Embajada Británica
en México

Programa en
Anticorrupción y para
el Estado de Derecho

RECOMENDACIONES PARA ABORDAR LA DETECCIÓN E INVESTIGACIÓN DEL FRAUDE CIBERNÉTICO EN MÉXICO

PERSPECTIVA DESDE EL SISTEMA JUDICIAL

Octubre 2021

RECOMENDACIONES PARA ABORDAR LA DETECCIÓN E INVESTIGACIÓN DEL FRAUDE CIBERNÉTICO EN MÉXICO

Autoras
Estefanía Medina Ruvalcaba
Cristos Velasco San Martin
Andrés Velázquez Olavarrieta

Coordinadora del Equipo Técnico
María Novoa Cancela

Contribuidoras
Samahanta Bautista Paredón
Monserrat López Pérez

Coordinación editorial
Lorena de la Barrera
Adriana Reyes

Colaboradoras/es: PA Consulting
Gabriela Capó
Mikel Santos
Neil Amos

Embajada Británica en México

Embajador
Jon Benjamin

Consejero de Prosperidad
Martin Johnston

Director del Programa de Prosperidad
Richard Rose

Directora Adjunta del Programa de Prosperidad
Claudia Pando

Gerente de Gobernanza y Comunicación Estratégica del Programa de Prosperidad
Ofelia Ortega

Gerente del Programa de Prosperidad en Anticorrupción y Estado de Derecho
Carlos Hernández

Asesora del Programa de Prosperidad en Anticorrupción y Estado de Derecho
Daniela Álvarez

Lugar y fecha de publicación:
Ciudad de México, México, octubre de 2021.

PRÓLOGO

Las relaciones entre el Reino Unido y México son históricas y se han basado en el apoyo mutuo para promover la economía, el desarrollo y la prosperidad de ambos países. A fin de fortalecer esta relación, en 2017 se puso en marcha el entonces llamado Fondo de Prosperidad (ahora Programa de Prosperidad). Dichos Fondo ha sido una aportación del gobierno del Reino Unido a la comunidad internacional para contribuir a la reducción de la pobreza, promover el crecimiento y desarrollo económico inclusivo y la igualdad de género en los países socios que enfrentan desafíos de desarrollo persistentes, así como problemas asociados con la desigualdad, la rápida urbanización, la corrupción y el cambio climático.

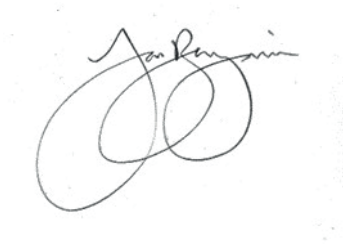
En ese sentido, en el año 2019 nació el ***Programa de Prosperidad en Anticorrupción y Estado de Derecho*** con el propósito de fortalecer el estado de derecho, la gobernabilidad y la seguridad para las y los ciudadanos y empresas de México, a través de un entorno empresarial más justo, abierto y competitivo. Nuestra tesis, es que entre mayor certeza jurídica haya en el país, habrá mejores oportunidades de prosperidad. Es por ello, que este Programa enfocó sus esfuerzos en atender tres fenómenos criminales que ponen en peligro el crecimiento y desarrollo de este gran país: el ***homicidio***, el ***peculado*** y el ***fraude cibernético*** en el sector financiero.

El trabajo que hemos llevado a cabo en estos años se ha concentrado en Tabasco, Jalisco, Ciudad de México y la federación, siendo esta última, el espacio donde desarrollamos el presente **Informe Exploratorio en materia de Fraude Cibernético Financiero** en México, de la mano de la **Comisión Nacional Bancaria y de Valores**. Sin pensarlo, nuestro trabajo en este tema se volvió muy relevante a causa de la pandemia COVID-19. La aceleración de la digitalización y el uso de la tecnología fue necesaria para que el mundo la enfrentase.
Sin lugar a dudas, la reducción de la brecha tecnológica que hemos logrado deberá traer consigo muchas ventajas de competitividad en los diferentes sectores; pero también está generando muchos más riesgos de los que ya existían; ya que, a partir de la pandemia, se ha presentado un incremento en delitos cibernéticos, siendo el fraude en el sector financiero el de mayor preocupación.

Este aumento de nuevas formas de delincuencia que incluyen el uso de la tecnología ha tomado desprevenidos a los gobiernos ya que es necesario mayor conocimiento para combatirlos. Es aquí donde radica la importancia del presente Informe. En él, se analiza el fenómeno desde la perspectiva legislativa, de políticas públicas, de detección, investigación y persecución penal, así como desde la colaboración internacional. Su mayor virtud es poner al centro del análisis a las víctimas; es decir las y los *individuos* y *empresas*.

Sé que este Reporte se convertirá en un instrumento de consulta obligatoria para todas y todos aquellos encargados del diseñar políticas públicas para prevenir y combatir este fenómeno. Espero que, sobre la base de este instrumento, pronto ambos países, Reino Unido y México, compartamos estrategias innovadoras para proteger a nuestras empresas y ciudadanas y ciudadanos de los delitos de la 4ª revolución industrial. Tengan certeza de que el Reino Unido tiene como objetivo principal promover y proteger el futuro a largo plazo de un ciberespacio libre, abierto, pacífico y seguro y gestionado por múltiples partes interesadas. En ese sentido, seguiremos trabajando con México para brindar desarrollo de capacidades a medida para ayudar a aumentar la seguridad cibernética a nivel global.

Agradezco el apoyo brindado por la CNBV por su liderazgo durante el proceso de construcción de este documento. ¡En hora buena!



Jon Benjamin
Embajador del Reino Unido de la Gran Bretaña e Irlanda del Norte en México

CONTENIDOS

1. PRESENTACIÓN

El presente documento es un estudio exploratorio sobre el delito de fraude cibernético en el ámbito financiero en cuatro países seleccionados de América Latina y el Caribe (ALC) con particular énfasis en México. Los principales aspectos abordados son los siguientes:

- definición del fraude cibernético en el sector financiero
- marco jurídico internacional aplicable
- estrategias exitosas en la investigación, persecución y persecución del delito en países selectos de ALC
- análisis conciso sobre el marco jurídico y entramado institucional respecto a los ciberdelitos en México
-

El estudio se realizó con el apoyo de personas expertas con amplia trayectoria en la materia, el uso de fuentes públicas, estudios y reportes recientes de organizaciones nacionales y organismos internacionales. El reporte está estructurado en ocho secciones principales:

1. La **sección dos** proporciona un **resumen ejecutivo** del contenido incluido en el documento.

2. La **sección tres** describe los **objetivos** y la **metodología** empleados para el desarrollo del estudio.

3. La **sección cuatro** presenta una **definición** sobre fraude cibernético en el ámbito financiero, que incluye a las personas usuarias como víctimas y presenta datos sobre las afectaciones económicas de este tipo de ciberdelitos.

4. La **sección cinco** incluye un compendio de los **tratados internacionales** y de las **legislaciones aplicables** sobre **ciberdelito en países seleccionados de ALC**, incluido México.

5. La **sección seis** presenta un catálogo de **buenas prácticas** aplicadas en países seleccionados de ALC que presentan un avance considerable respecto a la prevención, investigación y combate al ciberdelito.

6. La **sección siete** analiza las instituciones nacionales involucradas y marco jurídico aplicable a la investigación, prevención y sanción de los **ciberdelitos en México**.

7. La **sección ocho** proporciona un resumen con las **conclusiones** sobre el estado actual del fraude cibernético en el ámbito financiero, primordialmente en México.

8. La **sección nueve** establece una serie de **recomendaciones** para mejorar la eficiencia en la investigación y persecución del delito de fraude cibernético.

2. RESUMEN EJECUTIVO

Las tecnologías de la información no sólo han tenido un rol trascendental para realizar distintas actividades, también han contribuido al acceso universal de servicios y derechos tan básicos como la educación y la economía. Debido a la crisis sanitaria mundial generada por el COVID-19, las distintas formas de interacción se han transformado y han favorecido aún más el uso de dichas herramientas. Sin embargo, esto también ha conllevado a que la comisión de delitos a través de las tecnologías de información y comunicación sea actualmente una de las principales amenazas a la seguridad para todos los países de América Latina y el Caribe (ALC), dentro de los que se incluye México.

El presente reporte parte de un estudio del estado actual del delito de fraude cibernético en México desde la perspectiva del Sistema de Justicia y lleva a cabo un análisis de mejores prácticas que se han desarrollado en ALC para plantear una serie de recomendaciones que permitan abordar el fenómeno criminal. Los principales objetivos del documento son los siguientes:

- Determinar los alcances del fraude cibernético financiero
- Analizar la situación actual del fraude financiero cibernético en México desde tres principales enfoques:
  - Eficacia del marco jurídico vigente
  - Respuesta del Sistema de Justicia hacia las víctimas tanto personas usuarias como entidades financieras
  - Actores clave y su interrelación ante la comisión de un fraude financiero cibernético
- Identificar buenas prácticas en la investigación y persecución del fraude financiero cibernético en ALC
- Recomendar acciones de mejora para México considerando las mejores prácticas a analizadas

Dentro de algunos de los hallazgos en el ámbito internacional se destaca el Convenio sobre la Ciberdelincuencia del Consejo de Europa mejor conocido como “Convenio de Budapest” que es el principal instrumento internacional que ha contribuido al desarrollo de la legislación sustantiva, procesal y sobre disposiciones de cooperación internacional para investigar, procesar y sancionar ciberdelitos. Este instrumento ha sido firmado y ratificado por 66 países, de entre los que destacan ocho países de ALC. A este convenio, se suman iniciativas sobre construcción y fomento de las capacidades tales como el Proyecto GLACY+ (*Global Action against Cybercrime Extended)* impulsado por el Consejo de Europa para que los estados que son parte del Convenio de Budapest puedan llevar a cabo reformas a su legislación sustantiva y procesal en materia penal y actividades de capacitación a las autoridades del sistema de justicia penal, entre otras actividades clave para combatir el ciberdelito.

En ALC, algunos países destacan por los avances realizados en la materia que les han permitido mejorar las investigaciones y la persecución de ciberdelitos. Especialmente, se analizaron buenas prácticas detectadas en los siguientes cuatro países: Argentina, Colombia, República Dominicana y Chile.

Para el caso concreto de México, se destacan como aspectos muy positivos la reciente creación del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información en el que participan instituciones públicas y privadas relacionadas con el ámbito de la ciberseguridad y ciberdelincuencia, así como el hecho de que cuenta con policías cibernéticas de investigación criminal y de seguridad pública a nivel federal y en algunas entidades federativas. Sin embargo, se identifican como áreas de oportunidad las siguientes: (i) formalizar el proceso de adhesión al Convenio de Budapest; (ii) impulsar reformas legislativas necesarias para mejorar los procedimientos de investigación y persecución de los ciberdelitos, así como fortalecer la coordinación y las capacidades de las autoridades encargadas de la investigación, persecución y sanción de ciberdelitos en el ámbito federal y local. Lo cual, desde la perspectiva de lo que ha acontecido en otros países de ALC, puede generarse mediante un liderazgo institucional y voluntad política.

Por último, el reporte establece recomendaciones que pueden ser de gran utilidad para que México adopte experiencias exitosas que han sido eficaces en otros países, así como la mejora e impulso de los esfuerzos que se están realizando en el plano nacional. Estas recomendaciones se dividen en dos principales dimensiones, la primera es la dimensión normativa y, una segunda, desde el plano completamente operativo. Con dos perspectivas, una es de la mejora de los procesos de las instituciones involucradas en los procesos de detección, investigación y persecución de la cibercriminalidad, y la otra es la mejora en el esquema de coordinación y articulación de las labores realizadas por esas autoridades.

El objetivo final es que este reporte sea un documento de consulta para el diseño de nuevas políticas y estrategias tanto públicas como privadas que buscan prevenir, detectar, investigar y sancionar los delitos de fraude financiero cibernético.

3. INTRODUCCIÓN

Las tecnologías de la información no sólo han tenido un rol trascendental para realizar distintas actividades, también han contribuido al acceso universal de servicios y derechos tan básicos como la educación y la economía. Debido a la crisis sanitaria mundial generada por el COVID-19, las distintas formas de interacción se han transformado y han favorecido aún más el uso de dichas herramientas. Sin embargo, esto también ha conllevado a que la comisión de delitos a través de las tecnologías de información y comunicación sea actualmente una de las principales amenazas a la seguridad para todos los países de América Latina y el Caribe (ALC), dentro de los que se encuentra México.

La atención de riesgos y amenazas a la seguridad que ocurren por el uso de las tecnologías de la información y comunicación puede ser identificada en tres rubros principales: I) ciberseguridad, relacionada con medidas de carácter preventivo; II) ciberdefensa, relacionada con seguridad de la información desde el ámbito de la seguridad nacional; y, III) ciberdelitos, relacionada con los procesos de tipificación, investigación, persecución y sanción de las conductas consideradas como delitos.

3.1 Objetivos

El presente reporte parte de un estudio del estado actual del delito de fraude cibernético en México desde la perspectiva del Sistema de Justicia y lleva a cabo un análisis de mejores prácticas que se han desarrollado en ALC para plantear una serie de recomendaciones que permitan abordar el fenómeno criminal. Los principales objetivos del documento son los siguientes:

- Determinar los alcances del fraude cibernético financiero.
- Analizar la situación actual del fraude financiero cibernético en México desde tres principales enfoques:
  - Eficacia del marco jurídico vigente.
  - Respuesta del Sistema de Justicia hacia las víctimas y personas usuarias como entidades financieras.
  - Actores clave y su interrelación ante la comisión de un fraude financiero cibernético.
- Identificar buenas prácticas en la investigación y persecución del fraude financiero cibernético en ALC.
- Recomendar acciones de mejora para México considerando las mejores prácticas analizadas.

Para lograr sus objetivos, el documento pretende dar una respuesta una serie de preguntas, tomando en cuenta algunas de las mejores prácticas que se han desarrollado en algunos países de la región, las cuales podrían ser replicables en otros países de ALC. Las preguntas clave a responder son las siguientes:

- ¿Cuál es la conceptualización del fraude financiero cibernético?
- ¿Cómo el fraude financiero afecta a las personas usuarias del sistema bancario a través de tecnologías de la información?
- ¿Cuáles son las opciones de respuesta del sistema de justicia para esas víctimas?
- ¿Cuál es la situación actual de la investigación, persecución y adjudicación de ciberdelitos en la región de ALC, con especial énfasis en el fraude financiero cibernético?
- ¿Cuál es el estado actual de la investigación, persecución y adjudicación de estos delitos en México?

Es importante mencionar que este documento es de carácter exploratorio, con lo que se busca tener un panorama y análisis general sobre la problemática desde las perspectiva de las personas usuarias que son víctima de un fraude financiero cibernético y las soluciones que provee el sistema de justicia penal para, derivado de ello, presentar una referencia que sea de utilidad, principalmente, para identificar los retos prioritarios en la materia, reconocer las mejores prácticas en la región, y establecer una serie de recomendaciones para identificar y presentar soluciones de mejora para el caso concreto de México.

3.2 Metodología

La metodología de este reporte se basa en el análisis y estudio del marco jurídico regulatorio vigente, el análisis documental de información disponible en fuentes abiertas, así como en entrevistas con actores clave y con reconocida trayectoria en la materia de los ámbitos público y privado. Asimismo, se realizaron tres comunidades con ejercicios prácticos en los cuales personas expertas nacionales e internacionales, del sector académico y público, presentaron sus perspectivas sobre las buenas y malas prácticas detectadas a nivel de política pública y de operación en la investigación y persecución de los delitos, lo cual fue posteriormente fortalecido con el diálogo y experiencias de las personas operadoras asistentes.

Entre las personas expertas participantes se encuentran académicos y académicas, personas funcionarias y exfuncionarias públicos del sector financiero; autoridades y exautoridades encargadas de la investigación y persecución de ciberdelitos; y personas expertas encargados sobre ciberseguridad de instituciones financieras de entre los que destacan Andrés Velázquez, Presidente y Fundador de MaTTica, Franco Pilnik, Fiscal Especializado en Ciberdelitos de la Provincia de Córdoba, Carlos Leonardo, Director del Equipo de Respuesta a Incidentes Cibernéticos CSIRT-RD del Centro Nacional de Ciberseguridad y PoC 24/7 Cibercrimen de República Dominicana, Daniel Soto, Unidad de Cooperación, Internacional y Extradiciones (UCIEX) de la Fiscalía de Chile y Marcos Salt, Profesor de la Universidad de Buenos Aires. Además, se recabaron cuestionarios de información con la Comisión Nacional Bancaria y de Valores (CNBV) y de la Comisión Nacional para la Protección y Defensa de los Usuarios de Financieros (CONDUSEF).

4. Definición del fraude financiero cibernético

4.1 ¿Qué entendemos por fraude financiero cibernético?

Derivado de la revisión y análisis del marco jurídico, tanto a nivel nacional como internacional, se identificó que no existe algún referente a nivel internacional que formalmente regule el concepto de fraude financiero cibernético de manera específica. Sin embargo, considerando los diversos enfoques consultados con las personas expertas para efectos de este reporte se considerará como fraude financiero cibernético a:

"Todo aquel acto de engaño[1] que se realice con la finalidad de obtener beneficios económicos indebidos en agravio de instituciones o personas usuarias del sistema financiero mediante el uso de las tecnologías de la información."

