Manual para la protección y autoprotección de activistas LGBTI

en medios digitales

Caribe afirmativo

triángulo

AEXCID cooperación extremeña JUNTA DE EXTREMADURA

Manual para la protección y autoprotección de activistas LGBTI en medios digitales

Corporación Caribe Afirmativo

NIT. 900321082-6

Equipo de investigación
Lizeth Paola Charris Díaz
Franklin de Jesús Martínez

Director
Wilson de Jesús Castañeda Castro

Diseño
Mayling Chico Guzmán

Con el apoyo de:

Fundación Triángulo

Agencia Extremeña de Cooperación Internacional para el Desarrollo

www.caribeafirmativo.lgbt
Carrera 60 No. 58-70
Barranquilla, Colombia

2021

Caribe afirmativo

Este informe se realizó gracias al apoyo de Fundación Triángulo y la Agencia Extremeña de Cooperación Internacional para el Desarrollo.

Tabla de contenido

Introducción

Introducción

En escenarios de represión a la movilización social como los que actualmente se presentan en países como Colombia, Nicaragua y El Salvador, las personas que visibilizan sus orientaciones sexuales, identidades de género y expresiones de género (OSIGEG) diversas siguen siendo señaladas como inmorales, inferiores y transgresoras de la heteronormatividad. Por esto, las personas que se autoreconocen como LGBTI y ejercen activismo, defensa de derechos y liderazgo social se encuentran expuestas a situaciones de riesgo, rechazo e invisibilización asociadas a violencias por prejuicios.

Con el auge de nuevas tecnologías de la información, todos estos riesgos y violencias se han trasladado a los espacios virtuales, medios de comunicación y redes sociales. Generalmente, la visibilidad de las OSIGEG en los entornos digitales trae consigo situaciones que agudizan los riesgos y los prejuicios negativos en contra de las personas LGBTI. Adicionalmente, quienes realizan las amenazas y ataques muchas veces se aprovechan del anonimato de estos medios, afectando los procesos activistas LGBTI.

Tales actores violentos encuentran en los espacios virtuales un entorno en el que las normas sociales no son necesariamente obligatorias, donde las interacciones pueden darse sin ningún tipo de restricción en el uso de la información personal, y en los que la violencia hacia personas LGBTI puede ser impune. La defensa de los derechos de las personas, en escenarios de este tipo, es mucho más difícil, y se encuentra además mediada por el conocimiento de las tecnologías de la información y comunicación, muchas de las cuales aún no han sido reglamentadas ni reguladas por el Estado y por entes de control.

En este contexto, las personas LGBTI que hacen activismo a través de redes sociales pueden tomar en consideración herramientas de autoprotección, de modo tal que los riesgos inherentes a los medios digitales puedan ser disminuidos. El objetivo de este manual es luego brindar herramientas oportunas en materia de autoprotección que puedan ser usadas de forma efectiva. El uso de las herramientas de este manual permitirá que puedan seguir ejerciendo sus labores de defensa y promoción de derechos humanos de forma visible y segura.

Glosario de conceptos clave en diversidad sexual y género

Enfoque de género:

Es un enfoque diferencial que está orientado a observar, estudiar y transformar las diferencias culturales, económicas y políticas, en la construcción del reconocimiento, posicionamiento y visibilización de mujeres y personas LGBTI en agendas sociales, políticas estatales entre otras.

Expresiones de género:

Es la manifestación externa de distintas características culturalmente consideradas como masculinas o femeninas, es decir, no sólo se refiere al cómo me siento frente al género, sino a la manera en que expreso 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 no necesariamente "el parecer indica el ser..

Identidades de género:

Son construcciones sociales y culturales que establecen maneras de "ser hombre" o "ser mujer", a partir de las diferencias biológicas de los sexos. Esta mirada determinista deja por fuera formas singulares de subjetivar el género pues las identidades, incluyen un componente subjetivo vinculado al sentir y al ser. Por esto, el género con que las personas se identifican puede o no corresponder con el sexo-género jurídicamente asignado al nacer.

LGBTI:

La sigla LGBTI se refiere a una forma de nombrar a la colectividad comprendida por mujeres lesbianas, hombres gais, personas bisexuales, personas trans y personas intersexuales; y en ocasiones también se incluyen las identidades queer y otras formas de nombrarse en la diversidad sexual y de género. Sin embargo, estas no son las únicas maneras en que se puede nombrar la diversidad sexual y de género, ni todas las personas deben sentirse recogidas en dicha sigla.

Orientaciones sexuales:

Se entiende como la capacidad de cada persona de sentir una profunda atracción emocional, afectiva y sexual por personas de un sexo o género diferente al suyo (personas heterosexuales), o de un mismo sexo o género (personas homosexuales), o de más de un sexo o género (personas bisexuales), así como a la capacidad de tener relaciones íntimas y sexuales con estas personas. Al referirnos a personas homosexuales podemos hablar de hombres gais y mujeres lesbianas.

OSIGEG:

Es un acrónimo utilizado para referirse a la orientación sexual, identidad de género y expresiones de género.

