UNIVERSIDAD LAICA VICENTE ROCAFUERTE

DE GUAYAQUIL

FACULTAD DE CIENCIAS SOCIALES Y DERECHO

CARRERA DE DERECHO

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

TEMA

EL TRATAMIENTO LEGAL DE LOS DELITOS CIBERNÉTICOS

TUTOR

Mg. RUTH LIBERTAD RONQUILLO ALVARADO

AUTOR

ERICK DARIO BÁRCENAS GONZÁLEZ

GUAYAQUIL

2025

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO Y SUBTÍTULO: El tratamiento legal de los delitos cibernéticos		
AUTOR/ES: **Bárcenas González Erick Darío**	**TUTOR:** Mg. Ronquillo Alvarado Ruth Libertad	
INSTITUCIÓN: Universidad Laica Vicente Rocafuerte de Guayaquil	**Grado obtenido:** ABOGADO	
FACULTAD: CIENCIAS SOCIALES Y DERECHO	**CARRERA:** DERECHO	
FECHA DE PUBLICACIÓN: 2025	**N. DE PÁGS:** **89**	
ÁREAS TEMÁTICAS: Derecho		
PALABRAS CLAVE: Derecho, Delito, Tecnología, Legislación		
RESUMEN: Esta investigación aborda el tratamiento legal del delito informático en Ecuador desde una perspectiva jurídica que considera la constante evolución de la tecnología. A través de un análisis documental, encuestas ciudadanas y entrevistas a expertos, el estudio identificó limitaciones clave en la legislación actual y su capacidad para responder de manera efectiva a las nuevas formas de delincuencia digital. Los hallazgos evidencian una débil preparación institucional, una educación pública limitada sobre los riesgos digitales y mecanismos insuficientes para la protección de datos. Como aporte, se propone una reforma legislativa que mejore la prevención y persecución del delito informático, adaptando el Derecho a los desafíos modernos que plantea la tecnología.		
N. DE REGISTRO (en base de datos):	**N. DE CLASIFICACIÓN:**	
DIRECCIÓN URL (Web):		
ADJUNTO PDF:	**SI** [X]	**NO** [ ]

CONTACTO CON AUTOR/ES: Bárcenas González Erick Darío	**Teléfono:**	**E-mail: ebarcenasg@ulvr.edu.ec**
CONTACTO EN LA INSTITUCIÓN:	Abg. Carlos Manuel Pérez Leyva -Decano **Teléfono:** (04) 259-6500 **Ext.** 249 **E-mail:** cperezl@**ulvr.edu.ec** Abg. Geancarlos Steven González Solorzano - Director de Carrera **Teléfono:** (04) 259- 6500 **Ext.** 233 **E-mail:** **ggonzalezso@ulvr.edu.ec**	

CERTIFICADO DE SIMILITUD

CERTIFICADO DE ANÁLISIS
magister

BARCENAS GONZALEZ - TESIS DELITOS CIBERNETICOS OR

3% Textos sospechosos

- 1% Similitudes
  - 0% similitudes entre comillas
  - 0% entre las fuentes mencionadas
- 2% Idiomas no reconocidos
- 29% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: BARCENAS GONZALEZ - TESIS DELITOS CIBERNETICOS OR.pdf
ID del documento: 962c527a706679a3998aa6a6988ba228c0d4893
Tamaño del documento original: 1 MB

Depositante: Federico Varas Chiquito
Fecha de depósito: 17/8/2025
Tipo de carga: interface
fecha de fin de análisis: 17/8/2025

