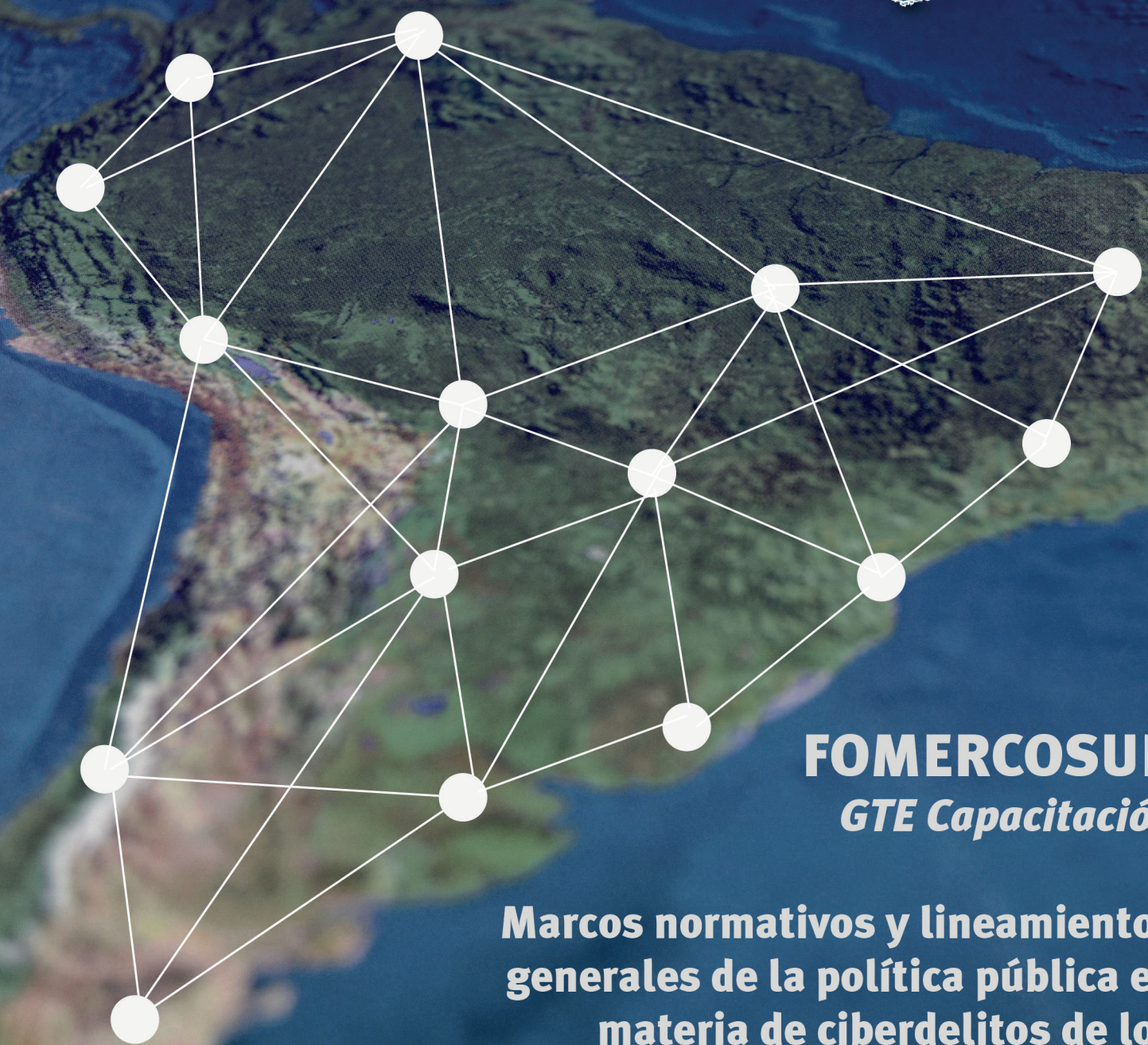
REVISTA
MERCOPOL

Capacitación y Cooperación Policial del Mercosur
Capacitação e Cooperação Policial do Mercosul

Edición Uruguay – Año XVII – Nº15 Mayo 2024
Presidencia Pro – Tempore – ISSN 2336-9236



FOMERCOSUR
GTE Capacitación

Marcos normativos y lineamientos generales de la política pública en materia de ciberdelitos de los países del MERCOSUR

Edición Uruguay – Año XVII – N°15 Mayo 2024
Presidencia Pro – Tempore – ISSN 2336-9236

Editores responsables del copilado:

Lic. Ana Ochoa Castellanos
Lic. Evelyn Dacil Garrote

Publicación anual
Formato digital

Edición Gráfica
DIRCOM - Ministerio del Interior

Indice

Prólogo

Jhonny Diego, subdirector de la Dirección de la Policía Nacional

Es un honor participar en la revista MERCOPOL, la cual vi nacer hace unos cuantos años, y en la que, en el pasado, he trabajado como redactor y compilador de artículos para ediciones similares.

Hoy, desde otro sitio, se me invitó a participar para adjetivar la importancia que tiene, que los profesionales de las Policías del MERCOSUR puedan aportar conocimiento basado en la experiencia sobre un tema tan delicado como lo es el Ciberdelito.

Esta forma de fenómeno delictivo, invade al mundo entero, se presenta en constante cambio y a una velocidad arrolladora, obligándonos a poner en marcha todos los dispositivos de formación y capacitación posibles con la finalidad de preparar a nuestros policías para hacerle frente, combatirlo y dar pronta y efectiva respuesta a las demandas de nuestras sociedades.