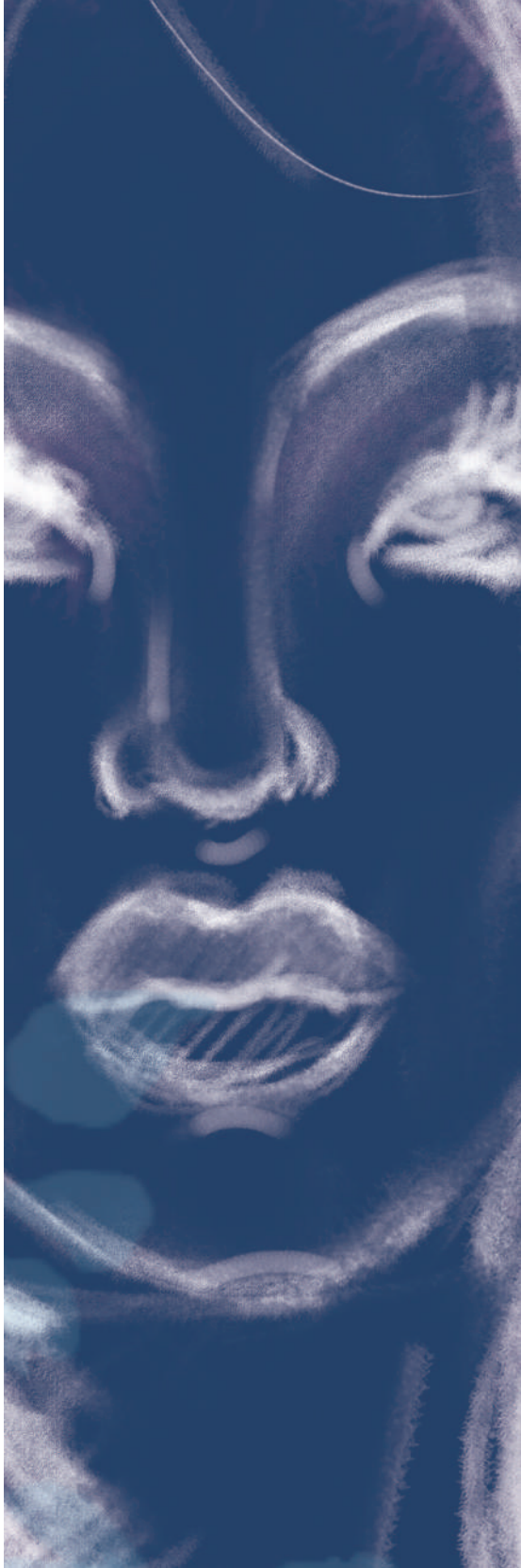
Perspectiva interseccional: La interseccionalidad es una perspectiva que 'mira' las diferentes realidades, vivencias que cruzan a una persona en razón del sexo, OSIGEG, pertenencia étnica o racial, la clase, entre otras, que dificultan el goce efectivo de derechos por los diversos sistemas de opresión que se ejerce sobre esta persona o grupo de personas.

Sexo:

Para entender el concepto de sexo, es necesario entender primero que no es un asunto netamente biológico, objetivo y binario (macho/hombre-hembra/mujer) como se ha difundido y enseñado de manera avasalladora en la cultura occidental. Así, debemos entender que tanto el sexo, como el género son construcciones sociales, pero cuya diferencia radica en que las primeras se hacen a partir de comportamientos y roles sociales (modo de vestir, hablar y comportarse) y las segundas a partir de características biológicas (genitalidad, identidad cromósomica, etc.). En este sentido, ambas forman parte del discurso que ha caracterizado y moldeado la manera en cómo entendemos el mundo desde una perspectiva sexo-género binaria.

Violencia por prejuicio:

Son aquellas conductas violentas motivadas en actitudes valorativas negativas respecto de la víctima, en razón de su pertenencia a un grupo poblacional determinado, que permiten racionalizarlas y justificarlas. Por ejemplo "cuando le cortan el cabello a una mujer trans porque son hombres queriendo imitar a las mujeres"; el padre de familia que al enterarse que su hijo es gay decide sacarlo de su hogar con el fin de que este desista de su orientación sexual.



Glosario de conceptos clave en temas de seguridad digital

Antivirus: Son programas diseñados para identificar, clasificar y eliminar virus informáticos (In Cuatro, 2019).

Ciberseguridad: Son herramientas que se utilizan para proteger la información que se produce o se efectúa en computadoras, dispositivos móviles, redes y sistemas electrónicos (Kaspersky, 2021).

Copia de seguridad: Es una copia de seguridad de uno o más archivos informáticos con el fin de prevenir perdidas a futuro de la información.

Encriptación: Se refiere al proceso matemático de hacer que un mensaje sea ilegible, a menos que se cuenta con una "llave" que permita desencriptar el mensaje. Actualmente, la encriptación es hecha por computadores, y usada correctamente, es inquebrantable (Electronic Frontier Foundation, 2018).

Extensión para navegador: Una extensión le agrega características y funciones a un navegador. Estas pueden complementar las funciones o información de los sitios web, agregar o remover contenido de sitios, agregar herramientas de trabajo a los navegadores, y las funciones que consideren necesarias (Mozilla Foundation, s.f.).

Firewall: Es un software o hardware diseñado con un conjunto de reglas para bloquear el acceso de usuarios no autorizados. Son excelentes líneas de defensa para evitar la interceptación de dato o bloquear virus.

Hardware: Es la parte tangible del computador, por ejemplo, la pantalla, el teclado, el mouse, CPU, entre otros.

IP: Es una dirección única que identifica a un dispositivo en internet o en una red local. Su sigla significa "protocolo de internet".

