MANUAL DE PROCESOS COMUNICATIVOS, AUTOPROTECCIÓN Y SEGURIDAD

Caribe afirmativo

Seguridad para todas y todos
Una mirada desde el enfoque de diversidad sexual y de género

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

www.caribeafirmativo.lgbt

Manual de Procesos Comunicativos, Autoprotección y Seguridad

Investigadores
Alfredo Bula Beleño
Yesselys Barros Reyes
Dagoberto Lavalle Navarro

Pedagogos y trabajo de campo
Heriberto Mejía Mercado
Edwin Nemes Martínez
Carolina Fonseca Anaya

Diseño y Diagramación
Oscar Santana

Director de Caribe Afirmativo
Wilson de Jesús Castañeda Castro

Agencia de los Estados Unidos para el Desarrollo Internacional (USAID/Colombia)

Lawrence J. Sacks
Director

Elizabeth Ramírez
Directora de la Oficina de Democracia, Derechos Humanos y Gobernabilidad

Programa de Derechos Humanos de USAID/Colombia:
Leonardo Reales
Gerente

Fernando Calado
Director

Manuel Gómez
Asesor Móvil

www.caribeafirmativo.lgbt

Caribe afirmativo

Seguridad para todas y todos
Una mirada desde el enfoque de diversidad sexual y de género

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

Esta publicación fue posible gracias al apoyo del pueblo americano y el gobierno de Estados Unidos, a través de su Agencia para el Desarrollo Internacional (USAID). Los contenidos de este documento son responsabilidad exclusiva de sus autores y no necesariamente reflejan los puntos de vista de USAID ni del gobierno de los Estados Unidos.

Corporación Caribe Afirmativo
2019

MANUAL DE PROCESOS COMUNICATIVOS, AUTOPROTECCIÓN Y SEGURIDAD

Introducción

Líderes y lideresas lesbianas, gays, bisexuales y trans enfrentan situaciones de riesgo asociadas a prejuicios relacionados con su orientación sexual, identidad y/o expresión de género diversa. Estos riesgos se presentan comúnmente a través de los medios de comunicación y redes sociales, y en algunos escenarios, son propiciados desde el ejercicio de los mismos liderazgos, debido a la falta de medidas de seguridad y autoprotección. La ausencia de un manejo adecuado de información sensible en el acompañamiento de casos de violencia a personas LGBTI y el uso sin las debidas precauciones de las redes sociales, son ejemplos de acciones que dan lugar a riesgos. En la búsqueda de generar mayor impacto a través de medios de comunicación y redes sociales, se omite el análisis del tipo y la calidad de la información, ignorando así los efectos nocivos que esto puede causar en los colectivos, organizaciones, ciudadanos y ciudadanas beneficiarias de diversos procesos de liderazgo, activismo y participación .

Por ello es importante que, para un adecuado y eficaz ejercicio del liderazgo, activismo y participación en procesos colectivos o de visibilidad, se tengan pautas claras en materia de seguridad y autoprotección para la utilización de herramientas comunicativas, a fin de un desarrollo positivo del trabajo colectivo, con el fin de mitigar los riesgos a los que se ven expuestos líderes y lideresas.

La apropiación de estas recomendaciones resultará con la mitigación de los riesgos a los que se ven expuestas las personas con orientaciones sexuales, identidades y expresiones de género diversas, sobre todo cuando nos referimos a personas que ejercen actividades de liderazgo social en zonas donde ha existido violencia o conflicto armado por parte de opositores, y en algunos casos la indiferencia de los actores estatales u organizaciones, la cual radica a la falta de conocimiento, interés y articulación con las situaciones de riesgos vivenciadas por las lideresas y líderes en el territorio

Comprendiendo que las lideresas y líderes se ven expuestos a diferentes situaciones de riesgo que emergen de los contextos de violencia presentes en los territorios en los que desempeñan sus procesos de liderazgo social, se hace necesaria la sensibilización en la adopción e implementación de medidas

de autoprotección que salvaguarden el goce de sus libertades y derechos humanos. Al identificar las diferentes situaciones de riesgo en los procesos comunicativos a los que diariamente se ven expuestos, se expondrán una serie de recomendaciones sobre el uso correcto de las comunicaciones, su utilidad para la mitigación de riesgos y las históricas barreras para acceder a servicios de seguridad y protección del Estado.

