UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

BRECHAS JURÍDICAS EN ECUADOR EN LA INTERFERENCIA ILÍCITA DE DATOS PERSONALES INFORMÁTICOS, CASO DEL ATAQUE A LA CONTRALORÍA GENERAL DEL ESTADO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO (A)

AUTORES: MARÍA PAZ LOPEZ JARA

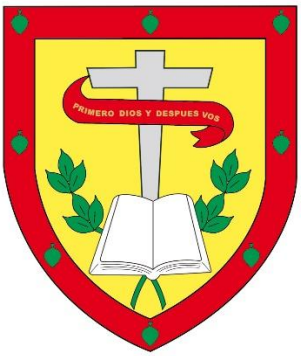
JOAQUIN FRANCISCO ORTIZ RAMIREZ

DIRECTOR: DR. BERNARDO XAVIER MONSALVE ROBALINO, MGS.

CUENCA- ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

BRECHAS JURÍDICAS EN ECUADOR EN LA INTERFERENCIA ILÍCITA DE DATOS PERSONALES INFORMÁTICOS, CASO DEL ATAQUE A LA CONTRALORÍA GENERAL DEL ESTADO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO(A)

AUTORES: MARÍA PAZ LOPEZ JARA

JOAQUIN FRANCISCO ORTIZ RAMIREZ

DIRECTOR: DR. BERNARDO XAVIER MONSALVE ROBALINO, MGS.

CUENCA- ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Ortiz Ramirez Joaquin Francisco portador(a) de la cédula de ciudadanía Nº **0151138377,** y **López Jara María Paz** portador(a) de la cédula de ciudadanía Nº **0150112977**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Brechas jurídicas en Ecuador en la interferencia ilícita de datos personales informáticos, caso del ataque a la Contraloría General del Estado"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **10 de noviembre de 2025**

F: .....

Joaquin Francisco Ortiz Ramirez

C.I. **0151138377**

F: .....

López Jara María Paz

C.I. **0150112977**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por: **LOPEZ JARA MARÍA PAZ**, con el Tema: **"Brechas Jurídicas En Ecuador En La Interferencia Ilícita De Datos Personales Informáticos, Caso Del Ataque A La Contraloría General Del Estado"**, bajo mi supervisión.

DR. BERNARDO MONSALVE ROBALINO, MGS

Tutor

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por: **ORTIZ RAMIREZ JOAQUIN FRANCISCO**, con el Tema: **"Brechas Jurídicas En Ecuador En La Interferencia Ilícita De Datos Personales Informáticos, Caso Del Ataque A La Contraloría General Del Estado"**, bajo mi supervisión.

DR. BERNARDO MONSALVE ROBALINO, MGS

Tutor

Dedicatoria

A mis padres quienes han sido un especial portento dentro del desarrollo de mi formación profesional académica, por ser quienes han sido partícipes y pilares fundamentales en el desarrollo, no solo de mi vida, sino de mi carrera futura, por todos los recursos que han invertido, por todo el tiempo, consejos y sabiduría imbuida en mi persona, dedico la realización de mi tesis académica a quienes estuvieron a mi lado desde el primer momento.

Joaquin Ortiz

A la Abogada Diana Lorena Jara Pesantez y al Economista Ángel Patricio López Naula, las personas más importantes en mi vida, a quien con amor, respeto, agradecimiento y sobre todo admiración espero poder honrar en un futuro.

Paz López

Agradecimiento

Le agradezco a Dios, mis padres y mi compañera de tesis López Jara María Paz, a todos ustedes por ser parte de mi vida, por estar en todo momento, por formar parte de un largo y duro proceso académico, y estar ahí como una voz de ayuda, consejo y solidaridad ante las adversidades propias de la vida universitaria, siendo su ayuda y amistad las que de una u otra forma han logrado generar un sentimiento de superación en mí, logrando motivarme a continuar mi formación profesional.

Joaquin Ortiz

Para mis adorados padres, a quienes agradezco de todo corazón, por haber trabajado toda su vida de manera tan dura, para que la mía sea más sencilla, agradezco los consejos, el amor y la sabiduría, espero poder algún día hacerles sentir la mitad de orgullosos de mí de lo que yo me siento por ustedes, y agradezco a la vida y a Dios por haberme puesto en las manos de los seres humanos más respetables y valientes, por haberme brindado una vida bella y llena de todo lo que a ustedes les falto. Mamita y papito, entrego ante ustedes mi título y vida profesional, los amo y muchísimas gracias. A mi querido Joaquin, no he encontrado amistad con cariño más sincero que el tuyo, gracias por estar, y por quedarte ante cada problema, te llevo en mi corazón y espero poder estar contigo durante toda mi vida, te quiero. Con amor tu amiga María Paz López Jara.

Paz López

Resumen

Con la expansión de la era digital dentro del país, la sociedad ecuatoriana ha creado innegables ventajas pero a su vez también han presenciado lo vulnerable que puede llegar a ser el país frente a la ciberdelincuencia con el ataque informático que sufrió la Contraloría General del Estado en el Ecuador en el año 2020 se constituye como un caso que establece un nuevo paradigma pues reveló no simplemente la fragilidad técnica de las instituciones públicas sino que también ayudó a que las brechas jurídicas que se encuentran presentes en la sociedad actual sean expuestas más aún cuando se trata de la fragilidad que recibe las instituciones públicas a nivel técnico y legal pues todas estas brechas jurídicas que se encuentran de manera persistente en el ordenamiento ecuatoriano hacen que rentar los delitos informáticos sea una tarea bastante difícil para los juristas ecuatorianos y el sistema legal. Desde la perspectiva del derecho penal y del derecho informático la política criminal de este estudio nos ayuda a plantear una urgente necesidad para que se diseñen y creen nuevas políticas públicas que sean fuertes ante estos delitos y que estén articuladas con una legislación más moderna y adaptada a los estándares internacionales. Este punto de vista plantea la examinación de diferentes tratados internacionales y jurisprudencia relevante como lo es el convenio de Budapest sobre la ciberdelincuencia ya que el mismo se constituye como un cuadro principal al momento de hablar sobre la cooperación internacional dentro de los aspectos destacables en la ciberdelincuencia.

Palabras Clave: *ataques informáticos, Contraloría General del Estado, políticas públicas, ciberseguridad, ciberdelincuencia.*

Abstract

As the digital age has expanded throughout the country, Ecuadorian society has made undeniable progress; however, it has also witnessed how vulnerable the nation can be to cybercrime. The cyberattack suffered by the Comptroller General of the State of Ecuador in 2020 marked a new paradigm, as it revealed not only the technical fragility of public institutions but also helped expose the legal gaps present in today's society, particularly the technical and legal vulnerability of public institutions. These persistent legal gaps within Ecuador's legal framework make prosecuting cybercrimes a difficult task for Ecuadorian jurists and the legal system. From the perspective of criminal law and computer law, the criminal policy addressed in this study highlights the urgent need to design and implement new public policies that are strong in addressing these crimes and aligned with more modern legislation adapted to international standards. This perspective requires examining various international treaties and relevant case law, such as the Budapest Convention on Cybercrime, which serves as a key framework for discussions on international cooperation in the most notable aspects of cybercrime.

Keywords: *cyberattacks, Comptroller General of the State, public policies, cybersecurity, cybercrime.*

Índice

Introducción

Con la evolución que se ha presenciado de la tecnología tanto en la información como en la comunicación se han obtenido en los últimos años un nuevo enfoque para el desarrollo humano, a nivel económico como social, siendo este un impacto notorio a nivel global. El camino hacia una nueva sociedad que se está haciendo digitalizada a pasos gigantescos ha hecho que ciertas actividades de la vida cotidiana, ya sea en un ámbito público o privado empiecen a transcurrir dentro de un espacio completamente intangible considerado como "ciberespacio".

A raíz de este nuevo fenómeno digital la humanidad ha dado una especie de revolución industrial que ha obtenido el significado no de una simple evolución en la manera en la que esta se efectúa, se comunica o incluso se puede administrar, pero, también en la manera de la cual surgen nuevas problemas sociales y jurídicas que nacen a partir de diferentes tipos de interacciones humanas en los entornos digitales.

Para el Ecuador, durante este proceso evolutivo de la digitalización se ha presenciado con mayor fuerza y frecuencia en el campo financiero, estatal y a su vez en la forma en la que el ciudadano puede ingresar a diferentes tipos de servicios electrónicos, estos incluyendo redes sociales y plataformas en donde es evidente el intercambio de información; no obstante con el aumento que se ha obtenido en el uso de la tecnología podemos decir que este acarrea una serie de peligros constantes como en la rama de ciberdelincuencia, creándose así nuevas formas de criminalidad, que ya no están limitadas por ningún tipo de obstáculo, pues, puede romper barreras económicas políticas institucionales y sociales con un casi inexistente costo de ejecución pero que obtiene consecuencias devastadoras.

Uno de los hitos históricos que se pueden utilizar como prueba de esto y de la vulnerabilidad digital que existe en el Ecuador es el ataque informático del cuál fue víctima la

Contraloría General del estado en el año 2020, bajo el contexto histórico en el cual se desataron intensas jornadas de protestas sociales dentro de toda la extensión territorial del Ecuador. En estas jornadas ocurrieron varios disturbios, saqueos y una larga serie de diferentes actos en donde la violencia fue el principal recurso para afectar a las instituciones estatales y privadas.

Durante estas protestas la Contraloría General del Estado en Ecuador no fue únicamente atacada de manera física a su infraestructura, pues se había generado un incendio dentro de su edificio el cual destruyó las instalaciones de manera parcial, pero, también hubo un ataque digital que afectó la integridad de su base de datos, sistemas informáticos, obteniendo como resultado la pérdida de la información y la paralización de las funciones de control dentro de la institución.

La gravedad de este ataque hizo que existan varias consecuencias importantes que afectaron a todos los ciudadanos del Ecuador, pues, se había sustraído e incluso destruido documentos de auditorías, varios servidores informáticos resultaron perjudicados y con esto la transparencia de la institución se vio cuestionada, pues la rendición de cuentas y el control sobre el uso que se tiene de los recursos públicos estaban completamente alterados. La Contraloría General del Estado siendo el organismo que se encuentra a cargo de la vigilancia y el control del patrimonio del Estado es poseedor de información extremadamente sensible y de importante relevancia para que se dé el correcto funcionamiento del Estado y también para poder hacer frente a un constante periodo de lucha contra la corrupción del país.

Siendo por esta razón que el ataque cibernético contra la institución no debería en ningún momento ser considerado como un caso aislado de vandalismo, de hecho, debería ser todo lo contrario y tomarlo como una acción que puso en evidencia lo frágil que puede llegar a ser el país ante los hechos de ciberdelincuencia y cómo este tiene un mecanismo completamente insuficiente de herramientas jurídicas para sancionar o prevenir este tipo de delitos. Desde la

perspectiva jurídica este acontecimiento logró revelar de manera cruda la existencia de brechas jurídicas dentro del sistema legal del país, pues, si bien el Código Orgánico Integral Penal posee algunos delitos que se relacionan con actividades criminales dentro del campo informático, como lo es el acceso no consentido a sistemas o incluso la intersección ilícita de datos y la alteración de la información, no se puede decir con completa seguridad que estas disposiciones puedan resultar adecuadas para la complejidad que está presentando los diferentes problemas, ni relacionados ataques cibernéticos dentro de la práctica legal; las leyes ecuatorianas son poseedoras de varios vacíos legales, como lo es una definición precisa de ciertos tipos penales o incluso la regulación de diversas modalidades criminales.

Esta tesis está redactada bajo este contexto jurídico y social pues tiene como finalidad principal analizar las brechas jurídicas en la materia de delitos informáticos de nuestro país a partir del estudio del ataque a la Contraloría General del Estado siendo este considerado un caso paradigmático que ayuda a revelar las falencias tanto normativas como institucionales que presenta el Ecuador. De ese análisis nace la necesidad por buscar determinar en qué medida el ordenamiento jurídico del país se encuentra preparado o no para afrontar los diferentes desafíos que impone la sociedad digital y su evolución dentro del campo legal. De esta manera se puede decir que la importancia que tiene este trabajo escrito en los delitos informáticos constituye una realidad concreta pues la cotidianidad que está siendo afectada directamente para la sociedad y el estado es una experiencia que se observa en el caso de la Contraloría General del Estado considerándose así una advertencia fuerte y clara de lo que puede suceder en un futuro en caso de que no se fortalezcan los mecanismos jurídicos y protocolos legales de las instituciones estatales.

Glosario

Ataque DDoS: Este ataque consiste en una técnica informática por medio de la cual hay una gran cantidad de sistemas que están vinculados para que se envíen solicitudes masivas a un servidor, logrando así que este se sature para que impida su funcionamiento. Estos sistemas son conocidos como "botnets" y se los reconoce también como una especie de sabotaje en ámbito digital que puede llegar a tener consecuencias graves y peligrosas para la disposición y habilidad correcta de los servicios y bases de datos (Incibe,2024).

Datos personales: Dentro de la Constitución de la República del Ecuador del año 2008, se reconoce a los datos personales como un conjunto que sigue una estructura con un objeto de tratamiento automatizado o ejecutable de forma manual, y estos se encuentran organizados según un criterio de información determinada.

Base de datos: Para la Ley Orgánica de Protección de Datos Personales, la cual fue emitida en el año 2021. La base de datos es un conjunto de estructura con datos personales, es decir, la recopilación de información. Estos también pueden ser bancarios comerciales o electrónicos puede contener mensajes o páginas web.

Phishing: Este ataque consiste en una técnica enfocada en el fraude cibernético, pues tiene como objetivo alcanzar datos personales y bancarios mediante el uso de trampas por medio de correos electrónicos y mensajes basura.

Spear Phishing: Es un derivado del phishing, pues en este consiste específicamente en ataques que personalizan el mensaje a una persona o institución determinada y se basa en información que ya había sido recopilada anteriormente, lo cual lo hace más efectivo y llevadero.

Kaspersky: Esta es una institución y empresa de nivel internacional que se enfoca en la ciberseguridad por medio de software y antivirus, los cuales brindan herramientas que permiten analizar el malware y dar soluciones en caso de ciberataques.

Ataque de insiders: Los insiders son considerados una amenaza directa y preocupante para la seguridad informática, pues tiene origen en personas naturales con un acceso autorizado a diferentes sistemas, ya sean empleados o contratistas que abusaron de su autorización para poder robar y extorsionar, e incluso manipular o sabotear información de procesos de la institución.

Sextorsión: Consiste en una nueva forma de extorsionar información de carácter sexual por medio de plataformas digitales. Es conocido como un ciberdelito en el cual se amenaza a la víctima con la divulgación y manipulación de imágenes privadas o información. Íntima, en caso de que no se cumplan exigencias específicas que por lo general tienen un carácter económico o sexual.

Malware: Es definido de manera general como un software de carácter malicioso que está específicamente desarrollado para dañar e infiltrar, Y robar información de un sistema informático. Lo que hace diferente de otros ataques es que éste incluye virus, gusanos, troyanos, spyware y ransomware

Ramsomware: Es un malware. Que obstaculiza el acceso libre a diferentes sistemas y archivos de la persona o institución víctima del mismo Para lo cual exigirá un rescate, el cual por lo general es de carácter económico.

Sabotaje digital: Consiste en una actividad destinada a dañar y lesionar diferentes sistemas informáticos y bases de datos con el objetivo de perjudicar a una institución o persona, este consiste en un delito informático Que ha estado presente en los últimos años con mayor frecuencia.

Cultura digital: En la actualidad se entiende como cultura digital a este conjunto de prácticas, actividades, conocimientos y comportamientos que están directamente vinculados con el uso consciente, ético y moral de las diferentes tecnologías por parte de la humanidad, en donde está en constante uso, información y comunicación.

Plataforma digital: Una plataforma digital es también conocida como una especie de entorno en donde la tecnología permite interactuar entre usuarios y servicios digitales. De esta manera, facilita a las personas el intercambio de información sobre sus bienes o servicios por medio de Internet.

Ciberdelincuencia: Consiste en una conducta ilícita, la cual se realiza por medio del uso de tecnologías y entornos digitales, como lo es el acceso no autorizado a plataformas, el robo de datos o los fraudes en línea.

Ingeniería social: Viene de una rama técnica, la cual se encarga de manipular psicológicamente por medio de ciber delincuentes, para así convencer a las personas de exhibir información personal o confidencial para que se realice acciones de dudosa seguridad.

Capítulo 1: Marco jurídico penal vigente en Ecuador sobre delitos informáticos

1.1 Introducción al derecho penal informático

Desde la antigüedad, el Derecho ha ido experimentando una constante y continua evolución, en la medida en que su principal función desde su existencia ha sido regular la convivencia social en las múltiples actividades sociales que el ser humano realiza cotidianamente a lo largo de su vida. Esta necesidad regulatoria del derecho responde al carácter inherentemente social que posee el ser humano y a los constantes avances dentro del ámbito de la tecnología que, con el paso del tiempo, transforman la vida cotidiana. En este contexto, y a diferencia de lo que se puede observar en otras ramas del Derecho que cuentan con fuentes normativas tradicionales que provienen directamente desde épocas remotas, la regulación de los delitos dentro del ámbito informático constituye un campo que resulta ser relativamente reciente en cuanto a los avances que surgen a diario, tales avances impactan significativamente en la sociedad, y estos exigen respuestas jurídicas que estén acordes con los nuevos y crecientes desafíos que plantea la era digital. Espinoza Coila, M. (2023)

A su vez, el Derecho Penal Informático se puede definirse como el saber dentro del ámbito jurídico penal, el cual, mediante la interpretación de las leyes penales existentes sobre delitos informáticos, propone de una u otra forma un sistema legal, el cual, reduce el poder de vigilancia y el poder punitivo dentro de la sociedad. Espinoza Coila, M, (2023)

1.2 Evolución de la legislación penal sobre delitos informáticos en Ecuador

En Ecuador la historia de los delitos informáticos proviene de una necesidad latente de la creación de herramientas que faciliten la vida en sociedad y el control de la misma, sin ser la excepción la legislación penal, la cual, requiere de información recopilada a lo largo de la

historia y el transcurso del tiempo para almacenar una gran cantidad de información que sirva como memoria colectiva al momento de juzgar y sancionar delitos informáticos (Cepeda, 2005).

El avance tecnológico ha alcanzado al Ecuador igual que al resto del mundo, y con ello se han hecho presentes nuevos conflictos sociales que, al igual que cualquier otro problema, deben ser controlados por el derecho. En reacción de la llegada de dispositivos móviles, electrónicos y con las nuevas tecnologías se genera una reciente preocupación por la responsabilidad del usuario y dueño de dichos dispositivos, reflejándose así al derecho penal en ámbito informático (Castro, 2025).

La aparición de los nuevos tipos de delitos informáticos tiene por base el internet y sus diferentes plataformas digitales en donde se reposa grandes cantidades información, donde por medio de su uso se ha realizado innumerables cantidades de perjuicios, para ello es importante destacar que existen 2 medios. El primer medio es el internet que es conocido también como en abstracto (software), y, el segundo medio es la computadora (u otro medio tecnológico físico) el cual es conocido como instrumento físico (hardware) (Espinoza, 2012).

Considerando los sucesos más relevantes en cuanto al presente ámbito es importante mencionar que cronológicamente en el año 1999 aparece por primera vez en Ecuador la Ley de Comercio Electrónico Mensaje de Datos y Firmas Electrónicas la cual representó sin lugar a dudas un gran avance para la normativa ecuatoriana en cuanto a delitos tecnológicos debido a que se crea un nuevo mecanismo jurídico adaptable para asegurar la confianza a los usuarios de cuentas tecnológicas en donde se repose una base de datos con gran cantidad de información. Posteriormente en el año 2002 surge la Ley De Protección De Datos, la cual no ha sido reformada hasta la actualidad, es por eso que la importancia que tiene el Código Orgánico

Integral Penal en la regulación de delitos informáticos es clave, por lo tanto, la inclusión de los delitos en dicho cuerpo normativo ha sido de gran ayuda para desarrollo de los procesos abiertos con los delitos tipificados. Luego, para el año 2012 surge el Código Orgánico Integral Penal donde se pudieron observar tipificaciones de nuevos delitos, entre ellos, algunos de carácter informático, marcando así un avance para la evolución de nuevos métodos de sanción y control de delitos, en el campo de la informática y la tecnología (Salgado,2021).

1.3 Análisis del Código Orgánico Integral Penal y la tipificación de delitos informáticos

Por medio de la sección tercera del código orgánico integral penal entre el artículo 178 hasta el artículo 234 se establecen los delitos informáticos y su manera en la cual van a ser sancionados. Estos delitos cumplen la cualidad de atentar contra la seguridad de información considerada como confidencial e incluso la revelación ilegal de datos informáticos o de daños financieros que hayan sido ocasionados por accesos no autorizados (Alvarado, 2015).

Artículo COIP	**Delito**	**Conducta**	**Sanción**
Art. 178	Violación a la intimidad	Para cualquier individuo que de manera no consentida o autorizada legalmente acceda, intercepte, examine, retenga, grave, reproduzca, difunda, o, publique datos personales, ya sea, mensajes de voz, audio y video o incluso objetos postales con información que contenga soportes informáticos, comunicaciones privadas o reservadas de otra persona.	Pena privativa de libertad de 1 a 3 años
Art. 190	Apropiación fraudulenta por medios electrónicos	Se aplica para aquella persona que haga uso de manera fraudulenta cualquier tipo de sistema informático, redes electrónicas, o telecomunicaciones para facilitar la apropiación de cualquier bien ajeno o que procure la transferencia no consentida de bienes, valores, o, derechos en perjuicio de una persona o terceros.	Pena privativa de libertad de 1 a 3 años

Art. 229	Revelación ilegal de base de datos	Para todo aquel que aprovecho propio o por medio de un tercero expone información restringida que esté contenido en bases de datos electrónicas o semejantes y de manera intencional viole el secreto a la intimidad y la privacidad de las personas.	Pena privativa de libertad de 1 a 3 años
Art. 230	Interceptación ilegal de datos	Se establecen cuatro numerales en los cuales se especifica casos en concreto en donde las personas vulneran o violentan por medio de la intercepción de datos el derecho a la privacidad de las personas, en este caso usuarios de medios electrónicos e informáticos.	Pena privativa de libertad de 3 a 5 años
Art. 231	Transferencia electrónica de activo patrimonial	Es aplicable para todos los sujetos que con la intención de manipular o alterar cualquier tipo de sistema informático o sus derivados.	Pena privativa de libertad de 3 a 5 años
Art. 232	Ataque a la integridad de sistemas informáticos	La persona que modifique de manera negativa y cause daño a cualquier base de datos electrónicos o informáticos	Pena privativa de libertad de 3 a 5 años
Art. 233	Delitos contra la información pública reservada legalmente	Para la persona servidor público que destruya o altere información que esté clasificada en base a organismos legales	Pena privativa de libertad de 5 a 7 años
Art. 234	Acceso no con sentido del sistema informático	Sujeto que explote o trafique datos informáticos, electrónicos, o sistemas informáticos o telemáticos de manera opuesta a la voluntad de la persona que tenga el legítimo derecho de acceder al mismo	Pena privativa de libertad de 3 a 5 años

Tabla de mi autoría*

A modo de análisis general del cuadro precedente en primer lugar podemos referir que el artículo 178 del COIP habla sobre la violación a la intimidad, dicho precepto legal contempla una sanción específica para delitos que involucren el acceso o uso indebido de información

personal, no obstante, dicho artículo resulta ser insuficiente frente a la aparición de nuevos tipos de tecnologías como por ejemplo el uso de la inteligencia artificial para suplantar la identidad de una persona, cosa que no está contemplada dentro del dicho artículo.