Esta definición deriva, en gran parte, del artículo 8° del "Convenio de Budapest"[2] establece la obligación de tipificar en el derecho interno a quien cometa actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante introducción, alteración, borrado o supresión de datos informáticos, y cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener ilegítimamente un beneficio económico para uno mismo o para terceros. Si bien, no existe una referencia puntual y precisa respecto al fraude cibernético en el ámbito bancario o financiero a nivel internacional, se consultaron diversas fuentes para establecer una mejor conceptualización.

[1] Se aclara también que en algunos casos haremos referencia a incidentes distintos a los engaños como pueden ser los ataques a instituciones bancarias y financieras como a aquellos actos que con intensiones fraudulentas o delictivas intentan obtener un beneficio económico mediante el uso de tecnologías de la información.

[2] El Art. 8o. del Convenio de Budapest es el siguiente: "Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a. cualquier introducción, alteración, borrado o supresión de datos informáticos, y b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener ilegítimamente un beneficio económico para uno mismo o para terceros."

En este sentido, distintas personas expertas en la materia concluyeron que la visión del fraude cibernético en el ámbito financiero y bancario debe incluir tanto los casos en los que las instituciones financieras resultan afectadas por la comisión de un fraude a través de medios tecnológicos, así como aquellos casos en los que las personas usuarias (clientes directos como personas físicas y proveedores) resultan afectados en su patrimonio; es decir, resulta indispensable contar con una conceptualización amplia y no limitada. Las afectaciones de un fraude cibernético en el ámbito financiero y bancario podrían incluir a los siguientes actores:

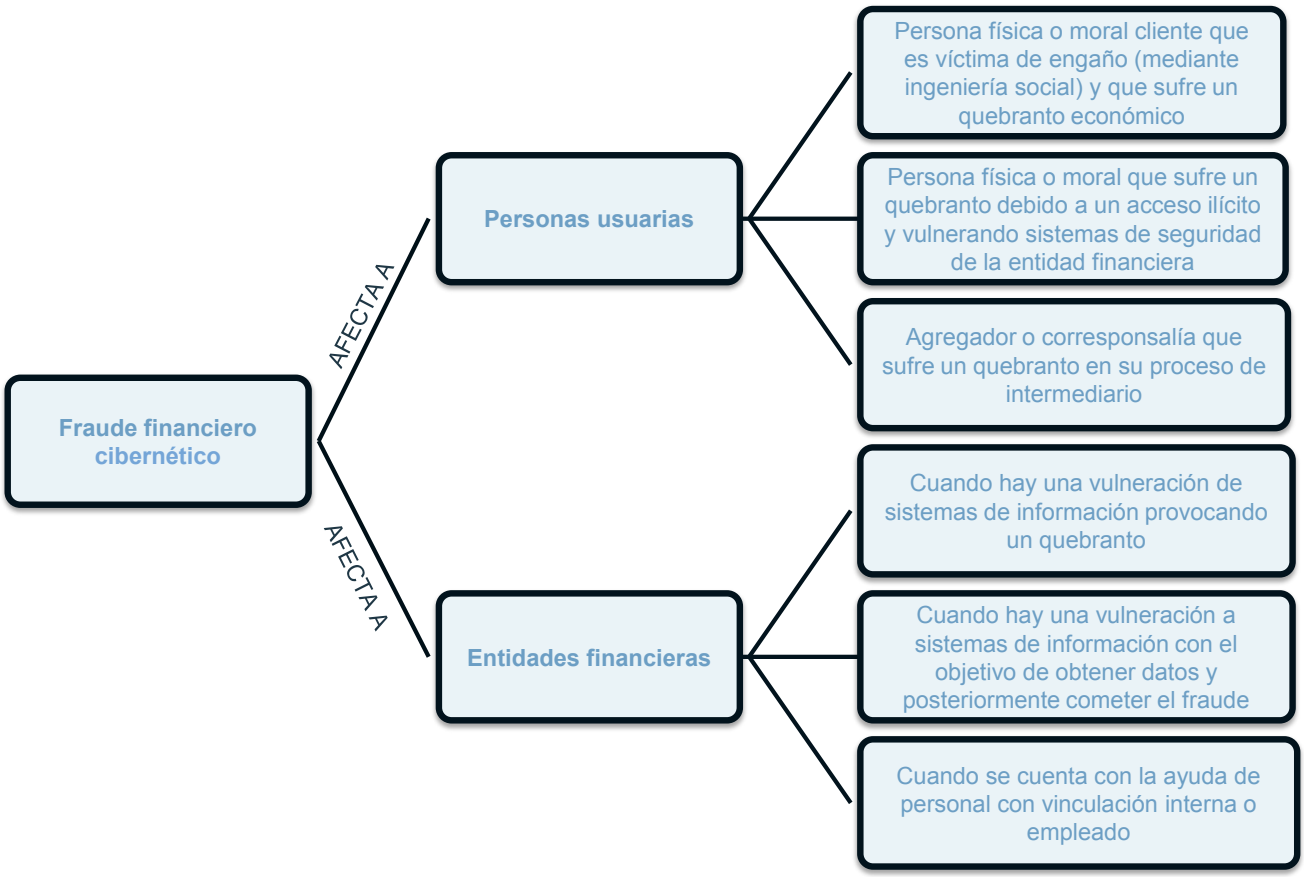


Figura 1. Elaboración propia.

Es importante destacar que en términos generales se detectó que los delitos cibernéticos dentro de los cuales se encuentra el fraude financiero cibernético son delitos sumamente complejos que abarcan desde el ámbito de la comisión de nuevos delitos, delitos tradicionales cometidos a través de tecnologías de la información y además evidencia digital que se genera para cualquier tipo de delitos.

4.2 Impacto del fraude financiero cibernético en América Latina

Los sectores bancario y financiero han tenido una mayor transición -y más acelerada- al uso de las tecnologías de la información en sus actividades, especialmente en un contexto en el que se ha reducido sustancialmente la movilidad de dinero en efectivo, y la movilidad de personas por la pandemia. Por ello, ante el creciente uso de estas herramientas para el uso de servicios financieros y bancarios, el fraude financiero cibernético se ha convertido en uno de los mecanismos más atractivos del crimen organizado. De acuerdo con el informe "Cibercrimen: impacto del COVID-19" publicado por la Organización Internacional de Policía Criminal (INTERPOL) durante 2020, las condiciones impuestas por la crisis sanitaria han incrementado los ataques de criminales a través de tecnologías de la información. Otro de los aspectos importantes referidos por la INTERPOL es que esta forma de criminalidad ha cambiado sus víctimas objetivo pasando de individuos y pequeños comercios a grandes empresas, instituciones gubernamentales e infraestructura crítica del Estado.[3] En el caso de México de acuerdo con cifras de la Guardia Nacional de febrero a marzo de 2020, la cibercriminalidad aumentó en un 14% siendo el fraude financiero cibernético la tercera modalidad con mayor incidencia[4].

De acuerdo con un reporte de la Organización de los Estados Americanos (OEA) en 2018[5], que incluye cifras previas al confinamiento, el 92% de las entidades financieras identificaron algún tipo de evento (ataques[6] exitosos y no exitosos) de seguridad digital en su contra durante 2017. Por su parte, el 37% de las instituciones bancarias identificaron ataques exitosos, de los cuales la principal motivación fueron motivos económicos. Asimismo, la mitad de las entidades bancarias de la región indicaron contar con estrategias de gestión, respuesta y recuperación ante estos ataques. Los tipos de eventos más comunes identificados por dichas instituciones fueron los siguientes:

- Código malicioso o malware (80%)
- Violación de políticas de escritorio limpio "clear desk" (63%)
- Phishing dirigido para tener acceso a los sistemas del banco (24%)

[3] Cibercrimen: Impacto del COVID-19, INTERPOL, página 4, disponible en: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[4] Ciberdelitos aumentan en la contingencia; incrementaron 14% entre marzo y abril, el Economista, disponible en: https://www.eleconomista.com.mx/politica/Ciberdelitos-aumentan-en-la-contingencia-incrementaron-14-entre-marzo-y-abril-20200513-0063.html

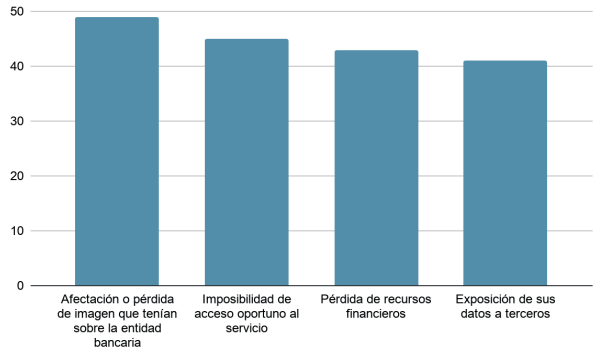
[5] Estado de la Ciberseguridad en el Sector Bancario de América Latina y el Caribe, Organización de los Estados Americanos, páginas 9 y 10, disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

[6] Los ataques a través de tecnologías de la información o ataques cibernéticos son intentos maliciosos de acceder o causar daños a un sistema de computadora o red. Los ataques cibernéticos pueden causar pérdida de dinero, robo de información personal, financiera o médica que puede dañar su reputación y seguridad.

Asimismo, las entidades bancarias indicaron que los eventos más frecuentes en contra de sus personas usuarias fueron: 1) phishing; 2) ingeniería social; y, 3) software espía (malware o troyanos); situación que, conforme al reporte de la OEA tiene sustento con lo referido por las propias personas usuarias. A continuación, se presentan los principales efectos y el impacto económico derivado de los ataques cibernéticos según las personas usuarias:

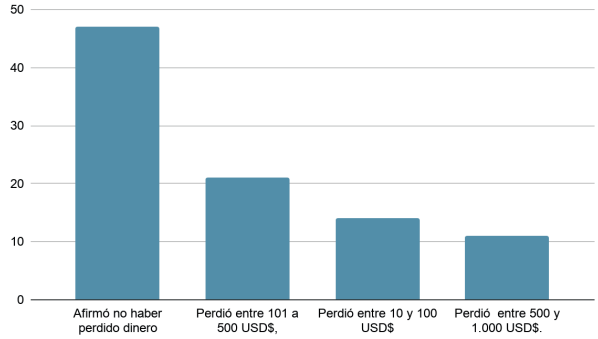
Efectos negativos de los ataques según las personas usuarias

(% de personas usuarias que afirmaron sufrir el efecto)



Impacto económico de los ataques según las personas usuarias

(% de personas usuarias que afirmaron sufrir el efecto)



Nota: Elaboración propia con información extraída del reporte Estado de la Ciberseguridad en el Sector Bancario de América Latina y el Caribe realizado por la Organización de los Estados Americanos.

Según las gráficas anteriores, desde la perspectiva de las personas usuarias se identificó como efectos negativos de dichos ataques los siguientes:

- Afectación o pérdida de imagen que tenían sobre la entidad bancaria (49%)
- Imposibilidad de acceso oportuno al servicio (45%)
- Pérdida de recursos financieros (43%)
- Exposición de sus datos a terceros (41%)

Asimismo, en lo que respecta al impacto económico sufrido por las personas usuarias, el reparto fue el siguiente:

- 47% afirmó no haber perdido dinero
- 21% que manifestó haber perdido entre 101 a 500 USD$
- 15% que expresó haber perdido entre 10 y 100 USD$
- 11% que registró haber perdido entre 500 y 1.000 USD$

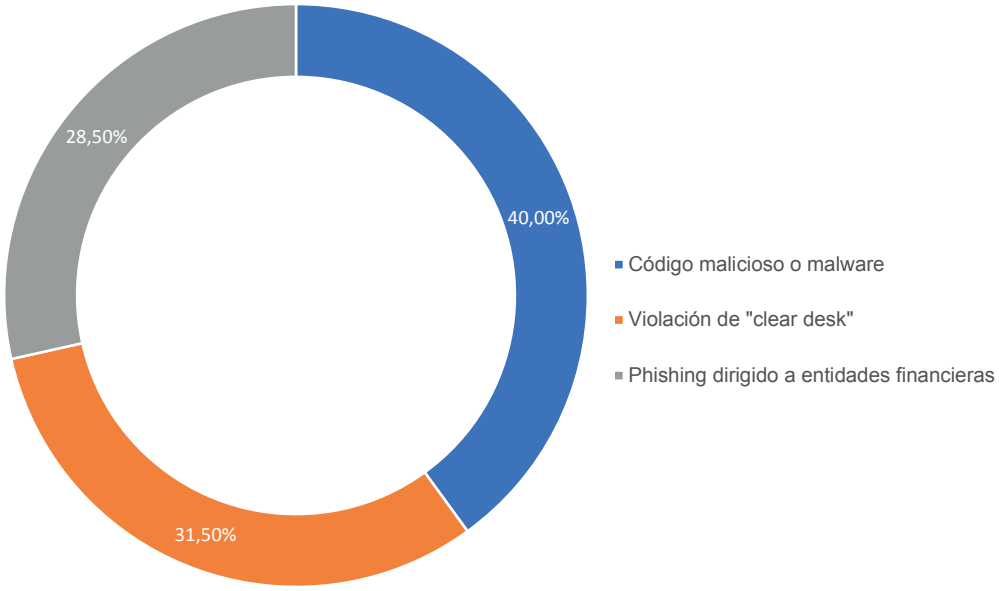
De las personas usuarias con pérdida, el 45% manifestó haber sido resarcida o compensada totalmente, mientras que el 26% fue resarcida parcialmente, y el 29% no recibió ningún tipo de indemnización.

En relación con los mecanismos, el informe señala que 65% de las personas usuarias entrevistadas informó que la institución bancaria sí ofrece un mecanismo para reportar incidentes, y que el 71% ha reportado el incidente ante su banco. Sin embargo, **es importante destacar que sólo el 37% afirma que en su país existe un mecanismo para reportar incidentes ante una institución gubernamental**, **el 32% indica que no existe y un 31% no sabe de su existencia. Resulta, además, relevante que sólo el 23% de las personas encuestadas indicó haber presentado un reporte ante autoridades policiales o judiciales**.

En el caso de México, de acuerdo con datos del Informe de Ciberseguridad del Sistema Bancario Mexicano[7] emitido durante 2019 todas las entidades e instituciones financieras identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en su contra. De acuerdo con este informe, entre los eventos de ciberseguridad mayormente identificados durante el año 2018 destacan los siguientes:

- El código malicioso o malware (56% del total de entidades)
- El phishing dirigido para tener acceso a sistemas de la entidad (47% del total de entidades)
- La violación de políticas de escritorio limpio “clear desk” (31% del total de entidades)

Principales eventos de ciberseguridad



Nota: Elaboración propia con información extraída del reporte Estado de la Ciberseguridad en el Sector Bancario de América Latina y el Caribe realizado por la Organización de los Estados Americanos.

[7] Informe de Ciberseguridad del Sistema Bancario Mexicano, Organización de los Estados Americanos, página 11, 2019, disponible en: http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

Además, un 19% de las entidades e instituciones financieras identifican ocurrencia de eventos de malware diariamente.[8]

Siguiendo con lo referido por el informe del de Ciberseguridad del Sistema Bancario Mexicano, el 55% de las entidades financieras ofrece un mecanismo para que sus usuarios y usuarias internos (empleados, empleadas y contratistas) reporten incidentes de ataques exitosos; el 41% cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida; y, **el 44% de las entidades financieras reporta los ataques sufridos ante una autoridad de procuración de justicia en México**.

Sin embargo, sobre la efectividad de las autoridades de procuración de justicia, se destaca que sólo el 10% los consideró altamente efectivas con algunas deficiencias, el 36% medianamente efectivas, el 15% nada efectiva, el 31% poco efectiva con algunos resultados, y el 8% totalmente inefectiva.

Aunado a lo anterior, por lo que respecta al fraude financiero cibernético es relevante considerar que, de acuerdo con las personas expertas consultadas, la crisis por COVID 19 ha constituido un factor detonador en incremento en los delitos toda vez que se ha incrementado en el uso de tecnologías de la información para servicios financieros y comerciales. Por ejemplo, de acuerdo con [Daniel Soto] de la Fiscalía de Chile, a penas después de unas horas de anunciarse una serie de apoyos que serían remitidos por el gobierno Chileno a los ciudadanos como apoyo por la crisis sanitaria, a través de cuentas bancarias del Banco Nacional de Chile, algunas personas usuarias empezaron a recibir mensajes de correos electrónicos apócrifos con la intención acceder a información de las personas usuarias para posteriormente cometer los desfalcos. En el caso de Argentina el Fiscal Azollín dio a conocer que dentro de las cifras de denuncia detectadas de 2019 a 2020 respecto de los mismos periodos de 2020 a 2021 se identificó que el número de fraudes en general aumento de 668 a 2295, en el caso de Banca en Línea de 16 a 1004 y en los casos de compraventa de 603 a 5200, lo que evidencia un exponencial crecimiento de estos delitos. Por su parte, en Chile y República Dominicana también se detectan nuevas y rápidas tipologías destinadas a la comisión de este ilícito, sin embargo, las personas expertas de la región consultadas coinciden en que la principal tipología utilizada por los criminales es la ingeniería social a través de la cual se obtienen datos confidenciales de las y los usuarios para posteriormente cometer los ilícitos. Es decir que preponderantemente se estafan “personas” no “sistemas”, salvo en casos mucho más sofisticados, los que principalmente van dirigidos contra instituciones financieras o infraestructuras críticas, tales como el ataque bancario de Chile en 2018 o los ataques al Sistema de Pagos Financieros Interbancarios (SPEI) de México también del 2018.

