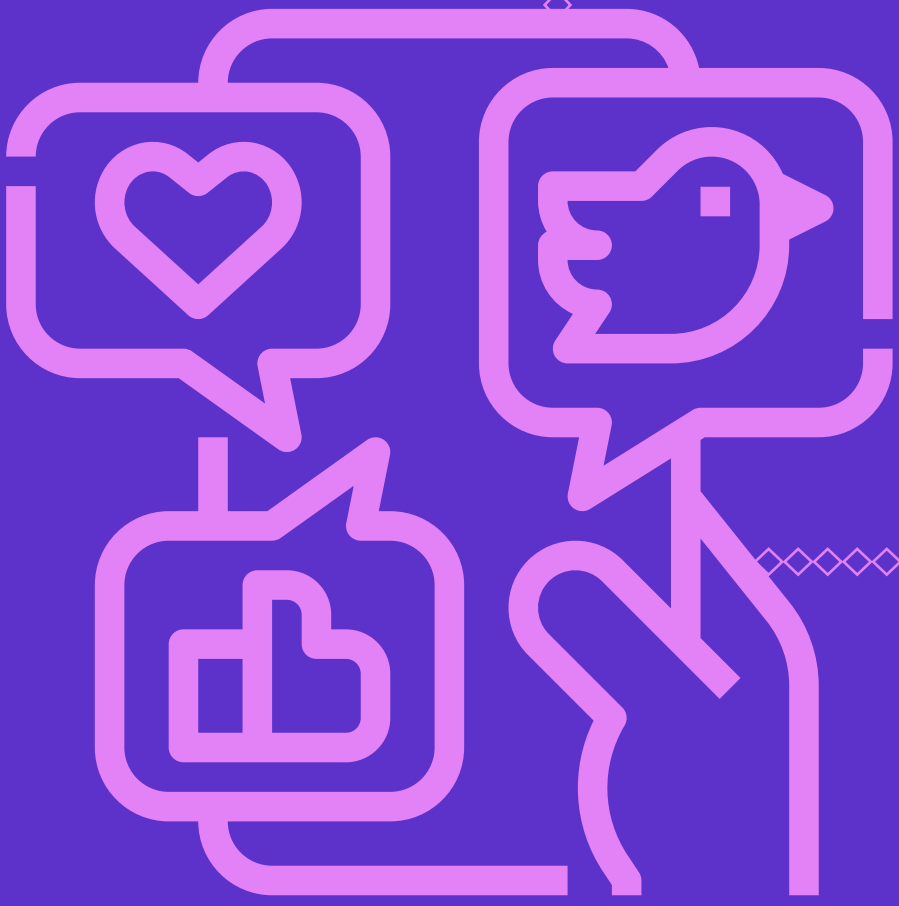
MANUAL

PRÁCTICAS Y HERRAMIENTAS DE CUIDADOS Y SEGURIDAD PARA LAS JUVENTUDES EN EL ESPACIO DIGITAL



RED LAC
JÓVENES POR LOS DERECHOS SEXUALES Y REPRODUCTIVOS

ÍNDICE

GLO

JA

RIO

MUNDO ANÁLOGO:

Espacio en el que estamos presentes en cuerpo e interactuamos de forma física y tangible.

ESPACIO DIGITAL:

Lugar generado a través de las tecnologías de la información, particularmente el Internet, donde la interacción es de forma virtual e instantánea a través de plataformas, dispositivos y redes sociales.

JUVENTUDES:

Grupo poblacional perteneciente al rango de 15 a 30 años de edad.

CIBERFEMINISMO:

Corriente feminista de pensamiento y acción que explora la relación entre las mujeres, Internet y las tecnologías.

AUTOCUIDADO DIGITAL:

Conjunto de técnicas, prácticas, acciones y herramientas que permiten a una persona tener un habitar más seguro dentro del espacio digital.

RESISTENCIA FEMINISTA:

Acciones que tienen el objetivo de hacer frente a la violencia machista y patriarcal con un enfoque de género, reivindicando el papel de la diversidad de mujeres en la sociedad.

SEGURIDAD DIGITAL:

Medidas que se toman para la navegación segura en el espacio digital. Esta incluye la protección de dispositivos, información, softwares y uso de Internet.

LGBTTTIQ+:

Lesbiana, Gay, Bisexual, Transgénero, Transexual, Travesti, Intersexual, Queer y otras personas de la diversidad sexual.

CIBERACTIVISMO:

Es la organización y acción colectiva en el espacio virtual que ve al internet como una herramienta política y crítica para posicionar temas específicos en la agenda pública, defender derechos humanos y generar movilizaciones.

DERECHOS DIGITALES:

Derechos digitales son los derechos existentes construidos a partir del espacio digital y de todas las interacciones que se generan en dichos espacios; Libertad de expresión, Censura, Acceso al Internet, etc.

VIOLENCIA DIGITAL:

La violencia digital son los actos perjudiciales ejercidos por la fuerza contra las personas, perpetuados a través de diferentes herramientas y plata-

PLATAFORMAS DIGITALES:

formas digitales, la mayoría de estas violencias no se entienden como delitos.

Las plataformas digitales se entienden como cualquier aplicación que utilizamos en nuestra navegación por Internet, pueden ser redes sociales, videojuegos, aplicaciones de comunicación y hasta navegadores.

INTRODUCCIÓN

A través del seguimiento a los Ciclos de Diálogo **“Juventudes y la reinvención del espacio digital”**, en el cual participaron diversas organizaciones de la región, expertas en el tema; así como por medio de un acercamiento teórico y desde la experiencia en la navegación en Internet, como personas usuarias de este espacio, nos dimos a la tarea de recopilar y construir nuevas estrategias para una navegación segura en diversas plataformas digitales. Estas prácticas y herramientas van desde lo digital, hasta lo análogo y legal, para poder construir un manual accesible para quienes consulten material en busca de asesoría o ayuda.

Este Manual nace de la necesidad urgente de reconocernos dentro de los espacios digitales que habitamos las juventudes. Para la Red Latinoamericana y Caribeña de Juventudes por los Derechos Sexuales y Reproductivos, es importante nombrar el espacio digital como una extensión de nuestras interacciones sociales y, por tanto, de las múltiples situaciones que podemos experimentar. Por eso, esperamos aportar y acompañarte para construir espacios digitales seguros.

Recuerda que cualquier situación de violencia jamás será tu culpa. Este manual está creado para ofrecerte una manera de autocuidado digital a través de herramientas que logran una navegación más segura en las diversas plataformas y dispositivos.

¡LO DIGITAL ES REAL!

DERECHOS DIGITALES

Desde 2011, la Organización de las Naciones Unidas reconoció el acceso a internet como un derecho humano básico. A nivel internacional y regional, existen distintos documentos que respaldan y reconocen nuestros derechos humanos que se relacionan con el acceso a internet, así como con un habitar seguro del mismo, tal como: la Declaración Universal de Derechos Humanos; Pacto Internacional de Derechos Civiles y Políticos; Pacto Internacional de Derechos Económicos, Sociales y Culturales; Derechos Humanos en Internet; Convención Belém Do Pará.

Aquí te mencionamos algunos de nuestros derechos digitales:

- ACCESO UNIVERSAL E IGUALITARIO
- LIBERTAD DE EXPRESIÓN Y OPINIÓN
- ACCESO A INFORMACIÓN
- PRIVACIDAD Y PROTECCIÓN DATOS
- IGUALDAD
- VIDA LIBRE DE VIOLENCIA
- ACCESO A LA JUSTICIA
- PARTICIPACIÓN EN LA VIDA PÚBLICA

CONTRASEÑAS SEGURAS

Las contraseñas seguras son una parte fundamental para el autocuidado digital, las contraseñas seguras son una buena práctica para la interacción y navegación por la web. Actualmente algunas plataformas digitales y navegadores brindan un almacenamiento de las contraseñas para facilitar el acceso, sin embargo, esto no siempre es buena idea la mayoría de las veces ya que las contraseñas pueden ser vulneradas muy fácilmente.

¿Cómo es una contraseña segura? Las contraseñas seguras constan de pasos muy específicos para su generación:

1. Uso de números, signos y letras al azar con datos que no sean públicos.
2. Contraseñas únicas para cada plataforma que lo solicite.
3. Renovar las contraseñas cada cierto tiempo
4. Evitar guardar las contraseñas para fácil acceso en páginas sin conexión segura o en redes sociales.

¿Cómo identificar una contraseña insegura? Enseguida te enseñamos algunos ejemplos para que evites usar este tipo de contraseñas:

- Nombre de mascota
- Banda favorita + tu cumpleaños
- Fechas de nacimiento, aniversario, etc.
- Cualquier información que hayas compartido en un cuestionario web, publicación o que socialices con más personas.

Importante: Evita usar datos de conocimiento público.

Herramientas:

- Gestiona todas tus contraseñas en un espacio seguro (PC: KeePass Password Safe)
- ¡Genera contraseñas seguras!
- ¿Cuánto tardarían en descifrar mi contraseña?

NAVEGACIÓN SEGURA

Cuando nos dedicamos a navegar por la web puede ser que pasemos por algunas situaciones que a largo plazo podrían generar algún riesgo para nuestra seguridad en la web, pero también para nuestros dispositivos, existen situaciones que pensamos son inofensivas ¡y es normal! Nadie nace siendo experto en Internet. A continuación, te mostraremos herramientas y prácticas que lograrán que la Internet sea un espacio seguro para ti.