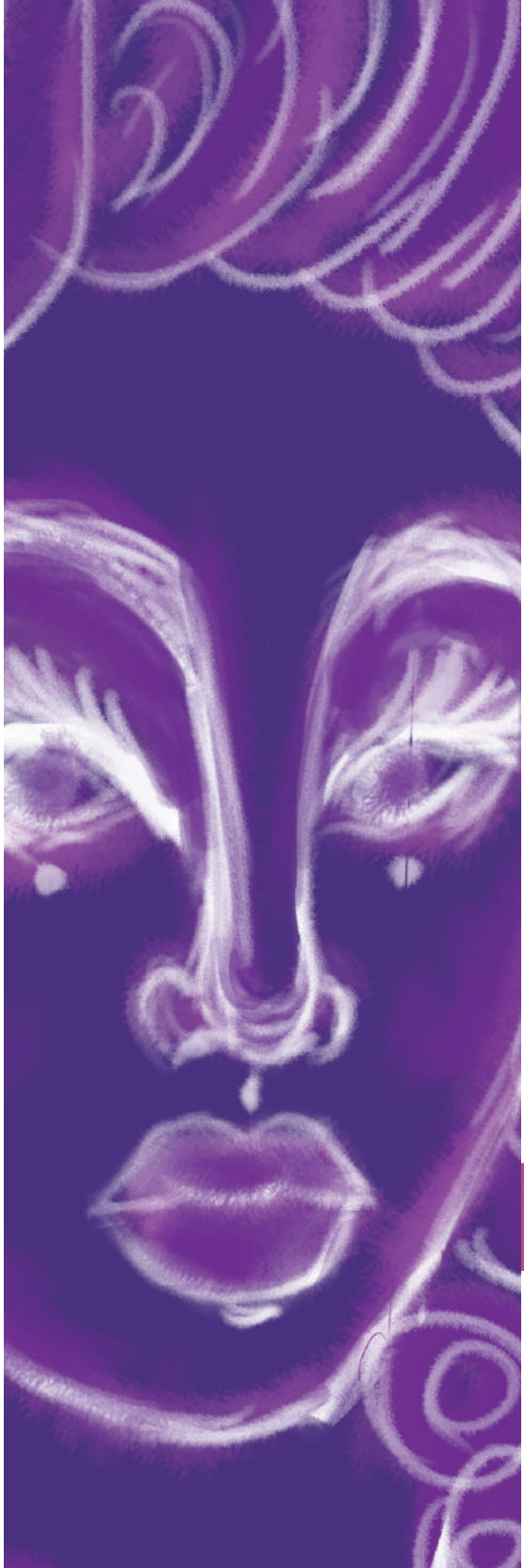
Plataformas digitales: Son espacios de internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades. Por ejemplo: Zoom, Meet, Teams, entre otras.

Signal: Es una aplicación de mensajería instantánea orientada a la seguridad y privacidad de la información (Pérez, E.2018).

Software: Es la parte intangible de la computación, lo cual incluye programas, aplicaciones, antivirus, información, entre otros.

Spammers: Individuos o empresas dedicadas al envío masivo de correos no deseados o también llamados spams.

SSL: Sigla de Secure Sockets Layer (capa de sockets seguros), un protocolo para navegadores y servidores web que permite autenticar, cifrar y descifrar la información enviada a través de Internet.



Sobre este manual

La seguridad digital en los procesos de activismo LGBTI es fundamental. Con el advenimiento del confinamiento como medida para controlar la pandemia por COVID-19, muchas personas se vieron obligadas a utilizar herramientas en Internet que les permitieran continuar con sus actividades laborales y de activismo. En muchos casos, las ventajas del trabajo a distancia se hicieron visibles. Sin embargo, particularmente para las personas LGBTI, esta situación no ha sido necesariamente buena. La violencia, discriminación, abuso sexual y exclusión, fueron situaciones comunes para las personas LGBTI (Caribe Afirmativo, 2021, pág. 10).

Esta misma situación se ha extrapolado a los ambientes digitales. La presencia en Internet, cada vez más ubicua, aumenta los lugares de riesgo para el activismo LGBTI. Discriminación, exclusión, amenazas y violencia han sido constantes en las vidas de personas LGBTI, cuyas expresiones de género visibles, su trabajo o su activismo, las han hecho blanco de violaciones a sus derechos.

La seguridad digital inicia con el reconocimiento del derecho a la privacidad en perspectiva de género y diversidad sexual, incluido como Principio 6 para la Privacidad de los Principios de Yogyakarta, en el año 2017. Según este, los Estados deben:

1. Asegurar que los requerimientos individuales de proveer información sobre sexo o género sean relevantes, razonables y necesarios en los casos que requiera la ley, cuando se deban a un propósito legítimo en las circunstancias en que se pida, y que tales requerimientos respeten el derecho de todas las personas a la autodeterminación de su género.
2. Asegurar que los cambios al nombre o al género, cuando este último exista, no sean difundidos sin la autorización previa, libre e informada de la persona concerniente, a menos que sea ordenado por una corte judicial (Yogyakarta Principles plus 10, 2017, pág. 18).

Este derecho a la privacidad, sin embargo, no es necesariamente protegido por los Estados. La pandemia por COVID-19 ha demostrado que existe un arreglo institucional que no protege la identidad de los individuos en sus ambientes digitales. La creación de aplicaciones para registrar los síntomas de personas con posible COVID-19, por ejemplo, y el acceso que estas aplicaciones tenían a los datos personales, ubicación, e información privada de salud de la persona, demuestran que, de parte de los Estados, la protección de la

información digital no es necesariamente una prioridad (Electronic Frontier Foundation). Por el contrario, tal información fluye de manera constante, en subastas, hacia grandes corporaciones digitales, quienes crean perfiles individuales que pueden llegar a predecir las preferencias, gustos, y compras futuras de esa persona (Orlowski, 2020).

Más aún, la situación de activistas y periodistas está en un momento preocupante. Las recientes revelaciones del software Pegasus, que hizo seguimiento a más de 50.000 personas periodistas, activistas, y defensoras de derechos humanos en todo el mundo, mostraron que son aquellas que trabajan en temas de garantía de derechos humanos y libertad de prensa quienes se ven más vulnerados en una era digital (Bassets, 2021). En el caso colombiano, las personas periodistas y comunicadoras son quienes más sufren violencia en sus entornos laborales y personales. El 73% de las periodistas y comunicadoras sufren violencia psicológica al ejercer su trabajo, y un 67% sufre también acoso sexual. De estas, el 11% de la violencia psicológica sufrida proviene de usuarios anónimos en internet (Fundación Karisma, 2021). No se cuenta además con legislación que aborde y controle estas dinámicas de violencia en espacios digitales, ni tampoco formas de denunciar tales situaciones de forma efectiva. El anonimato además permite que se den situaciones como ciberacoso, la publicación de mensajes denigrantes, la publicación de fotos con contenido íntimo sexual, la revelación de información personal como ubicación, contactos, el chantaje con imágenes de contenido sexual, amenazas de violencia física o muerte, entre otras (Fundación Karisma, 2017).

