LIII GELAVEX
Reunión del Grupo de Expertos para el control del Lavado de Activos

OEA | DDOT

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

UIF UNIDAD DE INTELIGENCIA FINANCIERA MÉXICO

Ministerio de la Presidencia Costa Rica
Instituto Costarricense sobre Drogas
ICD

DEPARTAMENTO CONTRA LA DELINCUENCIA ORGANIZADA TRANSNACIONAL (DDOT)
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

LII REUNIÓN (VIRTUAL) DEL GRUPO DE EXPERTOS
PARA EL CONTROL DEL LAVADO DE ACTIVOS
16 de Noviembre de 2022
Washington DC – Estados Unidos de América

OEA/Ser.L/LIII.4.53
DDOT/LAVEX/DOC.6/22
Original: Español
Textual

Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA

2022

LIII GELAVEX
Reunión del Grupo de Expertos para el control del Lavado de Activos

OEA DDOT

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

UIF UNIDAD DE INTELIGENCIA FINANCIERA MÉXICO

Ministerio de la Presidencia Costa Rica
Instituto Costarricense sobre Drogas
ICD

53 REUNIÓN DEL GRUPO DE EXPERTOS
PARA EL CONTROL DEL LAVADO DE ACTIVOS
17 de noviembre de 2022

Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA

Subgrupo de Decomiso y Cooperación Internacional

2022

INTRODUCCIÓN

El Grupo de Expertos para el Control de Lavado de Activos (GELAVEX), en su en su XXIV Reunión plenaria que tuvo lugar del 7 al 9 de noviembre de 2007, en la ciudad de Santiago de Chile, definió como sus áreas de acción el decomiso, extinción o pérdida de dominio, organismos de recuperación de activos, coordinación e integración entre las unidades de inteligencia financiera (UIF) y los organismos de persecución e investigación, y financiamiento del terrorismo.

El GELAVEX preparó el Plan estratégico para el Trienio 2021-2023 del Grupo en la XLIX Reunión celebrada formato virtual desde Asunción Paraguay el 10 de noviembre de 2020.

La Planificación Estratégica 2020-20231, constituye la pauta para las actividades a desarrollar por el Grupo en este trienio. De acuerdo con la Planificación Estratégica 2020-2023 aprobada, el Subgrupo de Trabajo en Cooperación Internacional y Decomiso trabaja en:

- Impulsar la creación de la Red de Administración de Activos Ilícitos a nivel hemisférico o subregional, con apoyo de la Secretaría Técnica (DDOT);
- Propiciar la creación de un modelo de repartición de bienes, como documento de referencia para los Estados miembros de la OEA;
- Desarrollar un trabajo de identificación y análisis de las herramientas con las que cuentan las oficinas de administración de activos para la gestión de bienes sujetos a decomiso, como bases de datos o programas informáticos para llevar inventarios, a fin de crear un modelo conceptual que tenga un denominador común mínimo de referencia para los Estados a nivel hemisférico, incluyendo directrices para compartir información a nivel externo;
- Desarrollar un estudio sobre la conveniencia de avances en el procesamiento electrónico de solicitudes de cooperación legal internacional en materia de lavado de activos.

[1] Organización de Estados Americanos, Grupo de Expertos para el control del Lavado de Activos (GELAVEX), "Planificación Estratégica 2020-2023", *op. cit.*

- Desarrollar trabajos para favorecer la Cooperación Internacional y Decomiso de Bienes vinculados a nuevas tendencias delictivas asociadas al lavado de activos;
- Desarrollar herramientas para facilitar la cooperación en materia de administración de bienes sujetos a Decomiso.

Para el período 2021-2022, con base en lo anterior el Subgrupo de Decomiso y Cooperación Internacional debe elaborar, entre otros:

- Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA.

Sin duda alguna, la tecnología llegó para la simplificación de la vida. Sin embargo, esto ha conllevado que sea utilizada para la comisión de ilícitos, ya que casi cualquier delito puede cometerse usando o a través de la tecnología. Y sin duda, uno de los usos que se le ha dado a la tecnología es precisamente el lavado de activos. De hecho, en algunos países parece haber existido un repunte durante los dos primeros años de la pandemia del COVID 19.

OBJETIVO GENERAL

El objetivo general de un diagnóstico es realizar un proceso de planeación incluyente y participativo para conocer a determinada situación o problemática de una región y así proponer acciones oportunas al respecto. En el caso del diagnóstico encomendado, su objetivo es precisamente conocer si los Estados miembros de la región cuentan con los requerimientos tanto legales, tecnológicos, humanos y de capacitación para hacer frente a esta forma de lavar activos.

METODOLOGÍA

De acuerdo con el plan propuesto por la Presidencia del GELAVEX, se realizaron reuniones. Inicialmente, con la Presidencia y Vicepresidencia de GELAVEX y la Secretaría Técnica, para exponer observaciones y consideraciones con relación al tema objeto del trabajo.

Posterior a la reunión, la Secretaría Técnica extendió una cordial invitación a los países de la región y a los invitados al grupo de expertos, atendiendo el llamado los siguientes: Panamá, Uruguay, Colombia, México, Argentina, Perú, Paraguay e INTERPOL.

En la reunión sostenida con las únicas delegaciones que pudieron finalmente acudir al llamado se acordó la necesidad de contar realmente con información de los países de la región, para que el documento cumpla precisamente de plasmar la realidad de la región en cuanto al tema propuesto.

Es así como se define que la forma más expedita y que representa una menor carga para las delegaciones representadas en el GELAVEX, es la formulación de un cuestionario que permita al subgrupo de trabajo obtener la información necesaria para cumplir con el mandato del plenario respecto al diagnóstico.

Debido a ello se elaboró un borrador del cuestionario que se presentó en la reunión plenaria del primer semestre de 2022. Su propósito fue que el grupo de expertos pueda tanto manifestar su satisfacción respecto al abordaje de las preguntas y el contenido esperado, así como presentar sus propuestas de mejora de su redacción y alcance.

Habiendo sido aprobado el cuestionario en esa reunión plenaria, se remitió solicitud a la Secretaría Técnica para que sea circulado entre las delegaciones, con el fin compilar la información para presentar el informe final en la reunión del GELAVEX del segundo semestre.

ANTECEDENTES

La Organización de las Naciones Unidad advierte que no existe un concepto uniforme, pero que se puede definir a la ciberdelincuencia como un acto que infringe la ley, que se comete a través de las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, páginas web y tecnología o para facilitar un delito. Tiene la ventaja con relación a los delitos comunes en que no tiene barreras físicas o geográficas y sin duda alguna, se puede cometer de una forma más fácil y veloz, aprovechando el desconocimiento que existe debido a su novedad.

Por su parte EUROPOL distingue la ciberdelincuencia en delitos *dependientes de los medios informáticos* (es decir, «todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación» y en delitos propiciados por los medios informáticos (es decir, delitos comunes facilitados por Internet y las tecnologías digitales).

Con el objetivo de crear "una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional", se crea y suscribe el Convenio del Consejo de Europa sobre la Delincuencia Cibernética (Budapest, 2001). Pese a que su origen es europeo, su artículo 37 establece que cualquier Estado que no sea miembro del Consejo de Europa puede convertirse en Parte mediante su adhesión o ratificación, si el Estado está preparado para implementar el convenio.

De acuerdo con la información en el sitio web de la ONU, a junio 2021, 66 Estados ya forman parte del Convenio (países europeos, Argentina, Australia, Canadá, Cabo Verde, Chile, Colombia, Costa Rica, Estados Unidos de América (EUA), Filipinas, Ghana, Israel, Japón, Mauricio, Marruecos, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga, otros 2 países ya lo firmaron (Irlanda y Sudáfrica) y 9 países han sido invitados a adherirse (Benín, Brasil, Burkina Faso, Guatemala, México, Nueva Zelanda, Níger, Nigeria y Túnez).

Este convenio surge como una respuesta ante la ventaja que resulta para la delincuencia organizada transnacional el uso de las tecnologías de información y comunicación, así como de todos los medios tecnológicos que facilitan el uso de servicios

financieros. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados parte de él. En el convenio se establecen las medidas que deberán adoptar los países con relación a los delitos cibernéticos, categorizados de la siguiente forma:

1. Delitos contra la confidencialidad, la integridad y la accesibilidad (*Triada CIA*) de los datos y sistemas informáticos:
    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la comisión de delitos.

2. Delitos informáticos:
    - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido:
    - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (copia y distribución de programas informáticos, o la piratería informática).

Adicionalmente y por disposición de lo establecido en su Capítulo III, proporciona un marco legal para la cooperación internacional en materia de ciberdelito y evidencia digital. El convenio establece disposiciones generales y específicas para la cooperación entre las partes, tanto con relación a ciberdelitos como con relación a cualquier delito relacionado con evidencias electrónicas.

Por su parte, la Organización de Estados Americanos (OEA) a través Departamento de Cooperación Jurídica Internacional (DCJI) promueve la cooperación jurídica internacional en materia de justicia y lucha contra la corrupción y el fortalecimiento de la cooperación

entre los Estados en materia de asistencia mutua penal y combate de los delitos cibernéticos en el marco de la Reunión de Ministros de Justicia u otros Ministros, Procuradores o fiscales generales de las Américas (REMJA). Adicionalmente, REMJA junto con socios estratégicos procura y coordina capacitaciones para oficiales de gobierno para el enjuiciamiento exitosos de los delitos cibernéticos, talleres legislativos para actualizar las leyes en materia de delito cibernético y para promover mejores prácticas contra los delitos cibernéticos.

Con fundamento en estos documentos, se consultó a las delegaciones que conforman el GELAVEX, sobre aspectos específicos que permitan elaborar el presente diagnóstico regional. Participaron con sus respuestas Brasil, Colombia, Ecuador, Guyana, México, Panamá, República Dominicana y Uruguay.

RESULTADOS CUESTIONARIO PARA DIAGNÓSTICO

Los siguientes fueron los resultados al cuestionario remitido a todas las delegaciones por parte de la Secretaría Técnica, a instancia del Subgrupo de Decomiso y Cooperación Internacional:

❖ Cuenta su país con legislación sobre ciberdelitos

Argentina responde afirmativamente. Sobre la normativa, detalla las siguientes:

- Ley 27.436 modifica el artículo 128 del Código Penal de la Nación e incluye los delitos relacionados a las imágenes de abuso sexual de menores (antes conocido como pornografía infantil) y su Decreto Reglamentario 349/2018.
- Ley 26.904 incorpora los delitos de grooming al Código Penal de la Nación y su Decreto Reglamentario PEN 2036/2013.
- Ley 25.930 incorpora una disposición vinculada a la defraudación mediante el uso de tarjetas de compra, crédito o débito al Código Penal de la Nación y su Decreto Reglamentario PEN 1232/2004.
- La Ley 27.590 que crea el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes y su Decreto Reglamentario PEN 407/2022.

- Ley 25.326 de Protección de los Datos Personales y su Decreto Reglamentario PEN 1558/2001.
- Resolución 234/2016 del Ministerio de Seguridad de la Nación aprueba el "Protocolo general en la investigación y proceso de recolección de pruebas en ciberdelitos"
- Ley 27.411 que aprueba la Convención sobre Ciberdelito del Consejo de Europa.
- Resolución 1291/2019 del Ministerio de Justicia y Derechos Humanos de la Nación que crea la Unidad de Delitos Informáticos y Evidencia Digital (RED 24/7).

Bolivia, de acuerdo con la respuesta de la Fiscalía General, si cuenta con legislación. Informan que las conductas ilícitas cometidas por ciberdelincuentes se encuentran reguladas en el Título XII, Capítulo XII (Delitos informáticos) del Código Penal (Ley 1768), con los *nomen iuris* de: Manipulación informática (art. 363 Bis.) y Alteración, acceso y uso indebido de datos informáticos (art. 363 Ter.).