Es así como surge el presente manual integral de insumos, el cual contribuirá al empoderamiento en conocimiento de rutas de protección, indispensables en el planteamiento de estrategias de autoprotección y mitigación de riesgos.

¿Qué es un manual y para qué sirve?

Un manual es un instrumento importante en cuanto a que de forma detallada y concisa imparte unas prácticas correctas y descripción de actividades de realización de un trabajo en particular, así como las rutas y operaciones a realizar para la prevención y mitigación de riesgos.

De acuerdo a lo conceptuado por Duhalt K.M. un manual

> "*Es un documento que contiene en forma ordenada y sistemática, información y/o instrucciones sobre historia, políticas, procedimientos u organización de un organismo social, que se consideran necesarios para la mejor ejecución del trabajo*".[1]

Por su parte el presente manual está diseñado para fortalecer los liderazgos, el activismo y la participación en procesos colectivos o de visibilidad en territorios permeados por violencia contra lideresas y líderes sociales LGBTI que, desde un trabajo organizativo o no, deben procurar por el uso adecuado de procesos comunicativos, el empleo de herramientas comunicativas para la autoprotección y el conocimiento de rutas de protección para la atención de distintas situaciones de riesgos.

Así mismo, este manual se focaliza en los riesgos diferenciados de personas LGBTI que atienden a escenarios de peligro asociados a violencias basadas en el prejuicio y la discriminación, a través de información recopilada mediante jornadas de formación dirigidas al diagnóstico de riesgo, mapeo de actores, entrevista de percepción sobre el contexto territorial y riesgos asociados población LGBTI realizadas en los municipios de Montería, Montelibano, Puerto Libertador , Caucasia y Segovia con apoyo del Programa de Derechos Humanos de USAID, pero que dan cuenta de la situación general de la población LGBTI en cuanto a los procesos comunicativos.

1 K.M. Duhalt. Los manuales de procedimiento en las oficinas públicas. UNAM. México. p. 20.

En este manual se encontrará un diseño de estrategias de autoprotección que se nutre de las experiencias de liderazgos, activismo y participación, de la gestión de los procesos comunicativos asociados al desarrollo de sus objetivos y a fines misionales propios de cada organización o colectivo, y que al mismo tiempo, se emplea como herramienta para la minimización de escenarios de riesgos. Por ello resulta vital el conocimiento en rutas de acceso a servicios de protección del Estado y manejo de segundas estrategias para la superación de barreras propias de la interacción con las instituciones y los agentes del Estado.

¿Qué son los procesos comunicativos?

La comunicación es el proceso a través del cual transmitimos y recibimos ideas, información, mensajes y demás, a través de palabras, gestos o medios de comunicación.

Cuando hablamos de los procesos comunicativos, nos referimos al conjunto de actividades encaminadas a la transmisión e intercambio de datos e información. Se conoce como proceso comunicativo, por lo tanto, al conjunto de actividades vinculadas a este intercambio de datos. Dicho proceso requiere de, al menos, un emisor y de un receptor. La definición de estos dos elementos de la comunicación podrá ser definido de la siguiente manera:

> *"El **emisor** envía ciertas señales (un texto escrito, palabras, un gesto) para difundir un mensaje; cuando estas señales llegan al **receptor**, éste debe decodificarlas para interpretar el mensaje. El proceso contempla una "devolución" del mensaje, a través de la cual el receptor se convertirá en emisor, y viceversa.*[2]*"*

En lo que refiere a las organizaciones y colectivos sociales, los procesos comunicativos tienen un papel muy importante, en cuanto a que es a través de estos que se logra la visibilización de las luchas y procesos de incidencia. Más aun, y hablando de personas LGBTI en el contexto de una sociedad heteronormada,

[2] Do Campo Spada, D. Curso General de Comunicación. Recuperado de http://webcache.googleusercontent.com/search?q=cache:RHVVRYJpm00J:www.komunicacion.com.a r/CdeCO_Unidad_2_EmisoryReceptor.pdf+&cd=11&hl=es-419&ct=clnk&gl=co

es común que miembros de la comunidad se vean obligados a guardar silencio sobre lo que piensan, sienten y sufren. Se convierten entonces los procesos comunicativos en la única ventana de expresión de las personas LGBTI – y en general, en la única forma de dar a conocer su trabajo en pro de sus derechos.

