quién está distribuyendo el aplicativo, quién lo administra/gestiona y quién es la entidad propietaria.

Existen muchos aplicativos que son "copias" de apps conocidas que intentan hacerte picar el anzuelo con algo que quieres como un juego, un mapa del transporte público cuando en realidad están diseñadas para hacer otra cosa como mandar tu ubicación a terceros.

Quienes desarrollan o tengan la propiedad de la app aparece en la descripción de la tienda/centro de descargas. Comparte cómo averiguas de qué empresa es una app o quienes la gestionan y cómo investigas si los valores que tienen coinciden o no con los tuyos, además de cómo afecta tu privacidad y seguridad usar esta app. Si quieres escoger entre varias apps que se ven parecidas, busca más información en internet (desarrolladores, lugar de descarga...)

Actividad práctica: Evaluar apps de chat - 30 minutos

Forma grupos pequeños

- identifica 2-3 apps que están usando para chatear
- contesta a las preguntas orientativas

En plenaria - puesta en común: por turnos, cada grupo comparte una app hasta que hayan compartido todas

Preguntas orientativas:

- ¿quiénes, entre las participantes, utilizan esta app? ¿es fácil de utilizar?
- ¿Quiénes son los propietarios? ¿Quiénes manejan el servicio?
- ¿Dónde se almacenan tus mensajes?
- ¿Están cifrados? ¿Qué otras configuraciones de seguridad te permite establecer?
- ¿De qué otras maneras puedes resguardar tus comunicaciones a la hora de utilizar este aplicativo?
- ¿En qué contextos está bien utilizarlo? ¿En qué contextos está bien utilizarlo?

Lista de apps de chat y consideraciones

SMS

- Todo el mundo utiliza SMS
- Empresa telefónica. Particularmente arriesgado si hay un historial de tensión y conflictos entre la empresa telefónica y el gobierno o si es una empresa del propio gobierno o si la empresa telefónica es corrupta.
- Mensajes enviados a torres entre la persona con la que te estás comunicando y tú. Mensajes enviados a torres entre la persona con la que te estás comunicando y tú.
- Sin cifrar
- Bueno para comunicarse sobre temas que no son arriesgados
- Generalmente se cobran los mensajes

Llamadas

- Todo el mundo utiliza llamadas.
- Empresa telefónica tiene control
- Almacenadas por empresa telefónica -- con certeza por lo menos los metadatos
- Ejemplo de inseguridad: ¡Hola Garcie! Incidente en Filipinas: una llamada entre ex-presidente Arroyo y el jefe de la Comisión Electoral fue interceptada, revelando cómo la presidente le decía al jefe de COMELEC cuánta ventaja quería en las próximas elecciones.
- Buena opción para comunicarse sobre temas que no son arriesgados

- Generalmente se cobran las llamadas.

Facebook Messenger

- Cualquier persona que tiene cuenta en Facebook lo puede utilizar
- Viene con su propio aplicativo
- Dicen cifrar, pero no está verificado
- Facebook es propietaria.
- En vez de usar la app de FB, puedes utilizar Chat Secure. Puedes utilizar tus credenciales de FB con otras usuarias de FB. Pero para habilitar el cifrado, las otras personas tienen que utilizar Chat Secure también y comunicarse por ahí.
- Gratuito, pero tienes que tener internet (WiFi o datos celulares)

GoogleTalk

- Cualquier persona con cuenta Google
- Viene con su propio aplicativo
- Dicen que tiene cifrado, pero no está verificado
- Google es propietaria.
- Puedes utilizar Chat Secure también.

Signal (App recomendada)

- Gestionada por activistas de tecnologías libres y seguras
- Cifrado de extremo a extremo
- No se almacenan en "la nube". Almacenas tus mensajes en tu celular o computadora. SIgnal no almacena tus mensajes una vez que los hayas enviado.
- Llamadas cifradas
- Para comunicación confidencial

Telegram

- App de chat conocida
- Cifrado extremo a extremo sólo en chats secretos

WhatsApp

- Muchas personas usuarias
- Facebook es propietaria de Whatsapp aunque el equipo de desarrollo de Whatsapp asegura proteger la privacidad de las usuarias en su Política de Privacidad.
- Sólo almacenan mensajes que no se han enviado.
- Cifrado extremo a extremo, pero si los mensajes están respaldados en tu cuenta de correo asociada, se almacenan sin cifrar.
- Buena opción para comunicarte con muchas personas
- Inquietudes sobre Facebook como entidad propietaria

