UNIVERSIDAD SIGLO 21

TRABAJO FINAL DE GRADO. MANUSCRITO CIENTÍFICO

CARRERA: Abogacía

ANÁLISIS DE LA LEY DE DELITOS INFORMÁTICOS DE ARGENTINA - IMPACTO SOBRE LAS PERSONAS Y EMPRESAS

Tema: Grupos Vulnerables

Autor: Juan Edgardo Meza

Legajo N°: VABG101558

Tutor: Claudio Marcelo Suarez Barrera

Rawson, Chubut, República Argentina. Junio 2024

Índice

Agradecimientos

Agradecer es mirar atrás, recorrer nuevamente el camino andado, observar desde la distancia y sentir que cada una de las personas aquí mencionadas fue esencial para que este trabajo se concretara. Agradecer es una necesidad del alma, porque sabemos que juntos podemos llegar mejor, más lejos, aprender de la visión del otro y, además, disfrutar del camino.

Por ello, quiero expresar mi más profundo agradecimiento a:

A mis padres Juan y María por ser mis pilares a lo largo de todo ese proceso, por su sacrificio y por su apoyo incondicional, al igual que mis hermanos y hermanas.

A mi esposa Natalia y a mi hija Camila, quienes me acompañaron en todo este trayecto universitario y son el sostén de esta carrera que tanto me apasiona.

A mis amigos y familiares por la dedicación y apoyo continuo a la distancia.

Un especial agradecimiento a la Universidad Siglo 21, a mis profesores y tutor de TFG que me guiaron en esta elaboración.

Resumen

El desarrollo exponencial de las Tecnologías de la Información y la Comunicación (TICs) ha facilitado la vida diaria pero también ha sido aprovechado por ciberdelincuentes para cometer diversos delitos ciber-asistidos. En respuesta, Argentina promulgó la Ley Nº 26.388 en 2008, con el objetivo de regular delitos como la piratería informática, el fraude electrónico y el material de abuso sexual infantil en línea. Esta legislación se basa en la protección de la integridad, confidencialidad y disponibilidad de la información y fomenta la cooperación internacional, apoyándose en instrumentos como el Convenio de Budapest.

El estudio también destaca la importancia de adaptar la legislación de manera proactiva para abordar las nuevas realidades tecnológicas y mejorar la cooperación internacional. Se subraya la necesidad de actualizar continuamente la Ley de Delitos Informáticos y de implementar tecnologías avanzadas de ciberseguridad para proteger a los ciudadanos y las instituciones contra las amenazas del ciberespacio en constante evolución.

Palabras clave:

Delitos informáticos, ciberseguridad, phishing, ransomware, Convenio de Budapest

Abstract

The exponential development of Information and Communication Technologies (ICTs) has made daily life easier but has also been used by cybercriminals to commit various cyber-assisted crimes. In response, Argentina enacted Law No. 26,388 in 2008, with the goal of regulating crimes such as computer hacking, electronic fraud, and online child sexual abuse material. This legislation is based on the protection of the integrity, confidentiality and availability of information and encourages international cooperation, based on instruments such as the Budapest Convention.

The study also highlights the importance of proactively adapting legislation to address new technological realities and improve international cooperation. The need to continually update the Computer Crime Law and implement advanced cybersecurity technologies to protect citizens and institutions against constantly evolving cyberspace threats is underlined.

Keywords:

Computer crimes, cybersecurity, phishing, ransomware, Budapest Convention

I. INTRODUCCIÓN

En la actualidad, las TICs (Tecnologías de la Información y Comunicación), han sufrido un desarrollo exponencial en cuanto a sus avances científicos y tecnológicos a modo tal de formar parte de la cotidianeidad del ser humano, ya sea para facilitar la labor diaria, satisfacer necesidades, etc. Pero también estas ventajas han sido aprovechadas por los "Ciber-criminales" para llevar a cabo distintas maneras de realizar delitos por medio del uso o del abuso de la confianza de los usuarios (personas y/o empresas) de distintas plataformas y sistemas informáticos, con el fin de realizar daños o perjuicios con sus víctimas, hacerse de cuantiosas sumas de dinero e incluso en los casos más graves, suprimir datos o afectación de grandes sistemas de salud, poniendo en riesgo vidas humanas.