- **NAVEGADORES Y BUSCADORES**

Imaginemos que el navegador es una caja con una cantidad inalcanzable de contenido, pero para acceder a este contenido necesitamos una llave. La caja es el navegador y la llave es el buscador. Muchos navegadores ya vienen con algún buscador predeterminado y no lo notamos, pero a veces es interesante ver que ventajas tienen unos sobre otros y cuales nos brindan mayor seguridad.

- Google
- Brave
- DuckDuck Go

- **CONEXIÓN SEGURA**

Cuando hablamos de conexión segura nos referimos al momento que sucede cuando das clic a la página que deseas, en ese momento la página se traslada a un servidor que es el que se encarga de mantener activa la página y puedas navegar sin ningún problema. Pero dentro de estas conexiones al instante tenemos que fijarnos claramente que al inicio de la página aparezca **https** esto te asegura que estás accediendo a una página con una conexión más privada y segura.

- **¡ME ESTÁN ESPIANDO!**

Seguramente en alguna ocasión estabas platicando con tus amistades sobre lo mucho que deseabas comprarte audífonos que viste con descuento y cuando entraste a ver memes ¡ya te salían publicaciones sobre esos audífonos! Pero mantén la calma, en realidad no están espiando solo obtienen la información que se guarda en tu dispositivo sobre los sitios que más visitas y en los que pasas más tiempo para después incluir más información que te gusta en algún algoritmo de alguna aplicación. Aquí te vamos a enseñar a disminuir ese contenido en tus redes sociales.

Herramientas:

- ¿Este sitio es seguro?
- ¡Usa siempre HTTPS! (solo en Google)
- ¿Ya conoces las apps que bloquean anuncios y ventanas sospechosas?

- **¿DIRECCIÓN IP?**

Imaginemos que tu casa es tu modem y así como tu casa tiene una dirección ¡también tiene una dirección tu modem!, pero esta se conforma únicamente de número, algo así: **192.168.255.255** o **192.168.0.0**, este conjunto de número es tu dirección IP. Pero, ¿para qué quiero saber mi dirección IP? A través de este conjunto de números, la empresa que te brinda el servicio puede monitorear tu navegación en Internet y por esto mismo en algunas ocasiones no puedes acceder a ciertas páginas web o contenido en la red, pero también ¡pueden rastrear nuestra navegación personas externas!

¡Quiero saber mi dirección IP!

- **¿Y CÓMO PUEDO OCULTAR MI NAVEGACIÓN?**

La VPN o Red Privada Virtual es una herramienta muy útil para tus dispositivos, al usar cualquier VPN podemos asegurarnos de tener una navegación casi anónima ya que es un túnel que nos conecta a otra red y nadie puede rastrear nuestra actividad en la red.

Herramientas:

- ProtonVPN (para dispositivos móviles y PC)
- Google
- Psiphon3
- RiseUP.net

CONTENIDO NO AUTORIZADO

En internet es muy fácil encontrar contenido no adecuado, este contenido puede ser violento, racista, machista y discriminatorio. Este contenido es controlado por las empresas dueñas de las plataformas digitales y que funciona de acuerdo a sus normas comunitarias de interacción dentro de las mismas. En algunas ocasiones, estas normas comunitarias funcionan también para censurar contenidos políticos a conveniencia de los gobiernos o de las mismas plataformas. Pero ¿qué pasa cuando aun así vemos contenido que no queremos o cuando censuran algo que nos interesa? Bueno, esto dependerá mucho de la plataforma en la que lo visualicemos así que te dejaremos unas herramientas para ciertas plataformas que no son 100% efectivas.

- **GOOGLE**

  - Retira información de Google
  - Retira pornografía falsa
  - Retira imágenes personales
  - Denuncia contenido por motivos legales

Para mayor información visita la página de La clika

- **FACEBOOK**

Programa piloto Nunca sin tu consentimiento es un programa que pretende reducir, o eliminar, el contenido publicado sin consentimiento,

este contenido incluye: fotos, vídeos o audios. El programa aún se encuentra en calidad de prueba, pero funciona de la siguiente manera solo en Facebook e Instagram:

- Es necesario que te pongas en contacto con las organizaciones que trabajan con Facebook para realizar el reporte, estas organizaciones te vincularán al programa si así lo solicitas.
- Enseguida te mandarán un formulario para que ingreses los siguientes datos: tu nombre, el enlace de tu perfil de Facebook, dirección de correo electrónica segura y cualquier información adicional.
- El equipo de Facebook te mandará un enlace de un solo uso para que ahí puedas subir el contenido que ha sido difundido.
- El contenido será cifrado para que cuando se comparta sea bloqueado inmediatamente.

• DENUNCIA MASIVA

- Si descubres que cierto contenido es difundido por algún perfil en Facebook (página, grupo o perfil personal) puedes pedir un reporte masivo.
- Pide a tus conocidos, o colectivos, que reporten la publicación como ... y si llegan a un número solicitado el contenido será eliminado automáticamente.
- ¡Cuantas más reacciones negativas tenga el contenido es probable que sea eliminado!

• POLICÍA CIBERNÉTICA – MÉXICO

A nivel federal en México, existe una institución gubernamental que se enfoca en la denuncia y atención de delitos que suceden en el espacio digital, esta institución algunas veces tiene las herramientas necesarias para bajar contenidos inmediatamente. Solo tienes que comunicarte a través de correo electrónico, página web, redes sociales o teléfono y anexar la siguiente información:

- Tipo de delito digital
- Pruebas (si es que existen), recuerda que pueden ser capturas de pantalla o videos, también sirven los enlaces de las publicaciones y perfiles de las personas.

Te invitamos a hacer una búsqueda rápida sobre si en tu país existe una institución similar, ya que esta puede ser una de las varias opciones de denunciar violencias en internet. Considera también que se trata de la policía, por lo que no sabemos con certeza si se respetan los Derechos Humanos en todo momento.

HUELLA DIGITAL

¿QUÉ INFORMACIÓN EXISTE SOBRE MÍ EN LA WEB?

Es necesario que de vez en cuando realicemos un mapeo digital sobre lo que hay en la red sobre ti, o como diríamos nosotras, un autodoxeo. Es como ponerte a buscar tu nombre en los buscadores de las redes sociales y navegadores para ver qué información aparece sobre ti y así poder estar al pendiente.

¡Crea una alerta en Google!

DISPOSITIVOS SEGUROS

Para que nuestros dispositivos sean seguros es importante conocer su funcionamiento general desde la configuración del mismo, ¡Navega en la configuración de tu dispositivo, puedes encontrar cosas increíbles!

- Recuerda siempre tener actualizado el Sistema Operativo de tus dispositivos para evitar cualquier falla en el sistema con respecto a la privacidad, la mayoría de los dispositivos se actualizan automáticamente o sólo te llega una notificación, pero por si las dudas ve a... Configuración > Sistema > Actualizaciones del sistema.
- No olvides usar una contraseña para tu dispositivo ya sea NIP, Huella dactilar, reconocimiento facial, patrón, etc. Así tu dispositivo y lo que contiene estará más seguro en casos de extravíos o robos.
- **¡Instala un antivirus!**
- Es importante que todas las descargas de archivos que realices en tus dispositivos sean desde espacios web seguros, es decir, que sean de una conexión segura y si son aplicaciones de las tiendas oficiales. En caso de que necesites descargar una app desde su archivo APK (son archivos que contienen la información de la aplicación fuera de la tienda oficial) procura que sea de confianza. **Si todo esto falla el antivirus te avisará a tiempo <3**

REDES DE APOYO

Es importante contar con redes de apoyo dentro y fuera de estos espacios digitales para tener una navegación más segura y cómoda en todos los sentidos. Con redes de apoyo externas nos referimos a tus amistades, comunidad, familia, etc., con quienes estás en constante comunicación y que te brinden la confianza y apoyo en caso de experimentar alguna situación desagradable.

- Habla con tu círculo de confianza sobre tu navegación en redes: ¿te molesta una publicación? ¿Te robaron tu celular? ¿Alguien te insultó? ¿Usaron tus fotos para otra cosa?
- Siempre platica sobre las emociones que sientes cuando navegas en redes sociales o en cualquier sitio web e identifica de dónde nace ese sentimiento para poder trabajarlo. **Te compartimos un insumo <3**

- **GRUPOS DE WHATSAPP, FACEBOOK O MESSENGER**

La creación de los grupos en estas plataformas digitales ha sido una parte fundamental de nuestra convivencia e interacción en espacios digitales. Estos grupos se crean a partir de intereses en común para compartir lecturas, para debatir, para conocer otras personas, para comprar artículos o incluso para hacer trueque, para hablar de tus emociones, etc. Pero también para estar cerca a tus amistades y familiares y poder divertirse a la distancia con una infinidad de stickers y emojis.

La importancia de este grupo nace cuando se crean con la intención de brindar apoyo a personas a la distancia, son grupos donde las mujeres nos avisamos de nuestra llegada a nuestras casas, donde compartimos nuestra ubicación para que otras puedan ir siguiéndonos, para auxiliarnos. Pero también para gestionar el intercambio de saberes colectivos y fomentar la economía local. Así que no lo dudes y ¡crea tu grupo con tus amistades!, puede ser una manera de construir redes de apoyo digitales.

CORREO ELECTRÓNICO

Una de las plataformas más usadas en el ámbito laboral y escolar es el correo electrónico y es que a veces pensamos que es imposible que estas plataformas sean inseguras, pero es donde sucede la mayoría de fraudes con información personal. Aquí te presentamos unos tips y herramientas para un uso adecuado de un email.