En estos procesos comunicativos es de vital importancia el contexto como elemento de la comunicación, en tanto que las circunstancias o situaciones que sucedan alrededor del emisor permearán la creación del mensaje. Es aquí donde las organizaciones y colectivos en calidad de emisores, deberán obrar con cautela en relación a la información que se transmite, el lenguaje utilizado, y el impacto que este tendrá sobre la organización o colectivo.

Términos Claves

- *Personas LGBTI:* Sigla que agrupa a las personas que se reconocen como gays, lesbianas, bisexuales, trans e intersex. A la vez es una categoría de incidencia política desde la cual es posible hacer luchas y exigibilidad de derechos.
- *Orientación sexual:* Se refiere a la atracción erótico afectiva hacia personas del mismo sexo, sexo contrario o de ambos sexos. Cuando se habla de gays, lesbianas, bisexuales o heterosexuales, se hace referencia a las orientaciones sexuales..
- *Identidad de género:* Son las maneras de sentirse frente al género, la forma de auto determinarse y presentarse frente a los demás. Está referido concretamente a aquellas personas en las que su construcción de identidad no está en sintonía con el género asignado al sexo anatómico con el que nacieron, como lo son las personas trans.
- *Expresión de género:* Se refiere no sólo al cómo se siente una persona frente al género, sino a la manera en que expresa ese sentir a través de unos roles referidos a lo masculino y femenino, y que trascienden lógicas binarias de masculino=hombre, femenino=mujer. En ese sentido, es un error establecer relaciones binarias y deterministas entre orientación sexual y expresión de género, puesto que ello se expresa en una trama de posibilidades y roles, donde parecer no necesariamente indica el ser.

Glosario

- **Seguridad.**

  Cuando hablamos de seguridad nos referimos al respeto y protección de múltiples derechos como la vida, la libertad, la integridad, entre otros.

  Para las organizaciones sociales la seguridad se entiende como la libertad de la que gozamos en la realización de acciones y en las reales garantías de tener una vida digna en su entorno.

- **Autoprotección.**

  La autoprotección se traduce en las acciones que ejecuto para propender por el bienestar propio, lo que va a dar como resultado una eliminación o mitigación de riesgos.

  Esta se refiere a las formas de cuidarse, y está encaminada a fortalecer en ciudadanos y ciudadanas, capacidades de autocuidado y bienestar, que se traducirán en acciones a aprender para evitar afectaciones a la seguridad personal y colectiva.

- **Riesgo.**

  El riesgo es una posible ocurrencia de algo que tendría un impacto negativo o no deseado en la persona o la sociedad que lo identifica.

  Con esta palabra se hace una descripción desde la racionalidad, sobre la posibilidad o probabilidad de sufrir una carga de negativo de algo o por alguien. Para la identificación de un riesgo se deberá verificar que este contenga dos componentes: la probabilidad real de que ocurra una situación de connotación negativa, y el tamaño de ese resultado.

  En los procesos comunicativos, las organizaciones y colectivos sociales se ven expuestos a diferentes tipos de riesgos, como la sobre-exposición de la vida personal u organizacional por los medios de comunicación, el sexting, bullying, la exposición a ser objeto de amenazas y señalamientos, la perdida de información valiosa, susceptible y/o confidencial para la organización y colectivo, entre otras a ser desarrolladas en el presente manual.

- **Redes sociales**.

  Las redes sociales son una herramienta que permite la socialización entre personas, paralelo a la socialización de manera física, dado de que esta se realiza de manera virtual.

