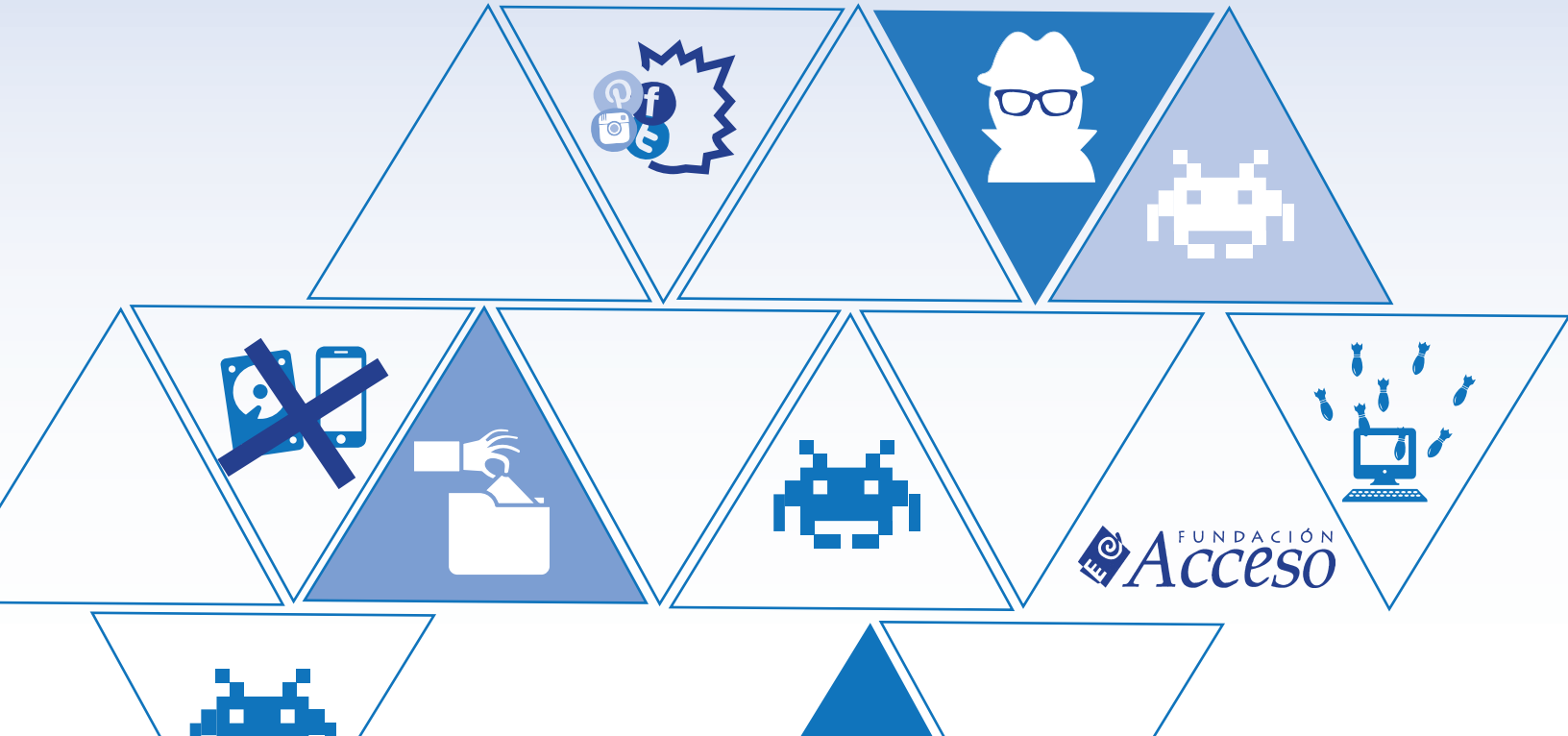
Observatorio Centroamericano de Seguridad Digital

Informe anual 2019



FUNDACIÓN Acceso

ÍNDICE

A.1 Introducción

El Observatorio Centroamericano de Seguridad Digital (OSD) surgió en el año 2016 como una iniciativa de Fundación Acceso.

El objetivo general del OSD es registrar y analizar incidentes de seguridad digital de personas defensoras y organizaciones de derechos humanos que estén ejerciendo su defensoría en Guatemala, Honduras, El Salvador y/o Nicaragua.

Para alcanzar este objetivo, Fundación Acceso visita y da seguimiento a las personas u organizaciones defensoras de DDHH que reportan un incidente a su seguridad digital, lleva un registro de los incidentes reportados y elabora el presente informe anual con la información recolectada.

Con esto se busca fortalecer los mecanismos de seguridad de defensoras y defensores de DDHH, posicionar el tema de la seguridad digital como un componente clave de la seguridad integral, fortalecer el análisis de la seguridad integral de quienes defienden DDHH en Centroamérica y apoyar potenciales litigios estratégicos con información basada en análisis jurídico e informático.

Durante los meses de registro y análisis del Observatorio (durante el 2019) registramos 15 casos de Honduras (2), Nicaragua (8) y Guatemala (5).

A.2 Derechos Humanos e Internet

Es importante destacar que el derecho a la privacidad e intimidad personal representa un valor por si mismos dentro de los Derechos Humanos en Internet, reconociendo su importancia, en el artículo 12 de la Declaración Universal de los derechos humanos[1], en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[2], así como en el artículo 11 de la Convención Americana de derechos humanos[3]. En estos artículos se reafirma el derecho a no ser objeto de injerencias arbitrarias o ilegales en nuestra vida privada, así como el deber del Estado de garantizar la seguridad jurídica y legitimidad de las normas constitucionales.

1 Organización de Naciones Unidas. **Declaración Universal de derechos humanos.** Disponible en: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf
2 Organización de Naciones Unidas. **Pacto Internacional de Derechos Civiles y Políticos.** Disponible en: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx
3 Organización de Estados Americanos. **Convención Americana de derechos humanos.** Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Es por ello, que el derecho a la privacidad se convierte en un elemento importante para la consolidación de sociedades democráticas, en el ejercicio de otros derechos fundamentales como el libre acceso a la información pública, libertad de expresión y libertad de asociación y manifestación en Internet. Los cuales resultan aún más necesarios de protegerse en el contexto de la defensa de los derechos humanos, a consecuencia a este bien común debe realizarse un análisis holístico del marco jurídico internacional y nacional que trascienda a la esfera digital.

En la última década y, principalmente tras las revelaciones de Edward Snowden, es de conocimiento público - derivado de esas y otras filtraciones posteriores - que los gobiernos de todo el mundo, incluyendo varios de América Latina, han adquirido diferentes mecanismos y programas informáticos para la vigilancia masiva de las comunicaciones. Estas herramientas de vigilancia están dirigidas principalmente a personas opositoras, defensoras de derechos humanos y activistas de diferentes causas, con la finalidad de intimidar y censurar, por la naturaleza de la información que pueden obtener.

El derecho a la privacidad se convierte en un elemento importante para la consolidación de sociedades democráticas, en el ejercicio de otros derechos fundamentales como el libre acceso a la información pública, libertad de expresión y libertad de asociación y manifestación en Internet.

Claramente, la indebida utilización de los mecanismos de vigilancia masiva atenta contra los estándares internacionales en materia de derechos humanos consagrados en diferentes tratados y legislaciones que limitan los principios de legalidad, transparencia, debido proceso, y proporcionalidad, entre otros. Los gobiernos a escala nacional y local están utilizando diferentes herramientas de vigilancia digital sin considerar alguna regulación o control, como nuevas estrategias de represión social.

Los principios antes mencionados, forman parte del catálogo de los *Principios Internacionales sobre la Aplicación de los derechos humanos sobre la Vigilancia de las Comunicaciones*[4] desarrollados por un grupo de organizaciones de sociedad civil, entre ellas Electronic Frontier Foundation, Article 19, Privacy International, entre otras.

Estos principios ampliamente desarrollados también funcionan como una guía de buenas prácticas para los gobiernos que deciden actualizar su marco jurídico relacionado a la vigilancia de las comunicaciones, garantizando los derechos humanos. Los 13 principios desarrollados son un análisis basado en estándares

4 Electronic Frontier Foundation (2014). **Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.** Disponible en: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

internacionales (interamericanos[5] y universales) y cómo se deben aplicar a la vigilancia de las comunicaciones. Sirven como guía para que los gobiernos tengan un marco normativo y de control al momento de realizar actividades de vigilancia masiva, además permiten que la sociedad civil posea mecanismos de fiscalización frente a posibles arbitrariedades. En este sentido, la Corte Interamericana de Derechos Humanos (CorteIDH) ha determinado que una de las causas directas del monitoreo de las comunicaciones de las y los defensores de derechos humanos sin la observación de los requisitos legales, causa temor y altera el normal ejercicio del derecho de asociación.[6] Lo cual es perjudicial para la actividad de defensa de los derechos humanos en la región.

A pesar que la mayoría de Constituciones de los países centroamericanos reconocen la privacidad e intimidad como derechos inherentes a las personas, los legisladores de las Asambleas y Congresos olvidan estos preceptos constitucionales al momento de presentar y aprobar proyectos de legislación ordinaria.

A pesar que la mayoría de Constituciones de los países centroamericanos reconocen la privacidad e intimidad como derechos inherentes a las personas, los legisladores de las Asambleas y Congresos olvidan estos preceptos constitucionales al momento de presentar y aprobar proyectos de legislación ordinaria. La Electronic Frontier Foundation desarrolló una serie de recomendaciones[7] para los gobiernos de América Latina, incluida Centroamérica, en las que detalla las disposiciones legislativas sobre vigilancia masiva de las comunicaciones que deben ser derogadas o reformadas. En el sentido, destaca especificamente que las legislaciones sobre Internet no deben incluir definiciones vagas que puedan permitir posteriores vulneraciones desproporcionadas de los derechos fundamentales.

Michel Frost - Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas - ha demostrado en sus informes gran preocupación por los diferentes mecanismos que utilizan los gobiernos para restringir la libertad de expresión y otros derechos fundamentales en Internet. Considera que Internet es una de las plataformas más relevantes que facilitan el acceso a la información y la exigencia de transparencia. Sin embargo, los gobiernos realizan diferentes actividades - desde limitar el acceso a Internet hasta remoción de contenido, pasando por implantación de spyware - con la finalidad de censurar las voces de defensores y defensoras de derechos humanos.

---

5 Electronic Frontier Foundation y Derechos Digitales (2016). **Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones y el Sistema Interamericano de Protección de derechos humanos.** Disponible en: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf

6 Comisión Interamericana de derechos humanos (2016). **Informe Criminalización de defensoras y defensores de derechos humanos.** Disponible en: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf

7 Electronic Frontier Foundation (2016). **Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica.** Disponible en: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf

En este sentido, una de sus preocupaciones principales se refiere al efecto que estos mecanismos han tenido en las y los defensores de derechos humanos, ya que utilizan las tecnologías, como Internet y redes sociales para promover el respeto a los derechos fundamentales. Los gobiernos se han dedicado a presentar acusaciones de difamación e desinformación contra defensoras y defensores, incluso iniciando campañas de desprestigio y acoso, con la finalidad de reprimir sus opiniones.

Por su parte David Kaye - Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de las Naciones Unidas - también ha señalado en sus informes anuales que los gobiernos últimamente tienden a controlar, limitar o vigilar el derecho a la libertad de expresión en Internet. Incurren en prácticas como interferir las conexiones, interceptar comunicaciones privadas, generalmente con asistencia de actores del sector privado de las telecomunicaciones, como los proveedores de servicios de Internet. Además, también se reporta el uso de técnicas como el filtrado de contenido, censura, priorizar contenidos o aplicaciones, vulnerando la Neutralidad de la Red, una de las invariantes de Internet.

Es necesario que "los Estados prevengan, protejan e investiguen las agresiones que se comentan en detrimento de quienes informan a través de Internet."

Edison Lanza - Ex Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos - ha expresado que Internet es una herramienta que facilita que las personas busquen, reciban y difundan información, potencializando el ejercicio del derecho a la libertad de expresión en sus comunidades. Sin embargo, también ha señalado diferentes prácticas de violencia e intimidación hacia periodistas y personas defensoras derechos humanos en la región. Por ejemplo, mecanismos de vigilancia masiva, censura estatal e incluso ataques cibernéticos. También enfatizó que es necesario que "los Estados prevengan, protejan e investiguen las agresiones que se comentan en detrimento de quienes informan a través de Internet."[8] Así mismo ha enfatizado que la protección de la libertad de expresión en Internet también debe aplicarse a códigos, protocolos, hardware e infraestructuras de telecomunicaciones.

Amnistía Internacional en su informe anual[9] (2017) enfatizó en la gran preocupación derivada de los mecanismos desproporcionados que utilizan los gobiernos para acosar e intimidar a las personas que se dedican a la defensa de los derechos humanos y

8 Comisión Interamericana de derechos humanos (2017). **Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf Pág. 122.

9 Amnistía Internacional (2017). **Informe anual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

el rol que juegan las nuevas tecnologías en este ámbito. Se ha comprobado que diferentes gobiernos han adquirido diferentes clases de software, como malware y spyware, para vigilar a las y los defensores de derechos humanos. Además se dedican a realizar campañas de difamación, propagando noticias falsas a través de las redes sociales en contra de personas activistas y defensoras. Esto sigue aún vigente y ya se han identificado tecnologías de vigilancia utilizadas en diversos países de América Latina.

Front Line Defenders en su informe anual[10] (2016) también expresó su preocupación en relación a las malas prácticas que están adoptando los gobiernos para silenciar y perseguir a las personas defensoras de derechos humanos. Se trata de la utilización de herramientas digitales para restringir el acceso a Internet y aplicaciones, también el bloqueo de contenidos e incluso pagar a personas (destacando los perfiles falsos en redes sociales) para que difundan rumores y calumnias, así como la adquisición de software y herramientas de vigilancia masiva que generalmente son utilizadas en contra de activistas, personas opositoras y defensores y defensoras.

A.3 ¿Qué es un incidente de seguridad digital?

Se registran los casos ocurridos a personas defensoras de DDHH en Centroamérica relacionados con su información y comunicación digital almacenada, en movimiento y en servicios.

En el marco de las actividades del Observatorio Centroamericano de Seguridad Digital se registran los casos ocurridos a personas defensoras de DDHH en Centroamérica relacionados con su información y comunicación digital almacenada, en movimiento y en servicios.

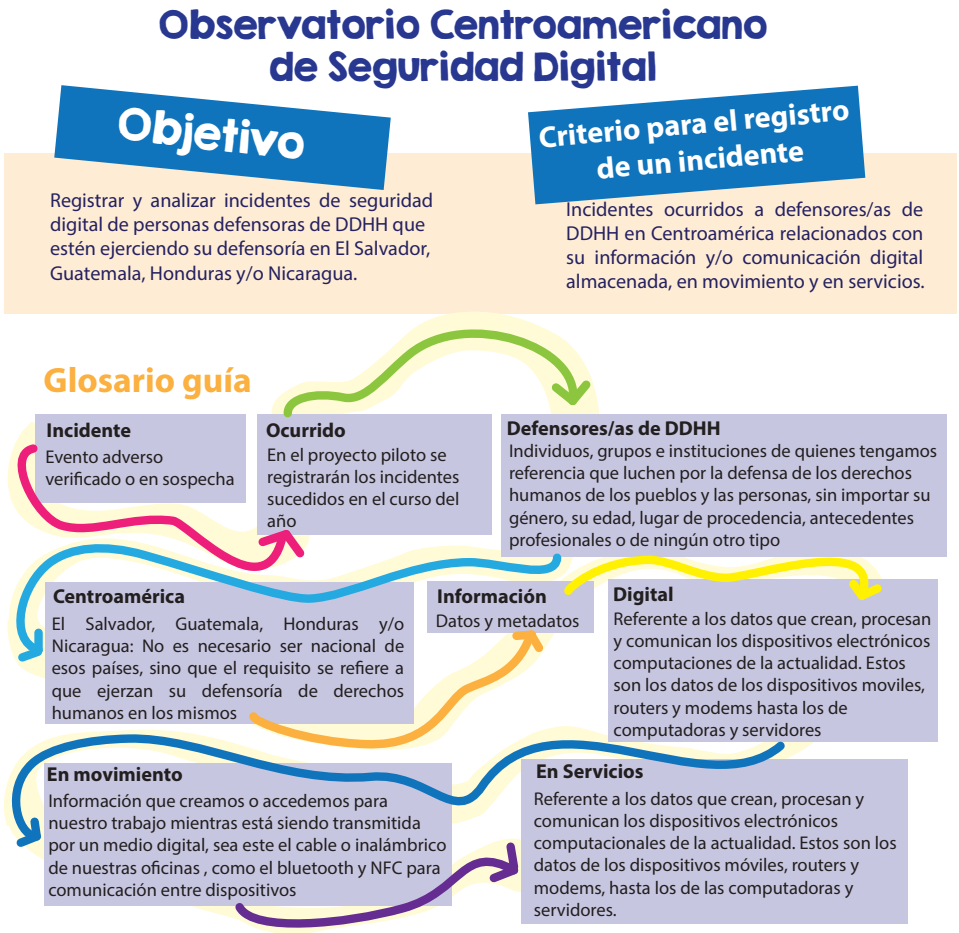
En consecuencia, con base en lo establecido por la Organización de las Naciones Unidas, se entiende que un persona defensora de derechos humanos es un individuo, grupo e institución de quienes se tenga referencia que luchen por la defensa de derechos humanos de los pueblos y las personas, y, en el contexto de este proyecto, que ejerzan su labor en Guatemala, Honduras, El Salvador y Nicaragua, sin importar su género, edad, lugar de procedencia, antecedentes profesionales o de ningún otro tipo[11]. Además, en el marco del Sistema Interamericano de Protección de derechos humanos (SIDH), la Comisión Interamericana de derechos humanos (CIDH)

10 Front Line Defenders (2016). **Annual Inform Human Rights Defenders at risk in 2016.** Disponible en: https://www.frontlinedefenders.org/en/resource-publication/2016-annual-report

11 Organización de Naciones Unidas. **Resolución 53/144 del 8 de marzo de 1999.** Disponible en: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

reconoce la existencia de el derecho a defender los derechos humanos de las personas defensoras.[12]

Por otra parte, incidente se refiere a cualquier evento adverso (verificado o en sospecha) relacionado con la información (incluyendo datos y metadatos) y/o comunicación digital.



12 Comisión Interamericana de derechos humanos. **Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas.** Disponible en: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

Para que esta información y/o comunicación se considere digital debió ser creada, procesada y comunicada por los dispositivos electrónicos computacionales de la actualidad, y que puede estar almacenada, transmitida o puede encontrarse en un servicio en línea o en cualquiera de las aplicaciones que se utilizan para acceder a ellos (como correo electrónico, redes sociales, blogs y medios independientes en línea).

Cuando se identifica un incidente que no cumple con estos criterios para ser registrado por el Observatorio, desde Fundación Acceso se brinda la atención técnica necesaria, en caso que la información que pudo estar comprometida o en el caso que sea un incidente de otra variable de la seguridad, ya sea física, legal o psicosocial, con la finalidad de referir el caso con organizaciones aliadas u otras instancias, nacionales o regionales que trabajen ese tema en particular.

A.4 Tipología de incidentes

Los incidentes se catalogan con base en la siguiente tipología:

- **Ataques LAN[13]:** Bloqueo del tráfico de datos que circula en la red local, interrupción de las conexiones entre las computadoras de la red, denegación de acceso de servicios y generación de tráfico en la red. Un ejemplo es el de reconfigurar los routers o modems para bloquear determinadas páginas**.**
- **Ataques remotos:** Toma de control del equipo o extracción de información del mismo de forma remota, logrando el acceso mediante una conexión a Internet o a una red. Los ataques remotos aprovechan vulnerabilidades del módem[14] o del sistema operativo.
- **Ataques Web:** Toda ataque a los servicios de Internet que utilizamos y el monitoreo de los mismos. Estos pueden ser los servicios de blogs, noticias, radios en línea, nuestros sitios web, bloqueo de nuestro canal de Youtube, otros así como el monitoreo de nuestro comportamiento a partir de los sitios que visitamos.

13 LAN en inglés significa Red de Área Local y se refiere al conjunto de computadoras ubicadas en un espacio determinado (como las oficinas de una organización), que pueden compartir archivos entre ellas y también pueden compartir salida a la Internet.
14 El Módem es el aparato proporcionado por el proveedor del servicio de Internet. Convierte la información digital generada por las computadoras en frecuencias de sonido para ser transmitidas por una red telefónica, es decir, el aparato por medio del cual las computadoras se conectan a Internet.

