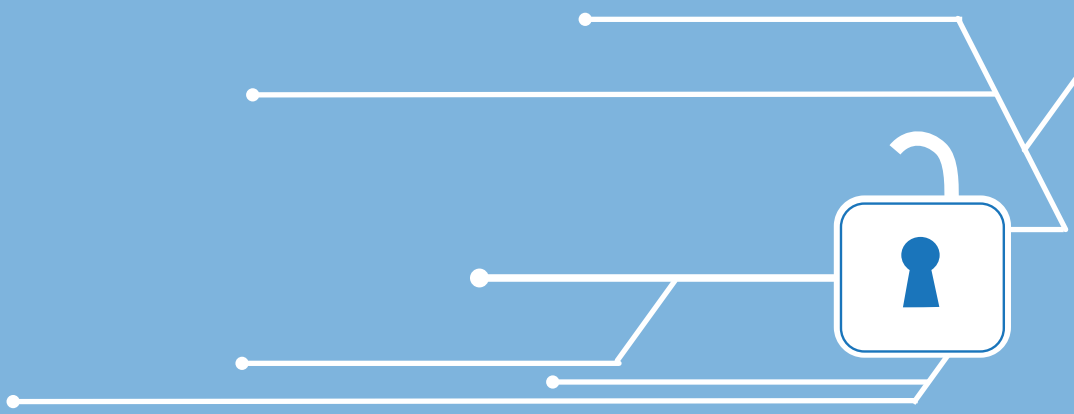
Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

Honduras



Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

Honduras

Observatorio Centroamericano de Seguridad Digital

Informe anual 2016

HONDURAS[1]

INTRODUCCIÓN

El Observatorio Centroamericano de Seguridad Digital (OSD) surge como una iniciativa de Fundación Acceso que logra consolidarse en el año 2016.

El objetivo general del OSD es registrar y analizar incidentes de seguridad digital de personas defensoras de DDHH que estén ejerciendo su defensoría en El Salvador, Guatemala, Honduras 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 un informe anual con la información recolectada.

Con esto se busca fortalecer los mecanismos de seguridad de defensores/as 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.

a) ¿Qué es un incidente de seguridad digital?

El Observatorio Centroamericano de Seguridad Digital registrará aquellos incidentes ocurridos a personas defensoreas de DDHH en Centroamérica relacionados con su información y/o comunicación digital almacenada, en movimiento y en servicios.

Por defensor/a de derechos humanos tomamos el concepto amplio que se maneja en la declaración de Naciones Unidas[2], considerando individuos, grupos e instituciones de quienes

1. El capítulo de Honduras ha sido elaborado por la asesora legal en el país, Kenia Oliva, con el apoyo de los técnicos Mario Ávalos y Alejandro Durón, y de la Encargada de Desarrollo Organizativo, Luciana Peri.

2. Organización de Naciones Unidas, *Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos.* Disponible en http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

tengamos referencia que luchen por la defensa de derechos humanos de los pueblos y las personas en El Salvador, Guatemala, Honduras y/o Nicaragua, sin importar su género, edad, lugar de procedencia, antecedentes profesionales o de ningún otro tipo.

Por incidente entendemos cualquier evento adverso (verificado o en sospecha) relacionado con la información (incluyendo datos y metadatos) y/o comunicación digital.

Para que sea digital, esta información y/o comunicación debe haber sido creada, procesada y comunicada por los dispositivos electrónicos computacionales de la actualidad, y puede estar almacenada, puede estar siendo transmitida o puede encontrarse en un servicio en línea o en cualquiera de las aplicaciones que utilizamos para acceder a ellos (desde el correo electrónico hasta las redes sociales y los blogs y medios independientes en linea).

