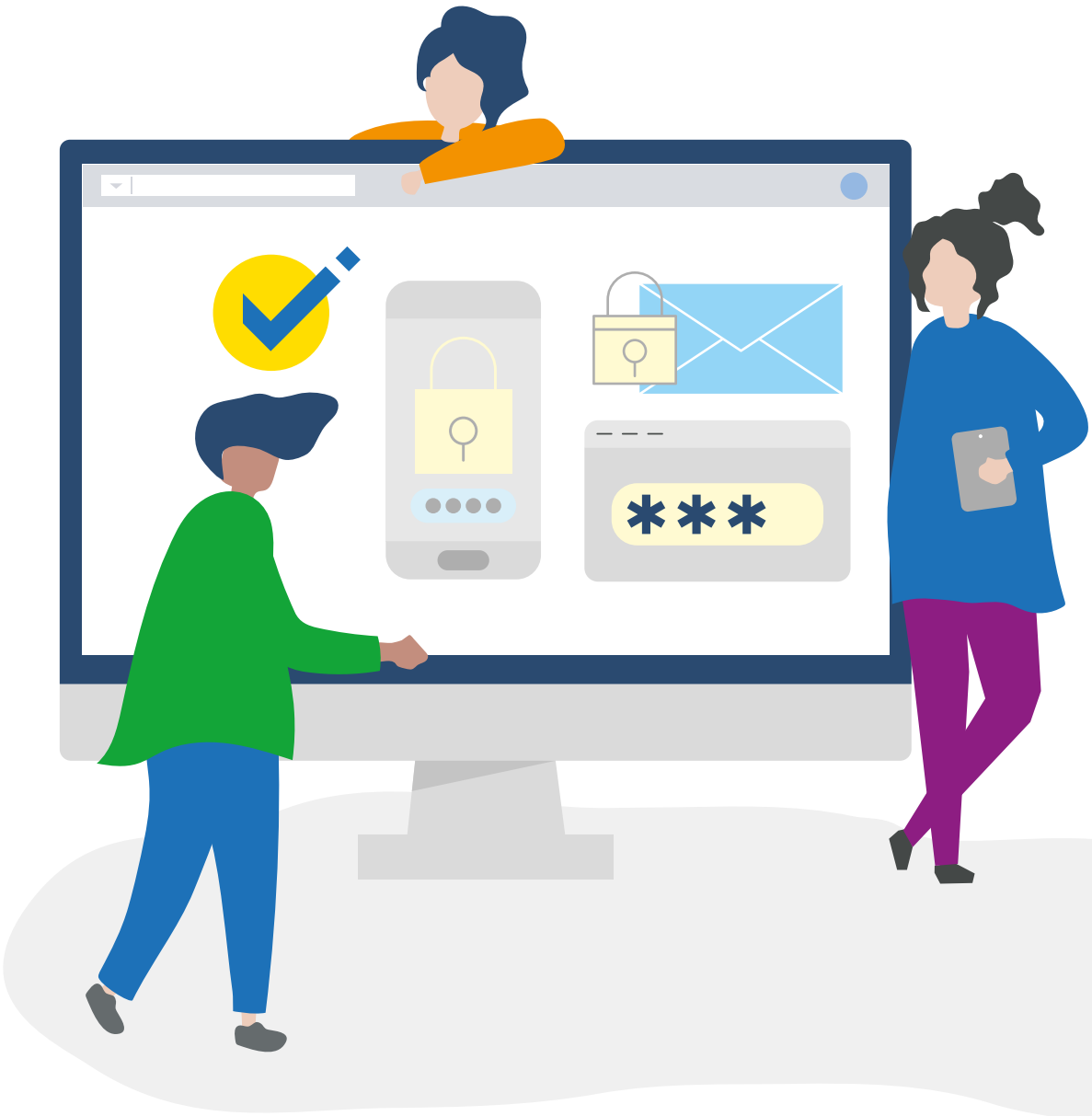
Guía de ciberseguridad para organizaciones LGBTI



Guía de ciberseguridad para organizaciones LGBTI.

Av. José Pardo 601, oficina 603-604, Miraflores, Lima, Perú.
Teléfono: (51) (1) 447 8668 / Fax: (51) (1) 243 0460.
www.promsex.org
f/promsex
t/promsex
ig/promsexcomunica

Autor: Roberto Bustamante Vento.
Cuidado de edición: David Arguedas Olave, Sara Ramirez Zubillaga, Aarón Puescas Argote.
Corrección de estilo: Regina Contreras Limo.
Diseño y diagramación: Yuriko Tanaka Rimarachin.
Coordinación comunicacional: Jorge Apolaya Quintanilla.
Supervisión de diseño: Yazmin Trujillo Raa.
Ilustraciones Vectoriales: Freepik.com

Editado por: Promsex
Av. José Pardo 601 oficina 604, Miraflores
Lima – Perú
1a. edición – mayo 2019

Índice

Introducción

Esta es una guía de ciberseguridad para organizaciones que defienden los derechos de las personas LGBTI. Es, al mismo tiempo, una guía de ciberseguridad para personas LGBTI. No es exactamente un manual, aunque daremos indicaciones de qué hacer en distintos tipos de escenarios de ataques cibernéticos (o ciberataques, como ven, a todo le anteponemos el cíber) o cómo hacer para prevenirlos.

¿Por qué pensamos que una guía sobre ciberseguridad es especialmente importante para las personas LGBTI? En general, todos y todas deberíamos tener nociones básicas sobre la seguridad de nuestra información y sobre el cuidado de nuestros datos. Todos y todas deberíamos saber qué hacen las corporaciones como Facebook con toda nuestra información, con nuestras fotos, con nuestros "me gusta" y con nuestros "compartidos".

Sin embargo, vemos con preocupación un crecimiento de sectores conservadores que usan los medios digitales como instrumentos de hostigamiento, acoso y violencia contra aquellos y aquellas que defienden los derechos sexuales y reproductivos. Sectores conservadores, vinculados a grupos y organizaciones de ultraderecha, que están no pocas veces coludidos con personas que saben usar bastante bien los medios digitales para exponer, hostigar, violentar a personas LGBTI. Esta violencia puede ir desde la verbal hasta la física, exponiendo datos privados que pueden derivar en un ataque al cuerpo de estas personas.

El mundo de internet es tan inseguro como el mundo de a pie. Y este mundo de internet está atravesado también por variables y vectores de saber y poder. Seguramente leerán a varios expertos que dicen que las tecnologías son como martillos sin mano, objetos neutrales que no son ni buenos ni malos, que todo depende de quien las empuñe.