Una de las principales técnicas informáticas para este tipo de ataque es DDoS (ataque de denegación de servicios), que es un ataque a la red que causa que un servicio o recurso sea inaccesible. También entran en esta categoría la censura de determinados sitios web por parte del Proveedor del Servicio de Internet (ISP), el monitoreo de tráfico, robo de identidad en la Web, suplantación de sitio web, aparición de publicaciones no autorizadas en el sitio Web, cambios en el Servidor de Nombres de Dominio (DNS), inadecuada actualización y respaldo del sitio Web.

- **Compromiso de cuentas:** Ésta es una categoría especial que debería estar contenida en "Ataques a Web" pero que específicamente trata de craqueo de nuestras credenciales para acceder a los servicios que utilizamos. Se decide separar por la cantidad de incidentes de éste tipo que normalmente se dan[15].

  Una de las principales técnicas informáticas para este ataque es el Phishing[16] o suplantación de identidad, caracterizado por intentar adquirir información confidencial de forma fraudulenta, particularmente las contraseñas de cualquier cuenta de correo electrónico, de suscripciones en Internet, de redes sociales, de administración de Hosting y sitios Web, cuentas bancarias, tarjetas de crédito, etc.

- ***Malware*[17] o *software malicioso*:** Cualquier tipo de software[18] que se ejecuta en los dispositivos para interrumpir las operaciones y recolectar información sensible sin consentimiento del usuario/a administrador/a. También se pueden instalar simultáneamente, pero de manera oculta como complementos extras de algunos programas aparentemente legítimos, legales, sin mala fe o sin terceras u ocultas intenciones.

  Uno de los malware más peligrosos es el conocido como ***spyware*[19]** o **programa espía** el cual recopila información almacenada en el dispositivo y la transmite a una entidad externa sin consentimiento del usuario administrador. Los programas instalados en celulares que realizan escuchas telefónicas, o incluso

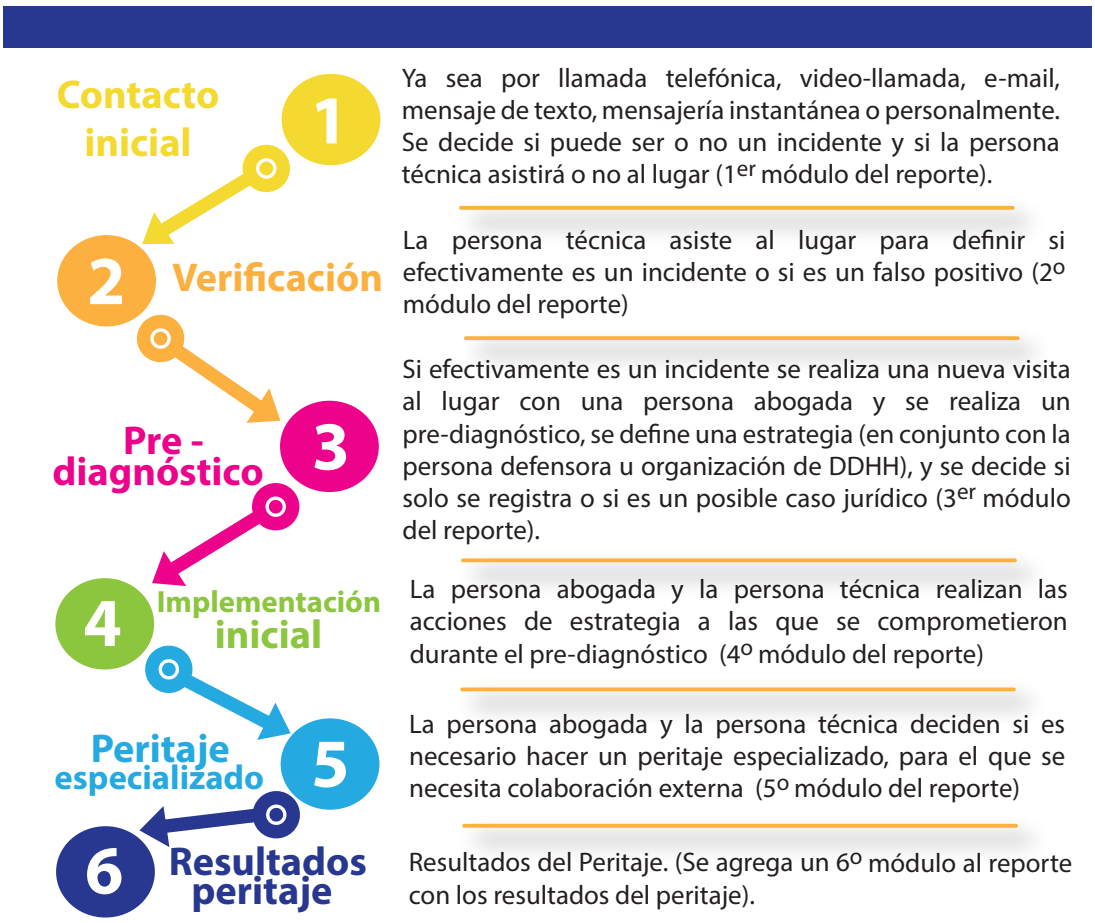
15 Recomendación del equipo de Access Now a partir de su experiencia con el Help Desk. https://www.accessnow.org/linea-de-ayuda-en-seguridad-digital/
16 Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks.
17 *Definición de Malware obtenida de techterms.com http://techterms.com/definition/malware*
18 Se entiende Software como cualquier componente no tangible, por medio del cual se ejecutan determinadas instrucciones o rutinas que permiten utilizar un dispositivo.
19 FTC Report (2005). Disponible en: http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

que activan vídeo y audio también son considerados malware.

- **Pérdida de hardware:** Robo, hurto, destrucción, o extravío del equipo. Un ejemplo de esto es la destrucción de equipo en un allanamiento ilegal.
- **Retención de hardware:** Equipo incautado, confiscado y/o retenido por parte de agentes del Estado, con o sin orden legal, con o sin justificación legítima.

Observatorio Centroamericano de Seguridad Digital

Momentos de intervención



A.5 Procedimiento para el registro de incidentes

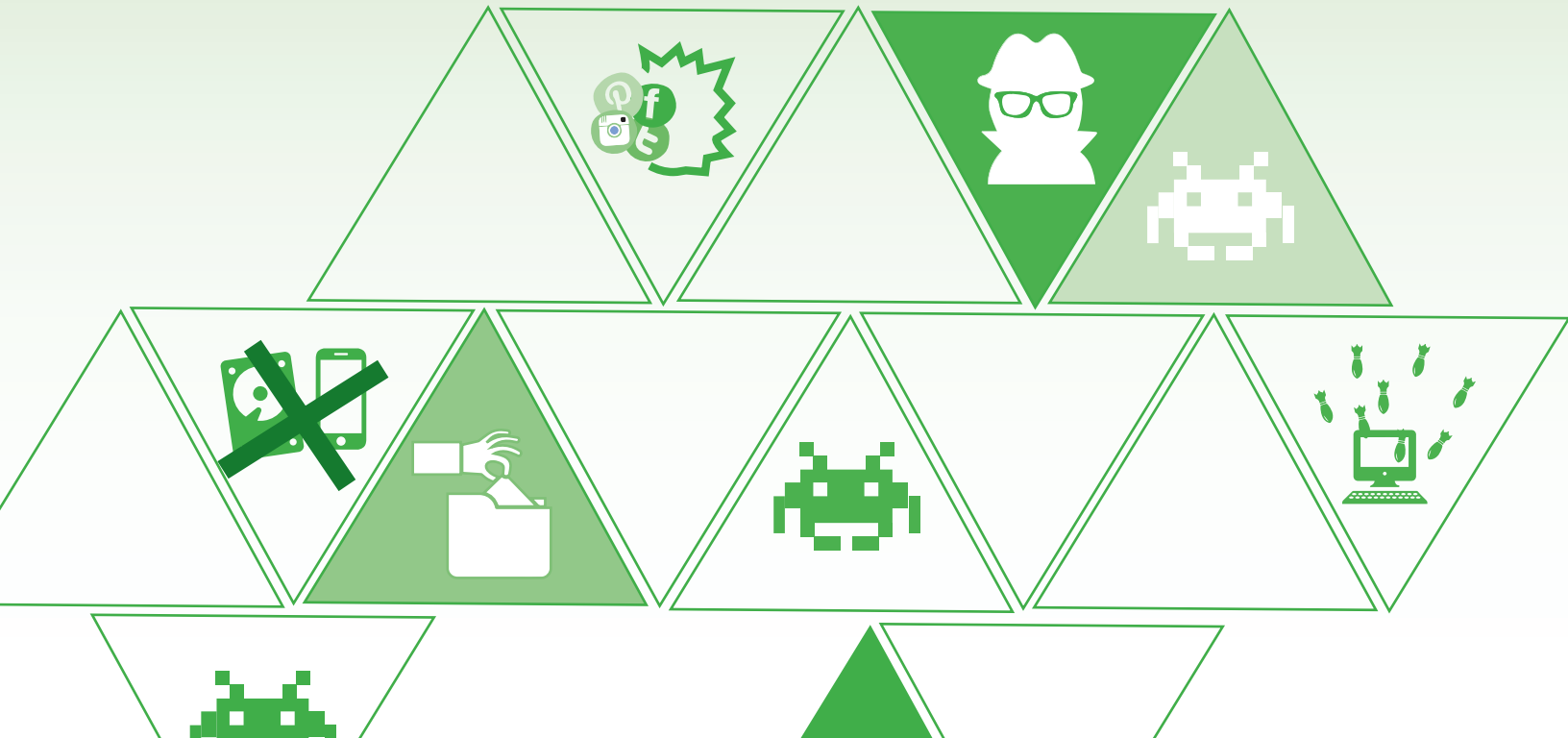
Al momento que el equipo de Fundación Acceso tiene conocimiento sobre un posible incidente de seguridad digital se procede al registro del mismo, además de prestar el servicio técnico necesario para proteger la información digital de la persona u organización.

Se inicia con la obtención del consentimiento informado para asegurarse que la persona usuaria está enterada de la intervención que se realizará sobre su equipo. Posteriormente se obtiene su autorización para realizar la inspección técnica (dependiendo del tipo de incidente que se trate, esto puede llevar desde horas hasta algunas semanas).

Durante el período que dure la revisión, la persona técnica encargada debe llenar una bitácora donde registra todas las acciones llevadas a cabo en el equipo, con el fin de demostrar que en su intervención se han realizado únicamente aquellas acciones dirigidas a determinar el origen del problema que presenta el equipo. Por último se registra la finalización de la revisión y devolución del equipo, donde constan las conclusiones del análisis y posibles acciones de seguimiento.

Los casos registrados para este año del Observatorio han sido producto del conocimiento y de la relación que el equipo de la Fundación Acceso tiene con diversas organizaciones y personas que trabajan en la defensa de los derechos humanos en cada país.

Guatemala



B. CAPÍTULO GUATEMALA

B.1. Seguridad Digital y Derechos Humanos en Guatemala

En el 2015, Fundación Acceso realizó una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[20]. En esta se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. Como resultado de esa esa investigación se establecieron algunos parámetros que son aplicables en el análisis del contexto nacional. Esos parámetros continúan vigentes casi en las mismas condiciones en las que se plantearon en ese estudio, el cual fue actualizado en 2018.

En Guatemala hay un reconocimiento constitucional del derecho a la privacidad. Sin embargo, en la legislación penal existente con respecto a la protección del derecho a la privacidad digital, esta aún no se encuentra regulada.

En términos generales se estableció que en Guatemala hay un reconocimiento constitucional del derecho a la privacidad[21]. Sin embargo, en la legislación penal existente con respecto a la protección del derecho a la privacidad digital, esta aún no se encuentra regulada.

En este sentido, desde el 2009 la Iniciativa 4090, que dispone aprobar la Ley de Protección de Datos Personales[22] posee dictamen favorable y se encuentra pendiente del tercer debate en el Pleno del Congreso desde el año 2010[23]. La existencia de un marco jurídico en materia de protección de datos personales favorecería a una

20 Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: 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 defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

21 *Ibíd.* Pág 175.

22 Congreso de la República de Guatemala. **Iniciativa 4090, Ley de Protección de Datos Personales.** Disponible en: ttp://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf

23 El proceso legislativo en Guatemala se desarrolla seún establece la Ley de Régimen Interior, a partir de la presentación de una iniciativa de ley. Esta se presenta al pleno cuando es incluida en agenda, el pleno decide a qué Comisión la envía para dictamen. La Comisión revisa y emite dictamen que puede ser favorable (sin cambios o con reformas) o negativo. Si es negativo allí queda. Si es favorable, se envía para su discusión al pleno cuando la incluyan en agenda. Una vez en agenda el pleno puede decidir conocerla de urgencia nacional, lo cual significa aprobación en una sola lectura. Para ello necesita 2/3 del total de votos (108). Si no, va en proceso ordinario que significa tres lecturas que pueden ser en sesiones continuas o ir a ritmo lento (puede durar años). Una vez superada la tercera lectura hay una discusión más que es por redacción final. Hahy leyes que han logrado tener tres lecturas de aprobación y siguen sin ser conocidas en redacción final por lo que están sin aprobación final.

adecuada protección de la privacidad en línea de las y los defensores de derechos humanos, ya que tendrían mecanismos para ejercitar sus derechos en general y particularmente frente al gobierno o empresas.

Durante el 2017 se presentó un catálogo de iniciativas de ley en el Congreso de la República, las cuales de una u otra manera pueden perjudicar el ejercicio de diferentes derechos humanos en Internet, especialmente para las personas defensoras. Entre estas se puede citar la iniciativa 5239 que dispone aprobar la Ley Contra Actos Terroristas[24]. Dicha iniciativa ya posee dictamen favorable por la Comisión de Gobernación y se encuentra pendiente de ser conocida en el Pleno del Congreso. En términos generales, este proyecto tiene como finalidad criminalizar las protestas ciudadanas[25]. El Artículo 24 configura el delito de "terrorismo cibernético o ciberterrorismo" y lo sanciona con prisión de 10 a 30 años. Además, establece que se promoverá una red de inteligencia para controlar el movimiento de presuntos terroristas. Sin embargo, no determina los estándares mínimos para este control y posible vigilancia masiva, además de que se contradice con lo regulado en la Ley Marco del Sistema Nacional de Seguridad y los capítulos sobre el sistema de inteligencia y controles democráticos. Por otro lado, la iniciativa 5254 que dispone aprobar la Ley contra la Ciberdelincuencia[26], ya posee dictamen favorable de una comisión y se encuentra pendiente de Dictamen por la Comisión de Gobernación. Este proyecto de ley carece de enfoque de derechos humanos y criminaliza conductas que en algún momento podrían afectar el derecho de expresión y asociación en línea, de las personas usuarias y de la labor de defensoría y denuncia de violación a derechos humanos.

En sintesis, se han presentado tres iniciativas de ley en los últimos 3 años: la iniciativa 5254 Ley de Ciberdelincuencia (2017), la Iniciativa 5339 Ley contra Actos Terroristas (2018) y la iniciativa 5601 Ley de Prevención y Protección contra la Ciberdelincuencia (2019). Las iniciativas no han sido aprobadas y debido a que tienen condiciones que atentan contra el derecho a la libre expresión particularmente, no deberían continuar su trámite.

Por otro lado, se han aprobado políticas públicas con relación a la temática de Internet y Tecnologías de la Información y Comunicación. En el transcurso del 2018 se

24 Congreso de la República de Guatemala. **Iniciativa 5239, Ley contra Actos Terroristas.** Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=3607
25 Prensa Libre. **Una peligrosa propuesta de ley.** Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley
26 Congreso de la República de Guatemala. **Iniciativa 5254, Ley contra la Ciberdelincuencia.** Disponible en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf

desarrollaron algunos proyectos que deben ser mencionados por el posible impacto, positivo o negativo, para las personas defensoras en Guatemala.

Desde la Superintendencia de Telecomunicaciones (SIT), con el apoyo de otras entidades gubernamentales, se desarrolló la agenda digital denominada Nación Digital[27]. Esta posee como ejes de acción el uso de las Tecnologías de la Información y Comunicación en la salud, educación, ***seguridad***, desarrollo y transparencia. Sin embargo, esta agenda aún carece de objetivos reales y concretos. Hasta el momento se desconocen los sectores o entidades que participarán en su ejecución y carece de un eje que eleve la protección de derechos humanos en Internet.

La elaboración de la Estrategia Nacional de Ciberseguridad no involucró a sectores clave como las organizaciones que defienden derechos humanos, cuya ausencia es perjudicial.

Desde 2018, el Ministerio de Gobernación, por medio del IV Viceministerio de Tecnologías de la Información y Comunicación, con el apoyo de la Organización de Estados Americanos (OEA), realizó el lanzamiento de la Estrategia Nacional de Ciberseguridad[28]. Esta Estrategia en términos generales pretende generar y coordinar una hoja de ruta a mediano y largo plazo para diseñar e implementar acciones para proteger la seguridad nacional frente a la ciberdelincuencia. En este proceso, se ha convocado a diferentes sectores (instituciones gubernamentales, del sector justicia, sector privado, academia, comunidad técnica y sociedad civil) para su elaboración. No obstante, la Estrategia carece de un enfoque de derechos humanos,además de que la protección de la privacidad en línea y datos personales no es una prioridad[29].

Es necesario destacar esto último, ya que la creación de políticas públicas relacionadas con la Internet y las nuevas tecnologías, requiere del reconocimiento a nivel nacional de estándares mínimos de protección de derechos fundamentales en el contexto digital. La elaboración de esta Estrategia no involucró a sectores clave como las organizaciones que defienden derechos humanos, cuya ausencia es perjudicial. De esa cuenta, es muy preocupante que las políticas públicas contenidas en la estrategia sean elaboradas únicamente bajo el enfoque de "seguridad nacional", divorciado de la indispensable correlación con los derechos humanos. Esta falencia puede afectar la labor de las personas que los defienden, debido a la persistente estigmatización gubernamental que suele catalogarles como desestabilizadoras o terroristas. Lo que representa además un riesgo puesto que será la base para el desarrollo e implementación de futuras políticas públicas relacionadas con ciberseguridad.

27 Nación Digital. https://www.naciondigital.gob.gt/
28 Ministerio de Gobernación. **Presentan Estrategia Nacional de Ciberseguridad.** Disponible en: http://mingob.gob.gt/estrategia-nacional-de-seguridad-cibernetica/
29 Estrategia Nacional de Seguridad Cibernética. Disponible en: https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf

El 25 de octubre 2018 se desarrolló el segundo Foro de Gobernanza de Internet de Guatemala[30]. En este se discutieron temas relacionados con la protección de usuarios en Internet, así como la libertad de expresión en el contexto electoral, relacionados con la privacidad digital. Sin embargo se abordaron de manera muy general y no se incluyó la protección de las personas defensoras de derechos humanos.

En el contexto actual, 2019, es importante compartir que se encuentra vigente el "Plan Estratégico de Seguridad de la Nación 2016-2020". Se trata de un plan de carácter general, que se plantea en articulación con el Libro Blanco de la Seguridad Nacional y la Política Nacional de Seguridad. En consecuencia, a partir de los desafíos planteados en el Libro Blanco y los lineamientos que desarrolla la Política, el Plan detalla objetivos y acciones estratégicas[31].

Son de particular relevancia el Objetivo 9 - Producir Inteligencia Estratégica de Estado, que coadyuve a la toma de decisiones en función de los Objetivos Nacionales - y el Objetivo 12 - Desarrollar la investigación científica, tecnológica y la transferencia de capacidades para atender integralmente la Seguridad de la Nación. El objetivo 9, busca consolidar el Sistema de Inteligencia del Estado. Para ello propone acciones como: desarrollar la carrera profesional en el Sistema de Inteligencia de Estado; desarrollar, implementar y optimizar las plataformas tecnológicas institucionales interoperables; o implementar el Centro Nacional de Inteligencia para ejercer el Comando, Control, Computación, Comunicaciones e Inteligencia. Por otro lado, el Plan también cuenta con una propuesta dirigida al ámbito legislativo, en la cual se propone tanto la aprobación de normativa nueva, como la reforma de algunas de las leyes existentes. Entre la nueva normativa a promulgar se propone la formulación de la Ley del Sistema Nacional de Inteligencia y la Ley de Tecnología –seguridad cibernética[32].

A partir de la revisión del Plan Estratégico Seguridad de la Nación se puede concluir que dicho documento no parte de un enfoque de derechos humanos y que el resguardo de la privacidad no es una preocupación contemplada en su formulación. En consecuencia, cuando se plantea el fortalecimiento de los sistemas de inteligencia no se consideran medidas para garantizar que esto no vulnere el derecho a la privacidad de la ciudadanía o la protección de las personas y organizaciones defensoras de derechos humanos.