Esta maquinaria delictiva se ha instalado en nuestros países. Es el ataque a la Seguridad Pública, a la intimidad de nuestros habitantes en cualquiera de los aspectos de la vida cotidiana, al derecho a disfrutar con libertad de la convivencia pacífica y al goce de sus derechos, en una sociedad racional y sustentada en regímenes democráticos que se consolida a partir de la defensa de los Derechos Humanos de sus ciudadanos.

La creciente relevancia de la tecnología en el ámbito de la Seguridad Pública y la lucha contra el delito digital en un mundo cada vez más interconectado, interpela a los organismos gubernamentales de nuestros países.

La Policía se enfrenta a desafíos significativos en pro de la realización de un trabajo eficiente y eficaz en la protección de datos sensibles y la prevención de los ciberataques.

El conocer y combatir los modus operandis de estas organizaciones que mediante sus acciones menoscaban la seguridad e intimidad de los ciudadanos, sus empresas o simplemente sus formas de vida es actualmente abordada en diversas estrategias y enfoques, en trabajos en conjunto con las fiscalías, el Poder Judicial y otras instituciones públicas y privadas. Estas organizaciones delictivas que sin ningún tipo de escrúpulos y con la sola intención de obtener beneficios económicos, se valen de distintos artilugios para golpear en los lugares más débiles y desprotegidos de las sociedades, sin importar la magnitud de los daños ocasionados.

Perseguir este delito, a sus autores y someterlos a la justicia, recuperar los bienes y la seguridad de nuestros ciudadanos, es parte de un amplio decálogo de funciones que cumplen nuestras policías, ya sea en la faz preventiva como en la represiva, buscando en forma constante mejorar la calidad de vida de nuestros ciudadanos desde una visión genérica de la Seguridad Pública.

Agenda

Webinario Regional sobre Macro criminalidad y Ciberdelitos -MERCOSUR-	
Videoconferencia Zoom, 14 de octubre de 2022	
09.30 hs	Apertura de conexión
10:00 hs	**Bienvenida** Director Nacional de la Educación Policial, Crio. General Efraín Abreu y equipo de trabajo
10.10 hs	*Primer Panel* **Marco normativo, tipos penales, especificidades del ciberdelito, macro criminalidad y delitos transnacionales en los países de la región**
10.10 - 10.25hs	**Uruguay** Fiscal Letrada de la Fiscalía General de la Nación, Dra. Sandra Fleitas
10.25 - 10.40hs	**Argentina** Jefe de la División Investigación de los Ciberdelitos, de la Central de Investigación Criminal de la Prefectura Naval Argentina, Subprefecto Gonzalo Catanzariti y Especialista en informática forense de la Gendarmería Nacional Argentina, Segundo Comandante Lautaro Martín GIMENEZ
10.40 - 10.55hs	**Paraguay** Depto. Especializado en la Investigación del Cibercrimen y los delitos Informáticos, Oficial Primero de la Policía Nacional Carlos Insfran.
10.55 - 11.10hs	**Intercambio** Espacio de preguntas y respuestas
11.10 hs	*Segundo Panel* **Políticas públicas en materia de prevención e investigación de ciberdelitos**
11.10 - 11.25hs	**Argentina** Director de investigaciones del Ciberdelito, Ministerio de Seguridad, Sr. Pedro Daniel Janices.
11.25 - 11.40hs	**Brasil** Coordinador del Laboratorio de Operaciones Cibernéticas del Ministerio de Justicia, Dr. Alessandro Barreto
11.40 - 12.00hs	**Uruguay** Director de la Unidad de Cibercrimen de la Dirección de Investigaciones de la Policía Nacional, Crio. Gral. Paulo Rocha y Ofl. Ppal Oscar Pérez.
12.00 – 12.15	**Intercambio** Espacio de preguntas y respuestas
12.15 hs	Cierre de la actividad

Horario apertura: PRY | 8:30h | ARG, BRA, URY | 9:30h

Introducción

El advenimiento del fenómeno informático, ha impulsado una revolución digital en todo el mundo. Las innovaciones y avances tecnológicos ponen a disposición la posibilidad de recopilar, procesar y analizar enormes cantidades de datos, redundando en beneficios, tanto sociales como económicos, para innumerables áreas de investigación y desarrollo.

Al tiempo que las nuevas tecnologías han contribuido al desarrollo -ampliando potencialidades y generando mayor eficiencia y productividad- también se han multiplicado las posibilidades de cometer delitos, los que, en muchos casos, trascienden las fronteras.

En este contexto de alta complejidad y continua expansión de los delitos cibernéticos, nuestros países se ven obligados a profundizar cada vez más los conocimientos acerca de estas conductas delictivas y a implementar políticas y estrategias orientadas a prevenir, abordar e investigar los mismos.

El carácter transfronterizo de las amenazas plantea un desafío a nivel global y regional, que requiere de acciones coordinadas entre los Estados, generando las mayores sinergias posibles.

En este marco, bajo la organización del Grupo de Trabajo Especializado Capacitación (GTECAP) dependiente de la Reunión de Ministros del Interior y de Seguridad del MERCOSUR, el día 14 de octubre de 2022 se desarrolló el Webinario Regional sobre ciberdelitos, con el propósito de generar un espacio de intercambio entre los Estados Partes, en materia de macro criminalidad y delitos cibernéticos.

El webinario abordó principalmente marcos normativos y lineamientos generales de las políticas públicas implementadas por los distintos países de la región en materia de combate al ciberdelito. Tiene como finalidad, contribuir al enriquecimiento de perspectivas y abordajes, para encontrar las mejores respuestas ante los diferentes escenarios y situaciones delictivas que se presentan. En la actividad participaron como disertantes especialistas de Argentina, Brasil, Paraguay y Uruguay.