Ahora bien, pese a ello, ha surgido la necesidad de realizar modificaciones en las leyes respecto a los delitos informáticos en Argentina, los cuales están regidos por la Ley Nº 26.388, promulgada en el año 2008 y modificada posteriormente. Esta ley establece disposiciones específicas para combatir delitos como la piratería informática, el fraude electrónico, el material de abuso sexual infantil (mal llamada "pornografía infantil") en línea y otros delitos relacionados con el uso indebido de tecnologías de la información y la comunicación. (Ley Nº 26.388, 2008).

El marco teórico que sustenta esta legislación incluye principios como la protección de la integridad, la confidencialidad y la disponibilidad de la información, así como la protección de la privacidad de las personas. Incluye disposiciones relacionadas con la cooperación internacional en la lucha contra el ciberdelito, estableciendo mecanismos de colaboración entre Argentina y otros países para investigar y perseguir delitos informáticos

que trascienden las fronteras nacionales, entre los cuales se encuentran los instrumentos provenientes de la Unión Europea como el “Convenio de Budapest” y “Los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal”. Además, se busca garantizar la seguridad de las transacciones electrónicas y fomentar el buen uso y responsable de la tecnología. Cómo se definirá más adelante, el delito informático es toda conducta realizada mediante el uso de sistemas informáticos que afecte la confidencialidad, integridad o disponibilidad de datos, sistemas o programas informáticos, o que implique el acceso no autorizado a sistemas informáticos.

El Convenio de Budapest, firmado el 23 de noviembre de 2001 y entró en vigor el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría, es el primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo.(Convenio de Budapest sobre el Cibercrimen, 2001).

Consiste en el único acuerdo internacional sobre delitos informáticos que hace hincapié en las infracciones de derechos de autor, fraude informático, MASI, los delitos de odio y violaciones de seguridad de red. Gracias al reconocimiento de la necesidad de prevenir dichos actos que puedan poner en peligro la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, es que se determina la lucha eficaz contra estos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo acciones que permitan una cooperación internacional rápida y fiable. También, busca homogeneizar las definiciones sobre ciberdelito, establecer el intercambio

de información en lo que respecta a estos ilícitos, garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada.

Tiene en cuenta los convenios existentes y actúa complementándose para incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos, así como para permitir la obtención de pruebas electrónicas. En conclusión, el convenio es el instrumento internacional vigente hoy en día para hacer efectiva la lucha contra el cibercrimen.

La pregunta del trabajo de investigación planteada es la siguiente: ¿Las leyes, que modifican el Código Penal Argentino en conjunto con demás leyes y convenios internacionales, han conseguido la regulación de los delitos informáticos a nivel nacional y provincial, como así también, su disminución a lo largo de estos últimos años?

Como hipótesis principal de este trabajo, se plantea que la ley 26.388 ha introducido modificaciones al Código Penal Argentino, no parece haberse ajustado a las normativas internas del país a los estándares internacionales de regulación y control de los delitos informáticos. A pesar de que la legislación argentina ha avanzado al sancionar esta ley, aún no logra tipificar todas las formas delictivas que se vuelven cada vez más comunes en nuestra sociedad contemporánea.

La realidad es que el rápido desarrollo tecnológico y la constante evolución de las amenazas ciber-asistidas superan la capacidad del marco legal existente para mantenerse al día. Resulta evidente que el ordenamiento jurídico argentino aún carece de las herramientas

necesarias y adecuadas para detectar, prevenir y reducir la incidencia de estos delitos informáticos.

