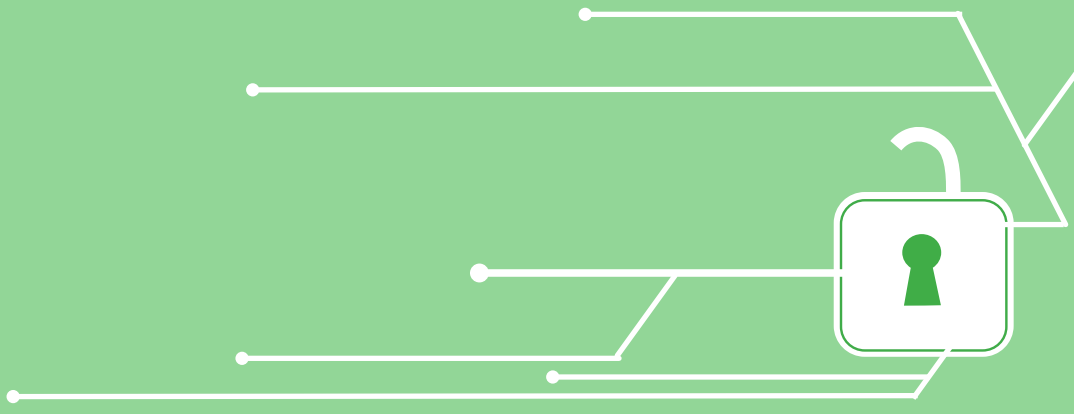
Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

Guatemala



Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

Guatemala

Observatorio Centroamericano de Seguridad Digital

Informe anual 2016

GUATEMALA[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 tengamos referencia que luchen por la defensa de derechos humanos de los pueblos y las personas

1. El capítulo de Guatemala ha sido elaborado por el asesor legal en el país, Ernesto Archila Ortiz, con el apoyo de los técnicos David Oliva y Arturo Chub, 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

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:

Contacto Inicial 1

Ya sea por llamada telefónica, video-llamada, e-mail, mensaje de texto, mensajería instantánea, o personalmente. Se decide si puede o no ser un incidente, y si el/la técnico/a asistirá o no al lugar (1° Módulo del reporte)

2 Verificación

Técnico/a asiste al lugar para definir si efectivamente es un incidente o si es un falso positivo (2° Módulo del reporte)

Pre-diagnóstico 3

Si efectivamente es un incidente, se realiza una nueva visita al lugar con el/la abogado/a y se realiza un pre-diagnóstico, se define una estrategia (en conjunto con el/la defensor/a u organización de DDHH) y se decide si solo se registra o si es un posible caso jurídico (3° Módulo del reporte)

4 Implementación de Estrategias

Abogado/a y técnico/a realizan las acciones de la estrategia a la que se comprometieron durante la estrategia (4° Módulo del registro)

Peritaje Especializado 5

Abogado/a y técnico/a deciden si es necesario hacer un peritaje especializado para el que se necesita apoyo externo (Se agrega un 5° Módulo al registro con las acciones a tomar)

6 Resultados Peritaje

Resultados del peritaje (Se agrega un 6° Módulo al registro con los resultados del peritaje)

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 esa investigación se establecieron algunos parámetros aplicables al contexto nacional que hoy siguen estando vigentes casi en las mismas condiciones en las que se planteó en el estudio. En términos generales se estableció que hay un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[11], sin embargo a nivel de regulación penal el Estado no ha actualizado su catálogo de delitos para incluir aquellas acciones que afectan el derecho a la privacidad digital.

De igual forma existe muy poca discusión a nivel público respeto de la importancia que tiene proteger la privacidad digital de todas las personas, en especial 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 queden en la impunidad.

Ataque a defensores y defensoras de derechos humanos

En el último año se han publicado informes preocupantes que establecen una serie de amenazas para la labor que desempeñan las y los defensores de derechos humanos. La Corte Interamericana de Derechos Humanos en un informe especifico sobre la situación de las personas defensoras en el Continente identificó que, más allá de generar espacios y mecanismos para que pudiesen desempeñar su función en forma libre y segura, se estaban generando desde el Estado procesos de criminalización a través de la judicialización de los conflictos sociales y el encarcelamiento de líderes y lideresas locales, abusando del uso de los procesos penales.[12]

De igual forma en el caso de Guatemala un informe elaborado por un conjunto de organizaciones a nivel regional y publicado en febrero de 2016 indica que los procesos de criminalización en contra de personas defensoras exceden cualquier racionabilidad en los plazos. Plantean el caso de Saul y Rogelio, dos defensores del territorio quienes, luego de un proceso sumamente complicado, fueron absueltos. Sin embargo, ya habían pasado casi dos años y medio privados de libertad.[13]

Se puede ver que en estos documentos son abordados los incidentes que tienen que ver con la seguridad física de las y los defensores pero no son identificados o abordados los incidentes que

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. Comisión Interamericana de Derechos Humanos*, Criminalización de la labor de defensores y defensoras de derechos humanos*, (CIDH: 2015), 44.