De igual forma el experto Daniel Soto de la Fiscalía de Chile, precisó que existen diversos casos en los que las personas usuarias y especialmente las instituciones financieras deciden no denunciar a fin de evitar un desprestigio reputacional o en algunos casos se denuncia, pero no se le da continuidad al caso debido a que el único interés es contar con los elementos para obtener un resarcimiento derivado del incidente mediante el cobro de un seguro.

Finalmente, de acuerdo con el reporte “El lado oscuro de América Latina: criptomonedas, cárteles, *carding* y el incremento del cibercrimen”, en países de ALC, la comisión de fraudes a través de tecnologías de la información está ampliamente relacionada con estructuras del crimen organizado[9]. Lo anterior implica que el alcance de estos delitos conlleva no solamente una afectación de tipo económico, sino que tiene implicaciones mucho más amplias asociadas a la seguridad, al estado de derecho y la propia estabilidad del Estado.

[8] Informe de Ciberseguridad del Sistema Bancario Mexicano, Organización de los Estados Americanos, página 11, 2019, disponible en: http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

5. Marco jurídico sobre ciberdelito

5.1 Marco jurídico internacional

La comisión de delitos a través de sistemas informáticos, y a través del uso de tecnologías de información implican cada vez un riesgo más alto para los países de ALC ya que pueden ser cometidos no solamente por personas aisladas, sino también por grupos del crimen organizado con altos niveles de sofisticación y articulación, caracterizados por tener una base organizacional transnacional debidamente coordinada. Esto se traduce necesariamente en que el esclarecimiento de hechos, así como la investigación y persecución de este tipo de delitos requiere de un alto nivel de especialización técnica y jurídica, capacitación, y en particular una cooperación internacional eficiente y coordinada.

Existen diversos tratados internacionales para combatir el crimen organizado transnacional, tales como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos; instrumentos que son utilizados como mecanismos de cooperación por diversos países para prevenir y combatir aspectos relacionados con delincuencia organizada transnacional, primordialmente entre países miembros de la Organización de las Naciones Unidas (ONU). Sin embargo, el único tratado internacional existente relacionado con el combate al ciberdelito, y que actualmente es utilizado como un vehículo de cooperación internacional para combatirlo en forma más efectiva, es el Convenio sobre Ciberdelincuencia del Consejo de Europa, mejor conocido como el "Convenio de Budapest".

5.1.1 Convenio de Budapest

El Convenio de Budapest ha sido firmado y ratificado por un total de 66 países. A la fecha, únicamente ocho países de ALC lo han firmado y ratificado con ciertas reservas: República Dominicana, Panamá, Chile, Costa Rica, Argentina, Paraguay, Perú y Colombia. El Consejo de Europa invitó formalmente al gobierno de México en el año 2009 a acceder al protocolo de adhesión del Convenio de Budapest, ello considerando que México tiene el estatus de país observador ante el Consejo de Europa desde 1o. de diciembre de 1999.[10]

Para formar parte del Convenio de Budapest, el Consejo de Europa requiere que los países interesados primeramente reformen su legislación penal sustantiva y procesal para hacerla compatible, en la medida de lo posible, con las disposiciones de ese tratado. Asimismo, tomando en cuenta que el ciberdelito tiene una dimensión transnacional, el Convenio de Budapest requiere además que

[10] El lado oscuro de América Latina: criptomonedas, cárteles, carding y el incremento del cibercrimen, Insights, México país observador el Consejo de Europa https://www.coe.int/en/web/portal/mexico

los países incorporen medidas de cooperación internacional para suplirlas o complementarlas en caso de que un país no cuente con tratados de asistencia y cooperación mutua en materia penal, y en particular para dotar a las autoridades investigadoras con las herramientas y los mecanismos necesarios para poder llevar a cabo investigaciones. Entre los mecanismos y medidas que el Convenio de Budapest requiere que las autoridades del sistema de justicia implementen se encuentran: (i) la conservación rápida de datos informáticos almacenados; (ii) la revelación de datos conservados sobre tráfico; (iii) medidas de asistencia mutua con relación al acceso a datos informáticos almacenados; (iv) acceso transfronterizo a datos almacenados; (v) obtención en tiempo real de datos sobre el tráfico; (vi) asistencia mutua para la interceptación de datos sobre el contenido; y (vii) la creación de una red o punto de contacto 24/7 para centralizar las investigaciones y procedimientos relacionados con las solicitudes de datos informáticos y de asistencia mutua relacionados con investigaciones sobre ciberdelito.

Algunos países de la región ya cuentan con marcos jurídicos sustantivos penales para castigar y sancionar conductas relacionadas con ciberdelitos. Sin embargo, a la fecha, todavía son muy pocos países los que cuentan con las medidas de derecho procesal y de cooperación internacional en su legislación nacional para poder investigarlos de forma más efectiva y coordinada, y en particular con el apoyo de una comunidad de autoridades investigadoras, puntos y redes de contacto y cooperación de los proveedores de servicios de los países que forman parte del Convenio de Budapest.

La gran mayoría de los países de la región siguen utilizando y apoyándose en disposiciones de derecho procesal penal tradicionales por analogía para obtener y preservar evidencias electrónicas, para ordenar y ejecutar órdenes de allanamiento y secuestro de equipos y para procesar a los delincuentes, situación que no solamente establece serias limitantes y obstáculos para la investigación en el contexto tecnológico actual, sino también para la protección de derechos fundamentales de los investigados; aspectos que también deben ser debidamente abordados por los países que forman parte del Convenio de Budapest para evitar posibles dilaciones e impugnaciones en el proceso penal derivado de posibles violaciones a los derechos fundamentales de las partes investigadas.

En la región, únicamente la República Dominicana, Costa Rica, Chile y Argentina han establecido la Red 24/7 prevista en el Artículo 35 del Convenio de Budapest como órgano central de asesoramiento vinculado con la Fiscalía y los organismos de investigación policial para garantizar la asistencia jurídica inmediata relacionada con investigaciones penales en el contexto tecnológico y/o para solicitar pruebas contenidas en formato electrónico a otras autoridades a través de las redes de contacto de los 66 países que forman parte del Convenio de Budapest.

En opinión del Consejo de Europa y de algunas personas expertas sobre ciberdelito en la región, emprender reformas en materia procesal penal y establecer facultades y poderes procesales para que las autoridades investigadoras puedan ordenar y asegurar la preservación de evidencias en el proceso penal sujeto a las condiciones y salvaguardias previstas en el Art. 15 del Convenio de Budapest es una labor mucho muy compleja y especializada que requiere del apoyo de personas expertas y la creación y construcción de capacidades necesarias a través de una capacitación y entrenamiento continuo.

Derivado de la problemática que ha supuesto para algunos países para poder investigar, procesar y sancionar ciberdelitos el Consejo de Europa se ha enfocado desde el 2013 en fomentar y construir las capacidades necesarias para que los países (sin importar si forman parte del Convenio de Budapest) puedan combatir el ciberdelito efectivamente en distintos frentes. Actualmente, el Consejo de Europa, a través de su Oficina del Programa sobre Ciberdelito (C-PROC) en Rumania, administra diversos proyectos cuyos fondos provienen principalmente de instituciones y organismos de la Unión Europea y de contribuciones voluntarias de algunos países que

ya forman parte del Convenio de Budapest que son utilizados para apoyar a países a reformar sus marcos jurídicos penales sustantivos y procesales, entre otras muchas actividades incluida la capacitación de las autoridades investigadoras del sistema de justicia.

El proyecto más relevante para países de ALC es el Proyecto GLACY + (*Global Action against Cybercrime Extended)* que tiene como principal objetivo fortalecer las capacidades de los países para mejorar y aplicar la legislación sobre ciberdelitos y evidencias electrónicas, y ayudarlos a mejorar sus capacidades para fortalecer la cooperación internacional en la materia. A través del GLACY+, se ha apoyado a países como Panamá, Guatemala, Chile, Costa Rica, República Dominicana, Belice, Paraguay, Ecuador y Colombia para asistirlos en la redacción de legislación sobre ciberdelito y evidencia electrónica, y para ayudarlos a encaminar reformas en materia procesal penal consistentes con las disposiciones del Convenio de Budapest. También, se han llevado a cabo diversas actividades de capacitación y formación de las autoridades del sistema de justicia penal encargadas de investigar, procesar y sancionar ciberdelitos (policías, fiscales y personas juzgadoras) y el fortalecimiento de las capacidades de respuesta de la Red 24/7 en países como República Dominicana, Costa Rica y Chile.

5.1.1.1 Implicaciones de la adhesión al Convenio de Budapest

De las entrevistas sostenidas con los personas expertas, algunos mencionaron que la adhesión al Convenio de Budapest en ocasiones se encuentra sobrevalorada ya que no implica un cambio interno per-se, sin embargo la mayoría destacó la importancia del Convenio de Budapest como un instrumento relevante de cooperación internacional que puede ser de gran utilidad para los países de ALC para mejorar su legislación sustantiva y procesal en materia penal y para llevar a cabo en forma más eficiente y coordinada las investigaciones relacionadas con ciberdelitos.

Al respecto el experto Marcos Salt, académico argentino, destacó que si bien el Convenio de Budapest no puede considerarse como una solución única, si es un gran referente en cuatro principales aspectos: i) como una herramienta que permite establecer una regulación mínima de carácter sustantivo, procesal y de cooperación internacional, ii) como una herramienta para tener acceso a mecanismos eficaces de capacitación, iii) como un detonador de la red 24/7 que permite tener acceso a cooperación para la preservación y acceso a evidencias en otros países de manera inmediata, iv) como una herramienta de carácter político, esto considerando que los países dan mucho mejor atención y cooperación con los países que forman parte del Convenio de Budapest. Indicó, que la adhesión al Convenio de Budapest es un elemento fundamental para la investigación y persecución del ciberdelito.

El fiscal experto de Argentina, Horacio Azzolin, indicó que aún y cuando ese país ya forma parte del Convenio de Budapest desde 2018, ha identificado que todavía existen algunos problemas de cooperación con las y los proveedores de servicios para que las fiscalías de ese país puedan obtener correctamente, en tiempo y forma, información y datos relacionados con investigaciones penales en curso. En opinión de este experto, los tiempos y las medidas de cooperación para obtener datos informáticos almacenados no se han flexibilizado ni reducido desde que Argentina forma parte del Convenio de Budapest. Es importante destacar que, en opinión de ese experto, la Adhesión al Convenio de Budapest no implicó, en sí mismo, un cambio sustancial en la mejora de la investigación y persecución de cibercriminalidad en Argentina, sin embargo, si fue sumamente positivo como una medida complementaria a la inercia interna de voluntad política y construcción de capacidades para investigar estos delitos. **Sin embargo, considera que para países como México la adhesión al Convenio puede ser muy efectiva ya que la obligación de dar cumplimiento a los requerimientos internacionales puede convertirse en un motor que impulse la voluntad política y la construcción de capacidades internas para la**

investigación y persecución de estos delitos. En el ámbito operativo, soslayó que, si bien el Convenio de Budapest les ha servido como un vehículo en el ámbito de cooperación con países de Europa y Estados Unidos dicho instrumento es inoperante para la cooperación con países tales como China, lugar donde se generan y cometen un número importante de ataques.

Por su parte, Carlos Leobardo de República Dominicana indicó que este país ha recibido importantes beneficios por formar parte del Convenio de Budapest, especialmente en el ámbito de capacitación, acceso a cooperación internacional y al tener un lugar dentro del Comité de Expertos del Convenio de Budapest (T-CY Committee) lo que permite la participación de ese país en la creación y negociación de protocolos adicionales y mejoras operativas continuas.

Una de las personas expertas entrevistadas de origen mexicano hizo énfasis en el problema de coordinación entre la policía y la fiscalía para priorizar y eficientizar las investigaciones relacionadas con ciberdelitos. En opinión de este experto, sería ideal que las autoridades investigadoras se fortalezcan a través del entrenamiento y cuenten con las capacidades suficientes para solicitar cooperación con otros países. Destacó que el Convenio de Budapest podría ayudar a México a fortalecer las capacidades investigadoras, y en particular a mejorar la asistencia mutua y cooperación internacional a través de la creación y formalización de la Red 24/7 dentro del Ministerio Público. Asimismo, la Unidad de Investigaciones Cibernéticas de la Fiscalía General de la República indicó que el hecho de que México no forme parte del Convenio de Budapest, implica una limitante para acceder a esquemas de cooperación de evidencia digital transfronteriza.

Se destacó que la firma y adhesión al Convenio de Budapest es resultado de la voluntad política y el interés particular de los Estados para generar mecanismos eficaces y eficientes en la investigación de ciberdelitos y la preservación y obtención de evidencias que puede servir como un detonador para generar mejoras en el ámbito legislativo y creación de políticas públicas para combatir efectivamente este tipo de delitos a nivel nacional. Sin embargo, como se señaló en párrafos anteriores, el proceso de adhesión al Convenio de Budapest puede durar algunos años, y dependerá de las circunstancias específicas de cada país, tales como tener una legislación sustantiva y procesal, medidas de cooperación internacional adecuadas, facultades y poderes necesarios para que las autoridades correspondientes puedan investigar ciberdelitos, y que el país esté en condiciones de facilitar la cooperación internacional con autoridades y puntos de contacto para investigar ciberdelitos en forma efectiva.

5.1.2 Resolución de FOPREL para legislar en materia de ciberdelito

Durante la XII Reunión de la Comisión Interparlamentaria de Seguridad Ciudadana y Administración de Justicia y la IX Reunión de la Comisión Interparlamentaria de Asuntos Internacionales e Integración del Foro de Presidentes de Poderes Legislativos de Centroamérica y la Cuenca del Cari-be (FOPREL), realizada en julio de 2019 en la sede de la Asamblea Legislativa en la ciudad de El Salvador, el Consejo de Europa, a través del Proyecto GLACY +, junto con los presidentes de los 10 países miembros de FOPREL aprobaron una Resolución muy relevante que recomienda a los países miembros la aprobación de legislación para combatir el ciberdelito.

La Resolución de FOPREL vincula a los representantes parlamentarios de 10 países (Belice, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, México, Panamá, Puerto Rico y República Dominicana) para redactar y aprobar legislación sustantiva y procesal en materia penal para poder combatir eficazmente el ciberdelito y poder establecer medidas para su detección, investigación, persecución y sanción a nivel nacional y facilitar la cooperación internacional con otros países con base en las disposiciones del Convenio de Budapest. Dicha Resolución también recomienda al Congreso Mexicano “llevar a cabo

las gestiones necesarias para definir la adhesión al Convenio de Budapest dentro del plazo de vigencia de la invitación del Consejo de Europa".

De los 10 países miembros de FOPREL, únicamente República Dominicana, Costa Rica y Panamá forman parte del Convenio de Budapest; países que aunque ya tienen legislación sustantiva y procesal, todavía no han encaminado reformas legislativas en materia procesal y de cooperación internacional para hacerlas compatibles con las disposiciones del Convenio de Budapest y las recomendaciones del Comité del Convenio de Budapest (T-CY) (del cual forman parte los estados que ya han ratificado el Convenio de Budapest y cuyo propósito es facilitar el uso y la implementación más efectiva del Convenio de Budapest y el intercambio de información entre los países parte).

Vale la pena destacar que Belice aprobó en 2020 una ley sobre ciberdelitos (*Cybercrime Act* 2020[11]) que incorpora la gran mayoría de las disposiciones de derecho sustantivo, derecho procesal y cooperación internacional previstas en el Convenio de Budapest, con lo cual se facilitará la futura adhesión de ese país a ese tratado internacional.

5.1.3 Otros instrumentos

El Convenio Iberoamericano sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Ciberdelincuencia creado por la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) es un instrumento cuyo objetivo es establecer disposiciones de carácter procesal y de intercambio de información y de actividades de solicitudes de asistencia y cooperación entre los ministerios de justicia de diversos países. Este instrumento es aplicable a algunos países de América Latina, España y Portugal, aunque no tiene el carácter y la fuerza vinculatoria de un tratado internacional. México forma parte de este instrumento desde el 9 de junio de 2014.

Se considera que este instrumento no ha tenido una aplicación práctica en los países que ya lo firmaron, ya que, derivado de una investigación realizada, no se encontró algún proyecto de construcción de capacidades administrado por algún país u órgano de justicia miembro del COMJIB que pueda ayudar a los miembros a implementarlo eficientemente a nivel regional.

5.2 Legislaciones, jurisdicción y competencias en ALC: ciberdelito y fraude financiero

A lo largo de esta sección se explora la legislación existente en algunos países referentes de ALC así como las cuestiones de jurisdicción y competencias y el contexto legislativo en México.

5.2.1 Contexto de Argentina, República Dominicana, Colombia y Chile

Argentina es uno de los países de la región con mayor desarrollo de investigaciones relacionadas con ciberdelito. Argentina se adhirió al Convenio de Budapest desde el 5 de junio de 2018 y cuenta con cierto grado de armonización legislativa en materia sustantiva para la investigación y persecución de estos delitos, incluido el fraude cibernético en el ámbito financiero incorporado al Código Penal mediante las reformas a la Ley N° 25.930 B.O. 21/9/2004 y la Ley N° 26.388, B.O. 25/6/2008, respectivamente.