Wire

- Asegura cifrar de extremo a extremo. Aún pendiente de verificación.
- Desarrollado por personas que antes trabajaban en Skype -- importante considerar porque Skype filtraba datos (a través de 'puertas traseras' en el código) al gobierno Chino.
- Llamadas cifradas

Materiales complementarios

- Qué es el cifrado - https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- MyShadow - Alternativas de apps de chat: https://myshadow.org/alternative-chat-apps
- Por qué Signal y no Whatsapp
- Consejos, Herramientas y Paso a Paso para Comunicaciónes más seguras | EFF- https://ssd.eff.org/es
- Te sugerimos también realizar una búsqueda en internet sobre los temas más actuales de seguridad relacionados con los aplicativos que piensas recomendar y utilizar en las sesiones. Palabras clave de búsqueda que puedes utilizar: nombre de app + revisión/auditoría seguridad + año + nombre de app + temas seguridad conocidos (también puedes buscar en inglés para obtener más resultados). Según qué encuentras, quizás quieras dejar de recomendar/usar un aplicativo que tenga temas de seguridad sin resolver.

image-1605451879726.png
Image not found or type unknown

Usar celulares para documentar casos de violencia: Planeación y práctica [actividad táctica]

Esta actividad táctica es para activistas que quieren utilizar sus celulares para documentar casos de violencia.

Acerca de esta actividad

activ-tacticas_200px-con-texto.png
Image not found or type unknown

Esta **actividad táctica** para activistas que quieren utilizar sus celulares para documentar casos de violencia. Desarrollaremos habilidades para hacer una evaluación de seguridad y un plan de documentación. Después pasaremos a una sesión práctica con nuestros celulares donde documentaremos utilizando los aplicativos y herramientas que hemos escogido según el trabajo anterior en la sesión.

> ***Nota de cuidados:*** *si vas a facilitar esta actividad, toma en cuenta que puede durar hasta un día. Asegúrate de programar descansos y toma en cuenta que documentar puede ser estresante, así que, compartir entre todas prácticas de autocuidado y relajación como respiraciones y movimiento corporal puede ser buena idea.*

Esta actividad se divide en dos momentos:

Parte 1: Evaluar y planear

Primero vamos a planear nuestro trabajo, evaluando temas de seguridad y bienestar. A partir de esta evaluación, crearemos procedimientos de seguridad y tomaremos decisiones con respecto al manejo de nuestros celulares y archivos.

Parte 2: Preparar, configurar y practicar

Ponemos en práctica tácticas para documentar casos de violencia utilizando nuestros celulares.

Recomendamos complementar esta actividad con las actividades Debate: Documentar casos de violencia y ¡Respalda! ¡Bloquea! ¡Elimina!

Objetivos de aprendizaje

- compartir y poner en práctica estrategias y tácticas de seguridad celular para manejar los impactos de la comunicación celular en nuestras vidas y de nuestras compañeras y movimientos/redes/grupos.

¿Para quién es esta actividad?

Grupos que están o planear documentar casos de violencia con sus celulares

Tiempo requerido

Aproximadamente **1 hora 45 minutos.**

Materiales requeridos

- Información de casos prácticos impresa o proyectada

Mecánica

Introducción - 5 minutos

Comparte ejemplos recientes de grupos/redes que utilizan celulares para documentar violencia. Pide a las participantes compartir ejemplos de cómo utilizan sus dispositivos para documentar y compartir documentación.

Los ejemplos pueden incluir: documentar violencia ejercida por el Estado, re-enviar videos de actos violentos y las implicaciones de tener este tipo de registro en nuestros dispositivos.

Parte 1: Evaluar y planear – 30 minutos

Forma grupos según qué tipo de casos de violencia está documentando cada quien.

> ***Nota de cuidados:*** *anima a las participantes evaluar y planear tomando en cuenta sus propias necesidades de cuidado. Documentar casos de violencia puede ser un disparador psicológico y generar estrés para quienes documentan. Invita a las participantes a compartir cómo están encontrando recursos y herramientas y cómo están trabajando con otras activistas para abordar los impactos de documentar.*

véase también ¡Respalda! ¡Bloquea! ¡Elimina!

Propósito y planeación: Discute el propósito de documentar

- ¿Qué estás documentando? ¿Por qué?
- ¿De qué situación se trata?
- ¿Cuál es el propósito de tu documentación? Si está siendo utilizada como prueba/evidencia, planea tomando en cuenta los requisitos procesales pertinentes. Para más información, echa un vistazo a este material desarrollado por WITNESS sobre utilizar registros de video como pruebas: https://vae.witness.org/video-as-evidence-field-guide/

Evaluar riesgos y tomar cuidados: Hablen sobre temas de seguridad conocidos y probables para las personas que están documentando y siendo documentadas.

