UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

CARRERA: DERECHO

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"LA GARANTÍA A LA PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN EL MARCO LEGAL DE LOS DELITOS INFORMÁTICOS EN ECUADOR Y COLOMBIA"

Trabajo de titulación previo a la obtención del título de Abogada de la República del Ecuador

Línea de investigación: Desarrollo social y del comportamiento humano

AUTORA:

Inés María Sánchez Quishpe

DIRECTORA:

Msc. Alexandra Cristina Pupiales Proaño

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1751989516		
APELLIDOS Y NOMBRES:	Sánchez Quishpe Inés María		
DIRECCIÓN:	Malchinguí- Pichincha		
EMAIL:	imsanchezq@utn.edu.ec		
TELÉFONO FIJO:	022158325	**TELÉFONO MÓVIL:**	0980757265

DATOS DE LA OBRA	
TÍTULO:	"LA GARANTÍA A LA PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN EL MARCO LEGAL DE LOS DELITOS INFORMÁTICOS EN ECUADOR Y COLOMBIA"
AUTOR:	Sánchez Quishpe Inés María
FECHA: AAAMMDD	21/06/2024
SOLO PARA TRABAJOS DE GRADO	
CARRERA/PROGRAMA:	■ **GRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Abogada
DIRECTOR:	Msc. Pupiales Proaño Alexandra Cristina

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de febrero del 2025

EL AUTOR:

Firma: .....

Nombre: Sánchez Quishpe Inés María

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 01 de marzo de 2024

Msc. Alexandra Cristina Pupiales Proaño

TUTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

ALEXANDRA CRISTINA PUPIALES PROANO

Firmado digitalmente por ALEXANDRA CRISTINA PUPIALES PROANO
Fecha: 2024.03.01 10:42:57 -05'00'

Msc. Alexandra Cristina Pupiales Proaño

C.C.: 1004418917

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificador del trabajo de Integración Curricular "LA GARANTÍA A LA PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN EL MARCO LEGAL DE LOS DELITOS INFORMÁTICOS EN ECUADOR Y COLOMBIA" elaborado por SÁNCHEZ QUISHPE INÉS MARÍA, previo a la obtención del título ABOGADA DE LA REPÚBLICA DEL ECUADOR, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

ALEXANDRA CRISTINA PUPIALES PROANO

Firmado digitalmente por ALEXANDRA CRISTINA PUPIALES PROANO
Fecha: 2024.03.01 08:25:22 -05'00'

Msc. Alexandra Cristina Pupiales Proaño
Nombre de la Tutora
C.C 1004418917

STEFANIE CAROLINA AUMALA VISCARRA

Msc. Stefanie Carolina Aumala Viscarra
Nombre de la Asesora
C.C 1724150733

DEDICATORIA

A mis padres Guillermo e Inés, a quienes admiro y agradezco todo su cariño e incondicional apoyo tanto emocional como económico a lo largo de mis años de estudio y en cada aspecto de mi vida. Han sido mi guía y ejemplo a seguir.

A mis hermanos Gabriela y Carlos, quienes me han apoyado y ayudado, cada a uno a su modo, pero siempre han estado conmigo en mis momentos de crisis y han sabido guiarme de la mejor manera.

A mis sobrinos Jordana y Gael, que aunque tal vez no lo sepan son mi mayor alegría y motivación. A pesar de las circunstancias espero en adelante estar presente en cada una de sus vidas.

A mi abuelita Rosario, que con su calidez me alienta a cumplir mis metas. A mis abuelitos Julia y Carlos que los recuerdo con amor y nostalgia, y aunque ya no estén físicamente conmigo siempre los llevo en mis pensamientos junto con sus enseñanzas.

Por último, pero no menos importante, a mi hijo de cuatro patas, Charly, que me da mucha felicidad, aprecio mucho su lealtad, compañía y cariño.

AGRADECIMIENTOS

Agradezco infinitamente a mi familia, por los sacrificios que han hecho estando a la distancia para que el día de hoy yo esté culminando una de mis metas.

A mi pareja, le agradezco por su cariño y por haber estado presente en cada una de mis facetas universitarias, alentándome y motivándome, especialmente en este proceso de investigación. También quiero expresar mi gratitud hacia su familia, quienes con su afecto han dejado una huella imborrable en mi camino.

A la Universidad Técnica del Norte y a mis respetados docentes, les estoy profundamente agradecida por la invaluable enseñanza que me han proporcionado durante estos cinco años de formación académica.

A mi directora Msc. Alexandra Pupiales y a mi asesora Msc. Carolina Aumala, que, con su guía, han desempeñado un papel fundamental en la culminación de este trabajo de investigación. Su apoyo ha sido crucial para la realización de este proyecto.

RESUMEN EJECUTIVO

La presente investigación tiene como objetivo analizar la incidencia de los delitos informáticos en la protección de datos e intimidad personal y familiar en Ecuador. Con el fin de desarrollar estrategias efectivas de prevención y mitigación de estos delitos, considerando aspectos básicos adoptados por la legislación colombiana. La evolución tecnológica y la creciente dependencia de la sociedad a la tecnología, así como el fácil acceso a herramientas informáticas, representan desafíos para el mundo actual y ponen en riesgo la garantía de derechos constitucionales, especialmente en países como Ecuador con un marco legal débil. Por lo tanto, este estudio se basa en comprender y abordar los riesgos asociados con la protección de datos e intimidad personal y familiar en Ecuador, con el fin de determinar si se garantizan efectivamente estos derechos constitucionales.

Se utilizó un enfoque cualitativo con un estudio descriptivo, histórico y hermenéutico, combinado con una revisión detallada de la legislación de ambos países sobre protección de datos e intimidad personal y familiar. Se analizaron leyes, reglamentos y jurisprudencia para comprender el marco legal de los delitos informáticos. Además, se llevaron a cabo entrevistas a expertos en derecho y ciberseguridad para obtener perspectivas especializadas sobre la efectividad de las leyes y posibles estrategias de mitigación de delitos informáticos.

Los resultados destacaron que los delitos informáticos se aprovechan de las oportunidades brindadas por las Tecnologías de la Información y la Comunicación (TIC), generando vulnerabilidades que los criminales explotan para robar datos y violar la intimidad. Ecuador y Colombia enfrentan desafíos similares en protección de datos, sin embargo, Colombia muestra un enfoque más punitivo y reparador en delitos informáticos, a diferencia de Ecuador que presenta deficiencias en políticas públicas, sanciones y tutela judicial.

Palabras clave: delitos informáticos, derechos constitucionales, ciber seguridad, protección de datos, intimidad personal y familiar.

ABSTRACT

The objective of this research is to analyze the incidence of computer crimes on the protection of data and personal and family privacy in Ecuador. In order to develop effective strategies for the prevention and mitigation of these crimes, considering basic aspects adopted by Colombian legislation. Technological evolution and society's growing dependence on technology, as well as easy access to computer tools, represent challenges for today's world and put the guarantee of constitutional rights at risk, especially in countries like Ecuador with a weak legal framework. Therefore, this study is based on understanding and addressing the risks associated with the protection of personal and family data and privacy in Ecuador, in order to determine whether these constitutional rights are effectively guaranteed.

A qualitative approach was used with a descriptive, historical and hermeneutical study, combined with a detailed review of the legislation of both countries on data protection and personal and family privacy. Laws, regulations and jurisprudence were analyzed to understand the legal framework of cybercrime. Additionally, interviews were conducted with law and cybersecurity experts to obtain specialized perspectives on the effectiveness of laws and possible cybercrime mitigation strategies.

The results highlighted that computer crimes take advantage of the opportunities provided by Information and Communication Technologies (ICT), generating vulnerabilities that criminals exploit to steal data and violate privacy. Ecuador and Colombia face similar challenges in data protection, however, Colombia shows a more punitive and remedial approach in computer crimes, unlike Ecuador, which presents deficiencies in public policies, sanctions and judicial protection.

Keywords: computer crimes, constitutional rights, cyber security, data protection, personal and family privacy.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El presente trabajo de investigación centra su interés en la protección de datos e intimidad personal y familiar en el marco legal de los delitos informáticos en Ecuador y Colombia. En primer lugar, es importante destacar cómo el avance tecnológico ha impactado en la sociedad, brindando herramientas que permiten realizar tareas de manera más eficiente y rápida. Sin embargo, esta dependencia de la tecnología también ha dado lugar a nuevas formas de delincuencia que transgreden los derechos constitucionales, especialmente el derecho a la protección de datos e intimidad personal, que son objeto de estudio de esta investigación.

Sin duda, en su mayoría, las personas tienden a ser indiferentes o inconscientes con la información que se proporciona en las páginas web, sin considerar que estas pueden ser de origen dudoso y los datos personales ingresados pueden utilizarse de manera incorrecta, dándose el robo de datos, suplantación de identidad, saqueo de cuentas bancarias y la venta de información personal en el mercado negro. Ante esto los diferentes Estados han mostrado preocupación y han optado por unirse al convenio de Budapest. Este acuerdo tiene como objetivo combatir la ciberdelincuencia mediante la creación de leyes adecuadas sobre delitos informáticos y la mejora de las técnicas de investigación.

Ecuador solo ha actuado como observador en relación a este acuerdo, mientras que países cercanos como Colombia han sido parte del acuerdo desde el año 2020. Es evidente que han mejorado la gestión de los delitos cibernéticos en su legislación, principalmente gracias a la introducción de cambios en su Código Penal a través de la Ley 1273 (2009). Es pertinente mencionar que la Ley 1237 (Ley de delitos informáticos) y la Ley 1581 (Ley de protección de datos personales), son leyes que en ciertos aspectos se asemejan a la normativa de Ecuador, es decir al Código Orgánico Integral Penal y la Ley Orgánica de Protección de Datos Personales (LOPDP), esta última que en Ecuador se expidió en el 2021, no obstante, su aplicación sancionadora entró en vigor en mayo del 2023, lo que esto significa es que Ecuador está muy

por detrás de otros países en términos de desarrollo normativo. En general este estudio busca contribuir al debate sobre la importancia de salvaguardar la privacidad y los datos personales en el contexto de los delitos informáticos.

El problema de Investigación

Con la aparición de las Tecnologías de la Información y Comunicación (TIC), el ciberespacio se ha visto afectado por algunos usuarios que hacen un uso inapropiado de ellas, poniendo en peligro la seguridad y privacidad de los demás usuarios. Es de suma importancia reconocer la gravedad de los delitos cibernéticos, y tanto la Unión Europea como la Organización de las Naciones Unidas han identificado los delitos más comunes, como el fraude con tarjetas, el *phishing*, el *pharming*, el *scamming*, el *cibergrooming*, el *spyware*, el *skyming*, el *cardado*, el *numerati*, los virus informáticos y la suplantación de identidad.

Es necesario tener en cuenta que, aunque exista una legislación que busca proteger los derechos constitucionales e incluso una ley de protección de datos, se requiere una evolución en la normativa penal para abordar de manera óptima estas nuevas formas de delitos cibernéticos. El hecho de que una norma importante como el Código Orgánico Integral Penal se mantenga estática genera dudas sobre la protección de los derechos.

En Ecuador, la naturaleza de estas prácticas delictivas es incierta. Aunque el COIP establece diferentes tipos de delitos informáticos, como la interceptación y divulgación de datos o mensajes informáticos, así como los daños y fraudes informáticos, no se hace una distinción clara entre ellos y se agrupan en distintos capítulos. Esta falta de claridad dificulta denunciar los delitos informáticos y confunde a menudo a las autoridades encargadas de hacer cumplir la ley. Además, la ausencia tanto de cooperación internacional como un marco legal sólido y preciso complica los procesos legales y la identificación de los responsables, lo que puede llevar a una mayor impunidad en estos casos.

Pregunta de investigación

¿Cómo garantiza el Estado ecuatoriano el derecho a la protección de datos e intimidad personal y familiar ante los delitos informáticos y qué aspectos se puede tomar como base de la legislación colombiana?

Justificación y pertinencia

La elaboración de esta investigación académica es pertinente, aunque existen investigaciones previas sobre delitos cibernéticos y protección de datos, es importante profundizar en el contexto específico de Ecuador y Colombia, ya que las leyes, regulaciones y políticas públicas pueden variar entre estos países. La protección de datos como la intimidad personal son derechos primordiales reconocidos en las constituciones y marcos legales de ambos países. Estudiar el impacto de los delitos informáticos en estos derechos permitirá evaluar si la normativa existente en el Ecuador es suficiente para enfrentar los desafíos actuales en torno a los datos personales e intimidad personal y familiar.

Esta investigación pretende analizar los desafíos y las garantías legales en las jurisdicciones específicas, centrándose en los delitos informáticos y la protección de la intimidad personal en Ecuador y Colombia. Ambos países reconocen estos derechos en sus marcos legales y es fundamental salvaguardarlos en el entorno digital. Al estudiar las diferentes modalidades de delitos informáticos en relación con estos derechos, se podrá evaluar la efectividad de las leyes y regulaciones existentes, identificar posibles lagunas y proponer medidas para fortalecer la protección de los ciudadanos.

Establecer marcos legales claros que tipifiquen y penalicen los delitos informáticos es tan pertinente como promover la cooperación internacional para abordar los desafíos transfronterizos asociados a la ejecución de estos delitos, así como a la extradición de los delincuentes involucrados en la vulneración de los derechos fundamentales de los ciudadanos. La falta de vinculación de Ecuador con el Convenio de Budapest sobre el cibercrimen es una

cuestión relevante que justifica la investigación académica en relación con la protección de datos y la intimidad personal en el contexto de los delitos informáticos.

En este orden de ideas, investigar el tema propuesto permitirá comprender y abordar los riesgos asociados con la protección de datos e intimidad personal y familiar. Teniendo como beneficiarios directos a todos los ecuatorianos, legisladores, autoridades competentes y otras partes interesadas en fortalecer las regulaciones y salvaguardar los derechos de los individuos en el entorno digital, puesto que se otorgará un aporte que permita orientar la toma de decisiones en la formulación de políticas públicas relacionadas con la protección de datos y la seguridad cibernética. Como beneficiarios indirectos se encuentra la comunidad jurídica, y aquellos individuos interesados en enriquecer la literatura en el campo de la seguridad cibernética, el derecho informático, el derecho a la protección de datos e intimidad personal.

Objetivos

Objetivo General

Analizar la incidencia de los delitos informáticos en la protección de datos e intimidad personal y familiar en Ecuador, con el fin de desarrollar estrategias efectivas de prevención y mitigación de estos delitos, considerando aspectos básicos adoptados por la legislación colombiana.

Objetivos Específicos

1. Realizar un estudio de derecho comparado sobre la regulación y tipificación de los delitos informáticos en la legislación ecuatoriana y colombiana a fin de conocer su aplicación y sanción.
2. Identificar los principales retos que enfrenta la normativa que regula los delitos informáticos en Ecuador, a fin de determinar si garantiza los derechos de la población.
3. Analizar las medidas de prevención y protección más efectivas contra los delitos informáticos para precautelar los datos y la intimidad personal en la legislación

colombiana y que puedan ser implementadas en la legislación ecuatoriana.

CAPÍTULO I: MARCO TEÓRICO

1.1. Delitos informáticos

1.1.1. Ciberespacio y las Tecnologías de la Información y Comunicación (TIC)

El ciberespacio y las tecnologías de la información y comunicación están intimamente ligadas, siendo estas herraminetas de interación para el intercambio de información en la cibersociedad. De manera puntual las TIC "se constituyen como una fuente funamemtal para que las personas puedan comunicarse, intercambiar contenido e información, actualmente las TIC están asociadas a redes, servicios y dispositivos electrónicos, como celulares, computadoras, tablets, etc" (Fundación Evolución & Fundación Carlos Vélez, 2020, p. 7).

En esencia, las TIC pueden ser catalogadas como recursos, pues estas han abierto el camino para que en la actualidad sea mucho más sencillo compartir información y a la vez facilitar la comunicación e interacción entre los individuos, a través de herramientas tecnológicas. Por esta razón, se puede afirmar que la forma de acceder al conocimiento ha evolucionado. Cuando se menciona que las TIC se asocian a las redes se hace alusión a medios como la radio, televisión y redes móviles; al hablar de servicios se refiere a la amplia gama de servicios que se brindan por medio de los dispositivos electrónicos, siendo ejemplos, los correos, aplicaciones, y todo aquello que puede almacenarse en la nube.

La influencia de las TIC refleja una amenaza al ciberespacio, siendo este la zona o sitio en donde interactúan estas. Al describir al ciberespacio se destaca la aportación de Martínez (2020), él define a este como el: "conjunto de medios y procedimientos basados en [...] tecnologías, configurados para la prestación de servicios, que se encuentra en evolución dinámica; y está constituido por hardware, software, internet, servicios de información y sistemas de control [...]" (p. 23)

Desde luego, el avance tecnología ha permitido que en el ciberespacio se pueda compartir, crear, intercambiar, eliminar y usar información de forma mucho más rápida, eliminando las barreras de comunicación que pudieron haber existido en épocas anteriores. Esto también trajo desventajas que afectan a la seguridad y privacidad de las personas, ya que al exponer su información personal en un sitio tan grande como el ciberespacio no existe un pleno control, lo que permite manipular y amenazar la información. Por lo que en la misma línea de análisis se menciona que:

> El ciberespacio es un dominio caracterizado por ser común, global, artificial, inmaterial, permeable, transversal y con capacidad para alterar el resto de las realidades, lo que va a dificultar su seguridad, que constituye un objetivo estratégico de la seguridad nacional donde se debe fomentar la cooperación internacional. (Martínez, 2020, p. 23)

La iniciativa para que distintos países a través de sus legislaciones se adhieran a convenios de cooperación internacional, refuerza la ciberseguirdad y combate las nuevas modalidades de delincuencia, que son dos temas con auge en el siglo XXI. A medida que la sociedad y los medios tecnológicos van avanzando es necesario que las normas y leyes también vayan adaptandose a estos cambios, es decir actualizandose a fin de proteger y sobre todo sancionar a aquellos individuos que de forma dolosa han vulnerado los derechos constitucionales de las personas.