Nada más lejos de la realidad. Tanto el internet como esto que comúnmente se llama "redes sociales", son tecnologías o, mejor dicho, herramientas que fueron hechas por personas, personas que tienen sus propios sesgos e intereses como todos nosotros. Por muy buena que haya sido la intención, incluso abriendo o barajando tal posibilidad, el caso es que no es posible que deje de estar afectada por los prejuicios o desconocimientos de sus creadores. Así, Facebook, una de las "redes sociales" (el

término técnico es "medio social") más populares hoy en día, no es solamente una herramienta para la comunicación entre contactos; es también un espacio donde quienes participan están en constante competencia por figuración, reconocimiento y publicidad, a través de "premios" y valoración colectiva. En otras palabras, lo que escribimos está hecho para que "juguemos" a ver quién colecciona más likes, más "rebotes" (compartidos), etc., lo cual es un caldo de cultivo terrible para quienes buscan notoriedad a través de la difusión de mensajes de odio.[1]

De esa forma, las herramientas de comunicación como Twitter, Facebook, Instagram, y Youtube incentivan a que publiquemos constantemente, ya que su modelo de negocio se basa en la capacidad "innata" por escribir y compartir nuestras ideas, fotos, datos de gustos culturales, etc., porque toda esa información puede luego ser combinada y condensada en reportes que a su vez pueden servir para acercar a distintas empresas a ofrecernos sus productos. Es lo que varios autores han denominado Capitalismo de Plataformas [2]. Su papel es de intermediario, ofreciendo lo que los usuarios de estas plataformas producen o crean a cualquier empresa que pague por esa información condensada. Si el principio del capitalismo es el de la acumulación de capital a través de la apropiación del plusvalor, todos nosotros sin pedir casi nada a cambio le damos nuestro plusvalor (los contenidos que creamos, la información que compartimos) a estas empresas como Facebook o Google, por ejemplo, para que a su vez ellas las puedan revender a otras empresas menores [3].

No todo es tan malo, sin embargo. Es a través de estos mismos medios sociales que distintas organizaciones han podido dar a conocer sus trabajos, sus aspiraciones, sus expectativas. Ha permitido que estas mismas organizaciones lleguen a personas que buscan información, contacto, ayuda de todo tipo (por ejemplo, ayuda legal). A través de estos medios sociales, las organizaciones están difundiendo sus documentos de trabajo, sus videos, documentales, sus podcasts, sus mensajes de información sobre derechos humanos.

Así, el objetivo de esta guía es ofrecer pautas para la protección y prevención frente a ataques que pudieran ocurrir en internet, pero también un contexto para entender por qué estos ataques ocurren.

1 La escritora feminista Mikki Kendall (@Karnythia en Twitter) acuñó a todo esto como "la gamificación del odio". Gamificación es un anglicismo que refiere a la acción de convertir una interacción en un tipo de competencia en búsqueda de puntos, medallas y que se viene aplicando a varios escenarios, como la educación, la publicidad y las comunicaciones en general.

2 Srnieck, N. (2018). Capitalismo de plataformas. Buenos Aires: Caja Negra.

3 Fuchs, C. (2017). Social Media: A Critical Introduction. London: Sage.

Soberanía Tecnológica

El término que nos interesa introducir aquí es el de soberanía tecnológica. Asumamos, como lo hemos descrito líneas arriba, que estamos en un escenario de dominio, en el que las personas y las organizaciones sociales (la llamada sociedad civil) estamos en total desventaja. La llamada "red de redes" no es ni por asomo democrática ni permite un intercambio horizontal, de igual a igual, entre los que participan allí. Organizaciones como la Asociación para el Progreso de las Comunicaciones vienen trabajando en cuanto foro internacional haya, para llevar temas como la regulación y combate a los ataques de género, ataques misóginos, lesbofóbicos, homofóbicos y transfóbicos, a nivel mundial[4]. Esto porque ni los estados ni las empresas que hoy dominan las comunicaciones digitales por sí solas van a cambiar o darse cuenta de lo que ocurre con las herramientas de información y comunicación.

El concepto que nos interesa introducir aquí es el de **soberanía tecnológica.** Por definición, esto quiere decir la capacidad que tenemos para adueñarnos de la tecnología y, por consecuencia, tener capacidad de decisión sobre ella.

Sobre la soberanía tecnológica, Margarita Padilla (2017) escribe que (el énfasis es nuestro):

4 La Asociación para el Progreso de las Comunicaciones en sí misma es una organización de organizaciones, compuesta por asociaciones de todo el mundo. Se puede saber más sobre esta red en https://www.apc.org/es

"Trasladando la cuestión de la soberanía a las tecnologías, la pregunta sobre la que queremos conversar es ***quién tiene poder de decisión sobre ellas,*** *sobre su desarrollo y su uso, sobre su acceso y su distribución, sobre su oferta y su consumo, sobre su prestigio y su capacidad de fascinación... (...)*

Todas las tecnologías se desarrollan en comunidades, que pueden ser, más o menos, autónomas o pueden estar, más o menos, controladas por las corporaciones. ***En la lucha por la soberanía, la cosa va de comunidades.*** *Nadie inventa, construye o programa en solitario, sencillamente porque la complejidad de la tarea es tal que eso resultaría imposible.*

La premisa de una comunidad que aspira a ser soberana es que el conocimiento debe ser compartido y los desarrollos individuales deben ser devueltos al común. El conocimiento crece con la cooperación. La inteligencia es colectiva y privatizar el conocimiento es matar la comunidad. La comunidad es garante de la libertad, es decir, de la soberanía."[5]

Así, lo que se busca es que ese empoderamiento de las organizaciones sea no solamente en el conocimiento de alguna aplicación o secuencia de procedimientos, sino a la apropiación colectiva del "saber tecnológico" (valga la redundancia, porque tecnología es mucho más que un conjunto de herramientas) y que el aprendizaje de protocolos de ciberseguridad apunte a una apropiación de un tipo de tecnología, la digital, hoy por hoy envuelta en un marco comercial, donde el tráfico y la compra y venta de datos es una norma.

5 Padilla, M. (2017). Soberanía tecnológica Vol. 2. Recuperado de https://wp.sindominio.net/wp-content/uploads/2018/01/sobtech2-ES-with-covers-WEB-150dpi-2018-01-13-v2.pdf

Las organizaciones

Esta guía parte de la conversación y recojo de información con las siguientes organizaciones: Cattrachas (Honduras), Colombia Diversa (Colombia), Diversas Incorrectas (Colombia), Comunidad Homosexual Esperanza de la Región Loreto-CHERL (Perú), Diversidad Sanmartinense-DISAM (Perú) y el Centro de Promoción y Defensa de los Derechos Sexuales y Reproductivos- Promsex (Perú).

