GUÍA METODOLÓGICA SOBRE VIOLENCIA DE GÉNERO DIGITAL

DIRIGIDA A EQUIPOS DE ATENCIÓN A PERSONAS EN MOVILIDAD HUMANA

Taller de Comunicación mujer

UNHCR ACNUR
La Agencia de la ONU para los Refugiados

CRÉDITOS

Coordinación general: Corporación Promoción de la Mujer / Taller de Comunicación Mujer

Elaboración de contenidos: Susana Godoy
Apoyo redacción y materiales didácticos: Priscilla Purtschert
Revisión Técnica: Equipo ACNUR Ecuador

Edición de texto: Blanca D. Vicente
Ilustraciones: Sofía Acosta Varea Diseño
Diagramación: Mishell Cárdenas

Corporación Promoción de la Mujer / Taller de Comunicación Mujer. Quito-Ecuador
Teléfono: 593 2 2553542 cpmujer@tcmujer.org
www.tcmujer.org

Moverse Seguras y Seguros: Guía Metodológica sobre Violencia de Género Digital dirigida a Equipos de Atención a Personas en Movilidad Humana.

Taller de Comunicación Mujer. Quito, Ecuador.
Febrero 2022.

Con el apoyo de la Agencia de la ONU para los Refugiados (ACNUR, Ecuador).

ABREVIATURAS

ACNUR
Alto Comisionado de Naciones Unidas para los Refugiados

DDHH
Derechos Humanos

GMSS
Guía para Moverse Seguras y Seguros

Guía Metodológica
Guía Metodológica sobre Violencia de Género Digital dirigida a Equipos de Atención a Personas en Movilidad Humana

Navegando Libres
Programa Navegando Libres por la Red

NNA
Niñas, Niños y Adolescentes

SDH
Secretaría de Derechos Humanos

TCM
Taller de Comunicación Mujer

TICs
Tecnologías de la Información y la Comunicación

VGD
Violencia de Género Digital

ÍNDICE

• ÍNDICE DE TABLAS

PRESENTACIÓN

Taller de Comunicación Mujer (en adelante, TCM), organización feminista que lleva más de 30 años trabajando por la eliminación de la violencia de género, se centra en el acompañamiento feminista a sobrevivientes de violencia de género digital (VGD), la investigación y la capacitación sobre dicho fenómeno en Ecuador, a través de su programa "Navegando Libres por la Red" (en adelante, Navegando Libres).

Al respecto, para TCM el acompañamiento constituye una propuesta necesaria en los procesos de prevención, atención, mitigación y eliminación de la VGD; que permite dotar a las sobrevivientes de herramientas útiles, a la vez que genera condiciones seguras para elaborar estrategias de acción entre mujeres y población LGBTIQ+ en toda su diversidad, acompañantes, organizaciones sociales, instituciones y otras entidades.

En el contexto de la pandemia por COVID-19, las medidas de confinamiento y aislamiento social para la prevención del contagio del virus adoptadas por los gobiernos en diferentes países, han generado un aumento del uso del internet y de los dispositivos digitales. Esta situación ha supuesto un incremento de los riesgos y delitos en el ámbito de las Tecnologías de la Información y la Comunicación (TICs) a nivel mundial y local, especialmente para aquellas poblaciones en condiciones de vulnerabilidad y desventaja social, que enfrentan brechas digitales en el acceso, uso y conocimiento de las tecnologías, incluidas las personas en movilidad humana.

En el año 2020, con el apoyo del Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR), TCM realizó el estudio ***Moverse Seguras y Seguros. Análisis de la situación de Violencia de Género Digital contra mujeres y población LGBTIQ+ refugiada y migrante en Ecuador***[1], además de una guía de protección digital denominada: Guía para Moverse Seguras y Seguros (GMSS)[2]. Ambos documentos se dirigen a personas migrantes y refugiadas y proporcionan herramientas para disminuir los impactos de la VGD en sus vidas.

La presente ***Guía Metodológica sobre Violencia de Género Digital dirigida a Equipos de Atención a Personas en Movilidad Humana (Guía Metodológica)*** complementa los documentos anteriores, en particular, constituye un instrumento de aplicación y facilitación de la GMSS.

1. Taller de Comunicación Mujer (TCM): ***Moverse Seguras y Seguros. Análisis de la situación de Violencia de Género Digital contra mujeres y población LGBTIQ+ refugiada y migrante en Ecuador,*** 2020. Disponible en: https://www.navegandolibres.org/images/navegando/medios/otros/Moverse_seguras_final_compressed.pdf

2. ***TCM: Guía para Moverse Seguras y Seguros,*** 2020. Disponible en: https://www.navegandolibres.org/images/navegando/medios/otros/Guia_Acnur_migrar_final_compressed.pdf

¿Qué es la Guía para Moverse Seguras y Seguros?

Es un manual para promover la protección digital que incluye recomendaciones sobre seguridad y cuidados digitales destinados a población migrante y refugiada. Los contenidos de la GMSS se centran en:

	**Definición de protección digital**
	**Contraseñas seguras**
	**Reducir el rastro de datos personales en internet**
	**Aplicaciones seguras de mensajería instantánea**
	**Ubicación segura y privada**
	**Privacidad y seguridad en redes sociales**
	**Conocimiento sobre celulares**
	**Búsqueda segura de trabajo por internet**

¿Para qué sirve la Guía Metodológica sobre Violencia de Género Digital dirigida a Equipos de Atención a Personas en Movilidad Humana?

La presente Guía Metodológica se ha concebido como un instrumento que parte de los contenidos de la GMSS, los amplía y actualiza, a la vez que propone recursos para la atención y detección de la VGD. La Guía Metodológica permite a los equipos de atención a población refugiada y migrante conocer herramientas y metodologías para prevenir y disminuir los impactos de la VGD en la vida de las personas en movilidad humana.

¿A quién está dirigida la Guía Metodológica?

La Guía Metodológica está dirigida a los equipos técnicos que atienden a personas en movilidad humana. Por sus contenidos, resulta una herramienta útil para cualquier profesional que se desempeñe en el acompañamiento y atención de población en movilidad, tanto de instituciones estatales como de organizaciones de la sociedad civil, entidades privadas y agencias de Naciones Unidas en Ecuador.

Contenidos de la Guía Metodológica

La guía se divide en 5 secciones: **la primera** está dedicada a situar el derecho a una vida libre de violencia de género digital como parte del derecho a una vida libre de violencia; **la segunda**, expone un catálogo de tipos de VGD y de formas de ataques específicos, con el fin de fortalecer la comprensión del fenómeno de las violencias basadas en género en el ámbito digital.

La tercera sección se centra en exponer y ampliar las recomendaciones de protección digital contenida en la GMSS, así como facilitar herramientas a fin de que los equipos de atención puedan transmitir información sobre seguridad digital de manera sencilla y comprensible. **La cuarta** sección contiene claves para la detección de la VGD y **la quinta**, y última, sección recoge acciones de respuesta generales frente a este tipo de violencia.

1 El derecho a una vida libre de **Violencia de Género Digital**

En el Reporte de 2017 "*Situación de América Latina sobre la Violencia de Género ejercida por los Medios Electrónicos*", elaborado para la Relatoría sobre la violencia contra la mujer de Naciones Unidas, se muestra que el crecimiento de la violencia de género en Latinoamérica se refleja también en el aumento de la violencia digital hacia niñas, adolescentes y mujeres.[3]

Ante estos datos, resulta indispensable focalizar las acciones y las estrategias de protección y promoción de los derechos humanos en la prevención y eliminación de la violencia de género en todos los ámbitos donde se reproduce y perpetúa, incluido los espacios digitales.

En Ecuador, la *Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres (LOIPEVCM)*, refuerza los derechos constitucionales y amplía su interpretación en dimensiones fundamentales para el fenómeno de la violencia de género en el país. La norma enfatiza que mujeres, niñas, adolescentes, jóvenes, adultas y adultas mayores, en toda su diversidad, tienen derecho a una vida libre de violencia en el ámbito público y privado, que favorezca su desarrollo y bienestar; al respeto de su dignidad, integridad, intimidad, autonomía y a no ser sometidas a ninguna forma de discriminación, ni tortura; a que se les garanticen la confidencialidad y la privacidad de sus datos personales, entre otros.[4]

En agosto de 2021, entró en vigor la *Ley Orgánica Reformatoria del Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos*, que generó cambios en la LOIPEVCM y la norma penal, a la vez que estableció disposiciones específicas, dirigidas a la Secretaría de Derechos Humanos (SDH) y al Ministerio de Educación,[5] para elaborar programas de sensibilización de la ciudadanía frente a la VGD, lo que supone un avance en el reconocimiento de la necesidad de luchar contra la VGD y de garantizar el derecho a una vida libre de violencias en todos los ámbitos de interacción social.

3. Peña Ochoa, Paz (coord.): *Reporte de la Situación de América Latina sobre la Violencia de Género ejercida por Medios Electrónicos*, 2017. Disponible en: https://hiperderecho.org/wp-content/uploads/2018/03/Reporte_Violencia_Genero_Linea_Latinoamerica.pdf

4. Asamblea Nacional del Ecuador, *Ley Orgánica Integral para la Prevenir y Erradicar la Violencia contra las Mujeres*, Registro Oficial Suplemento 175, 2018.

5. Asamblea Nacional del Ecuador, *Ley Orgánica Reformatoria del Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos*, 2021.

Por su parte, el derecho a una vida libre de VGD de las personas en movilidad en Ecuador debe entenderse de manera interdependiente al ejercicio del conjunto de derechos digitales, los cuales promueven la igualdad y la protección de los ciudadanos y las ciudadanas dentro de internet, la libertad de expresión, la intimidad en el ámbito laboral, el respeto a la vida privada, la protección de datos, el acceso a servicios de redes sociales y equivalentes, entre otros.

De manera específica, las personas refugiadas y migrantes tienen derecho a mantener y fortalecer sus redes de apoyo, tanto en el país de acogida como en el país de origen. Estas relaciones se sostienen a través de las comunicaciones mediadas por la tecnología, es decir, redes sociales, llamadas telefónicas, mensajería instantánea, correo electrónico y videoconferencias. Si bien, mantener comunicaciones inseguras con el país de origen puede suponer riesgos de protección para las personas refugiadas o las que sufren amenazas de persecución, se debe garantizar su derecho a acceder a las TICs de manera segura y protegida.

Por todo esto, resulta imprescindible fortalecer los procesos de atención a personas en movilidad con el fin de ayudar a garantizar un uso seguro de redes sociales y otros medios de comunicación y de prevenir posibles riesgos; al mismo tiempo, de garantizar un uso de las TICs como herramienta que permita crear, mantener y fortalecer las redes de apoyo, socialización e información, ya que las TICs son un instrumento fundamental para conocer y solicitar servicios esenciales de ayuda humanitaria, búsqueda de trabajo y vivienda, así como acceder a trámites para la regularización de la situación migratoria.

2 ¿Qué es la **Violencia de Género Digital?**

La Violencia de Género Digital es toda forma de discriminación, acoso, explotación, abuso y agresión que se produce a través del uso de redes sociales, correos electrónicos, teléfonos celulares, computadoras y todo medio y dispositivo que comprenden las Tecnologías de la Información y la Comunicación (TICs).

Esta violencia afecta principalmente a mujeres, niñas, niños, adolescentes y personas LGBTIQ+ debido a la reproducción de relaciones de poder que se dan en contextos de desigualdad social e histórica. Dichas relaciones de poder se manifiestan en brechas de acceso a servicios y recursos, incluidas las TICs; la reproducción de condiciones de vulneración en espacios fuera y dentro de línea y la limitación del ejercicio de los derechos humanos en el ejercicio de los derechos humanos, lo que se extiende a los derechos digitales.

2.1. Tipos de Violencia de Género Digital y formas de ataque.

A continuación, se expone una categorización de la Violencia de Género Digital y sus formas de ataques recurrentes contra mujeres, niñas, niños y adolescentes (NNA) y población LGBTIQ+.

TCM, en estudios previos, ha identificado que entre estas violencias, aquellas que se dan de manera frecuente contra la población en movilidad humana son: el acoso digital, la violencia sexual digital, los discursos de odio y el acceso no consentido a dispositivos.[6]

Sin embargo, la Guía Metodológica amplía dichas situaciones a través del presente catálogo, por cuanto estas violencias también se dan hacia las personas migrantes y refugiadas.

6. Véase *TCM: Moverse Seguras y Seguros. Análisis de la situación de Violencia de Género Digital contra mujeres y población LGBTIQ+ refugiada y migrante en Ecuador*, 2020.

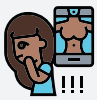
2.1.1. Acoso digital

Se refiere al hostigamiento, amenaza, agresión, difamación o extorsión con la intención de discriminar, disuadir o amedrentar a una persona por razones de género. Las diferentes formas de acoso digital se suelen interrelacionar con otros tipos de violencia de manera sistemática. El acoso digital también se denomina ciberacoso o acoso en línea.