- ¿Cuáles son los temas de seguridad que más probablemente vayan a suceder? ¿Es probable que te cruces con la policía o personas que están en tu contra?
- ¿Tu contexto puede cambiar en maneras que afecte tu seguridad? ¿Cómo vas a planear para esto? Discute sobre situaciones probables. Por ejemplo, puede ser que la policía u otras personas adversarias se vuelvan más agresivas o violentas. En respuesta, puedes seguir documentando o, justamente lo contrario, dejar de documentar. También puedes comunicarte más con tu grupo de confianza y mantenerles al tanto de cómo estás.
- ¿Quién va a estar documentando (grabando, apoyando, en comunicaciones, etc.)? ¿Qué tipo de apoyo tienen y necesitan?
- ¿Qué sabes de temas de seguridad? Por el tipo de contenido y el contexto en el que están documentando, ¿las personas involucradas se sienten más o menos seguras?
- ¿Qué roles pueden asumir con comodidad? ¿Qué estrategias llevarás a cabo tus aliadas y tú para mantenerse seguras durante el proceso de documentación? ¿Qué papel tiene el consentimiento aquí? ¿Buscarás el consentimiento de las personas que estás

documentando? ¿Cómo documentarás o grabarás este consentimiento? ¿Buscarás el consentimiento de las personas que estás documentando sobre compartir el registro y posterior documentación?
- ¿Cuáles son los temas de seguridad relacionados con tener el registro en tu posesión?
- ¿Cuáles son los temas de seguridad relacionados a las personas que aparecen en el registro? ¿Cómo cuidarás el registro una vez grabado y almacenado en tu dispositivo? ¿Harás un respaldo en otro disco de almacenamiento? Piensa en dónde lo vas a guardar, quién tiene acceso, si está cifrado, cuándo lo vas a eliminar.
- ¿Cuáles son los posibles impactos de documentar violencia? ¿Qué recursos necesitas como individuo para estar bien y estar en eje durante este trabajo? ¿Qué recursos pueden brindar los demás? ¿Cómo se apoyarán en el grupo?

Conoce tus derechos

- En el lugar donde te encuentras, ¿cuáles son tus derechos con respecto a la documentación?
- ¿Cómo se relaciona con el contexto en que estás documentando? Ejemplos de preguntas que puedes hacer - ¿es legal grabar a la policía? ¿es legal la reunión pública?
- ¿La policía puede mirar lo que tienes en tus dispositivos?
- ¿Puede obligarte a borrar archivos?

Preparar tus dispositivos

- ¿Estás usando tu celular personal?
- ¿Qué archivos vas a eliminar? ¿Por qué?
- ¿Qué aplicativos vas a instalar o desinstalar? ¿Por qué?
- Servicios de ubicación: ¿es más seguro habilitar o deshabilitar la ubicación y rastreo? ¿Quieres que personas de confianza puedan seguir tu ubicación?
- Eliminar archivos remotamente: ¿quieres habilitar esta funcionalidad en caso de perder el acceso a tu dispositivo?

Discusión: Pros y contras de utilizar tu propio celular para documentar casos de violencia

Recomendación

Utiliza información de ¿Qué es un celular? para explicar cómo los celulares se vinculan a las personas que los están utilizando, cómo funciona la vigilancia en tiempo real, cómo los metadatos generados al utilizar un celular y los metadatos EXIF DE fotografías pueden ser utilizados para identificarte.

Después

- Crea un plan para juntarse como grupo y ponerse al día. ¿Cómo estuvo todo? ¿Qué cosas inesperadas sucedieron? ¿Cómo respondió el grupo? ¿Qué está pendiente de respuesta? ¿Cómo se sienten? ¿Quién va a participar en los próximos pasos?
- Compartir - revisa tus acuerdos sobre temas de consentimiento y compartir. Asegúrate de compartir estos acuerdos con todas las personas con las que vas a estar trabajando.

Discusión

¿Qué más quieres hacer después de documentar?

image-1605452256072.png
Image not found or type unknown

Parte 2: Preparar, configurar, prácticar - 60 minutos

Según el tiempo disponible, puedes realizar estas actividades como grupo grande o formar grupos más pequeños y que las personas se unan, por afinidad, al que quieran.

Consejos y trucos para hacer registro

Cómo utilizar fotos, videos y/o audios para documentar casos de violencia.

