Mujeres Activistas por el software libre

Guía 3

Lo que debes hacer en caso de ser víctima de violencias digitales.

Créditos

Investigación:

Nerissa José, Aguilera Arteaga
María Germana, Oliveira Blazetic
María Ángela, Petrizzo Páez

Diseño e Ilustración:
Sandra ,Triana Duarte

@sandra_triana77

@activistassl
@activistassl
contacto@activistasxsl.org
http://activistasxsl.org

Mujeres Activistas XSL

Caracas, marzo 2022

Presentación

Mujeres Activistas por el Software Libre.

Es es un colectivo de mujeres venezolanas que viene trabajando desde el 2009 en acciones para empoderar a las mujeres en el uso efectivo de herramientas de tecnologías libres, habilitándolas en la identificación, prevención y mitigación de situaciones riesgosas para ellas, de forma de impactar positivamente en su entorno y reducir la brecha de género digital.

Desde el 2011 nos interesamos en indagar sobre aspectos de seguridad digital que afectan a mujeres y cuya resolución pasa por un conocimiento especializado de los riesgos y vulnerabilidades de nuestro uso en la Red. Un año después iniciamos talleres sobre cibercuidados para colectivos activistas e iniciamos el proceso de atención a víctimas y sobrevivientes de Violencias Digitales Basadas en Género (VDBG).

De esa experiencia, hemos compilado este trabajo que hoy te presentamos en formato de talleres de formación que, si bien venimos trabajando desde hace ya varios años, también actualizamos de forma permanente para poder acercar esta información a más y más mujeres de nuestro país.

Cada uno de nuestros talleres está acompañado de una guía en la que detallamos la información que presentamos. Esta guía que verás ahora, es posible gracias al apoyo recibido a través del Fondo de Mujeres del Sur y su programa Liderando desde el Sur, en el año 2022.

3 Guía

Lo que debes hacer en caso de ser víctima de violencias digitales.

1.- Primeros Auxilios en caso de ser víctima de violencia digital: ¡No estás sola!.

Si alguien que conoces o tu misma estás siendo víctima de un caso de violencia digital, te recomendamos que cuentes lo que te ocurrió a personas de tu confianza, no es recomendable enfrentar este tipo de violencias sola: mientras más redes de apoyo tejas a tu alrededor será mejor para ti. Si no cuentas con una red de apoyo con personas de tu confianza te recomendamos que recurras a una organización feminista que tengas cerca. En nuestro país, tienes a tu disposición **este directorio** preparado por las organizaciones sociales del Clúster de Protección y las Áreas de Responsabilidad que brindan sus servicios en el país.

- Antes de empezar, respira. No es tu culpa, siempre es culpa del agresor.
- No cedas ante el chantaje o extorsión y no respondas a tu(s) agresor(es).
- Documenta y guarda evidencia de lo ocurrido. Toma capturas de pantalla con hora y fecha visible, guarda la página como pdf, el link y cualquier mensaje o conversación que esté relacionado, audios, videos, links de los foros, números de teléfono o enlaces de los perfiles desde los cuales te están atacando. Crea una carpeta con toda esta evidencia y realiza copia de seguridad o respaldo en la nube de esta información, si hacer esto te resulta incómodo y revictimizante, pídele ayuda a tu persona de confianza
- Aplica medidas de seguridad digital en tus cuentas de correos, mensajería instantánea y redes sociales, cambia tus contraseñas y configura el 2FA[1], revisa la política de privacidad que tienes en todas las plataformas.

[1]Dos factores de autenticación. Se refiere a la utilización de dos opciones para verificar la identidad de quien intenta utilizar una cuenta de correo, mensajería y redes sociales.

- Analiza sobre tus expectativas y opciones. Si no tienes toda la información o tienes dudas, consulta o busca asesoría legal.
- Aunque en un mismo caso de violencia digital se pueden manifestar una serie de agresiones distintas en varias plataformas, si estás siendo violentada en una o varias plataformas, ubica el proceso de denuncia que disponen esas plataformas (más adelante en esta guía se mencionan) y realiza el reporte.
- Tomate un tiempo de desconexión temporal. Por tu salud mental te recomendamos que realices alguna actividad que te guste y que te aleje de las redes de forma temporal pero sin caer en la autocensura, recuerda que la internet es de todas y todos, y también tenemos derecho de habitar los espacios digitales.

