GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

INFORME DE EVALUACIÓN INICIAL

Pais: COSTA RICA

Capacidades de Justicia Penal en materia de cibercrimen y evidencia electrónica

Elaborado en el marco del proyecto GLACY+

08 Agosto 2018

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

CONTENIDOS

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

1. Introducción

El presente informe ha sido preparado en el marco del proyecto ampliado GLACY+, sobre Acción Global contra el ciberdelito, con la finalidad de realizar una evaluación inicial sobre el estado de la Justicia de Justicia Penal en Costa Rica en lo que se refiere tanto al tratamiento del ciberdelito como al uso, reconocimiento y admisión de evidencias electrónicas y el fortalecimiento de las capacidades institucionales del sistema de justicia penal para llevar a cabo investigaciones en materia de ciberdelitos.

1.1 Objetivos

El Proyecto se dirige a fortalecer las capacidades del estado costarricense en la aplicación de la legislación sobre cibercriminalidad, evidencia electrónica y medidas de cooperación internacional como medios para garantizar una respuesta eficaz, y armonizada con la normativa internacional, en la lucha contra la ciberdelincuencia. Para ello, el programa se divide en tres componentes cada uno de los cuales persigue un objetivo diferente:

- Objetivo 1: Promover la adopción e implementación de legislación, políticas y estrategias efectivas en la lucha contra la ciberdelincuencia.

- Objetivo 2: Fortalecer la capacidad de las autoridades policiales en la investigación del ciberdelito y promover una cooperación inter-policial efectiva a nivel interno así como a nivel internacional con las unidades de cibercrimen de Europa y otras regiones del mundo.

- Objetivo 3: Facilitar a las autoridades del sistema de justicia penal la aplicación de la legislación y la persecución y atribución de la competencia en los asuntos de ciberdelincuencia y evidencia electrónica y promover su compromiso para la cooperación internacional

Para la consecución de estos logros, se encomendó a este equipo de expertos la realización de un trabajo preliminar que ha estado marcado por un doble propósito:

- En primer lugar la realización de una evaluación inicial sobre el estado de la legislación costarricense en materia de ciberdelincuencia, sus políticas de ciberseguridad y ciber-defensa enfocadas a combatir el ciberdelito, e identificación tanto de sus puntos fuertes como de las debilidades que puedan requerir del apoyo del proyecto GLACY+, estableciendo para ello las líneas de actuación a seguir y acordando un plan de trabajo dirigido a cumplir los tres objetivos del Proyecto GLACY + anteriormente mencionados.

- En segundo lugar promover el establecimiento de un equipo nacional de GLACY+ con la función de apoyar al Consejo de Europa en la ejecución del programa, liderado por un coordinador nacional que habrá de actuar como punto de contacto para el desarrollo del plan de trabajo del proyecto.

En atención a ello, la información reflejada en éste informe deberá servir como punto de partida en el desarrollo del Proyecto, fijando los parámetros iniciales que permitirán comprobar los progresos que se obtengan a medida que se van ejecutando las distintas fases del mismo.

1.2 Procedimiento

La elaboración de este informe preliminar, en tanto no se constituya el Equipo Nacional de Coordinación a que se ha hecho referencia, ha sido posible gracias a la valiosa colaboración de un

equipo provisional -principalmente integrado por miembros de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial de la República de Costa Rica (en particular la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General de la República y la Procuraduría de Derecho Informático de la Procuraduría General de la República (PGR) que han facilitado al equipo desplazado del Consejo de Europa los contactos y entrevistas necesarias para poder llevar a cabo el trabajo encomendado, prestando también el apoyo logístico y material necesario para esta primera toma de contacto.

El resultado de la evaluación también es fruto del trabajo de los representantes de las distintas Instituciones que fueron entrevistadas a lo largo de nuestra estancia en Costa Rica. La información que proporcionaron al equipo de expertos y su interés e implicación con el proyecto GLACY+, han resultado decisivos para poder conocer aspectos tan relevantes para los objetivos perseguidos como lo son el estado de la legislación sustantiva y procesal relacionada con el ciberdelito, las reformas legislativas en curso, las Instituciones responsables de la investigación y aplicación de la Ley, los programas de formación específica en investigaciones tecnológicas existentes en las distintas instituciones, la existencia de políticas de ciberseguridad y ciber-defensa, posibles relaciones entre Instituciones públicas y privadas y la situación de los registros estadísticos sobre ciberdelincuencia.

El trabajo efectuado en ésta primera misión, se ha llevado a cabo en los siguientes pasos:

- Tras la designación del equipo de expertos, y antes de nuestro desplazamiento a San José de Costa Rica, hemos realizado una labor de acercamiento a la legislación y políticas en materia de ciberseguridad y ciberdelincuencia vigentes en el País. Para ello se ha analizado la legislación nacional sobre ciberdelincuencia y ciberseguridad – que nos fue proporcionada desde la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI), oficina adscrita a la Fiscalía General de la República de Costa Rica – complementando esta información con la lectura de diversa documentación e información publicada en Internet sobre esta materia, especialmente artículos de prensa sobre el estado de la ciberdelincuencia y ciberseguridad en la República de Costa Rica.

- Entre los días 21 y 24 de mayo de 2018 el equipo del proyecto GLACY+ se desplazó a San José de Costa Rica con la finalidad primordial de intercambiar información con las principales instituciones y organismos involucrados en la lucha contra la ciberdelincuencia de la República de Costa Rica. A lo largo de estos días algunos de nuestros interlocutores también nos proporcionaron documentación que complementaba la información obtenida en el curso de las entrevistas realizadas.

- Esta primera fase concluyó que La Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial es una entidad que aglomera y cuenta con el respaldo de un diverso número de actores clave del sistema de justicia penal que cuenta con la capacidad y atribuciones necesarias para desarrollar una estrategia eficaz de combate al ciberdelito derivada de la Estrategia Nacional de Ciberseguridad de Costa Rica publicada en 2017.[1] Asimismo se identificó a la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General Ministerio Público como la autoridad central encargada para ver asuntos de cooperación internacional relacionados con el combate al ciberdelito y la evidencia digital, por lo que se recomienda que sea la propia OATRI la autoridad central y el punto de contacto oficial bajo el Convenio de Budapest.

1 Disponible en: https://goo.gl/yQCGrF

- La última actividad realizada por el equipo desplazado fue la preparación de una presentación, celebrada en la sede del Colegio de Abogados y Abogadas, a la que asistieron la gran mayoría de los representantes Institucionales entrevistados en los días precedentes realizado con el propósito de presentar las primeras conclusiones y propuestas de actuación futuras en desarrollo del proyecto GLACY+ que serán desarrolladas a mayor detalle en el presente informe.

1.3 Instituciones que han colaborado a la preparación de este informe en Costa Rica

Ha de destacarse la decisiva participación para la elaboración del presente informe de los siguientes organismos e instituciones a través de sus principales responsables:

- Comisión de Seguridad y Ciberdelincuencia del Poder Judicial
- Corte Suprema de Justicia
- Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General
- Procuraduría General de la República (PGR), Procuraduría de Derecho Informático
- Organismo de Investigación Judicial (Sección de Delitos Informáticos - INTERPOL)
- Agencia de Protección de Datos (PRODHAB)
- Instituto Costarricense de Electricidad, CSIRT-ICE
- Dirección de Inteligencia y Seguridad (DIS)
- Ministerio de Ciencia, Tecnología y Telecomunicaciones, CSIRT-CR
- Contraloría General de la República
- Asociación Bancaria Costarricense
- Fundación PANIAMOR
- Sección de Estadística del Poder Judicial
- Claro

1.4 Equipo del Consejo de Europa desplazado a San José de Costa Rica para el desarrollo de la Misión

- Manuel de ALMEIDA PEREIRA, Jefe y Manager del Programa GLACY+,
- Cristos VELASCO SAN MARTÍN, profesor de Derecho, experto legal sobre ciberdelito y protección de datos designado por el Consejo de Europa,
- Francisco NEIRA BASSO, ingeniero de Sistemas, experto en ciberseguridad designado por el Consejo de Europa,
- Adrián ACOSTA, Digital Crime Officer (Oficial de Crimen Digital), de la Dirección de Cibercrimen para las Américas designado por la Interpol.

2. Consideraciones Previas

2.1 Información general sobre el impacto de las tecnologías de Información en Costa Rica

La República de Costa Rica, ubicada en la porción central de Centroamérica, está integrada por 7 provincias con una población que, según la proyección de población elaborado en el año 2014[2] , supera los 4.8 millones de habitantes, de los cuales más de 1.6 millones residen en la provincia de San José. De acuerdo con diversos estudios realizados, en los últimos años, Costa Rica ha experimentado un crecimiento explosivo tanto en lo que se refiere al uso de dispositivos electrónicos, como en lo que se refiere a acceso a Internet. Así, en cuanto a la penetración y acceso a Internet, medido por la cantidad de suscriptores, Costa Rica creció un 440 por ciento entre el 2010 y el 2015. La modalidad de conexión más usada fue la móvil, que registró un aumento de un 688 por ciento en ese período, mientras la banda ancha fija creció un 46 por ciento[3]. "Para el año 2015, los datos muestran que un 39% de las viviendas contaban con conexión fija a Internet y la penetración móvil alcanzó un 101% por lo tanto, es sumamente importante adoptar las medidas necesarias para que el país esté preparado ante posibles ataques y que los usuarios conozcan de los riesgos y acciones que deben tomar para proteger sus datos en el ciberespacio, especialmente porque el país viene haciendo esfuerzos por expandir las redes en todo el territorio y se espera que con el despliegue de las redes que se financian con los recursos del Fondo Nacional de Telecomunicaciones (FONATEL), toda la población cuente con acceso a las tecnologías." (MICITT, 2017)

Cuadro Suscripciones al servicio de transferencia de datos 2011-2015

Indicador	2011	2012	2013	2014	2015
Transferencia de datos					
Suscripciones totales acceso a Internet	2,008,763	3,118,155	4,028,302	4,806,217	5,420,554
Suscripciones totales acceso a Internet fijo-alámbrico	414,384	439,043	474,433	503,347	545,813
Suscripciones totales acceso a Internet fijo-inalámbrico	5,398	8,904	10,450	12,493	12,843
Suscripciones totales acceso a Internet móvil	1,588,981	2,670,208	3,543,419	4,290,377	4,861,898
Suscripciones totales acceso a Internet fijo/100 habitantes	9%	10%	10%	11%	12%
Suscripciones totales acceso a Internet fijo/100 viviendas	32%	34%	36%	37%	39%
Suscripciones totales acceso a Internet móvil /100 habitantes	35%	57%	75%	90%	101%
Suscripciones totales acceso a Internet móvil /suscripciones totales telefonía móvil	38%	50%	50%	61%	65%
Cantidad total conexiones de líneas dedicadas	10,273	11,993	16,375	16,286	14,093

[2] Disponible en: http://www.inec.go.cr/estadísticas

[3] Disponible en: https://goo.gl/wKJjLx

Fuente: Estadísticas del sector de telecomunicaciones 2015. Superintendencia de Telecomunicaciones SUTEL. Disponible en: https://sutel.go.cr/sites/default/files/estadisticas_del_sector_telecomunicaciones_costa_rica_2015.pdf

Por su parte, la Estrategia Nacional de Ciberseguridad de Costa hace referencia al índice Networked Readiness Index (NRI) del Foro Económico Mundial de 2016 en donde Costa Rica ocupó la posición 44 únicamente superado por Chile (38) y Uruguay (43) de los países de América Latina.[4]

Asimismo, el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 "Costa Rica: Una Sociedad Conectada" propone concretizar los proyectos de acceso universal, servicio universal y solidaridad, además de facilitar a nivel comercial y residencial el incremento de la calidad de los servicios de telecomunicaciones que se brindan al Público, incluyendo la ampliación de la oferta de los servicios asequibles e innovadores. El Plan esta articulado en tres grandes pilares: Inclusión Digital, Gobierno Electrónico y Transparente y Economía Digital. La máxima aspiración de ese plan de desarrollo es "Transformar a Costa Rica en una sociedad conectada, a partir de un enfoque exclusivo del acceso, uso y apropiación de las tecnologías de información y las comunicaciones; de forma segura, responsable y productiva."[5]

La ciberseguridad se destaca como un tema fundamental dentro del pilar de Gobierno Electrónico y Transparente del Plan Nacional de Desarrollo de las Telecomunicaciones y en este pilar se busca que el país cuente para el año 2021 con el desarrollo de protocolos de ciberseguridad en los diferentes Ministerios que conforman el Poder Ejecutivo, tal y como se señala en el apartado 3.2.3 de la Estrategia Nacional de Ciberseguridad.

2.2 Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)

El Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) del gobierno de Costa Rica opera dentro del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y fue creado mediante el Decreto Ejecutivo No. 37052 del 9 de marzo de 2012.[6] El CSIRT-CR es una entidad gubernamental oficial encargada de facilitar y coordinar cuestiones relacionadas con seguridad de la información y ciberdelito entre entidades e instituciones gubernamentales e instituciones financieras a nivel nacional e internacionales. El CSIRT-CR está conformado por los titulares de los principales Ministerios y es una unidad encargada de facilitar apoyo y cooperación con las autoridades administrativas y judiciales para la identificación de posibles conductas anti-delictivas cometidas a través del uso de tecnologías de información y amenazas a la estabilidad de la infraestructura critica nacional de Costa Rica.