Por su parte, el artículo 190 trata sobre la apropiación fraudulenta por medios electrónicos, dentro del presente tipo penal se sanciona a quien utilice sistemas informáticos, redes electrónicas o utilice telecomunicaciones de manera fraudulenta para poder apropiarse de bienes ajenos o para poder transferir bienes, valores o derechos sin consentimiento de la persona afectada. Este artículo, aunque puede resultar útil contra fraudes electrónicos, no prevé ninguna de las modalidades modernas para cometer delitos informáticos o estafas en cuanto al uso de criptomonedas, "*pharming"*, clonación de tarjetas virtuales o transacciones financieras a través de plataformas bancarias, dejando claramente vacíos importantes en cuanto a la protección económica dentro de lo digital.

Asimismo, el artículo 229 sanciona a quien o quienes, para beneficio propio o de terceras personas, expongan información restringida de bases de datos electrónicas confidenciales, violando así el derecho a la privacidad. No obstante, la regulación dentro del artículo no se adapta al contexto de la protección de datos personales, ya que no establece medidas diferenciadas para las bases de datos públicas o bases de datos privadas ni tampoco prevé sanciones acordes a filtraciones masivas de datos informáticos como las que ocurren en ciberataques actuales (*data breaches*).

El siguiente artículo 230 habla sobre la interceptación ilegal de datos, donde se penaliza la intercepción de datos transmitidos por sistemas electrónicos e informáticos, en este caso la disposición resulta ser demasiado general y no llega a contemplar ataques contemporáneos como

el "*sniffing"*, o sea, el espionaje mediante malware, la captura de contraseñas en redes inseguras o también la intercepción de datos en entornos de nube digital.

Por otro lado, el artículo 231 refiere a la transferencia electrónica de activo patrimonial, estableciendo una sanción a quienes manipulen o quienes alteren sistemas informáticos con el objetivo de transferir activos patrimoniales. A esto se debe mencionar que la tipificación es limitada, pues la misma no diferencia entre fraudes simples y otros más complejos, ni menciona como tal las transferencias a través de criptomonedas, de tokens o activos digitales, que hoy son mecanismos comunes dentro del cibercrimen financiero.

El artículo 232 habla sobre el ataque a la integridad de sistemas informáticos, penalizando así a quienes modifiquen o a quienes dañen bases de datos u otros sistemas informáticos, afectando su integridad. Pero dicho precepto legal no incluye ataques distribuidos como el *DDoS* (denegación de servicio), el secuestro de información mediante el uso de técnicas de *ransomware*, ni tampoco contempla las vulneraciones a otro tipo de infraestructuras críticas, limitando así la protección frente a ciberataques de gran magnitud.

Por su parte el artículo 233 de los delitos contra la información pública reservada legalmente plantea sancionar a los servidores públicos que destruyan o que alteren información clasificada por alguna disposición legal. Sin embargo, dicho artículo se centra única y exclusivamente en funcionarios públicos, pero no regula el acceso indebido de otras personas particulares a información estatal reservada ni tampoco contempla escenarios de ciber espionaje a nivel internacional, dejando así varios vacíos en cuanto a la protección de la seguridad nacional de la información digital.

Finalmente, el artículo 234 habla sobre el acceso no consentido a sistemas informáticos, dicho precepto legal sanciona a quien o quienes accedan, exploten o trafiquen datos informáticos

dentro de un sistema electrónico o un sistema telemático sin autorización de su legítimo dueño titular. El presente artículo aunque se refiere al acceso no autorizado, no tipifica adecuadamente el uso de otras prácticas modernas como por ejemplo la compraventa de accesos en la "*dark web"*, el *hacking ético* sin que exista consentimiento expreso, o la explotación de vulnerabilidades dentro del algún software, lo cual a su vez genera inseguridad jurídica en el ámbito digital.

1.4. Interferencia en sistemas y datos informáticos: definición y elementos

La interferencia dentro de sistemas y demás datos informáticos constituye una figura penal recogida dentro del Código Orgánico Integral Penal (COIP), dicha figura está orientada para poder proteger la integridad, la disponibilidad y la fiabilidad de los datos contenidos dentro de los respectivos soportes digitales. De acuerdo con lo mencionado en los artículos 232 y 234 del COIP, dicha conducta se configura cuando un individuo, sin autorización previa, accede, altera, daña, deteriora, interrumpe o también modifica sistemas informáticos, redes electrónicas o en general cualquier tipo de base de datos digitales, afectando así el normal funcionamiento dentro de dichos entornos informáticos.

Observado aquellos desde una perspectiva mucho más dogmática, es claro comprender que el COIP busca proteger frente a delitos contra la confidencialidad, integridad y disponibilidad de datos informáticos. El acceso no consentido a datos, la manipulación de la información digital y los ataques destinados a infraestructura informática no solo lesionan intereses individuales dentro de la sociedad como por ejemplo la privacidad o la propiedad, sino que además comprometen intereses colectivos como por ejemplo la seguridad pública y la confianza en los sistemas tecnológicos en general.

Sin embargo, el tratamiento normativo dentro del COIP presenta cierto grado de limitaciones significativas. Primeramente, los artículos mencionados adolecen de una excesiva generalidad en cuanto a sus preceptos jurídicos, puesto que describen la interferencia en términos muy amplios, sin siquiera diferenciar entre conductas de diversa gravedad ni tampoco contemplar nuevos tipos de modalidades de ataque digital que surgen con el paso del tiempo. Por ejemplo, no se hace distinción alguna entre la simple intrusión en un sistema de datos y el uso de técnicas sofisticadas como ataques distribuidos (*DDoS*), *ransomware* o el secuestro de información mediante el cifrado malicioso de los respectivos datos involucrados. Dicha falta en cuanto a la precisión dificulta en gran medida la subsunción de hechos concretos dentro de los tipos penales y a su vez genera inseguridad jurídica al momento de procesar a los responsables de cometer dichos actos delictivos.

Como segundo punto, el vacío normativo existente respecto al cuidado y correcto manejo de la prueba digital se traduce en serias complicaciones procesales al momento de pretender hacer uso de la justicia para poder enfrentar delitos informáticos. Dentro del COIP no se regula de manera adecuada la validez de la evidencia electrónica, su obtención o su preservación, dicha situación expone a que los procesos penales informáticos lleguen a ser ineficientes e inclusive que se pueda llegar a invalidar la prueba por no guardar la debida reserva y el debido manejo de la misma. Por todo lo manifestado, es importante hablar de una cadena de custodia digital misma que resulta ser fundamental dentro de este tipo de delitos que involucran el campo de lo informático, pues sin dicha cadena de custodia digital la prueba carece de desarrollo normativo específico, lo cual a su vez limita la eficacia de la persecución penal en el presente ámbito.

Como tercer punto, dentro de la legislación ecuatoriana se observa una clara falta de correspondencia con el derecho internacional, pues si bien existen instrumentos como el

Convenio de Budapest que establece parámetros claros para poder llegar a enfrentar la ciberdelincuencia, la normativa nacional vigente se mantiene totalmente desarticulada respecto a dichos estándares, generando discontinuidad y también falta de cooperación eficaz con otros países en cuanto investigaciones transnacionales de delitos informáticos.

En la práctica dichas falencias normativas se pueden ver claramente reflejadas en problemas recurrentes dentro de los procesos judiciales como son:

1. Riesgo de invalidez en cuanto a la evidencia digital por falta de reglas claras sobre cadena de custodia digital.
2. Insuficiente regulación técnica que impide abordar nuevas formas de ciberataques.
3. Protección deficiente frente a sabotajes tecnológicos a gran escala, es decir hackeos masivos.
4. Informes periciales incompletos, debido a la carencia de protocolos especializados y conocimiento suficiente.
5. Desconexión con los estándares internacionales informáticos, lo que limita la cooperación en investigaciones transfronterizas existentes.

1.5. Normativa complementaria nacional

Si bien el Código Orgánico Integral Penal es el referente principal al momento de hablar sobre conductas delictivas, este necesita ser complementado por otros cuerpos legales que puedan brindar soporte firme. Este apoyo es indispensable, pues, la adaptación al cambio constante que conlleva el ámbito tecnológico requiere de una evolución rápida, en razón de la constante aparición de nuevas conductas delictivas, como es de conocimiento general, el Código Orgánico Integral Penal no se puede actualizar o modificar de manera sencilla, y es por esta

razón que, tanto las leyes, las políticas públicas, y los protocolos brindan a la sociedad la oportunidad de obtener una respuesta jurídica más precisa y eficaz.

Por otro lado, visto desde el punto de vista de especialización técnica, los actos ilícitos a nivel informático, en procesos iniciados como el hacking, phishing, y el robo de datos se debe hacer uso de conocimientos mucho más avanzados a nivel técnico, esto en base a la tipificación y estudio de diferentes conceptos, como en el caso de la custodia digital y por supuesto la preservación de la prueba obtenida en bases informáticas y dispositivos electrónicos.

Gracias a la normativa complementaria se protege la seguridad jurídica de los ciudadanos que la requiera, pues los derechos fundamentales que se encuentren bajo peligro de vulneración pueden ser custodiados por otras opciones. Derechos como la privacidad, la seguridad de información personal privada y a su vez la propiedad intelectual de las personas. La protección de estos derechos sería más eficaz cuando el legislador y los ciudadanos buscan evitar el abuso en bases informáticas que vengan de terceros.

1.5.1. Ley de Protección de Datos Personales

La utilidad de esta ley es notoria para complementar la tipificación del COIP para tratar datos personales, debido a que nos definirán de manera clara lo que es un tratamiento de datos de manera ilícita y crea lazos con delitos especificados con anterioridad como el acceso no autorizado a sistemas informáticos, la comercialización de bases de datos sin consentimiento y por supuesto la suplantación de la identidad digital.

Con esta ley se previene y sanciona los comportamientos que dan mal uso de la información que reposa en bases digitales, una de las brechas más notorias que presenta en la actualidad el COIP se encuentra en los artículos 229 al 232, que si bien, penaliza algunos delitos informáticos no se amplía la dimensión al mal uso de datos, por ende, la Ley de Protección de

Datos Personales, se dio la tarea de aclarar principios y obligaciones para aquella persona que trate datos de manera ilícita, consiguiendo de esta manera que se reporten los incidentes relacionados a la seguridad informática.

1.5.2. Ley Orgánica de Telecomunicaciones

Desde el año 2015 esta ley se ha encargado de regular el uso y la operación de las telecomunicaciones en el país, si bien se sabe el enfoque principal de esta normativa es por lo general técnico y económico, pero, aun así, se busca cumplir funciones clave como apoyo al COIP, específicamente para prevenir e investigar más a profundidad los delitos informáticos.

Esta ley ha conseguido brindar mayor facilidad a la interpretación de comunicaciones y bases de datos, hablando así del cuidado de la seguridad y la continuidad de las redes que son afectadas por delitos como el sabotaje digital o el ataque DDoS.

1.5.3. Política Nacional de Ciberseguridad

Se ha percibido su influencia desde el año 2022 y fue emitida por la Secretaria de Seguridad y el Ministerio de Telecomunicaciones, se debe especificar que no fue creada como una ley, sin embargo, establece estructuras solidas estatales en contra de distintas amenazas cibernéticas, pues, si bien esta política contempla la situación social del Ecuador, se une con convenios internacionales como el Budapest, logrando lazos regionales que ayudaran a los doctrinarios para conseguir intercambio de información confiables y respuestas conjuntas respecto a problemas informáticos.

Brechas jurídicas en delitos informáticos	**Complementación con otras normativas**	**Campo en el que se centra**
Poca coherencia en COIP, LOPDP, LOT y Política nacional de ciberseguridad	Se hace uso de distinta normativa para obtener una mejor revisión y lograr	Cuerpos jurídicos y manejo legal

	armonizar diferentes leyes a favor del cumplimiento del debido proceso	
Escasez de técnicas para protección de ataques informáticos	Con el afán de gestionar problemas informáticos en relación con diferentes brechas jurídicas se intenta implementar CSIRTs a nivel nacional	Departamentos profesionales en protección informática
Poca preparación profesional en investigación de delitos informáticos	La concientización sobre materia informática a todos los servidores públicos, específicamente a los encargados de realizar investigación para iniciar procesos legales en cuanto a diferentes delitos informáticos	Instituciones estatales
Mala persecución de delitos como phishing o ransomware	Buscar relación internacional con diferentes convenios que ayuden al estudio y dirección de procesos penales enfocados en ataques informáticos y como afectan a la ciudadanía	Servidores públicos e instituciones gubernamentales
Desconocimiento de servidores públicos en cuanto a protección informática	Control y sanción para proteger derechos informáticos de los ciudadanos que acceden a servicios públicos	Servidores públicos, peritajes y sistemas de investigación

Tabla de mi autoría*

1.6. Tratados internacionales ratificados por Ecuador en materia de ciberdelitos

El Convenio denominado como “Budapest”, fue adoptado en el año 2001 por el Consejo de Europa, este vendría a ser el primer tratado de carácter internacional que de una u otra forma busca combatir de manera efectiva los delitos dentro del ámbito informático y también los delitos cometidos a través del uso de plataformas de carácter digital, afectando en gran medida datos e información que circulan a diario en internet. Su objetivo principal es poder llegar a armonizar las legislaciones nacionales mediante su uso, establecer los respectivos procedimientos de investigación, mismos que resulten ser eficaces y que ayuden a poder fomentar la cooperación de carácter internacional entre todos y cada uno de los Estados firmantes dentro del presente convenio.

Analizando la forma en la cual el Ecuador actúa en el ámbito legal, es evidente destacar que una de las causas por las cuales Ecuador no se ha ratificado en todo este tiempo se debe a la

reticencia misma del Estado por cuanto la adhesión podría llegar a generar una pérdida de soberanía respecto a la materia de investigación penal ejercida dentro del país. Este convenio establece múltiples mecanismos de cooperación internacional directa, como por ejemplo la entrega acelerada de datos informáticos y la asistencia judicial recíproca, lo cual a su vez implica que autoridades extranjeras puedan tener acceso a todo tipo de información localizada en servidores o en sistemas de datos informáticos dentro del Ecuador. Este aspecto ha sido visto con desconfianza por cierto tipo de sectores políticos que sostienen que con la adhesión a este convenio se podría vulnerar la autonomía dentro de las instituciones judiciales nacionales, arriesgando así la integridad y soberanía del territorio ecuatoriano. La falta de ratificación a este convenio trae consigo varias consecuencias negativas la cuales van desde la falta de cooperación internacional hasta la impunidad total en delitos informáticos internacionales.

La falta de adhesión del Ecuador al Convenio de Budapest limita en gran medida la cooperación internacional en cuanto a las investigaciones de ciberdelitos, esto ya que el país no cuenta con un marco jurídico uniforme y claro para el intercambio ágil de información y pruebas electrónicas con otros países. En la práctica, esto nos obliga a depender de tratados bilaterales tradicionales o de la emisión de cartas rogatorias, mecanismos lentos y burocráticos que resultan ser sumamente ineficientes frente a la rapidez con la cual se ejecutan y se cometen los delitos dentro de lo informático. Como consecuencia de aquello, muchas investigaciones internacionales que involucran delitos informáticos se ven frustradas, aumentando así el riesgo de impunidad y colocando al Ecuador en clara desventaja frente a otros países de la región que ya han adoptado desde hace tiempo este instrumento internacional.

Algunos de los temas clave que aborda el convenio son:

• El acceso ilegal dentro de los sistemas informáticos internacionales.

• La interceptación ilícita de los datos informáticos.

• La interferencia in autorización dentro de sistemas y de datos informáticos.

• El uso indebido de dispositivos.

• Fraude y falsificación informática.

• Delitos relacionados con el contenido (por ejemplo, pornografía infantil).

• Infracciones a los derechos de autor en entornos digitales.

Este convenio Budapest también entre sus preceptos incluye un protocolo adicional sobre la criminalización existente de actos tanto racistas como xenófobos cometidos haciendo uso de sistemas informáticos. Aunque en el Ecuador aún no se ha llegado a ratificar, el Convenio de Budapest en realidad sirve para usarlo como una referencia normativa dentro del ámbito internacional para poder llegar a legislar sobre ciberdelitos dentro de un determinado territorio.

1.7. Jurisprudencia nacional relevante en delitos de interferencia informática

Un precedente que resulta fundamental dentro del presente tema es el Dictamen 1-24-TI/24 emitido por la Corte Constitucional del Ecuador, emitido el 25 de abril de 2024, mediante el cual se analizó la constitucionalidad del Convenio de Budapest sobre la Ciberdelincuencia. Dicho pronunciamiento tuvo lugar en cumplimiento del artículo 438 de la Constitución de la República, dicho cuerpo normativo exige control previo de constitucionalidad para que se puedan llegar a ratificar tratados internacionales.

Este proceso se originó en el año 2021, cuando diversas instituciones estatales como por ejemplo la Fiscalía General del Estado, el Ministerio de Gobierno, la Policía Nacional y el Ministerio de Defensa dieron la sugerencia al ejecutivo de que se dé la adhesión del Ecuador dentro de dicho convenio. Estas entidades argumentaron principalmente que el instrumento internacional permitiría modernizar en gran medida los preceptos aplicables al ámbito

informático contenidos dentro de la legislación penal ecuatoriana, dotar de mejores herramientas a las investigaciones y también se podría llegar a fortalecer la cooperación internacional frente a la delincuencia informática actual.

En su análisis, la Corte Constitucional sostuvo principalmente que el Convenio de Budapest se encuentra en armonía con la Constitución de la República del Ecuador, en la medida en que dicho convenio puede ayudar a proteger bienes jurídicos reconocidos como la intimidad, la seguridad y la propiedad, además de que dicho convenio garantiza derechos fundamentales vinculados al uso de nuevas tecnologías de la información digital. La Corte Constitucional enfatizó en que el tratado no supone una cesión de la soberanía, sino más bien es un mecanismo de cooperación internacional regulada, mismo que está sujeto a controles jurisdiccionales internos.

El dictamen concluyó mencionando que la adhesión al Convenio Budapest si es jurídicamente viable, y su incorporación dentro del ordenamiento jurídico permitiría al Ecuador:

1. Armonizar lo establecido dentro de su legislación penal con estándares internacionales, subsanando de esta forma vacíos normativos en tipos como por ejemplo el acceso no autorizado, la interceptación de datos o los ataques a sistemas informáticos en general.
2. Adoptar procedimientos modernos para llevar a cabo su investigación en materia de evidencia digital y de la cadena de custodia, superando la actual dispersión normativa existente.
3. Fortalecer la cooperación internacional para la persecución de estos delitos, todo esto mediante canales ágiles de asistencia judicial y de conservación transfronteriza de datos informáticos.

Sin embargo, la Corte Constitucional también advirtió que el hecho de que se dé está adhesión generará la obligación inmediata para el legislativo de reformar el COIP y las normas procesales, esto para poder adecuarlas a los parámetros establecidos en el Convenio. Caso contrario, la ratificación podría quedar simplemente como un mero acto formal, sin impacto real en la persecución penal de los ciberdelitos actuales.

Capítulo 2: Deficiencias normativas y operativas en la prevención y sanción

2. 1 Revisión general del marco normativo y operativo vigente

En el Ecuador se cuenta con un marco normativo que, a simple vista, reconoce la existencia de ciertos delitos informáticos dentro del Código Orgánico Integral Penal (COIP). Desde el año 2014, dicha normativa incorporó cierto tipo de figuras como la del acceso no autorizado a sistemas informáticos, la interceptación ilegal de datos y los ataques contra la integridad de bases de datos informáticos. Las disposiciones antes mencionadas representaron en gran medida un avance en cuanto a la tipificación delictiva frente al indebido uso de las nuevas tecnologías modernas, puesto que reflejaron la voluntad que tenía el legislador de adecuar las disposiciones aplicables dentro del derecho penal a las transformaciones que en la era moderna han surgido en torno al ámbito informático misma que nos ha llevado a vivir en una sociedad de la información, es decir, la etapa evolutiva dentro de la sociedad donde la creación, distribución y la manipulación de la información en nuestro entorno tiene una importancia económica, cultural y social primordialmente.

Sin embargo, la regulación que habría sido creada por parte del legislador, en la actualidad resulta ser insuficiente. Los artículos vigentes en la actualidad, aunque constituyen un primer esfuerzo para regular los delitos informáticos, presentan un carácter demasiado amplio, general y sobre todo carecen de precisión frente a las nuevas modalidades existentes de

ciberdelito, como por ejemplo el *ransomware*, el fraude haciendo uso de criptomonedas, los ataques distribuidos de denegación de servicio (*DDoS*) o la explotación de vulnerabilidades en infraestructuras críticas. Dicho desfase normativo genera cierto grado de inseguridad jurídica, además dificulta que los operadores de justicia que trabajen dentro del presente ámbito puedan llegar a encuadrar adecuadamente conductas complejas dentro de los tipos penales existentes en la actualidad dentro de nuestro marco legal.

Hablando en el plano operativo, Ecuador ha creado instancias especializadas para enfrentar este tipo de delitos, por ejemplo se destaca la Unidad de Investigaciones Tecnológicas de la Policía Nacional, encargada de llevar a cabo la detección de ciberataques, fraudes electrónicos y cierto tipo de delitos relacionados con el uso de redes sociales y de comercio digital. De igual forma, entidades como la Fiscalía General del Estado ha podido elaborar protocolos para llevar a cabo la recolección de evidencia digital y también la conducción de investigaciones tratando de respetar las garantías del debido proceso tal como se establece dentro de la Constitución. Dichas iniciativas reflejan un gran esfuerzo institucional para intentar adaptarse a la complejidad del ciberdelito.

No obstante, dichas instituciones también enfrentan ciertas limitaciones estructurales que afectan su desempeño al momento de ejercer sus funciones habituales. Entre las limitaciones más relevantes se encuentran por ejemplo la falta de recursos técnicos, la escasez de personal que esté capacitado y especializado en cuanto a la informática forense y la débil coordinación interinstitucional, todo esto provoca solapamiento dentro de las funciones y también genera pérdida de eficiencia dentro de la investigación. De igual forma, la capacitación a los fiscales, jueces y policías dentro de la materia tecnológica sigue siendo altamente insuficiente, lo cual a su

vez se traduce en deficiencias dentro de la valoración de la prueba digital y por ende afecta en la resolución de casos (Álvarez & Maldonado, 2020).

2.2. Ambigüedades en la legislación penal sobre delitos informáticos

Si bien la entrada en vigor e implementación del Código Orgánico Integral Penal (COIP) ha representado un avance significativo en la tipificación de ciertas conductas relacionadas con la ciberdelincuencia desde 2014, su redacción aún presenta importantes ambigüedades, generando inseguridad jurídica tanto para los actores del sistema judicial (es decir, los funcionarios judiciales) como para la ciudadanía. Conceptos como "sistemas informáticos" o "acceso no autorizado" se formulan de forma genérica y sin tener en cuenta definiciones técnicas claras, lo que deja un amplio margen de interpretación para quienes intentan utilizar estos artículos.

Este problema vulnera el principio de legalidad y la especificidad del derecho penal, que exige que la conducta delictiva se describa de forma clara y precisa para evitar interpretaciones arbitrarias por parte de quienes la utilizan. La falta de definiciones regulatorias claras ha llevado a la adopción de criterios judiciales inconsistentes en situaciones similares. Esto ocurre particularmente en casos de fraude electrónico, donde la transferencia fraudulenta de fondos desde una dirección de correo electrónico falsa puede ser caracterizada de forma diferente por los jueces. Algunos lo clasifican como fraude o estafa común (artículo 186 del COIP), mientras que otros lo clasifican como apropiación fraudulenta por medios electrónicos (artículo 190 del mismo

Código). Esta divergencia de interpretación compromete la uniformidad del sistema de justicia penal.