2.- Documentar la violencia digital

Las violencias digitales pueden darse una sola vez o muchas veces y de manera continuada, por parte de un sólo responsable o de varios. Recientemente hemos visto proliferar una técnica que utiliza, además de las cuentas y perfiles falsos, bots para ataques programados y continuados en el tiempo, por este tipo de situaciones y por la viralización de este tipo de ataques, es recomendable sistematizar las pruebas de la agresión recibida y tener un registro ordenado de las mismas.

En caso de ser víctimas de alguna agresión o violencia digital tenemos que recordar la importancia de guardar las pruebas de esta agresión. Además La sistematización de estas agresiones permite a las personas sobrevivientes-tener una visión más profunda y ordenada de la violencia que ha sufrido, permitiéndole comprender varios aspectos, como los verdaderos objetivos de esos ataques o la alianza que existe entre los responsables.

El proceso de recolección o sistematización de las pruebas de una agresión de violencia digital puede resultar desagradable y/o revictimizante. En caso de

de no poder hacerlo, es necesario que pidas ayuda a alguna persona de confianza para realizar este proceso.

Se debe guardar capturas de pantalla, audios, vídeos, los enlaces en caso de que publique una información personal sin nuestra autorización, en caso de recibir mensajes o llamadas, guardar el número, realizar captura del día y hora de recepción de las llamadas y mensajes. Si recibimos mensajes de agresión en una red social, además de la captura del mensaje, también debemos guardar el nombre y captura del perfil del usuario de esa red social que nos está agrediendo, así como el enlace de ese perfil y el enlace de la agresión. Esta información recopilada debe guardarse de forma segura y ordenada, lo recomendable es tener un respaldo de la misma.

Las agresiones en línea en lugar de desaparecer más bien se pueden multiplicar por el fenómeno de la viralización, por esta razón es recomendable sistematizar estas violencias y tener un registro detallado. Esto ayudará a tener un dimensionamiento adecuado del problema y facilitará el proceso de control de daños.

Para ayudar en este proceso de sistematización creemos que el siguiente cuadro puede resultar de utilidad:

Fecha Hora	¿Qué Ocurrió?	Evidencia de lo que ocurrió	Identificación de posible responsable	¿Por qué crees que lo hizo?	Red o redes sociales desde donde se realiza la agresión	Evidencia que no tienes y consideras importante	Acciones emprendidas
La fecha y hora del evento	Descripción de lo ocurrido	Identificar la evidencia que ya se tiene, adjuntar una captura de pantalla, pdf, una publicación, un correo, un mensaje de voz. Colocar el nombre del archivo.	Para cada evento identifica a la posible persona responsable	Explicar las razones por las que cree que es o son responsables. Ejemplo: Porque Fulanito me envió un mensaje el 3 de enero diciéndome que si no le contesto publicaría todas mis fotos.	Capturas de pantalla y enlaces de la red(es) social(es) desde donde se realizó la agresión	Hacer una lista de posibles evidencias que no tienes pero que puede ser útil. Por ejemplo: El 5 de febrero Fulanito le envió un mensaje a mi mejor amiga diciéndole que me avisara que publicaría todas mis fotos.	Indicar si se realizó algún trámite, acciones o denuncias ante órganos competentes o ante alguna plataforma de red social

Cuadro 1. Registro de evidencias

No debe confundirse el proceso detallado arriba, que corresponde a una sistematización de pruebas de la violencia digital recibida, con la noción de evidencia digital que pueden ser usadas en un caso o proceso judicial. Veamos las diferencias:

La evidencia Digital:

Es la información almacenada digitalmente que puede ser utilizada como prueba en un proceso judicial. Para que esto sea viable debe ser necesario seguir unos procedimientos en su recuperación, almacenamiento y análisis, se debe seguir una robusta cadena de custodia que permita asegurar la inmutabilidad de la evidencia.

Este procedimiento lo realizan personas expertas en informática forense o peritos forenses informáticos.

Informática Forense:

Se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo.

Es la disciplina que combina los elementos del derecho y la informática para recopilar y analizar datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que sea admisible como prueba en un tribunal.

Perito Informático Forense

En la Informática Forense la principal figura que aporta a la realización de las investigaciones es el o la Perito Informático. Esta persona es la encargada de la confección y ratificación de un informe pericial presentado en un procedimiento

judicial a requerimiento de una de las partes o del propio juez. Debe dar garantía de inmutabilidad y protección en el tratamiento de las evidencias digitales relacionadas con un hecho presuntamente punible y al cual se le conoce como Cadena de Custodia.