- Busca las herramientas que ya vienen en tu celular para grabar: fotos, videos, audio
- Practica con estas herramientas tomando en cuenta los consejos de WITNESS sobre grabajar con celulares (enlace más abajo en Materiales).
- Planea lo que vas a grabar.
  - Graba detalles y perspectivas: acércate para grabar detalles y aléjate para tomar planos más generales de lo que está pasando.
  - Mantén el pulso: escoge lo que vas a grabar y mantén la cámara quieta al menos 10 seguros, evita hacer zoom, utiliza ambas manos y mantén tus codos contra tu cuerpo para mayor estabilidad.
  - Sostén tu celular horizontalmente para un encuadre con mayor ángulo.
  - Acércate para lograr mejor sonido: considera los ruidos fuertes que pueden interferir con el audio de las entrevistas.
  - Toma en cuenta la luz: intenta grabar en ubicaciones bien iluminadas y que las fuentes de luz estén atrás.

- Si tienes tiempo, trabaja en equipos y planea la documentación utilizando estas herramientas. Practica creando una pieza multimedia/audiovisual
- Si vas a compartir a través de Youtube, considera utilizar la funcionalidad de subtítulos: https://support.google.com/youtube/answer/2734796?hl=es

- Contexto y mensajes. Planea tus mensajes. ¿Dónde vas a publicarlos? ¿Qué texto va a acompañar la publicación? ¿Cómo vas a vincularlo a tu estrategia general?

Grabar llamadas

Comentario: ha sido útil para trabajadoras sexuales que están siendo amenazadas por las autoridades.

Utilizar una aplicación

Puedes instalar y utilizar un aplicativo que te permite grabar. El aplicativo utiliza datos de internet en vez de la línea telefónica por lo que tendrás que planear con anticipación y asegurar que tienes datos de antemano.

- Evalúa qué aplicativo quieres utilizar e instálalo.
  - Google Voice te permite grabajar llamadas entrantes, pero no entradas salientes (las que haces tú).
  - Tu celular quizás ya tenga una app para grabar.
- Prueba con alguna compañera.
- Practica ubicar el archivo de grabación y guardarlo fuera de tu celular en un lugar seguro donde puedas acceder después.

Utilizar una grabadora

Si no puedes o decides no utilizar una aplicación por cualquier razón, te puede apoyar alguien para registrar con una grabadora externa o con su celular la llamada (ponlo en manos libres/altavoz). Algunos teléfonos tienen grabadoras de voz por defecto.

- Evalúa qué herramienta o aplicativo quieres utilizar e instálalo.
- Prueba con alguna compañera. Para obtener un buen sonido, acércate y graba en un lugar donde no haya ruido.
- Practica ubicar el archivo de grabación y guardarlo fuera de tu celular en un lugar seguro donde puedas acceder después.

Capturas de pantalla

Puedes tomar capturas de pantalla de tu celular para documentar pruebas de acoso y violencia, por ejemplo, mensajes que recibes o ves.

- Escoge un aplicativo para tomar capturas de pantalla y practica.
  - En Android: en ciertas versiones, si pulsas el botón de bajar volumen y el botón de encendido al mismo tiempo toma una captura de pantalla y lo guarda en tu galería.
  - iPhone X, XS, XR: mantén pulsado el botón en el lateral derecho y el botón de subir volumen al mismo tiempo. Tomará una captura y lo guarda en un album de fotos llamado Capturas.

    - iPhone 8 y versiones anteriores: mantén pulsado el botón de encendido en el lateral derecho y el botón de Inicio al mismo tiempo. Guarda la captura en Fotos en el album Capturas.
- Practica ubicar el archivo de grabación y guardarlo fuera de tu celular en un lugar seguro donde puedas acceder después.

¡Ojo! No podrás sacar captura de todos los aplicativos. Algunos, como Signal, tienen una función de seguridad que te permite prevenir que otras personas saquen capturas de pantalla de determinadas conversaciones.

Documentar eventos para registro interno

Cuando sucede algo, ya sea algo breve, largo, que se vaya repetir o no, es importante documentarlo.

Transmisión en vivo

Adaptado a partir de: Livestreaming Protests, written for activists in the USA

Estás transmitiendo en vivo en un evento (en alguna protesta, manifestación, etc). Recomendamos **enfáticamente** que utilices las actividades de planeación y preparación para poder ver cómo se va desarrollando la actividad que estás documentando e implicar a las personas espectadoras para que apoyen la causa. Puede haber riesgos altos como la presencia de la policía y la identificación de activistas por parte de autoridades.