De la entrevista que sostuvimos con el coordinador general del CSIRT-CR, se nos informó que actualmente cuentan y operan siete personas y que sirve como un catalizador para informar sobre posibles amenazas a los sistemas de información de las instituciones gubernamentales en Costa Rica. Se nos indicó que han coordinado y resuelto diversos asuntos relacionados con ataques sobre denegación de servicios (DDOS) y se encargan de capacitar a su personal para identificar amenazas y darlas conocer a todas las instituciones que forman parte de la Comisión Nacional de Ciberseguridad. Indicaron que también coordinan actividades y tareas dentro del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) e Interpol.

4 Disponible en: https://goo.gl/bA5X6P

5 Disponible en: https://goo.gl/GCssvK

6 El Decreto Ejecutivo No. 37052 se encuentra en: https://goo.gl/qos5oT

Destacaron que el MICITT no cuenta con un presupuesto especialmente asignado al CSIRT-CR para la adquisición de herramientas y tecnologías para la detección y coordinación de respuestas a incidentes cibernéticos lo cual les impide operar como ellos quisieran y que mantienen un estrecho vínculo con entidades como el Instituto Costarricense de Electricidad (ICE) quien los apoya con herramientas e inteligencia para la detección de amenazas a las infraestructuras críticas.

Ahora bien, de las entrevistas sostenidas con los representantes del Instituto Costarricense de Electricidad (ICE) se pudo conocer que igualmente cuentan con un CSIRT que opera desde el 2012, cuya comunidad objetivo son sus usuarios internos y sus clientes. Por otra parte, el CSIRT-CR ha venido operando en forma más recientemente y con muy poco personal a pesar de que su comunidad objetivo es mucho más amplia ya que se trata de un CSIRT nacional.

Derivado de esta situación, se sugiere establecer un convenio de colaboración que permita formalizar la cooperación entre ambos CSIRTs con respecto a los incidentes que ocurran en cualquiera de las comunidades. Esta formalización debería de ocurrir hasta en tanto el CSIRT-CR adquiere mayor experiencia y herramientas y se incrementa el número de personas encargadas de las áreas de identificar incidentes de seguridad.

Durante la reunión se nos informó acerca del ataque a las páginas web del gobierno central y municipalidades de Costa Rica durante el 13 de Mayo de 2018. De acuerdo con los comunicados de prensa del MICITT *"se determinó que de acuerdo con los informes brindados por las entidades especializadas, la afectación es sobre un servidor que aloja varios sitios web estrictamente informativos (no transaccionales) de cuatro gobiernos locales y que toda la evidencia disponible apunta a que no hay ningún otro tipo de afectación sobre otros sitios web del gobierno, sobre la infraestructura de telecomunicaciones o sobre los dominios .cr."* Además se acordó entre otras cosas:

- "Operativizar las oportunidades que brinda la Estrategia Nacional de Ciberseguridad para mejorar las capacidades del Estado en materia de seguridad informática.

- En cuanto al origen del incidente, el OIJ tomara las acciones correspondientes para dicha investigación.

- Ofrecer de manera inmediata el apoyo al Instituto Costarricense de Electricidad (ICE) a los gobiernos afectados por el incidente."[7]

Cabe destacar que recientemente, la Comisión de Seguridad integrada por representantes del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), del Instituto Costarricense de Electricidad (ICE), del Organismo de Investigación Judicial (OIJ), del Ministerio de Seguridad Pública (MSP), de la Dirección de Inteligencia y Seguridad (DIS) del Instituto de Fomento y Asesoría Municipal (IFAM) y de NIC Costa Rica sostuvieron una reunión en la que:

- Se desarrolló la primera versión del Protocolo de Gestión de Incidentes de Ciberseguridad, que se empezará a implementar como un proyecto piloto junto al Ministerio de Seguridad Pública, para luego seguir con los demás Ministerios;

- Se constituyó la primera versión de la Red de Enlaces de Ciberseguridad, un mecanismo que permite contactar directamente a los encargados en materia de ciberseguridad de las

7 MICITT, "MICITT coordina fortalecimiento para gestión de incidentes en ciberseguridad", Comunicado de Prensa CP-031-2018 MICITT, 14 de Mayo de 2018, disponible en: https://goo.gl/4i1TAH

instituciones del Sector Público Costarricense, y que facilitará la coordinación en materia seguridad informática y atención de incidentes o recomendaciones internacionales en la materia; y

- Se implementaron herramientas de monitoreo en el CSIRT-CR, que permiten al MICITT contar con alertas tempranas respecto a potenciales nuevos incidentes de ciberseguridad.[8]

2.3 Políticas y Estrategias sobre Ciberseguridad y Cibercrimen

2.3.1 Política Nacional de Ciberseguridad

La República de Costa Rica, consciente de que las tecnologías de información facilitan el acceso a incalculables recursos y promueven la innovación, la eficiencia, la transparencia, y la prosperidad económica del país, apuesta por una fuerte promoción del uso de las TIC a la vez de fortalecer el marco normativo vigente, en aras de favorecer el desarrollo y uso de los servicios de telecomunicaciones/TIC dentro del marco de la sociedad de la información y el conocimiento y como apoyo a sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno electrónico.

Por otra parte, se desarrolló la Estrategia de Ciberseguridad en forma participativa con sectores vinculados a esta área, y estableció la figura de un Coordinador Nacional, que recayó en el MICITT y debió articular las acciones con los sectores, y un Comité Consultivo que se compuso por representantes del MICITT, del Poder Judicial, de la Superintendencia de Telecomunicaciones (SUTEL), de la sociedad civil, de la academia y del sector privado, para dar seguimiento a la implementación de la labor contra el cibercrimen.

El proceso inició en el 2015 con las mesas de discusión que en marzo y junio realizaron la discusión del texto, con la articulación del MICITT, la Embajada de Canadá, la Embajada Británica, el apoyo técnico especializado de la Organización de los Estados Americanos (OEA) y el trabajo colaborativo a nivel nacional por parte de cámaras empresariales, sector público, sector privado, organizaciones no gubernamentales, la sociedad civil y la academia. Ello permitió dar paso a talleres sectoriales en diciembre, a una consulta en línea en abril del 2016, nuevas mesas de discusión en junio del 2016, una segunda consulta en línea en junio del 2016, para enviar el proceso a revisión de especialistas, y una consulta pública en junio del 2017. (Fuente: gobierno.cr)

Con dicha Estrategia, se estableció un marco de orientación para Costa Rica en materia de seguridad para el uso de las TIC y se identificaron ocho objetivos específicos, alrededor de los cuales se ordenarán las acciones:

- Coordinación Nacional: Se debe designar un Coordinador Nacional, que recaerá en el MICITT, para articular acciones del país, junto con Consejo Consultivo. Esto permitirá implementar acciones, evaluarlas y proponer los ajustes.

- Conciencia pública: Se desarrollarán campañas para concientizar y educar a ciudadanos, funcionarios y empresas en ciberseguridad.

8 MICITT, "Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país", 2 de Julio de 2018, disponible en: https://goo.gl/4Mv4nx

- Desarrollo de capacidad nacional de ciberseguridad: Se implementarán medidas para aumentar la capacitación en estas materias y estimular formación de recurso humano especializado en el tema.

- Fortalecimiento del marco jurídico: Se creará comisión especializada para revisar la normativa de esta materia.

- Protección de infraestructuras críticas: Se deben identificar y clasificar las infraestructuras críticas. Posteriormente, se creará comisión para generar política pública en esta materia.

- Gestión de riesgo: Se debe promover la implementación de un modelo de gestión de riesgo.

- Cooperación internacional: Se debe fomentar la participación en foros y actividades internacionalizadas especializadas.

- Implementación, seguimiento y evaluación: Se requiere diseñar una metodología que permita implementar las acciones, evaluarlas y realizar ajustes. (Fuente: gobierno.cr)

2.4 Adhesión de la República de Costa Rica al Convenio de Budapest

El 19 de febrero de 2017, la Asamblea Legislativa aprobó la adhesión al Convenio sobre Ciberdelincuencia, conocido también como Convenio de Budapest, que pretende proteger a la sociedad de delitos informáticos a través de la adopción de legislación sustantiva y procedimental apropiada.

Posteriormente, el 22 de septiembre de 2017, Costa Rica depositó el instrumento de acceso y ratificación del Convenio de Budapest ante el Consejo de Europa y la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) del Ministerio Público de Costa Rica fue designada como la Autoridad Central para la implementación de este tratado.

De esta forma Costa Rica pasa a ser el miembro nº 55 del Tratado, asumiendo el compromiso de incorporar a su legislación interna las normas de legislación sustantiva y procesal así como las medidas de cooperación internacional previstas en la Convención de Budapest. Un proceso en el que se encuentra inmerso en la actualidad y al que se hará referencia en otro apartado de este informe.

En el instrumento de ratificación, Costa Rica no hizo reserva alguna de las previstas en el propio articulado del Convenio de Budapest. Sin embargo, se hicieron dos Declaraciones que son las siguientes:

- Con respecto al Artículo 10 de la Convención sobre Ciberdelito, la República de Costa Rica interpreta que se entiende que el uso del derecho de autor de obras literarias o artísticas obtenidas a través de un sistema informático no será punible cuando su propósito sea no lucrativo, en la medida requerida con fines de ilustración para la enseñanza, siempre que dicho uso se haga de acuerdo con el uso apropiado, y se haga mención de la fuente y el nombre del autor, si este autor aparece en la fuente. Del mismo modo, la reproducción y el almacenamiento digital de obras literarias o artísticas obtenidas por los estudiantes y el personal académico por medios informáticos con fines meramente ilustrativos y didácticos no serán punibles.

- Con respecto al Artículo 24 del Convenio sobre Delito Cibernético, la República de Costa Rica interpreta que se entiende que no se aplicará a la extradición de nacionales costarricenses que se encuentren en el territorio de Costa Rica.[9]

Recomendaciones

Se constata que Costa Rica cuenta con una Estrategia Nacional de Ciberseguridad (ENC) moderna y avanzada y con objetivos claros y concisos que se encuentran debidamente sustentados en su Plan Nacional de Desarrollo 2014-2018 y el Plan Nacional de Desarrollo de Telecomunicaciones 2015-2021, entre otros documentos oficiales. Además, Costa Rica cuenta con una Comisión Nacional de Seguridad en Línea debidamente conformada desde 2010 integrada por el MICITT y representantes del diversos Ministerios, el Poder Judicial y organizaciones de la sociedad civil que junto con la Comisión de Seguridad y Ciberdelincuencia del Poder Judicial y el Comité Consultivo conformado en el Capítulo Quinto de la ENC, pudieran ser clave en facilitar el desarrollo futuro de una estrategia nacional para combatir el ciberdelito que podría derivarse dentro de los planes de acción de los objetivos previstos en la propia ENC. Se sugiere la adopción de medidas y políticas de acción específicamente destinadas a combatir el cibercrimen en el marco del Proyecto GLACY+.

9 Ver Declaraciones de Costa Rica bajo el Convenio de Budapest en: https://goo.gl/Fop6gx

3. Objetivo 1: Promover la adopción e implementación de legislación, políticas y estrategias efectivas en la lucha contra la ciberdelincuencia

3.1 Marco legal Vigente

3.1.1 Derecho Sustantivo: Tipificación de los delitos informáticos en la legislación vigente

Según se desprende del objetivo 3.4.1. de la ENC relacionado con el Fortalecimiento del marco legal para la atención del delito cibernético, *"A menudo es complejo prevenir un delito cibernético y a veces es aún más difícil identificar al autor. Los delitos cibernéticos pueden ser descritos de dos maneras: los delitos contra un sistema informático (por ejemplo daño o acceso sin autorización a datos, programas o redes) y los delitos facilitados a través de un sistema informático (por ejemplo la publicación de pornografía infantil). En esa línea existen varias leyes en Costa Rica que se ocupan de la delincuencia cibernética directa e indirectamente."* La siguiente figura de la ENC resume los temas que abarcan:

Delitos Cibernéticos en general:	Protección de niñez y adolescencia:	Leyes Procesales:	Otros:
Exposición de datos personales, Fraude electrónico, Phishing, Pharming, Interrupción de Telecomunicaciones, entre otros.	Pornografía infantil, capacitación de menores con fines sexuales, Pseudo-pornografía, Pornografía virtual, posesión de este tipo de material, entre otros	Ley 7,425 sobre Telecomunicaciones, Ley 8754 sobre Delincuencia Organizada, Tratado de Palermo, Tratado de Nassau, Tratado Interamericano de Extradición, entre otros	Código Penal y otras Leyes, Propiedad Intelectual, Aduanas, Impuestos

Fuente: Estrategia Nacional de Ciberseguridad de Costa Rica.

Se pudo constatar, efectivamente que Costa Rica cuenta con una legislación sustantiva amplia para investigar diversos delitos relacionados con el uso de tecnologías de información que la colocan en una posición privilegiada respecto a la mayoría de los países de Latinoamérica que ya han ratificado el Convenio de Budapest y que tipifican como delito la gran mayoría de las conductas previstas en los artículos 2 a 11 del Convenio de Budapest.