Para la elaboración de la presente guía se aplicaron dos instrumentos, con el fin de contextualizar las recomendaciones de ciberseguridad. El primer instrumento fue una encuesta en línea, a través de la herramienta SurveyMonkey, que fue enviada a las personas que integran las organizaciones. El segundo instrumento fue una entrevista a profundidad.

En total se aplicaron 52 encuestas. Todas las personas encuestadas manifestaron tener un celular con acceso a internet. Y todas las personas encuestadas manifestaron que la aplicación de mensajería instantánea de mayor uso es Whatsapp. Las dos aplicaciones de mayor uso en general, son Facebook (100% de las personas encuestadas) e Instagram (71.15%). Y estas herramientas hoy vienen siendo usadas por estas personas para comunicarse con otras de sus organizaciones.

Un total de 17.65% de las personas encuestadas manifiestan haber sido hackeadas y un 7.69% que su cuenta fue "clonada" (es decir, que alguien creó un perfil falso con el mismo nombre y fotos).

A nivel de autopercepción, el 71.15% considera que su conocimiento informático es medio (11.54% considera que su conocimiento es alto y 17.31% considera que su conocimiento informático es bajo). Eso se condice cuando preguntamos por la necesidad de apoyo o ayuda para resolver temas informáticos. 67.31% considera que a veces necesita ayuda (28.85% dice que nunca la necesita, 3.85% considera

que siempre la necesita).

Como hemos señalado, se usa mucho el WhatsApp para la comunicación entre personas de la organización (86.54%), pero el correo electrónico llega al 92.31%, lo cual es interesante, porque, como veremos, este no es un medio mucho más seguro que algunas herramientas de mensajería instantánea. Pero, para envío y recepción de documentos, todos prefieren el correo electrónico (100%).

Los archivos son almacenados en su mayoría en una computadora o laptop de la organización (71.15% lo manifiesta así), pero también hay un alto número de personas que manifiesta que suben los archivos a la "nube" (42.31%).

Entre los hallazgos que han guiado la siguiente guía está, en primer lugar, que a pesar de que nos autoevaluemos como personas que tienen un conocimiento medio sobre el uso de las tecnologías digitales, no estamos libres de perder el control de nuestras cuentas de medios sociales o de que nos clonen las mismas[6].

De igual modo, es una preocupación constante el estar protegidos frente a la amenaza de los grupos extremos que agreden, hostilizan, acosan y violentan a las personas LGBTI en los medios sociales. El qué hacer frente a ellas, cómo combatirlas, si ignorarlas o no, cómo proceder frente a una agresión es una preocupación constante entre todas las organizaciones[7]. De igual modo, otra preocupación de las organizaciones consultadas es el referido a cómo publicar y qué herramientas son las más seguras, para evitar ser atacadas. También se recogieron buenas prácticas de las organizaciones para que estas puedan ser compartidas.

Esta guía busca responder a las distintas expectativas y dudas sobre la ciberseguridad. Comenzaremos con el problema de las contraseñas, trabajaremos sobre la identidad en medios sociales y terminaremos con la comunicación interna y el almacenamiento de datos.

6 Al menos dos organizaciones hicieron referencia a la existencia de o una persona capacitada al interior o de una persona "técnica amiga", de confianza, que ayudó a resolver temas informáticos.

7 En las entrevistas que se hicieron eran comunes los comentarios sobre los llamados "trolls" de internet y los mensajes de odio. "Ponen sus mensajes de odio en redes sociales. Se les ha denunciado. Ponen los logos, las fotos de las personas que dirigen las organizaciones, y dicen que hay que exterminarlas. Se han hecho las denuncias ante la Fiscalía General de la Nación. Sin embargo, en materia informática, este [Colombia] es un país "atrasado", se pueden demorar años en la investigación. Hay páginas creadas por grupos católicos de ultraderecha, que odian a todos los grupos minoritarios", señala la persona entrevistada de la agrupación Diversas Incorrectas.

52

encuestas realizadas

EL TOTAL tiene acceso a un celular con internet y usa WhatsApp para mensajería instantánea

17.65 % personas que fueron hackeadas

7.69% personas cuya cuenta fue "clonada"

11.54% autopercepción: conocimiento informático ALTO

71.15 % autopercepción: conocimiento informático MEDIO

17.31% autopercepción: conocimiento informático BAJO

Aplicaciones de mayor uso

100%

71.65%

Estar seguxs en la web

¿Cuándo una contraseña es segura?

Lo hemos leído todo el tiempo. “Hackers abren una brecha de seguridad en tal medio social. Es hora de cambiar nuestra contraseña” o “Mira cuáles son las contraseñas más comunes que existen”. La verdad, a estas alturas, no existe una contraseña 100% segura. Sin embargo, aquí vamos a poner algunos tips que son importantes para mantener nuestras cuentas más seguras:

1

No es más seguro escribir una contraseña con “$” en vez de “S” y “0” en vez de “o”.

Eso es un mito. De hecho, imaginemos que estamos usando nuestro apellido como contraseña, Bustamante, pero “lo vamos a hacer difícil” (sic). Suponemos que si cambiamos algunas letras haremos más difícil para cualquiera adivinar la contraseña: Bu$t4m4nt3. Sin embargo, son menos las veces en las que una persona se pone a adivinar la clave. Generalmente, son programas que van probando una clave tras otra a una gran velocidad, que para este ejercicio llamaremos velocidad absurda. Para una computadora no es más seguro escribir Bustamante que Bu$t4m4nt3. No hay una sola diferencia porque, para una computadora, se trata todo de caracteres. Cambiando algunas letras por números o signos no vamos a hacer nuestra contraseña más segura.

2

No es seguro usar la misma contraseña para todas nuestras cuentas, de correo o de medios sociales.

Lo hemos señalado más arriba. Cada cierto tiempo se abren brechas de seguridad y nuestra información termina circulando en foros, grupos y listas, para distintos fines. Pero, una cosa es que se filtre la contraseña de un servicio y otra que esa contraseña sea la misma para muchos otros. Tenemos que reducir al mínimo las posibilidades de ver vulneradas nuestras cuentas de servicios digitales.

3

Usar frases basadas en palabras aleatorias.

Las frases en las contraseñas tienen un doble fin. En primer lugar, aumentan la cantidad de caracteres. La Electronica Frontier Foundation (EEF) recomienda el uso de frases con seis palabras . Ellos han desarrollado el método del dado para crear dichas frases, basadas en un diccionario. Cualquier diccionario puede funcionar. Podemos lanzar un dado dos veces, ir a la página que nos indique ese número, lanzarlo de nuevo dos veces e ir a una palabra cualquiera. Y repetir el proceso seis veces. Digamos que obtenemos de ese modo las siguientes palabras: perro amalgama protocolo cubo rotario barca. Con esas seis palabras[8] podemos tener una nueva contraseña: perroamalgamaprotocolocuborotariobarca que es a la vez larga (38 caracteres y por lo tanto a una computadora le va a costar mucho "adivinarla") y al mismo tiempo está compuesta por palabras que podríamos recordar, incluso usando algún juego mnemotécnico (como los juegos de palabras cuando queríamos recordar una fórmula matemática en el colegio). Repetimos, una contraseña corta con signos y números no es nunca más segura que una contraseña larga de 30 caracteres a más.