La República Dominicana fue el primer país de ALC en acceder y ratificar el protocolo de acceso a la Convención de Budapest el 7 de febrero de 2013 y actualmente forma parte de los países prioritarios del Proyecto GLACY+ del Consejo de Europa, Asimismo, es de los pocos países de ALC que cuenta con una legislación independiente para investigar, perseguir y sancionar delitos cibernéticos, la *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología* vigente desde el 18 de enero de 2007. Esa ley tipifica la gran

[11] La Ley sobre Ciberdelitos de Belice de 2020 (Cybercrime Act 2020) se encuentra en: https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf

mayoría de las conductas y delitos previstos en el Convenio de Budapest. Entre las disposiciones más relevantes relacionadas con el fraude cibernético en el ámbito bancario se encuentran las siguientes: Art. 14 relacionado con obtención ilícita de fondos, créditos o valores a través del constreñimiento de servicios financieros cibernéticos, electrónicos, telemáticos o de telecomunicaciones; Art. 14 también relacionado con transferencia electrónica ilícita de fondos a través de códigos de acceso o de cualquier otro mecanismo; y Art. 15 sobre estafa informática.

Al respecto el experto de República Dominicana [Carlos Leobardo] precisó que actualmente la *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología* se encuentra en un proceso de reformas con dos principales finalidades. La primera es incluir nuevos tipos penales que no existían cuando se publicó la *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología* y la segunda es reducir el uso de tecnicismos en la legislación con el objeto de adecuar la norma en la investigación y persecución de los delitos. El experto recomendó que los países eviten el uso de tecnicismos de tecnología en sus legislaciones, debido a que ello puede implicar que las normas sean sumamente complejas y que puedan perder vigencia a causa de los avances y cambios tecnológicos. Asimismo, resulta destacado que en este nuevo proceso de reforma se ha invitado a participar activamente a los proveedores de servicios de comunicaciones, en el desarrollo de esta nueva legislación.

En relación con el marco jurídico para investigar, procesar y sancionar ciberdelitos, Colombia cuenta con la Ley 1273 de 2009, por medio del cual se adicionó al Código Penal con un Título VII BIS denominado de “De la protección de la Información y de los datos” y se adiciona al Artículo 58 del Código Penal con un numeral 17 para castigar y sancionar conductas cometidas a través de medios informáticos, electrónicos o telemáticos; y se adicionó al Artículo 37 del Código de Procedimiento Penal con un numeral 6 para que las y los Jueces Penales Municipales puedan conocer de los delitos contenidos en el Título VII BIS del Código Penal.

La Corte Constitucional de Colombia pronunció la Sentencia C-224/19 con fecha 22 de mayo de 2019 en donde analizó la asequibilidad de la incorporación de la Ley 1928 de 2018 y el Convenio de Budapest a la legislación nacional. La Corte Constitucional concluyó y resolvió que ambos instrumentos son plenamente respetuosos de las disposiciones constitucionales. Posteriormente, Colombia ratificó el protocolo de acceso a la Convención de Budapest el 16 de marzo de 2020. El Consejo de Europa, a través del Proyecto GLACY+, llevó a cabo en marzo de 2021 una evaluación inicial para conocer el estado actual de la legislación sobre ciberdelito en relación con las disposiciones del Convenio de Budapest, así como las capacidades de investigación de las autoridades de justicia de ese país y tiene proyectado organizar diversas actividades durante 2021 para apoyar a ese país a reformar su marco jurídico sustantivo y procesal, así como otras actividades relacionadas con la capacitación y entrenamiento de las autoridades investigadoras.

Chile fue uno de los primeros países de ALC en promulgar una legislación para sancionar y castigar delitos cibernéticos en 1993. La Ley 19,223, en vigor desde el 7 de junio de 1993. Tipifica en sólo cuatro artículos algunas figuras penales relativas a ciertas conductas relacionadas con delitos cibernéticos. Chile fue el tercer país de ALC en acceder y ratificar el Convenio de Budapest en abril de 2017 y actualmente forma parte de los países prioritarios del Proyecto GLACY+ del Consejo de Europa. El Senado Chileno aprobó en 2019 un proyecto de ley sobre ciberdelito y evidencia electrónica (Boletín No.12,192-25) que implementa la gran mayoría de las disposiciones sustantivas y procesales del Convenio de Budapest; sin embargo, ese proyecto de ley se encuentra aún pendiente de ser aprobado en la Cámara de Diputados y por el Poder Ejecutivo de Chile.

En cuanto a los delitos de fraude cibernético en el ámbito financiero, Chile cuenta con la Ley 21,234 de 9 de mayo de 2020. El Artículo 7º. de la Ley 21,234 contempla, entre otras, la responsabilidad de los Titulares o Usuarios de Tarjetas de Pago y

Transacciones Electrónicas, Hurto, Robo o Fraude y sanciona como delito la falsificación de tarjeta de pago; el uso, venta, exportación, importación o distribución de tarjetas de pago falsificadas; utilizar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas; suplantar la identidad del titular o usuario frente al emisor, operador o comercial afiliado para obtener la autorización que sea requerida para realizar transacciones. Asimismo, el Artículo 9º. de la Ley 21, 234 establece que las penas previstas en el Art. 7º de dicha ley se aplicarán sin perjuicio de las eventuales sanciones que también corresponda aplicar por los delitos contemplados en la Ley Nº 19.223, o aquella que la modifique, reemplace o sustituya en materia de delitos cibernéticos o ciberdelincuencia.

El experto Daniel Soto, de la Fiscalía Nacional de Chile, enfatizó la importancia de contar con un marco jurídico sustantivo y procesal efectivo para la investigación y persecución de los delitos, destacando que en el caso de Chile no existe un tipo penal que sancione de manera específica el fraude financiero cibernético, sino que la clasificación de esta conducta se penaliza como una estafa y espionaje cibernético. Sin embargo, Chile se encuentra en un actual proceso de reformas legales con la finalidad de establecer tipos penales mucho más claros y específicos. Lo anterior, debido a que el fraude financiero cibernético es un delito altamente complejo por lo que se considera que existen elementos que pueden quedarse fuera cuando se utilizan sólo tipos penales genéricos. No obstante, el experto indico que es muy relevante que la especialización en términos legales no debe implicar conceptos técnicos de tecnología, debido a que eso abona a la falta de claridad y certeza jurídica, así como a la pérdida de vigencia en muy corto plazo.

De todo lo anterior, es importante destacar que contar con una legislación clara y específica es un elemento crucial para garantizar la eficacia y eficiencia de la investigación y persecución de los ciberdelitos y en especial del fraude financiero cibernético. Además, si bien se recomienda tener legislación especializada, las personas expertas reiteran la relevancia de evitar conceptos demasiado técnicos en las normas. Finalmente, cabe destacar que, pese a los importantes avances legislativos de los países de la región anteriormente analizados, resulta evidente que la constante actualización y mejora de su marco jurídico, especialmente en el ámbito sustantivo, resulta fundamental para la efectividad en la persecución penal.

Otro de los aspectos de mayor relevancia en el análisis de los retos y complejidades que comparten los países de la región en la investigación y persecución del fraude financiero cibernético, es la jurisdicción y competencia, ello desde el ámbito nacional e internacional. En el plano nacional, el caso de Argentina resulta ser sumamente relevante debido a que, al ser un Estado Federado, conformado por una justicia de carácter federal y otras diversas de carácter local, la investigación de este tipo de delito que se caracteriza por su extraterritorialidad y volatilidad implica altas complejidades. Por ejemplo, [Franco Pilnik] el Fiscal Especializado en Cibercriminalidad de la Provincia de Córdoba en Argentina, indicó que los problemas de jurisdicción y competencia continúan siendo un obstáculo importante para la investigación del fraude financiero, en su caso, con la recepción de casos que incluso duran mucho tiempo en una provincia diversa y que posteriormente son trasladados a su jurisdicción, lo cual ya hace prácticamente imposible su esclarecimiento debido a la pérdida de la evidencia a causa de las problemáticas de competencia. Como respuesta a esta problemática, el experto considera que una opción es la definitiva federalización de estos casos ya sea en todos o en determinados supuestos, y en su caso, esquemas efectivos de coordinación, debidamente institucionalizados y que no sólo dependan de la buena voluntad de los operadores sino de elementos formales de coordinación. Por ejemplo, mediante el establecimiento de canales de coordinación digital, que garanticen el envío rápido y seguro y la recepción de evidencia digital de manera inmediata.

Asimismo, el experto argentino de la Universidad de Buenos Aires (UBA) [Macos Salt] coincide en que las cuestiones de competencia son uno de los mayores retos que enfrenta no solamente Argentina, sino

también muchos otros países, pero además que esta situación es mucho más grave aún en países como México en los que además de tener un sistema federal, existen además legislaciones específicas para cada entidad federativa, lo que torna sumamente compleja la definición de jurisdicción y competencias, no sólo desde el ámbito operativo, sino también desde la perspectiva jurídica. Como alternativas a esta problemática, el experto de la UBA propone como una opción el modelo Norteamericano, en el cual se clasifican los ciberdelitos del ámbito federal, por ejemplo cuando se trata de delitos de mayor impacto o cuantía, como ataques a las estructuras críticas o cuando se afectan diversos estados, así como también el modelo establecido por Unión Europea en el cual, se crean equipos conjuntos de investigación (ECI) que cooperan en la investigación del hecho para posteriormente judicializarse en alguna jurisdicción en específico.

En el caso de Chile, de acuerdo con el experto de la Fiscalía Nacional de Chile, si bien no se tienen problemáticas de jurisdicción a nivel interno, si ocurre esta problemática en el ámbito internacional, toda vez que es recurrente que las direcciones IP desde las que se comete un delito se encuentren en diverso lugares, pese que los efectos del delito tengan repercusiones en Chile, por lo cual se estima que deben establecerse medidas efectivas y rápidas de cooperación internacional, debido a las complejidades de la comisión del delito.

5.2.2 Contexto de México

México no forma parte aún del Convenio de Budapest. El Consejo de Europa, a través de la Dirección sobre Ciberdelitos y Derechos Humanos en Estrasburgo ha invitado formalmente a México desde el año 2009.

En junio de 2014, México se adhirió al Convenio Iberoamericano sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Ciberdelincuencia creado por la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB). Sin embargo, de las personas expertas consultadas, no se encontró que si exista evidencia acerca de sus beneficios a nivel operativo.

Respecto a la legislación vigente, México tiene una particularidad muy relevante ya que cuenta con un Código Penal Federal (CPF) que aplica para los delitos que se cometen a nivel federal, y, a su vez, cada entidad federativa cuenta con un Código Penal. En el ámbito procesal, existe un sólo Código Nacional de Procedimientos Penales (CNPP), mismo que sí es aplicable en las 32 entidades federativas. El Código Penal Federal prevé en su Título Noveno, Capítulo II, los delitos de acceso ilícito a sistemas y equipos de informática. Asimismo, algunas entidades regulan en sus códigos locales la investigación y sanción de otro tipo de conductas, tales como la suplantación de información.

Cabe destacar que en el ámbito del fraude financiero cibernético se contempla en el CPF el delito de Fraude de manera genérica, que puede ser cometido a través de cualquier medio. Asimismo, la Ley de Instituciones de Crédito establece diversos tipos penales que pueden ser consideradas como fraudulentas, ya sea tanto a instituciones financieras como a personas usuarias del sistema financiero y que pueden ser cometidos a través de tecnologías de la información (Arts. 112 quáter, 112 sextus, 113 Bis). Aunado a ello, la Ley para Regular las Instituciones de Tecnología Financiera (IFT) prevé sancionar como delito (Art. 133) cuando sin autorización se obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras.

Diversas entidades federativas han establecido en sus Códigos Penales Locales, tipos penales con la finalidad de sancionar de manera específica el fraude cometido mediante el acceso ilícito a sistemas de informática o programas del sistema financiero, con la finalidad de obtener un beneficio indebido. Entre éstas se encuentran la Ciudad de México (Art. 231 fracción XIV), Chihuahua (Art. 266 bis), Sinaloa (Art. 217), Durango (Art. 346 fracción, XXIII), Veracruz (Art.

217 fracs. VII y XI), Colima (Art. 202 fracciones III, IV VI, VI y VII), Tlaxcala (Art. 341), Puebla (Art. 404 fracción, XIX), Chiapas (Art. 304 fracción. XXIV) y Campeche (Art. 207 fracción. XIV).

Esta particularidad supone importantes retos y desafíos para la investigación y persecución de los delitos, ya que hay casos y supuestos en los que las líneas entre la aplicación del modelo federal y el modelo local no resultan tan claras. Es de destacarse que si bien hoy se cuenta con tipos penales especiales en la Ley de Instituciones de Crédito así como la tipificación del delito de fraude genérico en el Código Penal Federal e incluso algunos tipos penales de fraude equiparado en las federativas, el marco jurídico vigente presenta importantes áreas de oportunidad para lograr la adecuada y precisa clasificación del delito de fraude financiero cibernético así como para la definición de la competencia Este aspecto fue especialmente detallado con la información comentada por las y los representantes de la CONDUSEF quienes indicaron que el marco jurídico del fraude financiero a nivel nacional es diverso sería ideal homologar el tipo penal tanto a nivel local como federal, a efecto de mejorar las acciones de investigación y persecución de estos delitos y reducir las problemáticas actuales que en materia de competencia enfrentan las personas usuarias. Un ejemplo de ello es que algunas de las personas usuarias que como personas físicas presentan una denuncia ante la Fiscalía General de la República (FGR) por ser víctimas de un fraude financiero cibernético, en algunos casos experimentan limitaciones en este proceso, tales como la negativa de la recepción de su denuncia en el ámbito federal, y posteriormente en el ámbito local. Lo anterior evidencia la necesidad de no contar con las acciones para homologar el marco jurídico homologado sustantivo y procesal en materia de investigación y persecución de estos delitos, que contemple soluciones efectivas en beneficio de las personas usuarias.

Respecto a la normatividad procesal, como se mencionó anteriormente, el CNPP no prevé todas las medidas que permitan a las autoridades investigadoras ordenar la preservación de pruebas y evidencias que puedan ser útiles para investigar ciberdelitos, incluidos delitos relacionados con el fraude cibernético a nivel nacional. Las medidas de derecho procesal previstas en el Convenio de Budapest (Arts. 14 a 22), tales como la conservación rápida de datos informáticos almacenados, la conservación y revelación parcial rápidas de datos sobre tráfico, registro y confiscación de datos informáticos almacenados y la obtención en tiempo real de datos sobre tráfico y la interceptación de datos sobre el contenido, no se encuentran completamente previstas en la normatividad procesal mexicana.

No obstante, es importante mencionar que el último párrafo del Art. 303 del CNPP establece que las y los procuradores/fiscales podrán requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. Asimismo, el Art. 381 del CNPP prevé la posibilidad de que los tribunales en materia penal puedan admitir como prueba, evidencias y datos contenidos en formato digital, electrónico, óptico o contenido en cualquier otro medio tecnológico, siempre y cuando se faciliten los medios necesarios para su ejecución y reproducción, pero dicha disposición no establece las facultades y poderes necesarios para que las autoridades investigadoras, tales como la o el Ministerio Público, puedan ordenar la conservación y preservación de datos informáticos almacenados.

Asimismo, la Unidad de Investigaciones Cibernéticas de la Agencia de Investigación Criminal de la Fiscalía General de la República (FGR) indicó que en el marco de la Conferencia Nacional de Procuración de Justicia de 2018 celebrada en la Ciudad de México, se aprobó una guía que adecúa las reglas de cadena de custodia para los casos de evidencia digital[12]. Esta guía técnica es de flexible acceso y su adecuada aplicación puede generar una mejora sustancial en el manejo de evidencias digitales tanto en el ámbito federal como local.

[12] 1° Sesión Ordinaria 2018 de la Zona Centro de la Conferencia Nacional de Procuración de Justicia. Ciudad de México, 9 de marzo del 2018. Recuperado de 1ª Sesión Ordinaria 2018 de la Zona Centro de la Conferencia Nacional de Procuración de Justicia.pdf (cnpj.gob.mx) http://www.coahuilatransparente.gob.mx/disp/documentos_disp/GU%C3%8DA%20T%C3%89CNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf

6. Mejores prácticas en América Latina y el Caribe

Con el objetivo de identificar las acciones implementadas en países de ALC para hacer más eficaz y eficiente la investigación de estos delitos y que puedan ser compartidas con otros países de la región como México, se realizó un análisis de buenas prácticas en los siguientes países: Argentina, Colombia, República Dominicana y Chile. La selección de estos países fue con base en las experiencias compartidas por las personas expertas consultadas sobre algunos países con trabajos destacados de la región y que además cumplieran con al menos dos de los siguientes criterios:

- Que fueran países de América Latina adheridos al Convenio de Budapest
- Que hubieran generado acciones para dar cumplimiento al Convenio de Budapest a nivel interno
- Que preferentemente contarán con un sistema penal de corte acusatorio
- Que tuvieran similitudes con México en cuanto a problemáticas delictivas
- Que fueran países con esquema federal como México

Países	Adhesión Convenio de Budapest	Acciones internas	Sistema penal Acusatorio	Similitud delictiva con México	Estado Federado
Argentina	✓	✓			✓
República Dominicana	✓	✓			
Colombia	✓	✓	✓	✓	
Chile	✓	✓			

Tabla 1. Elaboración propia con información extraída de las legislaciones internas de Argentina, Colombia, República Dominicana y Chile.

Se destaca que, para este primer reporte exploratorio, se consideró fundamental hacer el análisis comparado con países de la región con estas similitudes antes de realizar un análisis comparativo con realidades distintas tales como países de Europa, ya que estas realidades pueden establecer un panorama mucho más concreto sobre la situación en la que se encuentra México respecto de países en circunstancias similares, incluso a nivel cultural en cuanto al actuar de las personas funcionarias públicas.