Algunas formas de ataque son:	
	**Amenazas y mensajes intimidatorios**
	**Llamadas y mensajes reiterados**
	**Suplantación de identidad:** indeseados mediante la creación de perfiles falsos en redes sociales con la misma identidad que la víctima.
	***Ciberstalkeo:*** seguimiento e investigación constante de información sobre una o varias personas, entidades, empresas, etc. Es un acto premeditado, repetitivo, obsesivo y, sobre todo, no deseado para las personas o entidades que son vigiladas.
	**Difamación:** difusión de información falsa sobre una o varias personas. Puede darse a través de fotomontajes, video montajes u otros soportes.
	**Extorsión:** chantaje realizado por redes sociales a través de cualquier dispositivo con el fin de obtener algún tipo de beneficio. Cuando se produce vía correo electrónico se conoce como *blackmailing*.

2.1.2. Violencia sexual digital

Se trata del hostigamiento, amenaza, agresión, difamación o extorsión de carácter sexual y/o con fines sexuales. Incluye aquellos actos que afectan al libre ejercicio de la sexualidad de las víctimas, incluidos los que se cometen por medio de intimidación, engaños, manipulación y violencia vulnerando la posibilidad de ejercer el consentimiento sexual de manera libre y consensuada.

Algunas formas de ataque son:	
	**Pornografía no consentida:** se refiere a la elaboración, almacenamiento y/o difusión de imágenes y vídeos íntimos o con contenido sexual o erótico sin autorización. Incluye el robo de imágenes y vídeos de redes sociales o dispositivos, la difusión de fotomontajes o video montajes de índole sexual; la publicación en espacios digitales de imágenes o vídeos que se compartieron de manera consentida, pero no se autorizaron para ser difundidos; la grabación de contenido íntimo sin autorización, entre otros.
	**Acoso de naturaleza sexual:** comprende diferentes situaciones como recibir mensajes y llamadas de carácter sexual, el envío de imágenes con contenido sexual y erótico explícito sin acuerdo o agresiones verbales sexuales.
	**Extorsión sexual:** es la solicitud de imágenes o vídeos de naturaleza sexual de forma coercitiva, bajo amenaza o intimidación.
	**Difamación de caracter sexual:** difusión de información falsa sobre una o varias personas de naturaleza sexual.
	**Explotación sexual facilitada por la tecnología:** toda actividad generada para beneficio propio o de terceros que aproveche a una o varias personas para realizar actividades de naturaleza sexual mediante las tecnologías e internet.
	**Difusión de imágenes o videos de agresiones sexuales**
	**Exponer o buscar pública la identidad de género y/o la orientación sexual sin consentimiendo**

Es fundamental agregar que, cuando las víctimas de este tipo de violencia son niñas, niños y adolescentes (NNA), la Violencia Sexual Digital adquiere particularidades que se concretan en tipos de violencia adicionales o situaciones de especial gravedad y vulnerabilidad. De esta manera, la Violencia Sexual Digital contra la niñez y la adolescencia incluye todos los actos de naturaleza sexual que se cometen hacia cualquier persona y situaciones específicas que se producen a partir de las relaciones de poder ejercidas por las y los adultos hacia NNA.

Algunas formas de violencia digital de carácter sexual específicas contra NNA son:

***Grooming* o el contacto de personas con NNA:** generalmente, para fines de explotación sexual o de extorsión a través de identidades falsas por las redes sociales, juegos en línea, mensajes, chats, entre otros.

Pornografía infantil: constituye una forma de trata de personas con fines de explotación sexual. Incluye la elaboración, almacenamiento y difusión de imágenes y vídeos sexuales donde aparecen NNA.

A su vez, el material pornográfico que involucra a NNA, puede ser utilizado para cometer **otras formas de explotación sexual** como la oferta y/o comercialización de NNA para fines sexuales.

2.1.3. Acceso no consentido a dispositivos, cuentas y servidores

Es el acceso sin autorización a cuentas de redes sociales, páginas web, dispositivos (celulares, computadoras, laptop, etc.) y servidores de internet, con el fin de intimidar, extorsionar, vigilar, manipular o usurpar información personal, laboral u organizacional.

Este tipo de acceso no consentido puede darse a través de técnicas de hackeo informático, de forma manual y a través de actos de intimidación, manipulación y violencia que fuerzan o presionan a las víctimas a entregar diferentes contenidos, datos e información personal o de otras personas y grupos.

Algunas formas de ataque son:	
	**Robo y/o eliminación de contraseñas, datos e imágenes** mediante diferentes técnicas como el envío de virus.
	**Instalación de software espía** en celulares, computadoras y otros dispositivos
	**Alteración y control de dispositivos y cuentas de forma manual** como la eliminación de imágenes y datos, sustitución de correos de recuperación, etc.
	**Suplantación de identidad** mediante la usurpación y apropiación de sitio web, cuentas de redes sociales, entre otros.
	**Obstrucción de ingreso a dispositivos, cuentas, dominios de internet, etc**
	**Entrega de contraseñas mediante intimidación y manipulaciones**
	**Forzar a revelar los contenidos de comunicaciones de personas y organizaciones**
	**Revisar sin consentimiento los dispositivos y las comunicaciones** de otra persona en su ausiencia.

2.1.4. Difusión de información privada

Se refiere a la acción de compartir información en línea sobre la identidad o la vida privada de una o varias personas sin su consentimiento. Este tipo de agresión tienen como objetivo exponer a las personas de tal manera que su seguridad física y psicológica se ponga en riesgo. Este tipo de violencia digital también es conocida como *doxing*.

Algunas formas de ataque son:	
	**Exposición y difusión de datos personales e información privada e íntima**
	**Revelar la ubicación sin consentimiento**
	**Filtrar bases de datos personales por parte de instituciones, empresas o el Estado**

2.1.5. Discursos de odio y expresiones discriminatorias

Se refiere a las agresiones, amenazas y afirmaciones discriminatorias por razones de género que tienen por objeto afectar a personas o grupos históricamente vulnerados, difundir mensajes de odio y/o legitimar estereotipos de género y la diversidad sexual.

Algunas formas de ataque son:	
	**Amenazas de violencia física o sexual** dirigidas contra mujeres, población LGBTIQ+, personas migrantes y refugiadas, entre otras, por el hecho de serlo.
	**Expresiones discriminatorias basadas en estereotipos y roles** de género, sobre la sexualidad, la edad, la etnia, la nacionalidad, la pertenencia cultural, la condición de discapacidad, entre otras, difundidas en chats, fotomontajes, vídeos, etcétera.
	**Lenguaje agresivo hacia grupos históricamente discriminados** por su identidad y contra defensores de derechos humanos.
	**Acciones antiderechos** como campañas xenófobas, racistas, homofóbicas, transfóbicas, entre otras.
	**Ataques coordinados y masivos de personas o bots** que promueven actos de odio y discriminación a través de redes sociales, páginas web, etc.

2.1.6. Ataques a la libertad de expresión

Cualquier acto dirigido a silenciar o amedrentar a una persona o grupo de personas a través de las TICs. Con frecuencia, los ataques son perpetrados contra personas que ejercen su derecho a la libertad de expresión en el espacio público, tales como defensoras de derechos humanos, periodistas y comunicadores sociales, líderes y lideresas sociales, candidatas políticas, población LGBTIQ+, personas en movilidad organizadas, entre otras.

Algunas formas de ataque son:	
	**Ataques coordinados y masivos de personas o bots** para bloquear cuentas de redes sociales, nubes de almacenamiento, denegar acceso a servidores y alterar dominios, entre otros.
	**Censura de contenidos y plataformas web.**
	**Acciones antiderechos** con finalidad de vulnerar la libertad de expresión.
	**Noticias Falsas** actos de desinformación.

2.1.7. Engaño y fraude

Corresponde a la acción de mentir o engañar a través de las tecnologías digitales para perjudicar a una o varias personas. Puede implicar el uso de diferentes estrategias virtuales para el robo de información privada o sensible.

Algunas formas de ataque son:	
	**Estafa nigeriana - Fraude 4-1-9 (o timo 419)**, que adquiere su nombre del código penal de Nigeria, donde se originaron los primeros reportes de esta estafa, consiste en que la víctima recibe correos electrónicos donde le ofrecen grandes sumas de dinero a cambio de hacer una transferencia de dinero o entregar datos bancarios personales. Este delito puede escalar a casos de secuestros y extorsiones.
	**Fraudes en compras en línea** a través de falsas tiendas virtuales.
	*Phishing:* práctica de obtener información confidencial a través de la manipulación. Consiste en engañar a una persona ganándose su confianza al hacerse pasar por una persona o empresa de confianza con el fin de manipularla para que entregue información personal.

Propuesta de actividad dirigida a los equipos de atención que a su vez facilitan espacios de sensibilización y capacitación.

Tabla 1. Actividad para abordar tipos de Violencia de Género Digital

Actividad para abordar tipos de Violencia de Género Digital
1. Estudio de casos. **Descripción:** actividad para identificar tipos de Violencia de Género Digital y sus formas de ataques. **Pasos:** distribuir a las y los participantes en diferentes grupos y repartir hojas con testimonios diversos sobre VGD que contengan preguntas generadoras para la reflexión por equipos y en plenaria. **[Ver material en Anexo 2.1.]**

2.2. ¿Quiénes son los agresores?

La Violencia de Género Digital puede ser cometida por cualquier persona o grupos de personas conocidas o no de las víctimas y sobrevivientes: familiares, parejas, ex parejas, amigos, compañeras de clase, vecinos, desconocidos, grupos antiderechos, redes de criminalidad organizada, agentes estatales, empresas privadas, entre otros.

De manera numerosa, los agresores utilizan el anonimato de internet para enmascarar su identidad. Sin embargo, el uso de perfiles falsos puede ser una estrategia de personas conocidas e, incluso, de familiares y de parejas que resultan ser responsables de las agresiones digitales.

2.3. ¿Quiénes son las víctimas y sobrevivientes?

Todas las personas pueden ser víctimas de violencias digitales y, en particular, de Violencia de Género Digital, por cuanto todas las personas son socializadas en las normas, cosmovisiones, estereotipos y mandatos socioculturales que la posibilitan y sostienen la discriminación basada en el género y la diversidad sexo-genérica.

Sin embargo, la VGD se ejerce mucho más hacia mujeres, niñas, niños, adolescentes y personas LGBTIQ+ en toda su diversidad y bajo cualquier circunstancia, como es el caso de personas en movilidad humana; debido a las relaciones de poder históricamente construidas en sociedades patriarcales que sitúan a estos grupos de la sociedad en contextos de desventaja social, vulnerabilidad, falta de acceso a servicios y recursos, entre otras situaciones de desigualdad.

2.4. Afectaciones psicosociales de la Violencia de Género Digital

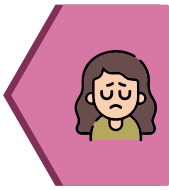
La Violencia de Género Digital puede provocar diferentes impactos en las víctimas, de carácter físico, psicológico, sexual y económico. Las agresiones digitales basadas en género repercuten en la vida privada y en las relaciones sociales de manera real e inmediata en las personas que la padecen y supone la continuidad de la violencia en otros ámbitos del desarrollo de la persona, tanto físicos y digitales, como públicos y privados.

Asimismo, la VGD afecta de manera diferenciada a las personas según sus condiciones y situaciones sociales e identitarias como edad, identidad de género, orientación sexual, situación de movilidad humana, etnia, nacionalidad, condiciones socioeconómicas y discapacidad, entre otras.

Se pueden identificar afectaciones en diferentes niveles:

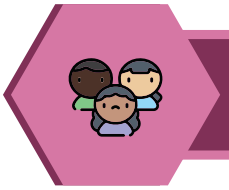
NIVEL PERSONAL

- Miedo, ansiedad, apatía, inseguridad, estado permanente de alerta, depresión, sensación de peligro, etc.
- Insomnio
- Autolesiones
- Suicidio
- Desórdenes alimentarios
- Reducción del uso de las TICs
- Aumento de la precarización económica debido a la pérdida de la fuente de trabajo.
- Bajo rendimiento escolar y otras afectaciones al derecho a la educación como el absentismo.
- Exposición pública: daño a la imagen y vida privada.
- Daños a la integridad sexual.



NIVEL RELACIONAL Y COMUNITARIO

- Aislamiento social.
- Deterioro de las relaciones de amistad, laborales, familiares, etc.
- Aumento de control por parte de familiares.
- Afectaciones personales en víctimas indirectas como familiares y allegados.
  Falta de confianza en proveedores de internet.
- Falta de confianza en las instituciones estatales y en los sistemas de protección
- públicos.
  Pérdida de confianza en los vínculos en entornos escolares, laborales, entre otros,
- al ser inoperantes o cómplices de las violencias digitales.



NIVEL SOCIAL

- Se fortalece la desigualdad social y la discriminación por razones de género dentro y fuera de internet.
- Pérdida de la contribución de mujeres, niñas, niños, adolescentes y población LGBTIQ+ en la construcción del tejido social, cultural, etc.
- Internet resulta un espacio inseguro.

