REPÚBLICA DE PANAMÁ
GOBIERNO NACIONAL

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

GUÍA DE DENUNCIA EN CASOS DE VIOLENCIA DE GÉNERO EN INTERNET

GUÍA DE DENUNCIA EN CASOS DE VIOLENCIA DE GÉNERO EN INTERNET

En esta guía se describen las conductas que podrían constituir violencia de género en internet, además se diseñan las etapas y ruta del proceso de denuncia e investigación para un adecuado abordaje institucional

Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI)

ÍNDICE

PRESENTACIÓN

Las violaciones a los derechos humanos afectan tanto a hombres como mujeres, sin embargo, su impacto varía de acuerdo con el género de la víctima. La violencia de género puede adoptar diversas formas, sobre todo en estos tiempos, donde el espacio físico se ha trasladado a un entorno virtual, lo que ha permitido una extensión de este tipo de violencia a la esfera digital.

Algunas investigaciones sobre el tema han arrojado que las mujeres son víctimas de ciertos tipos de violencia digital de manera desproporcionada en comparación con los hombres. De acuerdo con un estudio publicado en 2015 por la Comisión de la Banda Ancha para el Desarrollo Sostenible, de las Naciones Unidas, el 73% de las mujeres habían vivido alguna forma de violencia de género en línea, mientras que el 61% de los atacantes eran hombres (UNBC, 2015). [1]

De manera que, la variable de género no es invisible a este fenómeno, mismo que implica como nexo causal, la vulneración de los datos personales de las víctimas, hablamos de fotos, vídeos y audios de carácter íntimo que se exponen en el mundo virtual, acarreando consecuencias en todos los ámbitos de la vida de las víctimas. Ya que en sus derivaciones no solo vulnera la privacidad, sino también la honra, el derecho a la protección de los datos personales, la libertad de expresión, así como la integridad física, económica y psíquica de sus víctimas.

Es claro que el espacio digital no fue diseñado para reproducir dinámicas de opresión hacia ciertos grupos como mujeres activistas, feministas, comunidad LGBTIQ+, y en contra de contenidos que puedan estar relacionados con sus agendas de derechos humanos. No obstante, al día de hoy, no existe país en América Latina que escape a esta problemática, el desconocimiento sobre los mecanismos de protección existentes y el temor de las víctimas de ser doblemente victimizadas por denunciar sus casos ante instituciones que no cuentan con protocolos adecuados para su atención, supone una amplia subestimación de la violencia de género digital.

[1] *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta / [Preparado por la Secretaría General de la Organización de los Estados Americanos]. v; cm. (OAS. Documentos oficiales; OEA/Ser.D/XXV.25. Disponible en: https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf*

En el caso de Panamá, el estudio "Estado de la legislación en materia de violencia de género digital en Latinoamérica" publicado en el año 2021 por EUROsocial + Programa para la Cohesión Social en América Latina[2] , determinó que, existe una normativa integral de prevención de la violencia de género, y si bien, sus diferentes normas no contienen disposiciones expresas en materia de violencia digital, sí contiene algunas disposiciones relevantes que permiten abordar el fenómeno, mismas que se desarrollarán en la presente guía.

Por otro lado, deben llamar a la acción las estadísticas del Ministerio Público en los últimos cinco años, donde se ha registrado un incremento del 198% en el delito de extorsión, cerrando 2016 con 123 casos, mientras que el 2020 cerró con 424 casos por el mismo delito. De igual manera se reporta un aumento en denuncias por el delito contra la seguridad informática donde el incremento entre el año 2016 y el año 2021 fue de 421%, siendo los años 2020 y 2021 los de mayor incidencia de casos [3].

La presente guía, además de visibilizar el fenómeno de la ciberviolencia de género, pretende promover la implementación de protocolos y esfuerzos hacia la necesaria coordinación interinstitucional entre las autoridades competentes de prevenir, atender y sancionar la violencia de género en internet, ya que para atender este flagelo se requieren acciones y políticas coordinadas a nivel estatal, es decir, la necesaria coordinación entre entes pertenecientes a diferentes órganos y poderes (Legislativo, Ejecutivo y Judicial).

En concreto la legislación panameña otorga competencias en la materia al Ministerio Publico, al Servicio Policial Especializado en Violencia de Género del Ministerio de Seguridad y la División de Ciberdelito de la Dirección de Investigación Judicial. Además, existen otros organismos que cooperan y pueden dar soporte a las víctimas de violencia digital, entre estos: Instituto Nacional de las Mujeres (INAMU), el Comité Nacional contra la Violencia en la Mujer (CONVIMU) y el Observatorio Panameño contra la Violencia de Género (OPVG) en coordinación con la Autoridad Nacional de Transparencia, Acceso a la Información (ANTAI).

