PROGRAMA **JUNIOR**
FELLOWSHIP 2023

LEGISLACIÓN Y ENFOQUES EN CIBERDELITOS

Estudio comparativo para América Latina

Paula Otalora

CENTRO LATAM DIGITAL

cet.la
Centro de Estudios de Telecomunicaciones de América Latina

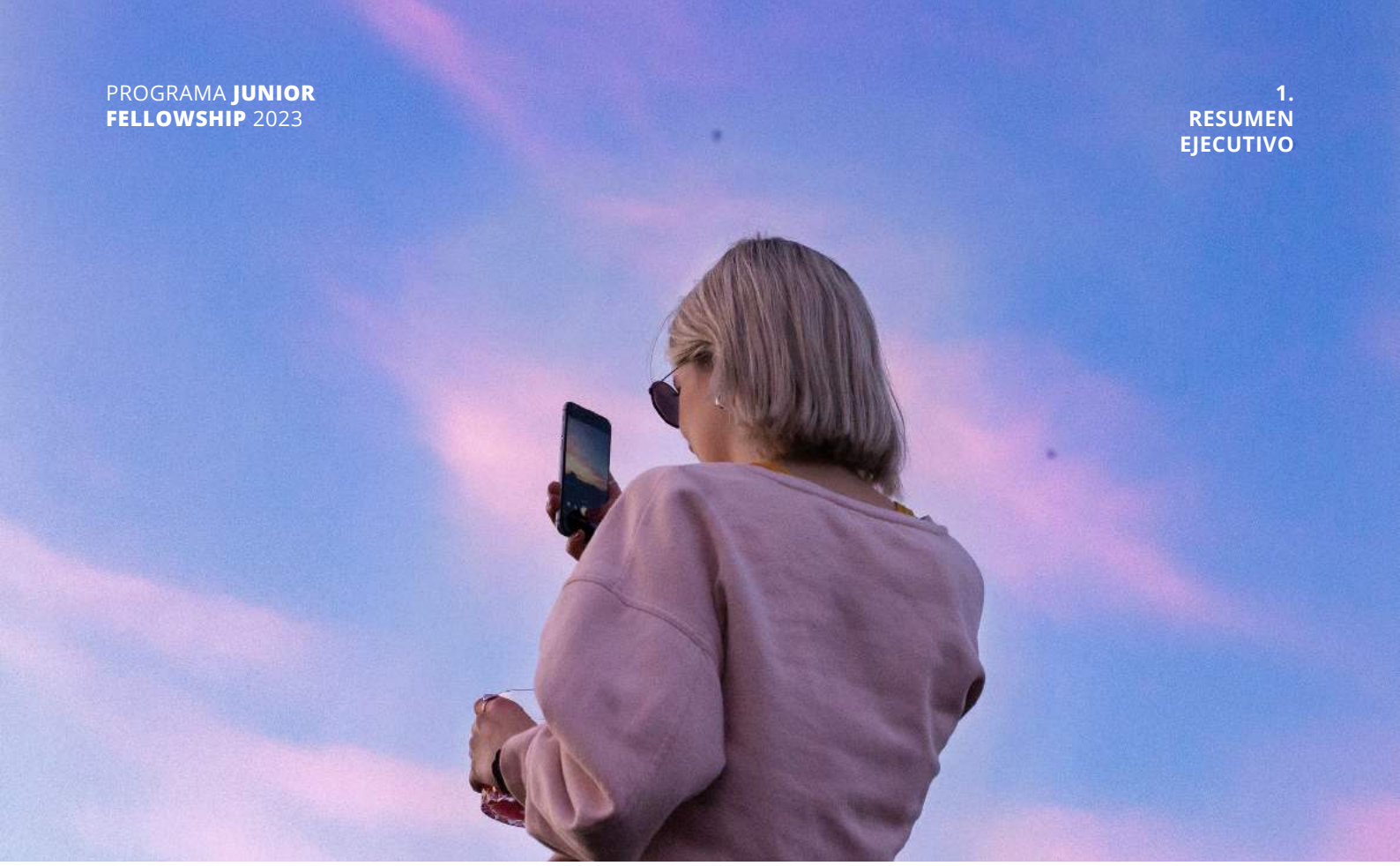
El Centro de Estudios de Telecomunicaciones de América Latina (cet.la) es una iniciativa de ASIET, Asociación Interamericana de Empresas de Telecomunicaciones, que tiene por objetivo promover y apoyar la reflexión y el debate sobre las políticas públicas orientadas al desarrollo de las telecomunicaciones y la sociedad de la información en la región, contribuyendo con elementos de análisis técnicos y económicos, a su diseño, ejecución y evaluación. El centro de estudios no expresa opiniones o recomendaciones en nombre de ASIET.

estudios@tel.lat
cet.la

El Centro LATAM Digital (CLD) es un centro de investigación que produce investigación relevante y rigurosa que contribuya a informar y enriquecer el diseño e implementación de políticas digitales que fortalezcan el desarrollo a través de un acceso equitativo e inclusivo a tecnologías digitales en México y América Latina. El objetivo de la organización es fomentar conocimiento que fortalezca el diseño de políticas digitales con el fin de impulsar un desarrollo social y económico en el cual se aprecie un futuro en el que las tecnologías de la información sean un motor de integración social, productividad y prosperidad para el bienestar de las personas en América Latina.

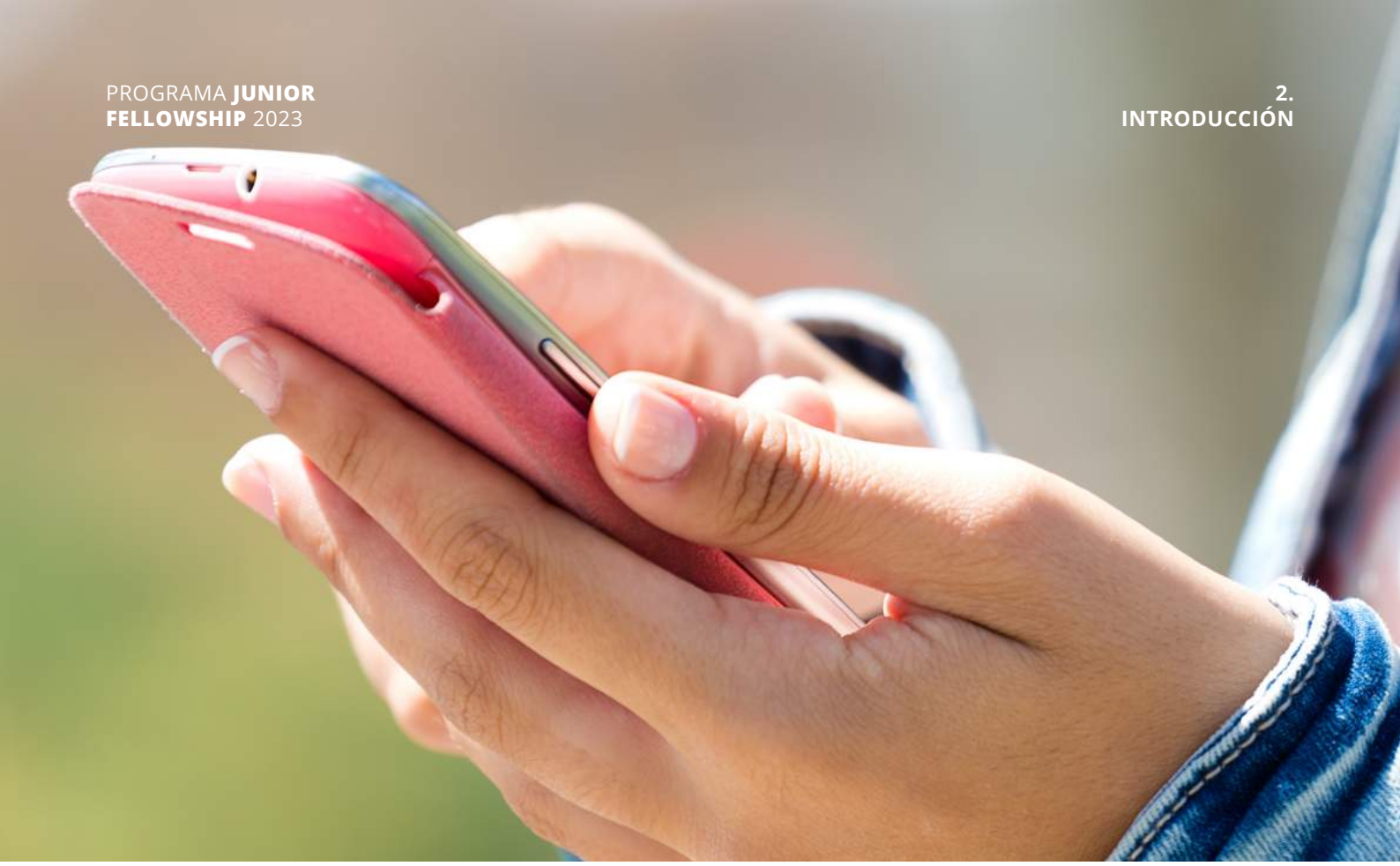
info@centrolatam.digital
centrolatam.digital

Contenido



1. Resumen Ejecutivo

Esta investigación analiza cuáles han sido las prioridades de los marcos normativos de 9 países latinoamericanos en ciberseguridad. Los resultados muestran que las prioridades se centran en la regulación de ciberdelincuencia, propiedad intelectual y protección de datos, por lo que se procedió a estudiar la normativa de ciberdelincuencia o delitos informáticos de cada uno. El análisis se enfocó en evaluar las prioridades de los 9 marcos normativos, tomando como referencia 7 delitos informáticos según el Convenio de Budapest. Cada disposición legal se examinó desde cuatro enfoques: protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables. La metodología utilizada combina el análisis legal con dos índices que evalúan el énfasis de cada país en relación con estos delitos.