- **Ubicación:** documenta tu ubicación intencionadamente: graba letreros de la calle, edificios y puntos de referencia. También considera como revelar tu ubicación en tiempo real tiene que ver con tu propia seguridad y las de las personas que estás grabando.
- **Identificar participantes:** ¿podrás obtener el consentimiento de aquellas personas que estás grabando? ¿cómo quieres y necesitas proteger sus identidades? Considera no grabar sus rostros.
- **Identificar tácticas:** tiene diferentes consecuencias e impactos según qué se documenta. Por un lado, puedes grabar sin querer tácticas de activistas de una manera que les impacta negativamente. Por otro, puedes documentar las tácticas de la policía para evaluar mejor qué hacen y predecir mejor cómo van a actuar en el futuro.
- **Público/audiencia:** ¿qué pretendes lograr con la transmisión en vivo? ¿Quieres transmitir para un grupo pequeño de confianza que puede apoyarte difundiendo tus contenidos?
- **Trabajo en equipo:** trabajar con otras personas que te pueden apoyar interactuando con espectadoras a través de comentarios y discusiones; y compartiendo los contenidos por mútiples canales**.**
- **Proponer una acción:** Invite a sus espectadores a actuar.
- **Tu dispositivo:** ¿quieres utilizar tu dispositivo personal? Cualquier dispositivo que utilices, recomendamos cifrarlo y ponerle contraseña de acceso y bloqueo. No utilices contraseña de patrón.

Puesta en común - 10 minutos

- Relacionen el ejercicio con una reflexión sobre cómo documentamos casos de violencia y cómo puede generar estrés.
- Comparte lo que cada grupo ha trabajado.
- Comparte aprendizajes, nuevas herramientas y consejos.

Materiales complementarios

- https://ssd.eff.org/es
- https://ciberseguras.org/
- https://cyber-women.com/es/
- https://es.gendersec.train.tacticaltech.org/
- Video For Change Network: https://video4change.org/
- WITNESS - Grabar en equipo: protestas, marchas y concentraciones (en inglés) - https://library.witness.org/product/filming-in-teams-protests-demonstrations-rallies/
- WITNESS - Cómo grabar con tu celular (en inglés)- https://library.witness.org/product/filming-with-a-mobile-phone/
- WITNESS - Guía para entrevistar a sobrevivientes de violencia sexual y violencia de género (en inglés) - https://blog.witness.org/2013/08/new-how-to-guide-for-interviewing-survivors-of-sexual-and-gender-based-violence/
- WITNESS - Cómo transmitir en vivo protestas y marchas (US) (en inglés)- https://library.witness.org/product/livestreaming-protests-usa/ and video https://es.witness.org/recursos/video-como-evidencia/
- https://library.witness.org/product/video-metadata/ (en inglés)
- UWAZI, https://www.uwazi.io/es - Uwazi es una opción gratuita y de código abierto para organizar, analizar y publicar tus documentos.

image-1605452256072.png
Image not found or type unknown

Reinicia tu seguridad para citas en línea [actividad táctica]

activ-tacticas_200px-con-texto.png
Image not found or type unknown

En esta **actividad táctica** compartiremos trucos y consejos de seguridad y privacidad para plataformas y apps de citas. Trabajaremos en grupos pequeños o parejas para actualizar nuestros perfiles y prácticas con estas herramientas. También pondremos en común nuestras distintas necesidades y preferencias a nivel de privacidad, seguridad y uso de herramientas.

> ***Comentario sobre interseccionalidad:*** *procura un espacio para que el grupo pueda relacionan sus distintas consideraciones y prácticas con su identificación de género y sexualidad. Entre las participantes, ¿cómo se relaciona el género y la sexualidad con las apps de citas? ¿Cómo se relaciona con nuestras inquietude sobre privacidad y seguridad?*

Esta actividad consiste en dos partes:

- Compartir trucos y consejos sobre apps/plataformas de citas y seguridad
- Actividad práctica: reinicia tu seguridad de citas en línea

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género;
- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas;
- adquirir y practicar estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Personas que utilizan apps/plataformas de citas y lo quieren hacer de manera más segura.

Tiempo requerido

Entre 2 horas y 2 horas y media.

> **Nota de facilitación:** recomendamos tomar descansos.

Materiales requeridos

- Acceso a internet.
- Celulares para actualizar perfiles.
- Papeles grandes/rotafolio/pizarrón

Mecánica

Compartir trucos y consejos sobre citas en línea

Romper el hielo - 5 minutos

- ¿Quiénes utilizan apps de citas? ¿Cuáles? ¿Cómo escogiste? ¿Por qué?
- ¿De qué maneras estás cuidando de tu privacidad y seguridad?