En **Brasil**, de acuerdo con lo que informan, no existe una ley específica que se ocupe exclusivamente de los delitos cibernéticos, porque la conceptualización misma de lo que debe considerarse este instituto está sujeta a discusión, interna e internacionalmente. La principal normativa que señalan es la siguiente, que tiene respaldo constitucional:

- Marco Civil de Internet (Ley N° 12.965 de 23 de abril de 2014)
- Estatuto del Niño y del Adolescente (Ley Nº 8069 de 13 de julio de 1990 - principalmente artículos 241-A a 241-E)
- Código Penal (DECRETO-LEY Nº 2.848, 7 DE DICIEMBRE DE 1940 y sus numerosos cambios a lo largo de los años) - Estos son algunos ejemplos de tipos penales que aplica en el campo de los delitos cibernéticos: 154-A y sus párrafos (piratería de dispositivos informáticos) - para varios casos de delitos de alta tecnología y algunos casos de fraude bancario electrónico; art. 155, §4, B y C (robo por fraude por dispositivo electrónico o informático) - especialmente para casos de fraude bancario electrónico, 158 (extorsión) - especialmente para ataques de ransomware, Art. 171, §2º A y §2º B (estafa/fraude electrónico), Art. 217-A (violación de personas vulnerables), 218-C (Divulgación de escena de violación o escena de violación de vulnerable, escena de sexo o pornografía), 265 (Ataque a la seguridad de los servicios públicos - para algunos casos de delitos de alta tecnología), 266 (Interrupción o interrupción de la información telegráfica, telefónica, informática,

telemática o de utilidad pública - para algunos casos de delitos de alta tecnología) y Art. 288 (asociación delictiva)

- Código de Procedimiento Penal (DECRETO-LEY Nº 3.689, AL 3 de octubre de 1941)
- Ley de Organizaciones Criminales (ley N° 12.850, de 2 de agosto de 2013)
- Ley de Lavado De Activos (ley N° 9.613, 3 de marzo de 1998)

Aclaran que la atribución de la Policía Federal en Brasil está restringida. Por lo tanto, hay una serie de otros delitos investigados a nivel estatal por la Policía Civil (policía judicial estatal), que pueden clasificarlos como "delitos cibernéticos". Por ejemplo, delitos contra la propiedad intelectual.

Chile indica que si cuenta con legislación sobre ciberdelitos. Informa que la principal legislación viene dada por la Ley N°21.459, la cual se encuentra vigente desde el 20 de junio de 2022. Además, hay normas relativas a esta materia en la Ley N°20.009.

Costa Rica también tiene legislación. Está contenida en una Sección del Código Penal denominada Delitos Informáticos, así como en el Convenio de Budapest. También existe un proyecto de ley para crear una ley especial.

Ecuador informa que cuenta con legislación en la materia. Se trata del Código Orgánico Integral Penal- publicado en el Registro Oficial N° 180 de 10 de febrero del 2014, específicamente sobre los numerales relacionados con supuestos de hechos con la utilización de las TIC´s dispuestos en los Art.103-104-190-173-17-229-230-231-232-233-234. También la Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos.

Guatemala no se queda atrás y regula el tema a través de los artículos del 274 “A” al 274 “H”, 190 bis, 190 ter, y 198 del Código Penal Decreto Número 17-73 del Congreso de la República de Guatemala y de artículos del 21 al 31 de la Ley de Terminales Móviles Decreto Número 8-2013 del Congreso de la República de Guatemala. Además, se cuenta con Iniciativa de Ley Número 4055 Ley de Delitos Informáticos

Honduras también cuenta con legislación, contenida en el Decreto 130-2017 contentivo del Código Penal (Titulo XXII) “Seguridad de las Redes y de los Sistemas

Informáticos". Señalan que dentro de la referida normativa diversos tipos penales que hacen uso de la Informática para su comisión, por ejemplo, estafas informáticas, pornografía infantil (Grooming y Sexting), violación y revelación de secretos y otros.

México también cuenta con legislación sobre ciberdelitos. La normativa está incluida en gran cantidad de instrumentos legales, a saber:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley de Seguridad Nacional.
- Ley General del Sistema Nacional de Seguridad Pública.
- Ley de la Guardia Nacional y su Reglamento.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley Orgánica de la Administración Pública Federal.
- Le y de Instituciones de Crédito (Capítulo IV, Art. 112 Quáter)
- Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas (Artículos 15 al 18).
- Ley Federal de Protección de la Propiedad Industrial (Artículo 223)
- Reglamento de la Oficina de la Presidencia de la República
- Plan Nacional de Desarrollo 2019 – 2024.
- Programa Nacional de Seguridad Pública.
- Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024.
- Estrategia Digital Nacional 2021 - 2024
- Códigos Penales Federal y de las Entidades Federativas
- Código Nacional de Procedimientos Penales
- Acuerdo A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal

Panamá no cuenta con legislación sobre ciberdelitos. Pero informan que, en la Asamblea Nacional de Diputados, fue presentado el 12 de julio de 2021 el Proyecto de Ley

N° 632, que modifica y adiciona artículos del Código Penal y del Código Procesal Penal, relacionado con los ciberdelitos. El proyecto para la fecha de respuesta del cuestionario se encontraba en primer debate. Fue facilitado el link: https://www.asamblea.gob.pa/APPS/SEG_LEGIS/PDF_SEG/PDF_SEG_2020/PDF_SEG_2021/2021_P_632.pdf.

Paraguay también cuenta con legislación, específicamente la Ley 4439/11.

Desde el 22 de octubre del 2013, responde **Perú** que cuenta con un marco normativo especializado, denominado "Ley de Delitos Informáticos" Ley 30096. En él se recoge parte el contenido del Convenio sobre Ciberdelincuencia de Budapest, ratificado recién por el Perú en marzo del 2019 y vigente desde el 01 de diciembre del mismo año 2019.

Posteriormente, mediante Ley 30171, publicada el 10 de marzo del 2014, se modificó la Ley 30096. A partir de ello, Perú regula los siguientes delitos: acceso ilícito, atentado a la integridad del dato, atentado a la integridad de sistemas, proposiciones a niños y adolescentes con fines sexuales por medios tecnológicos (Grooming), interceptación de datos informáticos, fraude informático, suplantación de identidad, abuso de mecanismos y dispositivos informáticos. La ley especializada también contempla cuatro modalidades agravadas en las que se contempla la comisión de estos delitos bajo organización criminal.

República Dominicana no se queda atrás con relación a la legislación sobre ciberdelitos. Los documentos relevantes remitidos por la delegación son:

- Resolución del Congreso Nacional núm. 158-12, del 11 de junio de 2012, que aprueba el Convenio sobre la Cibercriminalidad, suscrito el 23 de noviembre de 2001, en Budapest.
- Ley núm. 53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología.
- Ley núm. 126-02 sobre el Comercio Electrónico, Documentos y Firmas Digitales, del 4 de septiembre de 2002.
- Ley No. 310-14 que regula el envío de correos electrónicos comerciales no solicitados (SPAM), promulgada el 8 de agosto de 2014. - Ley núm. 1-12, del 25 de enero de 2012, que establece la Estrategia Nacional de Desarrollo 2030.

- Decreto núm. 313-22, del 14 de junio de 2022, que establece y regula la Estrategia Nacional de Ciberseguridad 2021-2030.
- Decreto núm. 230-18, del 15 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021.
- Decreto núm. 71-21, del 8 de febrero de 2021, que crea el Gabinete de Transformación Digital.
- Decreto núm. 527-21, del 26 de agosto de 2021, que aprueba los objetivos y líneas de acción de la Agenda Digital 2030 como estrategia nacional de transformación digital y define los objetivos a corto, mediano y largo plazo.
- Decreto núm. 229-07 que ratifica la OPTIC y establece ámbitos en los cuales se desarrollará el gobierno electrónico, del 19 de abril de 2007.
- Decreto núm. 709-07 que instruye a toda la Administración Pública a cumplir con las normas y estándares tecnológicos elaborados por la OPTIC, del 26 de diciembre de 2007.
- Resolución de la Junta Monetaria núm. 181101-02, del 1 de noviembre de 2018, que establece el Reglamento de Seguridad Cibernética y de la Información

Uruguay está creando legislación en el tema. actualmente se encuentra en consideración un proyecto de ley sobre tipificación del ciberdelito, por lo que técnicamente no es ley aún, pero sí se encuentran tipificados delitos vinculados con la temática en las siguientes normas: Ley N°18600 del 21 de setiembre de 2009 sobre Documento Electrónico y Firma Electrónica. Admisibilidad. Validez y Eficacia (artículo 4) ; Ley N° 17.815 del 6 de setiembre de 2004 y sus modificativas sobre Violencia Sexual contra Niños, Adolescentes e Incapaces (Pornografía infantil); y Ley N° 9739 del 17 de diciembre de 1937 y sus modificativas sobre Derechos de Autor (artículo 46 y siguientes. Estas normas se encuentran publicadas en la página de IMPO del Estado Uruguayo.

❖ Cuenta su país con medidas procesales necesarias que aseguren la investigación y procesamiento de los delitos cibernéticos en forma efectiva, eficaz y oportuna y que permitan la cooperación entre los Estados en el marco de esas mismas actividades.

Argentina responde afirmativamente. Respecto de medidas de cooperación internacional para la investigación y procesamiento de delitos cibernéticos menciona las siguientes:

Su ordenamiento jurídico cuenta con la Ley N° 24.767 de Cooperación Internacional en Materia Penal, que brinda un marco regulatorio a partir del cual se sientan las bases para la asistencia en la investigación y juzgamiento de delitos entre nuestro país y cualquier otro Estado que lo requiera. En ella se establecen las reglas de procedimiento aplicables a todas las solicitudes de asistencia judicial internacional y de extradición que recibe Argentina. También, aunque sólo para los casos en los que no exista tratado que vincule a su país con el Estado requirente y establece las condiciones bajo las cuales se otorgará la asistencia.

La Autoridad Central designada por la República Argentina para todos los Convenios sobre asistencia en materia penal (y para Convenios que contengan normas sobre asistencia en materia penal) es el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto. La excepción es el Tratado de Asistencia Jurídica Mutua en Asuntos Penales con los Estados Unidos de América, en el cual la Autoridad Central designada es el Ministerio de Justicia y Derechos Humanos.

La asistencia jurídica en materia penal entre la República Argentina y los Estados Unidos se regula por dos instrumentos: el Tratado de Asistencia Jurídica Mutua en Asuntos Penales, suscripto en Bs. As. el 4 de diciembre de 1990 y aprobado por Ley Nº 24.034 (bilateral); y la Convención Interamericana sobre Asistencia Mutua en Materia Penal, suscripta en Nassau, Bahamas, el 23 de mayo de 1992, aprobada por Ley Nº 26.139. Ambos instrumentos coexisten y se encuentran vigentes.

Por otro lado, la Unidad de Delitos Informáticos y Evidencia Digital -creada en noviembre de 2019 por Resolución N° 1291/2019 del Ministerio de Justicia y Derechos Humanos- funciona bajo la órbita de la Dirección Nacional de Asuntos Internacionales (DNAI) de esa cartera ministerial. A través de dicha Resolución se dispone el funcionamiento de la Unidad 24/7, en aplicación de lo dispuesto por el artículo 35 del Convenio de Budapest contra la Ciberdelincuencia (Red 24/7). El convenio establece que cada Estado Parte debe contar con un punto de contacto localizable las 24 horas los 7 días de la semana y entre sus funciones se encuentra la de brindar asesoramiento técnico y tramitar solicitudes de

conservación rápida de datos electrónicos, en virtud de lo dispuesto por el artículo 29 del Convenio de Budapest.

Bolivia señala, a través de la respuesta de la Fiscalía General, que los mecanismos legales que aseguran la investigación y procesamiento de los delitos informáticos se encuentran previstos, sobre todo, en las Leyes 1768 (Código Penal), 1970 (Código de Procedimiento Penal), Ley 260 (Ley Orgánica del Ministerio Público) y Ley 025 (Ley del Órgano Judicial).

La legislación de **Brasil**, incluidas las convenciones internacionales efectivamente internalizadas por el Brasil, como la de Palermo, prevé medidas como preservación, registro e incautación, detención, audiencia de testigos, infiltración policial, etc., así como también permite la cooperación entre los Estados en el contexto de las actividades de ciberdelincuencia. También son relevantes las disposiciones del Marco Civil de Internet (Ley Nº 12.965 del 23 de abril de 2014) relativas a la preservación y recopilación de datos, así como su aplicabilidad a las empresas extranjeras que opera un servicio que se ofrece al público.

Sin embargo, con la llegada de la pandemia de COVID-19, que causó una explosión de cibercrimen en el planeta, incluyendo y aumentando significativamente el nivel de sofisticación y la velocidad de las acciones delictivas, Brasil reconoce la necesidad de que el Convenio de Budapest entre vigor internacionalmente, ya que las disposiciones contenidas en él proporcionarán una actualización de la legislación penal y procesal brasileña, tanto en cuanto a medidas de cooperación internacional como con la necesaria normalización de conceptos.

Chile si cuenta con medidas procesales. El Título II de la Ley N°21.459 establece reglas especiales de procedimiento que pretenden generar una investigación efectiva, eficaz y oportuna, adaptándose a las exigencias del convenio de Budapest. Sin embargo, estas normas entraron en vigor en junio del año 2022, por lo que informan que aún no cuentan con datos concretos. Hasta antes de estas normas, señala la delegación que las herramientas para la persecución de los delitos informáticos eran completamente deficientes. En materia de cooperación internacional, no existen reglas especiales, pero la Unidad de Cooperación Internacional y Extradiciones (UCIEX) está encargada de la colaboración y coordinación internacional con las distintas agencias pertinentes.

