Vulnerabilidad, inclusión y seguridad digital en México

Coordinadora
Patricia Hernández Salazar

HM851
V85M4

Vulnerabilidad, inclusión y seguridad digital en México / Coordinadora Patricia Hernández Salazar.- México : UNAM. Instituto de Investigaciones Bibliotecológicas y de la Información, 2021.
vii, 246 p.- (Usos de la información : procesos y medios)
ISBN: 978-607-30-5585-7

1. Sociedad de la información. 2. Grupos vulnerables. 3. Integración social. 4. Brecha digital. 5. Alfabetización digital. 6. México. I. Hernández Salazar, Patricia, coordinadora. II. ser.

Diseño de portada: Sonia Wendy Chávez Nolasco

Primera edición, 2021

Universidad Nacional Autónoma de México,
C. P. 04510, Ciudad de México
Impreso y hecho en México
ISBN: 978-607-30-5585-7

Publicación dictaminada

Contenido

Introducción i
Patricia Hernández Salazar

La situación digital de los y las jóvenes en México 1
Rodrigo Castaneyra Hernández

Contexto digital de las personas adultas mayores
en México: vulnerabilidad e inclusión. 31
Patricia Hernández Salazar

La inclusión digital como reductor de la
vulnerabilidad de las mujeres 83
Patricia Navarro Suástegui

Discapacidad e inclusión digital: desde un modelo social. 121
María Guadalupe Vega Díaz

Los retos de la inclusión digital en el caso de
los migrantes en tránsito por el territorio mexicano 167
Araceli Mendieta Ramírez

La erosión de la privacidad en las personas
defensoras de derechos humanos: la vulnerabilidad
de los conectados 213
Valentín Ortiz Reyes

La erosión de la privacidad en las personas defensoras de derechos humanos: la vulnerabilidad de los conectados

Valentín Ortiz Reyes
Biblioteca Daniel Cosío Villegas
El Colegio de México

INTRODUCCIÓN

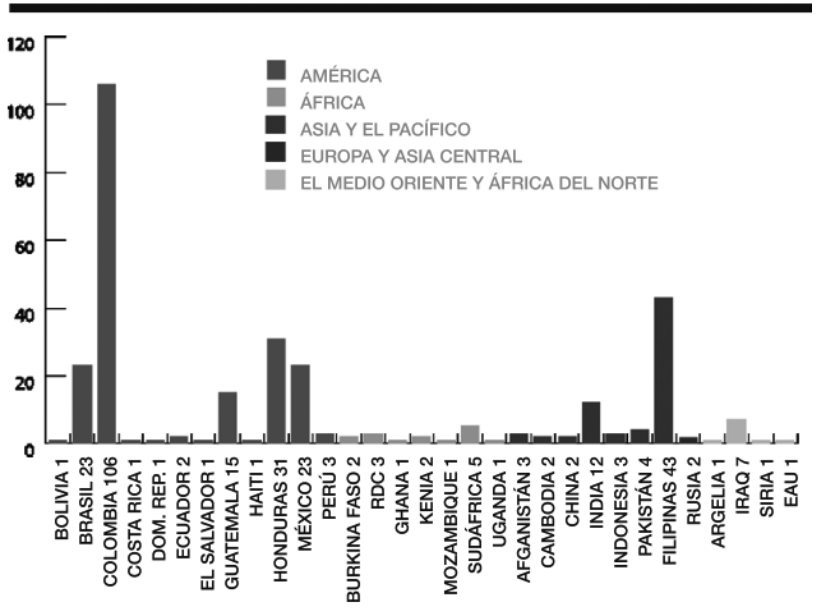
El entorno digital, el entorno de las personas conectadas, no deja a un lado las posibilidades de ser blanco de amenazas que pueden vulnerar derechos fundamentales, tales como la libertad de expresión, el derecho de asociación, el derecho a la información y el derecho a la privacidad. Tal es el caso de las personas defensoras de derechos humanos (DDH). De acuerdo con Naciones Unidas (s.f. a), las personas DDH son aquellas que actúan en favor de un derecho humano individual o grupal y se esfuerzan en promover y proteger los derechos civiles y políticos, así como en lograr la promoción, la protección y el disfrute de los derechos económicos, sociales y culturales. Algunos de los temas por los que se pronuncian en contra son: la detención y prisión arbitrarias, las desapariciones, la discriminación, las cuestiones laborales, las expulsiones forzadas, la violencia contra las mujeres, entre otros.

Los riesgos a los que se exponen las personas DDH son preocupantes, pues son víctimas de violencia física, psicológica, económica y social por parte de actores políticos, económicos, religiosos, estatales, civiles a causa de su trabajo por la democracia, los derechos

humanos y la justicia social (Neto 2017). En México las agresiones en contra de personas DDH forman parte de un entorno precario conformado por actos de persecución, hostigamiento, vigilancia y, en el peor de los casos, asesinatos (Comisión Mexicana de Defensa y Promoción de los Derechos Humanos A.C 2011). En 2019, Frontline Defenders (2020) reportó 304 personas defensoras de derechos humanos asesinadas a nivel mundial; de las cuales veintitrés perdieron la vida en México (ver tabla 1).

En un informe especial sobre la situación de las personas DDH en México (Comisión Nacional de los Derechos Humanos, 2011, p. 12) se describen algunas de las amenazas a las que se expone este grupo en especial situación de vulnerabilidad. Se habla de "amenazas, abusos, actos de hostigamiento, intimidación y ataques a sus libertades fundamentales, por parte de autoridades o agentes no gubernamentales". Este tipo de prácticas, de acuerdo con el

Tabla 1. Personas defensoras de derechos humanos que fueron asesinadas en 2019



Fuente: Front Line Defenders (2019,40).

mismo documento, se extiende a los familiares de los defensores como una forma coercitiva de generar miedo y orillar a las personas DDH a desistir de las actividades que realizan a favor de la defensa de los derechos humanos.

Además de la precariedad que persiste en la labor de las personas DDH en México y los agravios a los que se exponen, se suman los riesgos de vulnerar su derecho a la privacidad, principalmente en medios digitales. Hoy en día, la capacidad tecnológica de geolocalización, la identificación de redes de contacto, el robo de identidad y de información, así como programas de *spyware*, establecen una vulnerabilidad palpable para este grupo que, si bien aprovecha medios tecnológicos para amplificar sus denuncias, también se expone a nuevos riesgos que pueden llegar a erosionar su privacidad y a desgastar, en el peor de los casos, su integridad física y emocional.

El tema de la privacidad y el acceso a información sensible en el caso de los DDH resulta delicado, pues trabajan con datos, contactos y expedientes, evidencias que sirven, en muchos de los casos, para documentar y evidenciar situaciones o casos de acuerdo con el tema al que se abocan. Es por ello que los intentos de intromisión, vigilancia, cateos e intervenciones de sus comunicaciones son recurrentes. La intercepción, censura y vigilancia no son nuevas, históricamente abundan los casos de personas DDH y periodistas que han sido blanco de ataques e intromisiones por la naturaleza del trabajo que realizan.