Las buenas prácticas se conceptualizaron como acciones que implican una mejora en la investigación y persecución de estos delitos desde los ámbitos legislativos, de política pública, construcción de capacidades, coordinación interna y externa, técnicas de investigación especializada y cooperación internacional.

6.1 Análisis de mejores prácticas por país

A continuación, se describen las mejores prácticas identificadas en los distintos países objeto de estudio: Argentina, Colombia, República Dominicana y Chile.

6.1.1 Argentina

ASPECTO	ANÁLISIS
Buena práctica	Investigación y persecución de fraude financiero cibernético
Información adicional de referencia	Entrevista con Horacio Azzolin Fiscal Federal de Delitos Informáticos en Argentina (UFECI)
Elementos relevantes	Una parte fundamental para la adecuada investigación y persecución de este delito es contar una visión sistémica por su impacto a nivel global, y no sólo en su dimensión individual. Por ello, se requiere una perspectiva integral que considera el combate a la ciberdelincuencia como un pilar para el impulso económico y el combate al crimen organizado, lo cual inicia con la atención prioritaria a nivel nacional. Las acciones más representativas llevadas a cabo por Argentina han sido: 1. Nuevo marco legal. Implementaron reformas legislativas sustantivas y procesales para contar con mecanismos eficientes para la investigación de estos delitos. Si bien uno de los impulsos para estas reformas fue la adhesión al Convenio de Budapest, estas reformas se implementaron y se aplicaron mucho tiempo antes de su adhesión. 2. Liderazgo. El liderazgo de una institución del Estado es fundamental para lograr construcción de capacidades de investigación y persecución del delito. Este liderazgo fue asumido por la Fiscalía General 3. Construcción de capacidades. Se generó un alto nivel de especialización y capacitación para fiscales, policías y personal pericial. Asimismo, se generaron laboratorios altamente especializados principalmente al interior de las policías y algunos (en menor medida) al interior de las fiscalías en las diversas provincias. En todas las áreas incluso en las no especializadas se busca tener fiscales expertos y expertas en el manejo de evidencia digital que puede ser aplicable a cualquier delito 4. Coordinación. 1. Nacional: Argentina es un estado Federado por lo que la coordinación entre autoridades federales y locales ha sido fundamental. 2. Interinstitucional: debido a que la mayoría de los servicios forenses dependen de las policías se ha generado una gran cooperación entre fiscales, policías y personal pericial. 3. Internacional: se han generado mecanismos de cooperación con diversos países, especialmente con aquellos que forman parte del Convenio de Budapest Se puede identificar como factores determinantes y complementarios en la investigación los siguientes: • Argentina tiene la Unidad Fiscal Especializada en Ciberdelincuencia, a nivel federal, encargada de asesorar a las fiscalías de otros estados y provincias en la investigación de delitos cibernéticos graves o de alto impacto conforme al Código Penal vigente, incluido el fraude cibernético en el ámbito financiero y bancario • El 1º de marzo de 2020, el Ministerio Público Fiscal de Buenos Aires, creó la Unidad Fiscal de Delitos y Contravenciones Informáticas (UFEDyCI), cuyo propósito es dar una respuesta inmediata a los casos delictivos que ingresan en el ámbito de la justicia penal de la ciudad de Buenos Aires. La UFEDyCI tiene competencia exclusiva para conocer de delitos cibernéticos y contravenciones exclusivamente en la Ciudad de Buenos Aires conforme al Código Penal • Conferencia de Procuradores. Las decisiones colegiadas que se toman a través de las conferencias de procuradores que agrupa a la federación y las provincias se ha convertido en un mecanismo eficaz de coordinación • Grupos de coordinación informal. Actualmente, todos y todas las y los fiscales en el ámbito federal y local tienen una estrecha relación directa de coordinación incluso mediante chat en aplicaciones electrónicas • Recepción única. A fin de incentivar la denuncia ciudadana, las y los fiscales de cualquier competencia reciben cualquier denuncia en la materia y la canalizan a la fiscalía correspondiente

Tabla 2. Elaboración propia con información extraída de entrevista a Horacio Azzolin Fiscal Federal de Delitos Informáticos en Argentina (UFECI) en enero de 2021.

6.1.2 República Dominicana

ASPECTO	ANÁLISIS
Buena práctica	Investigación de ciberdelitos en República Dominicana
Información adicional de referencia	Claudio Peguero, Dirección de la Policía Cibernética de la Policía Nacional. "Seminario de la Unión Europea y Consejo de Europa sobre Ciberdelito en América Latina"
Elementos relevantes	A partir del primer gran caso de cibercriminalidad detectado en República Dominicana en 2003 se ha convertido en un tema de atención nacional prioritaria. Se identifican como los elementos más destacados los siguientes: 1. **Nuevo marco legal**. El país tiene una legislación independiente y robusta para investigar, perseguir y sancionar delitos cibernéticos: Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología vigente desde el 18 de Enero de 2007 2. **Apoyo internacional**. El primer país de ALC en adherirse y ratificar el protocolo de acceso a la Convención de Budapest el 7 de Febrero de 2013. Además, actualmente forma parte de los países prioritarios del Proyecto GLACY+ del Consejo de Europa. Esto le ha permitido contar con apoyos para la construcción de capacidades a nivel interno en materia de capacitación de las y los policías, jueces y fiscales 3. **Cooperación Internacional.** Tiene conformada la Red 24/7 ante tres organismos internacionales (G7, INTERPOL y Consejo de Europa) la cual se utiliza para centralizar la solicitud de pedidos de preservación de información y de asistencia mutua en el ámbito penal, incluidas las investigaciones relacionadas con ciberdelitos. Lo anterior, genera mecanismos de coordinación con diversos países, especialmente con países con los que no tiene otro tipo de instrumentos de asistencia legal como Estados Unidos 4. **Cobertura Nacional**. Pese a que en un inicio las unidades especializadas sobre cibercriminalidad se establecieron en Santo Domingo y Santiago, durante 2020 se ha impulsado su ampliación a una mayor cobertura nacional a fin de generar mecanismos mucho más eficaces 5. **Prevención**. Adicionalmente a la construcción de capacidades para la investigación y persecución del delito, durante 2020 la Policía Nacional se ha enfocado en ampliar una estrategia para impulsar la prevención ante la comisión de estos delitos

Tabla 3. Elaboración propia con información extraída del "Seminario Ciberdelincuencia y justicia Penal en el Ciberespacio" organizado por GLACY+ Project y la Unión Europea el 22 de julio de 2020.

6.1.3 Colombia

ASPECTO	ANÁLISIS
Buena práctica	Investigación de ciberdelitos en Colombia
Información adicional de referencia	Entrevista al experto Andrés Velázquez
Elementos relevantes	A partir del primer gran caso relacionado con evidencia digital en 2008, el tratamiento de esta evidencia se volvió un tema de atención nacional prioritaria que impulso la investigación y persecución de ciberdelitos. Se identifican como los elementos más destacados los siguientes: 1. **Nuevo marco legal.** Creación de la Ley 12-73 de 2009 que impulsó un marco legal mucho más robusto, especialmente en materia sustantiva 2. **Liderazgo colectivo.** Diversas instituciones policiales y de inteligencia generaron áreas especializadas para investigación, tales como la Dirección de Policía de Inteligencia, el Departamento Administrativo de Seguridad, y la Dirección General de la Policía Judicial 3. **Capacitación.** La capacitación fue un factor clave, no sólo para unidades especializadas, sino que se generó un modelo de capacitación uniforme para todas las policías de investigación con el fin de generar las primeras acciones necesarias frente al conocimiento de una evidencia digital. Esto especialmente se fortaleció y convergió con las capacitaciones y metodologías aplicadas en el marco del sistema penal acusatorio. Asimismo, existe una permanencia en el servicio lo que garantiza persistencia en el proyecto 4. **Definición de roles y permanencia.** Existe un claro entendimiento entre las labores de investigación de la policía con auxilio de servicios periciales que asumen la responsabilidad de su investigación, y el rol del fiscal como abogado encargado de presentar el caso ante tribunales 5. **Capacidades técnicas.** Se adquirieron herramientas técnicas eficaces y eficientes para la investigación de estas investigaciones

Tabla 4. Elaboración propia con información extraída de entrevista a Andrés Velázquez experto en ciberseguridad en enero de 2020.

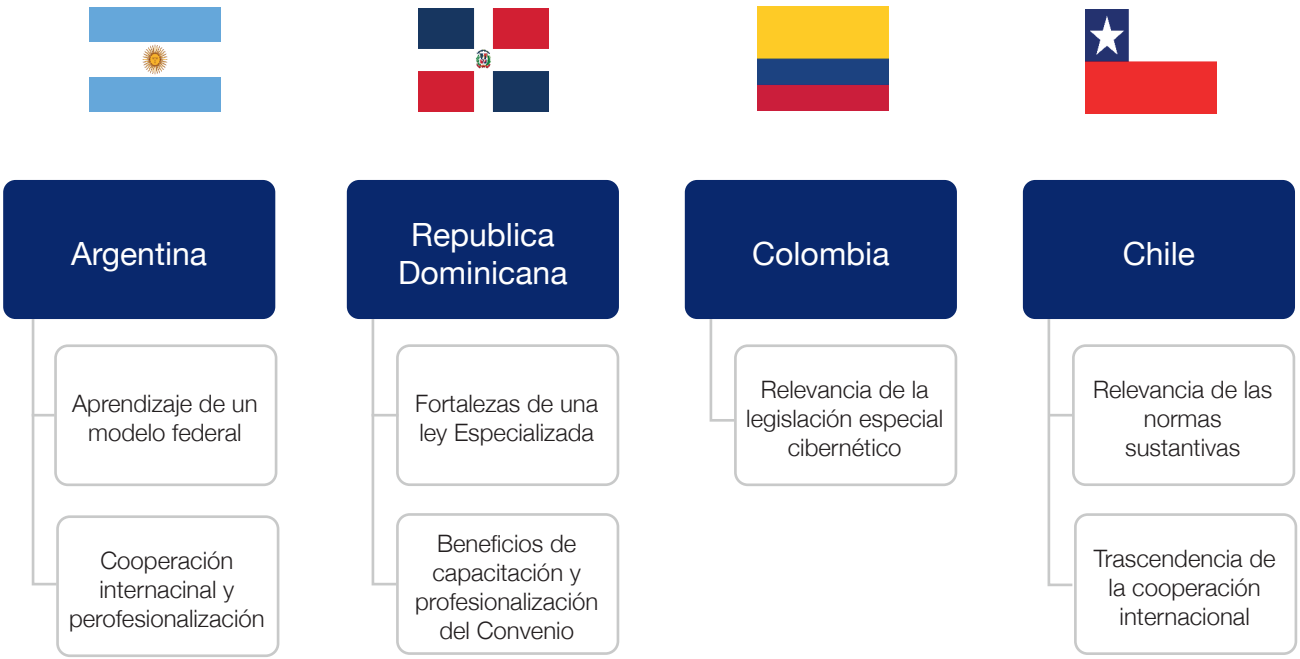
6.1.4 Chile

ASPECTO	ANÁLISIS
Buena práctica	Investigación de ciberdelitos en Chile
Información adicional de referencia de referencia	Entrevista al experto Andrés Velázquez
Elementos relevantes	Chile fue uno de los pioneros a nivel de América Latina en cuanto al inicio de construcción de capacidades para la investigación y persecución del ciberdelito. Se identifican como los elementos más destacados los siguientes: 1. **Creación de capacidades.** Fue el impulsor de la primera policía cibernética, conocida también como la Brigada de Cibercrimen 2. **Capacitación.** Las Policía de Investigación (PDI) a nivel nacional tienen un alto nivel de capacitación y especialización respecto al manejo de evidencia digital 3. **Cooperación internacional.** Cuenta con una red 24/7 que le permite un eficaz intercambio de información y evidencias y de solicitudes de cooperación y asistencia mutua con los países miembros del Convenio de Budapest

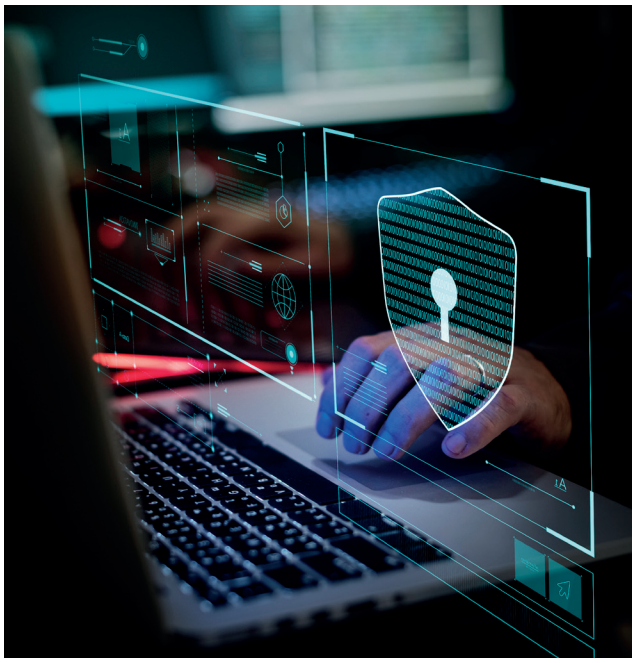
Tabla 5. Elaboración propia con información extraída de entrevista a Andrés Velázquez experto en ciberseguridad en enero de 2020.

6.2 Resumen de mejores prácticas identificadas

En conclusión, las mejores prácticas identificadas en las distintas regiones que fueron objeto de exploración son las siguientes:



Respecto de las buenas prácticas identificadas debe tomarse consideración que, al tratarse de un ejercicio exploratorio, se generó un análisis mucho más profundo en el caso de Argentina por ser el país con mayores criterios cumplidos. En lo referido a los demás países, si bien algunos cuentan con buenas prácticas, a nivel formal sería recomendable analizar de forma complementaria su eficacia a nivel práctico y operativo.



7. El fraude financiero cibernético en México

7.1 Alcances del fraude cibernético en el ámbito financiero en México

En la estadística nacional de incidencia delictiva no se cuenta con una segmentación específica en la que se pueda determinar el índice delictivo de delitos de fraude financiero cibernético desde la perspectiva del sistema de procuración e impartición de justicia. Sin embargo, existen dos tipos de registros que resultan de gran relevancia, el primero de ellos es el registro de la Comisión Nacional Bancaria y de Valores (CNBV), que tiene entre sus atribuciones la supervisión de las entidades financieras, y a través de la regulación, a la prevención de fraudes cibernéticos respecto de las instituciones que integran el sistema financiero.

En ese sentido, conforme a la Circular Única de Bancos se establecen las disposiciones aplicables a las Instituciones de Banca Múltiple que integran el sistema financiero. Estas instituciones tienen la obligación de seguir las reglas y estándares emitidos por la CNBV para evitar incidentes relacionados con los fraudes cibernéticos, así como a reportar ante la CNBV todos aquellos incidentes en los que las instituciones hayan sido vulneradas. Es importante destacar que este registro deriva de la obligación de las instituciones financieras de informar a la CNBV de estos incidentes, con el objetivo de que esa Comisión revise si se cumplieron las regulaciones en materia de ciberseguridad. Al respecto, los registros de la CNBV indican la siguiente incidencia:

# Eventos	Año	Tipo de incidente
39	2019	*Malware,* venta de bases de datos, brechas en infraestructura, phishing, ataques a ATM
21	2020	*Ransomware,* venta de bases de datos, brechas en infraestructura, spear phishing, ataques a ATM
17	2021	*Ransomware,* venta de bases de datos, brechas en infraestructura, ataques a ATM

Con base en las investigaciones que la CNBV inició respecto a estos incidentes, actualmente se encuentran en proceso de sanción los siguientes casos:

#	Año	Tipo incidente	Sanción
1	2020	Ataque a ATM	En proceso
1	2021	Brecha en infraestructura	En proceso

Para los casos de malware, phishing, venta de bases de datos dentro del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI) se generan comunicados para que las Instituciones Financieras identifiquen los Indicadores de Compromiso y actualicen sus sistemas de alerta, ya sea por la modalidad de operación o bien por el artefacto de ataque.