- Usa un correo para el ámbito laboral/escolar y otro para redes sociales, así evitarás spam excesivo en tu bandeja de entrada.
- Cuando quieras inscribirte a una plataforma de compra en línea, servicios de taxis, usa otro correo electrónico.
- Si navegas por una página que te pide el ingreso de un correo electrónico puedes usar una dirección anónima y temporal.
- ¡Navega por la configuración de tu correo electrónico!
- Activa la verificación en dos pasos así evitarás ingresar la contraseña en nuevos dispositivos.

• OTRAS OPCIONES

Existen otras opciones para correos electrónicos que no son de Gmail o Hotmail, estas opciones fueron creadas desde la experiencia de la persona usuaria y enfocado a la privacidad del mismo, brindando un doble candado de seguridad.

- Protonmail
- Disroot

FOTOGRAFÍAS E IMÁGENES

Cuando tomamos fotografías con nuestros dispositivos móviles, éstas guardan cierta información que puede vulnerarnos, entre los datos que guardan las fotos podemos encontrar: el modelo del dispositivo, fecha de registro, ubicación. Esta información se le conoce como metadatos, pero no pasa nada, los metadatos pueden ser eliminados con esta aplicación. Aunque la mayoría de las fotografías pierden esta información cuando son subidas a otras plataformas digitales pero no cuando se envían por correo. Si quieres permanecer en anonimato puedes intentar usar esa aplicación.

Para borrar rostros en fotografías que deseas subir a plataformas te recomendamos ObscuraCam, es recomendable cuidar las identidades de quienes salgan al fondo de tus fotografías sobre todo si son de protestas.

MENSAJERÍA INSTANTÁNEA

Y ¿QUÉ ONDA CON LA MENSAJERÍA INSTANTÁNEA SEGURA?

WHATSAPP. Esta plataforma de mensajería instantánea es, sin duda, la más popular y utilizada a nivel mundial.

Aquí debajo enlistamos algunas de sus características:

- Fue comprada por Facebook en 2014, por lo que pertenece a esta empresa y los datos que recopila son compartidos con esta.
- Cuenta con cifrado de extremo a extremo: una especie de candado por el que solo el emisor y receptor del mensaje pueden acceder a él. Asegura que ni esta aplicación, ni Facebook puedan saber o acceder al contenido de tus mensajes.
- Dentro de sus Políticas de Privacidad, la plataforma menciona que, además de recopilar información relacionada al nombre, número de teléfono y lista de contactos, también recopila datos sobre el tiempo y/o rendimiento en la plataforma, marca y modelo del dispositivo, tipo de conexión que se usa, ubicación (tú puedes controlarla) y cookies. Política de Privacidad de Whatsapp.

Sin embargo, al explorar las configuraciones de seguridad, puedes hacer que tu experiencia en esta plataforma sea más segura y benéfica para tu privacidad. Aquí abajo te contamos cómo:

- Accede a Configuración/Ajustes (Android en los tres puntos del extremo superior derechos, Apple en el extremo inferior derecho) y selecciona la opción de “Cuenta”.
- Al entrar a esta opción te aparecerá otra lista de opciones y entre estas están: “Privacidad” “Seguridad” “Verificación en dos pasos” y “Bloqueo de pantalla/con huella dactilar”. Son las que necesitas para configurar tu celular con mayor seguridad y privacidad, según tu preferencia.
- En “Privacidad” podrás configurar quién puede visualizar tu última conexión, foto de perfil, información, quién puede añadirte a grupos y quién puede ver tus estados/historias. Aquí mismo puedes ver y editar tu lista de contactos bloqueados, activar o desactivar confirmaciones de lectura (palomitas azules), verificar si estás compartiendo tu ubicación en tiempo real y, también, aquí podrás seleccionar si deseas que el acceso a tus chats WhatsApp sea utilizando tu huella dactilar o reconocimiento facial.
- En “Seguridad” la plataforma te ofrece una descripción de cómo están protegidos tus mensajes y te da la opción de activar recibir notificaciones si este código cifrado cambia. Cada chat tiene su código personal cifrado y puedes siempre verificarlo con el receptor de tus mensajes para confirmar esta función.
- En la opción de “Verificación en dos pasos” puedes activar un PIN (numérico) que se te solicitará siempre que registres tu número de teléfono en WhatsApp, ya sea en un nuevo dispositivo o por reinstalación de la App, dando mayor seguridad a tu cuenta.
- De igual forma, desde la configuración de tu dispositivo móvil, en la sección de aplicaciones, puede controlar a qué tiene acceso la aplicación, como a fotos, ubicación, cámara, micrófono y, también, puedes controlar como se muestran las notificaciones de esta.

SIGNAL. Esta aplicación de mensajería instantánea es una de las menos usadas y conocidas por la persona usuaria, sin embargo, su popularidad está en ascendencia por sus interesantes medidas de seguridad y poca o nula recopilación de datos.

Aquí te platicamos algunas de sus características:

- Es una aplicación de código abierto, esto quiere decir que es de libre acceso, por lo que el usuario es libre de manipular ese software y, por lo tanto, una vez obtenido puede ser usado, estudiado, cambiado y redistribuido libremente. Esto permite adaptarse a las necesidades de la persona usuaria.
- Al igual que Whatsapp, Signal está cifrado de extremo a extremo, por lo que solo tú y persona que recibe tus mensajes conocen el contenido de estos.
- La única información que esta aplicación recopila y guarda es cuánto tiempo lleva instalada la aplicación y última fecha en la que se instaló. por lo que no recopila ni tu nombre, contactos, ni la imagen que usas en tu cuenta.
- A partir de una nueva actualización, la plataforma ya cuenta con una opción de “difuminar rostros” antes de enviar una imagen, por lo que esto va un paso más allá en la seguridad y privacidad de las personas usuarias.

A pesar de ya ser una plataforma segura y con respeto a la privacidad, aquí te dejamos algunas configuraciones que puedes activar para hacer tu experiencia en esta plataforma más segura y privada:

- Al entrar a la aplicación y dar click en tu foto de perfil, que aparece en el extremo superior izquierdo, se despliega el menú de configuraciones. Las opciones que necesitas para una experiencia más segura son: “Cuenta”, “Notificaciones” y “Privacidad”.
- Al comenzar a usar Signal, la propia aplicación te va a pedir generar un PIN (numérico). Este se te será solicitado aleatoriamente al usar la aplicación con el fin de verificar tu identidad. En la sección de “Cuenta” puedes cambiar este PIN, activar o desactivar los recordatorios para verificar tu identidad o desactivarlo por completo (no recomendable). Asimismo, puedes activar el “Bloqueo de registro” que al volver a registrar tu número en Signal, este PIN te será solicitado como un tipo de verificación en dos pasos.
- En el apartado de “Notificaciones” podrás seleccionar qué contenido de tus mensajes se muestra al llegar una notificación a tu celular. Con el fin de obtener la mayor seguridad, se recomienda aplicar la opción de ni remitente ni contenido, con el fin de que al llegar una notificación no se pueda saber nada más al respecto hasta abrir la aplicación.
- En la sección de “Privacidad” podrás bloquear personas que no deseas que te escriban o llamen; puedes activar o desactivar las notificaciones de lectura e indicador de tecleo de mensaje; puedes activar una función para que tus mensajes desaparezcan en un tiempo de tu preferencia; se puede activar una función para bloquear la pantalla después de cierto tiempo y para el desbloqueo te solicitara tu huella o reconocimiento facial (los ya registrados en tu teléfono).
- Asimismo, podrás activar una función llamada “Remitente confidencial”, esta permite que ningún servidor identifique quién envía el mensaje y solo tengo información sobre el destino/receptor de este.

Desde el año pasado, con las movilizaciones sociales por el asesinato de George Floyd, Signal comenzó a popularizarse entre jóvenxs para la organización y movilización social. Al ser una de las aplicaciones más seguras para mensajería instantánea, es ideal para el uso de organizaciones y colectivos que defienden derechos humanos ya sea desde el espacio digital o el mundo análogo.

TELEGRAM. Es una aplicación de código abierto que se desarrolló enfocándose en la seguridad y privacidad de las y los usuarios. Su interfaz es muy accesible y el manejo de ella este diseño para tener una navegación adecuada.

Aquí te platicamos algunas de sus características:

- Si decides crear una cuenta en Telegram puedes ocultar tu número y usar únicamente un usuario.
- La app cuenta con cifrado end to end, no dejan rastros en los servidores de Telegram, permiten la autodestrucción de mensajes y no admiten el reenvío de los mismos.
- Los chats funcionan de manera similar a Whatsapp, puedes enviar notas de voz, fotografías y archivos que son más pesados que los que normalmente se envían por Whatsapp ¡puedes enviar libros completos en PDF!
    - Existe la opción de crear chats secretos en los cuales puedes bloquear las capturas de pantalla y programar una autodestrucción de mensajes. Esta opción te brinda una seguridad y privacidad más amplia que WhatsApp
- Los canales en Telegram funcionan para la divulgación de noticias y avisos de temas de interés, es como un grupo de chat pero sin tener que recibir mensajes de los demás integrantes. Estos canales son increíblemente amplios en cuanto a la cantidad de personas usuarias que pueden pertenecer.
- Los grupos tienen funciones muy similares a los de WhatsApp, pero tiene ciertas herramientas para facilitar la comunicación entre los integrantes ya que puedes colocar avisos, realizar encuestas, incluso si agregas a alguien después de la creación del mismo puedes decidir si puede ver los mensajes anteriores. Los grupos también pueden ser muy amplios y más seguros que los de WhatsApp por las configuraciones de la misma app que permiten un uso más anónimo e imposible de rastrear.
- Existen canales y grupos en donde la difusión de contenido es ilimitada y sin censura, tristemente es un arma de doble filo. Este contenido puede ser desde películas, aplicaciones, textos, artículos, libros hasta imágenes íntimas.