  Cada tipo de red ofrece una manera concreta o principal de relacionarse con los miembros que la forman, sin desconocer que además de manera principal de relacionarse existan otras que procuran hacerlas más atractivas a los usuarios. Por ejemplo, WhatsApp funciona principalmente a través de mensajería , pero también permite el envío de fotos, videos, audios y contactos; Instagram usa inicialmente fotos, pero también permite el envío de mensajes, comentarios, videos de corta duración y audios.

CAPITULO I

Seguridad de los procesos comunicativos

LLos procesos comunicativos han presentado un avance y diversificación con la llegada de la Internet, lo que se traduce en la creación y utilización de diferentes medios de comunicación. Este tipo de procesos son una herramienta importante para el fortalecimiento de los liderazgos sociales. Sin embargo, estos medios representan también un reto en la manera en que vienen utilizados como herramientas comunicativas, pues más allá de abrir espacios de interacción e interlocución, conllevan ciertos peligros – sobre todo relacionados a la gran cantidad de información sensible expuesta al público. En esto radica la importancia de la seguridad de los procesos comunicativos.

Los líderes y lideresas sociales, a través de sus colectivos y organizaciones, deben responder a los retos tecnológicos. Esto implica hacer efectivo el activismo y la incidencia política, por lo cual deben ambos asumir estrategias de seguridad y autoprotección para mitigar riesgos. De este modo, se propicia la interacción de lenguajes y espacios diversos, que arroje como resultado el fortalecimiento de estrategias como el autocuidado de la identidad digital, tanto en lo colectivo y como individual.

Para contribuir al empoderamiento de personas con orientaciones sexuales, identidades y expresiones de género diversas y al desarrollo de la sociedad inclusiva, se requiere que los líderes y lideresas LGBTI apliquen en sus actividades cotidianas estrategias de comunicación para interactuar con la comunidad y con aliados y aliadas en la defensa de Derechos humanos. Al respecto, estas estrategias deben tener en cuenta que la información publicada en medios de comunicación no será recibida exclusivamente por personas LGBTI, sino también por la sociedad en general. Surge entonces la necesidad de un lenguaje positivo, propositivo, que propicie el desarrollo de los objetivos de la organización o colectivo.

Por otra parte, hay elementos característicos a las organizaciones, y que pueden ser utilizados para establecer distinciones entre estas, como son:

1. Una finalidad existente y conocida por todos/as las/los miembros de la organización o colectivo.
2. Una distribución equitativa de roles y tareas a realizar.
3. Una división en lo posible de los poderes formales para toma de decisiones y representaciones oficiales.
4. La duración de la organización, que ha de ser indeterminada y que corresponde a la misión y objetivos a desarrollar permanentemente, los medios de comunicación utilizados, la coordinación y manejo de estos y por último el control de resultado.

Al mismo tiempo, es importante tener claridad en lo que respecta a los procesos comunicativos, especialmente en lo referente a ciertos conceptos como información y comunicación, para que, en relación a esta diferenciación, sepamos qué estrategias de seguridad aplicar.

Estas se diferencian en cuanto al objetivo perseguido y no en la estructura de los datos que se transmite: "la información remite simplemente a la transmisión (emisión y recepción) de conocimientos estructurados, mientras que la comunicación consistiría en intercambios de información con objeto de cambiar el comportamiento de los otros"[3].

En este sentido las y los líderes, deben abarcar el uso de las tecnologías desde un una red de seguridad de la información y no solo para la salvaguarda de esta, sino también como un medio de alertas temprana en materia de protección de la población LGBT y de ellos mismos. El acceso a internet a través del teléfono móvil, la descarga de audio y video, y demás herramientas comunicativas que posibilitan el almacenamiento e intercambio de información y comunicación por medio de sistemas digitales son fortalezas que modifican el esquema tradicional por medio de los cuales las organizaciones y colectivos ponen en conocimiento de las personas sus actividades, logros, dificultades y todo tipo de actuaciones que se llevan en cambio en marco de los liderazgos, el activismo y la participación colectiva.

