Observatorio Centroamericano de Seguridad Digital

-Informe anual 2018-

FUNDACIÓN Acceso

creative commons

Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional

índice

A. Introducción **5**

A.1. Derechos humanos en Internet 5

A.2. ¿Qué es un incidente de seguridad digital? 8

A.3. Tipología de incidentes 9

A.4. Procedimiento para el registro de incidentes 12

B. CAPÍTULO GUATEMALA **13**

B.1. Contexto Legal: Internet y Derechos Humanos en Guatemala 13

B.2. Ataques a defensoras y defensores de derechos humanos 15

B.3. Principales hallazgos en Guatemala 16

B.4. Casos registrados 16

B.5. Perfil de las personas/organizaciones que reportaron incidentes 17

B.6. Tipos de ataques 17

B.7. Posibles perpetradores 18

B.8. Mecanismos de Protección 19

B.9 Posibles derechos humanos vulnerados 19

B.10. Posibles tipificaciones penales 19

B.11. Estrategias legales de respuesta 20

B.12. Conclusiones y Recomendaciones 22

C. CAPÍTULO HONDURAS **25**

C.1. Contexto Legal: Internet y Derechos Humanos en Honduras 25

C.2. Ataque a defensoras y defensores de derechos humanos 25

C.3. Principales hallazgos en Honduras 28

C.4. Casos registrados 28

C.5. Perfil de las personas/ organizaciones que reportaron incidentes 28

C.6. Tipos de ataques 28

C.7. Posibles perpetradores 28

C.8. Mecanismos de Protección 29

C.9. Posibles derechos humanos vulnerados 29

C.10. Posibles tipificaciones penales 29

C.11. Estrategias legales de respuesta 30

C.12. Conclusiones y Recomendaciones 31

D. CAPÍTULO NICARAGUA **33**

D.1. Contexto Legal: Internet y Derechos Humanos en Nicaragua 33

D.2. Ataques a defensoras y defensores de Derechos Humanos 34

D.3. Principales hallazgos en Nicaragua 34

D.4. Casos registrados 35

D.5. Perfil de las personas/ organizaciones que reportaron incidentes **35**

D.6. Tipos de ataques 35

D.7. Posibles perpetradores 38

D.8. Mecanismos de protección 38

D.9. Posibles Derechos Humanos vulnerados 39

D.10. Posibles tipificaciones penales 39

D.11. Estrategias legales de respuesta 42

D.12. Conclusiones y Recomendaciones

Bibliografía 44

A. 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 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 defensores/as de 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 2018) registramos 22 casos de Honduras (2), Nicaragua (14) y Guatemala (6).

A.I. Derechos humanos en 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 los cuales 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.

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.

---

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

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 regulación o control alguno, 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 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 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. La Electronic Frontier Foundation desarrolló una serie de recomendaciones[7] para los gobiernos de América Latina, incluida Centroamérica, en la que detalla las disposiciones legislativas sobre vigilancia masiva de las comunicaciones que deben ser derogadas o reformadas, y en qué sentido. Específicamente en el sentido 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 en sus informes ha demostrado gran preocupación sobre 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 a exigir la transparencia. Sin embargo, los gobiernos realizan diferentes actividades, desde limitar el acceso a Internet hasta remoción de contenido, pasando por implantación de spyware, todo con la finalidad de censurar las voces de defensores y defensoras de derechos humanos.

---

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

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 las redes sociales para promover el irrespeto a los derechos fundamentales. Los gobiernos se han dedicado a presentar acusaciones de difamación e desinformación contra defensoras y defensores, incluso inician 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, con técnicas como el filtrado de contenido, censura, priorizar contenidos o aplicaciones, vulnerando la Neutralidad de la Red, una de las invariantes de Internet.

Edison Lanza, 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, 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 "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 gran preocupación sobre 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 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.

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. 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 es utilizada en contra de activistas, opositores/as y defensores y defensoras.

---

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 annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

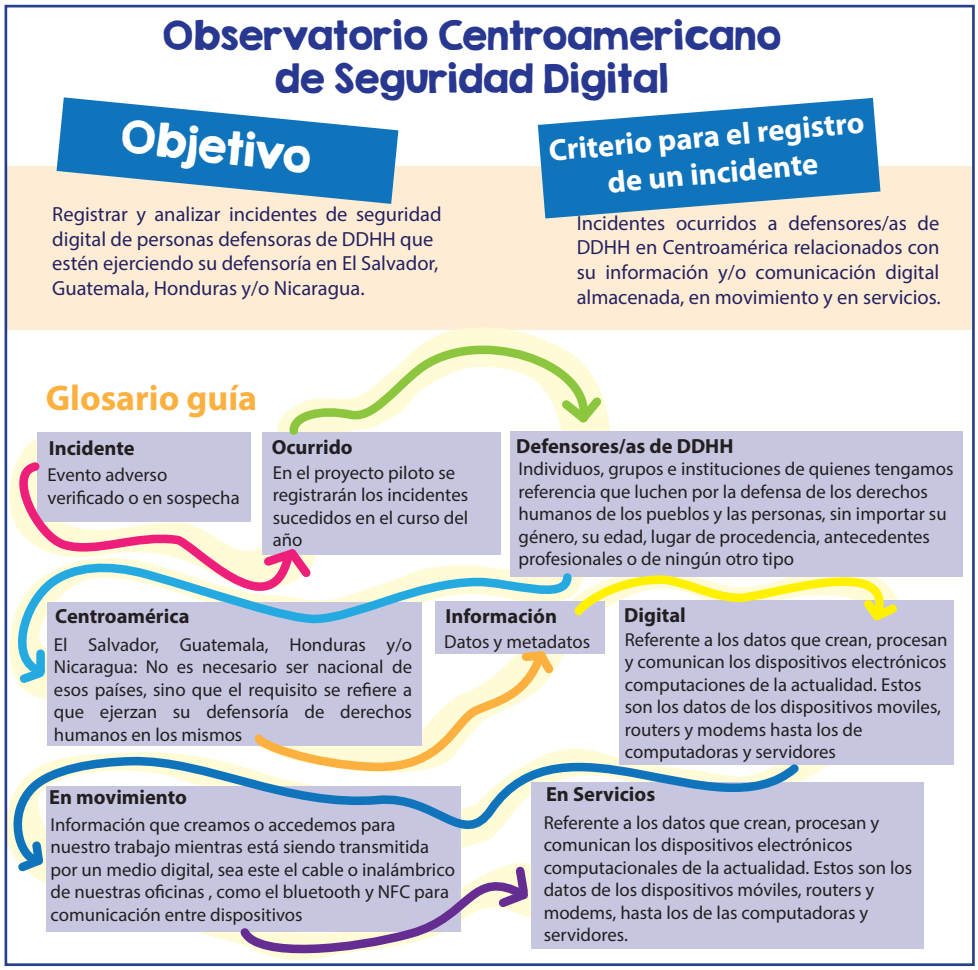
10 Front Line Defenders (2016). **Annual Inform Human Rights Defenders at risk in 2016.** Disponible en: https://www.frontlinedefenders.org/en/resource-publication/2016-annual-report

A.2. ¿Qué es un incidente de seguridad digital?

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/o 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 defensor/a 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/o 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) 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.



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

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.3. 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.

  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].

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.

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/

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 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.

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

Observatorio Centroamericano de Seguridad Digital

Momentos de intervención

Ya sea por llamada telefónica, video-llamada, e-mail, mensaje de texto, mensajería instantánea o personalmente. Se decide si puede ser o no un incidente y si la persona técnica asistirá o no al lugar (1er módulo del reporte).

La persona técnica asiste al lugar para definir si efectivamente es un incidente o si es un falso positivo (2º módulo del reporte)

Si efectivamente es un incidente se realiza una nueva visita al lugar con una persona abogada y se realiza un pre-diagnóstico, se define una estrategia (en conjunto con la persona defensora u organización de DDHH), y se decide si solo se registra o si es un posible caso jurídico (3er módulo del reporte).

La persona abogada y la persona técnica realizan las acciones de estrategia a las que se comprometieron durante el pre-diagnóstico (4º módulo del reporte)

La persona abogada y la persona técnica deciden si es necesario hacer un peritaje especializado, para el que se necesita colaboración externa (5º módulo del reporte)

Resultados del Peritaje. (Se agrega un 6º módulo al reporte con los resultados del peritaje).

A.4. 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.

B. CAPÍTULO GUATEMALA

B.I. Contexto Legal: Internet y Derechos Humanos en Guatemala

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[1], en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[2], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

En este sentido, desde el 2009 la Iniciativa 4090, que dispone aprobar la Ley de Protección de Datos Personales[3] posee dictamen favorable y se encuentra pendiente del tercer debate en el Pleno del Congreso desde el año 2010, previo a su aprobación. La existencia de un marco jurídico en materia de protección de datos personales favorecería a una adecuada protección de la privacidad en línea de las y los defensores de derechos humanos, ya que tendrían mecanismos para ejercitar sus derechos frente al gobierno o empresas.

Durante el transcurso del año 2017, se han presentado un catálogo de iniciativas de ley en el Congreso de la República que de una u otra manera pueden perjudicar en el ejercicio de diferentes derechos humanos en Internet, especialmente para las personas defensoras en el país. Entre las que se citan:

La iniciativa 5239 que dispone aprobar la Ley Contra Actos Terroristas[4], 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[5]. El Artículo 22 regula el delito de "terrorismo cibernético o ciberterrorismo" con prisión de 10 a 20 años. Además, se 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.

La iniciativa 5254 que dispone aprobar la Ley contra la Ciberdelincuencia[6], ya posee dictamen favorable y se encuentra pendiente de Dictamen por la Comisión de Gobernación. Sin embargo, el contenido de este proyecto 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/o denuncia de violación a derechos humanos.

---

1 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

2 *Ibíd.* Pág 175.