Por lo tanto, la autoprotección y la seguridad personales y en el trabajo son de vital importancia. Este manual presenta ideas clave para pensar en la seguridad digital, así como herramientas técnicas que pueden servir para guardar la seguridad propia en estos medios. Cada herramienta será acompañada de una explicación pedagógica, que permitirá hacer uso de estas herramientas sin necesariamente tener un conocimiento técnico específico sobre estas. Como se verá, muchas de las fuentes utilizadas están en inglés. Esto se debe a que gran parte del conocimiento disponible acerca de la seguridad digital se encuentra en países anglófonos, en donde las nuevas tecnologías han tomado más y más presencia en las vidas de las personas y en las actuaciones cotidianas del Estado.

De esta manera, es importante recalcar que este manual es un punto de partida a la seguridad digital. Las herramientas aquí presentadas son actualizadas constantemente, y existen nuevas y aún más avanzadas extensiones y programas. La seguridad digital es dinámica, y debe estar acompañada de una disposición para aprender. Sin embargo, y reconociendo que lo digital es a veces un campo lejano y quizá hostil para activistas, este manual está hecho pensando en que la persona que lo lea se sienta cercana y que pueda entender, en términos sencillos, por qué es importante instalar una u otra herramienta, hacer una copia de seguridad, o usar un administrador de contraseñas. Esperamos sea de utilidad, y que permita asegurar sus vidas, su trabajo y su activismo.

1. Herramientas básicas de la seguridad digital para activistas LGBTI

En esta sección, se presentarán diferentes escenarios, personales y laborales, así como casos y usos particulares de las tecnologías de la información, en los que se recomendarán herramientas, software, y principios para sostener la seguridad digital. Es importante recalcar que ninguna de estas herramientas garantizará, en un sentido absoluto, la total privacidad y seguridad de las comunicaciones de una persona activista. Sin embargo, sí creará condiciones para que la actividad sea más segura, dificultando en gran medida la capacidad de un actor criminal de acceder a información personal.

Cada una de las siguientes herramientas pueden ser usadas tanto en el ámbito personal como en el laboral. Sin embargo, también habrá una sección especial dedicada a la seguridad digital en el trabajo, ya que en este ámbito existe información potencialmente más sensible, y con repercusiones aún más graves, en caso de que esta sea accedida por actores no deseados o criminales.

1.1. Herramientas para realizar llamadas telefónicas o de video, individuales o grupales

1.1.1. Signal

Seguridad: Encriptada end-to-end, lo cual significa que solamente las personas en la llamada pueden escuchar o ver lo que se esté comunicando. Puede bloquearse con una contraseña, para evitar que terceros puedan entrar en la aplicación.

Características: Llamadas de voz, videollamadas, envío de archivos, chat y llamadas grupales. Las conversaciones sensibles pueden eliminarse de la aplicación. Permite la autodestrucción de mensajes después de un tiempo determinado.

¿Qué se puede compartir?: Información personal o laboral sensible.

Pros y contras: No es muy común que los contactos usen esta aplicación. Sin embargo, es la aplicación de mensajería más segura hasta el momento.

1.1.2. WhatsApp

Seguridad: Encriptada end-to-end, lo cual significa que solamente las personas en la llamada pueden escuchar o ver lo que se esté comunicando. Puede bloquearse con una contraseña, para evitar que terceros puedan entrar en la aplicación.

Características: Llamadas de voz, videollamadas, envío de archivos, chat y llamadas grupales. Las conversaciones sensibles pueden eliminarse de la aplicación.

¿Qué se puede compartir?: Información en general no sensible.

Pros y contras: Es muy usada. Sin embargo, la empresa está bajo el ala de Facebook, lo cual implica un riesgo de seguridad ya que esta compañía utiliza la información personal para brindar anuncios personalizados en la Web.

1.1.3. Wire

Seguridad: Encriptada end-to-end, lo cual significa que solamente las personas en la llamada pueden escuchar o ver lo que se esté comunicando. Puede bloquearse con una contraseña o PIN numérico, para evitar que terceros puedan entrar en la aplicación.

Características: Llamadas de voz, videollamadas, envío de archivos, chat y llamadas grupales. Las conversaciones sensibles pueden eliminarse de la aplicación. También pueden crearse mensajes que se autodestruyan después que el recipiente haya leído el mensaje.

¿Qué se puede compartir?: Información personal o laboral sensible.

Esta sección fue creada con insumos de organizaciones sin ánimo de lucro que trabajan por la seguridad digital de activistas y periodistas (ILGA-Europe, 2020; Electronic Frontier Foundation; Kelly, 2020).

a) Establecer siempre una contraseña para la reunión.

b) No compartir el enlace en redes sociales, ya que así cualquier persona puede unirse.

c) Compartir el enlace solamente por chats privados y seguros.

d) Solicitar que cada persona en la reunión se presente antes de iniciar la reunión, preferiblemente con su cámara encendida.

e) Si hay participantes sospechosos, que no responden a las preguntas o que comparten contenido no solicitado, es recomendable cerrar la reunión y generar un nuevo enlace. En algunas aplicaciones, es posible bloquear aquellos participantes que no se acojan a las normas establecidas.

1.1.4. Jitsi

Seguridad: Genera un enlace único para la reunión, y se puede proteger la entrada al espacio con una contraseña.

Características: Llamadas de voz, videollamadas, envío de archivos, chat, y compartir pantalla. Puede usarse tanto en equipos de mesa, portátiles, y teléfonos móviles.

¿Qué se puede compartir?: Información general , tanto no sensible como sensible.

Pros y contras: No es muy conocida, lo cual es una ventaja para la seguridad. Sin embargo, algunas veces se presentan problemas de conectividad.