4

Confiar en los administradores de contraseñas.

Si manejamos tres a cuatro cuentas, entre correos, servicios en la nube, medios sociales, quizá sea difícil memorizar tantas claves con tantas palabras. Es así que existen servicios gratuitos y seguros que administran nuestras claves por nosotros. Un servicio seguro y gratuito es el de KeePassXC (https://keepassxc.org/). Este servicio, que funciona de modo multiplataforma (puede instalarse en Windows, Mac o Linux), permitirá administrar las distintas contraseñas y crear nuevas por nosotros. Esto no exime de tener una contraseña para poder utilizar la herramienta. De hecho, necesitaremos una **contraseña maestra** (a modo de llave de llaves) para poder acceder al resto de contraseñas. Para crear esa contraseña, podemos ensayar el método descrito líneas arriba. ¿Por qué es seguro este servicio de administración de contraseñas? En primer lugar, porque toda la información se encuentra encriptada. Esto es, que sin la contraseña nadie podrá "ver" lo que hay guardado dentro del administrador, salvo caracteres sin sentido. En segundo lugar, porque no guarda la contraseña en la nube. Hay algunos servicios privados que administran nuestras contraseñas por nosotros (por ejemplo, Apple). Pero no son enteramente seguros, porque constantemente están expuestos a ataques que aprovechan sus vulnerabilidades. Al menos las contraseñas vinculadas a la organización deberían estar en un administrador.

8 Ver https://www.eff.org/dice (en inglés)

Nuestra identidad, protegida

Es difícil, pero no imposible, dejar de estar en los medios sociales. Podemos encontrar cualquier razón y muy probablemente sea importante: queremos comunicarnos mediante dicha red con nuestros familiares, con nuestros amigos y amigas, o simplemente queremos compartir cosas. Queremos, y no es algo bueno ni malo, entrarle al juego de los likes, los compartidos.

El problema, como lo señalamos en las primeras páginas de la presente guía, es que estas promueven constantemente la competencia entre los usuarios. Competencia por "me gusta", "me encanta", por textos, videos o fotos compartidas. Por cantidad de seguidores. A esta dinámica de textos por puntaje es que se le ha llamado "gamificación". Así, nuestra participación está mediada por estas reglas de juego, donde los comentaristas buscan reconocimiento a través de los "me gusta" o comentarios de respuesta.

Es por ello que, en medios como Facebook, Youtube o Twitter (aún no en Instagram, pero quizá prontamente lo veamos allí también), vemos la propagación de mensajes que incitan las ofensas y el odio hacia grupos como personas LGBTI o cualquier minoría que esté buscando fortalecer sus derechos.

Peor aún, cuando a través de sus algoritmos, las "líneas de tiempo" o muros de contenidos se personalizan para que podamos leer lo que según estas plataformas se acomoda más a uno. El resultado es que tenemos cajas de resonancia potentísimos y que sirven de caldo de cultivo para la propagación de mensajes de odio.

Entre los mensajes de odio que hemos encontrado a partir de las entrevistas tenemos: amenazas físicas a integrantes de la organización -que van desde el daño físico menor a convocatorias abiertas para "exterminarlas"-, información falsa sobre diagnósticos de salud de esas mismas personas, ataques verbales por parte de cuentas falsas o de cuentas asociadas a organizaciones convervadoras, información igualmente falsa sobre la organización, insultos, difamación, entre otros.

¿Qué debemos hacer en estas plataformas?

1 **Ante todo, contar con contraseñas seguras.**

Si, a pesar de lo expuesto, vamos a tener una cuenta en Facebook, Google (Youtube), Instagram o Twitter, debemos asegurarnos de que nuestra contraseña sea lo suficientemente segura como para que nadie o casi nadie pueda adivinarla. Seguir los pasos descritos más arriba.

2 **Activar la doble autenticación.**

Cada vez más servicios cuentan con un sistema de doble autenticación, que le permite vincular la cuenta del medio social con el celular, a través de un código de validación que se envía a través de un mensaje de texto.

3 **Activar los parámetros de privacidad.**

No debemos olvidar que pertenecemos a organizaciones que velan por derechos de personas, las cuales se encuentran hoy bajo la mira de grupos extremistas. Por lo tanto, estos mismos grupos buscarán contar con información nuestra. Dependiendo del servicio, podemos activar parámetros de privacidad, personalizando quién puede ver qué. Aquí podemos hacer como ejercicio tratar de ver nuestro perfil en cualquier medio social (por ejemplo, Facebook), sin estar loggeados.

4 **Publicar la menor cantidad de datos privados.**

No solamente porque así estos medios sociales "sabrán" menos de nosotros, sino porque así reduciremos la posibilidad para que cualquier agrupación extrema pueda, a través de algún descuido, conseguir información nuestra que delate nuestra ubicación, patrones de movilidad, gustos, información sobre nuestros contactos o actividades. Mientras menos información nuestra se encuentre en estos medios sociales, incluso es menor la posibilidad para que nos "clonen" la cuenta, es decir, que alguien cree una cuenta con información similar para despistar a nuestros contactos[9].

5 **Hacer doble validación de las personas que quieren convertirse en nuestros contactos.**

No aceptemos a cualquiera. Si no lo conocemos en persona, no aceptemos a nadie como contacto. Incluso si es una persona que conocimos en algún evento, es mejor hacer doble validación, escribirle a través del "interno" o "inbox" para corroborar que la persona en cuestión es quien asegura ser[10].

Esto último es un tema importante porque este es uno de los

9 De hecho, durante las entrevistas y encuestas, se recogió información sobre cuentas clonadas.

10 En las encuestas realizadas, se detectaron casos de cuentas de medios sociales que fueron "hackeadas".

procedimientos que usan los crackers o hackers no éticos para infiltrarse y robarse información personal. Por lo general, comienza con un perfil falso, con una foto y nombres falsos y a partir de allí van estableciendo una relación de confianza con la futura víctima. Y eso cierra cuando el cracker envía un archivo (foto, video, presentación de Powerpoint, un enlace) a la futura víctima. Lo que nos lleva a:

6 **Siempre hacer doble validación con respecto a cualquier archivo o enlace que alguien nos quiera compartir de modo interno.**

Incluso siendo un enlace de alguien que conozcamos, preguntemos antes de descargar o antes de hacer click en lo que nos están compartiendo. ¿Es algo seguro? ¿Están en pleno conocimiento de lo que me están enviando? Es posible que la cuenta del contacto ya esté comprometida con un virus o tomada por un cracker. Si conocemos a la persona y tenemos otras formas de comunicarnos con ella, usemos esos otros medios y preguntemos nuevamente. Los crackers usan generalmente archivos que dicen cosas como "fotos de la última fiesta", "te envío esta tarjeta musical" u otros nombres sospechosos. Incluso por correo electrónico usan supuestos correos financieros (de bancos conocidos) para robar información personal (números de banco, números de documentos de identidad). Es posible identificarlos cuando vemos que el correo no corresponde al nombre del banco o hay muchos errores ortográficos. Siempre hagamos doble validación.