Entre estas configuraciones de privacidad y seguridad de quienes deciden usar Telegram también podemos ubicar la verificación en dos pasos, la eliminación de la cuenta.

- Para la verificación en dos pasos en Telegram tienes la opción de establecer una contraseña de acceso y poder volver a abrir tu cuenta en cualquier otro dispositivo, sin embargo, si no haces un respaldo con un correo electrónico y olvidas la contraseña puedes perderla totalmente. Para poder volver a abrir la cuenta sin contraseña se tiene que restaurar desde el inicio y tarda 7 días.
- Puedes conectarte en cualquier momento a una conexión más segura a través de algún proxy específico.
- La aplicación puedes bloquearla con NIP, huella dactilar o contraseña.

¡TRANSFORMEMOS LAS REDES SOCIALES EN ESPACIOS SEGUROS!

INSTAGRAM

Más allá de ser una egoteca y álbum de recuerdos, se ha convertido en una plataforma que, debido al dinamismo de sus herramientas y número de usuarios, permite a las personas difundir información, ejercer el periodismo y generar nuevas formas de activismo o ciberactivismo a través de la creación de contenido multimedia.

Derivado de lo anterior, nos interesa que puedas continuar con un uso seguro de esta plataforma por lo que aquí te damos algunos tips:

- Activa la autenticación de dos pasos.
- Para un perfil personal, se recomienda activar la opción cuenta privada, esto te permite controlar quién te sigue y ve tu contenido. Si bien, para un perfil de organización o colectiva no conviene tener una cuenta privada, el resto de las opciones te pueden ayudar a mejorar la experiencia en la plataforma.
- Para las configuraciones de privacidad y seguridad haz lo siguiente: 1) ve a la página de tu perfil (donde están tus publicaciones) Da click en las 3 líneas en el extremo superior derecho selecciona “Configuración” ubica las opciones de “Privacidad” y “Seguridad”.
- En Privacidad, podrás configurar:
    - Comentarios: aquí puedes elegir quién puede comentar tus publicaciones (todos, personas que sigues y te siguen, personas que sigues, tus seguidores). Asimismo, puedes bloquear los comentarios de personas usuarias específicas. También, te permite generar filtros a comentarios, ocultando comentarios específicos que sean considerados ofensivos. Aquí podrás activar un filtro manual que te permite ocultar comentarios con palabras o frases que tú especifiques.
    - Publicaciones: puedes decidir ocultar el número de likes y visualizaciones, así como activar una función para aprobar las publicaciones en las que te etiquetan y definir quién puede etiquetarte en publicaciones (todos, personas que sigues, nadie).
    - Menciones: aquí puedes configurar quién puede hacer menciones de tu cuenta/nombre de usuario (todos, personas que sigues, nadie).
    - Historias: Aquí puedes controlar quién ve tus historias, así como quién puede interactuar con ellas.
    - En este apartado también podrás bloquear, restringir o silenciar una cuenta o nombre de usuario incómoda, grosera o no deseada.
- En Seguridad podrás realizar lo siguiente:
    - Cambiar contraseña
    - Revisar tu actividad de inicio de sesión: aquí puedes checar desde que ubicación has iniciado sesión, de no reconocer alguna, cierra inmediatamente esa sesión y cambia la contraseña. Se recomienda que solo una persona por colectiva u organización tenga acceso a la cuenta con el fin de evitar que muchas personas conozcan los accesos.
    - Activación de la autenticación en dos pasos: esta puede ser por mensaje de texto, se te hará llegar un número a la opción seleccionada e Instagram te lo solicitará para confirmar tu identidad.

Recurso: Seguridad Básica para Instagram

TIK TOK

Es la plataforma del momento. Su variedad de contenidos, así como sus herramientas para crearlos fácilmente ha hecho que millones de personas se unan a esta plataforma. Sus contenidos van desde la comedia, la sátira, hasta el activismo, defensa de derechos humanos, denuncia e, incluso, la publicación de noticias.

Si ya eres parte de esta plataforma, o tienes pensado unirte o posicionar a tu colectiva en esta, aquí te damos consejos para garantizar una experiencia más segura.

- Para iniciar una configuración más segura, posiciónate en la página principal de tu perfil y da click en los tres puntos en el extremo superior derecho. Una vez aquí, se te desplegarán varias opciones, identifica las siguientes: “Privacidad”, “Seguridad”, “Desintoxicación Digital”, “Centro de Seguridad”.
- En Privacidad, tendrás la oportunidad de configurar lo siguiente:
    - Si deseas tener una cuenta privada o pública. Tik Tok tiene la opción de elegir quién puede ver cada uno de tus videos de forma individual, así puedes tener un perfil público y compartir ciertos vídeos con un público exclusivo.
    - Controlar cómo se presenta tu cuenta en la plataforma
    - Cómo otras personas interactúan con tus contenidos: si permites que se descarguen o no (lo ideal es que se seleccione que no), puedes controlar quién comenta tus videos, así como aplicar filtros a estos de forma general a comentarios ofensivos o de forma personalizada con palabras clave.
    - Personalización del contenido y datos:
    - Permitir o no a anunciantes usar tus videos en sus anuncios externos.
    - Puedes seleccionar quién puede contactarte por este medio (tus amigos, todos o nadie).
    - Aquí puedes observar la lista de cuentas que tengas bloqueadas.
- En la opción de seguridad, puedes realizar lo siguiente:
    - Podrás verificar si tiene alertas de seguridad sobre el uso de tu cuenta.
    - Revisar en qué dispositivos está activa tu cuenta o está iniciada tu sesión.
    - Administrar las aplicaciones que tienen acceso a tus datos de Tik Tok.
    - Puedes activar la verificación de 2 pasos, donde puedes escoger que se te envíe un código de verificación a tu correo electrónico o celular (SMS).
- En el apartado de Desintoxicación Digital puedes gestionar el tiempo que pasas en Tik Tok y una vez que se cumpla se bloquea la aplicación, obligándote a desconectarte un rato. Asimismo, puedes restringir contenido que puede ser inapropiado. Si consideras que algún video es inapropiado, haz el reporte correspondiente.
- En la opción de Centro de Seguridad tendrás acceso a información y guías generadas por la plataforma para su uso seguro.

FACEBOOK

- Configuración y Privacidad: Seguridad
  - Seguridad e Inicios de Sesión
    - Comprueba la configuración de seguridad importante es una opción importante para saber qué tan segura es tu cuenta y que te falta por activar: Contraseña segura, Alertas de inicio de sesión y Autenticación en dos pasos.
    - Inicios de sesión: Revisa los inicios de sesión, es decir, dónde está abierta tu cuenta de Facebook, te aparecerá una ubicación aproximada, el dispositivo y la fecha de ingreso. Puedes eliminar en cualquier momento el dispositivo que ya no uses o no reconozcas.
    - Autenticación en dos pasos: te recomendamos activar esta opción desde un Mensaje de Texto y no desde una aplicación.
    - ¡Recibe alertas de inicios de sesión no reconocidos!
    - Advertencias si intentas acceder a un sitio web peligroso desde Facebook.
    - ¿Intentos de hackeos? Facebook te da la opción para darle seguimiento a estos casos a través de unas sencillas respuestas.
  - Apps y sitios web
    - Revisa las aplicaciones y sitios web externos que tienen acceso a tu cuenta de Facebook o que están vinculados, puedes eliminar en cualquier momento el permiso y desvincular tu cuenta.
- Controla el acceso de tu contenido a personas usuarias de Facebook a través de los controles de privacidad que ofrece esta plataforma: Bloqueos, Ocultar estados e historias, Reconocimiento Facial, Perfil y Etiquetado.

TWITTER

- Configuración y Privacidad
  - En el apartado de Cuenta vamos a encontrar algunas opciones que nos permiten mejorar la privacidad de nuestra cuenta:
    - **Contraseña**

      Recuerda que la contraseña tiene que cumplir con los requisitos de una contraseña segura que mencionamos al inicio del manual.
    - **Seguridad**
      - Autentificación en dos pasos: esta opción nos ofrece un acceso remoto a través de un código de verificación, el código llega como mensaje de texto y si iniciamos sesión en otro dispositivo nos pedirá ese código. Te recomendamos no elegir la opción de acceder a través de otra aplicación.
      - Restablecimiento de contraseña: para poder restablecer tu contraseña se te pedirá la confirmación de tu correo electrónico o número de teléfono. Esta herramienta brinda un nivel más alto de seguridad.
    - **Tus datos de Twitter:** en este apartado vamos a encontrar información útil para saber qué datos contiene nuestra cuenta de twitter: historial de acceso de la cuenta, lugares donde estuviste, aplicaciones que tienen acceso a tu cuenta, inicios de sesión, cuentas bloqueadas, incluso los anuncios que te aparecen en tu inicio. Esta información es útil para realizar un mapeo digital cada cierto tiempo y estar al tanto del nivel de seguridad que tiene nuestra cuenta.
    - **Desactivar tu cuenta:** ¿te cansaste de entrar a Twitter? ¿te han estado acosando en esta plataforma? Esta es una buena opción para retirarte el tiempo que creas necesario de esta plataforma. Siempre es buena idea darse un descanso de cualquier red social.
  - En el apartado de Privacidad y Seguridad existen ciertas herramientas para aumentar la privacidad de tu cuenta:
    - Protege tus tweets: puedes hacer que tu cuenta sea privada con esta opción, solo tu decides quien puede ver tus tweets.
    - Etiquetado de fotos: decide si pueden etiquetarte en contenido multimedia o no.
    - Mensajes Directos, la aplicación nos ofrece ciertas opciones para hacer más privada la comunicación a través de los mensajes que recibimos: Recibir solicitudes de mensajes de cualquier usuario o no recibirlos, mostrar confirmaciones de lectura o no mostrarlas.
    - Visibilidad y contacto, también podemos decidir cómo nos pueden buscar en Twitter: ¿Permitir que otros te encuentren por tu correo electrónico? ¿Permitir que otros te encuentren por tu número de teléfono? ¿Sincronizar contactos de tu directorio?
    - Mostrar fotos y videos que puedan incluir contenido delicado
    - Marcar el contenido multimedia que twitteas para indicar que podría incluir material delicado.
    - Cuentas bloqueadas y silenciadas.
    - Palabras silenciadas: ¡puedes seleccionar qué palabras omitir de tu inicio en Twitter!