La VGD afecta directamente al ejercicio de los derechos humanos por cuanto las víctimas limitan o restringen su derecho a la libertad de expresión, a la salud integral, al acceso a las TICs, así como a una libre vida sexual y la autodeterminación de la identidad de género u orientación sexual, entre otras

3 Protección digital dirigida a personas en movilidad humana

3.1. ¿Qué es la protección digital?

Es la búsqueda y adopción de estrategias y herramientas para cuidar la información personal, laboral y cualquier dato y material sensible que se guarda en dispositivos y en internet, mejorando la capacidad de asegurar las comunicaciones y las interacciones sociales en el mundo virtual.

De manera frecuente, en el ámbito digital se recibe información falsa, acoso digital y violencia sexual. Proteger la información que se encuentra en redes sociales y en los dispositivos electrónicos como celulares y computadoras es la manera de prevenir agresiones digitales, así como en otros espacios de la vida cotidiana.

La protección digital debe entenderse de manera integral en diferentes niveles: individual, relacional y social. De esta manera, las medidas y estrategias de seguridad deben promoverse y aplicarse de manera personal, en las relaciones interpersonales, espacios comunitarios y en la sociedad en su conjunto, entendiendo que los cuidados digitales son una responsabilidad individual y colectiva.

Así, la protección digital resulta una herramienta valiosa que permite ejercer el derecho a una vida libre de violencias de todas las personas, tanto en los espacios físicos como virtuales que se vincula a la seguridad física y emocional.

3.2. Medidas básicas de protección digital

Durante la atención de personas en movilidad humana es fundamental brindar información sobre medidas de protección digital básicas que puedan prevenir accesos no consentidos a dispositivos y cuentas, difusión de datos personales, acoso digital y otras agresiones digitales.

Para ello, es importante identificar qué medidas de protección digital ya aplican las personas en movilidad humana, cuál es su grado de conocimiento en el uso de las TICS y de acceso a internet y dispositivos electrónicos.

La aplicación de medidas de protección digital debe ir acompañada de un proceso de adopción de hábitos que posibilite que estas sean efectivas. Por lo tanto, es necesario que los equipos de atención hagan hincapié en que no son medidas aisladas y puntuales, sino que su utilización y revisión continuadas es recomendable para prevenir riesgos y vulnerabilidades en internet y en el uso de dispositivos electrónicos.

3.2.1. Uso de contraseñas seguras en cuentas y dispositivos

La utilización de contraseñas seguras permite que tanto las cuentas como dispositivos de las personas en movilidad, sean menos vulnerables a accesos no consentidos, ya sea que se realicen a partir de técnicas manuales como probar una contraseña a partir de información conocida de la persona (nombre de un familiar, su mascota, fecha de cumpleaños); o, a través de técnicas de hackeo informático como bots que cotejan listados de contraseñas de manera automática.

De esta manera, los equipos de atención a personas en movilidad humana deben conocer cómo identificar el uso de contraseñas seguras, qué es una contraseña segura y qué herramientas existen para crear contraseñas de manera ágil y sencilla.

El primer paso es identificar si las personas en movilidad **humana utilizan contraseñas en todas sus cuentas y dispositivos:** perfiles de redes sociales, correos electrónicos, celulares y otros dispositivos. Se debe tener en cuenta que no es suficiente con generar una contraseña segura en Facebook o Instagram, si el acceso al celular es abierto o viceversa.

Para ello, será importante consultar qué redes sociales y dispositivos utilizan en su cotidianidad y si aplican contraseñas.

Existen aplicaciones que permiten identificar si una contraseña es segura. Por ejemplo, en el siguiente enlace: https://www.security.org/how-secure-is-my-password/ se puede introducir una contraseña similar (nunca la misma) a la usada en la actualidad, y esta herramienta señalará en qué tiempo puede ser descifrada. Si la aplicación indica que la clave puede ser identificada en segundos, días, meses o un número reducido de años, se trata de una contraseña insegura.

[Ver Anexo 1.1.]

El siguiente paso es dar a conocer a las personas en movilidad humana **qué tipo de contraseñas son seguras** y qué elementos deben contener, tal y como se describe en la Tabla 2.

Tabla 2. ¿Qué es una contraseña segura?

¿Qué es una contraseña segura?
• Debe de tener al menos 12 caracteres. • Contiene letras mayúsculas y minúsculas, números y caracteres especiales (%&$#. /). • No usa datos personales como nombres de familiares, fecha de nacimiento, nombre de la mascota sino hacen referencia a nombres, objetos, hechos o expresiones fáciles de recordar, pero difíciles de adivinar por otras personas. • No se repite en cuentas y dispositivos, es decir, las contraseñas de redes sociales, correos, celulares, el acceso al banco, computadora, entre otros, siempre son diferentes. • Se cambia de manera periódica. En situación de residencia, al menos 1 vez al año. Si las personas están en movilidad, con mayor frecuencia: cada 3 a 6 meses. Ante incidentes de seguridad, es recomendable modificarla de forma inmediata.

En relación a los teléfonos celulares es importante informar a las personas atendidas que las diferentes opciones de seguridad disponibles para controlar el acceso al teléfono, como adoptar un pin, un patrón o una huella dactilar, pueden resultar inseguras; por lo tanto, es preferible el uso de contraseñas alfanuméricas.

Algunas de las razones por las que no se recomienda el uso de pin o patrón tienen que ver con que es fácil que terceras personas puedan reconocer, memorizar y acceder a los dispositivos tras haberlos visto. Por otra parte, el uso de huellas dactilares no garantiza que estas no sean utilizadas sin el consentimiento de los y las usuarios.

¿CÓMO ELABORAR UNA CONTRASEÑA SEGURA?

Para cuando se necesiten cambiar contraseñas, se puede mostrar una técnica para generar contraseñas fáciles de recordar y seguras, que consiste en escoger una frase que recuerden o el fragmento de una canción. Después, se debe transformar la frase con símbolos, mayúsculas y números tal y como se muestra en la Tabla 3.

Tabla 3. Pasos para elaborar una contraseña segura

Pasos para elaborar una contraseña segura
1. Debe de tener al menos 12 caracteres.
2. Elige una frase fácil de recordar: "yo me llamo cumbia"
3. Junta las palabras: yomellamocumbia
4. Incluye mayúsculas: yoMellamoCumbia
5. Sustituye vocales por números: yoMellam0Cumbi4
6. Sustituye otras letras por símbolos y/o incluye símbolos a la frase: yo%Mellam0%Cumbi4
¡Perfecto! Una clave segura es: yo%Mellam0%Cumbi4 (¡Solo usar esta contraseña a modo de ejemplo!).

La mejor contraseña es aquella que no se olvida, por lo que una buena estrategia es tomar nota de las contraseñas seguras que se han creado y registrarlas en una agenda o cuaderno, al que no tengan acceso otras personas. Se recomienda apuntarlas en las páginas centrales para que no sean fáciles de ubicar y no identificar en el texto del cuaderno que se trata de contraseñas de cuentas o dispositivos.

Los equipos de atención a las personas en movilidad humana deben informar de que la elaboración de una contraseña segura es un ejercicio individual y, por tanto, dicha contraseña no debe compartirse con otras personas, ni siquiera con familiares, parejas o personal de atención de entidades y organizaciones.

En caso de que alguna contraseña haya sido identificada por otras personas es fundamental que se recomiende el cambio inmediato de las mismas.

Recursos para descargar y compartir:

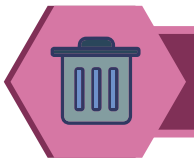
Gráficas informativas de Navegando Libres sobre contraseñas seguras en https://www.navegandolibres.org e **Instagram:** @NavegandoLibres.

3.2.2. Reducir el rastro de datos personales alojados en internet

Cuando se introducen datos personales, información privada, se abren cuentas de usuaria/o, se revela la ubicación o se accede a diferentes páginas y navegadores, se deja una huella digital en internet que puede generar vulnerabilidades si no se toman medidas preventivas. Si bien tener el control absoluto del rastro que se deja en Internet resulta difícil, es posible adoptar precauciones para reducir la huella digital y evitar que exista en línea excesiva información pública sobre las personas en movilidad humana.

Huella digital. Hace referencia al rastro que las personas dejan en Internet a través de sus comunicaciones y conexiones. Es decir, se refiere a toda la información que se sube o baja de internet a través de redes sociales, páginas web y aplicaciones de mensajería, entre otros. Incluye las búsquedas que se realizan en los diferentes navegadores y los datos que se comparten en servidores de internet (por ejemplo, la ubicación).

A continuación, se enumeran recomendaciones sobre protección digital relativa a datos personales:



Eliminar cuentas que no se utilizan

Es importante informar a las personas en movilidad humana que cuentas **de correos antiguos y redes sociales que no se usan**, pueden ser una fuente de búsqueda de datos personales por parte de personas y bots que intentan vulnerar su seguridad. Al eliminar dichas cuentas, **se reduce el riesgo de ser encontradas e identificadas;** algo que puede resultar clave para la protección de personas en situación de refugio.

Todas las cuentas de redes sociales y correos tienen una opción de configuración que permite borrar la cuenta de manera sencilla.

Utilizar aplicaciones de comunicación segura

Facebook Messenger, WhatsApp, Telegram o el chat de Instagram guardan conversaciones y los datos personales compartidos de manera automática, aunque las personas usuarias no generen una copia de seguridad de sus comunicaciones. Esto aumenta la huella digital de las usuarias/os en internet y dispositivos, incluso si algunas de estas aplicaciones ofrecen cifrado de extremo a extremo como WhatsApp.

- En este sentido, **existen aplicaciones de mensajería instantánea más seguras** como Signal. Esta aplicación, además de permitir cifrar los mensajes, no guarda la información en sus servidores reduciendo así el rastro digital de las personas en movilidad humana. Se trata de una aplicación gratuita y se puede descargar fácilmente a través de PlayStore, AppStore u otras tiendas de aplicaciones.

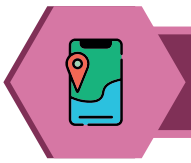
- Si descargar Signal no es una posibilidad porque el teléfono no soporta la aplicación o familiares y amistades no pueden instalarla, **se recomienda que la información sensible se comunique a través de llamadas telefónicas** vía celulares o convencionales (teléfonos fijos).

- En los casos donde las personas en movilidad humana, en particular en situación de refugio, opten por utilizar a la vez aplicaciones como WhatsApp y Telegram debido a que son canales de preferencia para comunicarse con familiares y amistades, es importante recomendar que no se comparta información personal, íntima o sensible mediante mensajes, audios, fotografías, vídeos o llamadas; además de **activar la opción demensajes temporales** en la opción de menor tiempo disponible (de preferencia, menos de 24 horas cuando exista), especialmente si las personas se encuentran en riesgo.
  [Ver Anexo 1.2]

- Es importante mencionar a las personas en movilidad humana que **enviar información sensible a través de audios** (mediante WhatsApp, Instagram Direct, Facebook Messenger, Telegram, y otras aplicaciones) **supone un riesgo adicional.** A diferencia de lo que ocurre con los mensajes escritos donde no siempre será posible identificar a la persona que escribe, la voz permitiría vincular a la persona que enuncia mayor certeza. Por tanto, es importante recomendar el uso de llamadas telefónicas fuera de estas aplicaciones o mensajes escritos mediante aplicaciones seguras como Signal cuando se necesite compartir información delicada o riesgosa.

Recursos para descargar y compartir:

Gráficas informativas de Navegando Libres sobre contraseñas seguras en https://www.navegandolibres.org **e Instagram:** @NavegandoLibres.
Vídeo sobre la huella digital: https://bit.ly/3EvECd7



Ubicación segura y privada

Que las personas en movilidad humana, en particular aquellas que se encuentran en situación de refugio o asilo, revelen su ubicación resulta un factor de riesgo para que terceros accedan a su localización y a información sobre lugares y direcciones que frecuentan.

- Por tanto, **se recomienda que la ubicación esté desconectada tanto en redes sociales, celulares, computadoras y otros dispositivos;** y que solo sea activada de forma controlada y de manera temporal para un determinado fin (como solicitar un taxi), y después sea desactivada.

- Asimismo, en los celulares inteligentes, las aplicaciones instaladas tienen una opción para activar la ubicación. **Para mayor seguridad, es importante que los permisos de ubicación estén desactivados en todas las aplicaciones** y solo sean activados de manera manual y temporal para una actividad específica. Una vez terminada dicha actividad, es preferible desconectar la ubicación de nuevo.
  [Ver Anexo 1.5.]

Al respecto, se debe prestar especial atención a las aplicaciones que no necesitan tener activos los permisos de ubicación en el celular, y si los tuvieran, desactivarlos. A la vez, revisar periódicamente si se mantienen desactivados ya que ciertas actualizaciones del teléfono o de la conexión podrían reactivarlos.

La mayoría de aplicaciones no requieren permisos de ubicación, a excepción de:

- Aplicaciones de taxis o pedidos de comida a domicilio.
- Aplicaciones de mapas y rutas.