[2] Estado de la legislación en materia de violencia de género digital en Latinoamérica. Ana Karen Cortés Víquez y Jessica Matus Arenas. EUROsocial + Programa para la Cohesión Social en América Latina. Publicado en el año 2021: https://eurosocial.eu/wp-content/uploads/2022/06/Herramientas_103_Estado_de_la-legislacion_materia_de_violencia_genero.pdf

[3] Nota de prensa página oficial del Ministerio Publica Panamá, disponible en sitio web: https://ministeriopublico.gob.pa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/

OBJETIVOS

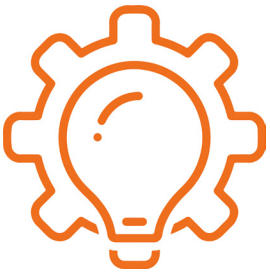
Objetivo general

La presente guía pretende describir las conductas que podrían constituir violencia de género en internet, así como orientar sobre las etapas y ruta del proceso de denuncia e investigación de los casos de violencia digital que puedan llegar a conocer las instituciones públicas competentes de la República de Panamá.

Objetivos específicos

- Reconocer mediante la concientización institucional, la violencia de género en línea como una forma de violencia que debe prevenirse, atenderse y sancionarse oportunamente.
- Incorporar una perspectiva de género en el accionar institucional que permita abordar de manera eficiente en las diversas las etapas y ruta de denuncia para su debida atención, investigación y sanción.
- Promover que las unidades de atención de las instituciones competentes en materia de violencia de género, coordinen, atiendan y asesoren adecuadamente a las víctimas en casos de violencia en línea.

METODOLOGÍA



El fenómeno de la violencia de género digital ha sido poco explorado en la región centroamericana, por lo que las técnicas aplicadas para diseñar esta guía fueron revisión documental, análisis de distintas normas y revisión de fuentes digitales. Los datos cualitativos se han obtenido en un período de cuatro semanas entre octubre y noviembre mediante recopilación de información obtenida de repositorios públicos, páginas oficiales de las instituciones públicas y algunas entrevistas a funcionarios/funcionarias públicas en instituciones clave en el tema.

Las solicitudes de entrevistadas fueron dirigidas mediante correos electrónicos a personas funcionarias públicas que trabajan en instituciones claves para atender los casos de mujeres víctimas de violencia en línea en Panamá. La duración de las entrevistas se diseñó para aproximadamente 30 minutos y fueron realizadas mediante plataformas digitales y a través de un cuestionario por escrito remitido mediante correo electrónico. El guión de la entrevista se estructuró en seis preguntas, algunas de estas con sub preguntas a desarrollar.

Así, se obtuvo una entrevista con la Dirección de Derechos Humanos del Instituto Nacional de la Mujer (INAMU), cuya información fue de gran utilidad pues el INAMU funciona como ente rector del Comité Nacional contra la Violencia en la Mujer (CONVIMU) en Panamá, dicha fuente proporcionó información de relevancia para la construcción de la presente guía.

Por otro lado, se remitieron una serie de solicitudes vía correo electrónico a diversas instituciones públicas, donde fue posible obtener información suministrada por la Procuraduría General de la Nación (Ministerio Público/ Fiscalía de la República de Panamá) a través del formulario remitido y contestado vía correo electrónico.

De conformidad con los procedimientos éticos y de salvaguardia, se coordinó de previo con la institucionalidad por parte de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) para informar sobre el proyecto en desarrollo y la exploración.

1. GUÍA DE DENUNCIA EN CASOS DE VIOLENCIA DE GÉNERO EN INTERNET

La ciber violencia se compone de una diversidad de conductas que avanzan de manera paralela a la introducción y adopción de nuevas tecnologías, servicios y plataformas en el ámbito de las tecnologías de la información y comunicación.

La violencia de género en internet es definida de manera particular por la Relatoría Especial de las Naciones Unidas sobre la Violencia de Género, sus causas y consecuencias como: *"(...) todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada"*

1.1. Descripción de las conductas que constituyen este tipo de violencia

LEGISLACIÓN PENAL EN PANAMÁ

A. Divulgación indebida de grabaciones o documentos sin autorización o consentimiento

A nivel de legislación penal, se encuentra tutelado el secreto y la intimidad dentro del Título de los Delitos Contra La Libertad. El primero de ellos consagra la protección a la correspondencia en diferentes modalidades, la cual no podrá hacer apoderada, ni informada sobre su contenido por una persona distinta a la que le fue dirigida.

Si bien el Código Penal panameño no tipifica la violencia digital o ciberviolencia de manera expresa, en su artículo 166, si plantea un tipo penal relacionado al derecho a la intimidad y la violación de datos personales, como lo sería la divulgación indebida de grabaciones o documentos sin autorización o consentimiento, indicando lo siguiente:

"Artículo 166- Quien posea legítimamente una correspondencia, grabación o documentos privados y de carácter personal, no destinados a la publicidad, aunque le hubieran sido dirigidos, y los haga públicos sin la debida autorización y de ello resultara un perjuicio será sancionado con doscientos a

quinientos días-multa o arresto de fines de semana. No se considerará delito la divulgación de documentos indispensables para la comprensión de la historia, las ciencias y las artes. Si media el perdón de la víctima se ordenará el archivo de la causa".