Como producto del encuentro, tomando como insumo las disertaciones realizadas, así como posteriores aportes consignados por los Estados participantes, el GTECAP elaboró el presente documento compilado, que se estructura en dos partes, un primer apartado describe los marcos normativos y avances en relación a la incorporación de nuevos tipos penales, al marco jurídico de los países de la región; y un segundo título, desarrolla algunos de los lineamientos generales de las políticas llevadas adelante en materia de prevención e investigación de ciberdelitos.

Entendemos que la producción de conocimiento sistematizado y actualizado, es un aporte clave para la definición de políticas públicas eficaces y acordes a la realidad regional.

Finalmente, cabe destacar que estas contribuciones se articularán para la elaboración de futuras propuestas de capacitación específicas.

Marco normativo y especificidades del ciberdelito en los países del Mercosur

Argentina

En el año 2008, se aprueba en la República Argentina la Ley N° 26.388 de Delitos Informáticos, la cual clasifica a los delitos informáticos en cuatro grupos:

- Accesos ilícitos
- Interceptación ilícita
- Atentados contra la identidad de los datos
- Atentados contra la integridad de los sistemas

La ley a lo largo de su articulado, tipifica distintos delitos informáticos e incorpora figuras a diversos artículos del Código penal en vigencia, con el fin de regular las nuevas tecnologías como medios de comisión de delitos.

Por otra parte, en el año 2013 se aprueba la Ley 26.904, mediante la cual se incorpora la figura de grooming al código penal. Esta ley establece una pena de entre seis meses y cuatro años al que "por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

Por grooming se entiende a la acción deliberada de un adulto al contactar a una niña, niño o adolescente con el propósito de cometer cualquier delito contra la integridad sexual, a través de un medio digital como por ejemplo, redes sociales, correo electrónico, mensajes de texto, sitios de chat, juegos en línea, entre otros.

En general las personas que realizan esta actividad, utilizan perfiles que son creados con este propósito, simulan interés y se involucran en lugares que son frecuentados por niñas, niños o adolescentes.

El delito de grooming tiene la particularidad de que en general la evidencia se encuentra expuesta en correos electrónicos, redes sociales o algún servicio que posea mensajería. Poder recolectar y resguardar esa evidencia, resulta fundamental para el proceso probatorio.

A su vez, en el año 2017 se aprueba la ley 27.319 de Investigación, prevención y lucha de delitos complejos, con el objeto de brindar a las Fuerzas Policiales y de Seguridad, al Ministerio Público Fiscal y al Poder Judicial las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de delitos complejos.

Esta ley regula las figuras de agente encubierto, agente revelador, informante, entrega vigilada y prórroga de jurisdicción.

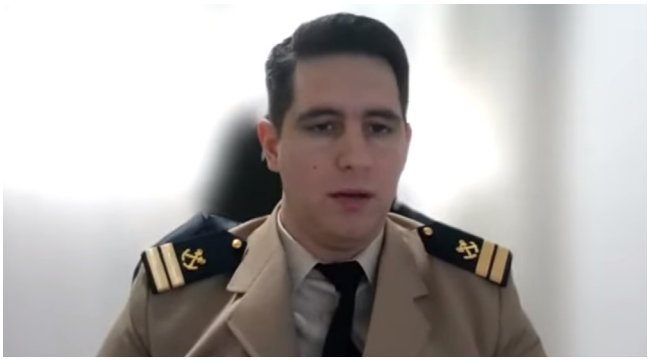
Uno de los desafíos que actualmente tiene la Argentina, es buscar la manera de adecuar la figura de agente revelador al ámbito de lo virtual, ya que hoy se aplica sólo a algunos delitos: comercio y tráfico de estupefacientes, delitos contra la integridad sexual, delitos aduaneros, secuestros extorsivos, trata de personas, asociación ilícita, lavado de activos, terrorismo.

Por otra parte, en el año 2016 mediante la Resolución 234/2016 del Ministerio de Seguridad, se aprueba el "Protocolo general de actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos". El mismo tiene por objeto establecer las pautas, procedimientos y principios a tener en cuenta al momento de la investigación, modo de obtención, conservación y tratamiento de las evidencias digitales, desde la actuación de los agentes de prevención, hasta la entrega de las mismas para su análisis. Al presente, el mencionado Protocolo se encuentra en proceso de actualización.

En cuanto al marco legal internacional, en el año 2017 -mediante la sanción de la Ley Nro. 27.411, la Argentina adhirió el convenio de Budapest sobre ciberdelincuencia[1] .

Asimismo, el "SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO SOBRE CIBERDELINCUENCIA, SOBRE COOPERACIÓN REFORZADA Y ¡¡¡¡DIVULGACIÓN DE EVIDENCIA ELECTRÓNICA", fue adoptado por los Estados Miembros del Consejo de Europa y los Estados partes de la Convención de Budapest el 17 de noviembre del año 2021. El día 16 de Febrero de 2022, el Sr. Ministro de Seguridad, Cdor/Dr. Aníbal Domingo Fernández, con plenos poderes otorgados por el del Sr. Presidente de la Nación, firmó la adhesión sujeta a ratificación de la República Argentina, al citado Segundo Protocolo en la Ciudad de Estrasburgo, República de Francia ante la Sra. Secretaria General del Consejo de Europa, Marija Pejcinovic Buric.