Costa Rica no cuenta con una legislación especial al respecto, se siguen las determinadas en el Código Procesal Penal.

Ecuador pese a tener legislación sobre ciberdelitos, señala que no cuenta con medidas que aseguren la investigación y procesamiento de ellos en el sentido de la pregunta.

Guatemala responde afirmativamente e indica que están contenidas en el Código Procesal Penal Decreto Número 51-92 del Congreso de la República. Entre las medidas, se deberán observar las siguientes:

El proceso penal guatemalteco tiene por objeto la averiguación de un hecho señalado como delito o falta y de las circunstancias en que pudo ser cometido; el establecimiento de la posible participación del sindicado; el pronunciamiento de la sentencia respectiva, y la ejecución de esta.

Al respecto, el artículo 24 del Código en referencia establece que la acción penal corresponde al Ministerio Público, sin perjuicio de la participación que se concede al agraviado. Por tanto, deberán ser perseguidos de oficio todos los delitos, incluyendo los delitos cibernéticos.

En ese sentido, el artículo 107 de esta ley, establece que el ejercicio de la acción penal corresponde al Ministerio Público como órgano auxiliar de la administración de justicia conforme las disposiciones de ese código y que tendrá a su cargo el procedimiento preparatorio y la dirección de la Policía Nacional Civil en su función investigativa dentro del proceso penal.

Adicionalmente, el artículo 181 fundamenta al Ministerio Público y los tribunales de justicia el deber de procurar por sí, la averiguación de la verdad mediante los medios de prueba permitidos y de cumplir estrictamente con los preceptos del Código Procesal Penal.

En **Honduras** las medidas establecidas en su código procesal penal, Decreto N°9-99-E, donde establecen cuáles son los procedimientos y medidas para la investigación de todos los delitos, entre ellos, los delitos cibernéticos.

México también cuenta con medidas. La Fiscalía General de la República (FGR), a través de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT) de la Agencia de Investigación Criminal, realiza la investigación de los delitos cibernéticos y conductas ilícitas asociadas a éstos.

Todos los actos de investigación se apegan el Modelo de Investigación Cibernética que se aplica en la UICOT, apoyado con el uso de técnicas de investigación y herramientas tecnológicas especializadas en búsquedas, análisis y procesamiento de datos

Agrega que algunas de las medidas también están contenidas en:

- Estrategia Digital Nacional 2021 - 2024
- Códigos Penales Federal y de las Entidades Federativas
- Código Nacional de Procedimientos Penales
- Acuerdo A/009/15 por el que se establecen las directrices que deberán observarlos servidores públicos que intervengan en materia de cadena de custodia
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Panamá también cuenta con medidas procesales necesarias. Mediante Ley N° 14 del 18 de mayo de 2007, en el Código Penal se tipifican delitos que involucran medios tecnológicos, así como que violentan la seguridad informática: https://www.gacetaoficial.gob.pa/pdfTemp/26519/27147.pdf.

La Constitución Política de Panamá, producto del numeral 4 del artículo 220, obliga al Ministerio Público a perseguir los delitos y contravenciones de disposiciones constitucionales y legales. Aunado a ello, mediante la Ley No. 63 de 28 de agosto de 2008, se adoptó el Código Procesal Penal, que establece que, para el ejercicio de la persecución penal, el Ministerio Público dirige la investigación de los delitos, practicando u ordenando la ejecución de las diligencias útiles para determinar la existencia del ilícito y los responsables, auxiliándose de los organismos de investigación y la fuerza policial.

Adicionalmente, desde el 22 de octubre de 2013 aprobaron el Convenio de Budapest mediante la Ley N° 79.

En materia de cooperación internacional, resaltan que de conformidad con lo establecido en el artículo 4 de su Constitución Política, acatan las normas del Derecho Internacional y en ese sentido, aprobaron la Ley No. 11 de 31 de marzo de 2015. Esa ley "dicta disposiciones sobre asistencia jurídica internacional en materia penal", (https://www.gacetaoficial.gob.pa/pdfTemp/27752/50288.pdf), la cual establece que Panamá a través de sus entidades competentes facilitará la más amplia asistencia internacional posible en las actuaciones, procesos e investigaciones penales cuando sean requeridas por otros Estados, con fundamento en los Tratados Internacionales ratificados por el país o, en su defecto, con base al principio de reciprocidad entre las naciones. Debido a la anterior, el país es capaz de brindar cooperación internacional eficiente, efectiva y oportuna a otras jurisdicciones en materia de delitos cibernéticos.

Paraguay no cuenta con las medidas procesales necesarias.

Perú responde afirmativamente e indica que las medidas que permiten alcanzar efectividad y eficacia corresponden, en gran manera a las mismas acciones aplicadas para los delitos convencionales, a partir de la apertura de una investigación preliminar.

Sin embargo, a partir del reconocimiento del principio de libertad probatoria contenida en el artículo 157.1 del Código Procesal Penal, es posible tomar métodos de obtención de información de orden público, como, por ejemplo, técnicas de búsqueda en fuentes abiertas -OSINT-

De manera complementaria, el Código Procesal Penal permite, en tanto los delitos que se investiguen sean de gravedad, la ejecución de técnicas especiales de investigación, como las operaciones encubiertas, prevista en el artículo 341-A del referido código. La ley especializada permite en determinados casos, la actuación del agente encubierto informático.

Asimismo, el procedimiento especial por colaboración eficaz debidamente comprobado puede permitir la eficacia y efectividad de una investigación en delitos informáticos.

Finalmente, el marco procesal de la cooperación y asistencia internacional regulada en el código procesal penal, como en los convenios de cooperación suscritos por el Perú, así como en las representaciones que asume el Ministerio Público a través de la Unidad de Cooperación Judicial Internacional y Extradiciones, permite recabar información relevante para cada investigación.

La respuesta de **República Dominicana** también fue positiva. Señalan que el artículo 155 del Código Procesal Penal Dominicano es la base legal y procesal para la cooperación internacional por parte de los jueces y el Ministerio Público. En adición, el país es signatario del convenio de Budapest sobre delitos de alta tecnología y debido a esto también es parte de GLACY (Global Action on Cybercrime Extended), un proyecto de acción global que busca fortalecer las capacidades de los Estados en todo el mundo para aplicar la legislación sobre delitos cibernéticos y evidencia electrónica y mejorar sus habilidades para una cooperación internacional efectiva en esta área, esto le permite al país tener una red de información donde se toman medidas de carácter urgente transnacional (Red 24-7), por medio de lo que el convenio define como tratado de asistencia legal multilateral (MLAT).

En el caso de **Uruguay**, las medidas se están trabajando actualmente dado que por Ley N° 20.004 del 25 de noviembre de 2021 fue aprobado por Uruguay el Convenio Iberoamericano de Cooperación sobre Investigación Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia.

- Cuenta su país con medidas procesales necesarias que aseguren la obtención, incautación, decomiso o secuestro y mantenimiento en custodia todas las formas de evidencias electrónicas y su admisibilidad en procesos judiciales

Argentina si cuenta con esas medidas. En su respuesta al cuestionario indica que las autoridades encargadas de realizar las investigaciones y procesamientos en causas que involucran ciberdelitos utilizan las herramientas procesales existentes, establecidas en el Código Procesal Penal de la Nación (y en los Código Procesales Penales de las Provincias).

A su vez, su Código Procesal Penal Federal (CPPF), que se encuentra siendo implementado paulatinamente en la justicia federal, cuenta con disposiciones específicas al respecto. El artículo 150 establece que el juez podrá ordenar, siempre que resulte útil

para la comprobación del delito, a petición de parte, la interceptación y secuestro de correspondencia electrónica y la intervención de las comunicaciones. Señala que las empresas que brindan el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.

Por su lado, el artículo 151, que versa sobre la incautación de datos, dispone que "El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 136".

A su turno, el artículo 310 del CPPF ordena que el juez, a pedido del representante del Ministerio Público Fiscal, deberá adoptar las medidas cautelares suficientes para asegurar el decomiso de elementos informáticos, técnicos y de comunicación.

La Fiscalía General de **Bolivia** responde que las medidas procesales que permiten asegurar la obtención, custodia, secuestro, incautación, confiscación (comiso) de las evidencias electrónicas e incluso que sean admitidos en calidad de prueba, se encuentran, sobre todo, insertas en: 1. El Código de Procedimiento Penal- Ley 1970 (artículos 54, 184, 186, 222, 252, 253, 333, entre otros); 2. Código Penal - Ley 1768 (artículo 71) y: 3. Ley Orgánica del Ministerio Público - Ley 260 (artículo 40 numerales 12, 13 y 14).

Brasil si cuenta con medidas en este sentido, incluidas las convenciones internacionales internalizadas por el Brasil, prevé medidas procesales que en parte de los casos de investigación, pueden garantizar la obtención, incautación, custodia y uso admisible de pruebas electrónicas en procedimientos judiciales.

Sin embargo, destacamos: a) la necesidad urgente de mejores definiciones, a nivel normativo (legal e infra legal), sobre la responsabilidad por la custodia de cripto activos incautados; b) la controversia judicial discutida en el ADC 51 -TRIBUNAL SUPREMO FEDERAL, porque hay países que niegan la aplicación del Marco Civil de Internet a empresas extranjeras que operan en Brasil; c) la necesidad de que el Convenio de Budapest, en relación con Brasil, entre efectivamente en vigor internacionalmente, ya que las disposiciones contenidas en él proporcionarán una actualización de la legislación penal y

procesal brasileña, medidas de cooperación internacional, con impactos importantes y positivos en el campo de la prueba electrónica, además de ayudar en la necesaria estandarización de conceptos.

Chile informa que sí. Señala que se establece el comiso para los instrumentos de los delitos penados por esta ley, los efectos de que estos provengan y las utilidades que estos hayan generado. Se establece comiso por equivalencia siempre que, por cualquier circunstancia, no sea posible decomisar estas especies.

Costa Rica no cuenta con medidas especiales. Nuevamente, la referencia es a las medidas generales contendidas en el Código Procesal Penal.

Ecuador señala que existen parcialmente. Se refiere al Código Orgánico Integral Penal, que en el artículo 500 regula el proceso de análisis, valoración, recuperación y presentación del contenido digital, para cuyo mantenimiento y custodia existen el Centro de Acopio de Evidencias. Sin embargo, en lo relacionado con el decomiso o secuestro y mantenimiento de evidencia como criptomonedas, señala que no cuentan con medidas procesales que aseguren su obtención, incautación, decomiso o secuestro y mantenimiento. Sobre los medios de prueba existentes en el Código Orgánico Integral Penal, artículo 498 señala: 1) El Documento, 2) El Testimonio 3) La Pericia. Art. 454 IBIDEM se establece los principios para el anuncio y la práctica de la prueba, siendo uno de ellos la libertad probatoria.

Guatemala indica que sí. Responde que su Código Procesal Penal, Decreto Número 51-92 del Congreso de la República de Guatemala, establece en el artículo 187, la facultad del Ministerio Público, de realizar cuando sea necesario la inspección de lugares, cosas y personas porque existen motivos suficientes para sospechar que se encontrarán vestigios del delito, o se presuma que en determinado lugar se oculta el imputado o alguna persona evadida, para lo cual procederá a su registro con autorización judicial.

Respecto al secuestro de todas las formas de evidencias electrónicas y su admisibilidad en el proceso penal, de conformidad con el artículo 200 de la Ley en referencia, establece que, la orden de secuestro será expedida por el juez ante quien penda el procedimiento o por el presidente, si se tratare de un tribunal colegiado.

No obstante, en caso de peligro por la demora, el Ministerio Público podrá ordenar el secuestro, pero deberá solicitar la autorización judicial inmediatamente, consignando las cosas o documentos ante el tribunal competente.

Asimismo, el Ministerio Público podrá dictar las medidas razonablemente necesarias para proteger y aislar indicios en los lugares en que se esté investigando un delito, a fin de evitar la contaminación o destrucción de rastros, evidencias y otros elementos materiales, lo cual se fundamenta en el artículo 314 del Código Procesal Penal.

Con la finalidad de proteger todas las formas de evidencia electrónica, los efectos secuestrados serán inventariados y puestos bajo segura custodia, a disposición del tribunal correspondiente, en el Almacén Judicial, según la reglamentación dictada por la Corte Suprema de Justicia, de conformidad con el Artículo 201 del Código Procesal Penal.

Respecto a la admisibilidad de un medio de prueba, se debe de considerar que un medio para ser admitido debe referirse directa o indirectamente al objeto de la averiguación y ser útil para el descubrimiento de la vedad, por lo que únicamente se considerarán medios inadmisibles, los elementos de prueba obtenidos por medios prohibidos, tales como la tortura, la indebida intromisión en la intimidad del domicilio o residencia, la correspondencia, las comunicaciones, los papeles y los archivos privados.