La Red en Defensa de los Derechos Digitales R3D, en su informe sobre Transparencia y vigilancia en México (2019), ha hecho énfasis en la evidencia que coloca a México como uno de los principales compradores de herramientas de vigilancia ofrecidas por empresas como NSO Group y Hacking Team, en especial de un *malware* de vigilancia ofrecido a gobiernos para combatir al crimen organizado y el terrorismo. Sin embargo, en el caso de México, se ha utilizado en contra de periodistas y defensores de derechos humanos (Red en Defensa de los Derechos Digitales 2019).

La privacidad y la seguridad digital

En el artículo 12 de la Declaración Universal de los Derechos Humanos se menciona a la letra que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Naciones Unidas, n.d.-b). Una lectura actual en el entorno digital de este derecho se contrapone por una realidad distópica en que la ubicuidad digital se torna en un ojo vigilante. Basta pensar en todos los datos que se generan a partir de las interacciones en la red, los sitios que se visitan, el tiempo que se consultan, los vínculos a los que se da clic, los datos personales que se registran para obtener un servicio, los gustos y las preferencias políticas, así como las redes de contactos. Estos son algunos de los elementos que ahora son fácilmente identificables e incluso monetizados. Es así como la vigilancia de datos a través del análisis de los datos de comunicaciones ha crecido de la mano de avances en los dispositivos de comunicación. Un elemento esencial en este escenario es el asunto de los metadatos, los cuales se han convertido en una mina que alimentamos todos los días y que han tenido un aumento proporcional en su generación, recopilación y análisis (Dwyer 2020).

En 2013, las filtraciones realizadas por Edward Snowden, entonces contratista de la Agencia Central de Inteligencia, revelaron que alrededor del 90 por ciento de las comunicaciones interceptadas eran de personas comunes y no de objetivos específicos (Oficina del Alto Comisionado para los Derechos Humanos (OACNUDH) 2018). Este evento es considerado como un catalizador que puso en primer plano el tema de la privacidad en la discusión sobre las implicaciones de la vigilancia moderna de las comunicaciones (Nyst y Falchetta 2017).

Como indica Ricci (2017, xii), la vigilancia gubernamental hacia individuos comunes de forma masiva por medio del acceso, la retención e intercepción de sus comunicaciones es una práctica cada vez más común entre los estados democráticos. Se debe considerar,

además, que resguardar el derecho a la privacidad es también una forma de proteger otros derechos relacionados como lo son el libre acceso a la información pública, la libertad de expresión y la libertad de asociación.

La privacidad y la seguridad son dos conceptos estrechamente unidos y complementarios, pues muchas de las estrategias y herramientas de seguridad incluyen ambos aspectos. Al hablar de la seguridad digital en personas DDH, entendemos que nos referimos a "un conjunto de prácticas relacionadas con la confidencialidad, integridad y disponibilidad de la información; prácticas que ayudan a las personas DDH a alcanzar sus objetivos y que encajan dentro de estrategias de seguridad más amplias en el trabajo de derechos humanos" (Kazansky 2015, 7). Se debe considerar que la seguridad digital es un campo que cambia rápidamente, como ocurre también con las propias tecnologías y su uso. Hasta hoy, los fundamentos conceptuales de la seguridad digital refieren al almacenamiento seguro de datos, la gestión de contraseñas, la elusión de la censura, el anonimato en línea y el uso seguro de dispositivos, sean computadoras o teléfonos (Dunn y Wilson 2013). Es así como la capacitación en el terreno de la seguridad para personas DDH puede verse como una forma de construir capacidades para lograr aminorar las vulnerabilidades a las que están expuestas.

En los últimos años, hay evidencia de la adquisición o contrato de mecanismos y programas informáticos para la vigilancia masiva de las comunicaciones por parte de distintos gobiernos en todo el mundo. Muchas de estas herramientas son utilizadas de forma discrecional sin regulación o control para la vigilancia de personas DDH, activistas y fracciones opositoras con el fin de intimidar y censurar (Fundación Acceso 2018, 5-6). Este escenario, la evolución de las tecnologías y el interés de utilizar los datos digitales para propósitos de vigilancia e intimidación hacen necesarios la difusión y sistematización de los esfuerzos que muchas organizaciones han impulsado para propiciar un entorno más seguro para las personas DDH.

A continuación se exponen algunas de las principales vulnerabilidades a las que están expuestas las personas DDH en el entorno

digital y se compila un conjunto de guías y manuales para reforzar su seguridad digital.

Principales vulnerabilidades

En este apartado se describen algunas de las amenazas digitales a las que están expuestas las personas DDH. Como se podrá apreciar, abunda el uso de tecnologías duales o de doble uso; es decir, aquellas tecnologías que son utilizadas originalmente para propósitos legítimos, pero que pueden utilizarse para socavar derechos humanos dependiendo de cómo se implementen (ver Anstis, Chan, Senft, y Deibert 2019). Por ejemplo, los metadatos que a menudo se utilizan para uso comercial pueden utilizarse para identificar patrones en los gustos, preferencias o filiaciones políticas. Lo mismo ocurre con los programas para la gestión de tráfico de red, los programas para filtrar información o los receptores IMSI, los cuales son programas que, bien empleados, son útiles para optimizar servicios, pero también pueden ser utilizados para conocer hábitos focalizados de una persona, bloquear contenido político u opositor e interceptar comunicaciones.

Uso inadecuado de metadatos

Una de las dimensiones de la privacidad es la información relativa a las actividades o los comportamientos en el uso de comunicaciones e intercambios de datos. Aspectos como la geolocalización, los registros de búsquedas, las interacciones con otras personas e instancias, los historiales de navegación, la duración y registro de llamadas telefónicas, la instalación de aplicaciones, entre otras, van conformando un conjunto de metadatos tan importantes y sensibles como el contenido de las propias comunicaciones. Tal como lo ha resaltado la Alta Comisionada de Derechos Humanos, el acceso a esta información de forma invasiva puede "incluso dar una mejor idea del comportamiento, las relaciones sociales, las

preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada" (Naciones Unidas-Consejo de Derechos Humanos 2014, 7).

Se habla, además, de numerosas pruebas de que los gobiernos recurren al sector privado para que realicen las actividades de vigilancia digital. "Gobiernos de todos los continentes han utilizado tanto mecanismos legales formales como métodos encubiertos para tener acceso a los contenidos, así como a los metadatos" (Naciones Unidas 2014).

El documento de los "Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones" (Electronic Frontier Foundation 2013) ha resaltado el papel de los Estados en las intenciones de acceder al contenido de las comunicaciones y a los metadatos sin que haya controles adecuados. Sumando además el poco nivel de protección que hay sobre los metadatos y las escasas restricciones para que los Estados los utilicen. En este punto no sólo hablamos de la intervención de comunicaciones, sino también de actividades como la cosecha de datos personales, el análisis, la interferencia, la gestión, la venta y la compra de información sensible. Para brindar elementos de seguridad a los DDH y a todo ciudadano, es necesario que los Estados garanticen y respeten la libertad de expresarse y no trastoquen la información o datos de carácter privado, ya sea de forma directa o con el uso de intermediarios.

Malware

El *software* malicioso denominado comúnmente *malware* es un "programa que es introducido en un sistema normalmente camuflajeado con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos de la víctima, aplicaciones o sistema operativo, o con el propósito de molestar o perturbar a la víctima" (Souppaya y Scarfone 2013). En el caso de México, se tiene documentado el uso de este tipo de herramientas para vigilar a personas DDH y periodistas entre 2015 y 2016 (ARTICLE 19, R3D y SocialTic 2017).