Número de palabras: 13.772
Número de caracteres: 92.083

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.puce.edu.ec | "El hacker como sujeto activo el delito: límites y excepc... http://repositorio.puce.edu.ec:80/xmlui/bitstream/22000/13655/3/TESIS FINAL MSVL.pdf.txt 5 fuentes similares	< 1%		Palabras idénticas: < 1% (42 palabras)
2	Documento de otro usuario #fe7d19 Viene de de otro grupo 5 fuentes similares	< 1%		Palabras idénticas: < 1% (42 palabras)
3	www.microbank.com | ¿Qué es el phishing? Cómo identificarlo y protegerse de e... https://www.microbank.com/es/blog/prueba-es-el-phishing.html	< 1%		Palabras idénticas: < 1% (32 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.utn.edu.ec | La debilidad del proceso investigativo de los delitos info... http://repositorio.utn.edu.ec/bitstream/123456789/11747/6/PG 933 TRABAJO GRADO.pdf.txt	< 1%		Palabras idénticas: < 1% (20 palabras)
2	dspace.udla.edu.ec | La problemática de la protección de datos personales y la g... http://dspace.udla.edu.ec/bitstream/33000/10973/1/UDLA-EC-TAB-2018-53.pdf	< 1%		Palabras idénticas: < 1% (20 palabras)
3	kuex.es | Cómo identificar el phishing: una explicación con ejemplo | Kuex https://kuex.es/como-identificar-el-phishing-una-explicacion-con-ejemplo/	< 1%		Palabras idénticas: < 1% (11 palabras)
4	Documento de otro usuario #ef1d1 Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (10 palabras)
5	repositorio.uti.edu.ec | Ciberdelitos, y las dificultades que tiene la justicia para p... https://repositorio.uti.edu.ec/handle/123456789/5512	< 1%		Palabras idénticas: < 1% (10 palabras)

RUTH LIBERTAD RONQUILLO ALVARADO

Firmado digitalmente por RUTH LIBERTAD RONQUILLO ALVARADO
Fecha: 2025.10.03 09:33:20 -05'00'

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

El estudiante egresado **ERICK DARÍO BÁRCENAS GONZÁLEZ** declara bajo juramento, que la autoría del presente Trabajo de Titulación, **EL TRATAMIENTO LEGAL DE LOS DELITOS CIBERNÉTICOS**, corresponde totalmente al suscrito y me responsabilizo con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedo los derechos patrimoniales y de titularidad a la **UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL**, según lo establece la normativa vigente.

Autor

ERICK DARÍO BÁRCENAS GONZÁLEZ
C.I: 0924335417

CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR

En mi calidad de docente Tutor del Trabajo de Titulación **EL TRATAMIENTO LEGAL DE LOS DELITOS CIBERNÉTICOS**, designado(a) por el Consejo Directivo de la Facultad de **CIENCIAS SOCIALES Y DERECHO** de la Universidad **LAICA VICENTE ROCAFUERTE DE GUAYAQUIL**.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Trabajo de Titulación, titulado: **EL TRATAMIENTO LEGAL DE LOS DELITOS CIBERNÉTICOS**, presentado por el estudiante **ERICK DARÍO BÁRCENAS GONZÁLEZ** como requisito previo, para optar al Título de **ABOGADO**, encontrándose apto para su sustentación.

Ruth Libertad Ronquillo Alvarado
Firmado digitalmente por Ruth Libertad Ronquillo Alvarado
Fecha: 2025.08.16 23:40:43 -05'00'

MGTR. RUTH LIBERTAD RONQUILLO ALVARADO.
C.I. 0912365061

.

AGRADECIMIENTO

En primer lugar, tengo que reconocer y dar gracias a Dios, ya que ha estado presente en cada una de las etapas de este trabajo de investigación. Así mismo reconozco el arduo trabajo y dedicación de la asignada Tutora, la Doctora Ruth Ronquillo Alvarado, quien en todo momento estuvo al tanto de la elaboración de este trabajo.

A mis padres, quienes han sido el motor principal durante todo el trayecto de la carrera, preocupados porque no me falte nada durante la misma, estar al día en los pagos, comprensión y sobre todo apoyo total durante el tiempo de mis prácticas preprofesionales, además de darme aliento en días en que sí veía las cosas difíciles, pero no me dejaban caer.

A mis hermanos, Joel y Miguel que me han dado el apoyo y ánimo de seguir adelante y no quedarme atrás, a pesar de nuestras constantes peleas me han dejado saber siguen ahí para cuando necesite de ellos.

A mis amigos que hice durante el periodo de la carrera, Jhael Iza y Denisse Jiménez, con quienes compartí los momentos más duros y a la vez los mas buenos durante este periodo y las risas nunca faltaron, además fue el grupito con quienes nos apoyábamos en todos los trabajos grupales como lo prometimos desde un inicio.

A esas amistades externas, aquellas que a pesar de no tener frecuente contacto con ellas me daban ese mensaje de ánimo de seguir y no rendirme hasta conseguir mi objetivo, el de sacar el titulo que alguna vez le comenté que me gustaría obtener.