1.1.5. **Microsoft Teams Seguridad:** Encriptada end-to-end, lo cual significa que solamente las personas en la llamada pueden escuchar o ver lo que se esté comunicando. Se puede establecer una contraseña para la reunión.

Características: Llamadas de voz, videollamadas, envío de archivos, chat, y compartir pantalla. Puede usarse tanto en equipos de mesa, portátiles, y teléfonos móviles.

¿Qué se puede compartir?: Información general no sensible.

Pros y contras: Es muy conocida. Es manejada por Microsoft, lo cual genera consideraciones de seguridad debido al modelo de negocio de esta empresa.

1.2. Herramientas para la navegación segura en internet

Estas herramientas permiten mantener un nivel básico de seguridad al navegar la Web. Todas las herramientas son gratis, y son desarrolladas por organizaciones reconocidas internacionalmente por su compromiso con la privacidad y la seguridad.

1.2.1. Privacy Badger

Es una extensión para navegador (Google Chrome, Mozilla Firefox, Microsoft Edge) que permite bloquear enlaces y sitios web que rastrean la actividad individual en cada uno de los sitios en internet. Cuando la extensión detecta que un sitio ha rastreado a la persona 3 veces en 3 sitios web diferentes, el sitio web es bloqueado. La aplicación funciona automáticamente, y es desarrollada por la Electronic Frontier Foundation (EFF), una organización sin ánimo de lucro con amplia trayectoria internacional.

1.2.2. HTTPS Everywhere

Es una extensión para navegador (Google Chrome, Mozilla Firefox, Microsoft Edge) que automáticamente utiliza protocolos seguros de navegación, encriptados end-to-end, de forma tal que la información vista por la persona usuaria no sea vista por terceros. Es desarrollada por la Electronic Frontier Foundation (EFF), una organización sin ánimo de lucro con amplia trayectoria internacional.

Existen más opciones para realizar videollamadas en grupo. Sin embargo, solo han sido publicadas aquellas con un nivel mediano de seguridad, con soporte a largo plazo, y con disponibilidad en diferentes plataformas, tanto en computadores como en teléfonos móviles.

1.2.3. VPN

Una VPN (Virtual Private Network, por sus siglas en inglés) es una red privada (un software) que permite una conexión segura y privada a Internet. Generalmente, las conexiones no son privadas: estas pueden ser monitoreadas por los proveedores de Internet, e interceptadas por actores maliciosos, criminales, o Estatales. Una VPN permite que la conexión sea totalmente privada, de forma tal que incluso si un actor lograra interceptar las comunicaciones, lo único que este podría ver serían caracteres aleatorios encriptados, sin ningún sentido. Las VPN son comúnmente usadas en los lugares de trabajo, aunque también son recomendadas en el ámbito personal.

Las VPN cuestan generalmente un valor mensual. Aunque existen VPN gratis, es recomendable utilizar una VPN con un costo, así sea mínimo. Esto garantiza que el modelo de negocio de la empresa desarrolladora de la VPN sean las suscripciones, y no la venta de los datos de navegación de sus usuarios.

Actualmente, una VPN segura, utilizada en múltiples ambientes y recomendada por expertos en seguridad digital, es Mullvad VPN. Es desarrollada por una empresa basada en Suecia, donde las leyes para la privacidad son muy estrictas. La empresa no mantiene documentos que prueben el uso o no de su software, y el pago puede ser realizado de múltiples maneras, incluso en efectivo (Gilbertson, 2021; Grauer, 2021).

1.3. Administradores de contraseñas

Las contraseñas son ubicuas a las actividades en internet. Debido a la gran cantidad de sitios web que requieren una contraseña, es importante tener un lugar seguro donde guardar todas las contraseñas. Si bien es una práctica común, es importante que NO se utilice la misma contraseña para diferentes sitios en internet. Esto es clave ya que, en caso tal una de las cuentas sea accedida de forma maliciosa por algún actor, este no pueda acceder al resto de cuentas pertenecientes a la persona afectada. Para este mismo fin, las contraseñas también deben ser actualizadas constantemente.

Es aquí donde entran los administradores de contraseñas. Son programas (tanto para computadores como para teléfonos móviles) que permiten almacenar todas las contraseñas, correos electrónicos, y sitios web donde se utilicen cada una de estas. Permiten además que estas se autocompleten en los sitios web utilizados.

1.3.1. Bitwarden

Es un administrador de contraseñas seguro, con aplicaciones para iPhone, Android, así como computadores de escritorio y portátiles. Este programa permite la creación de una contraseña maestra, con la cual se pueden acceder al resto de contraseñas y cuentas. Permite organizar las contraseñas en carpetas, así como almacenar PINs numéricos y demás.

La aplicación también permite generar contraseñas seguras, de modo tal que cada contraseña en cada sitio web visitado sea única.

1.3.2. 1Password

Es un administrador de contraseñas seguro, con aplicaciones para iPhone, Android, y computadores de escritorio y portátiles. Permite el almacenamiento seguro de contraseñas, necesitando solamente tener una contraseña maestra para acceder. El programa es gratis, aunque funciones adicionales de seguridad pueden ser accedidas a través del pago de una suscripción mensual.

2. Principios básicos de la seguridad digital

Además de las herramientas descritas, es importante tener unos principios básicos a seguir a la hora de trabajar y hacer activismo en internet.

2.1. Recomendaciones generales

1. Diferenciar y utilizar los equipos personales de los del trabajo. Esto permite que la información esté dividida y disminuir los riesgos de seguridad en lo personal y en el trabajo.
2. No guardar información del trabajo en dispositivos personales, y viceversa.
3. Usar un administrador de contraseñas.
4. Generar contraseñas con combinaciones de mayúscula, símbolos y números.
5. Realizar cambios de las contraseñas regularmente.
6. A la hora de tener enlaces o URL desconocidos, revisar la dirección web del sitio, de forma tal que al inicio de esta esté escrito: "https". Es importante la "s" al final, dado que indica que la conexión es segura. Si esta no lo tiene, deben abandonar o cerrar de forma inmediata el lugar, ya que sus datos personales o información confidencial que esta almacenada en el equipo no están seguros.