Se puede configurar estas aplicaciones para que solo activen el permiso de ubicación cuando estén en uso en las opciones de ajustes que ofrecen las propias aplicaciones.

- Es importante recomendar a las personas en movilidad que **eviten realizar publicaciones en sus redes sociales en tiempo real o con elementos que puedan identificar dónde viven o qué lugares frecuentan** (como fotografías y videos), ya que este tipo de publicaciones puede revelar su ubicación en un momento determinado, haciendo que sea fácil localizarlas.

- **La ubicación debe ser compartida sólo en casos de emergencia y a personas de confianza.** Por ejemplo, si la persona se encuentra en un lugar inseguro y necesita que alguien conocido esté pendiente de su ruta. En otros casos, como por ejemplo la venta de productos o emprendimientos, es preferible que los encuentros se hagan en espacios públicos no cercanos a la vivienda y que no se entregue la información del domicilio. Priorizar la seguridad física debe ser una prioridad.

Recursos para descargar y compartir:

Gráficas informativas y cuña de Navegando Libres sobre ubicación en https://www.navegandolibres.org **e Instagram:** @NavegandoLibres.

Eliminar datos personales y contenido privado de redes sociales

Es importante recomendar a las personas en movilidad que revisen sus contenidos publicados en redes sociales y eliminen **posibles documentos, imágenes, archivos que contengan datos personales** como la dirección, número de documentos de identidad, nombres y fotografías de familiares e información íntima o privada. Incluso si las personas tienen este contenido en una opción para que únicamente la vea la usuaria de la cuenta, puede resultar información a la que acceder mediante hackeo informático o la identificación de sus contraseñas.

Eliminar la información y contenidos que se utilizan en las diferentes cuentas

Si las redes sociales se utilizan con más de un fin, por ejemplo, para compartir fotos personales y para promocionar un emprendimiento, es **recomendable usar diferentes cuentas para cada función.** Esto permite que las cuentas públicas de los emprendimientos y negocios no se vinculen con la información que se comparte a amigos/as, familia y personas conocidas en perfiles privados.

A continuación, se expone un listado de preguntas para que los equipos de atención puedan indagar sobre los hábitos de las personas en movilidad respecto al uso de redes sociales y dispositivos e identificar el nivel de rastro digital que alojan en internet. Obtener este tipo de información con el consentimiento de las personas en movilidad, permitirá a la persona de atención asesorar adecuadamente sobre las medidas de reducción del rastro de datos personales que son necesarias aplicar.

Tabla 4. Preguntas para indagar sobre el rastro de datos personales

Preguntas para indagar sobre el rastro de datos personales
• ¿Utilizas todas las redes sociales en las que te has creado una cuenta? (Facebook, Instagram, Twitter, Tik Tok, Tinder, otras). • ¿Necesitas todas las cuentas de redes sociales y correos que tienes? • ¿Qué aplicaciones usas para chatear o llamar? Y ¿para hablar con tu familia y amistades que siguen en tu país? • ¿Tienes siempre activada tu ubicación? Si no es así ¿en qué momentos activas la ubicación del celular? • ¿Tus cuentas de redes sociales son públicas o privadas? • ¿Publicas fotografías o vídeos tuyos o de tus familiares/amistades en todas tus redes sociales? • ¿Has compartido tu dirección, número del banco, cédula o número de teléfono por Facebook, WhatsApp, Instagram, Gmail u otra red social o aplicación? • ¿Tienes páginas o redes sociales de algún emprendimiento o de tu perfil profesional? Si es así ¿publicas en estas cuentas también información personal o datos/imágenes de amistades o familiares?

3.2.3. Aumentar la privacidad y la seguridad de redes sociales y comunicaciones

Las redes sociales constituyen uno de los espacios donde se dan situaciones de Violencia de Género Digital con mayor frecuencia, en particular, a través de Facebook e Instagram, por tanto, es necesario aumentar la privacidad y la seguridad de las redes sociales, así como de cuentas de correo electrónico y aplicaciones de mensajería instantánea.

Una de las medidas comunes que se pueden aplicar en Facebook, Instagram, WhatsApp, Twitter y Gmail, entre otros, si las personas en movilidad tienen celulares particulares y tarjeta sim, es la **Autenticación en dos pasos,** también conocida como Verificación en dos pasos y Autenticación de dos factores, porque añade una capa de seguridad al acceso de las cuentas y permite prevenir accesos no consentidos cuando las contraseñas han sido vulneradas de alguna manera.
[Ver Anexo 1.3.]

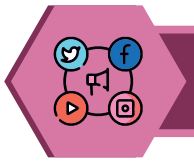
Esta medida de seguridad consiste en verificar la identidad de la usuaria/o una segunda vez tras ingresar la contraseña, mediante el envío de una confirmación de acceso al número de teléfono o al celular a través de internet que se mostrará directamente en la pantalla y bastará con hacer clic, o mediante un mensaje de texto o llamada con un código el cual se deberá ingresar al iniciar sesión en la cuenta. Es fundamental que los equipos de atención señalen que la Autenticación en dos pasos, es viable cuando la personas en movilidad humana cuentan con celular y tarjeta sim propia.

En caso de pérdida o robo del celular es importante que se bloquee la tarjeta sim con la operadora telefónica cuanto antes para que otras personas no puedan tener acceso a este tipo de verificación. Asimismo, tras un robo o pérdida, el acceso a las cuentas donde se hubiera activado la Autenticación en dos pasos, tendrá que hacerse mediante otras preguntas de comprobación a través de correos de recuperación de las redes sociales, el correo electrónico, etc.

En algunas plataformas como Facebook, se pueden activar códigos de recuperación que permiten la entrada a la red social desde otro teléfono. Los códigos de recuperación deben ser anotados y guardados en lugar seguro que no sea el celular (por ejemplo, en un cuaderno) sin mencionar que son códigos para acceder a cuentas personales.

Por otro lado, si las personas en movilidad van a iniciar un tránsito a otro país a corto plazo, es pertinente informarles que en caso de pérdida o robo de la sim o del celular, solo podrán hacer duplicados de su tarjeta sim en el territorio al que pertenezca el número de teléfono que tenían. Adicionalmente, si se planea cambiar de modelo de celular, es necesario desactivar la verificación de dos pasos y activarla al adquirir el nuevo para registrarlo.

Otras medidas sobre las que se puede informar a la población en movilidad son:



EN REDES SOCIALES

• Tener cuentas siempre privadas y no publicar el número de teléfono, dirección, datos bancarios o información íntima.

• Solo utilizar la opción de cuenta pública para emprendimientos o perfiles profesionales. Evitar incluir en estos últimos información personal o íntima, incluida la de familiares y allegados, ni datos que puedan vincular dichas cuentas a los perfiles personales como la dirección o números de teléfonos personales.

• Evitar interactuar con perfiles desconocidos, ya que pueden ser personas interesadas en acceder a información personal o perfiles falsos. En los casos donde se necesite, debido a la búsqueda de trabajo o situaciones afines, no entregar información personal innecesaria como la dirección de vivienda o de familiares. Además, es importante utilizar en las comunicaciones con personas desconocidas correos electrónicos o redes sociales para evitar facilitar el número de teléfono personal o, si se tiene la posibilidad, manejar un chip adicional específico para conversaciones sobre temáticas laborales.
Si se trata de personas que puedan ofrecer un trabajo, revisar la existencia real de la oferta en redes sociales para prevenir situaciones de captación de trata de personas.

• Configurar las opciones de privacidad y seguridad de tal forma que se tenga mayor control sobre la información, como, por ejemplo:

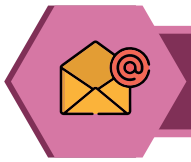
- Ocultar el listado de amigos y amigas en las plataformas que lo permiten para que posibles agresores no puedan ubicar a familiares y allegados.
- Establecer que las publicaciones puedan ser vistas sólo por amigos o amigas.
- Revisar las alertas de inicio de sesión.

Si se ha pasado de tener una cuenta pública a tener una cuenta privada se debe revisar la lista de amigos y amigas y eliminar cualquier perfil sospechoso o desconocido.

• No aceptar solicitudes de amistad de perfiles desconocidos. Si se desconoce el perfil, pero se tiene amistades en común, es importante consultar a las y los perfiles amigos si se trata de una persona conocida en común, ya que podría tratarse igualmente de un perfil falso o malicioso que ha enviado solicitudes a varias personas conocidas.

• Revisar los lugares en los que está abierta la sesión y cerrar las sesiones que sean sospechosas.

• Revisar los inicios de sesión de manera periódica para descartar posibles intentos de acceso no consentido a las cuentas personales en otros dispositivos.



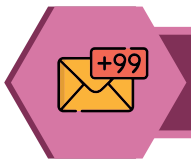
CORREOS ELECTRÓNICOS

• Revisar el correo y el teléfono de recuperación asignado a la cuenta y eliminar cualquier correo o teléfono antiguo o desconocido.

• En el caso de que haya una cuenta de drive vinculada al correo, es importante revisar que esta información no sea pública ni se esté compartiendo con otras personas.

• Revisar los lugares en los que está abierta la sesión y cerrar las sesiones que sean sospechosas.

• Activar las notificaciones de inicio de sesión para poder recibir alertas de posibles accesos no consentidos en otros dispositivos.



CHAT DE MENSAJERÍA INSTANTÁNEA

• Configurar la cuenta para que la foto de perfil y estados sean visibles únicamente para los contactos. Evitar poner fotografías en el perfil donde aparezcan familiares en cuentas que se usan para comunicarse con perfiles desconocidos por asuntos de trabajo o emprendimientos.

• En el apartado de grupos, seleccionar la opción para que no se pueda agregar el número a grupos sin consultarlo previamente mediante un enlace.

• Configurar la pantalla de inicio del teléfono para que no aparezcan los mensajes sin leer cuando la pantalla está bloqueada.

Recursos para descargar y compartir:

Gráficas informativas de Navegando Libres sobre privacidad y seguridad en redes sociales en https://www.navegandolibres.org **e Instagram:** @NavegandoLibres.

3.2.4. Mantenimiento de celulares y seguridad de las aplicaciones

Los dispositivos celulares necesitan de actualizaciones, protección, limpieza de contenidos y revisión para su buen funcionamiento y ser una herramienta segura. Algunas recomendaciones dirigidas al mantenimiento de celulares son:

- Revisar la memoria de almacenamiento y eliminar todo lo que no sea necesario en el "Administrador de archivos".

- Si se encuentra una cuenta de correo vinculada al celular, asegurarse de que está actualizada y no está comprometida con alguna falla de seguridad como un acceso no consentido o robo de contraseñas.

- Eliminar las aplicaciones que no se usen o que se desconozca por quien han sido instaladas en el celular.

- Revisar los permisos que conceden las aplicaciones de tal forma que ninguna tenga acceso a opciones del teléfono innecesarias, por ejemplo:

  - Permiso de ubicación: es preferible que esté desactivado para todas las aplicaciones y solo activarlo en momentos específicos (para llegar a un sitio, pedir un taxi, etc.). Después de realizar la actividad, desactivar la ubicación.

  - Micrófono: se recomienda que esté desactivado en aplicaciones que no se utilicen para hablar.

  - Cámara: se recomienda desactivarla en aplicaciones que no se usen para hacer vídeos o fotografías.

  - Si el teléfono tiene poca memoria interna, una medida para mejorar su funcionamiento es ampliarla con una tarjeta de memoria externa.

  - Realizar respaldos de la información y formatear, al menos una vez al año el celular para asegurar más tiempo de vida. **[Ver Anexo 1.6.]**

  - Tener un antivirus instalado y actualizado en el celular. Algunas opciones que se pueden descargar de manera gratuita en el Play Store o AppStore del

3.2.5. Precauciones en el uso de celulares y computadoras de otras personas

Las personas en movilidad humana pueden tener dispositivos de uso particular o acceder a los de otros de familiares o conocidos, además de conectarse en dispositivos de terceros como computadoras de cybers, celulares de terceras personas, entre otros.

En aquellos casos donde se accede a dispositivos diferentes del particular o no se cuenta con dispositivos propios es importante tener en cuenta lo siguiente:

- Asegurarse de cerrar los inicios de sesión de cuentas de redes sociales y correos antes de abandonar la computadora o el celular.
- Borrar el historial de navegación o acceder directamente desde el modo incógnito del navegador. **[Ver Anexo 1.4.]**
- No almacenar imágenes o información privada en otros dispositivos y cuentas. Si se descargaron por alguna necesidad, se recomienda borrarlas incluso de la papelera de reciclaje y del gestor de eliminación de archivos del celular.
- No guardar contraseñas privadas en otros dispositivos ni en navegadores como *google.*

3.2.6. Medidas de seguridad en la búsqueda de trabajo por internet

Entre los diferentes usos de internet que hacen las personas en movilidad humana está la búsqueda de trabajo. Es importante que los equipos de atención puedan realizar recomendaciones de seguridad para la búsqueda de ofertas de trabajo de manera segura, como, por ejemplo:

- En anuncios, revisar que aparezca el nombre de la persona contratante, empresa o negocio, la dirección o algún dato que permita verificar la existencia real de la oferta de trabajo; también se puede comprobar buscando en redes sociales.
- Solicitar información sobre el trabajo a través de un correo de preferencia o redes sociales, evitando compartir el número de celular directamente.
- No entregar datos personales como dirección de vivienda o número de pasaporte o cédula de ciudadanía.
- Es importante que aquí se tome en cuenta la seguridad física, si el lugar de encuentro es muy apartado o parece ser sospechoso, es preferible que no se asista a la reunión con el supuesto empleador.