- Ubicación: decide si tener activa tu ubicación o no.
- Personalización y datos: en esta opción la aplicación de permite controlar el modo en que personaliza contenido y como recolecta y comparte ciertos datos:
  - Anuncios personalizados: estos anuncios dependen de tu actividad en Twitter, y fuera de Twitter.
  - Personalizar según tu identidad inferida: esta opción es muy interesante ya que Twitter puede obtener datos de acuerdo a tu navegación, es decir, puede relacionar tus intereses desde el uso de cierto dispositivo, el tipo de correo electrónico, el navegador que usaste.
  - Personalizar según los lugares donde estuviste: si activas esta función Twitter te mostrará anuncios o información relacionada a los lugares en donde iniciaste sesión.

TIPS BÁSICOS

TIPS BÁSICOS PARA APLICACIONES SEGURAS

PERMISOS DE ACCESO

- Revisa los permisos de acceso que tiene cada aplicación en tu dispositivo: Configuración > Aplicaciones > Permisos, en esta opción vas a encontrar los permisos que les asignamos a cada aplicación como la ubicación, la cámara, el micrófono, contactos, etc. Pero la verdad es que no todas las aplicaciones usan estos permisos.
- Si usas Facebook pero jamás subes historias puedes desactivar el micrófono y cámara, y así con cada aplicación.
- Las aplicaciones siguen funcionando de manera correcta aun cuando no tengan todos los permisos.
- Eliminar algunos permisos evitará la publicidad en tus cuentas y posibles fallas en tu privacidad.

VERIFICACIÓN EN DOS PASOS

La verificación o autenticación es una herramienta buenísima para controlar el acceso a tus aplicaciones o redes sociales. La mayoría de las aplicaciones de comunicación o compras en línea tienen esta opción.

- Ingresa a la aplicación: Configuración > Seguridad y Privacidad > busca la opción de verificación en dos pasos y ¡actívala!
- Esta herramienta permite que tu acceso sea más rápido y seguro en otros dispositivos, es decir, si deseas ingresar a

tu Gmail desde una PC y tienes activada esta herramienta te solicitará el acceso a tu dispositivo seguro (como tu celular) y solo si lo aceptas puedes ingresar.

MAPEO DIGITAL

El mapeo digital es similar al que proponemos en el apartado de la huella digital, pero nos referimos básicamente a un chequeo cada cierto tiempo en nuestras redes sociales y verificar si hay algo raro en nuestros contactos, en nuestros inicios de sesión, etc.

- Agrega y acepta solo a personas conocidas
- Haz chequeo mensual en tus seguidores y amistades y elimina o bloquea cuentas raras (que no tengan fotos, que no conozcas, que tengan contenido que no te guste, etc.)
- Procura tener tu contenido en la configuración privada o solo para amistades.
- Revisa quienes miran tus historias en Instagram y elimina a quienes no te hagan sentir segura.

IMPORTANTE: ¡No abras enlaces que recibes a tus bandejas! Pueden ser virus.

RECONOCIENDO LOS TIPOS DE VIOLENCIA EN EL ESPACIO DIGITAL

El espacio digital es una extensión del mundo análogo y, por ende, en este espacio también se reproducen violencias que pueden llegan a afectar y conmocionar nuestra salud emocional, mental, psicológica y física. En este sentido, resulta fundamental que aprendamos a reconocer y nombrar los tipos de violencia a los que nos podemos enfrentar al habitar y ser usuarias constantes del espacio digital, para así saber cómo reaccionar ante estas.

Para ayudarte con este reconocimiento, aquí debajo enlistamos los tipos más comunes de violencia que podemos experimentar dentro del mundo digital.

Es importante destacar que las mujeres y niñas, así como personas de la comunidad LGBTTTIQ+, personas racializadas, y personas con neurodivergencias y/o discapacidad, se encuentran mucho más expuestas a sufrir cualquier tipo de violencia tanto en el espacio digital como en el análogo. Aunado a lo anterior, las periodistas, defensoras de derechos humanos y activistas se encuentran doblemente expuestas a estas agresiones por su labor y género.

Asimismo, esta sección te ofrece tips sobre acciones que puedes llevar a cabo ante los distintos tipos de violencias que puedes experimentar. Es importante destacar que vivir, experimentar o ser víctima de alguna de las violencias mencionadas jamás será tu culpa. Tener a tu disposición herramientas y conocer y reconocer buenas prácticas siempre te ayudará a disminuir el riesgo de sufrirlas y a actuar de forma informada en caso de experimentar alguna de una de estas.

- **VIOLENCIA DE GÉNERO**

De acuerdo con ONU Mujeres, la violencia de género se refiere a los actos dañinos dirigidos contra una persona o un grupo de personas en razón de su género. Tiene su origen en la desigualdad de género, el abuso de poder y la existencia de normas dañinas. El término se utiliza principalmente para subrayar el hecho de que las diferencias estructurales de poder basadas en el género colocan a las mujeres y niñas en situación de riesgo frente a múltiples formas de violencia.

- **Violencia de género digital:** Actos de violencia cometidos instigados o agravados por razones de género a través del uso de las TICs, redes sociales y/o correo electrónico.

TIP 1

Genera redes entre amistades y con colectivas feministas presentes en el espacio digital, que permitan que al ser víctima de esta violencia puedas activar estas redes y saber que no estás sola.

TIP 2

Si experimentas este tipo de violencia documenta la agresión, así como todos los datos que te sea posible de la persona agresora. Reporta la publicación donde se manifiesta esta agresión e incluso el perfil. Pide la ayuda de tu comunidad y redes para que te apoyen con el reporte. Si lo consideras necesario, puedes hacer una publicación para advertir al resto de las usuarias que esta persona tiene conductas inadecuadas y agresivas. Acércate a colectivas y organizaciones feministas para acompañamiento y asesoría, siempre recuerda que ¡No estás sola!

- **HACKEO**

Ataques no autorizados que tienen el fin de acceder a las cuentas o dispositivos de otras personas. Esto puede implicar la recopilación no autorizada de información, el bloqueo o desactivación de la cuenta de la persona víctima, así como la utilización de la cuenta hackeada para ejercer comportamientos que generen desprestigio o desacreditación de la persona titular de la cuenta.

TIP 1

Utiliza frases de acceso con el uso intercalado de minúsculas, mayúsculas y números (alfanuméricas) y procura cambiarlas con frecuencia. Evita utilizar la misma contraseña para todas tus plataformas y no las compartas con nadie, si es necesario que lo hagas procura que sea por canales seguros y a personas de confianza.

TIP 2

Al darte cuenta de algún hackeo cambia todas las contraseñas de tus plataformas digitales (correo electrónico, redes sociales, aplicaciones bancarias, etc.). Haz saber a tus amistades que fuiste víctima de un hackeo y realiza una evaluación de daños ¿A qué información tuvieron acceso? ¿Qué daños provocaron? ¿Está relacionado con mi activismo o labor de defensa?

- **DIFUSIÓN DE IMÁGENES ÍNTIMAS O INFORMACIÓN PRIVADA**

Compartir o publicar sin consentimiento cualquier tipo de información, datos, contenidos multimedia o detalles privados relacionados a una persona. En algunas ocasiones, la persona agresora es una ex-pareja sentimental o sexual.

TIP 1

Cuando envías imágenes íntimas siempre procura ponerles una marca distintiva, ya sea una frase, un sticker, un dibujo, una marca de agua, que te permita reconocer a quién le mandaste esa imagen en particular. Si así lo deseas, evita enviar fotos donde se vea tu rostro o alguna cosa que permita que te reconozcan. Procura nunca enviar estas imágenes cuando tengas conexión a una red de Wi-Fi pública y evita almacenarlas en una nube.

TIP 2

Si tus imágenes íntimas son difundidas toma captura de pantalla a la publicación o publicaciones donde se muestren. Haz la denuncia de las publicaciones con las imágenes y pide a tus amistades que hagan lo mismo, cada plataforma digital ofrece distintas opciones para esto. Si la plataforma no cuenta con la opción de denuncia por difusión de contenido íntimo, puedes reportar la imagen por pornografía o desnudez, por Privacidad o por derechos de autor. De igual forma, algunos países cuentan con leyes que te protegen ante este tipo de violencia digital. Véase

• RECEPCIÓN DE MATERIALES SEXUALES NO SOLICITADOS

Cuando una persona hace llegar imágenes y/o videos sexuales, de forma anónima o no, sin que la otra persona los haya solicitado, deseado o consensuado. En esta categoría entra la famosa recepción de “dick pics”.