Citas más seguras – 30 minutos

Antes de ponerse a hablar específicamente de apps y entrar en la parte práctica, compartiremos consejos.

- ¿Qué entiendes por conductas seguras a la hora de usar apps/plataformas de citas?
- ¿Qué cuidados tomas cuando te encuentras con tus "matches" en persona?
- ¿Cuáles son tus estrategias para saber qué es seguro encontrarte con alguien?

- ¿Tienes algún Plan B pen caso de que algo salga mal? ¿Te mantienes en comunicación con alguna amiga durante el encuentro? ¿O le avisas antes dónde vas a ir y con quién, etc.?

Anota las respuestas en grande en algún lugar visible para las participantes. Comparte más consejos sobre seguridad en el grupo.

Apps de citas (consejos de seguridad)

- Asegúrate que tu foto no revele más información de la cuenta, sobre todo tu ubicación, la escuela donde estudias, tu lugar de trabajo, etc.
- Utiliza un correo seguro que no esté asociada a otra cosa
- No utilices un nombre de usuaria que se parezca a tus otras cuentas
- No utilices las mismas fotos que salen en tus cuentas de redes sociales
- Evita utilizar datos personales
- Toma cuidado y presta atención a la hora de escribir tu perfil en la app de citas
- Seguimiento offline: encuéntrate con la persona en un lugar público la primera vez. Si es posible, avisa alguna amiga, familiar, persona de confianza sobre tu lugar y hora de encuentro
- Ponle contraseña al aplicativo si te da opción
- Ponle contraseña y cifra tu dispositivo (cel, compu, tablet)

Nuevos modelos de citas

¿Hay alguna característica que te gusta especialmente de las aplicaciones de citas existentes que podrias buscar en las aplicaciones más recientes?

¿Qué posibilidades y funciones ofrecen las nuevas aplicaciones? (por ejemplo, señalar de alguna manera a los usuarios con mala reputación, documentar a los estafadores, compartir consejos sobre la selección de parejas).

¿De qué manera te relacionas ya con tus amigos/amigas/amigues de confianza y los miembros de tu comunidad en torno a las citas en línea?

Actividad práctica: Reinicia tu seguridad en tus apps de citas - 60-90 minutos

Empieza buscando en internet si hay información sobre ti (hacerte 'Doxxing') utilizando el nombre de usuaria o algún otro dato que tengas en tu perfil de app/plataforma de citas. Reflexiona sobre qué información hay disponible asociada a ti en internet que no quisieras que las usuarias de la app de citas supieran. Según eso, actualiza tu perfil.

En parejas, revisen los Consejos de Seguridad y actualicen sus perfiles. Hablen entre sí y apóyense para verificar si hay información que las identifica y si pueden cambiarla por datos menos

personales siguiendo sus necesidades en relación a la seguridad.

Actualiza tu foto

Verifica y sustituye cualquier imagen/foto en tu perfil y cuenta si no cumple con las consideraciones de seguridad que quieres aplicar. Puedes sacar los metadatos y cualquier otra información que pueda identificarte en estas imágenes.

Actualiza tu descripción

Verifica y escribe de vuelta tu descripción si crees que revela más información de la cuenta sobre ti. ¡Puedes pedirle ayuda a alguna compa si quieres!

Crea una cuenta de correo segura independiente

Puesta en común - 10 minutos

¿Cómo te fue? ¿Cómo te sientes? ¿Te sorprendió? ¿Se te hizo fácil, difícil? ¿Qué vas a hacer ahora?

Facilitatadoras: Si hay interés en Sexting, puedes complementar con la actividad Sexting más seguro.

Materiales complementarios

En español

- Privacidad y seguridad en contextos conservadores: las apps de citas para mujeres de la diversidad sexual. Steffania Paola: https://www.genderit.org/es/articles/edicion-especial-privacidad-y-seguridad-en-contextos-conservadores-las-apps-de-citas-para
- Busca "Riesgos y estrategias usando plataformas para citas" en https://es.gendersec.train.tacticaltech.org/
- https://chupadados.codingrights.org/es/suruba-de-dados/
- https://cyber-women.com/es/sexting/
- https://www.libresenlinea.mx/autodefensa/
- Grindr - https://help.grindr.com/hc/es-419/articles/217955357-Consejos-de-Seguridad-
- Planet Romeo - https://www.planetromeo.com/es/care/safety/
- Tinder - https://policies.tinder.com/safety/intl/es/