3.2.7. Verificación de noticias (evitar la difusión de información falsa)

Una de las formas de garantizar la seguridad en internet es facilitar información sobre cómo detectar noticias falsas que puedan ocultar estafas económicas, engaños sobre trámites migratorios relativos a la solicitud y renovación de visa, entre otras.

Para ello, es necesario que las personas en movilidad se familiaricen con hábitos de validación de noticias que permitan diferenciar entre información confiable e información problemática. Algunos indicadores de noticias falsas son:

- Las fotos de noticias donde no es clara cuál es la fuente. En estos casos, se recomienda contrastar con la fuente original. Si fuera información relativa a leyes migratorias, acceso al asilo u otras normas del país, es preferible revisar las fuentes públicas de las instituciones estatales correspondiente como el Ministerio de Relaciones Exteriores y de Movilidad Humana o solicitar información en consulados y embajadas.
- Si en vídeos o audios que se reciben por WhatsApp aparece una pestaña donde se lee “reenviado muchas veces”.
- Si en los vídeos o audios recibidos por WhatsApp no se menciona lugar y fecha en la que ocurren los eventos porque puede que esa información haya sido sacada de contexto para promover noticias falsas.
- Las fotos de noticias que no van acompañadas con el enlace del artículo completo pueden haber sido alteradas.
- Los títulos sensacionalistas que no están acompañados de las fuentes de donde se ha obtenido la información pueden tratarse de información falsa o tergiversada.

Material para las atenciones: Checklist de básicos sobre protección digital.

En el anexo 2.1. se incluye un formato de lista de tareas para imprimir que puede ser entregado a las personas atendidas a modo de recordatorio sobre las medidas de protección a adoptar y como un plan de recomendaciones para aplicar.

Tabla 5. Actividades sobre medidas de protección digital

Propuesta de actividades dirigida a los equipos de atención que a su vez facilitan espacios de sensibilización y capacitación.

Actividades sobre medidas de protección digital

1. Lluvia de ideas sobre seguridad y protección en internet

Descripción: actividad para identificar cuáles son las percepciones que tienen las y los participantes sobre seguridad y protección en internet.
Pasos: formular al grupo las siguientes preguntas generadoras y anotar las respuestas en papelotes, post-it u otros materiales: ¿Qué es para ti la seguridad en internet? ¿Y la protección en internet?

2. Mi huella digital en internet.

Descripción: actividad para reconocer el rastro de datos personales que se ubican en internet y orientar a la persona a que revise qué información aparece sobre ella de manera pública. En el caso de que las personas encuentren datos personales como la dirección u otros que podrían ser comprometedores o se deseen desalojar de internet, se puede solicitar a las páginas web o plataformas que bajen esta información, o solicitar acompañamiento a Navegando Libres para asistir en esta solicitud.
Pasos: introducir nombres y apellidos en un navegador de búsqueda de internet como Google y revisar en las primeras páginas qué datos aparecen. Según los datos que aparezcan, generar recomendaciones sobre protección digital contenidas en el punto 3.2.

3. Mapa de los usos de internet, detección de riesgos y necesidades de protección

Descripción: actividad para identificar el uso de internet y de dispositivos de las y los participantes, así como elementos y situaciones de riesgo y medidas de protección que son necesarias aplicar.
Pasos: elaborar un mapa imaginario donde se ubique la información que responde a las siguientes preguntas mediante dibujos, listados y/o símbolos:

- ¿En qué lugares usas Internet?
- ¿Qué cuentas de redes sociales y correos electrónicos utilizas?
- ¿Qué dispositivos manejas? ¿Los compartes?
- ¿Qué aplicaciones usas?

Una vez incluida la información, se puede solicitar a las personas que añadan dónde existen riesgos y amenazas en sus usos de internet, cuentas y dispositivos, como, por ejemplo, si se conectan en lugares peligrosos, si tienen comunicaciones inseguras, si usan o no contraseñas para sus cuentas, etc.

En otro momento de la actividad, se puede ampliar el ejercicio del mapa con una tercera intervención respecto a la información que conocen sobre medidas de protección necesarias, tras haberlas explicado previamente. Una pregunta generadora puede ser: ¿qué medidas de protección de las que hemos revisado consideras que necesitas aplicar de manera prioritaria?

3.3. ¿Qué recomendaciones puedo priorizar en una atención?

Todas las medidas básicas de protección digital expuestas en el apartado anterior son relevantes e importantes para prevenir situaciones de VGD o mitigar que persistan agresiones que ya están sucediendo. Sin embargo, en aquellas situaciones donde los equipos cuenten con un tiempo limitado de atención pueden priorizar las siguientes recomendaciones:

- El uso de contraseñas seguras.
- Optar por cuentas de redes sociales personales en modo privado en lugar de perfiles públicos.
- Mantener el GPS y los permisos de ubicación de las aplicaciones desactivados. Solo activarlos al utilizar servicios específicos y después desconectarlos.
- Usar aplicaciones de mensajería instantánea segura como Signal.
- Evitar compartir datos personales (nombres, cédula, pasaporte, dirección, datos bancarios etc.), publicaciones en tiempo real o imágenes en donde se reconozcan lugares frecuentes o de residencia.
- Activar un antivirus en el celular.

4. ¿Cómo detectar la Violencia de Género Digital?

La detección de la Violencia de Género Digital es un paso fundamental en la atención a personas en movilidad humana porque permite identificar, de manera oportuna, agresiones específicas, posibles amenazas de vulneración a la seguridad de dispositivos y cuentas, entre otras situaciones relevantes, y saber si las personas atendidas son víctimas de este tipo de violencia o de otras basadas en el género.

4.1. ¿Qué debo detectar?

Para detectar si las personas en movilidad humana viven una situación de Violencia de Género Digital, se debe prestar atención a:

Los tipos de VGD y las agresiones recurrentes descritas en el Capítulo 2 de esta Guía Metodológica constituyen una orientación clave para determinar situaciones concretas de VGD que pueden estar atravesando las personas en movilidad humana, sin que las violencias expuestas constituyan un listado excluyente de otras

formas de VGD. Es necesario recordar que las TICs son dinámicas cambiantes, así como las agresiones que pueden producirse a partir de ellas.

En caso de determinar la existencia de VGD, es importante brindar información y orientar sobre posibles acciones que se pueden llevar a cabo para enfrentarlas. Para ello, véase el Capítulo 5.

Incidentes de seguridad y eventos extraños

La presencia de incidentes fuera de lo normal, que en apariencia no se relacionan con agresiones específicas de VGD y que se producen en celulares, comunicaciones, redes sociales, e incluso espacios físicos donde se desenvuelven las personas en movilidad humana, pueden vincularse a situaciones de VGD relativas a tentativas de vulneración de dispositivos y cuentas, o a actividades de inteligencia social para recabar información personal y contenido sensible o privado.

Ejemplos de incidentes de seguridad y eventos extraños:

• Inicios de sesión de cuentas de redes sociales y correos electrónicos en dispositivos que no sean utilizados por las personas en movilidad humana. [Ver el ANEXO dónde veo los inicios de sesión]

• Una o múltiples solicitudes de perfiles desconocidos.

• Llamadas reiteradas de números desconocidos, incluidos de otros países o del país de origen, ya sea a teléfonos celulares o convencionales.

• Llamadas que se cortan al descolgar o producen silencios.

• Recibir enlaces extraños con publicidad o información desconocida.

• Que la personas en movilidad perciban que alguien les persigue o vigila físicamente. En estos casos debe valorarse la posibilidad de reasentamiento geográfico.

Agresiones digitales previas

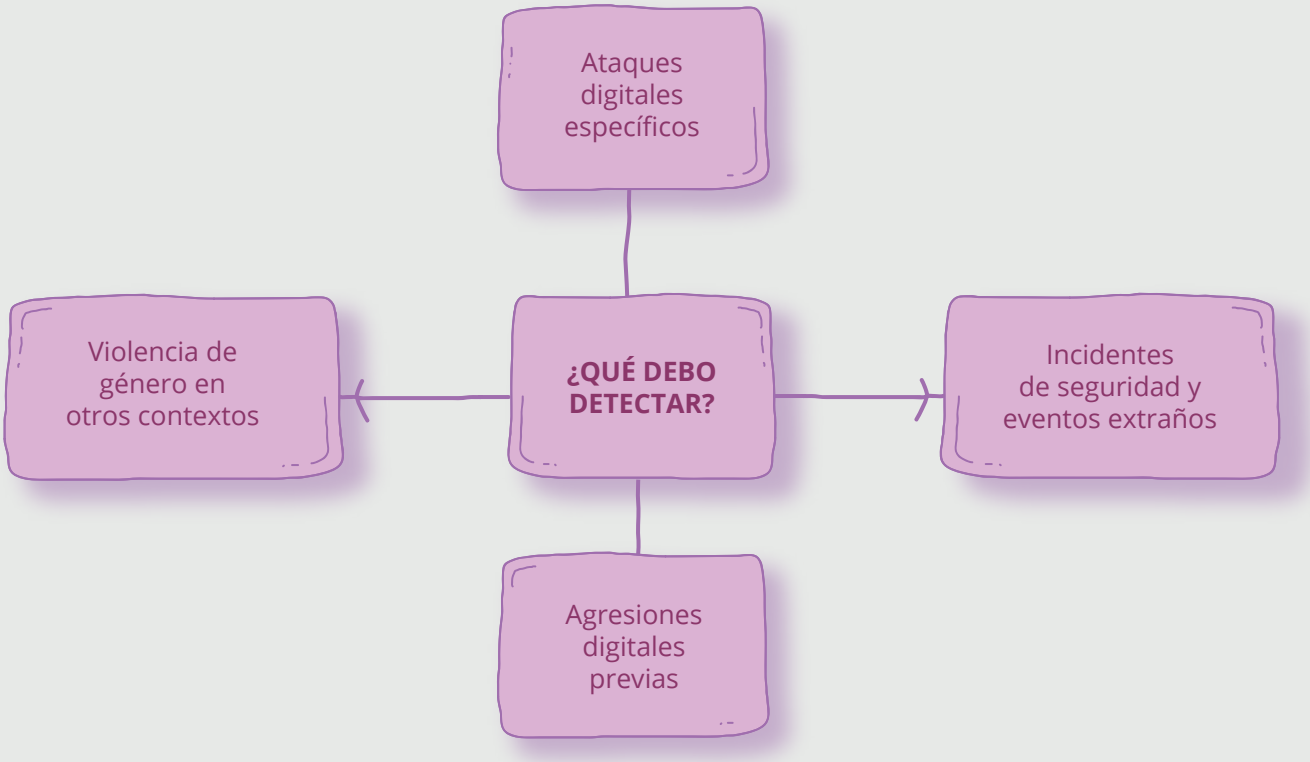
La VGD puede manifestarse de manera periódica y discontinua, es decir, una persona en movilidad humana que no esté viviendo una agresión digital al momento de la atención, no significa que no esté en riesgo o bajo amenaza por ataques digitales ocurridos con anterioridad; es decir, estos ataques o amenazas han podido cesar durante un determinado período de tiempo, pero podrían volver a ocurrir.

Por tanto, identificar si las personas han vivido VGD con anterioridad es una oportunidad para consultar sobre la percepción del riesgo que ellas mismas tienen. En estos casos, será importante realizar un seguimiento sobre las medidas de protección que las personas en movilidad humana han podido aplicar en sus dispositivos y cuentas, y orientarlas nuevamente con las medidas descritas en el apartado 3.2. de la presente Guía Metodológica.

Violencias de género que se producen en otros contextos

En numerosas situaciones, la VGD se inscribe en un continuo de violencias que exceden el ámbito virtual. Nos referimos a mujeres, niñas, niños y adolescentes o población LGBTIQ+ que pueden estar viviendo violencias fuera de los espacios digitales que guardan relación estrecha con la manifestación de VGD como una forma de extender las agresiones que se producen en otros contextos familiares, institucionales, comunitarios y sociales. Es decir, si existe violencia de género en otros contextos, es probable que estas dinámicas se estén reproduciendo en el entorno digital.

Al respecto, será fundamental revisar, con un enfoque interseccional, si las personas atendidas son víctimas de violencia política, violencia de género en el ámbito intrafamiliar, actos de odio por su identidad de género, orientación sexual, etnia, nacionalidad, edad, entre otras condiciones y situaciones.