Otro ejemplo de esta ambigüedad regulatoria se encuentra en el acceso no autorizado a los sistemas. La falta de una delimitación tipológica clara ha dado lugar a decisiones contradictorias, lo que pone de manifiesto las limitaciones del marco jurídico actual. Además, la legislación vigente no prevé tipificaciones penales específicas para las nuevas formas de ciberdelito, como el phishing, el ransomware o los deepfakes. En la práctica, estos tipos de conducta se castigan de forma similar, lo cual resulta insuficiente dada su complejidad técnica. Un caso típico es el phishing bancario, que la fiscalía suele clasificar como fraude ordinario, a pesar de que el engaño se lleva a cabo a través de medios digitales con características específicas no expresamente previstas en la ley.

Estas lagunas regulatorias también reflejan una falta de armonización con las directrices internacionales, en particular el Convenio de Budapest sobre Ciberdelincuencia (2001), que proporciona definiciones precisas y clasificaciones actualizadas. A diferencia de países de la región como Chile y Colombia, que han incorporado estas directrices, Ecuador persiste en aplicar definiciones genéricas que no tienen en cuenta la naturaleza dinámica del ciberdelito. En resumen, las imprecisiones del COIP tienen tres consecuencias principales:

Incertidumbre jurídica: La interpretación de los comportamientos técnicos queda a discreción del juez.

Riesgo de impunidad: Los delitos modernos no siempre encajan perfectamente en las clasificaciones penales existentes.

Desconexión internacional: Las regulaciones no son coherentes con los estándares internacionales, lo que dificulta la cooperación y los procesos judiciales transnacionales. Por lo

tanto, es imperativo adoptar una reforma penal especializada que defina los elementos característicos de cada ciberdelito, distinga entre formas simples y complejas, y modernice la legislación de acuerdo con los estándares internacionales. Esta actualización es esencial para garantizar el respeto al Estado de derecho y dotar a las autoridades judiciales de las herramientas necesarias para combatir eficazmente la ciberdelincuencia en el Ecuador.

2.3. Obstáculos en la investigación de delitos informáticos en Ecuador

En Ecuador, las investigaciones de ciberdelitos se enfrentan a numerosos obstáculos estructurales y operativos que merman la eficacia del sistema judicial ante un fenómeno dinámico y transnacional. Las principales limitaciones identificadas son:

Recursos técnicos limitados: Si bien la Policía Nacional cuenta con una Unidad de Investigaciones Tecnológicas y el Ministerio Público ha establecido ciertos protocolos, ambos organismos carecen de la tecnología necesaria o de laboratorios especializados para el análisis digital. El equipo existente está en gran medida obsoleto, lo que imposibilita el análisis digital complejo, el rastreo de direcciones IP o la inspección de dispositivos modernos. Esta deficiencia tecnológica limita la capacidad de respuesta ante delitos que a menudo se cometen utilizando criptomonedas, redes cifradas o servidores ubicados en el extranjero.

Falta de formación profesional: Los funcionarios judiciales, incluidos fiscales, jueces, peritos forenses y policías, carecen en gran medida de una formación exhaustiva en informática y ciberseguridad. Predomina una perspectiva tradicionalista que prioriza el derecho penal y devalúa el conocimiento tecnológico. Esto genera errores de procedimiento, informes incompletos y lagunas en la evaluación de la evidencia digital. La falta de programas

sistemáticos de capacitación crea una brecha significativa entre la complejidad técnica de los delitos y las habilidades de los investigadores.

Problemas de cadena de custodia: La evidencia digital requiere protocolos específicos para su almacenamiento debido a su facilidad de alteración o eliminación. Si bien el Ministerio Público ha emitido directrices, su aplicación es inconsistente y, a menudo, depende de la experiencia individual de los peritos. Esta falta de uniformidad compromete la validez procesal de la prueba, lo que puede llevar a la suspensión de los procedimientos judiciales o al sobreseimiento de los casos por insuficiencia de pruebas.

Obstáculos a la cooperación internacional: La naturaleza transnacional de los delitos cibernéticos requiere mecanismos de cooperación flexibles. Sin embargo, Ecuador no ha implementado plenamente las directrices del Convenio de Budapest sobre Ciberdelincuencia, lo que retrasa el intercambio de datos y la asistencia judicial recíproca. Esto complica la atribución de responsabilidad por delitos cometidos por autores o cómplices en el extranjero y aumenta el riesgo de impunidad.

Factores socioculturales: Las investigaciones criminales también enfrentan barreras sociales. Muchas víctimas no denuncian los delitos por desconocimiento, desconfianza en el sistema judicial o vergüenza. Las autoridades tienden a subestimar la ciberdelincuencia, especialmente cuando no genera pérdidas económicas significativas. Esta cultura social e institucional contribuye a la baja tasa de procesamiento y a la invisibilidad del fenómeno.

En resumen, estas barreras demuestran que el sistema de justicia penal ecuatoriano aún carece de un enfoque integral para combatir la ciberdelincuencia. La falta de recursos técnicos, la capacitación inadecuada, las deficiencias en la cadena de custodia, las limitaciones en la cooperación internacional y factores socioculturales dificultan la eficacia del sistema. Superar

estas barreras requiere no solo un marco legal actualizado, sino también inversión tecnológica, la profesionalización de los funcionarios judiciales, una mayor cooperación internacional y una mayor concienciación pública sobre la gravedad de la ciberdelincuencia.

2.3.1. Prueba digital y cadena de custodia

Uno de los principales desafíos en las investigaciones de delitos informáticos en Ecuador es la gestión de la evidencia digital, que abarca su recolección, preservación y evaluación. Debido a la naturaleza intangible y fácilmente manipulable de los datos electrónicos, se requieren normas claras y procedimientos técnicos estrictos para garantizar su autenticidad y también su validez procesal. No obstante, el sistema de justicia penal ecuatoriano presenta serias limitaciones regulatorias y prácticas.

Deficiencias Regulatorias: El Código Orgánico Integral Penal (COIP) no incluye disposiciones específicas sobre evidencia digital ni regula en detalle su cadena de custodia. Las normas generales sobre evidencia que sí incluye son insuficientes, dada la naturaleza de los datos electrónicos, que pueden ser fácilmente alterados, duplicados o eliminados. Esta omisión compromete la seguridad jurídica, ya que la aplicación de criterios queda a discreción de fiscales y jueces, lo que puede llevar a la invalidación de procesos penales por falta de pruebas. La falta de un marco legal especializado también coloca a Ecuador en desventaja frente a estándares internacionales, como los del Convenio de Budapest, que establecen normas precisas para la recolección, preservación y transmisión de evidencia digital entre Estados. Sin esta

armonización, las investigaciones que involucran datos alojados en servidores extranjeros se vuelven lentas e ineficaces.

Deficiencias prácticas: En la práctica, los funcionarios judiciales enfrentan serios obstáculos. Muchas unidades de la fiscalía y la policía carecen de laboratorios forenses digitales certificados y del equipo adecuado para realizar exámenes forenses especializados. Esto limita su capacidad para realizar análisis avanzados como la recuperación de metadatos, el rastreo de direcciones IP o el análisis de dispositivos móviles modernos. La situación se ve agravada por la falta de capacitación de fiscales, jueces y peritos forenses, quienes a menudo desconocen los procedimientos básicos para el manejo de evidencia digital. Esta falta de capacitación técnica conduce a errores en la preservación de datos, la pérdida de información crucial y la interrupción de la cadena de custodia. Como resultado, las pruebas son frecuentemente impugnadas por la defensa y, en ocasiones, declaradas inválidas en los tribunales. Otro problema recurrente es la falta de protocolos uniformes para el almacenamiento seguro de evidencia digital a nivel nacional, lo que genera inseguridad jurídica y contradicciones entre casos similares.

En conclusión, las debilidades regulatorias y las deficiencias prácticas hacen que la gestión de la evidencia digital y su cadena de custodia sea un problema crítico para la persecución de los delitos cibernéticos en Ecuador. La ausencia de regulación específica en el COIP, la falta de laboratorios especializados y la falta de conocimientos técnicos de los operadores de justicia comprometen la eficiencia procesal y contribuyen a la impunidad. Por lo tanto, es fundamental promover una reforma legal que regule expresamente la evidencia digital, invertir en infraestructura forense y establecer programas de capacitación continua para garantizar que la evidencia electrónica cumpla con los estándares de confiabilidad y respeto a los derechos fundamentales.

2.3.2 Capacidades técnicas en Fiscalía y Policía

La investigación llevada a cabo para los delitos informáticos en Ecuador depende de directamente de dos instituciones principalmente: la Fiscalía General del Estado (FGE) y la Policía Nacional, esto mediante sus unidades tecnológicas. Ambas instituciones como tal han llegado a realizar esfuerzos para poder adaptarse a las exigencias de la criminalidad digital; no obstante, sus capacidades técnicas de cierta forma resultan ser limitadas y sumamente desiguales.

Los recursos que están disponibles se encuentran altamente centralizados en ciudades grandes del Ecuador como por ejemplo en Quito y en Guayaquil. Dicha concentración de cierta forma provoca que las demás provincias más pequeñas carezcan de acceso directo e inmediato a laboratorios forenses, equipos de análisis y personal especializado en el ámbito digital. En la práctica, esto obliga a que se deba trasladar la evidencia digital a las otras ciudades, lo que, por la complejidad puede llegar a generar demoras procesales y además pone en riesgo la cadena de custodia, consecuentemente afectando la validez probatoria en cualquier juicio penal que involucre prueba digital.

A dicha limitación se suma la escasez existente de peritos informáticos certificados dentro del sistema judicial del consejo de la judicatura, y que estén debidamente capacitados para tratar con delitos que involucren el uso de herramientas digitales modernas. Muchos procesos judiciales dependen de pocos especialistas, lo que inevitablemente reduce la cobertura nacional y genera retrasos en las investigaciones llevadas a cabo. Además, la falta de formación continua y permanente impide que se pueda llegar a consolidar un cuerpo técnico estable y actualizado dejando a la justicia sin posibilidad de poder hacerle frente a las nuevas modalidades bajo las que se manifiestan los delitos informáticos.

Como consecuencias de esta desfavorable situación tenemos por ejemplo muchas investigaciones penales informáticas que no prosperan, esto por ausencia de recursos tecnológicos suficientes o por las demoras en la realización de pericias, lo que a su vez incrementa los niveles de impunidad respecto a estos casos penales. Por lo tanto, mientras la criminalidad digital se continúa expandiendo con rapidez y cada vez con más sofisticación, las instituciones estatales en el Ecuador permanecen rezagadas, sin tener un plan integral que ayude al fortalecimiento de sus capacidades investigativas en el ámbito digital.

Por lo tanto, la centralización de los recursos empelados en esta área, la falta de un presupuesto estable y sobre todo la escasa profesionalización existentes respecto a peritos limitan enormemente la eficacia de instituciones como la Fiscalía General del Estado y la Policía Nacional en su lucha contra el cibercrimen. Abordar este tipo de falencias requiere que se pueda descentralizar las unidades especializadas, garantizar un financiamiento sostenido y también priorizar el hecho de invertir en el talento humano de peritos y otros operadores de justicia; estas condiciones resultan ser indispensables para poder asegurar investigaciones técnicas, oportunas y que sobre todo resulten efectivas ante los delitos informáticos.

Dentro del contexto actual, donde se puede observar una creciente digitalización a nivel global, el combate efectivo para los delitos informáticos requiere no solamente de la existencia de un marco normativo que esté debidamente actualizado, sino que también se requiere de una infraestructura tecnológica adecuada y también se requiere de un presupuesto suficiente para poder llegar a sostener todas y cada una de las capacidades operativas de las instituciones estatales responsables de llevar a cabo la investigación y propinar la posterior sanción penal a los involucrados. No obstante, en el Ecuador se enfrentan serias limitaciones tecnológicas y también

presupuestarias que de una u otra forma debilitan en gran medida su capacidad institucional para poder llegar a hacerle frente al cibercrimen.

Si observamos dicha problemática desde una perspectiva institucional, se puede mencionar que tanto la Fiscalía General del Estado como también la Policía Nacional carecen de la existencia de laboratorios forenses digitales con cobertura a nivel nacional. Por lo tanto, la investigación de delitos informáticos se da solo en las principales ciudades, e inclusive en ellas existen unidades que están mínimamente equipadas para poder darle un adecuado tratamiento a la evidencia digital, y aun así, en dichos establecimientos no se cuenta con la debida tecnología avanzada ni tampoco con el suficiente personal debidamente capacitado para que puedan llegar a afrontar las complejidades, que pueden surgir cotidianamente a raíz de la existencia de los delitos informáticos. Dicho déficit al momento de darle seguimiento a los delitos informáticos impide que se dé la recolección eficaz, oportuna y adecuada de pruebas digitales, generando de este modo múltiples vulnerabilidades en cuanto a la cadena de custodia penal y también por dichas falencias también se está comprometiendo la validez jurídica que se tiene de la evidencia digital.

Ahora bien, hablando a nivel presupuestario, es de suma importancia destacar que no existe como tal una asignación económica específica, sostenida ni mucho menos planificada para la ciberseguridad dentro del sistema judicial o dentro de la organización policial ecuatoriana. Por lo que, los recursos económicos que son destinados a esta área en específico suelen ser ampliamente escasos y por la falta de importancia que se le da, están sujetos a cambios administrativos, lo cual, en gran medida dificulta que se dé la implementación de programas de formación o capacitación técnica, tampoco se da una correcta adquisición de software

especializado e inclusive se ve afectada la contratación de peritos en el ámbito de la informática forense (Veliz & Lou, 2025, p. 34).

Dichas limitaciones presupuestarias también se pueden llegar a ver reflejadas en el débil mantenimiento que se les da a los sistemas informáticos dentro del ámbito público, esto por cuanto muchos de la gran mayoría de dichas instituciones operan haciendo uso de plataformas obsoletas, que no tienen actualizaciones regulares, y que tampoco cuentan con el respaldo técnico adecuado ni tampoco con protocolos de contingencia para hacerle frente a eventuales ataques informáticos a dichos sistemas. Por lo que, debido a esta desfavorable situación, varias de las instituciones del Estado, como por ejemplo, la Contraloría General del Estado han llegado a ser blancos de ciberataques acontecidos en los últimos años, sin que exista ningún tipo de respuesta técnica efectiva inmediata, ni tampoco medidas judiciales concretas aplicables ante dicha situación de clara vulnerabilidad (Veliz & Lou, 2025, p. 8).

Asimismo, en términos de capacitación es importante destacar que existe una brecha considerablemente significativa en cuanto al conocimiento técnico que poseen los operadores de justicia ya sean policías, fiscales y jueces, muchos de los cuales, en múltiples ocasiones no reciben la adecuada formación ni capacitación continua sobre el adecuado manejo de la evidencia digital, las medidas a tomar respecto a los delitos informáticos o también desconocen de las herramientas tecnológicas que podrían llegar a ser utilizadas. Dicha carencia educativa en cuanto a lo tecnológico genera en gran medida cierta dependencia excesiva d lo que se manifiesta dentro de los informes periciales externos, y al tener al informe como única prueba de un delito informático, se pueden llegar a propiciar errores en cuanto a la valoración de la prueba a lo largo de un proceso penal. Por lo tanto, el sistema de justicia actual, no solo se encuentra mal equipado, sino que además carece de suficiente capital humano que esté preparado para poder

llegar a afrontar la sofisticación técnica del ciberdelito a nivel nacional (Veliz & Lou, 2025, p. 35).

Además, las múltiples campañas institucionales para generar concientización y prevención en este ámbito han resultado llegar a ser insuficientes Dicha percepción evidencia que, además de las múltiples falencias técnicas que se dan internamente dentro de las instituciones del Estado, también sucede que el Estado no ha logrado de manera efectiva llegar a construir una cultura preventiva de este tipo de delitos que reduzca la exposición de los usuarios y de las organizaciones frente a los ataques informáticos que puedan llegar a ocurrir.

Hablando dentro del ámbito judicial, es importante destacar que el sistema procesal penal actual no dispone de plataformas tecnológicas que estén específicamente diseñadas para el correcto manejo de pruebas digitales, que por su naturaleza pueden llegar a contener registros de datos complejos, u otros tales como por ejemplo imágenes encriptadas, registros de IP, archivos encriptados o tráfico de redes. A todo esto también se debe destacar que el Sistema Automático de Trámite Judicial Ecuatoriano (SATJE), no se encuentra adaptado para que se dé el procesamiento de este tipo de evidencias informáticas, lo que a su vez obliga a que se incorporen documentos físicos, es decir, impresos o copias simples, lo que conlleva el riesgo de que se pueda dar la alteración o la pérdida de autenticidad del medio probatorio en cuestión (Veliz & Lou, 2025, p. 20).

Adicionalmente, por todo lo manifestado se puede llegar a determinar que a nivel institucional, las instituciones estatales actualmente no cuentan con los medios tecnológicos, ni tampoco con los medios económicos debidos para poder llegar a prevenir ni mucho menos perseguir de manera eficaz los delitos informáticos.

Además, cabe resaltar que el sistema judicial ecuatoriano en general carece de la suficiente infraestructura tecnológica, misma que por obvias razones resulta ser necesaria para poder llegar a tratar adecuadamente los delitos dentro del campo informático, y por esta misma razón los operadores de justicia enfrentan dificultades a diario para poder llegar a recolectar, preservar y también para poder presentar pruebas digitales y que las mismas puedan ser utilizadas a lo largo de un proceso penal de forma válida. Adicionalmente, es importante recalcar que la ausencia casi total de una normativa técnica y también de protocolos operativos puede llegar a agravar estas limitaciones, y por todo lo manifestado se puede generar inseguridad jurídica e inclusive impunidad por la falta de regulación adecuada dentro del ámbito informático (Veliz & Lou, 2025, p. 33).

Otro de los problemas que afectan dentro de la investigación penal informática es que no se tiene ninguna política nacional destinada para la inversión sostenida en cuanto al tema de la ciberseguridad judicial, ni tampoco para la innovación tecnológica dentro del sistema penal ecuatoriano. Dicha omisión en cuanto al ámbito presupuestario debilita en gran medida no solo la capacidad que posee el Estado para poder llegar a sancionar delitos que ya hubiesen sido cometidos, sino que también se ve debilitada su habilidad para poder llegar a prevenir nuevos ataques en cuanto a lo informático, así como también se debería buscar educar en debida forma a la ciudadanía respecto a cómo deben actuar dentro del campo informático, asimismo, se deberían desarrollar alianzas estratégicas con otras entidades del sector privado e inclusive con otros organismos a nivel internacional que estén especializados en para afrontar la ciberdefensa.

Por lo tanto, frente a esta realidad que vive el sistema judicial ecuatoriano, es de carácter urgente que en el Ecuador se desarrolle un adecuado plan nacional que fomente el fortalecimiento tecnológico y también el desarrollo presupuestario en cuanto al tema de la

ciberseguridad y también que se invierta en el tema de la justicia digital, dichas acciones para mejorar podría incluir: la asignación por parte del estado periódica de fondos públicos para que se dé la adquisición de tecnologías forenses informáticas, software especializado y actualizado para adaptarse a las nuevas tecnologías, también se debería contar con sistemas de detección de intrusiones indebidas y capacitación técnica a los profesionales del derecho que ejerzan en cuanto a lo informático. La creación de un fondo de emergencia para la respuesta a ciberataques en entidades públicas y servicios críticos. También se debería contar con la debida implementación de cierto tipo de laboratorios digitales forenses descentralizados dentro de cada provincia a nivel nacional para facilitar las labores informáticas. Asimismo sería importante considerar que se dé el desarrollo de una política clara de formación continua y permanente en cuanto a la evidencia digital, la criptografía, los análisis realizados en torno a un determinado proceso forense y que se fomente el conocimiento respecto al tema de la legislación tecnológica para todos los operadores de justicia que laboran en el Ecuador. También sería importante que las respectivas instituciones del Estado inviertan en el tema de la modernización del sistema judicial en cuanto al ámbito digital esto para permitir que exista una gestión cifrada, eficaz, segura y legítima de las pruebas digitales presentadas dentro de un determinado proceso. Igualmente deberían velarse por la generación de alianzas estratégicas con los otros tipos de actores dentro del sector privado y también la cooperación con organizaciones internacionales para que se pueda llegar a dar el desarrollo de las capacidades técnicas y el financiamiento compartido entre estas instituciones.

Por lo tanto, mientras en el Ecuador no se lleguen a resolver las limitaciones tecnológicas y también las limitaciones presupuestarias para el correcto desarrollo de las investigaciones dentro del ámbito informático, por lo tanto, si no se les da especial atención a estos puntos es

evidente mencionar que el abordaje legal que se les da a los delitos informáticos sería incompleto, carente y altamente vulnerable en cuanto a su desarrollo. Evidentemente, por todo lo mencionar, combatir el cibercrimen no sería solo una cuestión de carácter normativa, sino que también sería una decisión política y también una decisión presupuestaria, la cual exige la voluntad estatal, la visión estratégica y también la planificación a largo plazo de estos puntos para su correcta ejecución.

2.4. Falencias estructurales del sistema judicial frente al cibercrimen

Más allá de las claras limitaciones técnicas y también presupuestarias que llegan a enfrentar instituciones como la Fiscalía General del Estado y la Policía Nacional, el sistema de justicia ecuatoriano también presenta múltiples deficiencias las cuales impiden que se pueda llegar a dar una respuesta eficaz, adecuada y contundente frente al cibercrimen. Dichas deficiencias como tal no se reducen a que exista falta de equipos o de personal debidamente capacitado, sino que además se debe a un diseño institucional el cual no prioriza los delitos informáticos, uno que ni siquiera los considera relevantes como tal y que más bien refleja una visión rezagada de la administración de justicia frente a la nueva era digital en general.

El primer problema se debe a la ausencia de juzgados especializados en cuanto al tema de los ciberdelitos, esto pues contrario a otras ramas del derecho en las que se reconoce la necesidad de especialización como por ejemplo en penal, civil, contencioso administrativo, etc. El Consejo de la Judicatura hasta el momento no ha considerado la idea de crear unidades judiciales que estén dedicadas exclusivamente a la materia informática penal. Dicha situación provoca que los jueces penales ordinarios, sin ningún tipo de formación técnica ni tampoco con la debida capacitación en derecho digital, deban necesariamente resolver sobre casos altamente complejos

para su conocimiento en la materia. Como consecuencia a esta situación recae en una deficiente valoración de los medios de prueba digital y una posible aplicación errónea e inconsistente de los tipos penales relacionados con el ámbito informático.

Como segundo punto, por la falta de interés por parte de la legislación en el ámbito digital es evidente destacar que actualmente existe una falta de criterios jurisprudenciales consolidados en cuanto a materia de delitos informáticos. Por lo que, la escasa jurisprudencia disponible en el ámbito de lo digital es fragmentaria y como tal no nos ofrece lineamientos claros y suficientes sobre la interpretación que se le debe dar a ciertas figuras como por ejemplo la interferencia informática a datos, el acceso no autorizado o el fraude digital mediante el uso de criptomonedas. Dicha dispersión genera cierta inseguridad jurídica tanto para los fiscales como para los defensores de justicia, y a su vez debilita la confianza que tiene la sociedad en cuanto a la capacidad del sistema judicial ecuatoriano de enfrentar fenómenos delictivos que se encuentran en constante evolución a diario.

Otra de las deficiencias que podemos hallar es la carencia existente en cuanto a protocolos uniformes y también respecto a la coordinación interinstitucional. La agilidad con la cual deberían preservarse y analizarse las pruebas digitales contrasta en gran medida con la falta de guías operativas entre servidores públicos como jueces, fiscales y agentes de la policía. Esto incrementa el riesgo de pérdida o de contaminación de la evidencia digital, con el consiguiente peligro de que esta situación acarré la nulidad procesal respectivamente.