En 2016, Citizen Lab hizo público un informe que explica la forma en que opera Pegasus, un producto de la empresa israelí NSO Group cuya principal función es intervenir la comunicación de voz, texto e imagen de un teléfono móvil con fines de monitoreo (ARTICLE 19, R3D y SocialTic 2017). Esta herramienta maliciosa utiliza mensajes SMS con vínculos a un servidor que comprueba el modelo del teléfono y envía un *exploit* remoto (datos o secuencia de comandos que aprovechan una vulnerabilidad de seguridad) para el sistema operativo y de esta forma el dispositivo se infecta.

> Una vez infectado, un teléfono se convierte en un espía digital en el bolsillo de una víctima, totalmente bajo el control del operador. Un teléfono infectado se puede configurar para informar de todas las actividades en el dispositivo, desde mensajes y llamadas (incluso aquellos a través de aplicaciones de mensajería cifrada de extremo a extremo), a la grabación de audio y tomar fotos (Scott-Railton, Marczak, Razzak, Crete-Nishihata, y Deibert 2017)

En México, uno de los casos con mayor resonancia fue el del Centro de Derechos Humanos Miguel Agustín Pro Juárez, A. C. (Centro PRODH), una asociación sin fines de lucro cuyo propósito es promover y defender los derechos humanos de personas en situación de vulnerabilidad. En ese mismo año, tres personas de esta asociación recibieron mensajes de texto con intentos de infectar con el malware Pegasus sus dispositivos móviles. En el periodo en el que se presentaron los intentos de infección, estas personas estaban trabajando intensamente en la documentación y defensa de violaciones de derechos humanos vinculados con "la desaparición forzada de los 43 normalistas de Ayotzinapa, la ejecución extrajudicial de civiles por parte del ejército mexicano en el municipio de Tlatlaya, Estado de México; las sobrevivientes de tortura sexual durante el operativo de San Salvador Atenco en 2006 y la discusión de la Ley General contra la Tortura" (ARTICLE 19 *et al.* 2017).

Phishing o suplantación de identidad

El *phishing* es un *malware* que se vale de comunicaciones, aparentemente legítimas, que pueden recibirse por correo o por vía SMS y que remiten a los usuarios a vínculos o sitios fraudulentos en los cuales pueden solicitar información sensible como cuentas bancarias, direcciones o contraseñas que pueden comprometer su seguridad. Puede también activar una secuencia de comandos que vulneran el dispositivo desde el cual se accede pues habilita el robo de datos personales u organizacionales.

CitizenLab ha documentado el uso de un *software* de vigilancia de la compañía FinFisher, la cual se dedica a ofrecer programas de intrusión y vigilancia remota para agencias policiales y de inteligencia. Aunque su objetivo es el seguimiento de actividades delincuenciales, esta empresa y sus productos han sido utilizados en ataques perpetrados a activistas de derechos humanos. Un ejemplo es el caso de Etiopía, en el cual FinFisher, por medio de su *software* FinSpy, utilizó imágenes de un grupo de oposición etíope como gancho para infectar a un grupo de activistas. En México organizaciones como Sontusdatos han señalado el presunto uso de esta herramienta, por parte de la PGR, para espiar a activistas o personas disidentes al gobierno (Laguna y Laurant 2014). En conjunto, CitizenLab ha identificado servidores de esta empresa en los siguientes países: Australia, Baréin, Bangladesh, Brunéi, Canadá, República Checa, Estonia, Etiopía, Alemania, India, Indonesia, Japón, Letonia, Malasia, México, Mongolia, Países Bajos, Qatar, Serbia, Singapur, Turkmenistán, Emiratos Árabes Unidos, Reino Unido, Estados Unidos y Vietnam (Marquis-Boire *et al.* 2013).

La suplantación de identidad, como también se le conoce a esta práctica, no sólo se vincula con el espacio digital, también puede valerse de llamadas telefónicas, empleando un tono amigable e información previa sobre las personas a las que llaman. Su intención es obtener datos sensibles sobre la ubicación, prácticas y vínculos con otras personas (Hassan y Hijazi 2017). Esta práctica es conocida como una de las más "baratas y fáciles" (Front Line Defenders 2019). Otra forma de infectar un dispositivo es por medio de una

memoria USB que se deja de forma intencional cerca de la persona que interesa "infectar". Esto requiere un conocimiento de las prácticas y horarios de las personas. Cuando la víctima encuentra el USB y lo conecta a su dispositivo para verificar su contenido, queda infectado de forma inmediata (Rumsey 2016, 14).

IMSI CATCHERS

Los receptores IMSI, *stingrays* o falsas antenas, como popularmente se conocen, son receptores de telefonía que engañan a los dispositivos móviles con la finalidad de rastrear la ubicación de un teléfono móvil en tiempo real (Fundación Acceso 2015). Los IMSI catchers, llamados así por almacenar códigos IMSI vinculados con la tarjeta SIM de los teléfonos, permiten conocer el proveedor del servicio, la ubicación aproximada e incluso revelar el contenido de mensajes y llamadas (Protege.LA 2020). A decir de la Red en Defensa de los Derechos Digitales, este tipo de dispositivos son "altamente intrusivos y violatorios de las libertades y derechos civiles como la privacidad. Son utilizados con secrecía y sin una observancia o autorización judicial" (R3D: Red en Defensa de los Derechos Digitales 2016).

Recientemente, los periodistas de investigación Ricardo Balderas y Eduard Martín-Borregón describieron un proyecto de la organización South Lighthouse denominado Fake Antenna Detection, el cual monitoreó durante noventa días distintas ciudades latinoamericanas, entre ellas México, en busca de antenas falsas.

> Ciudad de México cuenta con 22 antenas sospechosas [...]. Hay antenas en dos de las principales salidas de la ciudad, ambas muy cerca de complejos militares, y presencia de varias antenas que cubren prácticamente el centro histórico de la ciudad. Dados los antecedentes de espionaje a periodistas y defensores de derechos humanos, durante el monitoreo, la organización local SeguDigital situó dispositivos para detectar antenas falsas en las principales redacciones de medios y oficinas de organizaciones sociales,

pero no se encontró ningún patrón al respecto" (Balderas y Martín-Borregón 2020).

Manuales y guías

Los manuales y las guías que aquí se compilan están dirigidos en su mayoría a proporcionar ayuda a personas u organizaciones orientadas al trabajo de personas DDH, o a personal que les brinda capacitación en el reforzamiento de seguridad digital. Ofrece consejos prácticos para un uso seguro de dispositivos con consejos particulares para cada sistema operativo sobre cifrado, contraseñas, protección y resguardo de información; navegación segura, así como guías para realizar un análisis sistemático de su seguridad integral. Todos son de acceso abierto y se brinda información sobre la institución que lo respalda y el vínculo para su consulta.