1.1.2. Definición del delito informático

Al conceptualizar a los delitos informáticos nos encontramos con varias posturas, sin embargo todas estas concepciones van dirigidas sobre la evolución abrupta que ha sufrido la sociedad al implementar las TIC en su vida cotidiana, de forma que se asume que un delito informático es “toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”

(Castillo & Ramallo, 1989, como se citó en Acurio del Pino, 2016, p. 12)

Varios autores describen a los delitos informáticos como actos ilícitos informáticos que además de atentar contra la intimidad personal, la esfera privada derivada de la enorme acumulación de datos y el patrimonio de las personas, presentan complejidad para lograr su regulación y prevención en el marco jurídico actual de cualquier país, debido a que vivimos una competencia diaria con los avances tecnológicos y las nuevas formas de delinquir (Hernández, 2009).

El crecimiento de delitos informáticos tuvo un pico de crecimiento a raíz de la pandemia, debido a que por el confinamiento las actividades diarias de las personas se vieron limitadas y de una u otra forma tuvieron que adaptarse a la digitalización; además que la población en general recurrió al internet tanto para cumplir con el teletrabajo como para entretenerse en su tiempo de ocio.

En el caso de Ecuador con la llegada de la pandemia de COVID-19 trajo consigo un preocupante incremento en los ciberdelitos contra niños, niñas y adolescentes (NNA). Las estadísticas muestran que durante este período se registraron 242.631 incidentes de este tipo, lo que representa un alarmante aumento del 100% en comparación con años anteriores. Las plataformas digitales en las que se reportaron estos hechos delictivos fueron diversas, incluyendo populares redes sociales como Facebook, Zoom, Twitter, TikTok, así como algunas relacionadas con videojuegos. A nivel geográfico, la provincia del Guayas se destacó como uno de los lugares donde más se produjeron este tipo de ciberdelitos contra los menores de edad durante la pandemia (Henríquez, 2023)

Como vemos con la llegada del internet y el avance tecnológico surgen nuevas modalidades para que los individuos puedan atacar, hoy en día es más común de lo que pudo haber sido hace unos años, tanto ha sido que hoy es tema de preocupación de los ciudadanos y del Estado. De forma generalizada los delitos informáticos no son otra cosa que delitos que se

cometen en el ciberespacio, Jenkinson (2022) afirma que “los ciberataques en la actualidad son más comunes que cualquier otro delito cometido, de forma que tienen hasta mayor éxito que los crímenes organizados” (p. 19).

Por este motivo es que ahora los delitos informáticos se consideran una subespecie del derecho penal. Principalmente porque son objeto de estudio de esta rama del derecho, en donde ciertamente se trata de identificar a los atacantes, aunque en la mayoría de las ocasiones esto resulta muy complejo. Varios autores han afirmado que:

> Cualquier individuo que disponga de una computadora, de acceso a internet, y que cuente con conocimientos y habilidades técnicas, puede llevar a cabo un ataque cibernético; estos ataques, sin excepción, generan un efecto de vulnerabilidad y carencia de protección individual. (Gamón, 2017)

Es decir, un usuario con la suficiencia asutucia podría manipular la tecnología a su favor y cometer crimenes cibernéticos. Además, lleva una ventaja ya que estos delitos no los comete de forma física, por lo que es más dificil determinar su culpabilidad. De forma definitiva los delitos informáticos son conductas realizadas por individuos de forma dolosa, los cuales se valen de los sistemas informáticos computarizados con el propósito de llevar a cabo actividades ilegales contra los sistemas de información, perturbar el funcionamiento de los dispositivos, alterar el *software* para perpetrar delitos logísticos.

Desde luego considerando que existe una amplia gama de delitos que se cometen en el ciberespacio surge la necesidad de ejercer un mayor control. En palabras de Parada & Errecaborde (2018) esto solo sería posible a través de:

> Una colaboración interdisciplinaria entre profesiones relacionados con el estudio de la informática, y los estudiosos del derecho. Esto podría dar lugar a la formulación de un nuevo marco jurídico que aborde cuestiones como el derecho del consumidor en el

ámbito informático o el derecho a la privacidad del consumidor. (p. 160)

Aquella colaboración es indispensable, principalmente porque hoy se vive una era en donde se interactúa de forma inconciente con la tecnología; objetivamente nadie está absuelto de ser víctima de un delito cibernético, y por lo mismo resulta fundamental reexaminar la teoría jurídica aplicable a los nuevos escenarios tecnológicos. De hecho, es necesario llevar a cabo un seguimiento minucioso y realizar investigaciones futuras para abordar los nuevos desafíos que plantea el Internet de forma que se pueda contrarestar estas nuevas modalidades de delincucncia y se puedan proteger los derechos constitucionales de los ciudadanos.

1.1.3. Modalidades más utilizadas para cometer delitos informáticos

Es sustancial considerar las múltiples formas en que se presentan los delitos informáticos, aunque estos actos ilegales contienen particularidades que los distinguen de los delitos tradicionales, presentan características especiales que de cierto modo pueden parecer "similares" entre sí, lo que conlleva a una confusión. Por ello es indispensable identificar y diferenciar aquellas variaciones más utilizadas por los delincuentes en la actualidad. Además, que una sociedad informada es mucho más consiente de los riesgos de vivir en una era digitalizada, por lo que a su a vez puede tomar medidas para proteger su privacidad, seguridad y bienestar. Las modalidades más utilizadas son:

1.1.3.1. *Phishing* o suplantación de identidad

Si bien la mayoría cataloga al *phishing*, *pharming, grooming*, etc., como delitos en realidad estos son "modalidades", es decir formas de cometer un delito; siendo el *phishing* el más común, Shekhar Khandelwal y Rik Das explican que:

El *phishing* es un término derivado de pesca, al reemplazar "f" por "ph", pero contextualmente significan lo mismo […] Así como los peces quedan atrapados en las redes de pesca, también los usuarios inocentes de la web quedan atrapados en los sitios web de *phishing*. (Khandelwal & Das, 2022)

Dicha concepción es la más acertada, pues este delito trata de engañar de manera sofisticada a las personas, el termino pescar hace alusión a enganchar a una víctima por medio de correos electrónicos, llamadas telefónicas, sitios web, mensajes de texto, etc. El *phishing* es un fraude informático con múltiples estilos, pero que en forma generalizada busca adquirir información de índole confidencial, como contraseñas, números de tarjetas, datos personales, etc. Aquí el sujeto falsifica su identidad (persona o empresa) y dolosamente solicita al otro individuo que se le entregue datos personales o que ingrese a una página web (ficticia), que bien podría infiltrar un *software* malicioso que cause daños en el dispositivo o que robe directamente sus datos.

1.1.3.2. *Pharming*

El *pharming* y el *phishing* comparten características similares, no obstante, el *pharming* se caracteriza por ser un tipo de ataque en el que el individuo redirige a la víctima a una página que a primera vista parece legítima, sin embargo, esta es falsa y es controlada por el atacante, lo que generalmente hace es ejecutar códigos en el dispositivo de la víctima para que estos los redirijan inmediatamente a estas páginas *fake*. El *Pharming* se puede dar por medio de dos modalidades, una en el que se ataca el proveedor de internet y otra en la que se ataca el servicio de red local. Es decir, el *pharming* pretende vulnerar los DNS del servidor, o directamente el dispositivo de la víctima. Con estos ataques se puede obtener información privada como sus datos personales, contraseñas, números de tarjetas de crédito, etc. (Banco Pichincha, 2021).

Para evitar sufrir un ataque como el de *pharming*, es esencial utilizar programas de software especializados, navegar por sitios web seguros, ignorar correos de personas desconocidas, y por supuesto no hacer clic en enlaces sospechosos que se muestras en páginas web, es más hay que estar alerta ante cualquier error o problema de conexión, esto puede ayudarnos a evitar ser víctimas de este tipo de delitos.

1.1.3.3. *Scamming*

El *scamming* se constituye como un delito que se basa en el engaño y la manipulación de la víctima para obtener información personal, dinero o acceso a cuentas. Los estafadores utilizan diferentes técnicas para ocultar su identidad y crear daños. Ejemplos de este tipo de delitos son correos en que anuncian que una persona es la número 1000000 en un sitio, y que puede reclamar un premio tan solo registrándose, o también puede suceder que requieran se confirme cierta información personal de un sujeto. Como tal estos delitos son más difíciles de evidenciar, dejando a una persona propensa a ser víctima de estos delincuentes.

1.1.3.4. *Cibergrooming*

El *cibergrooming* también conocido como *grooming* o *child-grooming* es el tipo de delito informático que ataca la integridad de los menores de edad, causándoles afecciones a corto o largo plazo; además de un daño emocional y psicológico, esto porque este delito "se produce cuando un adulto contacta con un menor a través de internet, con el objetivo de entablar una relación de confianza y engatusarle para obtener algún tipo de beneficio sexual" (Rubio, 2021)

Para el cometimiento de este acto, el atacante finge también ser un menor de edad, o crea un perfil con gustos similares al de su víctima, así es un perfil atractivo, y empieza a interactuar con sus víctimas, esto puedo tardar meses o pocos días, dependiendo del nivel de confianza que vaya teniendo con la persona; una vez establecido una relación entre los sujetos el atacante ve el momento oportuno para aprovecharse del menor, llegando al punto de chantajearlo.

1.1.3.5. *Spyware*

El término *"spyware"*, de origen inglés, se refiere a una modalidad para cometer delitos informáticos, aunque carece de una definición propia y precisa, se sugiere que esta modalidad delictiva además de liar la infiltración y monitoreo no autorizado de sistemas informáticos es

“un tipo de *software* malicioso que accede a los datos de una computadora (ordenador) y los envía a otros dispositivos sin que el usuario lo advierta” (Pérez & Gardey, 2016)

Así, el *spyware* se vincula con el ciber espionaje, diseñando un *software* malicioso que recopila información del sistema informático de un usuario, puede obtenerse con o sin consentimiento. Las tácticas aplicadas en esta modalidad de *spyware* incluyen el uso de herramientas y técnicas inteligentes, aunque cualquier ciudadano puede ser víctima. De las maneras más comunes de sufrir un ataque de *spyware* está la instalación de *software* falsos, en internet hay una variedad de “tutoriales” en donde prometen de forma gratuita instalar un programa o *software* que generalmente es de paga; al realizar esto parecería que todo funciona correctamente, pero es indetectable que el *software* malicioso está operando en segundo plano, recopilando toda la información y la actividad que realiza el usuario de forma silenciosa.

El *spyware* se ve reflejado principalmente cuando los usuarios de internet buscan sitios para ver películas, escuchar o descargar música o incluso utilizar programas, el truco detrás de este consiste en que el usuario al momento de ingresar a una página para realizar alguna actividad, no se le va a abrir porque “hace falta complementos para abrirla” pero en el momento de seguir intentando, le va a saltar la página en donde aparentemente no pasa nada, pero aunque parezca indetectable, el virus ya ingresó al sistema.

1.1.3.6. *Cardado*

También conocido como “*Carding*” es una forma grave de fraude en línea que:

> Implica el uso de Internet para engañar, defraudar o aprovecharse de personas u organizaciones. Esto puede incluir una variedad de actividades, como ataques de phishing, robo de identidad y tarjetas, todas las cuales pueden causar pérdidas financieras y daños a la reputación y el crédito de una persona. (Jenifa, 2022)

Es decir, el *cardado* es un registro basado en el *Skyming* cuyo propósito es buscar los saldos de las tarjetas de crédito y a utilizan este método cuando el usuario realiza compras,

pagos, servicios o transferencias vía internet de tal manera que el *hacker* o delincuente informático aproveche la situación en la compra de montos mínimos para que la víctima no se dé cuenta de que está siendo robada.

El delito de *cardado* es una técnica de fraude que consiste en la clonación de tarjetas de crédito o débito para realizar compras no autorizadas. Por lo que este ciber delito se ha vuelto cada vez más común en la era digital, y puede ser perpetrado por individuos o grupos organizados, principalmente porque consiste en la obtención ilegal de datos personales y financieros de terceros con el fin de realizar transacciones fraudulentas. Este delito se acompaña de técnicas como el *phishing*, *spyware* y la ingeniería social, así como los sujetos obtienen la información ilícita.

1.2. La intimidad personal y la protección de datos

1.2.1. Derecho a la intimidad

Para Morales (1995), el término "intimidad" se refiere a la esfera privada de una persona, que puede incluir cosas como su vida personal, correspondencia y comunicaciones privadas, entre otras cosas. La creciente importancia del concepto de intimidad en el campo del derecho es una muestra de la fuerza expansiva y el dinamismo asociado con él. (p. 169). En su obra “El *right of privacy* norteamericano y el derecho a la intimidad en el Perú. Estudio comparado” el autor explica de forma histórica el surgimiento de este derecho constitucional.

Empezando por el año 1879, en donde Thomas Cooley, juez norteamericano, desarrolló en el tratado de Derecho de *Torts*, la expresión *“The right to be let alone”* haciendo alusión al derecho a ser dejado solo, es decir un derecho a no ser molestado, ni perturbado. Esta propuesta inicial del derecho a la intimidad fue acogida por el Tribunal norteamericano para resolver los casos en que se viera vulnerado el derecho a la privacidad; Cooley aseguró que este derecho estaba amparado por la Cuarta y Quinta enmienda de la Constitución. Esto sin duda marcó el comienzo del tratamiento y reconocimiento constitucional del derecho de la persona a la

privacidad y la intimidad.

Ya para el año de 1890 se fortaleció el *"righ of privacy"* o derecho a la privacidad, generalmente se presentaron casos por divulgación de hechos o imágenes personales. Un caso destacable de ello es*: Daily Times Democrat vs. Graham*, donde una chica fue fotografiada en un parque de diversiones justo cuando el viento había levantado su vestido, el tribunal determinó que aun estando en un lugar público a la vista de todos, hay cosas que siguen siendo privadas. En aquel entonces se trataba de proteger no solo al individuo, sino también a la familia, por lo que se quiso evitar la intromisión especialmente de la prensa sobre la vida privada de las personas. La Declaración Universal de Derechos Humanos acogió con gran aceptación la propuesta del derecho a la privacidad.

Es decir, la Declaración Universal de Derechos Humanos (1948) fue de los primeros textos en reconocer en su artículo 12 el derecho a la intimidad, lo que hizo que diferentes países adapten este derecho a sus Constituciones. Internacionalmente encontramos otro instrumento que ampara este derecho, siendo el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales (1950) en su artículo 8.1, en el mismo contexto el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966) configura a la intimidad como derecho fundamental (Martínez de Pisón, 2016).

Como se aprecia el derecho a la intimidad siendo un derecho fundamental no data de la antigüedad, de hecho, su aparición es cercana, sin embargo, es reconocido como uno de los derechos y libertades pertenecientes a la primera generación debido a su importancia. La protección del derecho a la intimidad y los derechos que se derivan de él (derecho a la protección de datos) ha adquirido una mayor relevancia social y jurídica en los últimos tiempos, especialmente debido al desarrollo tecnológico. Esta importancia incluso supera a otras

libertades individuales tradicionalmente mucho más importantes.

Ciertamente las primeras ideas sobre el derecho a la privacidad estaban centradas en el daño derivado de la publicación de una imagen (cámara), donde se afectaba la reputación e intimidad de una persona. Esta concepción dista del sentido actual de la necesidad de proteger los datos personales, esto por la revolución tecnológica en donde nos vemos inmersos (Platero & Acedo, 2021, p. 37).

Las nuevas tecnologías nos han dado nuevos problemas por los que preocuparnos, antiguamente eran escasas las formas en que se vulneraba el derecho a la intimidad, porque lo común era ser fotografiado y publicado en periódicos sin el debido consentimiento, pero actualmente hay múltiples formas de invadir la privacidad, ya no solo se toma la imagen de las personas, sino que se apropian de los datos de estas, ya sea para extorsionar, divulgar o procesar sus datos para diversos propósitos. Coadyuvante de esta situación ha sido el internet que a diario es utilizado por millones de habitantes en el planeta.

Debido al avance de la tecnología se ha visto vulnerable el derecho a la intimidad, debido a que existen nuevas modalidades que comprometen la intimidad personal y familiar; la invasión a la intimidad de una persona versa sobre su personalidad, aspecto, imagen, emociones, domicilio, datos personales, y todo espectro íntimo de la persona, además que su protección debería estar garantizado por el Estado para evitar la intromisión de terceros. (Nino, 2005).

Considerando que la intimidad es un derecho fundamental de todas las personas, para Mendoza et al. (2021) este derecho ostenta la capacidad de las personas para poseer un ámbito propio, es decir una vida privada sin la injerencia de terceros. El derecho a la intimidad forma parte del bloque de constitucionalidad, además tiene como componentes la honra, el buen nombre, el domicilio, y todos los ámbitos correspondientes a la esfera privada como la salud y vida sexual. La intimidad personal y familiar está protegida por las Constituciones de los

diferentes países, los instrumentos internacionales, la jurisprudencia y la doctrina (p. 278).

Es un derecho que protege jurídicamente la autonomía, hábitos, costumbres y la esfera familiar, es decir, por una parte, salvaguarda la privacidad de la familia en relación con la sociedad y por otro establece límites dentro de la propia familia, cada miembro mantiene una vida privada, con relaciones interpersonales y demás aspectos de carácter reservado. De forma generalizada se reconoce la intimidad personal y familiar, sin que esta pueda ser objeto de divulgación salvo que se tenga el consentimiento de la persona o personas.

1.2.1. Derecho a la protección de datos

Primeramente, hay que entender que los nombres, números de teléfono, direcciones, correos electrónicos, estado civil y cualquier otra información de índole privada conforma lo que son datos personales. Es por eso por lo que "la protección de datos personales es un derecho que permite el control del uso y destino de la información personal lo cual impide su tráfico ilícito y vulneración" (Infoem, 2019).

La protección de datos es uno de los derechos constitucionales más importantes, pero a la vez puede ser entendido como un mecanismo para proteger el derecho a la vida privada. La protección de los datos personales es crucial porque las personas, empresas y hasta el propio estado pueden usar la información personal de manera inapropiada; con el uso inadecuado de la información personal se puede cometer discriminación, agresión, robo de identidad y otros delitos cibernéticos.

Sobre esto, hay que considerar que del derecho a la intimidad se desprende la protección de datos, ya que esta última al alcanzar un gran auge se precisó a nuevas interpretaciones, lo que llevó a una ramificación de derechos como el honor, la imagen, la vida privada y la protección de datos personales. El derecho de protección de datos se basa en el derecho a la intimidad, donde el Estado debe garantizar la protección de la información personal

documental y digital.