3 Weiss citado por, Bartoli, comunicación y organización. La organización comunicante y la comunicación organizada.1992: p. 69

Esta variedad de estrategias y procesos comunicativos contribuyen a la interacción e incidencia generada por grupos y colectividades LGBTI, siendo posible además activar un sistema de alarmas en el eventual caso de encontrarse expuesto a una situación de riesgo. La labor de los grupos y colectivos de la comunidad LGBTI que sobresalen por su rol social y político implica un necesario acompañamiento de su red de apoyo, tanto institucional como ciudadana, para poder activar diferentes rutas de protección y de acceso a la justicia.

CAPITULO II

Gestión de herramientas comunicativas para la seguridad y autoprotección (mitigación de riesgos)

Para mitigar los riesgos se deben establecer estrategias de seguridad, dado que muchos líderes y lideresas guardan en su poder información confidencial de ciudadanos/as en temas sensibles de defensa de derechos humanos. Así las cosas, una herramienta para aplicar medidas de protección y seguridad con la finalidad de evitar sesgos en la cadena de confidencialidad de la información, que debe ser transmitida por las lideresas y líderes a las organizaciones, instituciones o colectivos por medio del uso de las. tecnologías de la información y comunicación en adelante las TIC.

Resulta acertado entonces considerar la protección de los equipos y los usuarios, la actualización de software y antivirus, como prácticas adecuadas en la gestión de herramientas comunicativas para la seguridad y autoprotección. Se protegerá de este modo el entorno informático de la organización, sus miembros y la comunidad mitigando los riesgos a que están expuestos. A continuación, se exponen y desarrollan recomendaciones para tener en cuenta.

- **Protección y prevención de los equipos**

  En lo que respecta a los equipos de trabajo de las organizaciones y colectivos, se debe hacer énfasis en diferenciar cuáles corresponden al inmobiliario organizacional y cuáles al personal de cada líder o lideresa que forman parte del colectivo.

  De allí se hace necesaria una distinción entre la información que hace parte de la vida personal de cada lideresa y líder que nada tiene que ver con los procesos comunitarios, y cual guarda íntima relación con su rol de defensa y liderazgo, para así determinar el grado de seguridad que se establece al momento de hacer uso o difusión de esta información a través de las TIC. Así las cosas, se recomienda no descargar actualizaciones de programas o aplicaciones de sitios web

públicos sin tener certeza de la seguridad del sitio, fijarse siempre en los comentarios y puntuación otorgada por usuarios a diferentes tipos de aplicaciones y comentarios en sitios web.

En materia de buenas prácticas de protección de los equipos y la información contenida en estos, se recomienda una restricción en la utilización de equipos de carácter organizacional. Es decir, que no todas las personas puedan tener acceso a este y a la información contenida allí, ya que puede ser susceptible de ser copiada por personas inescrupulosas y con intenciones en contra de la organización o colectivo, y con ello de sus lideresas y líderes.

Así mismo, se podrá evitar el incremento de riesgos si se adoptan prácticas de autoprotección como la utilización de contraseñas seguras y cambios de estas regularmente. En los casos en que una persona diferente al colectivo o la organización requiera de la utilización de los equipos, es preferible que existan cuentas, usuarios y equipos con restricciones.

- **Seguridad y autoprotección de correos electrónicos**

  Es importante que líderes y lideresas LGBTI incorporen en los hábitos organizacionales medidas proactivas que eviten los ataques a través de los correos electrónicos, dado que este medio de comunicación es uno de los más utilizados para las interacciones entre sociedad civil e institucionalidad, y donde en muchas ocasiones se halla información confidencial de personas que han sido víctimas de violencia de cualquier tipo.

  Se recomienda en lo posible no registrar los correos por medio de los cuales se trate información confidencial o sensible en sitios web desconocidos como páginas de pornografía, citas en línea, chats, entre otros. De hacerlo, aumentará la posibilidad que el correo quede guardado en listas de spammers[4].

[4] Individuos o empresas dedicados al envío masivo de correos no deseados o también llamados spams.

Así las cosas, como medida de autoprotección, es recomendable que los correos electrónicos tengan claves seguras y que sean cambiadas con una periodicidad de 3 meses, así se evitará la intromisión de usuarios no deseados y con ello compartir información de reserva.