Por otra parte, la República Argentina, mediante la Dirección de Investigaciones del Ciberdelito del Ministerio de Seguridad de la Nación, en conjunto con otros organismos del Poder Ejecutivo Nacional, forma parte del Comité Especial de las Naciones Unidas encargado de elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. Dicha Convención se encuentra en proceso de elaboración.



1 - El Convenio de Budapest es el primer instrumento internacional que trata de manera específica aspectos relacionados con el ciberdelito con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet. El mismo fue sancionado en noviembre de 2001 por el Consejo de Europa y entró en vigencia en 2004.

Brasil

A nivel internacional, Brasil es signatario de la Convención de Budapest sobre la Cibercriminalidad y promulgó la Convención sobre el Cibercrimen en noviembre de 2001, con la aprobación del Congreso Nacional, en diciembre de 2021 y promulgada por el Decreto 11.491, de abril de 2023.

A nivel nacional, aunque no existe en el país una ley específica que aborde exclusivamente los delitos cibernéticos, existen normas que tratan sobre conductas y sanciones relacionadas con la comisión de delitos virtuales:

- Ley 12.965 del 23 de abril de 2014, que establece el Marco Civil de Internet en el país;
- Ley 12.737/2012, conocida como "Ley Carolina Dieckmann"; • Ley 9.609/1998;
- Ley 8.069 del 13 de julio de 1990, Estatuto del Niño y del Adolescente (ECA); y
- Código Penal-Decreto-Ley 2848, del 7 de diciembre de 1940 y sus enmiendas.

A continuación, se presentan aspectos relevantes de las leyes mencionadas anteriormente.

Para comprender las normas brasileñas relacionadas con los delitos cibernéticos, es esencial abordar la Ley 12.965/2014, que establece el Marco Civil de Internet en el país. Esta ley regula el uso de esta tecnología en Brasil, delineando principios, garantías, derechos y deberes de los usuarios de la red, así como orientando la actuación del Estado. El Marco Civil de Internet aborda cuatro pilares fundamentales: los derechos de los usuarios, la responsabilidad por el contenido disponible, el almacenamiento y suministro de datos de conexión y acceso, y la neutralidad.

Desde la perspectiva de la investigación de delitos cibernéticos, el Marco Civil de la misma, aborda de manera significativa la cuestión del almacenamiento y la disponibilidad de datos personales, de contenido y registros de conexión (IP), además de las condiciones que deben observar estas empresas al proporcionar dicha información a las Policías Civiles y la Policía Federal.

En relación a la solicitud de conservación de datos y protección de la privacidad, aunque la legislación impone plazos cortos para el almacenamiento de datos por parte de las empresas de Internet y los proveedores de conexión, el Marco Civil prevé la figura de la solicitud de conservación de datos (Art. 13, § 2, y Art. 15, § 2). Este mecanismo permite a las autoridades policiales, administrativas y al Ministerio Público solicitar cautelarmente que los datos personales, datos de contenido o registros de conexión, se conserven por un período superior a un año (para proveedores de acceso) o seis meses (para proveedores de aplicaciones).

Por otra parte, el Marco Civil, antes mencionado establece que el almacenamiento y la disponibilidad de registros de conexión y acceso, datos personales y contenido de comunicaciones privadas, deben respetar la preservación de la intimidad, la vida privada, la honra y la imagen de las partes involucradas, directa o indirectamente. Esto significa que esta información forma parte del ámbito de protección de la privacidad de las personas y no puede accederse libremente, ni siquiera por parte de órganos de persecución penal, como el Ministerio Público, la Policía Civil y la Policía Federal. Dicho Marco Civil, a través del Artículo 10, § 1, somete los registros de conexión (o acceso), datos personales y contenido de comunicación, como reserva de jurisdicción.

Con la promulgación de la Ley 12.737/2012, conocida como "Ley Carolina Dieckmann", se instituyó el delito de invasión de dispositivo informático. Esta legislación tiene como objetivo criminalizar la creación y difusión de virus informáticos, así como la invasión de sistemas (hacking), entre otras conductas, incluyendo la inserción del artículo 154-A en el Código Penal. El bien jurídico protegido es la privacidad, que abarca la intimidad y la vida privada, según lo establecido en el Artículo 5, X, de la Constitución Federal de 1988 (CF/88). Por lo tanto, este nuevo tipo penal busca proteger valores amparados constitucionalmente.

Por otro lado, el delito de violación de derechos de autor de programas de computadora, está regulado por la Ley 9.609/1998, también conocida como la Ley del Software. Esta ley protege la propiedad intelectual de los programas de computadora, garantizando a los titulares de los derechos de autor de los programas de computadora, los mismos derechos conferidos a las obras literarias por las leyes de derechos de autor vigentes en el país.

Con respecto al Estatuto del Niño y del Adolescente (ECA), Ley 8.069/1990, establece un delito cibernético propio en el Artículo 241-A. Este delito se refiere a la circulación de material pornográfico infantil a través de sistemas informáticos o telemáticos.

Esta norma tiene como objetivo frenar la difusión de material pornográfico que involucra a menores de edad y abarca diversas acciones relacionadas con la divulgación de este tipo de contenido, así como la provisión de medios para almacenarlo o acceder a él.

Asimismo, el Artículo 218-C del Código Penal establece el delito de divulgación de escenas de violación o de violación de persona vulnerable, de escenas de sexo o pornografía, principalmente cuando involucran a víctimas menores de edad.