13. Observatorio para la Protección de Defensores de Derechos Humanos, *Criminalización de defensores de derechos humanos en el contexto de proyectos industriales: un fenómeno regional en América Latina,* (2015), 12.

ponen en riesgo su seguridad digital. Esto puede deberse a dos circunstancias: no existen estos incidentes y por lo tanto no hay nada que registrar; o sí existen pero estos no son registrados por falta de conocimiento o sensibilización respecto de su importancia.

De los resultados preliminares de este Observatorio se puede determinar que estos incidentes sí existen y que pueden poner en riesgo la vida y la integridad de las y los defensores de derechos humanos.

1. 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 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.

Los casos registrados para el 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. Concretamente con personas y organizaciones que realizan periodismo independiente y organizaciones feministas. Con algunas de ellas se tuvo contacto al momento que alguien del equipo realizó las visitas periódicas a las organizaciones; y en otros, al momento de compartir distintos espacios de reflexión con colectivos, donde surge la necesidad de revisar alguna situación que pueda ser un incidente digital.

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. Esto llevó a que los primeros meses de implementación sirvieran para el montaje organizacional y la construcción de los protocolos y formatos necesarios. Posteriormente se pudo dar inicio a la etapa de registro. Durante el año 2016, en Guatemala se registraron tres casos.

a) Perfil de las personas/ organizaciones que reportaron incidentes

Periodista/comunicador individual: Este fue el primer caso sobre el que se tuvo noticia y que cumplía inicialmente con los criterios para ser registrado en el Observatorio. Este periodista ha trabajado para varios medios alternativos que difunden su trabajo por medios digitales. Su trabajo ha sido periodismo de investigación relacionado a las actividades de proyectos mineros e hidroeléctricos y su posible relación con escenarios de alta conflictividad en las comunidades donde estos proyectos se han asentado o pretenden hacerlo. De igual forma ha abordado temas vinculados al funcionamiento del sistema de justicia y la lucha contra la impunidad de casos del pasado y del presente.

Organización feminista: La organización trabaja por la defensa y promoción de los derechos de las mujeres, principalmente aquellas en condiciones de mayor vulnerabilidad. Ha tenido un trabajo activo en la labor por la transformación de esas condiciones de discriminación, además ha trabajado en el empoderamiento de las mujeres, sobre todo en el ámbito de acceso a la justicia, logrando avances importantes en materia de reconocimiento de la violencia patriarcal y las consecuencias que esta ha tenido a nivel social.

Medio digital independiente: Este medio aborda temas de alta conflictividad a nivel nacional. Ha presentado importantes investigaciones y reportajes relacionados al funcionamiento del sistema de justicia, las actividades mineras e hidroeléctricas. Junto con otros medios independientes ha logrado marcar un contrapeso en la opinión pública frente al control monopólico de los medios de comunicación masivos que tradicionalmente han estado a favor de las empresas extractivas y la criminalización de defensores y defensoras de derechos humanos.

b) Tipos de ataques

En el caso del periodista independiente su computadora realizaba capturas de pantalla sin que él estuviera dando ese comando específico. Ante la sospecha de que podía responder a una **infección de malware a la medida** se corrieron todos los programas de verificación con los que cuenta Fundación Acceso para identificar este tipo de malware, sin embargo ninguno de ellos presentó un resultado positivo para este tipo de software malicioso.

Finalmente se determinó que no había existido un ataque al periodista, que las capturas de pantalla podían obedecer a la posición del botón que tiene ese comando en esa computadora específica, lo que provocaba que él mismo lo presionara involuntariamente al estar utilizando el teclado.

El caso de la organización feminista tiene que ver con **pérdida de hardware y de información digital**. El problema que se presentó fue que una persona externa a la organización prestó los

servicios de mantenimiento informático para la organización y al hacerlo hurtó tres computadoras que se encontraban en la organización, pero no pertenecían a la misma. Además hurtó información de las computadoras institucionales que revisó, así como de su sitio web.

Por la gravedad del caso la organización puso los hechos en conocimiento del Ministerio Público, para que procediera con la investigación. Paralelamente la organización contactó al Observatorio para que prestara la atención técnica y se procediera al registro del caso. Desde el Observatorio se tomaron las siguientes medidas: como ya era un caso de conocimiento del Ministerio Público se decidió no manipular el equipo hasta que los análisis correspondientes fueran realizados por el ente fiscal; por otro lado se reactivaron el servidor y el firewall para que la organización pudiera tener acceso seguro a sus datos.