Es importante tener en cuenta que las entidades bancarias no solicitan información sobre claves de cuentas u otro tipo de datos confidenciales a través del correo electrónico. Por ello, al recibir un correo de esta naturaleza, lo recomendable es ignorarlo y borrarlo a fin de minimizar los riesgos de infiltración.

- **Seguridad y autoprotección en redes sociales**

  Primordialmente, hay que tener mucha cautela con la información que se maneja, siendo cuidadosos en los datos que se publicarán en redes sociales. Es recomendable no dejarse llevar por la efusividad de los momentos para así poder seleccionar la información a ser publicada, procurando siempre que ello genere un impacto agradable y de beneficio para la organización, con la cautela de no revelar información que pueda ser utilizada con propósitos maliciosos.

  Por ello, es preferible no publicar información confidencial en estas redes, tales como fotos de eventos de participación de víctimas o personas que consideren que su seguridad puede estar en riesgo, ubicaciones de lugares de homosocialización, entre otros. Esto debido a que si bien lo que se busca es la interacción con un público masivo, podríamos dejar expuestos a víctimas o ciudadanas y ciudadanos participantes de actividades susceptibles de seguimientos, hostigamientos, persecuciones, amenazas y demás situaciones de riesgo.

  Si se busca tener evidencia física de actividades de la organización, se recomienda que se haga un trabajo de estudio y elección cuidadosamente antes de publicar mensajes, fotografías, videos o audios que se publicarán, para evitar hacer pública las identidades e historias personales de personas LGBTI sin su consentimiento, dado que muchas de las personas con las que realizamos las actividades han sido afectadas por la violencia o la discriminación.

Cuando se trate de redes sociales de las organizaciones o colectivos en defensa de derechos de las personas LGBTI, es importante que exista una delimitación entre cuáles son las redes personales y cuáles las organizacionales, ya que estas últimas deberán ser usadas para la consecución de los fines y objetivos, y la visibilización del colectivo u organización. Así las cosas, no es viable publicar fotos o información de carácter personal a través de estas redes organizacionales, y evitar rotundamente ciertas prácticas que podrían ser generadoras de riesgo como sexting o bullying por las redes de la organización o colectivo. En caso de presentarse estas situaciones se recomienda ignorar cualquier mensaje que contengan material pornográfico y hacer los reportes pertinentes en las administraciones de los sitios web y redes sociales.

En las redes personales de líderes y lideresas, evitar poner información muy personal, ubicaciones y fotografías, que puedan dar lugar a un seguimiento o ubicación. Del mismo modo, se recomienda tener cierto grado de privacidad, como, por ejemplo, tener la posibilidad de aceptar las solicitudes de personas que puedan ver el contenido de las publicaciones y rechazar a quienes no conocemos o no deseamos en nuestras redes sociales, además de ello debemos establecer claves de seguridad y cambiarlas con una periodicidad de al menos 3 meses.

De encontrarse en situaciones de riesgo en redes sociales, se recomienda guardar las evidencias que resulten, mediante una captura de pantalla, a fin de formular las denuncias o trámites pertinentes, donde se pueda evidenciar la identificación o nombre de usuarios del autor o la persona a denunciar. Asimismo, las redes sociales tienen espacios en los cuales los usuarios pueden denunciar a otros o a publicaciones si las consideran ofensivas, inapropiadas o que inciten al odio, discriminatorias, a las violaciones de derechos humanos o a la violencia.

- **Seguridad en mensajería instantánea**

  Cuando hablamos de mensajería instantánea nos referimos a aquella forma de comunicación que se produce en tiempo real, aun cuando las personas interlocutoras se encuentren separadas por miles de kilómetros. Entre ellas encontramos WhatsApp, mensajes de texto, Messenger, Skype, entre otras.

  Debido a la inmediatez de la información, este tipo de comunicación ha tomado un auge importante que ha hecho que cada vez sean más las personas que utilicen estos medios para comunicarse.