La protección de datos significa las medidas legales adoptadas a través de derechos y principios para que la información o los datos personales sean tratados de forma segura y adecuada, estableciendo control sobre el almacenamiento, uso y divulgación de los datos. Por su parte, el derecho a la intimidad personal es un derecho fundamental que todas las personas poseen para controlar su privacidad y decidir la información que se desea compartir con otras personas o entidades. Estos derechos están conectados por el hecho de que el procesamiento inadecuado de los datos personales puede vulnerar la intimidad de las personas.

Siendo la protección de datos uno de los derechos constitucionales primordiales se afirma que:

> La protección de datos personales, aun reconociendo la dinamicidad de su contenido objetivo, derivada de los cambios tecnológicos, garantiza a la persona un poder de control de contenido positivo sobre la captura, uso, destino y posterior tráfico de los datos de carácter personal. Por tanto, este derecho abarca aquellos datos que sean relevantes para el ejercicio de cualesquiera derechos de la persona, sean o no constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar. (Galán, 2005, como se citó en Arellano & Ochoa, 2013)

En el derecho a la protección de datos se funda respectivamente la responsabilidad del Estado para proteger la información personal de forma digital y documental. De tal forma que el propio Estado impone el tratamiento adecuado de los datos personales a empresas privadas y públicas. De ahí que la Organización de los Estados Americanos [OEA] (2022) considera como principios rectores para la protección de la privacidad y la gestión de datos personales los siguientes:

1. Finalidades Legítimas y Lealtad: la información o datos personales recopilados deben

utilizarse únicamente con fines legítimos y a través de medios legítimos.

2. Transparencia y Consentimiento: principio por el cual el individuo tiene la libertad para decidir qué tipo de información desea compartir con el resto. En las empresas este es un principio infaltable, en donde este consentimiento se lo debe hacer de forma escrito, de lo contrario estaría incurriendo en un delito. Además, por este principio se garantiza proporcionar al titular en el momento en que este lo requiera la información acerca de la administración que se le esté dando a sus datos.
3. Pertinencia y Necesidad: los datos personales se deben recopilar si son apropiados, relevantes y limitados.
4. Tratamiento y Conservación Limitados: aquellos encargados de recaudar los datos personales están obligados a cumplir con las políticas de protección de datos, en caso de conflicto deben atenerse a la normativa impuesta por el respectivo Estado y de la forma en que lo establezca la ley.
5. Confidencialidad: los datos personales no deben ser divulgados, ni utilizados para fines distintos a los autorizados, a menos de que exista un consentimiento.
6. Seguridad de datos: se rige por mantener la seguridad del manejo de datos, es decir, la información personal es estrictamente de carácter privado, por lo que se debe crear sistemas aptos que impidan el acceso de esta información a terceros.
7. Exactitud de los datos: los datos deben mantenerse precisos y actualizados para garantizar su veracidad.
8. Acceso, Rectificación, Cancelación, Oposición y Portabilidad: las personas cuyos datos se recopilan deben tener métodos eficaces y gratuitos para acceder, corregir, eliminar, oponerse al tratamiento y, si corresponde, portar sus datos personales.
9. Datos personales sensibles: ciertos tipos de datos sensibles, que pueden causar daño significativo, deben recibir una protección especial, y los responsables deben tomar

medidas de privacidad y seguridad adecuadas.

10. Responsabilidad: los responsables y encargados del tratamiento de datos deben implementar medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de estos principios y cooperar con las autoridades de protección de datos.
11. Flujo Transfronterizo de Datos y Responsabilidad: se fomenta la cooperación entre los Estados para facilitar el flujo transfronterizo de datos y garantizar la responsabilidad de los responsables y encargados del tratamiento que operan en múltiples jurisdicciones.
12. Excepciones: cualquier excepción a estos principios debe estar claramente definida en la legislación nacional y limitarse a razones de seguridad nacional, salud pública, combate a la criminalidad, entre otros.
13. Autoridades de Protección de Datos: los Estados deben establecer órganos de supervisión independientes para monitorear y promover la protección de datos personales, con recursos suficientes y cooperación entre ellos (p.14).

1.2.2. Delitos informáticos relacionados con la protección de datos e intimidad personal

La gama de delitos informáticos que afectan a la protección de datos e intimidad personal existentes en el Ecuador abarca tipos penales como:

- La oferta de servicios sexuales con menores de dieciocho años por medios electrónicos (Art. 174): Este artículo, conocido como grooming, prohíbe la oferta, promoción o publicidad de servicios sexuales con participación de menores de dieciocho años a través de anuncios en línea, redes sociales u otros entornos digitales. Se busca así sancionar al adulto que, mediante estos medios, vulnere las leyes de protección a la niñez y adolescencia.
- Violación a la intimidad (Art. 178): Incurre en este delito quien, sin consentimiento de la víctima, divulgue, distribuya o utilice indebidamente información personal o privada capaz de afectar su intimidad. Por ejemplo, cuando se difunden datos,

imágenes o comunicaciones privadas sin autorización, se atenta contra este derecho fundamental.

- Intercambio ilegal de información de dispositivos móviles (Art. 192): Se prohíbe aquí el intercambio, comercialización o compra no autorizados de datos vinculados a teléfonos u otros equipos móviles. Por ejemplo, números telefónicos, códigos de desbloqueo o cualquier información relacionada sustraída sin consentimiento de su titular.
- Revelación ilegal de bases de datos (Art. 229): Será sancionado con pena privativa de libertad quien, en su propio beneficio o de un tercero, revele indebidamente información almacenada en archivos, bases de datos o sistemas informáticos, vulnerando así la privacidad e intimidad de las personas afectadas.
- Interceptación ilegal de datos (Art. 230): Se establece también una pena privativa de libertad para quien intercepte, desvíe, grabe u observe indebidamente contenidos o transmisiones digitales en tránsito dentro de sistemas informáticos, dispositivos electrónicos o redes de telecomunicación, materializando un tipo de espionaje o fraude informático.
- Integridad de sistemas informáticos públicos (Art. 233): Finalmente, buscando proteger información pública legalmente reservada, se sanciona a los servidores que divulguen indebidamente este tipo de datos confidenciales, poniendo en riesgo la seguridad de las personas afectadas.

En conjunto, esta normativa busca proteger los derechos a la intimidad y protección de datos frente a diversas modalidades de delitos informáticos mediante la imposición de sanciones como penas privativas de libertad. Sin embargo, los datos recopilados por la Unidad de Ciberdelitos de la Policía Nacional demuestran que es muy común sufrir un ataque cibernético hoy en día.

Figura 1.

Denuncias de delitos informáticos 2017- 2023

DELITOS CIBERNÉTICOS DENUNCIADOS EN ECUADOR

Desde 2017 hasta junio 2023

DELITO	2017	2018	2019	2020	2021	2022	2023
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	42	56	55	46	78	84	54
Acoso sexual	12	19	13	10	18	13	10
Apropiación fraudulenta por medios electrónicos	113	158	216	153	896	562	185
Ataque a la integridad de sistemas informáticos	21	16	21	19	32	36	20
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	4	14	8	7	18	15	18
Estafa	139	96	103	105	212	107	36
Intimidación	93	78	95	61	73	58	23
Pornografía con utilización de niñas, niños o adolescentes	27	33	42	35	66	42	23
Suplantación de identidad	9	13	18	10	59	59	18
Violación a la intimidad	50	58	76	101	222	120	49
OTROS DELITOS (actos de odio, abuso de confianza, robo, etc)	199	197	288	135	177	244	137
TOTAL	709	738	935	682	1851	1340	573

Tomado de: *Unidad de Ciberdelitos de la Policía Nacional, Diario el Expreso* (2023).

Como lo indica Ramos (2020), todos estos articulados de la norma penal ecuatoriana son el reflejo de la intención del órgano legislador por regular los delitos de tipo informático, no obstante, esta carece de parámetros técnicos y exigencias normativas internacionales (p. 81).

La Constitución de la República del Ecuador otorga la protección al acceso de las TIC y con ayuda del COIP se busca salvaguardar el bien jurídico de “protección de datos e intimidad personal y familiar”, sin embargo, en esta norma existe una carencia de la individualización de cada tipo penal sobre delitos informáticos, por lo que afectan los derechos constitucionales. Esta categorización inadecuada de los delitos reconocidos en Ecuador se da porque los delitos se encuentran en secciones diferentes, pero a la vez comparten características similares. Además, que genera conflicto en cuanto a la aplicación de estos tipos penales al no adecuar medidas de orden internacional en su normativa.

1.3. Marco Legal

1.3.1. La protección de datos e intimidad personal como bien jurídico protegido en Ecuador

El bien jurídico protegido es un concepto que señala intereses, valores y aspectos de la vida social que las normas jurídicas intentan proteger y conservar mediante regulaciones jurídicas y puniciones, además un bien jurídico puede ser material (vida, propiedad,

patrimonio, salud, etc.) e inmaterial (libertad, honor, intimidad, etc.), a todo esto, se entiende que la protección de datos e intimidad personal y familiar se encuentra dentro del Estado y es amparado por el Derecho (Carrion, 2020).

La protección de datos personales nace como una consecuencia del derecho a la privacidad y la intimidad. Este derecho, que inicialmente se concebía como una protección contra la interferencia en la vida privada, ha evolucionado hasta convertirse en un derecho positivo que permite a las personas controlar el uso de su información personal (*Dictamen No. 13-18-TI/19*, 2019).

Actualmente, los datos personales en Ecuador están protegidos por la acción de hábeas data, que, la Corte Constitucional reconoce como una garantía jurisdiccional que permite a las personas naturales y jurídicas conocer la información que sobre sí mismas reposa en registros o bancos de datos, públicos o privados (*Sentencia No. 182-15-SEP-CC*, 2015). Este derecho tiene como finalidad proteger la privacidad, y permite a las personas rectificar o eliminar información que sea incorrecta o dañina. En un contexto histórico, desde la Constitución de 1998 se procuraba proteger la información personal reservada en instituciones públicas o privadas; fue así como al rigor de este cuerpo normativo surge el hábeas data, como un mecanismo que permitía al titular no solo tener el acceso, el conocimiento del uso que se le da a la información, sino su posterior actualización e incluso anulación.

Con la promulgación de la Constitución de la República del Ecuador del 2008, se da una importante relevancia a la protección de datos y al derecho a la intimidad personal y familiar, acogiendo en su artículo 66, en los numerales 11, 19 y 20 la garantía de reserva respecto a sus datos e intimidad, además se enmarca una diferenciación de esta personal con la información considerada de interés público, ya que esta última es parte del derecho a la información, siendo auxiliar para promover la transparencia. Sobre esto la Corte Constitucional señala que el derecho a la vida privada y familiar exige al Estado el deber no interferir en la

esfera personal y familiar de los individuos, respetando su autonomía y libertad (*Sentencia No. 11-18-CN/19*, 2019).

De los artículos citados merece una mención el numeral 19 del artículo 66, mismo que busca proteger los datos personales por medio de la Constitución, estableciendo que:

> El derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter, y su protección correspondiente. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2021, Artículo 66, numeral 19)

Bajo este parámetro es que la Asamblea Nacional en el 2021 aprobó la Ley de Protección de Datos personales, sin embargo, entró en vigor su régimen sancionatorio el 26 de mayo del 2023, pues se habría dado un plazo prudente para que las empresas públicas y privadas adopten estas disposiciones en sus prácticas; sobre todo esta ley espera proteger a los propietarios de los datos para que puedan elegir quién debe recibir su información personal, ya que confían en los proveedores de servicios digitales. En Ecuador, la protección de datos se basa en la gestión de riesgos para la protección de los derechos y libertades. Se estima que los procedimientos para la seguridad de la información cambien significativamente como resultado de esto.

Analizando esta ley queda por sentando que entre sus principales objetivos está proteger los derechos de los ciudadanos ecuatorianos incluyendo su información personal, para que tengan el acceso y libre decisión de ella. En consecuencia, la ley regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de salvaguardia, además se identifica que varios derechos que se desprenden de los datos personales, tales como: derecho a la información, acceso, eliminación, actualización, suspensión, oposición, portabilidad, consulta,

educación digital y a no ser objeto de una decisión basada en valoraciones automatizadas.

No cabe duda de que el tratamiento de nuestros datos antes de esta ley tenía otro tratamiento, pues ahora se brinda o trata de brindar un tratamiento especializado de ciertas categorías de datos personales, como datos sensibles, datos de niños, adolescentes y de salud, así como datos relativos a personas con discapacidad, asimismo que se hace gran énfasis en el consentimiento y la voluntad del titular de los datos personales para que ponga a disposición su información, evitando inconvenientes a futuro.

Y aunque Ecuador no cuenta con una regulación específica del tema en cuestión, en la búsqueda de la protección de datos se ha valido de instrumentos importantes, empezando por:

- La Declaración Universal de Derechos humanos (1948): específicamente su artículo 12 guarda relación con el derecho a la intimidad, pues en este se impide la intrusión de terceros en la vida privada, familiar, incluso sobre el domicilio de una persona.
- Pacto Internacional de Derechos Civiles y Políticos (1966): el numeral 1 del artículo 17 al igual que la DUDH garantiza el derecho de tener una vida privada y por ende proteger la intimidad personal, el numeral 2 en concordancia con lo mencionado, infiere limites en tanto a la intervención y vigilancia que debe tener el Estado para brindar protección en este ámbito o a su vez sancionar las acciones dolosamente cometidas.
- Convención Interamericana sobre Derechos Humanos (1969) o Pacto de San José: a través de su numeral 2 y 3 de su artículo 11 se pretende prevenir las injerencias abusivas en la vida privada de la persona, de su familia y domicilio, además de precautelar la seguridad de la información personal.
- Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea (2016): por medio de este protocolo el Estado ecuatoriano pretendió mejorar el escenario internacional para el intercambio de bienes y servicios con

países que forman parte de la Unión Europea, pero esto se ha visto limitado porque para cumplir con aquel objetivo se requiere el flujo fronterizo de datos personales, una cuestión que resulta inverosímil en Ecuador al no contar con la normativa que acapare todo este ámbito, lo que crea una desventaja para el país, pues este no es tomando en cuenta y diferentes Estados optan por países latinoamericanos que si cuentan con una legislación especializada, como lo son Colombia y Perú.

- Código Orgánico Integral Penal: Este cuerpo normativo concibe una gama alta de delitos informáticos, pero tipifica aquellas acciones que vulneren los derechos de las personas.
- Código Orgánico Monetario y Financiero: específicamente el artículo 360 establece la protección de la información, prohibiendo el mercadeo de referencias crediticias para un uso diferente al impuesto al tema crediticio.
- Ley Orgánica de Telecomunicaciones (2015): ratifica su artículo 78 el Derecho a la intimidad, el artículo 79 exterioriza sobre el de deber de información, el artículo 80 se enfoca en los procedimientos para la revelación de información, el artículo 82 que habla del uso comercial de estos datos personales junto con el consentimiento previo y expreso del titular de los datos, el artículo 84 manifiesta que la entrega de la información debe ser únicamente a las autoridades competentes bajo el debido proceso.
- Ley Orgánica de Comunicación (2013): sobre el mercadeo indica el artículo 49 que quienes aparezcan en los registros de las bases deberán dar su consentimiento para el uso de datos.
- Ley Orgánica del Sistema Nacional de Registros de Datos Públicos (2010): normativa encargada de regular el registro de datos y el acceso por parte de entidades privadas y públicas, esto está a cargo de la Dirección Nacional de Registro

de Datos Públicos, el artículo 6 especifica el tipo de información que se puede almacenar, siendo datos personales que incluyen información religiosa, política, orientación sexual, salud, status migratorio, y toda aquella considerada de la esfera privada de los individuos, se procura la protección de la Plataforma del Sistema Nacional de Registro de Datos Públicos (SINARDAP) al mismo tiempo que se fortalece la base de datos a escala nacional del Registro Civil, Servicio de Rentas Internas, Agencia Nacional de Tránsito, Instituto Ecuatoriano de Seguridad Social, Consejo Nacional Electoral, etc.

- Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2014): Se protege datos, se regulan los mensajes de datos, la firma electrónica, prestación de servicios, redes de información, etc.
- Ley Orgánica de Protección de Datos Personales (LOPDP) (2021): cuyo objetivo es garantizar la protección de datos, el acceso, rectificación, oposición, eliminación de información errónea y la decisión sobre la información contenida en cualquier base que recolecte datos.

Como se puede apreciar, en Ecuador, se ha implementado medidas para proteger este derecho a la intimidad personal y familiar y los datos personales, en el Código Orgánico Integral Penal específicamente en el artículo 178 se ha establecido una normativa similar a la del país vecino de Colombia, con una pena de uno a tres años para aquel que trasgreda la intimidad de una persona. Cabe señalar que la Constitución del Ecuador en el artículo 66 numeral 18 garantiza el derecho al honor y buen nombre. Es decir, este derecho se empareja aún con más derechos constitucionales, en virtud de que la violación a la intimidad involucra la trasgresión directa a la dignidad, el honor y buen nombre como ya se mencionó con

anterioridad.

1.3.2. La protección de datos e intimidad personal como bien jurídico protegido en Colombia

La noción de expectativa de privacidad e intimidad adoptada por el Estado colombiano se basa en la Sentencia C-881 de 2014 emitida por la Corte Constitucional de Colombia, así como en decisiones de otros tribunales, como la Sentencia 170/2013 del Tribunal Constitucional de España y la del caso Barbulescu contra Rumania (2017) dictada por la Corte Europea de Derechos Humanos. Siendo así que lo considera derechos fundamentales y protegido constitucionalmente. Incluyendo la protección de los datos personales, el acceso a la información pública, la protección de la intimidad personal y familiar y la confidencialidad de la información.

La protección de datos personales siendo uno de los objetos de estudio de la presente investigación se dista por estar regido por una ley estatutaria que establece principios y excepciones claras. Afecta tanto a entidades públicas como privadas y se extiende a tratamientos de datos dentro y fuera del país en ciertos casos. Sin embargo, hay situaciones específicas, como el uso personal o doméstico, que están excluidas de su ámbito de aplicación (*Sentencia T-129/22*, 2022).