Honduras también responde de forma positiva, indicando de manera general que se realiza a través del “aseguramiento de todas las evidencias digitales”.

México responde afirmativamente y señala que El Código Nacional de Procedimientos Penales contempla algunas disposiciones vinculadas a la prueba digital, entre las que destacan:

- Artículo 227, establece y define la existencia de la figura denominada Cadena de Custodia, como el sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión.
- Artículo 252, relativo a los actos de investigación que requieren autorización previa del Juez de Control, entre las que se encuentra “la intervención de comunicaciones privadas y correspondencia”.

- Artículo 291, establece la necesaria autorización judicial para llevar a cabo la intervención, la cual abarca todos los sistemas de comunicación, o programas que sean resultado de la evolución tecnológica, que permita el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación. Es importante subrayar que este mismo criterio aplica para la extracción de información de cualquier tipo de dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento, incluyendo plataformas y centros de datos remotos;
- Artículo 301, referente al deber de los concesionarios, permisionarios y demás titulares de medios o sistemas susceptibles de intervención para colaborar eficientemente con la autoridad competente.
- Artículo 303, relativo a la localización geográfica en tiempo real y solicitud de entrega de datos conservados.

Adicionalmente, y en estricto apego a lo señalado en el artículo 227, informa que existen criterios jurisprudenciales que establecen que, para su eficacia probatoria en el proceso penal, la prueba electrónica o digital debe ser obtenida lícitamente y que su recolección conste en una cadena de custodia. Este criterio se encuentra para su consulta en el siguiente link: https://sjf2.scjn.gob.mx/detalle/tesis/2013524

En este sentido, señala que la UICOT desarrolló la Guía Técnica de Cadena de Custodia de Evidencia Digital, la cual fue presentada en la XXXIX Asamblea Plenaria de la Conferencia Nacional de Procuración de Justicia (CNPJ) y aprobada el 4 de julio de 2018 por mayoría de votos de los integrantes de dicha Conferencia.

Panamá también cuenta con medidas adecuadas. Informan que el Ministerio Público, de conformidad con su Código Procesal Penal, puede decretar o solicitarle al Juez de Garantías que decrete la aprehensión provisional con miras a un eventual decomiso de los instrumentos, bienes muebles e inmuebles, valores y los productos derivados o relacionados, directa o indirectamente, con la comisión de delitos contra la administración pública, blanqueo de capitales, financieros, contra la propiedad intelectual, seguridad informática, extorsión, secuestro, pandillerismo, sicariato, terrorismo y financiamiento del terrorismo, narcotráfico y delitos conexos, contra la trata de persona y delitos conexos, delincuencia organizada, tráfico ilícito de migrantes y delitos conexos. Esos bienes quedan

a las a órdenes del Ministerio de Economía y Finanzas hasta que la causa sea decidida por el juez competente. Si la medida cautelar real de aprehensión provisional fue ordenada por el Fiscal sin la intervención del Juez de Garantías, debe ser sometida a control posterior de éste, dentro del término de diez (10) días siguientes a su ejecución.

El Código Procesal Penal de Panamá, faculta al Juez de Garantías, a solicitud del Fiscal, a decretar el secuestro penal de las cosas relacionadas con el delito, para evitar el peligro de la eventual disposición, desaparición o destrucción de los bienes sujetos a comiso. Ese instrumento cautelar real puede recaer sobre bienes muebles e inmuebles, dineros, títulos, valores, correspondencia y cuentas que se encuentren en bancos u otras instituciones de crédito públicas o privadas.

En cuanto a la incautación, se constituye en otro mecanismo que el Ministerio Público de Panamá tiene, previa autorización de un Juez de Garantías, para privar de instrumentos, dineros, valores y bienes empleados en la comisión del hecho punible o los que sean producto de este, así como también copias, reproducciones o imágenes de los objetos cuando resulten convenientes para la investigación. Esta medida puede ser complementada con la aprehensión provisional de bienes descrita, dentro de causas penales instruidas por los delitos específicos que lo permiten.

Por otro lado, la legislación panameña establece el comiso de aquellos fondos, activos y demás productos derivados de la comisión de un delito, una vez que el proceso sea decidido por un Juez competente. De igual forma, su Código Procesal Penal señala que la extinción de la acción penal no impide el comiso de los instrumentos con los que se cometió el hecho punible y de los efectos que de él provengan, ni la responsabilidad civil derivada de él.

Por otro lado, el Instituto de Medicina Legal y Ciencias Forenses, mediante Resolución No. JD-008-15, de fecha 28 de mayo de 2015, publicada en la Gaceta Oficial No.27831-A, del día 24 de julio de 2015, aprobó el “Manual de Procedimiento del Sistema de Cadena de Custodia, versión 02” y derogó la Resolución No. JD-009-11, de fecha 30 de marzo de 2011, mediante la cual se adoptó la versión 01 de dicho manual. Este manual tiene como objetivo general “establecer los criterios técnico-científicos que sirvan de fundamento al sistema de cadena de custodia en Panamá, mediante la estandarización y control de los procedimientos que llevan a cabo los servidores públicos y los particulares en

las diferentes etapas de la investigación de un hecho, con el propósito de mejorar la calidad del servicio de la administración de justicia".

Como objetivos específicos, se tienen los siguientes:

- Definir los principios para el fiel cumplimiento del sistema de cadena de custodia, con el propósito de garantizar la administración de justicia.
- Unificar y establecer procedimientos sencillos, obligatorios y de fácil aplicación para el manejo de los indicios y/o evidencias relacionadas con las investigaciones penales.
- Detallar los procedimientos para que los funcionarios y particulares realicen sus diligencias en forma ordenada, confiable y organizada, conforme a las disposiciones establecidas.

El "Manual de Procedimiento del Sistema de Cadena de Custodia, versión 02", está destinado para el uso de los servidores públicos y los particulares que se relacionen con el manejo de los indicios y/o evidencias y que están obligados, conforme al Código Procesal Penal y disposiciones establecidas sobre la materia, a garantizar el aseguramiento y conservación de las características originales y registros de continuidad, de las modificaciones que pudieran sufrir los mismos, identificando a los responsables en cada etapa desde su recolección hasta su disposición final.

El marco normativo sobre la admisibilidad de la evidencia digital como pruebas ante los tribunales, se encuentra en su Código Procesal Penal, en los artículos 17, 130, 273, 311, 376, 377, 378, 340, 346, 347, 349, 381, 406, 407, 411, 413, 414. 419 y 421. La Constitución Política de Panamá, lo regula en su artículo 29.

Paraguay no cuenta con las medidas procesales necesarias.

En el caso de **Perú**, las medidas están contenidas en el Código Procesal Penal. El título III del citado código, sobre búsqueda de pruebas y restricción de derechos, permite a la investigación fiscal:

- Ejecutar videovigilancias, ejecutar pesquisas, retener y registrar personas, realizar exámenes corporales, allanamiento de inmuebles, exhibir e incautar bienes, incluso

conservarlos o secuestrarlos previamente a su incautación, obtener copias, interceptar comunicaciones, obtener el levantamiento del secreto bancario y tributario, vigilar y clausurar locales, embargos, ordenes de inhibición, secuestros, medidas preventivas contra personas jurídicas.

- La admisibilidad en los procesos judiciales es posible en la medida que la evidencia digital se haya obtenido respetando los derechos fundamentales de las personas o con el correspondiente mandato judicial según el caso

En el caso de **República Dominicana**, que también cuenta con esas medidas señala que la ley 53-07 en su Sección II, Capítulo II contempla las medidas cautelares y procesales, donde se determina el alcance de la aplicación del código procesal penal en cuanto a las reglas de comprobación inmediata y medios auxiliares, la conservación de los datos, las facultades del Ministerio Público, así como las mejores prácticas de recopilación de evidencia, identificación de los proveedores de servicios, responsabilidad del custodio, entre otros.

Al igual que con que con la investigación, en **Uruguay** las medidas se están trabajando actualmente dado que por Ley N° 20.004 del 25 de noviembre de 2021 fue aprobado por Uruguay el Convenio Iberoamericano de Cooperación sobre Investigación Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia.

❖ Existen en su país estrategias nacionales que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos

En su respuesta afirmativa, **Argentina** destaca las siguientes estrategias, programas y/o planes nacionales:

- Comité de Ciberseguridad creado mediante el Decreto PEN N° 577/17;
- Programa Nacional de Protección de Infraestructuras Críticas de Información y Seguridad, creado mediante la Resolución de la Jefatura de Gabinete de Ministros N° 580/11;

- Estrategia Nacional de Ciberseguridad aprobada mediante la Resolución N° 829/19 de la Ex Secretaría de Gobierno de Modernización;
- Plan Federal de Prevención de Delitos Tecnológicos (2019 - 2023) que fuera aprobado por Resolución del Ministerio de Seguridad de la Nación N° 977/2019;
- Resolución del Ministerio de Seguridad de la Nación Nº 75/22 que aprobó el "Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2021 - 2024)";
- Resolución del Ministerio de Seguridad de la Nación Nº 86 de fecha 11/22 que crea el "Programa de Fortalecimiento en Ciberseguridad y en Investigación del Cibercrimen (ForCIC) y el Centro de Investigaciones del Ciberdelito de Alta Tecnología (CICAT);
- Resolución del Ministerio de Seguridad de la Nación N°167/2022 que crea el Centro de Operaciones y Entrenamiento del Equipo de Respuestas ante Incidentes de Seguridad Informática (COE);
- Resolución del Ministerio de Seguridad de la Nación N° 175/2022 que crea el "Comité de Gestión De Incidentes Prioritarios" (CGIP).

Bolivia responde afirmativa y amplía indicando que la labor de prevención de delitos cibernéticos la realiza la Policía boliviana nacional. Ese cuerpo policial implementó la división denominada "Ciber Crimen", desde donde combaten, desde el ámbito preventivo, los ciberdelitos vinculados a la pornografía infantil, trata y tráfico de personas, estafas, tráfico de armas, delitos sexuales, entre otros.

Por su parte, la labor de investigación la realiza el Ministerio Público como institución constitucional que defiende la legalidad y los intereses generales de la sociedad; labor que implica investigar todos los delitos de orden público contemplados en la Ley 1768 (Código Penal), norma donde se encuentra inserta los Delitos informáticos regulados en Bolivia.

En el ámbito procesal, son las autoridades del Órgano Judicial quienes ejercen labor de control de la investigación, procesamiento y sustanciación de aquellos delitos de índole privado y público; autoridades que ejercen jurisdicción y competencia para conocer y juzgar, si así corresponde, todas las conductas que se ajusten a los delitos de Manipulación informática (art. 363 Bis.) y Alteración, acceso y uso indebido de datos informáticos (art. 363 Ter.).

Por su parte, **Brasil** indica que sí y facilita el siguiente link https://www.cisoadvisor.com.br/governo-anuncia-plano-tatico-contra-cibercrimes/ De acuerdo con la información de esa publicación del 24 de marzo de 2022, el Ministerio de Justicia publicitó el Plan Táctico de Lucha contra los Delitos Cibernéticos. Uno de los pilares del Plan Táctico es el Acuerdo de Cooperación entre la Policía Federal y la Federación Brasileña de Bancos (Febraban). Este plan contiene ejes temáticos que destacan la prevención y mitigación de las ciber amenazas; gestión de los riesgos e incidentes derivados de los ciberdelitos; mejora en la infraestructura crítica para combatir el ciberdelito; apoyo legal y regulatorio; alianzas nacionales y cooperación internacional; estandarización e integración de la información; así como la investigación, el desarrollo, la innovación y la educación para hacer frente al ciberdelito. El documento sigue los lineamientos establecidos en el Decreto N° 10.222/2020 que aprobó la Estrategia Nacional de Seguridad Cibernética (E-Ciber) y forma parte de los vectores rectores derivados del Convenio de Budapest.

El Ministerio espera que esto facilite el intercambio de información, favoreciendo la adopción de medidas preventivas y educativas, “con el fin de hacer más seguro el ciberespacio, identificando y sancionando a las organizaciones criminales”, según señala el organismo en su comunicado sobre el tema compartido en el link.

Adicionalmente, se anunció que crearán un programa para prevenir el fraude bancario electrónico, las estafas digitales y un programa de formación de agentes de seguridad para que puedan hacer frente a los distintos tipos de delitos cibernéticos

Chile nuevamente responde afirmativamente. Manifiesta que el país trabajó arduamente para actualizar su legislación en materia de cibercrimen, dado que forma parte del Convenio de Budapest. Asimismo, ha participados en diversos foros internacionales en la materia.

Adicionalmente cuenta con un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), el cual depende del Ministerio del Interior y Seguridad Pública, cuya estrategia nacional consiste en apoyar y fortalecer la acción tecnológica gubernamental, ampliando el uso de tecnologías de información y comunicación en la gestión pública, a través de la mantención y control de la Red de Conectividad del Estado.