Por otro lado, la ausencia de peritos especializados y con suficientes conocimientos en cuanto a temas informáticos suficientes que estén certificados también genera un importante obstáculo recurrente. Dentro del sistema judicial se carece de la existencia de un cuerpo técnico estable de expertos en temas de informática forense que apoyen a los jueces mediante sus

pericias para poder comprender de mejor forma temas como el análisis de metadatos, redes o autenticidad de documentos digitales relevantes. Pero, esta situación obliga a que los juzgadores dependan casi en su totalidad de los informes periciales presentados por una parte para tomar su decisión, sin la posibilidad de contrastar o de poder ampliar criterios técnicos todo esto por su falta de conocimiento en el ámbito digital.

Dichas falencias se ven claramente agravadas por la falta de estadísticas oficiales y también de planificación judicial en materia de delitos informáticos.

Por lo tanto, el problema como tal no radica únicamente en la falta de recursos materiales, sino que también en la estructura judicial, que no ha incorporado la especialización en el ámbito de la informática, los protocolos ni tampoco la visión tecnológica que exige la nueva realidad en la que vivimos frente al tema del cibercrimen. Superar dichas falencias requiere no solo de inversión en el área de la tecnología, sino que también de una reforma institucional profunda, la cual, contemple juzgados especializados, protocolos estandarizados, formación obligatoria y continua en derecho digital y la consolidación de jurisprudencia en cuanto a lo digital.

2.5. Problemas de coordinación interinstitucional

Si se habla de la eficacia en cuanto a la investigación y la persecución de delitos informáticos hay que destacar que esta depende no solo de contar con la normativa adecuada y los recursos técnicos suficientes, sino que también requiere de una adecuada coordinación interinstitucional. En el Ecuador, uno de los más grandes obstáculos frente al cibercrimen es la fragmentación existente entre entidades estatales como la Fiscalía General del Estado, la Policía Nacional, El Consejo de la Judicatura, las unidades periciales y otras entidades con competencias complementarias dentro del ámbito judicial.

Un claro ejemplo es la relación existente entre la Fiscalía General del Estado y la Policía Nacional. Aunque la primera es la entidad que ostenta la titularidad de la acción penal pública, esta misma en algunas ocasiones suele delegar a la Policía cierto tipo de actos investigativos. No obstante, en cuanto a los delitos informáticos la delegación de competencias y funciones se vuelve de cierta forma ineficaz: muchas de las unidades policiales carecen en gran parte de personal especializado en el ámbito informático y tampoco existe un sistema compartido para que se pueda dar la gestión de las respectivas evidencias digitales. Dicha brecha ha derivado en ciertos casos en donde se asegura un dispositivo electrónico, pero el análisis forense del mismo se retrasa varios días o inclusive varias semanas porque los laboratorios también dependen de trámites paralelos en Fiscalía y Policía, rompiendo la continuidad de la cadena de custodia de dichos medios de prueba.

De manera ilustrativa, a modo de ejemplo concreto en junio del año 2020, la Contraloría General del Estado sufrió un ataque informático directamente a sus servidores, mismo que comprometió el normal y correcto funcionamiento dentro de su página web y también facilitó el ingreso no autorizado y envío de correos electrónicos haciendo uso de sus cuentas, así como también de comunicados falsos en su nombre. Dicho incidente pone claramente en evidencia las debilidades dentro de la coordinación entre entidades estatales encargadas de investigar ciberdelitos. Por tanto dentro del presente caso podemos destacar ciertas cuestiones relevantes:

2.5.1. Ausencia de canales formales y protocolos con alcance institucional

Dentro de este caso de ataque a la Contraloría, no existen informes públicos los cuales indiquen la participación coordinada de entidades como la Policía Nacional y la Fiscalía General del Estado para asegurar la información dentro de los servidores atacados, preservar la evidencia o identificar al autor de dicho fraude electrónico. En este

caso, si desde el primer momento se hubiese contado con los protocolos interinstitucionales indicados, la respuesta brindada por parte de las autoridades podría haber sido mucho más rápida y eficaz.

2.5.2. Riesgo de pérdida o manipulación de evidencia digital

La demora que hubo en la intervención de instancias forenses y también la ausencia de cultura conjunta para preservar los registros electrónicos haciendo uso de métodos como logs de acceso o metadatos pone en riesgo los elementos clave para la trazabilidad y eficacia del proceso penal informático.

2.5.3. Dificultades en la comunicación de alerta y prevención

- Al no haber canales claramente definidos de comunicación entre entidades como la Contraloría, Policía, Fiscalía y ARCOTEL o CNT, la alerta pública mediante el uso de comunicados internos o a través de redes sociales fue la principal medida de mitigación, en lugar de dar una respuesta técnica entre las instituciones antes mencionadas.

Por lo tanto, la falta de uso de protocolos conjuntos, los canales formales de comunicación y los sistemas interoperables generan una duplicidad de esfuerzos, pérdida de evidencia y también múltiples retrasos procesales, debilitando de esta forma la lucha de las instituciones del Estado contra el cibercrimen. Superar las limitaciones mencionadas con anterioridad requiere urgentemente de la implementación de una política pública integral que nos sirva para fomentar la coordinación interinstitucional, a través de mesas técnicas permanentes, protocolos unificados de actuación interinstitucional, sistemas digitales compartidos y demás mecanismos de cooperación ágil entre todas y cada una de las entidades del Estado que laboran dentro de sistema judicial ecuatoriano.

2.6. Análisis comparado con otros países de la región

En la actualidad el fenómeno de los delitos informáticos que surgen cada vez con más frecuencia ha obligado de cierta forma a todos los Estados latinoamericanos y también en general a todos los estado alrededor del mundo a tomar la decisión de replantear el ordenamiento jurídico contenido dentro de sus respectivos marcos legales y también conlleva a la necesidad de llegar a fortalecer sus capacidades institucionales con el objeto de poder hacerle frente a este nuevo y creciente fenómeno social. No obstante, en cuanto al desarrollo de las respuestas jurídicas para hacerle frente a esta nueva forma de criminalidad desafortunadamente no ha podido ser uniforme dentro de la región. Por lo que, dando la debida introducción al presente capítulo es de suma importancia recalcar que hacer un análisis comparado nos permite identificar las buenas prácticas, pero también las debilidades comunes y también las estrategias que podrían llegar a ser adaptadas por el Ecuador para que se pueda llegar a mejorar el abordaje del cibercrimen como tal. Para ello se debe acotar que la legislación ecuatoriana aún en la actualidad presenta cierto tipo de rezagos en cuanto a la tipificación, la persecución y también prevención de los delitos en el ámbito informático, situación que contrasta en gran medida con todos y cada uno de los avances logrados por otros países como por ejemplo Colombia, Chile, Argentina y Brasil.

En cuanto al caso del país de Colombia, este mismo a lo largo de los años ha sido reconocido ampliamente como pionero en la región en cuanto al reconocimiento legal de los delitos informáticos dentro de su ordenamiento jurídico. Esto a raíz de la promulgación de la Ley 1273 del año 2009, ya que en dicha ley se introdujeron algunos tipos penales específicos que están relacionados con el acceso abusivo a los sistemas informáticos, la obstaculización de datos informáticos, la interceptación ilícita de las comunicaciones y el daño informático en general. Adicionalmente, en el país de Colombia se cuenta con la denominada: Dirección de

Investigación Criminal e INTERPOL (DIJIN), dicha institución se encuentre ampliamente especializada en el tratamiento de datos informáticos que puedan verse comprometidos dentro del algún acto de ciberdelincuencia, así como también cuenta con laboratorios especializados en el tema de la informática forense, y estos poseen cobertura a nivel nacional. Dicha institucionalidad aplicada en Colombia ha permitido que se pueda llegar a mejorar la tasa de judicialización respecto a los ciberdelitos y también se ha podido llegar a establecer canales de cooperación internacional que de una u otra forma resultan ser mucho más eficientes al momento de manejar evidencia digital (Ramírez & Castro, 2020).

Mientras tanto por su parte, Chile ha podido llegar a desarrollar una estrategia más integral para poder llegar a hacerle frente a los delitos informáticos, pues la misma combina legislación, formación judicial y también cooperación a nivel internacional. Aunque dentro de la Ley N.º 19.223 del año 1993 este campo era limitado, el país chileno aprobó en el año 2022 la denominada como: Ley Marco sobre Ciberseguridad e Infraestructura Crítica, dicha ley reconoce de manera formal a los delitos dentro de lo informático como potenciales amenazas a la seguridad dentro del Estado y además establece mecanismos para que se dé una adecuada coordinación entre el Ministerio Público, la Policía de Investigaciones (PDI) y otras entidades privadas. Además de todo lo que ha sido mencionado con anterioridad, el país de Chile también cuenta con una Fiscalía, la cual, se encuentra especializada en el ámbito de los delitos tecnológicos, y también sus jueces reciben constantemente formación y capacitaciones regulares en todo lo relacionado al campo de lo informático, desde el manejo adecuado de la prueba digital, el hacking ético y también el uso de la cadena de custodia informática (Subsecretaría del Interior de Chile, 2023).

Asimismo, por su parte, en Argentina, el Código Penal habría llegado a ser modificado en el año de 2008 esto para poder llegar a incluir delitos informáticos como por ejemplo el acceso ilegítimo a sistemas informáticos, la interceptación de comunicaciones informáticas y el cometimiento de fraude haciendo uso de medios digitales. En este sentido, si bien la legislación argentina ha avanzado en gran medida, cabe mencionar que los mayores logros han sido en cuanto al desarrollo institucional. A esto, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), es dependiente de la entidad conocida como Ministerio Público Fiscal, que sería el equivalente a la Fiscalía General del Estado ecuatoriana que se encarga de liderar las respectivas investigaciones a nivel nacional y que además cuenta con las respectivas herramientas para que pueda darse la geolocalización de aquellos individuos considerados sospechosos dentro del ámbito informático, pero también se encarga de otras cuestiones relacionada con el tema como por ejemplo el análisis de malware o la conservación de evidencia digital de la manera más íntegra posible. Adicionalmente, en Argentina se han llegado a promover ciertas políticas públicas de alfabetización dentro de lo digital, esto con el objetivo de poder llegar a prevenir los delitos informáticos, todo mediante la concienciación directa hacia la ciudadana (UFECI, 2022).

En contraste de todo lo analizado con anterioridad, en el Ecuador desafortunadamente se presentan limitaciones que resultan llegar a ser significativas en contraste con el trato dado por estos otros países. A pesar de que en el Código Orgánico Integral Penal (COIP) del año 2014 se incluyeron algunos delitos informáticos, estos realmente con el pasar de los años se han quedado desactualizados frente a las nuevas y constantes amenazas que son actualizadas con frecuencia como por ejemplo con el desarrollo de algún tipo de ransomware, el uso del phishing avanzado o por ejemplo la explotación de vulnerabilidades en cierto tipo de infraestructuras críticas.

También, el Ecuador tampoco cuenta con una unidad fiscal específicamente especializada en lo informático a nivel nacional ni tiene juzgados especializados específicamente en dicha área, sus cuerpos policiales en muchas de las ocasiones carecen de una adecuada cobertura ni se tienen los equipamientos suficientes.

Otro de los factores que marcan diferencia entre otros países y el Ecuador dentro del presente tema es el uso de la cooperación internacional y también la adhesión a los tratados regionales o incluso globales donde se dé análisis a todo lo relacionado con el ámbito informático. Esto porque, mientras que en Colombia o en Chile se han ratificado al Convenio Budapest sobre la Ciberdelincuencia, lo que les permite poder llegar a intercambiar información en tiempo real con otras agencias internacionales, en el Ecuador apenas en el mes de abril del año 2024 se obtuvo el dictamen de constitucionalidad el cual permite su adhesión, según lo que habría sido resuelto en el *Dictamen 1-24-TI/24* de la Corte Constitucional (Corte Constitucional del Ecuador, 2024).

Por lo tanto, la gran falta de participación en los foros internacionales que hablan sobre temas relacionados con la ciberseguridad ha debilitado en gran medida la capacidad que tiene el país para poder llegar a enfrentar ataques de carácter transfronterizo o inclusive para poder llegar a solicitar cooperación en tiempo oportuno a otras entidades de carácter internacional.

De igual forma, observando desde el punto de vista presupuestario en contraste con el Ecuador, en Argentina se han destinado fondos específicamente para la lucha efectiva contra los delitos informáticos y se le ha dado mucha más prioridad a la modernización judicial mejorando su sistema judicial significativamente. En cambio, en el Ecuador no se cuenta con ninguna línea presupuestaria permanente ni tampoco estratégica para mejorar la tecnología forense, con la que se cuenta, ni tampoco se considera invertir en capacitación para los jueces ni en adquisición de

software moderno, especializado y actualizado a las nuevas tecnologías. Dicha situación desfavorable impide que se dé el desarrollo sostenido en cuanto a las capacidades técnicas, y además perpetúa que exista dependencia de otros recursos que en la práctica resultan llegar a ser obsoletos y poco eficientes para el combate de delitos informáticos actuales.

Otro de los aspectos comparativos que resulta relevante es en cuanto a la clara falta de formación y debida capacitación profesional, puesto que en contraste con la falta de capacitación en el Ecuador, por su parte, tanto en Chile como en Colombia, la capacitación judicial referente al ámbito de los delitos informáticos se da de manera continua, y además, ya que en la actualidad el campo de lo informático se encuentra más arraigado a la sociedad dicha capacitación también resulta ser de carácter obligatorio para estos operadores de justicia a fin de ampliar su conocimiento y consecuentemente esgrimir una mejor decisión respecto a este tema. Mas sin embargo, en el Ecuador, como se ha mencionado, no existe ningún programa nacional de formación en cuanto a cómo hacerle frente al cibercrimen, ni tampoco se da formación ni capacitaciones en instituciones como por ejemplo las academias de Policía ni en la Escuela de la Función Judicial, si bien en ocasiones existen talleres ocasionales para trata el tema, estos no suelen ser continuos ni tampoco obligatorios. Dicha situación derivada de la falta de conocimientos limita en gran medida la capacidad que poseen tanto los jueces como los fiscales para que estos mismos puedan llegar a entender y también aplicar de manera adecuada las normas respecto a la evidencia digital, el cifrado y otros tópicos como el blockchain o delitos de intercepción de datos en la nube.

Por lo tanto, el análisis comparado entra la forma en que se lleva el tema de los delitos informáticos en el Ecuador con respecto a otros países de la región como Colombia, Chile o Argentina muestra que, a pesar de que en América Latina aún se enfrentan desafíos comunes

frente a la existencia recurrente del cibercrimen, el Ecuador en la era digital que vivimos hoy en día lamentablemente se encuentra de cierta forma rezagado en varios aspectos clave mencionados a lo largo del presente capítulo como la actualización de la normativa vigente, el desarrollo institucional lento, la infraestructura tecnológica obsoleta, la falta de capacitación continua y cooperación internacional efectiva. Tomando esto en consideración, es importante observar la experiencia adquirida en los otros países entes mencionados, pues estos demuestran que sí es posible avanzar en cuanto al ámbito informático mediante el uso de reformas legales, inversión pública sostenida y también haciendo uso de la creación de múltiples unidades técnicas que se encuentren especializadas en el presente tema. Si bien en el Ecuador se desea enfrentar con eficacia los distintos tipos de delitos informáticos, para lograrlo se debería adoptar un enfoque multidimensional, que esté basado en el aprendizaje regional y que se encuentre adaptado a su contexto ya sea institucional o jurídico.

Tal como se ha podido observar a lo largo del desarrollo del presente capítulo es importante destacar que el fenómeno del cibercrimen como tal ha obligado a los Estados de América Latina a fortalecer y reformar constantemente sus marcos normativos e institucionales, esto con el objetivo de poder enfrentar una creciente y moderna criminalidad cada vez más sofisticada en cuanto a sus métodos y cuyos límites llegan a ser incluso transnacionales. No obstante, los avances realizados no han sido homogéneos. Mientras que en algunos países se han desarrollado sistemas legales e inclusive institucionales sólidos para poder llegar a responder a los delitos informáticos, en el Ecuador las reformas que se han realizado a lo largo de estos años han sido parciales y con serias limitaciones evidentes. El análisis comparado que ha sido realizado permite que se pueda identificar buenas prácticas regionales, las cuales, podrían llegar

a ser adoptadas para así poder mejorar la prevención, persecución y la sanción de los delitos informáticos.

En Colombia, se tiene la Ley 1273 del año 2009 pues esto marcó un hito en cuanto a la tipificación de los delitos informáticos, todo esto al introducir figuras específicas como por ejemplo el acceso abusivo a sistemas, la obstaculización de datos, la interceptación ilícita y el daño informático a infraestructuras digitales. Dicho marco legal, complementado con protocolos claros respecto al manejo de la cadena de custodia digital, ha permitido a los servidores judiciales contar con criterios mucho más uniformes en cuanto a la valoración de evidencia electrónica. Adicionalmente, la Dirección de Investigación Criminal e INTERPOL (DIJIN) y sus respectivos laboratorios forenses especializados en temas informáticos proporcionan gran apoyo técnico en todo el territorio, lo que a su vez reduce la impunidad y mejora en gran medida la cooperación con otros organismos internacionales (Ramírez & Castro, 2020).

Por otro lado, el país de Chile ha avanzado enormemente hacia un modelo integral mucho mejor. Si bien su Ley 19.223 del año de 1993 se ve claramente limitada, en el año 2022 se aprobó la Ley Marco sobre Ciberseguridad e Infraestructura Crítica, dentro de dicha ley se reconoce a los delitos informáticos como potenciales amenazas directas en contra de la seguridad nacional. Dicha norma obliga a la coordinación entre el Ministerio Público, la Policía de Investigaciones (PDI) y demás actores pertenecientes al sector privados. También la Fiscalía de Alta Complejidad en Delitos Tecnológicos cuenta con múltiples fiscales y demás operadores de justicia especializados en cuanto a lo tecnológico, asimismo los jueces reciben formación permanente y continua sobre la prueba digital y el correcto uso de la cadena de custodia digital, lo que nos que dentro de la legislación chilena los juzgadores aseguran decisiones judiciales más consistentes (Subsecretaría del Interior de Chile, 2023).

Por su parte en México, aunque el reto de prever y frenar la ciberdelincuencia resulta ser más complejo dada la magnitud del país, pese a ello se han logrado importantes avances. Dentro del Código Penal Federal se tipifican varias conductas como el acceso ilícito, el fraude informático y la revelación indebida de datos, mientras que por su parte la Ley Federal de Protección de Datos Personales sirve para poder llegar a complementar la defensa de la privacidad en el ámbito informático. Institucionalmente, existen autoridades especializadas como la Policía Cibernética de la Guardia Nacional la cual coordina investigaciones junto con otras fiscalías estatales y federales, todo esto aplicando protocolos avanzados de cadena de custodia digital esto para poder evitar futuras nulidades procesales que entorpezcan las actuaciones de los servidores de justicia mexicanos. De igual forma, en México se ha fortalecido la cooperación internacional, especialmente mediante su continua y constante participación en la Red 24/7 de la INTERPOL, esto permite una respuesta mucho más rápida a ciertas solicitudes de información en casos transnacionales (González, 2021).

En contraste a los países antes mencionados, en el Ecuador evidentemente se nos muestra un rezago significativo frente a las regulaciones vigentes en otros Estados. Aunque dentro del COIP del año 2014 se incluyó algunos delitos informáticos, las figuras presentadas ahí son muy generales y no abarcan las nuevas modalidades de delitos informáticos como por ejemplo el uso de ransomware o el phishing avanzado. En contraste con Colombia o con Chile, no existe ningún tipo de protocolos unificados ni de cadena de custodia digital o laboratorios forenses operativos en todas las provincias del país, lo que inevitablemente genera riesgo de nulidad de pruebas digitales. Adicionalmente, en el Ecuador aún se carece de fiscalías especializadas y de juzgados especializados en temas de ciberdelincuencia, de igual forma la capacitación de jueces y de fiscales es escasa y tampoco resulta ser obligatoria. Hablando en el plano internacional, mientras

que en países como Chile y Colombia ya han ratificado el contenido del Convenio de Budapest, en el Ecuador recién en el año 2024 se obtuvo un dictamen de constitucionalidad para que se pueda dar su adhesión, lo que indudablemente ha retrasado la cooperación ágil en casos de delitos informáticos que se manifiestan de manera transnacional (Corte Constitucional del Ecuador, 2024).

Por lo tanto, el contraste regional existente entre la legislación de otros países y el Ecuador evidencia que la modernización dentro de la normativa deberá ir acompañada de inversión institucional y también de coordinación interinstitucional. Los casos de Colombia, Chile y México nos demuestran que sí es posible avanzar en este ámbito con reformas legales claras, protocolos especializados en cuanto a la evidencia digital, y programas de capacitación continua y permanente para los ciudadanos ecuatorianos.

Capítulo 3: Estudio del caso: ataque informático a la Contraloría General del Estado (2019)

3.1. Contexto histórico y político del ataque

Durante el año 2019 Ecuador fue víctima de una serie de ataques informáticos que posicionaron al país en el quinto lugar de los países con más ciberdelitos, esto hasta el año 2024, pues, se ha convertido en el blanco más fácil para ciberdelincuentes, ya que, varios de estos delitos han consistido en el engaño y confusión a los usuarios de plataformas digitales con el fin de conseguir que se comparta información privada o confidencial, en dónde se extraen contraseñas o incluso números de tarjetas de crédito y datos bancarios (Lago,2024).

Kaspersky, una empresa dedicada a la ciberseguridad de Rusia examinó los ataques informáticos sucedidos en América Latina y determinó una creciente ola de ciber delitos, siendo así que se aumentó en un 6% la cantidad de inseguridad en los diferentes tipos de plataformas digitales. Después de este estudio, se llegó a la conclusión de que Ecuador con un total de 12.2 millones de ataques anuales está dentro del top global de ciberdelincuencia (Kaspersky, 2024).

La Contraloría General del Estado, institución estatal encargada del cuidado y buen uso de los recursos que posee el Estado dio aviso a las autoridades sobre un incendio en su edificio el día 12 de octubre del 2019 durante el paro nacional extendido en todo el territorio ecuatoriano, un grupo de personas encapuchadas ingresaron de manera sospechosa al edificio de la Contraloría después del mediodía, accediendo a las oficinas de los servidores públicos y también la terraza del edificio en dónde, alrededor de las 18:00 horas desataron un incendio, el cual dejó tras de sí terribles consecuencias, a nivel de infraestructura y daño a sistemas informáticos en la sede ubicada en Quito (Primicias, 2020).

Posteriormente aconteció un ataque informático en sus sistemas, que además, se repitió constantemente. Se sabe hasta ahora que los ciberdelincuentes se encargaron en utilizar la información sustraída para enviar diferentes tipos de telecomunicaciones y correos electrónicos fraudulentos a los diferentes ciudadanos ecuatorianos. Estás acciones afectaron el funcionamiento y actividades de la página web y a las tareas de los funcionarios públicos de la Contraloría; se programó una reunión inmediata entre la fiscal Diana Salazar y el contralor Pablo Celi en el edificio de la Contraloría el día 6 de noviembre del 2019, en dónde como punto principal se conversó sobre la poca seguridad informática que poseen los sistemas digitales en los que reposa la información de los ciudadanos (Primicias,2020).