Cuando se identifica un incidente que no cumple con los criterios para ser registrado por el Observatorio, de todas formas Fundación Acceso brinda la atención técnica necesaria para asegurar la información digital que pudo haber sido comprometida, y si se tratara de un incidente de otra variable de la seguridad, ya sea física, legal o psicoscoal, se refiere el caso con organizaciones aliadas a nivel local y regional que trabajen ese tema en particular.

b) Tipología de incidentes

Los incidentes registrados se catalogan según la siguiente tipología

- **Malware[3] o software malicioso:** Cualquier tipo de software[4] que se ejecuta en los dispositivos para interrumpir las operaciones y recolectar información sensible sin consentimiento del usuario administrador. También se pueden instalar de manera oculta como complementos 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[5]** 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 activan vídeo y audio también son considerados Malware.

- **Pérdida de hardware:** Robo, hurto, destrucción, o extravío del equipo.

- **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.

- **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

3. Techterms, *Malware.* Disponible en http://techterms.com/definition/malware.

4. Vamos a entender como Software como cualquier componente no tangible, por medio del cual se ejecutan determinadas instrucciones o rutinas que permiten utilizar un dispositivo.

5. Federal Trade Commission, *Staff Report. Monitoring Software on Your PC: Spyware, Adware, and Other Software*, (2005). Disponible en http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

6. 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 nuestras computadoras se conectan a internet.

7. La Red de Área Local (LAN, por sus siglas en inglés) 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 internet.

ataques remotos aprovechan vulnerabilidades del Módem[6] o del sistema operativo.

•**Ataques LAN[7]:** Bloqueo del tráfico de datos que circula en la red local, interrupción de las conexiones entre las computadoras de la red, denegación de acceso a servicios y generación de tráfico en la red. Un ejemplo es el de reconfigurar los routers o modems para bloquear determinadas páginas.

•**Ataques Web:** Toda ataque a los servicios de internet que utilizamos y el monitoreo de los mismos. Estos pueden ser servicios de blogs o noticias, nuestros sitios web, bloqueo de nuestro canal de Youtube u 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 se incluyen en esta categoría la censura de determinados sitios web por parte del Proveedor del Servicio de Internet, 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[8].

Una de las principales técnicas informáticas para este ataque es el **Phishing[9]** 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.

8. Recomendación de el equipo de Access Now a partir de su experiencia con el Help Desk.
9. Ed Skoudis, *Phone phishing: The role of VoIP in phishing attacks.*

Observatorio Centroamericano de Seguridad Digital

Momentos de Intervención:

FUNDACIÓN Acceso

c) Contexto nacional

Fundación Acceso elaboró una investigación en 2015 titulada "¿Privacidad digital para defensores y defensoras de derechos humanos?"[10] , en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región. En esta investigación se corroboró que en Honduras, en enero de 2011, con la entrada en vigencia de la Ley de Intervención de las Comunicaciones Privadas, se derogaron las normas del Código Procesal Penal sobre intervención de las comunicaciones. Esta nueva ley tiene por finalidad "establecer el marco legal de regulación procedimental de la intervención de las comunicaciones" y constituir "una herramienta esencial en la lucha contra la criminalidad tradicional, y sobre todo contra la criminalidad organizada o no convencional"; es decir que la ley tiene aplicabilidad en la investigación de cualquier delito.[11]

Por ejemplo, en febrero de 2013, el Poder Judicial ordenó la intervención de las comunicaciones privadas de una Defensora de Derechos de las Mujeres por una denuncia de supuesta difamación en la red social "Facebook"[12]. Es decir, la Ley que fue concebida para la investigación de la criminalidad organizada y del narcotráfico, abrió las puertas para la intervención de la investigación de cualquier tipo de delitos, inclusive para aquellos delitos de acción privada.

Es importante señalar que, previo a la aprobación de esta Ley de Intervención a las Comunicaciones, se aprobó la Ley contra el Financiamiento al Terrorismo, las dos normas legales han puesto en alerta a los y las defensoras de derechos humanos que desde el golpe de Estado del año 2009 han señalado que sus comunicaciones pueden estar intervenidas con el propósito de perseguir y criminalizar su labor.