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

4 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

5 Prensa Libre. **Una peligrosa propuesta de ley.** Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley

6 Congreso de la República de Guatemala. **Iniciativa 5254, Ley contra la Ciberdelincuencia.** Disponible en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf

Por otro lado, desde la parte gubernamental se han aprobado políticas públicas en relación a la temática de Internet y Tecnologías de la Información y Comunicación, en el transcurso del año se han desarrollado 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[7]. La cual posee como ejes de acción la utilización 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 tampoco tiene un eje que eleve la protección de derechos humanos en Internet.

Desde 2018, el Ministerio de Gobernación, a través del IV Viceministerio de Tecnologías de la Información y Comunicación, con el apoyo de la Organización de Estados Americanos (OEA), aprobó el lanzamiento de la Estrategia Nacional de Ciberseguridad[8]. 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 convocado a diferentes sectores (instituciones gubernamentales, del sector justicia, sector privado, academia, comunidad técnica y sociedad civil) para su elaboración. La Estrategia carece de un enfoque de derechos humanos, además la protección de la privacidad en línea y datos personales no es una prioridad.

Esto último es necesario destacar, ya que la creación de políticas públicas relacionadas a Internet y las nuevas tecnologías requiere de un elemento de reconocimiento a nivel nacional de estándares mínimos de protección de derechos fundamentales en el contexto digital. La falta de participación de organizaciones que se dedican a la defensa de derechos humanos también es perjudicial, ya que en la elaboración de esta Estrategia no involucro a sectores claves. Además, es muy preocupante que las políticas públicas contenidas únicamente sean elaboradas bajo el enfoque de "seguridad nacional", lo cual puede perjudicar el actuar de las personas defensoras, principalmente por la tradición que tiene el gobierno de catalogar a estas organizaciones como grupos desestabilizadores o terroristas. Además, será la base para el desarrollo e implementación de futuras políticas públicas relacionadas con ciberseguridad.

Durante el 2018 no han existido importantes avances en materia de discusión alrededor de temáticas sobre Internet y derechos humanos. Por un lado, la organización internacional The World Wide Web Foundation elaboró un proceso colaborativo y descentralizado para promover el diálogo alrededor de los derechos humanos en línea entre diferentes sectores de la sociedad civil, denominado la Carta de Derechos de Internet en Guatemala[9].

La Alliance for Affordable Internet (A4AI) se encuentra promoviendo la Coalición Guatemalteca para una Internet Asequible[10], con la finalidad de construir diálogo entre el sector público, privado y sociedad civil para el desarrollo e implementación de políticas públicas y regulatorias para que el acceso a Internet sea asequible en el país.

Por otro lado, el 25 de octubre 2018 se desarrolló el segundo Foro de Gobernanza de Internet de Guatemala[11], en el cual se discutieron temas relacionados con la protección de usuarios en internet y

7 Nación Digital. https://www.naciondigital.gob.gt/

8 Ministerio de Gobernación. **Presentan Estrategia Nacional de Ciberseguridad.** Disponible en: http://mingob.gob.gt/estrategia-nacional-de-seguridad-cibernetica/

9 World Wide Web Foundation. **Carta de Derechos de Internet en Guatemala.** Disponible en: http://1e8q3q16vyc81g8l3h3m-d6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2017/06/Carta-de-Derechos-de-Internet-para-Guatemala.pdf

10 Alliance for Affordable Internet. **Coalición Guatemalteca para una Internet Asequible.** Disponible en: http://a4ai.org/guatemala/

11 Foro de Gobernanza de Internet de Guatemala. http://igf.gt/

libertad de expresión en el contexto electoral relacionados a privacidad digital, aunque de una manera muy general, sin incluir la protección de las personas defensoras de derechos humanos.

Estos espacios reflejan que cada vez se hace más necesario promover diálogos alrededor de la protección de los derechos humanos en línea y que la población exija reconocimiento y respeto de estos, así como la inclusión en estas conversaciones en la protección de las defensoras y los defensores. Esto les coloca en una situación de especial vulnerabilidad pues ante esos vacíos normativos es más probable que este tipo de ataques y sus perpetradores, ya sean empresas o agentes del propio estado, queden en la impunidad.

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

La UDEFEGUA, en su reciente informe[12] semestral *(enero-junio 2017),* indica que sólo en 6 meses se registraron un total de 236 agresiones contra personas defensoras en Guatemala. Estas agresiones en su mayoría corresponden a: asesinatos, intimidación, difamación, denuncia judicial, detenciones arbitrarias e ilegales y amenazas. Así mismo, 72 de estas agresiones se dieron contra personas que defienden el derecho humano a un ambiente sano (tierra, territorio y recursos naturales), y un 45% de las agresiones fueron contra mujeres defensoras.

Esta situación también es evidenciada en el informe anual de Amnistía Internacional[13], que establece que las personas defensoras aún son objeto de amenazas, estigmatización, intimidación, agresión y, en algunos casos, hasta víctimas de homicidio. Los grupos más vulnerables ante estos ataques son organizaciones de defensa de la tierra, territorio y medio ambiente.

Michel Frost, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas en sus informes 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."[14]

Es importante destacar el rol de las plataformas de redes sociales para las personas defensoras en Guatemala y medios de comunicación e investigación independientes, en el sentido que son un espacio para difundir sus opiniones y actividades, principalmente en la creciente lucha contra la corrupción en el país; la defensa del territorio, el derecho a la consulta previa, el medio ambiente, y durante los procesos de acceso a la justicia por la violación histórica a los derechos humanos.

En el último año, para la población y sociedad civil Twitter ha sido fundamental para la movilización ciudadana para exigir, entre otras cosas, la renuncia de funcionarios públicos de altos cargos, incluido el actual Presidente de la República. Como consecuencia, el aumento de perfiles considerados como bots o net centers[15] han propiciado la desinformación (desde propagación de noticias falsas hasta difamación

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

13 Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Pág. 217.

14 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

15 Soy502. **Los netcenteros de la impunidad.** Disponible en: http://www.soy502.com/articulo/netcenteros-impunidad-20878

en contra de activistas y medios independientes), principalmente para debilitar el trabajo de investigación realizado por la Comisión Internacional contra la Impunidad en Guatemala (CICIG)[16], el Ministerio Público (MP)[17], y múltiples organizaciones nacionales de derechos humanos (y particularmente a las mujeres defensoras).

En el 2017, un grupo integrado por 12 medios de comunicación solicitó al Ministerio Público que investigue el acoso que han sufrido en redes sociales, principalmente por cuentas de net centers, afirman que han sufrido "hackeos, ataques de net centers y amenazas directas, en especial contra mujeres".[18] Claramente el tema de la utilización de bots en contra de activistas y medios independientes con la finalidad de difamar o desestabilizar, la están utilizando directa o indirectamente varios gobiernos, uno de los problemas principales es lograr identificar si existe financiamiento público para estas actividades. Por otro lado, lamentablemente el Ministerio Público no posee la capacidad técnica para establecer cuáles son los perfiles "falsos o bots", lo cual podría traer un peligro aún mayor como vigilancia y posible criminalización de activistas y personas defensoras de derechos humanos.

Finalizando la edición del informe del Observatorio en 2017, salió a la luz pública un interesante artículo titulado Los Netcenters: negocio de manipulación de Luis Assardo, el cual detalla cómo han funcionado en Guatemala y cuáles son sus efectos[19].

Por otro lado, en el marco de las investigaciones alrededor de diferentes delitos cibernéticos, desde el Ministerio de la Defensa, han manifestado públicamente la intención que sea el Ejército de Guatemala el encargado de realizar las investigaciones sobre las amenazas cibernéticas para resguardar la economía e instituciones del país[20]. El peligro que el Ejército realice investigaciones sobre ciberamenazas es terrible para la ciudadanía, porque existe una gran posibilidad que se dedique a vigilar y colectar información de ciudadanos, activistas y personas defensoras de derechos humanos.

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 registrados entre los meses de marzo y setiembre de 2018. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de los mismos.

B.4. Casos registrados

Durante el transcurso del período antes mencionado, fueron registrados un total de **seis** casos e incidentes de seguridad digital con diferentes componentes y móviles, todos en la Ciudad de Guatemala.

16 Comisión Internacional contra la Impunidad en Guatemala. http://cicig.org/

17 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/

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

19 Medium.com. Los Netcenters: Negocio de Manipulación. https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc

20 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

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

El primer caso involucró a una periodista de un medio independiente de Guatemala. El segundo caso se relaciona con una persona defensora y artista quién contacta el Observatorio a través de una organización nacional de derechos humanos.

El tercer y cuarto caso involucra a dos defensoras que se encuentran en un proceso de acceso a justicia por un juicio por crímenes de lesa humanidad. El quinto caso se relaciona con una persona defensora que realiza investigación e incidencia en Guatemala. El sexto caso involucra una organización de acompañamiento a víctimas de crímenes de lesa humanidad.

B.6. Tipos de ataques

A continuación una breve descripción de los incidentes registrados.

En el primer caso de la periodista fueron varios incidentes los que se registraron y analizaron desde el Observatorio. Entre ellos: a. Ataques de phishing en su cuenta de icloud, b. Subida de foto de familiar a su cuenta de Instagram, c. Mensajes de texto que le indican que se ha conectado a una IP en otra región de Guatemala (desde su cuenta de Gmail), d. Registro de llamadas salientes de números a las que ella nunca ha llamado, así como números entrantes que no conoce, e. Cambio de contraseña en Gmail. En el proceso de análisis se pudo identificar que la IP donde está alojado el sitio del phishing contiene varios sitios asociados a URL's que intentan hacer ataques phishing. Después de revisar las direcciones IP vinculadas a los mensajes se pudo determinar que en efecto las IP están dedicadas a hacer hackeos phishing a dispositivos Apple. La empresa se encuentra en Panamá, hasta ahora sabemos que el número de teléfono de la defensora se encuentra comprometido, así como los detalles de sistema operativo de su teléfono. Se determina que es un incidente digital de "Compromiso de Cuentas" y se clasifica como un incidente positivo.