Entre la legislación que se pudo revisar se encuentra el Código Penal (Ley No. 4573), el Código de Normas y Procedimientos Tributarios (Ley No. 4755), Ley General de Aduanas, Ley de la Administración Financiera de la República y Presupuestos Públicos (Ley No. 8131), Ley sobre Protección de la niñez y adolescencia frente al contenido nocivo de Internet y otros medios

electrónicos (Ley No. 8934), Obligaciones de Centros de Cómputo y Cafés Internet de cumplir con la Ley No. 8934 sobre la Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos, Ley sobre Delincuencia Organizada (Ley No. 8754), Ley de Protección de la persona frente al tratamiento de sus datos personales (Ley. 8968).[10]

Las conversaciones mantenidas a lo largo de nuestra estancia en Costa Rica con los representantes de los diversos organismos e instituciones vinculados a la lucha contra la ciberdelincuencia en particular con los representantes de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial, nos permite afirmar que, con carácter general, dichas Instituciones perciben la adhesión de Costa Rica a la Convención de Budapest "como *una excelente oportunidad para actualizar y mejorar la normativa tanto sustantiva como procedimental sobre delitos informáticos y sobre todo para poder fomentar y mejorar las capacidades de investigación de las autoridades del sistema de justicia penal encargadas de investigar ciberdelitos a nivel nacional.*

Durante las entrevistas que mantuvimos con representantes de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial se nos informó que dicha Comisión se ha reunido únicamente dos veces desde la publicación de la ENC e indicaron que trataran de reunirse en forma más regular y ser más proactivos en los temas relacionados con ciberseguridad y la lucha contra el ciberdelito durante este año. EL PRESIDENTE DE LA CORTE SUPREMA DE JUSTICIA quien estuvo presente durante la reunión que sostuvimos con los representantes de esa Comisión, dio una breve explicación sobre cómo funciona es Comisión, las instituciones y organizaciones nacionales que la respaldan y la cooperación internacional que actualmente tienen con la Embajada de los EUA, Canadá y la OEA y otros organismos internacionales relacionados con políticas en materia de ciberseguridad. Señaló que pretenden fortalecerla e incluir a otras entidades para que sea un modelo que pueda funcionar a nivel nacional e internacional.

Vale la pena destacar que durante el taller de trabajo donde se presentaron las conclusiones y recomendaciones preliminares, la Titular de la Fiscalía General del Ministerio Público de Costa Rica hizo un atento llamado para que se fortalezcan las actividades y los trabajos de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial y se comprometió a que esa Comisión pueda ser más proactiva, se reúna en forma más regular y se dé continuidad a los trabajos ya encaminados en los temas relacionados con el combate al ciberdelito.

En lo que se refiere a las normas de derecho sustantivo, del examen de la legislación interna, así como de los informes aportados y entrevistas realizadas, podemos concluir que el estado de la legislación vigente en Costa Rica sobre los delitos relacionados en los Artículos 2 a 10 del capítulo II del Convenio de Budapest es el siguiente:

Comenzando por los *delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos,* cuya regulación exige y desarrolla el Título 1 de la Sección 1 del Capítulo II de la Convención de Budapest, Costa Rica no tiene tipificada la conducta de acceso ilícito a sistemas de cómputo dentro de su Código Penal. El Art. 196 del Código Penal castiga el acceso ilícito, copia, modificación, venta y compra de datos personales con el propósito de dañar la esfera privada o la privacidad de un individuo y el procesamiento no autorizado de datos e imágenes de una persona o entidad contenida en sistemas de cómputo e información y servidores, incluyendo la información contenida en bases de datos públicas o cuando la información pertenezca a un menor o cuando la conducta revele datos sensibles de una persona.

---

10 Un resumen de las disposiciones sustantivas analizadas se encuentra en el perfil Wiki de Costa Rica del Consejo de Europa en https://goo.gl/WbM1yS. La legislación completa puede ser consultada directamente en el Sistema Costarricense de Información Jurídica (SCIJ) del Poder Judicial en: http://jurisprudencia.poder-judicial.go.cr/pj/scij/

Por su parte el Art. 94 Código de Normas y Procedimientos Tributarios (Ley. No, 4755) castiga el acceso a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente. por cualquier medio tecnológico.

Los Arts. 221 y 222 de la Ley General de Aduanas (Ley, No. 7557) castiga el acceso ilícito, copiar, destruir, inutilizar, alterar, facilitar, transferir o tener en posesión, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad y facilitar el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos.

La Interceptación Ilícita se encuentra prevista en el Art. 196 y 229 ter del Código Penal (Ley No. 4573)|. Adicionalmente, el Art. 94 del Código de Normas y Procedimientos Tributarios (Ley. No, 4755) castiga la interceptación de sistemas de información o bases de datos de la Administración Tributaria y el Art. 221 de la Ley General de Aduanas (Ley, No. 7557) castiga la interceptación ilícita de sistemas de cómputo utilizados por el Servicio Nacional de Aduanas.

Con respecto a ataques a la integridad de los datos previstos en el Art. 4 del Convenio de Budapest, el Art. 229 bis del Código Penal prevé la figura de 'daño informático' y castiga con prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. La conducta de daño informático también se castiga en otros ordenamientos legales tales como el Art. 95 del Código de Normas y Procedimientos Tributarios (Ley. No, 4755); el Art. 221 de la Ley General de Aduanas (Ley, No. 7557) y el Art. 111 de la Ley de Administración Financiera y Gasto Público (Ley No. 8131).

Ahora bien, con respecto a ataques a la integridad del sistema previstos en el Art. 5 del Convenio de Budapest, el Art. 229 ter del Código Penal prevé la figura de 'sabotaje informático' y castiga con pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático. Esta conducta también se castiga en otros ordenamientos legales tales como el Art. 95 del Código de Normas y Procedimientos Tributarios (Ley. No, 4755); el Art. 221 de la Ley General de Aduanas (Ley, No. 7557); y el Art. 111 la Ley de Administración Financiera y Gasto Público (Ley No. 8131).

En lo que se refiere a 'abuso de los dispositivos" previstos en el Art. 6 del Convenio de Budapest, el Art. 229 ter del Código Penal castiga la instalación de programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. Otros apartados de ese artículo, también castigan la propagación, distribución de programas informáticos maliciosos, invitar a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos; ofrecer, contratar o brindar servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

El Art. 233 castiga con penas de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

El Art. 62 de la Ley de Procedimientos de Observancia de los derechos de Propiedad Intelectual (Ley No. 8039) castiga con penas prisión de uno a cinco años o multa de cinco a quinientos salarios base, quien, de cualquier forma, altere, evada, suprima, modifique o deteriore medidas tecnológicas efectivas de cualquier naturaleza que controlen el acceso a obras, interpretaciones o fonogramas u otra materia objeto de protección y el Art. 62 bis castiga con penas de prisión de uno a cinco años la fabricación, importación, distribución, ofrecimiento o tráfico de dispositivos, productos, componentes o servicios para la evasión de medidas tecnológicas efectivas contra la

comunicación, la reproducción, el acceso, la puesta a disposición del público o la publicación de obras, interpretaciones o ejecuciones o fonogramas.

Ahora bien, con respecto a los delitos informáticos previstos en el Titulo 2 del Convenio de Budapest, "Falsificación Informática' y "Fraude Informático', con relación a la primera conducta, el Art. 217 bis del Código Penal prevé la figura de "Estafa Informática' y se castiga con penas de prisión de tres a seis años y de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Con respecto al "Fraude Informático', dicha conducta se encuentra también tipificada por el propio Art. 217 bis del Código Penal y además el Art. 229 ter del Código Penal hace referencia al sabotaje informático que sanciona a quien impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

Con relación a los delitos relacionados con la pornografía infantil previstos en el Art. 9 del Convenio de Budapest, la legislación de Costa Rica es bastante en amplia y castiga esa y otras conductas relacionadas en diversos ordenamientos legales que a continuación se mencionan:

El Art. 167 del Código Penal castiga la "corrupción de menores" con penas de 4 a 10 años de prisión cuando el infractor utilice redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busque encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.

Por su parte, el Art. 167 bis del Código Penal castiga el "Grooming" con diversas penas a quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona menor de quince años o incapaz; a quien suplante la identidad de un tercero por cualquier medio y cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad incapaz.

El Art. 173 párrafo tercero del Código Penal establece una definición de "Material de Pornografía Infantil" que encuadra completamente con la prevista el numeral 2 del Art. 9 de la Convención de Budapest y dicho precepto castiga con penas de prisión que van de 3 a 8 años a quien fabrique, produzca o reproduzca, por cualquier medio, material pornográfico infantil, así como a quien transporte o ingrese en el país este tipo de material. El Art. 173 bis castiga la tenencia de material pornográfico infantil con penas de prisión de uno a cuatro años.

El Art. 174 del Código Penal castiga la comercialización, difusión, distribución o exhibición de material pornográfico a personas menores de edad o incapaces con pena de prisión de uno a cuatro años; y el segundo párrafo de ese mismo precepto castiga la exhibición, difusión, distribución, financiación o comercialización, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o la posesión para estos fines con penas de cuatro a ocho años.

Por su parte, el Art. 174 bis del Código Penal castiga con penas de prisión de seis meses a dos años la "pornografía virtual' y la 'Pseudo-pornografía' a quien posea, produzca, venda, distribuya, exhiba o facilite, por cualquier medio, material pornográfico en el que no habiendo utilizado personas menores de edad: a) Emplee a una persona adulta que simule ser una persona menor de edad realizando actividades sexuales; b) Emplee imagen, caricatura, dibujo o representación, de

cualquier clase, que aparente o simule a una persona menor de edad realizando actividades sexuales.

Con respecto a los delitos relacionados con infracciones de propiedad intelectual y de los derechos afines contenidos en el Art. 10 del Convenio de Budapest, Costa Rica ha ratificado la gran mayoría de los tratados internacionales relacionados con propiedad intelectual y derechos de autor. Asimismo en el área de derechos de autor, Costa Rica cuenta con la Ley sobre Derechos de Autor y Derechos Conexos (Ley No. 6683) y la Ley de Procedimientos respecto a Derechos de Propiedad Intelectual (Ley No. 8039) que sanciona las conductas previstas en el propio Convenio y establece sanciones administrativas y penales derivadas de su incumplimiento.

Con respecto al Art. 11 del Convenio de Budapest, conforme al cual los Estados han de prever las medidas legislativas y de otro tipo necesarias para tipificar como delito no sólo la complicidad, sino también toda tentativa intencionada de cometer alguno de los delitos previstos en los Arts. 2 a 10 del Convenio, los artículos 46, 47, 48 del Código Penal de Costa Rica cubren y cumplen con esos supuestos cabalmente. Además el Art. 234 del Código Penal prevé la figura de "Facilitación del delito informático" y castiga con penas de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

En lo que concierne a la responsabilidad de las Personas Jurídicas prevista en el Art. 12 del Convenio de Budapest, la legislación de Costa Rica cubre algunos supuestos relacionados con la obligación solidaria de los autores de un hecho punible. El Art. 106 del Código Penal prevé acciones de reparación civil para personas naturales, jurídicas, administradores o personas legales como resultado de la acción de los partícipes de un hecho punible. Asimismo, el Art. 363 del Código Penal establece ;a figura de "Malversación" y se castiga con penas prisión de uno a ocho años a funcionarios público, particulares, gerentes, administradores o apoderados de las personas jurídicas privadas, beneficiarios, subvencionados, donatarios o concesionarios que hagan un mal uso de los fondos a los que están destinados.

3.1.2 Derecho Procesal: Regulación de la Evidencia Electrónica

El vigente Código Procesal Penal de Costa Rica (Ley No. 7594), carece de una regulación específica y detallada de las medidas de investigación tecnológica que son necesarias para el esclarecimiento de los delitos cibernéticos a través del uso de la evidencia electrónica. Los procedimientos de investigación se llevan a cabo en forma general con base en las disposiciones de ese Código Procesal, y cuando se trata de órdenes de registro, secuestro o examen de documentos privados contenidas en sistemas de cómputo o comunicaciones electrónicas para esclarecer asuntos penales sometidos al conocimiento de los tribunales de Justicia, se justifican con base en los dispuesto por el Art. 24 de la Constitución Política de la República de Costa Rica y el Art. 1o. de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425)

Consideramos que la evolución y adaptación de la normativa procesal al fenómeno de la ciberdelincuencia resulta absolutamente imprescindible ya que enfrenta a las autoridades e instituciones encargadas de su persecución y castigo a la necesidad de apoyarse de las herramientas tecnológicas necesarias para poder llevar a cabo una investigación de naturaleza penal y, en consecuencia, averiguar cómo se ha llevado a cabo la actividad delictiva e identificar a sus autores. Es un hecho que muchas de las técnicas de investigación policial tradicionalmente utilizadas para combatir los delitos que se cometen en el mundo físico resultan totalmente ineficaces ante la ciberdelincuencia, pues su investigación no persigue la obtención de huellas físicas sino de evidencias electrónicas.