El Comité por la Libertad de Expresión (C-Libre) publicó un análisis sobre la Ley de Intervención a las Comunicaciones, en el cual plantea que esta ley abre la puerta para violentar la garantía constitucional a la privacidad, es decir, ese derecho individual a no sufrir intromisiones en la intimidad por parte del Estado, que encuentra hoy reconocimiento tanto a nivel nacional como internacional. La Constitución de la República en su artículo 100 establece que "Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales telegráficas y telefónicas, salvo resolución judicial". Si se toma en cuenta este último mandato podríamos decir que la existencia de una ley especial restringiendo este derecho no es inconstitucional, pero esa restricción debe ser proporcional a la afectación del bien jurídico que se

10. Fundación Acceso, *¿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* (San José, Costa Rica: 2015). Disponible en http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf

11. Fundación Acceso, *¿Privacidad digital para defensores y defensoras de derechos humanos?*, 175.

12. Caso Lesbia Pacheco, ante el Tribunal de Sentencia de Tegucigalpa, Honduras, Exp. 68-2013.

pretende proteger, por existir visiblemente un conflicto de bienes jurídico protegidos: por un lado la privacidad y por el otro cualquiera que podría lesionar el actuar ilegal de una persona o un grupo de personas en perjuicio de otros.

Es así que la pretensión de aprobar este tipo de ley debe estar sujeta al establecimiento de mecanismos de control adecuados, y resultará un arma poderosa para violentar este derecho garantizado por la Constitución y demás tratados internacionales, como los desprendidos en los Art. 11 inc. 2do. del Pacto de San José de Costa Rica, 17.1 del Pacto Internacional Derechos Civiles y Políticos, 12 de la Declaración Universal de Derechos Humanos, 5 de la Declaración Americana de Derechos y Deberes del Hombre.[13]

En los últimos meses del año 2016, organizaciones de derechos humanos, denunciaron hackeos a sus páginas web y señalaron como responsables a funcionarios del Estado. Las denuncias fueron dirigidas a las autoridades encargadas de realizar investigación al respecto, sin embargo el Ministerio Publico en resolución 347-2016, de fecha 16 de noviembre del 2016, respondió una solicitud de información respecto a las denuncias registradas por intervención a las comunicaciones digitales. El Ministerio Público, a la fecha de esa resolución, informó que en la Fiscalía Especial de Protección a la Propiedad Intelectual y Seguridad Informática, no tiene registrada ninguna denuncia del 2015-2016. Lo anterior debe de llevarnos a la reflexión.

Ataque a defensores y defensoras de derechos humanos

En Honduras durante los años 2015-2016 al menos dos organizaciones de derechos humanos denunciaron públicamente ataques a sus sitios web [14](CITA) y al menos cuatro personas defensoras de derechos humanos denunciaron ataques a sus redes sociales y correos electrónicos.

Los ataques que han denunciado organizaciones como por ejemplo la Asociación para una Ciudadanía Participativa (ACI Participa), se refieren al hackeo de su cuenta institucional. Esta organización denunció que “el 22 de Septiembre del año 2015, utilizando entre otras, la técnica el Phishing, para hacerse de la información contenida en dicha cuenta. En su ciber delito, el o los delincuentes, lograron obtener y posteriormente borrar todos los contactos de la organización como todos sus archivos, carpetas y correos enviados y recibidos, perjudicando grandemente, la comunicación tanto de organismos e institucionales nacionales e internacionales como de nuestros beneficiarios del trabajo de defensoría que realizamos” [15].

13. http://conexihon.hn/site/opiniones/palabra-libre/an%C3%A1lisis-sobre-la-ley-especial-de-intervenci%C3%B3n-de-las-comunicaciones

14. C-Libre, “ACI Participa sufre ciberataque”, Alerta 162-15, 24 de septiembre de 2015. Disponible en http://www.clibrehonduras.com/alerta/aci-participa-sufre-ciberataque y Criterio, “COFADEH denuncia hackeo de su página y construcción de falsos positivos”, 16 de diciembre de 2016. Disponible en http://criterio.hn/2016/12/16/cofadeh-denuncia-hackeo-pagina-construccion-falsos-positivos/

15. C-Libre, “ACI Participa sufre ciberataque”, Alerta 162-15.

Los ataques registrados corresponden a un posible delito de suplantación de identidad e intervención a las comunicaciones privadas. Hasta la fecha, en Honduras, personas que se dedican a la labor de defensa de derechos humanos constantemente denuncian en las redes sociales o en los medios de comunicación este tipo de ataques.