2. Introducción

La ciberseguridad es un tema de creciente importancia en la actualidad. El aumento de la digitalización de la sociedad ha generado nuevas amenazas cibernéticas que ponen en riesgo la seguridad de las empresas, los ciudadanos y los gobiernos.

En respuesta a estas amenazas, los países de las diferentes regiones del mundo, especialmente Estados Unidos, Estonia, Israel, y países europeos[1] han adoptado una serie de medidas para fortalecer su ciberseguridad, como la expedición de marcos normativos y guías de buenas prácticas, inversión en capacitación y tecnología, entre otros.

La región latinoamericana se ha convertido en un epicentro de actividad cibernética, destacándose por su alta incidencia de ciberataques en comparación con otras partes del mundo.[2] De acuerdo con información recopilada por diversas firmas de ciberseguridad, esta región es blanco de una asombrosa cantidad de más de 1.600 ciberataques por segundo. Un dato particularmente revelador reside en el aumento de los ataques de distribución global de *ransomware*,[3] los cuales alcanzaron un

1. Lewis, James Andrew. Banco Interamericano de Desarrollo. Experiencias avanzadas en políticas y prácticas de ciberseguridad Panorama general de Estonia, Israel, República de Corea y Estados Unidos. 2016

2. Logicalis. Tres tendencias de ciberataques en 2023 y cómo prevenirlas. Cámara uruguaya de tecnologías de la información. 2023

3. El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de varias maneras, cifrando la información, bloqueando la pantalla, etc. El usuario es víctima de una extorsión, se le pide un rescate económico a cambio de recuperar el normal funcionamiento del dispositivo o sistema.Tomado de: Banco Santander. Glosario, ¿Qué es el ransomware? https://www.bancosantander.es/glosario/ransomware

La ciberseguridad constituye un área compleja que comprende diversos aspectos de gobernanza, políticos, operativos, técnicos y jurídicos.

impresionante total de 384.000 en los primeros seis meses de 2022, con América Latina representando el 14 % de dicho total.[4]

Esta cifra plantea interrogantes cruciales en cuanto a la relación entre el tamaño de las economías y su grado de digitalización, y la cantidad de ciberataques que enfrentan. Entre las naciones de la región, Brasil se encuentra en el primer puesto, sufriendo más de la mitad de estos ciberataques, seguido por México (23%), Colombia (8%) y Perú (6%). Estas preocupantes estadísticas arrojan luz sobre una situación que demanda una atención crítica y la implementación de estrategias efectivas de ciberseguridad.[5]

La ciberseguridad constituye un área compleja que comprende diversos aspectos de gobernanza, políticos, operativos, técnicos y jurídicos. En el contexto internacional empezaron a emerger las primeras definiciones a principios de 2011, cuando un grupo de trabajo ruso-estadounidense del EastWest Institute (EWI) y la Universidad de Moscú elaboró un marco de terminología internacional. Este grupo definió la ciberseguridad como una propiedad del ciberespacio, que debe tener la capacidad de resistir las amenazas intencionales y no intencionales, así como de responder y recuperarse de los ciberataques[6].

Sin embargo, esta no es la única definición de ciberseguridad, existen otras para este término a escala nacional e internacional. Uno de los referentes más citados es la Unión Internacional de Telecomunicaciones (ITU) que es el organismo especializado de Naciones Unidas para las tecnologías de la información y la comunicación (TIC), que se encarga de regular las telecomunicaciones a nivel internacional entre los Estados miembros y empresas operadoras. El instituto plantea lo siguiente sobre la ciberseguridad:

> **"se entiende como el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético"[7]**

La ciberseguridad se refiere generalmente a la capacidad de gestionar el acceso a redes, sistemas de información y diversos recursos de información. En esta situación, la efectividad de los controles de seguridad cibernética determina la confiabilidad, flexibilidad y seguridad del ciberespacio. En ausencia, insuficiencia o diseño deficiente de los controles de seguridad cibernética, el ciberespacio se percibe como un área desprotegida en donde los actores involucrados se enfrentan a ciberamenazas, entre las que se destacan: el fraude electrónico, el robo de la propiedad intelectual y de la información de identificación personal, la interrupción de los servicios y los daños o la destrucción de la propiedad.

4. Perspectivas de los Líderes de la Industria. Informe de ciberseguridad LATAM CISO 2023. Duke University. Center for Cybersecurity Policy and Law. Página 6

5. Perspectivas de los Líderes de la Industria. Informe de ciberseguridad LATAM CISO 2023. Duke University. Center for Cybersecurity Policy and Law. Página 6

6. Leiva E. 2015. Estrategias Nacionales de ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642.

7. Definición adaptada de https://www.bcmpedia.org/wiki/Cyber_Security. La Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). 2018. Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

En respuesta a esta dinámica, los líderes a nivel nacional han empezado a crear y diseñar estrategias de seguridad cibernética que apunten a mejorar y proteger la confidencialidad, integridad y disponibilidad de la infraestructura de las TIC. Para que ello proteja la implementación de los proyectos que amplían la conectividad a Internet, la seguridad nacional, el crecimiento económico, la oferta de servicios, el desarrollo de la innovación, la educación en línea, etc.

En este contexto, una de las formas de abordar la ciberseguridad es mediante leyes de sancionen conductas delictivas que transgreden directamente la seguridad en el ciberespacio y en la red; dentro de los cuales prevalecen el acceso ilícito a los medios informáticos, ataques a la integridad y conservación de los datos y de los sistemas, el acceso a los dispositivos tecnológicos, fraude informático sobre internet, pornografía infantil, entre otros. "Dada la naturaleza transfronteriza de las redes de información, se hace necesario un esfuerzo internacional concertado para hacer frente al uso impropio de estas" por lo que se crea el Convenio sobre la Ciberdelincuencia firmado el 23 de noviembre de 2001 en Budapest por los Estados miembros del Consejo de Europa y demás signatarios.[8]

El Convenio de Budapest[9] es un conjunto amplio de términos y definiciones relacionadas con delitos informáticos, que establece un marco penal común y estándares mínimos para procedimientos legales y recolección de pruebas. Abriendo el escenario de formar parte de una comunidad de cooperación global en ciberseguridad.[10] Siendo así, el objetivo de esta convención es "recurrir a la colaboración internacional entre países, de manera que se establezca que una conducta lesiva sea delito en cada jurisdicción. Así, no obstante, se mantengan y se respeten las legislaciones locales, los Estados deben definir delitos informáticos basados en un modelo común."[11]

Desde el impulso de este Convenio, se ha evidenciado la importancia de involucrar a todos los países en la protección cibernética. En América Latina, las iniciativas de ciberseguridad han surgido de la Organización de Estados Americanos (OEA). Desde principios del siglo, la Comisión de Seguridad Hemisférica (CSH) y el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (CITEL) reconocieron la urgencia de desarrollar estrategias contra las amenazas cibernéticas. Múltiples entidades, como la Reunión de Ministros de Justicia o Procuradores Generales de las Américas (REMJA) y el Comité Interamericano contra el Terrorismo (CICTE), resaltaron la cooperación y la legislación en delitos cibernéticos, considerándolos como amenazas emergentes.[12] Estos organismos acordaron la creación de una estrategia de seguridad cibernética para los Estados miembros, culminando en la aprobación de la "Estrategia Interamericana Integral de Seguridad Cibernética" por la Asamblea General en 2004.[13]

Esta estrategia se convirtió en un pilar para la OEA, abordando la protección de redes e Internet, la cooperación interamericana en ciberseguridad, y promoviendo la educación, estándares técnicos y leyes sin infringir derechos individuales. Desde entonces, el Programa de Seguridad Cibernética del CICTE ha trabajado para suplir la escasez de literatura sobre ciberseguridad en América Latina, generando informes colaborativos y detallados junto a líderes de la industria, proporcionando una visión exhaustiva de la situación de seguridad cibernética y delitos en la región.

