GUÍA PARA BRIGADISTAS

Acciones de acompañamiento ante violencias DIGITALES contra mujeres

Guía para ciberbrigadistas. Acciones de acompañamiento ante violencias digitales contra mujeres

Instituciones que apoyan:
Fundación Internet Bolivia
Hivos
Fondo de Mujeres Apthapi Jopueti

Elaboración y edición:
Diandra Céspedes
Cecilia Huasebe
Lu An Méndez
Guillermo Movia
Roxana Pérez Del Castillo
Eliana Quiroz
Cielito Saravia

Diseño:
Marcelo Lazarte

Diagramación:
Guillermo Movia

Esta obra está bajo una Licencia Creative Commons Atribución 4.0 Internacional. Puede usarla para crear otras obras con fines no comerciales o comerciales (se agradece que cite créditos).

Guía para ciberbrigadistas.
Acciones de acompañamiento ante violencias digitales contra mujeres

Glosario	4
0. Presentación	8
1. Violencia digital	13
1.2 Violencia digital de género	13
1.3 Efectos de las violencias digitales	14
2. Seguridad digital holística y autodefensa	19
3. De seguridad digital	22
3.1 Análisis de riesgo, vulnerabilidades y estrategias de acción	23
3.2 Bloqueo de cuentas	25
3.3 Contraseñas seguras y administradores de contraseñas	27
3.4 Tipos de Software Malicioso (Malware)	27
3.5 Navegación segura	29
3.6 Cifrado de archivos	32
3.7 Software libre vs. Software privativo	35
4. Figuras legales y delitos digitales	41
4.1 Ciberacoso	41
4.2 Ciberbullying	43
4.3 Fraude cibernético	45
4.4 Robo y suplantación de identidad	47
4.5 Grooming	49
4.6 Difusión no consentida de imágenes íntimas	53
4.8 Tráfico	58
4.9 Amenazas	60
4.10 Doxing	61
4.11 Delitos virtuales contra el honor	62
4.12 Para la denuncia de un delito se deberán seguir los siguientes pasos	63

4.13 Entidades donde se puede hacer la denuncia 64
4.14 ¿Qué roles tienen los jueces, abogados, fiscales, policía, etc? 65
4.15 Recolección de pruebas digitales 66
4.16 Peritos informáticos 67
5. De contención emocional 70
5.1 Identificar una persona de confianza de contención emocional 70
5.3 Autodefensa psicológica 74
5.4 ¿En qué momento derivar a centros profesionales? 74
6. El paso a paso de una brigadista para asesorar 78
6.1 Contacto con la persona agredida 78
6.2 Contacto inicial 78
6.3 Consigue consentimiento para documentar el caso 78
6.4 Comunicaciones seguras 79
6.5 Respuestas y procedimientos en base a principios de atención a víctimas 79
6.6 Acciones adicionales 79
7. Lista de profesionales que pueden dar apoyo 81
7.1 Abogados 81
7.2 Peritos especializados 82
7.3 Psicólogos 82
7.4 Técnicos en seguridad en línea 84
7.5 Nuestros contactos 84
8. Sitios y manuales de interés 85

Glosario

Acoso: acciones repetidas, a menudo abusos verbales, con el objetivo de controlar, denigrar y/o menospreciar a una persona.

Android: Sistema operativo de Google para Smartphones

Amenazas: contenidos violentos, lascivos o agresivos que manifiestan una intención de daño a una persona, sus seres queridos o bienes

Bloquear: En redes sociales, esta opción se utiliza para evitar interacciones con personas no deseadas.

Cifrado: es la conversión de datos de un formato legible a un formato codificado, que solo se pueden leer o procesar después de haberlos descifrado.

Cifrado de extremo a extremo: Es un protocolo de encriptado por el cual solo las personas que se comunican pueden descifrar los mensajes. Por lo tanto, no pueden intervenir las empresa que brinda el servicio, ni otros puntos por los que fluye la información. Aun así, los metadatos(Receptor, remitente, hora, fecha) siguen siendo visibles[1] .

Ciberbullying: agresión psicológica, que se ejecuta repetida y sostenidamente en el tiempo, utilizando medios digitales como correo electrónico, mensajería instantánea, redes sociales, páginas web y otros.

Cookies: es información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad de navegación de la usuaria.

Difusión de información íntima o personal sin consentimiento: incluye imágenes o videos íntimos, conversaciones de chats, lugar de trabajo, orientación sexual, cuenta de banco, placa de auto, etc. También son datos personales en general como: nombre, número de celular, correo electrónico, carnet de identidad, etc.

Dirección IP: es el número que identifica a un dispositivo que se conecta a internet.

Dispositivo: aparato electrónico que me permite conectarme a internet.

Doxing: revelar información personal sobre alguien en espacios digitales sin su consentimiento.

Fraude cibernético: se refiere al fraude realizado a través del uso de una computadora o del Internet.

Grooming: conductas o acciones que realiza un adulto para ganarse la confianza de un menor de edad, con el objetivo de obtener beneficios sexuales.

HTTP: Hypertext Transfer Protocol o en español Protocolo de transferencia de Hipertexto,

es un protocolo de comunicación que permite el envío de información, como archivos HTML, imágenes y otro tipos de archivos.[2]

HTTPS: Hypertext Transfer Protocol Secure o en español Protocolo Seguro de transferencia de Hipertexto. Funciona de la misma forma forma que HTTP, pero este trabaja cifrando los datos que se envían, mientras que HTTP al enviar la información lo hace de manera legible para cualquiera que intercepte la comunicación[3] .

Internet: es un conjunto descentralizado de redes de comunicación interconectada.

iOS: Sistema operativo de Apple para iPhones

Software: conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Malware: programa o software que tiene la intención de dañar nuestros dispositivos o robar información de los mismos[4] .

Menú hamburguesa: Lo encuentras abriendo la aplicación, son las 3 rayas en la parte superior derecha . Se la llama así porque tiene 3 capas, como una hamburguesa.

Menú desplegable: Lo puedes encontrar abriendo la aplicación en la parte superior derecha, son 3 puntos

Metadatos: los datos detrás de lo datos. Es la información como la hora, el lugar de una foto o de un mensaje que mandamos a través de internet.

Navegador: un programa informático que permite acceder a páginas web en Internet.

OTR: Off-the-record Messaging. Es un protocolo de cifrado para mensajería instantánea, que se puede utilizar en diferentes servicios ya conocidos por el usuario, por ejemplo: Google Hangouts y Facebook.

Phishing: robo o suplantación de identidad.

Rastreadores de Internet: o Rastreo de Navegación, son tecnologías que hacen seguimiento de nuestros hábitos en internet,como ser donde hacemos clic, en que parte de un página nos detenemos, qué sitios visitamos con frecuencia, etc.[5]

Reportar: Ver *Denunciar*.

Servidor: Se define de dos formas, que trabajan de forma conjunta. a)Hardware: Es una máquina dentro de una red, donde funcionan servidores(software) b)Software: Un programa que ofrece un servicio -intercambio,descarga, consulta y almacenado de datos- que funciona dentro de una red o de forma local.

Silenciar: Una forma de minimizar la visibilidad de un usuario. En redes sociales esto significa no perder el contacto por completo, es decir no desagregar de tu red de contactos pero dejar de ver sus actualizaciones, publicaciones o estados.

Servidor: Se define de dos formas, que trabajan de forma conjunta. a)Hardware: Es una

2 Marshall, James. HTTP Made Really Easy. 2012. DIsponible en: https://www.jmarshall.com/easy/http/#whatis Consultado el: 27/02/2020

3 Introbay. HTTPS ¿Qué es y para qué sirve?. 2016. DIsponible en: https://introbay.com/es/blog/2016/07/05/https-que-es-y-para-que-sirve Consultado el: 27/02/2020

4 Para información más detallada consulta el punto 3.4 Tipos de Software malicioso (Malware)

5 Cookiebot. ¿Cómo hacen las webs el seguimiento de sus usuarios? | El cumplimiento del RGPD. s.f. Disponible en: https://www.cookiebot.com/es/seguimiento-online/ Consultado el: 29/02/2020

máquina dentro de una red, donde funcionan servidores(software) b)Software: Un programa que ofrece un servicio -intercambio,descarga, consulta y almacenado de datos- que funciona dentro de una red o de forma local[6] .

VPN (Red Privada Virtual): es un servicio que protege el tráfico y datos en línea, asegurando una navegación privada y el acceso sin restricciones a cualquier contenido en línea.

Violencia digital: agresiones que se sufre a través de medios digitales.

XMPP: Es un protocolo de mensajería, que da soporte a videoconferencias, mensajerìa instantánea y transferencia de archivos[7] .Hipertextual. ¿Qué es el protocolo XMPP y dónde se usa?. 2014. DIsponible en: https://hipertextual.com/archivo/2014/07/protocolo-xmpp/ Consultado el: 29/02/2020

6 IONOS. ¿Qué es un servidor?. 2019. DIsponible en: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/ Consultado el: 27/02/2020

7 Hipertextual. ¿Qué es el protocolo XMPP y dónde se usa?. 2014. DIsponible en: https://hipertextual.com/archivo/2014/07/protocolo-xmpp/ Consultado el: 29/02/2020

0. Presentación

Los eventos de violencia en Internet han sido parte de la vida digital prácticamente desde su creación, sin embargo, solían ser experiencias marginales, propias de grupos específicos racistas, nazis o machistas. En los últimos años, ha habido un cambio, diversas formas de violencia se han masificado, ya forman parte de la experiencia propia o de los círculos cercanos de la mayor parte de usuarias y usuarios de Internet.

Las principales violencias digitales reproducen la violencia offline contra personas por su identidad sexual, su identidad étnica, su ideología o por su apariencia. El ejercicio de estas violencias digitales, en varias ocasiones, implica la comisión de ciberdelitos, cuyo tratamiento es complejo debido precisamente a su carácter digital. En muchos casos, los fiscales e investigadores dejan los casos por no contar con las herramientas necesarias para poder sancionarlos de manera efectiva.

En Bolivia, la Policía se ha percatado de este incremento de acciones violentas y delitos cometidos en espacios digitales y ha iniciado algunas acciones para hacerles frente como la creación de la División de Cibercrimen de la Fuerza Especial de Lucha Contra el Crimen (FELCC) en La Paz en julio de 2018.

Sin embargo, esta División de cibercrimen de la Policía dista mucho de ser suficiente para enfrentar la cantidad y la naturaleza cambiante de estos fenómenos de violencia digital. Muchas personas en Bolivia son víctimas de estos delitos y no cuentan con la orientación para saber cómo actuar ante estas situaciones, ni para poder iniciar un proceso judicial en caso que decidan hacerlo.

Si bien no existen estadísticas de Bolivia, como es un fenómeno global, sí contamos con algunas cifras de otros contextos. Por ejemplo, según Haltabuse.org, entre el 60% y el 87% de los casos de acoso digital que se registraron en esta plataforma entre los años 2000 y 2013 fueron hacia mujeres http://www.haltabuse.org/resources/stats/index.shtml[8]

Entonces, nos hemos percatado de la necesidad de una intervención desde nosotras para nosotras, entendimos que había que actuar donde se daban las violencias: en las redes sociales, en el mundo virtual. Así, nos lanzamos a formar un grupo de ciberbrigadistas que apoyen a mujeres en situación de violencia digital, así como para prevenir violencias digitales y dar a conocer los pasos para actuar frente a ataques de este tipo. Se creó el grupo de ciberbrigadistas llamado SOS Digital para hacer acompañamiento preventivo y reactivo a mujeres que experimenten o sean posible blanco de violencias digitales.

Nos dimos cuenta también de la necesidad de un enfoque holístico de seguridad digital o más bien de autodefensa digital, que incluyera aspectos tecnológicos, legales y psicológicos.

8 Las estadísticas exactas por año son: 2000, 87%; año 2001, 73%; año 2002, 71%; año 2003, 70%; año 2004, 69%; año 2005, 77%; año 2006, 70%; año 2007, 61%; año 2008, 71%; año 2009, 78%; año 2010, 73%; año 2011, 74%; año 2012, 80%; año 2013, 60%.

Esos son los tres aspectos que ordenan este documento.

El primer aspecto es el **tecnológico**, tanto para prevenir como para actuar en los momentos de ataque. Hemos elaborado una lista de sugerencias y herramientas mínimas de prevención y reacción frente a ataques pero, ante todo, brindamos una lista de documentos, guías y textos para quien desee ampliar estos aspectos (muy cambiantes) porque entendemos que lo importante no son las herramientas sino una actitud de empoderamiento frente a la tecnología, una actitud liberadora en la que la tecnología está ahí para ayudarnos, no para dañarnos. Queremos crear con la tecnología, no defendernos de ella.

En lo **jurídico**, es verdad que falta un marco legal específico para tratar estos delitos en Bolivia, pero también es cierto que tenemos varias normas dispersas que sirven para llevar adelante acciones legales de ciberdelitos. Hemos elaborado una recopilación de estas normas para nueve figuras legales y delitos, que ponemos a disposición con un breve análisis caso por caso, con la intención de que sean orientativas para las mujeres que experimentan violencias digitales[9] .

La contención **psicológica** es importante cuando se tiene en frente a una persona que está siendo atacada, la culpabilidad y el sentido de vulnerabilidad son comunes y devastadores en estos casos. Brindamos técnicas para poder contener emocionalmente en este sentido.

Presentamos este protocolo de prevención y reacción contra ataques hacia mujeres que tiene como objetivo principal proveer información a las ciberbrigadistas contra la violencia digital en aspectos de contención emocional, autodefensa digital y orientación legal, de manera que nos convirtamos en un grupo de primera respuesta con conocimientos básicos y podamos guiar a terceros que sean testigos de algún tipo de vulneración o delito.

¿Qué somos las ciberbrigadistas contra la violencia digital?

Las ciberbrigadistas SOS Digital son voluntarias bolivianas contra la violencia digital cuya función principal es apoyar en la prevención y reacción contra ataques y vulneración de Derechos Humanos que ocurren en entornos virtuales.

Somos ciudadanas sin afiliación político-partidaria ni religiosa y no discriminamos a ninguna persona que quiera recibir consejos preventivos o requiera un acompañamiento al ser objeto de ataques de violencia digital. Si bien nuestro interés especial son las mujeres, la información que proveemos puede adaptarse a otros grupos de personas.

Nuestros principios de brigadistas

Creemos en los siguientes principios que guían nuestras acciones:

• **Dignidad**. Derecho que tiene cada ser humano de ser respetado y valorado como ser individual y social, por el solo hecho de ser persona.

9 En Latinoamérica acoso.online ha hecho una recopilación normativa también y puede consultarla en este enlace https://acoso.online/bo/ La nuestra es complementaria y proviene de una experiencia de base

• **Igualdad**. Todos los seres humanos y humanas tenemos los mismos derechos y oportunidades. No generamos relaciones de jerarquía con las mujeres que acompañamos.

• **Seguridad**. Protección ante cualquier tipo de abuso, garantizando derechos y libertades fundamentales.

• **Interculturalidad**. Interacción entre personas de diversas culturas que ayudan a la construcción de relaciones de igualdad y equidad de manera respetuosa.

• **Equidad**. Reconocimiento a la diferencia y el valor social equitativo de las personas.

• **Protección**. Igual protección para todas y todos los seres humanos que implica una reparación o satisfacción justa y adecuada por cualquier daño sufrido como consecuencia de actos discriminatorios y violentos.

• **Integridad**. Respecto al manejo de datos, de los mensajes que se emiten y al comportamiento en el acompañamiento que se hace a las víctimas.

• **Confidencialidad**. La información que sea comunicada a un brigadista deberá ser protegida, resguardada y manejada en absoluta reserva. Los pormenores de cada caso pueden ser comunicados a profesionales para el asesoramiento técnico respectivo, resguardando siempre la identidad de la presunta víctima.

• **Consentimiento**. Cualquier acción que se sugiera será sujeta al consentimiento de la víctima antes de realizarla e informando de la manera más precisa posible las consecuencias de dichas acciones.

.hacker
persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.
CrackeR
PILLADO
seRA LINCHADO

1. Violencia digital

Es un nuevo tipo de violencia que se produce cuando una persona ejerce la fuerza o el poder sobre otra persona utilizando tecnologías de información y comunicación, como Internet, las telecomunicaciones o dispositivos móviles. Este tipo de violencia afecta directamente a las personas, vulnerando principalmente su dignidad, su libertad y su vida privada. La diferencia entre la violencia digital y los delitos informáticos, es que la primera, no está normada en el derecho internacional y nacional, pero se practica ampliamente por la ciudadanía y afecta directamente a las personas; mientras que los delitos informáticos, se encuentran reconocidos en el derecho penal internacional, directamente relacionados con la "protección o vulneración de las herramientas tecnológicas" que almacenan información.

La violencia digital atiende las prácticas agresivas de las personas en la sociedad de la información (con particular atención a internet), y se basan en el uso de imágenes, símbolos, lenguajes y contacto virtual que puede terminar en encuentros reales con personas de cualquier parte del mundo. En cambio, los delitos informáticos atienden la protección de las herramientas o "patrimonio" que tiene información valiosa.

1.2 Violencia digital de género

Así como en la vida real hay sistemas de dominación y opresión contra la mujer y diversidades sexuales, para perpetuar el control y la dominación masculina, ahora estamos en un escenario digital que reproduce estos mismos ideales[10] . La violencia en espacios digitales es una herencia del patriarcado, estas conductas humanas ahora son trasladadas y han cobrado otras dimensiones en tecnologías e Internet. La violencia digital de género no es un fenómeno nuevo, sino una continuación de la violencia machista que ahora se reproduce espacios tecnológicos desde el acceso a tecnologías hasta prácticas de vigilancia, control y manipulación.