En el caso de la persona defensora y artista, ésta fue invitada a unirse a un grupo de Facebook de artistas reconocidos, cuando ingresa al link del grupo éste lo redirige a un sitio de phishing. La persona defensora ingresa al link e incluye datos falsos en el sitio de phishing, después de esto cuando le da ingresar el celular se apaga y no vuelve a encender. Posteriormente la persona defensora lleva el teléfono a arreglar pero al momento del análisis no le han devuelto el dispositivo. Se realizó un análisis de sus redes sociales y correos electrónicos buscando algún rastro de intrusión, pero no se encontró ningún ingreso no autorizado a su cuenta. Se determina que es un incidente digital de "Compromiso de Cuentas", y se clasifica como un falso positivo.

Una de las defensoras, quien se encuentra en un juicio por crímenes de lesa humanidad, contacta al Observatorio a través de un defensor digital de una organización nacional de derechos humanos. El caso de la defensora está relacionado con un correo electrónico avisando que alguien había solicitado cambiar su contraseña de Facebook, sin embargo ella de inmediato indica que no hizo la solicitud y actualizó su contraseña de la cuenta. Se analizó cronológicamente el incidente, sin embargo el correo de aviso fue borrado por la defensora por lo que la persona técnica no pudo realizar mayores averiguaciones sobre el incidente. Se determina que es un Ataque Web y se clasifica como un falso positivo.

Otra de las defensoras, quien se encuentra en un juicio por crímenes de lesa humanidad, contacta el Observatorio. La defensora recibe en el chat de la aplicación Messenger de Facebook un video con su nombre y una descripción. En el Thumbnail del video aparecía una foto de ella, y posteriormente hace clic en el video y éste la redirige a una página de Phishing. La defensora ingresa sus credenciales y luego se da cuenta que había cometido un error, por lo cual actualiza rápidamente sus datos. Desde

el Observatorio se copiaron los links para hacer un análisis detenido. La vista preliminar del video es en realidad una imagen alojada en un blog de blogger, esto nos indica que se tomaron el tiempo para diseñar una imagen con los detalles de la defensora y hacerla ingresar a un link falso. El tiempo y el trabajo para confeccionar la imagen nos hace concluir que este incidente digital fue un ataque dirigido. Se determina que es un ataque digital denominado "Compromiso de Cuentas" y se clasifica como un incidente positivo.

En cuanto al quinto caso, la defensora de Guatemala quien realiza investigación e incidencia, contactó al Observatorio directamente con el fin de que el técnico analizara la posibilidad de instalación de malware en su teléfono y computadora. A raíz de la publicación del periodista Luis Angel Sas sobre los diferentes tipos de programas que el gobierno de Guatemala ha comprado para hacer vigilancia a activistas y organizaciones de derechos humanos, y debido a que la defensora en cuestión cuenta con un perfil muy alto, se decidió visitarla y realizar el registro y análisis. Se realizó captura del tráfico de red de su computadora y de su teléfono móvil, esto con el objetivo de poder revisar las conexiones que establecen sus equipos y así determinar si existe una posible fuga de datos. Se analizaron todas las conexiones y se estableció que todas las direcciones IP a las que se conectan los dispositivos son direcciones legítimas y por lo tanto no representan ningún peligro. Se determina que es un incidente de "Malware" y se clasifica como un falso positivo.

Con respecto al sexto y último caso registrado en Guatemala, la organización de acompañamiento a víctimas de crímenes de lesa humanidad contacta directamente al técnico del Observatorio. La directora y miembros del equipo de la organización recibieron un correo electrónico de su propio correo institucional con un mensaje de extorsión. Dicho mensaje hace alusión a que han *hackeado* su servidor y piden dinero para no publicar datos íntimos de las personas de la organización. Se le solicitó a la directora de la organización que enviara los encabezados del correo electrónico para verificar si en efecto éstos mensajes provienen desde el servidor de la organización, y de esta forma determinar si su red interna y cuentas de correo se encuentran comprometidas. Al revisar los encabezados se pudo determinar que los correos en efecto provienen de la dirección de la organización, lo que significa que están comprometidas. Se solicitará a la organización el permiso para poder revisar todos los logs, los cuales ayudarán a determinar de dónde se originó el ataque y por qué medio se hizo.

B.7. Posibles perpetradores

La identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, pero se debe informar que no siempre se logra porque un atacante regularmente tratará de *anonimizarse* y para ello utilizará los recursos técnicos y metodológicos que convengan para el tipo de ataque.

En tal sentido, esta tarea 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 se puede delinear un posible perfil técnico del atacante y sus objetivos.

En el primer caso, los incidentes sucedieron después de varios "hackeos" no comprobados a personas defensoras a finales del 2017, y luego del robo del teléfono móvil de la defensora periodista en enero de 2018. Los múltiples incidentes de compromiso de cuentas indican un patrón de ataque constante a la defensora. Adicionalmente a través de este caso se logra identificar una IP utilizada para realizar Phishing a través de varios URL's, y que esta IP es de una región especifica de Guatemala (Mazatenango). Adicionalmente se logra ubicar que las direcciones IP vinculadas a los mensajes están dedicadas a hacer hackeos phishing a dispositivos Apple desde una empresa se encuentra ubicada en Panamá.

En cuanto al segundo y tercer caso, debido a que se determina como falso positivo por falta de datos para análisis, los posibles perpetradores o sus mecanismos de ataque no pudieron ser identificados.

Con respecto al cuarto caso, no fue posible identificar el origen del ataque. Lo que si determinamos es que el ataque fue dirigido a la defensora, y que el perpetrador tenía tiempo y recursos tecnológicos para montar el vídeo en imagen. Debido a que la defensora ha estado involucrada activamente en un juicio por crímenes de lesa humanidad, podemos suponer que este ataque fue contratado o confeccionado por las personas (o familiares y/o amigos de ellas) quienes están siendo juzgados por dichos crímenes.

En cuanto al quinto caso se declara como falso positivo, y por tanto no se encuentran perpetradores del posible incidente. Sin embargo es importante evidenciar que las personas defensoras cada vez más están aumentando su conciencia sobre posibles ataques digitales y han incorporado la observancia como acción preventiva a incidentes digitales. El que se clasifique un caso como falso positivo no debe ser entendido como un error, es una alerta atendida a tiempo y en la que se descarta intencionalidad de actores externos.

En cuanto al sexto caso, los posibles perpetradores no han sido identificados hasta que se complete el análisis de logs.

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 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, independientemente de que los casos hayan sido registrados como positivos o falsos positivos.

B.9 Posibles derechos humanos vulnerados

Dentro de la Constitución de la República de Guatemala se regula el derecho a la privacidad digital, su base legal:

> 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”

Es decir, la inviolabilidad de correspondencia, documentos y libros en cualquier formato que atente contra la intimidad personal, es prohíba salvo por orden previa de juez competente.

B.10. Posibles tipificaciones penales

A partir de la investigación de marcos legales realizada en 2015 por Fundación Acceso y actualizado en el 2018[21], 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. A pesar de ello, el Código Penal de Guatemala con las últimas reformas

21 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

del Decreto N# 17-73[22] Capítulo VII amplia aquellos acciones relativas a los delitos contra los derechos de Autor, Propiedad Industrial y los Delitos Informáticos ante la comisión de daños o perjuicios en contra de personas naturales o jurídicas; a través de una tercera persona o programas informáticos en las que afecten su integridad digital, podrán aplicarse los siguientes:

- Destrucción de sus registros informáticos, el Artículo 274 "A". Señala "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".
- Alteración de programas, el Articulo 274 "B". "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".
- Reproducción de instrucciones o programas de computación Articulo 274 "C".. 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.
- Registros prohibidos Artículo 274 "D". 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.
- Manipulación de información Artículo 274 "E".. 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.
- Uso de información Artículo 274 "F". 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.

Sin embargo, en la relación de sus datos personales, la legislación actual en materia penal no regula los delitos de suplantación de identidad personal en redes sociales y otros medios digitales.

B.II. Estrategias legales de respuesta

Las personas u organizaciones afectadas deberán de planificar litigios estratégicos a través de casos fundamentados. Estos pueden ser entablados ante los órganos jurisdiccionales o Ministerio Público. El litigio estratégico ha sido usado durante muchos años para promover la defensa de los derechos humanos en la región, siendo una herramienta que puede ser utilizada por las víctimas, organizaciones de la sociedad civil, así como ciertos órganos del Estado como Ministerios Públicos y Defensorías del Pueblo. Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

1. Denuncias/Querella ante el Ministerio Público

En los casos registrados en Guatemala, corresponde constitucionalmente realizar denuncias ante el Ministerio Público, que por su naturaleza ejerce la acción penal pública, en el sector justicia, promoviendo la persecución penal de los delitos informáticos antes mencionados, y en su defecto podrá

22 http://www.oas.org/es/sla/ddi/docs/G6%20Codigo%20Penal%20de%20Guatemala.pdf

dirigir la investigación de los delitos cometidos en contra de las personas u organizaciones defensoras de derechos humanos.

Bajo su cadena de custodia y presentando 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 establece el recurso de Amparo ante las violaciones a la privacidad e intimidad personal, este recurso por su naturaleza 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 experto en la materia**, su base legal:**

> 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 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 establecen la figura de Habeas Data, La normativa restringe la comercialización de datos personales a terceros sin la debida autorización y consentimiento del titular; para incurrir a la acción penal deberá comprobarse que el encargado o persona que brinda el tratamiento de los datos personales ha comercializado o compartido información sensible, al comprobarse el hecho será sancionado de cinco a ochos años de cárcel según establece el Art. 66, en lo que respecta a la Responsabilidad y Sanciones en el tratamiento de la información.