El segundo registro es el de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). Esta institución cuenta con un Portal de Fraudes Financieros por medio del cual las personas usuarias, pueden reportar las quejas. Este registro cuenta con un rubro específico para contabilizar las quejas que pueden derivar de un fraude cibernético en línea. Dentro del periodo 2019 a junio de 2021 las personas usuarias reportaron los siguientes incidentes:

Año	No. Reclam.	Tipo incidente [13]	Monto reclamado	Clase Financiera	Princ. Inst. Financiera
2019	12,800	Posible Fraude Virtual	$1,377,414,575	Banca de Múltiple	BBVA (47%), HSBC (23%) y Banorte (9%)
	34	Posible Fraude Virtual	$332,257	Sofom ENR	Soriana (94%), Directodo (3%) y Financiera Cuallix (3%)
	11	Posible Fraude Virtual	$88,760	Sofom ER	Globalcard (100%)
	3	Posible Fraude Virtual	$742,300	Banca de Desarrollo	B. del Bienestar (100%)
2020	16,036	Posible Fraude Virtual	$1,648,204,471	Banca de Múltiple	BBVA (24%), Santander (23%) y Banorte (21%)
	42	Posible Fraude Virtual	$354,554	Sofom ENR	Soriana (98%) y S. de Transf. y Pagos STP (2%)
	11	Posible Fraude Virtual	$1,052,407	Banca de Desarrollo	Banjercito (64%), B. del Bienestar (27%) y Nacional Financiera (9%)
	2	Posible Fraude Virtual	$2,000	Sofom ER	Crédito Familiar (50%) e Invex Consumo (50%)
2021 (Ene-Jun)	12,138	Posible Fraude Virtual	$1,126,857,783	Banca de Múltiple	Santander (23%), BBVA (16%) y HSBC (15%)
	15	Posible Fraude Virtual	$3,306,073	Banca de Desarrollo	Banjercito (80%) y B. del Bienestar (20%)
	7	Posible Fraude Virtual	$145,683	Sofom ENR	Soriana (71%), Fimubac (14%) y Financiera Cuallix (14%)
	2	Posible Fraude Virtual	$47,815	Sofom ER	Invex Consumo (100%)

[13] Incluye 6 causas: Consumos por teléfono no reconocidos, Consumos vía internet no reconocidos, Envío y/o retiro de dinero móvil no reconocida, Inconformidad por el importe de un consumo en comercio por internet, Inconformidad por el importe de un consumo en comercio por teléfono y Transferencia electrónica no reconocida

Respecto al número de delitos que son denunciados ante la o el Ministerio Público, no se cuenta con datos estadísticos específicos a nivel federal ni local. Lo anterior debido a que los datos estadísticos actuales se encuentran mezclados; por ejemplo, el delito de fraude genérico está considerado en una misma cifra para todos los delitos de fraude cometidos por medios tradicionales y no tradicionales. Por su parte, los delitos establecidos en la Ley de Instituciones de Crédito se encuentran en el mismo dato estadístico de los delitos de dicho ordenamiento legal sin que sea posible determinar aquellos que puedan considerarse como fraude financiero específico. No obstante, de acuerdo con información proporcionada por la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal de la Fiscalía General de la República (FGR) se identificó que el 50% de los casos que se atienden en la dirección de ciberseguridad de esa unidad corresponden a fraude financiero cibernético, de entre los cuales en el 20% de los casos corresponden a ataques en contra de instituciones financieras y el 80% a personas usuarias del sistema financiero. Asimismo, se identificó que de 2017 a julio de 2021 esa Unidad ha atendido alrededor 17 casos relevantes en contra de instituciones financieras. Sin embargo, la mayoría de los casos no llegan a una resolución eficaz, principalmente debido al mal manejo de la evidencia derivada del incidente.

De igual forma, esa Unidad señala la existencia de casos de éxito como el del sistema Swift de 2018. En este caso, una institución financiera fue vulnerada por atacantes con sede en otro país, lo cual generó un quebranto de 108 millones de dólares que pudieron ser recuperados. Otro caso fue en 2019, en el cual un grupo criminal generó un ciberataque a aproximadamente ocho entidades financieras contra las conexiones al Sistema de Pagos Electrónicos Interbancarios (SPEI). Pese a que no todas las instituciones afectadas decidieron presentar una denuncia y aportar evidencias, la investigación permitió lograr la detención y procesamiento de diversas personas integrantes de un grupo criminal encargado de estos ataques. El éxito de esta investigación radicó en la selección y recolección de evidencia digital en forma adecuada.

7.1.1 Políticas públicas sobre ciberdelito

Como antecedente de los esfuerzos que se han realizado en materia de ciberdelitos, se destaca la publicación de la Estrategia Nacional sobre Ciberseguridad de México en 2017[14], realizada en cumplimiento a lo establecido en el Plan Nacional de Desarrollo 2013-2018. No obstante, dicha estrategia no contempló un pilar específico sobre investigación y persecución de ciberdelitos.

Por lo que hace al enfoque de investigación y persecución de ciberdelitos, los esfuerzos más destacados y que cuentan con un sustento institucional es la creación de las policías cibernéticas impulsadas a través del Acuerdo 06/XLI/16 del Consejo Nacional de Seguridad Pública de acuerdo con el Modelo Homologado para las Unidades de Policía Cibernética. Sin embargo, pese a que este esfuerzo es relevante, algunos de las personas expertas consultados señalan que no se encuentra articulada como una política integral y que operativamente no es utilizada de manera efectiva.

En lo referente a las acciones que se encuentran en curso, se destaca la presentación de tres iniciativas de ley durante la LXIV Legislatura del Congreso de la Unión, por senadores y senadoras de diversos partidos (Senadores Miguel Mancera, Alejandra Lagunes, Diputado Javier Salinas Narváez). Pese a que en dos de ellas destaca la intención de generar tipos penales para sancionar ciberdelitos a nivel nacional, así como la creación de una instancia de coordinación a nivel nacional, se advierte que ninguna de ellas cumple con los requerimientos mínimos necesarios para armonizar los puntos clave que la legislación penal sustantiva y procesal mexicana requiere para cumplir con las disposiciones del Convenio de Budapest, así como para trazar una estrategia eficaz contra la cibercriminalidad a nivel nacional.

[14] Gobierno de México, Estrategia Nacional sobre Seguridad, 13 de noviembre de 2017, disponible en: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

En cuanto a las acciones recientes, se destaca que en 2018 el Banco de México, la CNBV, la CONDUSEF, la FGR, la Asociación de Bancos de México, entre otras, suscribieron las Bases de Coordinación en Materia de Seguridad de la Información conforme a las cuales las autoridades crearon el Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI), en el que podrán ser invitados las asociaciones gremiales y entidades financieras particulares. En este grupo, las diversas autoridades evalúan la naturaleza, alcance e impacto de los incidentes cibernéticos con la finalidad de compartir información y prevenir nuevos ataques de la misma naturaleza. No obstante, pese a los relevantes esfuerzos realizados por estas autoridades, se destaca que hasta el momento el enfoque de estas acciones ha tenido un enfoque de ciber resiliencia y, en mucho menor medida de investigación y persecución de ciberdelitos.

Sin embargo, existen acciones importantes que están en desarrollo que pueden ser sumamente eficaces en la mejora de la investigación y persecución del ciberdelito. Por ejemplo, el Banco de México dio a conocer que actualmente está impulsando dos estrategias desde el GRI, específicas para este fin. La primera es fortalecer el sustento del intercambio de información que se genera entre las autoridades respectivas que forman parte del GRI, a fin de que haya una mejor y más robusta colaboración en el intercambio de información sensible, y la segunda es la próxima elaboración de un “Decálogo para la Atención de Incidentes” que indique los criterios mínimos que podrían seguir las instituciones para generar y preservar la evidencia digital, y promover actividades de capacitación en la materia; a fin de que se cuente con carpetas de investigación más robustas.

7.1.2 Mapa de actores ante un fraude financiero cibernético

La prevención, investigación y persecución de un fraude financiero cibernético implica la acción de diversos actores en el ámbito público y privado que se describen a continuación:

Actor	Naturaleza	Rol
Personas usuarias	Personas físicas o morales que contratan o utilizan alguna operación o servicio prestado por una Institución Financiera	• Víctima del delito
Instituciones Financieras	Instituciones públicas o privadas reguladas por el Sistema Bancario Mexicano	• Víctimas del delito • Funcionan como intermediarios entre la víctima y el victimario
Comisión Nacional para Protección de la Defensa de los Usuarios (CONDUSEF)	Organismo público descentralizado con personalidad jurídica y patrimonio propio	• Recibir quejas de personas usuarias ante la comisión de un fraude • Asesora a las personas usuarias que son víctimas de un delito en el proceso de presentación de una denuncia
Comisión Ejecutiva de Atención a Víctimas	Organismo descentralizado de la Administración Pública Federal, no sectorizado, con personalidad jurídica, patrimonio propio y autonomía técnica y de gestión	• Brindar asesoría Jurídica a las Víctimas
Comisión Nacional Bancaria y de Valores (CNBV)	Órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, con autonomía técnica y facultades ejecutivas	• Establecer las medidas que deben seguir las instituciones financieras de Banca Múltiple en materia de ciberseguridad • Supervisar el cumplimiento de las normas. • Recibir, analizar y dar seguimiento a las notificaciones de incidentes de ciberseguridad / así como alertar a otras instituciones y autoridades • Imponer sanciones cuando el incidente deriva de un incumplimiento normativo

Actor	Naturaleza	Rol
Banco de México	El banco central del país, constituido como organismo constitucional autónomo que tiene entre sus finalidades promover el sano desarrollo del sistema financiero y funcionamiento del sistema de pagos	• Emitir disposiciones en materia de ciberseguridad para las instituciones bancarias interconectadas a los sistemas que opera, incluido el sistema de pagos SPEI • Recibir reportes sobre la comisión de incidentes de violación a la ciberseguridad de dichas disposiciones. • Supervisar el cumplimiento de las disposiciones referidas • Sancionar en caso de incumplimiento a esas disposiciones • Presentar denuncias cuanto tiene conocimiento de un hecho delictivo que inciden en sus sistemas o equipos
Policías cibernéticas estatales de Seguridad Pública, Policía Cibernética de la Guardia Nacional y policías ministeriales federal y local.	Instituciones policiales dependientes del poder ejecutivo local con facultades de prevención y/o investigación de los delitos	• Recibir reportes o denuncias • Canalizar a la o el Ministerio Público • Colaboran con la o el Ministerio Público en la investigación de los hechos
Servicios periciales de la Fiscalía General o las fiscalías estatales	Cuerpos auxiliares del Ministerio Público para la búsqueda de pruebas, la acreditación de los elementos que definen la probable responsabilidad, así como en la reconstrucción de los hechos	• Colaborar con la o el Ministerio Público en el procesamiento e interpretación de la evidencia científica
Fiscalía General de la República y Fiscalías locales.	Órganos constitucionales autónomos a cargo de la investigación y persecución de los delitos	• Recibir denuncias e iniciar investigaciones • Coordinar policías y personal pericial para investigar el hecho • Presentar el caso ante el juez para lograr una sanción

Tabla 6. Elaboración propia con información extraída de la Ley de Protección y Defensa al Usuario de Servicios Financieros, Ley del Banco de México, Ley de la Comisión Nacional Bancaria y de Valores, Ley del Banco de México y Ley Orgánica de la Fiscalía General de la República.

7.1.3 Interrelación de actores ante un fraude financiero cibernético

El proceso no es lineal en todos los casos, pues tiene diversas posibilidades que dependen principalmente de si el afectado es la persona usuaria, la entidad financiera o ambos.

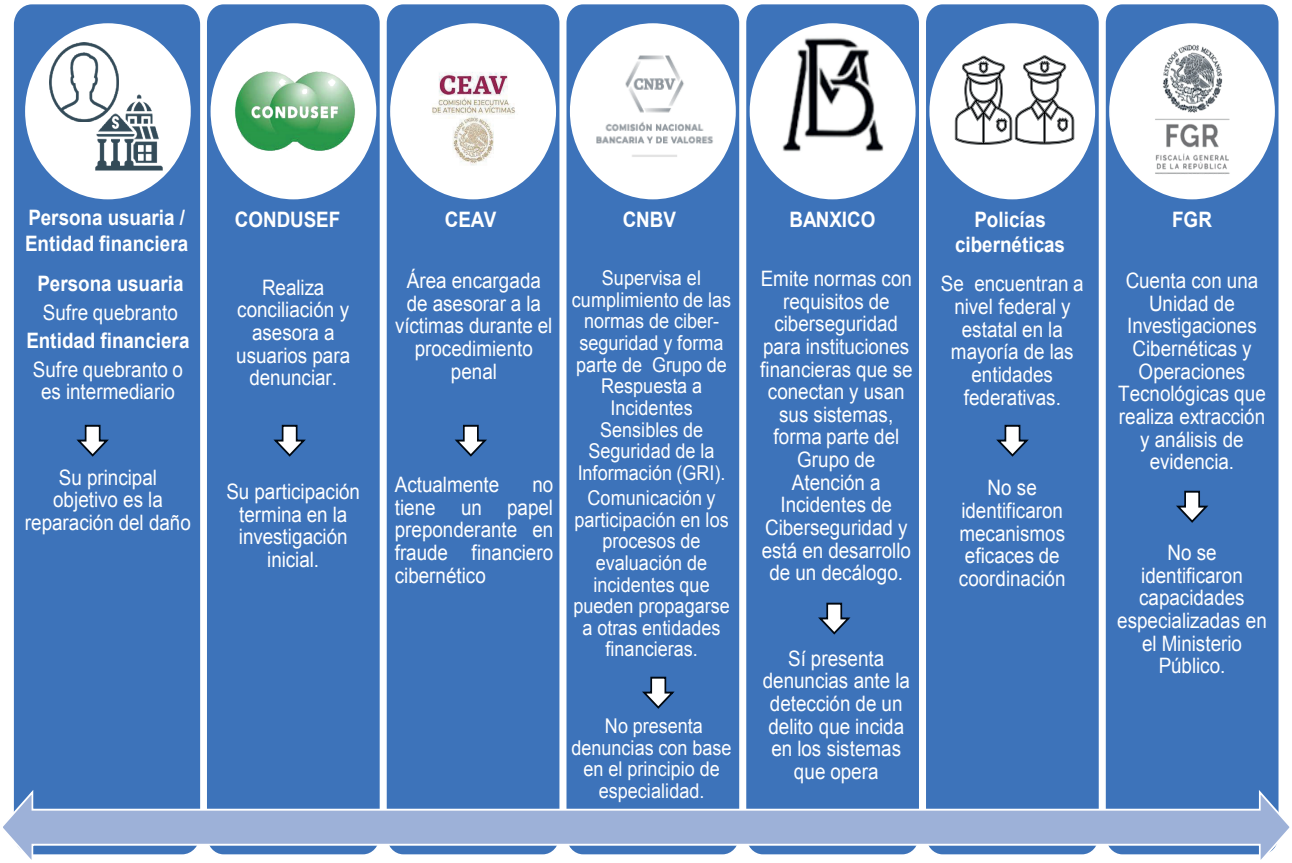


Figura Elaboración propia con información extraída de la Ley de Protección y Defensa al Usuario de Servicios Financieros, Ley del Banco de México, Ley de la Comisión Nacional Bancaria y de Valores, Ley del Banco de México y Ley Orgánica de la Fiscalía General de la República.

7.1.4 Principales hallazgos del proceso de interrelación de actores

Actualmente, las personas usuarias son las principales afectadas ante la comisión de fraude financiero cibernético. Sin embargo, su participación en cuanto al acceso a la justicia para la investigación y sanción de estos hechos se encuentra sumamente reducida ante la falta de información y conocimiento de los derechos y procesos que se deben seguir y principalmente la competencia jurisdiccional de las autoridades. Dentro de las interacciones institucionales más relevantes se destacan las siguientes:

Personas usuarias e instituciones financieras

Si bien la metodología no contempló la existencia de encuestas abiertas a personas usuarias directos o víctimas de fraude financiero cibernético, de la información recabada en las entrevistas con operadores y personas expertas, se identificó que el en la mayoría de los casos las personas físicas

o morales usuarias que son víctimas de un fraude financiero cibernético tienen como principal interés la reparación del daño que les fue causado por el delito, más allá de la sanción de la persona que pudo cometerlo, además de que encuentran el proceso de denuncia y seguimiento del procedimiento penal sumamente complejo y limitado para los resultados que se esperan.

De igual forma, en el caso de las instituciones financieras, especialmente las Instituciones de Banca Múltiple que son víctimas, el principal interés es investigar el incidente que causó el quebranto, ello principalmente con la finalidad de reforzar las medidas de seguridad al respecto. El segundo objetivo de estas instituciones es recuperar el daño que le fue causado y además evitar que el público en general tenga conocimiento de ataque debido a que esto puede poner en riesgo su prestigio institucional. Por tal motivo, en los casos de ser víctimas las instituciones bancarias realizan investigaciones internas y en algunos casos, posteriormente presentan una denuncia ante el Ministerio Público, sin embargo, es recurrente que esta denuncia no vaya acompañada de toda la información relevante y destacada con la que cuentan, debido a que el principal incentivo de la denuncia es en algunos casos, sólo cubrir con el requisito para acceder a seguros para reparar el daño causado, debido a que el procedimiento penal no es percibido como un mecanismo de reparación del daño ni de prevención de otros delito.

Asimismo, las instituciones bancarias consultadas refirieron que perciben la colaboración de la CNBV y del Banco de México con un enfoque más sancionador de entes reguladores y del cumplimiento de sus obligaciones, más que un apoyo en la prevención de estos delitos.

La normativa que en materia de ciberseguridad contempla los mínimos de seguridad que deben observar las Instituciones de Banca Múltiple fue actualizada y publicada en el 2018 por la CNBV, dando un marco mínimo normativo de prevención para cumplimiento[15], a fin de estar en condiciones de hacer frente a riesgos y ataques informáticos que pudieran ocasionar afectaciones a las instituciones de crédito y a la realización de operaciones con los clientes.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

De acuerdo con la información proporcionada por la CONDUSEF, esta institución es la encargada de recibir quejas en contra de una Institución Financiera por parte de las personas usuarias del Sistema Financiero, en los casos de quebrantos inferiores a tres millones de unidades de inversión, y en caso de reclamaciones en contra de instituciones de seguros en el cual la cuantía debe de ser inferior a seis millones de unidades de inversión y que lo reclamado no exceda del periodo de dos años, contados a partir de que se presente el hecho que les dio origen, a partir de la negativa de la Institución Financiera a satisfacer las pretensiones del usuario o, en su caso de que se trate de reclamaciones por servicios no solicitados, a partir de que tuvo conocimiento del mismo. La CONDUSEF, a efecto de brindar una solución expedita a las personas usuarias, lleva a cabo un mecanismo alterno de solución, por medio del cual se invita a las partes a llegar a un acuerdo para resolver las controversias, de forma previa a presentar una reclamación.