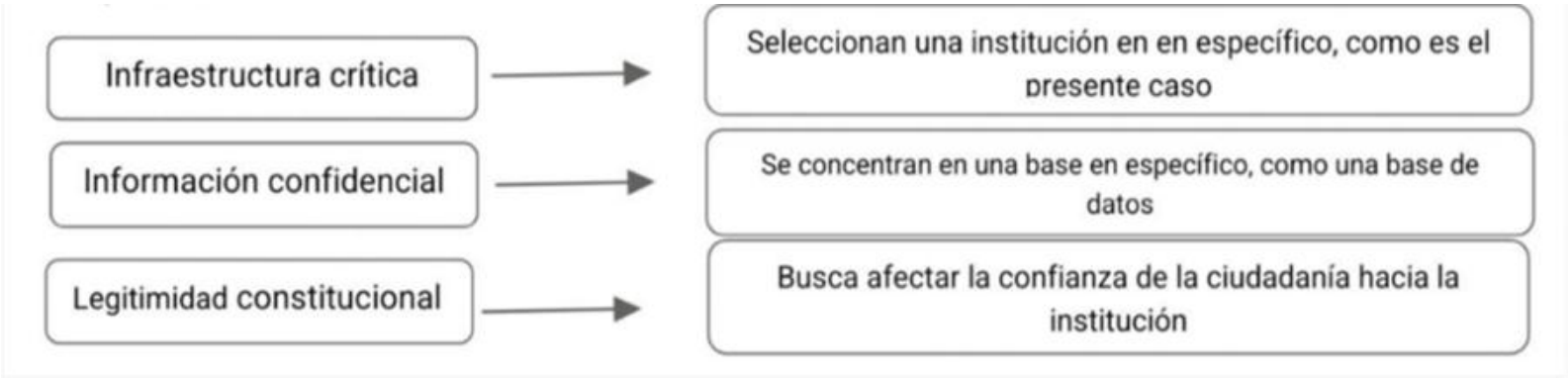
Sin embargo, lastimosamente, la Contraloría y sus autoridades no supieron actuar de acuerdo a las necesidades del caso y emitieron un comunicado en dónde se pidió a los ciudadanos evitar brindar información o responder a diferentes correos electrónicos a menos de que sea emitido desde fuentes oficiales de la Contraloría General del Estado (Primicias, 2020).

El día 05 de junio del 2020 se vuelve a emitir un comunicado en dónde se avisa a la ciudadanía sobre una nueva serie de ataques informáticos, posteriormente, sus autoridades se

encargaron de desestimar todos los correos cercanos a esa fecha que se emitieron bajo el nombre de la institución pública, se vio la repetición de las mismas acciones ocurridas en el 2019. Aunque está vez se esperaba una mejor reacción por parte de la Contraloría no existió ningún tipo de protocolo o auxilio legal para esta situación, por lo tanto, simplemente se emitió otro mensaje de alerta para ignorar cualquier tipo de telecomunicación que no provenga de una fuente oficial (Pichincha,2020).

3.2. Caracterización del ataque informático

Desde el punto de vista legal, los ataques informáticos se caracterizan primordialmente por la manera en la que afectan a los ciudadanos, la seguridad jurídica del pueblo, y las funciones



de las instituciones públicas, pues la información que reposa en las bases de datos dentro de los aparatos electrónicos es interferida y desestabilizada por ciberdelincuentes con el único objetivo de extraer datos personales con carácter privado (ZUMBA, 2022).

Para el Ecuador, este tipo de ciberdelitos son consecuentes en el daño tecnológico de manera específica, pero vulneran bienes jurídicos protegidos (privacidad, intimidad, confidencialidad, etc.) siendo estos protegidos por la Constitución de la República y el Código

Orgánico Integral Penal, entre otra normativa que contemplan diferentes conductas sancionables.

Gráfico de mi autoría*

Se sabe perfectamente que los ataques informáticos no se realizan de forma aleatoria, de hecho, en el caso del ataque dirigido a la Contraloría General del Estado se siguió un proceso en específico para determinar su ataque y lo que se desea conseguir del mismo, el cual, al igual que varios ataques a diferentes plataformas hay tres objetivos a los cuales se dirige este ataque a tener en cuenta.

3.2.1. Mecanismos utilizados

Para realizar un ataque informático se puede utilizar diferentes herramientas y procesos que cuando se combinan generan un fortalecimiento de estructura tecnológica, generando un daño inmediato que se extiende en un considerable periodo de tiempo, entre esos mecanismos, podemos observar los siguientes.

El uso combinado de diversos vectores de ataque fue una herramienta informática utilizada de forma evidente durante el ataque a la Contraloría, pues, al ser una institución del Estado, los ciberdelincuentes buscan diferentes factores que les ayuden a incrementar su porcentaje de éxito, por ende, si el delito se lleva a cabo de forma simultánea y siguiendo una secuencia se interrumpirá las funciones de la base de datos y de los funcionarios públicos. En nuestro caso, las conductas delictivas a utilizar se destacan por phishing en cooperación de spear phishing, pues se emitieron una serie de correos electrónicos con carácter fraudulento, engañando a los servidores públicos y también a los ciudadanos (Mieres, 2009).

Ataque DDoS, la contraloría sufrió saturación en todos sus servicios institucionales, producto de una serie de solicitudes emitidas con el objetivo de alcanzar el colapso de los servicios y la plataforma web. Ataque de Insiders, los ciberdelincuentes aprovecharon la existencia de servidores que estaban involucrados en acciones corruptas y negligentes, teniendo así mayor facilidad durante su ingreso a la institución (Pichincha, 2020).

Se puede decir que, el ataque sufrido por la Contraloría General del Estado es un Sabotaje Digital, el cual aconteció por medio de Malware y un ataque dirigido, debido a que el fin de este no fue netamente económico, sino que se presenció la interrupción y detrimento a la infraestructura tecnológica de la institución estatal, de hecho, los reportes que se consiguieron establecieron los servidores públicos de dicha institución presenciaron la perdida de la información dentro de las bases de datos. Se podría llegar a decir que este delito se encuentra tipificado con el artículo 232 del Código Orgánico Integral Penal, sin embargo, como se ha mencionado anteriormente la tipificación del mismo es bastante general, lo cual conlleva a un vacío legal que deja en la impunidad a este tipo de conductas delictivas.

3.2.2. Vulnerabilidades explotadas

Un elemento fundamental de los ataques informáticos que estuvo presente al momento del ataque que se dio en contra de esta institución estatal fueron los daños de derechos protegidos por la Constitución ecuatoriana, entre estos, la seguridad de la información pública e integridad de los sistemas informáticos, por otro lado, se alteró la confidencialidad de los datos personales de los ciudadanos y se perdió el interés y la cooperación pública (Cabrera, 2017).

Varios bienes jurídicos fueron vulnerados de forma directa con estas acciones, haciendo que los ciudadanos se preocupen por las facultades legales que les corresponde, se perdió de forma intempestiva la seguridad que deben brindar todos los sistemas públicos, misma que se

encuentra tipificada en el artículo 232 del COIP, el cual contempla el ataque a la integridad de sistemas informáticos (Pino, 2016).

Pero, dentro de este artículo, no se contemplan situaciones actuales en donde los derechos humanos corren la posibilidad de ser afectados, como lo es el caso de ataques combinados, y el uso de diferentes tipos de conductas delictivas, de hecho, no se exploran las diferentes consecuencias de estas acciones, pues solo se concentra en la acción, en el caso del ataque a la Contraloría el país entero resultó vulnerado, pues, se exhibieron datos personales que comprometieron la privacidad y la integridad de la sociedad.

Por lo tanto, se debe contemplar una mayor precisión al momento de la tipificación de delitos informáticos más complicados, Ecuador ha sido susceptible a una gran cantidad de vacíos legales, procesales e incluso técnicos que ha dado paso a una facultad muy limitada para la investigación y sanción de delitos informáticos, pues las instituciones públicas del Estado como lo es la fiscalía quien se encarga de la investigación de delitos no cuenta con un cuerpo legal que contenga un proceso especial para casos informáticos, y si bien, se encuentran ciertos delitos contemplados en la ley no se puede decir que los mismos logren englobar las diferentes situaciones sociales por las cuales la sociedad está atravesando (Pino, 2016).

Desde la perspectiva jurídica el ataque informático puede subsumirse a la vulneración a nivel constitucional del artículo 82, pues existe la creación de una gran dificultad al momento de obtener un buen control sobre el acceso a la información pública. Una posible solución a esta problemática actual es la actualización y capacitación de nuestro sistema legislativo y por supuesto la emisión de nueva doctrina y jurisprudencia que se dedique específicamente al análisis y solución de casos informáticos actuales que se vean con más repetición. Si nuestros juristas y doctrinarios emitieron nuevos estudios en dónde se destaquen temas sobre ciberdelitos

y su correcto proceso y sanción lograríamos asegurar la protección de derechos humanos constitucionales.

Por lo ende, es claro que se necesita de manera urgente la tipificación de delitos concentrados en temas como:

1. La creación y propagación de sistemas malware
2. Secuestro y retención ilegal de bases de datos por medio de ransomware
3. Ataque de DDoS a nivel institucional

3.3. Evaluación del daño a sistemas y datos institucionales

Con la creciente digitalización de los sistemas estatales se ha aumentado la posible vulneración en el funcionamiento de sistemas informáticos en contraste con los sistemas informáticos. Para la jurisdicción ecuatoriana y la evaluación que destina a los detrimentos ocasionados por esta clase de delitos es necesario crear puntos claves que centralicen la forma en la que se determina la sanción penal y con eso la reparación integral a cargo del estado (Cabrera, 2017).

En medio del ataque informático acontecido a la Contraloría se debilitó a su archivo digital, servidores y sus bases de datos, en ellas se contenía la información sobre auditorías, procesos de control y documentos Probatorios con contenido que probaba diferentes casos de corrupción. La pérdida a niveles materiales y físicos fue descomunal, sin dejar de lado la perdida y alteración de diferentes datos primordiales para el desarrollo de la función fiscalizadora del país, con esto, tambaleando por completo la transparencia del sistema y la seguridad jurídica.

Para la rama del derecho penal en Ecuador, todos estos actos tienen la probabilidad de encuadrarse en distintos tipos penales, como lo es el caso del delito de ataque a sistemas

informáticos, mismo que se encuentra tipificado en el artículo 234 del COIP, en este apartado se sancionar a cualquiera que acceda, interfiera, dañe o intercepte sistemas informáticos sin autorización previa (Pino, 2016).

Con este análisis de los sistemas afectados no simplemente se limita a daños económicos, sino más bien, englobar el impacto que el mismo tiene hacia la función pública y las consecuencias como la obstrucción de procesos legales y administrativos, contando también con el detrimento a la confianza del pueblo hacia el sistema de justicia.

En nuestro caso de investigación lamentablemente es imposible recuperar varios de los archivos digitales que fueron vulnerados y se comprometió con esto el proceso de fiscalización que se encontraban en curso. Hay una alteración inmediata al derecho a la verdad, e incluso la lucha que enfrenta el país en contra de la corrupción, sin dejar de lado que todo esto son derechos protegidos constitucionalmente en los artículos 204 y 208 de la Constitución de la República del Ecuador.

La manera en la cual se evalúan daños informáticos debe ser realizadas por peritos certificados que se destaquen por su especialización en el tema, lograríamos así la determinación correcta de que tan grande puede ser una pérdida de datos y conseguir trazar la ejecución del ataque, consiguiendo así saber si puede ser posible o no que se recupere la información afectada. Se puede clasificar a los daños sufridos durante este ataque de la siguiente manera:

Clase de Daño	**Daño**	**¿De qué manera?**
Materiales	Equipos de hardware, alteración de base de datos, interrupción de servicios informáticos	El ataque informático causo detrimento en la infraestructura en donde se guardaban datos tecnológicos, pues, el malware elimino registros informáticos que poseían información sobre auditorias. Por otro lado, la paralización que sufrió la red impidió el desarrollo y continuidad de las funciones de los servidores públicos.
Jurídicos	Vulneración al principio de transparencia y seguridad jurídica, afectación al debido proceso	Con el extravió de la información y las auditorias en casos anticorrupción se obstaculizo la certeza de los procesos de control, vulnerando así directamente el artículo 82 de la Constitución.

		Este ataque informático impuso obstáculos ante la Contraloría para que esta no pueda mantener el control sobre la forma en la que se administran los fondos públicos. Afectando al artículo 3.8 de la Constitución el cual vela por el derecho a vivir en un país libre de corrupción. Para cuando se dio la perdida de documentos oficiales, el artículo 76 de la Constitución fue violentado, teniendo en cuenta que genero una situación de riesgo e impunidad en los diversos casos de corrupción, los cuales estaban siendo seguidos por parte de la Contraloría, ya que, para entonces se daría la pérdida total de elementos probatorios útiles en el proceso judicial. Todo esto ha logrado incrementar la posibilidad de que se comentan actos ilícitos a sabiendas de que la probabilidad de impunidad es más alta que la de emitir una sanción justa.

Tabla de mi autoría*

La evaluación de los daños en el ataque a la Contraloría es un serio problema a nivel penal y administrativo en nuestro país pues, no simplemente compromete a la infraestructura tecnológica, sino que vulneran las funciones principales del Estado y sus funcionarios. Entre las problemáticas actuales más preocupantes se encuentran la siguientes:

Problemática:	**Solución:**
Ausencia de mecanismos jurídicos para determinar el daño judicial	Ampliamiento normativo en COIP en dónde se añadan nuevas descripciones de daños informáticos y se incluyan los detrimentos informáticos constitucionales, si se diera una actualización de este cuerpo normativo entonces se conseguiría la incorporación de criterios tanto cuantitativos como cualitativos y se exploren tema como los diversos grados de afectación (incluyendo los servicios públicos, como es el caso de la Contraloría) o el tipo de datos que se vieron vulnerados. Se podría incluso llegar a comprender las consecuencias de este tipo de delitos, como la confidencialidad o temas estraticos e incluso personales. Esta nueva actualización no deberá dejar de lado el daño causado por la alteración de procesos administrativos y judiciales o el costo que se obtendría de este tipo de altercados.
Ineficacia en la cadena de custodia digital y obtención de evidencia	Adoptar la creación de protocolos a nivel nacional con el afán de preservar la evidencia digital, este protocolo tendría que ser obligatorio a nivel de instituciones públicas y se incluiría la actuación continua y conjunta con fiscalía y la policía nacional en dónde la recolección obtenga una estandarización y resguardo para lograr un análisis forense profundo a nivel de elementos de convicción.
Carencia de políticas públicas de ciberseguridad institucional	La ciberseguridad en el campo de instituciones estatales carece completamente de políticas públicas que vele por la seguridad digital de sus bases de datos, es de urgente necesidad crear responsabilidades, auditoría digital y por supuesto,

	brindar al ciudadano respuestas inmediatas y claras a los distintos tipos de problemáticas cibernéticas actuales.
Inexistencia de protocolos y coordinación interinstitucional para judicialización	La posible solución más idónea para este conflicto es la creación y trabajo conjunto de unidades judiciales centradas en la ciberseguridad, misma que posea servidores especializados en temas como la informática forense, derecho penal tecnológico y derecho cibernético, esto con el propósito de obtener mejores procesos de judicialización de estas conductas penales.

Tabla de mi autoría*

3.4. Reacción institucional y medidas adoptadas

La Contraloría General del Estado es un órgano imprescindible centrado en el control fiscal a nivel nacional, no obstante, jamás se había tomado en cuenta posibles, situaciones críticas, y por este motivo, cuando el ataque físico y cibernético golpeó en el 2019 y se repitió en el 2020 sus métodos de protección, prevención e investigación fueron inexistentes. Este acontecimiento fue tan grave que la ciudadanía no se concentró únicamente en la perdida datos sino también en como desestabilizó la seguridad jurídica, veracidad y control contra la corrupción.

Desde una perspectiva legal, este ataque saco a la luz problemas que engloban estructura y desarrollo, primeramente, se presencia como se afecta al desempeño de la base de datos públicos, ya que, no había existencia previa de medidas eficaces que prevengan con protocolos de recuperación de datos y protección de información en caso de que se suscite un posible desastre informático.

La clara ineficacia del sistema legal causó la colisión de los artículos 226 y 227 de la Constitución de la República del Ecuador en donde se obliga a las instituciones estatales a implementar sus funciones con coordinación y responsabilidad.

Cómo segundo punto, se expuso la falta y necesidad de una legislación centrada en ciberseguridad en nivel Estado, incluso si el COIP, en su artículo 232 establece sanción al daño

dirigido a sistemas informáticos, en esta tipificación se presenta insuficiencia frente a diversos tipos de escenarios en dónde la complejidad del mismo aumente por diferentes factores sociales, estos riesgos acarrean hechos activos como sabotaje digital y la pérdida masiva de datos públicos, colocando al país en momentos de inseguridad críticas.

Desde una sociedad moderna que enfrenta cada día conflictos legales que se adaptan al avance tecnológico se puede observar que la ausencia de normativas que dirijan el correcto servicio de instituciones estatales puede enlentecer e incluso dejar en la impunidad este tipo de actividades delictivas, pues en el caso del ataque a la Contraloría las respuestas que las autoridades emitieron fueron tardías y dispersas. La inexistencia de algún ente rector que como único objetivo sea la seguridad digital contradice el principio constitucional de eficiencia administrativa, además de estorbar el proceso de judicialización de los responsables (Pino, 2016).

Durante el ataque que sufrió la institución estatal de nuestro interés no existía ninguna ley que ampare lo acontecido, hasta el año 2021 en donde se da la promulgación de la Ley Orgánica de Protección de Datos Personales, y, aun así, en esta norma, lo único que se puede apreciar es el establecimiento de parámetros de seguridad digital con aspecto personal.

Debido al ataque informático perpetrado en contra de la Contraloría General del Estado, incentivo a la Política Nacional de Ciberseguridad del año 2022 para que sea un respaldo que responda a la necesidad de generar respuestas en situaciones relacionadas a ataques informáticos, dentro de esta política se analiza ciertos lineamientos en donde se destaca la protección a infraestructuras y el fortalecimiento de instituciones, esto con bases normativas, teniendo en cuenta todo lo sucedido en el ataque a la Contraloría, se puede decir que esta Política actual, se vincula con nuestro caso de estudio. El vínculo existente entre el ataque y la promulgación de

esta ley es bastante claro, el primer punto a destacar fue esta demostración empírica de cuan vulnerable es el Estado cuando se trata de amenazas cibernéticas; y, como segundo punto se tiene a la respuesta legal estratégica que esta específicamente destinada a la mitigación de posibles riesgos futuros.

Este ataque sufrido sirvió para motivar y acelerar la adopción de la Política Nacional de Ciberseguridad del Ecuador, siendo considerado como un antecedente directo dentro del avance que puede alcanzar el derecho en cuanto a ciberdelitos, podría incluso alcanzarse niveles más altos y satisfactorios de seguridad jurídica, seguridad digital, y la eficacia de los derechos humanos a nivel estatal.

La reacción que se obtuvo por parte de la Contraloría General después de lo acontecido fue reactiva y a su vez limitada, con esto se consiguió la continuidad de las obligaciones de los servidores ppúblicos, estas medidas fueron:

1. Recuperación parcial de la información perdida gracias a copias y respaldos

2. Constantes denuncias presentadas ante fiscalía en dónde se cita el artículo 232 del COIP, de las cuales, hasta la actualidad ninguna ha conseguido ser atendida de manera satisfactoria, de hecho, la investigación que se dio en los casos relacionados con la perdida de datos genero desconforme social y legal, pues la normativa nacional volvió a tambalearse en cuanto se vio la necesidad de nuevas leyes que velen por garantizar el cumplimiento de derechos fundamentales.

3. Se dio contratación de servicios tecnológicos, los cuales no fueron de mucha utilidad, debido a que para cuando se decidió actuar para recuperar la información, los datos ya se habían extraviado. Se puede decir que algunos fueron recuperados de forma parcial, sin embargo, otra parte se perdió totalmente.

Estas medidas adoptadas fueron especialmente utilizadas para conseguir estructuras digitales fuertes, a su vez la Contraloría acudió a la ayuda de organismos interinstitucionales para que con su apoyo técnico se refuercen los sistemas que almacenan información en la nube. Ahora bien, incluso si la práctica de estas medidas fue importante no fue de mucha utilidad para que se alcance a solventar la perdida de varios archivos documentales.

Para la jurisprudencia, en la sentencia emitida por la Corte Constitucional del Ecuador con el número 2064-14-EP/21 se dio la tarea de reconocer la forma en la cual se vulnera los datos informáticos e institucionales, así como el derecho a la intimidad, honra e incluso la autodeterminación informativa, por ende, estás barreras demuestran la necesidad de crear una mayor protección para garantizar el cumplimiento de derechos que reposen en sistemas informáticos de entidades públicas.

Por otra parte, en la sentencia con número 1145-19-EP/22 resalta la obligación de la cuales son portadoras las instituciones estatales para proteger la información que está vinculada con el principio de seguridad jurídica, esto incluso al momento en el que se adapten medidas tecnológicas que puedan hacer frente a todos los riesgos informáticos (Ponce, 2021).

Capítulo 4: Principios y lineamientos para una política criminal integral

4.1. Importancia de una política criminal en delitos informáticos

Para el desarrollo del presente apartado es oportuno mencionar que el crecimiento exponencial que ha dado la tecnología en cuanto al ámbito digital ha ido transformando profundamente la forma en la que se desarrollan las dinámicas sociales, las dinámicas económicas y también las jurídicas alrededor del mundo actual. No obstante, es evidente que de la mano con este proceso de cambio, también han surgido los delitos informáticos, también denominados como ciberdelitos o también como cibercrímenes, los cuales han ido adquiriendo un protagonismo que resulta ser creciente, al ser actualmente una de las formas más complejas, modernas, anónimas e inclusive transnacionales para poder llegar a cometer actos de criminalidad contemporánea. Por lo tanto, frente al este nuevo y creciente fenómeno, el Derecho Penal como tal, no puede llegar a actuar de una forma aislada ni reactiva, lo cual minimiza su eficacia para hacerle frente a estos novedosos delitos, sino que el derecho penal debe de integrarse dentro de un marco normativo que resulte ser coherente, sistemático y prospectivo,

esto con el afán de darle un mejor tratamiento a este tipo de ilícitos: o sea, se requiere de una política criminal que resulte ser integral y especializada en este ámbito informático.

Primeramente se debe comprender qué es una política criminal, para ello, en términos generales, esta puede llegar a definirse como el conjunto de los principios, las estrategias y las acciones llevadas a cabo por el Estado y que están orientadas a prevenir, a controlar, a investigar e inclusive a sancionar la criminalidad, esto acorde a los fines constitucionales reconocidos dentro de la Constitución de la República, como por ejemplo la seguridad jurídica, la tutela de derechos fundamentales de las personas y la defensa del orden social en general. En este caso específico, hablando de los delitos informáticos, es menester comprender que la apremiante necesidad de instaurar una política criminal cobra una importancia fundamental, esto no solo por la complejidad técnica que supone el cometimiento de estos delitos, sino que también por el creciente impacto que ha ido adquiriendo estos delitos dentro de la seguridad nacional, la economía, la confianza de la sociedad en cuanto a lo digital y la protección de bienes jurídicos adicionales que emergen como por ejemplo la identidad digital de la persona, la privacidad informática y la integridad de los sistemas de datos informáticos.

Hablando específicamente dentro del contexto ecuatoriano, tal como se ha podido llegar a evidenciar a lo largo del desarrollo del presente trabajo de titulación, la respuesta institucional que las autoridades pertinentes dentro del Estado ecuatoriano han dado frente a la ciberdelincuencia ha sido claramente dispersa, incompleta, limitada y deficiente. Por lo que, la clara falta de un enfoque de política criminal en el Ecuador ha dado lugar a un conjunto de medidas que están aisladas, sin coordinación interinstitucional alguna, sin planificación previa ni tampoco se cuenta con el debido respaldo presupuestario sostenido por parte del Estado. Dentro del presente escenario, el hecho de que como sociedad intentemos avanzar hacia una renovada

política criminal que refiera específicamente a los delitos informáticos se vuelve cada vea más de carácter indispensable para poder llegar a superar las deficiencias estructurales que se presenten, así como también brindar una respuesta en el ámbito penal que sea mucho más inteligente, más eficaz e inclusive respetuosa de los derechos humanos reconocidos constitucionalmente.

