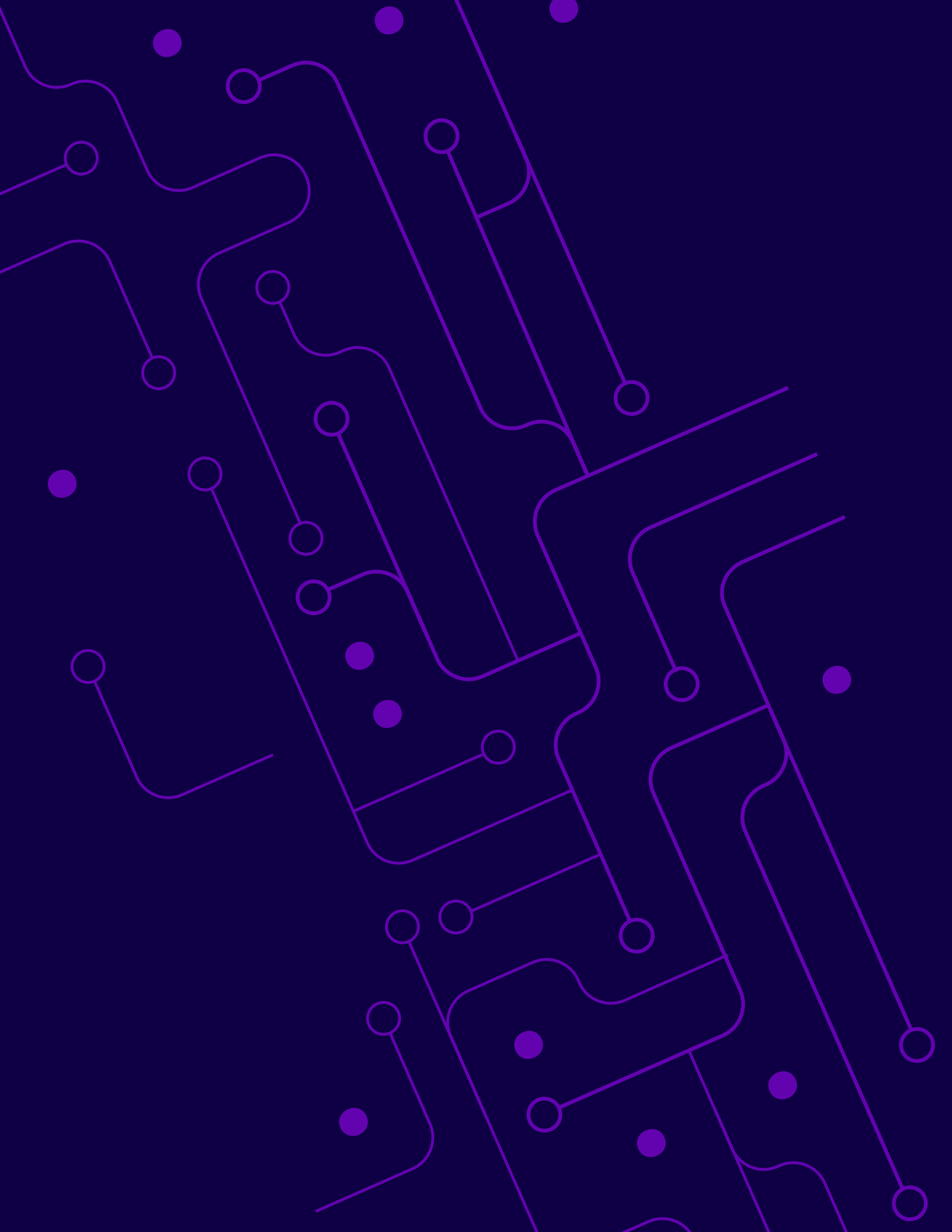
Protocolo de Ciudadanía y Seguridad Digital

SEPTIEMBRE 2025

fcam
FONDO CENTROAMERICANO DE MUJERES
FOUNDATION

Fundación
OXLAJUJ N'OJ



Dirección de Investigación
Andrea Lourdes López Véliz

Especialista en Violencia Digital
Angie Contreras

Comité de Guardias Digitales:
Andrea Velásquez
Leila Chún
Génesis López
Belinda Chá
Kleimy Summer Prera
Hermelinda Velásquez
Madelyne Hernández

Primera Edición

Ilustración de portada, maquetación y diseño:
Andrea González

Fundación Oxlajuj N'oj

con el apoyo de:

Fondo Centroamericano de Mujeres Foundation

Correo electrónico:
Fundacionoxlajujnoj@gmail.com

Guatemala, Fraijanes 2025

ÍNDICE

01 INTRODUCCIÓN

En los últimos años, el entorno digital se ha convertido en un espacio hostil para las mujeres que ven en esta herramienta una extensión de sus activismos, luchas y trabajos. Las violencias que las mujeres —jóvenes de diversas identidades y contextos, indígenas, afrodescendientes, con discapacidad, periodistas, políticas y defensoras— enfrentan en lo digital son múltiples y complejas. No solo afectan sus cuerpos digitales: estas violencias traspasan la pantalla e impactan su seguridad, bienestar emocional, físico y laboral, limitando su autonomía y su derecho a participar libremente en la vida pública así como articular otros activismos, debido a las consecuencias de la violencia o trauma posterior. Así, la violencia digital amplifica las desigualdades estructurales y refuerza los mecanismos de exclusión que históricamente han intentado silenciar a las mujeres.

La investigación "Cuerpos y voces vigiladas: violencia de género facilitada por la tecnología en la esfera pública" identificó la violencia de género facilitada por la tecnología (VGFT) como un mecanismo de control, de disciplinamiento y como un mecanismo de desarticulación de organizaciones colectivas pacíficas y que amenazan con crear fisuras en las estructuras del sistema social hacia las mujeres que ocupan espacios de liderazgo, comunicación y toma de decisiones. Este estudio visibilizó cinco formas de VGFT recurrentes que atraviesan los testimonios de activistas, políticas y periodistas:

- **1. Discurso de odio:** ataques sistemáticos y misóginos dirigidos a deslegitimar la voz de las mujeres por su identidad, apariencia, discapacidad, orientación sexual u origen étnico. A través de insultos cargados de racismo y LGBTfobia, se busca erosionar su credibilidad, destruir su autoestima y desmotivar su lucha o causa creando una violencia instrumental: "se lo hago a una, para que veas lo que te puede pasar si continuas con esto.." y ahí es donde las consecuencias no se limitan a lo individual o privado, sino a lo público y colectivo que se desea gestar para crear una verdadera transformación, , generando miedo y autocensura.
- **2. Ciberturba:** ataques coordinados desde múltiples cuentas —reales o falsas— que operan como campañas de desprestigio masivo, con el fin de silenciar y expulsar a las mujeres de los espacios digitales y de debate público.
- **3. Desinformación y difamación:** manipulación de imágenes, videos o narrativas para desacreditar la reputación y trayectoria de mujeres en la esfera política o mediática, alimentando rumores que escalan a acoso y amenazas.

- **4. Doxing:** exposición no consentida de información personal —direcciones, teléfonos, placas de vehículos o datos familiares— como forma de intimidación y control, que incrementa los riesgos físicos y emocionales.
- **5. Amenazas violentas:** mensajes directos con advertencias de daño físico o feminicidio, utilizados para sembrar terror y expulsarlas de la participación pública.

Estos hallazgos confirman que la VGFT no es un fenómeno aislado, sino una estrategia sistemática para limitar la voz y la incidencia de las mujeres en la esfera digital y política. Al igual que en los espacios físicos, las mujeres que se expresan, lideran o desafían el poder son castigadas por salirse de los roles de género impuestos en la sociedad con violencia que puede ir desde lo psicológico, emocional, económico, físico, sexual y digital. Las consecuencias de estos ataques son profundas: aislamiento, autocensura, ansiedad, y la renuncia a participar activamente en espacios de incidencia.

Ante este panorama, este proyecto surge como respuesta a la pregunta colectiva: ¿qué hacemos ante la VGFT? La falta de un protocolo específico y de herramientas de prevención y acompañamiento ha dejado a las mujeres en un estado de vulnerabilidad y dependencia, donde su autonomía y participación se ven comprometidas.

Para asegurar un enfoque representativo e inclusivo, el Protocolo de Ciudadanía y Seguridad Digital fue elaborado tras amplios procesos de conversación, reflexión colectiva y el desarrollo de un diagnóstico en los departamentos de Guatemala, Baja Verapaz, Quetzaltenango y Chimaltenango, territorios seleccionados por su diversidad y por el trabajo previo que Fundación Oxlajuj N'oj ha impulsado en ellos.

Este protocolo busca ser una ruta práctica y accesible que brinde a las mujeres que participan en la política, que ocupan cargos en el servicio público o de elección popular pero también a periodistas, activistas y a todas las escuchan y brindan acompañamiento en casos de VGFT, información, herramientas y acciones concretas para su protección, acompañamiento y seguridad, fortaleciendo sus derechos digitales y su ciudadanía plena en entornos virtuales.

Te invitamos a apropiarte, compartir y viralizar este protocolo, que es de todas y para todas, con la convicción de que el espacio digital también debe ser un territorio libre de violencia.

02 Metodología

Para llegar a construir el Protocolo de Ciudadanía y Seguridad Digital recorrimos un largo camino resultado de la investigación-acción participativa, exploratoria y descriptiva Prevención de la Violencia de Género Facilitada por la Tecnología contra Mujeres Jóvenes en la Política desde un Enfoque Interseccional y del diálogo con las participantes del Comité de Guardias Digitales.