Manual de seguridad y privacidad digital para los defensores de los derechos humanos

Este documento, elaborado por Vitaliev, tiene como propósito "informar a los usuarios de ordenadores comunes y ofrecerles soluciones a los problemas de privacidad y seguridad que pueden surgir en un entorno digital moderno" (Vitaliev 2009, 1). Es también una introducción a la seguridad digital, sus riesgos y la forma de abordarlos. Su estructura abarca temas como la evaluación de amenazas y el círculo de seguridad; la seguridad de Windows; copia de seguridad, destrucción y recuperación de la información; la vigilancia en Internet; cifrado en Internet; esteganografía; *software* malicioso; cómo generar una contraseña segura; casos prácticos, entro otros temas. Está disponible en: https://protege.la/seguridad-y-privacidad-digital-para-los-defensores-de-los-derechos-humanos/. Elaborado por Front Line Defenders.

Autoprotección digital contra la vigilancia: consejos, herramientas y guías para tener comunicaciones más seguras

Esta página ofrece un conjunto de guías avanzadas para protegerse del espionaje en línea. Parte de sus contenidos están orientados a personas con pocos conocimientos técnicos y otros a personas con mayores conocimientos en privacidad y seguridad digital. Parten de un modelo de amenaza que hace énfasis en el tipo de personas o grupos que desean obtener datos personales; tener claridad sobre los posibles propósitos de su uso, y la forma en que pueden conseguirlos. Para ello se plantean distintos escenarios de posibles ataques y a partir de ello se establece un análisis de riesgos. Otro de sus propósitos es conjuntar herramientas y prácticas sofisticadas para hacer frente a la evolución de los riesgos a la privacidad y seguridad en la red. Algunos de los temas que cubre son: por qué los metadatos son importantes; cómo crear una contraseña segura; proteger tu dispositivo de *hackers*; usar gestores de contraseñas; cifrar comunicaciones; mantener datos seguros; cómo evitar los ataques de phishing o suplantación de identidad; cómo borrar de forma segura información en distintos sistemas operativos; cómo esquivar la censura en línea. Está disponible en https://ssd.eff.org/es. Elaborada por: Electronic Frontier Foundation.

Manual para facilitadores sobre diagnósticos en seguridad digital para organizaciones defensoras de derechos humanos

Este manual está dirigido a facilitadores, talleristas y expertos que trabajan con organizaciones sociales. Ofrece un programa detallado de formación con actividades colectivas de intervención. Toma en consideración el contexto político, regional, nacional y local de las organizaciones, así como los actores y la información sensible que producen y resguardan. Incorpora mejores prácticas en

el uso de herramientas de seguridad digital, así como guías para realizar un análisis del entorno físico de las organizaciones. También incluye una guía para evaluar el trabajo con los archivos y realizar un análisis de amenazas a la información. Por último, ofrece recomendaciones para la elaboración de un informe final para la organización y un listado de recursos útiles. Está disponible en https://gendersec.tacticaltech.org/wiki/index.php/Diagn%C3%B3sticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitadores#Presentando_el_manual. Elaborado por Tacticaltech.

Research and writing conducted by the engine room to inform the levelup project's support of digital security trainers

Este manual para capacitadores en seguridad digital es el resultado de entrevistas y un gran número de recomendaciones para mejorar el diseño de cursos orientados a personas en alto riesgo. Busca atender el apoyo sostenido para formadores de seguridad digital. La creación de marcos estandarizados para los capacitadores en este rubro y mejorar los enfoques pedagógicos empleados en este tipo de capacitaciones. Uno de sus objetivos es apoyar el desarrollo de capacidades en personas DDH para hacer frente a las amenazas digitales.

Está disponible en https://internews.org/sites/default/files/resources/InternewsWPDigitalSecurity_2013-11-29.pdf. Elaborado por Internews.

Manual sobre seguridad: pasos prácticos para defensores/as de derechos humanos en riesgo

Este manual fue desarrollado a partir de la experiencia de impartir talleres sobre seguridad y protección en más de cincuenta

países. Conjunta la experiencia de especialistas en seguridad y contribuciones de los propios participantes. Brinda información para desarrollar un plan de seguridad para las personas DDH que trabajan en organizaciones afines. Ayuda a evaluar de forma sistemática la situación de seguridad que se requiere y el desarrollo de estrategias para reducir las situaciones de vulnerabilidad. Parte de sus contenidos son:

- Análisis de amenazas y riesgos.
- Seguridad en ordenadores y teléfonos.
- Tecnología y metodología de la vigilancia.
- Bienestar y estrés.
- Creación de planes de seguridad.
- Comprensión del contexto propio.

Está disponible en https://www.frontlinedefenders.org/es/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk. Desarrollado por FrontLine Defenders.

PLANIFICADOR DE SEGURIDAD

Se trata de un recurso elaborado por expertos para mantener la seguridad en línea cuyo contenido está orientado a usuarios promedio que necesiten implementar de forma rápida algunas medidas para reforzar la seguridad de sus comunicaciones en Internet. Las preocupaciones que motivaron este proyecto son: proporcionar consejos confiables y creíbles; brindar un asesoramiento personalizado, amigable y actualizado. Los contenidos que ofrece este planificador se dividen en cuatro apartados:

Navegación segura:

- Instalación de un navegador Tor.
- Instalación de Chrome y FireFox.
- Instalar Privacy Badger para evitar que determinados sitios recopilen información del usuario.

Asegurar el equipo de cómputo:

- Protección de datos de Windows con el cifrado del dispositivo.
- Actualización constante en Windows y Mac.
- Cifrado en equipos Mac.
- Uso de antivirus integrado de Windows.
- Copia de seguridad de Mac y Windows.

Protección de cuentas en línea:

- Comprobación de la seguridad de una cuenta.
- Detección de sitios y mensajes malintencionados.
- Autentificación en dos pasos.
- Administrador de contraseñas.
- Configuración de la privacidad.

Asegurar la conexión a Internet:

- Usar el cortafuegos en Mac y Windows.
- Uso de una red privada VPN.

Mantener los datos del teléfono seguros:

- Enviar mensajes con Signal.
- Copia de seguridad de iPhone y Android.
- Uso de la función buscar mi iPhone y Buscar mi Android.
- Cifrado de iPhone y Android.
- Uso de aplicaciones seguras.

Recursos que proporcionan asistencia adicional:

- Apoyo de emergencia.
- Información para usuarios de alto riesgo.
- Guías avanzadas de anonimato y seguridad.
- Informes de transparencia.

Está disponible en https://securityplanner.org/#/. Elaborado por: CitizenLab.

MANUAL DE SEGURIDAD HOLÍSTICA

Se trata de un manual de estrategias global para personas, colectivos u organizaciones defensoras de Derechos Humanos orientado a la seguridad digital y a la seguridad de su información. Considera el contexto personal y de género e integra de forma holística y relacional aspectos de seguridad digital, bienestar psicosocial y seguridad organizacional. Se divide en cuatro secciones:

Preparar: en esta etapa se reconocen las medidas de seguridad que cada persona toma, las estrategias que emplean los participantes para la salud y el bienestar, sus creencias personales, sus fuentes de resiliencia y sus respuestas ante amenazas y peligros.

Explorar: a partir del reconocimiento del contexto y la ubicación de amenazas específicas derivadas del trabajo que realizan los participantes y sus retractores, se realizan algunas acciones para identificar y catalogar la información de los participantes, identificar sus hábitos para resguardar su información, analizar quiénes tienen acceso a estos datos e identificar la mejor forma de protegerlos.