Las mujeres bolivianas, especialmente en las áreas periurbanas y rurales, usan las tecnologías y acceden a Internet de manera diferenciada, exponiendo sus vidas a fraudes y robos a través de suplantaciones de identidad, acoso, amenazas físicas, hackeo y difusión de imágenes íntimas sin consentimiento (DIISC), entre otras. Este tipo de violencias inician en el entorno digital y se concretan en la vida real mediante secuestros, violaciones y feminicidios. Están expuestas a otros riesgos por la falta del acceso a tecnologías e Internet en sus áreas lo que influye en sus habilidades y costumbres digitales. Así mismo por las respuestas tardías de las plataformas y empresas de telecomunicaciones que dificultan el acceso a la justicia.

10 pf. Alto Comisionado de Naciones Unidas, 2018, p. 5

Por otro lado, las mujeres bolivianas del área urbana tienen un conocimiento más profundo de los funcionamientos y lenguajes en Internet por su uso cotidiano. Pero de igual manera se ven afectadas por las mismas empresas y Estado al estar expuestas a: censura, discurso peligroso, difusión de información personal sin consentimiento (imágenes íntimas, datos personales, orientación sexual, etc.), hackeo, uso indebido de imágenes, ataques coordinados, difamación y persecución política que tiene consecuencias físicas, emocionales y psicológicas.

Por otro lado, las activistas, periodistas y políticas son un blanco de ataques coordinados, organizados y con objetivos claros. Hay un uso intencional de viralizar imágenes íntimas sin consentimiento, objetivizar los cuerpos, insultos racistas, de ejercer violencia psicológica mediante amenazas por apps de mensajería y amedrentamiento al difundir datos personales.

Se han identificado grupos en WhatsApp y Telegram que se organizan con el uso de hashtags para ordenar la información: #objetivo, #caído, #reportado, etc. Los ataques coordinados han incrementado desde la creación del grupo los *guerreros digitales*[11] en el 2018 que a legitimado y facilitado los intentos de vigilancia, crear desinformación, acosar y censurar, entre otros. El 2019, las agresiones han incrementado y vemos organizaciones ciudadanas conservadoras, de clase media que viven en el área urbana con estrategias similares de ataque. Estos grupos de ataque tienen mayor alcance en sus publicaciones gracias a estrategias elaboradas por la experiencia profesional y familiaridad con las plataformas. Tienen un presupuesto para llegar a más personas y conocimientos de herramientas necesarias para viralizar contenido que se alinea con su acción política como noticias falsas y discursos peligrosos. Esto agudiza las desigualdades que afecta principalmente a personas del área rural y mujeres como una herencia histórica del colonialismo.

Casos de violencia digital generalmente no son reportados por lo tanto es difícil tener una muestra representativa sobre la diversidad de ataques.

1.3 Efectos de las violencias digitales

Las violencias que ocurren en Internet son reales y como todo tipo de violencia tiene efectos en la vida de las personas, es común que se minimice estas experiencias, porque existe una computadora o un teléfono celular que hace como mediador entre el atacante y la víctima, lo que hace pensar; “que no hay una interacción directa, por lo que, los ataques que se reciben en línea, no serían tan graves”. Este argumento ignora o no toma en cuenta que estos tipos de violencias responden a un orden estructural más grande, es decir, la causa de las violencia de género que se vive en las calles, escuelas, trabajos u hogar, es la misma causa de las violencias que ocurren en internet, es por eso que los efectos de las violencia digitales son

11 Disponible en: https://eldeber.com.bo/141954_guerreros-digitales-operan-medios-digitales-y-cambian-su-estrategia-operativa

bastante parecidas a los efectos de la violencia en general, ya que ambas atacan a la integridad, sin embargo muchas veces en violencias digitales se desconoce la identidad de tu agresor..

En ese sentido, al ser la culpabilización (culpar a la víctima por lo que ha ocurrido) un aspecto en común en distintos casos de violencia de género, esto también se observa en las violencias digitales. Comentarios como "no debiste compartir esta foto" o "es tu culpa por haberte expuesto así en Facebook", son bastante comunes. Responsabilizar a la víctima por la violencia que ha sufrido o está sufriendo tiene como efecto la revictimización o victimización secundaria. Es decir, la persona que está viviendo una situación de violencia además de afrontar la misma, se enfrenta a que la sociedad, el Estado, amigos/as y familiares le echen la culpa por lo que está pasando o no le crean.

La revictimización incrementa los efectos psicológicos de la violencia, existe mayor angustia, mayores niveles de depresión y es probable que la persona que sufre de revictimización, no denuncie futuros episodios de violencia por temor a no que no le crean.

Por otro lado, como se mencionó anteriormente; que personas extrañas tengan acceso a tus cuentas en Internet, puedan revisar tus conversaciones, te acosen en redes sociales, publiquen un video tuyo sin tu consentimiento, son sólo algunos ejemplos de los distintos tipo de violencias a las que las personas se enfrentan durante su actividad en línea. La mayoría de estos ataques son violaciones a la privacidad y también son vulneraciones a la intimidad, por lo que sus efectos pueden ser serios a nivel psicológico y también físico.

1.3.1 Efectos psicológicos[12] :

• Ansiedad y miedo

• Desprendimiento, como si fuera una extraña en su propia vida.

• Angustia intensa

• Inseguridad, incluso cuando no tiene sentido sentirse de esta manera

• Irritabilidad

• Enfado

• Culpabilidad, vergüenza y culpa de uno mismo (a).

• Depresión y desesperanza.

• Vergüenza y exposición

• Pensamientos o recuerdos intrusivos y molestos que pueden venir de repente.

• Memoria poco confiable, como dificultad para recordar exactamente detalles.

12 Violet Blue. The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online. Disponible en: https://we.riseup.net/assets/355960/smartgirlsguidetoprivacy.pdf

• Pesadillas e insomnio.

1.3.2 Efectos físicos[13] :

•Latidos cardíacos acelerados

•Respiración acelerada,

•Náuseas,

•Tensión muscular

•Sudoración.

•Dificultad para concentrarse

• Evitar personas, eventos o situaciones.

Es posible que las personas víctimas de este tipo de violencias pueden sentir algunas de los efectos mencionados o todos, dependiendo de la gravedad del caso o de los recursos emocionales de cada persona. No todos, ni todas respondemos a la violencia de la misma forma y tampoco todos los casos son iguales.

13 Violet Blue. The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online. Disponible en: https://we.riseup.net/assets/355960/smartgirlsguidetoprivacy.pdf

A
HACKEARLO
ToDO

2. Seguridad digital holística y autodefensa para activistas y personas públicamente expuestas: acciones preventivas, de emergencia y posteriores.

Trabajamos en la seguridad digital holística desde tres miradas: tecnológica, legal y psicológica con el fin de concientizar sobre los riesgos para activistas y personas públicamente expuestas, para orientarlas/los si están en situación de violencia digital y para mejorar sus estrategias y usos de herramientas.

Damos orientación en el aspecto tecnológico en usos de herramientas como la compresión de procesos de denuncia y bloqueo en plataformas o el ajuste de configuraciones de privacidad y seguridad. Prácticas un tanto básicas, pero que según nuestra experiencia, poco conocidas por las personas atendidas. Es importante notar que las brigadistas deben estar informadas sobre cambios de estos aspectos en la plataformas ya que esto significa nuevos riesgos para las personas atendidas.

La normativa está mejor detallada en el punto 4 de orientación legal, sin embargo, las personas atendidas generalmente no buscan hacer una denuncia por los procesos burocráticos, largos y caros. De igual manera es importante estar actualizada en la normativa cambiante que puede afectar nuestros derechos o erradicar violencias digitales.

La contención psicológica es quizás el factor definitivo que hace que las personas atendidas recomienden al grupo de brigadistas a otras personas en situación de violencia o que vuelvan a contactarse con nosotras para tener una asesoría de seguridad digital ya que en el contexto actual es difícil encontrar espacios seguros donde las personas puedan contar por lo que atraviesan y ser acompañados(as)..

coMo
CONDÓN para SEXO
segurO,
TOR para NAVEGAR
segurA

3. De seguridad digital (seguridad digital y autodefensa digital)

La seguridad informática se refiere a la práctica de proteger las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. La definición de seguridad de la información no debe ser confundida con la de seguridad informática, ya que la seguridad informática solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no sólo en medios informáticos.

Empresas y Estados tienen nuestra información, por lo que se espera que cuenten con protocolos de seguridad para preservarla de ataques externos y de accesos ilegales por personal dentro de las organizaciones o personas externas. También se espera que cuenten con mecanismos para que las usuarias y usuarios puedan estar informados de las filtraciones, incidentes y accesos ilegales. Pero como se dice: "ningún sistema es completamente seguro", así que debemos desarrollar prácticas de autodefensa digital para, precisamente, poder defendernos.

Hablar de seguridad digital es entender Internet como un escenario real (como el hogar o la calle), donde se viven situaciones de riesgo o de peligro, por lo que es necesario cuidarse y tomar ciertos recaudos para evitar situaciones como: la pérdida, daño o robo de información de computadoras y celulares, el acceso de otras personas a las cuentas personales en redes sociales, acceso a la información con la que usuarias y usuarios realizan transacciones bancarias en línea entre otras.

La diferencia entre seguridad digital y seguridad informática es que la primera tiene que ver con el proceso humano de protección de información, privacidad y libertad de expresión, entre otros, en espacios digitales; y la segunda se encarga de la protección del hardware mismo.

Es necesario, tener cuidado y evitar situaciones de riesgo, como por ejemplo, la pérdida de información al dañarse o extraviar, nuestras computadoras o celulares, el acceso de otras personas a las cuentas en redes sociales o a las transacciones bancarias que se encuentran registradas en el celular, entre otras[14] .

En ese sentido, la autodefensa digital comprende una serie de acciones de las propias usuarias y usuarios para reducir vulnerabilidades e incrementar el conocimiento de cómo reaccionar en casos de sufrir ataques relacionados con las violencias digitales.

La autodefensa digital es, entonces, una decisión consciente de tomar control sobre nuestra relación con la tecnología: nuestros hábitos, comportamientos y la toma de decisiones informadas para proteger nuestra privacidad entre otros derechos y libertades fundamentales

14 Seguridad Digital es tan importante como la seguridad en el hogar o en la calle. Disponible en: https://www.colnodo.apc.org/es/opiniones/seguridad-digital-tan-importante-como-la-seguridad-en-el-hogar-o-en-la-calle-2

que tenemos en Internet.

3.1 Análisis de riesgo, vulnerabilidades y estrategias de acción

El análisis de riesgo y de vulnerabilidades, se utiliza de forma preventiva ya que nos ayuda a identificar la probabilidad de que una amenaza pueda convertirse en algo real (riesgo) y a conocer cuál sería nuestra capacidad de respuesta, cuales son nuestras capacidades existentes y cuales son las faltantes (vulnerabilidad). Por ejemplo, una mujer activista tiene la amenaza de que personas extrañas ingresen a sus cuentas en redes sociales, una vulnerabilidad puede ser que la información como correo electrónico o número de teléfono que utiliza para iniciar

<table>
<tr><td colspan="2">ANÁLISIS DE RIESGO</td></tr>
<tr><td>1. Si supieras que todos pueden ver lo que haces en Internet (el gobierno, las empresas o cualquiera que puede interceptar tu conexión), ¿qué te gustaría mantener en privado?</td><td>2. En caso de responder durante la primera pregunta: ¿Qué tan sensible es esta información?</td></tr>
<tr><td>3. ¿A quién le interesa estos aspectos de mí? (Identificar enemigos)</td><td>4. ¿Qué es lo peor de puede pasar si consiguen mi información?</td></tr>
<tr><td colspan="2">ANTECEDENTES DE VIOLENCIA DIGITAL</td></tr>
<tr><td colspan="2">5. ¿Haz tenido alguna experiencia de violencia digital?
6. ¿Ha sido un hecho aislado o un patrón? (¿Pasa siempre o de vez en cuando?)
7. ¿Quién (crees) que era el/la responsable?</td></tr>
<tr><td colspan="2">AUTODIAGNÓSTICO
Durante la entrevista es importante poder identificar las vulnerabilidades que sienten las asesoradas.</td></tr>
<tr><td>8. ¿Crees que de alguna forma, navegar en Internet podría ponerte en peligro? ¿Porqué?</td><td>9. ¿Qué haces para no sentirte en peligro? o ¿cómo te proteges?</td></tr>
<tr><td colspan="2">CONSEJOS DE SEGURIDAD: AUTODEFENSA, RESISTENCIA, AUTOCUIDADO</td></tr>
<tr><td colspan="2">10. Estrategias a tomar y herramientas recomendadas
a. Configuraciones de privacidad en Facebook, WhatsApp, Twitter, Instagram
b. Buenos hábitos digitales: cerrar sesión cuando te conectas desde una computadora ajena, no prestarle el celular a nadie, no hacer clic en enlaces desconocidos, identificar HTTPS, etc.</td></tr>
<tr><td colspan="2">11. Observaciones finales</td></tr>
<tr><td>14. Al finalizar la asesoría preguntar: ¿crees que la información que te hemos dado es útil para tu vida digital?</td><td>15. Del 1 al 10 ¿Harías este ejercicio otra vez dentro de 6 meses?

Nivel de interés en protegerlo
/10</td></tr>
</table>

sesión en estas redes, no esté actualizada.

Con esta información podemos diseñar estrategias personalizadas para minimizar la vulnerabilidad dependiendo el contexto de cada persona, en el caso del ejemplo se brindará apoyo para actualizar la información de sus cuentas y se sugerirá el cambio de contraseñas a unas más seguras.

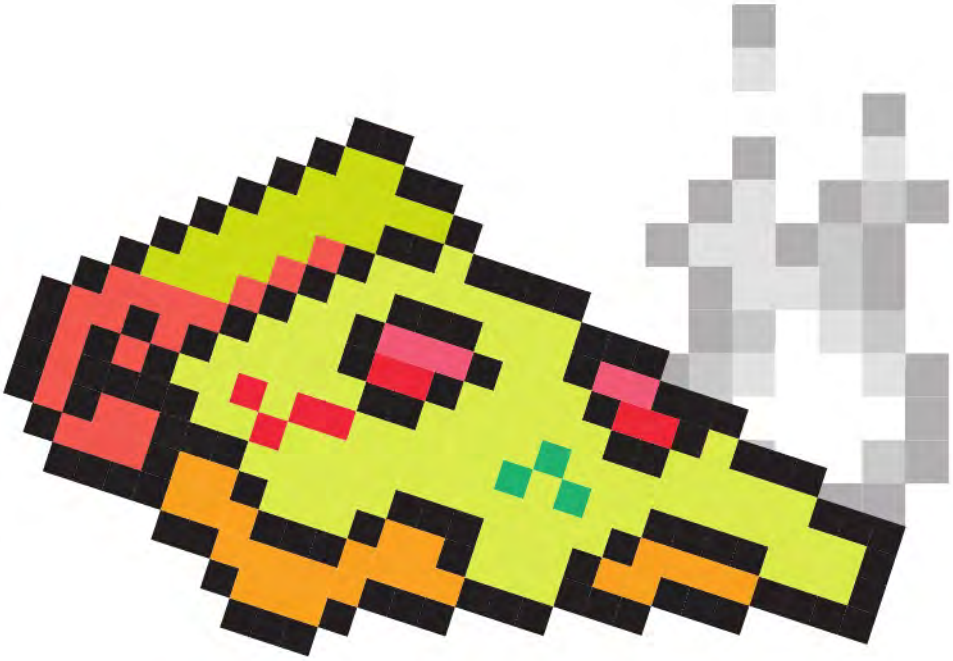
En este sentido, el grupo de ciberbrigadistas cuenta con un instrumento para asesorar a personas en seguridad digital, el diagnóstico de riesgos y vulnerabilidades. Este diagnóstico consiste en: el análisis de vulnerabilidades para identificar los aspectos más importantes a proteger y los riesgos a los que está expuesta, un autodiagnóstico, brindar estrategias de seguridad digital y obtener retroalimentación de la persona.

Las preguntas pueden ser hechas en un orden distinto y no son excluyentes a otras que puedan darse durante la conversación.

3.2 Bloqueo de cuentas

Contamos con una herramienta para orientar sobre el bloqueo de cuentas en redes sociales, es una guía antiacoso en línea[15] y tiene procedimientos para reconocer cuando una persona está siendo acosada, datos sobre el ciberacoso en Internet, pasos a seguir para bloquear cuentas en Facebook, Twitter y WhatsApp, lugares a dónde acudir para conseguir más ayuda y otros consejos.

15 Disponible en: https://internetbolivia.org/8M/



DaLEX

Yo no puedo compartirte,
eres como la clave de mi celular

3.3 Contraseñas seguras y administradores de contraseñas

Para evitar que otras personas ingresen a nuestras cuentas de redes sociales, se aconseja tener contraseñas seguras. Una contraseña segura es una contraseña que otras personas no pueden adivinar o conocer fácilmente utilizando programas informáticos.

Las características de una contraseña segura son:

- Debe incluir números.
- Debe tener una combinación de letras mayúsculas y minúsculas.
- Incluir caracteres especiales. ¿Cuáles son los caracteres especiales? Cualquiera de los siguientes caracteres: - * ? ! @ # $ / () {} = . , ; :
- Tener una longitud mayor o igual a 8 caracteres.
- Usualmente no deben tener espacios en blanco aunque algunas contraseñas sí las aceptan.

Por ejemplo, esta contraseña "XdeTrabajo27@" es más segura que esta "firulais".

Para comprobar qué tan segura es tu contraseña puedes usar este servicio que te dice cuánto tiempo le tomaría a una computadora adivinar tu contraseña. https://howsecureismypassword.net/

Además, otros consejos prácticos para mantener nuestras contraseñas de manera segura:

- Si vas a usar palabras reales en tu contraseña, trata de usar palabras y referencias poco conocidas o mal escritas. Palabras de diccionario o de cultura popular no son una buena idea.
- No repitas la misma contraseña en múltiples sitios.