4.2 Signos de Violencia de Género Digital

Todas las medidas básicas de protección digital expuestas en el apartado anterior son relevantes e importantes para prevenir situaciones de VGD o mitigar que persistan agresiones que ya están sucediendo. Sin embargo, en aquellas situaciones donde los equipos cuenten con un tiempo limitado de atención pueden priorizar las siguientes recomendaciones:

Las situaciones que se enumeran a continuación, pueden ser indicios de agresiones digitales o amenazas de intentos de dichas agresiones.

- Si una persona durante la atención expresa que otras personas conocen constantemente dónde está, lo que hace o con quién conversa, sin que les haya facilitado esta información, puede ser que alguien que haya tenido acceso a sus contraseñas o dispositivos esté accediendo a su información.

- Cuando se observe que existen personas que presionan para que la persona en movilidad comparta sus contraseñas.

- En los casos donde mencione que otras personas utilizan sus dispositivos sin su consentimiento, en su ausencia o por otros motivos.

- Si utilizan información personal para chantajes u obtener algo a cambio.

- Si se reciben enlaces extraños o desconocidos de manera repentina o con publicidad de ofertas de trabajo, premios, entre otros.

- Si perfiles desconocidos les solicitan datos personales sin un motivo o sin explicar adecuadamente para que serán usados, incluyendo las situaciones de búsqueda de trabajo.

- Cuando la batería del celular se descarga constantemente o nunca tiene memoria suficiente después de borrar archivos, puede ser una señal de intento de acceso a dispositivos o cuentas mediante la instalación de aplicaciones espía, rastreo de ubicación, clonación de cuentas u otros mecanismos de vigilancia. En estos casos se recomienda, revisar las aplicaciones instaladas y eliminar aquellas que se desconozcan, además de resetear el celular cuando las persona atendidas sospechen que están siendo espiadas. Para reestablecer los valores de fábrica de un celular es importante guardar primero la información y archivos del mismo, ya que se eliminarán todos los contenidos. [Ver Anexo 1.6]

Para detectar las señales mencionadas, es necesario contar con una lista de interrogantes clave para indagar sobre posibles situaciones indicadoras de Violencia de Género Digital:

Tabla 6. Preguntas para detectar Violencia de Género Digital

Preguntas para la detección de Violencia de Género Digital
• ¿Has recibido enlaces extraños o desconocidos en tu correo, número o en redes sociales?
• ¿Hay personas que conozcan tus claves del teléfono o redes sociales?
• ¿Hay personas que tengan acceso a tu celular y computadora?
• ¿Se descarga la batería del celular con frecuencia o tienes problemas con la memoria llena de manera recurrente?
• ¿Te sientes vigilada/o o espiada/o?
• ¿Ha habido personas que conocen los movimientos que realizas o datos personales sin saber exactamente cómo han tenido acceso a esta información?

4.3 ¿Qué hacer si detecto casos de Violencia de Género Digital?

A continuación, se señalan algunas recomendaciones para la actuación frente a la Violencia de Género Digital que pueden contribuir a su mitigación y a aumentar la protección de las personas en movilidad humana.

• Fortalecer las capacidades de protección digital de las personas atendidas

En todos los tipos de violencia y ataques digitales identificados, será fundamental aumentar las medidas de protección y reforzar las recomendaciones de seguridad. En este sentido, se debe sugerir:

1. El **cambio de contraseñas seguras** en todos los dispositivos y cuentas comprometidas donde se hayan detectado VGD o incidentes y eventos extraños.

2. **Revisión de los correos de recuperación de cuentas de redes sociales y correos electrónicos** y su modificación en el caso de que se hallen correos desconocidos, antiguos o su seguridad esté comprometida. Un correo es inseguro cuando otras personas tienen acceso a las contraseñas o se reciben alertas recurrentes de intentos de inicios de sesión.

Si las personas necesitan cambiar sus correos de recuperación y crear una cuenta nueva, una opción segura y de libre acceso es ProtonMail https://protonmail.com/es/. Este proveedor cifra de manera automática el contenido de los correos, con lo que aporta mayor protección a las personas usuarias.

3. **Aumentar la privacidad y seguridad en redes sociales** tal y como se describe en el apartado 3.2.3 de la presente Guía, en especial la modificación de cuentas públicas a privadas y la activación de la Autenticación en dos pasos si las personas en movilidad tienen las condiciones para ello.

Es importante tener en cuenta que frente a situaciones VGD que estén implicando afectaciones graves a las víctimas, se debe valorar la suspensión temporal de las cuentas. Por ejemplo, en casos de acoso digital mediante llamadas y mensajes indeseadas que no cesen; amenazas que impliquen riesgos a la integridad física de las víctimas o puedan comprometer la reserva de la información sobre su estatus de refugio o asilo; así como en situaciones de difusión de datos personales e imágenes y vídeos de índole sexual sin consentimiento.

Una opción alternativa a la suspensión de cuentas que puede beneficiar a las personas en movilidad para asegurar la continuidad de sus comunicaciones con sus familiares y personas allegadas, es la creación de nuevas cuentas con nombres diferentes o pseudónimos. En estos casos las personas en movilidad deben agregar exclusivamente a personas de su confianza y de las que tenga certeza de que no comprometerán su seguridad, además de mantener las recomendaciones de protección digital en redes sociales expuestas en el apartado 3.2.

4. **Bloquear números y perfiles responsables de las agresiones,** generando previamente evidencias de los ataques con capturas de pantalla y la copia de los enlaces de las publicaciones donde aparezcan. A continuación, se detallan recomendaciones para el registro de evidencias:

Tabla 7. Registro de evidencias de las agresiones digitales

Registro de evidencias
• Realizar y guardar capturas de pantalla de las agresiones. • Si las agresiones se dan en alguna red social o plataforma, adjuntar también el URL o enlace del sitio donde estas se ubican. • Realizar un respaldo de las evidencias en un lugar seguro, de preferencia un disco externo o pen drive.

• Denuncia de las agresiones en las plataformas y páginas web

Tanto las redes sociales como otras plataformas de internet contienen "Normas Comunitarias y Términos de Uso" que ofrecen rutas de denuncia de incidentes. En este sentido, es fundamental que los equipos de atención informen a las personas en movilidad sobre cómo denunciar contenidos maliciosos, perfiles agresores y actos violentos.

Si bien se recomienda que el reporte en plataformas se interponga en cualquier situación de VGD, es imprescindible que se realice en los siguientes casos:

- Suplantación de identidad: ya sea por la clonación o duplicación del perfil de la usuaria o cuando se produce una apropiación no autorizada de sus cuentas y las personas quedan sin acceso a las mismas.

- Robos de contraseñas.

- Extorsión, incluida de carácter sexual.

- Actos de difamación, incluida de naturaleza sexual.

- Contacto de adultos con NNA (grooming).

- Pornografía infantil y otros casos de explotación sexual a NNA por redes sociales y difusión no consentida de imágenes y vídeos íntimos o sexuales de personas adultas.

Para estos casos, y cuando se ha producido a través de la red social Facebook, esta plataforma tiene una opción de denuncia directa que permite identificar imágenes y vídeos de desnudos y desalojarlos de la red. Sigue las indicaciones aquí: https://bit.ly/3Hhmo0J .

- Difusión de datos personales e información privada sin autorización.

- Mensajes y publicaciones de incitación al odio o expresiones discriminatorias.

Para denunciar las agresiones, las redes sociales ofrecen diferentes rutas de reporte de situaciones que infringen sus normas comunitarias y términos de uso y corresponden a violencias digitales como la difusión no consentida de imágenes y vídeos, la suplantación de identidad, la obstrucción al acceso a cuentas, entre otras. La Tabla 5 contiene enlaces con instrucciones de cómo denunciar dichas situaciones en diversas plataformas de redes sociales.

Tabla 8. Información sobre cómo denunciar agresiones en las plataformas de redes sociales

Red Social	Enlaces informativos
Facebook	https://www.facebook.com/help/263149623790594
Instagram	https://www.facebook.com/help/instagram/547601325292351
Twitter	https://help.twitter.com/es/safety-and-security/report-abusive-behavior
Tiktok	https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-user
Tinder	https://policies.tinder.com/safety-and-policy/intl/es/

Respecto a los casos de pornografía no consentida, existen plataformas en América Latina que pueden orientar los procesos de denuncia como Acoso.online. Consulta más información aquí: https://acoso.online/ec/

• Brindar información sobre atención psicológica y asistencia legal gratuita

En toda atención se debe indagar sobre expectativas y necesidades de las víctimas sobre la asistencia de servicios. En este sentido, es una buena práctica recomendar servicios de atención psicológica públicos, como el Sistema Nacional de Salud y los Servicios de Protección Integral de la SDH, y aquellos descentralizados de gobiernos locales.

Por otro lado, es necesario facilitar información sobre orientación y patrocinio legal gratuitos de tal forma que las personas atendidas puedan conocer las posibles opciones de denuncia. Para ello, una opción es la Defensoría Pública https://bit.ly/3Jjqd7H así como organizaciones de la sociedad civil especializadas.

• Facilitar información sobre cómo acceder a medidas de protección

Las víctimas de VBG tienen derecho a medidas de protección. En este sentido, es importante informar sobre cómo obtenerlas tanto en la Fiscalía General del Estado y

Unidades Judiciales, como en las Juntas Cantonales de Protección de Derechos o Tenencias Políticas.

Para ello, se recomienda facilitar información clave como:

• **Cómo hacer una denuncia:** https://www.fiscalia.gob.ec/como-hacer-una-denuncia/

• **Direcciones de ubicación de las instituciones públicas:** FGE y Unidades Judiciales especializadas en violencia contra las mujeres o Unidades Multicompetentes https://www.fiscalia.gob.ec/directorio-fiscalias/ https://bit.ly/3z70UAP o Juntas Cantonales de Protección de Derechos y Tenencias Políticas https://www.funcionjudicial.gob.ec/es/genero

• **Tiempo estimado de atención:** tanto en las Unidades Judiciales como en las Juntas Cantonales de Protección de Derechos, las medidas deben ser entregadas en el mismo día que se soliciten en el horario de atención dichas instituciones (lunes a viernes de 08h00 a 17h00).

• **Requisitos:** no es necesario tener un documento de identificación personal para acceder a las medidas, aunque de preferencia se puede llevar cédula o pasaporte si las personas en movilidad cuentan con dicho documento. Es importante informar que en caso de que el personal de atención se niegue a receptar la denuncia, se debe solicitar la presencia de la máxima autoridad de la institución y, en caso de no obtener el trámite, acudir a instancias como la Defensoría del Pueblo para buscar asesoramiento.

• Facilitar información sobre cómo denunciar

Las víctimas de VGD tienen derecho a denunciar. Se recomienda que se brinde información sobre orientación legal gratuita para acompañar el proceso de denuncia, así como los lugares donde interponer una denuncia: https://bit.ly/3z70UAP

• Ofrecer información sobre grupos de apoyo y organizaciones especializadas en violencia de género de la sociedad civil

Una buena práctica es facilitar a las personas en movilidad humana información sobre organizaciones de la sociedad civil que brindan acompañamiento en situaciones de violencia de género. Además de aquellas especializadas en el acompañamiento a sobrevivientes de VGD; en el caso de Ecuador existen la línea de atención de Navegando Libres es accesible mediante correo electrónico seguro: reportaviolencia@navegandolibres.org y la página de Ayuda de ACNUR: https://help.unhcr.org/ecuador/

Por otro lado, existen líneas de atención a nivel regional creadas por organizaciones de la sociedad civil que pueden brindar asesoría y contactos de derivación en materia de VGD. En los casos de personas en movilidad humana en tránsito que vayan a cambiar de país a corto plazo y estén siendo víctimas de VGD, una opción para garantizar acompañamiento en el país de destino es informar sobre dichas líneas de atención:

- Access Now - América del Sur: https://www.accessnow.org/help-es/?ignorelocale
- Acoso Online - Recursos para Latinoamérica: https://acoso.online/
- Vita Activa - Centro América y México: https://vita-activa.org/tag/linea-de-ayuda/
- Luchadoras – México: https://luchadoras.mx/
- María Lab – Brasil: https://www.marialab.org/

REFERENCIAS BIBLIOGRÁFICAS

• Asamblea Nacional del Ecuador, *Ley Orgánica Reformatoria del Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos, 2021.*

— *Ley Orgánica Integral para la Prevenir y Erradicar la Violencia contra las Mujeres*, Registro Oficial Suplemento 175, 2018.

• Peña Ochoa, Paz (coord.): ***Reporte de la Situación de América Latina sobre la Violencia de Género ejercida por Medios Electrónicos***, 2017. Disponible en: https://hiperderecho.org/wp-content/uploads/2018/03/Reporte_Violencia_Genero_Linea_Latinoamerica.pdf

• Taller de Comunicación Mujer: ***Moverse Seguras y Seguros. Análisis de la situación de Violencia de Género Digital contra mujeres y población LGBTIQ+ refugiada y migrante en Ecuador***, 2020. Disponible en: https://www.navegandolibres.org/images/navegando/medios/otros/Moverse_seguras_final_compressed.pdf

— *Guía para Moverse Seguras y Seguros*, 2020. Disponible en: https://www.navegandolibres.org/images/navegando/medios/otros/Guia_Acnur_migrar_final_compressed.pdf

ANEXOS

1 Recursos y enlaces informativos

1.1. Sitio Web "How Secure Is My Password?":

Enlace de acceso: https://www.security.org/how-secure-is-my-password/

Imagen 1. Al entrar al enlace, aparece un campo para introducir la contraseña de prueba.