También se analizan los flujos de la información dinámica o en movimiento; esto es, las distintas transacciones que se realizan por medio de llamadas telefónicas, correos, mensajes de voz, mensajería instantánea, servicios en la nube, descargas o navegando en Internet para mostrar que en muchos casos estos canales no están diseñados para proteger la información de la vigilancia, considerando que el contenido de estas comunicaciones está ligado al trabajo que realizan sobre derechos humanos.

Se analizan también las propiedades de la información digital en términos de replicación: distintas versiones de un documento al modificar, enviar o guardar; permanencia de la información: el riesgo de que la información sea retenida en servicios de carga y descarga; metadatos: datos sobre la información, los procesos y tratamientos, archivos y dispositivos que en su conjunto son sensibles y pueden revelar información sobre patrones movilidad y comportamiento, entre otros.

Desarrollar estrategias: este apartado se aboca al desarrollo de estrategias para contrarrestar las amenazas identificadas y asegurar la seguridad de los participantes durante su accionar. Se brindan elementos para crear un plan de seguridad cuyos propósitos son la prevención de amenazas y la disminución del impacto de éstas por medio de un plan de contingencia.

Se trata además la planificación de la seguridad a partir de la dinámica en grupos y organizaciones. Se definen funciones y responsabilidades en casos de emergencia, así como canales de comunicación. Por último, se realiza un análisis de eventos y se define cómo mejorar las estrategias de prevención y respuestas a amenazas futuras.

Actuar: en este apartado se detallan habilidades, mejores prácticas y recursos útiles para aumentar la seguridad en actividades propias de las personas DDH. Además, se ofrece una pequeña guía sobre el ejercicio del derecho a la libertad de asociación orientado al tema de protestas y manifestaciones, desde su preparación, realización y seguimiento. Se habla de la creación de grupos de afinidad; es decir, un grupo que opere como una unidad para participar en las protestas juntos con roles y responsabilidades en casos de emergencia.

Además, se muestran estrategias para gestionar el bienestar de los participantes en relación con su trabajo frente a amenazas como el trauma, el cinismo y el agotamiento. Por último, se incluyen recomendaciones para construir un movimiento inclusivo y un conjunto de ejercicios para los participantes que ayudan a obtener una mejor perspectiva de su situación de seguridad general a nivel personal y organizacional; un apartado de organizaciones que brindan apoyo para personas DDH; un conjunto de recursos adicionales, y un manual para facilitadores. Está disponible en https://tacticaltech.org/#/projects/holistic-security. Elaborado por Tacticaltech.

SECURITY IN A BOX

Como su nombre lo indica, esta guía básica ofrece tácticas para el uso seguro de dispositivos móviles y redes sociales de activistas y personas DDH, así como una guía de herramientas con pasos a seguir para el uso de programas y servicios de seguridad digital. Incluye también un conjunto de guías comunitarias para personas que son blanco de amenazas digitales en el que se ofrecen recursos de acuerdo con las necesidades de grupos específicos. La guía está estructurada a partir de tácticas generales y recomendaciones por tipo de sistema operativo. Cada rubro se detalla de una forma clara y concisa.

Tácticas generales:

- Proteger los dispositivos de *malware* y ataques de *phishing*.
- Proteger la información de amenazas físicas.
- Crear y mantener contraseñas fuertes.
- Mantener comunicaciones privadas.
- Permanecer anónimo y eludir la censura en Internet.
- Usar teléfonos inteligentes de forma segura.

Linux y Windows

- Administradores de contraseñas.
- Almacenamiento seguro de archivos.
- Navegación web segura.
- Correo electrónico seguro.
- Anonimato en línea y evasión de censura.

Android

- Configuración básica de seguridad.
- Comunicación segura.

Web

- Uso seguro de redes sociales.
- Correo encriptado.

Está disponible en https://securityinabox.org/es/. Elaborado por Front Line Defenders y Tactical Technology Collective.

Kit de primeros auxilios digitales

Se trata de un material de referencia que ofrece respuestas rápidas y concisas a entrenadores en seguridad digital y activistas para mejorar su autoprotección y la de su comunidad en este rubro. Está pensado también para personas DDH, blogueros, periodistas y personas interesadas en ayudar a otros. El propósito de este recurso es diagnosticar los problemas de seguridad digital que experimentan y los remite a los proveedores de soporte adecuado. Consta de nueve apartados vinculados con problemas comunes de seguridad digital, cada uno incluye preguntas que ayudan a diagnosticar mejor el problema experimentado y recursos que servirán de ayuda.

1. Perdí mi dispositivo.
2. Perdí acceso a mis cuentas.
3. Mi dispositivo está actuando de forma sospechosa.
4. He recibido mensajes sospechosos.
5. Mi sitio web no está funcionando.
6. Alguien me está suplantando en Internet.
7. Estoy siendo acosada o acosado en línea.
8. Perdí mi información.
9. Alguien que conozco ha sido arrestado o arrestada.

Incluye además una página con vínculos a otras organizaciones que brindan apoyo. Está disponible en https://digitalfirstaid.org/es/. Elaborado por Computer Incident Response Center for Civil Society (CIVICERT).

Línea de ayuda de seguridad digital

Ofrece prácticas de seguridad digital para personas y organizaciones, así como asistencia técnica directa y en tiempo real a personas DDH, periodistas, blogueros y medios de comunicación. La línea brinda asesoría para realizar una evaluación de los riesgos a

partir de la labor que desarrollan, ayuda a identificar prioridades de seguridad digital y brinda apoyo para resolver los problemas identificados. Organiza clínicas de seguridad digital en las que participan personas de alto riesgo para exponer sus problemas y recibir asistencia experta para resolver los problemas que enfrentan en relación con su seguridad digital. Las áreas más comunes en que apoya la línea de ayuda son:

- Modelado de amenazas y análisis de riesgos
  - Asesoría en seguridad digital.
  - Asistencia en seguridad organizacional.
  - Recomendaciones de seguridad al viajar.

- Comunicaciones seguras
  - Seguridad en el uso del correo electrónico y servicios de mensajería.
  - Seguridad en el uso de dispositivos móviles.
  - Seguridad en llamadas de voz o video.

- Seguridad de almacenamiento de archivos
  - Almacenamiento de información sensible.
  - Borrado seguro.
  - Estrategias de respaldo.

- Vulnerabilidades y *malware*
  - Vulnerabilidades.
  - *Malware.*
  - Análisis y contención de *phising/malware.*

- Seguridad de acceso
  - Creación y administración de contraseñas.
  - Autenticación multifactor.

- Navegación web
  - Navegación segura.

- Seguridad en redes sociales
  - Privacidad y seguridad en redes sociales.
  - Recuperación de cuentas.

- Anonimato y censura
  - Anonimato.
  - Evasión de censura.
  - Apagones.
  - Prevención y reacción de ataques.
  - Reportes de dominios falsos.

Está disponible en https://www.accessnow.org/help/. Elaborado por Access Now.

Organizaciones

La mayor parte de las organizaciones que aquí se describen ofrecen servicios y recursos de protección y asesoría para personas DDH, activistas, blogueros y organizaciones de la sociedad civil. En su mayoría ofrecen guías y manuales disponibles en distintos idiomas.