8. Fratti, S. (junio de 2018). Panamá: Un país con la necesidad de una legislación sobre cibercrimen. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC), Derechos Digitales y Tecnología en América Latina. https://www.derechosdigitales.org/wp-content/uploads/minuta_ipandetec.pdf

9. Consejo de Europa. Convenio sobre Ciberdelincuencia (Convenio de Budapest). Disponible en: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{

10. Argote Guerrero, Carlos. De Budapest al Perú: Análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo. Derechos Digitales. Junio 2018. Página 4.

11. Temperini, Marcelo Gabriel Ignacio. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Universidad Nacional del Litoral. 2013. Página 3.

12. Concepción Anguita Olmedo y Mariano Bartolomé. El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea (UE) y La Organización De Estados Americanos (OEA). Comunicación Política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad. Madrid – 2021. SBN 978-84-1377-562-3. Página 639- 641.

13. Ibidem

En colaboración con el BID y el Centro Global de Seguridad Cibernética de la Universidad de Oxford, la OEA lanzó el Observatorio de Seguridad Cibernética en América Latina y el Caribe. Además, se ha desarrollado el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM)[14], un marco integral basado en cinco dimensiones, como políticas, cultura, educación, marco legal y tecnologías, consultando a 200 expertos internacionales. Este modelo se revisa periódicamente para mantenerlo actualizado y busca evaluar la madurez de las capacidades en seguridad cibernética en la región.[15]

La dimensión 4 del CMM, Marcos legales y regulatorios, se enfoca en la formulación y promulgación de legislación nacional relacionada con la ciberseguridad, tanto en su aspecto directo como indirecto. Presta atención particular en áreas clave, incluyendo los requisitos regulatorios relacionados con la ciberseguridad, la normativa referente a delitos cibernéticos y otras legislaciones pertinentes. Adicionalmente evalúa la capacidad para hacer cumplir tales leyes, se examina a través de la aplicación de la ley, el enjuiciamiento, los órganos reguladores y los tribunales.[16]

Problema

Dado que los delitos cibernéticos representan una creciente amenaza a nivel mundial, es crucial entender si los marcos legales de los países abordan adecuadamente aspectos clave de ciberseguridad.

En la región Latinoamericana se ha avanzado en la promulgación de leyes para abordar el cibercrimen, sin embargo, persiste la incertidumbre sobre si estas regulaciones reflejan enfoques como la protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables.

Además, el presente artículo busca cuantificar y comparar el grado de énfasis de cada país en estos enfoques a través de indicadores específicos, lo que permitirá una evaluación integral de la respuesta legal a los ciberdelitos en la región latinoamericana.
Esta alineación es crucial para garantizar una aplicación efectiva de la ley y abordar de manera adecuada las amenazas cibernéticas en la región.

Este artículo se enfoca en realizar un análisis comparativo de los marcos normativos de ciberdelincuencia de algunos países de América Latina, teniendo como referencia 7 delitos definidos en el Convenio de Budapest[17] a partir del cual se identifican los principales enfoques en la redacción de cada disposición o tipo penal que sanciona las conductas delictivas informáticas.

Uno de los objetivos de esta investigación es proporcionar una visión de los enfoques abordados en la legislación de 9 países latinoamericanos. Esto permitirá comprender si se requieren ajustes en las regulaciones para mejorar la eficacia en la lucha contra los ciberdelitos y proteger la seguridad nacional, financiera, la privacidad de las personas u ofrecer una mayor protección a poblaciones vulnerables de acuerdo a las necesidades de cada país en el ciberespacio.

14. También, Modelo de Madurez de Capacidad de ciberseguridad para las Naciones (CMM)

15. OEA. ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?. Banco Interamericano de Desarrollo; Organización de los Estados Americanos. Mar 2016. Página 53.

16. OEA. ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?. Banco Interamericano de Desarrollo; Organización de los Estados Americanos. Mar 2016. Página 57.

17. Council of Europe. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Disponible en: http://www.coe.int/t/dghl/standardsetting/tcy/ETS_185_spanish.PDF

Uno de los objetivos es proporcionar una visión de los enfoques abordados en la legislación de 9 países latinoamericanos.

Si bien, el abordaje de la ciberseguridad no se limita a un enfoque penal o punitivo, la decisión de abordar esta investigación centrándose exclusivamente en la legislación de ciberdelitos, está respaldada por varias razones metodológicas:

1. Enfoque Específico: La ciberseguridad es un campo multidisciplinario que abarca aspectos técnicos, legales, económicos y sociales. Limitar el alcance a la legislación de ciberdelitos permite un análisis más profundo y detallado de esta área específica. Se pueden examinar en detalle las disposiciones legales, e identificar posibles lagunas o inconsistencias. Esto proporciona una visión más completa y precisa de la situación actual.

2. Coherencia Temática: Al centrarse únicamente en la legislación de ciberdelitos, se mantiene la coherencia temática en el estudio. Esto facilita la recopilación de datos, el análisis y la presentación de resultados de una manera más precisa y estructurada. La investigación se enfoca en un aspecto específico y crucial de la ciberseguridad.

3. Métricas Objetivas: Al centrarse en la legislación de ciberdelitos, se pueden utilizar métricas objetivas y cuantitativas para evaluar la coherencia. Esto facilita la medición de los enfoques en las disposiciones legales.

4. Relevancia Práctica: La legislación de ciberdelitos es esencial para la lucha contra las amenazas cibernéticas y la protección de la sociedad. Un análisis académico riguroso de estas leyes es de gran relevancia práctica para legisladores, expertos en ciberseguridad y tomadores de decisiones. Proporciona información valiosa sobre la efectividad y coherencia de las regulaciones en un campo crítico.

En este contexto, esta investigación plantea las siguientes preguntas

- **¿Cómo tipifican y sancionan los países latinoamericanos los 7 delitos informáticos definidos en el Convenio de Budapest en sus respectivas legislaciones penales?**
- **¿En qué medida se reflejan en las legislaciones de los países latinoamericanos los enfoques de protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables en relación con los delitos informáticos?**
- **¿Existe una variación significativa en la atención dada a estos enfoques entre los países analizados?**

Objetivos de la Investigación

Los objetivos principales de esta investigación son los siguientes:

- Identificar las prioridades en los marcos normativos de ciberseguridad de estos países.
- Analizar la legislación de ciberdelincuencia o delitos informáticos en 9 países latinoamericanos.

- Determinar el grado de incorporación de enfoques de protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables en las legislaciones penales de los países analizados.
- Cuantificar y comparar el énfasis dado a cada enfoque en las legislaciones de los países latinoamericanos.

Metodología

Para llevar a cabo esta investigación, se utilizó una metodología que combina el análisis legal y dos índices que evalúan el énfasis de cada país en relación con 7 delitos. El proceso se dividió en varias etapas clave:

1. Selección de países latinoamericanos: Se seleccionaron 9 países latinoamericanos con variaciones en su desarrollo legislativo. Estos países se eligieron para representar una muestra diversa de la región. Los países escogidos se detallan a continuación por orden alfabético: Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, Paraguay, Perú, República Dominicana. Si bien se ha intentado analizar la mayor cantidad de los países de la región señalada, algunos de ellos han debido ser excluidos del estudio.[18]

2. Recopilación de legislación penal: Se realizó una recopilación de legislación penal de los países seleccionados, centrándose en las disposiciones relacionadas con delitos informáticos. Se identificaron y recopilaron todas las disposiciones relevantes que tipifican y sancionan los 7 delitos informáticos definidos en el Convenio de Budapest.

3. Análisis de la tipificación: Se procedió al análisis de las disposiciones legales de cada país con el fin de evaluar la manera en que tipifican los delitos informáticos. Para llevar a cabo esta comparación, se elaboró un cuadro que proporciona una visión equiparable de los 7 delitos escogidos del Convenio de Budapest y las normas de cada país analizado. Estos hallazgos se han condensado en el anexo 1 que complementa este informe.

4. Evaluación de enfoques: Cada disposición relacionada con delitos informáticos se evaluó según cuatro enfoques clave: protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables. Se asignó un valor numérico (1) a cada disposición para cuantificar el grado de incorporación de cada enfoque.

5. Desarrollo de indicadores cuantitativos: Se crearon dos índices cuantitativos que reflejan la intensidad de cada enfoque en la legislación penal de cada país. Se detallan en el capítulo del desarrollo.