En el mundo y en Venezuela hay déficit de personas formadas en informática forense, más aún con perspectiva de género, por lo que no es desestimable impulsar iniciativas de formación en esta área.

El proceso de sistematización facilitará, por un lado, el proceso de narración de la agresión recibida en caso de acudir a algún órgano receptor de denuncia y por el otro lado, facilitará el proceso de levantamiento de información e investigación del caso. Sin embargo, no perdamos de vista que un pdf o una captura de pantalla no será suficiente para considerarse una evidencia digital, por muchas razones, la principal es que estos elementos pueden ser modificados o eliminados fácilmente.

3.- Reportar o denunciar casos de violencia digital a través de las plataformas digitales y redes sociales en las que ocurren.

Actualmente todas las plataformas y redes sociales tienen a disposición de las usuarias y usuarios centros de atención para reportar casos de agresión o de cualquier tipo de violencia digital. Cada red social ha definido procesos para realizar este tipo de reportes y si estás siendo víctima de este tipo de agresión o conoces de alguna persona que se encuentra en esta situación, a continuación te mostramos como realizar este reporte en cada plataforma.

Muchas de estas plataformas, luego de realizar el reporte, toman un tiempo en responder. Lamentablemente en muchos casos nunca responden, por lo que te sugerimos que realices captura de pantalla del reporte o guardes el enlace como pdf para, luego de esperar un tiempo prudencial, insistir en la denuncia a través de la misma plataforma.

facebook

¿Cómo reportar un post?	1.- Hacer click en la esquina superior derecha del post. 2.- Reportar publicación o buscar ayuda. 3.- Selecciona la categoría “desnudos” y luego “se comparten Imágenes íntimas” u “otros”. 4.- Seleccionar la opción “sí me gustaría reportar este post”.
¿Cómo reportar un perfil?	1.- Ingresar al perfil. 2.- Ubicar los tres puntos debajo de la opción enviar mensaje. 3.- Seleccionar buscar ayuda o denunciar. 4.- Seleccione la opción de acuerdo a su caso
Si se tardan	1.- Guardar el enlace como PDF en tu computadora o realizar captura de pantalla. 2.- Guardar el número de reporte para posteriormente solicitar avance del mismo.

Instagram

¿A dónde ir?	1.- Hacer click en los tres puntos en la esquina superior derecha del post. 2.- ¿Por qué quieres denunciar este post? Selecciona: desnudos o Actividad sexual, si es el caso. 3.- Después selecciona “pornografía o desnudos” o “comparte Imágenes privadas”
Si se tardan	1.- Guardar el enlace como PDF en tu computadora o realizar captura de pantalla. 2.- Guardar el número de reporte para posteriormente solicitar avance del mismo.

WhatsApp

Consideraciones Importantes	1.- Es sumamente importante que reportes el contacto lo más pronto posible para que Whatsapp puede guardar el reporte de esa conversación. 2.- Cuando reportas un contacto o grupo, WhatsApp recibe los mensajes más recientes que recibiste de ese usuario, así como información sobre sus interacciones recientes. No obstante, el tiempo para esto es limitado por lo que documentar la agresión y reportar lo más rápidamente posible es lo ideal.
Pasos para reportar	1.- Abre el chat. 2.- Toca el nombre del contacto o grupo para abrir la información de su perfil. 3.- Desliza hasta el final de la pantalla y toca Reportar contacto o Reportar grupo.

twitter

¿A dónde ir? **Recordar que twitter le da Prioridad a las denuncias Realizadas por la parte Afectada**	1.- Haz click en los tres puntos en la esquina superior derecha del tweet. 2.- Click en “Denunciar este tweet” 3.- Ante la pregunta: “¿Qué hay de malo con este tweet?" Selecciona “Comete abusos o es perjudicial”. 4.- Ante la pregunta: Ayúdanos a entender el problema. ¿Qué hay de malo con este Tweet?, selecciona “incluye informaciónPrivada”. 5.- Luego saldrá la pregunta, “¿de qué forma es este Tweet abusivo o perjudicial? Selecciona otra. 6.- “Esta información privada pertenece a:” Selecciona: a mí. 7.- En caso de que te permite incluir más información escribe en el bloque de texto: “es contenido sexual sin Consentimiento 8.- Después selecciona los tweet donde la cuenta haya publicado el contenido sexual sin consentimiento. 9.- Guarda el número de reporte que te llegue al correo.
Si se tardan	1.- Guardar el enlace como PDF en tu computadora o realizar captura de pantalla. 2.- Guardar el número de reporte para posteriormente solicitar avance del mismo.