La violación del derecho a la protección de datos personales ha ido en aumento de manera alarmante. Según las estadísticas, solamente en el año 2021, la Superintendencia de Industria y Comercio (SIC), entidad encargada de vigilar y sancionar el incumplimiento de las normas sobre protección de datos personales en Colombia, recibió un total de 28.610 quejas relacionadas con este tema. De este total de quejas recibidas por la SIC en 2021, el 90%, es decir, 25.749 de ellas, correspondían a presuntas infracciones a la Ley Estatutaria 1266 de 2008, la principal norma que regula la protección de datos personales en el país.

Cuando hablamos de datos personales e intimidad nos referimos a la esfera privada de

una persona, que puede incluir cosas como información sobre su vida personal, correspondencia y comunicaciones privadas, entre otras cosas. Al posesionar a la protección de datos e intimidad personal como bienes jurídicos nos referimos a que estos son “bienes o interés preexistentes a la norma, pero que son reconocidos por una fuente jurídica superior, que es la Constitución” (Salgado, 2012, p. 154).

Adentrándose un poco en la historia y evolución del Colombia en el ámbito de los delitos informáticos hay hechos importantes como que Colombia fue el primer país latinoamericano en contar con una conexión a internet de alta velocidad, sin embargo, con el aumento de la conectividad empezó una crisis debido a la criminalidad cibernética que iba en aumento, aquello motivó al Estado colombiano a implementar una normativa acorde a los estados soberanos quienes ya habían tipificado las infracciones correspondientes al abuso de los sistemas informáticos y datos personales. Todo esto Carlos Molina en su obra “Un análisis desde el ordenamiento jurídico colombiano” lo detalla, haciendo un énfasis en la evolución de la normativa colombiana entorno a la aparición de los delitos informáticos, es así que esta se dio de la siguiente manera:

Para desarrollar una normativa que proteja a las personas de los delitos informáticos y que se resguarde los derechos constitucionales de protección de datos e intimidad personal y familiar, se creó el decreto 1360 dictado en 1989, el primer acercamiento de Colombia a los delitos cibernéticos. En este se reguló un software que protegería la producción intelectual y aquellos problemas que se suscitan en torno a los derechos de autor. Con esa iniciativa se desprendió varias leyes de apoyo para combatir ciberdelitos que vulneran los derechos de los ciudadanos colombianos.

En el año 2007 mediante el proyecto de ley 042, Colombia tuvo la iniciativa de regular temas de ciberdelincuencia, modificando algunos de los tipos penales regulados en el Título III del libro Segundo del Código Penal, llamado “de la violación a la intimidad, reserva e

interceptación de comunicaciones", endureció las penas para delitos que sean cometidos por medios informáticos como el hurto calificado, daño en bien ajeno, violación de reserva industrial o comercial y el espionaje. De esta manera se estaría protegiendo bienes jurídicos importantes como la intimidad, la propiedad, la competencia y seguridad del Estado.

Después, en el mismo año, se presenta un nuevo proyecto de ley 123, que se oponía al proyecto de ley 042, ya que en este se planteó la creación de un nuevo bien jurídico para la protección de la información y no estaba de acuerdo con la tipificación de los delitos de la ley 042. En un inicio se acumularon los dos proyectos, por lo que se propuso crear el Título VII BIS, parte del Libro Segundo de la Parte Especial del Código Penal, que velaría por la seguridad de la información y los datos, y se apoyaría en los lineamientos regulados por el Convenio de Budapest. El senado no estuvo de acuerdo con los proyectos de ley en conjunto, así que decidieron que para poder aprobarlos lo ideal sería eliminar de los articulados los delitos de: falsedad informática, el de espionaje informático y por último la violación de reserva industrial.

Dos años después, en 2009 se promulgó la llamada "Ley de delitos informáticos" también conocida como "Ley 1237", siendo esta la norma que modificó el Código Penal del país vecino, dándole relevancia y tutelando un nuevo bien jurídico; la información y protección de datos contenidos en los sistemas informáticos, debemos recordar que la ley referida fue expedida gracias a la conjunción de los proyectos de ley 042 y 123. Tras estos hechos Colombia no descartó la cooperación internacional, siendo así que en julio de 2018 el Congreso aprueba una nueva ley "Ley 1928" siendo esta la herramienta para adherirse al Convenio sobre la Ciberdelincuencia, sin embargo como parte de los requisitos el Consejo de Europa solicita que el Estado que ha de querer incorporarse al mencionado convenio ha de presentar un instrumento de adhesión ante el Consejo, en vista de ello la ministra de relaciones exteriores solicito una prórroga para que el país se pueda cumplir con lo requerido.

Con fecha 16 de marzo de 2020 Colombia presenta ante el Consejo Europeo su

instrumento de adhesión, por lo que a partir del 01 de julio de 2020 entró en vigor. No obstante, en el transcurso mientras Colombia preparaba su instrumento y no estaba adherido como tal al Convenio, en la "Ley 1237" supo incorporar términos indispensables del Convenio de Budapest. Lo que ya era un gran avance para proteger los derechos de los ciudadanos colombianos, por lo que la intención del Estado colombiano de salvaguardar la seguridad y protección siempre estuvo presente.

Según Molina (2021) el Convenio al que Colombia se adhirió es imperante, pues:

> En un primer lugar por ser este el único instrumento internacional que abarca todas las áreas concernientes a la ciberdelincuencia (el derecho penal, el derecho procesal penal y la cooperación internacional), y en segundo lugar porque el convenio trata con un carácter prioritario la política penal contra la ciberdelincuencia en cada uno de los Estados parte del mismo. (p. 24)

El Convenio de Budapest es preciso, en él se han intentado incorporar los diferentes delitos informáticos para que los Estados adheridos al convenio puedan mejorar sus respectivas normativas, asumiendo la lucha contra los ciberdelitos. Colombia representativamente ha entablado esta relación y ha fortalecido su legislación. Ciertamente este convenio contiene una parte sustantiva que especifica aquellas conductas que merecen una sanción penal, esto se lo distingue por cuatro grupos; delitos contra la integridad, confidencialidad, disponibilidad de datos y sistemas informáticos; delitos informáticos como: falsificaciones, fraudes; delitos de pornografía infantil; delitos en contra de la propiedad intelectual.

Colombia constantemente a través del Ministerio de Tecnologías de la información y las Comunicaciones promueve programas y políticas públicas que promuevan el uso responsable de las TIC, uno de sus programas destacables es "En TIC confió", está dirigido a toda la población, con esto se quiere concientizar a la ciudadanía, especialmente a los niños y a los adolescentes de los riesgos asociados al uso incorrecto de las TIC, delitos informáticos,

al mismo tiempo se fomenta una cultura de uso responsable y seguro.

La jurisprudencia colombiana reconoce el derecho a la privacidad y la intimidad, aún más en el ciberespacio, especialmente en el contexto de la comunicación por plataformas y redes sociales que es en donde mayormente se difunde fotografías sin el consentimiento del titular, lo cual versa en la vulneración del derecho a la intimidad. Se emplea una "expectativa de privacidad" amplia al analizar posibles vulneraciones de este derecho, considerando la protección contra divulgaciones no autorizadas y las intervenciones arbitrarias de terceros (*Sentencia T-339/22*, 2022).

En ese sentido es prudente mencionar que actualmente Colombia en el artículo 15 de la Constitución Política de la República, tutela el derecho a la intimidad personal y familiar. Esto implica que el Estado debe respetar y hacer respetar este derecho fundamental. Este derecho constitucional tiene una relación de similitud con el derecho a la protección de datos, sin embargo, hay que aclarar que este derecho no lo reconocen las personas jurídicas, se dirige al pleno desarrollo personal y familiar de toda persona natural.

Considerando el impacto y evolución de los delitos informáticos, es que Colombia ha creado normas que protejan el derecho de toda persona a la vida privada y familiar, y se sancione con una pena de entre uno y cuatro años o se le imponga una fuerte multa, si el sujeto activo descubre que actuó con dolo queriendo manipular, almacenar, registrar, usar o transmitir datos personales por medios electrónicos, telemáticos u otros medios informáticos, sin consentimiento. Casos muy particulares se han dado en torno a la violación de este derecho, por ejemplo, la divulgación de videos o fotos íntimas, las grabaciones de llamadas sin consentimiento, instalación de cámaras ocultas, etc.

En términos generales, Colombia cuenta con un marco legal destinado a proteger el derecho a la privacidad y la protección de datos personales de los delitos informáticos. Y como se mencionó con la ley 1273 se pudo incorporar al código penal en el título VII BIS el bien

jurídico “De la protección de la información y de los datos”, reformando la versión del código penal del año 2000, y a su vez incorporando delitos como “el acceso abusivo al sistema informático, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, suplantación de sitios web para capturar datos personales, etc.” (Trávez, 2018).

Es decir, Colombia consideró los problemas existentes y también los futuros respecto a los tipos penales derivados de los delitos informáticos, siendo esta una medida para mitigar afectaciones en los derechos constitucionales, además que su incorporación al convenio de Budapest permitió concentrar sus disposiciones en el código penal colombiano, quedando su relación de la siguiente forma:

Art. 2. Acceso ilícito (Convenio de Budapest) = Art. 269A. Acceso abusivo a un sistema informático (Ley 1273);

Art. 3. Interceptación ilícita (CB) = Art. 269C. Interceptación de datos informáticos (Ley 1273);

Art. 4. Ataques a la integridad de datos (CB) = Art. 269D. Daño Informático (Ley 1273);

Art. 5. Ataques a la integridad del sistema (CB) = Art. 269D- Daño Informático (Ley 1273);

Art. 6. Abuso de dispositivos (CB) = Art. 269E. Uso de software malicioso (CB), Art. 269G.Suplantación de sitios web para capturar datos personales (Ley 1273);

Art. 8. Fraude informático (CB) = Art. 269I. Hurto por medios informáticos y semejantes, Art. 269J. Transferencia no consentida de activos (Ley 1273);

Art. 9. Delitos relacionados con la pornografía infantil (CB) = Art. 218. Pornografía con personas menores de 18 años (Ley 1273), Art. 219A. Utilización o facilitación de medios

de comunicación para ofrecer servicios sexuales de menores (Código Penal);

Art. 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (CB) = Art. 272. Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones (Código Penal).

Considerando la gran clasificación de los datos personales (datos identificativos, laborales, académicos, migratorios, de salud, biométricos, administrativos, jurisdiccionales y patrimoniales), Colombia ha conseguido crear una estructura un tanto más sólido a comparación del resto de países latinoamericanos, pues en su regulación anuncia delitos que en la actualidad son de los más cometidos, de tal forma se ha creado una herramienta para prevenir la violencia digital que trasgrede al derecho a la protección de datos.

Así mismo, en Colombia se desprende un importante avance en materia de delitos informáticos. Pues establece elementos normativos que deben ser cumplidos para la configuración de delitos como el acceso abusivo a un sistema informático, lo que brinda seguridad jurídica a las instancias judiciales que deben juzgar estos delitos. No obstante, también plantea algunos retos pues señala que es necesario incluir un margen de análisis jurisprudencial para estos temas respecto al grado de intensidad de la evaluación jurisprudencial. Esto es necesario para que la corte suprema de justicia pueda brindar una seguridad efectiva sobre delitos cibernéticos novedosos y que no dejen espacio a interpretaciones amplias (Sentencia SP 592/22 (50621), 2023).

Para tratar los delitos informáticos, el Estado colombiano se apoya en la ley 1237 y la ley 1581, la cual permite que quienes hayan sido víctimas de estos delitos presenten una denuncia inmediata, se realice el respectivo proceso con las compañías donde se difundió el contenido, en un tiempo relativamente corto por la situación de gravedad. Esto considerando que cualquier forma del delito informático que trasgreda la intimidad personal es de suma gravedad, pues se despoja la privacidad a una persona, se le causa un daño emocional y una

afectación a su reputación.

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Tipo de investigación

En este apartado se trata de precisar la naturaleza del estudio, es decir, el tipo de enfoque que tendrá el proyecto. El enfoque "comprende todo el proceso investigativo y las etapas y elementos que lo conforman, lo cual implica que cada enfoque tenga características particulares respecto a diversos aspectos de la investigación" (Mata, 2019), es decir, existen dos metodologías: la cuantitativa y la cualitativa. El enfoque cuantitativo utiliza datos numéricos y métodos experimentales, mientras que el enfoque cualitativo emplea técnicas interpretativas y un método más analítico e inductivo para la obtención de resultados.

En ese sentido, el enfoque de esta investigación será cualitativa, por cuanto se analizará y estudiará documentos, libros y demás material bibliográfico (Corona, 2016, p. 2). Este tipo de estudio permitirá una comprensión más completa y profunda del fenómeno analizado, que es el manejo y protección de la protección de datos e intimidad tanto en la legislación ecuatoriana como colombiana. Dado su enfoque, permitirá recopilar, analizar datos y abordar múltiples aspectos del problema de investigación.

2.2. Métodos

Considerando que se trata de un tipo de investigación cualitativa, la obtención de la información se logrará por medio del:

- Estudio descriptivo: Este tipo de estudio tiene como objetivo analizar y describir las características y normas en materia de delitos informáticos contenidas en la legislación ecuatoriana y colombiana y que guarda relación con el derecho a la protección de datos e intimidad personal y familiar. Los estudios descriptivos pueden involucrar la revisión y análisis de informes estadísticos, la recopilación de

datos a través de encuestas o entrevistas, y la revisión de literatura científica previa (Vargas et al., 2015, p. 6).

Por ello, se recopilará datos a través de fuentes primarias y/o secundarias para obtener información detallada sobre las leyes, reglamentos y normativas en ambos países, identificando las disposiciones específicas relacionadas con la protección de datos y la intimidad personal en el ámbito de los delitos informático.

- Estudio histórico: El método o estudio histórico "permite estudiar los hechos del pasado con el fin de encontrar explicaciones causales a las manifestaciones propias de las sociedades actuales" (Dzul, s. f.), el utilizar un enfoque histórico permite comprender de una mejor manera cómo han cambiado los marcos legales en ambos países con relación a los delitos informáticos y la protección de datos.

  El análisis de leyes anteriores, reformas legislativas y precedentes históricos puede proporcionar una visión más completa sobre los fundamentos y propósitos de las disposiciones actuales y revelar el contexto en el que se han desarrollado las normativas actuales. Esto ayudará a contextualizar y comprender mejor las leyes vigentes, así como su aplicabilidad y relevancia en el entorno actual.

- Estudio hermenéutico: La hermenéutica es "el arte de interpretar textos, principalmente los de tipo religioso o filosófico. Este método implica que cualquier cosa puede ser comprensible a partir de métodos que lleven el pensamiento a la interpretación" (Monroy & Nava, 2018, p. 99), por eso este estudio es útil para comprender y analizar las disposiciones legales que protegen los datos y la intimidad personal en el marco de los delitos informáticos.

  La interpretación de textos legales y su aplicación práctica son el centro de la hermenéutica. La intención legislativa y los principios interpretativos utilizados en la aplicación de las leyes en casos particulares se pueden examinar examinando la

legislación y la jurisprudencia relevante. Esto permitirá una interpretación crítica de las disposiciones legales y su relación con la protección de datos e intimidad personal, lo que enriquecerá el análisis y los hallazgos de la investigación.

2.3. Técnicas y Materiales

2.3.1. Técnica

En la presente investigación sobre la garantía del cuidado de información personal y los delitos informáticos en Ecuador y Colombia, se utilizarán diversas técnicas que proporcionen información relevante y actualizada. Se incluyen en este apartado:

- Revisión documental: Esta estrategia requiere la recopilación y análisis de leyes, reglamentos, jurisprudencia, doctrina jurídica, informes gubernamentales y otros documentos pertinentes en ambos países sobre delitos informáticos, protección de datos e intimidad personal. La revisión documental proporcionará una base sólida para comprender el marco legal actual y las disposiciones relacionadas con la protección de datos en el contexto de los delitos informáticos.

  Para eso, para el estudio de leyes, se empleará la revisión de textos normativos tales como la Constitución de la República del Ecuador (2008) y la Constitución de Colombia, el Código Orgánico Integral Penal (2014), al igual que la normativa que involucra el tratamiento de protección de datos personales (Ley Orgánica de Protección de Datos Personales) en Ecuador, y por supuesto el Convenio de Budapest.

- Entrevistas: Se entiende a la entrevista como “uno de los instrumentos de recolección de datos más utilizados para la investigación cualitativa, principalmente por su enfoque personal” (QuestionPro, s. f.), aquí el entrevistador o el investigador recoge los datos directamente del entrevistado. Es por ello por lo que la realización de entrevistas con especialistas en derecho penal, derecho informático y protección

de datos en Ecuador permitirá obtener conocimientos prácticos y perspectivas especializadas sobre el tema de investigación. Estas entrevistas, serán semiestructuradas, proporcionarán información cualitativa que ayudará a enriquecer el análisis y las conclusiones de la investigación.

La técnica por emplear en este proyecto de investigación se apoyará en un cuestionario. Sirviendo como técnica de investigación óptima en este caso para recopilar información relevante que será obtenida de juristas y profesionales expertos en la protección de datos personales, privacidad e intimidad personal. Es importante que los profesionales entrevistados posean conocimiento sobre las TIC, derecho informático y demás materias relacionadas a la protección de datos e intimidad personal en el mundo digital que actualmente estamos viviendo, para que así aporten significativamente a esta investigación.

2.3.2. Instrumento

Respectivamente se empleará el cuestionario, en donde el investigador se reúne con el informante, el cual debe contar con información y experiencia sobre el tema de estudio que permita conocer aspectos de primera mano del problema (Monroy & Nava, 2018). En virtud de ello, se formulará de una serie de preguntas no estructuradas (preguntas abiertas) a los profesionales del derecho, quienes son conocedores de delitos informáticos, temas de interés penal, derecho constitucional, derecho informático, etc., con el objetivo de recabar información, conocer sus criterios y opiniones respecto a la normativa vigente en ambos países sobre delitos informáticos y protección de datos personales.

2.3.3. Población

En el caso del estudio sobre la garantía a la protección de datos e intimidad personal en el marco legal de los delitos informáticos en Ecuador y Colombia, la población versa sobre un

total de 4 profesionales del derecho tanto de Ecuador como de Colombia, quienes tienen conocimiento de las causas sobre delitos informáticos y las distintas normas que los regulan.