6. Análisis comparativo: Se realizó un análisis comparativo de los indicadores cuantitativos para determinar las diferencias en la atención dada a los enfoques de seguridad nacional, protección financiera, privacidad y poblaciones vulnerables entre los países estudiados.

18. La exclusión de algunos países en esta investigación se basó principalmente en el enfoque de seleccionar aquellos que cuentan con una regulación específica sobre ciberdelitos. Los países escogidos han incorporado normativas especiales o han modificado sus códigos penales para abordar los delitos informáticos o ciberdelitos. Esta decisión se tomó con el objetivo de profundizar en el análisis de la legislación en torno a este tema particular, lo que permite una evaluación más precisa y detallada de las medidas legales adoptadas en relación con los delitos informáticos.

Para la recopilación de los datos, se emplearon las fuentes oficiales de publicación de normatividad en cada uno de los 9 países latinoamericanos[19], centrándose en las leyes que regulan específicamente los delitos informáticos o ciberdelitos, en el caso de que existan. Además, se ha examinado el contenido de los códigos penales vigentes, ya que, en varias instancias, incluso si no hay una legislación especializada, los delitos analizados pueden ser sancionados por las disposiciones penales convencionales. Se enfatiza que esta investigación se limita a abordar la legislación sustantiva y no abarca aspectos relacionados con el derecho procesal penal.

Como se indica, la investigación abarca 9 países, es importante destacar que Argentina y Brasil, presentan un sistema federal, razón por la cual se optó por analizar las leyes federales de estos países en lugar de abordar las legislaciones de sus estados individuales. Esto se llevó a cabo con el objetivo de establecer una base armonizada y un estándar común para el análisis de los otros siete países, que siguen un modelo unitario en su estructura legal.

3. Desarrollo

Como primer paso se llevó a cabo una revisión de los marcos legales de 9 países, tomando como referencia la dimensión 4 del CMM[20]. Este enfoque metodológico se fundamentó en la recopilación y examen de la normativa legal existente en cada nación. El objetivo fue analizar la adopción y avance de estas regulaciones, identificando las disposiciones existentes y aquellas ausentes en cada país.

Esto permitió determinar el grado de implementación y lagunas legales relacionadas con ciberseguridad, brindando una visión del panorama en la región. A continuación, se listan en las normativas y marcos jurídicos que se examinaron, tomando como fecha de corte 30 de julio de 2023:

- Seguridad de las TIC
- Marco jurídico sustantivo sobre ciberdelincuencia
- Marco jurídico procesal sobre ciberdelincuencia
- Protección de datos
- Protección infantil en línea
- Protección al Consumidor o Comercio electrónico
- Derechos humanos en línea
- Infraestructura Crítica (IC)
- Propiedad Intelectual
- Estándares técnicos

Al sistematizar los diversos tipos de normativas, se identificó que la mayoría de los países han promulgado marcos legales relacionados con la seguridad de las Tecnologías de la Información y Comunicación (TIC). Estas regulaciones se han establecido a través de leyes que fomentan el desarrollo y la adopción de las TIC, incluyendo la implementación de planes nacionales de tecnología, estrategias de ciberseguridad y ciberdefensa. El mismo

19. Argentina, Brasil, Colombia, Costa Rica, Chile, El Salvador, Perú, Paraguay, República Dominicana.

20. Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM)

comportamiento se identificó frente a la adopción de la legislación de protección de datos, protección al consumidor o comercio electrónico y propiedad intelectual.

Esta priorización puede deberse en gran medida a que los países latinoamericanos participan activamente en instancias internacionales y organizaciones relacionadas con temas de comercio y tecnología. Así como la adhesión a tratados bilaterales y la participación en organismos multinacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), Asociación Latinoamericana de Integración (ALADI), el Sistema Económico Latinoamericano y del Caribe (SELA), entre otros. En el ámbito de la propiedad intelectual, la mayoría de los países de la región se han adherido a convenios de la Organización Mundial de la Propiedad Intelectual (OMPI), logrando avances notables. También se han registrado progresos en transacciones electrónicas, firmas electrónicas y su autenticación. Algunos ejemplos notables son las regulaciones de México, Colombia y Guatemala, que incorporaron las leyes modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre comercio y firma electrónica.[21]

En cuanto a la tendencia regulatoria que busca fortalecer medidas legales, tecnológicas y de control para garantizar un tratamiento seguro de datos personales. La Red Iberoamericana de Protección de Datos Personales, con la participación de varios países, influye positivamente en la legislación. Chile y México son influenciados por la OCDE y Cooperación Económica Asia-Pacífico (APEC) en sus políticas y legislación de protección de datos.[22]

En lo relativo a los ciberdelitos, los nueve[23] países han implementado leyes o reformas específicas para abordar esta problemática. Por lo tanto, la investigación se enfocó en examinar disposiciones legales específicas y reformas que abordan estos delitos, así como su inclusión en los códigos penales vigentes. Esta evaluación permitió identificar la presencia o ausencia de tipificación de los delitos escogidos en las leyes especializadas y observar que algunos son sancionados como delitos convencionales en el código penal. Se optó por centrar el análisis en los siguientes artículos de la Convención de Cibercriminalidad de Budapest, las definiciones proporcionadas se fundamentaron en el informe explicativo del Consejo de Europa:[24]

Art. 2.

Acceso ilícito: abarca intrusiones no autorizadas en sistemas informáticos. Incluye acciones como piratería, sabotaje o intrusión en un ordenador, perturbando el uso legítimo de datos y sistemas. Estas incursiones pueden posibilitar el acceso a información confidencial, contraseñas o secretos sin autorización, propiciando delitos informáticos adicionales. Se considera ilegítimo el acceso a sistemas no autorizados, a menos que sea de acceso público o se cuente con el permiso del propietario.

Art. 3.

Interceptación ilícita: busca salvaguardar la privacidad en las comunicaciones de datos, equiparando la intrusión a las escuchas telefónicas. Este delito incluye la monitorización o acceso no autorizado a comunicaciones electrónicas, ya sea mediante dispositivos o técnicas, involucrando la grabación o acceso a datos transmitidos. La ley aplica a comunicaciones no públicas, protegiendo transmisiones

21. Navarro Isla, Jorge. Ciberlegislación en América Latina. CEPAL. Newsletter eLAC no 15 junio 2011. Página 2.

22. Navarro Isla, Jorge. Ciberlegislación en América Latina. CEPAL. Newsletter eLAC no 15 junio 2011. Página 3.

23. Argentina, Brasil, Colombia, Costa Rica, Chile,, El Salvador, Paraguay, Perú y República Dominicana

24. Consejo de Europa. Convenio sobre la ciberdelincuencia (STE número 185) Informe explicativo.

confidenciales, incluso las realizadas por empleados en el ámbito comercial. Para ser penalizada, la interceptación debe ser deliberada y no legítima, aunque ciertas prácticas comerciales como el uso de cookies no son consideradas ilegales.

Art. 4.

Ataques a la integridad de los datos: busca proteger la integridad y el funcionamiento correcto de datos y programas informáticos. Incluye actos como dañar, deteriorar, borrar, suprimir o alterar información, abarcando la introducción de códigos maliciosos como virus y caballos de Troya. Estas acciones son penalizadas si se realizan ilegítimamente, excluyendo modificaciones autorizadas por los propietarios o actividades comunes para la seguridad de sistemas informáticos.
Art. 5. Interferencia en el sistema: se define como la interferencia deliberada en el funcionamiento legítimo de sistemas informáticos, incluyendo las telecomunicaciones, a través de la manipulación de datos. Protege los intereses de operadores y usuarios. La obstrucción puede incluir daño, alteración, supresión o transmisión de datos y debe ser grave para ser penalizada, con criterios definidos por cada parte. Se excluyen actividades legítimas como verificaciones de seguridad. El envío masivo de correos no solicitados puede considerarse delito si obstruye gravemente las comunicaciones.

Art. 6

Abuso de los dispositivos: establece como delito la manipulación deliberada de dispositivos o datos de acceso con el propósito de cometer delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Se penaliza la producción, venta, importación, distribución u oferta de dispositivos o programas diseñados para tales delitos. La posesión de contraseñas o datos de acceso también constituye un delito. Excluye herramientas legítimas para verificar o proteger sistemas informáticos.

Art 7.

Falsificación informática: este delito es equiparable a la falsificación de documentos físicos. Se busca cerrar brechas legales, especialmente respecto a la manipulación de datos con valor legal. Penaliza la creación o alteración ilegítima de datos para influir en transacciones legales, basadas en la autenticidad de la información. Protege la seguridad y fiabilidad de datos electrónicos, relevantes en asuntos legales. Abarca datos equivalentes a documentos legales, castigando la introducción no autorizada de datos. Además, el término “autenticidad” se amplía para incluir la autenticidad genuina de los datos.

Art. 8.