El protocolo es parte de un proyecto más amplio que surgió de varios incidentes de hostigamiento digital documentados entre 2022 y 2023 y que evidenciaba la creciente amenaza que representa la violencia de género facilitada por la tecnología (VGFT) contra mujeres jóvenes que participan en la política y la vida pública en Guatemala, en estos casos, las redes sociales y otras plataformas digitales se han utilizado para deslegitimar y socavar el trabajo de defensoras de derechos humanos y figuras políticas femeninas, afectando incluso procesos judiciales y la formación de casos legales en su contra por actores de poder.

El proyecto se enfocó en mujeres jóvenes de diversas identidades y contextos, incluyendo a aquellas que se identifican como indígenas, afrodescendientes, LGBTIQ+, y mujeres rurales, quienes enfrentan múltiples capas de discriminación y violencia, tanto en entornos físicos como virtuales.

Además, la investigación evidenció que la falta de un protocolo específico y herramientas de prevención para enfrentar la VGFT deja a las mujeres en un estado de vulnerabilidad y dependencia, donde su autonomía y participación se ven comprometidas. Por lo que se recomendó crear y elaborar un protocolo de seguridad y ciudadanía digital dirigido a mujeres, funcionarias, líderes, activistas y organizaciones de la sociedad civil.

Para llegar a este protocolo fue importante la participación activa del Comité de Acompañamiento denominado “Guardias Digitales”, un espacio de articulación y liderazgo, conformado por 12 mujeres jóvenes involucradas en la política y la vida pública, incluyendo representantes de 7 organizaciones de sociedad civil (OSC), personas individuales y funcionarias de la Secretaría Presidencial de la Mujer.

Las Guardias Digitales asumieron diversas actividades clave para la investigación, asesoramiento estratégico, revisión y validación de los contenidos y materiales utilizados en las actividades, promoción y difusión de las iniciativas del proyecto.

El 21 de diciembre de 2024 se llevó a cabo la primera validación con el Comité Guardianas Digitales, la segunda validación, tuvo como objetivo principal garantizar la pertinencia y claridad de los instrumentos de investigación diseñados para el estudio sobre Violencia de Género Facilitada por la Tecnología (VGFT).

Además para esta investigación-acción participativa, exploratoria y descriptiva, se llevaron a cabo 6 entrevistas individuales semiestructuradas con mujeres jóvenes entre los 19 y 34 años que participan en política y en la vida pública, con el objetivo de profundizar en sus experiencias de VGFT y se realizó la Encuesta sobre la violencia de género facilitada por la tecnología que afrontan las mujeres jóvenes que participan en la política y la vida pública donde participaron 100 mujeres jóvenes participan en política y en la vida pública en el seno de las organizaciones de la sociedad civil y entre particulares, de distintas regiones del país, principalmente de Baja Verapaz, Chimaltenango, Quetzaltenango y Guatemala.

A partir de los resultados se identifica que la violencia de género facilitada por la tecnología (VGFT) funciona como un mecanismo de control sobre las mujeres que son activistas, políticas y periodistas. Los testimonios recabados en la investigación reflejan cómo la violencia digital, lejos de ser un fenómeno aislado, tiene implicaciones estructurales que refuerzan las desigualdades de género. Las agresiones en línea no son solo ataques individuales, sino mecanismos que buscan desalentar la participación de las mujeres en espacios políticos y sociales, restringiendo su libertad de expresión y su capacidad de incidencia.

Otro factor determinante es la etnicidad, que agrava la violencia cuando se intersecta con el género y la juventud. Las mujeres indígenas que desafían los roles tradicionales enfrentan no solo violencia machista, sino también racista y clasista. Esto se traduce en ataques que buscan limitar su identidad y su derecho a participar en espacios de toma de decisión.

En el caso de las mujeres indígenas, los ataques incluyen desvalorización de su participación, cuestionamientos sobre su vestimenta y comentarios racistas sobre su identidad cultural. En redes sociales, esto se manifiesta a través de discursos que refuerzan la idea de que su lugar no es la política, sino la servidumbre o el ámbito comunitario. Lo anterior se ve reflejado en el siguiente comentario:

“Ser mujeres indígenas nos hace aún más vulnerables. Nos violentan porque rompemos estereotipos: el de que las mujeres no tienen derecho a estudiar, el de que los hombres son los únicos que pueden liderar, y el de que las mujeres no pueden tener poder.” (Mujer, Maya mam, 27 años).

Sabemos que lo digital y la tecnología está en constante evolución, lo que implica un reto constante para mantener actualizados los términos, las situaciones de violencia y las rutas de acompañamiento, este es un primer ejercicio para construir diálogos que permitan crear una conversación sobre como acompañarnos.

03 Definición

de violencia de género facilitada por la tecnología

Antes de acompañar, es importante tener un código común en conceptos, seguramente podrás encontrar muchas definiciones desde la Fundación Oxlajuj N'oj, entenderemos por:

Según Carrillo et al. (2024), la VGFT es un fenómeno complejo que engloba diversas formas de violencia perpetradas a través del uso de tecnologías de información y comunicación (TIC), incluyendo redes sociales, plataformas digitales, dispositivos móviles y otras herramientas tecnológicas. Se distingue de la violencia digital en que no solo ocurre en línea, sino que también puede incluir el uso de tecnologías para rastreo, control o difusión de información sin consentimiento (UNFPA, 2021).

Cuevas & Sequera (2024) definen la VGFT como: "cualquier acto cometido, asistido, agravado o amplificado por el uso de tecnologías de la información y la comunicación u otras herramientas digitales, que resulte o pueda resultar en un daño físico, sexual, psicológico, social, político o económico, u otras violaciones de los derechos y libertades". Además, la VGFT es un continuo de las violencias basadas en género que enfrentan las mujeres en los espacios físicos, resultado de estructuras patriarcales, racistas y coloniales (Ananías & Vergara, 2019).

Glosario:

ABUSO BASADO EN IMÁGENES Y VÍDEOS	Publicar o amenazar con compartir fotos o videos íntimos de una mujer sin su consentimiento, para controlarla o humillarla.
AMENAZAS VIOLENTAS	Mandar mensajes en redes sociales o por teléfono diciendo que harán daño a una mujer o a su familia para asustarla.
ASTROTURFING	Generado una ola de repudio u odio hacia la persona a través de cuentas ficticias o coordinadas que divulgan contenido en contra de la persona.
CIBERACOSO	Mensajes ofensivos, amenazas o comentarios constantes que molesten a la persona o la agredan mediante plataformas digitales.
CIBERTURBA	Insultos, amenazas y acoso de manera organizada por muchas personas dirigida a alguien de manera intencional y repetida.
DESINFORMACIÓN Y DIFAMACIÓN	Es usar internet para decir mentiras sobre una mujer o compartir cosas falsas para Dañar su reputación.
DISCURSO DE ODIO	Son mensajes en internet que atacan o humillan a las mujeres por ser mujeres, por cómo se ven, o por lo que piensan.
DOXING	Divulgar información personal (dirección, teléfono, datos privados) sin la autorización de la persona para exponerla.

FORMAS DE PARTICIPACIÓN	Participación política, una acción que busca involucramiento en las decisiones y ser parte activa y fecunda en la solución de los problemas que afectan a las personas en su vida diaria.
GRUPOS INCEL	Comunidades en línea formadas por personas, principalmente hombres, que se identifican como incapaces de encontrar una pareja romántica o sexual a pesar de desearlo que han adoptado ideologías que promueven actitudes negativas, misóginas y violetas hacia las mujeres.
HACKEO Y ACECHO	Cuando alguien vigila y entra sin permiso a tus cuentas, como redes sociales o correo, para controlar, robar información o dañar tu privacidad.
PORNOVENGANZA	Propagación de imágenes o vídeos privados/íntimos con intención de humillar o perjudicar a la persona.
SHALLOWFAKE	Es una persona que critica o juzga superficialmente a las mujeres en redes sociales, fijándose solo en su apariencia o en lo que publican.
SUPLANTACIÓN EN LÍNEA	Creación de uno o varios perfiles falsos en redes sociales con tus datos como nombre e imágenes para falsificar tu identidad y engañar a otros individuos.
VIOLENCIA DE GÉNERO FACILITADA POR LA TECNOLOGÍA	Es una persona que critica o juzga superficialmente a las mujeres en redes sociales, fijándose solo en su apariencia o en lo que publican.

04 Marco legal y normativo internacional y nacional

Los avances al reconocimiento de los derechos de las mujeres no serían posible sin el trabajo que se ha realizado a lo largo de los años, en 1979 la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW) reconoció la necesidad de que los estados erradiquen la violencia contra las mujeres en diferentes ámbitos como el económico, social, cultural y político, en 1994, la Convención de Belém do Pará (1994) nombro las diversas formas de violencia e hizo un llamado para establecer medidas de prevención, protección y sanción. Sobre la violencia política de género, la Resolución 68/181 de la Asamblea General de la ONU (2013), nombro dicha violencia como un obstáculo para la democracia, el desarrollo y los derechos humanos.

Organizaciones como ONU Mujeres y Fondo de Población de las Naciones Unidas (UNFPA, 2021): Legislación contra la Violencia Digital, hizo un llamado a los estados parte a establecer legislación especifica contra la violencia de género facilitada por la tecnología.