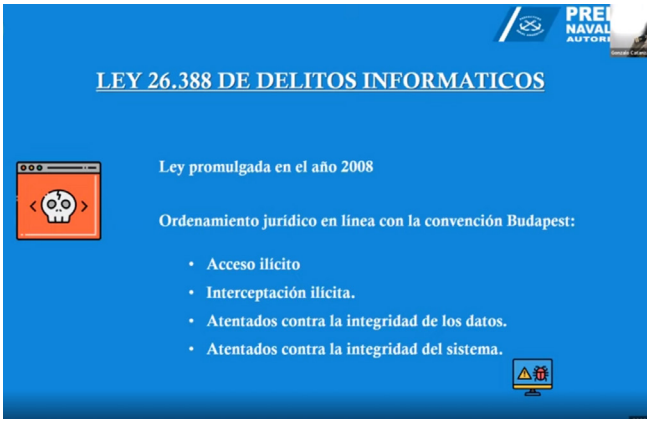
El Artículo 154-A del Código Penal, penaliza a quienes fabrican, ofrecen, distribuyen o venden a terceros, o simplemente difunden dispositivos o programas de computadora, que puedan utilizarse para invadir dispositivos informáticos o instalar vulnerabilidades en ellos. Esta disposición legal abarca, por ejemplo, acciones relacionadas con troyanos y keyloggers, que a menudo se utilizan para obtener indebidamente las contraseñas bancarias de los usuarios. Además prevé un aumento de la pena de un sexto a un tercio, si la invasión resulta en daño económico.

Es importante destacar que el delito previsto en el Artículo 154-A del Código Penal no debe confundirse con el delito descrito en el Artículo 10 de la Ley 9.296/1996. Mientras que el primero se refiere a la invasión de dispositivos informáticos seguido del acceso a comunicaciones electrónicas privadas almacenadas en una computadora, el segundo trata sobre la interceptación de estas comunicaciones en tiempo real.

Otro delito cibernético es la inserción de datos falsos en sistemas de información, introducida en el Código Penal por la Ley 9.983/2000, conocido como "peculado electrónico", ocurre cuando un funcionario público autorizado introduce o facilita la inserción de datos falsos, modifica o elimina datos correctos en sistemas informatizados o bases de datos de la Administración Pública, con la intención de obtener una ventaja indebida o causar daño. La pena por este delito varía de dos a doce años de reclusión y multa.

Además, la misma ley también introdujo el delito de modificación o alteración no autorizada de sistemas de información.

Finalmente, el delito de interrupción o perturbación de un servicio telegráfico, telefónico, informático, telemático o de información de utilidad pública, establecido en el Artículo 266 del Código Penal, abarca diversas conductas que afectan a los servicios de comunicación e información de utilidad pública. Por lo tanto, se considera un delito cibernético propio.



Paraguay

En el año 2011, Paraguay introduce los delitos informáticos en su legislación. Mediante la Ley 4439/11 se modifican e incorporan nuevos artículos al código penal, tipificando y estableciendo sanciones para los distintos tipos de delitos:

- Pornografía relativa a niños, niñas y adolescentes.
- Acceso indebido a datos (phishing)
- Interceptación de datos.
- Preparación de acceso indebido e interceptación de datos.
- Acceso indebido a sistemas informáticos.
- Sabotaje de sistemas informáticos.
- Estafa mediante sistemas informáticos.
- Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago.

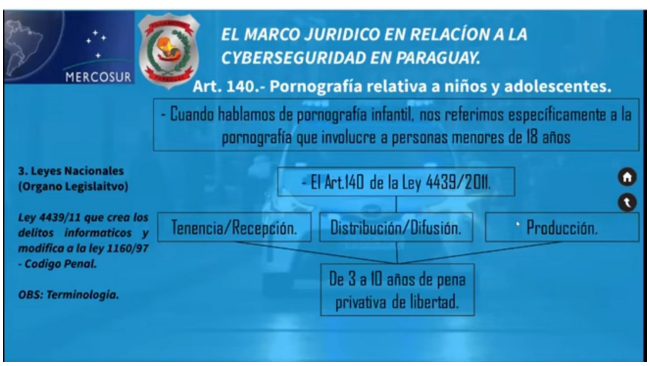
En el año 2015, se aprueba la ley 4633/15 contra el acoso escolar en instituciones educativas públicas, privadas o privadas subvencionadas, incorporando las figuras como el grooming, el bullying y el ciberbullying. En el año 2017, la Ley 6002/17 que modifica artículos del código penal paraguayo, tipificando el abuso por medios tecnológicos.

Asimismo, se ha aprobado una Resolución que establece el protocolo de actuación ante vulneración de derechos sexuales en instituciones educativas.

En cuanto al marco normativo internacional, en el año 2017, mediante la Ley N° 5994/17, Paraguay aprueba la convención de Budapest sobre ciberdelincuencia y el protocolo adicional al convenio relativo a la penalización de actos de índole racista y xenofobia, cometidos por medio de sistemas informáticos. Asimismo, el segundo protocolo adicional al convenio sobre cooperación reforzada y divulgación de pruebas electrónicas, se encuentra próximo a ser aprobado por Ley.

El Decreto N° 7052/2017 del Poder Ejecutivo aprueba el Plan Nacional de Ciberseguridad, elaborado por la Secretaría Nacional de Tecnologías de Información y Comunicación (SENATICS), en coordinación con el Ministerio de Relaciones Exteriores (MRE) y con el apoyo de la Organización de los Estados Americanos (OEA). El Plan Nacional de Ciberseguridad es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente.

En resumen, no existe una regulación específica que trate la ciberseguridad en un solo cuerpo normativo, sino que esta se encuentra diseminada en varias normativas que tratan diversos aspectos vinculados al tema.