Fraude informático: se refiere a manipulaciones indebidas en la manipulación de datos con la intención de realizar transferencias ilegales de bienes. Penaliza la alteración, eliminación, o interferencia con sistemas o datos, causando pérdidas económicas directas a terceros. Este delito involucra obtener beneficios económicos ilegítimos deliberadamente. Excluye prácticas comerciales legítimas como la recopilación de información para comparar precios, siempre y cuando no busquen un beneficio fraudulento o dañino, requiriendo la intención tanto para la manipulación como para el beneficio económico.

Se decidió excluir de este análisis, el articulo 9 relativo a la sanción de la pornografía infantil, debido a que no se percibió la necesidad de incorporar los cuatro enfoques propuestos en este estudio a la hora de su inclusión en las legislaciones. El delito vinculado a la pornografía infantil se enfoca en una población específica, y no resulta fundamental que se integren enfoques de seguridad nacional, protección de la privacidad o financiera de manera explícita en su redacción. Su propósito principal radica en fortalecer las medidas de protección de menores, incluida su salvaguardia contra la explotación sexual, a través de la modernización de las disposiciones del derecho penal para restringir más eficazmente la utilización de sistemas informáticos en la comisión de delitos de naturaleza sexual contra menores.

Asimismo, no se incluyó el artículo 10 relacionado con infracciones de la propiedad intelectual y de los derechos afines, debido a su enfoque particular y a la ausencia de la necesidad de integrar los cuatro enfoques en su redacción.

De acuerdo a lo mencionado, para este estudio se consideró importante que los países, al incorporar delitos informáticos en su legislación, contemplaran la necesidad de agravar o incluir enfoques que abordan la protección de la seguridad nacional, la protección económica y financiera, la privacidad y los datos personales, así como la protección de poblaciones vulnerables.

En primer lugar, el enfoque de seguridad nacional debe ser considerado debido a la creciente interdependencia de sistemas críticos en un mundo digitalizado. “Las infraestructuras críticas abarcan una gran variedad de aspectos funcionales del Estado, tales como plantas eléctricas, sistemas industriales y de salud, telecomunicaciones, tránsito terrestre, aéreo y marítimo, y el sistema económico y financiero. No obstante, a medida que se vuelven más vulnerables a los ataques de ransomware, su protección se inicia con el diseño de políticas e implementación de estrategias de ciberseguridad para la protección del país.”[25] Por lo que es esencial contar con disposiciones legales que disuaden a las ciberdelincuentes y sancionen estos ataques.

El enfoque de protección económica y financiera es igualmente relevante, ya que los delitos informáticos pueden tener un impacto significativo en la estabilidad financiera y la confianza en las transacciones electrónicas. La inclusión de enfoques para proteger sistemas bancarios, datos de clientes y propiedad intelectual es esencial para mantener la integridad económica. Asimismo, es necesario integrar en este panorama a los activos digitales “teniendo en cuenta las características que hacen referencia a las propias criptomonedas, pero también las que tienen que ver con la seguridad del mundo digital. Si no se definen las cuestiones de ciberseguridad asociadas a este tipo de moneda digital, su crecimiento, evolución y adaptación serán afectados, a pesar de ser una tendencia en auge con fuerte arraigo en sectores de alto valor financiero y económico.”[26]

La privacidad y los datos personales son cada vez más vulnerables en el mundo digital, por lo que el enfoque en la protección de la privacidad y los datos personales es crucial. Los individuos deben confiar en que su información personal está segura en línea, y las legislaciones deben garantizar que quienes infrinjan esta confianza enfrenten

25. Saavedra, Boris. ciberseguridad en América Latina: retos, preocupaciones y oportunidades. Desafíos y amenazas a la seguridad en América Latina. Primera edición digital, noviembre 2022 Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2022-11055 ISBN: 978-612-47954-4-2. Disponible en www.ceeep.mil.pe. Página. 195.

consecuencias legales. Por lo tanto, para tener un abordaje de ciberseguridad integral es primordial que se "respeten los valores fundamentales, dentro de los cuales incluyen la privacidad, la libertad de expresión y el libre flujo de información."[27]

Finalmente, el enfoque en la protección de poblaciones vulnerables se basa en un compromiso con la equidad y la justicia. Se entiende que la vulnerabilidad de la víctima aumenta el impacto del delito. Esto se debe a que estas poblaciones suelen tener menos recursos para defenderse de los ataques informáticos y a que los delitos informáticos pueden ser utilizados para explotar su vulnerabilidad. En este sentido se considera, que el agravante o la inclusión de un delito informático que protege poblaciones vulnerables es una medida necesaria para disuadir a los delincuentes de atacar a estas personas y para protegerlas de los ataques informáticos. Además, "cabe destacar que un aspecto importante sobre el primer protocolo adicional del Convenio de Budapest es el intento de establecer una dinámica equilibrada entre la libertad de expresión de los usuarios de Internet y una lucha eficaz contra la difusión y la práctica del racismo y la xenofobia en el ámbito digital."[28]

En general, la inclusión de estos enfoques en la legislación de delitos informáticos refleja la necesidad de adaptarse al entorno digital actual y proteger los intereses de la sociedad en su conjunto.

Cuadro explicativo de los Cuatro Enfoques en Delitos Informáticos

Enfoque	Descripción	Ejemplos
Seguridad nacional	Protección de infraestructuras críticas y sistemas estatales de información.	Ataques a sistemas de defensa, telecomunicaciones, energía, etc.
Protección económica y financiera	Enfocado en salvaguardar sistemas bancarios, económicos y activos digitales.	Robo de datos bancarios, manipulación de datos financieros, alteración fraudulenta de datos económicos.
Privacidad y datos personales	Protección de la información personal y privada almacenada en sistemas informáticos.	Acceso no autorizado a datos privados, violaciones de la privacidad y explotación de información personal.
Protección de poblaciones vulnerables	Dirigido a prevenir delitos informáticos que afectan a grupos vulnerables.	Delitos que explotan la vulnerabilidad de ciertos grupos, como estafas dirigidas a personas de la tercera edad o menores.

Fuente: elaboración propia

26. Saavedra, Boris. ciberseguridad en América latina: retos, preocupaciones y oportunidades. Desafíos y amenazas a la seguridad en América Latina. Primera edición digital, noviembre 2022 Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2022-11055 ISBN: 978-612-47954-4-2. Disponible en www.ceeep.mil.pe. Página. 213.

27. ADC - Cyber Stewards Network. ciberseguridad en la era de la vigilancia masiva. Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina. 2016. Página 15.

28. Martins dos Santos, Buna. Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. Derechos Digitales. Mayo 2022. Página 17.

Como se puede observar los enfoques delictivos propuestos comprenden cuatro áreas específicas: seguridad nacional, protección económica y financiera, privacidad y datos personales, y protección de poblaciones vulnerables. Para cuantificar y valorar su presencia, se utilizan dos índices. El Índice de Enfoque Delictivo (IED), el cual evalúa la presencia de cada uno de estos enfoques en el delito. Por otro lado, el Índice de Penetración Delictiva por Enfoque (IPDE) determina la prevalencia de estos enfoques dentro de los delitos analizados por país. Se presentan a continuación los índices detallados:

- Índice de Enfoque Delictivo (IED)

El IEDP es un indicador que evalúa la presencia de enfoques específicos en la naturaleza delictiva. Se basa en la ponderación de valores asignados a cada disposición, reflejando la importancia relativa de cada enfoque en la evaluación de un delito. Se consideran cuatro enfoques delictivos, a los cuales se les asigna un valor de 1 si el delito posee ese enfoque, y 0 si no lo tiene. La fórmula para calcular el IEDP es:

$$IEDP=(ResultadoEnfoque1+ResultadoEnfoque2+ResultadoEnfoque3+ResultadoEnfoque4)\times 100\ 4$$

La fórmula pondera la presencia de cada enfoque y genera un valor porcentual que refleja el grado de integridad de los enfoques delictivos evaluados basado en la combinación de los mismos.

- Índice de Penetración Delictiva por Enfoque (IPDE)

El IPDE es un indicador diseñado para medir la prevalencia de enfoques delictivos en delitos específicos en diferentes países. Este índice se basa en determinar si un país tiene o no un enfoque particular entre un conjunto de siete delitos, asignando un valor de 1 si el delito cuenta con el enfoque y 0 si no lo tiene. La fórmula para calcular el IPDE es:

$$IPDE=(ResultadoDelito1+ResultadoDelito2+...+ResultadoDelito7)\times 100\ 7$$

El cálculo se realiza sumando los resultados de la columna del enfoque específico de los siete delitos y generando un valor porcentual que refleja la presencia de dicho enfoque en la tipología delictiva de cada país

4. Hallazgos

A través de la revisión de la legislación y el análisis de los datos cuantitativos, se destaca en primera instancia la marcada diversidad y heterogeneidad de abordajes legales empleados para abordar los delitos informáticos en los nueve países estudiados.