B. Protección a la privacidad de la correspondencia

Asimismo, el Código Penal en su Capítulo III Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad contiene una pena privativa de libertad en su artículo 164 relacionado a la inviolabilidad de la información, nos indica que:

"Artículo 164. *Quien se apodere o informe indebidamente del contenido de una carta, mensaje de correo electrónico, pliego, despacho cablegráfico o de otra naturaleza, que no le haya sido dirigido, será sancionado con prisión de uno a tres años o su equivalente en días-multa o arresto de fines de semana."*

Dicho tipo penal contiene además una condición agravante, sea:

"Cuando la persona que ha cometido el delito obtiene algún beneficio o divulgue la información obtenida y de ello resulta perjuicio, será sancionada con dos a cuatro años de prisión o su equivalente en días-multa, prisión domiciliaria o trabajo comunitario. Si la persona ha obtenido la información a que se refiere el párrafo anterior como servidor público o trabajador de alguna empresa de telecomunicación y la divulga, la sanción se aumentará de una sexta parte a la mitad"

C. Producción, comercio, publicidad, difusión, distribución de material pornográfico con menores de edad

Por otro lado, el artículo **184** del Código Penal hace referencia expresa a la producción, comercio, publicidad, difusión, distribución de material pornográfico con menores de edad, norma que no solo protege a la persona del menor de edad, sino a su imagen, sea real o producto de una fabricación tecnológica, a la apetencia del autor. Cuando el delito adopta la forma de crimen organizado local o internacional, se reprende con una pena de prisión máxima de hasta 15 años. Su referencia a continuación:

"Artículo 184. *Quien fabrique, elabore por cualquier medio o produzca material pornográfico o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de Internet o de cualquier medio masivo de comunicación o información nacional o internacional, presentando o representando virtualmente a una o varias personas menores de edad en*

actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de cinco a diez años"

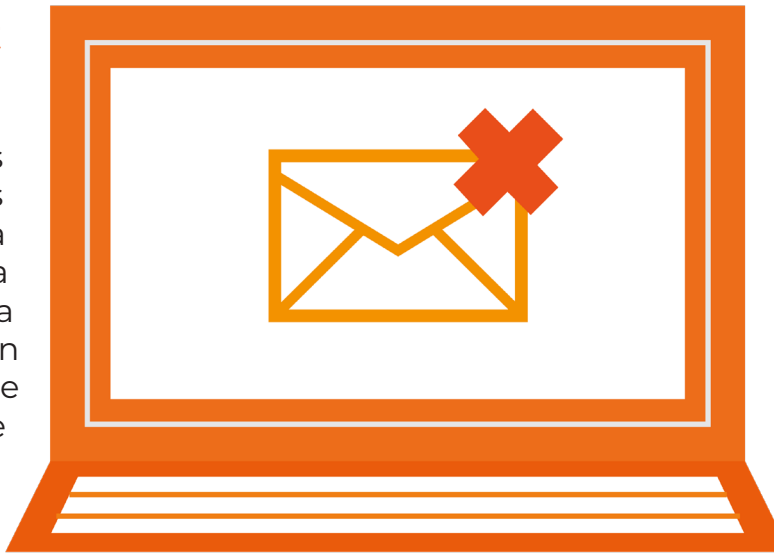
D. Violencia mediática

A lo largo de los años, han sido discutidas las conductas que constituyen violencia de género en línea, considerando la naturaleza dinámica y creciente de este tipo de violencia. Por lo que fuera del Código Penal podemos encontrar otra fuente legal relac ionada a la ciberviolencia, sea, la Ley N.° 82 del 24 de octubre del 2013, que tipifica el femicidio y la violencia contra las mujeres, así como su respectivo reglamento. Dicha ley establece en el artículo 31 que el Ministerio de Seguridad Pública deberá crear un Servicio Policial Especializado en Violencia de Género, el cual se estableció en el año 2017.

Aunado a esto, el artículo 4 inciso 21) de la supra citada ley estableció una aproximación a lo que podríamos denominar otra categoría de violencia de género en internet, por medio del término "violencia mediática" descrita como:

"aquella publicación o difusión de mensajes e imágenes estereotipados a través de cualquier medio masivo de comunicación, que directa o indirectamente, promueva la explotación de mujeres o sus imágenes, injurie, difame, deshonre, humille o atente contra la dignidad de las mujeres, así como la utilización de mujeres en mensajes e imágenes pornográficas, legitimando la desigualdad de trato o que construya patrones socioculturales reproductores de la desigualdad o generadores de violencia contra las mujeres"

E. Otras categorías relevantes a tomar en cuenta



*E*xisten otras categorías relevantes de este fenómeno que son descritas a partir de un informe sobre violencia de género en internet elaborado por la organización de la sociedad civil mexicana Luchadoras MX en 2017, en conjunto con SocialTIC y la Asociación por el Progreso de las Comunicaciones. [4] En dicho informe se establece una tipología de conductas de violencia de género digital, a partir de un ejercicio de documentación y acompañamiento de mujeres víctimas de este tipo de violencia.

Esta tipología describe 13 tipos de conductas, a saber:

1. **Acceso no autorizado (intervención) y control de acceso a las cuentas o dispositivos de una persona:** uso, manipulación, intercambio o distribución de datos personales.

   Puede suceder a un dispositivo, al no tener configurado un mecanismo de acceso adecuado como contraseña o usuario de inicio de sesión, o como consecuencia de la pérdida o robo del dispositivo; o a una cuenta o servicio en línea, se puede dar por filtraciones o robo de usuarios y contraseñas, por ataques de fuerza bruta (mecanismos automatizados para probar combinaciones de contraseñas) o mediante la suplantación de un sitio web mediante phishing. [5]

2. **Control y manipulación de la información:** Es el robo u obtención de información que puede provocar la pérdida del control sobre aquella, y su modificación no consentida.