En inglés

- Self-Doxxing (en inglés): https://gendersec.tacticaltech.org/wiki/index.php/Step_1#Self-Doxing
- OKCupid (en inglés) - https://www.okcupid.com/legal/safety-tips
- Hornet (en inglés) - https://hornet.com/community/knowledge-base/tips-on-how-to-stay-safe/
- Scruff (en inglés) - http://www.scruff.com/gaytravel/advisories/

image-1605451879726.png
Image not found or type unknown

Sexting más seguro [actividad táctica]

activ-tacticas_200px-con-texto.png
Image not found or type unknown

En esta **actividad** compartiremos y pondremos en práctica estrategias para un sexting más seguro.

Objetivos de aprendizaje

- entender cómo el acceso a los celulares y la comunicación es algo íntimo y depende de nuestra identidad de género;
- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas;
- adquirir y practicar estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Personas que hacen sexting (o están interesadas en hacerlo) y quieren hablar y aprender sobre aspectos de seguridad.

Tiempo requerido

Aproximadamente **2 horas**

Materiales requeridos

- Conexión a internet (WiFi o datos celulares)
- Celulares

Mecánica

Conversación en parejas - 10 minutos

- ¿Alguna vez has hecho sexting? ¿Cuándo fue tu primera vez? ¿Qué medio utilizaste - teléfono fijo, cartas, chat?
- ¿Cómo utilizas tu celular para hacer sexting? ¿Apps, mensajes de texto, mensajes de audio, fotos, video, etc.? ¿Qué te gusta? ¿Cuáles son las ventajas y desventajas para ti?
- ¿Qué temas de seguridad y privacidad tomas en cuenta cuando estás haciendo sexting? ¿Qué medidas de cuidado, seguridad y privacidad tomas?

Poner en común y compartir estrategias - 35 minutos

Compartimos qué es divertido y placentero para nosotras a la hora de hacer sexting con nuestros celulares.

> ***Indicación de interseccionalidad:*** *¿existe un estigma social en relación al sexting? ¿cómo viven el estigma las participantes según su género, sexualidad, origen étnico, clase social, edad, experiencias? ¿Cómo afrontan esta desaprobación social?*

Algunas preguntas para la conversación:

- ¿Qué tipos de archivos multimedia y apps te gusta utilizar? ¿Por qué? ¿Qué otras cosas te gustaría hacer con estas herramientas?
- ¿Cuándo te has divertido más a la hora de hacer sexting? ¿Por qué?

Compartir estrategias

Prepara pedazos grandes de papel con los siguientes títulos:

- Venir(se) con acuerdos
- Hacer el amor, compartir los datos
- Apps y consideraciones básicas de seguridad
- Carta blanca

Facilita una conversación basándote en las preguntas orientativas a continuación. Toma notas en un papel grande o pizarrón con las estrategia compartidas.

Venir(se) con acuerdos

- Toma acuerdos con tus parejas de sexting - ¿qué decisiones quieres tomar con respecto a guardar y compartir información (tanto digital como fuera de la pantalla)?
- ¿Alguna vez negociaste acuerdos con parejas de sexting? ¿Cómo lo hiciste?
- A veces las cosas se acaban. ¿Cómo negocias con parejas después de una ruptura sobre el sexting? ¿Guardan los archivos?

Hacer el amor, compartir los datos

–qué información contienen nuestras fotos, qué historias cuentan:

- Piensa si quieres compartir imágenes íntimas con tu rostro visible
- Intena cubrir rasgos corporales identificativos como tatuajes, marcas de nacimiento, etc.
- Utiliza editores Exif para borrar los metadatos y etiquetas de ubicación de tus fotos.
- Utiliza apps para poner tu cara, tatuajes y otros rosgos borroso (como Pixlr)

Apps y consideraciones básicas de seguridad

- Escoge una app que ofrece funciones de privacidad y seguridad como cifrado, borrar mensajes y bloqueo de capturas de pantalla
- Utiliza un servicio de mensajería seguro para que puedas tener control sobre las imágenes y mensajes que envías y puedas eliminarlos cuando quieras.
- *Indicación técnica: autodestrucción/desaparición* - utilizamos snapchat y otras apps que dicen "autodestruir/desaparecer mensajes automáticamente", pero muchas veces no las eliminan por completo y se puede todavía acceder a las imágenes para difundirlas después
- Establece una contraseña y cifra tu dispositivo
- Si es posible, aplica una contraseña a tus apps
- Considera utilizar una cuenta de correo independiente (que no utilizas para otra cosa) y segura, además de un número telefónico alternativo para hacer sexting
- Aprende cómo borrar y guardar
- Revisa si tu app está sincronizando datos y toma una decisión consciente si quieres hacer esto o no.