La obtención de estas evidencias suelen requerir la adopción de medidas que invariablemente afectan a los derechos fundamentales del investigado. De ahí la necesidad de incorporar a la

normativa procesal la regulación de aspectos tan relevantes en las investigaciones tecnológicas como pueden ser el acceso a datos contenidos en dispositivos electrónicos o de almacenamiento masivo, la posible utilización de artificios técnicos para la identificación de terminales, la incorporación de datos almacenados al proceso o la cadena de custodia de las evidencias electrónicas.

En Costa Rica, la Interceptación e intervención de comunicaciones privadas para propósitos de investigación de delitos graves se lleva a cabo conforme al Capítulo II (Arts. 9-20) de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) en donde necesariamente se requiere la orden de un juez para llevar a cabo una intervención, la cual podrá autorizarse por un plazo máximo de tres meses prorrogable hasta dos veces como máximo. La intervención podrá solicitarse para el esclarecimiento de delitos graves previstos en el Art. 16 de Ley sobre Delincuencia Organizada (Ley No. 8754) entre ellos la explotación sexual en todas sus manifestaciones, la fabricación o producción de pornografía, sustracciones bancarias vía temática, terrorismo y su financiamiento, delitos de carácter internacional, entre otros.

Costa Rica cuenta con el Centro Judicial de Intervención de las Comunicaciones (CJIC) organismo dependiente del Poder Judicial que opera los 365 días del año y cuyo sustento se encuentra en el Art. 14 de la Ley sobre Delincuencia Organizada (Ley No. 8754).

Asimismo, conforme al Art. 20 de la Ley No. 7425, las empresas y las instituciones que brindan servicios de comunicación a nivel nacional están obligadas a conceder, a la autoridad judicial- a través de los jueces competentes-, todas las facilidades materiales y técnicas para que las intervenciones sean efectivas, seguras y confidenciales. Vale la pena destacar que conforme al Art. 17 de la Ley sobre Delincuencia Organizada (Ley No. 8754) cualquier empresa, pública o privada, que provea servicios de comunicaciones en el país, estará obligada a realizar lo necesario para la oportuna y eficaz operación del Centro Judicial de Intervención de las Comunicaciones (CJIC) y dichas empresas y los funcionarios de las instituciones públicas y privadas deberán (i) ofrecer todas las facilidades para que las medidas ordenadas por el juez competente se hagan efectivas; (ii) acatar la orden judicial, de manera tal que no se retarde, obstaculice ni se impida la ejecución de la medida ordenada.

Con respecto a la conservación rápida de datos informáticos almacenados prevista en el Art. 16 del Convenio de Budapest, dicha disposición se refiere a la conservación de cualquier tipo de datos, incluidos los relativos al contenido y la medida debería ser adoptada cualquiera que sea la naturaleza o características de la actividad criminal objeto de investigación. Por otro lado, los sujetos que pueden ser obligados por esta orden de conservación pueden ser personas físicas o jurídicas que tengan a su disposición datos informáticos de cualquier tipo que puedan ser útiles para una investigación penal. El supuesto previsto en ese artículo, se trata de una medida de aseguramiento que pretende la salvaguarda de determinadas evidencias electrónicas, en tanto se obtiene la necesaria autorización judicial para la incautación o acceso a dichos datos, razón por la cual la Convención de Budapest contempla un periodo de duración limitado y flexible, no superior a 90 días. Los supuestos de conservación de datos no se encuentran previstos propiamente en el Código Procesal Penal (Ley No. 7594) sino únicamente en la Ley No. 7425 que en su artículo quinto prevé el inventario, custodia y reproducción de documentos por el Tribunal de Justicia y la obtención de copias y reproducciones cuando los documentos secuestrados corran el riesgo de desaparecer, alterarse o sean de difícil custodia.

Consideramos que esta situación deberá ser tomada en cuenta por el Poder Judicial para proponer una reforma al Código Procesal Penal con el objeto de incorporar el alcance del Art. 16 del Convenio de Budapest en un corto plazo.

Ahora bien, con respecto a la conservación y revelación parcial rápidas de datos sobre el tráfico previstas en el Art. 17 del Convenio de Budapest, se trata de una disposición que igualmente

resulta relevante para que las autoridades puedan asegurar la conservación rápida de los datos de tráfico por parte de los proveedores de servicio cuando exista la suposición de que esos datos podrán ser útiles en una investigación. De igual forma, este supuesto no se encuentra regulado expresamente en el Código Procesal Penal (Ley No. 7594) sino únicamente dentro de la Ley No. 7425 y adicionalmente el Art. 199 del Código Procesal Penal prevé supuestos relacionados con la obtención de copias y reproducciones de los objetos secuestrados cuando estos puedan ser susceptibles de desaparecer o alterarse.

En lo que concierne a las medidas sobre orden de presentación previstas en el Art. 18 del Convenio de Budapest, se argumenta que son posibles en aplicación de lo dispuesto en los artículos 1, 2, 3, 5 a 13 y 20 de la Ley No. 7425 y los Arts. 14 y 17 de la Ley sobre Delincuencia Organizada (Ley No. 8754).

Con respecto a las medidas sobre registro y confirmación de datos informáticos almacenados previstas en el Art. 19 del Convenio de Budapest, se argumenta que son posibles en aplicación de lo dispuesto en los artículos 198 y 199 del Código Procesal Penal (Ley No. 7594) donde se regulan con carácter general las medidas de investigación a adoptar por los Fiscales, la conservación y el secuestro de objetos o instrumentos relacionados con el delito, o aquellos objetos que puedan servir como medios de prueba en una investigación. No obstante las peculiaridades de esas disposiciones con las medidas establecidas en el Art. 19 del Convenio de Budapest, consideramos que no encuentran adecuada respuesta en éstos preceptos, obligando a una labor de interpretación de los mismos que en determinados casos puede afectar a la propia validez de la medida adoptada.

Con relación a las medidas de recolección de datos de tráfico en tiempo real prevista en el Art. 20 y la Interceptación de datos de contenido prevista en el Art. 21 del Convenio de Budapest, de igual forma se argumenta que ello es posible conforme a lo dispuesto en los Arts. 198 y 199 del Código Procesal Penal (Ley No. 7594) y la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) que contiene disposiciones para la preservación rápida de información y la entrega de datos de tráfico a través de las comunicaciones que hayan sido intervenidas en el curso de una investigación penal.

Vale la pena destacar que la Comisión de Ciberseguridad y Ciberdelito del Poder Judicial externo su preocupación por la necesidad de actualizar el marco jurídico procedimental penal para regular adecuadamente el uso de la evidencia electrónica para investigaciones penales conforme a las mejores prácticas de los países miembros del Convenio de Budapest. Se nos dio a conocer que el Ministerio Público ya cuenta con un protocolo para la apertura y tratamiento de evidencia digital y que algunos tribunales han hecho interpretaciones y resuelto jurisprudencia en relación al reconocimiento y admisión de la evidencia digital para fines de investigación penal. Asimismo, la Fiscalía no externo su preocupación para el desarrollo e implementación de buenas prácticas para el uso y admisión de evidencia electrónica a nivel interno que pudiera servir como marco comparado de referencia entre las autoridades nacionales del sistema de justicia penal en Costa Rica.

3.3 Normativa sobre Protección de Datos Personales

Es importante señalar, que la ENC de Costa Rica contiene un apartado sobre respeto a los derecho humanos y privacidad que hace un particular énfasis en garantizar y salvaguardar el acceso a las TIC, el acceso a la información y el respecto a la privacidad como derecho humanos fundamentales de los habitantes del país.

La Constitución Política de Costa Rica reconoce en su Art 24. el derecho a la intimidad, a la libertad y al secreto de las comunicaciones como derechos fundamentales. El segundo párrafo del Art. 24 establece que "*son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República sin embargo la ley cuya aprobación y reforma*

requiriera de los votos de dos casos podrán los Tribunales de Justicia ordenar el secuestro registro o examen de los documentos privados cuando sea absolutamente indispensable para esclarecer asunto sometidos a su conocimiento."

Costa Rica cuenta con una legislación bastante amplia y una Autoridad Administrativa- PRODHAB- adscrita al Ministerio de Justicia y Paz. La Agencia de Protección de Datos de los Habitantes (PRODHAB)[11] tiene el principal propósito de garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes, a través del adecuado cumplimiento de la Ley de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales (Ley No. 8968) y su Reglamento No. 37554-JP y el Decreto Ejecutivo No. 40008-JP del 19 de Julio de 2006 que reforma el citado Reglamento.[12] Además, el PRODHAB, tiene como una de sus responsabilidades garantizar el derecho de acceso a la información y la redición de cuentas.

El establecimiento de un marco jurídico eficaz para la protección de datos es considerado internacionalmente como un elemento crucial para generar confianza en las relaciones que se desarrollan en línea y como medidas de salvaguarda para reducir medidas destinadas a combatir el ciberdelito. Actualmente, en Costa Rica, la regulación en materia de protección de datos se efectúa a través de Ley No. 8968 y su Reglamento No. 37554-JP cuyo ámbito de aplicación es principalmente a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de dichos datos.

A través de los responsables del PRODHAB entrevistados pudimos conocer la forma en la que se lleva a cabo un procedimiento cuando se vulnera por ejemplo alguna base de datos que contiene información personal. Las acciones del PRODHAB están principalmente a enfocadas a labores de concientización y educación a la población para dar a conocer los derechos de los ciudadanos bajo Ley No. 8968 y su Reglamento No. 37554-JP ya que señalaron que existe un gran desconocimiento del marco jurídico entre la población.

Los representantes entrevistados, indicaron que actualmente la PRODHAB está llevando a cabo actividades de capacitación a los largo de todo el país precisamente para difundir en forma más amplia el derecho a la protección de datos. Indicaron que las denuncias relacionadas con la violación a los preceptos del marco jurídico sobre protección de datos han aumentado considerablemente el último año.

El área de tecnologías de información de la PRODHAB indico que pretenden integrar la parte de seguridad informática en forma más proactiva ya que anteriormente no contaban con una área específica sobre seguridad de la información y pretenden incorporar metodología novedosa sobre la concepción del proceso de seguridad a través del diseño, así como implementar la figura y el rol del Chief Privacy Officer (CPO) dentro de las instituciones gubernamentales.

Indicaron que ya habían tenido acercamiento con el Consejo de Europa para explorar la posibilidad de adherirse al Convenio para la Protección de las Personas con respecto al tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y su Protocolo Adicional relativo a las

---

11 La PRODHAB fue creada mediante la Ley N° 8968 del 7 de julio del 2011, publicada en el Diario Oficial La Gaceta No. 170 del 5 de septiembre de 2011, portal disponible en: http://prodhab.go.cr Las atribuciones del PRODHAB se encuentran previstas en el Art. 16 de dicha ley.

12 Estos instrumentos se encuentran disponibles en el portal del PRODHAB en: http://prodhab.go.cr//reformas/

Autoridades de Control y los Flujos Transfronterizos de Datos y que están en disposición de colaborar con ese organismos para formalizar la adhesión de Costa Rica a dichos instrumentos.

Asimismo, se nos informó que el Poder Judicial de Costa Rica ha eliminado ciertas categorías de datos de las sentencias judiciales como motivo de la interpretación de la legislación y de algunas sentencias judiciales sobre la materia. La ENC de Costa Rica señala que derivado del aumento de número de casos de pruebas digitales, deberá tenerse en cuenta la interoperabilidad al interior del sistema judicial para pronunciarse sobre estas y de esa forma garantizar su seguridad e integración "para lo cual el Poder Judicial da a conocer la información judicial tomando como referencia lo establecido por la Ley No. 8968 y el documento Reglas Mínimas para la difusión de Información Judicial en Internet (Reglas Heredia) con lo cual implementan las mejores prácticas para encontrar un equilibrio entre privacidad y transparencia al momento de poner datos judiciales a disposición del público."13

3.4 Registros Estadísticos

La identificación y control estadístico de los procedimientos relacionados con la investigación del ciberdelito constituye un factor esencial de cara a conocer cuáles son las tendencias de este fenómeno criminal. El establecimiento por parte de los Estados de sistemas adecuados para el registro, producción y puesta a disposición de los datos sobre cibercrimen, constituye un factor esencial para, a partir de su análisis, combatir de forma más eficaz estos delitos, como se viene afirmando reiteradamente desde distintas Instancias dedicadas a la prevención y lucha contra la ciberdelincuencia.14

Costa Rica, como otros muchos países de la región, no dispone de un sistema de registro integrado que permita cruzar datos entre las distintas instituciones encargadas de investigar el ciberdelito, reflejando de forma global y única la incidencia de la ciberdelincuencia dentro del país.

Durante las entrevistas que sostuvimos con el Organismo de Investigación Judicial se indicó que no cuentan con un sistema estadístico de informes relacionados con ciberdelito y evidencias electrónicas. Sin embargo, se indicó que el Ministerio Público cuenta con un sistema de gestión de estadísticas sobre delitos en general al cual se le asigna un numero único de identificación. Asimismo, derivado de las obligaciones de transparencia previstas en la legislación respectiva, la Fiscalía tiene la obligación de compilar y contar con informes estadísticos relacionados con delitos y procuración de justicia y difundirlos a través de su portal.[15]

Asimismo se nos informó que la Policía Judicial cuenta con un sistema de denuncia anónima que se puede hacer a través de un número telefónico o de la aplicación *whatsapp*.