El compendio detallado de la equiparación de los delitos extraídos del Convenio de Budapest y la contextualización de las disposiciones legales de cada país se ha consolidado en el Anexo 1. Dentro de esta tabla comparativa se detallan elementos esenciales como el nombre del delito, su descripción, la sanción prevista.

En lo concerniente a las particularidades de cada país, se constata que en Argentina, la penalización del acceso ilícito y abuso de dispositivos, vinculan la protección de la seguridad nacional con la prevención de la intrusión en sistemas críticos del Estado y la salvaguardia de registros esenciales. Además, la protección a la privacidad se encuentra delineada a través de disposiciones específicas que sancionan la revelación de datos personales, siendo el enfoque más presente en 6 de los 7 delitos. En Brasil, las leyes abordan los delitos informáticos con énfasis en la protección de la seguridad financiera y la privacidad, incluyendo agravantes penales para delitos cometidos contra figuras importantes, en el delito de fraude informático consagra el enfoque de protección a poblaciones vulnerables al incorporar un agravante si el delito se comete contra personas mayores o vulnerables.

En Colombia, la Ley 1273, referente a delitos informáticos, aborda principalmente enfoques de protección a la seguridad ciudadana, seguridad nacional y aspectos financieros. A través del artículo 269H, se establecen circunstancias agravantes que reflejan la importancia de resguardar la integridad del Estado y prevenir actos con fines terroristas, relacionados con la protección de la seguridad nacional. Además, se contemplan sanciones específicas para quienes obtengan provecho económico a través de la comisión de estos delitos, reflejando un enfoque financiero.

En el caso de Costa Rica, la legislación se orienta a la protección de la privacidad, y la seguridad financiera. Por ejemplo, el artículo 196 del Código Penal se enfoca en la violación de la correspondencia o comunicaciones, sancionando la divulgación no autorizada de comunicaciones privadas. También se abordan temas financieros en relación con la obtención de ganancias ilícitas a través de conductas ilegales. Y el delito 196 bis incorpora la protección de poblaciones vulnerables al sancionar con una pena mayor si la información vulnerada corresponde a un menor de edad o incapaz. Así mismo, si las conductas afectan datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

Ahora bien, la actualización de la legislación chilena en materia de delitos informáticos, a través de la ley número 21.459, ha representado un cambio sustancial en su marco normativo, revocando la previa ley N° 19.223. Esta actualización se llevó a cabo con la

intención de adaptar la legislación a los estándares establecidos en el Convenio de Budapest. Dicha modificación es de suma importancia, ya que, de forma análoga a lo implementado en Colombia, Chile ha incorporado dos circunstancias agravantes en el artículo 10[29] de la ley 21.459, aplicables a todos los delitos informáticos.

Este paso denota una estrategia legal con énfasis en la consideración de agravantes para casos de delitos informáticos en el país. Además, esta actualización ha permitido alinear sus disposiciones con estándares internacionales y enfocarse en la protección y seguridad en línea. Sin embargo, a pesar de la inclusión de aspectos relacionados con la seguridad nacional, protección de poblaciones vulnerables y la consideración de agravantes generales, la redacción de los artículos de la legislación no enfatiza explícitamente la protección de la privacidad, excepto en el caso específico del delito de interceptación ilícita.

Mientras Colombia se enfoca en la protección de la seguridad nacional y financiera, Costa Rica pone énfasis en la privacidad y la seguridad financiera. Chile por su parte. amplía su alcance legislativo e incorporó de manera completa tres enfoques, por lo que destaca en la región.

Otro comportamiento presenta El Salvador, mediante la ley especial contra delitos informáticos (Decreto Legislativo No. 260) incorpora artículos que se enfocan en la protección de la privacidad, penalizando la utilización, modificación o transferencia de datos personales y confidenciales, pero sin descuidar los enfoques financiero y de seguridad nacional, al sancionar conductas ilícitas en contra de sistemas públicos, servicios financieros y sistemas de transacciones en criptomonedas.

En el contexto de la legislación paraguaya se observa una marcada ausencia de enfoques específicos en las disposiciones legales. Únicamente se identificaron dos disposiciones que dentro de su contenido incorporarán el enfoque de protección a la privacidad. De manera similar, el enfoque financiero solo se vislumbra en dos conductas. Además, en lo que respecta a la seguridad nacional, solamente un delito aborda esta perspectiva, y no se encuentran disposiciones relacionadas con la protección de poblaciones vulnerables.

Este escenario resalta que, a pesar de que Paraguay cuenta con la tipificación de todos los delitos informáticos analizados, los enfoques específicos no están explícitamente integrados en la redacción de sus disposiciones penales. Esta carencia de enfoques integrados en su legislación hace que Paraguay se posicione como el país con menos enfoques en su marco normativo en comparación con los nueve países analizados en esta investigación.

Perú, por su parte, se centra en la protección de la seguridad nacional y la privacidad. El análisis revela que el artículo 11[30] introduce agravantes relacionados con la seguridad nacional y la privacidad en la tipificación de seis delitos analizados. Sin embargo, se observa una falta de énfasis o disposiciones legales explícitas relacionadas con la protección financiera y la protección de poblaciones vulnerables.

Dentro del marco normativo de República Dominicana se evidencia un conjunto mayor a 30 disposiciones que abordan específicamente delitos informáticos. No obstante, a pesar de la presencia de disposiciones que tocan tres de los enfoques, con excepción del

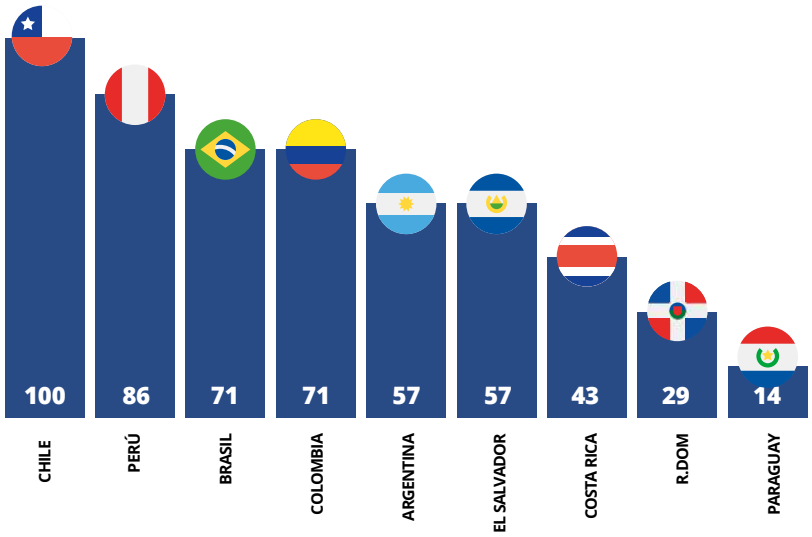
29. Artículo 10. Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley: 1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función. 2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores. Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiera la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley No 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

30. Artículo 11.- Agravantes El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando: 1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales

referente a la protección de la población vulnerable, ninguno de estos enfoques prevalece significativamente por encima de los demás.

Expuesto lo anterior, a continuación se ilustran los resultados de los datos analizados. En términos del enfoque de protección de la seguridad nacional, la investigación arrojó que Chile cuenta con un enfoque absoluto (100%) seguido por Perú y Colombia con un alto porcentaje (85,71% y 71,43% respectivamente).

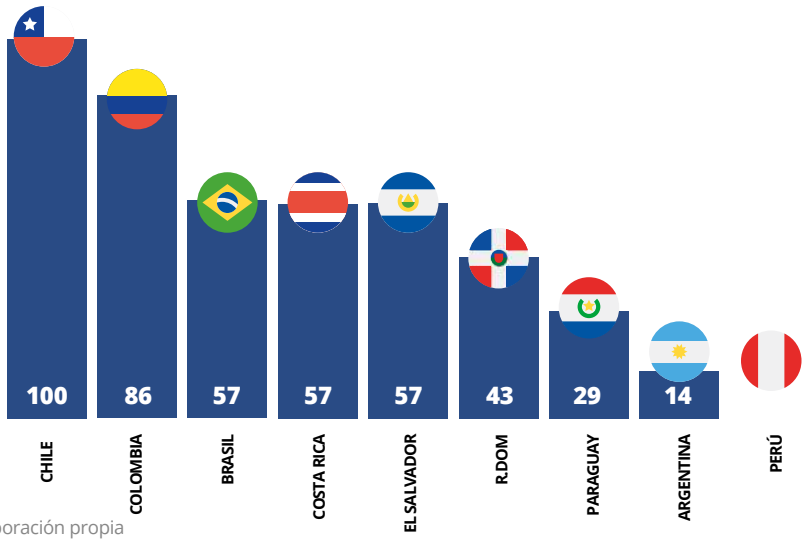
Figura 01
Enfoque de protección de seguridad nacional



Fuente: elaboración propia

En cuanto a la protección financiera, Chile y Colombia lideran con un enfoque total (100% y 85,71% respectivamente), seguidos por Costa Rica y El Salvador con porcentajes significativos (57,14% y 57,14% respectivamente).