2.3.4. Muestra

Se ha seleccionado como muestra a 2 profesionales ecuatorianos, residentes en la ciudad de Quito, bajo los siguientes criterios:

- Dr. Bryan Rurales: Abogado en el libre ejercicio de profesión. Especialista en el área corporativo empresarial, en materia penal y penal económico puro. Se inclina por ramas orientadas a la parte del crecimiento del neuro derecho, de la neurociencia. Actualmente es investigador de dos instituciones, una a nivel nacional y otra a nivel internacional, en el tema del derecho cibernético. Su experticia enriquecerá mi investigación al brindarme valiosa información que aborde los desafíos relacionados con la privacidad y la protección de datos en la era digital y el tratamiento que deberían recibir los mismos.
- Dr. Daniel Mejía: Analista de Privacidad-Tecnología, abogado destacado en la rama de derecho constitucional y penal. Con su basto conocimiento en el ámbito del derecho constitucional sabrá facilitar aportes significativos sobre la importancia de garantizar el derecho a la protección de datos e intimidad personal. Además, proporcionaría una crítica sobre la efectividad de las leyes y políticas existentes en el marco de la protección de datos, lo que me permitirá realizar una evaluación fundamentada de las fortalezas y debilidades del marco legal existente.

Así mismo, se ha seleccionado como muestra a 2 profesionales colombianos, bajo los siguientes criterios:

- Dr. Javier Guatame: Experto en ciberseguridad y protección de datos personales. Siendo así será de gran valor entrevistar a esta profesional con conocimientos especializados, que además podrá ofrecer una perspectiva regional y un enfoque

específico sobre la evaluación de la normativa y políticas de protección de datos manejado en Colombia.

- Dra. Zoila Cabrera: abogada especialista en derecho informático, derecho penal y constitucional. Posee experiencia a nivel internacional en casos delitos informáticos, por lo que, con la información obtenida por medio de la entrevista, se podrá hacer una evaluación detallada estas disposiciones legales y las medidas de protección de datos de Ecuador y Colombia, lo que ayudará a comprender las diferencias y similitudes en las leyes y regulaciones de ambos países en relación con la ciberseguridad, datos, e intimidad personal y familiar. Cumpliendo así con uno de los objetivos del proyecto de investigación que es evaluar las fortalezas y debilidades de cada marco legal y analizar aquellas bases de prevención y protección de datos personales más efectivas de la legislación colombiana que podrían ser implementadas en Ecuador.

Al tratarse de una población pequeña y precisa, es decir que no supera las 30 personas no es necesario utilizar la fórmula, porque se analizará a la totalidad de los individuos.

CAPÍTULO III: RESULTADOS Y DISCUSIÓN

3.1. Resultados

3.1.1. Entrevistas realizadas a los profesionales ecuatorianos

Tabla 1

Pregunta 1. *¿A qué se refiere el derecho a la protección de datos?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	La Protección de Datos como tal hace referencia a aquella cuestión o fuente de derecho personal, que tenemos las personas para poder controlar la información personal recopilada sobre en diferentes bases de datos, asegurando o respaldando el tema de seguridad y privacidad.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Es la disciplina jurídica que se dedica al estudio del derecho a la protección de datos personales y privacidad dentro de una realidad globalizada.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 2

Pregunta 2. *¿Qué es la intimidad personal y familiar y por qué es importante protegerlo?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	La intimidad personal y familiar se enmarca en el esquema de la Protección de Datos. Hace referencia al ámbito específico de la vida privada, incluye aspectos de privacidad en el hogar, privacidad con la familia, y el tema de correspondencia hoy en día a nivel cibernético. Se debe proteger para garantizar el respeto a la persona, esto nos permitiría que incluso el panorama de la Protección de Datos sea bien llevado.
Dr. Daniel Mejía	La intimidad personal hace referencia a una dimensión de información relativa a aspectos de

Analista de Privacidad-Tecnología. Experto en derecho constitucional.	carácter personal, con un nivel alto de privacidad. La intimidad familiar hace referencia a una dimensión de información relativa a los nexos familiares y consanguíneos que pueda tener un titular de la información con otros seres humanos, y que tiene un nivel alto de privacidad.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 3

Pregunta 3. *¿El derecho a la protección de datos e intimidad personal y familiar tienen un vínculo entre sí?*

ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	Sí, la protección de datos y la intimidad personal y familiar están sumamente ligadas, estrechamente vinculadas. Tenemos privacidad las personas como tal en diferentes ámbitos de la vida y obviamente en base a toda la información que deviene o se desprende de esto. Y sobre todo porque estamos hablando de elementos que van desde el aspecto más íntimo de la persona y que incluso trascienden al esquema familiar o al vínculo, al núcleo.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Si. Compréndase que un dato personal es toda aquella información que hace identificable a un ser humano. Esto quiere decir que, existen subcategorías de datos personales que tienen una relación estrecha con la intimidad personal y familiar. En esa misma línea, un dato personal está protegido por un sistema de derechos y garantías, incluyendo aquellos datos relativos a la intimidad familiar y personal. .

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 4

Pregunta 4. *¿Cuáles son las diferencias más destacadas entre la vulneración de estos derechos en el ámbito físico y en el ciberespacio?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	En el ámbito físico, la vulneración de derechos se puede ilustrar o se puede ver en el en el momento en el que una persona logra irrumpir o logra involucrar el espacio personal propio. En el aspecto físico, nosotros sabemos hasta dónde está ese límite y el momento en el que se transgrede se puede tipificar o se puede sancionar en base a un tipo penal. En el esquema cibernético propiamente no implicaría tanto el aspecto personal, el límite personal, sino el al acceso no autorizado a la información personal, que es un elemento totalmente diferente. O sea, no puedes simplemente acceder a una información porque quieres, sino que debes tener y tiene que ser consensuado y autorizado propiamente en el tema cibernético.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Para dar respuesta a esta pregunta, se identificarán dos diferencias: 1. Considerando que la sociedad cada vez aumenta su capacidad tecnológica, y enfoca su actividad política para brindar mayor acceso a las nuevas tecnologías, puede que los ciberataques se conviertan en una conducta común y cotidiana, promoviendo una evolución negativa de las vulneraciones de forma física frente al tratamiento de datos personales. 2. Una diferencia sustancial son los mecanismos y alternativas para resolver una vulneración física y una digital. Por ejemplo, las alternativas para mitigar un ciberataque, requiere de una intervención técnica enfocada al software del repositorio digital que fue vulnerado. Por otro lado, las alternativas para mitigar una vulneración física puede ser medidas de seguridad enfocadas al hardware del repositorio digital afectado.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 5

Pregunta 5. *¿Cuál es la normativa que actualmente regula el derecho a la protección de datos y respectivamente el derecho a la intimidad personal y familiar?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	- Constitución de la República del Ecuador. - Ley Orgánica de Protección de Datos. - Código Orgánico Integral Penal.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	- Constitución de la República del Ecuador - Derecho a la protección de datos personales / Habéas Data. - Ley Orgánica de Protección de Datos Personales. - Código Orgánico Integral Penal, para luchar contra los delitos informáticos. - Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional - Habeas Data.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 6

Pregunta 6. *Tomando en cuenta la rápida evolución de la tecnología, ¿Cree que la normativa actual es suficientemente flexible y adaptable para abordar los desafíos futuros respecto a delitos informáticos?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	En el ámbito penal es flexible porque permite avanzar, evita que las rompamos y además varía con el derecho. La normativa en el Ecuador sí está en constante avance, constante revisión, sin embargo, siempre existe el margen de que se pueda mejorar y para mejorar, pues debe entenderse que la normativa debe adaptarse o tratar de adaptarse al crecimiento rápido que tiene la tecnología, más no a la conducta de la persona, sino a entender qué es lo que va a poder

	pasar con el paso acrecentado que tiene la tecnología, que este es un aspecto que carece un poco el Ecuador.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	No lo es. Existe una falta de practicidad del marco normativo que regula los delitos informáticos y la protección de datos personales. Por esa razón, la mayoría de delitos informáticos pueden quedar impunes frente a la falta de investigación técnica que tiene el sistema judicial o administrativo de Ecuador.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 7

Pregunta 7. *¿Cuáles cree usted que son las fortalezas y debilidades del marco legal en relación con los delitos informáticos?*

ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	Son fortalezas que el panorama de la Protección de Datos que hace tiempo atrás no se consideraba como algo importante o valioso hoy en día se busque proteger. Como debilidades está la capacidad de la aplicación efectiva de la norma, es decir, carecemos de una norma clara, una que contemple una conducta específica, entonces estamos a un hablando de un contexto macro en donde no existe como tal esa tipificación. A esto se suma que muchas veces nuestras instituciones públicas tienen aún muy ligado y arraigado un sistema muy antiguo. Esto refriéndose a las autoridades, ya sea por falta de recursos, capacitación, no han podido adaptarse a la era tecnológica.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Fortaleza: El marco regulatorio actual es un antecedente perfectible, con bastantes insumos que podrían robustecer la protección de datos personales y la lucha contra los delitos informáticos.

	Debilidad: La falta de practicidad dentro del sistema de protección de datos personales y el sistema judicial - penal han causado la impunidad en la investigación de delitos informáticos.

Fuente: *Entrevistas realizadas a los profesionales del derecho, ecuatorianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 8

Pregunta 8. *¿Considera que la cooperación internacional juega un papel importante en la lucha contra los delitos informáticos y la protección de derechos constitucionales?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	Sí. Tomando en cuenta que el tema informático trasciende fronteras físicas en cuestión de segundos, o sea, no hay una barrera física como tal en el tema digital, entonces sí, la cooperación internacional es crucial para poder defender esto, y ya lo hemos visto hoy en día, incluso las redes en el tema de tráfico de datos, delitos sexuales, pornografía se están resolviendo a través de la colaboración internacional donde obviamente se valen de los elementos de tecnología para perseguir a estos grupos que realizan estos actos delincuenciales.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Sí, siempre y cuando, no sacrifique la soberanía del Estado. La intervención de la comunidad internacional requiere de un análisis sociológico sobre la protección de datos personales y delitos informáticos, y así poder brindar su cooperación y colaboración para construir una cultura de protección de datos personales.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por*: Inés Sánchez*

Tabla 9

Pregunta 9. *¿Está familiarizado con las estrategias y políticas gubernamentales sobre delitos informáticos? ¿Cree que estas son difundidas adecuadamente por el gobierno?*	
ENTREVISTADO	**RESPUESTA**

Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	Por el desempeño de mi trabajo sí estoy familiarizado, pero en el tema de Ecuador es un tema que se podría fomentar un poco más en especial para la población civil, que incluso desconoce de la normativa, esto incluso fortalecería la conciencia pública.
Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Si estoy familiarizado. Lamentablemente, no han existido campañas adecuadas para sociabilizar las estrategias y políticas gubernamentales para combatir los delitos informáticos. El derecho a la educación digital, previsto en la Ley Orgánica de Protección de Datos Personales, es una deuda pendiente para el Estado

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 10

***Pregunta 10.** En el marco de la norma, ¿qué políticas públicas debe implementarse?*	
ENTREVISTADO	**RESPUESTA**
Dr. Bryan Ruales Especialista en derecho penal. Investigador de derecho cibernético.	Primero deberíamos basarnos en diferentes países que tienen un nivel mucho más amplio en este esquema, como México y Estados Unidos que tienen instituciones especializadas como el Instituto de Investigaciones Jurídicas, entonces ellos hacen elementos de investigación a nivel tecnológico y obviamente esto trasciende en el País y les permite tener políticas gubernamentales mucho más constituidas, mucho más firmes. Así mismo, el caso de España que tiene un buen enfoque en proteger el derecho a la intimidad, hasta el punto de que dedicó una ley específica para este derecho fundamental. De igual forma se debe trabajar la educación en el tema digital, la concientización sobre la ciberseguridad, la prevención de delitos informáticos y políticas que permitan la cooperación internacional.

Dr. Daniel Mejía Analista de Privacidad-Tecnología. Experto en derecho constitucional.	Lo importante sería dar seguimiento a las políticas públicas que han sido promulgadas con anterioridad.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

3.1.2. Entrevistas realizadas a los profesionales colombianos

Tabla 11

***Pregunta 1.** ¿A qué se refiere el derecho a la protección de datos?*	
ENTREVISTADO	**RESPUESTA**
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Es el derecho que permite a los titulares la información personal, conocer el uso que se le va a dar por parte de las entidades que la requieren
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional. .	Es la facultad otorgada a las personas con la garantía de que sus datos, información personal será resguardada.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 12

***Pregunta 2**. ¿Qué es la intimidad personal y familiar y por qué es importante protegerlo?*	
ENTREVISTADO	**RESPUESTA**
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Es la reserva que se debe tener frente a la información personal o familiar que solo les interesa a ellos, y que ellos comparten si lo desean. Por ejemplo, la orientación sexual, las relaciones interpersonales, etc.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Es un derecho que garantiza que todas las personas tenemos la posibilidad de aquello que está en nuestra esfera más íntima, la esfera personal, la esfera familiar, pueda ser sacado del escrutinio público y mantenido en la propia conciencia de la persona.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*

Elaborado por: Inés Sánchez

Tabla 13

Pregunta 3. *¿El derecho a la protección de datos e intimidad personal y familiar tienen un vínculo entre sí?*	
ENTREVISTADO	**RESPUESTA**
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Sí, la reserva que se debe tener sobre la información por parte del custodio y los derechos del titular para modificar, borrar o actualizarla.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Sí, doctrinariamente son derechos complementarios.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 14

Pregunta 4. *¿Cuáles son las diferencias más destacadas entre la vulneración de estos derechos en el ámbito físico y en el ciberespacio??*	
ENTREVISTADO	**RESPUESTA**
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	- Permisos de acceso - Almacenamiento - Tiempo de vigencia
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	En el ámbito físico hablamos de la teoría de las esferas, y esta surge hace varias décadas por la intromisión del Estado en la vida privada de los ciudadanos. La intimidad en entornos digitales se da porque estamos hiperconectados y estamos bajo lo que se denomina una sociedad red.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
Elaborado por: Inés Sánchez

Tabla 15

Pregunta 5. *¿Cuál es la normativa que actualmente regula el derecho a la protección de datos y respectivamente el derecho a la intimidad personal y familiar?*	
ENTREVISTADO	**RESPUESTA**
	- Ley 1581 de 2012

Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	- Constitución - Ley 1266 que protege los datos personales financieros.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	- Constitución Política de Colombia, artículo 15 (1991). - Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección y tratamiento de datos personales. - Ley 1273 de 2009, por la cual se tipifican y sancionan delitos informáticos.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 16

***Pregunta 6.** Tomando en cuenta la rápida evolución de la tecnología, ¿Cree que la normativa actual es suficientemente flexible y adaptable para abordar los desafíos futuros respecto a delitos informáticos?*

ENTREVISTADO	RESPUESTA
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Considero que en Colombia hay una ley que permite adaptarse a las diferentes tecnologías, además de las tareas que realiza la SIC como ente vigilante.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Es una normativa óptima, pero nunca hay que descartar la evolución del marco legal en especial cuando se habla de delitos informáticos que avanzan a diario.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 17

***Pregunta 7.** ¿Cuáles cree usted que son las fortalezas y debilidades del marco legal en relación con los delitos informáticos?*

ENTREVISTADO	RESPUESTA
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Como fortaleza las definiciones de los derechos y deberes que se tienen frente a la protección de datos, las debilidades es que es difícil demostrar negligencia o incumplimiento de la ley

Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Fortalezas se puede considerar los convenios internacionales que Colombia hace, junto con las políticas públicas que desarrolla y debilidades sería que la norma debe evolucionar constantemente y se debe capacitar a los profesionales en temas relevantes de delitos informáticos.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 18

***Pregunta 8.** ¿Considera que la cooperación internacional juega un papel importante en la lucha contra los delitos informáticos y la protección de derechos constitucionales?*

ENTREVISTADO	RESPUESTA
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	Es vital, porque debe haber una sinergia que permita una colaboración entre los países de tal manera que los ciberdelincuentes no hagan sus fechorías en países donde no hay leyes o son muy laxas afectando los países vecinos. Por lo que debe ser una lucha en común.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Sí, siempre es indispensable que exista una cooperación internacional entre todos los países a través de las fiscalías de cada país, a través de la policía, Interpol o todos sus organismos para que puedan coordinar acciones.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 19

***Pregunta 9.** ¿Está familiarizado con las estrategias y políticas gubernamentales sobre delitos informáticos? ¿Cree que estas son difundidas adecuadamente por el gobierno?*

ENTREVISTADO	RESPUESTA
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	En la experiencia que he tenido, considero que se ha realizado un buen trabajo al respecto. Pero, debe fortalecerse la socialización para que los ciudadanos las conozcan.

Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Sí, el ámbito de mi trabajo me obliga a mantenerme informada, pero para el ciudadano común muchas veces es desconocido, a pesar de que hay normas y procedimientos para su difusión.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

Tabla 20

***Pregunta 10.** En el marco de la norma, ¿qué políticas públicas debe implementarse?*	
ENTREVISTADO	**RESPUESTA**
Dr. Javier Guatame Experto en ciberseguridad y protección de datos personales.	- Campañas de comunicación. - Programas educativos y la formación de profesionales en esta materia. - Fortalecimiento de las instituciones encargadas de la protección de la intimidad, como la Superintendencia de Industria y Comercio y la Fiscalía General de la Nación.
Dra. Zoila Cabrera Abogada especialista en derecho informático, derecho penal y constitucional.	Primero implementar herramientas tecnológicas. Y de políticas públicas es indispensable las capacitaciones gratuitas a centros estudiantiles, los gobiernos autónomos descentralizados, charlas de cómo darles un buen uso a las redes sociales, así mismo, charlas para aumentar el tema de la seguridad respecto de las contraseñas, y datos personales.