2.2. Recomendaciones en el ámbito laboral de organizaciones de la sociedad civil

1. Generar políticas de back-up para evitar pérdida de información. Es recomendable que se implementen políticas de cifrado en los equipos, servidores y herramientas transaccionales con el fin de mantener la protección de la información.
2. No utilizar las redes sociales de la organización para uso personal.
3. No utilizar redes wifi de uso público para compartir información de la organización o colectivo.
4. No descargar información confidencial en aparatos electrónicos de uso público.
5. Se recomienda restringir 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.
6. No dar información a beneficiarios, instituciones o personas no vinculadas a la organización de procesos jurídicos, de investigación, o comunitarios.
7. Evitar tener conversaciones por teléfono en lugares públicos sobre temas relacionados a los procesos ejecutados por la organización o colectivo.
8. No acceder a cuentas de correo, redes sociales, o personales, en equipos del trabajo, a menos que sean vitales para la realización de este.
9. No registrar los correos laborales en sitios web para uso personal.
10. Eliminar los correos desconocidos que contengan mensajes con enlaces o archivos adjuntos. Generalmente, son inseguros.
11. Evitar compartir la cuenta y la clave del correo institucional con personas ajenas la organización o colectivo.

2.3. Recomendaciones en el ámbito personal

1. Preferiblemente escoger smartphones que reciban actualizaciones constantes de su sistema operativo.
2. Actualizar las aplicaciones del celular regularmente.
3. Escoger proveedores de telefonía que respeten los derechos de sus usuarios.
4. Abstenerse de compartir la ubicación de su vivienda.
5. 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.
6. 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 marcarlo como spam en su servicio de correo.

2.4. Recomendaciones en el uso de redes sociales

Las redes sociales más populares actualmente tienen un modelo de negocio basado en la venta y subasta de la información personal de sus usuarios, de modo tal que pueda ser utilizada para brindar anuncios (Orlowski, 2020). En este sentido, cualquier tipo de comunicación en una red social es, intrínsecamente, insegura, ya que no es información observada y utilizada únicamente por quienes se comunican, sino también por la empresa bajo la cual opera la red social.

Sin embargo, dado lo generalizadas que están, es importante tener unas reglas básicas de uso de estas redes sociales.

2.4.1. Recomendaciones de no publicación

Se recomienda no publicar:

1. Fotografías donde se evidencien números telefónicos, números de identificación, direcciones de viviendas, números de cuentas bancarias, tiquetes aéreos, certificados o diplomas.
2. Fotos de eventos en los que se vean los rostros de asistentes sin tener diligenciado un consentimiento informado en el que estos den la autorización para publicar las imágenes.
3. Información de casos o datos sensibles que agudicen el nivel de riesgo de las personas involucradas.
4. Exámenes médicos en los que se indique información confidencial del estado de salud o patología de las personas.
5. Fotografías donde se evidencie la ubicación de lugares que son zonas de homosocialización o en los que se encuentren reunidas personas con medidas de protección.
6. Información sobre actividades de activismo y su ubicación de manera simultánea que pueda poner en riesgo a las personas presentes.

2.4.2. Recomendaciones de manejo de las redes sociales en el ámbito laboral

Se recomienda:

1. Utilizar las redes sociales de las organizaciones exclusivamente para subir o publicar contenido que se relacione con los objetivos, actividades y acciones desarrolladas por esta.
2. No se debe publicar información personal de ninguna persona que sea beneficiaria o haga parte de la organización.
3. Abstenerse de publicar opiniones personales.

2.4.3. Recomendaciones de uso de las redes sociales en el ámbito personal

Se recomienda:

1. No publicar ubicaciones o fotografías que revelen lugares de vivienda.
2. No utilizar redes WiFi de uso público para compartir información de la organización.
3. No aceptar solicitudes de conexión de personas desconocidas.
4. No dar información personal como contraseñas a través del chat privado de la red social.
5. No utilizar computadores públicos para iniciar sesión o administrar las redes sociales personales.
6. No ingresar a enlaces de origen desconocido.

La Fundación Karisma, en Colombia, publica anualmente un informe donde se analizan las políticas de datos de los diferentes proveedores de telefonía e internet en Colombia (Fundación Karisma, 2020).

2.5. Recomendaciones de uso de aplicaciones de mensajería y video grupal

Se recomienda:

1. Establecer normas de convivencia digital en grupos de chat, tanto de la organización como personales.
2. No enviar material sensible a través de chats grupales.
3. Establecer contraseñas o salas de espera en cada una de las reuniones grupales.

2.6. Recomendaciones en el almacenamiento de datos

Se recomienda:

1. Clasificar la información sensible y almacenarla en lugares seguros, privados, preferiblemente con contraseña.
2. Realizar copias de seguridad en dispositivos diferentes al lugar inicial donde está almacenada la información. Esto evitará que, en caso tal se pierda la información en el dispositivo inicial, esta pueda ser recuperada.
3. Instalar un firewall y una VPN que protejan el flujo de información o datos compartidos desde los equipos de trabajo.
4. Se debe asignar a una persona específica para el almacenamiento y custodia de la información. Esta persona guardará la información documental y fotográfica relevante para los procesos de la organización o colectivo.
5. Crear un sitio de almacenamiento de la información en la nube, de modo tal que si la copia de seguridad falla, los archivos también puedan ser recuperados.

3. ¿Qué hacer en situaciones de riesgo?

Aún con todas las medidas de seguridad tomadas, es posible que se presenten situaciones de seguridad que afecten el trabajo y activismo de las personas LGBTI. En este sentido, es clave utilizar medios de denuncia y documentación, tanto en las plataformas que se utilicen, como internamente en la organización. En esta sección, se recomendarán rutas particulares de actuación en casos de amenazas, hostigamientos y persecuciones, casos de acoso sexual, y casos de seguimiento policial.