Uruguay

Teniendo una Legislación en proceso de actualización a los tiempos que corren, Uruguay se encuentra en vías de incorporar a la normativa vigente, nuevas figuras delictivas, que favorecerán el actuar policial y judicial, desde un aspecto relacionado directamente a la Ciberseguridad. El anteproyecto de Ley que se encuentra en tratamiento en el Poder Legislativo busca tipificar e incorporar distintos delitos informáticos al Código Penal, contemplando entre otros:

- Stalking o acoso telemático
- Grooming, acercamiento físico o virtual
- Estafa informática
- Daños informáticos
- Acceso ilícitos a base de datos
- Vulneración sistemas informáticos

Cabe destacar que en la actualidad se investiga y se actúa sobre estos delitos con la legislación vigente, dado el complemento del uso de medios informáticos para llevar adelante los mismos.

Una de las leyes actualmente vigente es la Ley 17.815 de Violencia sexual comercial o no comercial cometida contra niños, adolescentes o incapaces, la cual tipifica y sanciona la fabricación, producción, comercio, difusión y facilitamiento de material pornográfico con niñas, niños, adolescentes o incapaces.

Asimismo, la Ley 18.383 del 2008 modificó el artículo 217 del Código Penal para tipificar el delito de Atentado contra la regularidad de las telecomunicaciones alámbricas o inalámbricas; así como también se tipificó el delito de Falsificación de documento electrónico – Artículo 4 de la ley 18.600 del año 2009 - y el delito de Grooming que fue incorporado al Código Penal – Art. 277 bis-.

Respecto al marco normativo internacional, si bien se cuenta con un fuerte relacionamiento con organismos internacionales para el tratamiento de ciertos delitos, a saber: Dir. Gral. Lucha Contra el Crimen Organizado e INTERPOL, EUROPOL - EC3 - Centro Europeo De Cibercrimen, El Centro Nacional para Niños Desaparecidos y Explotados NC MEC (siglas en inglés),

Oficina de Investigaciones de Seguridad Nacional de los EE.UU. HSI, entre otras; se entiende que los delitos transnacionales requieren una continua e ininterrumpida cooperación internacional. En ese sentido, Uruguay ha sido invitado a sumarse e integrar la Convención de Budapest, siendo este el primer tratado de acuerdo internacional, con una integración de más de 65 países, y cuyo objetivo es proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, por medio de tres grandes pilares: la elaboración de leyes adecuadas, la mejora de las técnicas de investigación, y el aumento de la cooperación internacional. Esta situación equipara al país en un mismo nivel, en relación al acceso a la información, a la colaboración internacional, así como también a la capacitación y formación de los funcionarios abocados al tratamiento de estos delitos.

Lineamientos generales de las políticas públicas que los Estados llevan adelante en materia de prevención e investigación de ciberdelitos y desafíos a futuro

Argentina

En el año 2019 se aprueba mediante la Resolución del Ministerio de Seguridad N° 977/2019 el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, que establece los lineamientos y prioridades de las políticas públicas relacionadas con las responsabilidades referentes al ciberespacio y su impacto en la Seguridad Nacional, se busca incrementar las capacidades en la materia, sobre la base de la coordinación y cooperación entre los organismos del sector público, el sector privado, las organizaciones no gubernamentales y las entidades académicas.

En ese marco, en el año 2022 se aprueba el "Programa de fortalecimiento en ciberseguridad y en investigación del cibercrimen" (Forcic) mediante la Resolución 86/22 del Ministerio de Seguridad, con el objetivo de coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales y en técnicas de investigación en materia de ciberdelitos.

Las acciones que se llevan adelante buscan incrementar las capacidades de prevención e investigación del ciberdelito, fortalecer los recursos humanos, así como también asesorar y brindar equipamiento específico en materia de investigación de ciberdelitos.

En ese sentido, se busca dotar a las fuerzas federales y provinciales, de equipamiento y herramientas tecnológicas. Al día de hoy se ha brindado el mecanismo equipamiento y las capacitaciones a 21 provincias adheridas al mencionado Programa, el cual tiene carácter federal.

Asimismo, se puso en funcionamiento y se está equipando el "Centro de investigación de ciberdelitos de alta tecnología (CICAT)" para la capacitación, prevención, análisis e investigación de ciberdelitos. Es el primer centro que incluye a las cuatro Fuerzas Federales que trabajan en conjunto en un mismo lugar.

A su vez, uno de los objetivos es fortalecer las acciones de prevención y de cooperación público-privadas con ONGs, universidades, empresas. En esta línea, se han firmado convenios de cooperación con distintas instituciones para capacitar a las fuerzas y poder acceder a información anticipada que permita prevenir esta clase de incidentes.

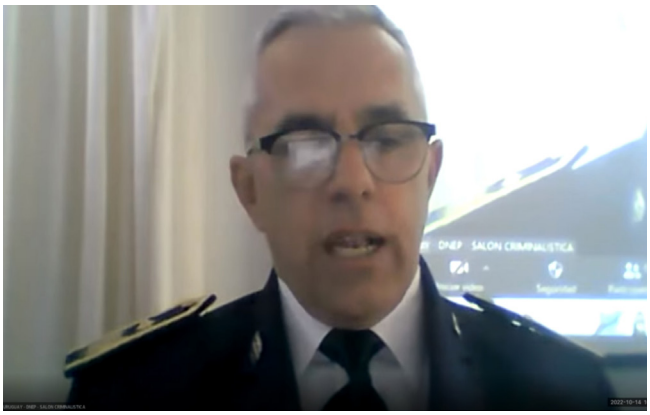
El ciberdelito está atravesando casi todos los delitos penales (lavado de activos, narcotráfico, falsificación de moneda, extorsión, etc). En ese contexto, Argentina entiende que es necesario incorporar y fortalecer las herramientas disponibles para enfrentar la complejidad actual, profundizando las acciones relativas a la capacitación y buscando fortalecer los canales de cooperación.