30 Foro de Gobernanza de Internet de Guatemala. http://igf.gt/
31 «Plan Estratégico de Seguridad de la Nación 2016-2020» (Consejo Nacional de Seguridad, junio de 2016), https://stcns.gob.gt/docs/2016/Plan_Estrategico/PESN%202016-2020.pdf.
32 «Plan Estratégico de Seguridad de la Nación 2016-2020»

Por otro lado, en el marco de las investigaciones alrededor de diferentes delitos cibernéticos, el Ministerio de la Defensa manifestó públicamente la intención de que sea el Ejército de Guatemala el que investigue las amenazas cibernéticas para resguardar la economía e instituciones del país.[33] De concretarse esta iniciativa, habría vulneración a derechos humanos y constitucionales de la ciudadanía.

B.2. Ataques a defensoras y defensores de derechos humanos

La Unidad de Protección a Defensoras y Defensores de Derechos Humanos de Guatemala (UDEFEGUA), en su reciente informe[34] 2019, *alerta* sobre los diversos ataques contra las personas defensoras de derechos humanos en el país. El reporte de la UDEFEGUA indica que se registraron 462 agresiones, 15 asesinatos y 5 intentos de asesinato. La entidad señala que el 2019 es el cuarto año más violento para las personas defensoras, desde el 2000, cuando inició ese registro.

El reporte de la UDEFEGUA indica que se registraron 462 agresiones, 15 asesinatos y 5 intentos de asesinato.

Esta situación también es evidenciada en el informe anual de Amnistía Internacional[35], la cual establece que las personas defensoras aún son objeto de amenazas, estigmatización, intimidación, agresión e incluso, son víctimas de homicidio. Los grupos más vulnerables ante estos ataques son organizaciones de defensa de la tierra, el territorio y el medio ambiente. Con ese análisis también coincide el informe (2020) Defending Tomorrow, de la organización Global Witness. La entidad indica que de las 212 personas defensoras del ambiente cuyos asesinatos recoge el informe, 32 fueron en Centroamérica. En Guatemala, indica, fueron asesinadas 12 personas defensoras del ambiente.[36]

En cuanto a ataques digitales, en el 2017, para la población y sociedad civil, Twitter fue fundamental para la movilización ciudadana para exigir, entre otras cosas,

33 Soy502. **El Ejército quiere encargarse de las amenazas cibernéticas.** Disponible en: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394

34 Udefegua (2019). *Situación de Defensoras y Defensores de derechos humanos en Guatemala Un Reflejo del Deterioro de los derechos humanos en el País. Disponible en: https://udefegua.org/informeshttp://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf*

35 Amnistía Internacional (2019). Situación de los derechos humanos en las Américas: Informe anual 2019. Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/https://www.amnesty.org/download/Documents/AMR0113532020SPANISH.PDF Pág. 55.

36 Defender el mañana: La crisis climática y amenazas contra defensores de la tierra y el medio ambiente. Global Witness (2020) https://www.globalwitness.org/es/defending-tomorrow-es/

la renuncia de funcionarios públicos de altos cargos, incluido el Presidente de la República. Jimmy Morales. Como consecuencia, el aumento de perfiles considerados como *bots* o *net centers*[37] propició la desinformación, ya fuera como propagación de noticias falsas hasta la difamación en contra de activistas y medios independientes. El propósito esencial de estas acciones se centró en debilitar el trabajo de investigación realizado por la Comisión Internacional contra la Impunidad en Guatemala (CICIG)[38], el Ministerio Público (MP)[39], y múltiples organizaciones nacionales de derechos humanos, particularmente, a las mujeres defensoras.

En grupo integrado por 12 medios de comunicación planteó al Ministerio Público que investigara el acoso que sufrieron en redes sociales, principalmente por cuentas de net centers.

En ese mismo año, un grupo integrado por 12 medios de comunicación planteó al Ministerio Público que investigara el acoso que sufrieron en redes sociales, principalmente por cuentas de net centers. Los medios denunciantes afirmaron haber sufrido *"hackeos, ataques de net centers y amenazas directas, en especial contra mujeres"*.[40] En estos hechos se evidenció el empleo de bots en contra de activistas y medios independientes, a fin de difamar o desestabilizar, la labor de los mismos. Una acción que no es novedosa pues, la están utilizando directa o indirectamente varios gobiernos. Sin embargo, uno de los problemas y desafíos principales es identificar si existe financiamiento público (uso de recursos del Estado), para estas actividades. Al finalizar la edición del informe del Observatorio de Seguridad Digital en 2017, salió a la luz pública un artículo del periodista Luis Asardo, titulado: Los Netcenters: negocio de manipulación. En este, Asardo detalla cómo han funcionado estos grupos en Guatemala y cuáles son los efectos de su actividad.[41]

A mediados del 2018, por medio de artículos de investigación, publicados por Nuestro Diario de Guatemala, se identificó una red ilegal de espionaje dirigido por los jefes de la Dirección General de Inteligencia Civil (Digici) *"de cuya institución salieron los fondos para armar el centro de operaciones ilegales. Otros equipos para espiar fueron comprados con fondos de la Policía Nacional Civil (PNC) y de la Secretaría de Inteligencia del Estado (SIE)...Documentos en poder de* ***Nuestro Diario*** *revelan que se*

37 Soy502. **Los netcenteros de la impunidad.** Disponible en: http://www.soy502.com/articulo/netcenteros-impunidad-20878
38 Comisión Internacional contra la Impunidad en Guatemala. http://cicig.org/
39 Nómada. **#JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo.** Disponible en: https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/
40 Soy502. **Periodistas exigen que el MP investigue a los "net centers".** Disponible en: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149
41 Medium.com. Los Netcenters: Negocio de Manipulación. https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc

adquirieron las versiones más avanzadas de Pen-Link, Conceptus, Circles, Citer 360, Avatar, Pegasus, Laguna, entre otros."[42].

En agosto del 2019, en el proceso de cierre, la CICIG le entregó al Ministerio Público alrededor de 60 investigaciones que estaban en diferentes estados de desarrollo. Una de las denuncias refiere al caso *Espionaje y Escuchas Telefónicas Ilegales en la compañía Tigo*, en la cual se encuentra involucrado el ex ministro de Economía, Acisclo Valladares Urruela, cuando fungía como director ejecutivo de dicha empresa. Según las investigaciones, las escuchas estaban dirigidas a su exposa, al Movimiento Semilla (partido político en formación en ese momento), así como a otras personas del entorno político y empresarial. Es importante recordar que: *"Los documentos presentes en la denuncia fueron incautados durante un allanamiento al apartamento de Valladares Urruela en zona 15, el 23 de noviembre de 2017. Allanamiento realizado como parte de las investigaciones de la Fiscalía Especial Contra la Impunidad (Feci) y la Cicig, sobre la compra de votos en el Congreso, para la aprobación de una reforma a la Ley de Telecomunicaciones en 2014, que benefició a la empresa Tigo, para la instalación de cableado reduciendo el pago a municipalidades y particulares."*[43]

Las escuchas realizadas por la compañía Tigo estaban dirigidas a su exposa, al Movimiento Semilla (partido político en formación en ese momento), así como a otras personas del entorno político y empresarial.

En cuanto a ataques digitales a nivel global en 2019, Front Line Defenders menciona que *"Los ataques más comunes por los que se solicitó el apoyo de Front Line Defenders fueron las campañas de difamación, los trolls, el acoso, y el acceso no autorizado a las cuentas de redes sociales, de donde se obtuvo información para poner en peligro la reputación y seguridad de las personas defensoras". Así mismo, indican "El robo y la confiscación de dispositivos también representaron un riesgo significativo para estas personas. En los casos en los que las autoridades confiscaron dispositivos, incluso estando cifrados, las personas defensoras se vieron obligadas a dar sus contraseñas, lo que les permitió el acceso a información confidencial. En general, estos dispositivos rara vez estaban cifrados y casi nunca se realizaron copias de seguridad. A veces dicha información fue utilizada como prueba para enjuiciar a los/as defensores/as o tomar medidas contra sus redes. ...El acoso en las redes sociales fue algo cotidiano para miles de defensores y defensoras, y las personas marginadas de la sociedad fueron a menudo las más atacadas".*[44]

42 Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I). Disponible en: https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/

43 Los ojos y oídos de Tigo en la política y los negocios. 30 agosto 2019. Disponible en: https://www.revistafactum.com/tigo-espionaje-guatemala/

44 Análisis Global de Front Line Defenders 2019. Disponible en: https://www.frontlinedefenders.org/sites/default/files/spanish_-_global_analysis_2019_web.pdf

B.3. Principales hallazgos en Guatemala

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Guatemala. Los mismos han sido reportados entre los meses de abril y setiembre de 2019. Para para definir los criterios de registro, se diseñaron herramientas tanto técnicas como legales que consideraron los parámetros a evaluar.

*En 2019 se registraron **cinco** casos e incidentes de seguridad digital, todos en la Ciudad de Guatemala.*

B.4. Casos registrados

Durante el transcurso del período antes mencionado, fueron registrados **cinco** casos e incidentes de seguridad digital, todos en la Ciudad de Guatemala.

B.5. Perfil de las personas/organizaciones que reportaron incidentes

En 2019, todos los casos registrados en Guatemala corresponden a mujeres defensoras de derechos humanos.

El primer caso fue atendido por el llamado de la directora de una organización de derechos humanos. El segundo caso corresponde a la coordinadora de un medio de comunicación independiente. El tercer caso involucra a una abogada de una organización internacional con presencia en Guatemala. El cuarto caso afecta a una periodista de un medio de comunicación independiente. El quinto y último es el de una defensora dedicada a la investigación.

B.6. Tipos de ataques

A continuación una breve descripción de los incidentes registrados.

En el primer caso la directora de la organización contacta al Observatorio e indica que a raíz del juicio contra un defensor indígena y del territorio, han notado que el correo electrónico institucional ha dejado de funcionar correctamente e indica: "*por momentos sirve y por momentos deja de hacerlo. Además, recibimos muchísimo spam*". Se visitó la organización y se revisaron las configuraciones del servidor de

correo y de los clientes de correo. Se pudo comprobar que la organización tiene un servidor de correo electrónico desactualizado y vulnerable, debido a falta de mantenimiento. También se encontraron varias vulnerabilidades de seguridad, serias. Por otro lado, no se encontró indicios de que existieran intrusos pero sí se pudo establecer que se encuentra en listas negras de *spam* y no posee un sistema de electricidad de respaldo. Esto genera comportamientos anómalos. Como resultado, se determinó que es un incidente de "Compromiso de Cuentas" y se definió como un falso positivo.

Para el segundo caso, la coordinadora de un medio independiente reportó al observatorio un posible incidente de censura del sitio web. Reportó que a través de redes sociales, el medio fue informado de que su sitio no podía ser visitado por algunas personas. Al indagar, pudieron identificar que un gran porcentaje de la población no podía ver el sitio. Sin embargo, otro porcentaje sí lo podía hacer por lo que, indicó: "*nos dio indicios suficientes para considerar que fuera un ataque de censura por parte de los proveedores de Internet*". El equipo del observatorio, luego de analizar los registros DNS, pudo determinar que el antiguo web máster del medio independiente hizo una mala configuración del servicio de seguridad de la página web, lo cual generaba los fallos al sitio. Se determinó que se trataba de un incidente de "Ataques remotos" y se catalogó como un falso positivo.

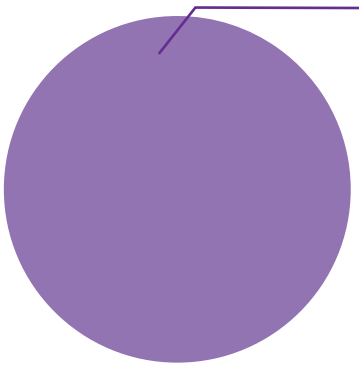
El tercer caso está relacionado con una abogada defensora, quien reporta al observatorio que su cuenta personal de facebook hizo cambios no autorizados por ella. Entre estos, el cambio de foto de perfil así como publicaciones no autorizadas. A la defensora le robaron su dispositivo móvil en un espacio público. Luego de ello se percató de los cambios que le hicieron a su perfil de Facebook. La propia defensora ya había realizado todas las acciones de seguridad digital como: cambio de credenciales a los dispositivos vinculados y activó la autenticación de dos pasos. El caso quedó registrado como un falso positivo y el incidente fue catalogado como "Compromiso de Cuentas".

En cuanto al cuarto caso, una periodista fue advertida por una entrenadora de seguridad digital que muy probablemente su móvil estaba infectado con malware y que se lo diera a un experto para una revisión más a fondo. La periodista contactó al equipo del Observatorio con el fin de que se revisara su dispositivo móvil. Luego de implementar el procedimiento de Security without Borders, se determinó que en efecto el equipo se encontraba comprometido con malware. Sin embargo, se concluyó que el malware encontrado era común y el equipo carecía de protección. En este caso se descartó un malware dirigido o confeccionado a la medida para la

periodista. El observatorio registró el incidente como un falso positivo y lo catalogó como un incidente de "Malware".

El quinto caso documentado por el observatorio durante el 2019 es el de una defensora dedicada a la investigación. Esta defensora indicó tener grandes sospechas de instalación de malware en su dispositivo móvil, luego de la publicación de un informe público sobre el uso de herramientas de vigilancia digital en el país. El equipo del observatorio revisó el dispositivo y concluyó que no hay indicios de instalación de malware ni tampoco intentos de infección al mismo. Este caso se registró como un incidente de "Malware" y se catalogó como un falso positivo.

5 casos atendidos



3 Mujeres

0 Hombres

+ 2 organizaciones

Perfiles

- 2 Derecho a la información
- 1 Acceso a la justicia
- 1 Derechos de los pueblos indígenas
- 1 Investigadora

Tipos de ataques

Falso positivo (1)

- 3 Compromiso de cuentas
- 1 Malware
- 1 Ataque remoto

B.7. Posibles perpetradores

Poder identificar a los posibles perpetradores de los ataques es algo que interesa al Observatorio de Seguridad Digital. Sin embargo, es necesario informar que esto no siempre se logra pues, un atacante regularmente tratará de *anonimizarse* y para ello utilizará los recursos técnicos y metodológicos que convengan para el tipo de ataque realizado.

En tal sentido, esta es una tarea que requiere, para los casos más complejos, recursos técnicos y acceso a servicios que están fuera del alcance de la organización. No obstante lo anterior, sobre la base de los hallazgos de los ataques es posible delinear un perfil técnico del atacante y sus objetivos.

El solo hecho de que se reporte un incidente digital al observatorio, refleja que las personas defensoras y organizaciones de derechos humanos están más conscientes de los riesgos y posibles incidentes digitales.

Los cinco casos registrados durante el 2019 se clasificaron como falsos positivos, por lo tanto los posibles perpetradores no se identificaron. No obstante, es necesario destacar que el solo hecho de que se reporte un incidente digital al observatorio, refleja que las personas defensoras y organizaciones de derechos humanos están más conscientes de los riesgos y posibles incidentes digitales. Además, que logran identificar posibles perpetradores en su contexto de defensa y también dimensionar las capacidades tecnológicas reales que tienen para realizar éste tipo de ataques.

B.8. Mecanismos de Protección

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de Guatemala del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos, independientemente de que los casos hayan sido registrados como positivos o falsos positivos.

B.9 Posibles derechos humanos vulnerados

Como en otros países de la región, la Constitución de la República de Guatemala, regula el derecho a la privacidad digital. En tal sentido, la base legal para dicha protección está en los siguientes artículos constitucionales:

"Artículo 24. Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegrafícas y otros productos de la tecnología moderna.

Artículo 31. Acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".[45]

Es decir, la inviolabilidad de la correspondencia, los documentos y los libros en cualquier formato que atente contra la intimidad personal, está prohíba. La intrusión a la misma solo puede darse mediante orden previa de juez competente ante quien debe sustentarse la necesidad de la misma. En el caso de la intervención a las comunicaciones telefónicas, solo puede ejecutarla la Unidad de Métodos Especiales (UME), de la Policía Nacional Civil (PNC), la cual funciona en el Ministerio Público (MP), bajo supervisión de la fiscalía.

El marco jurídico penal continúa siendo insuficiente para establecer mecanismos integrales de protección del derecho a la privacidad digital de las y los defensores de derechos humanos en el país.

B.10. Posibles tipificaciones penales

De acuerdo con la investigación de marcos legales, realizada en 2015 y actualizada en el 2018, por Fundación Acceso,[46] se puede establecer que el marco jurídico penal continúa siendo insuficiente para establecer mecanismos integrales de protección del derecho a la privacidad digital de las y los defensores de derechos humanos en el país. No obstante, el Código Penal de Guatemala, con las reformas al Decreto 17-73,[47] Capítulo VII amplía las sanciones relativas a los delitos contra los derechos de Autor, Propiedad Industrial y los Delitos Informáticos. Según dichos cambios para analizar el daño provocado y enmarcar los delitos, se podrán aplicar los siguientes criterios:

45 Asamblea Nacional Constituyente. Constitución Política de la República de Guatemala. Guatemala, 1985.
46 Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: 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 defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf y "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua" https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762
47 Código Penal de Guatemala. Disponible en: http://www.oas.org/es/sla/ddi/docs/G6%20Codigo%20Penal%20de%20Guatemala.pdf

1. Destrucción de registros informáticos. El Artículo 274 "A" señala que: "Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos".

2. Alteración de programas. El Articulo 274 "B" establece que: "La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras".

3. Reproducción de instrucciones o programas de computación. En el Articulo 274 "C" indica que: "Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación".

4. Registros prohibidos. En el Artículo 274 "D" se establece que: "Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático, con datos que puedan afectar la intimidad de las personas".

5. Manipulación de información. El Artículo 274 "E" señala que: "Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica".

6. Uso de información. Artículo 274 "F": Este indica que: "Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos".

Aún así, en lo que respecta a los datos personales, la legislación vigente en materia penal aún no contempla como delito la suplantación de identidad personal tanto en redes sociales como en otros medios digitales.

B.11. Posibles estrategias legales de respuesta

Una opción importante es el litigio estratégico para lo cual, las personas u organizaciones afectadas deberán prepararlo por medio de casos fundamentados. Estos procesos pueden ser entablados ante los órganos jurisdiccionales o el Ministerio Público. Es necesario tomar en cuenta que el litigio estratégico ha permitido promover la defensa de los derechos humanos en la región. Se trata de una herramienta que puede ser utilizada tanto por las víctimas y organizaciones de la sociedad civil, como por ciertos órganos del Estado. Por ejemplo, las oficinas generales de Fiscalía o Ministerios Públicos, así como las Defensorías del Pueblo.

En cuanto a los mecanismos legales que se podrían poner en marcha con motivo de los incidentes registrados por el Observatorio, se puede sugerir:

1. **Denuncias/Querella ante el Ministerio Público**

   En los casos registrados en Guatemala, corresponde constitucionalmente realizar denuncias ante el Ministerio Público (MP), que por mandato constitucional ejerce la acción penal pública. Por lo tanto, puede promover la persecución penal de los delitos informáticos antes mencionados y, en su defecto, podrá dirigir la investigación de los delitos cometidos en contra de las personas u organizaciones defensoras de derechos humanos.

   Mediante la cadena de custodia bajo su responsabilidad y con evidencia física y digital podrá resolver los incidentes digitales de "Compromiso de Cuentas", identificados como medio para interrumpir labores de organizaciones y personas en la defensa de los derechos humanos.

2. **Otras acciones/Recurso de Amparo**

   La Constitución de la República de Guatemala permite el recurso de Amparo ante las violaciones a la privacidad e intimidad personal. Por su naturaleza, este recurso se presenta ante la Sala de lo Constitucional de la Corte Suprema de Justicia. Es un proceso estratégico y la ley exige que la víctima cuente con la representación de un abogado experto en la materia. La **base legal del mismo está normada en:**

   > Artículo 24 "*Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegrafícas y otros productos de la tecnología moderna*".

Artículo 31 "*Acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos*".

3. Recurso de Habeas Data

Los recursos de Habeas Data son interpuestos por las víctimas o representante en los casos en que su información personal sea sustraída de una base de datos gubernamental. El decreto número 57-2008 que aprueba la Ley de Acceso a la Información Pública en su Capítulo Sexto, Artículos comprendidos del 30-34, establece la figura de Habeas Data. Esta normativa, además prohíbe la comercialización de datos personales a terceros sin la debida autorización y consentimiento del titular. Para recurrir a la acción penal en esta materia, es necesario comprobar que la persona encargada del tratamiento de los datos personales ha comercializado o compartido información sensible. De probarse el hecho, la persona responsable será sancionada con prisión de cinco a ochos años, según establece el Art. 66, sobre Responsabilidad y Sanciones en el tratamiento de la información.