Además, uno de los aspectos centrales en torno a la política criminal dentro de la presente materia es la definición clara de aquellos bienes jurídicos los cuales se buscan proteger. A diferencia de cómo se han venido manifestando los delitos comunes a lo largo del tiempo, cabe mencionar que actualmente los delitos de carácter informático pueden llegar a afectar bienes que en múltiples ocasiones resultan llegar a ser intangibles, difusos o por su naturaleza también novedosos, estos comúnmente llegan a interferir con la seguridad de los sistemas de datos informáticos, esto con el objetivo de vulnerar la integridad de datos, el acceso a la información reservada, la identidad digital de un determinado individuo o la confianza pública dentro de las plataformas electrónicas donde a diario circula información de índole personal. Dicha situación genera gran complejidad, y para poder responder adecuadamente es necesario mencionar que es importante exigir un enfoque penal mucho más moderno, mismo que ayude a reconocer la autonomía de dichos bienes jurídicos y evite que las respectivas autoridades lleguen a subsumirlos forzosamente dentro de figuras tradicionales como el hurto o el fraude, tipo penales que dentro del presente caso pueden llegar a resultar ineficaces (Veliz & Lou, 2025, p. 24).

La política criminal en torno al presente tema debe abordar igualmente la dimensión preventiva del delito, es decir, se debería llegar a promover cierto tipo de medidas estructurales para poder llegar a reducir los factores de riesgo que generan estos delitos, y asó poder aumentar la resiliencia dentro del entorno digital. Por lo tanto, resulta ser esencial combinar los preceptos jurídicos inherentes al derecho penal con ciertas políticas públicas que ayuden a fomentar la

educación dentro de lo digital, la alfabetización tecnológica, la promoción de buenas prácticas dentro del ámbito de la ciberseguridad y la protección de cierto tipo de datos personales, mismos que por su naturaleza podrían llegar a vulnerar gravemente los derechos de las personas al ser interceptados y utilizados con fines delictivos. Por tanto, la prevención dentro del ámbito de los delitos informáticos no solo debería recaer en la potencial víctima, sino que también debería recaer en el Estado, quien tiene la primordial obligación de poder generar entornos dentro de lo tecnológico que resulten ser mucho más seguros y accesibles para todos quienes son partícipes dentro de lo informático a diario.

Además, otro de los ejes centrales resulta ser la formación especializada, así como la debida y continua capacitación de los operadores de justicia que laboran cotidianamente en las instituciones del Estado, esta formación dentro de lo tecnológico incluye servidores públicos como por ejemplo los jueces, los fiscales, los defensores públicos, los peritos especializados dentro del ámbito informático e inclusive el personal policial. Una política criminal adecuada no puede ejecutarse correctamente con operadores de justicia, los cuales, por su falta de capacitación informática desconocen en su totalidad los fundamentos técnicos que rodean al delito que deben investigar y posteriormente juzgar, razón por la cual, el diseño de un nuevo sistema nacional que se preocupe por brindar capacitación en cuanto a la cibercriminalidad, la evidencia digital y el manejo de la prueba tecnológica resulta ser un componente insustituible e inherente a cualquier tipo de nueva política criminal integral que busque adecuarse a la modernidad y poder combatir de manera eficaz los delitos informáticos que constantemente pueden llegar a surgir dentro de la sociedad (Álvarez & Maldonado, 2020).

De igual forma, la política criminal deberá de llegar a contemplar el fortalecimiento de la infraestructura institucional, así como de la tecnológica aplicada por servidores públicos dentro

del sistema penal ecuatoriano. Esta situación implica que se debería llegar a dotar a la Fiscalía General del Estado y también a la Policía Nacional de instalaciones que cuenten con los equipos adecuados para la investigación dentro de lo informático, es decir, se debería instaurar laboratorios forenses que sean modernos, que posean software especializado, plataformas interoperables para facilitar la cooperación entre instituciones del Estado, y también personal técnico que esté debidamente capacitado para cumplir con dicha labor, por lo que, si no se cuenta con los recursos adecuados para hacerle frente a los delitos informáticos, cualquier tipo de plan de combate contra el cibercrimen será meramente declarativo. Además, la inversión pública sostenida, bajo cierto tipo de criterios como por ejemplo la eficiencia y transparencia, resultan ser elementos clave dentro de una política criminal efectiva contra los delitos informáticos.

Si hacemos referencia al plano internacional dentro del presente tema, es importante mencionar que una política criminal que busque erradicar el cometimiento de ciberdelitos deberá también basar sus actuaciones haciendo uso de la cooperación transnacional y también respetando el cumplimiento de compromisos internacionales destinados a ello, como por ejemplo el Convenio de Budapest sobre la Ciberdelincuencia, el cual ha sido recientemente aprobado por el Ecuador. Dentro de dicho tratado se establecen cierto tipo de estándares mínimos para la tipificación penal informática, la cooperación internacional, los mecanismos de conservación de datos informáticos y como se deberían llevar los principios que conforman el debido proceso en cuanto al tratamiento de la evidencia digital que pueda aparecer dentro de un determinado caso. El tratar de incorporar dichos estándares dentro de una política criminal aplicable dentro del territorio ecuatoriano, le permitiría al país no solo poder llegar a mejorar su respuesta interna a los distintos tipos de delitos informáticos, sino que además ayudaría a articularse con la

comunidad internacional en cuanto a la lucha en contra de este tipo de delitos, los cuales, por su naturaleza no reconocen fronteras.

Asimismo, la política criminal también debe contemplar la existencia de una dimensión ético-política dentro del uso del derecho penal para hacerle frente al cibercrimen. Esto significa que el Estado deberá garantizar en todo momento que las medidas adoptadas para poder llegar a combatir los delitos informáticos no vulneren por ningún motivo los principios inherentes a todo proceso como por ejemplo la legalidad, la proporcionalidad, la presunción de inocencia del procesado o el respeto a la privacidad de las personas. Es decir que, una política criminal que resulte ser integral no solo deberá llegar a ser eficaz, sino que además, deberá ser también garantista de los derechos, estos preceptos pueden llegar a verse en conflicto o vulnerados, por ejemplo, con el uso de tecnologías de vigilancia, programas de geolocalización o monitoreo de redes de comunicación informática, razón por la que, dichas interferencias deberán estar sometidas a controles judiciales recurrentes y la emisión de normas claras, las cuales, ayuden a evitar posibles abusos por parte de las autoridades encargadas de manejar dicha información, fomentando por encima de todo la protección de los derechos fundamentales de los ciudadanos ecuatorianos (Gómez Patiño, 2016).

De esta forma, una política criminal especializada en los delitos informáticos podrá ser concebida como un instrumento no solo flexible, sino también evolutivo, el cual es capaz de adaptarse rápida y continuamente a la transformación tecnológica, esto ya que, como se ha mencionado a lo largo del presen trabajo, los delitos informáticos no son fenómenos que se mantienen estáticos, sino que por el contrario, recurrentemente surgen recurrentemente manifestando nuevas formas de ataque, técnicas de evasión de antivirus, lenguajes cifrados, plataformas descentralizadas, todo esto sin mencionar las nuevas modalidades que surgen como

delitos emergentes como por ejemplo el reconocido: “deepfake”, es decir, el uso de material audiovisual como una forma avanzada de manipulación mediática, mismo que tendría el potencial de ser utilizado para difundir desinformación, discurso de odio, o inclusive suplantar identidades ajenas; o también el “cryptojacking”, es decir, un tipo de ciberataque mediante el cual los atacantes involucrados secuestran el poder de procesamiento que generan cierto tipo de dispositivos electrónicos como computadoras, teléfonos, etc. Cuyo objetivo es minar criptomonedas sin el consentimiento del propietario de dicho dispositivo. Por lo tanto, el diseño de una adecuada política criminal deberá llegar a contemplar mecanismos de revisión periódica, de evaluación de impacto, de participación de expertos dentro del ámbito de lo informático y también se debe procurar la apertura al diálogo con entidades del sector privado, con la academia y con la sociedad.

Por lo que, concluyendo el análisis dentro del presente capítulo, se puede mencionar que una política criminal diseñada para combatir los delitos informáticos no resulta ser un simple conjunto de normas penales sin más, sino que por el contrario, refleja la creación de una estrategia estatal compleja, debidamente articulada y multidisciplinaria, misma que se encuentra orientada para proteger los bienes jurídicos dentro de un entorno digital, así como también para poder llegar a prevenir la criminalidad tecnológica, para garantizar la seguridad jurídica dentro de lo informático y para poder promover una justicia penal que se separe de lo obsoleto y pase a ser moderna y eficaz para hacerle frente al cibercrimen. En el Ecuador, la debida adopción de una política criminal en el ámbito informático no solo es sugerente, sino que, dada la falta de actualización en Ecuador, su implementación resulta ser sumamente urgente si se desea superar los múltiples vacíos normativos, las falencias operativas y el rezago existente dentro de lo

institucional, situación que actualmente impiden que se pueda llegar a dar una respuesta penal que resulte adecuada frente a los desafíos que surgen diariamente en torno al cibercrimen.

4.2 Principios rectores de una política criminal sobre interferencia en datos

En la actualidad la interferencia de datos resulta ser uno de los núcleos elementales dentro del campo de la criminalidad informática. El presente tipo penal está caracterizado por la alteración indebida, la eliminación, el deterioro y la supresión no consentida de los datos informáticos que circulan a diario, esto representa una grave y compleja amenaza directa contra la seguridad e intimidad que por su naturaleza deberían tener estos datos, eso sin mencionar la clara vulneración al derecho, a la integridad de la información personal y la pérdida de la confianza social hacia las plataformas tecnológicas que acogen y resguardan este tipo de información de sus respectivos usuarios. Por lo tanto, frente a esta nueva realidad en la que estamos viviendo, es fundamental hablar del desarrollo correcto de una política criminal dirigida específicamente para el correcto tratamiento de casos donde tienen lugar los delitos de interferencia de datos, dicha política, por todo lo expuesto con anterioridad se torna imprescindible en cualquier Estado para poder llegar a responder de manera adecuada al fenómeno social antes descrito, por tanto, estas nuevas políticas deben sustentarse en una serie de múltiples principios rectores, los cuales, orienten la actuación de las respectivas instituciones del Estado como por ejemplo la racionalidad, la proporcionalidad y la eficacia.

Para dar inicio con el desarrollo del presente apartado primeramente hay que mencionar que la política criminal sobre la interferencia en datos debe fundarse principalmente en el principio de legalidad que se contempla en la ley, pues el mismo exige la existencia de una normativa clara y precisa que defina las respectivas conductas punibles a aplicarse dentro de un determinado proceso penal. Dado que por su naturaleza los delitos informáticos suelen

involucrar el uso de cierto tipo de tecnologías que se encuentran en constante evolución y actualización, asimismo la legislación deberá reformarse constantemente para poder llegar a evitar formulaciones que resulten ser ambiguas o que resulten ser excesivamente amplias, ya que estas podrían llegar a generar una situación de confusión que conduzca a interpretaciones arbitrarias o insuficientes. Por lo tanto, la existencia de un tipo penal dedicado al ámbito de la interferencia de datos debe ser concebido con rigor técnico y también lingüístico, delimitando claramente tanto sus elementos objetivos como subjetivos, considerando también que este pueda ser fácilmente aplicable y marcando diferencia con otras figuras similares como por ejemplo el acceso no autorizado o el sabotaje de datos informáticos.

Además, para garantizar el derecho de las partes dentro de algún proceso penal deberá de aplicarse el principio consagrado dentro de nuestro marco normativo que refiere a la mínima intervención penal, el presente principio consiste en que el Derecho Penal solo deberá llegar a ser aplicado cuando los otros mecanismos o alternativas normativas que establezca la ley resulten llegar a ser insuficientes para solventar un conflicto. Hablando específicamente de la interferencia de datos, resulta ser de vital importancia que la política criminal distinga de manera efectiva entre aquellas conductas que resulten ser lesivas de derechos, las conductas meramente riesgosas y las conductas insignificantes, evitando de esta forma que se dé la criminalización de actos que por su naturaleza poco lesiva pueden llegar a ser resueltos en otras instancias, como por ejemplo en sede civil. Esto considerando que el uso excesivo del sistema penal no resulta llegar a ser ineficaz, sino que además se pueden llegar a ver vulneradas las garantías individuales que rigen a todo proceso penal.

Hablando en cuanto al principio de proporcionalidad hay que mencionar que este es otro eje rector que resulta llegar a ser indispensable para el debido tratamiento de estos casos de

delitos informáticos. El presente principio impone la clara obligación de que las penas establecidas en contra del procesado dentro de la interferencia de datos guarden coherencia respecto a la gravedad del daño que ha sido provocado, es decir, el menoscabo que ha sido causado al bien jurídico protegido en torno al contexto del hecho. No toda modificación de datos informáticos está revestida de la misma peligrosidad o afectación, por ejemplo eliminar la información que está contenida en un sitio web no es equivalente a aquellos casos donde se llegan a alterar registros médicos o se interceptan datos referentes al ámbito financiero. Por lo mencionado con anterioridad es evidente recalcar que la política criminal deberá prever criterios que sean objetivos para poder llegar a valorar de manera correcta el daño causado, su potencial riesgo y la intencionalidad que tuviese el agente, estableciendo de esta forma sanciones mucho más justa que reflejen dicha diferencia (Martínez, 2021).

De igual forma la política criminal deberá considerar de manera fundamental la especialización institucional, esto implica que la persecución en cuanto a los delitos de interferencia de datos deberá estar a cargo de unidades técnicas que estén especializadas para la atención de tal situación dentro del sistema de justicia penal ecuatoriano. La complejidad tecnológica de la que se ven revestidos este tipo de delitos informáticos, los cuales, por ejemplo pueden involucrar procesos informáticos como la manipulación de bases de datos informáticos, el lenguaje SQL, las redes distribuidas o la tecnología blockchain requiere forzosamente de la intervención de servidores públicos de la justicia como por ejemplo los fiscales, los jueces, los peritos debidamente capacitados dentro del ámbito de informático y policías que cuenten con los conocimientos específicos en informática. Si es que no se cuenta con este tipo de especialización informática por parte de las autoridades antes mencionadas, la aplicación de la ley por parte de una juzgador inexperto en cuanto al ámbito tecnológico puede llegar a resultar ineficaz, con

interpretaciones erráticas o inclusive con decisiones, que, por simple desconocimiento pueden llevar al procesado a ser partícipe de una situación donde se vulneren injustamente sus derechos, lo que inevitablemente desembocan en una clara situación de inconstitucionalidad.

Asimismo es importante la tecnicidad en cuanto a la prueba, esto debido a que la interferencia de datos puede llegar a afectar contenidos intangibles lo cuales pueden llegar a ser manipulados fácilmente, por tanto, la política criminal deberá establecer múltiples protocolos técnicos que sean rigurosos, esto con el fin de que se pueda llegar a dar la recolección, la respectiva preservación, el análisis y finalmente la presentación de la prueba digital ante las autoridades pertinentes, lo que incluye el respeto incondicional y estricto a la cadena de custodia, también el uso de herramientas de auditoría informática que estén debidamente certificadas, la documentación detallada que respalden los procedimientos forenses realizados y la admisibilidad de las pruebas presentadas en formatos electrónicos. Por todo lo expuesto con anterioridad es evidente mencionar que el manejo inapropiado o indebido de la evidencia digital puede llegar a acarrear la nulidad del proceso o la impunidad del hecho imputado, todo a cauda del inadecuado manejo de las pruebas tecnológicas.

De igual forma la cooperación interinstitucional resulta llegar a ser esencial para que se pueda llegar a dar una política criminal eficiente en cuanto a los delitos informáticos. La interferencia de datos puede llegar a tener múltiples impactos en cierto tipo de sectores como por ejemplo en el sector financiero, el sanitario, el educativo e inclusive en el gubernamental, por lo que, para poder hacerle frente a esta desfavorable situación el Estado deberá llegar a garantizar canales adecuados que permitan la colaboración dentro del sistema penal, es decir, entre las instituciones públicas del Estado, los entes reguladores, las empresas privadas que puedan colaborar a la detección de delitos informáticos y la sociedad civil. Dicha cooperación no solo

nos permitirá alcanzar una mejor detección eficaz y prevención del delito informático, sino que además facilita que se pueda llegar a dar asistencia técnica, recuperación de datos informáticos comprometidos y respuesta rápida ante incidentes críticos como por ejemplo el robo masivo de datos de una entidad estatal.

Además resulta sumamente importante que dentro del marco legal ecuatoriano se dé una adecuación tecnológica, misma que se encargue de guiar esta política criminal. Esto implica que las estrategias aplicadas dentro del sistema penal deberán adaptarse a las condiciones tecnológicas actuales dentro del entorno digital. Por tanto, es evidente mencionar que no solo basta con tener normas vigentes, sino que además resulta ser necesario que el Estado considere invertir en cuanto a infraestructura tecnológica, a las plataformas forenses, a la obtención de software especializado y también al uso de sistemas interoperables, de este modo, las instituciones de Estado encargadas de combatir los delitos informáticos pueden aplicar efectivamente los preceptos contenidos en la ley aplicables dentro del presente contexto. La brecha tecnológica existente entre el Estado ecuatoriano y los actores delictivos dentro del presente ámbito no puede seguir ampliándose aún más si lo que se pretende es poder llegar a proteger de manera eficaz el bien jurídico de la integridad de los datos informáticos (Veliz & Lou, 2025, p. 33).

Haciendo referencia al marco constitucional aplicable dentro del Estado ecuatoriano, también se debe considerar lo que establece el principio de la tutela judicial efectiva, ya que dicho principio, aplicable al presente contexto puede llegar a exigir que las víctimas de interferencia de datos puedan llegar a acceder oportunamente a mecanismos ágiles, comprensibles y sobre todo eficientes para que se pueda plantear una denuncia, que se dé la investigación y posteriormente la reparación del daño ocasionado. En varias ocasiones son las

propias víctimas quienes desconocen cómo iniciar una acción dentro de lo penal o que a su vez enfrentan múltiples dificultades para poder llegar a acreditar la manipulación digital de su información personal. Por lo que, una política criminal que resulte ser eficaz debe facilitar que estas víctimas puedan llegar a acceder a canales especializados de atención para dichos problemas, así como contar con fiscalías que posean la debida atención técnica y herramientas de denuncia en línea eficaces y actualizadas, especialmente considerando la naturaleza digital del delito informático.

4.3. Elementos clave de una política integral

Los delitos informáticos en la actualidad pueden llegar a representar una de las expresiones más desafiantes, complejas y extenuantes a enfrentar dentro del ámbito de la criminalidad contemporánea, esto tanto por su carácter transnacional y también por su alta sofisticación empleada dentro del ámbito técnico, además de su capacidad de afectar en gran medida de manera directa los derechos fundamentales de las personas, o de los sistemas públicos y privados, así como también los delitos informáticos pueden llegar a comprometer en casos extremos la seguridad nacional existente dentro de instituciones estatales en el Ecuador. Considerando lo mencionado, y tal como se ha analizado a lo largo del presente trabajo, en el Ecuador, a día de hoy, lamentablemente aún carecemos de una política criminal que resulte ser integral, coherente y sobre todo especializada, misma que como sociedad nos permita llegar a enfrentar de forma eficaz y eficiente este nuevo y creciente fenómeno delictivo moderno. Por lo que, es importante mencionar que ante los nuevos delitos informáticos que surgen en la actualidad, para poder enfrentarlos no solamente basta con que existan ciertas normas penales

aisladas o que se den esfuerzos puntuales dentro de ciertas instituciones estatales, sino que resulta ser indispensable diseñar y también aplicar una política criminal que esté mucho más estructurada en cuanto a lo informático, dicha política deberá contemplar primordialmente bases estratégicas, el uso de tecnológicas jurídicas, y la misma debe estar orientada no solo a combatir delitos informáticos, sino también deberá estar enfocada en la prevención, la persecución y finalmente tras la realización de un juicio penal justo, la sanción efectiva de dichas conductas.

En este contexto, la necesidad de que surja una política integral principalmente radica en que los delitos dentro del ámbito de lo informático no pueden ser abordados solamente desde un punto de vista punitivo o reactivo, sino que por el contrario, para poder abordarlos de manera correcta se requiere de un enfoque multidisciplinario que articule acciones coordinadas entre la materia legislativa, institucional, el ámbito educativo, la tecnológica, presupuestaria y también la cooperación internacional para una respuesta mucho más ágil al momento de darle prosecución a cualquier proceso penal que involucre delitos informáticos internacionales. Si una política criminal no llega a contemplar estos componentes, resultará ser poco eficiente, lo que a su vez puede llevar a que la misma sea fragmentaria, limitada en cuanto a sus resultados y además vulnerable frente a la rápida, constante y sofisticada evolución de las amenazas digitales, mismas que se renuevan diariamente.

Considerando lo mencionado en líneas anteriores, el presente capítulo tiene por finalidad el poder identificar y también llegar a desarrollar los elementos clave y principales, que deben formar parte de cualquier política criminal integral en cuanto a la materia de delitos informáticos, examinando diversos aspectos como la prevención y educación digital , el fortalecimiento institucional y capacitación técnica, la cooperación nacional e internacional, la protección de datos personales y la legislación clara y efectiva.

El hecho de comprender y también de poder aplicar estos elementos no solo nos permitirá poder llegar a superar las deficiencias normativas y operativas que han sido mencionadas dentro de capítulos anteriores, sino que además contribuirá a que se pueda consolidar un renovado modelo de justicia penal, que sea mucho más eficiente, más proactivo, más garantista y que esté acorde con los estándares internacionales de ciberseguridad y también que respete de mejor forma lo establecido dentro de los derechos humanos. De ahí que surja la gran importancia de definir con suma precisión cuáles son los pilares primordiales sobre los que se debe cimentar una política criminal que sea verdaderamente integral y pueda enfrentar efectivamente los desafíos que plantea el ámbito delictivo informático en el Ecuador actual.

4.3.1. Prevención y educación digital

Para dar inicio con el presente apartado cabe destacar que la prevención como tal constituye uno de más grandes y fundamentales pilares dentro de toda política criminal integral sobre todo si se habla de un medio tan comúnmente utilizado como el informático, esto pues, a diferencia de lo que sucedía dentro del ámbito del delito tradicional, en el cibercrimen los actos ilícitos llevados a cabo se caracterizan por su capacidad rápida de expansión, la fuerte presencia de la figura del anonimato y la rápida evolución técnica de ciertos programas informáticos, todos estos aspectos hacen que las estrategias planteadas dentro del ámbito de la justicia resulten llegar a ser meramente represivas, o en su defecto lleguen a ser insuficientes o tardías. Por lo que en el presente contexto, la educación en cuanto a lo digital y sobre todo la concienciación hacia los ciudadanos se convierten en herramientas fundamentales para poder llegar a mitigar riesgos, para reducir la vulnerabilidad a la que están expuestos múltiples usuarios todos los días e inclusive para poder llegar a fortalecer la cultura general en cuanto a la ciberseguridad.

Una política criminal que quiera dar resultados efectivos deberá ir incluso más allá de la existencia de un castigo posterior al delito, puesto que se debería invertir mucho más en mecanismos estructurales destinados a promover la prevención, mismos que involucren tanto al Estado ecuatoriano como a la sociedad misma, al ser actores diarios dentro del ámbito informático. En este sentido, el Estado debería prestar mayor atención en cuanto a la incorporación de contenidos sobre seguridad digital, la privacidad del usuario en cuanto a su información personal que a diario circula por redes, enseñar y fomentar entre la sociedad el uso responsable de internet e informarles sobre los respectivos riesgos a los que se ven expuestos de manera cotidiana dentro de entornos virtuales, y dado el masivo fenómeno que resulto ser el internet en la vida de las personas en todas sus edades, dicha formación deberá ser promovida en general a toda la población, teniendo así que concientizar desde los centros educativos en todos los niveles, pasando por la educación básica hasta llegar a la formación universitaria e inclusive continuar capacitando a las personas dentro de lo profesional en medida de lo posible. La alfabetización digital no deberá únicamente limitarse al uso técnico de dispositivos electrónicos, sino que para tener una perspectiva mucho más amplia debe abarcar también la comprensión crítica de los riesgos y amenazas informáticas que pueden llegar a surgir y también se debería poner en conocimiento las formas legales de protección que existan ante ellas.