Actividades prácticas: Apps más seguras y edición de imágenes

Conversación sobre escoger apps

¿Qué apps utilizan para hacer sexting? ¿Por qué? ¿Qué consideraciones sobre seguridad tienes a la hora de escoger una app? ¿Qué funciones de seguridad te gustan de tu app? ¿Qué te preocupa?

Utiliza apps que:

- Permiten cifrar
- Se pueda establecer una contraseña de acceso
- Bloquea las capturas de pantalla
- Se puedan borrar los mensajes y archivos

Evaluando mensajes SMS y MMS. SMS y MMS no ofrecen estas características. Para más información sobre SMS, MMS y vigilancia, véase ¿Qué es un celular? ¿Cómo funciona la comunicación telefónica?

Actividades prácticas

Nota para facilitadoras: esta actividad es una oportunidad para las participantes poner en práctica estrategias de seguridad propuestas por facilitadoras/entrenadoras que han colaborado con FTX. Opta por las actividades que consideres más apropiadas para tu contexto. Otros temas a considerar:

- Cifrar dispositivos y establecer contraseñas
- Eliminar información identificatoria de nuestras fotos y celulares
- Crear una cuenta de correo independiente (que no utilizas para otra cosa) y segura, además de un número telefónico alternativo para hacer sexting

Comparte una lista de tareas con las participantes e invítalas a poner en práctica estos consejos en grupos pequeños, consultando entre ellas y utilizando internet para buscar información.

Practica con tus imágenes

- Prueba tomar fotos sin mostrar tu cara
- Intenta cubrir rasgos identificativos de tu cuerpo como tatuajes, marcas de nacimiento, etc.
- Utiliza editores Exif para borrar los metadatos y etiqueta sde ubicación de tus fotos.
- Utiliza apps para poner tu cara y tatuajes borrosos.

Practica con tus dispositivos y apps

- Escoge e instala una app más segura
- Establece una contraseña en tus apps
- Aprende a borrar y guardar historiales de chat
- Aprende a borrar imágenes de tu teléfono

Puesta en común - 10 minutos

¿Cómo te sentiste en esta actividad?

- ¿Qué te generó? ¿Cómo te impactó?
- Invita a las participantes a compartir lo que crearon en la sesión
- ¿Te resultó fácil, difícil? ¿Qué te sorprendió?
- ¿Dónde buscaste información cuando tenías alguna duda?

Materiales complementarios

Taller de Sexting de Luchadoras– diferentes momentos a la hora de hacer sexting - preliminares, durante, después... Almacenar y compartir. Consentimiento: cambios, negociaciones...

> **Nota de facilitación:** borrar imágenes de apps y dispositivos puede ser un poco más complicado ya que implica entender sobre almacenamiento y ubicación de carpetas y archivos. Aquí van algunas indicaciones más específicas (actualizado por última vez en Mayo 2019). En IoS (Mac), se complica aún más ya que no tienes acceso a los archivos fuera de la app que lo generó. También depende si tomaste las fotos directamente desde la app o utilizaste tu cámara y lo enviaste por la app.

En Telegram, pulsa la parte superior (encabezado) de la conversación. Te saldrá la opción de ver imágenes y videos. Aquí los puedes borrar de Telegram. Si los guardaste en otro lado de tu celular como tu galería, tendrás que ir allá para borrarlos también. En Telegram también puedes ver y navegar los archivos compartidos con usuarias y grupos. Todo esto aplica con respecto al dispositivo y archivos de la persona con la que hiciste sexting, es decir, no los borra de su dispositivo.

En Signal, pulsa la parte superior (encabezado) de la conversación. Verás miniaturas en Medios/archivos compartidos. Puedes borrarlos aquí. Al igual que Telegram, si los guardaste en otro lado de tu celular como tu galería, tendrás que ir allá para borrarlos también. Todo esto aplica con respecto al dispositivo y archivos de la persona con la que hiciste sexting, es decir, no los borra de su dispositivo.

En Android, utiliza el Navegador/gestor de archivos:

- Telegram: guarda archivos en el Almacenamiento interno. Busca la carpeta Telegram. Habrá subcarpetas para tipos de archivos.
- Signal: depende dónde lo guardaste. Puedes ver si está en: Almacenamiento Interno » Imágenes o Fotos

image-1605451879726.png
Image not found or type unknown