7 **Desactivemos en lo posible la georeferenciación en nuestros dispositivos móviles y cuentas de medios sociales.**

La georeferenciación es la información que generan los dispositivos digitales sobre nuestra ubicación geográfica. El nivel de detalle de esta información puede estar a nivel del lugar exacto donde estamos, el edificio donde vivimos, el restaurante en el que nos encontramos, la oficina a la que vamos a hacer un trámite o trabajaremos. En los celulares, tanto Android como iPhone, en la sección de configuración podemos decidir qué aplicaciones pueden aprovechar la información de geolocalización. Esto tiene dos fines. En primer lugar, las plataformas de medios sociales usan esta información para tener datos agregados y poder revenderlos (patrones de consumo, movilidad, quién hace qué, dónde y cómo). En segundo lugar, es probable que nuestras publicaciones y fotos compartidas luego tengan información (metainformación) sobre nuestros movimientos, dónde estuvimos, qué hacemos. Esta información podría ser aprovechada por agrupaciones extremas que quieran hacer algún tipo de acoso. En lo posible debemos desactivar esas opciones.

Podemos, por ejemplo, ver el historial de ubicaciones de Google.
https://www.google.com/maps/timeline?pb
Si este ha estado activado todo el tiempo, es posible que allí aparezcan todos nuestros pasos, rutas, viajes, todos los lugares por dónde hemos andado. Una acción a realizar es borrar ese historial (entrando a Administrar historial de ubicaciones).

De igual modo, servicios como Twitter ofrecen en Configuración y luego en Privacidad, la opción de borrar toda la información de ubicaciones.

Mientras menos información personal y privada publiquemos, mucho más segura estará nuestra identidad en los medios sociales.

Resumiendo

- **Revisemos primero quién puede ver qué. Antes de publicar, asegurémonos qué información va a ser pública.**
- **Revisemos qué está activado por defecto. Desactivemos las opciones de geolocalización.**
- **Validemos a los nuevos contactos y los archivos que nos quieren mandar por "interno".**

¿Qué hacemos con los *trolls*?

La palabra troll ya es parte del argot de los medios sociales. Se usa para describir a toda aquella persona, que usa un seudónimo, que puede incluso usar su nombre y apellido reales, o un anónimo, que busca incordiar a una persona o una organización en particular. En los últimos tiempos han adquirido relevancia porque cada vez más la acción de los trolls se ha refinado, no tanto en sus contenidos, pero sí porque hay empresas que brindan servicios de acoso y crean cientos de cuentas para ello. Es más, en algunos casos se pueden tratar de bots o cuentas que generan mensajes automáticos.

El problema es que nadie sabe bien qué hacer con los trolls. La regla general, por mucho tiempo, es que al troll no se le debe hacer caso o "no alimentarlo"[11]. Sin embargo, eso ya no es suficiente.

Los trolls pueden tener varios tipos de modalidades:

Desvían la atención sobre lo que un activista está escribiendo o reportando, abriendo el debate o haciendo preguntas.	**Atacan abiertamente a la persona o la organización.**	**Siembran mentiras sobre la persona o la organización.**

11 "No alimentes al troll" fue la ley en los medios sociales por mucho tiempo. La frase viene de los juegos de rol como Calabozos y Dragones.

En cualquiera de los casos, sea cual fuere la respuesta, siempre hay que evitar dar información personal. Lo que se recomienda en cualquiera de los tres casos es "responder sin responderle". Se puede hacer una captura de pantalla de lo que el troll escribe y responder abiertamente, reencausando el debate, rechazando el ataque o rebatiendo la mentira. Lo que hay que evitar es la respuesta directa que permita que el troll gane notoriedad, mucho menos compartir el enlace que dirija a los otros lectores al perfil del troll.

Si el troll usa información privada de la persona, lo recomendable es denunciar el perfil del troll al medio social correspondiente. Y convocar a que otras personas también lo denuncien. En estos momentos, hay muchas dudas sobre la eficacia de servicios como Twitter y Facebook para controlar los mensajes de odio, por lo que toda denuncia debe hacerse.

Ya hemos pasado, por mucho, la fase donde el ignorar los ataques era la forma más útil de controlar a los posibles agresores. Los agresores hoy se encuentran más cohesionados y, en algunos casos, organizados. La denuncia pública y la convocatoria a que otras personas se sumen al señalamiento del troll es hoy la estrategia más efectiva.

→ Resumiendo

- **Ya pasaron los tiempos del "no alimentes al troll". Al troll hay que responderle "sin responderle".**
- **Hay que desmentir rápidamente y reencausar las conversaciones y debates.**
- **Hay que denunciar a los trolls que atacan.**

Comunicarnos en la web segurxs

¿Qué programas de mensajería instantánea usar?

La mensajería instantánea es el término técnico que usamos para referirnos a todos aquellos sistemas que nos permiten comunicarnos en tiempo real entre dos dispositivos conectados a través de internet.

Con los años estos sistemas se volvieron populares y fueron reemplazando a la mensajería móvil (SMS) porque permitían enviar archivos adjuntos, como imágenes y fotos.

Uno podía o puede decidir guardar la información que se comparte en el celular. Puede decidir incluso que todos los archivos recibidos se almacenen automáticamente en el dispositivo móvil.

Estas comunicaciones parten de un dispositivo, pasan a través de la plataforma de mensajería, y llegan al otro lado.

Sin embargo, como veremos, todas estas son prácticas que generan o abren espacio para la inseguridad. En muchos países, los operadores de servicios de internet pueden tener acceso a las comunicaciones que se dan. Pueden “leer” lo que se envía de un lugar a otro. Cada vez se usan más sistemas de rastreo para ver “qué se dice” en los mensajes.

Sin embargo, es posible prever estos escenarios. Una opción (válida también para los correos electrónicos) es cifrar los mensajes. El sistema de cifrado implica esconder los textos detrás de otros.