Asimismo, cuando se identifica que la afectación a la persona usuaria pudiera configurar algún delito, la CONDUSEF orienta al usuario para que inicie la denuncia penal correspondiente. La CONDUSEF presenta las denuncias exclusivamente tratándose de los supuestos establecidos en el párrafo primero de la fracción XXVI del artículo 11 de la Ley para la Protección y Defensa al Usuario de Servicios Financieros y las promueve cuando se materializa el hecho. Asimismo, desde el 2016 la CONDUSEF implementó un protocolo de atención a personas usuarias en casos de Probable Robo de Identidad, denominado protocolo PORI. En este protocolo, cuando una persona usuaria se acerca a la CONDUSEF y de la problemática que presenta se desprenden argumentos con los que se pueda

[15] https://www.dof.gob.mx/nota_detalle.php?codigo=5544804&fecha=27/11/2018

considerar el asunto como un posible robo de identidad, el asesor o asesora mediante la Asesoría Técnica Jurídica orienta a la persona; primero se emite su reporte de crédito especial, para ver si el usuario identifica algún crédito que no reconozca o pudieran existir movimientos fuera de lo usual, como podría ser la consulta del reporte sin su consentimiento. En caso afirmativo, solicitará el bloqueo de consulta al historial crediticio del afectado y se orientará a que presente una denuncia ante la o el Ministerio Público.

Dentro de sus atribuciones, la CONDUSEF cuenta con facultades para asesorar a las personas usuarias que han sido víctima de un delito y en su caso, asesorar y acompañar durante el proceso de presentación de denuncia y hasta en tanto se determina la investigación inicial. Del periodo de 2019 a junio de 2021, la CONDUSEF cuenta con las siguientes estadísticas en materia de acompañamiento en materia penal:

Año	Asesorías Jurídicas Penales	Tipo incidente	Delito denunciado*	Clase Financiera	Fuero Federal/ Local
2019	728	Consumos y cargos no reconocidos, transferencias electrónicas no reconocidas y Disposición de efectivo en cajero automático no reconocida		Banca de Múltiple	
2020	209	Consumos y cargos no reconocidos, transferencias electrónicas no reconocidas y Disposición de efectivo en cajero automático no reconocida		Banca de Múltiple	
2021 (E-J)	54	Consumos y cargos no reconocidos, transferencias electrónicas no reconocidas y Disposición de efectivo en cajero automático no reconocida		Banca de Múltiple	

El procedimiento de asesoría penal puede brindarse una vez que se ha llevado a cabo el procedimiento de conciliación, dictamen y su respectiva solicitud de defensoría legal gratuita, si esta última es procedente y cuenta con los elementos necesarios para que se brinde este servicio de asistencia, se acuerda una entrevista con la persona usuaria y uno de los asesores en la materia para comentar la problemática y los alcances jurídicos que tendría la denuncia en caso de que el Usuario decida o no presentarla.

Una vez que se ha brindado la asesoría, si la respuesta es positiva para la presentación de la denuncia, se elabora la denuncia, la cual se hace a nombre de la persona usuaria como víctima del delito. Ésta se presenta ante la Oficialía de Partes de la Fiscalía General de la República (Delegación Central de la Ciudad de México), una vez que la misma se turna a una o un Ministerio Público Federal, éste envía un citatorio para llevarse a cabo la entrevista de ratificación de denuncia, misma que es notificada a la persona usuaria, y ya sea que se realice el acompañamiento presencial a la entrevista o vía remota se le explica en qué va a consistir, los alcances jurídicos que tendrá dicha entrevista, así como el procedimiento a seguir ante la o el Ministerio Público. Posteriormente a la entrevista de ratificación de denuncia, se queda en espera de alguna respuesta por parte de la o el Ministerio Público, ya sea en caso de necesitar documentación o información adicional, alguna entrevista adicional de ratificación o para brindar información sobre el avance de la carpeta de investigación y se continúa dando el seguimiento en conjunto con el Usuario ante el Ministerio Público. La CONDUSEF indica que no da seguimiento al proceso penal jurisdiccional, ya que sólo se asiste al usuario hasta que la o el Ministerio Público determina el ejercicio o no de la acción penal, en términos de lo establecido en el segundo párrafo de la fracción XXVI del artículo 11 de la Ley para la Protección y Defensa al Usuario de Servicios Financieros.

Aunado a lo anterior, la CONDUSEF indicó que el proceso de asesoría y acompañamiento durante el proceso de presentación de la denuncia implica una destacada diferencia para las personas usuarias. Ello debido a que en los casos en que acuden solas, las personas usuarias tienen importantes problemáticas para que les sea recibida su denuncia, esto principalmente debido a la falta de certeza jurídica de los delitos cometidos, así como de la definición de las competencias entre el ámbito federal y el ámbito local. Por ello, es que la asesoría jurídica en materia penal que brinda la CONDUSEF a las personas usuarias resulta de especial relevancia para el efecto de hacer más eficiente este proceso. Sin embargo, esta institución refiere que la mayoría de los casos terminan ya sea en un no ejercicio de la acción penal o en su caso, en un archivo temporal por parte de la o el Ministerio Público debido a que refiere que no se cuentan con evidencias suficientes para sustentar el caso. De igual forma, es altamente recurrente que las personas usuarias desistan del seguimiento de su caso, esto principalmente porque su interés principal es la recuperación del quebranto sufrido más allá del resultado del procedimiento penal.

Además, las y los representantes de CONDUSEF indicaron que, se tiene una estrecha comunicación con las y los representantes de la FGR, por lo que se han identificado situaciones como son: falta de homologación de criterios tanto de clasificación del delito, definición de competencias, así como de las evidencias relevantes que deben acompañarse o de las reglas de evidencia digital a aplicar y respecto de las cuales se están realizando acciones permanentes para su atención, hasta en tanto se llevan a cabo las adecuaciones legales necesarias. En ese sentido, esta institución colabora con la FGR, en el diseño de un protocolo que permita homologar estos criterios y mejorar la atención de los casos.

En el caso de la recolección de evidencias que se encuentran en poder de las instituciones financieras, la CONDUSEF ha identificado que las instituciones son renuentes a la entrega de esta información cuando la solicita la o el usuario, por lo que es mucho más accesible obtenerla a través del requerimiento de informe que realiza la CONDUSEF.

Es importante tomar en consideración que, pese a la asesoría y el acompañamiento brindado por parte de

la CONDUSEF, resulta de vital importancia una mejora en el acceso a la justicia de las personas usuarias. Ello, enfrenta importantes limitaciones, la primera son los alcances de las facultades conferidas a la CONDUSEF, toda vez que estas abarcan únicamente una etapa muy preliminar de la investigación, esto es ante el Ministerio Público y la otra es lo referente al número de asesores jurídicos, pues actualmente sólo brinda esta asesoría en la Ciudad de México y no en todas las entidades federativas de la República Mexicana.

Aunado a lo anterior, es importante señalar que este acompañamiento y seguimiento brindado por la CONDUSEF enfrenta diversos obstáculos, el primero de ellos es la falta de claridad y certeza jurídica por la ausencia de un tipo penal especializado, de una adecuada determinación de competencias en el ámbito federal y local, así como la ausencia de protocolos de actuación adecuados en el proceso de investigación, provoca que la denuncia sea hoy un mecanismo poco alentador para que las personas usuarias continúen con el proceso penal y en su caso, obtengan una reparación del daño.

Comisión Ejecutiva de Atención a Víctimas

La Comisión Ejecutiva de Atención a Víctimas (CEAV) es la institución encargada de brindar asesoría jurídica gratuita a todas las víctimas del delito en el ámbito federal, sin embargo, al momento esta institución indicó que actualmente no cuenta con la atención de acompañamiento directo a víctimas del delito de fraude financiero cibernético, sino que únicamente a víctimas que han presentado denuncias en contra de la mala actuación de funcionarias y funcionarios públicos a cargo de investigaciones relacionadas con el sistema financiero. Estos casos implican un importante reto ya que las y los asesores jurídicos son solicitados por la o el Ministerio Público Federal o en su caso por la o el Juez de Control, para que asistan a representar a las víctimas en las audiencias en las que se impugna alguna determinación de la investigación de esas posibles irregularidades. En términos generales, se ha asumido el criterio de que las y los asesores jurídicos de la CEAV tienen la obligación de impugnar las determinaciones de esas investigaciones y en caso de no hacerlo, pueden ser sujetos de una sanción.

Actualmente la CEAV está iniciando el proceso de cooperación y colaboración con la CONDUSEF a efecto de ejercer de manera más efectiva sus facultades y obligaciones en materia de asesoría jurídica a las víctimas de estos delitos. Pese a que la CEAV cuenta con recursos muy limitados y una alta incidencia en la atención de casos, especialmente de casos de alto impacto, esta institución considera en términos sistémicos que sería ideal que la CEAV contara con las capacidades institucionales para brindar el asesoramiento en materia penal a las víctimas de los delitos de fraude financiero cibernético, en lugar de contar con diferentes canales de atención para las víctimas.

Comisión Nacional Bancaria y de Valores

Como se mencionó anteriormente, la CNBV es el órgano encargado de regular y supervisar el cumplimiento de las obligaciones en materia de ciberseguridad de la información de las instituciones bancarias conforme a la normatividad aplicable y vigente. La CNBV es quien establece la obligación de que las instituciones bancarias cumplan con criterios mínimos en materia de ciberseguridad, vigila su cumplimiento e incluso sanciona el incumplimiento de tales disposiciones. En ese contexto, de acuerdo con el marco regulatorio, las instituciones bancarias referidas tienen la obligación de llevar a cabo una investigación de los incidentes cibernéticos de los que son víctima, aunque al momento dichas investigaciones se lleven de acuerdo a cada institución bancaria.

La CNBV indicó que el marco regulatorio no contempla una disposición expresa que obligue a las instituciones financieras a presentar una denuncia ante la o el Ministerio Público en los casos en que son víctima de un delito de fraude financiero cibernético. Cuando ocurren hechos que pudieran

ser constitutivos de delito y dado que los delitos financieros son competencia de la CNBV, mientras que el requisito de procedibilidad o querella es competencia por mandato legal de la Procuraduría Fiscal de la Federación (PFF), que también forma parte de la Secretaría de Hacienda y Crédito Público (SHCP), por lo que **únicamente la CNBV emite una opinión a la SHCP por estar expresamente facultada para ello** (art. 115, primer párrafo de la LIC). Por lo anterior, la CNBV no realiza la denuncia de manera directa.

En tanto, se tenga conocimiento de algún hecho o conducta que pudiera ubicarse en los delitos que son de su competencia conforme a las leyes financieras, podrá emitir una opinión de delito financiero con los elementos con los que cuente y comunicarlo a la PFF, para que esta última pueda pronunciarse al ser la instancia que legítimamente está facultada, al amparo del principio de especialidad que rige la materia de la que conoce la CNBV. Del análisis de lo previsto en el artículo 222 del CNPP, se identifica que la CNBV podría robustecer la recopilación de elementos causales objetivos que permitan, como parte de los protocolos de actuación ante incidentes cibernéticos, el emitir una opinión de delito a la PFF para la denuncia correspondiente, a efecto de que las autoridades puedan iniciar la investigación correspondiente. Esto con independencia de que la institución financiera afectada presente una denuncia.

En ese sentido se destaca que, si bien se detecta que a la fecha, la CNBV se está consolidando como una institución líder en el país en materia de ciberseguridad, su participación en el ámbito de la cibercriminalidad podría robustecerse al analizar los elementos con los que cuente para en su caso pronunciarse. Esto aún se encuentra limitado con base en la regulación aplicable, ya que la misma se enfoca en la emisión y supervisión del cumplimiento de regulaciones dentro del ámbito preventivo en materia de ciberseguridad. Por lo anterior, se advierte que la participación y liderazgo de esta autoridad podría fortalecerse y ampliarse en beneficio del combate a la cibercriminalidad y en particular del fraude financiero cibernético.

Banco de México

El Banco de México (BANXICO) es el banco central del país. encargado del Sistema de Pagos Electrónicos Interbancarios de México mejor conocido como SPEI. Adicionalmente, BANXICO cuenta con facultades para imponer a las instituciones financieras requisitos de ciberseguridad como parte de su conexión a los sistemas que les brinda el propio BANXICO, incluyendo los sistemas de pagos, como el SPEI, que este administra. En 2018, BANXICO creó una Dirección de Ciberseguridad que tiene entre sus funciones impulsar acciones para fortalecer la seguridad de la información de las instituciones financieras; para lo cual participa en la elaboración y supervisión de las disposiciones que se aplican en esta materia; así como diseña estrategias de colaboración con las instituciones y autoridades para prevenir y responder a ciberataques. Al respecto, algunos de las personas expertas los expertos de la industria consideran que existe una duplicidad y disparidad entre las labores de regulación, supervisión y sanción entre la CNBV y el Banco de México ante la atención de incidentes relacionados con fraudes cibernéticos en el ámbito financiero, sin embargo, considerando el marco regulatorio así como las acciones referidas por autoridades, se advierte que si bien ambas llevan a cabo actividades en el mismo ámbito, sus acciones son complementarias.

El Banco de México precisó que no ha sufrido un ataque exitoso a sus sistemas o infraestructura de manera directa. El Banco de México ha determinado que sus funcionarios y funcionarias, y su personal, tales como servidoras y servidores públicos, tienen la obligación de denunciar ante la o el Ministerio Público cuando se tenga conocimiento de la existencia de un hecho que se señale como delito, respecto de los sistemas o equipos que este administre. Por ello, el Banco de México presenta denuncias cuando las áreas técnicas detectan estos incidentes. Una vez que se detecta el incidente, se da conocimiento al área de ciberseguridad del Banco de México, se recaban los datos técnicos necesarios y hechos y posteriormente se hacen del conocimiento al área jurídica. El área jurídica elabora una denuncia y se

presenta a la FGR. La denuncia se apoya con la información que se aportó por las áreas técnicas. Esta denuncia, se puede presentar físicamente en papel o de manera electrónica, a través del correo proporcionado por la FGR. Posteriormente, la o el Agente del Ministerio Público cita a la o el representante del Banco de México a ratificar, y, en su caso, solicita que se aporten más datos. En caso de que no se cuente mayores elementos de investigación, la o el Ministerio Público determina el no ejercicio de la acción penal.

Las y los representantes del Banco de México identificaron como obstáculos de la investigación y persecución del delito los siguientes: prácticas forenses muy heterogéneas entre las instituciones, algunas tienen protocolos y equipos muy desarrollados para preservar y recolectar la evidencia de manera adecuada. Sin embargo, en las instituciones financieras pequeñas no hay protocolos robustos y se delegan los temas de ciberseguridad a un segundo plano. Otra limitante son las lagunas previstas en la legislación penal (Código Penal Federal), por lo que sería muy importante fortalecer el marco jurídico para la investigación y persecución de este tipo de delitos. Además, el hecho de que las instituciones financieras han mostrado tener mayor interés en sólo presentar una denuncia con limitadas evidencias, por ser un requisito formal para acceder a los seguros que tienen contratados, y no para que realmente que se investigue y sancione el hecho. Además, las instituciones tienen una amplia reticencia a aportar toda la evidencia posible por temor a que se les puedan incautar equipos, lo que detiene su operación o impacta su nivel de servicios. Por lo que consideran que existe una necesidad de contar con lineamientos y guías para que ayuden a las instituciones a aportar elementos suficientes dar un seguimiento puntual a los actos de investigación y que permitan dar un seguimiento puntual.

De lo anterior se desprende que, si bien el Banco de México busca tener un papel y participación mucho más activa para evitar que el fraude financiero cibernético permanezca en impunidad, en los hechos, esta participación queda sujeta a las facultades legales y operativas que le corresponden en el ámbito de sus atribuciones.

Fiscalía General de la República

La Dirección de Ciberseguridad adscrita a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal de la Fiscalía General de la República (FGR) cuenta con dos formas de recibir la atención de casos relacionados: participando en la investigación y en la atención ante un incidente cibernético.

El proceso de atención de incidentes es directo con la Unidad, donde las instituciones financieras pueden optar por contactarlos.

En el caso de investigaciones que requieren de un elemento técnico, la participación se da mediante una solicitud expresa de la o el Ministerio Público para fungir como peritos en la investigación. Esta actividad técnica que termina en una pericial puede ser realizada tanto por la Unidad de Investigaciones Cibernéticas, así como del área de Servicios Periciales en Informática y Telemática de la FGR.

Cuando las y los afectados son personas físicas y la carpeta se lleva a nivel federal, la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal únicamente colabora cuando le es solicitada una investigación por parte de la o el Ministerio Público dentro de una investigación.

Asimismo, esta Unidad es el contacto de cooperación internacional con la INTERPOL, un punto clave para la cooperación internacional que requieren este tipo de delitos.

En la opinión de esta institución dentro de la AIC, uno de los mayores retos de la investigación y persecución de estos delitos es la inadecuada preservación de evidencia digital, se considera que una investigación tiene mejor solución cuando la información es aportada por la víctima o la o el

denunciante. Los casos de éxito se caracterizan por una adecuada colaboración y coordinación entre la dirección por parte de la o el Ministerio Público y la investigación técnica proporcionada por la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal.