4. Denuncias ante la Procuraduría de Derechos Humanos

Es la principal instancia defensora de derechos humanos en Guatemala, ante el cual se puede interponer denuncias en materia de violación de libertades y derechos fundamentales, a la vez vela por su efectivo cumplimiento, esta instancia deberá investigar y denunciar comportamientos lesivos a los intereses de las personas u organizaciones; Sin embargo, el carácter de la sanción es de índole moral, porque está diseñado para desempeñar un rol de tribunal de conciencia; aunque tiene la capacidad legal de presentar denuncias ante los órganos jurisdiccionales competentes.

5. Denuncias ante Sistema Interamericano de derechos humanos

Guatemala forma parte del Sistema Interamericano de derechos humanos, su participación está regulada por el derecho internacional y posee ciertos requisitos previos para que las denuncias y casos sean llevados ante la Corte Interamericana de Derechos Humanos que por su autónoma judicial ejerce funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos. Sin embargo, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la Comisión Interamericana de derechos humanos 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, 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. Esta información ponerla de conocimiento de las respectivas Relatorías para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

B.I2. Conclusiones y Recomendaciones

Conclusiones

1. Persiste el contexto adverso para la defensa de las y los defensores de derechos humanos en el marco de protección de la seguridad digital en la labor que estos realizan, los cuales fueron identificados en la investigación de Fundación Acceso de 2015 y actualización del mismo en el 2018. En el Congreso de la República se han presentado y se están discutiendo iniciativas de ley que carecen seguridad jurídica y de legitimidad en la defensa de los derechos humanos, y en caso sean aprobadas pueden perjudicar la labor de organizaciones que se dedican a la defensa, denuncia y promoción de derechos humanos.

   Las actuales estrategias de Ciberseguridad deben ampliarse en apoyar las causas de los incidentes de seguridad digital de las organizaciones y personas, la actual estrategia podría estar afectando directamente la labor que las personas defensoras de derechos humanos, al no establecer mecanismos de controloria ciudadana esto pone en peligro su información personal, su trabajo e incluso sus vidas, al uso indebido de programas de vigilancia.

2. El tema de la seguridad digital continúa estando ausente de los informes que tratan sobre la seguridad de las personas defensores de derechos humanos, provocando áreas de vulnerabilidad a través de las cuales estos pueden ser atacadas.

3. Es necesaria la pronta aprobación de una Ley ordinaria 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 base de datos en el internet.

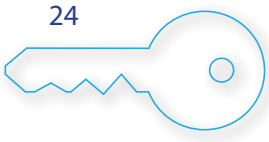
Recomendaciones

1. La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores, enfatizando la necesidad de incluir herramientas de seguridad digital, incluyendo estándares internacionales en materia de Internet y derechos humanos.

2. El sector justicia y organizaciones para la defensa de los derechos humanos deben realizar estrategias que incluya proyectos y programas orientados a la sensibilización de los derechos digitales y la aplicación de los mismos, actualmente los tribunales e instancias del sector justicia guatemalteco carecen de litigios estratégicos en el campo de las nuevas tecnologías y los ciberdelitos, siendo un área poco desarrollada jurisdiccionalmente por procuradores, jueces y abogados defensores de derechos humanos.

3. Los colectivos y organizaciones que se dedican a la defensa de derechos humanos deben generar mecanismos y protocolos internos enfocados a la seguridad digital y su privacidad en línea, lo cual se puede lograr a través de la generación de capacidades en este tema dentro de sus propias colectividades.

4. Dentro de los informes sobre la situación de las personas defensores de derechos humanos a nivel nacional y/o regional, es importante incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de ésta en materia de protección y seguridad integral.
5. Es necesario convocar una mesa nacional de consulta y análisis sobre la situación de gobernanza de Internet y derechos humanos, convocada desde las organizaciones de derechos humanos con la participación de comunidades académicas y expertos en derechos digitales que identifiquen los desafíos y actuales vacios legales, esta sería una estrategia importante para impulsar las tendencias globales en materia de regulación de Internet, y derecho a la privacidad, ambos derechos rápidamente están teniendo eco en los congresos de nuestros países centroamericanos.



C. CAPÍTULO HONDURAS

C.I. Contexto Legal: Internet y Derechos Humanos en Honduras

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[1], en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[2], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

Por otra parte, 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 que contenía un conjunto de reformas a diferentes legislaciones, 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. Esta Ley fue aprobada en el contexto de la lucha contra el crimen, provee una serie de disposiciones y modificaciones en materia penal con la finalidad de reducir los delitos. Sin embargo, varias organizaciones, locales e internacionales[3], se pronunciaron en contra de esta Ley, ya que carecen de enfoque de derechos humanos.

Se realizaron reformas al Código Penal, en las que se modificaron los delitos de Extorsión y Terrorismo, y a la Ley de Centros Penitenciarios. Fue una de las reformas más criticadas, específicamente en contra de una de las reformas más preocupantes fue al delito de terrorismo, ya que su regulación es muy amplía y existe un profundo temor que pueda ser utilizada como una "ley mordaza" vulnerando la libertad de expresión, ya que equipara las protestas ciudadanas como terrorismo[4]. Las reformas al Código Penal amplía las conductas "terroristas", incluyendo quien cause estragos o daño a la propiedad, o quien no participe directamente en esos daños, pero que si participe en un acto que sea para intimidar o causar terror al gobierno o población también es responsable del delito.

Además, el texto aprobado tipifica la apología e incitación a actos terroristas 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 en el contexto de quien convoque a manifestaciones ciudadanas o participe de estas, también puede ser objeto de proceso penal por ese delito. Lo cual vulnera los derechos de libertad de expresión, asociación y manifestación consagrados en la Constitución de Honduras, incluidas las personas

---

1 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

2 *Ibíd.* Pág 192.

3 Amnistía Internacional. **Declaración Pública AMR 37/5587/2017 del 27 de enero de 2017**.

4 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

defensoras de derechos humanos, quienes están desarrollando un papel muy importante para la defensa del territorio y de la democracia. 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.

En las reformas a la Ley Especial sobre Intervenciones de las Comunicaciones Privadas se determina la creación de la Unidad de Intervención de las Comunicaciones (UIC), a cargo, entre otras cosas, de realizar el procedimiento de obtención de detalle de llamadas entrantes y salientes de las personas en proceso de investigación, con orden de juez competente. Además, determina la obligación a los operadores de telefonía *a garantizar sin limitaciones el acceso inmediato a la UIC toda la información relacionada a la intervención y extracción del contenido de las telecomunicaciones.*

En 2018 la Asamblea Nacional formulo un proyecto denominado Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en Redes Sociales[5], abriendo el debato sobre su legalidad, en su defecto la relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos formulo su preocupación por los términos y alcance del proyecto[6]. Sin embargo, el Gobierno ha firmado un Acuerdo de Cooperación con el Gobierno de Israel para el fortalecimiento de la Dirección Nacional de Investigación e Inteligencia para la implementación de un CERT[7] en el país. Ambas acciones amenazan derechos como la privacidad digital y la libertad de expresión en el ciberespacio hondureño.

C.2. Ataque a defensoras y defensores de derechos humanos:

Honduras presenta desde el 2009 un contexto de violencia sistemática en contra de defensoras y defensores de derechos humanos, como asegura en su informe el Grupo Asesor Internacional de Personas Expertas[8]. Incluso ha sido considerado por Global Witness[9] 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.

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

Además, Michel Frost, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas en sus informes 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

5 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

6 La prensa. Ley de Cicerseguridad Amenaza la libertad de expresión. Disponible en https://www.laprensa.hn/honduras/1187050-410/ley-ciberseguridad-amenaza-libertad-expresion-cidh

7 El Heraldo. **Israel dotará de unidades en contra del cibercrimen en Honduras.** Disponibe en: http://www.elheraldo.hn/pais/1115476-466/israel-dotar%C3%A1-de-unidades-en-contra-del-cibercrimen-en-honduras

8 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.

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

que estos fueran sancionados."[10] Especialmente en Guatemala y Honduras donde persiste la impunidad y las y los defensores de derechos humanos no confían en órganos jurisdiccionales al momento de solicitar reparaciones judiciales.

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[11], la mayoría de casos siguen en la impunidad por diferentes razones desde falta de voluntad política hasta corrupción del Gobierno, Ejército y empresas extractivistas. El Gobierno hondureño, a través de sus fuerzas de seguridad, ha institucionalizado prácticas de control y represión a todos niveles.

De la misma manera, Freedom House en su informe del 2017 sobre Libertad de Prensa cataloga a Honduras como un país no libre[12], la metodología del informe incluye parámetros como entornos legales, políticos y económicos en los que medios de comunicación, impresos, radiales y digitales ejercen su labor informativa y sin miedo a represalias frente actores privados, políticos e incluso del crimen organizado. Indicando además, que continúa siendo uno de los países más peligrosos en el mundo para que periodistas ejerciten su labor[13].

Amnistía Internacional en su informe anual[14] 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[15] sigue sin ser aplicada adecuadamente.

El Estado ha invertido casi 2 mil millones de lempiras (casi 85 millones de dólares americanos) en actividades de inteligencia y espionaje[16] a opositores del gobierno, bajo el escudo de combatir la delincuencia. Estas actividades de inteligencia se incluyen interceptaciones telefónicas, infecciones con *malware* y seguimiento de activistas y periodistas; es necesario destacar que la Dirección de Inteligencia utiliza estos mecanismos sin orden judicial previa.

Además, en el marco del 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. En el que además se declaró Estado de Excepción[17], restringiendo garantías constitucionales, luego de la inconformidad de la población frente a los resultados de las votaciones y por un posible fraude electoral, lo que ha provocado hasta el momento protestas ciudadanas y excesivo uso de la fuerza por parte de las fuerzas de seguridad públicas; que incluso han dejado detenidos, heridos y muertos en todo el país[18].