Costa Rica no cuenta con estrategias específicas, aún y cuando durante y luego de la pandemia de COVID 19 este tipo de delitos aumentó significativamente en el país.

Ecuador indica que también cuentan con estrategias nacionales. Hace de conocimiento que dentro de la "Estrategia Nacional de Ciberseguridad del Ecuador" aprobada el 03 de agosto de 2022 se incluyeron las siguientes:

- Adoptar un marco para el gobierno de la ciberseguridad basado en la gestión del riesgo.
- Establecer a novel nacional el informe sobre el Panorama de Amenazas y riesgo y Monitoreo continuo, consolidando diversas fuentes de información nacionales e internacionales, incluyendo tipos comunes de ciberataques dirigidos a las ICD nacionales e institucionales gubernamentales.
- Identificar los operadores de servicios de telecomunicaciones para la respuesta y comunicación de emergencia.
- Crear un programa de coordinación designado para la adopción de normas de ciberseguridad y mejores prácticas tanto para los organismos gubernamentales de manera obligatoria, como para las contrapartes pertinentes del sector privado de manera voluntaria.
- Promover la creación de normas y la adaptación o adopción de mejores prácticas que hagan factible la cooperación entre las partes interesadas responsables de la ciberseguridad.
- Identificar escenarios de riesgo de ciberseguridad para los cuáles se deben desarrollar planes nacionales de contingencia.
- Organizar ejercicios nacionales de ciberseguridad para aprobar las capacidades del personal involucrado en la ciberseguridad de las organizaciones.
- Realizar pruebas de involucren los escenarios de contingencia establecidos por las organizaciones.

Por su parte **Guatemala**, señala dentro de sus estrategias:

- Fortalecer las Capacidades de la Nación, creando el ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y ejercicio de los derechos de las personas en el ciberespacio. (Ministerio de Gobernación, 2018).

- Protección de la infraestructura crítica, contenida en el Plan Estratégico de Seguridad de la Nación 2020 – 2024 (Secretaría Técnica del Consejo Nacional de Seguridad, 2020).
- Estrategia Nacional de Seguridad Cibernética. (Comité Nacional de Seguridad Cibernética de la Secretaría Técnica del Consejo Nacional de Seguridad, 2021).
- Política Pública Contra la Trata de Personas y Protección Integral a las Víctimas 2014 – 2024. (Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas).

Honduras desarrolla sus estrategias nacionales a través del Decreto N°139-2016 "Acuerdo de Cooperación entre el Gobierno de Honduras e Israel".

México por su parte, también cuenta con estrategias. Están contenidas en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, a cargo de la Presidencia de la República y de la Secretaría de Seguridad y Protección Ciudadana Guardia Nacional.

También **Panamá** cuenta con estrategias nacionales sobre el tema. A través de la Autoridad Nacional para la Innovación Gubernamental, creó el Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT). Ese equipo tiene entre sus objetivos la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre sistemas informáticos que conforman la infraestructura crítica del país, y el acceso a la información de parte de los ciudadanos del país. También informan que recientemente se ha conformado una Mesa Interinstitucional que agrupa a diversas entidades públicas, entre ellas, la Autoridad Nacional para la Innovación Gubernamental (AIG) y el CSIRT, para coordinar y establecer un "Protocolo de Actuación Interinstitucional", ante un eventual ataque cibernético.

En **Paraguay** las estrategias están contenidas en Ley 4439/11 y el Convenio de Budapest.

Perú no cuenta con estas estrategias.

Por su parte **República Dominicana**, que también cuenta con estrategias informa que el decreto núm. 313-22, de fecha 14 de junio de 2022, establece y regula la Estrategia Nacional de Ciberseguridad 2021-2030 para su país. Además, el decreto núm. 230-18, de

fecha 15 de junio de 2018, establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021.

En el caso de **Uruguay** la estrategia al respecto está dirigida a la aprobación de las normas antes indicadas en el cuestionario, con el objetivo de que la misma abarque no solo la tipificación penal sino también el aspecto procesal y evidentemente la cooperación internacional dado el carácter de delitos transnacionales de que se tratan y sus características especiales. Al margen de lo anterior, a nivel ejecutivo y de investigación el Ministerio del Interior (Policía Nacional) trabaja diariamente con este tipo de situaciones y sus circunstancias a través de su sección de Delitos Complejos.

❖ Su país se dio su adhesión o ratificó el Convenio de Budapest de 2001

Mediante la Ley 24.711, el día 15 de diciembre del año 2017, se aprobó la adhesión al Convenio de Budapest por parte de la **República Argentina**. El día 5 de junio del 2018 se adhirió al mencionado Convenio y entró en vigor el 1 de noviembre del 2018. Los delitos informáticos se encuentran receptados en el Código Penal de la Nación.

Bolivia no ha ratificado el Convenio de Budapest, tampoco **Honduras**. **Guatemala** fue invitado a adherirse, pero aún no lo ha hecho.

Brasil informó que ha ratificado el Convenio de Budapest, que fue aprobado en el Congreso Nacional a través del Decreto Legislativo No. 37 de 16 de diciembre de 2021, ya en vigor. Sin embargo, está pendiente el depósito del instrumento a nivel internacional. Todavía no hay cambios legislativos realizados en Brasil basados en la Convención de Budapest, aunque ya cuentan con disposiciones que pueden considerarse armónicas frente a este convenio internacional.

Chile si ratificó el Convenio de Budapest, que fue promulgado el día 28 de abril de 2017, el cual fue publicado en el Diario Oficial el día 28 de agosto de 2017.

Costa Rica también ratificó el Convenio de Budapest mediate Ley No. 9452, publicada el 3 de julio de 2017.

Ecuador no ha ratificado el Convenio de Budapest. Pero informa que el 01 de abril de 2022 la División de Derecho Internacional Púbico y Oficina del Tratado informó al Ecuador que el Comité de Ministros del Consejo de Europa, durante la sesión número 130 de marzo 30 de 2022, decidió extender una invitación a Ecuador para que acceda a la Convención. Significa lo anterior que Ecuador tendrá la calidad de observador en el Comité del Convenio y dispondrá de 5 años para finalizar el proceso de ratificación del instrumento, tiempo en el cual el país deberá adoptar las medidas necesarias para que su legislación interna esté en concordancia con el Convenio de Budapest.

México no ratificó el convenio, pero se encuentra como observador.

Panamá también lo ratificó, mediante la Ley 79 de 22 de octubre de 2013.

En el caso de **República Dominicana**, fue ratificado el 11 de junio de 2012, mediante la Resolución Núm. 158-12 del Congreso Nacional y el instrumento legal que tipifica los delitos que en él se definen es la ley núm. 53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología, que incluye, entre otros: (i) interferencia de sistemas; (ii) abuso de dispositivos; (iii) pornografía infantil; (iv) conservación rápida.

Paraguay informa que el convenio fue ratificado y adherido por Ley N° 5994 del 15 de diciembre del 2017.

El Convenio sobre Ciberdelincuencia de Budapest, fue ratificado por el **Perú** mediante Decreto Supremo N.° 010-2019-RE de fecha 10 de marzo del 2019. Entró en vigor el 01 de diciembre del 2019.

Pese a que el convenio fue suscrito por el Perú con posterioridad a la entrada en vigor de la Ley N° 30096, ley especializada en delitos informáticos, y su modificatoria a través de la Ley 30171; la ley especializada ya recogía una parte de los delitos contenidos en el Convenio, siendo estos: acceso ilícito, atentado a la integridad del dato, atentado a la integridad de sistemas, interceptación de datos informáticos, fraude informático, abuso de mecanismos y dispositivos informáticos.

Uruguay informa próximamente ratificará el Convenio sobre Ciberdelincuencia de Budapest.

- Existe en su país una fiscalía y un ente policial judicial investigador especializado en ciberdelitos

Argentina cuenta con fiscalía y ente policial judicial investigador especializado en ciberdelitos. De igual manera **Bolivia**, **Brasil**, **Chile**, **Costa Rica**, **Ecuador**, **Guatemala**, **Honduras**, **Panamá**, **Paraguay**, **Perú**, **República Dominicana**.

En el caso de **México**, la Fiscalía General de la República no cuenta con una Fiscalía Especializada en la investigación de delitos cibernéticos. Sin embargo, sí cuenta con una Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT) que coadyuva con los Ministerios Públicos o Fiscales en la investigación de los delitos cibernéticos o de aquellas conductas y situaciones de riesgo que se realizan a través de medios cibernéticos y del uso de las tecnologías.

Uruguay aún no cuenta con esos órganos especializados. Si cuentan con la Fiscalía de Delitos Económicos y Complejos que tramita los casos y pertenece a la Fiscalía General de la Nación.

- De ser si su respuesta, por favor indique si reciben capacitación y de parte de que instituciones, empresas u organismos internacionales. En caso de ser no su respuesta, por favor indique si existen proyecciones para su conformación.

En **Argentina** es el propio equipo de trabajo de la Unidad Fiscal el que brinda capacitaciones a los integrantes del Ministerio Público Fiscal. En el marco de la Procuración General de la Nación, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) fue creada en noviembre de 2015 con el objetivo de fortalecer la política criminal contra el cibercrimen, intensificar las tareas para su abordaje de modo articulado y atender a sus especificidades (resolución PGN N° 3743/2015).

En el caso de **Bolivia**, informan que el Ministerio Público cuenta con Fiscales de materia capacitados en el desarrollo de investigaciones por ciberdelitos; teniéndose investigadores especiales con preparación en ciberdelitos.

En **Brasil** la capacitación es impartida por la División de Represión a Delitos Cibernéticos de la Policía Federal brasileña. Ha recibido capacitación a través del proyecto GLACY, DOJ / USA, INTERPOL, OEA y grandes empresas como Microsoft, etc.

Chile señala que si reciben capacitaciones de parte de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (ULDDECO), que ofrece asesoría a los diversos fiscales especializados en materia de delitos informáticos, a lo largo de todo el territorio. Estas capacitaciones se han llevado a cabo por parte de los abogados asesores de esta Unidad Especializada, así como también destacados académicos especialistas en la materia.

Por la parte de la policía, se encuentra la Brigada Investigadora de Cibercrimen, la cual es la policía especializada en materia de delitos informáticos.

Costa Rica recibe muy poca capacitación al respecto, prácticamente solo la que proporcional los organismos internacionales.

Ecuador señala que también cuentan con capacitación. Informa que la Unidad de Ciberdelito de la Policía Nacional recibe capacitaciones por parte de instituciones públicas. Y que la Unidad Nacional Especializada en la investigación de Ciberdelitos de la Fiscalía General del Estado ha recibido capacitaciones por parte de la OEA-REMJA.

Sobre la capacitación, **Guatemala** señala que el Ministerio Público participó en el II Encuentro Regional de Coordinación Interinstitucional del 27 al 28 de agosto de 2019, el cual se desarrolló con el apoyo del Gobierno de Canadá y tuvo como objetivo el fortalecer e intercambiar las experiencias en la lucha contra el tráfico/trata de personas y el combate al Lavado de Dinero u Otros Activos y el Financiamiento del Terrorismo, para adquirir nuevas capacidades y destrezas por parte del personal de esta institución del personal de la Intendencia de Verificación Especial de la Superintendencia de Bancos.

El Ministerio de Gobernación tiene el Viceministerio de Tecnología y bajo inteligencia civil revisan aspectos de seguridad tecnológica y con la Unidad respectiva de la Policía Nacional Civil, para lo cual cuentan con una Guía para la Prevención de Delitos Informáticos, cuya Sección de Ciberdelitos, ahora es un Departamento de Investigación de Ciberdelitos e Información Forense que pertenece a la División Especializada en

Investigación Criminal, según la Orden general 08-2022 del Director General de la Policía Nacional Civil y han sido capacitados por el Departamento de Estado de los EEUU (enero-2021) para la Red 24/7 indicada; en conjunto también con el MP con la Red de Derivación.

En **Honduras** la capacitación se ha recibido de parte de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y de Agencia Española de Cooperación Internacional (AECI).

México brinda capacitación a esos órganos a través de la Coordinación de Estrategia Digital Nacional, de la Secretaría y Protección Ciudadana y de la Guardia Nacional. La Fiscalía General de la República cuenta con el Centro de Formación y Servicio Profesional de Carrera (CFSPC), a través del cual se imparten de manera permanente actividades formativas y de actualización sobre diversas materias relacionadas con la competencia de la Fiscalía a todo el personal que integra la institución, incluyendo el personal de la UICOT.

Adicionalmente, la Dirección General de Cooperación Internacional, en coordinación con el CFSPC, transmite a dicha Unidad de Investigaciones las convocatorias a capacitaciones realizadas por organismos internacionales y autoridades extranjeras, siempre que el contenido se vincule con sus atribuciones.