Protege.la

Se presenta como un "espacio abierto para compartir recursos sobre seguridad y privacidad digital". A partir de un lenguaje claro, con ejemplos ilustrativos y bien estructurados. Ofrece pequeñas guías sobre hábitos básicos de seguridad digital; protección de cuentas en Internet; manejo de agresiones y ataques en línea; comunicaciones seguras; encriptación de archivos; gestión de riesgo en la seguridad informática; manuales de seguridad digital para mujeres; un manual para facilitadores sobre diagnósticos en seguridad digital para organizaciones defensoras de derechos humanos; listas de verificación para equipos de cómputo, móviles

y servicios en línea, así como un conjunto de herramientas útiles para gestionar contraseñas, cifrar mensajes de texto y monitorear posibles filtraciones de datos. Disponible en https://protege.la/.

CITIZENLAB

Citizen Lab se presenta como "un laboratorio interdisciplinario [...] enfocado en la investigación, desarrollo, y políticas estratégicas de alto nivel e involucramiento legal en la intersección entre tecnologías de la información y comunicación, derechos humanos y seguridad global". Parte de su agenda se orienta a documentar el uso de tecnologías y prácticas que afecten la libertad de expresión en línea, así como analizar la privacidad, la seguridad y los mecanismos de rendición de cuentas en relación con los datos personales y actividades de vigilancia. Trabajan de cerca en la asesoría y el acompañamiento de personas de alta amenaza como periodistas y personas DDH. Además de ello, ha trabajado en el diseño y difusión de herramientas y recursos educativos para navegar de forma segura en Internet. Entre estos esfuerzos, resalta la página de Net Alert cuyo propósito es hacer asequible para el público en general, en distintos idiomas, algunas estrategias para protegerse de los ataques más comunes en línea. En el caso de la versión en español, se brinda información sobre la comunicación privada en Internet, la importancia de la mensajería privada y la importancia del cifrado de extremo a extremo, así como un conjunto de recursos que guían a las personas interesadas a proteger sus cuentas digitales y mantener siempre el control de éstas. Abunda en ejemplos de *phishing* y muestra los procedimientos para habilitar la verificación en dos pasos para reforzar la seguridad de las cuentas personales en Internet. Dsiponible en https://citizenlab.ca.

TACTICALTECH

Se trata de una organización fundada en 2003 que busca contribuir a una sociedad más equitativa, democrática y sostenible.

Pone en el centro de este cambio a las tecnologías digitales y la forma en que afectan a la sociedad y a los ciudadanos. Describen cómo surgen los problemas, exploran respuestas e implementan estrategias sostenibles. Dan salida a productos creativos orientados a desmitificar la tecnología y a crear prácticas seguras e informadas con respecto al uso de tecnologías digitales. Utilizan una metodología iterativa que da salida a productos e intervenciones relevantes y accesibles para su audiencia.

Los grupos en los que se enfoca esta organización son el público en general en torno a temas de privacidad y autonomía en línea, así como con periodistas y personas DDH en relación con el trabajo con datos y políticas sobre los usos de la tecnología en las democracias de todo el mundo. Está disponible en https://tacticaltech.org/#/.

SOCIALTIC

Se trata de una organización multidisciplinaria sin fines de lucro cuyo propósito es la formación, el acompañamiento y la promoción de la tecnología para su uso social. Parte de su visión es brindar entrenamiento en el uso de tecnologías digitales para propiciar el cambio social y apoyar en requerimientos de seguridad y privacidad digital. Trabajan de forma directa con organizaciones, grupos e individuos que buscan resolver problemas de carácter social y construir mejores condiciones de vida ya sean activistas, periodistas, investigadores, tecnólogos y personas que viven bajo riesgo en su contexto digital. Cuentan con un apartado para herramientas en relación con la seguridad y privacidad digital y otros temas como datos, gestión del trabajo, infoactivismo y recursos abiertos.

A partir de la necesidad identificada por el mecanismo de Protección Integral de Personas Defensoras de Derechos Humanos y Periodistas de la Ciudad de México, de atender las necesidades de formación de personas DDH y periodistas en relación con la seguridad digital, agruparon de forma conjunta una serie de herramientas para cuidados digitales que atendieran las necesidades

particulares de estos grupos, promoviendo hábitos de seguridad y prevención de riesgos en el entorno digital. Está disponible en https://socialtic.org/.

DIGITAL DEFENDERS PARTNERSHIP

Se trata de una asociación orientada a la protección de usuarios críticos de Internet, entre los que se suman las personas DDH, activistas, blogueros, organizaciones de la sociedad civil, periodistas, entre otros. Incorpora una perspectiva de igualdad de género en sus programas y actividades, considerando que las amenazas pueden ser diferenciadas a partir del contexto de las personas. Su principal causa es que Internet sea abierta, libre de amenazas a la libertad de expresión, a la asociación, la privacidad en contextos represivos y de transición.

Trabajan principalmente con:

- Personas que recolectan datos para públicos más amplios.
- Personas que defienden el medio ambiente, los pueblos originarios y territorios.
- Comunidades LGBTQI+ y quienes promocionan y defienden sus derechos.
- Personas y grupos que defienden los derechos de mujeres y de género

Está disponible en https://www.digitaldefenders.org.

CIVICERT

Computer Incident Response Center for Civil Society es una iniciativa de RaReNet (Rapid Response Network), una red de organizaciones orientadas a mejorar la seguridad de la sociedad civil que busca atender emergencias informáticas y ayudar a la sociedad civil a prevenir y abordar los problemas de seguridad digital. Son miembros de esta red:

- Accessnow
- Fundación Acceso
- Amnistia Internacional
- Center for Digital Resilent
- Co-Creation Hub
- DefendDefenders (África)
- Deflect
- Digital Defenders Partnership
- Digital Rights Foundation
- Digital Security Lab
- Freedom of the Press Foundation
- FrontLine Defenders
- Greenhost
- Human Rights Watch
- Internews
- Fundación Karisma
- Mido
- Media Diversity Institute
- Qurium
- TibTert
- ShareCert

Está disponible en https://www.civicert.org/.

Access now

Trabaja en la defensa y ampliación de los derechos digitales de los usuarios en alto riesgo en todo el mundo. Busca servir, influir, asesorar a los tomadores de decisión en relación con derechos humanos y el análisis de políticas. Cuenta con una línea de atención en tiempo real para personas en alto riesgo. Atienden cinco áreas sustanciales:

- Privacidad.
- Libertad de expresión.
- Seguridad digital.

- Negocios y derechos humanos.
- Discriminación en la red.

Está disponible en https://www.accessnow.org/.

Front line defenders

El principal objetivo de esta organización es proteger, defender, apoyar y actuar a favor de las personas DDH por medio de la incidencia en el plano internacional, ayuda en situaciones de emergencia, subvenciones para cubrir gastos de necesidades prácticas en materia de seguridad, capacitación y recursos materiales sobre seguridad y protección digital, así como una línea telefónica de emergencia 24/7 disponible en distintos idiomas. Ofrece herramientas y talleres sobre:

- Análisis de riesgo y planificación de seguridad.
- Seguridad digital.

Está disponible en https://www.frontlinedefenders.org/.

Internews

Esta asociación trabaja principalmente con medios de comunicación, pero también atiende el objetivo de generar entornos de información saludables por medio del reforzamiento de habilidades de personas DDH, activistas, profesionales de los medios de comunicación y ciudadanos, en temas como seguridad digital y el acceso a Internet abierta, segura y sin censura. Cuenta con una red de entrenadores en seguridad digital, apoya y asesora de forma directa a otras organizaciones de la sociedad civil con propósitos afines. Está disponible en
https://internews.org/.