4. Denuncias ante la Procuraduría de Derechos Humanos

La Procuraduría de Derechos Humanos (PDH), es la instancia estatal defensora de derechos humanos en Guatemala. Ante la misma se puede interponer denuncias en materia de violación de libertades y derechos fundamentales. La PDH vela por el efectivo cumplimiento de estos y está facultada para investigar y denunciar comportamientos lesivos a los intereses de las personas u organizaciones. Solo puede emitir sanciones de carácter moral porque está diseñada para desempeñar un rol de tribunal de conciencia. Sin embargo, tiene la obligación legal de presentar denuncias ante los órganos jurisdiccionales competentes, además de que para la designación de algunas personas titulares en cargos en el sistema de seguridad es requisito no haber sido sancionado por la PDH.

5. Denuncias ante Sistema Interamericano de derechos humanos

Guatemala es un estado parte del Sistema Interamericano de Derechos Humanos (SIDH). Su participación está regulada por la propia Constitución Política que otorga rango constitucional a los convenios y tratados internacionales de Derechos Humanos ratificados por el país. Además y

en virtud de ello, se rige en esta materia por lo establecido en el derecho internacional. Para la presentación de casos ante el SIDH se debe satisfacer varios requisitos de admisibilidad y gestión. Los mismos se gestionan inicialmente ante la Comisión Interamericana de DDHH (CIDH). De agotarse la vía ante la CIDH es esta misma instancia la que los presenta ante la Corte Interamericana de Derechos Humanos (Corte IDH), la cual por su autónoma judicial ejerce funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos. Ahora bien, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la CIDH para que el Estado adopte medidas para prevenir daños irreparables a las personas o al objeto del proceso en conexión con una petición o caso pendiente. También se pueden presentar audiencias temáticas en los períodos ordinarios de sesiones de la CIDH.

El SIDH es un buen espacio que permite documentar estos y otros casos para identificar patrones de actuación por parte de organizaciones y oficinas gubernamentales que puedan estar vigilando a defensores y defensoras de derechos humanos. Es importante que esta información sea del conocimiento de las respectivas relatorías para que pueda ser incluida en los informes periódicos de las mismas a fin de visibilizar la situación de la seguridad digital a nivel regional.

El contexto adverso para la labor de las y los defensores de derechos humanos, identificado en la investigación de Fundación Acceso de 2015, actualizada en el 2018, persiste.

B.12. Conclusiones

1. Aunque los 5 casos registrados durante este año se han clasificado como falsos positivos, es importante estar alerta y reportar los incidentes digitales. Es necesario tomar en cuenta que la seguridad digital es parte de las vulnerabilidades personales y colectivas, así como de las amenazas y ataques externos.

2. El contexto adverso para la labor de las y los defensores de derechos humanos, identificado en la investigación de Fundación Acceso de 2015, actualizada en el 2018, persiste. Prueba de ello es que en el Congreso de la República se han presentado y se discuten iniciativas de ley que carecen seguridad jurídica y de legitimidad en la defensa de los derechos humanos. En caso estas sean aprobadas, pueden perjudicar la labor de organizaciones que se dedican a la defensa, denuncia y promoción de derechos humanos.

3. Las actuales propuestas de ley sobre ciberseguridad no incorporan los derechos humanos y no han sido consultadas con la diversidad de sectores, entre ellos las organizaciones y personas defensoras. Así mismo, como lo han denunciado varias agrupaciones, atentan contra la libertad de expresión.

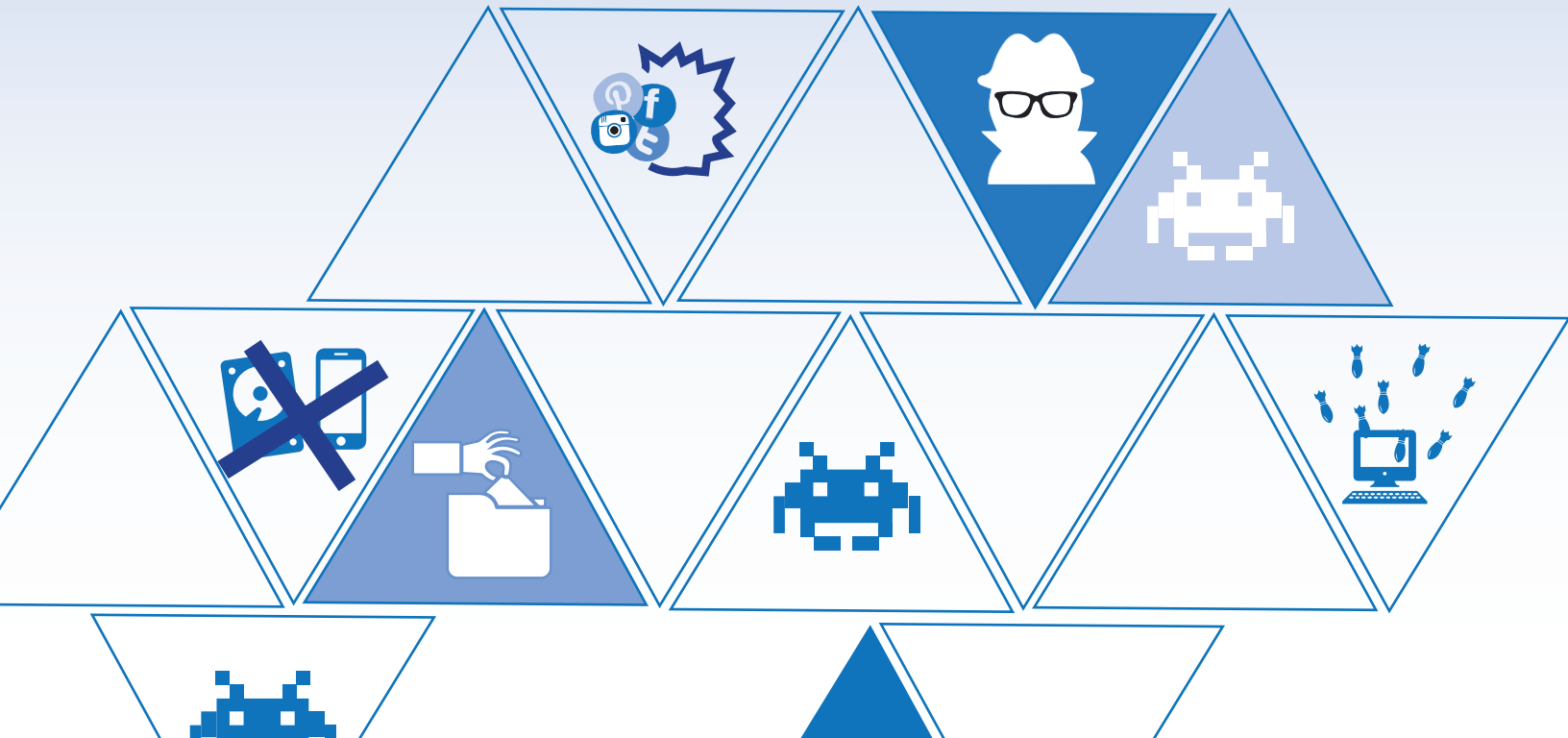
4. Ya ha sido visibilizado en el informe 2019 de la Relatoría Especial de la Situación de Personas Defensoras de Derechos Humanos de la ONU, que los incidentes digitales contra personas defensoras y colectivos de DDHH, no se están investigando lo suficiente y, por lo tanto éstas posibles violaciones están quedando también en la impunidad.

5. Las organizaciones de DDHH en Guatemala han identificado la capacidad que tienen actores estatales y no estatales para la adquisición y uso de tecnologías de vigilancia. También están más consciente de cómo los ataques digitales pueden vulnerar derechos fundamentales y constitucionales y a la vez comprometer la integridad de las personas y colectivos de defensa de derechos humanos.

6. Es necesaria la pronta aprobación de una Ley de Datos Personales que incluya procedimientos claros de Habeas Data y restrinja el uso indebido de la información personal que está siendo depositada en redes sociales o bases de datos en el Internet.

Las organizaciones de DDHH en Guatemala han identificado la capacidad que tienen actores estatales y no estatales para la adquisición y uso de tecnologías de vigilancia.

Honduras



C. CAPÍTULO HONDURAS

C.1. Seguridad Digital y Derechos Humanos en Honduras

En el 2015, Fundación Acceso llevó a cabo una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[48]. En esta se analizaron los marcos legales vinculados con el derecho a la privacidad en la región centroamericana. Como resultado de dicha investigación, se pudo establecer algunos parámetros útiles en el contexto hondureño, los cuales, casi en las mismas condiciones planteadas en esa oportunidad, continúan vigentes.

Hay un reconocimiento constitucional sobre el derecho a la privacidad. Sin embargo, en las leyes paneles existentes con respecto a la protección al derecho a la privacidad digital, esta aún no se encuentra regulada.

Por ejemplo, se pudo establecer que hay un reconocimiento constitucional sobre el derecho a la privacidad.[49] Sin embargo, en las leyes paneles existentes con respecto a la protección al derecho a la privacidad digital, esta aún no se encuentra regulada.

En febrero del 2017, el Congreso de Honduras aprobó la Ley para el Fortalecimiento y Efectividad de la Política de Seguridad, Decreto Número 6-2017. La misma contenía reformas a diferentes legislaciones tales como, el Código Penal y Procesal Penal, Ley contra el Financiamiento del Terrorismo, Ley de Inteligencia Nacional, Ley de Limitación de Servicios de Telecomunicaciones en Centros Penitenciarios, Granjas Penales y Centros de Internamiento de Niños y Niñas a Nivel Nacional, Ley Especial sobre Intervenciones de las Comunicaciones Privadas, Ley de Recompensas y Ley del Sistema Penitenciario Nacional. Dicha norma, que fue aprobada en el contexto de la lucha contra el crimen, provee un conjunto de disposiciones y modificaciones en materia penal que buscan reducir la comisión de delitos. Sin embargo, varias organizaciones locales e internacionales[50], se pronunciaron en contra de esta norma por considerar que la misma carece de enfoque de derechos humanos.

48 Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: 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 defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

49 *Ibíd.* Pág 192.

50 Amnistía Internacional. **Declaración Pública AMR 37/5587/2017 del 27 de enero de 2017**. Disponible en https://www.amnesty.org/download/Documents/AMR3755872017SPANISH.pdf

Se realizaron reformas al Código Penal y a la Ley de Centros Penitenciarios. En la primera se modificaron los delitos de Extorsión y Terrorismo la cual fue una de las más criticadas. Por ejemplo, una reforma muy preocupante es la que tipifica el delito de terrorismo, ya que su definición es muy amplía. Por lo tanto, existe un profundo temor de que pueda ser utilizada como "ley mordaza" y vulnerar la libertad de expresión. Esto porque equipara y conceptúa a las protestas ciudadanas como terrorismo[51]. Las reformas al Código Penal amplían las conductas consideradas "terroristas". En estas se incluye tanto quien cause estragos o daño a la propiedad como quien no participe directamente en esos daños pero que sí participe en un acto que sea para intimidar o causar terror al gobierno o población.

El texto aprobado tipifica la apología e incitación a actos terroristas y responsabiliza de ello a quien públicamente o a través de medios de comunicación incite a otros a cometer el delito de terrorismo. Ambas reformas se pueden analizar desde la perspectiva de las movilizaciones sociales en contra de actos de corrupción, ya que quien convoque a manifestaciones ciudadanas o participe de estas, puede ser objeto de proceso penal por tal delito. Esto vulnera derechos consagrados en la Constitución de Honduras, como los de libertad de expresión, asociación y manifestación, de todas las personas, pero en especial de las personas defensoras de derechos humanos. Estas últimas han desarrollado y continúan realizando un papel muy importante para la defensa del territorio y de la democracia. Por lo tanto, es alarmante que la criminalización de protestas ciudadanas y de la labor de defensoría sea validada a través de legislaciones que limitan libertades y derechos fundamentales.

Por otro lado, En las reformas a la Ley Especial sobre Intervenciones de las Comunicaciones Privadas, se crea la Unidad de Intervención de las Comunicaciones (UIC). Esta Unidad tiene a cargo, entre otras cosas y mediante orden de juez competente, obtener el detalle de llamadas entrantes y salientes de los dispositivos de las personas en proceso de investigación. De igualr forma obliga a los operadores de telefonía, *a garantizar sin limitaciones el acceso inmediato de la UIC a toda la información relacionada con la intervención y extracción del contenido de las telecomunicaciones.*

En 2018 la Asamblea Nacional formuló un proyecto denominado: Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación

51 El Heraldo. **Honduras: Congreso Nacional aprobó los dos artículos más polémicos de las reformas penales.** Disponible en: http://www.elheraldo.hn/pais/1046584-466/honduras-congreso-nacional-aprob%C3%B3-los-dos-art%C3%ADculos-m%C3%A1s-pol%C3%A9micos-de-las-reformas

en Redes Sociales[52]. Con ello abrió el debate sobre la legalidad de ese fenómeno. Al respecto, la Relatoría Especial para la Libertad de Expresión, de la Comisión Interamericana de Derechos Humanos (CIDH), externó su preocupación por los términos y alcance del proyecto[53].

Ese mismo año, durante la visita *in loco* de la CIDH a Honduras, ésta hizo mención de la iniciativa planteada para regular las redes sociales así como de las modificaciones al Código Penal. Destacó que dichas iniciativas podrían socavar el derecho a la libertad de expresión, en un país que ya cuenta con los más altos índices de violencia contra las personas periodistas y comunicadoras sociales: *"La libertad de expresión enfrenta un panorama de extrema complejidad en Honduras. La persistencia de elevados niveles de violencia contra periodistas y la impunidad de la mayor parte de los crímenes continúa siendo un grave problema. A este aspecto estructural hay que sumar la aparente la decisión del Poder Legislativo de mantener los delitos de injurias, calumnias y otras figuras que afectan a la libertad de expresión en la reciente reforma integral del Código Penal y la presentación de un proyecto para regular las redes sociales".*[54]

La CIDH, durante la visita in loco destaco que iniciativas legislativas podrían socavar el derecho a la libertad de expresión

Durante el 2019 ésta propuesta de ley esperaba su tercer y último debate para aprobación,. Sin embargo, gracias a la presión nacional, regional, internacional y multisectorial, el ante proyecto no avanzó.

En su informe de 2018, Amnistía Internacional hace referencia también al las reformas planteadas en el Código Penal: *"Las nuevas disposiciones del Código Penal sobre terrorismo y delitos conexos, aprobadas por el Congreso Nacional en febrero y septiembre, se definieron de una forma excesivamente amplia e imprecisa, contraria al principio de legalidad. Esas disposiciones podrían derivar en la aplicación arbitraria e inadecuada del Código contra manifestantes pacíficos y defensores y defensoras de los derechos humanos, lo cual podría criminalizar aún más su labor y obstaculizar el trabajo de los movimientos sociales".*[55]

La propuesta de reforma al código penal de Honduras ha generado muchas críticas respecto a la limitación de derechos humanos, particularmente el derecho a la libertad de expresión, así como a derechos civiles y políticos. Aunque la propuesta

52 Telesur.. Medios piden No aprobar Ley de Ciberseguridad en Honduras. Disponible en: https://www.telesurtv.net/news/medios-rechazan-ley-ciberseguridad-honduras-20180212-0038.html
53 La prensa. Ley de Ciberseguridad Amenaza la libertad de expresión. Disponible en https://www.laprensa.hn/honduras/1187050-410/ley-ciberseguridad-amenaza-libertad-expresion-cidh
54 Idem.
55 Amnistía Internacional (2017/2018). Informe anual. Disponible en: https://crm.es.amnesty.org/sites/default/files/civicrm/persist/contribute/files/Informeanual2018air201718-spanish%20web.pdf

ha tenido una gran oposición desde la sociedad civil, se teme que sea aprobada en el 2020. De ser aprobada la reforma al código penal en Honduras, se prevé un incremento de la criminialización y judicialización de personas y organizaciones que ejercen su derecho a la manifestación pública y pacífica. De igual forma se pronostica un incremento de la censura y la violación a la libertad de expresión de periodistas y personas comunicadoras sociales. Circunstancia que preocupa sobremanera en un país ya de por sí con los más altos índices de asesinatos y represión a la labor de defensoría en materia de derechos humanos y del medio ambiente.

Es importante indicar que Honduras ha suscrito diferentes acuerdos bilaterales o multilaterales en materia de seguridad. Uno de los más recientes es el Acuerdo Marco de Cooperación entre el gobierno de la República de Honduras y el gobierno del Estado de Israel, adoptado en 2016.[56] En dicho convenio se estable la cooperación para fortalecer con diversos sistemas y equipamientos al aparato de seguridad del Estado de Honduras, incluidas la Fuerza Armada y la Dirección de Investigación e Inteligencia. Llama la atención particular para el Observatorio, que el Estado de Israel acordó apoyar con un sistema informático de Seguridad del Estado (ciberseguridad), que vendría a "*fortalecer las capacidades de prevención, defensa y reacción ante eventuales ciberataques a instituciones gubernamentales, administradores de infraestructura y servicios críticos*". Es de alertar que este sistema estaría administrado y coordinado por la Dirección Nacional de Investigación e Inteligencia (DNII). En términos generales no se especifica ni publica qué tipo de sistema informático se pondría en marcha en el marco de este acuerdo.

Además de acuerdos bilaterales, se encuentran ejemplos de préstamos para adquirir equipamiento y sistemas para ciberseguridad u otros relacionados con investigación criminalística. A mediados de 2016 se realizó un préstamo con el Banco Interamericano de Desarrollo (Programa BID-Préstamo 2745/BL/HO), para la "*adquisición de Equipo para Laboratorios de Policía Científica y Criminalística de la Dirección Policial de Investigaciones –DPI*". Sin embargo, es imposible saber qué empresas obtuvieron el contrato así como qué equipamiento compraron, toda vez que el concurso no lo detalla claramente. Este se limita a describirlo como Equipo informático, Equipo audiovisual e incluso como Equipos misceláneos.[57] Similar circunstancia se da en el

56 «Acuerdo marco de cooperación entre el gobierno de la República de Honduras y el gobierno del Estado de Israel», 6 de diciembre de 2016. http://www.consejosecretariosdeestado.gob.hn/content/seguridad-y-defensa-israel-y-honduras-suscriben-acuerdo-para-potenciar-las-fuerzas-armadas

57 Expediente SS-PICSC-LPI-007-2016», Honducompras, 6 de mayo de 2016. http://sicc.honducompras.gob.hn/HC/Procesos/ProcesoHistorico.aspx?Id0=NwAAADEAAAA3AAAA-Fq0Qhrwnpd0%3D&Id1=MQA-AAA%3D%3D-OFoziWLXW%2Fg%3D&Id2=UwAAAFMAAAAtAAAAUAAAAEkAAABDAAAAUwAAAEMAAAAtA-AAATAAAAFAAAABJAAAALQAAADAAAAAwAAAANwAAAC0AAAAyAAAAMAAAADEAAAA2AAAA-ZchExUJx-gK0%3D

concurso para la "*Adquisición de equipo y software para laboratorios de informática forense de la DPI*", del mismo préstamo, cuya descripción del equipo es un "software de sistema experto", que incluía Estación de Trabajo Forense, un servidor de datos y un software de análisis forense.[58]

En otro orden de cosas, es importante recordar que en el 2015 la empresa Hacking Team sufrió una ataque digital, a partir del cual sus correos electrónicos y archivos se hicieron públicos. La organización Derechos Digitales realizó una investigación en el 2016 a partir de dichos documentos y mostró que Hacking Team fue contratado por el Estado hondureño.[59]

Un estudio realizado por la organización Derechos Digitales logró mostrar que la DNII había gastado 355,000 euros en realizar compras a la empresa Hacking Team en el año 2014.

Este mismo estudio logró mostrar que la DNII había gastado 355,000 euros en realizar compras a esta empresa en el año 2014. La adquisición la habría realizado a través de la empresa Nice, representada en la región por Ori Zoller.[60] En el 2018, el diario británico The Guardian publicó un artículo en el cual denunciaba que el gobierno británico habría autorizado la venta de sistemas de vigilancia a Honduras, antes del proceso electoral de 2017. Según este artículo, la venta de sistemas tuvo un valor de 300.000 libras esterlinas. Concretamente, se trataba de un sistema que permitiría interceptar y monitorear comunicaciones tales como correos, llamadas móviles o conversaciones en WhatsApp.[61]

Si bien el artículo no detalla cuál fue el tipo de software adquirido por Honduras, sí es bien sabido que el espionaje de comunicaciones mediante aplicaciones de Whatsapp suele requerir de la instalación de malware en el dispositivo de la persona que se quiere vigilar. Whatsapp declara contar con cifrado de extremo a extremo de manera que interceptar las comunicaciones por otras vías sería poco probable.