La complejidad de los delitos informáticos y su capacidad para trascender las fronteras nacionales plantean desafíos adicionales para la legislación y la aplicación de la ley. Es crucial que el sistema legal se adapte de manera proactiva para abordar estas nuevas realidades y proteger eficazmente a los ciudadanos y las instituciones contra los riesgos del mundo digital en constante cambio.

Mientras que el objetivo general de esta investigación será examinar en detalle lo expuesto anteriormente. Se aspira a profundizar en el análisis de la ley 26.388 para determinar si su implementación ha permitido al sistema jurídico penal argentino ponerse a la altura de los estándares internacionales relacionados con los delitos informáticos.

En este sentido, se pretende llevar a cabo una exploración exhaustiva de la legislación mencionada, con el fin de evaluar su alcance y eficacia en la protección de los ciudadanos y las instituciones contra los delitos informáticos. Se buscará identificar posibles brechas o limitaciones en la ley actual que impidan una respuesta adecuada a las amenazas de este delito en constante evolución.

Se planteará una investigación detallada sobre si el marco jurídico argentino proporciona los recursos y herramientas necesarios para prevenir, detectar y sancionar los delitos informáticos cometidos a través de las nuevas tecnologías. Esto incluirá un análisis de la capacidad de las autoridades para investigar y procesar estos casos, así como la efectividad de las medidas de prevención y protección implementadas en el ámbito digital.

Además de lo ya expuesto, se propone una serie de objetivos específicos que contribuirán a una comprensión más completa y detallada de la problemática de los delitos

informáticos. En primer lugar, se busca proporcionar una definición clara y precisa del concepto de delito informático, así como examinar sus características fundamentales para entender su naturaleza y alcance. En segundo lugar, se llevará a cabo un análisis en profundidad de los diversos medios utilizados para cometer estos delitos, con el objetivo de identificar las técnicas y herramientas más comunes empleadas por los perpetradores en el entorno digital. Asimismo, se pretende identificar y explicar los tipos de delitos informáticos más frecuentes en el contexto argentino, brindando ejemplos concretos y casos ilustrativos que permitan comprender la diversidad y gravedad de estas conductas.

Un objetivo adicional es estudiar en profundidad la regulación de los delitos informáticos en el ordenamiento jurídico argentino, centrándose especialmente en la ley de delitos informáticos que introduce modificaciones al Código Penal. Se analizará el contenido de esta legislación, evaluando su coherencia con los estándares internacionales y su efectividad en la prevención y persecución de los delitos informáticos.

Además, se realizará un estudio comparativo de forma cualitativa para examinar cómo otros países regulan esta materia, con el fin de identificar buenas prácticas y posibles áreas de mejora en el marco normativo argentino. Finalmente, se enunciarán y analizarán algunos precedentes jurisprudenciales relevantes relacionados con la temática de los delitos informáticos, con el objetivo de comprender cómo ha evolucionado la interpretación y aplicación de la ley en este ámbito y qué lecciones pueden extraerse de casos anteriores para fortalecer el sistema legal en el futuro.

II. RESULTADOS

A. Descripción General de los Datos

El presente estudio abarca un período de investigación que abarca esta última década, principalmente luego de la pandemia covid-19, durante el cual se recopilaron datos relevantes sobre incidentes de delitos informáticos. Estos datos se obtuvieron a partir de informes y reportes proporcionados por diversas agencias y bases de datos especializadas en seguridad cibernética, garantizando así una cobertura amplia y representativa de los delitos cibernéticos.

Estos incidentes se clasificaron en cuatro categorías principales para facilitar su análisis: ransomware, phishing, malware, y otros delitos. La categoría de "otros delitos" incluye actividades ilícitas tales como el robo de identidad y el fraude en línea. Cada una de estas modalidades representa un conjunto específico de habilidades y objetivos utilizados por los delincuentes, proporcionando una visión integral del panorama de amenazas cibernéticas durante los años estudiados.