Guatemala aunque es limitado tiene normativas especificas para la violencia facilitada por la tecnología como la Ley contra el Femicidio y otras Formas de Violencia contra la Mujer (Decreto 22-2008), a la fecha existen iniciativas legislativas en discusión que aportarían al reconocimiento de la tipificación de delitos de violencia sexual digital, protección al acoso escolar, el ciberacoso, entre otras.

Les invitamos a consular el apartado Marco legal y normativo internacional y nacional de la Investigación Prevención de la Violencia de Género Facilitada por la Tecnología contra Mujeres Jóvenes en la Política desde un Enfoque Interseccional de la Fundación Oxlajuj N'oj.

05 Checklist

operativo rápido ¿qué hago ahora?

Has identificado que estás pasando por alguna situación de violencia digital?, no importa si no sabes qué tipo de violencia es, lo importante es garantizar y resguardar tu seguridad,

El Checklist operativo rápido "¿Qué hago ahora?" son las primeras acciones que una persona debe hacer de forma inmediata si acompaña o vive violencia digital.

Estos pasos son sencillos y deben de hacerse lo antes posible al Identificar la violencia, recomendamos que sea dentro de las primeras 24 horas tras identificar VGFT.

- **1. Seguridad personal:** Si existe una amenaza física inminente, priorizar la seguridad física: alejarse del lugar, pedir acompañamiento físico, llamar a contactos de confianza o a autoridades.

- **2. Preservar evidencia:** No borres mensajes ni publicaciones. Hacer capturas de pantalla completas (incluyendo fecha y hora en la pantalla cuando sea posible) y guardar URLs y IDs de publicaciones/usuarios. Guardar copias en un dispositivo externo (pendrive cifrado o disco duro cifrado).

- **3. Aislar el dispositivo comprometido:** Si se sospecha que un dispositivo está comprometido, desconéctalo de Internet y apaga Bluetooth/Wi-Fi hasta que un experto evalúe su estado.

- **4. Documentar:** Registrar fecha/hora, descripción breve del incidente, plataforma, autor (si se conoce), testigos y acciones tomadas hasta el momento.

  Este registro tiene que realizarse por cada incidente de violencia que se registre y se recomienda realizarlo diariamente.

No. de incidencia:		Fecha:			Hora:		
Plataformas:		Se identifica al o los agresores:		Se cuenta con testigos:		Se realizaron capturas de pantalla	
Descripción de la situación de violencia:							
Acciones tomadas hasta el momento:							

- **5. Contactar red de apoyo:** Informar a las personas de confianza para acompañamiento emocional y operativo. La red de apoyo puede estar conformada por personas de toda tu confianza y que puedan brindarte soporte emocional, escucha y acompañamiento.

- **6. Contactar asistencia técnica:** Para solicitar asesoría en Guatemala puedes acceder a los recursos de la Fundación Oxlajuj N'oj como lo es:

  1. Sitio web DIgi Cuida en la web, para acceder al sitio web entra directamente desde https://www.fundacionoxlajujnoj.org/digicuida.html

  2. Chatbot "Cuídate Digitalmente", brindar apoyo práctico sobre seguridad digital, autocuidado y ciudadanía para mujeres jóvenes, políticas y activistas.

Para acceder al chatbot da clic en:

https://api.whatsapp.com/send/?phone=50236127669&text=Hola+me+interesa+m%-C3%A1s+informaci%C3%B3n&type=phone_number&app_absent=0

En caso de necesitar de necesitar asesoría y acompañamiento técnico, puedes escribir a:

SocialTIC seguridad@socialtic.org

Access Now https://www.accessnow.org/resources/ y **https://www.accessnow.org/help-es/**

Para conocer herramientas y recursos técnicos entra a **https://protege.la/herramientas/**

06 Claves para acompañar

Acompañar no es una receta que se siga con rigor, acompañar desde una perspectiva de derechos humanos tiene como ingrediente principal: escuchar a la persona que está pasando por la VGFT.

Antes de escuchar debemos:

Informarnos: Consulta las investigaciones de la Fundación Oxlajuj N'oj, también puedes solicitar información en DIGi Cuida https://www.fundacionoxlajujnoj.org/digicuida.html

Lenguaje: Hay códigos, expresiones, palabras y emojis que se usan como parte de la comunicación en los entornos digitales.

Preguntar: los entornos digitales están en constante actualización, no lo conocemos todo, reconocer que no lo vamos a saber todo es importante, para eso podemos contar con un directorio para preguntar y canalizar.

¿Escucha activa?

La escucha activa, como su nombre lo indica, consiste en escuchar activamente y con conciencia plena evitando los juicios o juzgar a la persona que estamos escuchando.

La escucha activa implica por un lado un trabajo interno donde todos nuestros sentidos se disponen a escuchar y ser empáticas, que nuestra comunicación no verbal (gestos, movimientos corporales, contacto visual, movimiento de las manos) comuniquen lo que queremos transmitir a la persona que nos ha brindado su confianza.

La escucha activa no implica solamente oír, es disponer de un espacio físico y/o virtual donde la persona pueda expresarse.

Recomendaciones para una mejor escucha activa:

- Evita distractores
- Coloca tu teléfono celular en modo silencio
- Si estas desde una plataforma digital (videollamada) activa tu cámara y micrófono.
- Evita juzgar, culpar o cuestionar las decisiones que ha tomado frente a la violencia que está o ha pasado.

- Evita interrumpir.
- No invalides las emociones que surgen frente a la violencia que ha vivido o vive.
- Evita ofrecer alternativas a la violencia que está viviendo si no has realizado la entrevista de primer contacto.
- Centrarse en tu historia y pasar la situación de violencia que vive la persona entrevistada a un segundo plano.

Primer contacto

La escucha activa es importante para poder realizar una entrevista en primer contacto que es fundamental para el acompañamiento en casos de violencia.

La entrevista servirá para que la persona que pasa por la violencia digital pueda expresar la situación por la que pasa y la persona acompañante (quien realiza la entrevista) obtenga toda la información para poder brindarle la información necesaria de acuerdo a la o las violencias que está pasando.

Te recomendamos consultar los Primeros Auxilios Psicológicos (PAP), puedes entrar a **https://cruzroja.org.ar/blog/primeros-auxilios-psicologicos-que-son-y-como-brindarlos/**

Para una entrevista en primer contacto:

La entrevista en primer contacto es el primer acercamiento que se tiene con la persona que esta viviendo violencia, en este caso violencia digital, servirá para realizar un diagnóstico, pronostico y un plan.

Para realizar una entrevista, toma en cuenta:

- Emplear la escucha activa
- Presentarte como acompañante

¿Quién puede ser una acompañante?, cualquier persona puede acompañar, tiene que existir confianza entre la persona que esta viviendo violencia y la persona que acompaña, su rol es brindar contención, escucha y soporte.

Es importante aclarar que la persona que acompaña no es quien presenta la denuncia, aunque no es obligatorio que cuente con formación en psicología o trabajo social te recomendamos leer este protocolo que te brindara herramientas y siempre tratar con dignidad y respeto a las personas.

- Toma en cuenta que la violencia no solo puede presentarse en los entornos digitales, puede existir otras violencias que también deben ser reportadas.
- En caso de dudas al realizar la entrevista o no tener claro un hecho puedes hacer preguntas clave para obtener más información.

- Al finalizar puedes hacer un resumen de la situación para dejar claro que todo ha sido comprendido. La persona puede agregar más información que recuerde al escuchar el resumen.
- Mantener una mirada interseccional.

La interseccionalidad permite identificar las desigualdades y la discriminación que se interseccional con otros factores como la edad, la clase, la etnia, la discapacidad, etc.

Por ejemplo,

Obviar que todas las personas tienen habilidades para el uso del teléfono celular, se debe usar un lenguaje claro y sencillo.

Creer que todas las personas tiene las mismas habilidades visuales, físicas, en caso de ser una persona con discapacidad por ejemplo con discapacidad visual se debe describir detalladamente sin hacer uso de frases que indiquen que debe visualizar algo.

- Las habilidades digitales de las personas son diferentes por lo cual será necesario realizar preguntas adicionales para comprender la situación digital.
- No es necesario que la persona comparta el contenido, mensajes que está recibiendo -menos si es contenido de abuso sexual digital- son la sola descripción.

Una vez realizada la entrevista en primer contacto, agradece a la persona la confianza y plantea las rutas de acompañamiento, protección y seguridad, es importante:

- Se busca brindar información y acompañar, debe centrarse en la persona que pasa por la violencia, pregunta ¿qué te gustaría hacer?
- Comunica a la persona la situación de violencia por la que está pasando, identifica los tipos de violencia, recuerda usar un lenguaje accesible y claro.
- Pide a la persona que realice capturas de pantalla y copiar los enlaces (links) de la violencia que está viviendo o vivo esto le servirá como evidencia en caso de ser necesario. Si la persona no puede realizar las capturas de pantalla en este momento pregunta por su red de apoyo.
- Sugiere un plan de acción y protección.
- No propongas como única acción o estrategia la denuncia penal, es importante recordar que es la persona que pasa por violencia quien debe decir que hacer, desde un acompañamiento se brinda la información para la toma de decisión.
- Recuerda, todos los casos son diferentes, no hay una receta única.