Erick Bárcenas González

DEDICATORIA

Este Trabajo se lo dedico en primer lugar a Dios por contestar siempre que lo busqué, sobre todo en aquellas noches que me encontraba confundido y desanimado, de alguna manera u otra siempre después de hablar con usted, sentía un alivio tremendo.

Luego a mis padres Luis y Elsy, por su manera incondicional de estar ahí para cuando necesite de ellos en todo momento, a mi querida madre por doblar rodilla y mantenerse firme en sus oraciones para que las cosas salieran bien. A mi viejo por motivarme siempre con su frase, Marino de Guerra.

A mis hermanos Joel y Miguel, por siempre brindarme ese apoyo y constante ánimo muchachos. Por todas esas veces que les comentaba mis logros y se alegraban como si fueran los suyos, además por nunca recibir un NO de sus partes cuando requería de sus conocimientos.

Erick Bárcenas González

RESUMEN

Esta investigación aborda el tratamiento legal del delito informático en Ecuador desde una perspectiva jurídica que considera la constante evolución de la tecnología. A través de un análisis documental, encuestas ciudadanas y entrevistas a expertos, el estudio identificó limitaciones clave en la legislación actual y su capacidad para responder de manera efectiva a las nuevas formas de delincuencia digital. Los hallazgos evidencian una débil preparación institucional, una educación pública limitada sobre los riesgos digitales y mecanismos insuficientes para la protección de datos. Como aporte, se propone una reforma legislativa que mejore la prevención y persecución del delito informático, adaptando el Derecho a los desafíos modernos que plantea la tecnología.

Palabras clave: Derecho, Delito, Tecnología, Legislación.

ABSTRACT

This research addresses the legal treatment of cybercrime in Ecuador from a legal perspective that considers the constant evolution of technology. Through documentary analysis, citizen surveys, and expert interviews, the study identified key limitations in the current law and its ability to respond effectively to new forms of digital crime. The findings highlight weak institutional preparedness, limited public education on digital risks, and insufficient mechanisms for data protection. As a contribution, a legislation reform is proposed to improve the prevention and prosecution of cybercrime, adapting law to the modern challenges posed by technology.

Keywords: Law, Crime, Technology, Legislation

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En los últimos años, el desarrollo tecnológico ha transformado la manera en que las personas se comunican, realizan transacciones y acceden a la información. Sin embargo, esta evolución digital también ha dado paso a nuevas formas de criminalidad, conocidas como delitos cibernéticos. En Ecuador, estos delitos han ido en aumento y se manifiestan principalmente a través de estafas virtuales, hackeos, acceso no autorizado a sistemas y robo de datos personales. No solo los ciudadanos, sino también las instituciones públicas y privadas se ven perjudicados por estos actos ilegales.

El propósito de este trabajo de titulación es examinar cómo se tratan legalmente los delitos cibernéticos en Ecuador, particularmente la legislación que rige en el Código Orgánico Integral Penal (COIP). El estudio se concentra en determinar cómo están clasificados estos crímenes, qué tan eficaces son las sanciones establecidas y los retos que afronta el sistema legal con respecto a esta forma delictiva que está en permanente cambio.

La legislación ecuatoriana vigente y casos significativos divulgados por medios de comunicación del país serán utilizados como referencia en el estudio. La relevancia de la investigación reside en que es necesario reforzar el marco legal para salvaguardar a los usuarios digitales de amenazas virtuales cada vez más sofisticadas y comunes.

La investigación estará dividida en cuatro secciones. La introducción general del tema, el problema de investigación, la justificación, los objetivos y la delimitación se encuentran en el primer capítulo.

El segundo capítulo desarrolla el marco teórico, abordando conceptos clave sobre ciberdelincuencia y su clasificación. El tercer capítulo analiza el marco legal ecuatoriano aplicable a los delitos cibernéticos. Finalmente, el cuarto capítulo expone las conclusiones y recomendaciones resultantes del estudio.