Existen administradores de contraseñas que crean contraseñas seguras y las guardan de manera que no es necesario acordarse de todas las contraseñas de los servicios y redes sociales en las que estamos sino solo una contraseña que es la que permite ingresar al administrador de contraseñas. Se puede usar LastPass[16] y KeePass[17] .

3.4 Tipos de Software Malicioso (Malware)

La palabra malware en inglés, se refiere a "software malicioso", como el nombre lo dice, un malware es un tipo de software que tiene como objetivo robar información de nuestros dispositivos (computadora, celular, etc) o dañar alguno de estos, sin el consentimiento del/la propietario (a). Los malwares son creados y liderados por diferentes estrategias:

Malware general: Algunos malwares son creados o comprados por personas, que luego los liberan en Internet y ayudan a propagarlos de forma masiva.

Malware dirigido: El malware dirigido se usa normalmente para interferir o espiar a una persona, organización o red en particular. Personas mal intencionadas utilizan estas técnicas

16 Tutorial de LastPass disponible en: http://bit.ly/SEGURIDADPASS

17 Tutorial de KeePass disponible en: https://www.youtube.com/watch?v=4f2WS8n65l4

para sacar provecho, pero también las usan los servicios militares y de inteligencia, teorroristas, acosadores en línea, actores políticos, es probable qué los ataques dirigidos incluyan mensajes cuidadosamente personalizados, información falsa del remitente, adjuntos con nombres de archivo apropiados en el contexto, acceso físico a dispositivos específicos y otros trucos similares[18] .

En ese sentido malware es la palabra que se utiliza para referirnos a todas las amenazas informáticas, describiremos las más comunes a continuación[19] :

3.4.1 Virus: son programas diseñados para infiltrarse en nuestros dispositivos y dañar o alterar nuestros archivos y datos. Los virus tienen la capacidad de modificar o eliminar nuestros archivos de nuestros equipos. Los virus no se esconden, suelen transportarse dentro de archivos ejecutables, "exe" pueden ocultarse con los nombres de otras aplicaciones, con la finalidad de engañarnos y así poder infectarnos.

3.4.2 Troyanos: Se toma el nombre de la historia del Caballo de Troya, un troyano es un programa destructivo que se hace pasar por una aplicación auténtica. A diferencia de los virus, los troyanos no se replican, pero pueden ser igual de dañinos. Además, los troyanos abren una puerta trasera en el equipo que facilita a usuarios y programas maliciosos el acceso al sistema para robar información personal y confidencial[20] .

3.4.3 Spyware: Es un malware diseñado para espiar a víctimas potenciales. Se esconde en el sistema y trabaja sin que el usuario lo note, para observar la actividad en línea que incluyen contraseñas, números de tarjetas de crédito y hábitos de navegación en redes sociales, entre otros.

3.4.4 Ransomware: Este tipo de malware bloquea un dispositivo y amenaza con borrar todos sus datos, a menos que se pague cierto monto de dinero.

3.4.5 Keylogger (registrador de teclas): se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente guardarlas o enviarlas a través de Internet.

3.4.6 ¿Cómo nos infectamos? Para que un malware infecte nuestros equipos, este software tiene que instalarse en nuestro dispositivo. Existen diversos métodos para introducir esos programas y lograr que los ejecutemos sin que nos demos cuenta, algunas de estas formas, son las siguientes:

1. El malware puede estar adjunto a un correo electrónico que simula información importante y personal, puede ser un documento de Word o Excel, fichero ZIP, etc.

2. Fichero descargado de Internet, normalmente en un correo electrónico aunque también a través de mensajería instantánea y SMS, en los que incluyen un enlace para descargar "algún documento" como documento de Office, archivo de sonido, visor de vídeos, actualización de Flash, etc.

3. USB's infectados por malware.

18 Protege tu dispositivo de malware y ataques de Phishing. Disponible en: https://securityinabox.org/es/guide/malware/

19 Qué es Malware? Disponible en: https://www.enticconfio.gov.co/que-es-malware

20 ¿En qué consisten el malware, los virus, el spyware y las cookies? Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

4. Programas conocidos que nos descargamos “gratis” de sitios no autorizados.
5. Falsas aplicaciones que hacen más cosas de las que dicen.
6. Llamadas a WhatsApp sin haber contestado[21]
7. Hacer clic en enlaces desconocidos

3.4.7 Cómo podemos protegernos? [22]

1. Tener un antivirus instalado y actualizado.

2. Precaución en los correos que tengan archivos adjuntos, si algún archivo nos genera duda, mejor no descargarlo.

3. También puede que nos manden enlaces para descargar algo por correo, se debe comprobar siempre el certificado de la página de descarga. Ante la menor duda, no hacer clic.

4. Las aplicaciones que descargamos para los teléfonos celulares, también pueden tener funcionalidades “ocultas”. Solo debemos descargar aplicaciones desde la tienda oficial: Play Store o Apple Store.

3.5 Navegación segura

Cuando navegamos por Internet recibimos mucha información, pero al mismo tiempo también vamos dejando mucha por el camino. En un documental de Werner Herzog sobre Internet, uno de los primeros hackers contaba que en un principio no pudieron imaginar el éxito que tendría después, y que algunas decisiones técnicas que tomaron fueron muy inocentes. Entre ellas, la cantidad de información que intercambian un navegador y un servidor cuando se comunican. En aquella época no pensaban que esa información podría ser usada por gobiernos para perseguir personas. Eso está ocurriendo ahora, y no solo por gobiernos, sino también por grandes corporaciones.

En nuestra navegación hay información que se intercambia necesariamente entre nuestro navegador y los servidores y otra que los sitios web que visitamos van recolectando a medida que navegamos por sus páginas y, en muchos casos, nos siguen incluso cuando ya hemos salido de ellas.

3.5.1. Navegando por internet

Para entender cuál es la información que intercambian nuestro navegador y los servidores, deberemos empezar por algunos conceptos iniciales:

a) Navegador es la aplicación que utilizamos comúnmente para visitar sitios web, tanto

21 Más información disponible en: https://www.grahamcluley.com/urgent-update-whatsapp-now-to-add-new-sticker-support/

22 Malware. Cuál es su objetivo y cómo nos infecta. Disponible en: https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta

en nuestros equipos de escritorio como en los dispositivos móviles. Ejemplos de navegadores son Chrome, Firefox, Edge, Opera, Safari.

b) El servidor es donde está alojada la página web que queremos visitar (por ejemplo donde está www.bolivia.bo).

Para que podamos ver una página web, nuestro navegador le hace el pedido al servidor. Tanto nuestro equipo como el servidor están identificados con un número único (a través de un protocolo, lo que generalmente se conoce como número IP). La dirección IP más otra información se intercambia de una forma en que puede ser mirado por dispositivos que estén en el medio, y necesariamente hay varios de ellos. Por lo tanto, nuestra dirección IP es conocida y queda registrada. Este número es tan único que se puede identificar al equipo que accedió a un sitio web. Esto que generalmente no conlleva problemas, puede ser preocupante si estamos accediendo a un sitio web que por alguna razón está prohibido o contiene información que no debería ser pública.

Además de la dirección IP, nuestro navegador comparte la identificación de nuestro navegador, como la marca, el sistema operativo, etc (lo que se conoce como user-agent).

Posiblemente hayas visto que algunas direcciones de Internet comienzan con https en lugar de http. Esa “s” significa que la comunicación entre tu navegador y el servidor web va cifrada y que cierta información que intercambian no puede ser vista por tu proveedor de Internet, por ejemplo cuando ingresas el nombre de usuario y la contraseña del sitio. Por lo tanto, cada vez que vayas a ingresar tu usuario y contraseña en un sitio, debes fijarte que la dirección incluya el https o un candado verde, que significa que la conexión está cifrada.

3.5.2 Cookies y otros métodos de rastreo

El principal rastreo que se realiza de nuestra navegación por la web es por publicidad. Se busca crear un perfil de cada uno de nosotros (qué buscamos, qué sitios visitamos, dónde hacemos clic) con el objetivo de crear un perfil sobre nosotros y mostrarnos publicidad que creen nos alentará a consumir. En la mayoría de los sitios que visitamos vemos publicidad, la forma predominante de conseguir dinero de las páginas web.

Las cookies son el método original mediante el que los sitios webs recolectan información de nuestros comportamientos. Estos son pequeños archivos que van guardando en nuestro equipo con información. En algunos casos es útil cuando queremos que recuerden nuestro usuario y las preferencias de la página. Pero en general son usados para recopilar mucha más información personal y luego venderla a otros sitios. Lo otro que pasa es que nosotros entramos en el sitio que queremos visitar, pero el sitio guarda cookies de varios otros sitios que no conocemos.

3.5.3 Medidas de protección en el navegador

Algunos navegadores cuentan con ciertas medidas de protección contra las cookies de forma predeterminada. Tanto Firefox como Safari y Brave, bloquean las cookies de terceros, y los rastreadores que ya están identificados por seguirte a través de internet[23] .

Además los navegadores permiten instalar complementos que agregan funcionalidades, entre ellas las de bloquear algunos de estas herramientas de seguimiento. Entre los recomendados están:

3.5.3.1 Privacy Badger[24] , de la Electronic Frontier Foundation, que ayuda a bloquear rastreadores encargados de recopilar la información de nuestra navegación.

3.5.3.2 Https Everywhere: Que habilita automáticamente el cifrado HTTPS, el candado verde que mencionamos anteriormente.

3.5.3.3 Facebook Container: Que impide que Facebook siga nuestros movimientos por la web.

3.5.3.4 uBlock Origin: Que bloquea publicidad de las páginas y evita su descarga.

3.5.4 Navegación más privada

Si por alguna razón necesitas ocultar la dirección IP de tu máquina, hay dos opciones principales:

3.5.4.1 Virtual Private Network (VPN) es un método mediante el cual te conectas de forma cifrada con un servidor y sales a Internet a través de él. De esta forma, tu dirección IP será la de este servidor que brinda el servicio de VPN y no la de tu máquina. Existen VPNs gratuitas, pagas y tú misma podrías configurar una. El principal punto a tener en cuenta es que debes tener mucha confianza en tu proveedor de VPN, porque ellos sí pueden saber qué equipo fue el que utilizó la red para ver un sitio, y llegado el caso, podrían dar esa información a la justicia. Por lo tanto, elegir un servicio de VPN no siempre es fácil, y en general se recomienda no utilizar los gratuitos, al menos para investigaciones que realmente queramos mantener privadas.

3.5.4.2 The Onion Router (TOR) es un sistema que incluye un navegador web y que oculta nuestra dirección IP al hacer que nuestra comunicación pase por varios servidores antes de llegar a destino, y lo mismo al volver. La comunicación entre los servidores intermedios se realiza de una forma en que entre ellos no saben cuál es la ruta completa que deben trazar (es decir, alguno sabe el equipo de origen, otro sabe el destino final, pero no ambas cosas a la vez). Esta es una forma fácil de esconder o minimizar las oportunidades de ser rastreados cuando navegamos. Es importante que mantengamos el navegador o cualquier otra herramienta que

23 Basados en https://disconnect.me/

24 https://www.eff.org/privacybadger

usemos de TOR actualizada, porque muchas veces se encuentran vulnerabilidades en la seguridad y se corrigen esos errores.

El navegador TOR, además, nos permite utilizar el protocolo .onion, a veces conocido como la web oculta, páginas web que no están disponibles para los buscadores o para los navegadores más comunes. El problema de esta web es que para dificultar que se pueda encontrar información que quiere estar oculta, las urls (es decir el nombre de las páginas) no son tan fáciles de recordar.

3.5.4.3. Tails, TOR + Amnesia como última opción para navegar de forma más cautelosa podemos mencionar a TAILS. TAILS (The Amnesiac Incognito Live System) es un sistema operativo que funciona desde una memoria USB con el que podemos iniciar cualquier equipo de escritorio o notebook. Es una distribución de GNU/Linux pensada para el uso de herramientas de privacidad. Una vez que la conectamos a Internet, todas las aplicaciones que usemos utilizaran la red de TOR ocultando nuestra dirección IP. Viene con el navegador TOR preinstalado, por lo que podremos navegar por la web oculta, además de otras herramientas muy interesantes. Una vez que apagamos el equipo, TAILS se encarga de no dejar rastros de qué hicimos en el equipo mientras lo usamos.

3.6 Cifrado de archivos

El cifrado es una técnica matemática que nos permite elegir quién puede ver el contenido de nuestros archivos. Si utilizamos técnicas de cifrado fuertes, casi podemos asegurar que solo aquellas personas que sean las destinatarias del mensaje o de los archivos, podrán acceder a ellos[25]. Si bien, como decimos, hablamos de técnicas matemáticas, no somos nosotros quienes debemos realizar los cálculos, si no que tendremos programas/aplicaciones que nos ayudarán tanto a cifrar los archivos, como a descifrarlos.

El cifrado se puede realizar tanto en archivos individuales, como en todo el disco duro, o en los mensajes que enviamos a través de distintos servicios de mensajería.

3.6.1 Cifrado de archivos individuales

Cuando queremos enviar un archivo a otra persona y asegurarnos de que solo ella o ellos pueden descifrarlo, utilizaremos una aplicación que lo cifre con sus “llaves” y de esa forma solo ella/s podrán ver el contenido. Una primera opción sería cifrar el archivo con una contraseña segura (vease punto 3.3), pero cuando pasemos el archivo a las otras personas, deberemos pasarles la contraseña, y también deberemos asegurarnos que nadie pueda acceder a ella. Cuantas más personas conozcan la contraseña, más fácil será que se haga pública.

La mejor opción, entonces, será utilizar un método de cifrado asimétrico, el más conocido

25 Mientras el poder de procesamiento de los equipos siga mejorando, es posible que se llegara a romper el cifrado, pero igualmente estamos hablando de muchos años y mucho esfuerzo. Generalmente se considera que con un cifrado fuerte los costos para romperlo son tan grandes (en recursos y tiempo) que no se realizan.

es PGP (o GPG en su versión libre). Este método implica que cada persona tiene dos "llaves": una pública (que será la que comparta con otras personas) y una privada (que mantendrá en su poder y nunca compartirá). Para poder cifrar un archivo para que solo Ana pueda leerlo, necesito tener acceso a su llave pública. El archivo se cifra contra esta llave, y solo quien posea la llave privada podrá descifrarlo. Las llaves públicas pueden estar en repositorios o la propias personas pueden pasarlo. Incluso en poder de la llave pública de una persona, su llave privada no corre peligro. Este mismo sistema se utiliza para cifrar mensajes por correo electrónico para que nadie pueda leer el contenido en el camino (aunque hasta hace poco tiempo, el asunto del mensaje si era público), por lo que se recomendaba dejar este campo en blanco..

La mayor dificultad con GPG es que no hay muchas herramientas amigables (con entorno gráfico) y se necesita conocer la llave pública de la otra persona para poder cifrar un archivo para ella. En el siguiente enlace puedes encontrar una explicación de cómo instalar GnuPG en sistemas windows: https://ssd.eff.org/es/module/como-usar-pgp-para-windows-pc

3.6.2 Cifrado de discos de uso personal

Una buena regla a tener en cuenta es cifrar los discos duros de nuestros equipos (computadora de escritorio, notebook o teléfonos móviles) para que nadie pueda ver su contenido, aún teniendo acceso físico al mismo. Es necesario notar que se puede perder un poco de rendimiento (la velocidad del equipo), pero según el trabajo que estemos realizando, podría ser una práctica necesaria. En caso de no querer cifrar todo el disco, se puede cifrar sólo un Directorio (una carpeta) donde tengamos documentos importantes.

El cifrado de disco completo conviene ser realizado cuando un equipo es nuevo o ha sido restaurado a la configuración de fábrica, ya que si lo queremos hacer posteriormente, en muchos casos deberemos borrar todo el disco y empezar de cero.

Este cifrado, si bien utiliza los mismos algoritmos matemáticos que el que vimos anteriormente, solo precisa una contraseña que, obviamente, recomendamos que sea lo más fuerte y segura posible, como hemos visto en el punto 3.3. No sirve de mucho, tener archivos o directorios cifrados si nuestra contraseña es fácil de adivinar.

En el momento de instalar GNU/Linux o la primera vez que utiliza un dispositivo Android o iOS, el cifrado en los dispositivos móviles no es completo, solo se cifran las carpetas modificadas por el usuario. En Android, el mayor problema es que hasta que no se introduzca la contraseña después de iniciar el teléfono, muchas de las características (como llamadas, alarmas, etc.) no están disponibles[26] .

En el caso de querer cifrar el disco o parte de él en un equipo de escritorio o notebook, hay muchas herramientas, siendo una de las más conocidas Veracrypt[27] . Es software libre y está disponible para todos los sistemas operativos más usados[28] .

26 Esto cambiará a partir de la versión 10 de Android, lanzada en Septiembre de 2019

27 https://www.veracrypt.fr/en/Home.html

28 Windows también proporciona su propia aplicación llamada BitLocker

En el caso de los dispositivos móviles, lo mejor es utilizar las herramientas que ya vienen en el sistema operativo (tanto de Android como de iOS).

3.6.3 Comunicaciones con otras personas

Ya hemos mencionado que el correo electrónico puede cifrarse con GPG, utilizando clientes de correo y no la versión Web de los correos (como por ejemplo Gmail). En caso de querer utilizar correo electrónico cifrado, la mejor opción que tenemos es instalar Mozilla Thunderbird y su complemento Enigmail. Con esta opción también deberemos crear un conjunto de dos llaves, la pública y la privada. Es común que las llaves públicas de correo estén publicadas en servidores a los que tenemos acceso desde el propio Thunderbird, lo que nos facilita escribir un correo cifrado a una persona que no conocemos. Pero tenemos que estar muy seguros que esa es la llave que aún están utilizando y que no haya sido comprometida (es decir, que no pueda estar en poder de otra persona). Por eso, igualmente es recomendable que la propia persona nos facilite esa clave. En este enlace[29] pueden encontrar una guía de cómo instalar todos los programas necesarios y crear su clave.