Fuente: *Entrevistas realizadas a los profesionales del derecho, colombianos, juristas y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad*
***Elaborado por**: Inés Sánchez*

3.1.3. Marco legal referente al derecho a la intimidad y protección de datos personales en la esfera de delitos informáticos

Tabla 21. Comparativa de la normativa, regulaciones, políticas públicas y estrategias

ECUADOR		COLOMBIA	
INTIMIDAD PERSONAL Y FAMILIAR			
Constitución de la República del Ecuador *(Art. 66, numeral 20)*	Reconoce y garantiza en uno de sus numerales el derecho a la intimidad personal y familiar.	***Constitución Política de Colombia*** *(Art. 15)*	Se reconoce el derecho a la intimidad personal y familiar, junto a este derecho en el mismo artículo se reconoce el derecho al hábeas data como una autodeterminación informativa.
Código Orgánico Integral Penal *(Sección sexta – Delitos contra el derecho a la intimidad personal y familiar)*	Tipifica: Art.178. La violación a la intimidad, con una pena de 1 a 3 años a aquel que acceda, intercepte, examine, retenga, grabe, reproduzca o difunda sin autorización datos personales, mensajes de datos, voz, audio, video, información en soporte informáticos, comunicaciones privadas o reservadas; Art. 179. Revelación de secreto o información personal de terceros, como estado, oficio, profesión, (prisión de 6 meses a 1 año), o contenido digital	***Ley 599 de 2000 - Código penal*** *(Capítulo Séptimo- De la violación a la intimidad, reserva e interceptación de comunicaciones)*	Tipifica: Art.192. La violación ilícita de comunicaciones, el que sustraiga, oculte, extravíe, destruya, intercepte, controle e impida una comunicación privada no dirigida al infractor; así mismo, el enterarse indebidamente del contenido de una comunicación privada (Prisión de 1 año y 4 meses a 4 años y 6 meses). Son agravantes el revelar el contenido de la comunicación, emplear la información de la comunicación para beneficio propio o de terceros y causar prejuicio a otro utilizando la información de la comunicación (Prisión de 2 años y 8 meses a 6 años);

íntimo de carácter sexual (prisión de 1 a 3 años), sin embargo, se señala que si lo revelado es de interés público no se estaría incurriendo en delito;

Art. 180. Difusión de información de circulación restringida, se refiere a la información protegida por cláusula de reserva legal, la producida por fiscalía en investigación previa, sobre niñas niños y adolescentes (prisión de 1 a 3 años).

Art.193. Se sanciona económicamente a quienes comercialicen con dispositivos para interceptar comunicaciones privadas sin autorización legal, protegiendo así la privacidad y la confidencialidad de las comunicaciones entre individuos, a menos que exista una disposición que contemple una pena más severa para la misma conducta;

Art.194. La Divulgación y empleo de documentos reservados, la norma busca proteger la confidencialidad de ciertos documentos, penalizando su divulgación o uso indebido con una multa, pero si la divulgación o su empleo constituye un delito más grave en otro artículo o ley, se aplicará la sanción correspondiente a ese delito y no la multa mencionada;

Art.196. La violación ilícita de comunicaciones o correspondencia de carácter oficial, se sanciona la sustracción ilícita, ocultamiento, extravío intencional, destrucción, interceptación, control no autorizado, impedimento de la comunicación o correspondencia de información generada o recibida por entidades gubernamentales o

			administrativas (Prisión de 4 a 9 años); Art.197. La utilización ilícita de equipos transmisores o receptores, se sanciona la posesión o uso de equipos de comunicaciones o medios electrónicos, específicamente aquellos diseñados o adaptados para emitir o recibir señales, cuando se hace con fines ilícitos (Prisión de 4 hasta 8 años)
Código de la Niñez y Adolescencia *(Art.251)*	Se establecen las infracciones contra el derecho a la intimidad y a la imagen, en los casos en que: Los medios de comunicación difundan información que permita identificar a un menor involucrado en un proceso penal, o a su vez publiquen datos, imágenes, audios que identifiquen a menores víctimas de maltrato o abuso sexual; Cuando funcionarios públicos divulguen antecedentes policiales o judiciales de adolescentes; Cualquiera que use la imagen de un menor en medios de comunicación o	***Ley 1098 de 2006 - Código de la Infancia y la Adolescencia*** *(Art. 33)*	Los niños, niñas y adolescentes gozan del derecho a la intimidad personal; se brinda protección contra injerencias arbitrarias en su vida privada, la de su familia, domicilio y correspondencia; son protegidos de aquellas conductas que afecten su dignidad.

	publicidad sin autorización; La persona natural o jurídica que distorsione ridiculice o explote la imagen de menores con discapacidad. Para los casos mencionados se impone una multa de $100 a $500.		
Código Orgánico Administrativo *(Art. 24)*	Las administraciones públicas que manejen información personal deben hacerlo protegiendo la intimidad de las personas y el respeto a su vida privada.	***Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo*** *(Art. 24)*	La norma clasifica ciertos tipos de información y documentos como reservados por razones de seguridad nacional, privacidad, competencia económica, entre otros. Además, restringe el acceso a dicha información, exigiendo que solo ciertas personas con autorización o relación directa puedan solicitarla. Es información y documentos reservados Documentos e informaciones relacionados con la seguridad del Estado y sus operaciones de defensa; Instrucciones y detalles de operaciones diplomáticas o negociaciones que no son públicas; Datos personales que incluyen hojas de vida, historias laborales, expedientes pensionales, registros de particular e historias clínicas; Detalles de las operaciones de crédito público y tesorería, con

			reserva de 6 mesespost-operación; Informaciones que afectan la competitividad de empresas de servicios públicos; Información protegida por la confidencialidad inherente a ciertas profesiones; Información relativa al ADN y la genética de individuos.
		Ley 906 de 2004 - Código de Procedimiento Penal *(Art. 14)*	Se reconoce el derecho a la intimidad de cada persona, se prohíbe la molestia a las personas en su vida privada sin justificación legal. Para intervenir en la intimidad de una persona (registros, allanamientos en domicilios o lugares de trabajo) se necesita la orden escrita del Fiscal General de la Nación.
PROTECCIÓN DE DATOS PERSONALES			
Constitución de la República de Ecuador *(Art.66. numeral 20)*	Garantiza el derecho a la protección de datos personales, considerando su acceso, decisión y protección. Así mismo se exige la autorización del titular para el manejo y difusión de la información.	***Constitución Política de Colombia (Art. 15)***	Como se mencionó con anterioridad este artículo reconoce indirectamente el derecho al hábeas data como una autodeterminación informativa y forma de garantizar los datos personales.
Ley Orgánica de Protección de Datos Personales *Disposiciones (Art. 23)*	En general obliga a las empresas que disponen de los datos personales a cumplir con medidas de	***Ley Estatutaria 1581 de 2012 - Disposiciones generales para la***	Establece el estándar general para proteger los datos personales. El propósito de esta ley número 15 de la Constitución, establecer el derecho de todas las personas a

seguridad para salvaguardar estos. Regula la transferencia de los datos e información solicitada por empresas; el plazo de conservación de datos; responsabilidad para bloquear o destruir los datos. Lo particular de esta Ley es que adicionalmente promueve el derecho a la educación digital, se garantiza el acceso y la disponibilidad de conocimiento relacionado con el uso responsable de la idiosincrasia, destaca la importancia de la inclusión y sensibilización en el ámbito de la protección de datos. El sistema educativo nacional, incluyendo el superior se compromete a garantizar la educación digital tanto a estudiantes, personas con necesidades educativas especiales y a los docentes. Este derecho debe ser ejercido teniendo en cuenta los derechos	***protección de datos personales***	conocer, actualizar y rectificar las informaciones que se hayan recopilado sobre ellas en bases de datos o archivos, así como los demás derechos, libertades y garantías constitucionales relacionados con la protección de los datos personales y la intimidad personal. Además, establece los estándares para el tratamiento de datos personales, las obligaciones de quienes los tratan, los derechos de los titulares de la información y las sanciones por no cumplir con las regulaciones, entre otros temas relacionados con la protección de datos personales.

fundamentales, libertades especialmente respecto a la intimidad, vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital.		
	Ley 1266 de 2008	Art.2. La ley reconoce la existencia de normas especiales que protegen la confidencialidad o reserva de datos en bancos de datos públicos, especialmente para fines estadísticos, investigación, sanción de delitos, garantía del orden público. Art.4. Establece principios para asegurar que la administración de datos personales sea precisa, legítima, y protegida contra accesos no autorizados. Estos principios buscan proteger la privacidad y derechos de los individuos en el manejo de su información particular. Art.5. La circulación de información particular está regulada y sujeta a condiciones específicas para proteger los derechos de los titulares. Es necesario verificar la finalidad de la circulación de datos y cumplir con los procedimientos establecidos para cada tipo de receptor. La

			autorización del nominal es un elemento clave en la circulación de datos, salvo en circunstancias específicas previstas por la ley.
DELITOS INFORMÁTICOS Y COOPERACIÓN INTERNACIONAL			
Ley Orgánica de Telecomunicaciones y Tecnologías de la Información y Comunicación (LOTTC)	Esta ley regula el uso de Ecuador de la tecnología de la información y la comunicación. Incluye temas de seguridad de la información, protección de datos personales, prevención de delitos informáticos y cooperación entre organizaciones para combatirlos. El artículo 1 garantiza el derecho a la protección de datos personales, que incluye el acceso y la toma de decisiones sobre datos personales y su correspondiente protección. El artículo 78 reconoce el derecho a la intimidad y el artículo 79 aborda el deber de información. El artículo 80 se centra en cómo revelar datos personales.	***Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest)***	Es el primer tratado internacional que aborda delitos informáticos y ciberdelincuencia, estableciendo un marco legal para la cooperación internacional en la lucha contra estos delitos. Aspectos importantes: - Definición de Delitos Informáticos: El convenio aborda la definición de delitos informáticos, incluyendo aspectos como el daño informático, sabotaje y ataques a la integridad de los datos, entre otros. - Infracciones Reguladas: El convenio regula una serie de infracciones relacionadas con la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Estas infracciones incluyen el hurto por medios informáticos, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva artificial o comercial valiéndose de medios informáticos, entre otros.

	El artículo 82 establece que las y los prestadores de servicios no pueden utilizar datos personales ni información sobre el uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que aquel haya dado su consentimiento previo y expreso.		- Implementación en la Legislación Nacional: En algunos casos, se ha mencionado la proposición de crear un título específico en el Código Penal, destinado a la salvaguarda de la información y los datos, tomando como base las conductas reguladas en el Convenio sobre la Ciberdelincuencia de Budapest.
Ley de comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	Art. 9. Indica cómo se protegerá datos, se regulan los mensajes de datos, la firma electrónica, prestación de servicios, redes de información, etc.	***Tratado de Asistencia Legal Mutua en Asuntos Penales entre los Estados Parte de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC)***	El objetivo de este acuerdo es mejorar la colaboración y ayuda legal entre los países integrantes de la CELAC en cuanto a asuntos penales. El objetivo principal del tratado es ayudar a los Estados a trabajar juntos para prevenir, investigar y perseguir delitos penales, incluidos los delitos informáticos y otros delitos transnacionales. Esto incluye el intercambio de información y pruebas, el apoyo en investigaciones y procedimientos penales, y la extradición de sospechosos o condenados por delitos.

Código Orgánico Integral Penal *(Sección Tercera - Delitos contra la seguridad de los activos de los sistemas de información y comunicación)*	Art. 174. Tipifica la oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. Art. 190. Sanciona a aquel que se apropie de información personal a través de medios electrónicos. Art. 192. Hace énfasis sobre el intercambio o comercialización de información de equipos móviles. Sección Tercera Art. 229. Prohíbe la revelación no autorizada de información registrada en sistemas electrónicos, con penas de uno a tres años, aumentando a tres a cinco años si es cometida por un servidor público o empleados bancarios. Art.230. Sanciona con tres a cinco años la interceptación ilegal de datos y actividades como diseñar páginas electrónicas fraudulentas. Art.231. Penaliza la alteración de sistemas	**Ley 599 de 2000 - Código Penal** (Adicionado por: Art 1 Ley 1237 de 2009) Título VII BIS -De la Protección de la información y de los datos. CAPITULO I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.	Art. 269 A. Acceso abusivo a un sistema informático. Conducta típica: El acceder sin autorización o más allá de la autorización concedida a un sistema informático; Mantenerse dentro del sistema informático contra la voluntad del titular del derecho de exclusión. (Prisión de 4 a 8 años) (multa de 100 a 1.000 salarios mínimos) Art. 269 B. Obstaculización ilegítima de sistema informático o red de telecomunicación Conducta Típica: Impedir u obstaculizar sin autorización el funcionamiento o acceso a: sistema informático, datos informáticos contenidos en el sistema, red de telecomunicaciones (Prisión de 4 a 8 años) (multa de 100 a 1.000 s.m.l.m.). Art. 269C. Interceptación de datos informáticos Conducta Típica: Interceptación de datos informáticos sin orden judicial, ya sea en: origen, destino, dentro del sistema informático, emisiones electromagnéticas que transporten los datos (Prisión de 3 a 6 años). Art. 269 D. Daño Informático. Conducta Típica: Sin autorización, realizar alguna de las siguientes

informáticos para la transferencia no consentida de activos, imponiendo la misma pena por facilitar datos bancarios con fines ilícitos.

Art.232. Aborda la destrucción de datos informáticos, programas maliciosos y afectación a bienes públicos con penas de tres a cinco años y si hay agravantes de cinco a siete años.

Art.233. Castiga la destrucción de información clasificada y la obtención ilegal por parte de servidores públicos.

Art.234. Prohíbe el acceso no autorizado a sistemas informáticos, con penas de tres a cinco años.

acciones: destruir, dañar, borrar, deteriorar, alterar, suprimir datos informáticos, afectar un sistema de tratamiento de información o sus componentes lógicos (Prisión de 4 a 8 años y una multa de 100 a 1.000 salarios mínimos).

Art. 269E. Uso de Software Malicioso.

Conducta Típica: producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer software malicioso o programas dañinos sin autorización (Prisión de 48 a 96 meses y una multa de 100 a 1.000 salarios mínimos).

Art. 269F.Violación de Datos Personales. Conducta Típica: obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear códigos o datos personales sin autorización, buscando provecho propio o de un tercero (Prisión de 48 a 96 meses) (multa de 100 a 1.000 s.m.).

Art. 269G. Sobre la suplantación de Sitios Web

Conducta Típica: Diseñar, desarrollar, traficar, vender, ejecutar, programar o enviar páginas electrónicas, enlaces o ventanas emergentes sin

autorización y con fines ilícitos; Modificar el sistema de resolución de nombres de dominio para redirigir usuarios a una IP fraudulenta, simulando ser un banco o sitio de confianza (Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos).

Art. 269H. Circunstancias de agravación punitiva. Se establece circunstancias específicas que, de presentarse, incrementan la severidad de las penas para delitos informáticos y contra la seguridad de sistemas y redes de información. Las penas de los delitos informáticos se aumentarán entre un 50% y un 75% si el delito se comete en alguna de las siguientes condiciones:

1.Redes/Sistemas Estatales o Financieros: Si el delito afecta redes o sistemas informáticos estatales, oficiales o del sector 76 financiero, ya sean nacionales o extranjeros.

2.Funcionarios Públicos: Cuando el autor del delito es un servidor público y lo comete en ejercicio de sus funciones.

3.Abuso de Confianza: Si se aprovecha la confianza del poseedor de la información o existe

un vínculo contractual.
4.Divulgación de Información: Cuando se revela o da a conocer información con intención de perjudicar a otra persona.
5.Beneficio Propio o de Terceros: Si se busca obtener un provecho económico o de otra índole para sí mismo o para terceros.
6.Fines Terroristas o de Riesgo Nacional: Si el delito tiene objetivos terroristas o compromete la seguridad o defensa nacional.
7.Uso de Terceros de Buena Fe: Cuando se involucra a un tercero que desconoce la naturaleza ilícita de la acción.
8.Responsables de la Información: Si quien comete el delito es responsable de la administración, manejo o control de la información, se le puede inhabilitar hasta por tres años para ejercer profesiones relacionadas con sistemas de información computarizados. (Aparte del aumento de la pena carcelaria, si el responsable del delito es quien administra la información afectada, podría enfrentar una pena adicional de inhabilitación profesional de hasta tres años).

		CAPITULO II De los atentados informáticos y otras infracciones.	El artículo 269I establece el hurto por medios informáticos. Conductas comunes: violar sistemas informáticos o redes electrónicas; infringir medidas de seguridad informáticas; manipular sistemas o redes; suplantar a un usuario en sistemas de autenticación. (Prisión de 6 a 14 años). El artículo 269J. Tipos de comportamiento: transferir activos sin consentimiento a través de manipulación informática o métodos similares, con fines lucrativos y en perjuicio de terceros; fabricar, introducir, poseer o facilitar software destinado a cometer el delito de transferencia no consentida o estafa. Si la cantidad de delitos cometidos supera los 200 salarios mínimos legales mensuales, la pena se aumentará en un 50%.
POLÍTICAS PÚBLICAS			
Plan Nacional de Seguridad Integral *(2019 – 2030)*	Es una política que busca la coordinación de actividades de todas las partes interesadas relevantes en seguridad cibernética, quienes deberían tener funciones, responsabilidades	***CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa***	Este documento busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa).

	respaldadas en sus competencias y con capacidades operativas suficientes.		
***Plan Específico de Defensa Nacional** (2019-2030)*	Indica que el ciberespacio es un también una unidad del territorio ecuatoriano. Las implicaciones están vinculadas al desarrollo de operaciones en este ámbito para defender la soberanía, con el fin de contribuir a la ciberseguridad nacional.	***CONPES 3854 Política Nacional de Seguridad Digital.***	Pretende mejorar las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital en un marco de cooperación, colaboración y asistencia. A fin de impulsar el crecimiento de la economía digital a nivel nacional, lo que a su vez conducirá a una mayor prosperidad económica y social.
***Plan Específico de Seguridad Pública y Ciudadana** (2019-2030)*	La implementación de políticas coordinadas y articuladas de prevención y control en relación con las diversas manifestaciones del delito y sus ámbitos permite la prevención, anticipación y lucha contra las amenazas locales, nacionales e internacionales. La distinción entre la seguridad pública y la seguridad ciudadana permite un enfoque	***CONPES 3995 Política Nacional de Confianza y Seguridad Digital.***	El objetivo es implementar acciones para fomentar la confianza digital a través de la mejora de la seguridad digital, con el fin de crear una sociedad inclusiva y competitiva en el futuro digital. Para lograr esto, Colombia debe fortalecer sus capacidades y actualizar su marco de gobernanza en seguridad digital, además de adoptar modelos enfocados en nuevas tecnologías.

	diferente en la suscitación de delitos. La seguridad ciudadana se centra en las acciones institucionales para reducir los factores que predisponen al cometimiento de delitos, mientras que la seguridad pública se centra en la protección del orden público y la seguridad interna.		
Plan Específico de Relaciones Exteriores y Movilidad Humana *(2019-2030)*	Objetivo Estratégico 3: Promover la cooperación internacional para combatir la delincuencia organizada transnacional y las amenazas a la seguridad nacional.	***Documento 3988 de 2020 dnp Tecnologías para aprender: política nacional para impulsar la innovación en las prácticas educativas a través de las tecnologías digitales***	Es una política nacional que estimula las prácticas educativas a través de las respectivas tecnologías digitales. Tiene un horizonte de ejecución hasta el año 2024 y cuenta con cuatro objetivos específicos relacionados con acceso a tecnologías, conectividad a Internet, apropiación de tecnologías digitales, y el monitoreo y evaluación del uso, acceso, e impacto de estas.
Política Ecuador Digital	Tiene 3 ejes Ecuador Conectado; Ecuador Eficiente y Ciberseguro; Ecuador Innovador y Competitivo.	***Documento 3975 de 2019 dnp Política nacional para la transformación***	Se centra en el uso estratégico de tecnologías digitales, involucrando al sector público y el sector privado con énfasis en el uso de las TIC como herramientas para impulsar la productividad y favorecer el

	Cada eje incluye un conjunto de proyectos para aumentar el acceso a las tecnologías de la información y comunicación, fortalecer las capacidades del talento humano, potenciar los sectores económicos e impulsar el emprendimiento y la innovación. El eje de acción "Ecuador Eficiente y Ciberseguro" garantiza la participación ciudadana, la democratización de los servicios públicos, la simplificación de trámites, la gestión de la seguridad de la información y la protección de datos personales.	***digital e inteligencia artificial***	bienestar de los ciudadanos, quienes son los beneficiarios y consumidores de estos servicios.
Política Pública por una Internet segura para niños, niñas y adolescentes	Es un instrumento cuyo objetivo es proteger la dignidad e integridad física, psicológica, emocional y sexual de los niños, niñas y adolescentes, y potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales.	***CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa***	Este CONPES busca crear el ambiente y las condiciones necesarias para brindar protección al Estado en el ciberespacio.

Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica *(2019 – 2030)*	Versa sobre una estrategia que permite prepararse con anticipación. Establece en su Objetivo 7: Implementar acciones públicas para enfrentar riesgos y amenazas, fundamentalmente los relacionados con el crimen organizado, el lavado de activos, la delincuencia transnacional, el terrorismo y la cibercriminalidad.	***Resolución 3484 de 2012 Portal Colombia TIC***	Es un sistema de información integral, que reúne datos, variables e indicadores sobre el sector de las TIC, con el fin de socializar a la ciudadanía información de interés como las metas, programas, metas actuales y proyectos referentes a las TIC. https://colombiatic.mintic.gov.co/679/w3-channel.html
Estrategia Nacional de Ciberseguridad del Ecuador *(2022-2025)*	PILAR 1 Gobernanza y coordinación nacional. Objetivo1.1 Establecer un marco de gobernanza sobre ciberseguridad. Objetivo1.2 Fomentar una comunidad sólida y articulada con expertos en ciberseguridad de las múltiples partes interesadas. Objetivo1.3 Desarrollar un marco legal y regulatorio que permita la gobernanza nacional de la ciberseguridad y ciberdefensa. PILAR 2 Resiliencia cibernética.	***Estrategia Nacional de Ciberdefensa y Ciberseguridad*** *(2020-2030)*	OBJETIVO GENERAL Garantizar y proteger la utilización segura del ciberespacio por parte de los ciudadanos y de la Nación, mediante el despliegue de las capacidades de defensa y seguridad del Estado, que permita mitigar los riesgos y amenazas mediante un trabajo coordinado y de cooperación, que contribuya al crecimiento económico y social del país. OBJETIVOS ESPECÍFICOS Objetivo 1 Fortalecer la confianza y la seguridad digital de los individuos y de la Nación, a través de la anticipación y prevención, de los riesgos identificados en el

Objetivo2.1 Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para afrontar ataques cibernéticos con el fin de fortalecer dichas capacidades a nivel nacional.

Objetivo2.2 Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información crítica nacionales.

Objetivo2.3 Continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos y del CERT nacional.

Objetivo2.4 Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia.

PILAR 3 Prevención y combate a la ciberdelincuencia.

Objetivo 3.1: Actualizar el ciberespacio, generando la cultura ciberseguridad.

Objetivo 2 Fortalecer la legislación, la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad, desde un enfoque de seguridad pública(ciudadana), garantizando los derechos fundamentales en el espacio digital.

Objetivo 3 Protección y seguridad de activos estratégicos y críticos del país, incluidos los ciberactivos.

Objetivos 4 Promover la cooperación interinstitucional y de los sectores público y privado para la protección del ciberespacio.

Objetivo 5 Promover la cooperación internacional y adhesión de Colombia a iniciativas de ciberseguridad y ciberdefensa.

Objetivo 6 Sensibilizar, concientizar, promover la educación y la cultura de ciberseguridad.

	marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio. Objetivo 3.2: Se enfoca en endurecer los aforos estratégicos de investigación sobre la cibercriminalidad.
	PILAR 4 Ciberdefensa Objetivo 4.1 Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, con el fin de proteger la infraestructura crítica digital (ICD) y los servicios esenciales en el ciberespacio.
	PILAR 5 Habilidades y capacidades de ciberseguridad Objetivo 5.1 Mejorar y ampliar la concientización sobre la ciberseguridad a

	todos los niveles de la sociedad. Objetivo 5.2 Reforzar las habilidades sobre ciberseguridad. Objetivo 5.3 Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad. PILAR 6 Cooperación internacional Objetivo 6.1 Identificar las prioridades internacionales de Ecuador y participar en la ciberdiplomacia regional e internacional. Objetivo 6.2 Fortalecer la participación de Ecuador en la cooperación bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio.	
	PROGRAMAS DIRIGIDOS A LA CIUDADANÍA	
	Respecto a Ecuador ha sido complejo encontrar programas que el gobierno desarrolle en beneficio de la población. Son asociaciones privadas como la Asociación Ecuatoriana de Protección	***1,2,3, X TIC*** Ayuda a los niños, niñas desde los 6 años hasta los adolescentes, jóvenes y adultos para mejorar sus habilidades digitales y gestionar su relación con las TIC para su uso seguro.

de Datos y la Asociación Ecuatoriana de Ciberseguridad que por su propia cuenta socializan talleres dirigidas a la comunidad. Se ha podido evidenciar de un taller "Taller académic o sobre Delitos Informáticos y Evidencia Electrónica" impartido por el consejo de la judicatura, pero únicamente a los jueces anticorrupción y servidores judiciales.		
	Teletrabajo incluyente y seguro	Promover el uso de las TIC en diversas formas de trabajo no presenciales para aumentar la productividad tanto en instituciones públicas como privadas y fomentar una cultura de ciberseguridad en las empresas privadas.
	Legado de Gabo	Para investigar, contar y compartir historias a partir del uso y la apropiación de las TIC, se crean espacios de reflexión, formación e intercambio de experiencias sobre el legado de Gabriel García Márquez. (Obligación establecida por la Ley 1741 de 2014).
	Dirección de Economía Digital	Énfasis de habilidades digitales a través de cursos cortos gratuitos

"Generación TIC"	para niños, niñas, estudiantes de 10 a 11 años, jóvenes y adultos. Pensamiento computacional, fundamentos de programación, uso y apropiación de herramientas digitales básicas, lenguaje de programación, analítica de datos, Inteligencia Artificial, Internet de las cosas, aplicación de las TIC para el agro y la economía popular, ciencia de datos y ciberseguridad son algunas de las temáticas disponibles en este programa.
En TIC confío	Este es un programa del MinTIC y promueve el uso seguro y responsable de las TIC. Este programa tiene como objetivo ayudar a las personas a desenvolverse e interactuar de manera responsable con las TIC, brindándoles herramientas para enfrentar con seguridad los riesgos asociados al uso de estas, como el grooming, el sexting, el acoso cibernético, la dependencia cibernética y los materiales de abuso sexual de niñas, niños y adolescentes.
Te protejo	Esta es una línea de reporte donde los ciudadanos pueden denunciar problemas que afecten a menores de 18 años, principalmente

contenido de pornografía infantil y explotación sexual de menores.

Fuente: *Comparativa del marco legal respecto al derecho a la intimidad y delitos informáticos*
***Elaborado por**: Inés Sánchez*

3.2. Discusión

Una vez analizada la actual normativa de Ecuador y Colombia y realizada las entrevistas a los profesionales del derecho y especialistas en causas de delitos informáticos y vulneraciones al derecho a la intimidad tanto de Ecuador como en Colombia se procede a hacer un análisis de los criterios obtenidos considerando que su conocimiento y experiencia fundamenta la veracidad de la información obtenida. Se toma en cuenta los criterios sugeridos por cada entrevistado a fin de contrastar sus respuestas y responder la pregunta del problema de la presente investigación, la cual es *¿Cómo garantiza el Estado ecuatoriano el derecho a la protección de datos e intimidad personal y familiar ante los delitos informáticos y qué aspectos se puede tomar como base de la legislación colombiana?*, así mismo en este capítulo se pretende dar cumplimiento a los objetivos planteados en este proyecto de investigación.

Internet y las tecnologías de la información y la comunicación han transformado la forma en que llevamos a cabo nuestras actividades diarias. Estas herramientas se han vuelto indispensables en nuestra sociedad actual. Sin embargo, a medida que nos adentramos en una era digital que sabemos no va a retroceder, también debemos ser conscientes de los desafíos y riesgos asociados con su mal uso. Es crucial estar informados sobre los delitos informáticos, ya que representan una amenaza directa a los derechos constitucionales de las personas. Mantenernos actualizados y preparados nos ayudará a proteger nuestra seguridad y privacidad en este entorno digital en constante evolución. Referente a ello Ecuador y Colombia han reconocido la gravedad de los delitos informáticos y han implementado normativas para

abordarlos. Sin embargo, existen diferencias significativas entre las legislaciones de ambos países.

Una de estas diferencias radica en la manera en que se tipifican y organizan estos delitos. En el caso de Ecuador, la normativa relacionada con los delitos informáticos se encuentra dispersa y desordenada en diferentes artículos del COIP, lo que genera confusión y dificultades en su identificación, interpretación y aplicación. Esto también complica el proceso legal y reduce la visibilidad de estos delitos en el marco legal. De las entrevistas realizadas los abogados ecuatorianos indican que al menos en el ámbito penal la norma es flexible lo que permitiría que esta esté en constante avance y constante revisión, porque el mundo del derecho no puede detenerse, las conductas de las personas van cambiando, se van repitiendo, se van formando y por lo mismo es importante que estas sean regularizadas; caso contrario estaríamos hablando de un libre albedrío que ocasionaría una situación social muy grave.

Por otro lado, Colombia determina en un solo capítulo y clasifica a cada uno los delitos informáticos de manera adecuada y aborda una amplia variedad de ellos, incluyendo la protección de grupos vulnerables como los menores de edad. Tener una organización adecuada y una correcta tipificación de los delitos informáticos ofrece claridad, facilita la persecución efectiva, protege a las víctimas y contribuye a prevenir y disuadir estos actos ilícitos. Esto garantiza un marco legal sólido y eficiente en la lucha contra los delitos informáticos.

En ese sentido y considerando que los delitos informáticos afectan derechos importantes como los estudiados en este proyecto de investigación, se determina, por un lado, que la Constitución de Ecuador reconoce la intimidad personal y familiar y la protección de datos personales como derechos constitucionales que deben ser garantizados por el Estado, mientras que la Constitución de Colombia reconoce el derecho a la intimidad como un derecho fundamental, pero no menciona explícitamente la protección de datos personales.

Sin embargo, la jurisprudencia colombiana ha interpretado que el derecho a la intimidad abarca la protección de datos personales, de modo que si se afectan los datos personales de los ciudadanos afectan directamente su derecho a la intimidad, además Colombia reconoce en el mismo artículo el Hábeas Data como una autodeterminación informativa, mientras que Ecuador reconoce a este en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Sobre esto tanto los abogados ecuatorianos como colombianos comparten esta noción, determinando el vínculo permanente entre estos dos derechos constitucionales que se complementan y que si son bien garantizados permitirían un mejor equilibrio en la esfera personal, protección de datos y todo el esquema que deviene de ellos.

En el ámbito normativo del derecho a la intimidad, Colombia destaca por tipificar al menos seis delitos contra la intimidad en su Código Penal, agrupados en el "Capítulo Séptimo, el mismo que habla de la violación a la intimidad, la reserva e interceptación de comunicaciones". Por otro lado, Ecuador contempla únicamente tres acciones en su Código Orgánico Integral Penal. Esta diferencia sugiere que contar con una mayor tipificación de delitos brinda ventajas al garantizar una mayor protección de los derechos ciudadanos y la seguridad de la información. Al ampliar la tipificación de delitos, se dificulta que los delincuentes informáticos queden impunes, ya que sus acciones tienen más probabilidades de ser consideradas como delitos, adicional a esto hay que reconocer que en términos de penas y sanciones Colombia ha incrementado estas casi el doble de la máxima pena que se rige en Ecuador, por ende, son más duras.

Sobre esto ambos países consideran importante proteger a los niños, niñas y adolescentes, por eso Colombia, a través de la Ley 1098 de 2006, establece medidas de protección para niños, niñas y adolescentes en el ámbito de la intimidad. Ecuador, por su parte, aborda la protección de menores en su Código de la Niñez y Adolescencia, imponiendo

sanciones económicas por la difusión de información que permita identificar a menores involucrados en procesos penales o víctimas de maltrato.

Respecto a esto hay un punto negativo, y es que ambas legislaciones carecen de una ley específica que regule de manera exhaustiva la intimidad personal y familiar, confiando principalmente en sus constituciones y códigos penales. Sobre esto, la abogada Zoila Cabrera indicó que se debería tomar como ejemplo el caso de España que a diferencia de estos países ha implementado dos leyes: la ley de protección de datos y la ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen., 1982).

Contar con una ley dedicada exclusivamente a este tema sería beneficioso, ya que establecería de manera precisa los casos en los que se ve comprometido el derecho a la intimidad. Además, brindaría un marco legal claro para el procedimiento, incluyendo la posibilidad de otorgar indemnizaciones, medidas cautelares para las víctimas, entre otros aspectos. Asimismo, se le daría la importancia adecuada a este derecho constitucional que cada vez está más expuesto a posibles vulneraciones cibernéticas.

Inclusive en la esfera de la administración pública, Colombia regula la clasificación y restricción de acceso a ciertos tipos de información a través de la Ley 1437 de 2011. Ecuador, por otro lado, aborda la protección de la intimidad en el ámbito administrativo a través del Código Orgánico Administrativo (Artículo 24), enfatizando la necesidad de manejar información de tipo personal con respeto a la privacidad de cada ciudadano.

En el mismo hilo de investigación, sobre las divergencias entre la normativa referente a la protección de datos personales estas son notorias, a pesar de que ambos países manejan leyes específicas para regular este derecho Colombia ha sabido incorporar al menos tres normativas con diferentes disposiciones, pero que de forma resumida garantiza el acceso,

actualización de la información personal y añade protecciones para los datos en bancos públicos y circulación de información.

En cambio, en Ecuador para garantizar la protección de datos personales cuenta con una sola normativa, que es la recién expedida LOPDP, no obstante, a través de otra normativa promueve activamente la educación digital para asegurar el uso responsable de las TIC, mostrando un enfoque integral hacia la privacidad en el entorno digital. Es decir que esta ley está bastante elaborada, pero existe confusión en tanto a los procedimientos y métodos para hacer cumplir los derechos de ley, pues no existe un reglamento que lo complemente, como en el caso de Colombia bajo la ley 1273 y 1581 que determina una responsabilidad penal, administrativa, contractual, económica y bancaria.

La creación de cuerpos normativos en la legislación de un país es trascendente; el propio estado mediante reglas establece parámetros aplicables a todos los ciudadanos sin excepción alguna, a fin de garantizar la seguridad y protección de los derechos constitucionales. Esto además de brindar seguridad permite fomentar un ambiente que mejore la calidad de vida de los ciudadanos. Cada país diseña su normativa con base en las necesidades de su población, sin embargo, el desarrollar políticas públicas y estrategias dirigidas a la ciudadanía es igualmente trascendental.

Sobre ello, en políticas públicas en materia de ciberseguridad y tecnologías digitales en Ecuador y Colombia revelan enfoques y prioridades distintas. Colombia destaca por sus políticas públicas, que abordan la ciberseguridad y ciberdefensa como componentes críticos para la seguridad nacional y la prosperidad económica. La Política Nacional de Seguridad Digital, la Política Nacional de Confianza y Seguridad Digital, y la Estrategia Nacional de Ciberdefensa y Ciberseguridad buscan fortalecer capacidades, promover la seguridad digital a la ciudadanía y fomentar la confianza en el entorno digital. Colombia también apunta al uso

estratégico de tecnologías digitales en sectores como la educación, impulsando la innovación y la transformación digital.

Por otro lado, Ecuador, sus planes estratégicos reconocen el ciberespacio como un componente clave para la defensa de la soberanía, destacando la importancia de la ciberseguridad en la estrategia nacional. La Política Ecuador Digital y la Estrategia Nacional de Ciberseguridad del Ecuador refuerzan estos esfuerzos al promover la educación digital, fortalecer la gobernanza y resiliencia cibernética, así como prevenir y combatir la ciberdelincuencia. Además, se enfoca en la cooperación internacional para abordar amenazas transnacionales. De esto el abogado Bryan Ruales sugiere un esquema como el de México y Estados Unidos para contar con instituciones especializadas como el Instituto de Investigaciones Jurídicas para la realización de investigaciones tecnológicas.

En términos de cooperación internacional, ambas naciones buscan fortalecer sus lazos, pero mientras Ecuador destaca la lucha contra la delincuencia organizada transnacional, Colombia amplía su enfoque a la adhesión a diferentes iniciativas internacionales y la participación en la ciberdiplomacia regional. Se debe destacar que, en el caso de Ecuador, la participación ciudadana y la protección de datos personales son elementos centrales, mientras que Colombia muestra una diversificación de sus políticas, abordando aspectos clave como la educación, la seguridad y la transformación digital en sectores específicos.