Imagen 2. Resultado de una contraseña insegura: se puede descifrar en 11 microsegundos.

Imagen 3. Resultado de una contraseña segura: se puede descifrar en 53 millones de años.

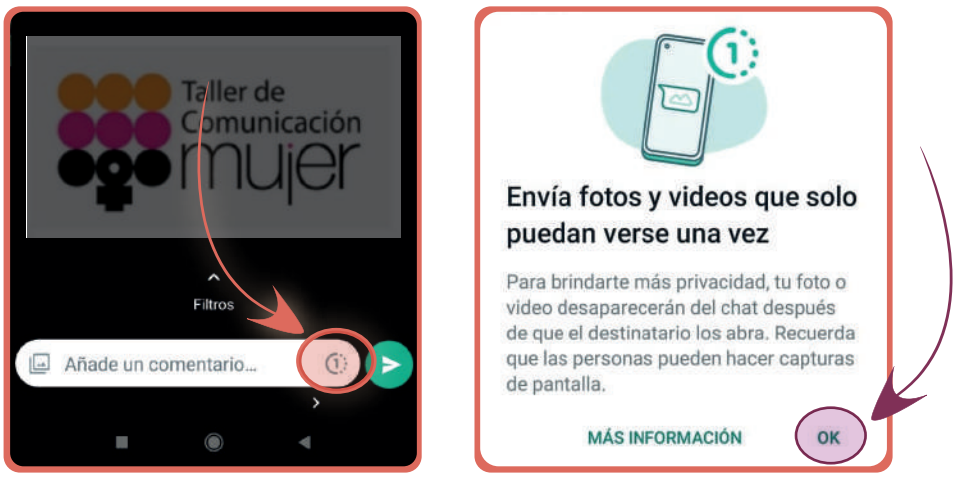
1.2. ¿Cómo activar las opciones de mensajes temporales, efímeros y autodestrucción de imágenes en aplicaciones de mensajería?

Eliminar mensajes, imágenes y vídeos en los chats de mensajería aumenta la seguridad de las personas usuarias y reduce el rastro de datos personales.

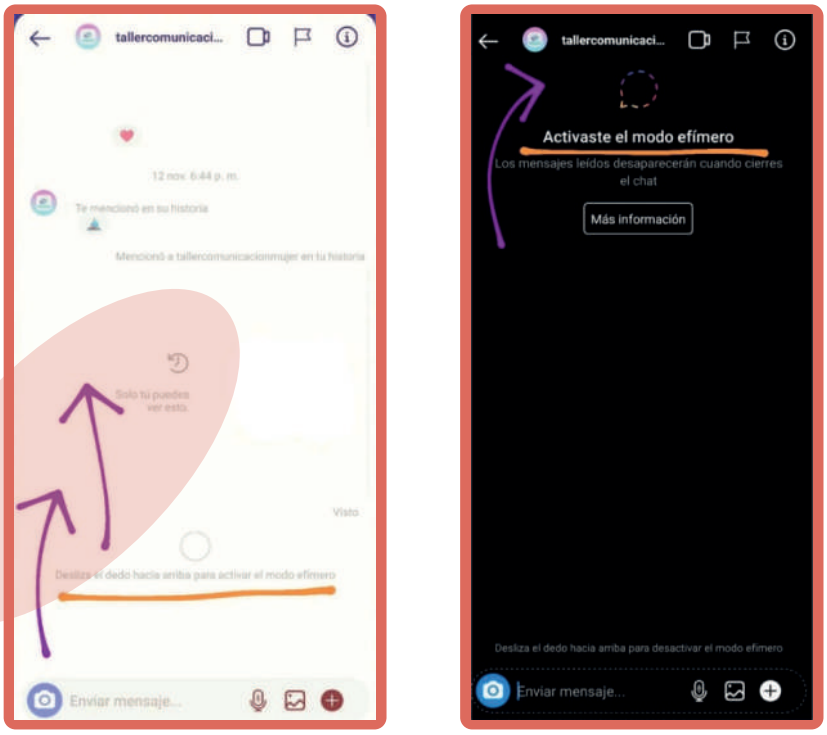
A continuación, se incluyen los pasos para activar estas opciones en diferentes aplicaciones desde un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el modelo y el sistema operativo del teléfono o si se trata de una computadora, así como ser actualizadas o modificadas por las plataformas de las aplicaciones con el tiempo.

En WhatsApp. Para activar los mensajes temporales abre el chat o conversación en la que quieras activarlos y presiona sobre el nombre de contacto. Ahí se abrirá la siguiente pantalla donde aparece la opción.

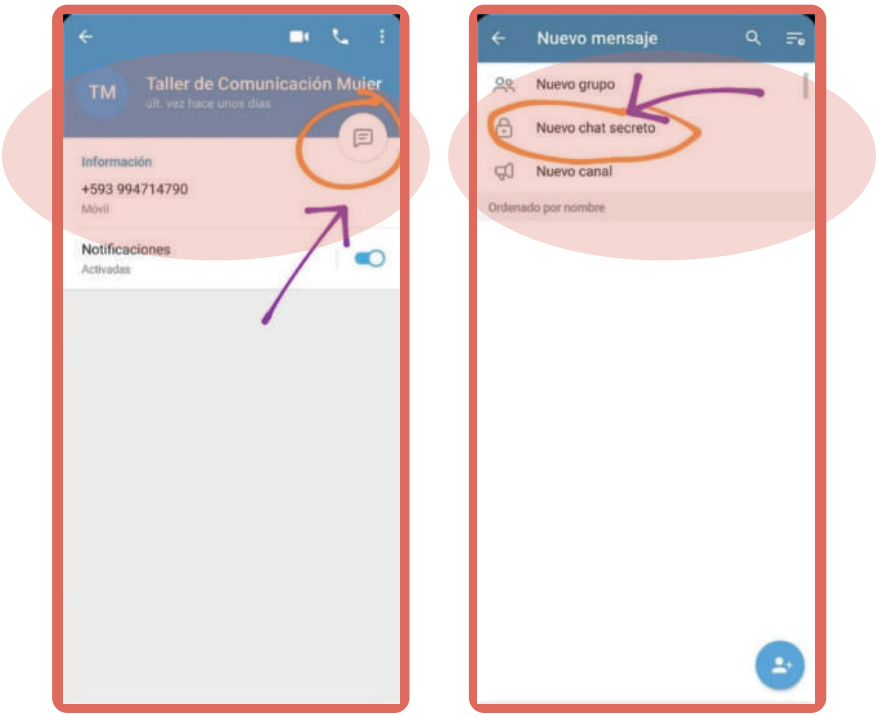
Adicionalmente, activa la opción para que las fotos y videos puedan ser vistos una sola vez. Selecciona un chat y aparecerá un símbolo en el campo de escritura donde se muestra el número 1 dentro de un círculo. Presiónalo y pulsa “OK”:



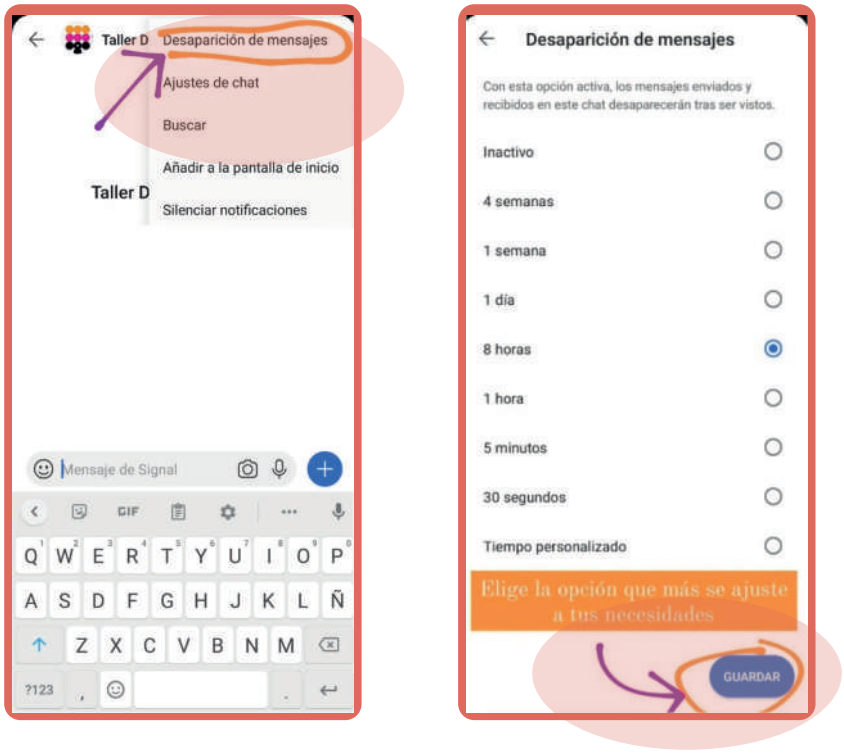
En Instagram. Abre el chat en el que quieres activar los mensajes efímeros y desliza el dedo hacia arriba.



En Telegram: Para activar la autodestrucción de mensajes antes se debe activar la opción de chat secreto. Esta opción se activa desde el chat que queremos convertir a chat secreto, se debe presionar en el nombre del contacto y seguir los pasos a continuación. Después pulsa en los 3 puntos y presionar sobre "Configurar autodestrucción".



En Signal: Para activar los mensajes temporales Signal debemos abrir el chat o conversación en la que queremos activarlos y, una vez abierto el chat, presionar sobre los tres puntos que aparecen en la esquina superior derecha. Ahí se abrirá la siguiente pantalla:

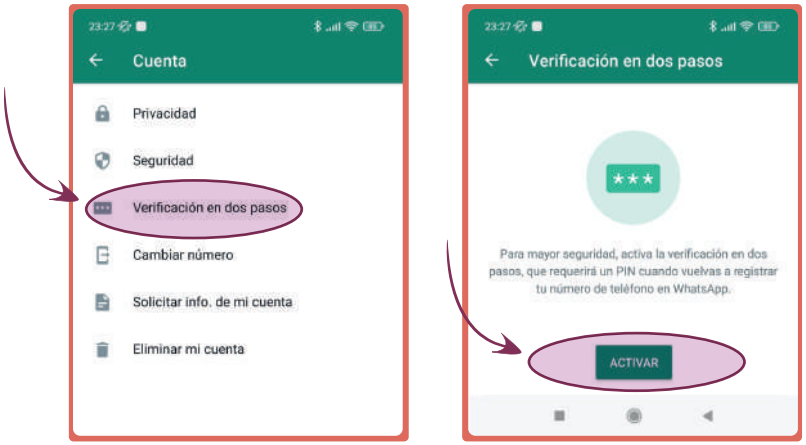


1.3. ¿Cómo activar la verificación en dos pasos?

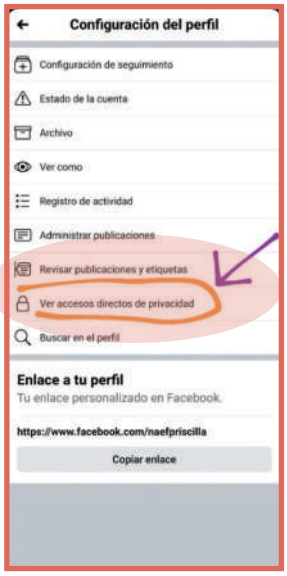
La verificación en dos pasos, Autentificación de dos pasos o Autentificación de dos factores aumenta la seguridad del acceso a cuentas de redes sociales, correos electrónicos y chats de mensajería.

A continuación, se incluyen los pasos para activar esta opción en diferentes plataformas desde un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el modelo y el sistema operativo del teléfono, y si se trata de una computadora, así como ser actualizadas o modificadas por las plataformas con el tiempo.

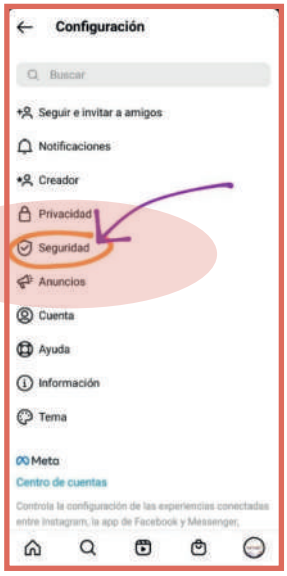
En WhatsApp. Entra en los «Ajustes», pulsa la opción «Cuenta» y, después: «Verificación en dos pasos». Enlace informativo: https://bit.ly/3mFY295



En Facebook. Entra en “Configuración del perfil”, pulsa en “Ver accesos directos de privacidad” y en el apartado de “Protección de la cuenta” selecciona “Usar la autentificación en dos pasos”. Enlace informativo: https://bit.ly/3sCEPZS



En Instagram. Entra en “Configurar”, pulsa “Seguridad” y la opción “Autenticación en dos pasos”.