En el caso de la mensajería instantánea tenemos diferentes opciones:

3.6.3.1 Whatsapp es el sistema de mensajería instantánea más utilizado. Desde hace unas versiones, Whatsapp cifra todos los mensajes que intercambiamos en nuestro dispositivo y solo podrá leerlo quien lo recibe. La tecnología que utiliza es la misma que Signal, una aplicación de la que hablaremos más adelante. El mayor problema con Whatsapp es que solo funciona en base a nuestro número de teléfono, que los metadatos no están cifrados y que pertenece a una empresa privada y centralizada que no sabemos qué hace o puede hacer con esa información.

3.6.3.2 Telegram es un rival de Whatsapp que adquirió mucha fama en los últimos tiempos como más seguro que Whatsapp. Pero esto no siempre es así. De forma predeterminada, los mensajes entre usuarias y usuarios no están cifrados de extremo a extremo, solo lo hará si decidimos iniciar un chat secreto. Y en este último caso, sólo puede hacerse desde el mismo teléfono, ya que las “llaves” que usa para descifrar son por dispositivo. Por ejemplo, si usan la versión de escritorio o web de Telegram, no podrán ver esos chats secretos. Por otro lado, si bien “cualquiera” puede hacer un cliente de Telegram, la forma en que cifra los mensajes no es pública y por lo tanto no es auditable por especialistas. No sabemos qué acceso pueden tener a nuestros mensajes en el servidor. Una ventaja es que no necesariamente debemos establecer un número de teléfono, o por lo menos ocultarlo posteriormente. Siempre es una información menos a ser compartida o vista por otros.

3.6.3.3 Signal es una de las aplicaciones más recomendadas por los expertos en seguridad. Es de código abierto, lo que permite que sea auditada por gente que sepa de seguridad. Ha sido apoyada por personas como Edward Snowden y recomendada por la Electronic Frontier

Foundation. Tiene versiones para Android, iOS y para equipos de escritorio. Puedes ver una guía de instalación en este enlace[30] . Permite enviar mensajes que se borran después de un tiempo, también puede hacerse cargo de los mensajes de texto del teléfono y enviarlos cifrados. Así como Whatsapp, tiene la contra de que sólo es válido registrar un teléfono, con lo cual, sí o sí, estaremos compartiendo es información con las personas que querramos comunicarnos. La otra contra es que al ser menos conocido, no todo el mundo lo tiene instalado. Tampoco permite clientes de terceros, solo podemos utilizar la versión de Signal.

3.6.3.4. Wire es otra aplicación de mensajería instantánea considerada segura. Como todas las anteriores permite videollamadas, que en este caso pueden ser entre más de una persona. Como gran ventaja tiene que no depende de un número de teléfono para registrar un usuario. También tiene aplicaciones disponibles para Android, iOS y equipos de escritorio. Pero tampoco permite que nos comuniquemos con personas que no tienen la aplicación instalada.

3.6.3.5 Otras aplicaciones y sistemas más abiertos y libres requieren más trabajo de nuestro lado. Delta Chat utiliza el protocolo de correo electrónico para lograrlo. La ventaja es que no dependemos de tener un servidor especial o de una compañía u organización, y podemos enviarle un mensaje a cualquier persona que use DeltaChat o pueda verlo en su correo electrónico. Otras implican utilizar protocolos de mensajería instantánea abiertos (como jabber, ahora XMPP) y un complemento llamado OTR que cifra los mensajes que se envían a través de él. Como decimos, estos sistemas tienen la ventaja de no depender de una empresa, organización o servidor en especial. Aunque tienen una mayor curva de aprendizaje y en muchos casos necesitamos nuestros propios servidores y tener aplicaciones para dichos servicios[31] . Otra ventaja que tiene este sistema es la posibilidad de crear cuentas mucho más anónimas, tener una conversación y después olvidarnos de esos usuarios, en caso de ser necesario.

En este sitio[32] puedes encontrar una comparación entre herramientas de mensajería en base varios criterios. Su recomendación pasa por Signal, Wire y Threema (esta última es de código cerrado y de pago).

3.7 Software libre vs. Software privativo

Lo que hace que un programa de computadora sea libre, es su licencia. Todos vienen con un documento que nos indica en qué forma podemos usarlo, si podemos copiarlo o modificarlo, etc. Los softwares más conocidos, como por ejemplo el sistema operativo Windows, permiten la instalación en una sola máquina y no ofrecen la posibilidad de modificarlos o ver cómo están hechos; ni siquiera se pueden prestar, al menos en teoría. Por el contrario, el “software libre” habilita al usuario a que vea cómo está hecho, lo modifique y después pueda dárselo a quien quiera.

29 https://ssd.eff.org/es/module/como-usar-pgp-para-windows-pc

30 https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-android

31 https://ssd.eff.org/en/module/how-use-otr-linux

32 https://www.securemessagingapps.com/

En los albores de la historia de la computación, cuando los monitores eran verdes y negros y las computadoras apenas si se veían en algún laboratorio muy especializado, todos los programas eran libres. Pocas personas se dedicaban a desarrollarlos y en general trabajaban en una gran comunidad donde el intercambio de los programas, todavía en disquetes, facilitaba que pudieran ayudar a mejorarlos.

Pero cuando las computadoras personales empezaron a ser masivas, algunas empresas consideraron que no era bueno que cualquiera pudiera ver cómo estaba hecho el programa: ellas habían invertido dinero en su desarrollo y cualquier otra empresa podría utilizar sus avances para su propio beneficio. Entonces comenzaron a esconder el código fuente de los programas –las instrucciones que los programadores le dan a la computadora– para que sólo puedan verlo quienes trabajaban allí.

Para su desgracia, en 1984, Richard Stallman, un investigador del Massachusetts Institute of Technology, inició un movimiento para mantener el software y su código libre de las trabas de las empresas. Compartiendo los conocimientos, pensaba que la sociedad se beneficiaría con mejores programas.

0 la libertad de usar el programa, con cualquier propósito (uso).

1 la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (estudio).

2 la libertad de distribuir copias del programa, con lo cual se puede ayudar a otros usuarios (distribución).

3 la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (mejora).

Las libertades 1 y 3 requieren acceso al código fuente, porque estudiar y modificar software sin su código fuente es muy poco viable.

3.8 De orientación legal: ¿Cuándo una acción se convierte en delito?

Entender cada figura legal

A continuación, se hará un desarrollo sobre algunos tipos de violencias digitales que pueden encontrarse, identificando la manera en la que están regulados en la normativa nacional y desarrollando una explicación de dichas figuras jurídicas.

Es importante determinar que muchas figuras delictivas o jurídicas no se encuentran establecidas de manera específica dentro de la legislación boliviana; sin embargo, algunas de dichas figuras pueden vincularse a delitos digitales por el hecho de que los medios a través de los cuáles se cometen dichos delitos se han ido amplificando, debiendo en ese sentido, también ampliarse la interpretación de la figura jurídica.

Usualmente, detrás de las figuras jurídicas, se verá un derecho humano que está siendo protegido, ello debido a que el ámbito de los derechos humanos se constituye en un área transversal en el derecho. Así, en materia penal, los tipos penales suelen proteger un bien jurídico específico, estando dividida la configuración del código penal, por delitos o tipos penales que regulan distintos bienes jurídicos. Sin embargo, en el ámbito de los delitos informáticos, no se determinará un solo bien jurídico protegido, sino, varios; esto debido a que la configuración de un delito informático, se vincula por su relación con ámbitos computacionales o de informática.

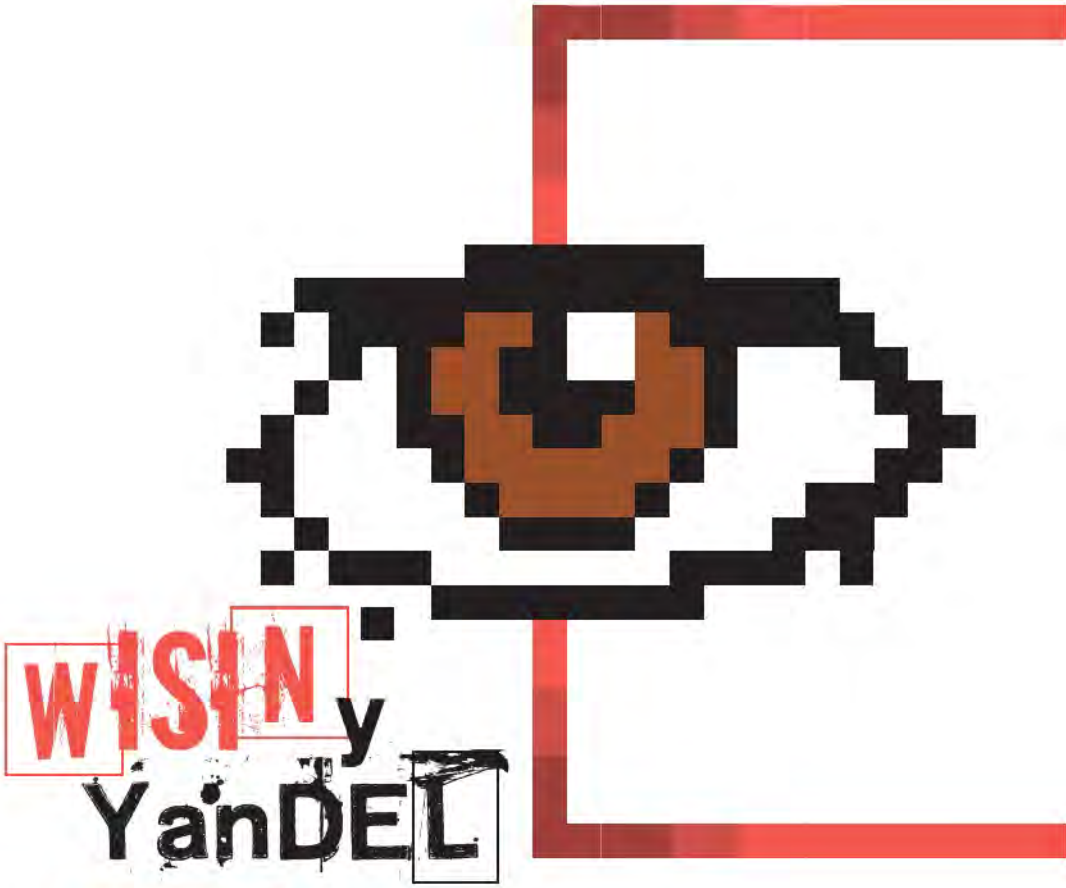
> En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información." [33]

Es por ello, como se mencionó, que existirán delitos que por más que no se encuentren tipificados de manera específica como digitales o informáticos, por el medio utilizado para la comisión del mismo, podrá determinarse como tal.

33 (Casabona citado Acuria, s.f., pg. 8)

El código penal boliviano data del 18 de marzo de 1997, y ha tenido una serie de modificaciones a lo largo de diversos años; sin embargo, son solo 2 los artículos determinados como informáticos de manera pura en la determinación del nombre de los mismos. Estos delitos son los estipulados en el artículo 363 bis (Manipulación informática) y el artículo 363 ter (Alteración, acceso y uso indebido de datos informáticos).

A pesar de dicha delimitación, como fue mencionado anteriormente, existirán delitos que por más que no estén tipificados como informáticos, podrán ser catalogados como tales si al cometerlos, se han utilizado medios digitales o informáticos.



Acosador, acosador, acosador...
maldita sea la hora en que te encontré
Acosadoooor con tu fake no me vas engañar.
Acosador, acosador, acosador...
maldita sea la hora en que te encontré

4. Figuras legales y delitos digitales

4.1 Ciberacoso

El ciberacoso puede definirse como el

> (...) conjunto de comportamientos mediante los cuales una persona, un conjunto de ellas o una organización usan las TIC para hostigar a una o más personas. Dichos comportamientos incluyen, aunque no de forma excluyente, amenazas y falsas acusaciones, suplantación de la identidad, usurpación de datos personales, daños al ordenador de la víctima, vigilancia de las actividades de la víctima, uso de información privada para chantajear a la víctima, etc. [34]

El ciberacoso se constituye en una figura compleja, debido a su amplitud, en la cual se pueden incluir diversas acciones. Como se mencionó, muchos de los delitos a desarrollar, no están establecidos de manera específica en un ámbito digital, ese es el caso del ciberacoso, que como figura específica no se encuentra tipificada en el Código Penal boliviano; sin embargo, la figura que llegaría a aplicarse en éstos casos sería el delito de "acoso sexual", regulado por el artículo 312 del Código Penal, el cual establece:

> Artículo 312 quater. (Acoso sexual).
>
> 1. La persona que valiéndose de una posición jerárquica o poder de cualquier índole hostigue, persiga, exija, apremie, amenace con producirle un daño o perjuicio cualquiera, condicione la obtención de un beneficio u obligue por cualquier medio a otra persona a mantener una relación o realizar actos o tener comportamientos de contenido sexual que de otra forma no serían consentidos, para su beneficio o de una tercera persona, será sancionada con privación de libertad de cuatro (4) a ocho (8) años.
>
> 2. Si la exigencia, solicitud o imposición fuera ejercida por un servidor público en el ámbito de la relación jerárquica que ostenta, será destituido de su cargo y la pena será agravada en un tercio.

Dicho tipo penal, presenta ciertas características, que se desarrollaran a continuación. Una de ellas, es la referida a la relación entre la persona que comete el delito y la víctima, debido a

34 Bocij y McFarlane citados por Verdejo, 2015, pg. 35

que el hostigamiento que es el eje central del acoso, debe ser realizado por una persona que realice dicho hostigamiento en base a ocupar una determinada posición jerárquica o de poder. Ahora, la determinación de dicha posición de poder, estará vinculada a las características del caso, porque la concepción de poder, usualmente se vincula con un ámbito político, pero debe entenderse en realidad en un ámbito de interrelación entre personas, por lo que puede desarrollarse también en ámbitos personales y sociales.

El hostigamiento presentado en el delito estará relacionado a producir un daño un daño o perjuicio cualquiera, como también, a condicionar la obtención de algún beneficio. Dichos aspectos, buscarán finalmente que se obligue por cualquier medio a mantener relaciones, actos o comportamientos de contenido sexual, que la persona que es víctima no hubiese consentido si no era por el mencionado hostigamiento, amenaza o el condicionamiento para la obtención de un beneficio.

El delito está vinculado de manera específica a ámbitos sexuales y a la presión de conseguir alguna relación de dicho tipo con la víctima. Se realiza ésta aclaración, porque también pueden existir amenazas o intimidaciones en otros ámbitos, pero los mismos se refieren a ámbitos económicos o más genéricos, y los mismos están establecidos en otros tipos penales.

Dentro del delito de acoso sexual, es importante mencionar que el beneficiario del delito puede ser tanto quien comete directamente el delito u otra persona; es decir, una persona puede hostigar, amenazar o cualquiera de las acciones establecidas, a otra persona, pero para que el acto o comportamiento sexual sea realizado con una tercera persona, que puede o no, conocer los antecedentes de cómo llegó a ocurrir el acto sexual.

Además, se establece que el hecho de que el delito sea cometido por un servidor público, agrava la pena en ⅓, teniendo como consecuencia además, la destitución de la persona del cargo público que ostenta y en base al cual habría realizado el acoso sexual.

Además del mencionado artículo, otro tipo penal establecido en la legislación boliviana es el “acoso político contra mujeres”, el cual se encuentra tipificado en el artículo 148 bis, que establece:

> Artículo 148 Bis (Acoso político contra mujeres). Quien o quienes realicen actos de presión, persecución, hostigamiento y/o amenazas en contra de una mujer electa, designada o en el ejercido de la función político - pública y/o de sus familiares, durante o después del proceso electoral, que impida el ejercicio de su derecho político, será sancionado con pena privativa de libertad de dos (2) a cinco (5) años.

Así, el acoso por medios digitales o informáticos también podrían estar direccionados a mujeres que se desenvuelven en un ámbito político o público. La configuración de dicho delito establece que pueden existir acciones de presión, persecución, hostigamiento y/o

amenazas a funcionarias públicas, debido a que el código abre la configuración al establecer que no son solo mujeres en cargos electos, sino también, designadas o que se encuentren en la función pública. Además las acciones que forman parte del delito pueden ser realizadas no de manera directa contra la mujer funcionaria pública, sino también, en contra de sus familiares.

El acoso político buscará impedir el ejercicio del derecho político de la funcionaria.

4.2 Ciberbullying

La figura del bullying es cada vez más conocida y se va haciendo más pública dentro de la sociedad. Es importante partir de ésta figura inicial para luego desarrollar qué es el ciberbullying.

El bullying se define "(...) como un acto o comportamiento agresivo e intencionado, llevado a cabo de manera repetida y constante a lo largo del tiempo por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente"[35] .

Por la evolución de la sociedad y los distintos medios por los cuales actualmente las personas se interrelacionan, es que un subtipo de bullying es el ciberbullyng, que respecto a las acciones no tendrá diferencia con la denominación genérica, lo que diferenciará a éste subtipo son los medios a través de los cuáles se realizan los actos.

Así, el cyberbullying, también denominado acoso escolar, tendrá lugar "(...) cuando una persona, de forma intencionada y repetida, ejerce su poder o presión sobre otra con ayuda de medios electrónicos y de forma maliciosa, con comportamientos agresivos, tales como insultar, molestar, el abuso verbal, las amenazas, humillaciones, etc."[36]

La teoría establece que en el cyberbullying, también se ven acciones de hostigamiento como en el cyberacoso; sin embargo, la diferencia es que el hostigamiento ejercido en el cyberbullying es realizado entre iguales, es decir, entre niños y/o adolescentes, debido a que su configuración está vinculada al ámbito escolar.