Policías Cibernéticas

En cuanto a la Policía Cibernética Federal, previo al 2019, la Policía Federal que dependía de la extinta Comisión Nacional de Seguridad tenía a su cargo el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT- MX), misma que fungía como una instancia encargada de vigilar la integridad de la infraestructura tecnológica estratégica, tener coordinación con policías cibernéticas nacionales e internacionales, así como un monitoreo permanente los 365 días del año. A partir del 27 de mayo de 2019 fecha en que se publicó Ley de la Guardia Nacional[16], que establece en su artículo noveno que dentro de las atribuciones del nuevo cuerpo de seguridad se encuentra "realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas", la Policía Cibernética y el CERT- MX forman parte de la Guardia Nacional.

En muchos de los casos, las funciones de la Policía Cibernética de la Guardia Nacional requerirán involucrar a un Ministerio Público quien a su vez también podrá nombrar perito o perita a los especialistas que hicieron la investigación pero que también podría requerir a los Servicios Periciales de la FGR.

Por su parte, las entidades federativas cuentan con policías cibernéticas que han sido impulsadas por el Modelo Homologado de Unidades de Policía Cibernética aprobado por el Consejo Nacional de Seguridad Pública (2016). El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública ha dado seguimiento a la creación de dichas unidades. Conforme al reporte del Modelo Único de Operación Policial (MOP) el Secretariado reportó que, al 30 de septiembre de 2020, 30 entidades federativas tenían una Unidad de Policía Cibernética, faltando los estados de Sinaloa y Tabasco.

[16] DECRETO por el que se expide la Ley de la Guardia Nacional, consulta en: https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019

8. Conclusiones

Los ciberdelitos, especialmente aquellos relacionados con el fraude cibernético financiero, **son una problemática que van al alza debido al incremento en la digitalización de actividades con motivo de la contingencia sanitaria generada por el COVID-19.** La importancia de estos delitos radica no sólo en las graves afectaciones económicas que genera para la personas e instituciones bancarias y financieras, sino también respecto a las consecuencias en la economía nacional y, en la mayoría de los casos, su estrecha relación con grupos y esquemas criminales vinculados al crimen organizado. Por lo anterior, la investigación y persecución de estos delitos debe comprender una visión sistémica y conceptualizarse desde una versión amplia de afectación al patrimonio de las personas usuarias y de quebrantos económicos en las Instituciones financieras.

La identificación y persecución de ciberdelitos presenta importantes retos a nivel jurídico, tanto en el ámbito sustantivo como en el ámbito procesal, de cooperación internacional y, principalmente, respecto a las capacidades institucionales que deben hacer frente a esta problemática criminal. Por lo tanto, resulta indispensable que los países se adhieran al Convenio de Budapest ya que es el único instrumento que prevé directrices y disposiciones efectivas para impulsar un marco jurídico mucho más eficaz para la investigación y persecución de esto delitos y para generar puentes de comunicación y coordinación internacional para cumplir sus objetivos.

Argentina, Colombia, Chile y República Dominicana -países que ya forman parte del Convenio de Budapest- comparten los siguientes factores clave respecto a la investigación de estos delitos: I) voluntad política de establecer el combate a la cibercriminalidad como un de las prioridades en política criminal basado en su impacto global y no sólo individual; II) la generación de un marco jurídico eficaz; III) la construcción de capacidades institucionales, principalmente a cargo de las fiscalías y el poder judicial; IV) la colaboración y participación de equipos de investigación técnicos forenses; y, V) mecanismos eficaces de cooperación internacional con diversos países. Pese a estos grandes avances, estos países aún cuentan con una diversidad de retos tales como mejorar y hacer más eficiente la cooperación y colaboración con los proveedores de servicios de comunicaciones, las dificultades de competencias jurisdiccionales que se generan ante delitos que pueden cometerse o surtir sus efectos en otro país o estado, y las complejidades para la revisión, evaluación y la legalidad del intercambio de información y la obtención de la evidencia digital.

En el ámbito normativo el hecho de que México no se encuentre adherido al Convenio de Budapest genera importantes limitaciones especialmente en materia de cooperación internacional, así como en los beneficios que ello podría traer para la construcción de capacidades con el apoyo de la comunidad internacional. En el ámbito legislativo a nivel interno, se detectan importantes deficiencias en la tipificación y homologación de delitos para la sanción del fraude cibernético financiero a nivel nacional, además de una importante problemática en la definición de competencias entre el ámbito federal y local, así como limitaciones legales y regulatorias en el ámbito de reglas procesales para la investigación y persecución de estos delitos.

En el ámbito operativo, actualmente se ha llevado a cabo un esfuerzo de coordinación nacional a través del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información en el que participan actores de alto nivel tal como la CNBV, el Banco de México, la CONDUSEF, la FGR entre otros, el cual constituye un ejercicio muy relevante a nivel de articulación entre los operadores más relevantes,

sin embargo, el enfoque de esta articulación se centra en el ámbito de la ciber resiliencia más que en la cibercriminalidad. Además, de que existe una ausencia en la articulación de procesos desde la recepción de denuncia, la investigación y persecución de los delitos. Aunado a lo anterior, no se logró constatar evidencia de una sólida construcción de capacidades especializadas de Ministerios Públicos y personas juzgadoras para la adecuada atención de estos casos.

Pese a que durante los últimos años México ha sido el blanco de ataques de alto nivel, tales como el ataque a algunas instituciones financieras en su conexión al sistema de pagos de la banca electrónica en 2018, se percibe en algunas instituciones del sistema de justicia poco interés en generar mayores y mejores condiciones para la investigación de este tipo de delitos. Adicionalmente, dado que el ámbito de facultades de los órganos reguladores financieros, tales como BANXICO y la CNBV, tiene un enfoque preventivo y normativo, su intervención en la presentación y seguimiento de denuncias por parte de las entidades está limitada.

Por su parte, las Instituciones de Banca Múltiple, en su rol como intermediarios entre el usuario víctima y los criminales, están mucho más enfocados en recuperar las afectaciones de carácter económico en vez de iniciar con las investigaciones de los hechos constitutivos de delito; y, a su vez, como víctima su mayor incentivo para presentar una denuncia penal es obtener un registro para resarcir su quebranto a través del cobro de un seguro. Por lo que se advierte un escenario con deficiencias en el que el más perjudicado resulta ser el usuario, ya sea persona física o moral.

9. Recomendaciones

En el presente apartado se presentan recomendaciones en tres principales rubros:

- acciones de índole normativa y regulatoria
- acciones de carácter operativo y procedimental
- acciones de coordinación interinstitucional

9.1 Recomendaciones sobre marco normativo y regulatorio

9.1.1 Impulsar la adhesión de México al Convenio de Budapest

Si bien a lo largo del presente reporte, se señaló que la adhesión al Convenio de Budapest no es una solución que por sí misma pueda implicar un cambio determinante en el corto plazo, resulta claro que la adhesión de México al Convenio de Budapest podría traer importantes beneficios en materia de mejora y actualización del marco jurídico penal sustantivo y procesal, cooperación internacional, acceso a capacitación, así como herramientas y mecanismos útiles para la eficacia y eficiencia en la investigación de este tipo de delitos de carácter transnacional.

Se sugiere que México, a través de las autoridades competentes, impulse la realización de las gestiones necesarias para solicitar al Consejo de Europa la adhesión formal al Convenio de Budapest a la mayor brevedad posible. Es importante señalar que este proceso es independiente a los avances legislativos que deben generarse a nivel interno, es decir, que la estrategia debe seguirse de manera paralela entre la adhesión al Convenio y la modificación al marco legislativo interno, sin que sea una limitante la falta de atención al Convenio para poder continuar con avances a nivel interno.

9.1.2 Impulsar una reforma constitucional y legal para expedir una Ley General en materia de Cibercriminalidad

Derivado de las complejidades del sistema federal mexicano, así como las limitantes del ámbito tanto sustantivo como procesal para investigar y perseguir los ciberdelitos y en especial el fraude financiero cibernético, se considera prioritario encaminar una reforma constitucional en materia penal a través de una Ley General que tenga alcance a nivel federal y de las entidades federativas que incorpore las disposiciones sustantivas, procesales y de cooperación internacional previstas en el Convenio de Budapest, evitando la duplicidad de la regulación existente, así como proponer soluciones viables para resolver la problemática de jurisdicción y competencias en el ámbito penal federal y local.

En ese sentido, si bien se está consciente del reto mayúsculo que esta reforma implica a nivel de aprobación constitucional y legal, de las lecciones aprendidas se advierte que esta es en definitiva la opción más adecuada para dar solución a las problemáticas planteadas a nivel normativo legal. Además, de que esta propuesta tiene completa viabilidad en caso de que se cuente con voluntad política, así como puntual asesoramiento técnico. Es además destacado, que esta propuesta coincide a nivel conceptual con las recientes propuestas legislativas presentadas por diversos legisladores.

Uno de los ejemplos más importantes para esta recomendación, son las lecciones aprendidas del análisis comparado con Argentina, quien al igual

que México es un Estado Federal, lo que implica un mayor grado de complejidad, sin embargo, a diferencia de México, Argentina cuenta con un solo Código Penal sustantivo aplicable a toda la República, lo que les permite hacer mucho más efectiva la clasificación jurídica de tipos penales relacionados con fraude financiero cibernético. Por lo tanto, en el entendido de que en el país la federación y las entidades federativas cuentan con un Código Penal sustantivo diverso, resulta de alta prioridad, con una Ley General que pueda establecer las reglas fundamentales que a nivel sustantivo y de cooperación internacional, puedan ser aplicables para el ámbito de cibercriminalidad.

9.1.3 Fortalecer las regulaciones emitidas al sector financiero y bancaria

Dentro de las importantes buenas prácticas de detectadas en Argentina, se identificó principalmente la importancia de contar con regulación del sistema financiero que cubra los siguientes aspectos: recolección de información, entrega de información y el establecimiento de medidas de seguridad. Por ejemplo, generando normatividad que obligue a las instituciones financieras a contar con un estándar mínimo de datos requeridos a sus personas usuarias a fin de contar con mayores evidencias que resultan cruciales cuando se está en la investigación de un fraude financiero cibernético, lo segundo es contar con normas que obliguen a las instituciones bancarias a entregar la información bancaria de manera inmediata cuando le son solicitadas por la autoridad en el marco de una investigación y finalmente la obligación de contar con mejores medidas de seguridad para evitar que las víctimas entreguen sus datos de seguridad, esto implica generar sistemas de alerta para evitar que generen medidas de seguridad adecuada en diversos movimientos relevantes.

Por lo cual, se recomienda hacer un especial diagnóstico de las actuales regulaciones en México a fin de poder ajustarlas a los mayores estándares que garanticen contar con la regulación financiera adecuada tanto para prevenir, detectar, investigar y sancionar el delito de fraude financiero cibernético.

9.1.4 Desarrollar un protocolo de actuación y operación para la investigación y persecución de fraude financiero cibernético

Uno de los aspectos cruciales es la clarificación de roles de los operadores involucrados y homologación de criterios de actuación para la investigación y persecución del fraude financiero cibernético. Si bien diversas instituciones han planteado la intención de generar documentos con esa finalidad, es de vital importancia que estos no sea esfuerzos aislados y temporales, sino que se concentren un documento uniforme que atienda la problemática de manera sistémica y que tenga la fuerza vinculatoria para dotarlo de aplicación y operación. Por ello, es que se sugiere impulsar la creación de un protocolo único de actuación para los delitos de fraude financiero cibernético que cubra las distintas vertientes y modalidades de delitos en contra de instituciones financieras y de personas usuarias del sistema financiero y bancario en México.

En este caso, resulta de especial relevancia tomar en consideración las aportaciones presentadas por los representantes de la Fiscalía General de la República quienes externaron que dentro de los elementos clave para tener resultados de éxito en la investigación y persecución del fraude financiero cibernético, se destaca en primer lugar la inmediata y adecuada conservación de la evidencia, así como la eficaz interrelación entre los roles a desempeñar por parte del Ministerio Público, policías, peritos e especialmente con las víctimas del delito, a efecto de allegarse de la información y datos de manera pronta y expedita y con ello lograr un mejor resultado. Por ello, es que la existencia de un protocolo que determine estos estándares mínimos a nivel nacional implicaría una mejora sustancial en la eficacia de las investigaciones.

9.2 Recomendaciones operativas y procedimentales

9.2.1 Fortalecer e incentivar la presentación de denuncias

Una de las principales limitantes para reducir los índices de impunidad en la comisión del delito de fraude cibernético, es incentivar la presentación de denuncias a través de distintos mecanismos y darle seguimiento activo ante el Ministerio Público, por lo que se sugiere impulsar en las personas usuarias la denuncia y fortalecer las acciones para que las entidades financieras que sean objeto de este tipo de delito, complementado con algún mecanismo de supervisión por las autoridades, tales como la CONDUSEF, la CNBV y el Banco de México, cuenten con los elementos necesarios para que puedan dar seguimiento en el ámbito de sus facultades

Además, resulta de especial relevancia que estas instituciones emitan y vigilen el cumplimiento de disposiciones que obliguen a las entidades financieras a cooperar de manera mucho más eficiente y rápida en caso de que ellas o sus personas usuarias sean víctimas de un fraude financiero cibernético.

9.2.2 Migrar a un modelo de investigación activa del fraude financiero cibernético

Los casos de delitos de fraude financiero cibernético son en la mayoría de los casos desarrollados por estructuras criminales que operan con patrones similares ya sea en el plano nacional o internacional. Sin embargo, el modelo de investigación actual está centrado en un esquema reactivo y segmentado de caso a caso, por lo que se sugiere que tanto la Fiscalía General como las fiscalías de las entidades federativas migren a un modelo activo en el cual con la información que se general tanto de las denuncias que se reciben, los boletines del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información y la cooperación internacional, se detonen investigaciones activas con el enfoque de atención del fenómeno criminal de manera sistémica no del caso a caso de manera aislada.

9.2.3 Mejorar la eficiencia los procesos de investigación y persecución del delito mediante modelos de investigación especializada

Se advierte que no todos las y los Ministerios Públicos cuentan con procesos y estrategias adecuadas para el diseño y ejecución de los planes de investigación del delito de fraude financiero cibernético, por lo que se recomienda el diseño y pilotaje de herramientas metodológicas operativas que hagan mucho más efectiva la investigación y persecución de estos delitos. Es de especial relevancia que estas herramientas contemplen el enfoque tanto federal como de las entidades federativas, así como de todas las instituciones involucradas en la detección, investigación y persecución del fraude financiero cibernético, para lo cual resulta de gran relevancia tomar como punto de partida los esfuerzos que se realizan en el marco del Grupo de Respuesta a Incidentes Sensibles del Seguridad de la Información.

9.2.4 Establecer un plan continuo de capacitación y profesionalización

Otra de las principales limitantes para la atención de los delitos de fraude cibernético es la ausencia del entrenamiento especializado que considere la formación y capacidades técnicas por parte de las autoridades del sistema de justicia penal, por lo que resulta de extrema relevancia desarrollar un plan nacional de capacitación y profesionalización para las autoridades del sistema de justicia penal involucradas en la investigación, persecución y adjudicación de estos delitos conforme a cursos de formación y capacitación que tengan mayor aceptación a nivel regional e internacional.

9.3 Recomendaciones de coordinación interinstitucional

9.3.1 Articular los mecanismos de orientación y asesoría a víctimas

Actualmente, las personas víctimas de fraude financiero cibernético no cuentan con una especial claridad respecto de la autoridad a la que deben acudir y los requisitos que se deben llenar para presentar una denuncia y dar seguimiento su caso, por lo que se sugiere continuar con los esfuerzos en la atención a víctimas por parte de la CEAV, la CONDUSEF y las fiscalías federal y local, a efecto de que se implemente una guía única de difusión en la que se pueda dar a conocer la ruta de atención y seguimiento, así como los actos mínimos que una persona víctima debe llevar a cabo para la denuncia y atención inmediata de su caso.

9.3.2 Fortalecer cooperación en la investigación criminal de la FGR y de las fiscalías de las entidades federativas

Se considera que la articulación entre las diversas instituciones tanto del ámbito federal como local que participan en la detección, investigación y persecución del fraude financiero así como la armonización de su actuación es de crucial importancia, por lo cual, se sugiere fortalecer y complementar el Grupo de Respuesta a Incidentes de Seguridad de la Información con las y los operadores del ámbito local, así como incluir un enfoque adicional que vaya dirigido no solo a la atención de incidentes, sino también a acciones de mejora para la investigación y sanción de estos delitos. Asimismo, se sugiere dar continuidad al decálogo que está en desarrollo por parte del Banco de México y la CNBV para buscar que este proyecto pueda tener un contenido y radio de acción de mayor alcance. Además, resulta de especial relevancia que estas autoridades, en el ámbito de sus atribuciones, emitan y vigilen el cumplimiento de disposiciones que puedan generar mayores incentivos para la que las instituciones financieras cooperen de manera o más eficiente y rápida en caso de que ellas o sus personas usuarias sean víctimas de un fraude financiero cibernético.

9.3.3 Fortalecer y unificar la información que se obtiene de los puntos y redes de contacto 24/7 a nivel internacional

Se detecta que actualmente se cuenta con puntos de contacto en el ámbito de ciberdelincuencia tanto en la Agencia de Investigación Criminal de la fiscalía general de la República, así como la Guardia Nacional por lo que se sugiere articular y orientar los esfuerzos de contacto internacional especialmente para fortalecer los esquemas para compartir evidencias y para la detección de tipologías novedosas.