58 Expediente SS-PICSC-LPI-015-2018», Honducompras, 1 de junio de 2018.http://sicc.honducompras.gob.hn/HC/Procesos/ProcesoHistorico.aspx?Id0=NwAAADEAAAA3AAAA-Fq0Qhrwnpd0%3D&Id1=MQAAAA%3D%3D-OFozi-WLXW%2Fg%3D&Id2=UwAAAFMAAAAtAAAAUAAAAEkAAABDAAAAUwAAAEMAAAAtAAAATAAAAFA AAABJA-AAALQAAADAAAAAxAAAANQAAAC0AAAAyAAAAMAAAADEAAAA4AAAA-DDGicaqHWvs%3D

59 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina» (Derechos Digitales, marzo de 2016), https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

60 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina» (Derechos Digitales, marzo de 2016), https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

61 Nina Lakhani, «UK Sold Spyware to Honduras Just before Crackdown on Election Protesters», *The Guardian*, 8 de febrero de 2018, sec. World news, https://www.theguardian.com/world/2018/feb/08/uk-sold-spyware-to-honduras-just-before-crackdown-on-election-protesters

C.2. Ataques a defensoras y defensores de derechos humanos

El Grupo Asesor Internacional de Personas Expertas,[62] asegura en su informe que Honduras presenta desde el 2009 un contexto de violencia sistemática en contra de defensoras y defensores de derechos humanos. Incluso ha sido considerado por Global Witness[63] como el país más peligroso del mundo para defender el planeta, por el alto índice de persecución, detención y asesinatos de personas defensoras de los derechos al agua y medio ambiente. Grupo Asesor Internacional de Personas Expertas,[64] asegura en su informe que Honduras presenta desde el 2009 un contexto de violencia sistemática en contra de defensoras y defensores de derechos humanos.

Organizaciones dedicadas a la defensa de derechos humanos y medios de comunicación independientes, han sido objeto de vigilancia, acoso, amenazas, robo de dispositivos e información, persecución, criminalización y judicialización e incluso atentados en contra de su integridad física y su vida.

Tanto organizaciones que se dedican a la defensa de derechos humanos así como medios de comunicación independientes, han sido objeto de vigilancia, acoso, amenazas, robo de dispositivos e información, persecución, criminalización y judicialización e incluso atentados en contra de su integridad física y su vida.

En sus informes, Michel Forst, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas ha mostrado preocupación "*por la falta de investigaciones independientes y diligentes sobre las agresiones cometidas contra los defensores de los derechos humanos ambientales, hecho que suele estar vinculado a la falta de recursos, la corrupción y la colusión entre los autores. Los Estados casi nunca han conseguido hacer comparecer ante la justicia a los autores y que estos fueran sancionados*".[65]

Según Global Witness, tras el Golpe de Estado del 2009 más de 120 personas defensoras de la tierra y el medio ambiente han sido asesinados en Honduras[66], la mayoría de casos sigue en la impunidad por diferentes razones. Entre otras, desde

62 Grupo Asesor Internacional de Personas Expertas (2017). **Represa de violencia: El plan que asesinó a Berta Cáceres.** Disponible en: https://www.cejil.org/sites/default/files/represa_de_violencia_es_final_.pdf Pág. 11.
63 Global Witness (2017). **Honduras: el lugar más peligroso para defender el planeta.** Disponible en: https://www.globalwitness.org/documents/18802/Spanish_single_v6.pdf
64 Grupo Asesor Internacional de Personas Expertas (2017). **Represa de violencia: El plan que asesinó a Berta Cáceres.** Disponible en: https://www.cejil.org/sites/default/files/represa_de_violencia_es_final_.pdf Pág. 11.
65 Relatoría Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas. **Informe sobre la Situación de los defensores de los derechos humanos 2016.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement
66 *Ibíd*. Pág. 5.

la falta de voluntad política hasta corrupción del Gobierno, Ejército y empresas extractivistas. El gobierno hondureño, por medio de sus fuerzas de seguridad ha institucionalizado prácticas de control y represión a todos los niveles.

Freedom House, en su informe del 2017 sobre Libertad de Prensa, cataloga a Honduras como un país no libre.[67] La metodología del informe utiliza parámetros como entornos legales, políticos y económicos. Según los cuales, hay libertad si los medios de comunicación, impresos, radiales o digitales, ejercen plenamente su labor informativa y sin miedo a represalias, ante actores privados, políticos e incluso del crimen organizado. La organización indica, además, que Honduras continúa siendo uno de los países más peligrosos en el mundo para que las y los periodistas ejerzan su labor.[68]

Es necesario anotar que durante el proceso de la elección presidencial del 26 de noviembre 2017, estas prácticas de violencia política y represión de la protesta social se han extendido a toda la ciudadanía. Por ejemplo, se declaró Estado de Excepción[69] y con ello se restringieron garantías constitucionales. La inconformidad de la población frente a los resultados de las votaciones ante la sospecha de un posible fraude electoral fue expresada mediante protestas. En ese marco se constató excesivo uso de la fuerza por parte de las fuerzas de seguridad. Incluso se documenta varias personas detenidas, heridas e incluso fallecidas en todo el país.[70]

Freedom House, en su informe del 2017 sobre Libertad de Prensa, cataloga a Honduras como un país no libre.

Amnistía Internacional en su informe anual[71] del 2017, destacó que se ha acusado al Ejército de infiltrarse en movimientos sociales, además de atacar a defensores y defensoras de derechos humanos. En este sentido, la Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia[72] sigue sin ser aplicada adecuadamente.

Entre el 30 de julio y el 3 de agosto de 2018, la Comisión Interamericana de Derechos Humanos (CIDH) realizó una visita *in loco* a Honduras, con el objetivo de observar en terreno la situación de derechos humanos en el país. En su informe inicial, la

67 Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon.** Disponible en: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf Pág. 24.
68 *Ibíd.* Pág. 21.
69 Reuters. **Honduras suspende garantías constitucionales en medio de fuertas protestas tras elecciones.** Disponible en: https://lta.reuters.com/article/domesticNews/idLTAKBN1DV4UW-OUSLD
70 Amnistía Internacional. **Honduras: represión violenta después de elecciones.** Disponible en: https://www.amnesty.org/es/documents/amr37/7550/2017/es/
71 Amnistía Internacional (2017). **Informe anual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Págs. 225-226.
72 Congreso Nacional de Honduras. **Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia.** Disponible en: http://www.tsc.gob.hn/leyes/Ley_Proteccion_defensores_der_humanos_periodistas_op_just.pdf

Comisión indicó que "...*ha observado asuntos de orden estructural en materia de justicia, seguridad, desigualdad y discriminación, que han afectado durante décadas los derechos humanos de sus habitantes. A partir del golpe de Estado de 2009, se produjeron graves violaciones a los derechos humanos que vulneraron a la población hondureña, y cuyas repercusiones persisten.*"[73]

En su informe 2019, Amnistía Internacional hace énfasis en el incremento de la criminalización y judicialización de personas defensoras de la tierra, el territorio y el medio ambiente en Honduras: "...*seguían sufriendo niveles elevados de violencia, que incluía amenazas, intimidación y asesinatos, así como estigmatización y campañas de desprestigio en las redes sociales. Muchas de estas personas fueron sujeto de procedimiento judiciales infundados concebidos para intimidarlas y hostigarlas, y para obstaculizar su labor de derechos humanos...Por ejemplo, algunos miembros del Comité Municipal de Defensa de los Bienes Comúnes y Públicos enfrentaron un proceso penal ante tribunales que normalmente se ocupaban de casos relacionados con la delincuencia organizada*".[74]

En su informe 2019, Amnistía Internacional hace énfasis en el incremento de la criminalización y judicialización de personas defensoras de la tierra, el territorio y el medio ambiente en Honduras.

En el informe de Global Witness (2020), Defending Tomorrow, la organización alerta que 212 personas defensoras del ambiente en el mundo fueron asesinadas. De éstas, 32 en Centroamérica: 14 en Honduras, 12 en Guatemala, 5 en Nicaragua y 1 en Costa Rica.[75]

En el informe de Front Line Defenders 2019, se indica que el número de asesinatos en Honduras se cuadruplicó en comparación con el 2018. Además expone: "*El proyecto del Observatorio de Personas Trans Asesinadas (Trans Murder Monitoring, TMM por sus siglas en inglés), confirmó un total de 331 casos de asesinatos reportados de personas trans y de género diverso entre el 1 de octubre de 2018 y el 30 de septiembre de 2019. El 7 de julio, la defensora hondureña Bessy Ferrera fue asesinada a tiros por hombres no identificados. Su asesinato confirma el clima de violencia extrema en el que operan las personas LGBTI+, especialmente los y las defensoras de los derechos de las personas trans y trabajadoras sexuales.*"[76]

---

73 Comunicado de prensa, (www.oas.org). OBSERVACIONES PRELIMINARES DE LA VISITA DE LA CIDH A HONDURAS. Disponible en: https://www.oas.org/es/cidh/prensa/comunicados/2018/ObsPrelHnd.pdf

74 Amnistía Internacional (2019). **Los Derechos Humanos en las Américas.** Disponible en: https://www.amnesty.org/download/Documents/AMR0113532020SPANISH.PDF Página 61.

75 Defender el mañana: La crisis climática y amenazas contra defensores de la tierra y el medio ambiente. Global Witness (2020). Disponible en: https://www.globalwitness.org/es/defending-tomorrow-es/

76 Análisis Global de Front Line Defenders 2019. Disponible en: https://www.frontlinedefenders.org/sites/default/files/spanish_-_global_analysis_2019_web.pdf

En cuanto a ataques digitales a nivel global en 2019, Front Line Defenders menciona que *"Los ataques más comunes por los que se solicitó el apoyo de Front Line Defenders fueron las campañas de difamación, los trolls, el acoso, y el acceso no autorizado a las cuentas de redes sociales, de donde se obtuvo información para poner en peligro la reputación y seguridad de las personas defensoras"*. Así mismo indican, *"El robo y la confiscación de dispositivos también representaron un riesgo significativo para estas personas. En los casos en los que las autoridades confiscaron dispositivos, incluso estando cifrados, las personas defensoras se vieron obligadas a dar sus contraseñas, lo que les permitió el acceso a información confidencial. En general, estos dispositivos rara vez estaban cifrados y casi nunca se realizaron copias de seguridad. A veces dicha información fue utilizada como prueba para enjuiciar a los/as defensores/as o tomar medidas contra sus redes. ...El acoso en las redes sociales fue algo cotidiano para miles de defensores y defensoras, y las personas marginadas de la sociedad fueron a menudo las más atacadas"*.[77]

*Durante el periodo revisado, se registraron **dos casos** e incidentes de seguridad digital con diferentes componentes y móviles. Uno se realizó en Catacamas, Olancho y otro en Tegucigalpa.*

C.3. PRINCIPALES HALLAZGOS EN HONDURAS

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Honduras. Los mismos han sido registrados entre junio y diciembre de 2019. Para desarrollar el monitoreo se construyó un conjunto de herramientas tanto técnicas como legales, para definir los criterios de registro de los mismos.

C.4. Casos registrados

Durante el periodo revisado, se registraron **dos** casos e incidentes de seguridad digital con diferentes componentes y móviles. Uno se realizó en Catacamas, Olancho y otro en Tegucigalpa.

C.5. Perfil de las personas/organizaciones que reportaron incidentes

El primer caso trata de un defensor e integrante de un colectivo del movimiento estudiantil hondureño. En tanto que el segundo caso está relacionado con un defensor

77 Ídem, página 22

de una organización de acompañamiento internacional a personas defensoras en Honduras.

C.6. Tipos de ataques

A continuación se describen brevemente los incidentes registrados.

En cuanto al primer caso, el defensor contacta al técnico del Observatorio por medio de mensajería instantánea. Indica que sospecha de una usurpación de identidad en redes sociales, específicamente en cuentas de Facebook. El defensor notificó que las dos personas afectadas habían descubierto publicaciones en la red social Facebook bajo sus identidades y señaló que dichas publicaciones habían sido usadas para difamar al propio movimiento estudiantil.

El técnico del Observatorio guió al defensor mediante video-llamada con el fin de realizar el análisis de la computadora en la cual, ambas personas accedían a sus cuentas de Facebook. El procedimiento consistió en la instalación de antivirus y antimalware, para determinar la presencia de intrusiones o posible robo de contraseñas. Posteriormente se procedió a la revisión de *logs* del sistema para verificar si existieron accesos y comparar horas de acceso con las publicaciones encontradas. Se determinó que las publicaciones correspondían a la copia exacta de los perfiles ya existentes y a través de estos perfiles falsos se habían realizado las publicaciones. Se concluye que es un incidente de "Compromiso de Cuentas" y se registra como positivo y en verificación. Dicho caso se derivó a la línea de ayuda (Help Line) de Access Now para su posterior análisis y asesoría.[78]

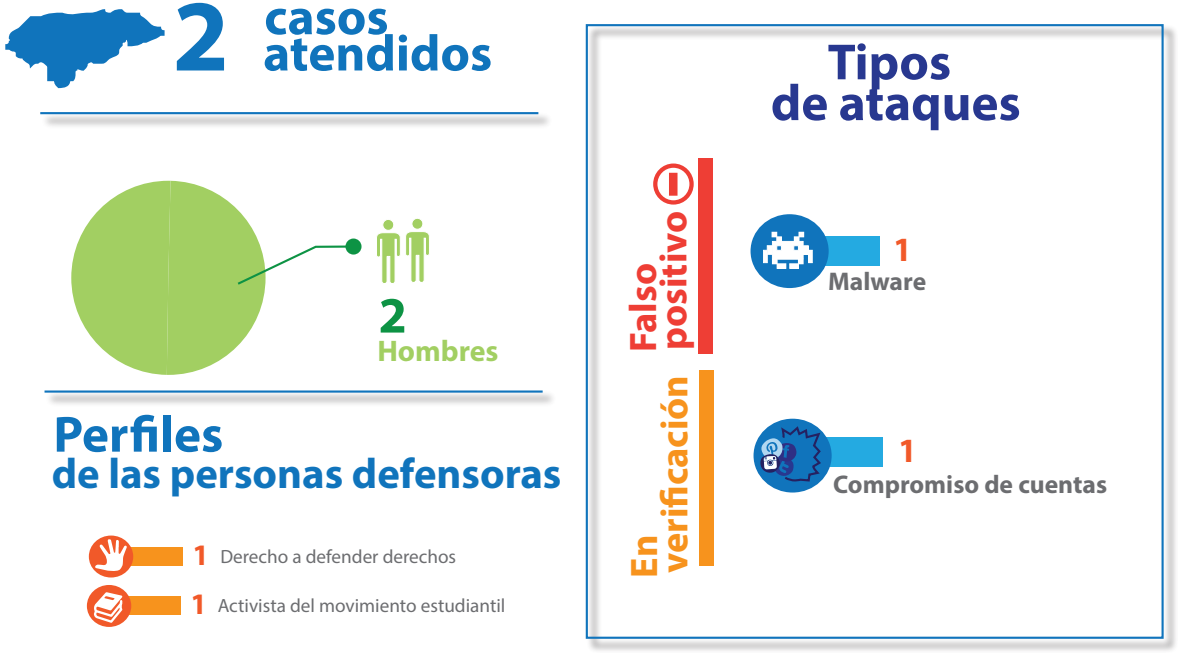
En cuanto al segundo caso, el defensor de la organización de acompañamiento internacional presente en Honduras, contacta al técnico del Observatorio e indica una supuesta extorsión por infección de virus en la computadora. El técnico realiza una visita al defensor con el fin de revisar su computadora. El defensor recibió un correo electrónico intimidatorio en el cual le expresaban que habían infectado su computadora con un virus y que si no pagaba una suma de dinero, se publicarían todos los archivos que estaban en la computadora afectada.

En primer lugar se analizó la computadora para identificar si había infección de malware. Como resultado, se determinó la imposibilidad de que hubiese una infección del tipo

78 Una vez derivado un caso de Access Now, éste le da seguimiento y queda en sus propios registros de asistencia y apoyo.

de malware como la ,que se describía en el correo electrónico recibido debido a que la computadora funcionaba con GNU/Linux y el virus/malware descrito funcionaba solo para Windows. Se procedió al análisis del trafico de la máquina durante 24 horas y posteriormente a dicho análisis se determinó que no existía ningún tipo de conexión anómala o flujos de información que no proviniesen de fuentes legítimas.

Posteriormente se examinó el código fuente del correo recibido. Se concluyó que dicho incidente correspondía a un correo masivo (Spam) que fue enviado a múltiples personas. El correo del defensor fue recopilado por *Spider Phishing* (técnica de navegación automatizada que busca patrones de cadenas determinadas en sitios web o el Internet mismo) y que el correo del defensor se encontraba publicado en el sitio web de la organización. El incidente es catalogado como "malware" y es como un ataque falso positivo.



C.7. Posibles perpetradores

En el primer caso se identifican perfiles falsos que se hacen pasar por las personas afectadas. En el segundo caso, se identifica que el perpetrador es un actor anónimo que quiere realizar estafas. Este envía correos masivos que se recopilan con *Spider Phishing* (técnica de navegación automatizada que busca patrones de cadenas determinadas en sitios web o el Internet mismo).

En el primer caso se identifican perfiles falsos que se hacen pasar por las personas afectadas. En el segundo caso, se identifica que el perpetrador es un actor anónimo que quiere realizar estafas.

C.8. Mecanismos de Protección

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de Honduras del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos, a pesar de que un caso ha sido identificado como falso positivo.

C.9. Posibles derechos humanos vulnerados

La Constitución Política de la República de Honduras garantiza el derecho a la privacidad Digital en:

> Artículo 76.- Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

La Constitución también garantiza otros derechos fundamentales como el derecho a la libertad de expresión por medio de la Ley de emisión del Pensamiento que brinda protección en la difusión de ideas y pensamientos en medios digitales o redes sociales y fomentando así el derecho a la circulación de información en línea. Están reconocidos en:

> Articulo 72.- Es libre la emisión del pensamiento por cualquier medio de difusión, sin previa censura. Son responsables ante la ley los que abusen de este derecho y aquellos que por medios directos o indirectos restrinjan o impidan la comunicación y circulación de ideas y opiniones.

Ambos preceptos constitucionales garantizan la protección de las libertades individuales, inclusive cuando el Estado y grupos de poder por acción u omisión y en beneficio de interés particular deseen censurar información depositada en

teléfonos celulares, equipo informático y dispositivos inteligentes de las personas y las organizaciones defensoras de derechos humanos.

C.10. Posibles tipificaciones penales

A partir de la investigación de marcos legales, realizada en 2015 por Fundación Acceso y actualizado en el 2018,[79] se pudo establecer que a pesar de las reformas al marco jurídico penal en 2017, este continúa siendo insuficiente para aplicar mecanismos integrales de protección del derecho a la privacidad digital de las personas defensoras de derechos humanos en el país. A efectos de no contar con una tipificación de los delitos a la privacidad y los delitos informáticos, deberá identificarse las mismas acciones que imponen los delitos homólogos dentro de su acción penal. Es decir, el mismo delito y la misma pena ya sea a una persona que vulnere el correo postal o a una persona que se valga de un programa informático para vulnerar el correo electrónico de una persona u organización.

Dado que los delitos informáticos pueden adoptarse a múltiples figuras delictivas en la legislación analizada, el Capítulo V hace relación en cuanto a los delitos de Coacciones y Amenazas entre las principales acciones penales que podrían ser de apoyo:

> Artículo 207. El particular que amenazare a otro con causar un mal a él o a su familia, en su persona, honra o propiedad, sea que constituya delito o no, será sancionado con reclusión de seis meses a dos años, y además, a las medidas de seguridad que el Juez determine.

El fraude o estafa a través de un de un programa informático, también se regula en el Capítulo VI que define las figuras de Estafa y Otros Fraudes, su base legal:

> Artículo 240. Comete el delito de estafa quien con nombre supuesto, falsos títulos, influencia o calidad simulada, abuso de confianza, fingiéndose dueño de bienes, créditos, empresas o negociación o valiéndose de cualquier artificio,

79 Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: 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 defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf y "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua" https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762

astucia o engaño, indujere a otro en error, defraudándolo en provecho propio o ajeno. Las sanciones varían en cuanto cuantía defraudada y su sanción con prisión están entre dos y siete años de cárcel.

Seguido de otras acciones penales y civiles en las que podría estar incurriendo el *hackeo* informático si expone información o comparte datos sensibles o privados de los teléfonos celulares, equipo informático y dispositivos inteligentes, que pongan en peligro la seguridad física de las personas.

C.11. Estrategias legales de respuesta

El litigio estratégico es una opción que vale la pena que consideren las organizaciones y personas afectadas. Necesitan un caso bien fundamentado para presentarlo ante órganos jurisdiccionales o la fiscalía. Cabe destacar que el litigio estratégico es una herramienta que ha permitido promover la defensa de los derechos humanos en la región. Puede ser utilizada tanto por las víctimas directas como por organizaciones de la sociedad civil. Incluso algunos órganos del Estado como Ministerios Públicos y Defensorías del Pueblo.