Cuentas de Google (Gmail, Google Fotos, Google Drive, etc.). Ver indicaciones aquí: https://bit.ly/3qzO4Y0

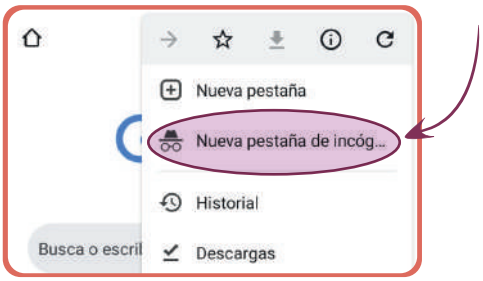
En Twitter.
https://help.twitter.com/es/managing-your-account/two-factor-authentication

Para otras cuentas, se puede buscar esta información en el explorador de preferencia.

1.4. Activar la navegación en modo incógnito y borrar el historial de búsqueda y activar

Navegar en incógnito evita que se guarde el historial de la navegación. A continuación, se incluyen los pasos para activar esta opción en el navegador Google Chrome desde un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el navegador, el modelo y el sistema operativo del teléfono, y si se trata de una computadora, así como ser actualizadas o modificadas por los servidores con el tiempo. No obstante, esta acción se puede hacer de manera similar en varios navegadores como Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, entre otros.

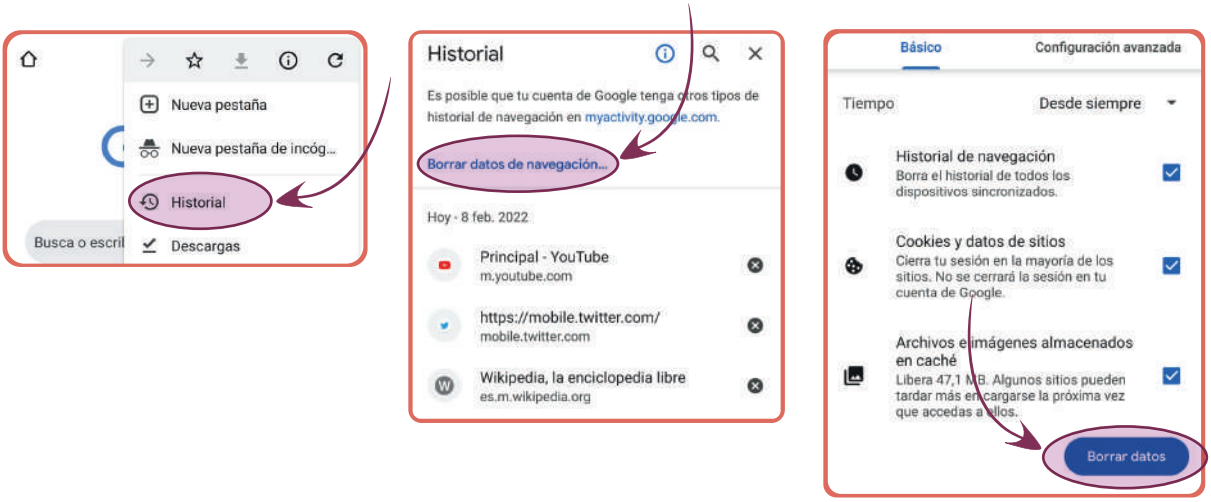
Al abrir el navegador y presionar en los tres puntos que aparecen en la esquina superior derecha, se abre la siguiente opción:



Eliminar el historial de búsqueda del navegador que se usa en computadoras propias o de terceros, permite reducir la huella digital.

A continuación, se incluyen los pasos para activar esta opción en el navegador Google Chrome desde un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el navegador, el modelo y el sistema operativo del teléfono, y si se trata de una computadora, así como ser actualizadas o modificadas por los servidores con el tiempo. No obstante, esta acción se puede hacer de manera similar en varios navegadores como Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, entre otros.

Al abrir el navegador y presionar en los tres puntos que aparecen en la esquina superior derecha se abre la siguiente opción:

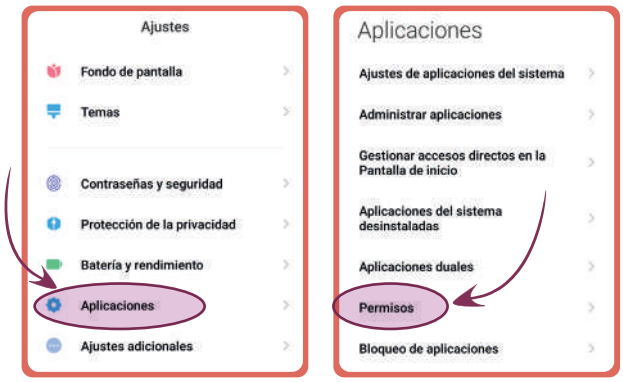


1.5. ¿Cómo revisar los permisos de las aplicaciones del teléfono?

Seleccionar de manera manual permisos de las aplicaciones del teléfono nos posibilita tener mayor control sobre los dispositivos electrónicos y la información que es alojada en internet de manera automática. Especialmente se deben tomar en cuenta las opciones de ubicación, micrófono y cámara y desactivarlos en todas las aplicaciones que sea posible o innecesaria.

A continuación, se incluyen los pasos para revisar esta opción en un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el modelo y el sistema operativo del teléfono, y si se trata de una computadora, así como ser actualizadas o modificadas por los fabricantes de telefonía con el tiempo.

Entra en Configuraciones > Aplicaciones >Permisos de Aplicaciones:

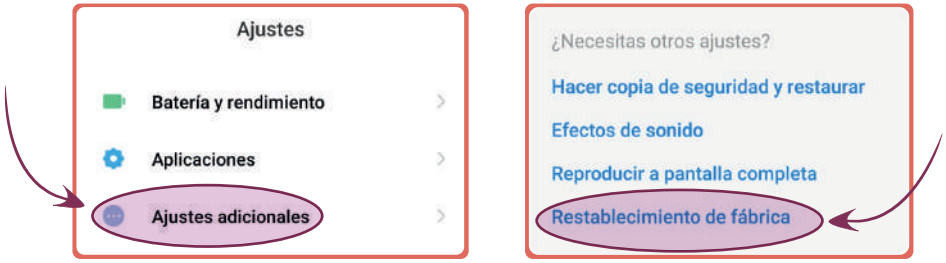


1.6. Reseteo o restauración del celular

Reestablecer los valores de fábrica del teléfono permite eliminar información y aplicaciones innecesarias o maliciosas. Se recomienda llevar a cabo este proceso al menos una vez al año y ante la sospecha de tener un virus o aplicaciones espía instaladas. Es necesario realizar un respaldo de la información antes de resetear el teléfono, ya que toda esta información será eliminada.

A continuación, se incluyen los pasos de esta opción en un celular Android. Sin embargo, debe tomarse en cuenta que las indicaciones pueden variar según el modelo y el sistema operativo del teléfono, y si se trata de una computadora, así como ser actualizadas o modificadas por los fabricantes de telefonía con el tiempo.

Entra en Configuraciones >Ajustes Adicionales >Restauración de Fábrica



2 | Materiales

2.1. Testimonios sobre Violencia de Género Digital y formas de ataques

"Y ella empezó a amenazarme por Facebook. Yo tengo todos los mensajes, donde decía que si yo no le pagaba la plata y yo no le daba la perra ella me podía mandar a deportar para mi país con mis hijos. Que no le importaba si tenía hijos o no. [...] Y agarró fotos de mi Facebook. Yo le dije que en mi país eso era un delito". (Mujer de nacionalidad venezolana).

[Testimonio sobre acoso digital y acceso no consentido a cuentas. Formas de ataque: amenazas y lenguaje violento, extorsión económica y robo de imágenes.]

"También cuando busco trabajo tengo pruebas de cómo la acosan a uno sexualmente cibernéticamente. He seguido buscando trabajo y recibo mensajes: ´que si me porto mal´, ´que cuál es la necesidad que tengo de trabajo´, o me dicen: ´bueno, pero mándame tu foto´, o ´que cuánto me atrevo´ insinuando que me acueste con él; ´que si soy una chica mala´ y cosas así". (Mujer de nacionalidad venezolana).

[Testimonio sobre Violencia Sexual Digital. Forma de ataque: acoso de naturaleza sexual].

"Mi ex pareja siempre sabe lo que estoy escribiendo y con quien me estoy escribiendo, pero yo ya no estoy con ella. Ella vive en otro país. Por eso, es que yo me entero que ella ha dejado en mis correos electrónicos su correo como correo de recuperación, siempre pudo acceder". (Mujer en movilidad humana).

[Testimonio sobre acceso no consentido a cuentas. Formas de ataque: manipulación de correos de recuperación].

“En los chats de WhatsApp de la escuela de mis hijas empezaron a correr los comentarios de parte de los padres de familia y la profesora no dijo nada, todos los comentarios eran en contra de los migrantes, y yo no podía decir nada” (Mujer en movilidad humana).

[Testimonio sobre discurso de odio y expresiones discriminatorias].

PREGUNTAS GENERADORAS:

1. ¿Qué tipo de Violencia de Género Digital identificas?

2. ¿Cuáles son las agresiones específicas que sucedieron?

Checklist de mis básicos de protección digital

(Llena esta lista de tareas según apliques las medidas recomendadas marcando la opción correspondiente)

PRIORIDADES

- [ ] Tener **contraseñas seguras** en todas mis cuentas de redes sociales, correos electrónicos, celular y otros dispositivos (¡ni pin ni patrón!).
- [ ] **Usar el GPS solo cuando lo necesito** como al pedir un taxi. Desactivarlo siempre tras utilizarlo.
- [ ] **Comunicarme de manera segura:** descargar Signal (¡es gratuito!) en mi celular y pedir a mi familia y amistades que hagan lo mismo. No usar WhatsApp, Facebook Messenger o Instagram para compartir información sensible.
- [ ] **No usar WhatsApp ni Telegram para conversaciones donde incluya datos personales o sensibles como mi ubicación.** Activar las opciones de mensajes temporales de estos chats.
- [ ] **Tener mis cuentas personales de redes sociales en modo privado** (solo perfiles públicos para mis emprendimientos).
- [ ] **Desactivar los permisos de micrófono, cámara y ubicación en las aplicaciones** de mi celular que no los necesitan.
- [ ] **Actualizar mi antivirus en el celular y computadora.** Hacer un escaneo periódicamente para eliminar posibles virus.

OTRAS MEDIDAS PARA APLICAR A CORTO PLAZO

- [ ] **Hacer una búsqueda en Google de mi información personal** y solicitar la eliminación de los datos que no quiero que sean públicos en los lugares donde encontré esta información.
- [ ] **Eliminar las cuentas de redes sociales o correos electrónicos que no uso.**
- [ ] **Activar la Verificación en 2 pasos** en todas las cuentas que lo permitan.
- [ ] **Revisar las configuraciones de privacidad** en mis cuentas de redes sociales y correo electrónico.
- [ ] **Eliminar datos personales y contenido privado en mis redes sociales** (incluso si está subido en modo "solo yo").
- [ ] **Desinstalar las aplicaciones que no utilizo,** incluidas juegos y aquellas que no conozco.
- [ ] **Revisar qué correos o números de teléfono tengo para recuperar mis cuentas** y asegurarme que son míos. Si no es así, cambiarlos.
- [ ] **Verificar la información de las noticias que recibo antes de reenviarla** (fuente, fecha, autoría).
- [ ] **Resetear mi teléfono** al menos una vez al año después de haber guardado mis datos y archivos.

*Para aplicar las medidas básicas de protección digital... **¡RECUERDA!**

Las contraseñas son seguras cuando:

• Tienen al menos 12 caracteres, mayúsculas, minúsculas, números, y %$/(&)

• Evitas nombres de mascotas, fechas de cumpleaños, nombres de familiares, etc.

• No repites nunca tus contraseñas entre diferentes cuentas y dispositivos.

• Las cambias al menos una vez al año o cuando has tenido incidentes de seguridad.

Sobre el antivirus:

• Nunca tengas más de un antivirus instalado.

• Si no puedes pagar un antivirus, puedes usar la versión gratuita de AVG, Avira o Avast.

Privacidad y seguridad en redes sociales:

• Evita aceptar solicitudes de personas desconocidas.

• No realices publicaciones en tiempo real donde se muestre tu ubicación.

• Si tienes un perfil de tu emprendimiento o un perfil de activista, no compartas información personal ni de familiares (incluidas fotografías y vídeos) en este medio. - Crea cuentas diferentes para separar tu información laboral u organizacional, de tus cuentas personales.

GUÍA METODOLÓGICA SOBRE VIOLENCIA DE GÉNERO DIGITAL

DIRIGIDA A EQUIPOS DE ATENCIÓN A PERSONAS EN MOVILIDAD HUMANA

Taller de Comunicación mujer

UNHCR ACNUR
La Agencia de la ONU para los Refugiados