Por su parte, **Panamá** ha procurado la especialización de los fiscales en las distintas modalidades delictivas que integran las conductas punibles que involucren el uso de tecnología o informática. En ese sentido, informan que el Ministerio Público, cuenta con un modelo de gestión de Fiscalías Especializadas, según el tipo de delitos. Es decir que, las estafas cibernéticas, la falsificación de datos digitales, la explotación sexual a través de redes, los delitos Contra la Seguridad Informática son tipos penales diversos que son atendidos por equipos distintos, cada uno con las competencias y conocimientos para atender estas investigaciones.

En el caso particular de los delitos Contra la Seguridad Informática, que tiene que ver con los ingresos no autorizados a redes, bases de datos o sistemas informáticos, así como la denegación de servicios o secuestros virtuales de sitios de internet o datos tipificados en el Código Penal, estos son de competencia exclusiva de la Fiscalía Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática, creada mediante Resolución N° 19 de 10 de julio de 2008, con competencia a nivel nacional.

Adicionalmente resaltan que la Dirección de Investigación Judicial, como brazos auxiliares operativos del Ministerio Público, cuenta con la Sección de Delitos Cibernéticos, la cual se compone de policías especializados en esa materia, que coadyuvan en las investigaciones.

Informan que la capacitación es constante capacitación y por parte de diversos sectores, tanto público como privado. Entre ellas, capacitaciones, seminarios, talleres auspiciados tanto por la Embajada de los Estados Unidos, OEA, UNODC, Consejo de Europa.

Paraguay responde que se reciben constantes capacitaciones de Organismos Internacionales como el Consejo de Europa, OEA, Aeicid y de instituciones nacionales como el Ministerio Público, que siempre impulsa la capacitación de sus funcionarios.

Perú responde que el grueso de la formación es interna, donde son los propios investigadores experimentados quienes forman al resto. En función de las necesidades, estos formadores especializados se capacitan mediante cursos *adhoc*, diseñados en función de las necesidades, pudiendo ser con empresas del sector privado, otras agencias policiales (P.e. EUROPOL), CEPOL, sector académico español y el Instituto Nacional de Ciberseguridad (INCIBE)

En el caso de **República Dominicana**, existe una Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología (PEDATEC), un Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología (DICAT) que forma parte de la Policía Nacional y la División de investigación de Delitos Cibernéticos (DIDI) en el Departamento Nacional de Investigaciones (DNI). Reciben capacitaciones de organismos internacionales como la OEA a través de las Reuniones de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas (REMJA), que es su principal foro político y técnico en materia de justicia y cooperación jurídica internacional con sus Estados miembros.

También se da esa participación en el caso de **Uruguay**

- Participa la unidad de inteligencia financiera de su país en la investigación de lavado producto de ciberdelitos

Argentina, Bolivia, Brasil, Chile, Ecuador, Guatemala, Honduras, México, Panamá, Paraguay, Perú, República Dominicana, Uruguay informan que las unidades de inteligencia financiera de sus países si participan.

En el caso de **Costa Rica**, podría darse esa participación siendo un delito cibernético el delito precedente en casos de legitimación de capitales. Pero es una situación que no es muy común.

- Existen controles en su país con relación a la prevención de lavado de activos producto de ciberdelitos

Argentina si cuenta con controles. Los ejerce a través de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias. Esta un órgano colegiado presidido por el Secretario de Estado de Economía.

En el caso de **Bolivia**, la Fuerza Especial de Lucha Contra el Crimen, de la Policía boliviana, registra la División de Cibercrimen, que se encarga de realizar controles con relación a la prevención de delitos relacionados con el cibercrimen.

Brasil también aplica controles. De acuerdo con lo que indican, las mismas reglas y estrategias para combatir el lavado de dinero en el país se aplican a los delitos cibernéticos. Hacen saber que es necesario adquirir tecnología de punta (herramienta de seguimiento cripto activo) para su uso en investigaciones criminales, incluidas las relacionadas con el lavado de dinero.

Chile informa que sí y que es la Unidad de Análisis Financiero quien puede recibir reportes de operaciones sospechosas por lavado de activo cuyo delito base sea alguno de los ocho delitos informáticos incorporados en su ordenamiento mediante la Ley N° 21.459. https://bcn.cl/34svf.

Costa Rica tiene controles incipientes, que no son suficientes en la actualidad.

Ecuador responde afirmativamente. Informa que los controles están a cargo de la Unidad Nacional de Delitos contra el Sistema Financiero y Económico que está a cargo de la Policía Nacional del Ecuador.

En **Guatemala** también se aplican controles. La Unidad de Métodos especiales del Ministerio Público de la República de Guatemala tiene como funciones, la Intercepción de comunicaciones para la persecución de los delitos atribuidos a los integrantes o participantes de las organizaciones criminales, de acuerdo con lo establecido en la Ley Contra la Delincuencia Organizada.

Asimismo, el Ministerio Público cuenta con una Fiscalía de Delitos Transnacionales, la cual ejerce una persecución penal estratégica contra el crimen organizado y la Fiscalía Contra la Trata de Personas, la cual promueve la investigación y persecución penal del delito de trata de personas en sus distintas modalidades, incluyendo los delitos contra la indemnidad sexual de las personas, incluyendo como tipo penal, la seducción de niños, niñas o adolescentes por el uso de las tecnologías de información, la solicitud o recepción de material con contenido sexual o pornográfico, propio o de terceras personas, ya sea que incluya o no medios audiovisuales.

De conformidad con el artículo 9 del Acuerdo Gubernativo Número 635-2007 del Presidente de la República, el 4º Viceministerio del Ministerio de Gobernación, tiene como funciones, entre otras, diseñar y supervisar el funcionamiento del eje de tecnologías de la información y la comunicación para el Ministerio de Gobernación, así como su interrelación con las dependencias que lo conforman y otras instituciones del sector público con que se relacione.

Asimismo, tiene como función la de proponer estrategias, políticas, planes, programas y proyectos orientados a la integración de los sistemas y productos de las diferentes áreas de tecnologías de la información y la comunicación del Ministerio de Gobernación y sus Dependencias y establecer los procesos de integración tecnológica con otras entidades públicas que apoyen el tema de seguridad pública ciudadana y comunitaria.

En cuanto a la Policía Nacional Civil de la República de Guatemala, como institución encargada de la seguridad pública en todo el territorio del Estado, cuenta con una Unidad de Cibercrimen, la cual cuenta con personal especializado, la cual tiene como objetivo el

combate y erradicación de la producción, tenencia, distribución y reproducción de pornografía infantil.

Para la ejecución de esta operación realiza allanamientos, registros, secuestro de dispositivos u objetos ilícitos y aprehensión de personas involucradas y responsables de consumo, almacenamiento, producción o reproducción de pornografía infantil.

En el caso de **Honduras**, los controles se ejecutan a través de Instituciones Financieras para prevenir ser víctimas del Ciberdelito, tanto los sistemas informáticos de la institución como sus clientes y usuarios. También a través de la Dirección Nacional de Investigación e Inteligencia (DNII) y de la Unidad de Inteligencia Financiera (UIF), mediante la publicación de Estudios y Tipologías en su página oficial.

En **México**, conforme a lo dispuesto en el artículo 15, fracción I, inciso a), compete a la Unidad de Inteligencia Financiera (UIF) de la Secretaría de Hacienda y Crédito Público el establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión del delito de operaciones con recursos de procedencia ilícita, mejor conocido como “lavado de dinero”.

En ese sentido, a través de sus diversas herramientas tecnológicas y sus capacidades técnicas-operativas, compete a la UIF la prevención y detección de dicho ilícito, cualquiera que sea su delito predicado, incluyendo los “ciberdelitos”.

En **Panamá** también existen controles. Informa que publicaron la Ley No.23 de 27 de abril de 2015, “Que adopta medidas para prevenir el blanqueo de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, y dicta otras disposiciones”. Esa ley tiene como objetivo ser el marco regulatorio para que los diferentes organismos de supervisión, así como las entidades, personas naturales y jurídicas sujetas a esta supervisión, establezcan las medidas para identificar, evaluar y entender los riesgos y consecuencias de estos flagelos delictivos. Asimismo, insta a las entidades correspondientes, a establecer los controles apropiados para la mitigación de estos riesgos identificados, con el objeto de proteger la integridad del sistema financiero y de otros sectores de la economía panameña. Con esta normativa, se facilita la cooperación internacional.

Esa misma ley establece la Comisión Nacional Contra el Blanqueo de Capitales, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva, adscrita al Ministerio de Economía y Finanzas, conformada por entidades tales como: Ministerio de Relaciones Exteriores, Ministerio de la Presidencia, Ministerio de Comercio e Industria, Ministerio de Economía y Finanzas, Superintendencia de Bancos de Panamá, Superintendencia de Sujetos no Financieros, Procuraduría General de la Nación, Unidad de Análisis Financiero y la Comisión de Economía y Finanzas de la Asamblea Nacional.

De acuerdo con los artículos 9 y 11 de esa ley, la Unidad de Análisis Financiero (UAF), es el centro nacional para la recopilación y análisis de información financiera relacionada con los delitos de blanqueo de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, así como para la comunicación de los resultados de ese análisis a las autoridades de investigación y represión del país. Entre sus facultades está la de centralizar los reportes de operaciones sospechosas (ROS), efectivo y cuasi efectivo que generen o emitan los sujetos obligados financieros, no financieros y actividades realizadas por profesionales sujetos a supervisión.

De conformidad con el artículo 54 de esta normativa, también se establece la obligatoriedad de reportar una operación sospechosa por parte de los sujetos obligados financieros, no financieros y actividades realizadas por profesionales sujetos a supervisión, ante la Unidad de Análisis Financiero (UAF), entidad que, posteriormente, analizará la información para comunicar sus resultados a las autoridades competentes descritas en la ley.

Paraguay responde que no cuenta con estos controles.

Perú tampoco cuenta con estos controles. Responden que lo que refiere al Sistema de Prevención de LA/FT, su país aún no ha considerado a los proveedores de activos virtuales (PSAV) como sujetos obligados (SO). Desde finales de 2021 la SBS, a través de la UIF, presentó ante el Ministerio de Justicia y Derechos Humanos (MINJUS) una propuesta de Decreto Supremo para PSAV como SO; sin embargo, aún se está a la espera de la emisión de la norma.

No obstante, se debe precisar que, al estar los delitos de ciberdelincuencia tipificados penalmente y generar ganancias ilícitas, son considerados delitos precedentes de lavado de activos y, por tanto, es posible que la UIF pueda recibir información a través de los Reportes de Operaciones Sospechosas (ROS) sobre el particular.

Asimismo, bajo el concepto de bienes regulado en la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes, pueden investigar actos de conversión, transferencia y ocultamiento, relacionados a monedas virtuales en el marco del Decreto Legislativo N° 1106.

República Dominicana también cuenta con controles. Se tratan de la Ley núm. 155-17 Contra el Lavado de Activos y Financiamiento del Terrorismo, de fecha 1° de junio de 2017, que en su artículo 2, inciso 11, contempla los delitos de alta tecnología como infracción precedente o determinante que genera bienes o activos susceptibles de lavado de activos. Asimismo, en el artículo 91 se establece que la Unidad de Análisis Financiero (UAF) como ente técnico tiene la responsabilidad de realizar el análisis para identificar y elevar al Ministerio Público informes de análisis financieros relativos a posibles infracciones al lavado de activos, infracciones precedentes y la financiación del terrorismo

En el caso de **Uruguay**, los controles están a cargo de Secretaría Nacional para la Lucha contra el Lavado de Activos y Financiamiento del Terrorismo (SENACLAFT) de Presidencia de la República y la Unidad de Inteligencia y Análisis Financiero (UIAF) del Banco Central del Uruguay. Estas instituciones participan en las investigaciones de lavado de activos producto de ciberdelitos o delitos informáticos en la medida que corresponda, asistiendo a Fiscalía General de la Nación.

Amplía Uruguay indicando que los controles existen dado que la Ley N°19.574 de 20 de diciembre de 2017, Ley Integral sobre Lavado de Activos, prevé que en la aplicación de un enfoque de riesgos, los sujetos obligados deberán intensificar el procedimiento de debida diligencia para las categorías de clientes, relaciones comerciales u operaciones de mayor riesgo, tales como los clientes no residentes -especialmente los que provengan de países que no cumplen con los estándares internacionales en materia de lavado de activos y financiamiento del terrorismo- operaciones que no impliquen la presencia física de las partes, prestando atención a las amenazas que puedan surgir de la utilización de tecnologías nuevas o en desarrollo que favorezcan el anonimato en las transacciones y en general todas

aquellas operaciones que presenten características de riesgo o señales de alerta, según lo que determine la reglamentación.