En cuanto a mecanismos legales que se podrían poner en marcha en el marco de los incidentes registrados por el observatorio, podemos considerar:

1. Denuncias / Querella ante el Ministerio Público

En Honduras, por ley corresponde al Ministerio Público la persecución penal. Por lo tanto, en los casos registrados por el Observatorio o en casos futuros, corresponde presentar las denuncias ante este organismo puesto que, por su naturaleza, ejerce la acción penal pública, en el sector justicia. Por ley, bajo su jurisdicción se lleva a cabo la persecución de los delitos identificados. Está obligado a dirigir la investigación en favor de las personas u organizaciones defensoras de derechos humanos, afectadas por estos delitos.

Mediante la cadena de custodia bajo responsabilidad del Ministerio Público y con base en evidencia científica (física y digital), puede conducirse una acción crucial para resolver los delitos de estafa y amenazas. Mismos que pueden ser los principales medios para interrumpir las labores de organizaciones y personas que defienden derechos humanos.

2. Recurso de Habeas Data

La Constitución de la República de Honduras establece la acción de Habeas Data, la cual constituye un mecanismo procedimental de aplicación inmediata por las autoridades jurisdiccionales hondureñas. Este recurso faculta a las autoridades para cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen. Por su naturaleza se presenta ante la Sala de lo Constitucional de la Corte Suprema de Justicia y es un proceso estratégico que exige la representación de un abogado experto en la materia. Para entablar el recurso de *Habeas Data* se debe considerar el siguiente artículo:

> Artículo 76 "Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen".

Al igual que el Decreto Legislativo N° 381-2005 que reformó el Capítulo I, del Título IV de la Constitución de la República, en el cual el Estado de Honduras establece la garantía del habeas data. En esta se reconoce: "Que toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y /o enmendarla".

3. Denuncias ante Mecanismo Nacional de Protección a Defensores/as de Derechos Humanos

En Honduras existe el Mecanismo Nacional de Protección a Defensores/as de Derechos Humanos, Periodistas y Comunicadores Sociales y Operadores de Justicia. Este mecanismo tiene la obligación de investigar los hechos denunciados y proteger la integridad de las personas defensoras, así como de evitar que, se les obstaculice su labor. Sin embargo, solo contempla medidas de protección física y, parcialmente, psicológica y legal. No contiene protección relacionada con la seguridad digital de las personas defensoras beneficiarias. Está a cargo de la Secretaría de Estado en el Despacho de Seguridad, específicamente, en el Departamento de Derechos Humanos.

4. Recursos ante el Sistema Interamericano de Derechos Humanos

El Estado de Honduras es parte del Sistema Interamericano de Derechos Humanos (SIDH). En tanto tal, se haya sujeto a las regulaciones que para esto define el internacional. Cualquier caso que se presente ante el SIDH debe reunir los requisitos que la normativa de este define. Como trámite, ha de ir en primera instancia ante la Comisión Interamericana de Derechos Humanos

(CIDH), cumpliendo las condiciones de admisibilidad. Una vez agotada la vía en la CIDH, es esta la que lleva el caso ante la Corte IDH. Tanto la Comisión como la Corte, por su autónoma judicial ejercen funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos.

En situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la CIDH, para que el Estado adopte medidas para prevenir daños irreparables a las personas o al objeto del proceso en conexión con una petición o caso pendiente.

Además de la posible presentación en audiencias temáticas ante la CIDH, las conclusiones del Observatorio son un recurso valioso que puede permitir documentar estos y otros casos para identificar patrones de actuación por parte de organizaciones y oficinas gubernamentales que puedan estar vigilando a defensores y defensoras de derechos humanos. Esta información puede ser puesta en conocimiento de las respectivas Relatorías de la CIDH para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

C.12. Conclusiones

Persiste la ausencia de marcos jurídicos adecuados en la defensa de los derechos en línea para la protección de las comunicaciones y privacidad digital.

1. Si bien Honduras cuenta con un Sistema Nacional de Protección para personas Defensoras de Derechos Humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia, este carece de institucionalidad en su funcionamiento. Desde su creación se han identificado muchas deficiencias en respuesta eficaz y eficiente. A tal grado que Honduras ha sido catalogada como uno de los países más peligrosos para ejercer la labor de defensa de derechos humanos.

2. Persiste la ausencia de marcos jurídicos adecuados en la defensa de los derechos en línea para la protección de las comunicaciones y privacidad digital. Algo que fue identificado en su momento en la investigación realizada por Fundación Acceso en el 2015 y actualizada en 2018.

3. El Gobierno hondureño ha invertido millones de lempiras para la implementación de su sistema de inteligencia, el cual no incluye en los mecanismos de control y vigilancia, los estándares internacionales en materia de derechos humanos.

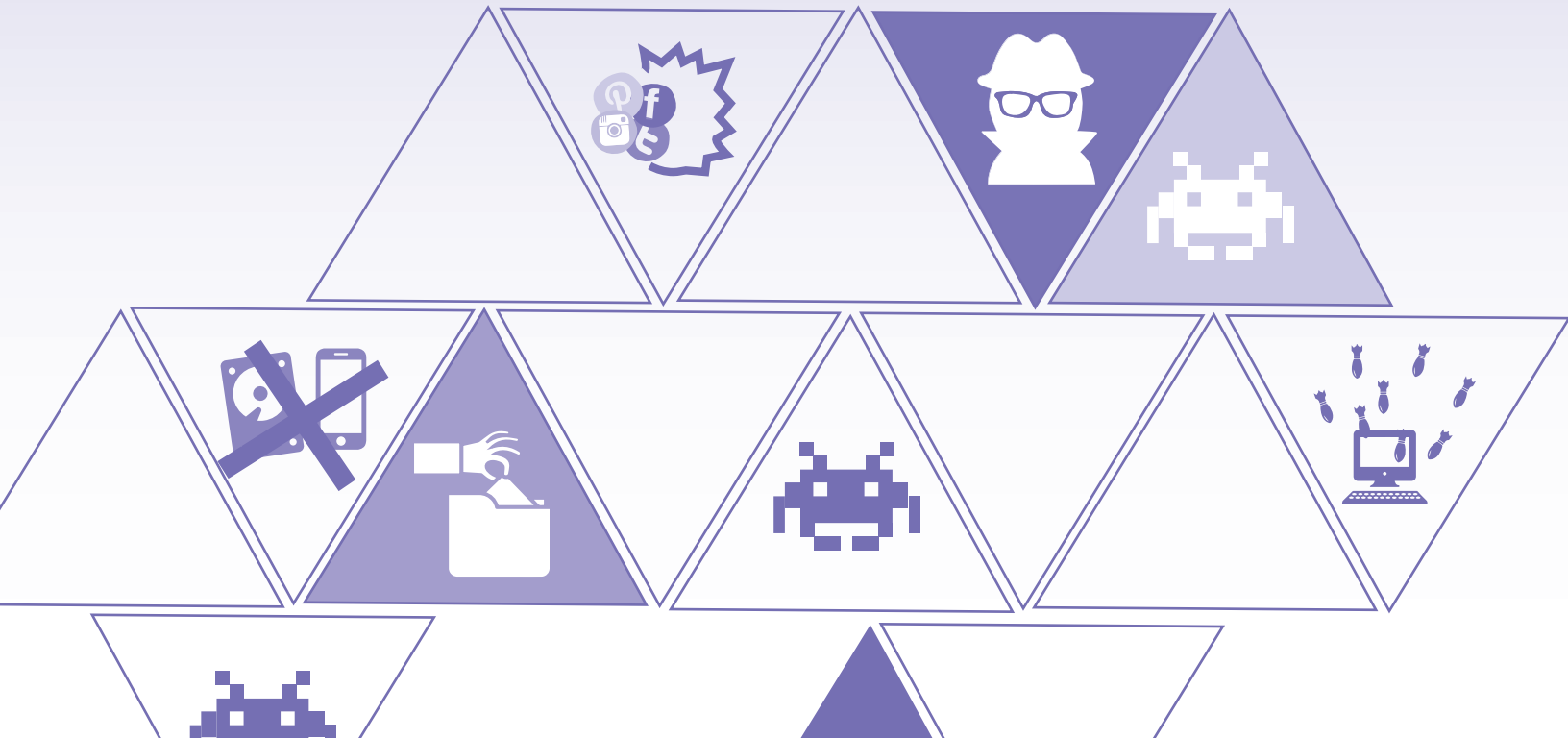
4. La amenaza que sufren directamente las personas defensoras de derechos humanos y periodistas independientes en el país, va desde la física hasta la digital. En este sentido, el riesgo al que estas personas son sujetas en su labor diaria incluye, entre otras cosas, el peligro a que se lesione su integridad física e incluso la vida, así como perjuicio a la información que generan alrededor de su trabajo y lucha cotidiana.

5. El tema de seguridad digital sigue estando ausente de los informes que tratan sobre la seguridad de las y los defensores de derechos humanos. Esta circunstancia genera áreas de vulnerabilidad a través de las cuales se les puede atacar.

6. Es necesaria la pronta aprobación de una Ley Ordinaria de Datos Personales que incluya procedimientos claros en habeas data y restrinja el uso indebido de la información personal depositada en base de datos o en la Internet.

7. En la actualidad, Honduras carece de una legislación adecuada en la materia, en el Código Penal. Se observan limitantes en la tipificación de delitos relacionados con la privacidad así como delitos informáticos y sus conexos. Esto dificulta la persecución delictiva por parte del Ministerio Público.

Nicaragua



D. NICARAGUA

D.1. Seguridad Digital y Derechos Humanos en Nicaragua

En el informe de la investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[80], desarrollada por Fundación Acceso en 2015, se examinó el marco legal aplicable para el derecho a la privacidad en varios países de Centroamérica. Como resultado de dicha investigación se pudo establecer un grupo de parámetros aplicables para analizar el fenómeno en cada contexto nacional. Parámetros que a la fecha, continúan vigentes pues aún se mantienen casi sin variación, las condiciones en las que se realizó el estudio.

En el caso de Nicaragua se pudo establecer que a nivel general hay un reconocimiento en la Constitución, sobre el derecho a la privacidad.

Como en otros países, en el caso de Nicaragua se pudo establecer que a nivel general hay un reconocimiento en la Constitución, sobre el derecho a la privacidad[81]. Sin embargo, la legislación ordinaria vigente, relaciona la penalización de este derecho con la indebida utilización de la privacidad digital.

Es importante destacar lo regulado en la Ley de Seguridad Soberana de la República de Nicaragua, Ley No. 919 del 2 de diciembre de 2015. En el artículo 8, esta ley determina que los ataques a la seguridad cibernética, principalmente aquellos que afecten los sistemas de comunicación nacional, son considerados como amenazas a la seguridad soberana[82]. Sin embargo, la ley no hace una determinación clara de lo que considera como "ataque cibernético", lo cual puede llegar a ser claramente perjudicial porque el marco normativo es muy amplio y ambiguo. En su artículo 13 **prohíbe** a las entidades públicas que forman parte del Sistema Nacional de Seguridad lo siguiente: realizar espionaje político, obtener o almacenar información

80 Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: 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 defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

81 *Ibíd.* Pág 260.

82 Dada la situación de crisis socio-política en Nicaragua y el enfoque represivo a las expresiones de disidencia social, es altamente preocupante que en una norma de esta naturaleza se utilicen conceptos como los de Seguridad Soberana que son equiparables a la Doctrina de Seguridad Nacional (DSN), puesta en vigor en América Latina en el marco de la guerra fría.

o datos sensibles de organizaciones sociales, asimismo la intercepción e intervención de comunicaciones, sin orden de juez competente. Esto último, refleja, al menos en el texto legal, que los mecanismos de vigilancia masiva deben cumplir con algunos de los principios y estándares internacionales. Entre estos, la legalidad, la autoridad judicial competente y el debido proceso.

Organizaciones de la sociedad civil como el Instituto de Estudios Estratégicos y Políticas Públicas (IEEPP), manifestaron su rechazo a esta ley ya que se enmarca en un proceso de reforma que habría tenido como objetivo "*profundizar un modelo donde los cuerpos armados predominan sobre las instituciones civiles, manteniendo su subordinación únicamente al Presidente de la República*"[83]. En este sentido, se plantea la preocupación por la falta de mecanismos de control civil. En un recurso de amparo, el Centro Nicaragüense de Derechos Humanos (CENIDH) también planteó sus preocupaciones con respecto a esta ley. En primer lugar, la ley le estaría atribuyendo soberanía a la seguridad, un concepto contradictorio, que implicaría darle a la seguridad un estatus superior a otros ámbitos y desconocería, al mismo tiempo, que la soberanía reside en el pueblo.[84] Finalmente, es importante señalar que Nicaragua no cuenta con normativa específica relativa a la[85] ciberseguridad. Además de que Nicaragua no es firmante del Convenio de Budapest sobre ciberdelincuencia.

Organizaciones como IEEPP y CENIDH han expresado su preocupación con respecto a la Ley de Seguridad Soberana.

Con respecto a prácticas de vigilancia, en su informe sobre la Situación de los derechos humanos en Nicaragua del CENIDH detallan que: "*...en enero 2019 la Asamblea Nacional había aprobado la Ley 985 Para una Cultura de Diálogo, Reconciliación, Seguridad, Trabajo y Paz, a través de la cual según ellos es para 'promover un modelo de reconciliación y convivencia armoniosa y una cultura de paz entre los nicaragüenses', materializada en la conformación de comisiones de reconciliación justicia y paz a nivel nacional, conformadas por los llamados Consejos del Poder Ciudadano o CPC, bases fieles y fanatizadas del partido FSLN, a través de los cuales* ***ejercen la vigilancia*** *y el control social, persiguen y amenazan a cualquier persona que difiera o critique las políticas gubernamentales,* ***institucionalizándose de esta forma un sistema de espionaje"***.[86]

83 Artículo Envío Digital. IEEPP. «10 peligros de la Ley de Seguridad Soberana». Disponible en: https://www.envio.org.ni/articulo/5121

84 Publicación en web del CENIDH. Disponible en: https://www.cenidh.org/noticias/871/

85 Asamblea Nacional de Nicaragua. «Ley de Defensa Nacional de la República de Nicaragua» (Asamblea Nacional de Nicaragua, 13 de diciembre de 2010). Disponible en: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/9F1F361C509ED3F706257825004FE9BC?OpenDocument.

86 CENIDH. Situación de los derechos humanos en Nicaragua, 2018-2019. Nicaragua, 2020. pp. 32. El subrayado es nuestro. Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_2018-2019_v.final.pdf

Es importante resaltar que en la Ley 735, "Ley de Prevención, Investigación y Procesamiento de la Delincuencia Organizada y Administración de Bienes Incautados, Confiscados y Abandonados"[87], en el capítulo VIII, Artículo 65, se establece que "*Las empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica y otras que utilicen el espectro electromagnético y radioelectrónico, ya sean personas naturales o jurídicas deberán prestar todas las condiciones y facilidades materiales y técnicas necesarias para que las intervenciones sean efectivas, seguras y* ***confidenciales*** *y estarán obligadas a permitir que se usen sus equipos e instalaciones para la práctica de las diligencias de investigación antes previstas. Las empresas que prestan los servicios aquí relacionados deben llevar un registro oficial de los usuarios o clientes que utilicen los servicios, los que podrán ser requeridos por autoridad competente para fines de investigación, persecución y proceso penal*". En general, y como bien lo apunta el comunicado de Access Now al respecto, "*Este* ***deber de confidencialidad*** *no parece expirar. Tampoco existe una obligación legal para el Estado o las empresas a notificar a los usuarios cuando sean sujetos de vigilancia*".[88]

La concetración de poder en la pareja presidencial ha provocado situaciones que van desde la destitución arbitraria de diferentes funcionarios y funcionarias del sector público opositores, hasta la limitación de diferentes derechos fundamentales.

D.2. Ataques a defensoras y defensores de derechos humanos

Daniel Ortega tomó posesión como Presidente, por tercera vez, el 10 de enero de 2017. Junto a él, su esposa Rosario Murillo asumió como Vicepresidenta. Desde entonces, la concentración del poder en esta pareja ha impactado en diferentes ámbitos de la institucionalidad en Nicaragua. Destacan situaciones que van desde la destitución arbitraria de diferentes funcionarios y funcionarias del sector público opositores,[89] hasta la limitación de diferentes derechos fundamentales.

Desde antes de la crisis de abril de 2018 y en forma continuada desde entonces, las defensoras y defensores de derechos humanos continúan siendo objeto de intimidación y amenazas por su labor. Tanto por sus actividades de registro de

87 Poder Judicial de Nicaragua. "Ley de Prevención, Investigación y Procesamiento de la Delincuencia Organizada y Administración de Bienes Incautados, Confiscados y Abandonados" Disponible en: https://www.poderjudicial.gob.ni/pjupload/comjib/Ley735.pdf

88 Comunicado Access Now. El subrayado es nuestro. Disponible en: https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/

89 CEJIL (2017). **Nicaragua: ¿cómo se reformó la institucionalidad para concentrar el poder?** Disponible en: https://www.cejil.org/sites/default/files/informe_cejil_sobre_nicaragua_-_derechos_politicos.pdf Pág. 22.

violaciones de derechos humanos, como por la denuncia internacional y los procesos de defensa en el sistema de justicia nacional. Al respecto, la Comisión Interamericana de Derechos Humanos (CIDH) ha denunciado la persistencia de la represión en Nicaragua y expresado su preocupación por el alza en el hostigamiento a personas defensoras de derechos humanos así como abogadas y abogados de personas excarceladas y/o que permanecen detenidas por hechos vinculados con las protestas iniciadas el 18 de abril de 2018.[90]

El *26 de agosto*, expertos en derechos humanos de Naciones Unidas y el Relator Especial para la libertad de expresión de la CIDH, denunciaron la represión sistemática contra los medios de comunicación y periodistas independientes en el país: CIDH denuncia la persistencia de la represión y expresa su preocupación por incremento de hostigamiento contra personas defensoras de derechos humanos y excarceladas en Nicaragua.[91]

En su informe sobre la Situación de los derechos humanos en Nicaragua, el CENIDH menciona la aprobación inconsulta y expedita de la Ley de Atención Integral a Víctimas (Ley 994) y la Ley de Amnistía (Ley 996) *"...se instrumentaliza una vez más al Poder Legislativo –bajo su control absoluto— para crear de manera expedita e inconsulta una inocua Ley de Atención Integral a Víctimas (Ley 994) y la Ley de Amnistía (Ley 996) que riñe con el derecho internacional y pretende borrar o dejar en la impunidad los crímenes de lesa humanidad cometidos por sus fuerzas de choque y policías. La Comisión Interamericana de Derechos Humanos (CIDH) y la Oficina Regional de la Alta Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) expresaron su preocupación por la aprobación de dicha Ley "por no cumplir con las normas y estándares internacionales en materia de verdad, justicia, reparación y garantías de no repetición"*.[92]

"Defensores de derechos humanos y otros actores críticos del gobierno en materia de derechos humanos se han convertido en blanco creciente de amenazas de muerte, intimidación, campañas de difamación en línea, hostigamiento, vigilancia, agresiones y persecución judicial" Human Rights Watch

Human Rights Watch alerta en su informe más reciente que "*Defensores de derechos humanos y otros actores críticos del gobierno en materia de derechos humanos se han convertido en blanco creciente de amenazas de muerte, intimidación, campañas de difamación en línea, hostigamiento, vigilancia, agresiones y persecución judicial*".[93]

90 Comunicado de prensa de la CIDH. Disponible en: https://www.oas.org/es/cidh/prensa/comunicados/2019/220.asp
91 Idem
92 Situación de los derechos humanos en Nicaragua, 2018-2019 CENIDH. Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_2018-2019_v.final.pdf
93 Informe Mundial de Human Rights Watch 2019. Disponible en: https://www.hrw.org/es/world-report/2019/country-chapters/325544

La organización, Global Witness en su reporte (2020), Defending Tomorrow, resalta que "*es preocupante la noticia de las 212 personas defensoras del ambiente en el mundo que fueron asesinadas*",[94]. El reporte refiere que el 15% de estos casos se dieron en Centroamérica, de los cuales, cinco asesinatos se dieron en Nicaragua.