3. **Suplantación y robo de identidad:** corresponde al delito que comete una persona que se hace pasar por otra en una red social, en un sitio de internet o en cualquier otro medio electrónico o tecnológico.

4. **Monitoreo y acecho:** esto es, vigilancia a las prácticas, la vida cotidiana o la información pública o privada de una persona.

5. **Expresiones discriminatorias por razones de género:** que pueden o no incitar a la violencia.

6. **Acoso:** esto es, conductas de carácter reiterado y no solicitado hacia una persona, que resultan molestas, perturbadoras o intimidantes.

7. **Amenazas de violencia física o sexual:** dirigidas hacia la persona, sus seres queridos o sus bienes.

8. **Difusión de información personal o íntima sin consentimiento:** que incluye la difusión de información privada (doxing), la exposición de la identidad de género o preferencias sexuales que genera riesgo (outing) y la revelación/difusión de contenido sexual de manera no consentida.

[4] Aguirre, I., Barrera, L., Zamora, A., & Rangel, Y. (2020). Justicia en trámite. El limbo de las investigaciones sobre violencia digital en México. Ciudad de México: Luchadoras https://luchadoras.mx/wp-content/uploads/2020/11/Luchadoras_JusticiaEnTramite.pdf

[5] Información obtenida del sitio web: fuente: https://protege.la/ataques/accesos-no-autorizados/ consultado el día 7 de junio del 2022

9. **Extorsión:** obligar a una persona a seguir la voluntad o peticiones de un tercero que ejerce poder adquirido por poseer algo de valor para la persona, como información personal u otras.

10. **Desprestigio, descalificación o daño a la credibilidad, trabajo profesional o imagen pública de una persona o grupo:** a través de la exposición de información falsa, manipulada o fuera de contexto.

11. Abuso y explotación sexual relacionada con las tecnologías.

12. **Afectaciones** a canales de expresión, esto es, acciones deliberadas para dejar fuera de circulación o expresión de una persona o grupo.

13. **Omisiones por parte de actores con poder regulatorio:** Esto es la falta de reconocimiento o acción para sancionar agresiones relacionadas con la tecnología. Por ejemplo: Reportes no atendidos, denuncias no levantadas, burlas, menosprecio o desconsideración de ataques.

Tipos de responsables de la violencia en línea

De acuerdo con el informe *"Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará",* publicado en el año 2022 por MSECVI OEA junto a la Iniciativa Spotlight, pueden identificarse dos tipos de responsables de la violencia en línea contra las mujeres y las niñas:

1. La persona perpetradora original: quien comete el acto inicial de violencia digital o crea, manipula o publica por primera vez la información dañina, datos personales o imágenes íntimas, sin el consentimiento de la víctima;

2. La o las personas perpetradoras secundarias: aquella persona o grupo de personas que participa en la continuación y propagación de un acto de violencia en línea al reenviar, descargar, volver a publicar o compartir información dañina, datos personales o imágenes íntimas obtenidas sin el consentimiento de la víctima.

1.2. ASPECTOS A CONSIDERAR EN LOS PROTOCOLOS DE ATENCIÓN

Se han analizado diversos protocolos de atención a víctimas, donde se establecen pautas de intervención esenciales para las fases de detección, identificación, prevención y educación en materia de violencia de género digital. En el marco de los servicios que ofrecen las instituciones competentes, se recomienda trabajar bajo el principio de **multidisciplinariedad e integralidad.** Por tanto, los servicios institucionales deberán coordinar lo correspondiente para incluir: la información a las víctimas, la atención psicológica, el apoyo social y acompañamiento, el asesoramiento legal, el apoyo familiar y el acceso a servicios social que favorezcan su autonomía.

FASE 1: DETECCIÓN

Cuando una mujer esté siendo víctima de ciberviolencia buscará ayuda e información, ya que generalmente, la víctima desconoce por cuales dispositivos está siendo ciber acosada y no se siente segura ni en su propia casa. Incluso puede llegar a desestabilizarse emocionalmente al desconocer los métodos que utiliza un ciberacosador para cumplir su objetivo.

1.1. Intervención de los Servicios de Salud

En algunas ocasiones a los servicios de salud le corresponde la detección, abordaje y atención de la violencia contra la mujer. Los/as profesionales de estos servicios son el primer o único contacto que muchas mujeres tienen con las instancias públicas cuando requieren apoyo o información.

La ciberviolencia puede generar episodios de depresión, ansiedad generalizada, nerviosismo extremo e incluso pensamientos suicidas. Por lo que es un escenario común que, la victima de violencia digital se acerque a recibir contención clínica bajo alguno de estos supuestos y será vital detectar lo que está sucediendo para activar el protocolo de coordinación interinstitucional. Dentro de un enfoque estatal donde se aborda y atiende la salud mental/ prevención del suicidio como parte integral del derecho a la salud, la contención del aparato estatal deberá ser inmediata.