La figura del bullying ha sido tomada en la legislación boliviana; sin embargo, no está tipificada como tal en el código penal, sino que su desarrollo se encuentra en el Código de la niña, niño y adolescente. El término utilizado en el mencionado código no es de bullying y cyberbullying, sino que se refieren a tipos de violencia en el sistema educativo, estableciendo distintos tipos de violencia, incluyendo también, acciones que no se consideran bullying de maner a específica, porque también hace referencia a la violencia que puede ser ejercida en contra de las niñas, niños adolescentes por parte de los padres y/o profesores. Lo interesante del desarrollo realizado por el Código niña, niño y adolescente, es que hace una referencia expresa a la violencia ejercida por medios digitales.

> Así, será el artículo 151 del Código niña, niño y adolescente, el que desarrolla los distintos tipos de violencia en el sistema educativo,

35 Olewus citado por Ardilla, Marín y Pardo, 2014, pg. 44
36 Cevera citado por Ardilla, Marín y Pardo, 2014, pg. 45

estableciendo:

Artículo 151. (Tipos de violencia en el sistema educativo).

I. A efectos del presente Código, se consideran formas de violencia en el Sistema Educativo:

a) Violencia Entre Pares. Cualquier tipo de maltrato bajo el ejercicio de poder entre dos (2) estudiantes, o un grupo de estudiantes contra una o un estudiante o participante, que sea hostigado, castigado o acosado;

b) Violencia Entre no Pares. Cualquier tipo de violencia con ejercicio y/o abuso de poder de madres, padres, maestras, maestros, personal administrativo, de servicio y profesionales, que prestan servicio dentro de una unidad educativa y/o centro contra las o los estudiantes y/o participantes;

c) Violencia Verbal. Referida a insultos, gritos, palabras despreciativas, despectivas, descalificantes y/o denigrantes, expresadas de forma oral y repetida entre los miembros de la comunidad educativa;

d) Discriminación en el Sistema Educativo. Conducta que consiste en toda forma de distinción, exclusión, restricción o preferencia fundada en razón de sexo, color, edad, orientación sexual e identidad de género, origen, cultura, nacionalidad, social y/o de salud, grado de instrucción, capacidades diferentes y/o en situación de discapacidad física, intelectual o sensorial, estado de embarazo, procedencia, apariencia física, vestimenta, apellido u otras, dentro del sistema educativo;

e) Violencia en Razón de Género. Todo acto de violencia basado en la pertenencia a identidad de género que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para cualquier miembro de la comunidad educativa;

f) Violencia en Razón de la Situación Económica. Todo acto orientado a la discriminación de cualquiera de las y los miembros de la comunidad educativa, basada en su situación económica, que afecte las relaciones de convivencia armónica y pacífica; y

g) Violencia Cibernética en el Sistema Educativo. Se presenta cuando una o un miembro de la comunidad educativa es hostigada u

> hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación.
>
> II. Los tipos de violencia descritos en el presente Artículo, serán considerados infracciones mientras no constituyan delitos.

Como se mencionó, la configuración de violencia en el sistema educativo, determina una figura específica para el cyberbullying, que correspondería a la figura del inciso g) denominada violencia cibernética; así, cuando el hostigamiento, las amenazas, acoso o humillaciones sean realizadas a través de medios digitales, nos encontraríamos ante una figura de cyberbullying. El inciso establece de manera expresa algunos de los medios digitales específicos mediante los cuales puede realizarse en cyberbullying, como por ejemplo: correos electrónicos, blogs, redes sociales, entre otros; sin embargo, el listado solo tiene carácter enunciativo y no limita el uso de otros medios que no estén en el listado.

Se debe tomar en cuenta que esta figura al no estar regulada por el Código penal, sino por el Código niña, niño y adolescente, no se constituye en delito; así se establece que dichas acciones, siempre y cuando no se constituyan en delitos, serán considerados como infracciones, las cuales no serán resueltas en ámbitos penales, sino que la autoridad que conocerá dichos procesos serán los juzgados públicos en materia de niñez y adolescencia.

4.3 Fraude cibenético

El fraude como figura jurídica, se determina como:

> Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio[37] .

Así, el fraude está configurado por acciones de engaño que principalmente buscan un beneficio de tipo económico, el cual va en perjuicio de la víctima. Dicho fraude si es realizado a través de medios digitales o cibernéticos, se constituirá en fraude cibernético.

Respecto a éste delito, se pueden observar diversas figuras vinculadas en la legislación

37 Instituto de Auditores Internos citado por Ortiz et al, 2018, pg. 239

penal boliviana. Como se mencionó, son sólo 2 los delitos determinados de manera expresa como informáticos, será en la figura del fraude cibernético donde se encontrará uno de esos delitos, correspondiente al artículo 363 bis del Código penal, que determina:

> Artículo 363 bis.- (Manipulación informática).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

La configuración del delito mencionado establece de manera precisa la manipulación de procesamiento o transferencia de datos informáticos, y la finalidad es la transferencia patrimonial indebida, por ello su naturaleza económica.

El delito de manipulación informática también establece que el beneficio de dicha transferencia, no es exclusiva de quién comete el delito, sino que puede ser en beneficio de terceros, y que debe existir un perjuicio de la persona afectada. es decir, la víctima.

Es ésta figura la que podemos vincular, a manipulaciones de transferencias bancarias o de compras vía internet, en las cuales al manipular los datos que se utilizan a través de medios digitales, se pueden desviar fondos provenientes de cuentas bancarios, por ejemplo.

Pero además de dicho delito que está vinculada a la manipulación de datos informáticos, se pueden determinar otros, que por más que no se determinen en la legislación como propiamente informáticos, si los medios para su comisión son digitales o informáticos, pueden configurarse en fraude cibernético. Estos delitos son el fraude comercial y la estafa.

El fraude comercial es regulado por el artículo 235 del Código Penal, que establece:

> ARTICULO 235°.- (FRAUDE COMERCIAL).
>
> El que en lugar público o abierto al público engañare al comprador entregándole una cosa por otra, siempre que no resulte delito más grave, será sancionado con privación de libertad de seis meses a tres años.

Así el fraude comercial, está referido a relaciones de compra y venta, determinando que dicho delito se configurará cuando en un ámbito comercial, un vendedor realizará un engaño, entregando a un comprador una cosa (la que es objeto de la venta) en lugar de la que hubiera ofrecido. Por más de tener una configuración genérica, dicho delito podría configurarse también cuando el ofrecimiento de los productos se realiza a través de medios digitales, siempre y cuando sean considerados públicos, entre los cuales se podrían mencionar las

páginas web, redes sociales, etc.

Por otra parte, es el artículo 335 del Código penal, el cual regula el delito de estafa, estableciendo:

> Artículo 335°.- (Estafa). El que induciendo en error por medio de artificios o engaños, sonsacare a otro dinero u otro beneficio o ventaja económica, incurrirá en privación de libertad de uno a cinco años y multa de sesenta a doscientos días.

En éste caso, el delito de estafa, que se configura a través de engaños que inducen al error, tiene la finalidad de obtener una ventaja de tipo económico. De igual manera, la configuración es genérica, pero si los medios que se utilizan son informáticos o digitales, estaríamos ante la figura del fraude cibernético.

4.4 Robo y suplantación de identidad

El robo o suplantación de identidad se define como la "suplantación o identidad a que finge ser una persona que no es"[38]. Dicha suplantación se puede realizar usando tanto documentos personales como documentos bancarios, por ejemplo tarjetas de crédito o de débito. Así mediante los datos obtenidos a través de dichos documentos u otros, una persona se hará pasar por una identidad que no es la propia.

A pesar de que los datos personales, usualmente se vinculan con documentos de identidad, en la sociedad actual, son otros lugares los cuales también almacenan gran cantidad de datos, los que puede ser utilizados para realizar una suplantación de identidad; por ejemplo los celulares, contienen muchos datos que permiten identificarnos, al mismo tiempo, las redes sociales, que cada vez son más utilizadas, también contienen una gran cantidad de datos personales.

La figura de suplantación de identidad no está regulada de manera específica en la legislación boliviana, pero existen 2 figuras que pueden vincularse, éstas son la falsedad material, tipificada por el artículo 198 del Código penal, y la falsedad ideológica, tipificada por el artículo 199 del mencionado código.

En cuanto a la falsedad material, se determina lo siguiente:

> ARTICULO 198°.- (Falsedad material). El que forjare en todo o en parte un documento público falso o alterare uno verdadero, de modo que pueda resultar perjuicio, incurrirá en privación de libertad de uno a seis años.

Así, la configuración del mencionado delito, está relacionado con la falsificación de algún documento público, o la alteración del mismo, debiendo necesariamente resultar algún

38 Cabinas citado por Colectivo Arción, 2013, pg. 14-15

perjuicio, debido a que si no existe un perjuicio, puede argumentarse que el mismo no cumplió con todos los aspectos necesarios para la comisión del delito.

Por otra parte, se tiene la falsedad ideológica, está tipificada de la siguiente manera:

> ARTICULO 199°.- (Falsedad ideológica). El que insertáre o hiciere insertar en un instrumento público verdadero declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con privación de libertad de uno a seis años.
>
> En ambas falsedades, si el autor fuere un funcionario público y las cometiere en el ejercicio de sus funciones, la sanción será de privación de libertad de dos a ocho años.

Dentro de la configuración de dicho delito, no existe la falsificación de un documento público como tal, lo que se determina es que dentro de un documento público se insertan datos que no son verdaderos y que se refieren a circunstancias que el documento busca probar; de igual manera, debe existir un perjuicio al momento de insertar dichas declaraciones falsas.

Además se establece que si ambos tipos de falsedades son cometidos por funcionario público en el ejercicio de sus funciones, se constituye en un agravante, siendo mayor la sanción.

Ahora, los aspectos en común que tienen ambos tipos de falsedades es que recaen sobre un documento público, para entender qué es considerado un documento público, debemos complementar la configuración con lo establecido por el Código Civil en el artículo 1287:

> ARTÍCULO 1287. (CONCEPTO).
>
> I. Documento público o auténtico es el extendido con las solemnidades legales por un funcionario autorizado para darle fe pública.
>
> II. Cuando el documento se otorga ante un notario público y se inscribe en un protocolo, se llama escritura pública.

Así, los documentos públicos en la legislación boliviana son aquellos que son emitidos por determinadas autoridades, y que guardan una serie de formalidades, o en su caso, aquellos protocolizados ante una notaria o un notario de fe pública. Por ende, al hacer referencia a documentos públicos, se pueden determinar diversos documentos como: cédulas de identidad, licencias de conducir, sentencias, escrituras públicas, entre otras.

En el caso de que una persona utilice una cédula de identidad falsa, haciéndose pasar por

una tercera persona, por ejemplo, se podría determinar la existencia de una suplantación de identidad a través de la comisión del delito de falsedad material.

Ahora, la sociedad en la que actualmente nos desenvolvemos, ha generado grandes cambios, y nuestra identidad que en algún momento estuvo vinculada de manera exclusiva al mundo material, ahora está también en relación al mundo digital, siendo nuestro ser digital una extensión de nuestro ser material. En ese entendido, en la doctrina se maneja el término de identidad digital, entendida como el "(...) conjunto de la información sobre un individuo o una organización expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital"[39] .

A pesar de dicha realidad, en la cual nuestra identidad digital, es solo una extensión de nuestra identidad material, la suplantación de identidad en ámbitos digitales, no se encuentra regulada en la legislación boliviana. Esto se debe a la caracterización mencionada, en vinculación con el requisito de que las falsedades recaigan sobre documento público, y el hecho de que los perfiles que construimos en el ámbito digital, no cumplen con los requisitos que la legislación establece para considerar a un documento público.

Es por ello, que dependiendo del caso, si existe la suplantación de identidad en un ámbito digital, podría establecerse más bien, la relación con otro delito, por ejemplo la estafa.

4.5 Grooming

Se define al grooming como

> "(...) un acoso ejercicio por un adulto hacia un menor y se refiere a acciones realizadas deliberadamente para establecer una relación y control emocional sobre uno niño o niña o adolescente con el fin de concluir con un abuso sexual"[40] .

En el grooming se tendrá cierta caracterización, debido a que necesariamente estamos hablando de un acoso ejercido por parte de un adulto hacia una niña, niño o adolescente, por lo que la víctima siempre será una persona menor de edad.

Además presenta fases: amistad, relación y comportamiento sexual. En la fase de amistad se realiza el primer contacto y las preguntas sobre gustos y preferencias, que lleven a una vinculación de tipo amistosa; la fase de relación se caracteriza por el vínculo de confianza que se genera y que por ende, permite obtener mayor información de la víctima; finalmente en la fase de comportamiento sexual, como su nombre lo indica, se consolidará una relación de tipo sexual, que hay que entenderla en el sentido amplio, porque puede estar en relación a un acceso carnal, pero no de manera limitativa, porque incluye otros actos de contenido sexual, como el envío de imágenes, la grabación de ciertos comportamientos sexuales, entre otros.

La figura del grooming no se encuentra tipificada de manera expresa, al igual que otras

39 INTECO citado por Santamaría, 2015, pg. 16
40 Verdejo, 2015, pg. 39

figuras revisadas; sin embargo, existen delitos que pueden vincularse, cuando el acercamiento y el relacionamiento se realice a través de medios digitales. Además, como el grooming tiene distintas fases, se pueden establecer relaciones de distinto tipo, por lo que es más de un tipo penal el que podría relacionarse con la figura del grooming.

El Código penal, en el artículo 342, determina el tipo penal de engaño a personas incapaces, que establece:

> Artículo 342°.- (Engaño a personas incapaces). El que para obtener para sí o para otros algún provecho, abusando de las necesidades, de las pasiones o de la inexperiencia de una persona menor de dieciocho años o abusando del estado de enfermedad o deficiencia psíquica de una persona, aunque no esté en interdicción o inhabilitada, la indujere a realizar un acto que implique algún efecto jurídico perjudicial para ella o para otros, incurrirá en privación de libertad de tres a ocho años.

El artículo presentado, hace referencia a engaños que se realizan a una persona menor de edad o con una discapacidad psíquica[41] , con el fin de que la persona realice un acto que llegue a tener un efecto perjudicial, ya sea de manera directa para la persona o para una tercera. Dicho establecimiento, es genérico porque la determinación de un "acto que implique algún efecto jurídico", es bastante amplia, pudiendo ingresar en dicho supuesto una amplia serie de acciones. Se debe tener en cuenta, que el delito no hace referencia a aspectos de contenido sexual; sin embargo, no se debe olvidar que el grooming presenta diversas fases, y que el presente delito, podría aplicarse en las primeras fases.

Otro de los delitos vinculado al grooming, es el de pronografía infantil, que se encuentra tipificado en el artículo 323 bis del Código penal:

> Artículo 323° Bis.- (Pornografía de niñas, niños o adolescentes y de personas jurídicamente incapaces).
>
> Comete el delito de pornografía de Niñas, Niños o Adolescentes y de Personas Jurídicamente Incapaces, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de cinco a diez años de presidio.

41 El artículo hace referencia a personas incapaces, debido a que las personas que no han alcanzado la mayoría de edad (18 años) y las personas interdictas declaradas judicialmente, se las considera sin capacidad de obrar, es decir no pueden adquirir obligaciones, ni ejercer sus derechos de manera directa, sino a través de sus representantes legales.

> A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias Niñas, Niños o Adolescentes y de Personas Jurídicamente Incapaces, se le impondrá la pena de tres a seis años de reclusión, así como el decomiso de los objetos, instrumentos y productos del delito.
>
> La misma pena del párrafo anterior, se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, envíe archivos, importe o exporte el material a que se refieren los párrafos anteriores.

La legislación boliviana dentro del delito mencionado, diferencia ciertas conductas y les da distintos tipos de sanciones. La primera parte del artículo hará referencia a las personas que induzca u obligue a niñas, niños y adolescentes, como también, a personas jurídicamente incapaces, a la realización de actos sexuales o de exhibicionismo corporal, entendiendo que la figura de pornografía infantil incluye un amplio espectro, ya que pueden incluir la realización de actos sexuales que incluyen coito hasta la muestra de alguna parte íntima o de vinculación sexual.

Dichos actos de contenido sexual buscan ser grabados, fotografiados o descritos, y ser además, distribuidos en redes tanto públicas o privadas. En éste caso, se podría incluir el hecho de inducir a la realización de actos de contenido sexual mediante una video llamada, o el envío de fotografías, por ejemplo, debido a que ya existe una transferencia de datos, por más que los mismos se mantengan solo entre la víctima y quien comete el delito.

La segunda parte del artículo, hará referencia a otro tipo de relación e involucramiento, porque ya no hará referencia a la persona que directamente induzca u obligue a la realización de los actos de contenido sexual, sino que se refiere a una persona, que posteriormente haya existido la acción de instigar, se encargue de grabar, fotografiar o guardar en algún medio, los actos de las niñas, niños o adolescentes, como también, de personas jurídicamente incapaces. En éste caso la pena es menor, porque no existió la acción de convencimiento para la realización del acto sexual, sino que se remite solo a la captación del acto.

La tercera parte, que se mantiene con la misma pena que en el supuesto anterior, se determina a personas que por más que no hayan participado directamente en la obtención o grabación del material, realice determinada acciones con dicho material, como ser: reproducirlo, almacenarlo, distribuirlo, venderlo, comprarlo, exponerlo, publicitarlo, enviar los archivos, importarlos o exportarlos.