B. Distribución de Incidentes por Año

La Tabla 1 presenta la distribución anual de los diferentes tipos de delitos informáticos registrados durante el período del año 2021, el cual surge del reporte "Ciberdelitos durante la pandemia del covid-19 en Argentina: Informe de denuncias judiciales y modalidades frecuentes 2020-2021 (Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal de la República Argentina, 2022). Este informe anual permite observar las tendencias y cambios en la frecuencia de estos delitos a lo largo del tiempo a nivel nacional.

Se ha detectado un gran incremento en la cantidad de incidentes relacionados con phishing y malwares. Este aumento puede atribuirse a la creciente sofisticación de las técnicas empleadas por los delincuentes, así como a la mayor exposición y vulnerabilidad de los sistemas informáticos a estos tipos de ataques. Por otro lado, los incidentes de phishing han mostrado una tendencia relativamente constante a lo largo de los años. Este fenómeno sugiere que las tácticas de phishing continúan siendo una herramienta eficaz para los delincuentes, aunque no se ha observado el mismo crecimiento explosivo que en las otras categorías.

La estabilidad en los incidentes de phishing puede deberse a una combinación de factores, como la adopción de mejores prácticas de seguridad por parte de los usuarios y las mejoras en los sistemas de detección y prevención. Sin embargo, la persistencia de estos incidentes indica que sigue siendo un problema relevante que necesita atención continua.

Tabla 1: Incidencia de Diferentes Tipos de Delitos Informáticos (2021)

Distrito	Delitos investigados
Provincia de Buenos Aires	6.700
Tierra del Fuego	1.930
Mendoza	1.144
Santa Fe	803
Río Negro	427
Justicia Federal/Nacional	411
Córdoba	305
CABA	157
Neuquén	151
Santa Cruz	94
Misiones	85
Chubut	78
Tucumán	63
Catamarca	51
La Pampa	45
Formosa	36
Entre Ríos	33
San Luis	20
Salta	20
La Rioja	16
Corrientes	13
Santiago del Estero	11
Jujuy	-
Chaco	-
San Juan	-
TOTAL	**12.593**

Fuente:https://www.argentina.gob.ar/sites/default/files/2020/11/informe_sobre_ciberdelitos_en_pandemia_en_argentina_2020-2021.pdf

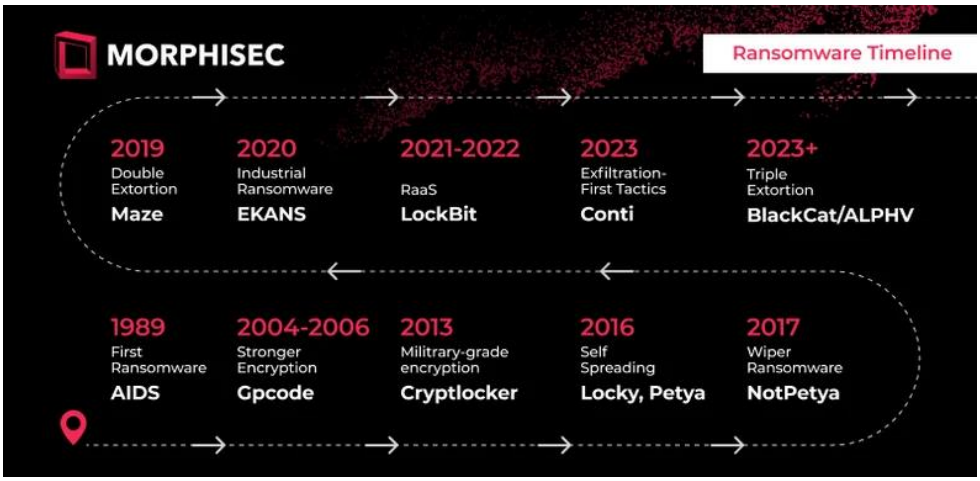
C. Análisis de Tendencias

El análisis de tendencias revela un notable incremento en los incidentes de ransomware en Argentina desde 1989 hasta 2023. Como se muestra en la Figura 1, ha habido un aumento constante en el número de versiones de este tipo de software malicioso, con un crecimiento particularmente pronunciado a partir de 2020, coincidiendo con la pandemia de Covid-19.