Es muy importante contar con acciones preventivas e investigativas, así como también estudiar cuales son las nuevas amenazas que se presentan.

Algunos desafíos por delante son:

- Avanzar en la instrumentación del acceso transfronterizo de datos;
- Fortalecer el intercambio de información entre países;

Promover el desarrollo regional de nuevas capacidades investigativas.



Brasil

Brasil ha adoptado un enfoque multifacético para combatir el delito cibernético, que involucra tanto la legislación nacional, como la cooperación internacional.

La creación de comisarías especializadas en delitos cibernéticos en varios estados, es un paso importante para investigar y combatir estas actividades. Además, Brasil ha cooperado internacionalmente en operaciones conjuntas para combatir el cibercrimen.

Algunas de las herramientas que se utilizan son: fuentes abiertas, interpretación telemática, infiltración policial, técnicas NIT – investigativas, diligencias.

En resumen, Brasil ha avanzado en la regulación y la lucha contra el cibercrimen, estableciendo un marco legal sólido y promoviendo la cooperación internacional.

Paraguay

En cuanto a lineamientos generales de las políticas públicas en materia de prevención e investigación de ciberdelitos, Paraguay posee un Plan Nacional de Ciberseguridad, puesto en marcha mediante decreto del Poder Ejecutivo Nº 7052. Este es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente. Establece principios orientadores en materia de ciberseguridad y 7 (siete) ejes y objetivos que incluyen: Sensibilización y Cultura, Investigación, Desarrollo e Innovación, Protección de Infraestructuras Críticas, Capacidad de Respuesta ante Incidentes Cibernéticos, Capacidad de Investigación y Persecución de la Ciberdelincuencia, Administración Pública y Sistema Nacional de Ciberseguridad.

En concordancia con lo anterior, la articulación se da a través de varias instituciones. En el caso de la Policía Nacional, esta cuenta con una dependencia especializada en materia de ciberseguridad, el Departamento Especializado en la Investigación del Cibercrimen y Delitos Informáticos, cuyas principales funciones son: Dentro de las políticas estatales en materia de delitos informáticos, también existe una Unidad Especializada del Ministerio Público, que trabaja de manera conjunta con la Policía Nacional para combatir los hechos punibles cometidos a través del uso de la tecnología, que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital.

En ese contexto, se encuentran en vigencia las Resoluciones Nº 3459/10 y 4408/11, que delimitan los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos que son los siguientes: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos.

Como otro aspecto resaltante dentro de las políticas públicas, se encuentra la realización y seguimiento de charlas en instituciones educativas de todo el país, en el marco del programa Fiscalía en la Escuela. Funcionarios de la Unidad brindan capacitaciones sobre el ciberbulling, sexting, pornografía infantil y grooming, es decir, sobre los peligros y amenazas existentes contra los menores en internet.

El trabajo coordinado de los órganos estatales, dio como resultado la masificación de campañas en redes masivas de comunicación contra los delitos informáticos, buscando generar consciencia y evitar que la ciudadanía sea víctima de hechos que guardan relación con los mismos.

En resumen, se destacan estrategias por parte del Estado, para la neutralización de esta clase de delitos; el Plan Nacional de Ciberseguridad, elaborado por la Secretaría Nacional de Tecnologías de Información y Comunicación (SENATICS), la ley contra los Delitos Informáticos, la firma digital, la ley de Comercio Electrónico, la aplicación y el uso de las TICs en la gestión pública, el trabajo coordinado de la Policía Nacional – Ministerio Público.

Uruguay

Uruguay cuenta con un Departamento de Delitos Informáticos dependiente de la Dirección General de Lucha contra el crimen organizado e Interpol, el cual tiene entre sus competencias:

• Investigación de los delitos computacionales e informáticos Realización de análisis forense de equipos electrónicos y medios informáticos

• Investigación contra la explotación sexual de personas menores de edad o incapaces

• Violencia sexual o no comercial contra niños, adolescentes o incapaces (Ley 17.815)

• Pornografía de menores o incapaces, comercial y difusión de material pornográfico en el que aparezcan imagenes de menores de edad
Por otra parte, mediante La Ley N° 19.996, de aprobación de rendición de cuenta, ejercicio 2020, se ha creado la "Unidad de Cibercrimen" bajo la órbita de la Dirección de Investigaciones de la Policía Nacional (art. 107) con el objeto de "Detectar, investigar, perseguir y reprimir las conductas antijurídicas de amenazas, hackeos, ataque o daño contra la seguridad, la confidencialidad y la integridad de sistemas informáticos, bancos o bases de datos y redes; sabotajes y espionaje informático, ataques Dos (Denial of Service) y Ddos (Distrinuted Denial of Service)"

La ley de rendición de cuentas incorpora un Consejo Asesor honorario de Seguridad Informática, integrado por representantes de distintos organismos como la Policía, Ministerio

de Defensa, la Agencia para el desarrollo de gestión electrónica, el Ministerio de Industria y el Banco Central de Uruguay. Es un canal para seguir avanzando.

También la ley da facultades a la Policía para coordinar y dar aviso a otras instituciones financieras, bancos, empresas, etc sobre ciertas situaciones relacionadas a estafas.