- Su país está vinculado a la Red de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días (Red G8 24/7)

Argentina está vinculada e indica que es efectiva, especialmente, con aquellos proveedores de servicios localizados en Estados donde no se admiten pedidos de preservación directa emitidos por parte de autoridades judiciales extranjeras. También la consideran efectiva toda vez que les agiliza la tramitación de pedidos de emergencia.

Bolivia no está vinculada a la red, tampoco **Guatemala** ni **Honduras**.

En **Brasil** la Policía Federal actúa como punto 24x7 del G7. Para ello, utilizan la dirección de correo electrónico cybercrime_brazil_24x7@pf.gov.br, divulgado a las redes, donde reciben las solicitudes de debida diligencia de varios países (fuerzas policiales, fiscales), así como de agencias brasileñas (policía civil, MPF, unidades de PF).

Chile si está vinculado. Ha utilizado la Red de Contactos sobre Delitos de Alta Tecnología (Red G8 24/7) para solicitar la preservación de datos o información sobre proveedores de servicio que se encuentren bajo la jurisdicción de los Estados miembros de la red. Advierten que solo utilizan esos contactos si el Estado no es parte de la Convención de Budapest, de lo contario, recurren al punto de contacto de la Red 24/7 de la Convención.

Costa Rica está vinculada en virtud de la ratificación del Convenio de Budapest. Ha tenido una única experiencia con la red, la cual resultó efectiva. Sin embargo, se pretende dar un impulso al uso de la red, para realmente aprovecharla. En el mes de noviembre Costa Rica es la sede escogida para realizar un foro de ciberdelincuencia, designación realizada por el Consejo Europeo.

La han utilizado en tres ocasiones en estos últimos cinco años (México, Colombia y Malasia), en ninguno de esos casos obtuvieron respuesta, ni siquiera un acuse de recibo.

Ecuador no está vinculado y no existen planes o proyectos para la inclusión en esa red.

México si está vinculado a la red.

Panamá está vinculado a la red. Sin embargo, trabaja vía INTERPOL a través de un punto de contacto designado por esa entidad. Informan que, en cuanto a la efectividad, se han tenido resultados positivos. Aclaran que por su modelo de justicia y las leyes que lo rigen, los miembros del orden público no cuentan con iniciativa investigativa, por lo que deben acudir a un miembro del Ministerio Público, para que conozca de la solicitud, para que ellos a su vez sean quienes giren las comisiones respectivas y se dispongan los actos investigativos necesarios.

Paraguay está vinculado y considera la red muy efectiva, eficaz y oportuna.

Perú también está vinculado. Responden que las comunicaciones se efectúan a través de la Unidad de Cooperación Judicial Internacional y Extradiciones del Ministerio Público, como autoridad central. La efectividad en su utilización ha sido positiva, por cuanto a la fecha se ha usado para establecer comunicación con funcionarios de Brasil, Hong Kong y Singapur- los cuales no son Estados Parte del Convenio de Budapest- y solicitar apoyo para la remisión de información relativa a IP, así como para requerir apoyo para la conservación de datos informáticos.

República Dominicana está vinculada y señala que es sumamente efectiva debido a que permite a su país tener una red de información donde se toman medidas de carácter urgente transnacional, ya que al tener acceso a contactos en otros países es posible solicitar preservación o resguardo de información hasta tanto se puedan remitir las órdenes judiciales correspondientes a través de un MLAT (tratado de asistencia legal multilateral). Señala que se han llevado a cabo investigaciones conjuntas con autoridades de los gobiernos de España y Colombia, y trabajado activamente en varias operaciones multilaterales exitosas. Como miembro del Convenio de Budapest y de varias de las redes 24-7 del G8, Interpol y Europol, el país cuenta con mecanismos de cooperación efectiva con autoridades de otros países. De hecho, el acceso del país al Convenio de Budapest y la importante ayuda obtenida para el desarrollo de las capacidades por parte de socios internacionales han fortalecido considerablemente la postura del país en términos de combate al cibercrimen.

Uruguay aún no está vinculado, pero dado el nivel de discusión y análisis del tema, en Uruguay existe proyección de vincularse a la Red 24/7 de conformidad con lo previsto por el artículo 35 del Convenio de Budapest.

- El sector privado, la sociedad civil y la academia aportan, cooperan activamente o forman parte de alguna estrategia, política, protocolo o instrumento nacional para la prevención o represión de la ciberdelincuencia

En **Argentina** si hay participación de esos sectores. El Anexo único (IF-2022-05822603-APN-UGA#MSG) del "Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2021-2024)", establecido por la Resolución N° 75/22 del Ministerio de Seguridad de la Nación, se fija como uno de sus objetivos principales "(...) Incrementar la colaboración con la Sociedad Civil y las instituciones educativas". A su vez, hace saber que uno de los principios rectores del mentado Plan es la conducción y articulación con las universidades, la sociedad civil y el sector privado de las acciones de fortalecimiento de capacidades para la prevención e investigación de ilícitos en el ciberespacio. Misma suerte corre el Anexo (IF-2019-94761790-APN-DIC#MSG) del Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2019 - 2023).

En **Bolivia** no si da esa participación e indican que se da en la forma de prevenir este tipo de delitos.

En **Brasil** hay muchas iniciativas relevantes en el sentido anterior, y se pueden mencionar:

- la asociación del NCMEC (ONG/EE.UU.) con la Policía Federal para el tratamiento más eficaz posible de las denuncias del NCMEC de interés para Brasil, relacionadas con el abuso sexual infantil;
- Proyecto TENTÁCULOS de la Policía Federal, en materia de fraude bancario electrónico estructurado, generalmente cometido por asociaciones u organizaciones criminales. Absolutamente consolidado a lo largo de los años, el Proyecto Tentáculos consiste en la recopilación de información sobre fraude bancario electrónico en una sola base de datos (National Electronic Banking Fraud Base -BNFBE), administrada e impulsada por PF, de modo que, con el uso de

software de análisis específico, es posible verificar convergencias entre varios delitos ejecutados contra cuentas bancarias de diferentes Unidades de la Federación, permitiendo la concentración de los esfuerzos de investigación en el estado en el que se encuentran los delincuentes. Por lo tanto, evita el establecimiento de procedimientos de investigación sin eficacia práctica en la localidad de las cuentas de las víctimas y el establecimiento de investigaciones se realiza en el lugar donde se encuentra el individuo o los grupos delictivos. Se aclara que la Base Nacional de Fraude Bancario Electrónico (BNFBE) es el resultado de dos importantes Convenios de Cooperación Técnica (TCA) entre la Policía Federal y CAIXA, y entre Policía Federal y FEBRABAN. La Policía Federal proporciona la recepción, tratamiento y gestión de datos de estas instituciones, así como capacita a oficiales de la policía federal de todo el país para operar, desde ella, de manera efectiva.

- La Policía Federal ha firmado con FEBRABAN otro ACT para hacer frente a los delitos de alta tecnología. Hay varias medidas en curso para permitir una mejora significativa en la lucha contra esos delitos.
- La Policía Federal ha participado o apoyado varias investigaciones académicas y científicas sobre el tema del delito cibernético.

Chile informa que no. Comentan que conforme con la Ley N°20.393, sobre responsabilidad penal de las personas jurídicas, los delitos informáticos tipificados en la Ley N°21.459 pueden ser delito base para generar este tipo de responsabilidad. Por tanto, el sector privado tiene el deber de adoptar medidas que permitan gestionar sus riesgos relacionados a esta clase de ilícitos. No obstante, no existe protocolo o instrumento nacional en esta materia en ese país.

En **Costa Rica** aún no participan tampoco en este tipo de estrategias. Así como no hay controles necesarios, falta la invitación y el involucramiento de la sociedad civil en esta materia.

Ecuador responde afirmativamente sobre esta participación. En el sector público, se da a través del Ministerio de Telecomunicaciones y Sociedad de la Información, juntamente con varias instituciones públicas y privadas que realizaron la “Estrategia Nacional de Ciberseguridad del Ecuador”, la cual fortalece lazos entre instituciones para combatir y erradicar los ciberdelitos en el país.

Adicionalmente, conforme el artículo 4 y 5 de la "Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos" con relación a Reportes de Operaciones Sospechosas – ROS, se señala que los Sujetos Obligados a informar tienen la obligación de reportar, bajo responsabilidad personal e institucional, a la Unidad de Análisis Financiero y Económico (UAFE) las operaciones o transacciones económicas inusuales e injustificadas, dentro del término de cuatro días, contados a partir de la fecha en que el comité de cumplimiento de la institución correspondiente tenga conocimiento de tales operaciones o transacciones. El artículo 7 de la misma ley señala que además de los deberes de los sujetos obligados de informar de acuerdo con las disposiciones del dicho capítulo, todo ciudadano que conociere de actividades que pudieran constituir operaciones inusuales, injustificadas o sospechosas deberá informar a la Unidad de Análisis Financiero y Económico (UAFE) o a la autoridad correspondiente según el caso.

En este contexto, la UAFE recaba la información remitida por denuncias de la ciudadanía o reportes de los Sujetos Obligados que tienen relación a delitos cibernéticos para procesarlos y de ser el caso remitir a la FGE para que ésta dentro del ámbito de sus competencias inicie las etapas judiciales correspondientes.

En el mes de abril del 2022 se publicó en Ecuador el informe de Evaluación Sectorial de Riesgo de Lavado de Activos en el sector Microfinanzas. En ese informe se determinó como una amenaza a los ciberdelitos; por lo tanto, se iniciaron reuniones interinstitucionales para establecer un marco de acción para mitigar los riesgos identificados.

En **Guatemala** actualmente no se cuenta con trabajo articulado entre el sector privado, la sociedad civil respecto a políticas y protocolos para la prevención o represión de la ciberdelincuencia.

En **Honduras** existen instituciones privadas que de forma aislada cooperan en la prevención del Ciberdelito.

En **México** también se da esa participación. Se logra a través de la Comisión de Ciencia, Tecnología e Innovación de la Cámara de Diputados, se cuenta con una Mesa

Permanente para Analizar el Marco Jurídico y Propuestas Legislativas en Materia de Ciberseguridad, en donde participa el sector público y privado.

También **Panamá** cuenta con esa participación. Esas acciones se han desarrollado a través de mesas de trabajo con varias organizaciones oficiales, entre ellas, la Superintendencia de Bancos, Superintendencia de Seguros y Reaseguros, Superintendencia del Mercado de Valores, Policía Nacional, Dirección de Investigación Judicial, Ministerio de Seguridad Publicas, entre otras entidades, a fin de hacer efectiva la propuesta del proyecto de ley sobre ciberdelitos.

Realizan campañas de sensibilización a la ciudadanía como medidas de prevención frente a este nuevo fenómeno. Colaboran con el Ministerio Público con el otorgamiento de información para sus investigaciones. No obstante, informan que es su interés mejorar los tiempos de respuesta y asegurar investigaciones asertivas, se trabaja en un plan de sensibilización y coordinación con las prestatarias y empresas de servicios públicos y de telecomunicación.

Paraguay responde que todas las iniciativas y estrategias de políticas para el combate o la lucha contra la ciberdelincuencia se abordan de manera integral y con todos los sectores de la sociedad. Señalan la importancia de contar siempre con el apoyo del sector privado (ISP, telefónicas), así como de la sociedad civil, a través de las cuales se mide el impacto de los fenómenos. La academia, siempre aporta con la investigación científica y se difunden los buenos fenómenos que impactan a la sociedad, de esta forma se pueden trabajar en políticas públicas que mitiguen los impactos negativos que pueda tener el uso y avance de la tecnología en todas sus formas.

En **Perú** aún no se da esta participación, pese a que el sector privado posee importante información relacionada a casos que se investigan como delitos informáticos, aún no se conforma estrategias junto con el Estado sobre temas preventivos relacionados a ciberdelincuencia.

El Ministerio Público viene procurando establecer convenios con algunos actores; como, por ejemplo, en el rubro de las comunicaciones, a fin de que los requerimientos de información bajo mandato judicial se atiendan en el menor plazo posible.

La participación en **República Dominicana** se da a través de la Estrategia Nacional de Ciberseguridad, donde se suman todos los sectores, tanto privados como públicos, siendo de carácter integral. El país ha establecido mecanismos judiciales para solicitar de manera oficial información por parte de entidades en el país. También se han mejorado los métodos para compartir información mediante el desarrollo de sociedades colaborativas entre el Gobierno y el sector privado, producto de los importantes esfuerzos previos realizados para generar conciencia y llegar a posibles socios del sector privado.