1.2. Intervención y actuación de Estamentos Policiales, de Seguridad y Administrativas

Los estamentos policiales y de seguridad suelen ser una de las primeras instituciones en atender los casos de violencia contra la mujer en general y su papel es central en la primera respuesta que se brinda a la víctima. Sus actuaciones deben estar regidas por protocolos internos que se completarán con lo establecido en esta guía de carácter interinstitucional.

En esta fase se ubica específicamente el Servicio Policial Especializado en Violencia de Género del Ministerio de Seguridad y la División de Ciberdelito de la Dirección de Investigación Judicial. Así como cualquier actuación administrativa por parte de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) u otra autoridad administrativa que pueda constituir antecedentes y evidencia en esta sede.

1.3. Intervención y actuación de las Instituciones Judiciales y Ministerio Público

El Ministerio Público podrá recibir directamente la denuncia o tener conocimiento de los asuntos de ciberviolencia digital.

Al momento de denunciar el hecho, de acuerdo a protocolos internos, se podrá ofrecer apoyo por parte de Unidad de Protección a Víctimas, Testigos, Peritos y demás Intervinientes en el Proceso Penal (UPAVIT) del Ministerio Público.

El Ministerio Público velará especialmente porque las víctimas de violencia sean informadas de sus derechos, de forma clara y accesible; porque se cumpla el deber de información del curso del proceso penal, así como por la protección de los datos personales de las víctimas.

Luego de ser informada sobre sus derechos y el ofrecimiento de la información de los recursos sociales y la asistencia letrada a la víctima, se tomará la declaración respectiva. Si la víctima fuera una persona menor de edad y en el caso que la ley lo permita, la menor declarará en presencia de alguna de las personas que ostente el ejercicio de la patria potestad, de su tutor/a legal o de la persona que represente al Centro en el que esté interna o detente su custodia.

1.4. Intervención de Servicios Sociales y Asistencia Legal Gratuita

La intervención y actuación de los servicios sociales tiene por base el catálogo de derechos a las víctimas expresamente determinado en la Ley 82 de 2013 en su artículo 14 y los recursos y servicios previstos en el Directorio de Recursos de Apoyo para Mujeres Víctimas de Violencia de Género en Panamá (2009-2012), elaborado por el INAMU/UNFPA/ AECID con el auspicio del Proyecto de Actuación Integral de la Mujer, MP y MEF.

En este sentido es importante mencionar la intervención del ente especializado, para orientar en materia psicológica, legal y social a mujeres víctimas de violencia de género en Panamá, sea, el Centro del Instituto Nacional de la Mujer (CINAMU PANAMÁ). Este centro fue creado por el Instituto Nacional de la Mujer (INAMU) y busca facilitar el acceso a las usuarias que requieran denunciar y ser orientadas sin costo alguno y de manera confidencial, a través de su personal especializado.

Por otro lado, el Órgano Judicial, a través del Departamento de Asesoría Legal Gratuita para las Víctimas del Delito, brindará el servicio a las personas que así lo requieran en virtud de los requisitos establecidos por Ley. Para ofrecer una protección real a las mujeres víctimas deberá proporcionarse la asistencia legal gratuita expedita, sin distinción en cuanto a situación socioeconómica, cuando las mismas no cuenten con representación legal particular alguna y si así lo han solicitado ante la oficina de Defensa de Víctimas.

FASE 2: IDENTIFICACIÓN

En esta fase de identificación es donde debe llevarse a cabo el peritaje informático especializado en violencia de género digital, por lo que se debe contar con este perfil profesional que se encargará de la extracción, análisis

y comprobación de las evidencias digitales, así como de redactar el informe pericial que será adjuntado a la denuncia de ciberviolencia como prueba del acoso al que está siendo sometida la víctima. Algunas las actuaciones que la persona especializada en peritaje informático realizará son las siguientes:

- Verificar correos electrónicos mediante un informe que demuestre la autenticidad o la manipulación de los elementos que forman parte de un correo electrónico.
- Realizar el informe pericial sobre un ordenador, para determinar una posible eliminación de archivos o robo de datos sensibles.
- Identificar posibles alteraciones en archivos multimedia. O llevar a cabo certificaciones de desarrollos de software.
- Recuperar imágenes, vídeos y aplicaciones borrados en dispositivos móviles y tabletas.
- Certificar acciones de ciberacoso en correos electrónicos y redes sociales.
- Detectar software de geo localización en teléfonos celulares.
- Detectar la intrusión de terceros sin consentimiento en dispositivos móviles y ordenadores.

Una vez activado el protocolo, en las siguientes entrevistas se deberá de ahondar en el caso de violencia digital detectado, para analizar los daños psicológicos causados a la víctima. Las áreas de atención psicológica competentes deberán realizar un informe de evaluación y diagnóstico de cómo ha ido superando la mujer su situación desde que se activó el protocolo.

FASE 3: PREVENCIÓN Y PROTECCIÓN

Tras haber identificado y analizado las evidencias, así como el informe pericial, se deben suministrar a la víctima herramientas de prevención necesarias para evitar futuros ataques de su agresor. Para ello será deseable la coordinación entre el Instituto Nacional de las Mujeres (INAMU), a través del Comité Nacional contra la Violencia en la Mujer (CONVIMU), el Observatorio Panameño contra la Violencia de Género (OPVG), la Autoridad Nacional de Transparencia, Acceso a la Información (ANTAI) y Ministerio Público, con el fin de generar mecanismos que permitan informar/capacitar a las personas sobre medidas de seguridad y prevención para evitar ser víctima de violencia de género digital.