07 Rutas de atención ante la VGFT

Estas rutas son opciones que puedes plantear a la persona que estás acompañando. Es importante tomar en cuenta que:

1. **Respetar los procesos de cada persona.**
2. **Elegir una ruta no limita elegir posteriormente otra.**

Reportar y bloquear en redes sociales y plataformas.

La mayoría de las redes sociales, plataformas, videojuegos ofrecen la opción de reportar, bloquear y eliminar. Te recomendamos que antes de elegir esta opción hagas captura de pantalla y lo guardes en un lugar seguro (dispositivo usb, disco duro)

Puedes consultar:

Meta, Centro de Seguridad https://www.meta.com/es-la/safety/

TikTok, envío de denuncias https://www.tiktok.com/safety/es/reporting

Google, bloquear o desbloquear cuentas de personas https://support.google.com/accounts/answer/6388749?hl=es-419&co=GENIE.Platform%3DDesktop

Si tienes dudas sobre cómo reportar en las plataformas consulta **https://acoso.online/guatemala/**

Acompañamiento psicológico:

Hablar con una persona especialista siempre es una gran opción, se puede brindar un acompañamiento terapéutico, la contención emocional en el momento o brindar herramientas para la contención para futuras situaciones de violencia.

Recomendamos desarrollar una alianza y tener un directorio por área de intervención, de Psicólogas(os) y Psiquiatras para realizar la referencia especializada de forma inmediata.

Redes de apoyo:

Desde los feminismos decimos y creemos que las redes de amigas salvan, ¿quiénes son las personas de mayor confianza con las que puedes platicar de cualquier tema y siempre te van a escuchar?

Tu red de apoyo también puede ser quien:

1. Observa en redes sociales los comentarios que se hacen, las publicaciones donde te etiquetan.

2. Quien o quienes realicen capturas de pantalla, copia de links, bloqueo o reportes.

Denuncia:

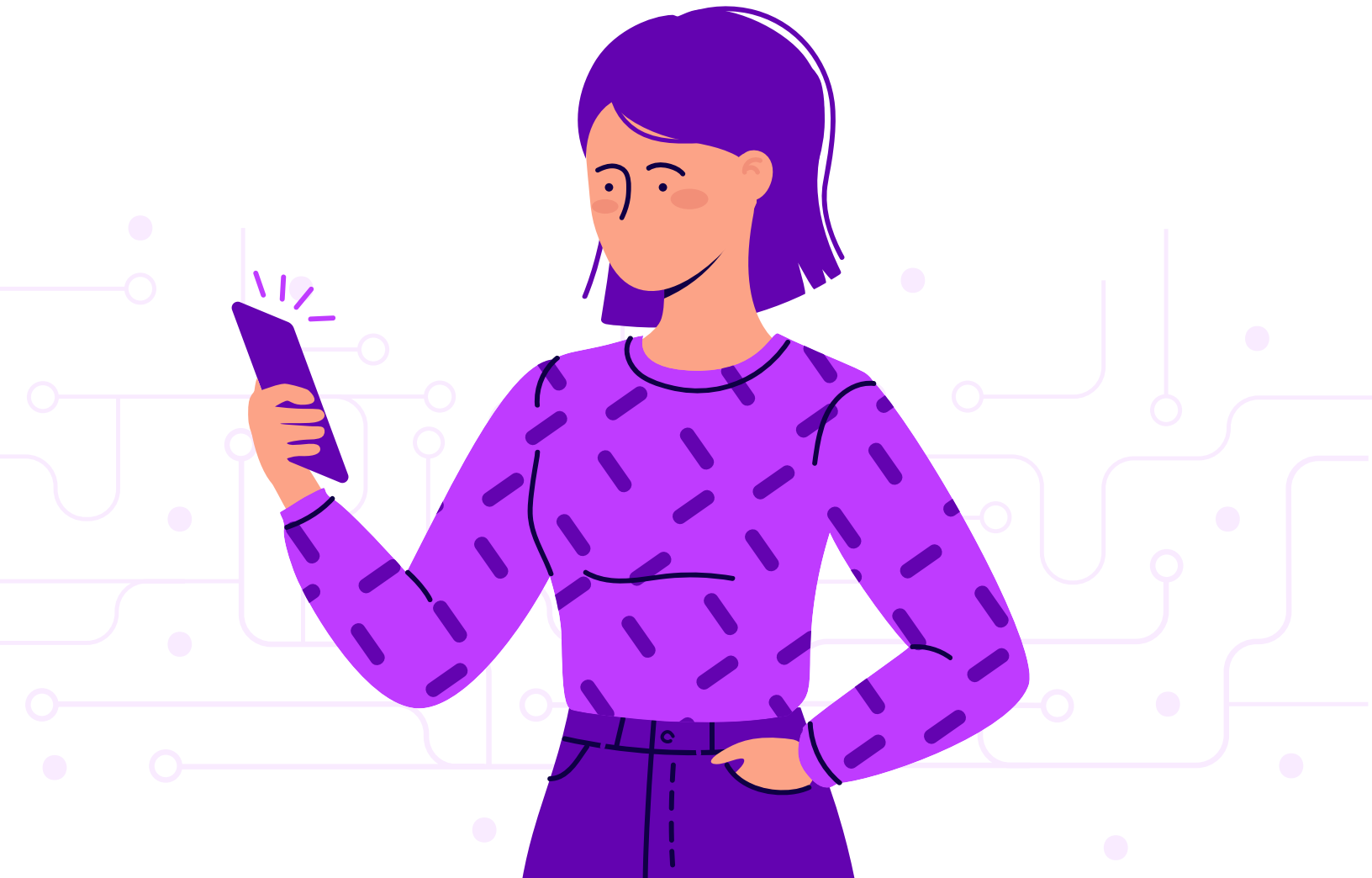
1. Puedes presentarla ante el Ministerio Público, la Fiscalía de la Mujer o la Policía Nacional Civil.

2. Si bien no es necesario que te presentes con una persona abogada te recomendamos contar con asesoría legal previo a tu denuncia.

3. En caso de niñas, niños y adolescentes será necesario que se presenten con madre, padre o tutor legal.

4. Si la violencia se dio en un espacio laboral, la denuncia se realiza en la Inspección General de Trabajo del Ministerio de Trabajo y Previsión Social.

5. En caso de que sea en un espacio escolar, se puede presentar una queja contra el centro escolar en **https://www.mineduc.gob.gt/qcs/app/view/frmIngresoQueja.aspx**



08 Recomendaciones de seguridad, protección y autocuidado digital

8.1 Seguridad en Dispositivos y Plataformas

- **Separación de dispositivos:**

  1. En la medida de lo posible es recomendable que los dispositivos (celular, computadora, laptop) personales no se usen para temas laborales o del activismo.

- **Conexiones seguras:**

  1. Evita conectarte a redes WiFi-públicas o desconocidas; en su lugar, utiliza datos móviles o una VPN.

  2. Una VPN es un Virtual Private Network es decir una red privada virtual que va a permitir que tu dispositivo cree una red privada entre los dispositivos que se van a conectar a Internet, algunos VPN que puedes usar: **https://protege.la/herramientas/#eq-comp-vpn**

- **Gestión de accesos:**

  1. No abras o inicies sesiones en dispositivos que no sean de uso personal, en caso de que tengas que abrir una sesión, recuerda cerrarlas.

  2. Te recomendamos también no vincular cuentas ni iniciar sesión accediendo a otra cuenta. Cada cuenta, perfil, red, plataforma debe tener su propio acceso.

- **Respaldos:**

  1. Genera un respaldo de la información de tus dispositivos, mantén en un lugar seguro y actualizado los respaldos.

  2. Para más información sobre el respaldo puedes consultar **https://protege.la/herramientas/#eq-comp-respaldos**

- **Autenticación robusta:**

  1. Configurar contraseñas seguras, deben llevar al menos letras mayúsculas, minúsculas, números y de ser posible algún signo.

  2. Activar la verificación en dos o tres pasos en todas las cuentas.

Cada red social, cuenta, perfil que crees debe tener su propia contraseña.

Para más herramientas consulta **https://protege.la/herramientas/#serv-linea-contrasenias**

- **Actualización de seguridad:**

1. Cambia contraseñas de redes sociales, correo electrónico, plataformas regularmente.

2. Mantén actualizado tus respaldos de cuentas, si ya no usas un correo electrónico o cambiaste de número de celular, actualiza los datos.

Recomendaciones:

1. Usar un protector de cámara web.

2. Herramienta de cifrado **https://protege.la/herramientas/#eq-comp-cifrado**

8.2 Protección de la Identidad y Privacidad

- **Exposición en redes:**

1. Antes de publicar o compartir en redes sociales haz una pausa e identifica qué vas a publicar, identifica qué información compartes en qué red social y quienes son las personas que te siguen en redes sociales, plataformas, etc.

2. Realiza un plan de publicaciones donde identifiques en qué redes sociales y plataformas vas a publicar qué tipo de información, es valido querer limitar el contenido que publicas.

3. Recomendamos no publicar información personal, sensible o datos de contacto, incluyendo ubicación en tiempo real.

4. En caso de eventos o actividades públicas, es importante reconocer los posibles beneficios o violencias que pueden existir, en caso de identificar alguna situación, recomendamos no publicar al momento que se encuentra participando, asistiendo al evento.

- **Anonimización:**

1. No revelar datos personales de identificación como dirección, número de teléfono, domicilio particular o detalles de familiares y personas cercanas.