Por otro lado, la organización internacional, Front Line Defenders, en su informe de 2019, indica que "*El 11 de junio, liberaron a 56 personas defensoras y presos/as políticos/as que habían sido injustamente detenidos/as por el Gobierno de Ortega en Nicaragua. Medardo Mairena, Irlanda Jerez, Ricardo Baltodano y Amaya Eva Coppens, entre otras personas, recibieron «amnistías» con la aplicación de la controvertida ley de amnistía general aprobada el 8 de junio. Esta ley también puede ser utilizada para otorgar protección a las fuerzas de seguridad, grupos paramilitares y autoridades responsables de graves violaciones de derechos humanos durante la crisis. El 14 de noviembre, Amaya Eva Coppens fue nuevamente detenida de forma arbitraria junto con otros/as 15 activistas y personas defensoras mientras brindaban asistencia humanitaria a un grupo de madres de presos/as políticos en Masaya, Nicaragua*".[95]

En cuanto a ataques digitales, en julio de 2018 la sociedad civil detectó una serie de cortes regionales de Internet e interrupciones intencionales de la conectividad. Esto coincidió con protestas generalizadas y violencia en Nicaragua.

Al 16 de marzo 2019 la Fundación Violeta Barrios de Chamorro (FVBCH), registraba 712 violaciones contra la libertad de prensa y medios de comunicación independientes en Nicaragua, desde el inicio de la represión gubernamental. El 30 de octubre de 2019, un grupo de policías atacó a periodistas que daban cobertura a una protesta pacífica. En el hecho fue lesionado el periodista Armando Amaya, de Canal 12. El 26 de octubre, fue apresado Leonardo Ortiz Avendaño, de Radio Atenas y cinco días más tarde, el periodista Álvaro Montalván, director de radio Mi Voz.

En cuanto a ataques digitales, en julio de 2018 la sociedad civil detectó una serie de cortes regionales de Internet e interrupciones intencionales de la conectividad. Esto coincidió con protestas generalizadas y violencia en Nicaragua. Las mediciones forenses digitales de NetBlocks en las regiones de Managua y Juigalpa, mostraron una fuerte correlación entre el momento de los ataques contra civiles y los incidentes observados de interrupciones y apagones de la red. Eso sugiere que se implementó un régimen de controles de Internet para restringir el flujo de información que entraba y salía de zonas de protesta en momentos críticos.[96]

94 Defender el mañana: La crisis climática y amenazas contra defensores de la tierra y el medio ambiente. Global Witness (2020) https://www.globalwitness.org/es/defending-tomorrow-es/

95 Análisis Global de Front Line Defenders 2019. Disponible en: https://www.frontlinedefenders.org/sites/default/files/spanish_-_global_analysis_2019_web.pdf

96 Joint submission to the United Nations Human Rights Council, on the Universal Periodic Review 33rd Session for Nicaragua. Access Now. Disponible en: https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/

Así mismo durante ese mismo año se registraron ataques distribuidos de denegación de servicio (DDoS), entendidos como un intento malicioso de interrumpir el tráfico normal a un servicio web. Este tipo de ataques fueron denunciados por los medios digitales La Prensa y El Confidencial, dos periódicos de gran circulación en el país. Ambos sitios web sufrieron ataques DdoS, precisamente cuando informaron sobre los resultados mortales de la represión gubernamental.[97]

En el 2018 se constató durante la represión social por parte del gobierno, que varios periodistas y activistas fueron víctimas de ataques denominados "doxxing"

Por otro lado es importante señalar que diferentes medios de prensa reportan que varios periodistas han denunciado públicamente el uso de drones como forma de intimidación y vigilancia. Tal el caso del periodista Miguel Mora quien denunció que un dron vigilaba su residencia el 25 de noviembre de 2018[98]. En la misma línea, en diciembre de ese año otro dron fue visto vigilando las instalaciones del canal 100% Noticias.[99]

En el 2018 se constató durante la represión social por parte del gobierno, que varios periodistas y activistas fueron víctimas de ataques denominados "doxxing".[100] Mediante los mismos se expuso la información personal de las personas afectadas y se les puso en riesgo. Anteriormente habían sufrido otros ciberataques, tales como el acceso no autorizado o el control de sus cuentas en redes sociales.[101]

Front Line Defenders refiere en su informe de 2019 que su apoyo fue solicitado por ataques tales como campañas de difamación, el uso de trolls, campañas de acoso, así como acceso no autorizado a las cuentas de redes sociales de personas defensoras de derechos humanos. Mediante dicho acceso los atacantes obtuvieron información que puso en riesgo la seguridad de las personas defensoras y atentó

97 Artículo periodístico Global Voices. Disponible en: https://es.globalvoices.org/2018/04/30/netizen-report-protestas-en-nicaragua-resultan-en-bloqueos-de-medios-ataques-ddos-y-la-muerte-del-periodista-angel-gahona/ y Artículo periodístico de Confidencial. Disponible en: https://confidencial.com.ni/confidencial-sufre-ciberataque-de-enemigos-de-libertad-de-prensa/

98 100% Noticias. Artículo de noticia «Paramilitares sandinistas envían dron a vivienda de Miguel Mora», 25 de noviembre de 2018. Disponible en: https://100noticias.com.ni/nacionales/94868-dron-casa-miguel-mora/

99 100% Noticias. Artículo de noticia «Dron de paramilitares sandinistas espían y asedian instalaciones de 100% Noticias», 7 de diciembre de 2018. Disponible en: https://100noticias.com.ni/nacionales/95205-dron-espia-100-noticias/

100 Es una práctica mediante la cual informáticos realizan una labor de investigación para recopilar toda la información posible sobre una persona, generalmente información en línea, aunque también en ocasiones puede incluir información de la vida real, de su vida personal, y la publica en la red con el fin de **incitar al acoso en la vida real**.

101 Joint submission to the United Nations Human Rights Council, on the Universal Periodic Review 33rd Session for Nicaragua. Access Now. Disponible en: https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/

contra su reputación. Front Line Defenders indica, además, que el robo o la confiscación de dispositivos fueron un riesgo significativo. Por ejemplo, en aquellos casos en los que dichos aparatos estaban cifrados, las personas defensoras fueron obligadas a proporcionar sus contraseñas, lo cual permitió a los atacantes tener acceso a información confidencial de las víctimas. No todos los dispositivos estaban cifrados y tampoco tenían copia de seguridad. El acceso a la información que estos contenían, dio lugar a que la misma fuera utilizada como evidencia para criminalizar a las personas defensoras. La organización indica también que el acoso en redes sociales resultó algo cotidiano para miles de personas defensoras, en especial aquellas con un mayor grado de vulnerabilidad y marginación.[102]

D.3. Principales hallazgos en Nicaragua

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Nicaragua. Los mismos han sido reportados entre los meses de mayo y noviembre de 2019. Para el registro se construyeron herramientas tanto técnicas como legales a fin de establecer los criterios de documentación de incidentes digitales.

Durante el período indicado se registraron ocho casos e incidentes de seguridad digital con diferentes componentes y móviles, en Managua, Chinandega y León, así como a una defensora periodista exiliada en Costa Rica.

D.4. Casos registrados

Durante el período indicado se registraron **ocho** casos e incidentes de seguridad digital con diferentes componentes y móviles, en Managua, Chinandega y León, así como a una defensora periodista exiliada en Costa Rica.

D.5. Perfil de las personas/organizaciones que reportaron incidentes

El primer caso está relacionado con una defensora de una organización reconocida por su lucha por la tierra, el agua y la soberanía alimentaria. El segundo caso está vinculado a la directora de una organización que promueve y defiende los derechos de las mujeres y las niñas, además de hacer acompañamiento a víctimas

102 Análisis Global de Front Line Defenders 2019. Disponible en: https://www.frontlinedefenders.org/sites/default/files/spanish_-_global_analysis_2019_web.pdf

de femicidios. El tercer caso afecta a un periodista de un medio independiente, y el cuarto caso a una defensora de una colectiva de mujeres. El quinto y sexto caso están relacionados con dos defensoras de una coalición de derechos de las mujeres. El séptimo caso se produjo contra una activista social, en tanto que el octavo caso a una activista feminista.

D.6. Tipos de ataques

A continuación se describen en forma breve los incidentes digitales registrados.

Primer caso: Desde la Rapid Response Network contacta al Observatorio para dar asistencia a un medio de comunicación independiente en Nicaragua. Las personas afectadas reportan ataques DDoS desde el 3 de mayo de 2019, aproximadamente. La técnica del Observatorio se pone a disposición del medio y brinda asesoría para implementar acciones de seguridad digital. Desde la red se realiza análisis de tráfico de las peticiones hacia el sitio web y se les brinda soporte. Este caso es un esfuerzo de alianza y colaboración. Se cataloga el incidente como "Ataques Web" y es clasificado como un caso positivo.

Segundo caso: Una defensora, integrante de una asociación de mujeres, contacta al Observatorio debido a que fue asaltada, hecho en el cual le robaron su dispositivo móvil. La técnica del Observatorio conversa más con la defensora sobre el incidente y debido a las circunstancias se determina que fue por robo común ya que sucedió en una zona donde se ha reportado esa ocurrencia en varias ocasiones. Según refiere la afectada, el dispositivo móvil fue sustraído de su bolso sin que ella se percatara. La técnica la orientó para el bloqueo de las líneas telefónicas que utilizaban el dispositivo y luego solicitar nuevos chips de la empresa de telecomunicaciones. Adicionalmente se le orientó sobre el proceso para asegurar sus cuentas, cerrar sesión en otros dispositivos y activar el 2FA (autenticación de dos pasos) tanto en sus cuentas de correo como en su cuenta de Facebook (solo se enseñó el proceso pues no tenía líneas activas para su configuración). Se registra el caso como "Robo / Pérdida de Hardware" y se clasifica como falso positivo debido a que el mismo no fue dirigido o relacionado con su labor de defensoría.

Tercer caso: Una defensora periodista en el exilio solicita apoyo del Observatorio sobre un incidente con su SIM Card de Nicaragua de la empresa Claro. La defensora explica el incidente "*durante un taller de seguridad digital intenté cambiar el código pin del SIM Card, el código por defecto no funcionó y cuando contacté al servicio*

al cliente vía chat, se mostraron comportamientos extraños (un agente de servicio entró al chat apenas confirmé mi identidad y permaneció sin interactuar durante toda la sesión). La agente del chat me brindó un código personalizado que no recordaba tener, y le brindé mi código PUK". La defensora intentó desbloquear la línea y al configurar nuevamente el PIN se bloqueó nuevamente. Al ingresar el PUK se dio cuenta de que su PIN seguía siendo el número personalizado que le entregó la agente de Claro. Cuando la defensora cerró la sesión, recibió una llamada del servicio al cliente del Claro (desde un número desconocido y que no dejó registro en el teléfono) en la cual le preguntaban si ella había realizado un reclamo por clonación de SIM Card. Esto alertó a la defensora de que podría estar siendo rastreada.

La técnica le dio contención a la defensora pues estaba muy nerviosa debido a la situación. Luego lle explicó que no hay manera de saber con certeza si su teléfono o línea está siendo rastreada activamente y se le dieron recomendaciones para comunicarse por medios más seguros.

Se consultó el caso con otros colegas del Observatorio y se llegó a un consenso de que el incidente pudo deberse a varias circunstancias: error por el Roaming; que la defensora haya colocado un PIN y no recordara haberlo hecho, o bien pueden ser restricciones de la operadora, entre otras. Como no se puede probar un rastreo o intrusión a nivel de línea telefónica (GSM, 3G o 4G), se le recomendó utilizar aplicaciones que ofrezcan cifrado de extremo a extremo para todas sus comunicaciones y evitar usar esa línea. El caso se registra como "Ataque Remoto" y se clasifica como un falso positivo.

Cuarto caso: El hijo de una defensora, abogada de los derechos de las mujeres, contacta al Observatorio y expone que a su mamá le han sucedido cosas extrañas con el teléfono. *"Hace llamadas solo, modifica y se elimina de grupos de chats en donde me comunico con otras personas y posteriormente comenzó a eliminar los contactos por sí solo"*.

La técnica del Observatorio, decide por el tema de la distancia y la hora del incidente (alrededor de las 9pm), proveerle orientación en forma remota. Primero se le indicó a la defensora que apagara el teléfono, extrajera la batería, la tarjeta SD y la tarjeta SIM. Luego se le indicó que colocara la tarjeta SIM en otro equipo y re-configurara sus aplicaciones de chat y que activara el bloqueo de registro. Se le recomendó a la defensora no utilizar el dispositivo móvil comprometido hasta que hubiera posibilidad de revisarlo físicamente. Posteriormente, la defensora pudo acceder a un fondo para la compra de otro dispositivo móvil, por lo que se le asistió en la configuración del

nuevo equipo. Se le recomendaron medidas de seguridad y la revisión del dispositivo anterior. El caso se registró como "Malware" y se clasificó como falso positivo.

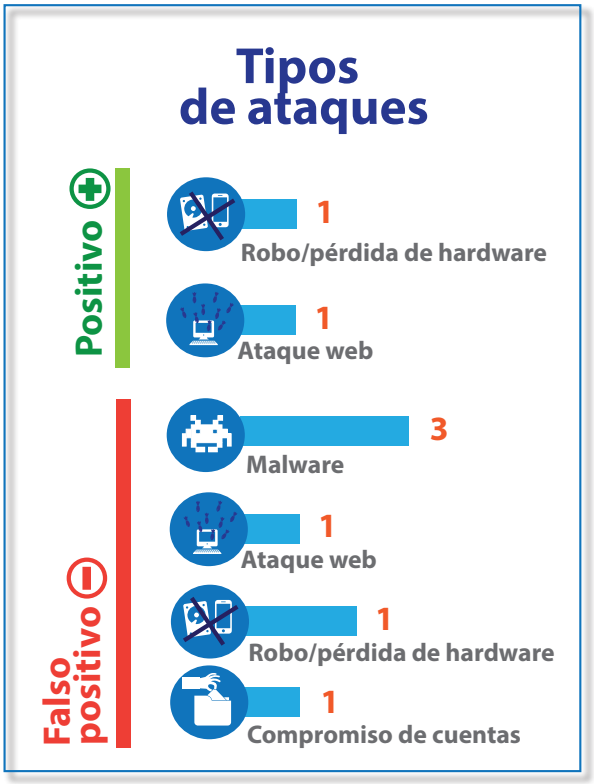
Quinto caso: Un defensor del sector cultura contacta a la técnica del Observatorio, informa que durante un taller de seguridad digital la coordinadora de la organización recibió un correo electrónico que parecía ser de un organismo donante, en el cual se le indicaba que debía descargar un documento y habilitar las macros para ejecutarlo. El correo parecía provenir de una dirección legítima y el contenido no aparentaba ser sospechoso. La coordinadora lo abrió y al no identificar nada visible, le reenvió el correo a su colega para que lo revisara. Este defensor se dio cuenta rápidamente de que no era un correo legítimo y solicitó apoyo para acciones mitigadoras de urgencia, pues justamente se había visto el tema de ransomware y malware en el taller.

La técnica del Observatorio le recomendó desconectar de Internet el equipo, apagar y montar las particiones de Windows con un Live-USB de GNU/Linux para revisar si han sufrido daño los archivos, pues el incidente sucedió unas horas antes. Se le indicó que se revisaran también todas las computadoras que estuvieran conectadas en red y que se procediera a desconectarlas hasta que se revisaran y se verificara que no había infección. Quedó pendiente la visita de la técnica. El incidente es registrado como "Malware" y se clasifica como un falso positivo.

Sexto caso: Una defensora feminista contacta a la técnica del Observatorio por mensajería instantánea y le indica que fue detenida por la policía durante varias horas el 19 de agosto. Informa que su teléfono fue confiscado junto con otras pertenencias. Añade que su teléfono carecía de mecanismos de bloqueo activos en ese momento. La defensora solicita una revisión de posible instalación de malware. La técnica visita a la defensora y revisa el dispositivo móvil. Revisa las aplicaciones instaladas, los archivos en tarjeta SD y memoria interna y corre un antivirus en el teléfono. En la revisión general no se detectó comportamiento extraño del dispositivo y no se encontraron archivos sospechosos. Debido a que el teléfono estaba desbloqueado al momento de la incautación, sí existe posibilidad de que hayan copiado la información de esta defensora. Sin embargo, es un extremo que no se puede verificar ni si hubo instalación de algún tipo de malware a la medida. Como recomendación se solicitó que una vez le entregasen nuevo equipo, coordinara una cita para apoyarla en su configuración. Este ataque se reporta como "Malware" y es clasificado por el momento como un falso positivo.

Séptimo caso: Por medio de redes sociales el Observatorio se entera de un atentado contra la vida de una defensora LGTBIQ. Según lo reportado, el 10 de setiembre varias personas ingresaron a la oficina de la organización mientras ella se encontraba allí. Los intrusos la agredieron físicamente, la apuñalaron y la golpearon con una piedra. La defensora debió ser hospitalizada por la gravedad de las heridas. Se informó que producto de este crimen, también le robaron su computadora personal y su teléfono móvil. La técnica del Observatorio contactó a la organización para ofrecer asistencia para la recuperación de las cuentas de la defensora una vez se estabilizara física y emocionalmente. Este incidente se reporta como "Compromiso de cuentas" y es clasificado por el momento como un falso positivo.

Octavo caso: Una organización defensora de los derechos LGBTIQ contacta a la técnica del Observatorio. La persona defensora de derechos humanos explica que agentes policiales robaron el dispositivo móvil de una miembra de la organización (y hermana de un ex-preso político). Añade que su casa está vigilada permanentemente. La defensora solicita ayuda remota para cerrar algunas cuentas de sus redes sociales y aplicaciones de mensajería. Debido a que no cuenta con su teléfono, otra defensora colega apoya la asistencia remota. La técnica del Observatorio las acompañó en el proceso de cerrar las sesiones de todas las cuentas y realizar cambios de contraseñas. También asesoró a las defensoras sobre la forma de activar la verificación en dos pasos para el acceso a los chat y redes sociales. Este incidente se reporta como "Robo / Pérdida de Hardware" y es clasificado como un incidente positivo.



D.7. Posibles perpetradores

Si bien la identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, esto no siempre se logra.

El contexto general de represión socio-política que sufre el país, lo cual incluye las estrategias de vigilancia comunitaria y estatal, hace más sencillo identificar a los posibles perpetradores.

En el primer caso es difícil determinar el o los perpetradores, aunque las sospechas de que sean aliados del partido Orteguista, son altas. Determinar quiénes han realizado un ataque DdoS a sitios web puede ser complejo. Por el caso de la gravedad de dicho ataque, otra organización especialista ha dado seguimiento

al análisis de tráfico de las peticiones al sitio web, y confiamos plenamente que han coordinado con el medio independiente afectado los pasos a seguir según los resultados obtenidos.

Para el segundo caso se determinó que fue perpetrado por personas que ejercen violencia para asalto y robo en las calles.

Con respecto al tercer caso, no es posible determinar si el incidente corresponde necesariamente a una situación de rastreo mediante empresa telefónica y actores estatales de represión. En tal sentido, no podemos concluir que éstos sean los perpetradores. El cuarto caso es parecido al tercero y, lamentablemente, por situaciones de distancia no se pudo tener acceso al dispositivo móvil para una verificación *in situ*.

En el quinto caso no se determinó la fuente de envío de correo malicioso ya que no se pudo concretar la visita *in situ* y el correo no fue reenviado al Observatorio para posterior análisis.

En el sexto caso, los perpetradores fueron agentes de policía nacional quienes retuvieron por algunas horas a la defensora y sus pertenencias, incluido el dispositivo móvil. En el octavo caso también fueron agentes de policía quienes se llevaron el dispositivo móvil de la defensora frente a su casa de habitación.

Las circunstancias generales del incidente del séptimo caso indican que fue un sujeto quién entró a la organización y agredió a la defensora LGTBIQ y sustrajo equipos de computación y dispositivo móvil. Si bien no se ha determinado quién fue exactamente el agresor y cuál fue el móvil, sí es evidente que el ataque se llevó a cabo con saña y dentro de las instalaciones de una organización de derechos humanos.

D.8. Mecanismos de protección

Aquí se exponen los marcos jurídicos que habrían sido vulnerados en los casos registrados por el Observatorio Centroamericano de Seguridad Digital, en el capítulo de Nicaragua. Se explican las estrategias factibles de llevar adelante, con base en estos casos, para promover los derechos digitales de las personas defensoras de derechos humanos, más allá de que los casos hayan sido registrados como positivos o falsos positivos.

D.9. Posibles Derechos Humanos vulnerados

La Constitución de la República de Nicaragua contempla y regula el derecho a la privacidad digital. En los casos revisados, el denominador común es la vulneración de datos personales e información clasificada como sensible. Esta fue sustraída de cuentas de redes sociales, correos electrónicos y contraseñas comprometidas de las y los defensores de derechos humanos. Esta afirmación tiene como base legal lo que se establece en:

Artículo. 26.- Toda persona tiene derecho:

1) A su vida privada y a la de su familia.

2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.

3) Al respeto de su honra y reputación.

4) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.

Es importante considerar que la constitución establece que el domicilio de las personas podrá ser allanado por orden de juez competente. Por tales efectos, las autoridades nacionales no pueden retener equipo informático, teléfonos inteligentes y dispositivos digitales de las personas u organizaciones en el ejercicio de su labor.