---

10 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

11 *Ibíd*. Pág. 5.

12 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.

13 *Ibíd.* Pág. 21.

14 Amnistía Internacional (2017). **Informe annual 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.

15 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

16 ConfidencialHN. **JOH gastó casi dos mil millones para espiar a opositores.** Disponible en: http://confidencialhn.com/2017/08/28/joh-gasto-casi-dos-mil-millones-para-espiar-a-opositores/

17 Reuters. **Honduras suspende garantías constitucionales en medio de fuertas protestas tras elecciones.** Disponible en: https://lta.reuters.com/article/domesticNews/idLTAKBN1DV4UW-OUSLD

18 Amnistía Internacional. **Honduras: represión violenta después de elecciones.** Disponible en: https://www.amnesty.org/es/documents/amr37/7550/2017/es/

C.3. Principales hallazos 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 los meses de mayo y junio de 2018. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de los mismos.

C.4. Casos registrados

Durante el transcurso del periodo antes mencionado, fueron registrados un total de **dos** casos e incidentes de seguridad digital con diferentes componentes y móviles, todos en Tegucigalpa, Francisco Morazán.

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

El primer caso trata de una reconocida periodista de varios medios internacionales, siendo corresponsal de Honduras. En segundo caso está relacionado con un defensor de una organización de acompañamiento internacional.

C.6. Tipos de ataques

A continuación una breve descripción de los incidentes registrados.

En cuanto al primer caso, la periodista contacta a la Red de Defensoras de Honduras quienes se contactan con el técnico del Observatorio. La periodista indica que está recibiendo amenazas, insultos y hostigamiento a través de sus redes sociales por parte de un perfil específico. Se comprueba el perfil y los mensajes y se acompaña a la periodista en el proceso de bloqueo del perfil. Así mismo se le insta a que denuncie las agresiones ante una instancia de libertad de expresión. Si bien no es un incidente digital, sino una amenaza y violencia directa a través de sus redes sociales, se clasifica como un falso positivo.

En cuanto al segundo caso, el defensor de la organización de acompañamiento internacional presente en Honduras, se contacta directamente con el técnico del Observatorio, debido a que su organización ha recibido al menos 3 correos electrónicos en distintas fechas amenazándoles con ransomware pidiéndoles además depósito de dinero a una cuenta bancaria o que publicarán información de su computadora. El técnico revisa el código fuente del correo del defensor y su equipo. No se encontró ninguna vulnerabilidad en el dispositivo o información almacenada. Se concluye que el incidente es un "Malware" y se clasifica como un falso positivo. El que se clasifique un caso como falso positivo no debe ser entendido como un error, es una alerta atendida a tiempo y en la que se descarta intencionalidad de actores externos.

C.7. Posibles perpetradores

En el primer caso sí se identifica el perfil de un individuo que se hace pasar por "Ramon Jérez". En el segundo caso se identifica el perpetrador como un "cracker" o "grupo de crackers" común quienes envían este tipo de correos electrónicos para estafas electrónicas.

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 todos los casos registrados fueron falsos positivos.

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, fomentando así el derecho a la circulación de información en línea 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[19], se puedo 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 y los defensores de derechos humanos en el pais. 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 a una persona que vulnere el correo postal que 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.

19 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

El fraude o estafa a través de un de un programa informático, también está regulada 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, 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 la que podría estar incurriendo el hackeo informático si expone información o comparte datos sensibles o privada de los teléfonos celulares, equipo informático y dispositivos inteligentes, en la que pongan en peligro la seguridad física de las personas.

C.II. Estrategias legales de respuesta

Las personas u Organizaciones deberán planificar litigios estratégicos a través de casos fundamentados. Estos pueden ser entablados ante los órganos jurisdiccionales o Ministerio Público. El litigio estratégico ha sido usado durante muchos años para promover la defensa de los derechos humanos en la región, siendo una herramienta que puede ser utilizada por las víctimas, organizaciones de la sociedad civil, así como ciertos órganos del Estado como Ministerios Públicos y Defensorías del Pueblo. Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

1. Denuncias/Querella ante el Ministerio Público

En los casos registrados en Honduras, corresponde constitucionalmente realizar denuncias ante el Ministerio Público, por su naturaleza ejerce la acción penal pública, en el sector justicia, bajo su jurisdicción se realiza la persecución de los delitos identificados, y en su defecto dirigirá la investigación en favor de las personas u organizaciones defensoras de derechos humanos

Bajo su cadena de custodia y presentando evidencia física y digital puede llegar a ser crucial para resolver los delitos de estafa y amenazas como los principales medios para interrumpir las labores de organización y personas en la defensa de los derechos humanos.

2. Recurso de Habeas Data

La Constitución de la República de Honduras establece la acción de Habeas Data constituyendo un mecanismo procedimental de aplicación inmediata por las autoridades jurisdiccionales hondureñas, este recurso está facultado 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, es un proceso estratégico que exige la representación de un abogado experto en la materia, Para entablar el recurso de Habeas Data debe de 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, donde el Estado de Honduras reconoce la garantía del Habeas Data “Que toda persona tiene el derecho a acceder a la información sobre si 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

Honduras posee el Mecanismo Nacional de Protección a Defensores/as de derechos humanos, este mecanismo tiene la obligación de investigar los hechos y de proteger la integridad de las personas defensoras, así como de evitar que, de alguna manera, se les obstaculice su labor. Sin embargo, este mecanismo únicamente contempla medidas de protección física, parcialmente psicológica y legal, pero no contempla protección relacionada a la seguridad digital de sus beneficiarios.

4. Recursos ante el Sistema Interamericano de Derechos Humanos

Honduras forma parte del Sistema Interamericano de derechos humanos, su participación está regulada por el derecho internacional y posee ciertos requisitos previos para que las denuncias y casos sean llevados ante la Corte Interamericana de Derechos Humanos que por su autónoma judicial ejerce funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos. Sin embargo, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la Comisión Interamericana de derechos humanos 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, 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. Esta información ponerla de conocimiento de las respectivas Relatorías para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

C.I2. Conclusiones y Recomendaciones

Conclusiones

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 funcionalidad, desde su creación se ha identificado muchas deficiencias en respuesta eficaz y eficiente. Honduras ha sido catalogada como uno de los países más peligrosos para ejercer esta labor.

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, los cuales fueron identificados en su momento en la investigación realizada por Fundación Acceso en el 2015 y actualizada la misma en 2018.

3. El Gobierno hondureño ha invertido millones de lempiras para la implementación de su sistema de inteligencia, sin incluir en los mecanismos de control y vigilancia 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 peligro al que son sujetos en su labor diaria incluye, entre otras cosas, el peligro en su integridad física e incluso la vida, como la información que generan alrededor de su trabajo y lucha cotidiana.

4. El tema de seguridad digital continúa estando ausente de los informes que tratan sobre la seguridad de las y los defensores de derechos humanos, provocando áreas de vulnerabilidad a través de las cuales estos/as pueden ser atacadas/os.

5. Es necesario 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 el internet.

6. Honduras actualmente carece de una legislación adecuada en el Código Penal, observando limitantes en la tipificación de delitos relacionados a la privacidad y delitos informáticos y sus conexos, esto dificulta la persecución delictiva ante el Ministerio Público

Recomendaciones

1. La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores de derechos humanos, enfatizando en la necesidad de incluir herramientas de seguridad digital que incluya estándares internacionales en materia de Internet y Derechos Humanos.

2. La ciudadanía debe exigir transparencia y rendición de cuentas sobre las diferentes herramientas de inteligencia y vigilancia, así como la regulación para que éstas sean utilizadas en el contexto de la necesidad, legalidad y proporcionalidad.

3. Los colectivos y organizaciones de derechos humanos deben generar mecanismos y protocolos internos enfocados a la seguridad digital y privacidad en línea, lo cual se puede lograr a través de la generación de capacidades en este tema dentro de las propias organizaciones y colectivos.

4. Dentro de los informes sobre la situación de las y los defensores de derechos humanos es importante incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de esta en materia de protección integral.

Convocar una mesa nacional de consulta y análisis sobre la situación de gobernanza de Internet y derechos humanos, puede ser convocada desde las organizaciones de derechos humanos con la participación de comunidades académicas y expertos en derechos digitales. A través de este espacio se deberán identificar desafíos y actuales vacios legales, esta sería una estrategia importante para impulsar.las tendencias globales en materia de regulación de Internet, y el derecho a la privacidad, ambos derechos rápidamente están teniendo eco en los congresos de nuestros países centroamericanos.

D. NICARAGUA

D.I. Contexto Legal: Internet y Derechos Humanos en Nicaragua

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[1], en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[2], A pesar de que la actual legislación ordinaria relaciona la penalización de este derecho en 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, se 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. 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 el artículo 13 **prohíbe** a las entidades públicas que forman parte del Sistema Nacional de Seguridad lo siguiente: realizar espionaje político, obtener o almacenar información o datos sensibles de organizaciones sociales, asimismo la interceptación e intervención de comunicaciones si 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, como la legalidad, autoridad judicial competente y debido proceso.

El 14 de noviembre de 2017 se llevó a cabo en Nicaragua el I Foro sobre Gobernanza de Internet y Seguridad Informática[3], en el cual desde una óptica multisectorial se discutieron temas relacionados con la privacidad digital, aunque de una manera muy general, sin incluir consideraciones respecto a la protección de las y los defensores de derechos humanos.

Sin embargo, la falta de otros espacios refleja que cada vez se hace más necesario promover diálogos alrededor de la protección de los derechos humanos en línea y que la población exija reconocimiento y respeto de estos, así como la inclusión en estas conversaciones de la protección de las y los defensores de derechos humanos.