Medidas de seguridad que se pueden compartir para evitar ser víctima de violencia de género digital:

A continuación, se ofrecen algunas recomendaciones -no exhaustivas- de medidas de seguridad que se deben compartir y sobre las cuales se recomiendan impartir talleres y materiales informativos, para evitar que las mujeres continúen siendo víctimas de violencia de género digital:

1. Nunca se debe de dar las contraseñas de nuestros dispositivos, redes sociales y correos electrónicos a nadie.
2. Tener instalado un antivirus en nuestros dispositivos digitales
3. No descargar archivos adjuntos de correos electrónicos desconocidos
4. No abrir archivos sospechosos en nuestras conversaciones de whatsapp o correos electrónicos
5. Mantener los perfiles en redes sociales privados, de esta forma nos seguirán las personas que nosotros aceptemos
6. Configurar la doble autentificación en las redes sociales, para evitar que terceras personas accedan sin nuestro consentimiento
7. Evitar subir contenido a las redes sociales que puedan ayudar a localizarnos
8. Desactivar la cámara en computadoras y portátiles, o al menos tener tapada con algún protector.
9. Desactivar el GPS del celular o dispositivo móvil.
10. Cambiar periódicamente nuestras contraseñas de correos electrónicos, dispositivos y redes sociales.
11. Se recomienda crear una cuenta de correo electrónico personal diferente para el contacto con abogados, psicólogos o cualquier profesional.

FASE 4: EDUCACIÓN

Si el aparato estatal promoviera enfoques preventivos desde las primeras etapas formativas, por ejemplo, mediante programas de educación digital en la currícula escolar, disminuiría la necesidad de activar la reacción del aparato represivo. Que además de ser una vía engorrosa, es económicamente costosa y no necesariamente ofrece soluciones reparadoras a las víctimas.

Por ello, los recursos educativos y formativos en esta materia deben instaurarse dentro de la cultura institucional en general, para esto se recomienda diseñar planes que permitan la constante formación, sensibilización y capacitación en coordinación con la Autoridad de Protección de Datos (ANTAI), Poder Judicial, Fiscalía, Instituto de la Mujer y los diferentes mecanismos nacionales enlazados, como el Comité Nacional contra la Violencia en la Mujer (CONVIMU) y Observatorio Panameño contra la Violencia de Género (OPVG).

En línea con la fase 3., los recursos formativos deben centrarse en la importancia de contar con contraseñas seguras, la configuración de medidas de seguridad en sus dispositivos móviles y ordenadores, las maneras en las que pueden salvaguardar la privacidad en redes sociales, el uso correcto y seguro de internet, entre otros.

RECOMENDACIONES

Los protocolos para este tipo de atención, en general, deberán contener pautas comunes para la intervención, aspectos que deben ser abordados por profesionales multidisciplinarios/as (abogadas/os en tecnologías de la información, peritos informáticos, expertas/os en seguridad informática, psicólogos/as, trabajadores/as y asistentes sociales), sean:

A. Escucha y comprensión a la víctima en todo momento:

- La atención con la víctima debe efectuarse de una manera cordial, haciéndola sentir en todo momento comprendida, apoyada y a salvo.
- Se debe de interactuar en un lenguaje comprensivo acorde al nivel socio cultural y edad de la víctima.
- Con las mujeres menores de edad, se debe usar el propio lenguaje de las nuevas tecnologías, redes sociales e internet. Es relevante contar con un glosario de términos.
- Nunca se debe culpabilizar a la mujer o hacerle ver que por culpa de su

desconocimiento digital está sufriendo un caso de violencia de género digital. Ni mostrar mensajes de rechazo o sorpresa.

- Se debe potenciar mensajes de cercanía y empatía. No se debe dudar de la mujer sobre si está siendo víctima o si realmente está sufriendo un tipo de violencia digital.

- La intervención puede llevarse a cabo mediante una comunicación personal, por teléfono o bien por escrito. Todas las intervenciones se deberán de documentar conforme a las pautas institucionales.

- En este sentido, no se debe entregar un teléfono/mail de contacto personal a quien realice la consulta, ni tampoco información que vuelva identificable a quien tome el caso. Esto para mantener la seguridad de quienes realizan el servicio de atención.

- En caso de requerir comunicación directa para poder comprender de mejor manera el caso expuesto, se puede coordinar una reunión con la persona que realiza la consulta. En caso de que la reunión online sea para recopilar información, la sesión debe ser grabada y se debe solicitar el consentimiento a la persona para hacerlo. Además, se debe considerar los roles y perfiles de quienes acceden a dicho contenido, y con qué tipo de permisos.

- Es importante que se le brinde toda la información necesaria para el conocimiento de sus derechos y las formas de protegerse.

B. Actuaciones en los momentos de crisis:

Si la mujer muestra una crisis de ansiedad, miedo o vergüenza se debe de intentar calmarla y hacerle ver que no tiene por qué avergonzarse, que se está aquí para ayudarle. Para ello se recomienda coordinar con las áreas de apoyo psicológico institucional de manera que puedan estar preparadas para hacer intervención en crisis.