¿A dónde ir?	1.- Ir a este link: https://support.google.com/websearch/answer/6302812 2.- Llenar el formulario:https://support.google.com/websearch/troubleshooter/9685456#ts=2889054%2C2889099
¿Cómo llenarlo?	1.- ¿Qué quieres hacer? Selecciona Eliminar información que aparece en la Búsqueda de Google. 2.- Indícanos dónde viste la información que quieres que eliminemos: En los resultados de búsqueda de Google y en un sitio web. 3.- "¿Te has puesto en contacto con el web master del sitio?" Escoge cualquiera de las opciones de acuerdo con tu caso: No, ¿cómo puedo hacerlo? No, prefiero no hacerlo. Sí. 4.- Quiero eliminar: Elementos sexualmente explícitos o desnudos: escoge la opción que aplique a tu caso en concreto: ● Una imagen o un vídeo íntimos, con desnudos o con contenido sexual. ● Quiero informar sobre contenido que supone abuso a menores. ● Una imagen pornográfica falsa en la que aparezco. 5.- ¿Apareces tú (o alguien que estés autorizado a representar) en las imágenes o vídeos, y estás desnudo o en situaciones sexualmente explícitas? Selecciona: Sí. 6.- ¿Alguna vez has dado tu consentimiento para distribuir las imágenes o los vídeos? Selecciona No.
¿Datos necesarios?	Nombre. ● País. ● Correo electrónico de contacto. ● URL donde se encuentra publicado el contenido. ● URL de muestra de los resultados de búsqueda de Google donde aparezca la imagen o el vídeo. ● Capturas de pantalla del contenido ofensivo, para asegurarnos de retirar los resultados correctos. Las capturas de pantalla pueden estar modificadas para ocultar las partes más explícitas, pero debe seguir siendo reconocible para que Google pueda retirarlo.

Estás son las plataformas de redes sociales más usadas actualmente, sin embargo también se puede reportar con procedimientos similares en otras redes sociales como OnlyFans y en plataformas de contenido pornográfico explícito como Youporn, Pornhub, entre otras.

4.- Como acompañar a mujeres y niñas víctimas de VD

Mujeres Activistas por el Software libre antes de la pandemia atendía como máximo dos casos semanales, estos eran remitidos por defensoras feministas de organizaciones hermanas que nos pedían asesoría. Hasta hace poco creímos que con la llegada de la pandemia estos casos se habían incrementado, ahora creemos que este incremento también se debe a que están reconociendo este tipo de agresiones como violencias digitales basadas en género. Después de 2020 llegamos a atender hasta 8 casos por semana y no a todos pudimos dar respuesta oportuna, por esta razón comenzamos a pensar en nuestro proceso de acompañamiento y, sobre todo, cómo hacerlo sostenible también para nosotras mismas.

Cada mujer y cada niña tienen necesidades y experiencias únicas y muy diferentes, por lo que cada una de ellas vive de forma muy distinta la violencia en línea, no se puede generalizar cuando se abordan estrategias para mitigar y/o acompañar a estas sobrevivientes, porque cada caso es distinto. Tomando en cuenta esa diversidad, a continuación, se presenta un proceso macro que ilustra los pasos que realizamos en el proceso de acompañamiento:

ETAPAS DE ACOMPAÑAMIENTO

1. Recepción del caso
2. Diseño de estrategias de abordaje
3. Seguimiento
4. Revisión
5. Cierre del caso

Para nosotras, el acompañamiento es un proceso que da respuesta a la violencia de género en línea, pero también busca generar herramientas o respuestas que le permitan a las sobrevivientes encontrar justicia y apoyo. Nuestro acompañamiento pone las necesidades de las acompañadas en el centro de las acciones, siendo nosotras mismas sujetas de aprendizaje durante el proceso, todo ello gracias a las investigaciones sobre herramientas y procesos que permiten abordar los cuidados de las personas que acompañan a víctimas y sobrevivientes de violencias digitales basadas en género.
Es por ello que realizamos el análisis conjunto de cada caso porque no se trata solo de la seguridad digital, hay que tomar en cuenta aspectos de salud mental y física, infraestructura, protocolos, herramientas de atención, evaluación de procesos, entre otras cosas.