Con respecto a la información estadística de incidentes de seguridad informática, durante 2021 en Uruguay se detectaron y respondieron 3948 incidentes informáticos de los cuales el 1,3% fueron calificados con severidad "alta" o "muy alta". Esto representa un crecimiento de un 41% en relación a los detectados en 2020.

En cuanto a los incidentes de seguridad informática, según las evaluaciones de riesgo realizadas, el malware y la recolección de información (pishing) han sido los que más han avanzado.

Los delitos mayormente trabajados desde el punto de vista policial en el año 2021 fueron:

- Delitos sexuales (23.1%)
- Difamación (21,9%) – duplicación de perfiles, cuentas anónimas
- Violación de correspondencia (13,2%)
- Extorsión (12,1%)

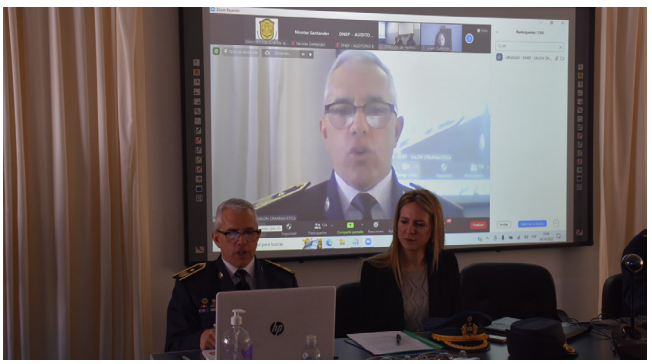
En cuanto a la cooperación internacional para el abordaje de delitos transnacionales, se trabaja en cooperación con organizaciones como Interpol, Europol, Ameripol, el National Center for Missing and Exploited Children, entre otros. A la vez, Uruguay integra a partir de la firma del convenio de Buenos Aires junto a otros doce países de América Latina y el Caribe la AC3, Centro Especializado en Cibercrimen, el cual facilita la cooperación para trabajar este tipo de delitos.

Finalmente, a pesar de que la promoción de la conectividad y el acceso a Internet en los hogares, junto con la mejora de los planes de conexión y la provisión de medios multimedia, es imperativo reconocer que desde una perspectiva profesional, esta situación puede dar lugar a vulnerabilidades significativas si no se le otorga la atención adecuada.

Esta situación se relaciona estrechamente con el hecho de que no toda la población dispone del conocimiento necesario para comprender la facilidad con la que su seguridad informática puede ser comprometida, lo que a su vez pone en riesgo su reputación y sus activos. En un enfoque preventivo, se destaca la importancia de la labor dirigida a evitar futuros delitos, a través de la educación y la concienciación de la comunidad, particularmente en lo que respecta a los riesgos del abuso sexual en línea de menores.

Adicionalmente, en relación con la carencia generalizada de conciencia y conocimiento, acerca de la exposición de datos e información, existen aspectos adicionales que merecen ser considerados como debilidades, que requieren atención conjunta y mejoras sociales en la lucha contra el cibercrimen.

Advertimos que, la escasez de profesionales en este campo y la necesidad de divulgar conocimiento en todos los niveles educativos, están siendo abordadas mediante la actualización de los planes de estudio, donde la formación en ciberseguridad se integra y se valora cada vez más. En resumen, la promoción y ejecución de campañas preventivas, con un enfoque en la seguridad de la información, se convierten en herramientas fundamentales.



A modo de cierre

El creciente número de delitos cibernéticos en la región es un desafío que requiere atención y acción inmediata por parte de las autoridades y la sociedad en su conjunto. El impacto financiero de estas actividades ilícitas es significativo y afecta, no sólo a las víctimas directas, sino también a la economía de los países en su conjunto.

A lo largo del documento hemos podido apreciar algunas tendencias compartidas en materia de prevención y abordaje de estos delitos.

Si bien con distinto grado de avance, los países de la región han comenzado un proceso de adecuación de sus legislaciones, orientado a incorporar nuevos tipos penales asociados a delitos informáticos, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos, así como de proteger datos personales e informaciones digitales como bienes jurídicos. Algunos Estados han promulgado leyes específicas en el área.

A la vez, se ha avanzado en la implementación de políticas públicas y programas de acción, existiendo un consenso general en destacar la importancia de la prevención e investigación de ciberdelitos, más allá de las soluciones legales.

Asimismo, se recalca que la rápida y constante evolución de las tecnologías y las tácticas criminales requiere una continua actualización de las leyes y estrategias de afrontamiento. Además, resulta fundamental concienciar a la población sobre la importancia de la ciberseguridad y la protección de sus datos personales para ayudar a reducir estos delitos.

Para finalizar, creemos enriquecedor recuperar algunos de los puntos que fueron referidos por los países durante el desarrollo del Webinario del 14 de octubre de 2022, como desafíos a trabajar a futuro.
En ese sentido, se destacó la importancia de:

- Fortalecer las instancias de capacitación en la temática.

- Generar más canales de cooperación internacional, tanto formales como informales.
- Trabajar y profundizar acciones vinculadas a la prevención del delito.

- Fortalecer los recursos humanos y capacidades operativas para combatir este tipo de crimen.

- Generar espacios de intercambio de experiencias e información vinculadas al abordaje de los ciberdelitos a nivel regional.


CCCP
CENTRO DE COORDINACIÓN DE CAPACITACIÓN POLICIAL
MERCOSUR
MERCOSUR
REVISTA
MERCOPOL
Capacitación y Cooperación Policial del Mercosur
Capacitação e Cooperação Policial do Mercosul