El ente especializado, para orientar en materia psicológica, legal y social a mujeres víctimas de violencia de género en Panamá es el Centro del Instituto Nacional de la Mujer (CINAMU PANAMÁ). Este fue centro creado por el INAMU y busca facilitar el acceso a las usuarias que requieran denunciar y ser orientadas sin costo alguno y de manera confidencial, a través de un personal especializado.

C. Análisis de evidencias digitales e informe pericial:

Detectado el tipo de violencia digital, a través de las entrevistas u otras formas de comunicación con la víctima, que serán determinadas por la unidad o funcionario a cargo dentro de la institución conforme a los hechos detallados por la víctima, procede la identificación de los canales mediante los cuales se sufre la agresión o ataque: dispositivos móviles, computadores o laptop, redes sociales, correos electrónicos, sitios web, etc.

Algunas de las evidencias digitales posibles de analizar según el canal, son: documentos y contenido multimedia (imágenes y videos); conversaciones de app de mensajería instantánea (WhatsApp, Telegram, Signal, otros); correos electrónicos; publicaciones en redes sociales; mensajes privados en redes sociales; perfiles sociales; publicación en sitios web; programas y aplicaciones de computadores y móviles; registro de llamadas en dispositivos móviles; SMS en móviles; registros de accesos a un computador; audios.

D. Actuaciones posteriores a la agresión:

Se deben proveer diferentes herramientas de prevención y protección para las víctimas, con el propósito de evitar ataques en el futuro. Entre estas medidas se encuentran impartir talleres formativos para mujeres y niñas en materia de seguridad digital, de prevención de sextorsión y de suplantación de identidad y las referidas en la fase 3.

En este sentido la coordinación interinstitucional es de vital importancia, pues si todos los entes involucrados en ofrecer soluciones aplican un protocolo ordenado y concatenado, no solo se hará un uso eficiente de los recursos públicos, sino que además y principalmente, se podrán ofrecer soluciones efectivas a las víctimas.

1.3. Etapas y ruta del proceso de denuncia e investigación de los casos de violencia digital dentro de las instituciones

Al constituir un fenómeno tan nuevo en su abordaje, se suele desconocer cómo atender este tipo de situaciones. Es por ello que a continuación, se plantean etapas del proceso en caso de recibir denuncias por violencia de género en internet, en este esquema se recomienda el trabajo colaborativo con el organismo encargado de la protección de datos personales, sea la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

PASO A: RECEPCIÓN DE LA DENUNCIA

Según información recopilada de las entrevistas semiestructuradas realizadas a personal de las instituciones relacionadas con la atención e investigación de la violencia de género en internet en Panamá, la autoridades competentes son el Servicio Policial Especializado en Violencia de Género del Ministerio de Seguridad y la División de Ciberdelito de la Dirección de Investigación Judicial, así como Ministerio Publico, encargado de ejercer la acción penal.

Además, existen otros organismos que cooperan y pueden dar soporte a las víctimas de violencia digital, entre ellas: Instituto Nacional de las Mujeres **(INAMU)**, el Comité Nacional contra la Violencia en la Mujer **(CONVIMU)** y el Observatorio Panameño contra la Violencia de Género **(OPVG)** en coordinación con la Autoridad Nacional de Transparencia, Acceso a la Información **(ANTAI)**. En esta fase será necesario considerar:

A. El derecho de una víctima de violencia digital respecto del resguardo de su identidad y sus datos personales:

Desde el accionar institucional existe el deber de informar sobre los derechos que existen para la protección de datos personales a mujeres víctimas de violencia digital e implementar las medidas para garantizar la confidencialidad de los datos personales de mujeres. Para ello, se debe contar con *políticas internas sobre seguridad de la información y protección de datos personales con enfoque transversal de género*.

B. Se deberá de informar que en ningún caso la víctima deberá:

- Eliminar conversaciones de WhatsApp.
- Eliminar fotografías, videos o archivos de audio.
- Formatear ordenador, portátil o móvil.
- Desinstalar aplicaciones móviles.
- Cambiar de dispositivo móvil sin hacer antes una copia de seguridad.
- Borrar correos electrónicos.

PASO B: SOLICITUD DE INFORMACIÓN

De acuerdo con la información recopilada de las entrevista semiestructurada, existe un protocolo genérico para la atención de denuncias penales; no obstante, se carece de un tratamiento especializado en casos violencia de género en internet, por lo que se recomienda incorporar los siguientes parámetros para proteger la identidad de las víctimas:

Información y datos personales que se pueden solicitar a una mujer víctima de violencia digital:

- Nombre / pseudónimo.
- Breve descripción de lo ocurrido.
- Fecha en que ocurrieron los hechos.
- Plataforma en que ocurrieron los hechos.
- URL de la cuenta afectada.
- URL de otras cuentas involucradas.
- Print de pantallas (pantallazos) / registros disponibles sobre lo ocurrido.
- Copia de contenidos subidos y que fueron dados de baja (cuando el caso así lo indique).
- Número de reporte entregado por la plataforma. Si no hay número de reporte, solicitar a la persona realizar esa acción. En caso de no recibir número de reporte, el caso se atiende de igual manera.
- Las evidencias digitales son de vital importancia para su aportación a la investigación de la denuncia y tramitación judicial.