Pensemos en el siguiente juego infantil:

MURCIÉLAGO

y luego asignamos un dígito a cada letra

M = 1
U = 2
R = 3
C = 4
I = 5
E = 6
L = 7
A = 8
G = 9
O = 0

Luego podríamos cifrar cualquier palabra

como por ejemplo
“SECRETO”
S6436T0

Este es un cifrado bastante simple. Cualquier sistema informático actual podría fácilmente descubrir de qué se trata. Hay cifrados bastante complejos que usan, por ejemplo, algunos servicios de “nube” (veremos eso luego) para almacenar su información.

Hay actualmente sistemas de comunicación que encriptan los mensajes antes de salir y que solamente el otro lado, el receptor puede abrirlos. Así, cualquier posibilidad de que el mensaje “se lea” en el camino queda descartada.

Para una mejor comunicación entre los miembros de la organización y con personas aliadas o que quieran dar o brindar un testimonio seguro:

1

Recomendamos usar aplicaciones de mensajería instantáneas que estén validadas como seguras.

Actualmente, el mejor sistema de mensajería instantánea, que asegura una encriptación total de punto a punto (de emisor a receptor) es la aplicación **Signal**[12]. Esta ofrece un sistema de protección de información tanto para el envío de documentos, mensajería instantánea, mensajería de voz, video de persona a persona y varias organizaciones defensoras de derechos digitales recomiendan su uso. Funciona en cualquier plataforma, iOS o Android, así como hay versiones para computadoras de escritorio.

2

Asignar un período de “vida” a los mensajes.

Signal además cuenta con una opción de destrucción de mensajes. Uno puede configurar si para una conversación en específico, el mensaje tenga una “vida” de una hora, veinte minutos, un día. Pasado el tiempo configurado los mensajes quedan totalmente destruidos.

Porque, incluso bajo el principio de que los mensajes sean cifrados, el perder un dispositivo móvil puede abrir la posibilidad de que alguien acceda a las aplicaciones (de conocer la contraseña del equipo) y poder leer los mensajes.

12 https://signal.org/

3

En lo posible no compartir archivos a través de los servicios de mensajería instantánea

Aun cuando estos puedan ser seguros, como Signal, los archivos pueden quedar almacenados en el dispositivo móvil. En caso de pérdida o robo o sustracción, estos archivos podrían quedar disponibles. Si no hay otra que recibir o enviar un archivo a través de una aplicación como Signal, se recomienda su descarga en un repositorio seguro (eso lo veremos a continuación) y su borrado del dispositivo móvil.

4

Verifiquemos nuestra lista de contactos telefónicos.

Las aplicaciones de mensajería instantánea usan como base la lista de contactos para saber "quiénes están dentro" y "quiénes cuentan con la aplicación". Eso puede exponer al dispositivo, ya que por error podría enviarse un archivo o recibir algún programa que se infiltre al equipo y pudiera robar datos personales.

Como con la lista de contactos de medios sociales, si no conocemos a la persona fehacientemente, no la agreguemos a la lista de contactos del dispositivo móvil, ya que automáticamente se convertirá en un contacto en las distintas aplicaciones de mensajería instantánea que tengamos en el equipo.

De igual modo, una persona podría cambiar de dispositivo y de teléfono. Comprobemos regularmente los números, para confirmar que estos siguen asociados a las personas que conocemos.

Resumiendo

- **Sugerimos el uso de la aplicación Signal, tanto para las personas que integran las organizaciones, como para los contactos de las mismas. Las comunicaciones que impliquen información sensible deberían pasar por Signal.**
- **Sugerimos asignar un período de vida en Signal para los mensajes.**
- **Sugerimos no usar los servicios de mensajería instantánea para el envío o recepción de archivos.**
- **Sugerimos revisar periódicamente la lista de**

contactos del dispositivo móvil.

Navegar de modo seguro

Como la canción de The Police, "Every breath you take", las corporaciones que manejan los buscadores y los sistemas de comunicación digital, vigilan o miran las cosas que publicamos, escribimos (incluso en la barra del buscador), para poder luego analizar esa información y poder venderla. En algunos casos, inclusive, han brindado esa información a agencias de comunicación política o agencias de inteligencia[13]. La verdad, no estamos seguros cuando navegamos y mucho menos cuando compartimos información.

Es más, cada vez que entramos a un portal a ver o buscar información, este puede saber desde dónde nos conectamos. Esto no es un secreto y es parte del funcionamiento de cualquier servidor que cuenta con un sitio web propio. Ahorita mismo podríamos ir al panel de control de nuestro sitio y ver desde dónde se conectan. En algunos casos, si es que fuera el caso de que nos conectamos desde un sitio que cuenta con fibra óptica, podríamos identificar con nombre propio el lugar de conexión.

13 Ver el caso de Facebook y Cambridge Analytica, por ejemplo. https://www.genbeta.com/redes-sociales-y-comunidades/facebook-conocia-practicas-cambrigde-analytica-meses-antes-que-se-destapara-escandalo

Hay algunas soluciones para navegar de modo seguro, y esto es igual para una computadora, laptop, tablet o celular:

1

Usar un navegador seguro que no almacene información personal.

Google Chrome está descartado. Todo lo que hace Google Chrome es usar toda la información personal para mejorar, desde su punto de vista, la "experiencia del usuario". Se recomienda usar navegadores más seguros, menos susceptibles de ser atacados para el robo de información personal. Distintas organizaciones recomiendan el uso de Firefox, ya que no solamente tiene parches de seguridad contra ataques de hackers regularmente (lo mismo hace Chrome), pero no vincula las búsquedas a su base de datos sobre personas y perfiles.

2

Usar en lo posible el navegador en modo navegación privada.

Todos los navegadores tienen un modo privado. Esto permite que el usuario navegue por internet, sin que se guarde nada de información que podría comprometer la privacidad del usuario. En el modo privado, Firefox no guardará cookies[14], ni búsquedas realizadas ni páginas visitadas. Por supuesto que no es para hacer búsquedas anónimas, ya que un operador de internet podrá saber a qué páginas visitas. Pero es un modo seguro en tanto no se deja huella en la computadora de a dónde se ha navegado.

14 Las cookies son pedazos de información que se almacenan en la computadora y que permite a ciertos sitios web "personalizar sus contenidos".

3

Limpiar constantemente el historial y las cookies del navegador.

Como práctica habitual, se debe borrar el historial y las cookies del navegador; no dejar nada de información privada del usuario que pueda luego ser usada.

4

En casos extremos usar TOR o un navegador con opción TOR.