  En lo que a organizaciones y colectivos LGBTI se refiere, estas aplicaciones de mensajería instantánea constituyen el medio, que acompañado de herramientas tradicionales como el "voz a voz" o el perifoneo, diversifican y nutren las convocatorias a eventos, marchas, formaciones y demás actividades relacionadas con los fines mismos de los liderazgos sociales.

  En este tipo de medios de comunicación se propicia la creación y participación en grupos de mensajería en los cuales todas las personas opinan con relación a diversos temas. Cuando ello suceda a través de medios de una organización o colectivo, se recomienda establecer normas de convivencia digital en grupos y redes sociales, y así evitar la ocurrencia de situaciones de violencia ya sean físicas o verbales.

  Como ejemplos de normas que se pueden establecer al momento de la creación de los grupos, podríamos mencionar el respeto como base fundamental de cualquier proceso de comunicación en que se escucharán opiniones, propuestas o sugerencias de cualquiera de las/los miembros; el manejo de un vocabulario adecuado; y siempre tratar temas referentes a la promoción y protección de derechos de las personas con orientación sexual, identidad y expresión de género diversa, procurando el adecuado manejo y protección de la identidad digital de los colectivos, organizaciones y sus respectivos líderes y lideresas.

  Es vital además no compartir información confidencial y/o sensible a través de estos medios de comunicación como mecanismo de autoprotección personal y colectiva.

Esta medida de seguridad cobra mayor intensidad dado que por tratarse de personas LGBTI y siendo esta una población históricamente discriminada, se manejan información respecto a las luchas, tanto desde lo personal como desde lo colectivo, que podrían poner en riesgo la seguridad, vida e integridad personal al abrir la posibilidad a la interceptación de comunicaciones.

Además de ello, toda la información expuesta a personas inescrupulosas puede ser utilizada para dañar la imagen de las organizaciones y colectivos, y sus respectivos líderes y lideresas, y en el peor de los casos, para la comisión de delitos.

- **Seguridad y protección del almacenamiento de datos**

  En los liderazgos sociales, en el activismo y en la participación de procesos colectivos, sobre todo en aquellos que están en proceso de consolidación, es importante el almacenamiento de información tanto física como digital. La información de colectivos y organizaciones cumple las veces de verificador de las actividades propuestas y desarrolladas en los liderazgos sociales, así que la pérdida masiva de información genera un vacío considerable. Todas estas muestras físicas del trabajo realizado generan un incentivo en las personas para seguir en el trabajo social, generando aceptación por las buenas prácticas adoptadas y una reflexión de los elementos que han de ser más para corrección que para juzgamiento.

  En vista de la importancia de la identidad digital de los liderazgos sociales, se hace necesario que, dentro de la organización o colectivo, se asignen funciones para el almacenamiento y custodia de la información a una persona específica, quien será el guardián de la información documental y fotográfica relevante para los procesos de la organización o colectivo.

CAPITULO III

Rutas de servicios de protección por parte del Estado

Entendiendo los riesgos particulares que sufren las personas LGBTI y las históricas barreras para acceder a los servicios del Estado, existe la necesidad de integrar en el manual insumos que contribuyan al empoderamiento en conocimiento de rutas de protección, las cuales son indispensables en el planteamiento de estrategias de seguridad, autoprotección y mitigación de riesgos.

- **Rutas de denuncias o reportes en redes sociales.**

  En cuanto a las redes sociales, presentaremos rutas de denuncias o reportes de material fotográfico y comentarios en tres de las redes sociales más utilizadas para la divulgación de información: WhatsApp, Facebook e Instagram.

  - **Facebook:** La red social Facebook, con el fin de fomentar que las personas se expresen en un entorno seguro, ha establecido un manual denominado “Normas Comunitarias” con políticas basadas en el principio de la seguridad. Por ello, ofrece opciones como bloquear, dejar de seguir u ocultar personas y publicaciones, denunciar perfiles, fotos, videos, publicaciones, comentarios, anuncios, eventos y más.

    Para hacer uso de esto, debemos dar clic en la parte inferior derecha y seleccionar la opción “Denunciar”. Seguido a esto la administración de la plataforma estudiará el caso y procederá a eliminar cualquier contenido que transgreda las “Normas Comunitarias”.