TIP

Si recibes un pack no solicitado, lo primero que debes hacer es tomar captura de pantalla de este material, de preferencia toma una captura donde se aprecie el nombre, usuario o teléfono celular de la persona que hizo el envío de este material. Asimismo, toma captura de pantalla del perfil de esta persona e intenta rescatar la mayor cantidad de datos que puedas o que esté disponible sobre esta persona usuaria, así como el URL del perfil. Si lo consideras necesario, puedes publicar en tus redes el nombre de la cuenta, perfil o teléfono de la persona que te mando los contenidos

• CREACIÓN DE PERFILES FALSOS O ROBO DE IDENTIDAD

Uso o falsificación de la identidad de una persona sin su consentimiento, así como la creación y divulgación de datos personales falsos, con la intención de dañar la imagen de una persona u organización. A través de la falsificación de la identidad se crean perfiles falsos en redes sociales para, usualmente, llevar a cabo acciones que dañen la reputación de la persona suplantada.

TIP 1

Procura mantener tus perfiles privados y limita el acceso a la información que publicas a tu lista de amigos. Asimismo, procura no tener, aceptar o incluir a personas desconocidas en tu lista de seguidores, conexiones o amigos.

TIP 2

En cuanto identifiques que hay un perfil falso utilizando tu información e identidad, puedes utilizar las herramientas que las plataformas digitales ofrecen para denunciar el perfil. En Facebook está la opción de “Buscar ayuda o reportar perfil”. En Instagram y Twitter, al ingresar a un perfil puedes “Reportar” (en Instagram) o “Denunciar” (en Twitter). Solicita el apoyo de tus amistades para hacer las denuncias o reportes de estos perfiles falsos.

• ACOSO (CYBERBULLYING)

Actos repetidos y no solicitados contra una persona u organización que son percibidos como intrusivos, amenazadores e intimidantes. Recepción constante de mensajes con tono ofensivo o descalificante.

TIP 1

Es recomendable mantener un balance entre lo público y privado y procurar tener una cuenta de uso personal y una por separado para uso profesional.

TIP 2

Mantén la calma y evita reaccionar de forma impulsiva ante estos ataques. Si así lo deseas, puedes responder a la persona agresora haciéndole saber que su comportamiento es incómodo y violento. Denuncia públicamente estas agresiones y reporta el perfil en la plataforma correspondiente. Pide a tu red de amistades que hagan lo mismo. Si este acoso es persistente, pide ayuda y acompañamiento, hay colectivas y organizaciones que te pueden ayudar.

• VIGILANCIA O MONITOREO

Acecho constante de las actividades en línea de una persona, su vida diaria, o información, sea pública o privada. Asimismo, puede darse a través del uso de spyware (software para espiar y obtener información de otros dispositivos) o acceso a cuentas sin consentimiento o a través del uso de GPS u otros servicios de geolocalización para rastreo de ubicación y movimientos.

TIP 1

Si te das cuenta o sospechas que alguien puede estar monitoreando virtualmente busca ayuda para identificar cómo pueden estar intervenidos tus dispositivos y qué soluciones existen. Una primera reacción podría ser la restauración completa del dispositivo, así como un cambio en las contraseñas y ajustes de privacidad de todas tus plataformas. Si consideras que se relaciona con tu labor de activismo o defensa haz saber a tu organización, redes y amistades de esta situación.

TIP 2

No debes limitar el contenido que desees compartir en este espacio, pero sí vigilar quién puede acceder a él. Por otra parte, el monitoreo se puede dar de forma más sofisticada a través de software (o malware) especializado. Para evitar esto, se recomienda el uso de antivirus y una Red Privada Virtual o VPN, que protegerá tu actividad en línea de todos los que quieran verla (hay opciones gratuitas).

• DISCURSO DE ODIO

De acuerdo con el Tribunal Europeo de Derechos Humanos, se define como cualquier forma de expresión que propague, incite, promueva o justifique el odio racial, la xenofobia, el antisemitismo o cualquier otro odio basado en la intolerancia, incluyendo la intolerancia expresada en nacionalismo agresivo o etnocentrismo, discriminación u hostilidad contra las minorías, las personas migrantes y personas de origen inmigrante.

TIP 1

El empoderamiento de la diversidad ya sea de raza, étnica, sexual, de género y más puede ayudar a mitigar los efectos contra los grupos más vulnerados por este. Promover comunidades y espacios seguros es fundamental para acabar con este discurso en el espacio digital.

TIP 2

Siempre documenta estos comportamientos (sobre todo porque muchas personas pueden llegar a borrar el contenido violento si se viraliza). La creación de nuevas narrativas desde el espacio digital puede crear contramovimientos que tundan estos comentarios llenos de odio.

• PHISHING

Es la pesca de datos a través de emails, o mensajes a través de redes sociales o servicios de mensajería instantánea que aparentan ser de un servicio real y te piden dar click a un link que te invita a proveer información sensible y/o personal, como datos bancarios, dirección de domicilio, contraseña y más.

TIP 1

Si diste click a este link y compartiste datos y después desconfiaste de esto, comunícate inmediatamente con el proveedor de servicios por el que se hicieron pasar y pregúntales cómo puedes proceder ante esto.

TIP 2

Desconfía de todos los mensajes que te soliciten información privada. Muchas veces estos agresores se hacen pasar por cuentas de servicios que más utilizamos (como puede ser tu banco, alguna plataforma digital como Uber, Rappi o DiDi, servicios de Apple o Android, entre muchos otros) y te hacen creer que, debido a algún problema, un posible hackeo o para confirmar tu identidad, debes compartirles información privada. De igual forma, te pueden hacer llegar un mensaje indicándote que ganaste algo y debes hacer click a un link para reclamarlo

• AMENAZAS

Contenidos violentos, lascivos o agresivos que manifiestan una intención de daño a alguien, a sus seres queridos o bienes.

TIP 1

Si estás siendo amenazada/o, documenta la amenaza, así como la información que puedas de la persona agresora y guarda todo en un usb. Procede con el reporte del perfil y comentario y solicita el apoyo de tu comunidad para hacer lo mismo. Si consideras que esta amenaza puede ir más allá del espacio digital y manifestarse en el mundo análogo, busca ayuda de las autoridades correspondientes o conéctate con alguna colectiva u organización que pueda darte acompañamiento y asesoría.

TIP 2

Las personas activistas, periodistas o defensoras de DDHH son más vulnerables ante estas ya que, derivado de su labor, pueden incomodar o molestar a grupos de poder específicos o, simplemente a personas que no coinciden con su labor. Una recomendación para protegerte de amenazas es evitar compartir demasiada información privada desde el perfil de activismo o defensa y tener las configuraciones de privacidad adecuadas.

• CAMPAÑAS DE DESPRESTIGIO (O ATAQUES COORDINADOS)

Descalificación de la trayectoria, credibilidad o imagen pública de una persona en específico a través de la exposición de información falsa, manipulada o fuera de contexto. Usualmente se dan de manera coordinada y participa más de una persona en los ataques.

TIP 1

En muchas ocasiones, para activistas y personas defensoras de derechos humanos, este ocurre cuando se tocan intereses de particulares, sobre todo de grupos de poder. Se recomienda evitar compartir información privada en los perfiles públicos o tener dos cuentas, una para uso privado y otra para uso personal. Asimismo, la creación de redes entre colectivos activistas y/o personas defensoras son fundamentales para contrarrestar los comentarios negativos derivados de estas campañas.

TIP 2

Si estás siendo víctima de una campaña de desprestigio, identifica qué esfera de tu vida están buscando afectar (laboral, privada, sexual, relaciones, etc). Puedes hacer una declaración pública de la falsedad de los comentarios parte de esta campaña y activar tu comunidad digital, redes de apoyo y de amistades para generar una contranarrativa positiva. Documenta los comentarios y busca encontrar la fuente inicial de este ataque, reúne los datos que necesites y archivarlos de manera segura por si gustas proceder por la vía legal.

• CENSURA

Tácticas o acciones para tirar y dejar fuera de circulación canales de comunicación o expresión de una persona o un grupo. Asimismo, pueden ser acciones que tengan el fin de controlar o suprimir determinados contenidos en internet.

TIP 1

Genera redes y alianzas estratégicas con otras personas defensoras o activistas que te apoyen a ti y tu trabajo en caso de ser censurado en alguna o múltiples plataformas. Estas redes son fundamentales para evitar que la información censurada se pierda y tu labor se vea afectada.

TIP 2

Si estás siendo censurada/o, activa tus redes de apoyo para manifestar inconformidad e informar de lo sucedido y para que continúen difundiendo la información que te puso en esta situación y no se limite el conocimiento de esta. Busca nuevos canales para que sigas expresándote y ejerciendo tu labor.

TIP 3

Es importante que conozcas y te familiarices con las políticas de seguridad y convivencia de las plataformas que usas.

• DESINFORMACIÓN

Difusión de información falsa de manera intencional que tiene el objetivo de causar un daño al confundir o engañar a la población en general. A menudo se utiliza para incitar al odio y/o violencia.

TIP 1

Nunca confíes completamente en lo que lees o ves en internet o las redes sociales. Es importante que antes de compartir, dar retweet o subir alguna información a una plataforma, confirmes el contenido con más de una fuente y verifiques su contexto. Por lo general, las noticias falsas o engañosas contienen información que busca una reacción emocional muy fuerte y, por lo general, nunca realiza citas de su fuente de información.

TIP 2

Si identificas que se está compartiendo información o noticias falsas, denuncia la publicación que la contiene. Si te interesa, puedes compartir datos, cifras, información u otras noticias de fuentes fidedignas que comprueben que la información de esa publicación es falsa o engañosa. Asimismo, la desinformación se combate compartiendo plataformas de fuentes abiertas que permitan a las personas acceder a mayor y diversa información.