Para poder construir estrategias y acciones de respuesta debe hacerse un abordaje holístico y muchas veces nuestra propia organización no tiene las herramientas para este tipo de acción y tenemos que derivar o buscar apoyo en otras organizaciones.

Pasos del proceso de acompañamiento:

- 1.-Cuando recibimos un caso, comenzamos a realizar la documentación del mismo, solicitamos información previa y luego agendamos una reunión/entrevista con la persona sobreviviente. Explicamos que este proceso de documentación es un proceso confidencial y lo realizamos mediante un proceso de anonimización de los datos de forma que resulte imposible identificar a la sobreviviente y se hace uso del cuadro de registro de evidencia compartido anteriormente, en algunos casos lograr la anonimización total es muy difícil, por ejemplo, cuando se trata de un caso de difusión de imágenes íntimas sin consentimiento ya que la cantidad de información personal que se obtiene es enorme. Otro ejemplo podría ser cuando se trata de un ciberacoso en una red social como Twitter porque es muy sencillo relacionar a la persona que recibe la

la agresión con un tuit, por ejemplo. En ambos casos se separan los datos personales de la sobreviviente de los archivos donde se tiene la información y descripción del caso y estos se relacionan a través de un número. La anonimización completa no es posible pero el cifrado de los archivos ayuda a lograr un nivel de seguridad superior.

Esta primera entrevista se realiza con la escucha activa de la persona que solicita ayuda. Es importante escucharla de forma que podamos entender las necesidades y circunstancias de la persona sobreviviente y poder también determinar qué espera de nosotras. No generar falsas expectativas es una de nuestras premisas por lo que explicamos muy bien que podemos ayudar con emergencias de seguridad digital, informática forense y/o asesorías puntuales en asistencia legal, porque contamos con la colaboración de algunas activistas abogadas que nos apoyan, pero no contamos con apoyo psicológico. En este punto es crucial determinar si tenemos la capacidad de ayudar o no, en el caso que no sugerimos contactar a otras organizaciones.

- 2.-En esta etapa se realiza un análisis de riesgo y se diseña la estrategia o las estrategias a seguir mediante un proceso de construcción en conjunto, intentamos entre todas definir estrategias que incluyan medidas que resulten reparadoras para la persona sobreviviente, consultamos con nuestra asesora legal (abogada) y compartimos herramientas de mitigación y estrategias de abordaje. Luego presentamos estas estrategias y los escenarios existentes para que la persona sobreviviente tome una decisión, es importante respetar su proceso, no presionar y respetar la decisión que ella tome.

- 3.-Luego hacemos un proceso de seguimiento que consiste en que dado un tiempo específico, contactamos a la sobreviviente, aunque casi siempre pasa al revés, es decir, es la sobreviviente que nos contacta y

cuenta cómo va su proceso. En ambos casos resaltamos que el proceso de seguimiento puede durar horas, días, meses, incluso años, lo que dure un caso abierto y por la diversidad de casos que recibimos, la velocidad casi que exponencial con la que mutan los ciberdelitos y las violencias digitales, algunos casos nunca llegan a cerrarse. Actualmente estamos en la búsqueda de herramientas que nos permitan sistematizar todo el proceso y que optimicen el seguimiento de los casos. También estamos explorando herramientas de cuidados colectivos para las personas que trabajan en esta atención.

- 4.-En esta etapa de revisión reflexionamos de forma colectiva sobre lo aprendido, reconocemos nuestros logros para celebrarlos, pero también identificamos nuestras debilidades y errores cometidos para buscar mejores estrategias, técnicas, recursos y herramientas que nos permitan mejorar. Es un proceso constante que exige investigación y actualización continua. Hay muchas preguntas que tenemos que responder y mucho trabajo aún por hacer.

- 5.-Para realizar el cierre del caso debemos llegar a la conclusión de que no se requiere ninguna acción adicional de nuestra parte. Hemos identificado oportunidades de mejora en esta etapa, un siguiente paso es construir un protocolo detallado de todo el proceso.

Mujeres
Activistas
XSL