Por su parte, el Instituto Costarricense de Electricidad (ICE) que es una empresa estatal que brinda servicios de electricidad y telecomunicaciones, incluida la protección de infraestructuras critica de

---

13 Ver ENC, p. 31.

14 Así, por ejemplo. lo recordaba recientemente el informe sobre la lucha contra la ciberdelincuencia (2017/2068(INI)), Propuesta de Resolución del Parlamento Europeo de 26 de Julio de 2017, en su consideración general 4º, disponible en: https://goo.gl/A5UxCK

15 El portal del Poder Judicial de Costa Rica cuenta con una sección de transparencia en donde se pueden consultar informes institucionales y datos abiertos en distintas áreas. De la consulta que pudimos hacer a ese portal, se constata que existen informes sobre el estado de justicia e informes anuales de desarrollo archivístico y datos abiertos en donde se pueden consultar diversas estadísticas tales como 'Ejecución Presupuestaria' y 'Estadísticas Policiales', disponible en: https://goo.gl/aMTfyE

Costa Rica, señalaron que han generado y que cuentan con registros de fraudes en materia de telecomunicaciones y que inclusive cuentan con estadísticas y registros más amplios que la gran mayoría de los operadores comerciales. Asimismo, se nos informó que actualmente se encuentran en un proceso de evaluación de los sistemas de reportes en materia de telecomunicaciones y que cuentan con un sistema de administración del registro de amenazas pero que dichos sistemas y las bitácoras no se encuentran todavía estandarizados. Los entrevistados expresaron su deseo de contar en futuro cercano con un protocolo estandarizado para el registro de bitácoras e informes sobre incidencias delictivas debidamente homologado con el Poder Judicial de Costa Rica.

Asimismo, de las entrevistas sostenidas con la Dirección de Inteligencia y Seguridad (DIS) se nos informó que actualmente se encuentran trabajando en un protocolo de atención a incidentes que están desarrollando en conjunto con el MICIT, Seguridad Pública y el sector Financiero. Se nos informó que el DIS no cuenta con estadísticas relacionadas con ciberdelitos o amenazas relacionadas con la Ciberseguridad

Ahora bien, con respecto a la entrevista sostenida con representantes del CSIRT-CR del Ministerio de Ciencia, Tecnología y Telecomunicaciones indicaron que no cuenta con reportes estadísticos ni herramientas tecnológicas con relación al registro de las amenazas e incidentes sobre ciberseguridad. Uno de los representantes del CSIRT-CR indico que derivado del reciente ataque a las páginas web del Instituto de Fomento y Asesoría Municipal de Costa Rica, indicaron que sería un buen momento para generar las herramientas necesarias para mantener un sistema nacional de reporte estadístico a nivel nacional. Indicaron que el CSIRT-CR pretende generar un análisis de vulnerabilidades de nombres de dominio y crear una hoja de ruta con relación a temas sobre ciberseguridad.

De las entrevistas sostenidas con representantes de la Asociación Bancaria Costarricense que es una asociación que aglomera a los principales bancos e instituciones financieras del país. como son el Banco Central y el Banco Nacional de Costa Rica indicaron que no cuentan con un sistema de control estadístico detallados con relación a delitos que afectan al sistema bancario y financiero de Costa Rica, únicamente cuentan con algunas estadísticas sobre incidentes de ciberdelito y ciberseguridad, las cuales recopilan y procesan por iniciativa propia. Comentaron que normalmente las incidencias y delitos relacionados con el contexto tecnológico tales como phishing y fraudes bancarios se comunican directamente al Órgano de Investigación Judicial del Poder Judicial. Indicaron que tienen gran credibilidad en el Poder Judicial y que no duplican esfuerzos cuando se trata de la investigación sobre ciberdelitos.

Para poder realizar una eficaz gestión de los incidentes, es muy importante contar con los respectivos indicadores y toda vez que es tendencia mundial el ataque a los sistemas de pago del sector financiero como los recientemente acontecidos en Chile y en México, resultará muy conveniente que tanto el CSIRT-CR, el OIJ y el Ministerio Público cuenten con información sobre los incidentes registrados contra el sistema financiero ya sean incidentes o ataques relacionados con la ciberseguridad o ataques en donde se cometan ciberdelitos.

Vale la pena destacar que la regulación del control estadístico en materia de ciberdelito, es percibida por el sector bancario en Costa Rica de forma muy positiva y dicho sector se encuentra en la mejor disposición de poder emitir regulación y decretos para permitir y regular el control estadístico de incidencias sobre ciberdelito y el uso de la evidencia digital en el sector bancario y financiero.

Con relación a la entrevista sostenida con la Dirección de Estadística del Poder Judicial, se pudo constatar que desde 2011 trabajan con dos sistemas de gestión para el control estadístico. El primer sistema está relacionado con el seguimiento de casos y resoluciones judiciales y otro sistema que se utiliza exclusivamente a nivel ministerial y que actualmente se encuentran en proceso de homologar el uso del Expediente Criminal Único Electrónico a través del Órgano de Investigación Judicial por conducto de una Comisión de Estandarización.

La representante comentó que la clasificación de los delitos, se lleva conforme a un catálogo general de delitos prevista en el propio Código Penal, pero que dicho catalogo no contiene la parte relacionada con el contexto tecnológico. Señaló que el sistema de gestión contiene una clasificación de delitos tales como estafa informática, daño y suplantación de información y que se encuentra a nivel de todas las instituciones y despachos encargados de la administración del sistema de justicia penal, tales como el Ministerio Público y los Tribunales Judiciales. Además, indicó que las estadísticas se publican en forma anual y que existe un sistema de estadísticas judiciales en línea conocido como SIGMA16 que permite visualizar el detalle de los casos concluidos, las cargas de trabajo de los despachos judiciales y otras estadísticas en forma trimestral o mensual. Finalmente, la representante indicó que trabajan conforme a la rectoría del sistema de censo del Instituto Nacional de Estadística y Censos de Costa Rica (INEC).[17]

Por último, con respecto a la entrevista sostenida con las empresas de telefonía y comunicaciones móviles CLARO, se nos informó que esa empresa tiene celebrado un Memorando de Entendimiento con el Poder Judicial de Costa Rica para facilitar el intercambio de información entre la Fiscalía y organismos de la autoridad judicial. El representante entrevistado señalo que cuenta con estadísticas particularmente relacionadas a solicitudes de información que solicita Centro Judicial de Intervención de las Comunicaciones (CJIC). Indico que cuentan con algunas estadísticas sobre incidencias delictivas y que cuando se da un incidente en donde se identifica a un usuario de los servicios de telefonía o Internet de esa empresa, normalmente le asignan un número único para darle el seguimiento correspondiente ante el Organismo de Investigación Judicial.

Recomendaciones:

- Consideramos necesario el establecimiento de un sistema adecuado e integrado para el registro, producción y puesta a disposición de datos e información relacionada con ciberdelitos, para conocer las tendencias de la ciberdelincuencia y establecer líneas y rutas de acción para poder hacerles frente. Se recomienda, la realización de gestiones para el establecimiento de un sistema estadístico integrado, que permita obtener un conocimiento lo más exacto posible del alcance de la ciberdelincuencia y de las modalidades delictivas de mayor incidencia en Costa Rica.

- En atención a la especial naturaleza de los delitos informáticos, caracterizados por la ausencia de límites espaciales, de forma que se desarrollen y pueden producir sus efectos de forma simultánea en diversos lugares del territorio nacional o más allá de las fronteras nacionales, se recomienda establecer sistemas que permitan el intercambio y cruce de información entre las Policías encargadas de la investigación permitiendo de esta manera vincular investigaciones que se estén realizando por los distintos cuerpos sobre una misma actividad criminal.

- Se observa que el sistema de registro del Organismo de Investigación Judicial, por su funcionamiento, puede ser de máximo interés para la implementación de nuevas políticas sobre registros estadísticos. De tal forma, que podría ser utilizado como base, mediante la introducción de los cambios que se estimen precisos para la obtención de datos estadísticos sobre cibercriminalidad.

- En el establecimiento del nuevo sistema de registro estadístico, habrá de tomarse en consideración el carácter transversal de los ciberdelitos, que se manifiesta a través de comportamientos ilícitos de muy diversa naturaleza, con encaje en diferentes tipos y

16 El portal de los informes estadísticos SIGMA se encuentra en: https://goo.gl/MVvMLi

17 Portal disponible en: http://www.inec.go.cr/

conductas penales. Esta circunstancia puede dar lugar a que su carácter cibernético quede oculto si se registra tan solo por el delito genérico de que se trate. Para ello, será preciso que en los sistemas y aplicaciones de registro se prevea la posibilidad de dejar constancia, con la debida precisión del carácter informático de la infracción.

- Asimismo, se recomienda explorar la creación de una regulación en el sector financiero y bancario que permita el uso de sistemas de control estadístico sobre ciberdelitos y evidencia electrónica que afectan al sistema bancario y financiero y que permitan ser compartidos con las autoridades del sistema de justicia penal, a través de un sistema homologado que opere con el sistema de registro del Organismo de Investigación Judicial y el de la Fiscalía General.

- Por otro lado, se recomienda darle continuidad a los trabajos encaminados por la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial y que esa Comisión se reúna en forma más periódica para analizar y discutir las problemáticas y políticas más recientes en materia de ciberdelincuencia y que a través de todas las instituciones que formen parte de esa Comisión, se elabore una estrategia específica para el combate al ciberdelito y el uso y manejo de la evidencia electrónica con líneas de acción y objetivos estratégicos en el mediano y largo plazo.

3.5 Cooperación entre el Sector Público y Sector Privado

La cooperación entre las autoridades del sistema de justicia penal y las entidades del sector privado se concibe como un elemento esencial para proteger a la sociedad contra el delito cibernético. De hecho, la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia constituye uno de los principios inspiradores de la Convención de Budapest, en cuyo seno se está trabajando para mejorar la cooperación pública/privada en materia de ciberdelincuencia y evidencia electrónica fortaleciendo las modalidades actuales de cooperación con el sector privado en investigaciones relacionadas con cibercrimen y el uso de evidencia electrónica por parte de las autoridades judiciales.

De esta forma, el establecimiento de plataformas de comunicación público-privada en las que se permita intercambiar información y experiencias se convierte en un factor clave para simplificar la asistencia mutua y establecer un entorno más seguro en lo que al acceso a la información se refiere.

Sin embargo, según se desprenden de las conversaciones mantenidas con las autoridades judiciales y policiales encargadas de las investigaciones criminales, actualmente uno de los principales obstáculos para que tales investigaciones criminales lleguen a buen término radica precisamente en las dificultades que existen para el acceso a los datos en poder del sector privado. Aun y cuando existe la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) que contiene obligaciones de cooperación de las empresas de telecomunicaciones con las autoridades judiciales, a través del Centro Judicial de Intervención de las Comunicaciones (CJIC), la cooperación es percibida aun como un tema muy incipiente y poco dinámico debido a diferentes motivos o razones. Primero, puesto que la legislación actual no aclara los límites y el alcance de cooperación para el acceso a datos o información que tengan empresas de telefonía, cable o servicios de Internet así como cuestiones de preservación y almacenamiento de datos. Segunda, aun y cuando existen más de 100 operadores nacionales de telefonía, muchos de ellos aún no cuentan con la infraestructura de seguridad y los mecanismos de cooperación con las autoridades del sistema de justicia penal. Por ejemplo, el coordinador de seguridad del Instituto Costarricense de Electricidad indico que generalmente almacenan los datos de los abonados por un periodo de tres años derivados de un Reglamento pero que los datos de conexión no se almacenan e indico que la cooperación con

Proveedores de Servicios de Internet ha sido mucho más lenta y que las reglas para la identificación y almacenamiento de direcciones IP no son completamente claras.

Por su parte el representante del CSIRT-CR del Ministerio de Telecomunicaciones señaló que se han celebrado convenios específicos con ISP's para fomentar y promover la cooperación en forma más amplia y que se encuentran actualmente en pláticas con vistas a celebrar un convenio para la protección de infraestructuras críticas.

Por otro lado, tal y como se indicó en párrafos anteriores, el sector privado tiene celebrado un memorando de entendimiento con el Poder Judicial para facilitar el intercambio de información que pueda ser útil en la investigación de delitos relacionados con el uso de tecnologías de información y adicionalmente los tres operadores principales de servicios de telefonía móvil cuentan con un protocolo general de actuación para facilitar entre ellos el intercambio de información y datos de sus abonados.

Una gran parte del problema se debe a la falta de una legislación procesal que defina correctamente cuales son las facultades que asisten a las autoridades judiciales y policiales para efectuar estas solicitudes en el marco de una investigación criminal y establezca específicamente sus limitaciones. Por ello, la existencia de una normativa moderna y eficaz, se convierte en un factor esencial que debe contribuir a obtener con mayor agilidad y eficacia el resultado de la investigación y que además proporcione a las entidades solicitadas, las salvaguardas necesarias frente a cualquier interferencia arbitraria en la privacidad de las personas a través del tratamiento y destino de sus datos e información.