2. Si tienes hijas e hijos te recomendamos no publicar fotos y/o vídeos de ellas y ellos, en caso de publicar fotos, tapa su rostro así como detalles de ubicación como escuela, nombre en el uniforme.

- **Configuración de privacidad:**

  1. Usar listas personalizadas como “close friends” para limitar quién puede ver el contenido en redes.

  2. Restringir el acceso a perfiles y eliminar a personas desconocidas o no confiables.

  3. No subir en tiempo real fotos, vídeos, publicaciones o ubicaciones.

  4. En caso de realizar un “en vivo” (transmisión en vivo) identifica previamente los riesgos existentes, si no quieres que identifiquen dónde estás ubicada, utiliza un fondo neutro que no de información de dónde te encuentras.

  5. Guardar números cercanos con otros códigos de seguridad, no usar parentescos y apellidos.

  6. Realiza una limpieza de tus redes sociales.

- **Protección de imágenes y archivos: :**

  1. Evitar almacenar información sensible en la nube o en dispositivos sin cifrado. Evitar compartir fotos de niñas, niños y adolescencias.

- **Monitoreo de reputación:**

  1. Realiza búsquedas periódicas del propio nombre (busca tu nombre con diferentes combinaciones) en buscadores, redes sociales y medios de comunicación para identificar posibles intentos de difamación o suplantación de identidad.

  2. Pide a tu red de apoyo que observen lo que se comparte o se dice de ti en redes sociales, en caso de identificar alguna publicación (texto, imagen) que pueda vulnerarte pide que realicen captura de pantalla y copien los links.

8.3 Manejo de Acoso y Ataques Digitales

- **Gestión de cuentas falsas y acoso en redes:**

  Documenta la situación, realiza las capturas de pantalla y copia los links (enlaces)

  Bloquear y reportar cuentas que hostiguen o difundan desinformación. La decisión que tomen las redes sociales y plataformas puede tardar hasta 72 hrs.

  En caso de no estar conforme con la decisión de la red social o plataforma apela la decisión.

  Es más efectivo que la persona que está siendo violentada haga el reporte.

- **Recibir acoso o amenazas:**

  1. Si se reciben amenazas o acoso, realiza captura de pantalla de los comentarios o mensajes que se reciben. Documenta los mensajes, puedes crear un diario de incidentes que te ayudará a identificar en qué momento y contexto se dan las amenazas y acoso.

  2. Ajustar la configuración de privacidad.

  3. Reportar el número con la compañía telefónica correspondiente.

4. Reporta en redes sociales.

5. De ser posible y se cuenta con los recursos cambia el número de teléfono. Pide a las personas cercanas que no compartan el nuevo número.

6. Si así lo consideras, acude con las autoridades correspondientes para denunciar.

7. Habla con tu red de apoyo para establecer un cuidado colectivo, puedes avisar cuando salgas de un lugar y llegues, tener alguna palabra clave.

- **Gestión emocional:**

1. Desactivar las notificaciones de las redes sociales, plataformas y correo electrónico.

2. Establecer límites en el tiempo de uso de redes sociales para reducir el impacto del acoso en la salud mental.

3. Habla con tu red de apoyo.

4. Date un detox de redes sociales.

5. Asegurar que tu perfil político o activista no difunda información personal o familiar. Si es posible, te sugerimos tener un perfil personal y otro para tu activismo.

6. Filtra todas las opiniones que recibas. No todas merecen tu tiempo o energía. Ten siempre presente tu propósito y si te sientes amenazada puedes bloquear, eliminar o denunciar.

7. Filtra periódicamente la lista de amistades de tus redes sociales. Haz una depuración si es necesario.

8. Tu valor como persona, profesional o lideresa no depende ni de la crítica o del aplauso. Mucho menos tu autoestima y autoconcepto.

8.4 Seguridad Física y Bienestar Mental

- **Protección en el hogar:**

1. Implementar medidas como persianas cerradas o cámaras de seguridad para evitar vigilancia externa.

2. Platicar con la familia y establecer acuerdos para la seguridad digital, por ejemplo no contestar llamadas desconocidas, no dar información personal, sensible o de contacto a nadie, no compartir el número de teléfono o número celular sin previa autorización.

3. Cambia las rutas de llegada a tu hogar, espacio de trabajo o lugares que frecuentas mucho.

- **Soporte emocional:**

1. Identifica tus redes de apoyo, puedes construir redes de apoyo dependiendo del momento o la situación.

2. Identifica persona especializado en psicología y contención emocional que pueda brindarte apoyo en caso de ser necesario o de una emergencia.

- **Evaluación de exposición**

  1. Documenta los incidentes, ya sean físicos, emocionales, digitales..

  2. Reflexiona sobre la visibilidad en redes sociales y plataformas: ¿Qué redes sociales y plataformas tengo? ¿Qué tipo de contenido publico? ¿Es contenido privado o público? ¿Publico contenido que aporta para mi proyecto político?

  3. Priorizar la seguridad física, emocional y psicológica sobre la presencia digital.

8.5 Movilidad

- **Compartir ubicación en tiempo real:**

  1. Enviar la ubicación a personas de confianza (puede ser a tu red de apoyo) antes de desplazarse a eventos o reuniones con una exposición relevante.

- **Modificación de rutas y medios de transporte:**

  1. Evitar rutinas predecibles y cambiar rutas frecuentemente.

  2. Priorizar el uso de transporte privado en lugar de transporte público en contextos de alto riesgo.

- **Acompañamiento en desplazamientos:**

  En viajes y eventos, evitar trasladarse solas y procurar estar acompañadas, preferiblemente por una persona de confianza.

8.6 Educación y Cultura Digital

- **Actualización:**

  Mantenerse actualizada e informada es importante, cada día surgen nuevas herramientas tecnológicas que pueden ayudarnos en nuestro trabajo y/o activismo, lamentablemente también puede ser usado para violentar los entornos digitales.

- **Capacitación continua:**

  Participar en espacios de formación para la prevención e identificación de riesgos y violencias digitales.

- **Sensibilización sobre la violencia en línea:**

  Reconocer que las dinámicas de violencia física se trasladan a lo digital y viceversa y que estas violencias en los entornos digitales son reales y tienen impactos reales en las personas.

  Por lo cual es importante contar con herramientas e información para identificarla y actuar en consecuencia a estas dinámicas.

- **Uso de herramientas tecnológicas:**

  Explorar aplicaciones que prioricen la protección, la privacidad y fortalezcan la seguridad digital.

  Se vale que tengas dudas y miedo de la tecnología pero juntas podemos apoyarnos. Pregunta a las personas de confianza y consulta las recomendaciones que hemos compartido en esta sección

- **Compartir contenidon:**

  Comparte información verificada, para identificarla revisa la fuente de origen de la información (qué medio ha publicado la información, quién da la información), cuándo se publicó la información.

  Busca en otras fuentes confiables para comparar la información.

  Revisa las fotos y vídeos.

  Identifica palabras clave, ¿usa un encabezado muy llamativo?, ¿no viene ninguna cita de la persona?, ¿la foto está desenfocada o no es actual?

- **Alfabetización mediática:**

  Desarrollar habilidades para identificar noticias falsas, campañas de desinformación y discursos de odio.

  Identifica herramientas de privacidad y seguridad que puedas compartir con otras personas.

- **Publicación estratégica en redes:**

  No compartir ubicación en tiempo real, preguntar antes de etiquetar a otras mujeres. Decidir cuándo, cómo y qué voy a publicar en redes sociales y plataformas.

- **Autodiagnóstico de riesgos digitales:**

  Un autodiagnóstico te permite prevenir algún ataque digital. Para realizarlo debes revisar que contenido has publicado, compartido o subido a redes sociales y plataformas en el pasado y que del material puede ser usado para violentarte

8.7 Redes de Apoyo y Seguridad Colectiva

- **Autocuidado:**

  Priorizar lo que siento frente a los comentarios en redes sociales y plataformas.

  No minimizar las emociones frente a la violencia en redes sociales y plataformas.

  Gestionar la desconexión como estrategia de autocuidado.

- **Elabora un plan de autocuidado:**

  -Identifica y valida los malestares

  -Vaciar los espacios para poder despresurizar la presión, estrés que genera la violencia.

  -No saturar redes naturales de apoyo.

  -Fortalecimiento de redes y alianzas.

  -Evitar la polarización.

-Evita la autoculpabilización y descalificación.

-Crear espacios libres para la mente y el cuerpo (yoga, caminar, meditar, bailar)

-Poner limites

-Establecer rutinas

-No caer en la evasión o paliativas como el consumo de sustancias.

Consulta:

Estrategias de autocuidado en escenarios de violencia de la organización Artículo 19 **https://seguridadintegral.articulo19.org/wp-content/uploads/2020/06/art19_2020_infografia-EstrategiasAutocuidado.pdf**

Manual de Auto cuidado, FUNDASIL, **https://www.unicef.org/elsalvador/media/5036/file/Manual%20de%20Autocuidado.pdf**

- Autocuidado en la intervención social, Manual de autoaplicación, Instituto Canario de Igualdad, **https://violenciagenero.org/web/wp-content/uploads/2020/07/guia-autocuidadodef.pdf**

Cuidado colectivo:

Comparte información con amistades, familia y redes de apoyo.

Construye una red de apoyo pero también se parte de una red de apoyo, nos cuidamos juntas.

Habla con tu red de apoyo de acuerdos de seguridad y privacidad.