COVIOLENCIAS

LA PANDEMIA Y EL AUMENTO EN LA VIOLENCIA DE GÉNERO

Durante el confinamiento por la pandemia, la tecnología y el Internet jugaron un papel preponderante para que algunas personas pudieran continuar con sus actividades cotidianas de forma virtual. Sin embargo, esta situación acentúo múltiples brechas en el acceso a internet por razones de género, raza y/o nivel socioeconómico. En la región de **América Latina se ha experimentado un alza en las violencias de género,** particularmente en lo siguiente:

- Violencia doméstica - Se limitaron las herramientas para el acceso al apoyo, atención y acompañamiento.
- Falta de acceso e información, particularmente sobre salud sexual y reproductiva.
- Agresiones digitales contra organizaciones, activistas y personas defensoras de derechos humanos que apoyan víctimas de violencia de género (suplantación de identidad, la exposición de datos personales, amenazas y reportes o denuncias a sus publicaciones en redes sociales).
- Vulneración de la libertad de expresión de activistas, feministas, grupos LGBTTTIQ+.
- En México el Observatorio Ciudadano Nacional del Feminicidio ofrece algunas herramientas para realizar denuncias en tiempos de covid.
- Durante la pandemia covid-19 las protestas sociales tomaron los espacios digitales a través del uso de hashtag, transmisiones en vivo, divulgación de problemáticas en infografías, convocatorias a nivel regional para poner en tendencia algún tema, incluso muchas campañas de change.org tomaron mayor fuerza.
- No cabe duda que el aumento del uso de las plataformas digitales y/o dispositivos durante esta pandemia creció a la par de las violencias digitales y por lo tanto usuarios y usuarias de Internet se vieron en la necesidad de crear redes de apoyo y empezar a generar herramientas para el autocuidado digital. Estas redes de apoyo han sido fundamentales para enfrentar la violencia digital.

Ante esto, es fundamental continuar generando redes de apoyo y resistencia feminista para proteger a las víctimas, pero también a las personas defensoras de derechos humanos y activistas que enfrentan agresiones racistas, misóginas y patriarcales en América Latina.

Más información: Otros Datos - Covid-19 y Violencia de Género; Mujeres buscan salir de la violencia durante el Covid-19; Covid-19 y la Violencia de Género en América Latina

RECOMENDACIONES GENERALES

RECOMENDACIONES GENERALES DE CUIDADO DIGITAL ANTE VIOLENCIAS

Conoce las configuraciones de privacidad de tus redes sociales para adecuarlas a tus necesidades.

Evita tener personas desconocidas en tu lista de contactos o seguidores. Tener un control sobre quién ve y tiene acceso a tu contenido te ayudará a evitar compartir información con personas no deseadas.

¡Genera una comunidad digital! Ya sea entre tus amistades, familiares, colegas, activistas, feministas u organizaciones, esto ayudará a contar con una red de apoyo y acompañamiento en caso de experimentar alguna violencia.

Utiliza contraseñas fuertes, de preferencias frases de acceso alfanuméricas.

Familiarízate con las plataformas que utilizas, conoce todas las herramientas que ofrecen, sus términos y condiciones a detalle, así como la dinámica grupal de las mismas.

Documenta con capturas de pantalla, videos o fotografías las agresiones que experimentes e identifica a las personas usuarias que las lleva a cabo. Guarda el URL del perfil de la persona agresora.

Si lo consideras necesario, solicita el apoyo de organizaciones o colectivas que brinden primeros auxilios digitales.

Como activista, persona defensora o periodista procura compartir lo menos posible información sobre tu vida privada o privacidad en las redes que utilizas para tu labor.

Protege todos tus dispositivos con antivirus y utiliza una VPN al navegar por internet.

TIPOS DE CIBER-AGRESORES

- **ACTORES ESTATALES – los únicos que pueden violar derechos humanos.**

Estos son las y los funcionarios públicos de cualquier nivel de gobierno, tal como la policía, diputados, senadores, presidentes, etc. Las agresiones que cometan pueden ser denunciadas ante los órganos de control interno y las comisiones de derechos humanos estatales o federales/nacionales. Igual estas violaciones pueden proceder a instancias internacionales.

- **ENTES PRIVADOS – pueden vulnerar derechos humanos básicos, pero sus agresiones son consideradas delitos.**

Todas las personas que no tienen un cargo de servicio público caen en esta categoría. Estas pueden ser desde personas individuales hasta grupos de personas pertenecientes a una organización en específico. Asimismo, pueden ser personas creadoras de malware o programas destinados a afectar nuestro habitar en internet. Por lo general muchas de las violencias que son ejecutadas por personas conocidas vienen de parte de familiares, parejas y amistades.

  - Personas (anónimas o conocidas)
  - Empresas
  - Organizaciones

CONSECUENCIAS DE LA VIOLENCIA

CONSECUENCIAS DE LA VIOLENCIA EN LÍNEA

Lo digital es real, por lo que experimentar violencia digital puede causar daños o afectaciones severas en nuestro bienestar físico y psicoemocional. Estas violencias atraviesan la cuerpa y pueden afectar nuestro bienestar biopsicoemocional. Algunos de los efectos de estas violencias pueden ser:

- Afectaciones psicoemocionales (Estrés, angustia, enojo, miedo, impotencia, frustración, depresión, paranoia, cansancio y confusión)
- Autocensura
- Síndrome de Burnout: estado de agotamiento físico, mental y emocional causado por el cansancio psíquico o estrés relacionado al trabajo o ejercicio de una labor.
- Afectaciones físicas en la cuerpa (Sudoración, dolor de distintas partes del cuerpo (cabeza, espalda, estómago), pérdida o exceso de apetito, tensión, llanto, angustia)
- Ansiedad
- Afectaciones a la autoestima
- Abandono del uso de las tecnologías
- Aislamiento social

Ante estas violencias, las redes de apoyo y tu comunidad resultan fundamentales para hacerles frente y para que podamos recibir el apoyo y ayuda que necesitemos, sobre todo si se desea proceder con alguna denuncia. Recuerda que ¡Nunca estás sola!

- **¿QUÉ HAGO SI ALGUIEN QUE CONOZCO ESTÁ SUFRIENDO ALGÚN TIPO DE VIOLENCIA?**

    - Acércate a la persona y trata de reconocer el tipo de violencia que está viviendo.
    - ¡Haz contención emocional! Platica con esta persona sobre sus emociones y sus intenciones sobre lo que esté viviendo: si decide denunciar, si siente miedo a volver a usar redes sociales, si necesita asesoría psicológica o simplemente necesita un espacio de escucha.
    - Construye redes de apoyo con otras personas cercanas a esta persona, estas redes de apoyo sirven para hacer listas de bloqueos y para mediar y contener los posibles ataques en alguna red social.
    - Acompaña con mucha paciencia, amor y cariño. Es necesario entender que cuando alguien sufre algún tipo de violencia tiene diferentes maneras de actuar y sucede lo mismo en espacios digitales, por lo tanto no podemos obligar a una persona a hablar sobre lo ocurrido ni forzar ese momento, solo nos queda escuchar y abrazar en todo el proceso que se viene.
    - Es importante que no hagamos menos la violencia digital y no victimicemos a la persona. La violencia digital es real y tiene efectos emocionales, jamás será la culpa de la persona que está pasando por esta situación.

LEYES QUE NOS PROTEGEN

- **LEY OLIMPIA - MÉXICO**

La ley Olimpia es un conjunto de reformas existentes en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y el Código Penal Federal que entró en vigor en México el 1 de junio del 2021, por lo tanto, la Ley Olimpia trabaja únicamente con delitos cibernéticos de índole sexual, es decir, difusión de contenido íntimo sin consentimiento, sextorsión, impulsado por el Frente Nacional por la Sororidad y Defensoras Digitales.

Denuncia aquí.

- **DECRETO LEGISLATIVO N° 1410 - PERÚ**

En septiembre de 2018, en Perú, se promulgó el decreto legislativo N° 1410 que modificó el Código Penal para incorporar los el acoso sexual y chantaje sexual, así como la difusión de imágenes, materiales audiovisuales o audios con contenido sexual. Esta modificación busca garantizar una lucha eficaz contra las diversas modalidades de violencia que afectan principalmente a las mujeres a lo largo de todo su ciclo de vida.

Decreto Legislativo N°1410

Conoce más sobre este tema en: Hiperderecho - Después de la Ley.

- **LEY 26.388 Y LEY 25.326 - ARGENTINA**

Si bien en Argentina no existe como tal una ley que sancione la violencia de género digital, a través de la Ley 26.388 (Delitos Informáticos) y la Ley 25.326 (Protección de Datos Personales) te protegen contra ciertos tipos de violencias que puedes experimentar en el espacio digital. En particular, estas leyes pueden ser aplicadas para la difusión sin consentimiento de material íntimo. Aquí en los links te dejamos más información.

Publicación de imágenes íntimas sin consentimiento

Ley de Delitos Informáticos

Ley de Protección de Datos Personales

- **LEY DE VIOLENCIA DIGITAL - ECUADOR**

También conocida como Ley para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad, es una Ley que se encuentra en proceso de aprobación en Ecuador. Si bien, esta Ley busca proteger a mujeres y niñas contra la violencia digital, algunas de sus disposiciones han sido criticadas por considerar que estas pueden afectar la libertad de expresión, sobre todo aquella ejercida por periodistas, personas defensoras de derechos humanos y activistas.