Cabe mencionar, que los supuestos determinados por el artículo del Código penal, pueden realizarse de manera independiente o conjunta; es decir, puede existir una persona que

realice solo uno de los supuestos, como ser obligar a una niña a que le envíe fotografías de contenido sexual; y podría existir otro caso, donde obligue a la niña a mostrar su partes íntimas, realice fotografías de las mismas y posteriormente venda el material.

En los casos en los cuales existan 2 o los 3 supuestos, se debe sancionar tomando en cuenta el rango del supuesto con mayor sanción.

La determinación del delito de pornografía, no hace alusión solo a contactos por vía digital, pero cuando la relación y la obtención del material se ha realizado justamente a través de medios digitales, se configurará como delito informático.

Otros delitos que pueden relacionarse con el grooming, se vinculan a ámbitos más delicados, porque en ellos ya existe un contacto íntimo de tipo sexual entre un adulto y una niña, niño o adolescente.

Si producto de la relación que surgió por medios tecnológicos, existe en la etapa final del grooming, donde ya existe un contacto de tipo sexual, un acceso carnal, podemos hacer referencia 2 delitos, dependiendo de la edad de la niña, niño o adolescente. Así se tendrá el tipo de violación de niña, niño o adolescente, estupro o en algunos casos violación.

La violación de infante, niña, niño o adolescente, se encuentra tipificada por el artículo 308 Bis, del Código Penal, que establece:

> Artículo 308 bis. (VIOLACIÓN DE INFANTE, NIÑA, NIÑO O ADOLESCENTE). Si el delito de violación fuere cometido contra persona de uno u otro sexo menor de catorce (14) años, será sancionado con privación de libertad de veinte (20) a veinticinco (25) años, así no haya uso de la fuerza o intimidación y se alegue consentimiento.
>
> En caso que se evidenciare alguna de las agravantes dispuestas en el Artículo 310 del Código Penal, y la pena alcanzará treinta (30) años, la pena será sin derecho a indulto.
>
> Quedan exentas de esta sanción las relaciones consensuadas entre adolescentes mayores de doce (12) años, siempre que no exista diferencia de edad mayor de tres (3) años entre ambos y no se haya cometido violencia o intimidación.

El mencionado artículo establece que cualquier acceso carnal con una persona menor de 14 años, se constituye en una violación, aun cuando se alegue que existió consentimiento, esto debido a que por la edad de la persona, dicho consentimiento no sería pleno, porque la persona no cuenta aún con capacidad de obrar.

En el caso de grooming, en su última fase, se podría establecer que exista un

consentimiento por parte de la persona menor de 14 años, pero no se debe olvidar que ésta última fase, se realiza después de que ya se ha afianzado una relación de confianza entre el agresor y la persona menor de edad.

Cabe aclarar que de dicha figura se exceptúan las relaciones entre adolescentes mayores de 12 años, siempre y cuando la diferencia de edad no sea mayor a 3 años y sea plenamente consentida.

En caso de que el acceso carnal sea con una persona mayor de 14 años, y medie en dicho acceso el consentimiento de la persona menor de edad, estaríamos ante otro tipo penal que es el estupro, regulado por el artículo 309 del Código Penal, que determina:

> Artículo 309. Estupro.
>
> Quien, mediante seducción o engaño, tuviera acceso carnal con persona de uno u otro sexo, mayor de catorce (14) años y menor de dieciocho (18), será sancionado con privación de libertad de dos (2) a seis (6) años.

De igual manera el delito mencionado podría configurarse en la etapa final del grooming, debido a que la persona adulta al crear ese vínculo de relación de confianza, ha engañado a la persona adolescente, porque nuevamente, a pesar de ser mayor de 14 años, aún no cuenta con la capacidad de ejercicio, para considerar a su consentimiento como un consentimiento pleno.

4.6 Difusión de imágenes íntimas sin consentimiento (DIISC)

La pornografía se define como:

"(...) una representación cuyo contenido ha de ser explícitamente sexual. Tendrá que hacer alusión, por lo tanto, a una forma de expresión —la cual puede plasmarse en libros, fotografías, películas, bandas sonoras, espectáculos teatrales, etc.— que versa, necesariamente, sobre los órganos sexuales, la actividad sexual o cualquier otro elemento que provoque irremisiblemente asociaciones estrictamente sexuales" (Malem, 1992, pg. 220). En ese entendido, hacer referencia el término pornografía es bastante amplio, tanto en contenido como el medio en el que se plasma.

En la actualidad, el contenido de carácter pornográfico se convierte en algo relativamente común, por la facilidad para el acceso, por los medios tecnológicos con los que la sociedad actual cuenta. Además el contenido también suele ser común en el sentido de que está siendo utilizado mediante el denominado sexting, para intercambiar contenido de carácter sexual entre personas entre las que existe o puede existir algún tipo de relación.

> ARTICULO 323° BIS.- (PORNOGRAFIA).

I. Quien procure, obligue, facilite o induzca por cualquier medio, por sí o tercera persona a otra que no dé su consentimiento a realizar actos sexuales o de exhibicionismo corporal con fines lascivos con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o de comunicaciones, sistemas informáticos, electrónicos o similares, será sancionada con pena privativa de libertad de diez (10) a quince (15) años. Igual sanción será impuesta cuando el autor o participe reproduzca o almacene, distribuya o venda material pornográfico.

II. La pena privativa de libertad será agravada en un tercio cuando:

1. La víctima sea niño, niña o adolescente o persona con discapacidad.

2. La autora o el autor sea cónyuge, conviviente, padre, madre o la persona que ejerza algún tipo de autoridad o responsabilidad legal sobre la víctima.

3. La autora o el autor mantenga una relación laboral, de parentesco consanguíneo o de afinidad con la víctima.

4. La víctima sea una mujer embarazada.

5. La autora o el autor sea servidora o servidor público.

6. La autora o el autor sea la persona encargada de proteger los derechos e integridad de las personas en situación vulnerable.

7. La autora o el autor hubiera sido parte o integrante de una delegación o misión diplomática, en el momento de haberse cometido el delito.

8. El delito se cometa contra más de una persona.

9. La actividad sea habitual y con fines de lucro.

10. La autora o el autor sea parte de una organización criminal.

III. Quien compre, arriende o venda material pornográfico, donde se exhiba imágenes de niños, niñas y adolescentes, será sancionado con pena privativa de libertad de cinco (5) a ocho (8) años.

4.7 Trata

La trata de personas es un delito que se encuentra regulado no solo a nivel nacional, sino también a nivel internacional, habiéndose dado una especial relevancia debido a su gravedad y a la amplia posibilidad de que se constituya en un delito que involucra a más de un Estado, al existir un traslado de personas, y redes criminales que operan en distintos países.

En ese sentido, a nivel internacional se encuentra la configuración de una normativa que regula esta figura, y a la cual se puede acudir para poder contar con una definición aceptada a nivel internacional.

El Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia organizada transnacional, define a la trata de personas en su artículo 3, inciso a), de la siguiente manera:

> Por 'trata de personas' se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos.

Así, la trata es un delito complejo, porque pueden realizarse todas las actividades descritas, como también una sola para que se ejecute el mismo; es decir, una persona podría realizar la captación, traslado y recepción de una persona, y estaría cometiendo el delito, pero también una persona que recibiera a la persona víctima de trata, aun cuando no la haya captado, también cometería el delito.

Dichas acciones pueden haber sido realizadas a través de distintos medios, desde el engaño hasta el uso de la fuerza; además, la finalidad propia de la trata es la explotación de la persona, que también puede darse en distintos ámbitos, como la explotación laboral, la explotación sexual e incluso la extracción de órganos.

El delito de trata se encuentra tipificado en el código penal en el artículo 281 bis, que determina:

> "ARTÍCULO 281 Bis. (TRATA DE PERSONAS).
>
> I. Será sancionado con privación de libertad de diez (10) a quince (15)

años, quien por cualquier medio de engaño, intimidación, abuso de poder, uso de la fuerza o cualquier forma de coacción, amenazas, abuso de la situación de dependencia o vulnerabilidad de la víctima, la concesión o recepción de pagos por sí o por tercera persona realizare, indujere o favoreciere la captación, traslado, transporte, privación de libertad, acogida o recepción de personas dentro o fuera del territorio nacional, aunque mediare el consentimiento de la víctima, con cualquiera de los siguientes fines:

1. Venta u otros actos de disposición del ser humano con o sin fines de lucro.

2. Extracción, venta o disposición ilícita de fluidos o líquidos corporales, células, órganos o tejidos humanos.

3. Reducción a esclavitud o estado análogo.

4. Explotación laboral, trabajo forzoso o cualquier forma de servidumbre.

5. Servidumbre costumbrista.

6. Explotación sexual comercial.

7. Embarazo forzado.

8. Turismo sexual.

9. Guarda o adopción.

10. Mendicidad forzada.

11. Matrimonio servil, unión libre o de hecho servil.

12. Reclutamiento de personas para su participación en conflictos armados o sectas religiosas.

13. Empleo en actividades delictivas.

14. Realización ilícita de investigaciones biomédicas.

II. La sanción se agravará en un tercio cuando:

1. La autora o el autor, o partícipe, sea cónyuge, conviviente o pareja de

> la víctima, tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad, tenga a su cargo la tutela, custodia, curatela o educación de la víctima.
>
> 2. La autora o el autor sea servidora o servidor público, goce de inmunidad diplomática, o sea profesional médico o a fin.
>
> 3. Se utilicen drogas, medicamentos o armas.
>
> III. La sanción será de quince (15) a veinte (20) años cuando la víctima fuere un niño, niña o adolescente, persona con discapacidad física, enfermedad o deficiencia psíquica, mujer embarazada, o el autor sea parte de una organización criminal, se produzca una lesión gravísima o se ponga en peligro la vida, la integridad o la seguridad de la víctima.
>
> IV. Si a causa del delito se produce la muerte de la víctima, se impondrá la sanción prevista para el delito de asesinato."

La concepción manejada a nivel internacional, se refleja en la legislación boliviana, estableciendo que el delito de trata igual se configura a través de varias acciones como: el traslado o reclutamiento, privación de libertad, resguardo o recepción de seres humanos. Además establece causales específicas en las que se considera esa finalidad de explotación a través de las finalidades determinadas en los diversos incisos.

Existen determinados agravantes que establecerán que la pena pueda establecerse en sus límites máximos o próximos a él. Así la pena se agrava cuando el/la autor/a o partícipe sea cónyuge, conviviente o pareja de la víctima, tenga determinados grados de parentesco o esté bajo la tutela o custodia de la víctima.

También se agrava cuando quien sea autor ejerza la función pública, tenga inmunidad diplomática o sea profesional médico o de ramas afines. De igual manera, cuando se utilicen drogas (legales e ilegales) o armas.

Existe una sanción diferenciada, la cual es más alta, pudiendo estar entre el margen de 15 a 20 años, que se establece cuando la víctima sea una niña, niño o adolescente, persona con discapacidad física, enfermedad o deficiencia psíquica, mujer embarazada, o el autor sea parte de una organización criminal. De igual manera, cuando se produzca una lesión gravísima o se ponga en peligro la vida, la integridad o la seguridad de la víctima.

Además, si por acciones u omisiones, vinculadas en el delito se causare la muerte de la víctima, el delito será juzgado como asesinato.

4.8 Tráfico

El tráfico muchas veces es confundido con la trata de personas; sin embargo, se constituyen en delitos distintos, que tienen características propias. Al igual que en el caso de la trata, se tienen instrumentos internacionales vinculados a dicha regulación.

El Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional, establece en su artículo 3, inciso a): “Por "tráfico ilícito de migrantes" se entenderá la facilitación de la entrada ilegal de una persona en un Estado Parte del cual dicha persona no sea nacional o residente permanente con el fin de obtener, directa o indirectamente, un beneficio financiero u otro beneficio de orden material”.

La entrada ilegal a la que se refiere el artículo mencionado, está en relación a que dicha entrada se realice sin cumplir las normas migratorias correspondientes; además, se determina que la persona que sea trasladada no sea nacional o residente permanente, y que debe existir un beneficio financiero o material para la persona que realiza el traslado de la persona.

Así, existen diferencias puntuales entre el delito de trata y el de tráfico, debido a que la trata necesariamente se habla de una captación indebida donde pueden haberse usado desde engaños hasta la fuerza, que busca la explotación de la persona que es víctima del delito de trata, de la cual, quien comete el delito se ve beneficiado.

En cambio, en el tráfico de migrantes a pesar de que existe un traslado de personas, no existen los otros elementos propios de la trata, porque dicho traslado es consentido de alguna manera por la persona, y el beneficio económico para la persona que comete el delito será el pago que el migrante ilegal de manera consentida le brinda para que pueda realizar el ingreso en otro Estado. Por ello, se establece que el delito de tráfico es un delito en contra del Estado y que vulnera las normas migratorias; en cambio, el delito de trata se establece claramente como una violación a los derechos humanos, siendo un delito en contra de las personas.

Ahora, dicha diferenciación no impide que los delitos puedan vincularse, por ejemplo que se haya iniciado como un delito de tráfico, simple traspaso de fronteras, y al momento de llegar a la frontera, la persona que debía recibir a quienes estaban siendo trasladadas, decida quitar la documentación de las personas y proceder a una explotación de las mismas, constituyéndose posteriormente el delito de trata.

El tráfico de migrantes también se encuentra tipificado en la legislación penal boliviana, en el artículo 321 bis, que establece:

> ARTÍCULO 321 Bis. (TRÁFICO DE PERSONAS).
>
> I. Quien promueva, induzca, favorezca y/o facilite por cualquier medio la entrada o salida ilegal de una persona del Estado Plurinacional de

> Bolivia a otro Estado del cual dicha persona no sea nacional o residente permanente, con el fin de obtener directa o indirectamente beneficio económico para sí o para un tercero, será sancionado con privación de libertad de cinco (5) a diez (10) años.
>
> La sanción se agravará en la mitad, cuando:
>
> 1. Las condiciones de transporte pongan en peligro su integridad física y/o psicológica.
>
> 2. La autora o el autor sea servidor o servidora pública.
>
> 3. La autora o el autor sea la persona encargada de proteger los derechos e integridad de las personas en situación vulnerable.
>
> 4. La autora o el autor hubiera sido parte o integrante de una delegación o misión diplomática, en el momento de haberse cometido el delito.
>
> 5. El delito se cometa contra más de una persona.
>
> 6. La actividad sea habitual y con fines de lucro.
>
> 7. La autora o el autor sea parte de una organización criminal.
>
> II. La sanción se agravará en dos tercios cuando la víctima sea un niño, niña o adolescente, persona con discapacidad física, enfermedad o deficiencia psíquica o sea una mujer embarazada.
>
> III. Quién promueva, induzca, favorezca y/o facilite por cualquier medio el ingreso o salida ilegal de una persona de un departamento o municipio a otro del cual dicha persona no sea residente permanente, mediante engaño, violencia, amenaza, con el fin de obtener directa o indirectamente beneficio económico para sí o para un tercero, será sancionada con privación de libertad de cuatro (4) a siete (7) años.
>
> IV. Si con el propósito de asegurar el resultado de la acción se somete a la víctima a cualquier forma de violencia o situación de riesgo que tenga como consecuencia su muerte, incluido el suicidio, se impondrá la pena establecida para el delito de asesinato."

En dicho tipo penal, se establecen diversas acciones que corresponden al delito de tráfico, como: la inducción, promoción, favorecimiento, financiamiento o facilitación de la entrada o

salida ilegal de personas del país, para obtener un beneficio económico.

Se determinan también agravantes, en los casos en los que existan inadecuadas condiciones de traslado, quien cometa el delito ejerza la función pública, también si el autor o autora sea encargada de proteger derechos de personas en situación de vulnerabilidad, o en su caso sea parte de una delegación diplomática, también si el delito se comete contra más de una persona, la actividad sea habitual, o el autor o autora sea parte de una organización criminal.

También se agrava si la víctima es niño, niña o adolescente, persona con discapacidad física, enfermedad o deficiencia psíquica o sea una mujer embarazada.

Dichos aspectos son establecidos para ingresos o salidas del país; sin embargo, el traslados ilegales al interior del país también es establecido en el artículo, en su parágrafo III, determinando que dicho traslado debe realizarse a través de engaños, violencia o amenazas con el fin de obtener beneficios económicos. Dicha determinación debe ser estudiada, porque de manera internacional se determina que el tráfico es por excelencia un delito transnacional, teniendo en cuenta que al interior del país no existen normas migratorias internas, que establezcan posibilidad de traslados ilegales en el sentido estricto de la palabra; sin embargo, sí podría existir traslados de personas a causa de engaños o uso de la fuerza.

Finalmente se establece que en el caso de que con el fin de asegurar el delito, la víctima sea sometida o formas de violencia o riesgo, que finalmente tengan como consecuencia la muerte, incluyendo el suicidio de la persona, el delito sería juzgado como asesinato.

Al igual que en otros tipos penales, la configuración de los delitos de tratar y tráfico de personas, no están vinculados de manera explícita a ámbitos digitales, pueden considerarse delitos digitales o mínimamente vinculados a los mismos, cuando el contacto con las personas se haya realizado por medios digitales o tecnológicos. Además, por el avance de la tecnología, y el uso cada vez más masivo de éstos medios, es bastante común el acercamiento utilizando medios digitales. Así, la Defensoría del Pueblo del estado Plurinacional de Bolivia establece que: “[un]a de las estrategias más utilizadas por las organizaciones y redes de tratantes para contactar, seducir e inducir a las víctimas de trata de personas son las Nuevas Tecnologías de Información y Comunicación (NTICs)” (s.f., pg. 4).

4.9 Amenazas

La amenaza se conceptualiza como “(...) la advertencia de males sujeta exclusivamente a una decisión del agente que las emite - puede ser valorada como expresión de una agresión futura sobre la integridad de los intereses de otro o, alternativamente, puede evidenciar la pretensión de interferir en la libertad de decisión de dicho destinatario” (Maldonado, 2018, pg. 3).