Asimismo, todas y cada una de las instituciones públicas e incluso también algunas de las instituciones privadas dentro del Estado deberían implementar e incentivar a la formación y educación en cuanto al ámbito de la tecnología, esto por ejemplo mediante el uso de campañas masivas de sensibilización, mismas que, como se ha mencionado en líneas anteriores deberán ir destinadas a varios grupos sociales dentro de la sociedad, incluyendo a los niños, a los adolescentes, los adultos mayores, los comerciantes que ejerzan su labor haciendo uso de

plataformas informáticas, a los funcionarios públicos y empresarios que operen haciendo uso de medios informáticos. Dichas campañas de educación pueden abordar cierto tipo de temas como por ejemplo la protección de datos personales, el reconocimiento de fraudes, estafas o mensajes engañosos usados en línea, el uso de contraseñas seguras para resguardar el acceso personal a información personal, el manejo adecuado de redes sociales y la denuncia a la que pueden acceder en caso de que surjan incidentes digitales, tras todo lo mencionado es evidente mencionar que estas medidas no solo ayudan para reducir el número de víctimas en cuanto a los delitos informáticos, sino que además puede ayudar a que las personas conozcan de los riesgos a los que están sujetos en el ámbito digital, pues una ciudadanía que esté bien informada y que sea consciente de dichos aspectos representa la primera línea de defensa de la sociedad frente a los delitos informáticos.

Igualmente, la prevención de los delitos informáticos requiere de la participación activa de otras entidades dentro del Estado que ayuden a difundir información a la ciudadanía en general, como por ejemplo los medios de comunicación, las universidades cuya malla curricular esté dirigida al ámbito informático, y todos los funcionarios quienes operen a diario dentro del sector tecnológico en general. El Estado, por su parte, al tener a su cargo la seguridad informática de las distintas personas dentro de la sociedad debe liderar en todo momento estrategias de prevención y delitos informáticos, esto mediante una política pública que fomente y respalde la educación digital, ayudando financiándola adecuadamente y monitoreando constantemente sus resultados en cuanto a la educación general de la población ecuatoriana.

Tras todo lo mencionado queda únicamente mencionar que los temas como la prevención y la educación respecto al ámbito de lo digital no resultan ser un complemento opcional, sino que por el contrario, es un fuerte componente central dentro de cualquier política criminal que aspire

a poder combatir de manera eficaz los delitos informáticos que puedan acontecer en toda sociedad moderna y conectada como resultar ser la sociedad ecuatoriana contemporánea.

4.3.2. Fortalecimiento institucional y capacitación técnica

Tal como se ha podido llegar a observar durante el desarrollo del presente trabajo, es claro que uno de los más grandes desafíos que llega a enfrentar el Ecuador frente a la aparición de los delitos informáticos recae en la notoria debilidad estructural que existe dentro de sus instituciones, mismas que se supone que son las encargadas de poder prevenir, investigar y sancionar a quienes cometan delitos informáticos. Aspectos negativos como las limitaciones en cuanto a recursos humanos, la falta de infraestructura tecnológica y la escasa preparación técnica en cuanto a este tipo de delitos han sido señaladas como factores críticos, los cuales, afectan gravemente y de manera negativa la eficacia existente dentro del sistema penal ecuatoriano en este ámbito. Por tal motivo, el fortalecimiento dentro de lo institucional y la continua, constante y permanente capacitación técnica especializada resulta ser uno de los elementos esenciales necesarios dentro de una política criminal integral destinada a enfrentar a los delitos informáticos.

Hablando respecto al fortalecimiento institucional, cabe mencionar que aquello implica dotar a instituciones del Estado como por ejemplo la Fiscalía General del Estado, la Policía Nacional, el Consejo de la Judicatura, de unidades especializadas en cuanto al ámbito de lo informático, de personal capacitado para ejercer labores que conlleven el uso de la tecnología, de laboratorios forenses que cuente con suficientes equipos para ejercer labores digitales y también de protocolos de actuación homogéneos que colaboren para que se dé una actuación eficaz para combatir los delitos informáticos. Actualmente, muchas de las instituciones antes mencionadas, si bien cuentan con ciertos equipos y algunos profesionales, también es importante mencionar

que carecen de múltiples áreas técnicas o que en su mayoría dependen de pocos funcionarios, mismos que poseen conocimientos limitados; dicha situación impide que se pueda llegar a dar una respuesta oportuna frente a los ataques informáticos o que se dé una inadecuada preservación de evidencia digital que pueda llegar a utilizarse en un caso penal.

Por todo lo mencionado se vuelve imprescindible que se dé la creación y posterior consolidación de Fiscalías y también de juzgados que estén especializados en cuanto al ámbito de la ciberdelincuencia, que estén equipados con tecnología forense, conectividad segura, sistemas interoperables y sobre todo personal técnico-jurídico que posea conocimientos en cuanto al ámbito del derecho penal informático, el análisis de metadatos, el correcto manejo de la cadena de custodia digital y criptografía. Dicha institucionalidad especializada no solo nos ayudaría enormemente para poder llegar a mejorar la calidad de las investigaciones llevada a cabo por las autoridades pertinentes, sino que además nos garantizaría que exista mayor seguridad jurídica y coherencia en cuanto a la aplicación de la ley en el Ecuador.

La capacitación y formación técnica constante y continua constituye otro de los ejes indispensables dentro de la constitución de toda política criminal informática. Así, los jueces, los fiscales, los defensores públicos, policías, peritos y demás auxiliares dentro del sistema judicial ecuatoriano deben encarecidamente recibir capacitación regular en múltiples áreas como los delitos informáticos, el manejo de la evidencia electrónica, la trazabilidad digital, el blockchain, estar al tanto de tecnologías emergentes y estándares internacionales respecto a la ciberseguridad en general. Dicha formación en cuanto al ámbito de lo informático no puede únicamente limitarse a que se den pocos cursos ocasionales o que sean voluntarios, sino que por el contrario deberá de incorporarse como una parte obligatoria dentro de los programas de formación y

capacitación, esto con el objetivo de mejorar la calidad de los servidores que laboran a diario en el sistema de justicia ecuatoriana.

De igual forma, el Estado ecuatoriano debe fomentar alianzas con otras universidades, centros de investigación, organismos internacionales y demás empresas que laboren dentro del sector tecnológico, esto con el objetivo de que se puedan llegar a impulsar procesos de actualización y también de certificación técnica en función de los cambios constantes y permanentes que caracterizan al entorno digital.

Por lo que, sin instituciones sólidas que colaboren entre sí, ni operadores que estén debidamente formados en cuanto al ámbito tecnológico, toda política criminal destinada a combatir los delitos informáticos terminará por ser insuficiente. Finalmente un sistema técnico, especializado y eficaz podrá responder adecuadamente a las nuevas formas de criminalidad digital que surgen a diario dentro de la sociedad.

4.3.3. Cooperación nacional e internacional

Por la naturaleza transnacional, descentralizada y sobre todo altamente técnica que caracterizan a los delitos informáticos, se exige fuertemente que cualquier política criminal eficaz incorpore principalmente y como eje estratégico la colaboración nacional e internacional para así poder hacerle frente a los delitos informáticos. Contrario a como se solía manifestar el delito tradicional, en su gran mayoría dichos actos ilícitos ocurren dentro de los límites territoriales definidos dentro de cualquier Estado, no obstante, el cibercrimen como tal puede llegar a originarse dentro de un país, y a su vez ejecutarse desde otro país totalmente distinto y así afectar gravemente a las víctimas de dichos actos dentro de múltiples jurisdicciones, lo cual, no solo plantea dificultades dentro del ámbito de la jurisdicción y competencia propias de cada país involucrado, sino que además, esta situación plantea enormes desafíos para que se pueda

llegar a dar una correcta investigación, persecución penal y afectando inclusive a la obtención de pruebas digitales. Por lo que, ante dicha complejidad que se presenta, es necesario actuar de forma conjunta y no aislada, ya que dicho actuar en solitario no solo resultaría llegar a ser ineficiente, sino que también puede llegar a ser inoperante.

Dentro del ámbito nacional, la cooperación interinstitucional debe estar orientada a la articulación efectiva entre las entidades estatales que conforman el sector público encargadas de la prevención, la detección, la investigación y por último la sanción de los delitos informáticos. Esto evidentemente incluye a entidades como por ejemplo la Fiscalía General del Estado, la Policía Nacional, el Consejo de la Judicatura y también a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), la Dirección Nacional de Registro de Datos Públicos (DINARDAP). Para lo cual, resulta ser indispensable que se establezcan protocolos comunes de actuación para dichas entidades, como también se deben tener canales seguros para que se dé el correcto intercambio de información, sistemas interoperables, mismos que eviten que se pueda llegar a dar la duplicación de funciones y pérdida de evidencia clave dentro de cualquier delito informático.

Es importante establecer que la cooperación internacional resulta llegar a ser un componente esencial en el presente ámbito, esto dado que múltiples ciberataques provienen en su gran mayoría de actores que están ubicados fuera del territorio nacional. En este sentido, la ratificación del Ecuador al mencionado Convenio Budapest sobre la ciberdelincuencia, la cual, ha sido declarada recientemente constitucional por la Corte Constitucional (Dictamen 1-24-TI/24, 2024), representa de cierta forma un gran y significativo avance. Al considerar lo establecido dentro de dicho tratado se nos proporciona un marco legal uniforme y actualizado en cuanto a la tipificación penal, a la asistencia mutua y también a la conservación transfronteriza

de datos informáticos, así como también se cuentan con mecanismos de cooperación urgente entre las respectivas autoridades competentes de cada país.

También el Ecuador debe fortalecer su participación activa dentro de cierto tipo de redes como por ejemplo la INTERPOL, el Grupo de Trabajo de Ciberdelincuencia de la OEA y también el Estado ecuatoriano debería considerar tener una presencia un poco más activa dentro de otros foros regionales, los cuales puedan ayudar a solventar las problemáticas que puedan llegar a surgir dentro del ámbito de la seguridad digital. Además es importante establecer acuerdos bilaterales en cuanto a la asistencia técnica y también en cuanto a la asistencia dentro del ámbito de lo judicial, las cuales permitan compartir buenas prácticas, fomentar la debida capacitación a los operadores de justicia, y acceder a diversas tecnologías modernas y metodologías propias de la investigación forense digital en la actualidad.

Por lo tanto, una política criminal que refiera sobre los delitos informáticos no puede llegar a ser concebida únicamente desde una lógica interna, pues como ha sido expuesto en líneas anteriores, solo mediante el uso de una adecuada cooperación fluida, estratégica y sostenida entre todas y cada una de las instituciones nacionales y también las instituciones internacionales dedicadas al tema del tratamiento de los delitos informáticos, será posible poder llegar a enfrentar con eficacia las amenazas que genera el cibercrimen dentro de un entorno globalizado e interconectado como en el que vivimos actualmente.

4.3.4 Protección de Datos Personales

Con el avance tecnológico de la sociedad actual, los datos personales se han convertido en un activo valioso, pero a su vez vulnerable. La transición digital, propulsada por el uso inmensurable del internet, redes sociales, plataformas dónde reposa información de comercio electrónico y dispositivos inteligentes, han creado novedosas formas en las cuales se puede

recopilar información, con el fin de tratar y explotar todo tipo de información personal. Bajo esta premisa, la seguridad que se brinda a los datos personales no está relacionada individualmente con la privacidad, más bien, consiste en una facultad de esencial garantía para la dignidad humana, en conjunto con la autonomía individual y por supuesto la seguridad en la que se basa el entorno digital

Actualmente los datos personales deben ser considerados como un bien jurídico protegido, teniendo en cuenta que, se comprenden como una de las bases claves para fomentar la defensa de la dignidad y autodeterminación afirmativa dentro de un entorno completamente digital. Para Ecuador, este principio se encuentra expresamente garantizado por el artículo 66 inciso 19 de la Constitución de la República del Ecuador, mismo en el que se da reconocimiento al derecho del ciudadano para el cuidado de sus datos personales; remarca el hecho de que todas las personas tienen la facultad de poder acceder, actualizar, rectificar y eliminar la información que se encuentre recolectada en bases de datos, y englobar dentro del mismo un tratamiento bajo el principio de confidencialidad (Labrin,2023)

Si bien el sistema jurídico ecuatoriano ha reconocido este derecho tanto en la Constitución como en la Ley Orgánica de Protección de Datos Personales, en la vía práctica del derecho las débiles maneras de implementar, fiscalizar y articular la protección de datos personales con la política criminal han persistido, de hecho, el uso de los cuerpos legales se ha utilizado de manera cerrada y con poca eficacia material, más aún cuando se trata de delitos informáticos relacionados con el acceso y manipulación abusiva de datos carentes de autorización. Dentro de la Ley Orgánica de Protección de Datos Personales se despliegan principios que fortalecen un marco jurídico dirigido específicamente a brindar la garantía

suficiente para un trato legal y confiable de datos, este ordenamiento legal dispone de principio bases como:

- Principio de legalidad
- Principio de seguridad jurídica
- Principio de contradicción
- Principio de tutela judicial efectiva

En caso de que estos análisis funcionen se podrá identificar con mayor precisión los problemas y proponer diversas soluciones con cuerpos legales ejemplares que sirvan para mejor protección de datos, los cuales sean fuertes y funcionales, este derecho reposa sobre las bases garantistas que se adaptan al modelo del estado ecuatoriano, en dónde se da amplio reconocimiento a derechos nuevos para la moderna generación tecnológica. Tanto el acceso a datos informáticos, como su robo, filtración, comercialización ilegal y otros delitos informáticos exponen la inexistente cultura digital sobre protección de datos, es más, la creación de la Superintendencia de Protección de Datos no ha hecho mayor cosa que exhibir la incapacidad de mantener el control, la fiscalización y sancionar la conducta delictiva.

La Corte Constitucional examinó mediante la sentencia No. 2064-14-EP/21 la alta vulneración que existe frente a la protección de datos personales, y pide al estado mayor control en el tratamiento de datos, al igual que mayor compromiso por parte de instituciones públicas y sus servidores. En esta sentencia se alcanzó un hito para el derecho informático, pues, se da el reconocimiento a la violación de la garantía de protección de datos personales, a su vez reconoce la vulneración de los mismos por medio de la afectación a la honra, buena imagen y el uso incorrecto de fotografías con órganos de identificación biométrica, más cuando se trate de plataformas digitales y base de datos.

Sin embargo, en la actualidad el acceso abusivo a la información privada continua, y hasta se podría decir que, con mayor frecuencia, como ejemplo de eso se ve el caso de "Novaestrat" en el año 2019, en el mismo se expuso millones de datos personales de ciudadanos ecuatorianos con una completa ausencia de sanciones proporcionales al delito. En este caso las sanciones presentadas fueron mínimas, por no llamarlas nulas, incluso cuando la magnitud del caso fue de suma importancia, dejando así en evidencia la urgencia que tiene el derecho penal

por enfocarse en implementar en su tipificación conductas detalladas, como lo es la reventa de datos y la manipulación de información con fines políticos o comerciales (Huaman,2024).Por esta razón, el desafío no radica sobre la existencia o no de normas, sino en su ejecución, por ende la necesidad de fortalecer y mejorar a la Superintendencia es urgente, al igual que la articulación de sus oficios en la fiscalía general del Estado, de hecho, se debería tomar a consideración a unidades especializadas en ciberdelincuencia que sirva para conseguir mayor vinculación entre el conocimiento técnico especializado y el conocimiento legal que amerita el país, sin dejar de lado el hecho de que se debería ratificar convenios internacionales para que se pueda dar mayor armonía a la ley ecuatoriana con la existente a nivel internacional.

Entre las principales situaciones en las cuales se da vulneración de datos personales se encuentra la rama de delitos informáticos, pues, sus conductas caen en circunstancias ilícitas bastante comunes actualmente, como lo es el acceso ilegal a bases informáticas o la interceptación de comunicaciones y datos, no obstante en el presente derecho penal la protección es obsoleta e inadecuada, ya que, únicamente se concentra en el enuncia miento de conductas penales bastante genéricas, esto teniendo como consecuencia la incapacidad de adaptarse a una nueva y sofisticada sociedad tecnológica.

4.3.5 Legislación clara y efectiva

Para lograr alcanzar un estado en dónde el derecho penal pueda estar enfocado en delitos informáticos se necesita de una legislación clara y efectiva para hacer cara a los problemas actuales en donde la tecnología ya es parte de la cotidianidad. No obstante, el ordenamiento legal dentro del país expone errores en su tipificación en relación a delitos informáticos. Dentro del Código Orgánico integral Penal en el título IV en dónde se encuentran los delitos relacionados a los derechos de libertad y contra los derechos de las personas, en este se trata figuras como el

acceso sin autorización a sistemas informáticos, aunque se puede decir que su tipificación es bastante cerrada y ambigua. El autor Aguilar Cavero se había dado la tarea de estudiar la manera correcta en la cual los delitos informáticos deben ser tipificados, y destaca lo esencial de una legislación más ágil y que posea un lenguaje preciso que pueda someterse a una revisión recurrente. En el COIP no se observa una respuesta correcta para lo que exigen los actuales ciberdelitos. Tanto el ransomware, como la ingeniería social o la sextorsión son conductas delictivas que claman atención urgente por los cuerpos legales, pero, la dispersión normativa dentro del COIP en base a la ciberseguridad repercute en conductas con carácter lesivo que vulneran principios del derecho penal como la legalidad y la mínima intervención.

La reforma integral del COIP y la capacitación a jueces y fiscales ecuatorianos forman parte de brindar una solución válida al problema actual, esto podría basarse en el convenio internacional Budapest con la finalidad de crear nuevos reglamentos técnicos con criterios uniformes en base a evidencias y cadena de custodia a nivel digital.

4.4 Propuesta de modelo de política criminal para Ecuador

Si bien el Código orgánico integral Penal en el título IV de su libro segundo específica y redacta ciertos tipos de delitos informáticos, como es el acceso no consentido de sistemas informáticos estipulado en su artículo 232, la interceptación ilícita de datos en su artículo 233 y

también el sabotaje informático en su artículo 234, estos no llegan a ser suficientes para enfrentar todos los problemas actuales que está sufriendo la sociedad, ya que, tal y como señala el estudioso y jurista ecuatoriano, José Luis Pérez Tapia (2020). La legislación del Derecho penal en una sociedad ecuatoriana no sirve como un reflejo que sea lo suficientemente transparente u hondo para hacer frente al tipo de fenómeno en el que consiste la ciberdelincuencia por el cual

está atravesando el país, y mucho menos establece estos criterios de imputación penal que estén adecuados a la complejidad del asunto. Incluso se sabe que la respuesta que se recibe por parte de las instituciones públicas es fragmentada, reactiva y bastante débil en términos de investigación para estos delitos. Según el Ministerio del Interior y del Centro de. Respuestas a incidentes informáticos, los ciberdelitos. Han aumentado alarmantemente, especialmente delitos como el phishing, el ransomware y el sabotaje a diferentes sistemas Informáticos de instituciones públicas. Todo esto sin que exista siquiera una estrategia mínima y coherente de política criminal (Arroyo,2020).

Haciendo uso de lo estipulado por Günther Jakobs (1996) Se llega a la conclusión de que la política criminal es este mecanismo de respuestas que debe proporcionar y adoptar el Estado para así conseguir una definición marcada de los diferentes tipos de conductas para que estos lleguen a ser penalmente relevantes como es en el caso del Derecho penal, estas tendrían que ser aplicadas y tener medidas con conceptos útiles para evitar la criminalidad. Con este punto de vista tendríamos que articular bajo el concepto del Derecho penal del enemigo, que también estás desarrollado por el doctrinario Jacobs, al menos cuando se trata de responder a las amenazas organizadas y sistemáticas, como es en el caso de los delitos informáticos.

El profesor argentino Eugenio Raúl Zaffaroni advierte también sobre los riesgos que se tienen al momento de utilizar plataformas digitales con el uso expansivo del Derecho penal. Nos

dice que el mismo no tendría que ser la primera ni la única herramienta para poder enfrentar una conducta delictiva, o mucho menos aun cuando debería ser este el único que conste como un sistema garantista para respetar los derechos Fundamentales, por esta razón se puede decir que cualquier política criminal que haga frente a diferentes conductas delictivas de rama informática tiene la obligación de moverse bajo un equilibrio entre eficacia, moralidad y eficiencia (Zaffaroni,1982).

En base a esto, nos gustaría proponer la prevención estructural y la cultura digital y su fomentación como una de las estrategias claves para mejorar la administración del Derecho penal frente a la investigación de ciberdelitos y a su funcionamiento, la educación digital ciudadana y la capacitación institucional obtendrá como consecuencia la inclusión en el currículo escolar y universitario para la formación ética y digital y continua la formación de ciberseguridad en funcionarios estatales. El fortalecimiento del ecuCERT Basándose en el personal técnico y también en el marco legal del mismo, actualizando así el catálogo del Código penal para que este incluya delitos como el ransomware o el phishing, evitando así la impunidad en casos en donde los datos personales de los ciudadanos se vean afectados y estén susceptibles a diferentes vulneraciones de derechos. La política criminal en Ecuador en cuanto a la rama de delitos informáticos debería tenerla obligación de atender a las características particulares que presenta la criminalidad transnacional de crímenes digitales las cuales consisten en el anonimato, las consecuencias generales y los obstáculos técnicos, no obstante, ante la carencia de políticas criminales en el país que traten ciberdelitos solo aumenta la impunidad. Este problema se podría prevenir por medio de la extensión de campañas de concientización sobre la seguridad informática a partir del sistema educativo, las cuales deberían ser impartidas a los estudiosos del derecho en todas las universidades (Sanchez,2019).

Cómo método secundario se habla de la programación a nivel nacional de ciberdelitos y crímenes informáticos, siempre que se mantenga debidamente activa la observación de delitos informáticos a nivel del territorio nacional conforme al control del Consejo de la Judicatura. De hecho, en la sentencia No. 11-18-CN/21 emitida por la Corte constitucional en donde se pronuncia sobre la observación y el análisis de la política criminal por medio del uso de principios constitucionales como la proporcionalidad y a su vez, esta va a poder instrumentalizarse para que con el fin de controlar el exceso de ciberdelitos el Estado pueda también advertir y prevenir el cometimiento de actos delictivos futuros La investigación dentro del Derecho penal con entornos digitales no va a poder implicar o vincular la forma en la que se da la lesividad arbitraria de los derechos humanos fundamentales, esencialmente cuando se trata de garantías al debido proceso.

Es por esta razón que el uso de diferentes mecanismos forenses e interpretaciones tanto electrónica como de geolocalización tendrían que realizarse por medio de compra estándares constitucionales de carácter rígido; De hecho, En la vida práctica del Derecho penal Constantemente. Se vulneran derechos constitucionales como el derecho a la defensa, a la intimidad o a la inocencia, más aún cuando se tratan de ciber delitos o crímenes informáticos (Sánchez, 2021).

Por lo tanto, tenemos que recalcar que uno de los problemas más comunes actualmente es que los elementos probatorios que reposan en bases digitales son adquiridos de manera arbitraria, pues carecen de una cadena de custodia válida o incluso la participación de servidores públicos de la fiscalía o los peritos. Se realiza. De manera. Ilegítima, pues se carece de certificación y de permisos. Por ende, se dice que, el factor que lleva a estos procesos al fracaso viene desde la raíz del asunto, pues Las nulidades ya están presentes desde el momento de la investigación. La Corte

Constitucional con sentencia No. 1149/18-EP/21 describe que todas las pruebas digitales que se obtengan de plataformas o bases de datos poseen la obligación de realizar el proceso de investigación con el mismo carácter de investigación que cualquier otro

medio probatorio, es decir, debe tener aspectos legales, pertinentes, conducentes y que sean sujetos al derecho de contradicción.