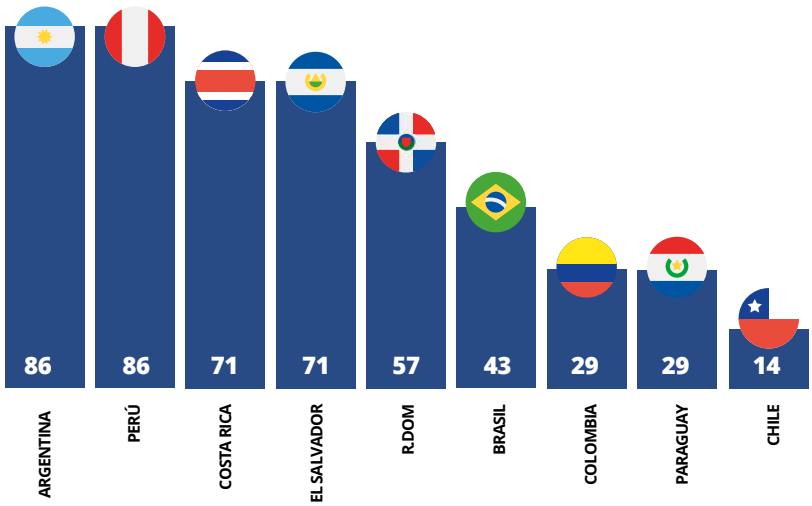
Figura 02
Enfoque de protección Financiera



Fuente: elaboración propia

La protección a la privacidad es un punto fuerte para la mayoría de los países, donde Argentina y Perú tienen un alto porcentaje (85,71% cada uno), seguidos por Chile y Costa Rica (71,43% y 57,14% respectivamente).

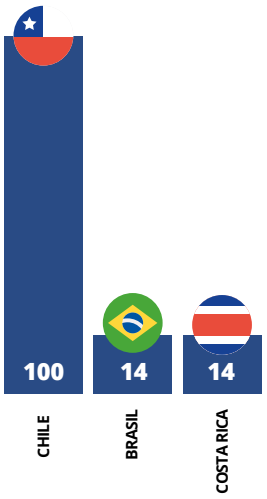
Figura 03
Enfoque de protección a la privacidad



Fuente: elaboración propia

El enfoque de protección de poblaciones vulnerables es el menos adoptado por los países analizados. Sin embargo, Chile lidera con un 100%, seguido por Brasil y Costa Rica (14,29% cada uno).

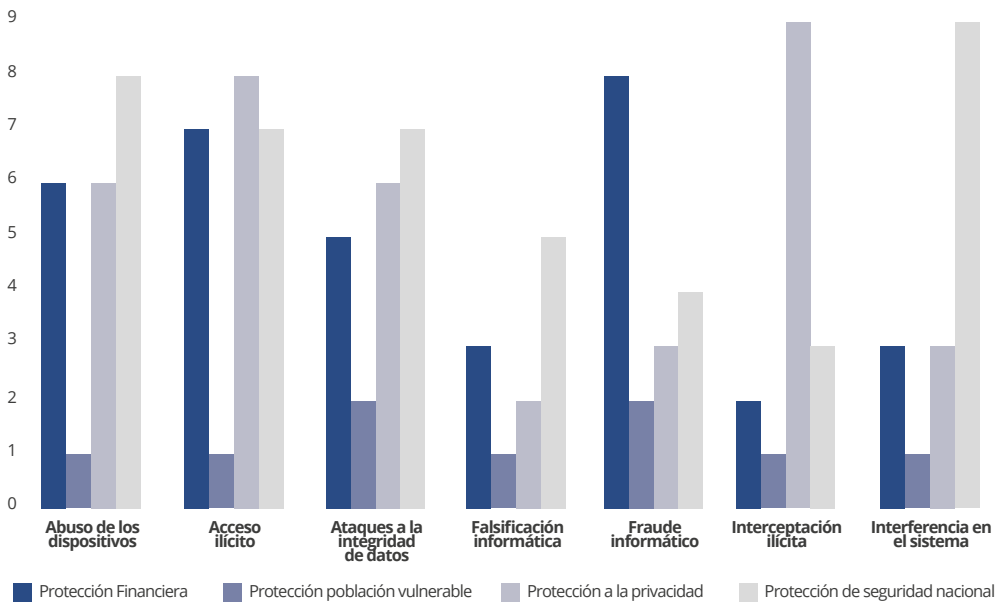
Figura 04
Enfoque protección población vulnerable



Fuente: elaboración propia

El análisis de los datos revela patrones significativos en los enfoques adoptados por países en relación con la protección frente a delitos informáticos. Se observa que, en general, los países tienen un enfoque más fuerte en la protección de la seguridad nacional y la privacidad en comparación con la protección financiera y la seguridad de poblaciones vulnerables. Se evidencia una atención más equilibrada en la protección a la privacidad y la seguridad de los sistemas nacionales, reflejada en las altas puntuaciones en "Acceso ilícito", "Ataques a la integridad de los datos" e "Interferencia en el sistema". Sin embargo, hay una marcada debilidad en la protección de la población vulnerable, lo que puede representar una brecha en la salvaguarda de los grupos más susceptibles.

Este patrón se hace más evidente en delitos como "Fraude informático" y "Falsificación informática", donde la protección de la población vulnerable es mínima en comparación con la seguridad nacional y la privacidad. La "Interceptación ilícita" destaca como un delito con un enfoque significativamente alto en la protección de la privacidad, lo que refuerza la importancia que se le otorga a resguardar la confidencialidad de las comunicaciones. Además, la "Interferencia en el sistema" muestra un énfasis considerable en la protección de la seguridad nacional, lo que refleja una preocupación por la defensa de los sistemas críticos del Estado.



Fuente: elaboración propia

5. Conclusiones

Las conclusiones extraídas de esta investigación reflejan la amplia heterogeneidad en los enfoques legislativos adoptados por los países latinoamericanos en respuesta a los delitos informáticos. Los resultados cuantitativos arrojan una diversidad marcada en cuanto a la incorporación de los enfoques de protección de seguridad nacional, protección financiera, protección a la privacidad y protección de poblaciones vulnerables en las legislaciones penales analizadas. Si bien hay similitudes generales en la presencia de estos enfoques, se evidencia una variación significativa en la atención otorgada a cada uno de ellos en los nueve países objeto de estudio.

Además, el análisis cuantitativo muestra que las diferencias en la atención a estos enfoques no son aleatorias sino que parecen estar condicionadas por factores socioeconómicos, culturales y políticos. Por ejemplo, países como Argentina y Brasil, con un mayor énfasis en la seguridad nacional, pueden reflejar una preocupación particular por la protección de sistemas críticos y registros gubernamentales. Por otro lado, Costa Rica orienta su enfoque hacia la protección de la privacidad y poblaciones vulnerables, lo que podría sugerir una prioridad hacia la salvaguarda de la intimidad y el bienestar de sus ciudadanos en el ámbito digital.

La necesidad de armonización legal y estrategias comunes para abordar delitos informáticos transnacionales es clara a partir de estas conclusiones. La variabilidad en los enfoques denota la importancia de una convergencia de estrategias legales y técnicas para abordar de manera efectiva los retos emergentes en ciberseguridad. Estos hallazgos cuantitativos resaltan la importancia de considerar, tanto para fines legislativos como para prácticas de cooperación regional, los factores que condicionan la priorización de los enfoques, y sugieren que la evolución futura de estas leyes debería considerar la variedad de enfoques para garantizar una protección sólida y completa en el ámbito de la ciberseguridad en la región latinoamericana.

6. Bibliografía

- ADC - Cyber Stewards Network. ciberseguridad en la era de la vigilancia masiva. Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina. 2016.

- Argote Guerrero, Carlos. De Budapest al Perú: Análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo. Derechos Digitales. Junio 2018.

- Arreola García, Adolfo. Desafíos a las estrategias de ciberseguridad en América. Revista del Centro de Estudios Superiores Navales. Octubre-Diciembre de 2019. Volumen 40. ISSN: 1870- 5480

- Aguilar-Antonio, Juan Manuel. Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. Revista Legislativa de Estudios Sociales y de Opinión Pública. VOL. 13 NÚM. 29 Septiembre- Diciembre de 2020.