Cabe destacar que los Arts. 1, 2, 3 y 5 a 13 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) establece los procedimientos, plazos, condiciones y forma para preservar evidencia o pruebas que puedan estar contenidas en documentos privados, tales como mensajes de datos. Asimismo, conforme al Art. 20 de dicha ley, las empresas y las instituciones que brindan los servicios de comunicación están obligadas a conceder, a la autoridad judicial, todas las facilidades materiales y técnicas para que las intervenciones sean efectivas, seguras y confidenciales. El Art. 23 de la Ley No. 7425 establece la obligación de los funcionarios responsables de las empresas o instituciones públicas y privadas a cargo de las comunicaciones de: (i) brindar todas las facilidades para que las medidas ordenadas por el Juez competente se hagan efectivas; (ii) acatar la orden judicial, de tal manera que no se retarde, se obstaculice o se impida la ejecución de la medida ordenada.

Durante el desarrollo de este primer módulo del Proyecto GLACY+ hemos tenido la oportunidad de entrevistar a distintas entidades del sector público y privado y la información que nos ha sido proporcionada refleja que, salvo excepciones muy puntuales, no se han establecido espacios de encuentro destinados a fomentar la cooperación del sector público-privado, aun así, desde ambos sectores se manifestó su disposición e interés por establecer vías de comunicación expeditas y ágiles que contribuyan al éxito en la lucha contra la ciberdelincuencia en Costa Rica.

Recomendaciones

Promover la creación de un reforma al marco jurídico nacional existente para permitir solicitudes de información en forma directa tanto a los proveedores de servicio de Internet como a los operadores del servicio de telefonía móvil, a través de los canales que tienen establecidos con las empresas del sector privado para que acompañados de la debida orden judicial, las entidades del sistema de justicia penal puedan requerir información rápida y oportuna, y de esta forma se puedan optimizar las investigaciones penales.

4. Objetivo 2: Fortalecer la capacidad de las autoridades policiales en la investigación del ciberdelito y promover una cooperación inter-policial efectiva a nivel interno así como a nivel internacional con las unidades de cibercrimen de Europa y otras regiones

4.1 Fuerzas de Orden y Seguridad Pública del Estado

El Art. 12 de la Constitución Política del Estado Costa Rica dispone que ese país no cuenta con un Ejército y por tanto Costa Rica esta proclamado como un estado neutro, sin un Ejército o fuerza armada como institución permanente en ese país. Dicho artículo señala textualmente que: *"Se proscribe el Ejercito como institución permanente. Para la vigilancia y conservación del orden público, habrá las fuerzas de policía necesarias. Solo por convenio continental o para la defensa nacional podrán organizarse fuerzas militares; unas y otras estarán siempre subordinadas al poder civil; no podrán deliberar, ni hacer manifestaciones o declaraciones en forma individual o colectiva"*

La autoridad competente para investigar delitos dentro del territorio de Costa Rica es el Ministerio Público, a través de sus Fiscales con el apoyo de la Policía Judicial. Las atribuciones y obligaciones del Ministerio Público están contenidas en la Ley Orgánica del Ministerio Público (Ley No.7442 de 25 de octubre de 1994)[18] y en los artículos 62 a 66 del Código de Procedimientos Penales (Ley N ° 7594 del 10 de abril de 1996). El Ministerio Público goza de una completa independencia funcional en el ejercicio de sus facultades y atribuciones legales.

Las atribuciones y obligaciones de la Policía Judicial, que funciona bajo la dirección y control del Ministerio Público están contenidas en la Ley Orgánica del Organismo de Investigación Judicial núm. 5524 del 7 de mayo de 1974 y en los artículos del 67 al 69 del Código de Procedimientos Penales (Ley N ° 7594 del 10 de abril de 1996). La policía judicial está encargada de investigar los delitos de acción pública, impedir que se consuman o agoten, y entre otras de sus actividades se encuentra, el individualizar a los autores y partícipes, reunir los elementos de prueba útiles para fundamentar la acusación y ejercer las funciones asignadas en su ley orgánica y el Código de Procedimientos Penales, respectivamente.

El equipo de expertos ha tenido la oportunidad de reunirse con autoridades del Organismo de Investigación Judicial (OIJ), obteniendo información sobre su estructura interna, funcionamiento, los principales problemas que se les plantean en el curso de las investigaciones tecnológicas que desarrollan y sus expectativas respecto del Proyecto GLACY+.

4.2 Cuerpos Especializados: Desarrollo de su Actividad

4.2.1 Organismo de Investigación Judicial (OIJ)

Como se indicó en párrafos anteriores, las facultades y atribuciones del Organismo de Investigación Judicial (OIJ) se encuentran previstas en la Ley Orgánica del Organismo de Investigación Judicial núm. 5524 del 7 de mayo de 1974 y en los artículos del 67 al 69 del Código

18 Disponible en: https://goo.gl/UX5ALc

de Procedimientos Penales (Ley N° 7594 del 10 de abril de 1996). EL OIJ es un organismo dependiente de la Corte Suprema de Justicia. Además este cuerpo policial tiene atribuida la representación de Costa Rica como miembro de la Organización Internacional de Policía Criminal (INTERPOL).

EL OIJ cuenta con un Departamento de Investigaciones Criminales con diferentes subdivisiones, entre ellas con una División de Delitos Informáticos y otra de Delitos Económicos y Financieros; así como un Departamento de Medicina Legal y un Departamento de Laboratorio de Ciencias Forenses. Además, los Arts. 11 y 19 de la Ley no. 5524 establece un Comité Asesor integrado por el Director General, el Subdirector, el Secretario General y los Jefes Departamentales con diversas atribuciones previstas en su Art. 21.

La investigación policial de los delitos está atribuida esencialmente a la Policía Judicial del OIJ que conforme al Art. 3º de la Ley no. 5524 tiene la obligación de investigar delitos de acción pública por denuncia o por vía de una autoridad judicial, impedir que los hechos sean llevados a consecuencias ulteriores, identificar y aprehender preventivamente a los posibles culpables y reunir, asegurar y ordenar científicamente las pruebas y demás antecedentes necesarios para la investigación. El inicio de las investigaciones realizadas por el Departamento de Investigaciones Criminales de la Policía Judicial puede venir determinado por la presentación de una denuncia por la víctima del delito o por un requerimiento del Fiscal o recepción de una *notitia criminis* o requerimiento internacional recibido por el sistema INTERPOL.

De la información que nos fue proporcionada durante la entrevista, en lo que concierne a las investigaciones tecnológicas, se nos informó que el OIJ cuenta con la Sección Delitos Informáticos desde el año 1997 siendo una de las unidades con más años de la región, la cual tiene 33 profesionales que manejan tres diferentes tipos de macro procesos encargándose del respaldo y pericia de evidencias digitales de dispositivos móviles y otros medios de almacenamiento de pruebas y evidencias contenidas en formato electrónico y que recientemente cuentan con una pequeña área de investigación en desarrollo, que antes de esta área de investigación solo hacían soporte a investigaciones. Asimismo, se nos explicó la forma en que realizan sus investigaciones y como las arman e integran ante el Ministerio Público. Se indicó que no existe aún la posibilidad de interponer denuncias vía online o a través de una aplicación móvil. La denuncia debe ser interpuesta directamente por la víctima en cualquiera de las oficinas de la Policía Judicial o ante un fiscal si se conoce al autor del crimen. Se nos informó que cuentan con un sistema de denuncia anónima, a través de un número telefónico y un número vinculado con una cuenta de la aplicación Whatsapp. De igual forma, indicaron que la Policía Judicial no hace uso de herramientas en fuente abierta para la investigación de ciberdelitos.

Las investigaciones sobre ciberdelitos que realizan en su mayor parte están relacionadas con delitos contra las personas y en menor proporción, delitos contra la propiedad de empresas privadas. Entre los delitos contra las personas, su labor se suele centrar en los supuestos donde se ven afectados adolescentes y menores de edad, tales como delitos de abuso sexual e imágenes de abuso sexual infantil, suplantación de identidad; fraudes y estafas informáticas. Indicaron que para delitos tales como phishing y pharming, no cuentan con la capacidad de investigarlos principalmente por la escasa falta de recursos humanos.

Con respecto al tema de formación y capacitación, indicaron que algunos de sus funcionarios ya han recibido capacitaciones en materia de ciberseguridad y ciberdelitos y evidencia digital por parte de organismos internacionales tales como la OEA, INTERPOL y del Gobierno de los Estados Unidos y Canadá. Si bien tienen una variada cantidad de herramientas para el análisis forense, se ha notado falta de capacitación formal en el uso de la mismas como Encase, FTK, y UFED de *Cellebrite.*

Asimismo, han puesto de relieve la necesidad de capacitación en Análisis de Malware, Investigación en *DarkWeb* y Cryptomonedas.

Cabe mencionar que el presupuesto anual asignado por la Policía Judicial a esta área muy bajo y gran parte de los recursos se destinan a cubrir la actualización de licencias de software y de sistemas de cómputo entre otros gastos, situación que les impide crecer y operar transversalmente, y sobre todo contar con personal calificado para el área de investigación sobre Delitos Informáticos. Además, indicaron que tienen cierta demora y retraso en resolver asuntos donde se encuentra involucrado el uso y manejo de pruebas y evidencias electrónicas para armar y justificar investigaciones penales en curso. En cualquier caso, la atribución de una determinada investigación por parte de la Policía Judicial va a depender en gran medida del Ministerio Público o Fiscal quien decide si la investigación es procedente conforme a legislación penal sustantiva y las garantías procesales previstas en la Constitución y en la legislación procedimental penal.

En lo que concierne al desarrollo material de las investigaciones especializadas, la ausencia de regulación específica respecto de las evidencias digitales y su tratamiento, se convierte en una fuente de problemas, pues se plantean muchas dudas en cuanto a su tratamiento que requieren de urgente solución aún y cuando este país cuenta con la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) vigente desde el año 1993. Indicaron que no disponen de un protocolo específico para el uso y manejo de evidencia electrónica, sino que utilizan el protocolo de cadena de custodia de carácter genérico para cualquier tipo de delitos, lo cual implica pérdidas importantes de tiempo y recursos humanos.

En el desarrollo de las investigaciones que afectan a delitos tecnológicos se encuentran con diversos obstáculos, el principal derivado de la falta de un relación fluida y dinámica con los Proveedores de Servicio de Internet y los Operadores del Servicio de Telefonía Móvil.

No obstante, tras la firma de la Convención de Budapest, la Comisión de Seguridad y Ciberdelincuencia del Poder Judicial les ha informado y dado instrucciones generales de que cualquier petición de información informática se habrá de canalizar a través de la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General, lo que a su entender podrá acortar el tiempo de respuesta de los proveedores de servicios y operadores del servicio de telefonía móvil.

En el caso de investigaciones que requieran solicitar información a empresas en el exterior como por ejemplo Facebook, Google, Microsoft, se hace a través del Departamento de Justicia de los Estados Unidos y eso provoca no tener la información en forma oportuna, y en algunos casos, en forma extemporánea para continuar con una determinada investigación. Asimismo han manifestado que en algunos casos la información les ha llegado años después. Cabe aclarar que a pesar de que existen canales de comunicación que permiten solicitar la información directamente a las empresas proveedoras de servicio, lo cual permitiría agilizar la obtención de la información, en algunas ocasiones no se considera como información útil legalmente.

4.2.2 Oficina de INTERPOL en San José

La Organización Internacional de Policía Criminal (INTERPOL) cuenta con una Oficina Central Nacional que está ubicada físicamente en la Dirección del OIJ en la ciudad de San José. De acuerdo con información extraída de la página de INTERPOL[19], esa oficina cuenta con una jefatura, doce investigadores y seis administrativos y sus prioridades son: Delincuencia organizada; drogas; delincuencia financiera y de alta tecnología; prófugos o fugitivos; seguridad pública y terrorismo; corrupción; trata de personas; y delitos contra el medio ambiente.

19 Portal disponible en: https://goo.gl/oQEsft

Los funcionarios de la OCN pueden ejecutar, entre otras, las siguientes funciones:

- Proceder a la aprehensión de los presuntos culpables;
- Disponer la incomunicación, por resolución escrita, de los presuntos culpables, para evitar que puedan ponerse de acuerdo con terceras personas que entorpezcan la investigación;
- Recibir declaración del imputado en la forma y con las garantías que establece la ley;
- Proceder a interrogar a todas las personas que pudieran aportar datos de interés a la investigación, practicando los reconocimientos, reconstrucciones, inspecciones y confrontaciones convenientes;
- Efectuar todos los exámenes, indagaciones y pesquisas que juzguen oportunas para la buena marcha de las investigaciones;
- Proceder a los registros, allanamientos y requisas que fueren necesarias para la buena marcha de las investigaciones, con las formalidades que prescribe el Código Procesal;
- Solicitar la colaboración de otras autoridades, las que no podrán negarla.

Tal y como se indica en portal de INTERPOL, "Como parte de una estrategia para reforzar la seguridad nacional y prevenir las actividades delictivas en Costa Rica, INTERPOL San José conectó el OIJ a las bases de datos de INTERPOL. Esto significa que cada miembro del OIJ tiene acceso directo, en cuestión de segundos, a datos esenciales sobre personas buscadas, vehículos robados y documentos de viaje perdidos o robados."