PASO C: CANAL DE COMUNICACIÓN

Considerar el canal de comunicación más seguro con la víctima para no perder el contacto o seguimiento del caso.

PASO D: IDENTIFICACIÓN DEL CASO

Una vez recibido el caso dentro del Ministerio Publico, se debe identificar y categorizar dentro de los tipos de violencia de género online, y crear un registro de la información en una base de datos que cumpla con los estándares de seguridad. Dicha base de datos deberá tener una persona responsable y otra encargada del tratamiento dentro de la institución, así como roles de acceso predeterminados.

Para ello, la información recopilada en el paso 2 será determinante: tipo de violencia identificada, canales por los que se realiza el ataque, necesidad de apoyo psicológico, tomar nota del relato y estado de la víctima, realización de un primer diagnóstico y evaluación, derivación correspondiente basada en la información entregada, analizar la documentación y evidencias digitales que se deben ir recopilando y almacenando en un lugar seguro para la investigación posterior por el profesional respectivo.

PASO E: REGISTRO Y SEGUIMIENTO

Entrega de un número de registro a la víctima para identificar la solicitud/ denuncia, que permitirá abrir un expediente del caso. Si la información se remite a algún ente encargado de estadísticas es de vital relevancia que la transferencia y custodia de la información se dé bajo estándares y protocolos mínimos de actuación, de manera que se resguarde adecuadamente la indentidad de las víctimas y testigos.

Asimismo, será de vital importancia entregar pautas básicas de seguridad informática y resguardo de las evidencias digitales, en este paso y el de acompañamiento.

También es importante incorporar al registro o expediente las situaciones de violencia de género digital que la víctima ha manifestado verbalmente, documentalmente o por alguna otra vía.

GLOSARIO

Activos digitales: Son aquellos elementos intangibles que forman parte de la identidad de la persona en un contexto digital, como sus diferentes perfiles en redes sociales, cuentas de servicios y correos electrónicos.

Doxing: El término proviene de la frase en inglés dropping docs, y consiste en la extracción y la publicación en línea no autorizada de información personal.

Género: Se refiere a los roles, comportamientos, actividades, y atributos que una sociedad determinada en una época determinada considera apropiados para hombres y mujeres.

Outing: Se refiere al hecho de revelar la orientación sexual de alguien en contra de su voluntad.

Phishing: Es un proceso fraudulento de la rama de la ingeniería social cuyo objetivo es adquirir información sensible como nombres de usuario, claves o datos de cuentas o tarjetas de crédito, a través de una comunicación electrónica, fingiendo ser otra persona.

Plataforma: Las plataformas digitales o plataformas virtuales, son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades

Red social: Las redes sociales son plataformas digitales formadas por comunidades de individuos con intereses, actividades o relaciones en común, como amistad, parentesco o trabajo. Estas permiten el contacto entre personas y funcionan como un medio de comunicación e intercambio de información.

TICs: Las tecnologías de la información y la comunicación son todas aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante tecnología.

Url: Por sus siglas en inglés “Uniform Resource Locator”, es la dirección específica que se asigna a cada una de las páginas, sitios, documentos, etc. con la finalidad de que puedan localizarse e identificarse.

Violencia en razón de género contra las mujeres: Todo acto de violencia por razón de género, con la asistencia, en parte o en su totalidad, del uso de las TICs, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada.

BIBLIOGRAFÍA

Organización de Estados Americanos. (1994). Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer "Convención de Belém do Pará". **https://bit.ly/3auZvsh**

Organización de Estados Americanos. (2020). Mecanismo de Seguimiento. Convención Belém do Pará. **https://bit.ly/3FzeOyM**

Organización de las Naciones Unidas [ONU]. (1979). Convención sobre la eliminación de todas las formas de discriminación contra la mujer. **https://bit.ly/3oJUgxv**

Organización de las Naciones Unidas [ONU]. (1999). Protocolo Facultativo de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer. **https://bit.ly/3oLOYBo**

Estándares Iberoamericanos de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales, aprobados en el 2017: **https://www.redipd.org/es/documentos/estandares-iberoamericanos**

Constitución Política de la República de Panamá, Gaceta Oficial **https://www.organojudicial.gob.pa/uploads/wp_repo/blogs.dir/cendoj/CONSTITUCIONES_POLITICAS/constitucion_politica.pdf**

Ley N.° 82 del 24 de octubre del 2013 Que adopta medidas de prevención contra la violencia en las mujeres y reforma el Código Penal para tipificar el femicidio y sancionar los hechos de violencia contra la mujer: **https://vlex.com.pa/vid/ley-n-82-24-864656264**

Ley No. 81 de 26 de marzo de 2019, sobre protección de datos personales del 26 de marzo de 2019 y su reglamento: **https://www.antai.gob.pa/reglamentacion-de-la-ley-n-81-de-proteccion-de-datos-personales/**

Rico, N. "Violencia de Género: Un problema de Derechos Humanos", Serie Mujer Y desarrollo, Nª 16, Julio de 1996, CEPAL **https://repositorio.cepal.org/bitstream/handle/11362/5855/1/S9600674_es.pdf**

REPÚBLICA DE PANAMÁ

GOBIERNO NACIONAL

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

www.antai.gob.pa