Conclusiones

En cuanto primer capítulo uno se ha podido determinar que el desarrollo normativo en cuanto a los ciberdelitos en el Ecuador evidencia avances relevantes, pero a su vez también nos permite ver la existencia de limitaciones sumamente profundas. El Código Orgánico Integral Penal (COIP) significó un gran paso al tipificar conductas delictivas informáticas como el acceso no autorizado, la interceptación de datos y la manipulación de sistemas informáticos, reconociendo de esta forma la necesidad de adaptar el derecho penal a las nuevas realidades tecnológicas que surjan. Dicho hito jurídico ayudó a marcar un inicio en la construcción de un marco legal para poder llegar a enfrentar la delincuencia en el ámbito informático.

Sin embargo, dichos avances resultan en gran medida insuficientes frente a la magnitud y a la complejidad del fenómeno delictivo cometido. El COIP, pese a que incorpora figuras básicas, mantiene un diseño general e inclusive ambiguo que no alcanza para cubrir modalidades contemporáneas de cibercriminalidad modernas, especialmente aquellas de carácter internacional como por ejemplo el ransomware, los fraudes con criptomonedas o los ataques distribuidos

contra infraestructuras críticas dentro del Estado ecuatoriano. Dicha laguna normativa genera un claro riesgo de inseguridad jurídica y a su vez dificulta la adecuada persecución penal en este campo.

Pese a ello, persiste el gran desafío de adecuar nuestra legislación nacional con lo establecido dentro de los estándares internacionales respecto a los temas informáticos. La falta de ratificación al Convenio de Budapest sobre la Ciberdelincuencia refleja la existencia de cierta distancia del Ecuador respecto con los compromisos globales en la materia. Dicho rezago limita la cooperación a nivel internacional lo cual es indispensable dentro de la investigación y sanción de delitos que, por su naturaleza, trascienden las fronteras.

Por su parte, del análisis que se ha desarrollado a lo largo de segundo capítulo se nos permite evidenciar que el sistema judicial ecuatoriano actual enfrenta una serie de debilidades significativas frente a la lucha contra el cibercrimen, los cuales se pueden sintetizar en tres ejes fundamentales para analizar: normativos, operativos y políticos. Dichos aspectos no solo limitan la eficacia dentro de la investigación y sanción de los delitos en el ámbito informático, sino que además afectan en gran medida la confianza ciudadana en la justicia y la capacidad que tiene el Estado para poder proteger los derechos fundamentales dentro de entornos digitales. Por tanto analizando los ejes antes mencionados tenemos:

1. Eje normativo

Dentro de la materia legal, el avance que se ha logrado con la inclusión de ciertos tipos penales informáticos dentro del Código Orgánico Integral Penal (COIP) en el año 2014 se dio un primer paso, no obstante, dicho avance hoy resulta ser insuficiente y desactualizado. Las figuras emergentes como por ejemplo el ransomware, el phishing avanzado o la suplantación de identidad mediante el uso de programas y herramientas que involucren inteligencia artificial no

están actualmente reguladas con clara precisión, lo cual, genera inseguridad jurídica y aumenta las dificultades probatorias. De igual forma, persisten ciertas ambigüedades en conceptos fundamentales como “acceso no autorizado” o “sistema informático”, lo que inevitablemente hace que se den interpretaciones dispares y debilitan en gran medida el principio de taxatividad penal. Asimismo, se suma la escasa armonización del COIP con los estándares internacionales, como por ejemplo los previstos dentro del Convenio de Budapest sobre Ciberdelincuencia, cuya adhesión recientemente se declaró constitucional en el año 2024, lo cual evidencia un grave retraso de aproximadamente dos décadas frente a otros países de la región que desde hace varios años ya han adaptado sus normativas a dicho instrumento internacional.

2. Eje operativo

Dentro del plano institucional y técnico, las limitaciones que podemos observar son igualmente graves. La Fiscalía General del Estado y la Policía Nacional carecen de la existencia de laboratorios forenses digitales dentro de la mayoría de provincias, lo cual obliga a centralizar investigaciones, lo que a su vez provoca retrasos, pérdida de evidencia relevante o el latente riesgo de que se produzcan nulidades procesales. La escasez que se puede observar en cuanto a peritos informáticos calificados y también la falta de formación especializada en otros operadores de justicia como jueces y fiscales comprometen gravemente la correcta valoración de los medios de prueba expuestos de manera digital. La coordinación interinstitucional actualmente continúa siendo fragmentada puesto que no existen protocolos concretos para la cadena de custodia en cuanto a la preservación de prueba digital ni tampoco hay plataformas de interoperabilidad que permitan compartir la información en tiempo real entre instituciones estatales como Fiscalía, Policía, Judicatura u otros entes de telecomunicaciones en el Ecuador. Dichos déficits operativos, unidos a la carencia de infraestructura tecnológica moderna dentro de

nuestro sistema judicial, hacen que se torne compleja cualquier persecución penal y a su vez refuerzan la impunidad de los involucrados en el cometimiento de algún delito informático.

3. Eje político

Por su parte, a nivel político, el principal problema existente dentro del presente eje radica principalmente en cuanto a la ausencia de prioridad estatal para invertir en materia de ciberseguridad y persecución penal dentro de lo digital. Los presupuestos que son asignados a unidades especializadas son mínimos y estos no responden a una estrategia sostenida para combatir estas nuevas modalidades de delitos. No existe una política pública integral que fomente conductas como la prevención, educación digital, fortalecimiento institucional y cooperación internacional con otras entidades dentro de la región. Mientras que otros países como Colombia, Chile o México han destinado recursos permanentes, han creado fiscalías especializadas y han adoptado protocolos avanzados para la cadena de custodia, en el Ecuador las iniciativas son actualmente fragmentarias. Dicha falta de visión estratégica genera rezago frente al creciente y constante avance tecnológico y debilita la capacidad del Ecuador para poder responder a amenazas transnacionales recurrentes.

Por otra parte, de la información derivada del tercer capítulo podemos concluir que, el ataque a la Contraloría General del Estado sirvió como un acontecimiento clave para destacar lo vulnerable que es el sistema legal en cuanto a sus normas y protocolos, sin dejar de lado el hecho de que consiguió revelar la insuficiencia por parte del Código Orgánico Integral Penal frente a acontecimientos relacionados con ciberdelitos. A su vez se consiguió demostrar la completa ausencia de ciertos protocolos necesarios para que se obtenga una correcta reacción estatal, generando así preocupación en la poca importancia por parte del sistema judicial del país en cuanto a la delincuencia cibernética; la vulnerabilidad a nivel institucional es un conflicto que

también se vinculan con los servidores públicos y por ende con el mal desarrollo de sus funciones y por supuesto la incrementación en la falta de confianza por parte de la ciudadanía.

El ataque suscitado fue la alerta que el sistema necesitaba para brindar más atención a las debilidades que tambalean al cuerpo normativo y el tecnicismo del Estado ecuatoriano. En cuanto a las ramas del derecho penal, constitucional y administrativo, la necesidad de una actualización de la normativa legal en el país se ve cada vez más presente, pues se requiere con urgencia formas en las cuales se logre garantizar una administración pública confiable, segura, verídica y fuerte, que no corra el riesgo de ser ineficaz, pues la información pública que reposa en base de datos y su protección no es un simple deber a cumplir por parte de los servidores públicos, todo lo contrario, se tendría que considerar como requisito fundamental para alcanzar la plena protección de los derechos humanos

El estudio y evaluación de las consecuencias tras estos delitos tendría que ser más más crítico a nivel técnico y teórico para alcanzar la comprensión del desempeño de implicaciones estructural dentro del Estado. El acceso limitado a la justicia en nuestro país y la memoria judicial del pueblo se ve rodeado de la urgencia por conseguir cuerpos normativos que obtengan reformas, actualizaciones y adaptaciones que consigan protocolos seguros para conseguir pruebas y protección a instituciones públicas.

Lograr una mejor capacitaciones que consiga generar interés en los servidores publicaciones y que de manera oportuna se consiga avances permanentes en todo lo relacionado con seguridad informática, ya sea por medio de campañas que generen conciencia sobre todas las maneras posibles para aprovechar todos los recursos que generen condiciones más óptimas para la base de datos y que con estos cursos se relacionen con la ética institucional y que se puedan exigir por medio de estándares con un nivel alto de responsabilidad administrativa.

Por otro lado, respecto del capítulo 4 podemos definir que la política criminal actual dentro de los delitos informáticos en el país todavía se hayan incipientes, incluso cuando se ha dado una mínima evolución en el cuerpo normativo como la LOPDP y algunas de las disposiciones en el COIP, se ven preocupantes brechas relacionadas a lo poco eficaz que es el derecho penal ecuatoriano en relación a la protección de los derechos digitales de los ciudadanos. Por esta razón, se puede llegar a decir que las soluciones que se deberían tomar en cuenta tendrán que involucrar de manera obligatoria ciertas reformas legislativas, esto incluyendo la mejor estructura y su fuerza en las instituciones, como lo es su articulación intersectorial, incluyendo una política criminal enfocada en las necesidades de la sociedad actual, esto enfocándose en la manera idónea de prevenir y conseguir respeto para las garantías constitucionales y derechos digitales.

Proteger datos personales en Ecuador posee varias desventajas, tanto legales e institucionales como culturales, sin embargo, tanto en el derecho constitucional como en el legal se da un reconocimiento con carácter formal al derecho a la autodeterminación informativa, aunque, la aplicación efectiva es considerablemente débil teniendo en cuenta el contexto actual y las necesidades que presentan, la ausencia de una política criminal centrada en ciberseguridad demuestra lo poco aptas que se encuentran las instituciones públicas para ejecutar sanciones, más

bien, se observa una enorme impunidad frente a casos de violación de datos personales que reposen en bases informáticas. En cuanto a la Superintendencia de protección de datos se debería garantizar una independencia que garantice el funcionamiento de esta institución, y de ser necesario se dé la creación de una unidad que tenga la eficacia suficiente para dar respuestas rápidas a los incidentes digitales, esto dando la capacidad de que se puedan ordenar inspecciones, y que se posea medidas cautelares y sanciones dependiendo el caso.

En general, el estudio que se ha realizado nos permite evidenciar claramente que en el Ecuador se enfrenta un escenario complejo y que requiere de una urgente reforma y especial atención en relación con el campo de los delitos informáticos. Si bien dentro del Código Orgánico Integral Penal (COIP) se dio un hito normativo importante al tipificar por primera vez cierto tipo de conductas como el acceso no autorizado, la interceptación de datos y el daño a sistemas informáticos, en la actualidad dichos artículos contenidos dentro del cuerpo normativo antes mencionado claramente resultan ser insuficientes frente a la rápida y constante evolución de las nuevas modalidades criminales de ciberdelitos que comúnmente son transnacionales como con el uso del ransomware, el phishing avanzado, el fraude con criptomonedas o la suplantación digital mediante el uso de la inteligencia artificial. Dicho rezago normativo, aunado a ciertas ambigüedades conceptuales y también a la lenta armonización con los estándares internacionales como los que se encuentran contenidos dentro del Convenio de Budapest, genera gran inseguridad jurídica y también limita la eficacia dentro de la persecución penal informática.

Dentro del plano operativo, las debilidades estructurales que se pueden encontrar son igualmente evidentes: falta de instalaciones adecuadas, es decir, laboratorios forenses digitales en gran parte del país, la escasez de peritos calificados dentro del campo de lo informático, la limitada capacitación técnica a otros operadores de justicia como los jueces y fiscales, la centralización de los recursos limitándose a pocas ciudades y la ausencia de protocolos claros para la cadena custodia en cuanto a la prueba digital. Dichas deficiencias, junto con la carencia de coordinación a nivel interinstitucional derivan en la existencia de investigaciones fragmentadas, pérdida de evidencia digital relevante para la investigación y, en muchos de los casos, se genera impunidad todo a causa de las falencias antes mencionadas que surgen durante el proceso. Casos relevantes como el ataque informático en contra de la Contraloría General del

Estado demuestran cómo la simple falta de protocolos establecidos y la escasa existencia de respuestas articuladas deja en evidencia la vulnerabilidad institucional del Ecuador respecto a los delitos informáticos, lo cual a su vez debilita la confianza que tienen los ecuatorianos respecto al sistema de justicia del país.

Visto a partir de una perspectiva política, se puede observar que en el Estado ecuatoriano todavía no se le ha otorgado a la ciberseguridad y a la persecución penal digital la prioridad estratégica que demanda dada la innovación tecnológica existente en los tiempos actuales. Los presupuestos otorgados son mínimos, las políticas públicas en varias ocasiones resultan fragmentarias y la cooperación internacional se ve limitada. Mientras que en otros países de la región como Colombia, Chile o México ya se han desarrollado fiscalías especializadas, se cuenta con protocolos avanzados y se tiene financiamiento sostenido para este tipo de delitos, no obstante en el Ecuador persiste una visión reactiva y parcial, misma que acentúa el rezago de nuestro país frente a las exigencias del cibercrimen mismo que día con día hace uso de tecnologías más modernas y sofisticadas.

Sin embargo, el análisis comparador realizado y los demás avances incipientes, como la reciente declaración de constitucionalidad por parte de la Corte Constitucional para la adhesión al Convenio de Budapest, abren una nueva oportunidad para poder replantear el modelo de política criminal dentro del país. Dicho modelo nuevo debe articularse en torno a tres ejes relevantes: i) reformas normativas continuas y actualizadas, ii) fortalecimiento operativo a través de la inversión en el talento humano, laboratorios forenses equipados y coordinación interinstitucional y iii) voluntad política expresada en una estrategia nacional de ciberseguridad con un plan de financiamiento sostenido y cooperación internacional para agilizar las investigaciones en torno a delitos informáticos trasnacionales.

Enfrentar los delitos informáticos no puede limitarse únicamente a la sanción; sino que además debe exigir ciertos tópicos como prevención, la implementación de educación digital a la ciudadanía y la constante capacitación a operadores de justicia. Solo de esta forma se podrá llegar a garantizar una respuesta ágil, moderna, integral y efectiva.

Actualmente el Ecuador se halla atravesando un punto de inflexión. Mantener la pasividad respecto a los delitos informáticos como se ha venido haciendo hasta ahora implicará mayor impunidad en cuanto a este tipo de conductas, genera debilitamiento de la tutela judicial efectiva consagrada en la Constitución y provoca la pérdida de confianza en las instituciones del Estado encargadas de impartir justicia.

Recomendaciones

Partiendo del análisis realizado dentro de los capítulos anteriores y considerando lo manifestado en las conclusiones alcanzadas, se pueden llegar a formular las siguientes recomendaciones destinadas a enfrentar deficiencias normativas, operativas e incluso institucionales en cuanto a los delitos informáticos en el Ecuador. Dichas propuestas buscan servir como una especie de lineamientos prácticos para guiar las actuaciones de legisladores, jueces, fiscales, policías, peritos y demás autoridades dentro del sistema de justicia ecuatoriana responsables de la seguridad digital y la justicia penal en general.

Primeramente, resultaría ser de carácter indispensable que se dé una urgente reforma del Código Orgánico Integral Penal (COIP) esto con la finalidad de actualizar los tipos penales relacionados con el ámbito de los delitos informáticos. Esta reforma deberá incorporar ciertas figuras emergentes en el ámbito de los ciberdelitos como por ejemplo el ransomware, la usurpación de la identidad digital haciendo uso de inteligencia artificial (IA), los ataques a infraestructuras críticas y también el fraude electrónico en las nuevas modalidades que surgen

actualmente. La tipificación de dichos tipos penales debe ser clara, técnica y armonizada con lo establecido dentro de los estándares internacionales, evitando así la aparición de vacíos legales y demás ambigüedades que puedan llegar a obstaculizar la labor judicial. De igual forma, se recomienda que se dé la incorporación expresa de principios referentes al correcto y manejo y preservación de la evidencia digital así como de la regulación detallada de cómo se debería acondicionar la cadena de custodia para llevarla al ámbito de lo tecnológico.

Como segundo punto, a modo de recomendación se podría dar la creación de fiscalías y juzgados penales que estén especializados únicamente en el ámbito de la ciberdelincuencia y que dichas entidades formen parte de la estructura del sistema judicial ecuatoriano. Dichas unidades deberán contar con personal altamente capacitado y especializado en temas de derecho penal informático, la informática forense e inclusive en la ciberseguridad. El uso de personal capacitado con esta especialización permitirá que se pueda llegar a dar una respuesta más ágil y técnica, reduciendo en gran medida la dependencia de otros peritajes externos y de esta forma se contribuirá con el fortalecimiento de la seguridad jurídica dentro de estos procesos judiciales. Adicionalmente, el Consejo de la Judicatura debería considerar la idea de implementar programas de certificación para jueces y fiscales en cuanto a materia de delitos informáticos, esto con el objeto de ampliar su conocimiento en dichas áreas.

Como tercer punto, resulta ser fundamental que dentro del Estado ecuatoriano se asigne recursos presupuestarios específicos destinados a invertir en la lucha contra el cibercrimen. Para que se pueda llegar a dar una adecuada lucha contra los delitos informáticos, entidades como la Fiscalía General del Estado, la Policía Nacional y el Consejo de la Judicatura forzosamente requieren laboratorios forenses digitales, mismos que estén debidamente equipados con software de última generación, licencias de programas informáticos diversos y plataformas digitales de

almacenamiento seguro de evidencia digital relevante. Dicha inversión presupuestaria deberá distribuirse de manera equitativa dentro de todo el territorio nacional ecuatoriano, esto con el objetivo de evitar la centralización de los recursos, es decir, evitar que dichas mejoras sean únicamente para las grandes ciudades como Quito o Guayaquil y garantizar que exista el acceso a justicia en las demás provincias y cantones del país.

Adicionalmente, otra recomendación importante es la implementación de un programa a nivel nacional de capacitación continúa, mismo que esté dirigido a operadores de justicia en el Ecuador. Dicho programa debería ser obligatorio, estructurado y actualizado periódicamente conforme las nuevas tecnologías que vayan surgiendo día con día, de manera tal que los fiscales, los jueces, los policías y los peritos informáticos puedan llegar a responder de manera eficaz a los cambios constantes que surgen en torno a la tecnología. Dicha capacitación deberá abarcar temas como análisis de metadatos informáticos, la trazabilidad digital, el blockchain, la criptografía, los delitos financieros electrónicos y demás estándares internacionales en cuanto a la materia de ciberseguridad y protección de derechos humanos fundamentales.

Dentro del ámbito de la prevención, se recomienda que el Estado se preocupe por la inclusión de una mayor educación digital tanto a nivel profesional como también a nivel escolar y universitario, así como también se preocupes por la implementación de campañas de concienciación pública sobre los posibles riesgos de navegar en línea, la protección de datos personales, los fraudes electrónicos y las prácticas seguras y correcto manejo de la información personal en el uso de redes sociales. Dicha estrategia deberá ser coordinada por entidades estatales como el Ministerio de Educación, el Ministerio de Telecomunicaciones y demás las universidades a nivel nacional inclusive pudiendo darse el apoyo del sector privado y organizaciones dentro de la sociedad civil ecuatoriana.

En cuanto al plano internacional, se recomienda que se aproveche plenamente la adhesión del Ecuador al Convenio de Budapest sobre Ciberdelincuencia, adoptando de esta forma mecanismos de cooperación ágiles destinados para la conservación y la posterior entrega transfronteriza de datos informáticos, así como también se recomiendo la participación activa en redes de colaboración internacional con entidades como la OEA y la INTERPOL. Además, resultaría beneficioso que se puedan llegar a celebrar acuerdos bilaterales con los otros países de la región, esto con el objetivo de que se pueda llegar a dar intercambio de buenas prácticas, asistencia judicial informática y capacitación técnica de otros profesionales de la región dentro del ámbito de la tecnología.

Para finalizar, todas y cada una de estas medidas deberán enmarcarse dentro de una política criminal integral y flexible, misma que pueda estar sujeta a una constante evaluación periódica y también a revisión constante en función de los cambios que se den respecto a la evolución tecnológica continua que reviste a la sociedad en la actualidad. En general, la aplicación de todas y cada una de estas recomendaciones le permitirá al Ecuador transitar desde el presente marco legal obsoleto en el que se encuentra hacia un modelo de justicia penal actual, especializado y eficaz para poder hacerle frente a los delitos informáticos modernos. Por lo que, no se trata únicamente de responder a la situación presente, sino que también se debería buscar prever y preparar al sistema jurídico y también a la sociedad en general para que podamos hacerles frente a los respectivos desafíos que seguramente surgirán dentro de la criminalidad digital en el futuro.

Bibliografías

Álvarez, C., & Maldonado, J. (2020). Ciberdelincuencia y sistema penal ecuatoriano: retos y perspectivas. *Revista Jurídica Iuris Dictio, 25*(2), 115-130. https://doi.org/10.31207/ih.v25i2.889

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. https://www.asambleanacional.gob.ec/es/leyes-aprobadas

Cabrera, I. (2017). *TE Tafur Callirgos*. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/4062

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Corte Constitucional del Ecuador. (2024, 25 de abril). *Dictamen 1-24-TI/24: Control de constitucionalidad del Convenio sobre Ciberdelincuencia* [Sentencia]. https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiI1Y2JlOGFiZS1kZWRjLTQwYmUtYjk1Yy02MjdjMDI2NWM5OGMucGRmIn0=

Fiscalía General del Estado. (2022). *Protocolo para el tratamiento de evidencia digital en procesos penales*. https://www.fiscalia.gob.ec/documentos-oficiales

Gómez Patiño, M. (2016). *Delitos informáticos y su tratamiento penal en el Ecuador* [Tesis de grado]. Universidad Central del Ecuador.

Martínez, L. (2021). La ciberseguridad en Ecuador: desafíos institucionales y normativos. *Revista Seguridad y Defensa, 14*(1), 73-90. https://doi.org/10.37156/rsd.v14i1.245

Mieres, J. (2009). *Manual de hacking y seguridad informática: Ataques informáticos* [Documento en línea]. elhacker.info.

https://elhacker.info/manuales/Hacking%20y%20Seguridad%20informatica/01_Ataques_informaticos-1.pdf

Ortiz Campos, N. J. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. http://revistas.pucese.edu.ec/hallazgos21/

Pichincha, R. (2020). *Contraloría revela que ha sufrido ataque informático en los últimos días*. Radio Pichincha. https://www.radiopichincha.com/contraloria-revela-que-ha-sufrido-ataque-informatico-en-los-ultimos-dias/

Pino, S. D. (2016). *Delitos informáticos en Costa Rica* [Tesis de licenciatura]. Universidad San Marcos. http://repositorio.usam.ac.cr/xmlui/handle/11506/2374

Ponce, C. C. (2021). *Sentencia de la Corte Constitucional del Ecuador sobre delitos informáticos* [Documento en línea]. Corte Constitucional del Ecuador. https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

Zumba, J. G. (2022). *Ciberdelincuencia en Iberoamérica*. *Revista Ibérica*. https://search.proquest.com/openview/02492b51bc001f7bf3254a198698d1d7/1?pq-origsite=gscholar&cbl=1006393

Anexos

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Ortiz Ramirez Joaquin Francisco portador(a) de la cédula de ciudadanía Nº **0151138377,** y **López Jara María Paz** portador(a) de la cédula de ciudadanía Nº **0150112977.** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Brechas jurídicas en Ecuador en la interferencia ilícita de datos personales informáticos, caso del ataque a la Contraloría General del Estado"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **10 de noviembre de 2025**

F: .....

Joaquin Francisco Ortiz Ramirez

C.I. **0151138377**

F: .....

López Jara María Paz

C.I. **0150112977**