Durante las reuniones sostenidas, estuvieron presentes representantes de la Oficina de Interpol en San José y se pudo constatar que efectivamente han tenido acceso directo a las bases de datos de INTERPOL, sin embargo uno de los entrevistados indicó que el OIJ todavía no cuenta con personal oficialmente asignado para el uso de la base de datos Internacional de Explotación Sexual Infantil de INTERPOL (ICSE), por lo cual no se está trabajando directamente sobre las imágenes para la identificación de víctimas de abuso sexual infantil.

4.2.3 Ministerio Público

El Ministerio Público dirige las investigaciones criminales y ejercita la acción penal conforme a lo dispuesto en los Arts. 62 a 66 del Código de Procedimientos Penales (Ley N ° 7594 del 10 de abril de 1996) y su Ley Orgánica (Ley No.7442 de 25 de octubre de 1994).

Los ciberdelitos y en general todos aquellos delitos que conlleven el uso de tecnologías de información, se dirigen desde la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI)[20] que es una Oficina adscrita la Fiscalía General de la República que actúa por delegación del Fiscal General como órgano encargado de los trámites de extradición y cooperación penal internacional del Ministerio Público a nivel nacional e internacional.

Vale la pena destacar que la OATRI ha sido designada como el punto de contacto y autoridad central ante el Consejo de Europa conforme al Art. 35 del Convenio de Budapest para garantizar la

20 Portal disponible en: https://goo.gl/egrwqJ

asistencia inmediata para investigaciones o procedimientos relacionados con ciberdelitos y evidencias electrónicas.[21]

El Ministerio Público también realiza funciones de cooperación internacional, por ejemplo el Art. 65 del Código de Procedimientos Penales (Ley N ° 7594 del 10 de abril de 1996) establece que "*Cuando las actividades delictivas se realicen, en todo o en parte, fuera del territorio nacional, o se les atribuyan a personas ligadas a una organización de carácter regional o internacional, en los casos en que deba aplicarse la legislación penal costarricense, el Ministerio Público podrá formar equipos conjuntos de investigación con instituciones extranjeras o internacionales. Los acuerdos de investigación conjunta deberán ser aprobados y supervisados por el Fiscal General.*"

Se pudo constatar que existe la Procuraduría General de la República (PGR)22 que cuenta con una división sobre Derecho Informático, sin embargo ese órgano tiene una función meramente consultiva en el ámbito técnico-jurídico dentro de la Administración Pública y es el representante legal del Estado en materias propias de su competencia. Dentro de la Procuraduría sobre Derecho Informático actualmente labora Francisco Ruiz Salas con quien establecimos contacto previo a nuestro desplazamiento a la ciudad de San José y quien fue una persona clave en la adhesión de Costa Rica al Convenio de Budapest y quien nos ha facilitado información y los contactos necesarios que ha sido de gran utilidad para la elaboración de este reporte.

Recomendaciones:

- En las investigaciones tecnológicas desarrolladas policialmente se aprecian obstáculos de carácter material determinados por la falta de herramientas tecnológicas y del software necesario. Se recomienda efectuar las previsiones necesarias para dotar a la Sección de Delitos Informáticos del OIJ de las herramientas necesarias para afrontar debidamente las investigaciones tecnológicas estableciendo sistemas que aseguren la actualización de las licencias y certificaciones que sean precisas a tal fin.

- Se observa que el ciudadano no tiene posibilidad de denunciar vía online ante los cuerpos policiales. La experiencia demuestra que la presentación de denuncias online en el caso de los delitos cibernéticos presenta indudables ventajas para la ciudadanía por el rápido y fácil acceso a la denuncia, como también para garantizar la salvaguarda de las evidencias y para obtener un acercamiento estadístico más exacto de los delitos cibernéticos que ocurren en el país. Se sugiere llevar a cabo las gestiones oportunas para el establecimiento de un portal específico en la página web del Organismo de Investigación Judicial, destinado a la recepción vía electrónica de denuncias sin perjuicio de su posterior ratificación en sede policial o ante el Ministerio Público.

- Dotar de mayores recursos a la Policía Judicial para que puedan contar con personal debidamente capacitado que pueda coadyuvar en el uso y manejo del equipo y software necesario para la obtención, preservación y presentación de evidencias digitales ante el Ministerio Público, así como para establecer un sistema de reporte y estadístico sobre ciberdelitos que pueda abarcar las distintas fases de investigación, conclusión y sentencia judicial de los mismos.

- Se recomienda realizar las gestiones necesarias para la rápida integración oficial de la OIJ para el acceso y uso de la base de datos ICSE de INTERPOL a la Sección de Delitos Informáticos como también a la Sección de Delitos contra la Integridad Física a efectos de

21 Ver portal del Consejo de Europa en: https://goo.gl/uydqL8

22 El portal de la PGR se encuentra en: https://www.pgr.go.cr/

poder trabajar más eficientemente en la identificación de víctimas de abuso sexual infantil, y por consiguiente preparar un equipo de psicólogos que asistan periódicamente a los investigadores que trabajan con la base de datos ICSE y otro equipo para asistir a las victimas rescatadas desde el primer momento en que se toma contacto con la misma.

- Se recomienda establecer un sistema de reporte y estadístico sobre ciberdelitos que pueda abarcar las distintas fases de investigación, conclusión y sentencia judicial de los mismos, así como también incidentes informáticos, por lo cual se sugiere que el mismo sea alimentado de información por el OIJ, el MICITT, el CSIRT-CR, y cualquier otro organismo de aplicación de la Ley que tenga información de ciberdelitos.

- Se observó que recientemente se ha creado el área de investigación dentro de la Sección Delitos Informáticos de la OIJ, lo cual permitirá realizar investigaciones más complejas y especificas en el área de ciberdelitos, por lo cual se recomienda que dentro de la Sección de Delitos Informáticos de la OIJ, se mantenga una adecuada independencia entre los investigadores y los especialistas forenses, con el objetivo de obtener la debida objetividad de los análisis forenses y la confidencialidad de las investigaciones.

4.3 Capacitación de Cuerpos Policiales

El fenómeno de la ciberdelincuencia obliga a las Fuerzas de Orden y Seguridad Pública a abordar estas investigaciones con un nuevo enfoque. La obtención de la evidencia electrónica y su tratamiento se convierte en un factor esencial en esta clase de investigaciones y exige una formación específica que evite la pérdida de la evidencia o, en su caso, provoque su invalidez por un mal manejo o tratamiento de la misma. Además, los agentes encargados de la investigación tecnológica se ven precisados del apoyo de expertos en criminalística formados para el análisis correcto de las evidencias electrónicas. Por otro lado, el carácter transnacional de la ciberdelincuencia, es un factor que necesariamente ha de ser tomado en consideración en la planificación de las actividades formativas destinadas a los policías que desarrollan las investigaciones tecnológicas.

4.3.1 Organismo de Investigación Judicial (OIJ)

La preocupación por la formación, tanto inicial como continua, es uno de los aspectos sobre el que más insistieron los responsables del OIJ en el transcurso de nuestra entrevista. De hecho, una de sus principales expectativas respecto del proyecto GLACY+, es la obtención de una mayor capacitación para la investigación de la ciberdelincuencia, así como la creación de nuevos espacios de intercambio de información y experiencias con otros cuerpos policiales a nivel regional.

Hasta donde se tuvo conocimiento, la Policía Judicial del OIJ no cuenta con una escuela de formación propia para sus oficiales, esto es compartido con la Escuela Judicial. Sin embargo como se indicó en la sección 4.2.1 algunos de sus funcionarios han recibido capacitaciones en materia de ciberseguridad y ciberdelitos y evidencia digital por parte de organismos internacionales tales como la OEA, INTERPOL y del Gobierno de los Estados Unidos y Canadá.

Actualmente se cuenta con un curso básico para investigadores sobre delitos informáticos e incautación de evidencia digital, pero solo se imparte una o dos veces al año en grupos de 20 o 25 personas.

Consideramos de gran importancia que la OIJ comience las gestiones necesarias para crear una unidad de formación especializada dedicada a la capacitación permanente en materia de ciberdelito y evidencia digital para formar y capacitar exclusivamente a las unidades operativas de la Policía Judicial a lo largo de todo el país, lo anterior con el propósito de que la legislación actual y el Convenio de Budapest puedan ser implementados en forma más dinámica y conforme a las pautas

y programas de formación en los que se encuentra trabajando el Consejo de Europa, a través del Proyecto GLACY+.

Según expresaron los representantes entrevistados del OIJ, una de las deficiencias que han detectado en éste área, se refiere precisamente a una formación básica para los agentes que reciben las denuncias, según han podido comprobar la relación entre la víctima y el policía que recibe la denuncia es fundamental para el manejo de la evidencia evitando que la misma pueda perderse o alterarse.

Recomendaciones

- Se detectan carencias en la capacitación de los policías a cargo de las investigaciones de delitos informáticos. Ciertamente, aún y cuando algunos policías dentro del OIL cuentan con conocimientos y formación básica en materia de ciberdelito y evidencia digital obtenida de la formación ofrecida por otros organismos internacionales, esa formación, a juicio de los propios cuerpos policiales involucrados en la lucha contra el cibercrimen, resulta insuficiente para afrontar con éxito las investigaciones tecnológicas.

- En relación con esta necesidad se recuerda que la especial naturaleza de estos delitos exige que, además de proporcionar una capacitación técnica avanzada a aquellos policías que desarrollen sus funciones en las unidades especializadas de cibercrimen, se realicen también actividades de capacitación básica dirigidas a policías destinados en otras unidades. Lo anterior con la finalidad de establecer mejores prácticas en el tratamiento de la víctima - preguntas que han de hacerse y recomendaciones para evitar la pérdida de la evidencia - así como, en su caso, en la recolección, manejo y tratamiento de las evidencias electrónicas que se aporten con la denuncia.

- En consecuencia, se recomienda la previsión e impartición de programas de formación en materia tecnológica dirigido a las Fuerzas del Orden y Seguridad del Estado. Para el adecuado tratamiento y aseguramiento de la cadena de custodia de la evidencia electrónica, se sugiere que la formación especializada se proporcione a dos niveles:

  a) Un nivel básico, dirigido a los agentes de policía que sin estar destinados en las unidades especializadas, se encargan de la recepción de denuncias. En este nivel formativo, el objetivo a cubrir será proporcionar la capacitación necesaria para la correcta elaboración de los atestados o constancias por delitos de esta naturaleza: determinación de los elementos concurrentes en los hechos denunciados que necesariamente deberán quedar reflejados en el atestado y el manejo y tratamiento de la evidencia electrónica que pueda ser aportada por el denunciante en estas primeras fases de la investigación, garantizando su integridad y posterior validez ante los Tribunales de Justicia.

  b) Un nivel avanzado, para los grupos especializados en investigaciones cibernéticas, actualizando periódicamente sus conocimientos y fomentando el intercambio de experiencias con otros cuerpos policiales y unidades de investigaciones nacionales e internacionales.

5. OBJETIVO 3: Facilitar a las autoridades del sistema de justicia penal la aplicación de la legislación y la persecución y atribución de la competencia en los asuntos de ciberdelincuencia y evidencia electrónica y promover su compromiso para la cooperación internacional

5.1 Autoridades del Sistema Judicial Penal con responsabilidades en la investigación del Cibercrimen y en la aplicación de la Ley

5.1.1 Ministerio Público

Tal y como se indica en la sección 4.2.3, el Ministerio Público de Costa Rica dirige las investigaciones criminales y ejercita la acción penal conforme a lo dispuesto en la Constitución Política, los Arts. 62 a 66 del Código de Procedimientos Penales (Ley N ° 7594 del 10 de abril de 1996) y su Ley Orgánica (Ley No.7442 de 25 de octubre de 1994).

El área de cibercrimen y en general de delitos cometidos a través de sistemas informáticos, se dirigen desde la Fiscalía Adjunta de Fraudes, como fiscalía rectora en materia de delitos de fraude informático; así como en cada Fiscalía Adjunta Territorial.

La Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) es una Oficina adscrita la Fiscalía General de la República que actúa por delegación del Fiscal General como órgano encargado de los trámites de extradición y cooperación penal internacional del Ministerio Público a nivel nacional e internacional.

La OATRI ha sido designada como el punto de contacto y autoridad central ante el Consejo de Europa conforme al Art. 35 del Convenio de Budapest para garantizar la asistencia inmediata para investigaciones o procedimientos relacionados con ciberdelitos y evidencias electrónicas y para temas relacionados con cooperación internacional.

5.1.2 Poder Judicial

La Ley Organiza del Poder Judicial de Costa Rica establece que corresponde al Poder Judicial- a través de la Corte Suprema de Justicia y demás tribunales que la ley establezca- *conocer de los procesos civiles, penales, penales juveniles, comerciales, de trabajo, contencioso-administrativos y civiles de hacienda, de familia, agrarios y constitucionales, así como de los otros que determine la ley; resolver definitivamente sobre ellos y ejecutar las resoluciones que pronuncie, con la ayuda de la fuerza pública si fuere necesario*. El Art. 3º. de dicha ley establece que le corresponde administrar justicia a: (i) Juzgados y Tribunales de menor cuantía, contravencionales y de asuntos sumarios; (ii) Juzgados de primera instancia y penales; (iii) Tribunales Colegiados; (iv) Tribunales de Casación; (v) Salas de la Corte Suprema de Justicia; y (VI) la Corte Plena.