Información sobre el proyecto de Ley

Noticias sobre Ley de Violencia Digital

Human Rights Watch - Ley de Violencia Digital

REPERTORIO DE HERRAMIENTAS

REPERTORIO DE HERRAMIENTAS DE SEGURIDAD, CUIDADO Y AUTOCUIDADO DIGITALES

- Declaración de Principios para habitar el espacio digital. ONG Amaranta (Chile) Declaración de Principios - Amaranta
- Proyecto Aurora iniciativa de ONG Amaranta (Chile) para la autodefensa digital a las mujeres Instagram; Facebook & Twitter
- Navegando Libres (Ecuador) es un programa que busca visibilizar, acompañar y mitigar la violencia de género que se da en el ámbito digital, https://www.navegandolibres.org/. Ejemplo de un recurso: Ciclo de Violencia de Género Digital
- Hiperderecho (Perú) - Guía de Autocuidado y Sororidad para la defensa del derecho a decidir. Hiperderecho cuenta con muchas más herramientas que puedes consultar ¡No dejes de revisarlas! Publicaciones - Hiperderecho
- Vita Activa (México) es una línea de ayuda y un laboratorio de soluciones. Proveen servicios uno a uno, disponibles por diversos canales para dar primeros auxilios psicológicos y digitales https://vita-activa.org/ Contacto Vita Activa: Whatsapp/Telegram/Signal +52 (1) 55-8171-1117 y en **apoyo@vita-activa.org**
- LATFEM (Argentina): Kit de cuidados digitales para periodistas feministas - LatFemSocial TIC (México) - serie de herramientas digitales que abarcan temas sobre: uso de datos, infoactivismo, seguridad y privacidad y sobre recursos abiertos. https://socialtic.org/herramientas/
- Sursiendo (México) Cuidados Digitales

- Sursiendo (México) - Registro y análisis de seguridad digital
- Infórmate y conoce los delitos informáticos con la información que provee Justia: https://mexico.justia.com/derecho-penal/delitos-informaticos/
- La iniciativa Libres en Línea provee un apartado con materiales para promover la autodefensa feminista en el espacio digital. http://www.libresenlinea.mx/autodefensa/
- PantallaAmigas (España) - Decálogo para el Sexting Seguro
- Colectivo Mecha (Chile) - Acuerdos sobre consentimiento y cómo explorarnos íntimamente a través de lo digital en https://colectivamecha.org
- Malvestida (México) - Guía Práctica: ¿Qué hacer si publican mis nudes?
- Luchadoras (México) comparte un set de herramientas que te pueden ayudar a hacer frente a la violencia digital: Herramientas - Internet Feminista- Luchadoras
- Acoso.Online - brinda orientación a víctimas cuyas imágenes íntimas fueron publicadas sin su consentimiento - https://acoso.online/mx/
- Facebook: No sin tu consentimiento. Asimismo, en el centro de seguridad de Facebook, podrás encontrar recomendaciones para un uso más seguro de esta plataforma: https://www.facebook.com/safety
- **Antivirus gratuitos:**
    - avast!: http://www.avast.com/en-za/index
    - Spybot: http://www.safer-networking.org
- Security in-a-box ofrece herramientas y técnicas para la seguridad digital: https://securityinabox.org/es
- Salama- herramienta permite hacer una autoevaluación para conocer el nivel de riesgo al que una persona se enfrenta al ejercer su labor como periodista o persona defensora de derechos humanos https://salama.io/#/
- Umbrella es una aplicación gratuita que ofrece guías y manuales de seguridad personalizados para periodistas y personas defensoras. https://secfirst.org/umbrella/
- La Electronic Frontier Foundation (Estados Unidos) ofrece diversos consejos y herramientas para una navegación web más segura: https://www.eff.org/pages/tools

- Artículo 19: Seguridad Digital - Artículo 19
- SIEMPRE VIVA, una metodología colaborativa para generar materiales de apoyo que ayuden a comunicar y reforzar la seguridad digital en comunidades de activistas, comunicadores y personas defensoras de derechos humanos: Ciber herbolaria y medicinas ancestrales para la seguridad digital
- Consorcio Oaxaca (México): Herramientas de autocuidado y sanación
- Corporación Sisma Mujeres y Fondo Acción Urgente (Colombia) lideraron la creación de: Autoprotección integral para mujeres defensoras de derechos humanos.
- Colnodo (Colombia) presenta un Kit de seguridad digital para la protección y el cuidado de la información en Internet.
- Calalá Fondo de Mujeres (España): Autocuidado emocional, físico y digital en tiempos de pandemia
- La organización Tedic (Paraguay) - recomendaciones para el cuidado de la salud mental y prácticas para cuidados digitales en tiempos de Covid-19: https://www.tedic.org/salud-mental-covid19/
- La organización Karisma (Colombia) Genios de Internet guía que te ayuda a mejorar tu seguridad en línea.
- La oficina del Alto Comisionado para los Derechos Humanos de Naciones Unidas presenta un compilado: Herramientas de seguridad digital
- Gender and Tech Resources pone a nuestra disposición el Manual Zen y el arte de que la tecnología trabaje para ti: Manual Completo de Gender and Tech Resources
- PEN America - Manual contra el acoso en línea
- Para talleres de seguridad digital contáctate al siguiente correo: **cyberpinkcolectivo@gmail.com**
- Cápsula sobre Autocuidado y Contención Emocional
- Cápsula sobre autocuidado: Depresión y duelo
- Cápsula sobre: Seguridad Digital y Redes para Periodistas
- Cápsula sobre: Seguridad y Autoprotección
- Kit de primeros auxilios digitales: https://digitalfirstaid.org/es/

CONCLUSIONES

Las TICs han permitido desarrollar nuevos espacios que nos permiten ejercer nuestros derechos, tal como la libre expresión, la libertad de opinión, la libertad de asociación pacífica, así como el libre desarrollo de nuestra personalidad. El espacio más importante que ha surgido de estas TICs, probablemente, es el digital. Este espacio virtual, ha permitido que algunas juventudes encontremos o construyamos lugares donde podemos comunicarnos instantáneamente, expresar nuestros posicionamientos frente a temas de agenda pública, organizarnos y movilizarnos. Sin embargo, el espacio digital también es un lugar donde se reproducen lógicas machistas, androcéntricas y patriarcales que perpetúan sistemas de discriminación y violencia estructural. En este sentido, es necesario que nosotras, nosotres y nosotros aprendamos a identificar y nombrar las violencias que se pueden experimentar en este espacio y encontrar la forma de resistirlas y enfrentarlas desde lo individual y lo colectivo.

Por otra parte, para los Estados y gobernantes, el espacio digital continúa siendo un desafío. La inmensidad del mundo virtual sigue superando todos los esfuerzos e intentos de políticas públicas que permitan su regulación democrática, basada en el respeto a los derechos humanos. A pesar de conocer y saber la violencia que se puede llegar a experimentar en el espacio digital, pocas han sido las acciones por parte de los Estados para lograr proteger a su población usuaria de Internet. Aunado a lo anterior, a pesar de que el acceso a internet es reconocido internacionalmente como un derecho humano, los estados han fallado en lograr un acceso universal e igualitario para su ciudadanía.

Finalmente, agradecemos a todas las organizaciones y colectivas que formaron parte del proyecto “Juventudes y la reinvención del espacio digital”: ONG Amaranta, Artículo 19, Ciberseguras, Cyberpink, Fundación Acceso, Hiperderecho, Latfem, Luchadoras, Sursiendo y Vita Activa. A través de estas colaboraciones se generan redes y conexiones para la resistencia antipatriarcal y feminista, para el combate conjunto de la violencia machista y para la construcción de espacios seguros en lo digital. Acompañarnos y apoyarnos es el primer paso para lograr una incidencia y un habitar más seguro del espacio digital.

¡ANTE VIOLENCIA MACHISTA, RESISTENCIA FEMINISTA!

- Hiperderecho

FUENTES

¿Qué es la autenticación en dos pasos y cómo funciona en Instagram? (s.f). Servicio de Ayuda de Instagram. Recuperado de: https://www.facebook.com/help/instagram/566810106808145

¿Qué es la violencia digital? (s.f). Internet Feminista. Luchadoras. Recuperado de: https://luchadoras.mx/internetfeminista/violencia-digital/

Artículo 19. (2015). Discurso de Odio. Recuperado de: https://www.article19.org/wp-content/uploads/2020/03/ARTICLE-19-Manual-sobre-el-%E2%80%98Discurso-de-Odio%E2%80%99.pdf

Boris Miranda. (14 de enero de 2021). WhatsApp, Signal y Telegram: en qué se diferencian y cuál ofrece más privacidad. BBC News Mundo. Recuperado de: https://www.bbc.com/mundo/noticias-55656428

Derechos Digitales (10 de julio de 2020). La otra pandemia: internet y violencia de género en América Latina. Recuperado de: https://www.derechosdigitales.org/14716/la-otra-pandemia-internet-y-violencia-de-genero-en-america-latina/

La violencia digital. (s.f). TEDIC. Recuperado de: https://violenciadigital.tedic.org/

Moxie Marlinspike. (5 de junio de 2020). Looking back at how Signal works, as the world moves forward. Signal Blog. Recuperado de: https://signal.org/blog/looking-back-as-the-world-moves-forward/

ProVoces. (2020). Manual Para la Elaboración de Protocolos de Seguridad. USAID México. Recuperado de: https://drive.google.com/file/d/1KS7WNuSIBZoqKUU5c126jMOX__KKxZwt/view?usp=sharing

Tips for Staying Safe on Instagram. (6 de junio de 2017). Blog de Instagram. Recuperado de: https://about.instagram.com/blog/tips-and-tricks/privacy-and-safety-tips-for-instagram

RED LAC

FUNDACIÓN Acceso

ARTICLE 19

Ciberseguras

LUCHADORAS

Luchiendo Comunicación Cultura Digital

AMARANTA

HIPER DERE CHO

CyberFLINK

VITA