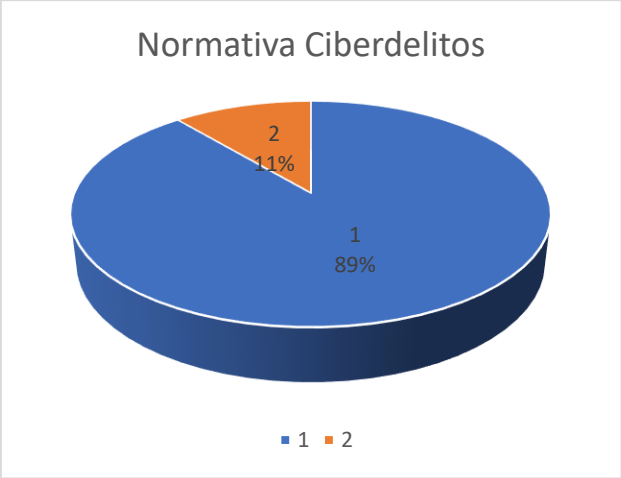
En **Uruguay**, debido a que en Uruguay existe un proyecto de ley sobre tipificación de ciberdelito a cargo de la Comisión Especial de Innovación Ciencia y Tecnología del Parlamento Nacional, bajo ningún motivo se encuentra ajeno a la discusión e implementación necesaria de las medidas y procesos que acompañen el combate de este fenómeno de características tan particulares que excede las fronteras de los estados.

En su caso, el sector privado, la sociedad civil y la academia, ciertamente cooperan activamente desde sus diferentes ámbitos, teniendo conocimiento que a nivel gubernamental se están tratando estos temas de fundamental importancia, lo que requiere un necesario *"aggiornamiento"* del país en la materia. Aun así, existen campañas de divulgación que buscan concientizar a la población sobre el tema, enseñando pautas a los efectos de que eviten caer o exponerse en estas situaciones que son tan perjudiciales. Dichas campañas tienen fines educativos que se verán reforzadas con la aprobación de la nueva legislación.

RESULTADOS GENERALES DEL DIAGNÓSTICO

Revisadas las respuestas de los 18 países de la región que facilitaron información, se obtuvieron los siguientes resultados:

- Países de la región con legislación sobre ciberdelitos:



Solamente dos países en la región y que respondieron, no cuenta con legislación en la materia. Los otros 16 que atendieron el cuestionario si poseen normativa.

- Países con medidas para la investigación y cooperación en ciberdelitos:

En cuanto a legislación para investigación y procesamiento de esto delitos, la cifra varía. Hay 14 países con normas adecuadas y 4 que no cuenta con normas adecuadas o que las que rigen son las mismas que para otros delitos.

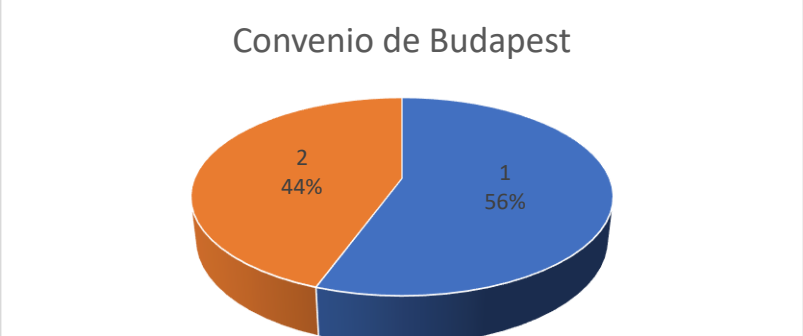
- Países con medidas para la incautación y custodia de evidencias electrónicas:

En cuanto ha medidas de aseguramiento y de custodia, 15 países cuentan con legislación adecuada y 3 no cuenta con ellas o utilizan normas generales.

- Países con estrategias para la prevención, investigación y procesamiento de ciberdelitos:

Existe también una mayoría de países que respondieron que si cuentan con estrategias, 16 en total y solamente 2 aún no cuentan con ellas.

- Países que dieron adhesión o ratificaron el convenio de Budapest



En el caso del Convenio, las cifras se acercan ya que 10 si lo han ratificado y 8 aún no, algunos están en proceso, alguno invitado y en otros no hay ni siquiera proyectos de ley para su adhesión o ratificación.

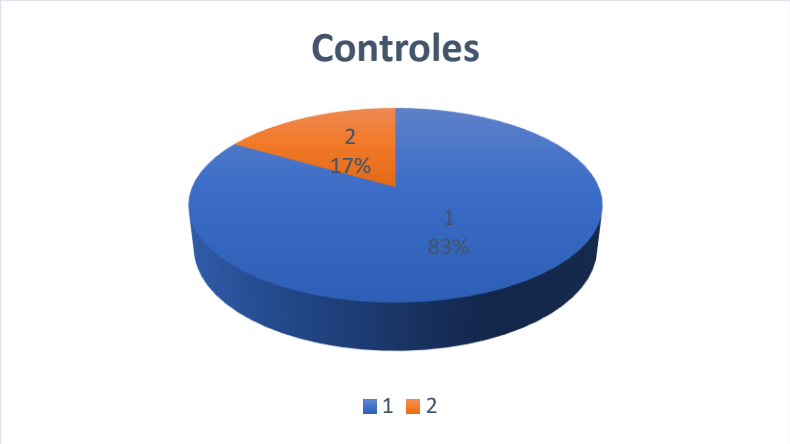
- Países con Fiscalía y Policía Investigativa especializada en ciberdelitos:

Casi concordante con la existencia o falta de legislación sobre el tema, 15 de los países que respondieron si cuentan con fiscalía y policía investigativa, 3 de ellos no poseen estos entes.

- Países con participación de la UIFs en investigaciones de ciberdelitos:

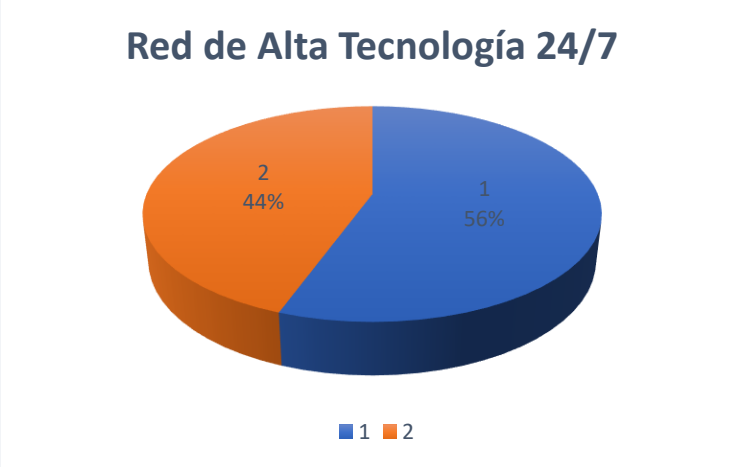
Con mayoría arrolladora, 17 de los 18 países que respondieron indicaron que sus unidades de inteligencia financiera si pueden participar o ya participan activamente en investigaciones de ciberdelitos en casos de legitimación de capitales.

- Países con controles en su país con relación a la prevención de lavado de activos producto de ciberdelitos:



Cómo podía predecirse con vista en los resultados de la normativa especial, los controles son ejecutados por la mayoría de los países, 15, contra 3 que no cuentan con ellos.

- Países vinculados a Red de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días (Red G8 24/7):



En correspondencia con la respuesta sobre adhesión

- Participación de sociedad civil en prevención o represión de la ciberdelincuencia:

Se observa con buenos ojos el involucramiento de la sociedad en la creación y elaboración de medidas preventivas y represivas. De 18 países que respondieron, solo en 4 no se da esa participación.

CONCLUSIONES

El plenario aprobó la realización del diagnóstico regional, sin embargo, la participación final de los países lo que permitió fue realizara una toma de muestra, prácticamente se recibieron respuestas de solamente la mitad de los estados miembros.

Sin embargo, se observa con aliento como una mayoría significativa ha procurado ajustar su legislación en materia de ciberdelitos. Ese ajuste legislativo comprende medidas de investigación, procesamiento y cooperación, así como en cuanto a medidas de aseguramiento con relación a los bienes que se incauten. Nótese que muchos de los países

ya contaban en sus Códigos Procesales con medidas aplicables, pero pese a ello, algunos legislaron de forma específica. El Grupo de Expertos encargados por la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDC) de realizar un estudio exhaustivo sobre el delito cibernético en el año 2019, hizo hincapié en que por la naturaleza evolutiva, complicada y transnacional, los Estados articular nuevas respuestas normativas internacionales contra el delito cibernético.

Es interesante observar ese avance legislativo, pese a que casi la mitad de los países que respondieron el cuestionario no han dado su adhesión o no han ratificado el Convenio de Budapest. Y en un porcentaje similar, debido al nexo del convenio, informaron que no están vinculados a la Red de Contactos sobre Delitos de Alta Tecnología 24/7 (Red G8 24/7). Se observó en las respuestas que esta es una herramienta que ha sido efectiva y de utilidad para los países que se encuentran vinculados y que la han podido utilizar. Como alternativa, los Estados de la región pueden promover la cooperación contra el lavado de dinero producto de ciberdelitos haciendo uso de los instrumentos existentes y promoviendo acuerdos bilaterales basados en el principio de reciprocidad.

Dichosamente, ese ajuste normativo ha conllevado a la creación de Fiscalías y Policías Investigativas especializadas, en casi la totalidad de las delegaciones que respondieron. Junto con estos entes, hay una participación activa de parte de las Unidades de Inteligencia Financiera, precisamente para comprobar el lavado de dinero cuando el delito cibernético es el precedente.

Sin embargo, a la región le aqueja una falta de capacitación en la materia a los integrantes de estos entes especializados. De las respuestas recibidas, se observa que los países se han esforzado en capacitarse a través de su mismo personal, recurriendo en la medida de sus posibilidades al acompañamiento de organismos internacionales como la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDC) y la Agencia Española de Cooperación Internacional (AECI). Este es un aspecto que urge atender, lo que procurará una mejora tanto en la investigación de este tipo de delitos, incluyendo cuando son los delitos precedentes en casos de lavado de dinero, así como en los resultados de las sentencias dictadas con base en una mayor comprensión y entendimiento de la materia. Por eso, pese a las limitaciones propias de muchos de nuestros países, debería procurarse destinar recursos y apoyo financiero necesario para brindar capacitaciones a estos funcionarios, que les permitan desarrollar conocimientos especializados que resulten en el

fortalecimiento de la capacidad de detección, investigación, procesamiento y condena legal y efectiva contra la ciberdelincuencia y el lavado de dinero producto de ella.

Esa comprensión de la materia incluso podrá fortalecer los controles que ejercen los países. Se observa con beneplácito como solamente el 17% de las delegaciones de la región que respondieron, indicaron que no cuentan con controles con relación a la prevención del lavado de activos producto de ciberdelitos.

Junto a esas acciones legislativas, una gran mayoría realiza un trabajo integral que incluye a participación de la sociedad civil en la prevención o represión de la ciberdelincuencia. El 78% de los países cuentan con estrategias, políticas, protocolos o instrumentos nacionales que permiten el aporte o la participación del sector privado, la sociedad civil y la academia. En algunos países están acciones son conjuntas, en otros, al promulgarse las normas, el sector privado se ve obligado a adoptar las medidas que se le imponen al respecto. Sin lugar a duda, se augura mayores y mejores resultados cuando las iniciativas y estrategias políticas para combatir el lavado de activos producto de ciberdelitos cuando se abordan de manera integral. En la prevención y represión juegan un importante papel los proveedores de servicios de internet, para que puedan apoyar la aplicación de la ley y de la investigación. La brecha digital puedes ser un obstáculo en algunos países en desarrollo con relación a las capacidades de prevención, detección y combate del ciberdelito y del lavado de dinero producto de él, volviéndolos más vulnerables.

El resultado global es que se trata de tarea en desarrollo, pero que ha provocado que la región dirija sus esfuerzos para enfrentar el desafío que significan los delitos cibernéticos, debido a su carácter transnacional y su complejidad. Se reportan esfuerzos contra la ciberdelincuencia por parte de la OEA. Estos son palpables a través del Departamento contra la Delincuencia Organizada (DDOT) encargado de la implementación de la Convención de las Naciones Unidas contra la Delincuencia Transnacional, que a su vez coordina con el Departamento de Cooperación Jurídica Internacional (DCJI). Este último promueve la cooperación jurídica internacional entre los Estados en materia de asistencia mutua penal y combate de los delitos cibernéticos en el marco de las Reuniones de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas (REMJA). Por su parte, el Portal Interamericano de Cooperación en Delitos Cibernéticos y el Grupo de Trabajo son dos de los mayores resultados de REMJA con el objetivo de fortalecer la cooperación hemisférica en la investigación y juzgamiento de estos crímenes. También la

Secretaría Ejecutiva del Comité Interamericano contra el Terrorismo (SE/CICTE) impulsa iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en la región.