- Crear Círculos de Sanación digital (CSD), espacios mensuales para compartir experiencias, arteterapia, duelo y resiliencia colectiva.

Protocolos de respuesta:

Construyan y aprópiense de sus propios protocolos. El protocolo que ahora estás leyendo puede servirte de inspiración.

- Compartan estrategias aprendidas de compañeras que han vivido experiencias de violencia digital, física, emocional y psicológica.

Intervención comunitaria:

Crear espacios de encuentro (físicos o virtuales) donde se compartan herramientas y recursos para la protección y seguridad digital.

Formación y difusión: Difundir información, desarrollar talleres o intercambios de prevención y activación para la VGFT en entornos comunitarios e institucionales en donde todo el liderazgo y resto de población este involucrada es vital.

- **Difusión de información:**

Construir campañas de información, concienciación y prevención sobre los riesgos en línea.

Promover el apoyo colectivo y la solidaridad digital entre mujeres.

Promover información sobre los derechos digitales y su uso responsable.

Compartir información de organizaciones, colectivas, redes que brinden información, capacitación y acompañamiento.

- **Estrategias de denuncia colectiva:**

  Desarrollar respuestas organizadas frente a casos de violencia digital para ejercer presión y exigir justicia.

- **Sostenibilidad del activismo:**

  Reconocer el desgaste emocional del activismo y fomentar el autocuidado.

  Construir estrategias desde la alegría y el arte como formas de resistencia y cuidado colectivo.

09 Preservación de evidencia digital: procedimiento mínimo

En el capítulo “Rutas de atención ante la VGFT” comentamos que la persona que está pasando por violencia digital puede recibir acompañamiento de diferentes rutas, una de las opciones es presentar una denuncia en las instancias correspondientes, consulta el apartado “Denuncia”.

- Puedes presentarla ante el Ministerio Público, la Fiscalía de la Mujer o la Policía Nacional Civil.
- Si bien no es necesario que te presentes con una persona abogada te recomendamos contar con asesoría legal previo a tu denuncia.
- En caso de niñas, niños y adolescentes será necesario que se presenten con madre, padre o tutor legal.
- Si la violencia se dio en un espacio laboral, la denuncia se realiza en la Inspección General de Trabajo del Ministerio de Trabajo y Previsión Social.
- En caso de que sea en un espacio escolar, se puede presentar una queja contra el centro escolar en https://www.mineduc.gob.gt/qcs/app/view/frmIngresoQueja.aspx

Puede ser que tu o la personas que acompañas quiera presentar la denuncia pero también es posible que tenga la duda o no sabe si quiere o no presentarla, sin importar cual sea su decisión es importante preservar las evidencias. Conservar la evidencia es útil legal y técnicamente.

Es importante enfatizar que no borres nada.

→ Capturas de pantalla completas

Realiza captura de pantalla, la captura debe incluir fecha/hora y URL visibles.

Te pedimos no recortar la imagen.

En caso de conversaciones o mensaje en plataformas de mensajería te recomendamos hacer grabación de pantalla.

Recomendación: Si tu o la persona que acompañas no puede realizar el resguardo de información pide a una persona de toda tu confianza que los realice.

Guardar enlaces y metadatos

Copia la URL completa, la URL es el link directo a la publicación, cuenta, etc.

Herramientas que puedes usar para la búsqueda de imágenes:

TinEye https://protege.la/herramientas-posts/tineye/

En caso de ser posible, descarga la página como PDF/HTML.

¿Cómo guardar una página web como PDF?

1. Abre la página web

2. Haz clic en los tres puntos (...) que se encuentran en la esquina superior derecha

3. Da clic en "Imprimir/Print"

4. Te aparecerá una ventana y te mostrará cómo se ve el documento, da clic en "Guardar/Save" y elige donde guardar el documento.

Otra opción para guardar en lugar de buscar la opción "Imprimir" es abrir la página web y presionar las teclas: Ctrl + P , te aparecerá la ventana y guardas el documento.

Preservar archivos originales

Es importante no borrar ningún archivo, conserva los archivos originales como fotos, vídeos, notas de voz, no los edites, cortes, manipules o conviertas a otros formatos.

Extraer metadatos (si aplica):

Los metadatos es la información que describe a un archivo y que no se ve a simple vista,

Recolectar metadatos de manera segura te recomendamos:

Exif https://exifinfo.org/

Exif cleaner https://exifcleaner.com/

Registro de bitácora y de cadena de custodia:

En tu bitácora de violencias o situaciones de riesgo incluye información del resguardo de evidencias, por ejemplo quién recopiló la evidencia, cuándo y cómo se almacenó.

Resguardo de evidencias:

Guardar copias en al menos dos ubicaciones por ejemplo: un disco cifrado y almacenamiento cifrado de confianza.

Es importante identificar que si hay una situación de riesgo físico una de estas copias se encuentre en otra ubicación que no sea la oficina o casa.

Nunca guardes tus evidencias en el celular o en la nube.

10 Protocolo

de respuesta ante sospecha de espionaje, acceso no autorizado a dispositivos, vulneración de cuentas

Comúnmente las personas llaman “hackeo” al acceso no autorizado a cuentas y/o la vulneración a cuentas, dispositivos, etc.

Hoy en día con los avances tecnológicos han sofisticado las formas de espionaje, acceso y vulneración a cuentas volviendo casi imposible identificar síntomas pues buscan pasar desaparecidos por las personas que están siendo atacadas, te recomendamos:

- Observar y conocer tu dispositivo para identificar algún cambio en la configuración, en los mensajes que llegan, que son enviados.
- Si cuentas con archivos en la nube revisa quien accede a ellos y los permisos que tiene para acceder.
- Cambios en la configuración de redes sociales.
- Aplicaciones instaladas que no identifiques
- Archivos ocultos que no identifiques

Pasos inmediatos si existe la sospecha de espionaje, acceso y vulneración a cuentas:

Pasos inmediatos si existe la sospecha de espionaje, acceso y vulneración a cuentas:

1. Poner el dispositivo en modo avión y apagar Wi-Fi/Bluetooth. Si es posible dejar de usar el dispositivo.

2. Cambiar acceso a cuentas críticas desde un dispositivo confiable.

3. No confiar en recuperación por SMS: usar apps autenticadoras o llaves físicas.

4. Buscar ayuda técnica especializada, te recomendamos:

SocialTIC seguridad@socialtic.org

Access Now https://www.accessnow.org/resources/ y https://www.accessnow.org/help-es/

5. Si se confirma malware, atender a las indicaciones de las personas especialistas para no eliminar la vulneración o poner en riesgo otras cuentas.

11 Flujo de escalamiento y contactos de apoyo

No hay una ruta obligatoria para cada caso de violencia, es importante tomar en cuenta:

-Si existen otras violencias además de la digital, por ejemplo amenazas en espacios físicos, violencia económica.

-Lo reiterado de la violencia.

-Si se conoce a quien o quienes generan la violencia digital

-El contexto, por ejemplo si la mujer está en campaña.

Esto no quiere decir que no debe de atenderse o que no hay nada que hacer, toda situación de violencia debe ser acompañada.

Al realizar la entrevista en primer contacto podrás identificar qué medidas deben proponerse y canalizarse, siempre respetando el proceso de la persona que pasa por la violencia de género facilitada por la tecnología.

Te proponemos un flujo de atención y canalización:

→ Persona receptora de VGFT

- **Primer contacto (escucha activa, contención, entrevista, recomendaciones de seguridad -capturas de pantalla (resguardo de evidencias), cambio de contraseñas- propuesta de rutas de atención**
- **Canaliza con persona legal**
- **Canaliza psicología**
- **Canalizar con especialista técnico**
- **Red de apoyo**

Si se identifican riesgos que ponen en peligro la vida y/o seguridad de la persona es importante que se notifique a áreas de seguridad y que se le brinde el acompañamiento legal, además de activar la red de apoyo.

Algunas recomendaciones, esta lista de sugerencias no es definitiva, recuerda que la tecnología está en constante avance y debe actualizarse, tampoco es obligatoria, cada proceso es único y debemos respetar la decisión de quien pasa por la violencia facilitada por la tecnología.