Durante ese período de espera ocurrieron dos cosas importantes. Primero el Ministerio Público no realizó los análisis correspondientes sobre el equipo que había sido comprometido, lo cual denota una falta de acceso a la justicia pues el hecho fue reportado y nunca se investigó. Por otro lado, cuando fue claro que el Ministerio Público no haría ninguna investigación, el equipo de Fundación Acceso realizó un análisis forense sobre el equipo en cuestión, llegando a la conclusión que el mismo había sido utilizado[14] contraviniendo la disposición del Ministerio Público y de la propia organización de no utilizar el equipo. Esto es particularmente grave porque supone una violación a los protocolos internos de la organización y la sospecha de que los perpetradores podían formar parte de la misma.

Luego de concluida la inspección técnica se presentó a la organización un reporte técnico descriptivo y gráfico sobre el comportamiento de los equipos que fueron objeto de la inspección. Además se le presentaron a la organización una serie de recomendaciones para mejorar sus protocolos de seguridad digital.

Como conclusión general del caso se estableció como un factor a considerar en futuras inspecciones el hecho de que las decisiones tomadas por las organizaciones no necesariamente son cumplidas por su personal, hace necesario que el equipo objeto de la inspección quede protegido de cualquier tipo de manipulación por parte de personal interno y externo de la organización.

Por último, el medio digital independiente reportó que se había enviado información desde un correo electrónico externo haciéndose pasar por su organización, por lo que se sospechó de una suplantación de correo electrónico, mediante la técnica de email spoofing. En estos correo electrónicos se enviaba información haciendo creer que era producida por el medio. Sin embargo estos correos electrónicos no guardaban ninguna relación con la línea editorial del medio, ni en

14. Extracción de datos, uso de memorias usb, navegación en internet y revisión de datos.

contenido ni en estética. Esto perjudicaba la imagen del medio, por lo que era necesario identificar el origen del problema para impedir que siguiera difundiéndose esa información falsa.

Desafortunadamente, luego del contacto inicial y de compartir alguna información primaria por correos electrónicos, no fue posible darle continuidad al caso pues la persona encargada desde el medio digital independiente no le dio seguimiento. Esto imposibilitó que el equipo de Acceso pudiera hacer su inspección técnica y correspondiente registro. Es lamentable porque parecía ser un ataque directo a la organización y un caso que podía ejemplificar de buena forma el tipo de ataques que pueden sufrir las y los defensores de derechos humanos.

c) Posibles perpetradores

En el caso del periodista independiente no fue identificado ningún posible perpetrador pues se descartó que la persona estuviera siendo víctima de una ataque a su seguridad digital.

En el caso de la organización feminista fue identificado el perpetrador como esa persona que robó equipo e información de la organización, y en su momento fue puesto de conocimiento de las autoridades. Hasta el momento no se logró determinar si esa persona obró en forma independiente o en comunicación con alguien más. Además en este caso se determinó que hubo otros perpetradores, quienes robaron información adicional ignorando la orden del Ministerio Público de no utilizar ese equipo mientras no fuera revisado por las autoridades.

En el caso del medio digital independiente al no poder realizarse la inspección técnica, no fue posible identificar posibles perpetradores.

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 Guatemala del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos.

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 del periodista independiente no resultó ser un caso de malware a la medida. Sin embargo, de haberse confirmado dicha sospecha, se le hubiera indicado a la persona que se le estaba violando su derecho a la privacidad contemplado en el Artículo 24 de la Constitución Política de Guatemala, que establece la inviolabilidad de correspondencia, documentos y libros pues ninguna persona tendría derecho de revisar su información sin su consentimiento, salvo que existiese una orden de juez competente para hacerlo.

En el caso de la organización feminista también fue violado el artículo 24 pues, más allá del robo del equipo, en el curso de la inspección técnica quedó demostrado que hubo personas que accedieron, sustrajeron o eliminaron información privada de la organización sin autorización para ello.

En el caso del medio digital independiente, no se tienen suficientes elementos para determinar qué derechos fundamentales pudieron haber sido violados.

b) Posibles Tipificaciones penales

En la investigación de 2015 de Fundación Acceso fue establecido que el marco normativo penal era insuficiente para proteger el derecho a la privacidad digital de las y los defensores de derechos humanos. Sin embargo, utilizando las herramientas con las que se cuenta se puede establecer que, en el caso de la organización feminista, además del robo de equipo físico, los perpetradores pudieron haber incurrido en el delito de violación de correspondencia y papeles privados (artículo 217) e intercepción o reproducción de comunicaciones (artículo 219) contemplados en el Código Penal, sin embargo las penas de ambos delitos constituyen multas de muy bajo valor (de U$65 a U$650 aprox.), lo que además denota la poca relevancia que el legislador le da a este tipo de delitos.