Por último, y de lo más importante hallado en esta investigación es que en cuanto a los programas dirigidos a la ciudadanía en Ecuador y Colombia, se observan diferencias significativas en términos de alcance y enfoque. En Ecuador, la información disponible indica que el gobierno no ha implementado programas específicos dirigidos a la ciudadanía en el ámbito de la ciberseguridad o el uso responsable de las TIC. En su lugar, se destaca la participación de asociaciones privadas.

En contraste, Colombia presenta una variedad de programas con un alcance más amplio y diverso. Iniciativas como “1,2,3, X TIC” buscan fortalecer las competencias digitales de ciudadanos de diferentes edades, fomentando el uso seguro y efectivo de las TIC. El programa “Teletrabajo incluyente y seguro” promueve la utilización de tecnologías para modalidades laborales no presenciales, incentivando la productividad y la cultura de ciberseguridad en el ámbito laboral. Además, programas como “Generación TIC” ofrecen formación en habilidades digitales a través de cursos gratuitos en diversas temáticas para niños, adolescentes, jóvenes y adultos.

Colombia también cuenta con programas específicos como “En TIC Confío” y “Te Protejo”, que se centran en la promoción del uso seguro y responsable de las TIC, abordando temas críticos como el ciberacoso, la explotación sexual de menores, y proporcionando una línea de reporte para denunciar situaciones que afecten a menores de 18 años. Estos programas reflejan un enfoque integral hacia la protección de la ciudadanía en el entorno digital, abordando tanto aspectos educativos como de seguridad.

En resumen, mientras Ecuador muestra una participación más limitada del gobierno en programas específicos dirigidos a la ciudadanía, Colombia ha implementado una serie de iniciativas con un enfoque más amplio y diversificado. Y por supuesto las consecuencias de no difundir información tan importante sobre los delitos informáticos y el manejo correcto de las TIC son graves; puede dificultar la prevención de estos delitos, obstaculizar la investigación y el enjuiciamiento de los responsables de estos delitos y por último puede problematizar la protección de las víctimas de estos delitos, lo que hace que actualmente sean más comunes ser víctima de cualquier tipo de delito informático.

CAPÍTULO IV: CONCLUSIONES

- Los resultados de la investigación revelan que los delitos informáticos aprovechan las oportunidades que brindan las tecnologías de información y comunicación (TIC). Si bien estas tecnologías han impulsado positivamente el mundo digital facilitando actividades y creando servicios que mejoran nuestra vida, trabajo y habilidades sociales, también generan vulnerabilidades que permiten el acceso no autorizado a datos confidenciales, hasta delitos sumamente graves como el ciberacoso. Algunos sujetos encuentran en ello una vía sencilla para cometer delitos informáticos, siendo que esta es una forma más sencilla de delinquir principalmente porque es de difícil rastreo.
- Con el apoyo de la bibliografía estudiada y el análisis de la normativa queda en evidencia el grave impacto negativo de estos delitos sobre toda persona o entidad usuaria de las TIC. Los ciudadanos son los más afectados, ya que son las principales víctimas de robo de datos personales y ciberacoso. No obstante, también se registran serias consecuencias para las empresas debido a que pueden tener pérdidas económicas por el robo de información confidencial o el sabotaje de sus sistemas informáticos. En el caso del Estado puede sufrir daños en su reputación. En conjunto, este tipo de actos ilícitos representan serias amenazas a los derechos, la seguridad y el sustento económico de la sociedad.
- La doctrina y jurisprudencia estudiada manifiesta que los derechos a la protección de datos personales y la intimidad personal y familiar están ligados; se basan en la salvaguarda de la información privada de las personas y en garantizar que la información sensible no sea utilizada de manera indebida. Ambos derechos se fundamentan en el respeto y la preservación de la intimidad de las personas, así como en su capacidad para controlar y decidir sobre el uso de su información. Aclarando que la protección de datos también se considera una libertad informática, ya que nosotros

proporcionamos libre y voluntariamente ciertos datos a empresas con fines específicos para que sean tratados de forma lícita y segura. A diferencia del derecho a la intimidad en el ámbito de los delitos informáticos, siendo que este último se refiere a una esfera privada e íntima que se ve vulnerada cuando un tercero sin consentimiento accede a nuestra intimidad utilizando herramientas tecnológicas para cometer delitos como robo de datos, información, suplantación de identidad, etc.

- Con el objetivo de salvaguardar el derecho a la protección de datos personales y la intimidad personal y familiar, Ecuador y Colombia han mostrado un interés en fortalecer su legislación en materia de delitos informáticos, poniendo especial énfasis en la protección de los derechos constitucionales. En este sentido, es destacable el enfoque adoptado por Colombia al momento de sancionar acciones delictivas que involucran el uso de medios tecnológicos, ya que no solo se impone una pena privativa de libertad, sino que también se busca reparar integralmente a las víctimas mediante medidas pecuniarias. En contraste, en Ecuador solo se contempla la privación de libertad como medida punitiva.
- Al analizar el impacto de los delitos informáticos en derechos fundamentales como la protección de datos personales y la intimidad personal y familiar, se llega a la conclusión de que en Ecuador no se brinda una garantía completa a la protección de estos derechos. Las sanciones impuestas son considerablemente bajas, llegando incluso a ser un 50% menor que las mínimas aplicadas en Colombia. Además, es inquietante la falta de tutela judicial por parte del Estado hacia las víctimas de delitos informáticos, ya que la legislación actual se ha mantenido inalterada y no puede hacer frente de manera adecuada a los nuevos tipos de delitos informáticos, lo cual dificulta la aplicación de la ley.

- Con relación a los Convenios Internacionales, es importante destacar que Ecuador a pesar de que en su normativa indique que fomenta la cooperación internacional no se ha adherido al Convenio de Budapest, el cual es considerado de gran importancia para combatir delitos cibernéticos. Esta situación ha provocado que Ecuador no cuente con las herramientas y mecanismos para combatir eficazmente los delitos cibernéticos, además, al no formar parte de este acuerdo, el país se encuentra un tanto excluido de la cooperación y el intercambio de información con otros países que sí están suscritos, lo que dificulta la investigación y persecución de los delitos informáticos a nivel internacional. Por otro lado, la adhesión de Colombia a este convenio ha tenido resultados positivos, como la modificación de su código penal para incluir una mayor variedad de delitos informáticos, sanciones fuertes, y un marco legal más sólido y actualizado.
- La mejor manera de garantizar los derechos a la protección de datos personales e intimidad personal y familiar frente a los delitos informáticos va más allá de tipificar conductas, la protección efectiva ante estas amenazas demanda políticas integrales de prevención y concientización ciudadana por parte del Estado. Esto se logra a través de la implementación de políticas públicas y estrategias dirigidas a la ciudadanía, que permiten prevenir y enfrentar de manera efectiva los delitos informáticos y proteger la privacidad de los ciudadanos.
- En cuanto a las políticas públicas, Ecuador las incorpora con una duración prolongada, a diferencia de Colombia. Por un lado, una política de larga duración permite una implementación más sólida y sostenible, ya que se dispone de tiempo suficiente para evaluar su impacto y realizar los ajustes necesarios. Sin embargo, una política de corta duración puede ser más ágil y adaptable a los cambios rápidos en la sociedad y las necesidades de la población. Se destaca el interés del Ecuador por desarrollar normativa

en ciberseguridad del Ecuador, sin embargo, esto no se cumple porque hasta la actualidad esa normativa es escasa y solo se encuentra en el COIP. Por otro lado, las políticas públicas de Colombia se enfatizan por concientizar, promover la cultura de ciberseguridad y la dependencia digital, al igual que sus estrategias dirigidas a la ciudadanía, que al menos en el caso de Colombia hay una gran variedad.

RECOMENDACIONES

- Al haber finalizado este proyecto de investigación, se resalta y se sugiere que este trabajo sea tomado en cuenta como un precedente investigativo para futuros proyectos y artículos científicos relacionados con delitos informáticos, derechos constitucionales como la protección de datos personales y la intimidad personal y familiar. De esta manera, se podrá continuar avanzando con las variables que se abordan, con el objetivo de resolver el problema jurídico planteado y reducir sus efectos e impacto en la sociedad.
- Ante el aumento de los delitos informáticos, es imprescindible que tanto Ecuador como Colombia actualicen y evolucionen su normativa de manera constante para enfrentar los desafíos emergentes. Esto implica la necesidad de revisar y modificar la tipificación de los nuevos delitos informáticos, así como establecer sanciones adecuadas que disuadan a los posibles infractores y protejan a la sociedad de los riesgos asociados a la ciberdelincuencia. Además, la incorporación de una ley especial dedicada a la intimidad personal y familiar coadyuvaría a proporcionar un marco legal más completo y actualizado que aborde los desafíos y riesgos emergentes con relación a este derecho, de tal forma también se establecerían medidas más efectivas para prevenir y sancionar cualquier acto que vulnere directa o indirectamente la intimidad personal y familiar.
- La falta de tutela judicial genera un ambiente de impunidad y desprotección para las personas afectadas, quienes no encuentran respuestas ni soluciones a sus problemas. Es necesario que se realicen actualizaciones y modificaciones en la legislación penal actual para adaptarse a los avances tecnológicos y garantizar una justicia efectiva en el ámbito de los delitos informáticos. Debido a que se estaría proporcionando herramientas legales actualizadas a jueces y fiscales para investigar y sancionar adecuadamente estos casos, lo cual reduciría la impunidad en casos de delitos informáticos y por lo tanto

tendría un efecto disuasorio en potenciales delincuentes informáticos. Además, que incluir una sanción pecuniaria que cubra la reparación integral de la víctima resulta favorecedor y sobre todo contribuiría a promover la justicia y resarcir los daños sufridos.

- Resulta fundamental llevar a cabo la implementación de las diversas medidas que Colombia ha considerado, comenzando por su compromiso con la cooperación internacional. Esto para fortalecer la lucha contra los ciberdelincuentes y mejorar la capacidad de respuesta ante delitos informáticos. En este sentido, Ecuador debe establecer mecanismos de colaboración con otros países que permitan intercambiar información, prácticas para combatir ciberdelitos y conocimientos sobre los ciberdelincuentes y sus actividades, esto permitiría una respuesta coordinada a nivel global. Además, es necesario desarrollar políticas públicas que establezcan normas y regulaciones para garantizar la seguridad de las Tecnologías de la Información y la Comunicación (TIC), al mismo tiempo que se promueva la concienciación sobre los riesgos de los delitos informáticos. Por último, se deben implementar estrategias dirigidas a la ciudadanía, como campañas de sensibilización, programas educativos y herramientas de autoprotección. Al educar y concientizar a las personas, se fomenta una cultura de seguridad digital y se les brinda los conocimientos necesarios para tomar medidas proactivas y protegerse contra estos delitos. Esta combinación de colaboración internacional, políticas públicas sólidas y empoderamiento ciudadano contribuirá significativamente a mejorar la seguridad de las TIC y la capacidad de respuesta ante los delitos informáticos en Ecuador.

BIBLIOGRAFÍA

Acurio del Pino, S. (2016). *Delitos informáticos: generalidades*. https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico

Arellano, W., & Ochoa, A. (2013). Derechos de privacidad e información en la sociedad de la información y en el entorno TIC. *IUS Revista del Instituto de Ciencias Jurídicas de Pueblas, México, 7*(31), 183-206. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010

Banco Pichincha. (2021, abril 9). *Pharming: qué debes hacer cuando los ciberdelincuentes se convierten en "granjeros"*. https://www.pichincha.com/blog/ataque-pharming

Carrion, F. (2020). *El Bien Jurídico Protegido*. El Bien Jurídico Protegido. https://cronica.com.ec/2020/09/02/el-bien-juridico-protegido/

Constitución de la República del Ecuador [CRE]. (2021). *Artículo 66, numeral 19 [Título II]*. Registro Oficial 449. https://biblioteca.defensoria.gob.ec/bitstream/37000/3390/1/Constituci%c3%b3n%20de%20la%20Rep%c3%bablica%20del%20Ecuador%20%28%c3%9altima%20Reforma%2025%20de%20enero%202021%29.pdf

Corona, J. (2016). Apuntes sobre métodos de investigación. *Apuntes sobre métodos de investigación* , *14*(1), 81-83. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=64300

Dictamen No. 13-18-TI/19 (2019). https://portal.corteconstitucional.gob.ec/Boletin300519/Sustanciacion/13-18-TI-19.pdf

Dzul, M. (s. f.). *Unidad 3. Aplicación básica de los métodos científicos*. uaeh.edu.m.

Fundación Evolución, & Fundación Carlos Vélez. (2020). *Introducción a las TIC. Serie "TIC en la Escuela y la Vida Cotidiana"*. https://fundacionevolucion.org.ar/wp-content/uploads/2020/10/Introduccio%CC%81n-a-las-TIC.pdf

Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Henríquez, R. (2023). Delitos informáticos: Vulneración de los derechos humanos en niñas, niños y adolescentes en la provincia de Guayas, 2014-2023. *Andares: Revista de los derechos humanos y de la naturaleza*, *4*, 32-41. https://doi.org/https://doi.org/10.32719/29536782.2023.2.4

Hernández, L. (2009). *El delito informático*. *23*, 227-243. https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Infoem. (2019). *Datos Personales | ¿Qué es la protección de datos?* infoem.org.mx. https://www.infoem.org.mx/es/contenido/datos-personales

Jenifa, A. (2022, diciembre 27). *¿Qué es el cardado y cómo protegerse de él?* . Geekflare.

Jenkinson, A. (2022). *Ransomware and Cybercrime* (1st Edition). https://doi.org/https://doi.org/10.1201/9781003278214

Khandelwal, S., & Das, R. (2022). Phishing Detection Using Content-Based Image Classification. *Taylor & Francis Group*, *1st ed.* https://doi.org/https://doi.org/10.1201/9781003217381

Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (1982). https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

Martínez de Pisón, J. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. *Anuario de filosofía del derecho, 32*, 409-430. https://investigacion.unirioja.es/documentos/5c13b280c8914b6ed377ea05

Martínez, G. (2020). *Ataques en el ciberespacio: conflictos armados y seguridad nacional*. https://elibro.net/es/lc/utnorte/titulos/167813

Mata, L. (2019). *El enfoque de investigación: la naturaleza del estudio*. investigalia. https://investigaliacr.com/investigacion/el-enfoque-de-investigacion-la-naturaleza-del-estudio/

Mendoza, F., Bechara, A., & Caballero, J. (2021). La intimidad como derecho humano y la solidaridad como valor constitucional en la era del Covid-19. *JURÍDICAS CUC*, *17*(1), 277-298. https://doi.org/https://doi.org/10.17981/juridcuc.17.1.2021.10

Molina, C. (2021). *El Convenio de Budapest: Un análisis desde el ordenamiento jurídico colombiano* [(Tesis de grado), Universidad Pontificia Bolivariana]. https://repository.upb.edu.co/bitstream/handle/20.500.11912/9409/Convenio_Budapest.pdf?sequence=1

Monroy, M. de los Á., & Nava, N. (2018). *Metodología de la investigación* (Grupo Editorial Éxodo, Ed.). https://elibro.net/es/lc/utnorte/titulos/172512

Morales, J. (1995). El right of privacy norteamericano y el derecho a la intimidad en el Perú. Estudio comparado. *Derecho PUCP*, *49*, 169-186. https://doi.org/https://doi.org/10.18800/derechopucp.199501.009

Nino, C. (2005). *Fundamentos de Derecho constitucional* (Editorial Astrea, Vol. 3).

Organización de los Estados Americanos [OEA]. (2022). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*.

Parada, R., & Errecaborde, J. (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*. BluePress SA. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Pérez, J., & Gardey, A. (2016, mayo 5). *Spyware - Qué es, definición y concepto*. Definición.de. https://definicion.de/spyware/

Platero, A., & Acedo, Á. (2021). El derecho fundamental a la protección de datos. En *El derecho al olvido en internet. La responsabilidad civil de los motores de búsqueda y las redes sociales: estudio doctrinal y jurisprudencial: Vol. 1st ed* (pp. 36-86). Dykinson, S.L. https://doi.org/10.2307/j.ctv282jg2r.6

QuestionPro. (s. f.). *¿Qué es la investigación cualitativa?* QuestionPro. Recuperado 15 de noviembre de 2023, de https://www.questionpro.com/es/investigacion-cualitativa.html#tipos_cualitativa

Ramos, J. (2020). *Delitos contra la seguridad de los activos de los sistemas de información y comunicación en el Ecuador*. Corporación de Estudios y Publicaciones. https://elibro.net/es/lc/uta/titulos/171995

Rubio, M. (2021, junio 1). *Grooming: ámbito legal y consecuencias penales*. Te pongo un reto. https://www.tepongounreto.org/2021/06/grooming-ambito-legal-y-consecuencias-penales/

Salgado, Á. (2012). Apuntes Sobre el Concepto de Bien Jurídico. *Revista Jurídica Mario Alario D´Filippo*, *4*(7), 317.

Sebastián Angulo. (2023). *El auge del cibercrimen en el país dispara el interés por los seguros*. https://www.expreso.ec/actualidad/economia/auge-cibercrimen-pais-dispara-interes-seguros-168387.html

Sentencia No. 11-18-CN/19 (2019). https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=11-18-CN/19

Sentencia No. 182-15-SEP-CC (2015). https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=182-15-SEP-CC#:~:text=Acci%C3%B3n%20de%20h%C3%A1beas%20data%3A%20La,ser%20el%20caso%2C%20exigir%20su

Sentencia SP 592/22 (50621) (2023). https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2022/SP592-2022(50621).pdf

Sentencia T-129/22 (2022). https://www.corteconstitucional.gov.co/relatoria/2022/T-129-22.htm

Sentencia T-339/22 (2022). https://www.corteconstitucional.gov.co/Relatoria/2022/T-339-22.htm

Trávez, N. (2018). *La vulneración de los Derechos Constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación (TICs)* [(Tesis de grado)]. Universidad Central del Ecuador.

Vargas, M., Galeano, C., & Jaramillo, D. (2015). El estado del arte: una metodología de investigación. *Revista Colombiana de Ciencias Sociales*, *6*(2), 423-442. https://www.researchgate.net/publication/282979831_El_estado_del_arte_una_metodologia_de_investigacion