También le corresponde al Poder Judicial la función de asegurar que se respeten los derechos de las partes en el proceso penal tanto de los imputados como de las víctimas. Ambas funciones trascendentales para la investigación y enjuiciamiento de los ciberdelitos. Ha de tomarse en consideración que la investigación tecnológica supone la adopción de medidas que invariablemente injieren en derechos fundamentales requiriendo la autorización judicial. Por otro lado, el adecuado

entendimiento de los hechos que han de ser objeto de enjuiciamiento resulta también esencial para el ejercicio de la función judicial. Es por ello que la capacitación específica en ésta materia de los miembros del Poder Judicial constituye una herramienta fundamental para el correcto desarrollo de tan altas funciones.

5.2 Sistema de Capacitación del Poder Judicial y Ministerio Público

En Costa Rica, la formación de los integrantes del Poder Judicial se lleva a cabo a través de la Escuela Judicial que es la institución oficialmente reconocida en la formación, capacitación e investigación de oficiales y empleados encargados de la administración de justicia a nivel nacional.[23] La capacitación de los Jueces y Magistrados del Poder Judicial y profesionales interesados en desarrollar la carrera judicial, se lleva a cabo a través de esa Institución.

Desafortunadamente, los representantes de la Escuela Judicial no pudieron ser convocados a tiempo a las reuniones sostenidas durante nuestra misión, sin embargo se nos hizo saber que esa Escuela Judicial cuenta con una Unidad de Capacitación y que podría ser la unidad encargada de poder vincular los temas de capacitación a nivel nacional con la capacitación en materia de ciberdelito y evidencia electrónica del Consejo de Europa. Derivado de esta situación, recomendamos que el Consejo de Europa, a través del Equipo de Coordinación Nacional de la OATRI establezca contacto permanente con dicha Unidad de capacitación para que en futuras reuniones o actividades en ese país puedan estar presentes los representantes de la Escuela Judicial y puedan formar parte de los cursos sobre formadores del Consejo de Europa.

Cabe destacar que los representantes del Colegio de Abogados y Abogadas de Costa Rica, lugar sede donde se llevó a cabo esta misión, mostraron una gran disposición con el Consejo de Europa en apoyarnos e inclusive se tuvo una reunión con su actual Presidente en donde nos indicó abiertamente que esa institución podría prestar sus instalaciones para futuras reuniones del Consejo de Europa relacionadas con la ejecución del Proyecto GLACY+.

Recomendaciones

- Se sugiere la programación de actividades formativas que integren a los diferentes actores del sistema de justicia penal – Jueces, Fiscales y Policías - por miembros de las distintas instituciones involucradas en las investigaciones tecnológicas.

- La participación conjunta de miembros del Poder Judicial, el Ministerio Público y la Fiscalía y entidades e instituciones especializadas en los cursos que se programen, permitirá visualizar la problemática que plantean las diligencias a realizar en las investigaciones tecnológicas desde sus distintas perspectivas conjugando los aspectos técnicos y jurídicos que surgen en relación con la adopción de medida de esta naturaleza.

- A estos efectos resulta igualmente necesario que el propio Poder Judicial- a través de la Escuela Judicial- que aglutina las unidades de capacitación del Ministerio Público, OIJ y Defensa Pública se involucre de forma activa en la programación futura de actividades de formación en materia de ciberdelitos y evidencia electrónica y pueda articular y promover junto con el Colegio de Abogados y Abogadas de Costa Rica las actividades de formación inicial y continua de los operadores del sistema de justicia penal en Costa Rica; y

23 El portal de la Escuela Judicial esta disponible en: https://goo.gl/xpEdN3

establecer sistemas internos de detección de necesidades y vías de comunicación efectiva con la Academia y el Colegio de Abogados y Abogadas respecto de las necesidades de capacitación que sean identificadas como prioritarias.

- La participación del Poder Judicial en el desarrollo del Proyecto GLACY+ resulta fundamental para el éxito de la misión, a tal fin se recomienda fomentar su participación en todas las fases del programa, participando junto a los miembros de otras instituciones en las actividades de formación especializada o de formación de formadores que se desarrollen en un futuro en el marco del Proyecto.

5.2.2 Formación especializada del Ministerio Público

El Ministerio Público en Costa Rica dispone de una unidad de capacitación interna para sus funcionarios conocida como la *Unidad de Capacitación, Supervisión-Reclutamiento y Selección*.[24] La misión general de esa unidad de capacitación es ser un órgano eficaz y eficiente en las labores de selección, reclutamiento, formación y capacitación por competencias del talento humano del Ministerio Público, y en la supervisión del cumplimiento de las directrices y circulares de la Fiscalía General de la República de Costa Rica, con el fin de garantizar la excelencia en el servicio público que se brinda.

De acuerdo con información proporcionada por la OATRI, dicha Unidad de Capacitación cuenta con un presupuesto propio para capacitación de los integrantes del Ministerio Público que se utiliza con el fin de poder contar con materiales y contratación de cuerpo docente para el cumplimiento de su plan anual. Se nos informó que esa unidad no cuenta con actividades de capacitación propias en material de ciberdelito y evidencias electrónicas e indicaron que la mayoría de las capacitaciones que se han brindado en esos temas se han realizado por medio de donaciones internacionales.

Recomendaciones

Resulta recomendable que además de las actividades de formación específica que actualmente lleva a cabo la Unidad de Capacitación, Supervisión-Reclutamiento y Selección del Ministerio Público en Costa Rica, lleve a cabo actividades de formación específica en materia de ciberdelito y evidencias digitales y que aborde programas de formación conjunta con otros actores del sistema de justicia penal involucrados en la lucha contra la ciberdelincuencia tales como son el OIJ y la Corte Suprema de Justicia.

---

24 Portal disponible en: https://goo.gl/hYHqBU Esta unidad fue creada mediante la Ley Orgánica del Ministerio Público (Ley No. 7728) del 15 de diciembre de 1997 que en su Art, 39 dispone lo siguiente:

"Artículo 39. La Unidad de Capacitación y Supervisión. Le corresponde a la Unidad de Capacitación y Supervisión organizar los programas de selección, ingreso y capacitación del personal del Ministerio Público, en coordinación con la Escuela Judicial y el Departamento de Personal en lo que corresponda. Los integrantes de esta unidad deberán desplazarse a las distintas oficinas del Ministerio Público del país, con el fin de verificar el cumplimiento de las directrices, así como el desempeño de las labores en general, e impartir las instrucciones técnicas necesarias para un mejor servicio público. Esta oficina será dirigida por un funcionario de amplia experiencia, que tendrá categoría de fiscal adjunto."

5.3 Combate a Delitos de Abuso Sexual e Imágenes de Abuso Sexual Infantil

Tal y como se indica en la sección 3.1.1. de este reporte, Costa Rica cuenta con un marco jurídico bastante completo en lo que se refiere a delitos relacionados con el abuso de menores y el combate a la producción y comercialización del uso de imágenes relacionadas con pornografía infantil y abuso sexual de menores en la red que se investiga a través de las disposiciones del Código Penal y la Ley de Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos (Ley No. 8934).[25]

La sociedad civil en Costa Rica trabaja muy activamente con las entidades gubernamentales en el tema de abuso sexual de menores desde hace algunos años. Durante esta misión mantuvimos una entrevista con la directora de la Fundación PANIAMOR organización no gubernamental encargada de velar por la defensa de los derechos de las niñas, niños y personas adolescentes en Costa Rica.[26] Esa organización trabaja actualmente en temas relacionados con prevención sexual y abuso de menores a través del uso de tecnologías de información y es miembro de ECPAT International[27] y de la Iniciativa sobre Protección de Menores en Línea de la Unión Internacional de Telecomunicaciones (UIT).[28]

Se nos informó que se encuentran trabajando en un proyecto de aplicación tecnológica (app) que pretende servir como una campaña de concientización y educación para fomentar el mejor uso de las tecnologías y prevenir violencia entre la población adolescente.

En opinión de la directora de la fundación, se han detectado vacíos legales en el marco jurídico penal de Costa Rica para tipificar conductas relacionadas con la violencia sexual y el hostigamiento en línea. Comentó que su fundación colaboró en un proyecto de iniciativa de ley que fue avalado por el MICITT para incluir la tipificación de algunos delitos que hacen falta en el Código Penal. Indicó que los delitos relacionados con el abuso sexual y explotación de menores de los que su fundación tiene conocimiento, se reportan directamente al Ministerio Público.

Hizo un particular énfasis en la necesidad de reforzar las técnicas actuales de investigación de delitos de abuso sexual de menores conforme a estándares internacionales y que las atribuciones y facultades para llevar a cabo investigaciones de esta índole por parte del Poder Judicial sean más efectivas y que puedan contribuir de mejor forma a proteger a las víctimas de este tipo de delitos y a castigar y sancionar a los responsables en el ámbito nacional.

Durante la presentación de las conclusiones preliminares, una Magistrada del Poder Judicial destacó la importancia de potencializar la institucionalidad del Poder Judicial, mediante la valoración de la generación de acciones integrales en forma transversal, para la atención de la persona víctima y de la protección a poblaciones vulnerables, previendo un mapa de acción y atención considerando la posible captación y atención de personas en condición de vulnerabilidad debido a los diversos factores multidimensionales de pobreza y desarrollo social del país.

---

25 Disponible en: https://goo.gl/GU1JD2

26 La fundación PANIAMOR fue creada en 1987 y declarada de interés público para los fines del Estado Costarricense mediante Decreto No. 19212-J-H de 13 de Septiembre de 1989, disponible en: https://paniamor.org/

27 Disponible en: http://www.ecpat.org/

28 Disponible en: https://www.itu.int/en/cop/Pages/default.aspx

Recomendaciones

- Recomendamos que se realicen las acciones necesarias para revisar el marco jurídico sustantivo relacionado con los delitos de explotación y abuso sexual de menores a través del uso de tecnologías de información, así como fortalecer las técnicas de investigación policial y judicial para investigar y procesar este tipo delitos que tienen una grave repercusión en niños, adolescentes y en el entorno familiar de las víctimas. Para ello, recomendamos tener una opinión previa debidamente sustentada del Ministerio Público y de la Comisión Nacional de Ciberseguridad y Ciberdelitos conforme a la experiencia lograda en la persecución de este tipo de conductas y delitos con el objeto de poder generar y proponer una reforma al marco jurídico sustantivo y procedimental penal, en caso de ser necesaria.

- Se recomienda que el gobierno de Costa Rica comience a realizar las gestiones necesarias para adherirse al Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual (Convenio de Lanzarote)[29] que estamos seguros ayudará a reforzar en gran medida el marco jurídico nacional relacionado con los delitos de pornografía infantil y la explotación y abuso sexual de menores a través del uso de tecnologías, así como fortalecer las técnicas de investigación policial y judicial para investigar y procesar este tipo de conductas, fomentar el intercambio de mejores prácticas con otros países que ya han ratificado ese instrumento y reforzar las capacidades de las autoridades encargadas de su investigación y persecución a nivel nacional, así como reforzar la labor de los actores de la sociedad civil que se encuentran trabajando activamente en la temática en Costa Rica.

- Se sugiere que la Comisión de Ciberseguridad y Ciberdelincuencia elabore e incorpore dentro de la estrategia sobre combate al cibercrimen, dentro de los delitos en los cuales se utiliza como modo de ejecución los medios tecnológicos (pornografía infantil, explotación sexual, trata de personas); un eje transversal de género, y estrategias integrales y diferenciadas para el abordaje y protección integral de los derechos de las víctimas (mujeres, niños, niñas, adolescentes) en condiciones de vulnerabilidad.

29 Texto disponible en Español en: https://goo.gl/vdEF4e

6. Equipo de Coordinación Nacional

La constitución de un equipo de coordinación nacional del Proyecto GLACY+ era uno de los objetivos prioritarios de esta primera fase. Dada la conformación reciente del Poder Judicial, que incorpora a la Corte Suprema de Justicia, la Fiscalía General de la República y el Organismo de Investigación Judicial y teniendo en cuenta las facultades y atribuciones internas y posición actual de la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General de la República, se propuso que dos funcionarios de esta oficina sean las personas designadas del Equipo de Coordinación Nacional ante el Consejo de Europa.

Se acordó esto teniendo además en cuenta que la OATRI desempeña un rol muy importante como autoridad central vinculada con la implementación de diversos tratados internacionales ratificados por Costa Rica.

Se recordó a los presentes que el Equipo de Coordinación Nacional deberá estar dirigido a ayudar a materializar las distintas actividades que se integren dentro del Proyecto GLACY+, que afectarán además a otras Instituciones vinculadas con el combate a la ciberdelincuencia. Se designó a dos altos funcionarios como coordinadores nacionales que además de actuar como punto de contacto oficial con el Consejo de Europa (CoE) asuman la labor de punto de contacto interno con las demás Instituciones haciendo un seguimiento del propio Proyecto GLACY+ y de un futuro plan de trabajo. La Fiscalía General de la Nación hizo recaer esta función de Coordinación Nacional en la Fiscal Adjunta Laura Monge Cantero y el Fiscal Juan Carlos Cubillo Miranda.