1. PRINCIPALES HALLAZGOS EN HONDURAS

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Honduras. Los mismos han sido registrados entre los meses de junio y noviembre de 2016. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

1.1) Procedimiento para el registro de incidentes

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

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 inspección, 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 inspección y devolución del equipo, donde constan las conclusiones de la inspección y posibles acciones de seguimiento.

1.2) Casos registrados

El inicio del Observatorio se vio marcado por una etapa de definir procesos tanto desde el ámbito técnico como desde el ámbito legal. En una primera fase, Fundación Acceso, junto al equipo técnico en Honduras, visitó a varias organizaciones de derechos humanos en en el país y posteriormente, se realizó una reunión de socialización de avances con las organizaciones visitadas en la primera etapa y se invitó nuevas organizaciones así como agencias de Cooperación en el País.

Para el Observatorio no fue posible registrar todos los casos, en vista que las personas que denuncian públicamente no tienen esperanza de que, al descubrir quién o quiénes realizan los ataques a sus redes sociales o correos electrónicos, estas reciban alguna sanción por parte de los operadores de justicia, lo que ayuda a comprender por qué la Fiscalía de Protección a la Propiedad Intelectual y a la Seguridad Informática, informa que no tiene registrado ningún caso sobre hackeos a cuentas de correos electrónicos o redes sociales.[16]

16. Resolución DGF-347-2016, de fecha 15 de noviembre del 2016.

Durante el año 2016, el Observatorio registró tres casos en Honduras, y otros dos casos no llegaron a ser registrados por no lograr concertar visitas con las personas denunciantes. Sin embargo, se tuvo algunos acercamientos con ellas a fin de darles a conocer la posibilidad de registrar su caso.

Los casos efectivamente registrados están relacionados con personas que trabajan como defensoras de derechos humanos. Una de ellas fue asesinada en marzo del 2016; otra es una defensora que se ha caracterizado por denunciar públicamente casos de corrupción de la Policía Nacional, señalando a personas de altos rangos como presuntas responsables; la tercera organización trabaja el derecho a la tierra y la seguridad alimentaria de grupos campesinos.

a) Perfil de las personas/ organizaciones que reportaron incidentes

Defensora de Derechos Humanos: El primer caso sobre el que se tuvo noticia y que cumplía, inicialmente, con los criterios para ser registrado por el Observatorio. Se trata de la hija de Bertha Cáceres, reconocida defensora de derechos humanos asesinada en marzo de 2016, cuyo asesinato ha sido atribuido al ejercicio de la defensa de territorios indígenas y del medio ambiente. Después de su asesinato sus hijas han denunciado y señalado públicamente a posibles responsables.

Defensora de Derechos Humanos: El segundo caso se trata de una Comisionada de Policía, que desde hace unos años ha denunciado de forma reiterada los actos de corrupción y abusos por parte de esa institución, fue separada de su cargo por estas denuncias, y ha sido perseguida y amenazada de diferentes formas.

Organización defensora de la Tierra: Esta organización trabaja para la defensa y promoción de los derechos de campesinos y campesinas, quienes luchan por reivindicar su derecho de acceso a la tierra. Honduras enfrenta graves denuncias por violaciones a derechos humanos relacionados con el acceso a la tierra, en ese contexto Vía Campesina ha sido una organización que constantemente ha acompañado a víctimas y ha denunciado y señalado posibles responsables de estas violaciones.

b) Tipos de ataques

Bertha Zúñiga Cáceres, se contactó con Fundación Acceso porque el correo personal de su madre estaba siendo utilizado después de que fuera asesinada, y solicitaba apoyo técnico para averiguar sobre la utilización indebida de su cuenta de correo electrónico de Gmail.