Esto les coloca en una situación de especial vulnerabilidad pues ante esos vacíos normativos es más probable que este tipo de ataques y sus perpetradores, ya sean empresas o agentes del propio gobierno, queden en la impunidad.

---

1 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

2 *Ibíd.* Pág 260.

3 Internet Society capítulo Nicaragua. http://isoc.org.ni/

D.2. Ataques a defensoras y defensores de Derechos Humanos

El 10 de enero del 2017, Daniel Ortega tomó posesión del cargo de Presidente por tercera vez, su esposa Rosario Murillo fue electa como Vicepresidenta. La concentración del poder ha impactado en diferentes ámbitos de la institucionalidad en Nicaragua, desde la destitución arbitraria de diferentes funcionarios/as públicos/as opositores[4] hasta la limitación de diferentes derechos fundamentales.

En Nicaragua las defensoras y defensores de derechos humanos continúan siendo objeto de intimidación y amenazas por sus actividades en Nicaragua. Según el informe anual de Amnistía Internacional[5] principalmente las comunidades indígenas y afrodescendientes han denunciado diferentes violaciones a sus derechos fundamentales, específicamente en el contexto de la construcción del proyecto multimillonario del Canal Interoceánico; el cual fue aprobado bajo una serie de irregularidades. Varias comunidades y organizaciones de derechos humanos expresaron preocupación ante el posible impacto negativo del canal sobre sus vidas. Las implicaciones negativas del Canal Interoceánico sobre los derechos humanos, han sido recogidas en el informe de la FIDH y CENIDH[6], en el que claramente relatan la criminalización de la protesta social, hostigamiento a la población y militarización de las comunidades sobre la ruta del Canal.

En el informe anual 2016 del CENIDH[7] sobre la situación de los DDHH en Nicaragua, incluye un apartado sobre la situación particular de las personas defensoras. En este tema indican que: *"La mayoría de los casos de agresiones, amenazas, estigmatización y judicialización hacia defensores y defensoras han partido de divulgación de información que denigra y difama en sitios virtuales y diversas redes sociales donde se publican no sólo fotografías y datos personales, sino también datos familiares, dirección de las casas de habitación, exponiéndoles frente a los sujetos y/o presuntos agresores, lo que pone en alto riesgo su seguridad, además, de las constantes amenazas tanto a ellas como a sus hijos e hijas."*

Front Line Defenders también menciona en su reciente informe de 2017, que se han registrado múltiples ataques a personas defensoras en Nicaragua, particularmente hacia mujeres defensoras. La **Iniciativa Nicaragüense de Defensoras de Derechos Humanos ha registrado en dos años 3**89 agresiones ocurridas (entre 2015 y 2017) en contra de 202 defensoras. Un 45 por ciento de los agresores señalados son autoridades estatales destacándose la Policía[8].

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 registrados entre los meses de enero y mayo de 2018. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

---

4 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.

5 Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de Derechos Humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Pág. 328.

6 FIDH (2016) – Concesión del Canal Interoceánico en Nicaragua: Grave Impacto en los derechos humanos. Disponible en: https://www.cenidh.org/media/documents/docfile/informe_nicaragua_canal_esp1.pdf

7 CENIDH (2016). Derechos Humanos en Nicaragua 2016. Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf

8 IM-Defensoras (2017). Audiencia 164 de la CIDH. Disponible en: https://www.youtube.com/watch?v=c4Pr6A3Yiq8

D.4. Casos registrados

Durante el transcurso del período antes mencionado, fueron registrados un total de **catorce** casos e incidentes de seguridad digital con diferentes componentes y móviles, en León y Managua, así como a una defensora de Nicaragua radicada en Ciudad de México.

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 una directora de una organización que realiza labores de promoción y defensa de los derechos de las mujeres y las niñas, y de acompañamiento a víctimas de femicidios. El tercer caso involucra 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 vincula a una activista social, y el octavo caso a una activista feminista. El noveno caso se relaciona con una defensora de derechos de las mujeres. El décimo y undécimo caso corresponden a una activista mujer y un activista hombre. El duodécimo caso está relacionado con una defensora mujer trans. El décimo tercer caso y el décimo cuarto caso están vinculados con una activista mujer y un activista hombre de León.

D.6. Tipos de ataques

A continuación una breve descripción de los incidentes digitales registrados.

Primer caso: Una organización de cooperación solidaria le informa a Fundación Acceso que la sub-directora de una de las organizaciones co-partes de Nicaragua está recibiendo llamadas de su oficina en Costa Rica que no se han realizado. La directora de Fundación Acceso contacta a la técnica del Observatorio en Nicaragua con el fin de que contacte la co-parte y les visite. Según el relato de la subdirectora de la organización ella recibió una llamada de un número convencional de Costa Rica, y no le aparece como conocido en su teléfono, pero se relaciona con la organización de cooperación solidaria. Relata la defensora que cuando contestó el teléfono en esa ocasión le cuelgan (ella estaba en medio de una reunión). Después de eso no la volvieron a llamar del número de Costa Rica. El otro incidente mencionado por la defensora está relacionado con dos 2 video llamadas por Whatsapp que recibió del número de su papá, las contestó y no había video (video en negro), ella contestó pero la pantalla le indicaba que tenía mala conexión. Posterior a este incidente, no ha recibido ni mensajes ni llamadas extrañas. La técnica realizó revisión del teléfono móvil de la subdirectora y no encontró nada extraño. Se le recomendó solicitar el registro de llamadas de su teléfono móvil y el registro de llamadas del teléfono de la organización. Posterior a este registro de incidente aún no conocemos el registro de llamadas para verificar más datos sobre este caso.

Segundo caso: Una defensora que conoce el Observatorio refiere a otra organización que vivió un incidente de robo de computadoras. La organización le informa a la técnica del Observatorio que en las computadoras que les robaron hay información sobe un proyecto sobre niñas en condición de violencia y que tienen miedo de que boicoteen el proyecto y usen la información para difamar y detener el trabajo de la organización. La defensora de la organización informa que a principios de febrero sujetos desconocidos entraron a las oficinas principales de la organización y robaron dos computadoras pertenecientes al área de contabilidad. Forzaron cerraduras y rompieron una cerca ubicada en una

calle privada. Solo robaron información financiera, dejando otros equipos en el lugar. Las compañeras de la organización tienen temor de que intervengan el sistema contable o intimiden a las defensoras para que no participen del proyecto. Se llevaron estados financieros, estados de cuenta de los bancos y contabilidad general. Debido a que no se pueden hacer procedimientos técnicos sin los dispositivos, se realizó una visita para apoyarlas en respaldos seguros de su información. Este tipo de casos de robo de dispositivos sólo pueden ser atendidos por el Observatorio una vez recuperados los equipos con el fin de analizar si hubo sustracción de información, instalación de malware o modificaciones al sistema operativo y documentos. Este ataque se reporta como "Pérdida de Hardware" y es clasificado como un incidente positivo.

Tercer caso: El periodista / comunicador contacta directamente a la técnica del Observatorio para reportar que a principios de febrero, al hacer una investigación sobre unas denuncias a trabajadores sindicales de una minera ubicada en la zona de León, no lograron entrar al sitio web de dicha empresa minera. Utilizando un navegador seguro lograron entrar al sitio. La técnica revisó el sitio web con ayuda de un plugin para detectar tecnologías utilizadas e Inspección de Elementos / Herramientas de Desarrollador que proveen los navegadores Firefox y Google Chrome. En el proceso se detectó el uso del servicio geolify dentro del sitio, este servicio es el que está haciendo re-dirección del sitio hacia la página de bienvenida o hacia el localhost (null) en dependencia de la IP geolocalizable de la persona visitante al sitio. Se concluye que esto es parte de la configuración del sitio web de la empresa minera y no tiene relación con bloqueos intencionados por el proveedor de servicios de Internet (ISP). Se cataloga como un "Ataque Web" y se le califica como un falso positivo.

Cuarto caso: Una organización de mujeres contacta a la técnica del Observatorio, ya que reportan el robo de equipo en vivienda de una defensora de la organización. Se robaron una tablet con información confidencial en horas de la tarde a principios de febrero, así como un televisor. El robo se da con intimidación, ya que la defensora estaba presente cuando el perpetrador entró a la vivienda. La defensora indica que cambió contraseñas de todas sus cuentas. La tablet estaba cifrada de inicio pero no sabe si estaba completamente protegida. En 2016 y 2017 su organización también sufrió robo de equipo. Este ataque se reporta como "Pérdida de Hardware" y es clasificado como un incidente positivo.

Quinto caso: Una defensora contacta directamente a la técnica del Observatorio. La defensora reporta que ha recibido llamadas internacionales donde le colgaban, este incidente sucedió en enero del 2018 y no volvió a suceder. La defensora cambió su teléfono móvil y número de teléfono. Este ataque se reporta como "Ataque remoto" y es clasificado como un falso positivo.

Sexto caso: Una defensora contacta directamente a la técnica del Observatorio. La defensora reporta dos casos de llamadas de números internacionales donde no responden y cuelgan. En Whatsapp también recibió llamadas extrañas. Se registra el incidente pero no se pudo realizar análisis el teléfono porque ya la defensora había cambiado de dispositivo. Este ataque se reporta como "Ataque remoto" y es clasificado como un falso positivo.

Séptimo caso: Una activista social contacta directamente a la técnica del Observatorio. Reporta que sus cuentas de twitter están bloqueadas por actividad sospechosa. La activista intentó recuperar las cuentas y no le llegan los códigos de verificación. Este incidente se escala hacia la línea de ayuda de Access Now. La activista recuperó el acceso a sus cuentas, y se sospecha que el incidente se dio por reportes masivos desde cuentas pro-gobierno debido a la crisis en Nicaragua y los diversos mecanismos que se han utilizado para bloquear la libertad de expresión en Internet. Este ataque se reporta como "Compromiso de Cuentas" y es clasificado como un incidente positivo.