TOR es un sistema VPN (Virtual Private Network) que permite enmascarar el lugar desde donde se conecta uno. Cuando nos conectamos a internet, se nos asigna un código o número para navegar. Cuando nos conectamos a un sitio web, el servidor donde se aloja este recibe una notificación que le señala que una computadora de tal lugar se ha conectado. A veces esto puede ser sensible y se sugiere enmascarar ese código. Esto se llama una **navegación anónima.**

TOR funciona del siguiente modo: nuestra computadora se conecta con otra computadora en un país que no es el nuestro y desde esa computadora uno se conecta con el sitio web al que quiere acceder. Para el servidor donde está alojado este sitio web, es como si una persona con una computadora alojada en este segundo país hubiera accedido a la información.

¿Qué podemos hacer para usar TOR? Hay dos opciones. La primera, es instalar el software TOR en nuestra computadora (no hay para móviles iOS pero sí Android)[15]. Instalamos el programa y luego activamos TOR **antes** de navegar. La segunda opción es instalar un navegador que cuente con TOR[16], donde todas las búsquedas o cargas de información en ese navegador se realizarán de modo anónimo.

5

Nunca instalar absolutamente nada que no hayamos solicitado.

Muchos sitios web perjudiciales envían avisos que señalan que nuestra computadora está infectada con algún virus, que el desempeño de la computadora puede mejorar o que se necesita limpiar de cookies u otras cosas. A menos que sea un diagnóstico que ustedes hayan solicitado, nunca le den validez a esos avisos o mensajes.

15 https://www.torproject.org/
16 https://www.torproject.org/projects/torbrowser.html

Resumiendo

- **Sugerimos el uso de la aplicación Firefox para navegar**
- **Sugerimos navegar en modo privado, para evitar que se guarde información en la computadora.**
- **Sugerimos borrar constantemente el historial, las cookies y los archivos temporales del navegador.**
- **En caso extremo, sugerimos el uso de la herramienta TOR.**
- **Nunca instalar absolutamente nada que no hayan solicitado y validado primero.**

Intercambiar y guardar archivos de modo seguro

El siguiente problema tiene que ver con el compartir archivos. No hay mejor modo de compartir un archivo de modo seguro que de forma presencial. Y que existan la menor cantidad de versiones diseminadas en computadoras. Encontramos una buena práctica entre las entrevistas a las organizaciones, donde o se está usando un servidor propio (no nube) o un disco duro externo que luego se guarda en una caja fuerte.

En el primer caso, para configurar un servidor propio, las organizaciones LGBTI contaron con una persona que tenía la experiencia para hacerlo o esta persona pudo saber qué pedirle a un técnico de confianza.

Para contar con un servidor propio se necesita, en primer lugar, configurar una red local (alámbrica o inalámbrica) y, en segundo lugar, contar con una computadora dedicada a esos fines. A su vez, se sugiere que, de apostar por un servidor propio, en su interior se cuente con un disco duro de estado sólido, cuyo período de vida es mayor a la de un disco duro normal (aunque su costo es mayor).
De igual modo, de no contar con los recursos para un servidor, la apuesta de tener un backup (copia de respaldo) en un disco duro externo (sugerido un disco duro de estado sólido) que se almacene en una caja fuerte, sigue siendo la opción más segura. Se deben hacer monitoreos permanentes para que los archivos más sensibles no se encuentren diseminados ni en las computadoras o laptops de la organización y mucho menos en los dispositivos móviles.

Sin embargo, a veces es necesario enviar un archivo de forma segura. Para los protocolos de internet no hay absoluta diferencia entre enviar un mensaje de 140 caracteres o de 25 MB. Sigue siendo información. Y queremos que la información no sea revisada por nadie.

Evitemos en lo posible usar servicios como Whatssap o el Messenger de Facebook para enviar archivos.

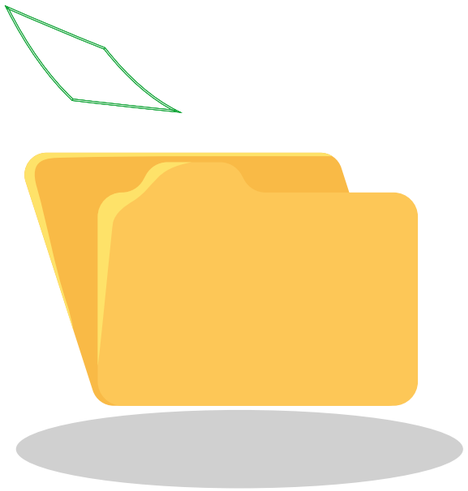
Si el envío de mensajes a través de esos servicios es inseguro, también lo es para el envío de archivos, con el agravante que es posible que se queden almacenados en el dispositivo de quien lo envía y quien lo recibe.

Si vamos a usar un servicio de mensajería instantánea para envío de archivos, usemos Signal.

Ya hemos comentado sobre por qué apostamos por Signal como sistema de envío de mensajes.

Evitemos usar WeTransfer, Mega, etc.

Muchos de esos servicios no cuentan con sistemas validados de caducidad de sus archivos.



Sugerimos el uso de Firefox Send

La organización Mozilla (los responsables del Firefox) han lanzado un producto llamado Firefox Send, que permite enviar (cuando uno se ha inscrito) archivos de hasta 2.5GB. Permite no solamente caducidad de vigencia de la descarga en términos de tiempo, sino también hasta cuántas descargas son posibles. A su vez, permite usar contraseñas por lo que, si alguien consiguiera el enlace, no podrá ver su contenido. Para ver qué contraseñas usar, nos remitimos a las pautas anteriores. Y se sugiere, encarecidamente, que las contraseñas no sean compartidas por mensajería instantánea.

Resumiendo

- **En lo posible, es mejor contar con un servidor propio o en su defecto con un disco duro externo para centralizar los documentos sensibles, y guardar el disco duro en un lugar seguro.**
- **Si vamos a usar mensajería instantánea para archivos pequeños, usemos Signal.**
- **Si vamos a usar algún servicio para enviar archivos muy grandes, sugerimos el uso de Firefox Send.**

Sobre el uso de correos cifrados

Hasta hace no mucho, se recomendaba usar sistemas de correo cifrado. Esto es, como vimos, un sistema que codificaba el contenido de los correos (y los adjuntos) y solamente la persona que lo recibía podía “abrir” su contenido.

El principio es el mismo o muy similar al de la mensajería instantánea como Signal, que recomendamos anteriormente.

Sin embargo, organizaciones como la Electronica Frontier Foundation (EFF) señalan que se han encontrado vulnerabilidades. Estas vulnerabilidades han permitido exponer sus bases de datos de claves, por lo que ya no es nada seguro usar estas herramientas.

Sobre el borrado seguro

Cuando borramos un archivo de un disco duro, o de un USB, no lo estamos borrando por completo. Muchas veces lo que hacen los sistemas operativos de las computadoras es “ocultar” lo que uno ha borrado. Así, borrar un archivo como siempre lo hacemos no hace que se borre de modo seguro, ya que alguien con un mínimo de conocimiento y una herramienta que se puede conseguir en cualquier lado, podría conseguir nuevamente esos archivos “borrados”.