En ese sentido, el delito de amenazas busca en última instancia causar miedo e inseguridad

en la persona que está siendo amenazada, pero además busca limitar la libertad de decisión de la persona, debido a que las amenazas usualmente se realizan buscando que una persona haga o deje de realizar determinada cuestión.

La legislación boliviana, tipifica el delito de amenaza en el artículo 293 del Código Penal, estableciendo:

> ARTICULO 293°.- (AMENAZAS). El que mediante amenazas graves alarmare o amedrentare a una persona, será sancionado con prestación de trabajo de un mes a un año y multa hasta de sesenta días.
>
> La pena será de reclusión de tres a diez y ocho meses, si la amenaza hubiere sido hecha con arma o por tres o más personas reunidas.

El delito de amenaza también está configurado de manera genérica, no vinculado a un ámbito digital; sin embargo, las amenazas podrían realizarse desde medios informáticos o digitales.

4.10 Doxing

El doxing se conceptualiza como:

> (...) un conjunto de estrategias destinadas a investigar, recopilar información y difundir información de una persona que fue específicamente seleccionada con un objetivo concreto o como vendetta. Esta búsqueda es de una naturaleza tal que revela información privada de contacto, la localización o, en algunos casos, la identidad real de la persona investigada.
>
> No se trata simplemente de almacenar datos, sino que este tipo de información privada se utiliza como una forma de acoso por Internet, amenazando y extorsionando a la víctima con hacer público lo que se ha descubierto sobre ella. (Badía, s.f., pgs.1 y 2)

La figura como denominación no se encuentra en la legislación boliviana; sin embargo, uno de los 2 delitos determinados como informáticos, se puede relacionar a la figura del doxing. El Código penal en el artículo 363 ter, establece:

> ARTICULO 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).-
>
> El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la

> información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Por lo tanto, el tipo penal de alteración, acceso y uso indebido de datos informáticos, determina que la persona que acceda, utilice, modifique, suprima o inutilice datos que se encuentran en soportes informáticos cometería el mencionado delito, pero que el mismo debe significar necesariamente un perjuicio a la persona que sea titular de dichos datos.

Así, por más que el delito esté referido a un acceso genérico de los datos de una persona, dicho acceso podría realizarse justamente con una intención investigativa y con la finalidad de revelar alguna información de la persona afectada, determinando en éste último aspecto la referencia al perjuicio que debe sufrir la persona.

Al mismo tiempo, ésta figura se podría vincular a ámbitos constitucionales, de manera específica con la acción de protección de privacidad.

4.11 Delitos virtuales contra el honor

Como fue mencionado, en materia penal los delitos se establecen protegiendo usualmente un derecho fundamental, que en materia penal se denominará bien jurídico protegido; así, el honor es protegido a través de determinadas figuras penales, que sancionan acciones que busquen dañar o menoscabar el mismo.

El honor como derecho está resguardado por la Constitución Política del Estado, estableciendo, en el artículo 21, numeral 2: “Las bolivianas y los bolivianos tienen los siguientes derechos: (...) 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad).

A pesar de dicha determinación, la configuración del honor como derecho es compleja, debido a su relación en cuanto a una percepción propia y a la percepción que de uno, tengan los demás. “No se discute la existencia del honor como algo apreciable o valorable por la persona. Pese a las dificultades que se presentan para definir el concepto de honor, podemos acordar con la posición más tradicional que lo entiende comprensivo del concepto que tenga la persona sobre sí misma y el que los demás tengan sobre ella” (Calvo, s.f., pg.1).

La legislación boliviana, determina varios delitos denominados “contra el honor”, que se regulan en el Código penal:

> ARTÍCULO 282°.- (DIFAMACIÓN).
>
> El que de manera pública, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá en prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días.

> ARTÍCULO 283°.- (CALUMNIA).
>
> El que por cualquier medio imputare a otro falsamente la comisión de un delito, será sancionado con privación de libertad de seis meses a dos años, y multa de cien a trescientos días.
>
> ARTÍCULO 284°.- (OFENSA A LA MEMORIA DE DIFUNTOS).
>
> El que ofendiere la memoria de un difunto con expresiones difamatorias o con imputaciones calumniosas, incurrirá en las mismas penas de los dos artículos anteriores.
>
> ARTÍCULO 287°.- (INJURIA).
>
> El que por cualquier medio y de un modo directo ofendiere a otro en su dignidad o decoro, incurrirá en prestación de trabajo de un mes a un año y multa de treinta a cien días. Si el hecho previsto en el Art. 283 y la injuria a que se refiere este artículo fueren cometidos mediante impreso, mecanografiado o manuscrito, su autor será considerado reo de libelo infamatorio y sancionado con multa de sesenta a ciento cincuenta días, sin perjuicio de las penas correspondientes.

Hay que realizar una diferenciación de las diversas figuras; así, la difamación está vinculada a expresiones que puedan llegar a dañar la reputación de la persona, vinculada a un ámbito de relación de la persona con su medio. La injuria, estará más vinculada a un ámbito subjetivo, llegando a afectar a la dignidad y a la autopercepción. La calumnia va a un punto más allá, debido a que se establece de manera concreta al referirse a declaraciones que vinculan a la persona con la comisión de un delito.

De igual manera, éstos delito no son estipulados como digitales, pero cuando los mismos se cometen por medios digitales o cibernéticos, pueden iniciarse procesos penales.

4.12 Para la denuncia de un delito se deberán seguir los siguientes pasos

- Generar un registro de los datos de la persona que denuncia.
- Registro de los hechos narrados por la víctima
- Preguntar cuántas veces ocurrió este hecho.
    - · En caso de ser primera vez, informarle a la víctima que en caso de que ocurra de nuevo, se vuelva a comunicar con la brigada.
    - · Si se presentó el hecho reiteradas veces seguir con los pasos siguientes.

• Preguntar si desea acudir a alguna instancia judicial.

· En caso de no denunciar, sugerir el bloqueo del contacto, usuario o perfil que comete el hecho.

· En caso de denuncia, seguir con los siguientes pasos.

• Informarle a la víctima que deberá documentar todas las pruebas necesarias para probar el delito.

· Capturas de pantallas.

• Realizar búsquedas en navegadores con el avatar del usuario.

• Investigar si el perfil es verdadero o falso, revisar los perfiles en redes sociales.

• Bloquear al contacto, perfil o usuario que esté cometiendo el delito.

4.13 Entidades donde se puede hacer la denuncia

En materia penal se establece que los procesos pueden iniciarse con dos tipos de escritos: las denuncias y las querellas.

• Las denuncias pueden ser realizadas tanto ante la policía como ante el Ministerio Público (Fiscalía). La denuncia puede ser verbal o escrita. Quien tome conocimiento de la denuncia deberá hacer constar la identidad y el domicilio de quien denuncia (estos datos pueden mantenerse en reserva a pedido del denunciante). La denuncia contiene un relato de los hechos ocurridos con el mayor detalle posible, indicando autores, víctimas, testigos y otros elementos de relevancia.

Se debe entregar una copia a la persona que ha denunciado.

Si la denuncia es presentada ante la policía, la misma, dentro de las 24 horas debe informar al fiscal para iniciar la investigación.

Si la denuncia se hace ante el Ministerio público, la o el Fiscal inicia la investigación, debiendo informar al juez de instrucción en materia penal.

• Las querellas se presentan ante el Ministerio Público de forma escrita. El artículo 290 del Código de procedimiento penal establece que la querella debe contener:

1) El nombre y apellido del querellante;

2) Su domicilio real y procesal;

3) En el caso de las personas jurídicas, la razón social, el domicilio y el nombre de su representante legal;

4) La relación circunstanciada del hecho, sus antecedentes o consecuencias conocidas y, si fuera posible, la indicación de los presuntos autores o partícipes, víctimas, damnificados

y testigos;

5) El detalle de los datos o elementos de prueba; y,

6) La prueba documental o la indicación del lugar donde se encuentra.

4.14 ¿Qué roles tienen los jueces, abogados, fiscales, policía, etc.?

En un proceso legal actuarán distintas partes, las cuales tienen diversos roles y tareas que cumplir. A continuación, se establecerá de manera genérica, los roles que tienen los distintos participantes en un proceso judicial.

• **Juezas y jueces**: Son las autoridades judiciales, quienes deciden sobre los distintos conflictos que se les presenten. Son quienes dentro de procesos judiciales dictan una sentencia que resuelva la controversia.

Los jueces son competentes en vinculación al territorio, es decir hechos ocurridos en una determinada ciudad, deben ser conocidos por jueces de dicha ciudad.

De igual manera los jueces son competentes por materia, en relación a un área del derecho en específico: penal, civil, laboral, familiar, etc. Así, un delito es conocido por un juez en materia penal, y no así, en materia familiar.

• **Tribunales**: Los tribunales también son autoridades judiciales, pero se refieren a un órgano colegiado, que está compuesto por más de un juez. En Bolivia, en una primera instancia, solo se tienen tribunales en materia penal, de manera específica los tribunales de sentencia, que conocen delitos de orden público.

Dichos tribunales, antes estaban configurados por 2 jueces técnicos y 3 ciudadanos; sin embargo, las reformas procesales penales han determinado que los nuevos casos se conozcan solo ante los jueces técnicos, eliminando la figura de los jueces ciudadanos

• **Tribunales Departamentales de Justicia**: Es el órgano judicial de máxima jerarquía dentro de los departamentos, las sentencias dictadas en primera instancia por los juzgados y tribunales de 1ra instancia, son revisados por los Tribunales Departamentales, que se dividen en salas por materia.

Resuelven recursos de apelación y dictan Autos de Vista.

• **Tribunal Supremo de Justicia**: Es el órgano judicial de mayor jerarquía a nivel nacional. Resuelven recursos de casación, pudiendo modificar sentencias y autos de vista, dictan Autos Supremos.

• **Denunciado, querellado, imputado o acusado**: Estas denominaciones se dan en materia penal, y corresponden a la persona a la cual se está investigando o juzgando por la comisión de un delito. Cambia el denominativo, dependiendo de la etapa del proceso penal en la que se encuentre.

• **Denunciante, querellante, parte acusadora**: La persona particular que inicia y prosigue un proceso penal en contra de otra persona.

• **Demandante**: Es quien inicia un proceso judicial en materias distintas a la penal, por ejemplo: civil, familiar, laboral, etc.

• **Demandada/o**: Es en contra de quién se inicia un proceso judicial en materias distintas a la penal, por ejemplo: civil, familiar, laboral, etc.

• **Ministerio Público**: Institución que dirige la investigación penal y que se convierte en la parte acusadora en delitos de orden público. Por ello, cuando se cometen delitos de orden público, se tiene la acusación del Ministerio Público y también la acusación particular.

El Ministerio Público está conformado por fiscales, existe un/a Fiscal General del Estado, Fiscales departamentales y fiscales por materia.

• **Policía**: Es la institución que tiene como misión la conservación del orden público a nivel interno. En procesos judiciales colaboran en la parte investigativa, especialmente en procesos penales, quienes bajo la dirección del Ministerio Público se encargan de recabar pruebas y denuncias.

• **Abogadas/os**: Son profesionales que brindan asesoramiento para la defensa de derechos e intereses. En los procesos judiciales, cada una de las partes debe contar con una abogada o un abogado.

Serán quienes realicen la estrategia jurídica para los procesos correspondientes, siendo quienes redactan los escritos, soliciten las pruebas correspondientes y realicen los argumentos en las audiencias.

4.15 Recolección de pruebas digitales

Para la recolección de pruebas digitales se debe consultar a la persona afectada si quiere iniciar un proceso formal con instancias de gobierno. Para iniciar el proceso es necesario conocer el tipo de delito digital, que tiene su propia ruta crítica, si de derecho privado o de derecho público, que son delitos penales o delitos civiles. Para esto, se recomienda contactar a los y las abogados especialistas listados en el punto 6.1.

En el Instituto de Investigaciones Forenses (IDIF)[42] o en el Instituto de Investigaciones Técnico Científicas (IITCUP)[43] se realizan pericias informáticas con una orden fiscal o requerimiento judicial emitido por el Ministerio Público.

Los notarios no sacan pruebas digitales. El notario da fé pública de un hecho, con un acta notariada, las pruebas las recaba un perito especialista informático.

42 Más información disponible en: https://www.fiscalia.gob.bo/index.php/institucional/idif

43 Más información disponible en: https://www.iitcup.org/

4.16 Peritos informáticos

La recolección de pruebas puede ser de manera anticipada o posterior, por lo general en un proceso digital se hace de manera anticipada. Esto depende del tipo de delito digital porque cada uno tiene su propia ruta crítica: si es un delito digital de derecho privado o

de derecho público. Si es de derecho público se recaban las pruebas dentro del mismo proceso, sin necesidad de hacer un proceso de anticipo de pruebas. Ambos necesitan requerimientos fiscales u orden jurídica para iniciar un proceso de recabación de pruebas.

Para iniciar una denuncia, se debe ir al Ministerio Público quien puede derivarte a la unidad especializada de Delitos Digitales en la Fiscalía. Cuando se inicia el proceso es muy recomendable hacerlo junto a un abogado o abogada especializada que tenga una estrategia clara de cómo abordar el delito digital.

Para la obtención de pruebas anticipadas o preventivas de un delito digital, es necesario obtener un requerimiento fiscal u orden judicial para que tengan validez jurídica Si se inicia un peritaje informático sin una orden o requerimiento este no tiene validez legal.

Por ejemplo, cuando quieres iniciar un proceso por un delito digital de difamación, calumnia o injuria, pero no sabes contra quién se inicia el proceso (identificar a la persona contra quien se inicia el proceso es un requerimiento legal), entonces debes iniciar una obtención anticipada de prueba con la unidad especializada del IDIF. El peritaje puede ser de correos electrónicos para encontrar el código fuente, la triangulación del correo, pedir a los operadores de telecomunicaciones te den una dirección IP, etc. Hasta obtener el lugar de dónde sale el correo, el propietario del celular o IP y con eso puedes identificar a la persona que cometió el delito e iniciar un proceso judicial.

Otro ejemplo, es para identificar a la persona que manda mensajes anónimos desde IP móviles, si lo hicieron desde un café Internet, para eso se necesita pedir una recolección de las pruebas de cámaras: ya sea del lugar, los cajeros colindantes por el lugar, etc.

Finalmente, en el caso de que sepas quién es el agresor o agresora puedes iniciar un proceso para que le quitan el celular legalmente y iniciar una pericia al celular. Esto se llama auditoria forense digital para recuperar la información borrada del celular.

.paks
conjunto de fotos y videos
íntimos de una persona.

5. De contención emocional

La contención emocional es la ayuda que se brinda a una persona afectada emocionalmente, para que pueda recuperar su tranquilidad y confianza en sus propias capacidades para continuar con su vida, respetando su propio ritmo y espacio[44]. Por lo que, la contención emocional tiene como objetivo generar un espacio seguro y tranquilo donde la víctima se sienta a salvo, en confianza y pueda relatar lo sucedido.

Es importante tomar en cuenta que es probable que la persona que tenga un primer acercamiento con las brigadistas se encuentre en un estado emocional de angustia y miedo, por lo que es necesario contar con ciertas herramientas básicas, que serán explicadas más adelante, para poder realizar el acompañamiento y orientación de una forma correcta y cálida.

El principal objetivo de la contención emocional es brindar el apoyo necesario para que la mujer pueda clarificarse la situación que está viviendo y defina las acciones a seguir en el corto plazo. Con la contención emocional, se busca que la persona atendida se sienta escuchada, que no se sienta sola y sobretodo, que no se sienta culpable por lo que le ha pasado.

Antes de brindar, contención emocional es importante tener claro algunos aspectos que fueron desarrollados a lo largo de este protocolo:

- Las violencias digitales tienen la misma raiz que las violencias contra las mujeres que ocurren fuera de línea.
- La violencia en Internet es real y tiene efectos psicológicos y físicos.
- No todos los casos son iguales.
- Las mujeres enfrentan la violencia de manera diferente.

5.1 Identificar una persona de confianza de contención emocional y tener un canal seguro abierto con esta persona

Es importante identificar la red de apoyo, muchas veces está constituido por amigas/as, familiares o compañeras/os de trabajo.

En una situación de violencia, lo que más se necesita es confidencialidad, confianza y validación. Las personas con las que se tenga un vínculo afectivo serán quienes formen la red de apoyo.

El canal de comunicación seguro puede ser Signal, por ejemplo, que tiene autodestrucción de mensajes, si se quiere mantener las conversaciones de forma más privada y segura se puede comunicar los aspectos que se consideren “delicados” por esta plataforma.

44 Ferrán Llorente. Guía básica de contención emocional para mujeres víctimas de violencia de género. 2008. Disponible en: Disponible en: http://189.240.117.226/biblos-imdf/sites/default/files/archivos/00390GuiacontencionEmoc.pdf. Consultado el: 2019/08/16

5.2 Primeros auxilios psicológicos (PAP)

En Primeros auxilios psicológicos es importante gestionar la expresión de sentimientos y emociones, procurando comprender a la persona afectada. Para lograr esto podemos tomar en cuenta:

- Se debe tratar con confidencialidad todo lo que nos van relatando. Las mujeres están confiando su experiencia y están compartiendo aspectos muy privados sobre sus vidas. Por lo que es importante dejarles claro que su información está a salvo.
- Las personas tiene diferentes experiencias de vida, vienen de lugares diferentes y tienen modos de vivir, pensar y decidir distintos, hay que aceptar esta diversidad sin juzgarla, se debe evitar emitir juicios, con palabras o lenguaje no verbal. Hay que considerar que la que sabe más sobre lo ocurrido es la persona que está siendo atendida y no nosotras. El papel de una brigadista es acompañarla a buscar soluciones, no imponerlas.
- No se deben prometer cosas que no se van a poder cumplir, es necesario hablar siempre con la verdad y además tratar de no brindar más información de la que necesita, al menos no, en el momento de crisis, la sobreinformación puede confundir.