La Fundación Karisma, en Colombia, publica anualmente un informe donde se analizan las políticas de datos de los diferentes proveedores de telefonía e internet en Colombia (Fundación Karisma, 2020).

3.1. Amenazas

La persona afectada informará de las amenazas a la persona representante legal de la organización, con toda la información disponible relativa a:

- Medio digital donde se dio la situación.
- Contenido explicito (expresiones utilizadas, móviles manifestados, autor expresado, daño que se ocasionará).
- Descripción de las circunstancias de tiempo y lugar, y del contexto que corresponde con los hechos.
- Identificación de presunto autor o grupo armado.
- Presencia o mención de otras personas en la amenaza.
- Medios de pruebas disponibles.
- Si se puede descargar la publicación o amenaza en forma de foto o video, es recomendable hacerlo. Estas pueden contener información valiosa, como el tipo de dispositivo en que se creó, qué día, a qué hora, e incluso la ubicación y nombre de usuario de la persona que hizo esa imagen o video. Esta puede encontrarse en las "Propiedades" del archivo.

3.2. Hostigamientos y persecuciones contra integrantes de la organización

La persona afectada informará de las amenazas a la persona encargada de seguridad en la organización, con toda la información disponible relativa a:

- El medio digital en que se presentó la situación.
- Identificación del agresor.
- Periodicidad y sistematicidad del hostigamiento o persecución.
- Descripción de las circunstancias de modo, tiempo y lugar, y del contexto que corresponde con los hechos.
- Identificación de posibles causas.
- Medios de pruebas disponibles.

3.3. Casos de acoso sexual

En este caso, se recomienda:

- Tomar pruebas (pantallazos, copias de chats, fotos, audios) de la situación de acoso sexual.
- Redirigir la denuncia hacia la persona encargada de asuntos de seguridad y género en la organización.
- En caso de que no haya una persona encargada, hacer la denuncia a la persona representante legal de la organización.

3.4. Casos de seguimiento policial

Estos casos son particularmente difíciles de probar. Sin embargo, si el teléfono celular o computador tiene algún tipo de actividad extraña, como:

1. El mouse se mueve solo.
2. La conexión a internet está más lenta de lo normal.
3. Hay aplicaciones en el computador que no recuerda haber instalado.
4. Cualquier otra acción que se considere extraña por la persona usuaria.

Es importante reportar el caso ante la persona encargada de seguridad en la organización, o a la persona representante legal de esta. En estos casos es importante el apoyo de personal técnico, que pueda brindar asesoría frente a qué acciones tomar, desde el restablecimiento de valores de fábrica del dispositivo, hasta el cambio total de este. Fundaciones en Colombia como Karisma brindan este tipo de apoyo.

3.5. Rutas de denuncias o reportes en redes sociales

Además de las rutas anteriormente mencionadas, es importante denunciar el contenido amenazante ante las empresas que manejan las redes sociales. Generalmente, se cuenta con un formulario y una ruta a través de la cual se pueden hacer tales denuncias, además de la posibilidad de bloquear o silenciar a aquellos individuos que estén compartiendo contenido hostil o amenazante hacia la organización o persona. A continuación, se describen las rutas de denuncia y bloqueo en algunas de las redes sociales más populares.

Es importante tener en cuenta que existe siempre la posibilidad de bloquear o silenciar a cualquier persona que esté siendo amenazante en contra de su bienestar personal. Esto no solamente es correcto, sino que además permite dar bienestar mental a las personas amenazadas.

3.5.1. WhatsApp

En sus políticas de condiciones de servicio contempla la suspensión de las cuentas de usuarios cuando detecta que se realizan actividades prohibidas al compartir contenido ilegal, obsceno, difamatorio, con muestras de odio entre otro. Así mismo, WhatsApp posibilita opciones tales como denunciar usuarios y grupos, a fin de ofrecer un entorno de comunicación seguro. De conformidad a las políticas de uso de esta red social, es necesario tener en cuenta las siguientes recomendaciones en materia de privacidad de los datos:

1. Esta red tiene una función útil de ubicación, la cual puedes compartir en tiempo real a través de un mensaje. A pesar de ser una opción muy funcional, se recomienda que al usarla se haga con una persona de confianza.
2. Cambia los ajustes de privacidad para controlar quién ve tu información sobre la hora, foto de perfil o el estado. Se puede elegir entre:
   - Todos: Todos los usuarios pueden ver esta información en el WhatsApp.
   - Mis contactos: Solo los contactos registrados en la libreta de tu teléfono podrán ver tu información.
   - Nadie: Nadie podrá ver tu información.

En materia de seguridad, esta red social provee acciones como bloquear o reportar contactos y mensajes si se recibe o se logra ver contenido o contactos conflictivos. Al bloquear a una persona en específico, el número aparecerá en las secciones de "Bloqueados", en dispositivos iPhone, o "Contactos bloqueados", en dispositivos Android. En los casos en que se reciba un mensaje no deseado, o de un usuario desconocido, el mensaje debe mostrar una opción de "Reportar spam", lo cual permitirá reportar y bloquear al usuario o grupo en mención.

3.5.2. Facebook

La política de uso de esta red social ha establecido una herramienta llamada "Normas comunitarias", por medio del cual las personas usuarias pueden bloquear, dejar de seguir u ocultar personas y publicaciones, denunciar perfiles, fotos, videos, publicaciones, comentarios, anuncios, eventos y más.

Para hacer uso de esto, se debe dar clic en la parte inferior derecha 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". Si se busca indicar que algo infringe las normas comunitarias (por ejemplo, desnudos, lenguaje que incita al odio, violencia, etc.), se puede utilizar el enlace 'Reportar' situado junto a la publicación, la foto o el comentario en cuestión.