Octavo caso: Una activista feminista radicada en México contacta a la técnica del Observatorio por chat. La activista reporta que su cuenta en Facebook está bloqueada debido a reportes masivos por parte de

cuentas pro-gobierno. Su cuenta fue suspendida por sus publicaciones sobre la situación en Nicaragua. Se escala el caso hacia la línea de ayuda de Access Now. El observatorio le dio seguimiento al caso hasta que la defensora recuperó su cuenta. Este ataque se reporta como "Compromiso de Cuentas" y es clasificado como un incidente positivo.

Noveno caso: Una defensora de los derechos de las mujeres contacta a la técnica del Observatorio. La defensora reporta que su cuenta de Facebook fue bloqueada. Al parecer su contraseña actual no era muy fuerte y lograron acceder al perfil. Se escala el caso hacia línea de ayuda de Access Now. Se da seguimiento y se intenta concertar visita con la defensora el cual no fue posible debido a la crisis del país. Se le recomendó a la defensora activar la autenticación de dos pasos para evitar ingresos no autorizados a su cuenta. Este ataque se reporta como "Compromiso de Cuentas" y es clasificado como un incidente positivo.

Décimo caso: Una activista feminista contacta directamente a la técnica del Observatorio por medio de chat. La activista indica que en una marcha ella subió unas fotos a su cuenta de Facebook, tuvo muchos problemas para subir la foto y a unos 15 minutos Facebook le reportó de que había una actividad inusual en su cuenta y encontró un inicio de sesión desde una dirección IP desconocida (que luego se confirma que estaba ubicada cerca del parque Luis Alfonso Velásquez). Ella cerró todas las sesiones y cambió la contraseña, luego la página no le cargaba en su teléfono. Ella apagó el teléfono móvil y entró nuevamente después de un tiempo, cerró su cuenta de Facebook, a este momento le aparecía la opción de cerrar la cuenta por hackeo. Envió capturas de pantalla de la información, y se confirma un inicio de sesión inusual. Adicionalmente reporta que en Telegram le aparecía una sesión abierta, ella revisó su aplicación y no aparecían sesiones activas. Luego informa que por Whatsapp recibió un mensaje de su novio, que su novio indica que no envió, la activista eliminó la cuenta que tenía en Whatsapp y posteriormente la volvió a abrir nuevamente. La técnica recomienda realizar una visita para analizar con detenimiento el teléfono móvil, sin embargo por la situación de crisis del país fue imposible coordinar dicha visita. Este ataque se reporta como "Compromiso de Cuentas" y no ha sido posible clasificarlo como positivo o falso.

Undécimo caso: Un activista hombre que colabora con la comisión mediadora del diálogo nacional reporta que la página oficial en Facebook de un importante figura religiosa ha sido suspendida por denuncias masivas. Al mismo tiempo, se han levantado al menos tres páginas y perfiles falsos con el objetivo de captar información de los perfiles que dan "me gusta" a estas páginas falsas. Pide apoyo con la recuperación de las cuentas y verificación de las mismas. Se escaló el caso a la línea de ayuda de Access Now, se dio seguimiento hasta conseguir la recuperación de las cuentas y la verificación tanto de su cuenta de Facebook como de Twitter. Se hicieron denuncias de los perfiles falsos y llamados a la población a revisar bien las páginas a las que están dando "me gusta" pues se ha detectado que lo hacen para conseguir los nombres de los perfiles. Se intentó coordinar una visita pero la situación de los tranques y ataques por parte de la policía impidieron que se encontrara el activista y la técnica del Observatorio. Este ataque se reporta como "Compromiso de Cuentas" y es clasificado como un incidente positivo.

Duodécimo caso: Una defensora mujer trans contacta a la técnica del Observatorio. La defensora fue interceptada por dos motorizados quienes sólo le robaron su teléfono móvil. Esta defensora ha venido siendo amenazada por un oficial de policía quien es familiar de una comisionada con cargo de poder. Este oficial le hizo confesiones por chat sobre los asesinatos de los estudiantes, y posteriormente la empezó a amenazar y le ha dado seguimiento con vehículos (y con otras personas). Este robo se dio por la noche, la defensora no atinó a bloquear su número teléfono con la empresa telefónica y al día siguiente no logró acceder a sus cuentas. El día siguiente, con apoyo técnico, se intentó recuperar

las cuentas, sin embargo ni Gmail ni Icloud reconocían las contraseñas ingresadas. Se constató que la defensora había cambiado sus contraseñas recientemente y que tenía la autenticación de 2 pasos activada a través de SMS y aplicación. Analizando la situación de contexto y el incidente reportado por la defensora, se presume que los atacantes lograron ingresar a las cuentas debido a que ella no bloqueó el SIM de inmediato. Se intentaron recuperar las cuentas, y al ser imposible la recuperación de las cuentas se traslada el caso a la línea de ayuda de Access Now. Este ataque se reporta como "Pérdida de Hardware " y es clasificado como un incidente positivo.

Décimo tercer caso: Una defensora de derechos humanos contacta a la técnica del Observatorio informando que le ha sido robado el teléfono de su esposo quien trabaja en una organización de cooperación internacional. Su esposo reporta que estaba en una zona de tranque y dos motorizados pasaron y le arrebataron el teléfono. Intentaron ingresar a sus cuentas para cambiar contraseñas debido a que sí tenía la autenticación de dos pasos, adicionalmente llamaron a la empresa telefónica para que desactivaran el chip. Posteriormente se les asesoró para que ingresaran a las cuentas por medio de la computadora de la casa y que hicieran el borrado remoto. Este ataque se reporta como "Pérdida de Hardware " y es clasificado como un incidente positivo.

Décimo cuarto caso: Una activista mujer contacta directamente a la técnica del Observatorio. La activista informa del robo de la computadora de otro activista quien administra las páginas de un movimiento social. Se hizo contacto con el afectado y según describe la circunstancias del robo no son claras, pues solo se llevaron su equipo y dejaron otras cosas de valor. Él indica que tenía toda la información protegida y logró acceder a sus cuentas desde su teléfono. Este ataque se reporta como "Pérdida de Hardware " y es clasificado como un incidente positivo.

D.7. Posibles perpetradores

La identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, pero se debe informar que no siempre se logra, principalmente en el contexto de la delincuencia común que se ha normalizado en los países de la región centroamericana. En tal sentido, esta tarea requiere, para los casos más complejos, recursos técnicos y acceso a servicios que están fuera del alcance de la organización.

El contexto general del país y la crisis que se vive en todo el territorio nacional, así como la identificación clara de actores de represión se identifica para el caso séptimo y octavo que el compromiso de cuentas se estableció por reportes masivos a las plataformas de redes sociales contra las personas activistas y defensoras, y en estos casos es asumido que las peticiones masivas se realizaron por parte de grupos pro-gobierno.

En todos los otros casos de "Pérdida de Hardware", aunque no están identificados los perpetradores en varios casos se indica que fueron personas motorizadas, y en el contexto de crisis las personas motorizadas están vinculados a grupos para-policiales en Nicaragua.

En el décimo caso se identifica una IP ubicada cerca del Parque Luis Alfonso Velázquez en el centro de Managua, sin embargo no existe mayor información para determinar el perpetrador.

D.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 Nicaragua 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.

D.9. Posibles Derechos Humanos vulnerados

Dentro de la Constitución de la República de Nicaragua se contempla y regula el derecho a la privacidad digital, el denominador común de los incidentes registrados es la vulneración de datos personales e información clasificada como sensible que fue sustraída de cuentas de, redes sociales, correos electrónicos y contraseñas comprometidas de las y los defensores de derechos humanos, su base legal está establecida 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 interrumpido 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

A partir de la investigación de marcos legales realizada en 2015 por Fundación Acceso y actualizado en el 2018[9], 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. A pesar de ello, la legislación penal prohíbe ante la comisión de daños y agravios 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.

9 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

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.II. Estrategias legales de respuesta

Las personas y Organizaciones afectadas deberán planificar litigios estratégicos a través de casos fundamentados. Estos pueden ser entablados ante los órganos jurisdiccionales o Ministerio Público. El litigio estratégico ha sido usado durante muchos años para promover la defensa de los derechos humanos en la región, siendo una herramienta que puede ser utilizada por las víctimas, organizaciones

de la sociedad civil, así como ciertos órganos del Estado como Ministerios Públicos y Defensorías del Pueblo. Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

1. Denuncias/Querella ante el Ministerio Público

Dentro de los casos registrados en Nicaragua, corresponde constitucionalmente realizar denuncias ante el Ministerio Público, que por su naturaleza ejerce la acción penal pública, en el sector justicia, bajo su jurisdicción se realiza la persecución de los delitos identificados, y en su defecto dirigirá la investigación en favor de las personas u organizaciones defensoras de derechos humanos

Bajo su cadena de custodia y presentando 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, como los principales medios utilizados para interrumpir labores de organizaciones y personas en la defensa de los derechos humanos

2. Recurso de Amparo

La acción constitucional de Amparo también es utilizado como un mecanismo legal para exigir la protección de derechos garantizados en la Constitución y, siendo la privacidad de las comunicaciones y sus bienes un derecho constitucional'

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, de experto en la materia, lo cual en algunas ocasiones 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

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, como máxima autoridad administrativa que la Ley de Protección de Datos Personales establece dentro de su marco de aplicación frente al tratamiento, automatizado o no, de 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, y establece los derechos y deberes de los usuarios y de las operadoras, en condiciones de calidad, equidad, seguridad, y el desarrollo planificado y sostenido de las telecomunicaciones y servicios postales. Donde el Art. 2 Numeral 6 Garantiza y protege la privacidad y la inviolabilidad de la correspondencia y las comunicaciones y la seguridad de la información transmitida.