En cuanto a los otros dos casos del Observatorio no se cuentan con los suficientes elementos para determinar posibilidad de responsabilidades penales.

c) Posibles infracciones administrativas

En el caso de la organización feminista se puede establecer que el Ministerio Público incurrió en responsabilidad administrativa por tener conocimiento del hecho delictivo y no haber investigado apropiadamente el hecho a pesar de la buena disposición de la organización para que se realizaran las pericias necesarias en el equipo comprometido.

De igual forma la organización falló en implementar protocolos que aseguraran que la orden emanada del Ministerio Público fuera cumplida a la perfección. Esto pudo haber puesto en riesgo la investigación penal si esta se hubiera llevado a cabo más adelante.

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 el caso del periodista independiente ya se ha indicado que no hay elementos para concluir que ha sido objeto de vigilancia. Pero de haber sido así, se pudo haber planteado una Acción Constitucional de Amparo en contra del Ministro de Gobernación pues es la autoridad encargada por velar que sea respetado el derecho a la privacidad digital, y en su caso, determinar el origen de la vigilancia ilegal de que pudiera estar siendo objeto.

  En el caso de la organización feminista procedería seguir presionando la investigación penal para lograr determinar la responsabilidad de los perpetradores. Si el caso no avanzara sí se podría interponer un amparo en contra del fiscal a cargo del caso para solicitar que las investigaciones se continúen.

- Denuncias Penales

  En el caso de la organización feminista la denuncia penal ya fue interpuesta. Lo que corresponde es presionar al Ministerio Público para que continúe con las investigación. En los otros dos casos del Observatorio no procede realizar denuncias penales.

•Vías Administrativas (Contencioso administrativo, acceso a la información, etc)

En el caso de la organización feminista lo que correspondería sería plantear una queja ante la Fiscal General por el mal proceder del Fiscal a cargo de la investigación. Pues éste indicó que llegarían de parte del Ministerio Público a realizar las averiguaciones correspondientes por lo que ellas tomaron la decisión de no utilizar el equipo hasta que el personal fiscal llegara, pero ellos nunca acudieron a la organización.

Esto tendría el objeto de activar la propia investigación pero también prevenir que estas situaciones se puedan dar en casos futuros. En todo caso promover que el Ministerio Público genere protocolos de actuación para este tipo de casos.

•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 actores que puedan estar vigilando a defensores y defensoras de derechos humanos. Esta información ponerla de conocimiento de las respectivas relatorías para que puedan ser incluidos en sus informes periódicos y así visibilizar la situación de la seguridad digital a nivel regional.

•Otros que se consideren pertinentes

Si es impulsada alguna de las estrategias legales contempladas en este apartado, acudir a la Procuraduría de los Derechos Humanos puede ser útil para presionar a algún funcionario público que no este realizando su trabajo en forma adecuada. De igual forma la Procuraduría de los Derechos Humanos puede documentar este tipo de incidentes de seguridad digital e incluirlos en sus informes anuales sobre la situación de derechos humanos en general y en particular los relacionados con la seguridad digital.

b) No legales

Se deben fortalecer los procesos de sensibilización y formación a lo interno de las organizaciones de defensa de los derechos humanos pues en muchos casos continúa habiendo poca conciencia sobre la importancia que tiene proteger la seguridad digital. Para ellos es necesario seguir promoviendo espacios de reflexión, talleres, conferencias, seminarios, etc. que permitan normalizar el discurso de la seguridad digital y que se vuelva un elemento esencial para el trabajo que realizan las organizaciones.

De igual forma se deben promover espacios de diálogo con instituciones aliadas que pueden contribuir a posicionar un discurso favorable para la protección de la privacidad digital de las y los

defensores de derechos humanos. Posteriormente, definir una estrategia para plantear la necesidad de reformar y actualizar el ordenamiento jurídico referente al tema.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1.Persiste el contexto adverso para la defensa de las y los defensores de derechos humanos y los 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

•Comisión Interamericana de Derechos Humanos. 2015. Criminalización de la labor de defensoras y defensores de derechos humanos. Comisión Interamericana de Derechos Humanos. 2015.

•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.

•Observatorio para la Protección de Defensores de Derechos Humanos. 2015. Criminalización de defensores de derechos humanos en el contexto de proyectos industriales: un fenómeno regional en América Latina. 2015

ioxwxvU

Eb

HlqVRomqggh

j86Z/sIDhll vy5V

j86Z/sIDhll vy5WvrrskJ

FUNDACIÓN Acceso