- Bechara, Y., Mosquera, A. y Ledezma, E. (2020). Análisis Jurídico de la Ley 1273 del 2009 y el Surgimiento y Expansión del Delito de Hurto y Semejantes por Medios Informáticos [tesis de licenciatura, Facultad de Derecho de la Universidad Cooperativa de Colombia]. Repositorio UCC. Recuperado de https://repository.ucc.edu.co/ bitstream/20.500.12494/19788/3/2020_analisis_delit os_informaticos.pdf

- OEA. ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?. Banco Interamericano de Desarrollo; Organización de los Estados Americanos. Mar 2016

- Congressional Research Service (2020), "Defense Primer: Cyberspace Operations", recuperado de https: / / fas.org/ sgp/ crs/ natsec/ I F10537.pdf (consultado el 09/ 08/ 2020)

- Concepción Anguita Olmedo y Mariano Bartolomé. El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea (UE) y La Organización De Estados Americanos (OEA). Comunicación Política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad. Madrid – 2021. SBN 978-84-1377-562-3.

- Council of Europe. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Disponible en: http://www.coe.int/t/dghl/standardsetting/tcy/ ETS_185_spanish.PDF

- Consejo de Europa. Convenio sobre la ciberdelincuencia (STE número 185) Informe explicativo. Disponible en: https://rm.coe.int/16802fa403

- Danya Centeno. México y el Convenio de Budapest: Posibles incompatibilidades. Derechos Digitales y Red en Defensa de los Derechos Digitales (R3D) 2018

- Diario Oficial de la Federación (01 de junio de 2021). Decreto. Por el cual se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal. Recuperado de https://www.dof.gob.mx/nota_ detalle.php?codigo=5619905&fecha=01/06/2021

- Fratti, S. (junio de 2018). Panamá: Un país con la necesidad de una legislación sobre cibercrimen. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC), Derechos Digitales y Tecnología en América Latina. https://www.derechosdigitales.org/wp-content/uploads/minuta_ipandetec.pdf

- Global action on Cybercimre Extended. Reporte Comparativo Misión Consultiva y Taller de Trabajo sobre ciberdelito y prueba electrónica y la implementación del Convenio de Budapest en los países que forman parte del FORPEL Reporte Final Preparado bajo el Proyecto GLACY+. 2019. Página 6. Disponible en: https://foprel.digital/wp-content/uploads/2022/04/07-REPORTE-CIBERDELITO- GLACY.pdf

- Leiva E. 2015. Estrategias Nacionales de ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642

- Lewis, James Andrew. Banco Interamericano de Desarrollo. Experiencias avanzadas en políticas y prácticas de ciberseguridad Panorama general de Estonia, Israel, República de Corea y Estados Unidos. 2016 Disponible en: https:// publications.iadb.org/handle/11319/7449?locale-attribute=es&.

- Logicalis. Tres tendencias de ciberataques en 2023 y cómo prevenirlas. Cámara uruguaya de tecnologías de la información. 2023

- Martins dos Santos, Buna. Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. Derechos Digitales. Mayo 2022. Página 17.

- Navarro Isla, Jorge. Ciberlegislación en América Latina. CEPAL. Newsletter eLAC no 15 junio 2011.

- Organización de Estado Americanos. La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. OEA/Ser.D/XXV.25, pág. 51. Disponible en:https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

- Peker, Luciana. El Congreso aprobó la Ley Olimpia contra la violencia digital. Octubre 2023. Disponible en: https://www.infobae.com/sociedad/2023/10/11/el-congreso-aprobo-la-ley-olimpia-contra-la-violencia- digital/#:~:text=La%20Ley%20Olimpia%20incluye%20a,su%20permiso%20es%20vi olencia%20digital

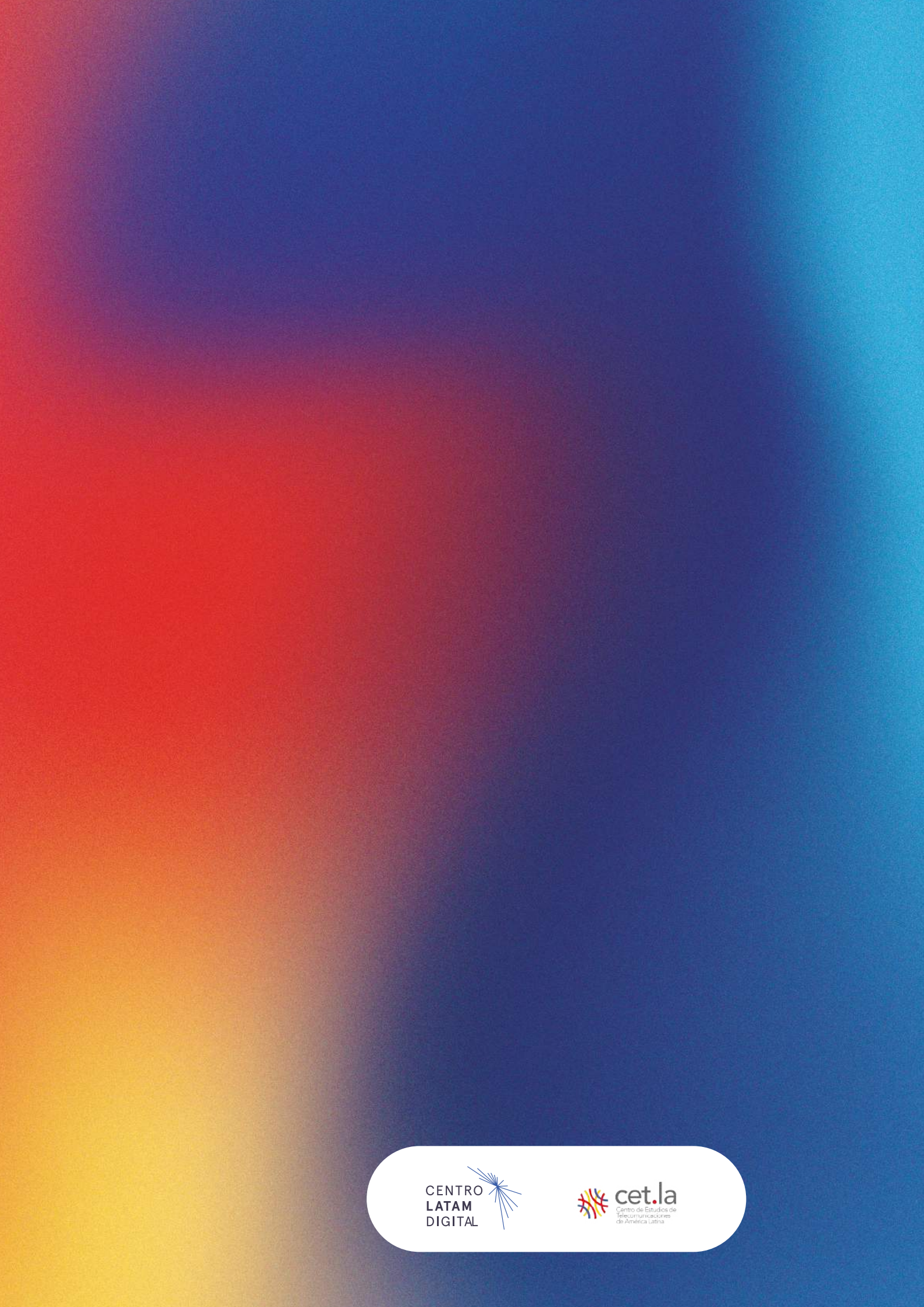
- Perspectivas de los Líderes de la Industria. Informe de ciberseguridad LATAM CISO 2023. Duke University. Center for Cybersecurity Policy and Law.

- Rodolfo Rafael Elizalde Castañeda, Héctor Hugo Flores Ramírez y Edwin Misael Castro Lorzo. Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado. Ius Comitiãlis. Universidad Autónoma del Estado de México, México. ISSN: 2594-1356. 2021. Disponible en URL: http://portal.amelica.org/ameli/journal/137/1372935014

- Saavedra, Boris. ciberseguridad en América latina: retos, preocupaciones y oportunidades. Desafíos y amenazas a la seguridad en América Latina. Primera edición digital, noviembre 2022 Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2022-11055 ISBN: 978-612-47954-4-2. Disponible en www.ceeep.mil.pe

- Sebastián Bortnik. Presidente de Argentina Cibersegura. Ley 26.904 sancionada el 13 de noviembre de 2013. Disponible en: https://www.argentinacibersegura.org/noalgrooming/ley-de-grooming

- Temperini, Marcelo Gabriel Ignacio. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Universidad Nacional del Litoral. 2013.


CENTRO
LATAM
DIGITAL
cet.la
Centro de Estudios de Telecomunicaciones de América Latina