Fundación acceso

Conformada por un equipo interdisciplinario, esta fundación tiene como propósito mitigar la violación de derechos asociados a la seguridad física, tecnológica y psicosocial en situación de vulnerabilidad. Trabaja en el desarrollo de soluciones tecnológicas para la promoción y defensa de derechos, así como en la apropiación de prácticas y conocimientos para empoderar a poblaciones que lo requieran. Ofrecen alternativas de protección integral a poblaciones en riesgo con las que trabajan. Centran su trabajo en tres áreas:

- Alternativas de protección integral.
- Área de innovación y desarrollo.
- Apropiación de prácticas y conocimientos.

Cada año publican el informe anual del Observatorio Centroamericano de Seguridad Digital con la finalidad de registrar y analizar incidentes de seguridad digital reportados por personas DDH que trabajan en Centroamérica. Está disponible en https://acceso.or.cr/.

Medidas de seguridad

A continuación, se compilan algunas de las principales estrategias que se han empleado para hacer frente a estas vulnerabilidades en el terreno de las personas DDH.

A nivel estructural

- Difusión y formación en el uso de herramientas específicas de software de seguridad digital, particularmente comunidades de *software* libre, libre y de código abierto (Hankey y ´O Clunaigh 2013).
- Trabajo en el desarrollo de políticas e investigación: investigación sobre vulnerabilidades específicas que enfrentan las personas DDH y las políticas relacionadas ejerciendo presión sobre el trabajo con gobiernos, reguladores, proveedores de servicios y plataformas (Hankey y ´O Clunaigh 2013).

- Desarrollo de capacidades: el desarrollo de herramientas y guías de sensibilización y desarrollo de habilidades para personas DDH y capacitación en seguridad digital (Hankey y ´O Clunaigh 2013).
- Autores como Caster (2017) sugieren la creación de grupos locales de retroalimentación que generen guías de seguridad digital y diseñen estrategias de asesoramiento participativo para el apoyo institucional.
- No pensar en una estrategia centrada en la tecnología ni asumir que el asesoramiento técnico resuelve por completo la seguridad de la comunicación. Frente a una amenaza física, es muy probable que las personas DDH entreguen sus credenciales de acceso a información sensible. Por ello, se recomienda un enfoque más integral sobre la seguridad digital (Caster 2017).
- Centrar las prácticas de protección en una concepción holística de la seguridad que cubra aspectos como la seguridad económica, política, ambiental y digital, además del bienestar psicosocial (Naciones Unidas, Consejo de Derechos Humanos 2016).

A nivel personal:

- Alentar a las personas DDH a integrar consideraciones de seguridad en su labor y atender de forma sistemática sus necesidades de protección. En muchas ocasiones, pasan por alto que pueden ser blanco de un ataque y otros asumen que los riesgos son inherentes a su trabajo y poco se puede hacer para afrontarlos (Naciones Unidas, Consejo de Derechos Humanos 2016).
- Cuando las personas DDH trabajan en equipo, se recomienda planificar la gestión colectiva de su seguridad, estableciendo políticas y protocolos organizativos (Naciones Unidas, Consejo de Derechos Humanos 2016).
- Se recomienda el uso de cuentas de correo electrónico exclusivas para su trabajo como DDH y mantener una política de buzón de entrada vacío; es decir, borrar siempre el

contenido, ya sea de forma manual o automática como la ofrecida por Protonmail y, en el caso de comunicaciones, por chat el uso de Signal o Telegram (Caster 2017).
- Se recomienda borrar adecuadamente los archivos que se utiliza. Se advierte que incluso al borrar archivos cifrados se puede acceder a ellos mediante programas de recuperación (Caster 2017).
- Se recomienda emplear una estrategia de navegador dual que consiste en utilizar un navegador para su trabajo relacionado con la defensa de los derechos y otro para fines de entretenimiento en el que se puedan guardar las contraseñas no sensibles (Caster 2017).
- Se recomienda mantener la computadora y USB con poca información y realizar respaldos periódicos de la información para guardar fuera de su oficina o casa (Comisión Mexicana de Defensa y Promoción de los Derechos Humanos A.C. 2011).

Conclusiones

Como hemos observado, hay notables desventajas entre los DDH en relación con los recursos que se pueden emplear para acceder a su información confidencial, a redes de contactos, conocer hábitos y rutinas. Esta situación asimétrica en la que se coloca a los DDH se acentúa cuando "se accede por la puerta de atrás a los sistemas, dispositivos y plataformas que utilizan" (Hankey y ´O Clunaigh 2013, 538). Es así que la ubiquidad del entorno digital se torna en una oportunidad y amenaza de forma simultánea, pues se cuenta con un amplio rango de canales para comunicar y ampliar una demanda o establecer redes, pero también se compromete el entorno de lo privado y se resta control sobre los datos que se generan.

El carácter evolutivo de las tecnologías de comunicación hace difícil la tarea de actualizarse frente a nuevas amenazas; por ello es importante alentar el trabajo de los facilitadores en la formación

de seguridad digital, profundizar en el conocimiento del contexto de las personas DDH en riesgo, así como promover el uso y regulación de herramientas y servicios de cifrado. Legislar sobre estas herramientas es clave para garantizar derechos asociados con la libertad de expresión y el derecho a la privacidad. En ese sentido, se deben buscar las formas de no socavar el cifrado y evitar disposiciones que busquen eliminar la protección de datos personales o confidenciales.

El reto para las sociedades modernas es construir los mecanismos para mantener a raya cualquier intento de intromisión en los datos privados y permanecer atentos al uso y legislación de tecnologías aplicadas a la vigilancia específica o masiva. Considerando el amplio rango de amenazas que representa el uso indebido de tecnologías, cabe preguntarse sobre la regulación de empresas que, bajo la cortina de ofrecer herramientas para la seguridad nacional, ofrecen herramientas potencialmente ofensivas no solo para las personas DDH, sino también para los ciudadanos en general. Por ello es importante que los gobiernos empleen reglas claras para el acceso a estos datos que respeten los aspectos de necesidad, idoneidad y proporcionalidad, y dejen en claro cuándo o en qué casos se permite el acopio de estos datos para un objetivo legítimo. Velar por la seguridad digital de las personas DDH es también velar por nuestros propios derechos como ciudadanas y ciudadanos.

Bibliografía

Anstis, S., Chan, S., Senft, A., y Deibert, R.J. (2019). *Annotated bibliography Dual-use technologies: Network traffic management and device intrusion for targeted monitoring.* University of Toronto. Munk School. Disponible en https://citizenlab.ca/2019/09/annotated-bibliography-dual-use-technologies-network-traffic-management-and-device-intrusion-for-targeted-monitoring/

Article 19, R3D, y SocialTIC. (2017). "Gobierno espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México". Disponible en https://articulo19.org/wp-content/uploads/2017/06/Reporte-Gobierno-Espía-Final.pdf

Balderas, R., y Martín-Borregón, E. (2020, 31 de mayo). Datos y llamadas de celulares, en riesgo de espionaje por antenas falsas en América Latina. *The Washington Post*. Disponible en https://www.washingtonpost.com/es/post-opinion/2020/05/31/datos-y-llamadas-de-celulares-en-riesgo-de-espionaje-por-antenas-falsas-en-america-latina/

Caster, M. (2017). To strengthen digital security for human rights defenders, behavior matters. *OpenDemocracy*. Disponible en https://www.opendemocracy.net/michael-caster/to-strengthen-digital-security-for-human-rights-defenders-behavior-matters.