La Figura 1 ilustra esta tendencia creciente de manera clara, destacando cómo los incidentes de ransomware se han multiplicado a lo largo de los años. El período posterior a 2020 muestra un incremento significativo, que puede estar relacionado con varios factores, incluyendo el aumento del trabajo remoto y la mayor dependencia de las tecnologías digitales durante la pandemia.

Este crecimiento en los incidentes de ransomware puede atribuirse a la creciente sofisticación de las técnicas utilizadas por los ciberdelincuentes, así como a la expansión de las oportunidades para realizar ataques debido a la transformación digital acelerada por la pandemia. Los delincuentes han aprovechado las vulnerabilidades de los sistemas de seguridad que surgieron durante la transición masiva al trabajo remoto, explotando tanto las debilidades tecnológicas como la falta de preparación de muchas organizaciones para enfrentar estas nuevas amenazas.

Figura 1: Tendencia de Incidentes de Ransomware (1989-2023)



Fuente: https://blog.morphisec.com/ransomware-history-evolution-of-attacks-and-defenses

D. Distribución Geográfica

Se llevó a cabo un análisis geográfico detallado de los incidentes de delitos informáticos registrados durante el período de estudio. Los resultados de este análisis revelaron que la mayoría de estos delitos se concentraron en las grandes áreas metropolitanas de América Latina.

Figura 2: Distribución Geográfica de los Incidentes de Delitos Informáticos en América Latina (2022-2023)

Fuente:https://blog.lacnic.net/ciberseguridad/lecciones-aprendidas-de-mas-de-100-casos-de-ransomware

En Argentina, particularmente en las grandes ciudades como Buenos Aires, Córdoba y Rosario, mostraron una mayor incidencia de delitos informáticos en comparación con las áreas rurales y menos urbanizadas. Esta tendencia puede deberse a varios factores, incluyendo la mayor densidad de población, la mayor cantidad de empresas y organizaciones con infraestructuras digitales, y el uso más intensivo de tecnologías de la información en estas áreas.

III. DISCUSIÓN

La presente investigación se propuso evaluar la efectividad de las leyes argentinas, en particular la ley de delitos informáticos N° 26.388, y los convenios internacionales en la regulación y disminución de los delitos informáticos a nivel nacional y provincial. Los resultados obtenidos revelan un panorama complejo y desafiante. La pregunta de investigación planteada sobre si las leyes han conseguido la regulación y disminución de los delitos informáticos encuentra respuestas parciales y sistematizadas en los datos analizados.

A. Impacto de las leyes frente al aumento de ransomware y phishing

El notable incremento en los incidentes de ransomware y la persistente presencia de ataques de phishing durante la última década, especialmente posterior a la pandemia de Covid-19, sugieren que los avances legislativos han sido insuficientes para mitigar estos delitos de manera efectiva. La hipótesis de que la ley 26.388, aunque ha introducido modificaciones significativas al Código Penal Argentino, no se ha ajustado completamente a las normativas internacionales ni ha logrado tipificar todas las formas emergentes de delitos informáticos, se ve respaldada por los hallazgos de este estudio.

La interpretación de estos resultados a la luz del modelo teórico adoptado, que se basa en la protección de la integridad, confidencialidad y disponibilidad de la información, así como en la cooperación internacional para combatir el cibercrimen, destaca la necesidad de un enfoque dinámico y adaptable en la legislación sobre delitos informáticos. La rápida evolución de las amenazas cibernéticas, acelerada por el incremento del trabajo remoto y la digitalización durante la pandemia, ha superado la capacidad del marco legal actual para mantenerse al día. Esto resalta la importancia de actualizar y fortalecer continuamente la legislación y los mecanismos de cooperación internacional.