Lo que necesitamos es un borrado seguro.

Muchos sistemas operativos, sobre todo los basados en UNIX (que incluyen a los sistemas operativos de las Apple), permitían un borrado seguro. Sin embargo, lo que se vio es que, a pesar de la promesa, los archivos no terminan de borrarse.

Hay formas para borrar los archivos de modo seguro. Depende del sistema operativo:

Windows y Linux

Para Windows, contamos con el programa gratuito y seguro Bleachbit. Este permite destruir los archivos completamente, como si los pasáramos por una trituradora (“shredder”).

Los pasos para usarlo son los siguientes:

Descargar Bleachbit del sitio https://www.bleachbit.org/download/windows

Correr el programa. No necesita instalarse. Escoger lo que se quiere borrar para siempre. Elegir Recycle Bin o Papelera. También los logs, archivos temporales.

MacOS

Como hemos indicado, MacOS no ofrece un borrado totalmente seguro por lo que ya no se cuenta con tal función.

Sobre volúmenes cifrados

MacOS y Linux ofrecen la opción de cifrar todos los contenidos de sus discos para que nadie pueda acceder a ellos sin el password o contraseña.

En el caso de MacOS, se puede ir a Preferencias del Sistema, luego a Seguridad y Privacidad y luego entrar a FileVault. Allí puede activar la encriptación de todo el volumen.

En el caso de Linux, al configurar el sistema por primera vez, se ofrece la opción de encriptación de todo el volumen.

En el caso de Windows, la aplicación que viene con dicho sistema se llama BItLocker, que se encuentra en el Panel de Control y luego en Cifrado de Unidad Bitlocker. En el caso de este sistema de cifrado, se elige el volumen que se quiere proteger.

No existe un sistema de cifrado total para USB, por lo que se recomienda su destrucción total, así como el de los CD-ROM.

Existen soluciones de destrucción de archivos. DBAN (Daryl Boot and Nuke) es una herramienta gratuita, pero que funciona solo en discos duros y no sobre unidades de memoria USB.

Resumiendo

- **Se ha descubierto que las formas de encriptación de correos no son totalmente seguras, por lo que se recomienda no usar el correo electrónico, pero sí servicios como Signal, incluso para el envío de archivos.**
- **Los sistemas de encriptación de volúmenes ofrecen un sistema de destrucción de archivos total, ya que, sin la clave de acceso, los volúmenes serán totalmente ilegibles.**
- **MacOS ofrece FileVault para protección del disco duro. Linux ofrece encriptación al momento de instalar el sistema. Windows ofrece BitLocker.**

En varios países existen oficinas de la policía especializada en delitos digitales (incluyendo la violencia en las redes).

En el caso colombiano, la Policía Nacional de Colombia cuenta con una ventanilla virtual para las denuncias: https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

En el caso peruano, existe la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), pero están más enfocados en extracción de datos financieros. Tenemos, por otro lado, la iniciativa del Ministerio de la Mujer y Poblaciones Vulnerables (MIMP) - "No al acoso virtual", la cual define al acoso como:

> *"El acto o conducta realizada por una persona o grupo de personas para amenazar, insultar, acusar falsamente, avergonzar, intimidar o criticar a una persona a través de los medios de comunicación digitales. Puede o no tener connotación sexual."*

La dirección de la iniciativa es http://www.noalacosovirtual.pe y cuenta con la opción de especificar la orientación sexual y la identidad de género de la persona denunciante, así como la condición de intersexualidad.

En el caso hondureño, existe la iniciativa de Ley Nacional de Ciberseguridad y medidas de protección ante los actos de odio y discriminación en internet y redes sociales[17], que ha sido aprobada en primera instancia por el Congreso Nacional de dicho país. Cabe resaltar que distintas organizaciones han llamado la atención sobre cómo esta iniciativa puede ser usada también como forma de censura[18].

Sin embargo, ante la ausencia de oficinas especializadas por parte de la policía, se aplica el mismo Código Penal, que protege el honor y la integridad de las

17 http://congresonacional.hn/wp-content/uploads/2018/02/DICTAMEN-LEY-DE-CIBERSEGURIDAD-I.pdf
18 https://www.alai.lat/el-proyecto-de-ley-en-profundidad/

personas. Así, la difamación está igualmente penada se dé esta a través de un medio impreso o un medio de comunicación digital. Con las amenazas de muerte o violencia, procede de igual modo. Por lo tanto, no es necesario que exista una oficina especializada en temas digitales para sentar la denuncia.

Siempre es importante tener en cuenta que en distintos países existen organizaciones que vienen trabajando temas de derechos digitales:

En Colombia, contamos con la Fundación Karisma, quienes no solamente hacen trabajo de incidencia sobre los derechos digitales, enfocados en la privacidad y la protección de datos personales, sino también en el fortalecimiento de capacidades de organizaciones. https://karisma.org.co/

En Honduras, existe la Asociación por una Ciudadanía Participativa, plataforma que trabaja en temas de derechos humanos, pero que tiene una división especializada en derechos digitales. http://aciparticipa.org/

En el Perú, tenemos a Hiperderecho, una organización sin fines de lucro que viene trabajando en derechos digitales, protección de información personal, y últimamente están trabajando desde un enfoque de género y apuntando a combatir el acoso sexual en redes. http://hiperderecho.org

A nivel latinoamericano, tenemos dos organizaciones importantes. En primer lugar, la Asociación para el Progreso de las Comunicaciones (APC), quienes están trabajando a nivel global los temas de las telecomunicaciones desde un enfoque feminista y cuya oficina regional en América Latina busca integrar todas las iniciativas sobre derechos digitales. https://www.apc.org/es/regions/latin-america-caribbean

En segundo lugar, Derechos Digitales, una organización con base en Chile, pero que está promoviendo la discusión sobre los derechos de los ciudadanos y ciudadanas en internet a nivel regional. https://www.derechosdigitales.org/

Todas estas organizaciones pueden ser contactadas para solicitar apoyo o asesoría.

Con el apoyo de:

arcus FOUNDATION

OrganizacionesIntegrantes:

PROMSEX
CENTRO DE PROMOCIÓN Y DEFENSA
DE LOS DERECHOS SEXUALES Y REPRODUCTIVOS

COLOMBIA DIVERSA

RED LÉSBICA CATRACHAS

DIVERSAS INCORRECTAS

CHERL
COMUNIDAD HOMOSEXUAL
ESPERANZA PARA LA REGION LORETO

DISAM

RD REDEFENSORA
DE LA DIVERSIDAD SEXUAL & DE GENERO