Violencia	Recomendación	Otras sugerencias de canalización
Acoso /insultos /discursos de odio	Bloquear o silenciar las cuentas que están generando los mensajes de acoso/odio/insultos. Preservar evidencias	Apoyo psicosocial Apoyo de su red Desconexión digital o la gestión en el tiempo de pantallas.
Amenaza con difundir contenido sexual íntimo (real o manipulado)	Contención emocional No caer en provocaciones o presión. Preservar evidencias	Apoyo psicosocial Apoyo legal
Difusión (viralización) de contenido sexual (real o manipulado)	Contención emocional Preservar evidencias No caer en depresión o provocación ¿Tienes las fotos y/o vídeos con lo que te esta amenzando? **Para mayores de 18 años,** crea un caso en https://stopncii.org/ **Para menores de 18 años,** crea un caso en https://takeitdown.ncmec.org/es/ ¿Cómo funciona stopNCII y TakeItDown? Si tienes más de 18 años entra a **https://stopncii.org/** Si tienes menos de 18 años entra a **https://takeitdown.ncmec.org/es/** Crea un “reporte” y sigue los pasos que te muestre la pantalla	Apoyo psicosocial Apoyo de su red Apoyo legal Te recomendamos no realizar ningún pago ni enviar fotos o vídeos

	Ambas páginas crearán un hash (un código de barras) que enviaran a las plataformas, sitios web y redes sociales aliadas avisando que el contenido no puede publicarse. Usa estas páginas para prevenir que el contenido íntimo se viralize en las plataformas y redes sociales. **¿Ya se publicó?** Identifica en qué red social y plataforma se ha publicado y reporta	
Amenazas violentas	Seguridad física, autoridades, apoyo técnico. Preservar evidencias	Apoyo psicosocial Apoyo de su red Desconexión digital o la gestión en el tiempo de pantallas.
Doxing	Documentar y preservar evidencias. Análisis de riesgos de la información vulnerada. Apoyo técnico para cambio de contraseñas y fortalecer la seguridad de cuentas.	Estrategia pública y mediática. Apoyo psicosocial Apoyo de su red
Desinformación / difamación	Contención emocional Análisis de la situación para establecer estrategias de respuesta (pueden ser individual, institucional, ambas) Preservar evidencias	Apoyo psicosocial
Ciberturba	Cambio de contraseñas Fortalecer estrategias de seguridad en redes y cuentas (personales, institucionales) Silenciar notificaciones Preservar evidencias	Revisión técnica de los perfiles, cuentas y plataformas una vez que ha disminuido el ataque. Desconexión digital o la gestión en el tiempo de pantallas.

*Si tienes duda sobre los conceptos consulta el apartado “Glosario”.

Organizaciones clave que pueden brindar acompañamiento:

Globales: Access Now, Front Line Defenders, Amnesty Security Lab,

Regionales: Ciberseguras, Acoso Online, Vita Activa, SocialTIC, Artículo19

Locales:

- **Unamg (Unión Nacional de Mujeres Guatemaltecas)**

  Teléfono: 2232-9737

- **MTM (Mujeres Transformando el Mundo)**

  Teléfono: 2254-2141

- **Asociación La Cuerda**

  Teléfono: 2253-9288

- **GGM (Grupo Guatemalteco de Mujeres)**

  Teléfono: 2285-2050

- **ASOGEN (Asociación Generando)**

  Teléfono: 7931-1091

- **Mujeres Iniciando en las Américas (MIA)**

  Teléfono: 2314-8740

- **Fundación Sobrevivientes**

  https://sobrevivientes.org/

- **Casa del Migrante**

  https://www.simn-global.org/centros-scalabrinianos/centro/mountain-cycling/

- **Refugio de la Niñez**

  https://refugiodelaninez.org/

Plantilla de respuesta institucional rápida

¿Quién puede utilizar esta plantilla? Desde los grupos e estrategia de campaña de las candidatas, las mujeres organizadas, colectivos, periodistas.

¿En qué casos se puede usar? En cualquier caso de violencia política digital puede utilizarse, es importante que la persona receptora de violencia digital este de acuerdo con realizar una respuesta.

Te recomendamos revisar el capítulo de **"Claves para acompañar".**

1. Mensaje inicial a la receptora de violencia: "Tu seguridad y bienestar es nuestra prioridad. ¿Necesitas atención inmediata?"

2. Brindar contención emocional y asegurarse de que la persona se encuentra bien y no hay un riesgo que deba ser atendido de forma inmediata.

3. Activar equipo interno de respuesta (legal, psicológico) y documentación del caso.

4. Coordinar cualquier comunicación pública con la persona receptora de violencia y asesoría legal.

5. Acompañarse en todo momento de una persona psicóloga para contención emocional.

Protocolo de comunicación segura para entrevistas y acompañamientos

1. Preferir llamadas por Signal o videollamadas seguras.

2. Contar con un canal de comunicación alterno, por ejemplo muchas personas cuentan solo con un canal de Whatsapp para comunicarse, en caso de que whatsapp sufre una caída se pierden las comunicaciones por lo que se propone tener un canal alterno para no perder comunicación, por ejemplo Signal.

3. Enviar contraseñas y archivos por canales distintos.

4. Limitar intercambio de datos personales por canales inseguros.

5. Mantener registro cifrado de entrevistas.

6. No responder a solicitudes de entrevistas de medios o personas que no se tengan identificadas.

7. No acudir sola a entrevistas, ya sean virtuales o presenciales.

8. Generar un respaldo de las entrevistas, publicaciones, artículos que salgan en medios de comunicación

12 Consideraciones Legales

En caso de que tu o la persona que acompañas decida proceder legalmente te recomendamos revisar el capítulo “Rutas de atención ante la VGFT” y “Preservación de evidencia digital: procedimiento mínimo”

1. Consultar asesoría legal antes de acciones públicas:

Si vas a presentar una denuncia, asesórate legalmente, pregunta todas tus dudas, inquietudes y plantea diferentes situaciones.

Una persona abogada no puede juzgar o cuestionar tus acciones, tampoco puede negarte información si no presentas una denuncia previamente. Si la persona abogada te hace sentir incómoda, realiza preguntas que no aportan al caso, te “regaña” o quiere educar entonces te sugerimos buscar otro acompañamiento jurídico.

2. Mantener evidencia en forma original con registro de custodia:

Revisa el capítulo relacionado con “Preservación de evidencia digital: procedimiento mínimo”

Tu bitácora y resguardo de evidencias serán importantes y clave para armar el expediente.

¿Y si no tengo evidencias?, eso no limita que no puedas presentar la denuncia.

3. Definir ruta jurídica adecuada (penal, administrativa o protección):

La asesoría es importante ya que cada caso es diferente y no hay una receta. Para poder definir la ruta cuenta a la persona abogada toda la situación de violencia que estás viviendo para que identifiquen las diferentes áreas de denuncia.

Nadie puede obligarte a presentar una denuncia si tú o la persona que acompañas no está de acuerdo.

No hay una ruta perfecta, pregúntate ¿cuál es para mí el proceso de justicia que quiero?

13 Bienestar
digital y soporte emocional

Para el bienestar de la persona que está pasando por violencia digital recuerda que no se debe priorizar lo que la persona siente, es importante escucharle en todo momento y no juzgarla.

Recuerda que para brindar recomendaciones que prioricen el bienestar no hay recetas, puedes preguntarle a la persona receptora de violencia ¿cómo se siente en este momento?, ¿qué le gustaría hacer?

Consulta las recomendaciones que compartimos en "Claves para acompañar"

También puedes incorporar e implementar la ficha "Seguimiento psicológico 7-30-90 días" con 3 preguntas: ¿Cómo te sientes?, ¿Qué funcionó? Y ¿Qué necesitas?.

1. Bloquea comentarios y desactiva notificaciones: No elimines nada, es importante hacerle saber a la persona que eliminar implica perder las evidencias.

2. Buscar apoyo psicosocial inmediato en crisis: Si vas a brindar acompañamiento puedes brindar contención inmediata -la contención no es dar terapia psicológica- invita a la persona a realizar respiraciones controladas para conectar consigo misma, por ejemplo respiración en 4, inhalar en 4 tiempos, sostener en 4 e inhalar en 4.

3. Crear plan de autocuidado y desconexión temporal: Responde o realiza la pregunta ¿qué necesitas en este momento para sentirte de la mejor forma?

Desconectarte no significa cerrar las redes sociales y plataformas de forma definitiva, la desconexión es gestionar tu uso de redes sociales y ponerte en el centro a ti y lo que en este momento sientes.

Por ejemplo, para crear **un plan de desconexión:**

-Decide qué aplicaciones tendrás activas en el celular y cuáles en el equipo de cómputo.

-Qué plataformas y redes sociales no te hacen bien en este momento y prefieres desinstalarlas.

-A partir de qué hora se silenciarán las notificaciones.

14 Pautas para formación y ejercicios prácticos

1. Simulacros de incidentes digitales.

2. Taller de preservación de evidencia.

3. Configuración segura de cuentas.

Configurar privacidad en Instagram

Instagram Autenticación en dos pasos

1.- Abre tu cuenta de Instagram

2.- Ve a tu perfil (donde se ven las fotos y reels que haz publicado)

3.- Da clic en las tres rayas (- - -) que se encuentran en la esquina superior derecha

4.- Da clic en “Centro de cuentas” (es la primera opción del menú

5.- Da clic en “Contraseña y seguridad”

6.- Da clic en “Autenticación en dos pasos”

7.- En caso de tener varias cuentas de Instagram, elige la cuenta en la que quieres activar la autenticación.

8.- Una vez que eliges la cuenta, te preguntará cuál método de autenticación quieres:

App de autenticación

SMS o Whatsapp

Métodos adicionales

Repite esta opción con todas las cuentas que tengas de Instagram

Instagram Alertas de inicio de sesión

1.- Abre tu cuenta de Instagram

2.- Ve a tu perfil (donde se ven las fotos y reels que haz publicado)

3.- Da clic en las tres rayas (- - -) que se encuentran en la esquina superior derecha

4.-Da clic en “Centro de cuentas” (es la primera opción del menú

5.- Da clic en “Alertas de inicio de sesión”

6.- En caso de tener varias cuentas de Instagram, elige la cuenta en la que quieres activar la autenticación.