En este contexto, es esencial profundizar en el análisis de la ley de delitos informáticos. Esta ley, promulgada en 2008, fue un avance significativo en la legislación argentina, incorporando nuevas figuras delictivas relacionadas con el uso indebido de tecnologías de la información y comunicación. La ley tipifica delitos como el acceso indebido a sistemas informáticos, la difusión de virus o "malwares", el fraude informático y el material de abuso sexual infantil en línea. Sin embargo, a pesar de estos avances, la ley no ha logrado mantenerse al ritmo de las rápidas innovaciones tecnológicas y las nuevas modalidades delictivas que han surgido en el ciberespacio. Por ejemplo, las técnicas de phishing y ataques de ransomware se han sofisticado considerablemente, y la ley 26.388 no contempla medidas en específico ni actualizaciones periódicas que aborden estas nuevas amenazas de manera efectiva.

Comparando estos hallazgos con la narrativa existente, se observa que estudios previos ya habían documentado un aumento global significativo en los delitos informáticos durante la pandemia de Covid-19. Investigaciones como las de Morphisec (2023) sobre la evolución del ransomware coinciden en señalar que la sofisticación de las técnicas de cibercrimen y la expansión de oportunidades para realizar ataques debido a la transformación digital acelerada superan las capacidades de las leyes vigentes. Además, la importancia de la cooperación internacional, destacada en el Convenio de Budapest (2001) y en el Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2021), se refleja en los resultados de este estudio, subrayando la necesidad de mejorar la colaboración internacional para enfrentar eficazmente estos desafíos.

Las implicaciones de estos resultados son múltiples y significativas. Teóricamente, subrayan la necesidad de un marco legal adaptable y proactivo que pueda responder a la

rápida evolución de las amenazas cibernéticas. Sugieren que tanto las entidades gubernamentales como las organizaciones privadas deben invertir en actualizaciones tecnológicas avanzadas de ciberseguridad y en constante capacitación de sus empleados. La concienciación sobre seguridad cibernética debe ser una prioridad para reducir la vulnerabilidad a ataques como el phishing y el ransomware.

B. Vulnerabilidad de grupos específicos frente a los delitos informáticos

Uno de los aspectos más críticos en la evaluación de la efectividad de la Ley de Delitos Informáticos es su impacto en los grupos vulnerables. Estos grupos, que incluyen a menores de edad, adultos mayores, personas con discapacidades y comunidades con menor acceso a la educación y a recursos tecnológicos, son particularmente susceptibles a ser víctimas de delitos informáticos debido a su ignorancia o escasa capacidad para reconocer y reaccionar ante este tipo de amenazas.

- Niños, Niñas y Adolescentes: Los NNA (menores de edad comunmente llamados) son un grupo especialmente vulnerable al Grooming, al MASI (material de abuso sexual infantil) en línea, así como a otras formas de explotación y acoso u hostigamiento cibernético. La Ley Nº 26.388 aborda estos delitos, pero es de gran importancia que se implementen programas educativos y preventivos dirigidos a este grupo para aumentar su conciencia y resiliencia frente a estas amenazas.
- Adultos Mayores: Los adultos mayores o de la tercera edad (baby boomer), que a menudo tienen menos experiencia con la tecnología, son objetivos comunes de fraudes y estafas en línea. La legislación debe considerar medidas específicas para proteger a esta población, incluyendo campañas de concienciación y apoyo técnico.

- Personas con Discapacidades: Este grupo puede enfrentar barreras adicionales en el acceso y uso seguro de la tecnología. Es esencial que las políticas y programas de ciberseguridad sean inclusivos y accesibles para todas las personas, independientemente de sus capacidades físicas o cognitivas.
- Comunidades con Menor Acceso a la Educación y Recursos Tecnológicos: Las comunidades que tienen menos acceso a la educación y a recursos tecnológicos son más vulnerables a los delitos informáticos. La legislación debe fomentar la inclusión digital y proporcionar recursos educativos que capaciten a estas comunidades en la utilización segura de la tecnología.