Según el caso el ente regulador podrá interponer sanciones e infracciones económicas según lo establece el Art. 82 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, ante el cual se puede interponer las violaciones a las libertades y derechos fundamentales para el efectivo cumplimiento de de los derechos fundamentales que la constitución establece.

La Procuraduría, según el caso tramitará la denuncia en la fase investigativa esto debe regir con sus actuaciones de acuerdo con lo establecido en la Ley 212, "Ley de la Procuraduría para la Defensa de los Derechos Humanos" y, prevaleciendo el proceso de simplificación de trámites en la atención, investigación, resolución y seguimiento de las denuncias,

Sin embargo, el carácter de la sanción es de índole moral, porque está diseñado para desempeñar un rol de tribunal de conciencia; aunque tiene la capacidad legal de presentar denuncias ante los órganos jurisdiccionales competentes.

5. Recursos ante el Sistema Interamericano de Derechos Humanos

Nicaragua forma parte del Sistema Interamericano de derechos humanos, su participación está regulada por el derecho internacional y posee ciertos requisitos previos para que las denuncias y casos sean llevados ante la Corte Interamericana de Derechos Humanos que por su autónoma judicial ejerce funciones jurisdiccionales y consultivas en la aplicación e interpretación de la Convención Americana sobre Derechos Humanos. Sin embargo, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la Comisión Interamericana de derechos humanos 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, 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. Esta información ponerla de conocimiento de las respectivas Relatorías para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

D.I2. Conclusiones y Recomendaciones

Conclusiones

1. Se pudo observar que en Nicaragua persiste la inadecuada aplicación del marco jurídico en privacidad digital, los cuales 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 del art. 26, 27, 96 y 188, Por consiguiente la Ley de Protección de Datos Personales facilita el recurso de habeas data, seguido de una serie de normas que prohíben las practicas del espionaje de las comunicaciones en todas sus formas por parte del Estado y empresas. Sin embargo, se vuelven poco efectivas por la actual incertidumbre institucional y política que se encuentra el país.

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

Recomendaciones

1. La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores de Derechos Humanos, enfatizando la necesidad incluir herramientas de seguridad digital, incluyendo estándares internacionales en materia de Internet y Derechos Humanos.

2. Los colectivos y organizaciones que se dedican a la defensa de derechos humanos deben generar mecanismos y protocolos internos enfocados a la seguridad digital, lo cual se puede lograr a través de la generación de capacidades en este tema dentro sus propias organizaciones.

3. Dentro de los informes sobre el panorama de las actividades de las y los defensores de derechos humanos deben incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de esta en la seguridad integral.

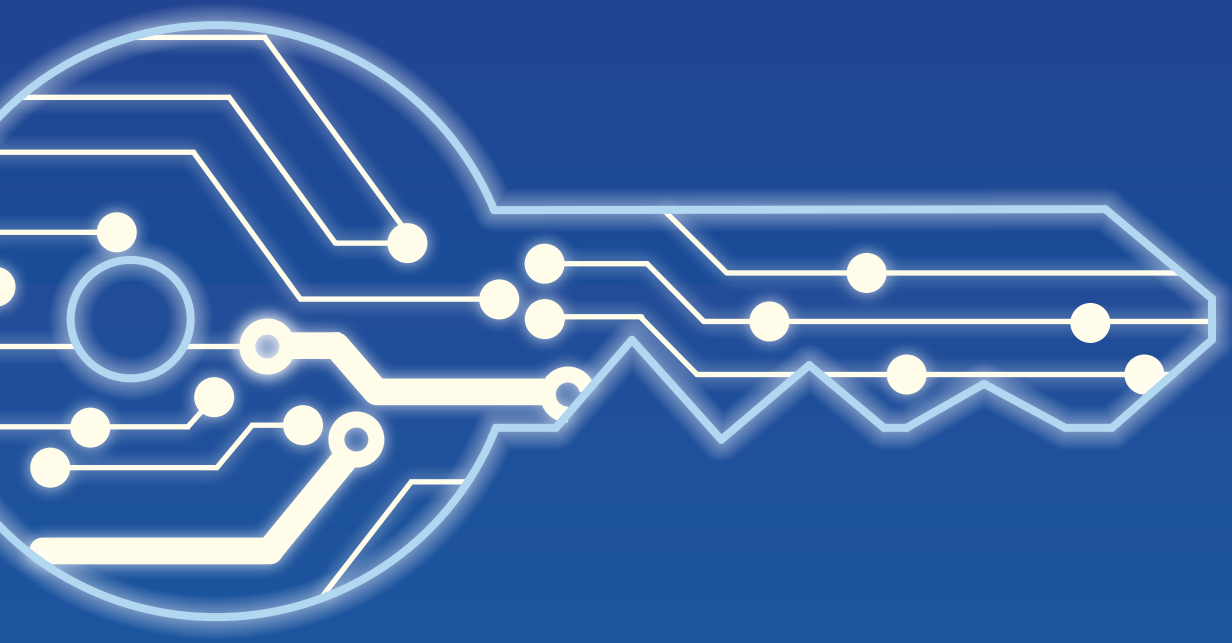
Bibliografía

- Alliance for Affordable Internet. **Coalición Guatemalteca para una Internet Asequible.** Disponible en: http://a4ai.org/guatemala/
- Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/
- Asociación de Derechos Civiles (2015). **Educar para vigilar: Una investigación acerca de la formación institucional estatal en vigilancia e investigación en el entorno digital.** Disponible en: https://adcdigital.org.ar/wp-content/uploads/2016/01/Educar-para-vigilar.pdf
- Banco Interamericano de Desarrollo y Organización de Estados Americanos (2016). Ciberseguridad: **¿Estamos preparados en América Latina y El Caribe?** Disponible en: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&
- CELE-UP (2012). **Hacia una Internet libre de censura: propuestas para América Latina.** Disponible en: http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf
- CELE-UP (2014). **Internet y derechos humanos: aportes para la discusión en América Latina.** Disponible en: http://www.palermo.edu/cele/pdf/InternetyDDHH.pdf
- CENIDH (2016). **Derechos Humanos en Nicaragua 2016.** Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf
- Congreso de la Repúbica de Guatemala. **Iniciativa 4090, Ley de Protección de Datos Personales.** Disponible en: http://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf
- Congreso de la República de Guatemala. **Iniciativa 5230**. Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=2636
- 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
- Congreso de la República de Guatemala. **Iniciativa 5254, Ley contra la Ciberdelincuencia.** Disponible en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf
- Consejo de derechos humanos - ONU (2014). **El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los derechos humanos.** Disponible en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjYmJj-8M3MAhXEHR4KHVVcCQYQFggdMAA&url=http%3A%2F%2Fwww.ohchr.org%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession27%2FDocuments%2FA-HRC-27-37_sp.doc&usg=AFQjCNGT_BPxxWGqFMXjIlOkF80ao6-TkA
- Comisión Interamericana de derechos humanos (2006). **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 (2013). **Informe Libertad de Expresión e Internet.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

- Comisión Interamericana de derechos humanos (2015). **Informe Situación de los derechos humanos en Guatemala: Diversidad, desigualdad y exclusión.** Disponible en: https://www.oas.org/es/cidh/informes/pdfs/Guatemala2016.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 Estándares para una Internet Libre, Abierta e Incluyente.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf
- Comision Interamericana de derechos humanos (2017). I**nforme de la Relatoría para la Libertad de Expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/anuales/InformeAnual2016RELE.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
- Derechos Digitales (2016). **Hacking Team Malware para la vigilancia en América Latina.** Disponible en: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.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
- 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.
- Front Line Defenders (2015). **Informe Anual 2015: Defensores (as) de derechos humanos en la cuerda floja.** Disponible en: http://www.coljuristas.org/documentos/adicionales/defensores_de_ddhh_en_la_cuerda_floja.pdf
- Front Line Defenders. **Annual Report Human Rights Defenders at risk in 2017.** Disponible en: https://www.frontlinedefenders.org/en/resource-publication/annual-report-human-rights-defenders-risk-2017
- Foro de Gobernanza de Internet de Guatemala. http://igf.gt/

- 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
- Medium.com. **Los Netcenters: Negocio de Manipulación.** https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc
- Ministerio de Gobernación. **Presentan conclusiones para mejorar Borrador de la Estrategia Nacional de Ciberseguridad.** Disponible en: http://mingob.gob.gt/presentan-conclusiones-para-mejorar-el-borrador-de-la-estrategia-nacional-de-ciberseguridad/
- Motherboard. **El imperio 'ilegal' de Hacking Team en América Latina.** Disponible en: https://motherboard.vice.com/es/article/wngqmx/el-imperio-ilegal-de-hacking-team-en-america-latina-5886b78158d4ae45b7112d84
- Nación Digital. https://www.naciondigital.gob.gt/
- 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/
- 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 (1999). **Resolución 53/144 del 8 de marzo de 1999.** Disponible en: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf
- Prensa Libre. **Una peligrosa propuesta de ley.** Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley
- Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2016). **Informe anual.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement
- Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2017). **Informe anual.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement
- Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2017). **Informe.** Disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/72/350

- 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
- Revista Factum. **Exterminio: El Estado cómplice.** Disponible en: http://revistafactum.com/exterminio-el-estado-complice/
- 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
- Soy502. **Los netcenteros de la impunidad.** Disponible en: http://www.soy502.com/articulo/netcenteros-impunidad-20878
- Soy502. **Periodistas exigen que el MP investigue a los "net centers".** Disponible en: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149
- Udefegua. **Situación de Defensoras y Defensores de derechos humanos en Guatemala Un Reflejo del Deterioro de los derechos humanos en el País.** Disponible en: http://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf
- Web We Want. **Carta de Derechos de Internet en Guatemala.** Disponible en: https://webwewant.org/es/guatemala/



FUNDACIÓN Acceso