Comisión Mexicana de Defensa y Promoción de los Derechos Humanos. (2011). *El derecho a defender los derechos humanos en México*. Disponbile en www.cmdpdh.org

Comisión Nacional de los Derechos Humanos. (2011). El derecho a defender: informe especial sobre la situación de las y los defensores de los derechos humanos en México. CNDH. Disponible en https://www.cndh.org.mx/sites/default/files/doc/Informes/Especiales/2011_julio_defensores.pdf.

Dunn, A. y Wilson, C. (2013). *Training digital security trainers: A preliminary review of methods, needs, and challenges*. Internews Center for Innovation & Learning. Disponible en https://internews.org/sites/default/files/resources/InternewsWPDigitalSecurity_2013-11-29.pdf

Dwyer, T. (2020). Privacy from your mobile devices? En Ling, R., Fortunati, L., Goggin, G., Lim, S.S. y Li, Y. *The Oxford Handbook of Mobile Communication and Society* (546-462). Oxford University Press. Disponible en https://doi.org/10.1093/oxfordhb/9780190864385.013.36

Electronic Frontier Foundation. (2013). *Necesarios & Proporcionados: sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones*. EFF. Disponible en https://necessaryandproportionate.org/es/

Front Line Defenders. (2020). *Global Analysis 2019*. Front Line Defenders. https://www.frontlinedefenders.org/sites/default/files/global_analysis_2019_web.pdf

———. (2019). *Análisis global de Front Line defenders 2019*. Front Line Defenders. https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2018

Fundación Acceso. (2018). *Observatorio Centroamericano de seguridad digital informe anual 2018.* Fundación Acceso. https://acceso.or.cr/assets/files/Informe_OSD_2018_espan%CC%83ol.pdf

———. (2015) *Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensor*. Fundación Acceso. Disponible en https://necessaryandproportionate.org/files/Investigacion-Privacidad-Digital-FA.pdf

Hankey, S. y Ó Clunaigh, D. (2013). Rethinking risk and security of human rights. *Journal of Human Rights Practice*, 5(3), 535–547.

Hassan, N. A., y Hijazi, R. (2017). Essential Privacy Tips. En *Digital privacy and security using Windows: a practical guide* (pp. 33–102). Springer. Disponible en https://doi.org/10.1007/978-1-4842-2799-2

Kazansky, B. (2015). *Digital Security in Context: Learning how human rights defenders adopt digital security practices*. Tactical Technology Collective. Disponible en https://cdn.ttc.io/s/secresearch.tacticaltech.org/pages/pdfs/original/DigitalSecurityInContext.pdf

Laguna, M. y Laurant, C. (2014). "El caso 'FinFisher': una historia de espionaje en México". Artículo 12, A.C. Disponible en https://sontusdatos.org/2014/09/09/el_caso_finfisher_historia_de_espionaje_en_mexico/

Marquis-Boire, M., Marczak, B., Guarnieri, C., y Scott-Railton, J. (2013). *You only click twice: FinFisher's global proliferation*.

University of Toronto. Munk School. Disponible en https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Naciones Unidas. Consejo de Derechos Humanos. (2016*).* Informe del relator especial sobre la situación de los defensores de los derechos humanos. A/HRC/31/55. Naciones Unidas. Disponible en https://doi.org/10.18268/bsgm1908v4n1x1

_———. (2014). El derecho a la privacidad en la era digital: informe de la Oficina del Alto Comisionado de los Derechos Humanos. Disponible en https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc

———. (s.f. a). Sobre los defensores de los derechos humanos. Oficina del Alto Comisionado de las Naciones Unidas para Derechos Humanos. Disponible en https://www.ohchr.org/SP/Issues/SRHRDefenders/Pages/Defender.aspx

———. (s.f.b). *La Declaración Universal de los Derechos Humanos: Artículo 12.* Fundación Internacional de los Derechos Humanos. Disponible en https://dudh.es/12/

Neto, U.T. (2017). *Protecting human rights defenders in Latin America: a legal and socio-political analysis of Brazil*. Springer.

Nyst, C., y Falchetta, T. (2017). The right to privacy in the digital age. *Journal of Human Rights Practice.* 9(1), 104-118. Disponible en https://doi.org/10.1093/jhuman/huw026

Protege.LA. (2020, 8 de junio). "¿Qué son y cómo funcionan los IMSI Catcher?" [Blog]. Protege.LA. Disponible en https://protege.la/que-son-y-como-funcionan-los-imsi-catcher/

Ricci, D.G. (2017). *The contribution of international human rights law to the protection of privacy : the case of Mexico*. [Tesis de doctorado, University of Toronto. Faculty of Law]. TSpace Repository. https://tspace.library.utoronto.ca/handle/1807/78987?mode=full

Rumsey, M. J. (2016). Cybersecurity: Challenging rhetoric to identify the future of defensive and offensive measures against defined threat actors. Tesis de maestría, San Diego State Uni-

versity. Disponible en https://search.proquest.com/docview/1833179701?accountid=26652%0Ahttp://link.periodicos.capes.gov.br/sfxlcl41?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&genre=dissertations+%26+theses&sid=ProQ:Military+Database&atitle=&title=Cyberse

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M. y Deibert, R. (2017*). Reckless Exploit: Mexican journalists, lawyers, and a child targeted with NSO Spyware*. University or Toronto. Munk School. Disponible en https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

Vitaliev, D. (2009). *Seguridad y privacidad digital para los defensores de derechos humanos.* Front Line. Disponible en https://www.frontlinedefenders.org/es/resource-publication/digital-security-privacy-human-rights-defenders

R3D Red en Defensa de los Derechos Digitales. (2019). "Transparencia y vigilancia en México: lo que no sabemos sobre lo que el gobierno sabe de nosotros". R3D. Disponible enhttp://www.usuariosdigitales.org/2018/08/06/transparencia-y-vigilancia-en-mexico-lo-que-no-sabemos-sobre-lo-que-el-gobierno-sabe-de-nosotros/

——. (2016). "5 datos que debes saber sobre los IMSI catchers o stingrays". R3D. Disponible en https://r3d.mx/2016/06/20/5-datos-que-debes-saber-sobre-los-imsi-catchers-o-stingrays/

Vulnerabilidad, inclusión y seguridad digital en México. Instituto de Investigaciones Bibliotecológicas y de la Información/UNAM. La edición consta de 100 ejemplares. Coordinación editorial, Anabel Olivares Chávez; revisión especializada, Valeria Guzmán González; corrección de pruebas, Carlos Ceballos Sosa; revisión de pruebas, Valeria Guzmán González; formación editorial, Sonia Wendy Chávez Nolasco. Fue impreso en papel cultural de 90 gr en los talleres de Servicios Editoriales Albatros, Av. Benito Juárez M 26 L 14, Colonia El Molino Tezonco, Ciudad de México. Se terminó de imprimir en octubre de 2021.