La dependencia de datos obtenidos de informes públicos puede haber limitado la precisión y representatividad de los resultados. Además, la concentración en áreas metropolitanas puede haber excluido incidentes relevantes en zonas rurales, lo que sugiere la necesidad de estudios más amplios y diversos en términos geográficos. Asimismo, la naturaleza transversal del estudio impide establecer causalidad entre las políticas implementadas y la incidencia de delitos informáticos, lo que podría ser abordado en investigaciones futuras.

A pesar de estas limitaciones, este estudio tiene varias fortalezas que deben ser destacadas. Proporciona una visión integral del panorama de amenazas cibernéticas en Argentina y resalta la necesidad de una legislación dinámica y adaptable. La contribución esencial de esta investigación radica en la identificación de brechas en la ley 26.388 y en la recomendación de mejoras para enfrentar las nuevas realidades tecnológicas y tácticas de los ciberdelincuentes. Además, subraya la importancia de la cooperación internacional y de la implementación de tecnologías avanzadas de ciberseguridad.

C. Conclusiones finales

De colofón, los resultados de este estudio indican que, aunque la ley de delitos informáticos y los convenios internacionales han logrado ciertos avances en la regulación de los delitos informáticos en Argentina, aún existen discrepancias significativas. La creciente sofisticación de las técnicas de cibercrimen y la rápida evolución tecnológica superan la capacidad del marco legal actual para mantenerse al día. Es de gran importancia que el sistema legal se adapte proactivamente para proteger eficazmente a los ciudadanos y las instituciones contra las amenazas del mundo digital en constante cambio y evolución.

Con base en estos hallazgos, es recomendable revisar y actualizar continuamente la Ley 26.388 para adaptarse a las nuevas formas de delitos informáticos. Las organizaciones público/privadas deben adoptar tecnologías avanzadas y promover la capacitación continua en ciberseguridad. Mejorar los mecanismos de cooperación internacional para la detección, investigación y sanción de delitos informáticos es fundamental. Además, futuros estudios deberían enfocarse en evaluar la efectividad de políticas específicas implementadas después de 2021 para combatir/prevenir el ransomware y en investigar el impacto de nuevas tecnologías de seguridad cibernética en diferentes sectores industriales. Un análisis comparativo con otros países que han implementado legislaciones similares brindarían valiosos aportes para mejorar el marco legal argentino.

La presente investigación contribuye al conocimiento sobre la regulación de los delitos informáticos en Argentina y proporciona una base para futuras investigaciones en este campo. Es fundamental que el sistema legal y las prácticas de ciberseguridad se adapten continuamente para enfrentar las amenazas emergentes y proteger a los ciudadanos e instituciones en el entorno digital en constante evolución.

Referencias

Doctrina:

Aboso, Gustavo E. y Zapata, María F.(2006): “Cibercriminalidad y derecho penal” - IB d F. Montevideo Bs. As., en Argentina Euros Editores SRL

Cibercrimen y Delitos Informaticos: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Ciberdelitos durante la pandemia del Covid-19 en Argentina: Informe de denuncias judiciales y modalidades frecuentes 2020-2021: https://www.argentina.gob.ar/sites/default/files/2020/11/informe_sobre_ciberdelitos_en_pandemia_en_argentina_2020-2021.pdf

Código Penal Argentino

Ley de delitos informáticos N° 26.388 del Código Penal Argentino

Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Convenio de Budapest

History of Ransomware: The Evolution of Attacks and Defense Mechanisms: https://blog.morphisec.com/ransomware-history-evolution-of-attacks-and-defenses

Lecciones aprendidas de más de 100 casos de ransomware: https://blog.lacnic.net/ciberseguridad/lecciones-aprendidas-de-mas-de-100-casos-de-ransomware

Sain G. y Azzolin H. (2017). Delitos Informáticos (1ª Ed.). Buenos Aires: B de F