El técnico de Fundación Acceso en Honduras solicitó apoyo a Access Now, quien nos comunicó que no existe un mecanismo legal para obtener información de Google acerca del uso que se dio a la cuenta. Esto solo podría ocurrir de abrirse un caso legal en Honduras, para lo cual habría que identificar responsables y que, llegado ese punto, solicitud judicial mediante, tal vez Google podría enviar información al respecto.

María Luisa Borjas: Defensora de derechos humanos, quien interpuso denuncia ante el Comité por la Libertad de Expresión (C-Libre), sobre hackeo a su cuenta de Twitter, suplantación de su fotografía de perfil y una amenaza en el mismo.

Su cuenta de Twitter fue manipulada, colocando como foto de perfil la imagen de una mujer ensangrentada, con la boca amordazada y un mensaje amenazante en su perfil. Esto ocurrió justamente después que ella diera declaraciones en los medios de comunicación sobre posibles implicados en la muerte de un miembro de la policía.

Fundación Acceso le realizó una visita, se le tomó declaración para entender el contexto en el que se dieron los hechos, y ella firmó la hoja de consentimiento informado, sobre la utilización de su nombre y su información por Fundación Acceso.

El técnico se comunicó con una organización aliada en Costa Rica que también trabaja el tema de seguridad digital, y esta informó que, por el trascurso del tiempo y las políticas de seguridad de Twitter, era difícil ya en ese momento determinar de dónde provenía el ataque.

Vía Campesina Honduras: Reportaron denegación de sitio en la página web institucional desde el mes de marzo, razón por las que se habían realizado algunas pruebas técnica y se realizó una visita, en la cual se nos informó que la organización había cancelado el alojamiento de la página y no utilizaban más la misma, sin embargo reportaron posible hackeo en su página de Facebook.

Se realizó el análisis técnico y se verificó que había una mala utilización de la página, dejando muchos canales abiertos, lo que permitía que otras personas pudieran publicar desde su página.

Además su router, no tenía ninguna contraseña y esto hacia que cualquier persona pudiera ingresar a su red de internet.

2. 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.

2.1) Violaciones de derechos

A continuación se presenta un análisis del marco jurídico, a través de cada una de las contravenciones en las que se pudo haber incurrido al analizar los casos que se han descrito en el apartado anterior.

a) Posibles Derechos fundamentales/humanos vulnerados

El caso de las dos defensoras puede tratarse de un delito de violación de su derecho a la privacidad contemplado en el Artículo art. 76 de la Constitución de la República, que garantiza el derecho a la intimidad personal, familiar y a la propia imagen.

El delito cometido en el caso de la utilización del correo electrónico de Berta Cáceres, después de su asesinato puede considerarse, además de un delito contra la privacidad a la intimidad personal, un delito de suplantación de identidad.

b) Posibles Tipificaciones penales

En Honduras no existe una legislación que regule debidamente el tema de la privacidad digital, hasta ahora las únicas sanciones por el tema suplantación de identidad o de intervención a las comunicaciones son contemplados como delitos de estafas o fraudes financieros, pero no hay ninguna normativa que regule y sancione la intervención ilegal a las comunicaciones, entre ellos la intervención a las comunicaciones digitales.

2.2) Estrategias de respuesta

En este apartado se presentan las distintas estrategias de respuesta que se pueden implementar para abordar los casos que han sido registrados en el Observatorio y prevenir futuros incidentes a

la seguridad digital de defensoras y defensores de derechos humanos.

a) Legales

Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

•Acciones constitucionales (Habeas Data, Amparos, Habeas Corpus, etc.)

En Honduras, se podría iniciar una acción de amparo, puesto que la ley de Justicia Constitucional, que es la que establece el procedimiento para los amparos, procura proteger derechos garantizados en la Constitución y, siendo a privacidad de las comunicaciones un derecho constitucional, se podría intentar un amparo para salvaguardar este derecho. Así como una acción de habeas data, ya que la Constitución establece el derecho a salvaguardar los datos personales.