Para aplicar los PAP no es necesario tener formación académica en psicología, trabajo social o etc. Cualquier persona puede aplicar primeros auxilios psicológicos con el entrenamiento adecuado, esta es la principal diferencia con la terapia. Sin embargo, es importante que antes de acompañar a alguien, la brigadista se haga una autoevaluación de la condición personal frente a la crisis. Si se está atravesando por alguna situación personal (ej. duelo, crisis familiar, experiencia traumática reciente), es recomendable no realizar el acompañamiento. De esta manera, se evita consecuencias negativas sobre la persona afectada y también sobre la brigadista, en ese caso se puede delegar el acompañamiento a otra brigadista.

Es probable que algunas personas que contacten a las ciberbrigadistas no quieran o no necesiten de primeros auxilios psicológicos, por lo que es importante evaluar la aplicabilidad de esta técnica, dependiendo de cada caso. Es muy importante respetar las decisiones de las personas.

Existen dos elementos importantes a la hora de aplicar primeros auxilios psicológicos[45] :

a) Escucha activa: El objetivo de escuchar activamente, es transmitir a la persona afectada que hay otro ser humano acompañándolo. Es demostrar con nuestro comportamiento que estamos escuchando a la que habla. No simplemente se está escuchando sino que se está entendiendo, comprendiendo, dando sentido a lo que se escucha. La escucha activa se logra de la siguiente manera:

- Respetando los silencios, tono de voz tranquilo, adecuarse al ritmo del relato de la víctima.

45 Servicio de Psicología de la Guardia Civil. Primeros Auxilios Psicológicos en Violencia de Género. 2011. Disponible en: https://www.mimp.gob.pe/files/programas_nacionales/pncvfs/Proyecto_Apoyo_Asociacion_Juristas/Guardia_Civil_Guia_Primeros_auxilios_psicologicos_en_VG.pdf Consultado el: 2019/08/1

• Respetando si es que a persona no desea dar detalles sobre su vivencia, lo ideal es que lo cuente cuando se sienta preparada.

• Parafraseando. Esto significa ir repitiendo con palabras lo que ella va diciendo.

• Reforzando lo que va diciendo: “entiendo”, “es normal que estés asustada”.

• Clarificando: términos o frases que no hayan quedado claros.

• Explicando que no sólo se escucha para tener su testimonio, si no que importa lo que le está pasando a nivel humano.

Es importante entender que relatar el evento traumático, si bien puede ser una experiencia positiva pues implica confianza, seguridad y capacidad de contención de las propias emociones, también conlleva un impacto psicológico, el cual se debe afrontar acudiendo a la empatía[46] .

b) Empatía: La empatía es la capacidad de contactar emocionalmente, en este caso, con la víctima. Sería como la habilidad de ser capaces de ponernos en su lugar e intentar llegar a sentir lo que ella siente. El objetivo es comprender, no evaluar.

Es importante evitar lo siguiente para poder crear un espacio seguro;

• Interrumpir el relato. Si algo no queda claro, esperar a que termine la frase y pedir que explique lo que no se ha entendido: ¿qué quieres decir cuando dices esto?

• Minimizar ni desvalorizar con este tipo de frases “no es para tanto, no se preocupe” “tranquilícese”.

• Contra argumentar, “no creo que fuese así”.

• Exigir a la víctima que actúe de una manera diferente.

• Emitir juicios.

• Culpabilizarla por lo que está pasando.

46 Programa de Capacitación y Formación Profesional en Derechos Humanos. Herramientas para la contención emocional en situación de derechos humanos. Disponible en: https://piensadh.cdhdf.org.mx/images/publicaciones/material_de_capacitacion/fase_de_actualizacion_permanente/2011_Herramientas_para_la_contencion_emocional_situaciones_violacion_dh.pdf

De mi perfil yo te bloqué, yo te bloqué.
Te encontré y denuncieee
A facebook le mandéee yo le mande.
De mi perfil yo te bloqueee

5.3 Autodefensa psicológica

Si estás atravesando una situación violencia digital y no sabes cómo enfrentar lo que estás sintiendo, en esta sección encontrarás información que puede ayudarte.

Cuando se habla de autodefensa psicológica, se hace referencia a ciertas técnicas que ayudan a responder o hacerle frente a las emociones negativas que se viven como resultado de la violencia, tienen como objetivo explorar y entender las emociones que se tiene a flor de piel y encontrar la fortaleza interior.

Algunas personas que están atravesando una situación violencia digital, sentirán confusión sobre cómo enfrentar lo que estás sintiendo, en esta sección encontrarás información que puedes proporcionarles[47] :

- Es importante escuchar, validar y compartir emociones, recurrir a los círculos de confianza cercanos, amigos(as) o familiares para poder expresar sentimientos, ayuda mucho. Puede contarles cómo se siente, qué necesita, y mencionarles cómo pueden ayudarle.
- Puede recurrir a grupos u organizaciones feministas, el acompañamiento colectivo es poderoso. Compartir su experiencia ayudará a quitarle la culpa y eso le fortalecerá.
- Que no se culpe por lo ocurrido, la persona agresora es la única culpable.
- Escribir sobre los sentimientos es bueno para exteriorizarlos y para entenderlos, es una actividad que ayuda el desahogo.
- Tomar un descanso de la tecnología, apagar el celular y dispositivos por unas horas ayuda a relajarse.
- Es comprensible que no quiera continuar con sus actividades diarias, incentívala a trata de recuperar tu rutina poco a poco, y a hacer actividades que le causen satisfacción.
- Una técnica sencilla que puede utilizar cuando siente que el miedo o la ansiedad desbordan su cuerpo, es la respiración profunda. Un ejercicio sencillo es el siguiente:

  Inspira profundamente mientras cuentas mentalmente hasta 5, suelta el aire,

  Inspira profundamente mientras cuenta mentalmente hasta 4, suelta el aire,

  Inspira profundamente mientras cuentas mentalmente hasta 3, suelta el aire. respira (Repítelo varias veces hasta que te sientas más relajada(o).

5.4 ¿En qué momento derivar a centros profesionales?

Es importante prestar atención a las señales que nos indican que las personas necesitan ayuda profesional, como mencionamos anteriormente la contención emocional no es terapia

47 Bernal, Marina. Autocuidado y defensa para mujeres activistas. 2006 Disponible en: http://juventudesmascairo.org/redlac2017/wp-content/uploads/2017/01/redlac-insumosfeminismo-autocuidado-y-autodefensa-mujeres-jovenes.pdf Consultado el: 2019/08/15

psicológica, por lo que no puede resolver problemas de grandes magnitudes.

Se debe derivar a centros profesionales, cuando las mujeres muestren alguna de las siguientes señales:

- Ideación suicida: es la presencia de deseos de muerte y de pensamientos persistentes de querer quitarse la vida, el término implica un rango de gravedad, toma en cuenta desde ideas vagas a un plan detallado.
- Querer hacerse daño: Tener impulsos de autolesión. Se trata de un comportamiento, una válvula de escape, para expresarse y sentirse mejor.
- Consumo excesivo de bebidas alcohólicas o sustancias controladas: un patrón de consumo de alcohol o drogas que comprende problemas para controlar el consumo.

AHORA SÍ sin
RESTRICCIÓN!

6. El paso a paso de una ciberbrigadista para asesorar

6.1 Contacto con la persona agredida

Por la particularidad de cada caso de violencia digital, no podremos sugerir un texto único de respuestas. Sin embargo, proponemos algunas respuestas y procedimientos en base a principios de atención a víctimas como: ofrecer ayuda, expresar preocupación por su seguridad y permitir que tome sus propias decisiones.

6.2 Contacto inicial

Cuando se recibe un caso de violencia, sugerimos iniciar la conversación de la siguiente manera:

> **Cibebrigadista**: Hola, soy Ale, ¿en qué te puedo ayudar?
>
> **Persona agredida**: explica la situación.
>
> **Ciberbrigadista**: Lamento mucho que esto te esté pasando y es normal que te sientas así. Sé que es difícil de discutirlo ahora, pero ten la seguridad que manejaremos toda la información con confidencialidad y que puedes hablar conmigo sobre esto libremente. Entiendo lo que te está pasando y quiero ayudarte ¿qué necesitas para que pueda apoyarte?

Este contacto inicial debe ir acompañado de 2 acciones adicionales: conseguir consentimiento de la documentación de su caso para uso interno y asegurar las comunicaciones.

6.3 Consigue consentimiento para documentar el caso

La persona agredida debe dar su autorización para el registro de su caso. Se debe informar sobre el registro, bajo las siguientes características, este es el texto sugerido:

> **Ciberbrigadista**: Me gustaría pedir tu permiso para registrar tu caso. El registro en anónimo y de uso interno. No compartiremos tu nombre o número a terceros. Lo que registramos es la fecha de contacto, lugar de dónde nos escribes, la razón y las recomendaciones que te brindamos. Si no estás de acuerdo, no hay problema.

Si la persona agredida decide no dar su consentimiento sobre el registro, no se anotarán los datos.

6.4 Comunicaciones seguras

Generalmente, las personas agredidas nos contactan por WhatsApp. Si es posible trasladar la conversación a Signal, se continúa la conversación allí.

6.5 Respuestas y procedimientos en base a principios de atención a víctimas

Creemos útil las siguientes respuestas para atender a la persona agredida de manera adecuada:

Ofrece ayuda

- No estás sola, estoy aquí para lo que necesites.
- No eres responsable de lo que te está pasando.
- No importa lo que hayas hecho, no mereces esto.
- Si necesitas hacer la denuncia puedo darte orientación legal y acompañarte a hacer la denuncia.
- Este es el contacto de un abogado de Derechos Humanos con especialidad en informática.
- Revisemos tus configuraciones de privacidad y seguridad en tus redes sociales para evitar que esto te pase otra vez.

Expresa preocupación por su seguridad

- Entiendo lo que te está pasando y quiero ayudarte ¿qué necesitas para que pueda apoyarte?
- Me preocupa tu seguridad, ¿hay algo que pueda hacer para evitar que esto pase en el futuro?
- Si necesitas hablar, puedes escribirme cuando gustes.

Permite que tome sus propias decisiones

- Quiero ayudarte. ¿Qué es lo que necesitas?
- ¿Qué puedo hacer para hacerte sentir más segura?

6.6 Acciones adicionales

6.6.1. Durante el contacto

Recopilar pruebas: se pide a la persona que recopile las pruebas y las guarde en otro lugar. Hay que explicar que si borran conversaciones o contenidos, no podrán ser recuperados y que

aun así se mantendrán en el dispositivo de la otra persona. Borrar un mensaje de una conversación no quiere decir que borra el mensaje para la otra persona.

Sugerir denunciar y/o bloquear el perfil del agresor/a. La diferencia entre bloquear los perfiles es que tú ya no verás su contenido pero esta persona puede seguir publicando contenido que te afecte. Denunciar es hacer un pedido a la plataforma de quitar acceso a la cuenta del agresor/a. Es posible que la persona intente crear otra cuenta para continuar violentando a la víctima.

6.6.2. Acciones al finalizar contacto

Documentar el caso en la base de datos de uso interno. Compartiremos contigo esta base de datos, junto al kit de herramientas digitales, una vez que te inicies como Ciberbrigadista.

Hacer seguimiento después de 1 semana para saber cómo está la persona afectada.

Es muy común que las personas nos contacten con el fin de hackear la cuenta del agresor o agresora para identificar a la persona o hackear cuentas en general. En este caso, se recomienda esta respuesta:

> **Ciberbrigadista**: Entiendo que quieres hackear la cuenta de XXX. Pero al hacer esto estarías violando su privacidad (o libertad de expresión) no podremos apoyarte en ese proceso pero sí podremos intentar identificar a la persona por otros medios. ¿Tienes el número de celular? ¿Cuál es su perfil en Facebook?

7. Lista de profesionales que pueden dar apoyo

Esta lista se actualiza permanentemente en esta dirección https://internetbolivia.org/listas-profesionales

7.1 Abogados

Los profesionales que mencionamos a continuación pueden dar apoyo en orientación legal a las víctimas.

Roxana Pérez Del Castillo

Constitucional y regulatorio. Telecomunicaciones

67000100

La Paz, Bolivia.

Félix Fabian Espinoza Valencia

Máster en derecho informático (UB)

Universidad Católica Boliviana SP

75851003

La Paz, Bolivia.

Ariel Agramont

Derecho Informático, Agramont Law Firm

681426044

La Paz, Bolivia.

Estrella De Los Ángeles Clapez

Derecho Penal e Internacional

76253752

Lorena Borda

Servicio Legal “Defiendete”

76225830

La Paz - Bolivia

Centro de Promoción de la Mujer “ Gregoria Apaza”

Asistencia Legal y Apoyo Psicológico

2841963

El Alto Bolivia.

7.2 Peritos especializados

Antes de contactar a cualquiera de estas organizaciones es necesario pedir una orden judicial o requerimiento fiscal para iniciar el peritaje informático, de otra manera las pruebas no tendrán validez legal.

Instituto de Investigaciones Forenses (IDIF)

Calle Indaburo, entre Genaro Sanjinés y Yanacocha. Al frente del Observatorio San Calixto. La Paz, Bolivia.

Instituto de Investigaciones Técnico Científicas (IITCUP)

Av. Hugo Ernst - Bajo Següencoma - Academia Nacional de Policías - Teléfono/fax: (591) 2786977. La Paz, Bolivia.

7.3 Psicólogos

Los/as profesionales citados/as a continuación tienen experiencia tratando temas de violencia, algunos de los contactos en la lista realizan consultas gratuitas.

Anahi Navarro

Psicoterapeuta/ Sexóloga/Terapia Breve Sistémica

70264656

La Paz, Bolivia

Paola Zubieta

Psicoanálisis y Psicología Clínica

69989808

La Paz, Bolivia

Leonardo Eyzaguirre
Psicólogo/Terapeuta/Hipnoterapeuta
65677086
La Paz, Bolivia

Innes Diana Bernhardt
Psicoterapia Sistémica
70534694
La Paz, Bolivia

Romina Boyerman
Psicoterapeuta
77793343
La Paz, Bolivia

Jazmin Mazo
Psicoterapueta
75251757
La Paz, Bolivia

Universidad Católica Boliviana
Consulta Gratuita
2782222 Int. 2258
La Paz, Bolivia

Consultorio Psicológico y Psiquiátrico
"Pensar Sentir Actuar"
65679868 - 67062611
La Paz, Bolivia

Consultorio Psicológico Psinergia
Terapia Psicológica
2421391
La Paz, Bolivia

7.4 Técnico en seguridad en línea

Loreto Bravo -
Maka@digitaldefenders.org
Digital Defenders Parternship

Nazly Borrero Vásquez
+573108979178
nazlyborrero@isberatung.com
scyberchildren@gmail.com
Fundación Saving CyberChildren Colombia
IT Service and Beratung SA

María Eugenia Orbea
eorbea@activismofeministadigital.org
Fundación Activismo Feminista Digital

Vita Activa
+52155-8171-1117
Línea de ayuda para enfrentar violencia en espacios digitales
www.Vita-Activa.org

7.5 Nuestros contactos

La línea de contacto para atención a víctimas de violencia digital es 62342340. El número es atendido permanentemente por turnos de ciberbrigadistas.

8. Sitios y manuales de interés

https://acoso.online/bo

http://www.comunidad.org.bo/assets/archivos/herramienta/f0da117d5444b7fcf32a3196ca9324b1.pdf

https://www.tedic.org/recomendaciones-de-proteccion-digital-2019/

https://internetbolivia.org/8m/

9. Bibliografía

Alto Comisionado de Naciones Unidas. (2018, junio 18). Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. Recuperado de https://daccess-ods.un.org/TMP/6495627.1648407.html

Athar, R. (2015). From impunity to justice: Improving corporate policies to end technology-related violence against women. 44.

Bernal, María. Autocuidado y defensa para mujeres activistas. Disponible en: http://juventudesmascairo.org/redlac2017/wp-content/uploads/2017/01/redlac-insumos-feminismo-autocuidado-y-autodefensa-mujeres-jovenes.pdf

CIGIDEN. Manual ABCDE para la aplicación de primeros auxilios psicológicos en crisis individuales y colectivas. Disponible en: https://www.preventionweb.net/files/59897_auxiliar.pdf

Ferrán Lorente (2008): Guía básica de contención emocional para mujeres víctimas de violencia de género.
Disponible en: http://189.240.117.226/biblos-imdf/sites/default/files/archivos/00390GuiacontencionEmoc.pdf

Programa de Capacitación y Formación Profesional en Derechos Humanos. Herramientas para la contención emocional en situación de derechos humanos. Disponible en: https://piensadh.cdhdf.org.mx/images/publicaciones/material_de_capacitacion/fase_de_actualizacion_permanente/2011_Herramientas_para_la_contencion_emocional_situaciones_violacion_dh.pdf

Servicio de Psicología de la Guardia Civil. Primeros Auxilios Psicológicos en Violencia de Género.
Disponible en: https://www.mimp.gob.pe/files/programas_nacionales/pncvfs/Proyecto_Apoyo_Asociacion_Juristas/Guardia_Civil_Guia_Primeros_auxilios_psicologicos_en_VG.pdf

Intente cambiar pero no me sale,
he hecho cosas muy repudiables
revisarte el pantalón, el correo, los mensajes...

INTERNET
BOLIVIA
.ORG

SOS
DIGITAL

Hivos
people unlimited

Apthapi
Jopueti
FONDO DE MUJERES
BOLIVIA