3.5.3. Instagram

En esta red se pueden denunciar cuentas, fotos, y videos. Para esto existen, al momento de escritura, dos opciones, las cuales dependerán de si se cuenta o no con cuenta activa en Instagram:

1. Si no se tiene acceso a una cuenta activa, se puede entrar a la opción "Servicio de Ayuda" y seleccionar la opción "Reporta infracciones a nuestras normas comunitarias". Debe luego llenarse un formato con preguntas acerca de la denuncia.
2. Si hay acceso a una cuenta activa, en las "Opciones" de la aplicación se selecciona "Reporta infracciones a nuestras normas comunitarias". Las opciones de privacidad y seguridad están ubicadas en el perfil presionando las tres rayas horizontales, en la parte superior derecha de nuestra pantalla, y luego presionando en la ruedita de "Configuración" en la parte inferior la derecha. Allí encontrarás el menú con todas las opciones que Instagram nos permite configurar.

3.5.4. TikTok

Con el fin de garantizar un espacio de interacción seguro, esta red social ha establecido unas "Normas de la Comunidad" las cuales definen una serie de indicaciones y códigos de conducta, que describen lo que está permitido y lo que no lo está. En cuanto a las herramientas proporcionadas por esta red social para denunciar, esta aplica para elementos como videos, usuarios, mensajes, comentarios y videos en vivo. Para llevar a cabo la denuncia se pulsa en el comentario, usuario, video en vivo, video y/o mensaje que esté ocasionando el conflicto, se selecciona la opción denuncia y a partir de ahí se siguen los pasos descritos.

3.5.5. Twitter

Ante la presencia de comportamientos abusivos, que vayan en contra de las normas de convivencia de la red social, esta da la opción de denunciar. Para realizar una denuncia se pueden seguir los siguientes pasos.

Para denunciar un tweet:

1. Dirigirse al tweet a denunciar en twitter.com o en la aplicación de Twitter.
2. Seleccionar denunciar y marca la opción "es abusivo o perjudicial".
3. Proporcionar información describiendo la norma que se infringe a través del tweet o tweets.

Al denunciar una cuenta:

1. Ir al perfil de la cuenta y hacer clic en el icono de contenido adicional.
2. Seleccionar "Denunciar" y marcar la opción "Es abusivo o perjudicial".
3. Proporcionar información describiendo la norma que se infringe a través del tweet o tweets.
4. Posterior a la denuncia, Twitter enviará un correo de seguimiento a la denuncia, explicando los correctivos que se tomaron (o no) frente a esta.

Conclusiones

Aunque las tecnologías de la información tienen ya varios años de trayectoria, aún no existen métodos efectivos de control, regulación y denuncia de las personas y organizaciones que interactúan en estas. Es por esto que las medidas de autoprotección de las organizaciones de la sociedad civil y de personas LGBTI activistas son tan importantes, ya que son un primer filtro de seguridad en un mundo que es aún hostil, discriminatorio y violento frente a personas disidentes de la heteronormatividad.

Como última recomendación de esta guía, es importante que se creen lazos de confianza en las redes sociales. Esto quiere decir que sea cual sea la red social que se use, es importante que la persona sepa de dónde proviene el contenido que ve, y con qué persona está hablando, de modo tal que se disminuya la posibilidad de recibir virus, amenazas, u hostigamientos.

Referencias

Bassets, M. (19 de Julio de 2021). Una filtración revela el espionaje de Gobiernos a periodistas y opositores con el programa Pegasus. El País.

Caribe Afirmativo. (2021). Herramientas de incidencia internacional para defensoras y defensores de derechos humanos de personas LGBTI en el marco de la crisis generada por la pandemia COVID-19.

Electronic Frontier Foundation. (s.f.). Electronic Frontier Foundation. Obtenido de COVID-19 and Digital Rights: https://www.eff.org/issues/covid-19

Electronic Frontier Foundation. (s.f.). Surveillance Self-Defense | Tips, Tools and How-Tos for safer online communications. Recuperado el 19 de Agosto de 2021, de Electronic Frontier Foundation: https://ssd.eff.org/en

Fundación Karisma. (2 de Noviembre de 2017). Asunto: Presentación sobre la violencia en línea contra las mujeres en Colombia. Bogotá. Obtenido de https://web.karisma.org.co/wp-content/uploads/download-manager-files/Violencia%20digital%20contra%20la%20mujer%20-%20Colombia.pdf

Fundación Karisma. (2020). ¿Dónde están mis datos? 2020. Obtenido de https://web.karisma.org.co/donde-estan-mis-datos-2020/

Fundación Karisma. (5 de Agosto de 2021). Violencias machistas atacan la libertad de expresión de periodistas y comunicadoras en Colombia. Obtenido de Fundación Karisma: https://web.karisma.org.co/violencias-machistas-atacan-la-libertad-de-expresion-de-periodistas-y-comunicadoras-en-colombia/

Gilbertson, S. (30 de 01 de 2021). The Best VPNs to Protect Yourself. Obtenido de WIRED: https://www.wired.com/story/best-vpn/

Grauer, Y. (18 de Mayo de 2021). The Best VPN Service. Obtenido de Wirecutter: https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

ILGA-Europe. (1 de Abril de 2020). COVID-19 and digital security: How LGBTI activists can safely work online. Obtenido de ILGA-Europe: https://www.ilga-europe.org/blog/covid-19-and-digital-security-how-lgbti-activists-can-safely-work-online

Kelly, M. (11 de Septiembre de 2020). The age of activism: Protect your digital security and know your rights. Obtenido de Blog | Mozilla Firefox: https://blog.mozilla.org/en/internet-culture/deep-dives/activism-digital-security/

Orlowski, J. (Dirección). (2020). The Social Dilemma [Película]. Netflix.

(2017). Yogyakarta Principles plus 10.

Manual para la protección y autoprotección de activista LGBTI en medios digitales