7.- Una vez que eliges la cuenta, te preguntará cómo quieres que te llegue la alerta:

Notificación en la app

Correo electrónico

Repite esta opción con todas las cuentas que tengas de Instagram

Privacidad

1.- Abre tu cuenta de Instagram

2.- Ve a tu perfil (donde se ven las fotos y reels que haz publicado)

3.- Da clic en las tres rayas (- - -) que se encuentran en la esquina superior derecha

4.-Da clic en “Privacidad de la cuenta”, te aparecerán dos opciones:

5.-La primera opción “Cuenta privada” elige si quieres mantenerla pública o privada

6.-En esa misma, la segunda opción “Permitir que las fotos y los vídeos públicos aparezcan en los resultados de motores de búsqueda” si elegiste cuenta privada esta opción debe ser “no”

Configurar privacidad en Facebook

Privacidad

1.- Da clic en tu perfil de Facebook

2.- Al dar clic a tu foto de perfil te aparece un menú, da clic en “Configuración y privacidad”

3.- Elige la opción “Centro de privacidad”

4.- Da clic en “Configuración para ayudarte a controlar tu privacidad” y abajo en azul aparece un botón “Revisar configuración”

5.- Al dar clic te abrirá una página de Opciones de privacidad frecuentes, elige la opción que quieres configurar

Privacidad

1.- Da clic en tu perfil de Facebook

2.- Al dar clic a tu foto de perfil te aparece un menú, da clic en “Configuración y privacidad”

3.- Elige la opción “Configuración”

4.- Te aparecerá una serie de opciones para configurar “Bloqueos”, “registro de actividad”, “modo oscuro”

5.- Entra a cada opción y elige lo mejor para tu perfil

Configurar Whatsapp

Configurar PIN de Whatsapp

1.-Abre Whatsapp

2.- Da clic en los tres puntos (...) esquina superior derecha

3.- Da clic en “Ajustes”

4.-Entra a “Cuenta”

5.- Elige la opción “Verificación en dos pasos”

6.- Te pedirá que escribas una clave formada por 4 números

Recuerda, jamas compartir con nadie esa clave

Configurar ¿Quién puede ver?

1.-Abre Whatsapp

2.- Da clic en los tres puntos (...) esquina superior derecha

3.- Da clic en “Ajustes”

4.-Entra a “Privacidad”

5.- Te saldrán las opciones “Hora de últ vez y En línea”, “Foto de perfil”, “info”, “Enlaces”, “Estado”

6.- De cada una de las opciones al entrar te saldrá un serie opciones:

Todos

Mis contactos

Mis contactos, excepto

Nadie

De cada una elige quien quieres que vea. Te recomendamos que solo las personas que tengas guardadas como contactos puedan ver tu información, es decir la opción “Mis contactos” o “Mis contactos excepto”

Configurar Tik Tok

Privacidad

1.- Entra a tu perfil, al abrir TikTok en la parte inferior encontraras el incoado de una persona y la palabra “Perfil”

2.- En la esquina superior derecha aparecen tres rayitas (- - -)

3.- Da clic en “Ajustes y privacidad”

4.- Elige la opción “Privacidad”

5.-Te mostrará cuales son tus permisos actuales y cuales te faltan configurar. Por ejemplo puedes decidir si quieres o no permitir que tu contenido se use para Dúos.

Cuenta

1.- Entra a tu perfil, al abrir TikTok en la parte inferior encontraras el incoado de una persona y la palabra “Perfil”

2.- En la esquina superior derecha aparecen tres rayitas (- - -)

3.- Da clic en “Ajustes y privacidad”

4.- Elige la opción “Cuenta”

5.-Te mostrará una serie de opciones, elige primero “Clave de acceso” (similar al pin de verificación), selecciona la clave y acepta.

6.- Regresa y ahora da clic en “Datos de la cuenta”, te mostrará el correo, número de teléfono que tienes registrado en esa cuenta, si alguno de esos contactos ya no cuentas con ellos, cambialo.

Más recursos:

Centro de Seguridad de Meta **https://www.meta.com/es-la/safety/**

Centro de seguridad de TikTok **https://www.tiktok.com/safety/es/**

15 Herramientas y buenas prácticas recomendadas

- **Comunicaciones:** Signal, Wire, Element.
- **Contraseñas:** Bitwarden, Strongbox, Authy, KeePassXC
- **Correo cifrado:** ProtonMail.
- **Gestores de contraseñas:** Bitwarden o KeePass.
- **2FA:** apps autenticadoras o llaves YubiKey.
- **Cifrado de disco:** Addy.oi, FileVault, BitLocker o LUKS.
- **VPN:** Mullvad VPN, Psiphon, OpenVPN, NprdVPN, Orbot,
- **Navegación segura:** D
- **Eliminación de metadatos:** Exif https://exifinfo.org/ y Exif cleaner https://exifcleaner.com/

Para conocer más herramientas entra a https://protege.la/herramientas/

16 DigiCuida, Herramientas

DigiCuida

Conoce las herramientas que Oxlajuj No'j ha creado para todas:

Sitio web DIgi Cuida en la web:

Para acceder al sitio web, puedes:

Entra directamente desde **https://www.fundacionoxlajujnoj.org/digicuida.html** o escribe en tu buscador favorito Fundación oxlajuj noj

Da clic en **https://www.fundacionoxlajujnoj.org/**

En la parte superior derecha te aparecerá la opción **DigiCuida**

En este sitio web encontrarás tres opciones:

- **Información:** Recomendaciones sobre el manejo de ataques digitales, seguridad en dispositivos y plataformas y protección de identidad y privacidad. También encontrarás la opción para solicitar ayuda.
- **Documentos de apoyo:** conoce la legislación en violencia de género facilitada por la tecnología en otros países, Guía de Seguridad Digital y física para activistas y el glosario.
- **Dashboard:** datos de Guatemala, Chimaltenango, Baja Verapaz y Quetzaltenango.

Chatbot “Cuídate Digitalmente”

El objetivo del chatbot es brindar apoyo práctico sobre seguridad digital, autocuidado y ciudadanía para mujeres jóvenes, políticas y activistas. En América Latina y el Caribe:

Para acceder al chatbot da clic en:

https://api.whatsapp.com/send/?phone=50236127669&text=Hola+me+interesa+m%C3%A1s+informaci%C3%B3n&type=phone_number&app_absent=0

El chatbot ofrece un menú de temas a los que puedes acceder:

- Seguridad en mis dispositivos
- Proteger mi identidad y privacidad
- ¿Qué hago si me acosan en línea?
- ¿Qué hago si me amenazan con compartir mi contenido íntimo?
- Bienestar mental y seguridad física
- Seguridad en mi movilidad
- Ver protocolo completo
- Necesito ayuda urgente

Cada uno de estos propone recomendaciones sencillas para tu seguridad y cuidado digital. Puedes regresar al menú principal las veces que quieras para consultar otro tema.

Ficha para registro de acompañamientos:

Fecha:				
Nombre de quien acompaña:				
Tipo de acompañamiento:				
Entrevista en primer contacto ( )		Seguimiento ( )		
Entrevista realizada por:	Teléfono ( )	WhatsApp ( )	Persona ( )	Correo electrónico ( )

Información de persona acompañada:		
Nombre:		
Pronombre: Ella ( ) El ( ) Elle ( )	Edad	Sexo: Mujer ( ) Hombre ( ) Intersexual ( ) Prefiere no decirlo ( )
Persona de pueblo originario: Sí ( ) ¿De cuál? ¿Lengua materna? No ( )		Identificar discapacidad: 1. Sensorial: auditiva ( ) visual ( ) habla ( ) 2. Física o motora ( ) 3. Intelectual ( ) 4. Psicológica o emocional ( ) 5. Múltiple ( )
Departamento:		
Situación de violencia:	Pasó por violencia ( )	Está viviendo violencia ( )

¿Has tenido pensamientos de que estarías mejor muerta o de hacerte daño?
(Si la respuesta es afirmativa, activar el protocolo de PAP inmediato y referencia de caso a psicología especializada)
Relatoría de la violencia:
Tipos de violencias identificadas:

Acciones que se propusieron:
Canalizacón: Sí ( ) No ( )

Organizaciones

En América Latina y el Caribe:

- Vita Activa (regional) https://vita-activa.org/
- Acoso Online (regional) https://acoso.online/
- Ciberseguras (regional) https://ciberseguras.org/

Locales:

- **Unamg (Unión Nacional de Mujeres Guatemaltecas)**

  Teléfono: 2232-9737
- **MTM (Mujeres Transformando el Mundo)**

  Teléfono: 2254-2141
- **Asociación La Cuerda**

  Teléfono: 2253-9288
- **GGM (Grupo Guatemalteco de Mujeres)**

  Teléfono: 2285-2050
- **ASOGEN (Asociación Generando)**

  Teléfono: 7931-1091
- **Mujeres Iniciando en las Américas (MIA)**

  Teléfono: 2314-8740
- **Mujeres Mayas Kaqla**

  Celular: 5000-1490
- **Organización de Mujeres Tierra Viva**

  Celular: 2238-0575 / 2232-9918
- **Centro de Urgencias Mínimas (CUM)**

  Celular: El Amparo 2: 2431-6242 / El Paraíso 2: 2242-7943
- **Centro de Salud Zona 1**

  Celular: 2232-7935

- **Centro Landivariano de Práctica y Servicios de Psicología**

  Teléfono: 2230-5339; 2230-5340 y 2230-5341

- **Fundación Sobrevivientes**

  https://sobrevivientes.org/

- **Casa del Migrante**

  https://www.simn-global.org/centros-scalabrinianos/centro/mountain-cycling/

- **Refugio de la Niñez**

  https://refugiodelaninez.org/

Fundación
OXLAJUJ N'OJ