  - **Instagram:** Esta red social por su parte permitirá denunciar cuentas, fotos y videos. Para esto tendremos dos opciones, lo cual dependerá de si tenemos o no cuenta activa en Instagram: 1) Si no tenemos cuenta activa debemos entrar a la opción “Servicio de Ayuda” y seleccionar la opción “Reporta infracciones a nuestras normas comunitarias”, para lo que debemos llenar un formulario muy sencillo y con preguntas

claras referentes a la denuncia. 2) Si contamos con cuenta activa, debemos dirigirnos a las opciones y seleccionar la opción “Reporta infracciones a nuestras normas comunitarias”.

Instagram también nos permitirá denunciar perfiles que suplanten nuestra identidad en la red. Debemos enviar el reporte a la administración a través de un formulario proporcionado en la cuenta en la cual debemos suministrar toda la información tendiente a validar que nuestra identidad es la real, esto se podrá hacer a través de la copia del documento de identidad.

- **WhatsApp:** SSi bien WhatsApp es un servicio de mensajería instantánea, no da opciones también ofrecidas en redes sociales como denunciar usuarios y grupos, a fin de ofrecer un entorno de comunicación seguro. Por ello a través de los reportes y de un estudio de caso ha permitido se bloqueen las cuentas de personas inescrupulosas que utilizan esta aplicación para el envío de spam (mensajes no deseados), realizar amenazas, estafas, extorsiones y cualquier otro tipo de conducta considerada como un delito.

  Para ello, al recibir un mensaje de un usuario desconocido, en la parte inferior de la pantalla, aparecerá una opción “Reportar Spam” que permitirá reportar y además bloquear al usuario o grupo en mención.

RECOMENDACIONES FINALES.

Protección de los equipos.	• Distinguir los equipos inmobiliarios organizacionales y personales. • Guardar con recelo la información confidencial de la organización. • No descargar actualizaciones de sitios de los cuales no tengamos certeza de su seguridad. • Permitir el acceso a los equipos de la organización o colectivo, solo a personas autorizadas. • Utilización de contraseñas seguras. • Realizar constante cambio de las contraseñas.
Seguridad y protección de los correos electrónicos	• No registrar correos electrónicos de carácter organizacional o por medio de los cuales se maneje información sensible, en páginas web de contenido pornográfico, citas en línea, chats, entre otros. • Establecer claves seguras a los correos electrónicos y que estas sean cambiadas con una periodicidad de 3 meses. • No suministrar información como claves de cuentas bancarias a través de correos electrónico. • Si se reciben correos electrónicos solicitando información confidencial, se recomienda ignorarlo. • Tener mucho cuidado en la información a publicar, procurando siempre que el impacto que esta produzca sea positivo. • No publicar información confidencial en estas redes, fotos de eventos de participación de víctimas o personas que consideren que su seguridad puede estar en riesgo, ni ubicaciones de lugares de homosocialización.

Seguridad y autoprotección en redes sociales	• No hacer pública la identidades e historias personales de personas LGBTI sin su consentimiento previo. • Delimitar las redes sociales organizacionales, de las redes sociales personales. • No publicar fotos o información de • en redes sociales carácter personal a través de estas redes organizaciones. • Evitar prácticas que podrían ser generadoras de riesgo como sexting o bullying por las redes de la organización o colectivo. • Guardar todo tipo de evidencia que dé cuenta de agresiones o situaciones de riesgo a través de redes sociales. **Redes personales** • Evitar publicar información muy personal, como ubicaciones, fotografías, que puedan dar lugar a un seguimiento. • Tener privacidad en las cuentas y así poder verificar quien ven nuestra información. • Establecer normas de convivencia digital en grupos y chats.
Seguridad en mensajería instantánea	• No compartir información confidencial y/o sensible a través de estos medios de comunicación, como mecanismo de autoprotección personal y colectiva.
Seguridad y protección del almacenamiento de datos	• Asignar funciones a una persona de la organización o colectivo, de la custodia y el almacenamiento interno y externo de la información importante para la organización tanto interna como externamente (USB o Disco Duro).

Notas

Notas