D.10. Posibles tipificaciones penales

Comparando la actualidad con los resultados de la investigación realizada por Fundación Acceso en 2015, así como en su actualización de 2018[103], se puede concluir que el marco jurídico penal continúa siendo insuficiente para establecer mecanismos integrales de protección del derecho a la privacidad digital de las y los defensores de derechos humanos en el país.

103 Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: 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 defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf y "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua" https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762

No obstante y si bien no se cumple a plenitud, la legislación penal prohíbe que un programa informático vulnere datos personales e información depositada en dispositivos inteligentes y equipo informático que ponga en peligro su privacidad y la integridad física y digital:

Artículo 192, regula la Apertura o Interceptación Ilegal de Comunicaciones

> Quien ilegítimamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido, será penado con prisión de seis meses a dos años.
>
> Si además difundiera o revelara el contenido de las comunicaciones señaladas en el párrafo anterior, se impondrá prisión de uno a tres años.

Artículo 193 regula la Sustracción, Desvió de Comunicaciones

> Quien sin enterarse de su contenido, se apodere ilegalmente, destruya o desvíe de su destino una comunicación que no le esté dirigida, será penado con prisión de seis meses a un año.
>
> Quien conociendo o presuponiendo el contenido de la comunicación realizare la conducta prevista en el párrafo anterior, será penado con prisión de uno a dos años.

Artículo 194, regula la Captación indebida de Comunicaciones Ajenas

> Quien ilegítimamente grabe las palabras o conversaciones ajenas, no destinadas al público, o el que mediante procedimientos técnicos escuche comunicaciones privadas o telefónicas que no le estén dirigidas, será penado con prisión de uno a dos años.

Artículo 195 Propalación

> Quien hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque le hayan sido dirigidos, será penado de sesenta a ciento ochenta días multa.

Artículo 197 Registros prohibidos

> El que sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que

puedan afectar a las personas naturales o jurídicas, será penado con prisión de dos a cuatro años y de trescientos a quinientos días multa.

Artículo 198 Acceso y uso no autorizado de información

Quien, sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos, será penado con prisión de uno a dos años, y de doscientos a quinientos días multa.

Artículo 199 Agravación por abuso de función o cargo

La autoridad, funcionario o empleado público que fuera de los casos autorizados por la ley y prevaliéndose de su cargo o función realice cualquiera de las conductas establecidas en el presente capítulo, se le impondrá la pena de tres a seis años de prisión e inhabilitación para ejercer el cargo o empleo público por el mismo período.

Artículo 245 Destrucción de Registros Informáticos,

Quien destruya, borre o de cualquier modo inutilice registros informáticos, será penado con prisión de uno a dos años o de noventa a trescientos días multa.

La pena se elevará de tres a cinco años, cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial.

El Artículo 246 Regula el Uso de Programas Destructivos,

Quien, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será penado con prisión de uno a tres años y de trescientos a quinientos días multa.

El Artículo 250 Regula la Protección de Programas de Computación.

Será sancionado de trescientos a quinientos días multa o prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la ley de la materia fabrique, distribuya o venda mecanismos o sistemas que permitan o faciliten la supresión no autorizada de

dispositivos técnicos que se hayan utilizado para evitar la reproducción de programas de computación.

D.11. Estrategias legales de respuesta

Una alternativa poderosa pueden ser los procesos de litigo estratégico. Esta herramienta ha sido empleada por organizaciones de derechos humanos desde hace varios años. Además de las propias víctimas de violaciones, el litigio estratégico puede ser utilizado por organizaciones de sociedad civil e incluso, ciertos órganos del Estado como, por ejemplo, fiscalías y oficinas de defensoría del pueblo. Para poder llevarlo a cabo se requiere que las personas y Organizaciones afectadas, ya sea individualmente o con asesoría especializada, planifiquen los procesos de litigio y aseguren que estos estén debidamente sustentados.

En todo caso, los incidentes registrados por el Observatorio pueden ser litigados mediante el uso de algunos de los siguientes mecanismos legales:

1. Denuncias/Querella ante el Ministerio Público

Como en otros países de la región, en Nicaragua corresponde al Ministerio Público, por mandato Constitucional, ejercer la acción penal pública. Bajo la conducción de dicha instancia se realiza la persecución de los delitos identificados y, en su defecto puede dirigir la investigación en favor de las personas u organizaciones defensoras de derechos humanos que han sido vulneradas en los mismos.

Esta entidad habrá de garantizar la cadena de custodia de las evidencias recabadas. Mediante el acceso a la evidencia física y digital podrá resolver los incidentes digitales reportados de: 1. Ataque remoto, 2. Compromiso de Cuentas, 3. Robo/Hurto de teléfonos inteligentes, dispositivos digitales y equipo informático, así como los principales medios utilizados para interrumpir labores de organizaciones y personas en la defensa de los derechos humanos.

2. Recurso de Amparo

Otro mecanismo legal de acceso inmediato es la acción constitucional de Amparo. Esta sirve para exigir la protección de derechos garantizados en la Constitución y, siendo la privacidad de las comunicaciones y sus bienes un derecho constitucional, puede ser de utilidad.

La acción de Amparo en Nicaragua se presenta ante la Sala de lo Constitucional de la Corte Suprema de Justicia. Es un proceso estratégico que exige la representación de un abogado o una abogada, con *expertise* en la materia. Esto puede ser una limitante en algunas ocasiones pues impide que las y los defensores de derechos humanos, y la población en general, tengan acceso a la justicia constitucional.

3. Recurso de Habeas Data y otras acciones

En tanto máxima autoridad administrativa que la Ley de Protección de Datos Personales cualquier persona o entidad de naturaleza pública o privada puede acceder a los mecanismos de la Dirección de protección de datos personales adscrita al Ministerio de Hacienda y Crédito Público. Esta entidad, dentro de su marco de aplicación frente al tratamiento, automatizado o no, establece el acceso de cualquier persona a sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa. Está figura está regulada en los Art. 9. 12-15, y los proceso sancionatorios respectivamente en los artículos del 47 – 52.

Otra acción legal para proteger la privacidad digital está contemplada en la Ley General de Telecomunicaciones y Servicios Postales que regula los servicios de telecomunicaciones y servicios postales. La misma establece los derechos y deberes de los usuarios y de las operadoras, en condiciones de calidad, equidad, seguridad, así como el desarrollo planificado y sostenido de las telecomunicaciones y servicios postales. El Art. 2 Numeral 6 de dicha ley, Garantiza y protege la privacidad y la inviolabilidad de la correspondencia y las comunicaciones y la seguridad de la información transmitida.

Según sea el caso, el ente regulador podrá interponer sanciones e infracciones económicas tal y como lo establece el Art. 82. En este se consideran infracciones muy graves: numeral 3) Interferir o interceptar intencionalmente los servicios de telecomunicaciones, afectar su funcionamiento e incumplir intencionalmente las leyes, reglamentos, tratados, convenios o acuerdos internacionales de telecomunicaciones en los cuales Nicaragua es parte, siempre y cuando se compruebe dolo manifiesto.

4. Denuncias ante Procuraduría para la Defensa de los Derechos Humanos

Frente a las denuncias de violación a los Derechos Humanos, Nicaragua regula la figura del ombdusman. Esta figura está determinada por el Procurador para la Defensa de Derechos Humanos. Para el efectivo cumplimiento de de los derechos fundamentales que la constitución establece, se puede interponer ante dicha entidad, las denuncias de violaciones a las libertades y derechos fundamentales.

La Procuraduría tramitará la denuncia en la fase investigativa según establece la Ley 212, "Ley de la Procuraduría para la Defensa de los Derechos Humanos". De acuerdo con dicha norma debe prevalecer el proceso de simplificación de trámites en la atención, investigación, resolución y seguimiento de las denuncias.

Una limitante es que el carácter de la sanción es de índole moral, porque está diseñado para desempeñar un rol de tribunal de conciencia. No obstante, tiene la capacidad legal de presentar denuncias ante los órganos jurisdiccionales competentes.

5. Recursos ante el Sistema Interamericano de Derechos Humanos

Al igual que los otros países de la región, Nicaragua forma parte del Sistema Interamericano de Derechos Humanos (SIDH). La participación del estado ante dicha instancia está regulada por el derecho internacional. Para la presentación de casos ante el SIDH se debe cumplir con los requisitos que la normativa del mismo establece. En primer lugar han de ser tramitados ante la Comisión Interamericana de Derechos Humanos (CIDH) y, con base en el tratamiento que se de en el proceso puede llegar a ser presentado por dicha Comisión, ante la Corte Interamericana de Derechos Humanos (Corte IDH). La Corte, por su autónoma judicial ejerce funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos. En situaciones de gravedad y urgencia, antes de plantear un caso es posible solicitar medidas cautelares ante la (CIDH), para que el Estado adopte medidas enfocadas a prevenir daños irreparables a las personas o al objeto del proceso en conexión con una petición o caso pendiente.

El SIDH es un espacio importante que permite documentar estos y otros casos para identificar patrones de actuación por parte de organizaciones y oficinas gubernamentales que puedan estar vigilando a defensores y defensoras de

derechos humanos. Con la finalidad de visibilizar la situación de la seguridad digital a nivel regional, es importante que esta información se ponga en conocimiento de las respectivas Relatorías para que sea incluida en sus informes periódicos.

D.12. Conclusiones

En Nicaragua persiste la inadecuada aplicación del marco jurídico en privacidad digital.

1. Se pudo observar que en Nicaragua persiste la inadecuada aplicación del marco jurídico en privacidad digital. Estos fueron identificados en su momento en la investigación realizada por Fundación Acceso en el 2015 y actualizada en 2018. En los casos expuestos, la Constitución Política de la República de Nicaragua da el debido reconocimiento al derecho a la privacidad a través de los art. 26, 27, 96 y 188. Por consiguiente, la Ley de Protección de Datos Personales facilita el recurso de habeas data. A este se suma un conjunto de normas que prohíben las practicas del espionaje de las comunicaciones en todas sus formas por parte del Estado y empresas. Sin embargo, en las actuales condiciones de incertidumbre institucional y política en que se encuentra el país, resultan poco efectivas.

2. La amenaza que sufren directamente las personas defensoras de derechos humanos y periodistas independientes en el país va, desde la agresión física hasta la digital, por la información que generan alrededor de su labor de defensoría.

3. El acceso a la justicia ha sido altamente obstaculizado. Por esta razón, plantear el uso de los recursos legales existentes es, prácticamente imposible.

4. Nos preocupa altamente los mecanismos de vigilancia de la policía nacional y de otros grupos afines al partido de Ortega, hacia personas defensoras de derechos humanos. Vigilancia que se produce incluso frente a sus casas, en sus barrios y comunidades y cuando necesitan acceder a la institucionalidad pública. En materia de violación al derecho de la privacidad, al Observatorio de Seguridad Digital también le preocupan mucho las disposiciones contenidas en la Ley 735, referidas en el apartado D1 de este informe, relativas a que "***las empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica y otras que utilicen el espectro electromagnético y radioelectrónico***, *ya sean personas naturales o jurídicas* ***deberán prestar todas las condiciones y facilidades materiales y***

técnicas necesarias para que las intervenciones sean efectivas, seguras y confidenciales *y estarán obligadas a permitir que se usen sus equipos e instalaciones para la práctica de las diligencias de investigación antes previstas"*[104].

104 El subrayado es nuestro.

Bibligrafía

Access Now (2018). **Joint submission to the United Nations Human Rights Council, on the Universal Periodic Review 33rd Session for Nicaragua**. Disponible en: https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/

Amnistía Internacional. **Declaración Pública AMR 37/5587/2017 del 27 de enero de 2017**. Disponible en: https://www.amnesty.org/download/Documents/AMR3755872017SPANISH.pdf

Amnistía Internacional (2017). **Informe anual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

Amnistía Internacional (2017/2018). **Informe anual**. Disponible en: https://crm.es.amnesty.org/sites/default/files/civicrm/persist/contribute/files/Informeanual2018air201718-spanish%20web.pdf

Amnistía Internacional (2019). **Los Derechos Humanos en las Américas.** Disponible en: https://www.amnesty.org/download/Documents/AMR0113532020SPANISH.PDF

Asamblea Nacional de Nicaragua (2010). **Ley de Defensa Nacional de la República de Nicaragua**. Disponible en: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/9F1F361C509ED3F706257825004FE9BC?OpenDocument.

CEJIL (2017). **Nicaragua: ¿cómo se reformó la institucionalidad para concentrar el poder?** Disponible en: https://www.cejil.org/sites/default/files/informe_cejil_sobre_nicaragua_-_derechos_politicos.pdf

CENIDH (2016). Publicación en web: **«CENIDH presenta recurso por inconstitucionalidad contra la Ley de Seguridad Soberana»**. Disponible en: https://www.cenidh.org/noticias/871/

CENIDH (2020). **Situación de los derechos humanos en Nicaragua, 2018-2019**. Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_2018-2019_v.final.pdf

CIDH (2019). Comunicado de prensa: **«CIDH denuncia la persistencia de la represión y expresa su preocupación por incremento de hostigamiento contra personas defensoras de derechos humanos y excarceladas en Nicaragua»**. Disponible en: https://www.oas.org/es/cidh/prensa/comunicados/2019/220.asp

Código Penal de Guatemala. Disponible en: *http://www.oas.org/es/sla/ddi/docs/G6%20Codigo%20Penal%20de%20Guatemala.pdf*

Comisión Interamericana de Derechos Humanos (2016). **Informe Criminalización de defensoras y defensores de derechos humanos.** Disponible en: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf

Comisión Interamericana de Derechos Humanos (2017). **Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf

Comisión Interamericana de derechos humanos. **Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas.** Disponible en: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

Comisión Interamericana de Derechos Humanos (2018). Comunicado de prensa. **Observaciones Preliminares de la visita de la CIDH a Honduras**. Disponible en: https://www.oas.org/es/cidh/prensa/comunicados/2018/ObsPrelHnd.pdf

Confidencial (2018). Artículo periodístico **«Confidencial sufre ciberataque de enemigos de libertad de prensa».** Disponible en: https://confidencial.com.ni/confidencial-sufre-ciberataque-de-enemigos-de-libertad-de-prensa/

Congreso Nacional de Honduras. **Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia.** Disponible en: https://www.tsc.gob.hn/biblioteca/index.php/leyes/619-ley-de-proteccion-para-las-y-los-defensores-de-derechos-humanos-periodistas-comunicadores-sociales-y-operadores-de-justicia

Congreso de la República de Guatemala. **Ley de Protección de Datos Personales.** Disponible en: ttp://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf

Congreso de la República de Guatemala (2017). **Ley contra Actos Terroristas.** Disponible en: https://www.congreso.gob.gt/detalle_pdf/iniciativas/3607#gsc.tab=0

Congreso de la República de Guatemala. **Ley de Prevención y Protección contra Ciberdelincuencia.** Disponible en: https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/748df-5601.pdf

Electronic Frontier Foundation (2014). **Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.** Disponible en: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

Electronic Frontier Foundation y Derechos Digitales (2016). **Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones y el Sistema Interamericano de Protección de derechos humanos.** Disponible en: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf

Electronic Frontier Foundation (2016). **Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica.** Disponible en: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf

El Heraldo (2017). Artículo ***«Honduras: Congreso Nacional aprobó los dos artículos más polémicos de las reformas penales».*** Disponible en: http://www.elheraldo.hn/pais/1046584-466/honduras-congreso-nacional-aprob%C3%B3-los-dos-art%C3%ADculos-m%C3%A1s-pol%C3%A9micos-de-las-reformas

Envío Digital (S/F). Artículo ***«10 peligros de la Ley de Seguridad Soberana»***. Disponible en: https://www.envio.org.ni/articulo/5121

Federal Trade Commission (2005). **Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff.** Disponible en: http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon.** Disponible en: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf

Front Line Defenders (2016). **Annual Report Human Rights Defenders at risk in 2016.** Disponible en: https://www.frontlinedefenders.org/en/resource-publication/2016-annual-report

Front Line Defenders (2019). **Análisis Global.** Disponible en: https://www.frontlinedefenders.org/sites/default/files/spanish_-_global_analysis_2019_web.pdf

Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: 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 defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

Global Witness (2017). **Honduras: el lugar más peligroso para defender el planeta.** Disponible en: https://www.globalwitness.org/documents/18802/Spanish_single_v6.pdf

Global Witness (2020). **Defender el mañana: La crisis climática y amenazas contra defensores de la tierra y el medio ambiente**. Disponible en: https://www.globalwitness.org/es/defending-tomorrow-es/

Global Voices (2018). Artículo periodístico: **«Netizen Report: Protestas en Nicaragua resultan en bloqueos de medios, ataques DDoS y la muerte del periodista Ángel Gahona».** Disponible en: https://es.globalvoices.org/2018/04/30/netizen-report-protestas-en-nicaragua-resultan-en-bloqueos-de-medios-ataques-ddos-y-la-muerte-del-periodista-angel-gahona/

Grupo Asesor Internacional de Personas Expertas (2017). Publicación **Represa de violencia: El plan que asesinó a Berta Cáceres.** Disponible en: https://www.cejil.org/sites/default/files/represa_de_violencia_es_final_.pdf

Human Rights Watch (2019). **Informe Mundial de Human Rights Watch 2019**. Disponible en: https://www.hrw.org/es/world-report/2019/country-chapters/325544

Lakhani, Nina. The Guardian (2018). Articulo **«UK Sold Spyware to Honduras Just before Crackdown on Election Protesters».** Disponible en: https://www.theguardian.com/world/2018/feb/08/uk-sold-spyware-to-honduras-just-before-crackdown-on-election-protesters

La Prensa (2018). Artículo de noticia. **Ley de Ciberseguridad Amenaza la libertad de expresión: CIDH**. Disponible en: https://www.laprensa.hn/honduras/1187050-410/ley-ciberseguridad-amenaza-libertad-expresion-cidh

Medium.com (2018). Artículo **«Los Netcenters: Negocio de Manipulación»**. Disponible en: *https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc*

Ministerio de Gobernación. **Estrategia Nacional de Ciberseguridad. Disponible en:** https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf

Nómada (2017). Artículo ***«Así se fabricó el* #JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo».** Disponible en: *https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/*

Nómada (2018). Investigación periodística de Nuestro Diario: ***«Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)»***. Disponible en: *https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/*

Organización de Estados Americanos. **Convención Americana de Derechos Humanos**. Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Organización de Naciones Unidas. **Declaración Universal de Derechos Humanos.** Disponible en: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Organización de Naciones Unidas. **Pacto Internacional de Derechos Civiles y Políticos.** Disponible en: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Organización de Naciones Unidas. **Resolución 53/144 del 8 de marzo de 1999.** Disponible en: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

Pérez de Acha, Gisela, Derechos Digitales (2016). **Informe: Hacking Team Malware para la Vigilancia en América Latina»** https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

Prensa Libre (2017). Artículo **«Una peligrosa propuesta de ley».** Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley

Poder Judicial de Nicaragua (2010). **Ley de Prevención, Investigación y Procesamiento de la Delincuencia Organizada y Administración de Bienes Incautados, Confiscados y Abandonados.** Disponible en: https://www.poderjudicial.gob.ni/pjupload/comjib/Ley735.pdf

Relatoría Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas (2016). **Informe sobre la Situación de los defensores de los derechos humanos 2016.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

Revista Factum (2019). Artículo **«Los ojos y oídos de Tigo en la política y los negocios»**. Disponible en: *https://www.revistafactum.com/tigo-espionaje-guatemala/*

Soy502 (2017). Artículo **«El Ejército quiere encargarse de las amenazas cibernéticas».** Disponible en: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394

Soy502 (2017). **«Periodistas exigen que el MP investigue a los "net centers"»**. Disponible en: *http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149*

Soy502 (2017). **«Los netcenteros de la impunidad».** Disponible en: *http://www.soy502.com/articulo/netcenteros-impunidad-20878*

Telesur (2018). Artículo de noticia **«Medios piden No aprobar Ley de Ciberseguridad en Honduras».** Disponible en: https://www.telesurtv.net/news/medios-rechazan-ley-ciberseguridad-honduras-20180212-0038.html

Udefegua (2019). **Situación de Defensoras y Defensores de derechos humanos en Guatemala: Un Reflejo del Deterioro de los derechos humanos en el País**. Disponible en: *https://udefegua.org/informeshttp://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf*

100% Noticias (2018). Artículo ***«Paramilitares sandinistas envían dron a vivienda de Miguel Mora»***. Disponible en: https://100noticias.com.ni/nacionales/94868-dron-casa-miguel-mora/

100% Noticias (2018). Artículo ***«Dron de paramilitares sandinistas espían y asedian instalaciones de 100% Noticias»***. Disponible en: https://100noticias.com.ni/nacionales/95205-dron-espia-100-noticias/