Estos recursos solo cabrían si se determinara que la intervención a las comunicaciones ha sido ordenada por alguna autoridad y que esta se haya realizado de alguna manera que violente el debido proceso.

•Denuncias

En los casos registrados en Honduras, corresponde denunciar al Mecanismo Nacional de Protección a Defensores/as de Derechos Humanos, pues este Mecanismo tiene el deber de investigar los hechos y de proteger la integridad de las defensoras, así como de evitar que, de alguna manera, se les obstaculice realizar de manera segura su labor como defensoras.

•Sistema Interamericano de Derechos Humanos

En relación al Sistema Interamericano de Derechos Humanos se debe tratar de documentar estos y otros casos que permitan identificar patrones de actuación de parte de organizaciones 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 y así visibilizar la situación de la seguridad digital a nivel regional.

•Otros que se consideren pertinentes (Sistema Nacional de Protección a Defensores/as de Derechos Humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia)

Una de las estrategias del Observatorio en Honduras, debe ser hacer que el Mecanismo Nacional de Protección a Defensores/as de Derechos Humanos asuma su responsabilidad legal de realizar todas las acciones encaminadas a brindar seguridad a las personas defensoras de derechos humanos, de promover políticas públicas que permitan la realización plena de la defensa de derechos humanos y de investigar los casos de cualquier tipo de ataque a personas defensoras.

Actualmente el Mecanismo Nacional de Protección, tanto en su ley como su reglamento, únicamente contempla medidas de protección física, parcialmente psicológica y legal, pero

no contempla protección a la seguridad digital de sus beneficiarios.

La implementación de algunas medidas de protección contempladas por el Mecanismo Nacional pueden poner en riesgo la seguridad digital de las personas beneficiarias, ya que una de las medidas de seguridad incluye botones de pánico, que es un dispositivo que será instalado en los teléfonos móviles de los y las beneficiarias del mecanismo y que será controlado por empresas de seguridad privadas, contratadas por el Estado de Honduras.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1.En Honduras la labor de defensa de derechos humanos se realiza en un contexto adverso para las y los defensores, y existen vacíos legales 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.

2.Existen incidentes de seguridad digital y estos afectan directamente la labor que las y los defensores de derechos humanos realizan, poniendo en peligro su información, su trabajo e incluso sus vidas.

3.El tema de la 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 pueden ser atacados.

Recomendaciones

1.Es necesario reformar el marco normativo legal para mejorar la protección que se le brinda a las y los defensores de derechos humanos, protegiendo sobre todo su seguridad digital.

2.Las y los defensores de derechos humanos deben generar protocolos internos dirigidos a

fortalecer sus seguridad digital, para que a través de ésta se fortalezca de manera integral sus seguridad en general.

3.Debe incluirse un apartado específico sobre seguridad digital en los informes sobre situación de defensoras y defensores de derechos humanos para visibilizar la importancia que esta tiene en un concepto integral de seguridad.

BIBLIOGRAFÍA

•C-Libre. “ACI Participa sufre ciberataque”. Alerta 162-15. 24 de septiembre de 2015. Disponible en http://www.clibrehonduras.com/alerta/aci-participa-sufre-ciberataque

•Criterio. “COFADEH denuncia hackeo de su página y construcción de falsos positivos”. 16 de diciembre de 2016. Disponible en http://criterio.hn/2016/12/16/cofadeh-denuncia-hackeo-pagina-construccion-falsos-positivos/

•Fundación Acceso. “Marco General para el funcionamiento del Observatorio de Seguridad Digital”. San José C.R. 2016.

•Fundación Acceso. “¿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”. San José C.R. 2015.

•Tribunal de Sentencia de Tegucigalpa, Honduras. “Caso Lesbia Pacheco”. Exp. 68-2013.

ioxwxvU

Eb

HlqVRomqggh
j86Z/sIDhll vy5

j86Z/sIDhll vy5Wvrrsk

FUNDACIÓN Acceso