CAPÍTULO I

ENFOQUE DE LA PROPUESTA

1.1 Tema:

El Tratamiento Legal de los Delitos Cibernéticos

1.2 Planteamiento del Problema:

Al estar inmersos en una era digital, donde la gran mayoría de las empresas se han visto en la obligación de actualizarse y brindar mejoras y comodidades en ejecución de sus servicios, la posibilidad del encuentro o el estrellón con el ciberdelito son muy altas, representando un riesgo para las mismas, además una considerable exposición y a la vulneración de sus datos. Esta afectación podría verse desde sus ingresos financieros hasta la reputación de esta.

Sabido es que quienes se dedican a este tipo de delitos, no son simples informáticos en el control y manejo de medios digitales, incluso podría resultar casi imposible detectarlos debido a que algunos de ellos son difíciles de fichar y rastrear porque tienden a evolucionar y así mismo incrementar su reproducción.

Por otro lado, cabe recalcar que la orientación del ciberdelito se basa en el cometimiento de infracciones legales a través de la tecnología. La UNIR al respecto menciona, que a través de las puertas de acceso de información (celulares, computadoras, etc.) los ciberdelincuentes no solo atentan contra la confidencialidad de los datos personales y comerciales de las empresas, lo más graves es que estos también podrían llegar a suplantar la identidad de estas. (Universidad Internacional de la Rioja, 2024)

De no atenderse este tipo de delitos y dejarlos en la impunidad por considerarse burocráticos o de difícil ejecución llegar a determinar su sanción, estamos expuestos a que esa constante evolución y desarrollo de las estrategias maliciosas de estos, incremente gradualmente con el tiempo. Debido a esto la Financial Crime Academy,

recomienda que es esencial mantenerse alerta y actualizar continuamente las medidas de seguridad para ir un paso adelante a los ciberdelincuentes. (FAC By Verdian, 2024)

El problema relacionado con los delitos cibernéticos se manifiesta con mayor frecuencia en zonas urbanas de alta conectividad digital, como la ciudad de Guayaquil, donde el uso de internet para transacciones financieras, comunicación y servicios públicos es cada vez más común. La digitalización en ascenso ha aumentado el riesgo de que los ciudadanos y las empresas sean víctimas de ataques cibernéticos, incluyendo fraudes virtuales, phishing, suplantación de identidad e intrusiones no autorizadas. A pesar de los avances en tecnología, las instituciones responsables de prevenir y sancionar estos delitos todavía se enfrentan a restricciones legales y técnicas para abordar de manera efectiva este problema.

Este análisis es fundamental porque posibilita entender a fondo cómo se enfrentan los delitos informáticos en el sistema jurídico ecuatoriano y qué tan bien equipada está la legislación vigente para afrontar los retos del entorno digital. Mediante la investigación, se podrá determinar si el marco legal actual resguarda de manera apropiada los derechos ciudadanos ante riesgos virtuales y si las instituciones judiciales están preparadas para implementar la ley de forma eficaz en tales situaciones. Asimismo, posibilita la reflexión acerca de lo necesario que es adecuar las leyes penales a los nuevos tipos de delitos tecnológicos.

El análisis permitirá identificar los desafíos prácticos, las carencias normativas y las debilidades en el manejo legal de los delitos cibernéticos en Ecuador, sobre todo en áreas urbanas como Guayaquil.

Asimismo, brindará herramientas conceptuales y jurídicas para recomendar mejoras normativas o institucionales que fortalezcan la protección de los usuarios en entornos digitales. Con ello, se contribuirá al desarrollo de políticas públicas más eficientes y a la formación de una cultura jurídica adecuada frente al cibercrimen.

1.3 Formulación del Problema:

¿De qué manera el ordenamiento jurídico ecuatoriano contempla y sanciona los delitos cibernéticos?

1.4 Objetivo General

Analizar vulneraciones de la ley en actividades cibernéticas.

1.5 Objetivos Específicos

- Evaluar el impacto de este tipo de delitos en esta era digital.
- Analizar el límite de legalidad permitido por la ley en actividades digitales.
- Sugerir medidas de seguridad digital contra ataques hackers a las empresas.

1.6 Idea a Defender

En la actualidad, los delitos cibernéticos representan una amenaza creciente para la seguridad jurídica y ciudadana, especialmente en ciudades altamente digitalizadas como Guayaquil. Aunque el Ecuador ha integrado en su Código Orgánico Integral Penal (COIP) reglamentaciones para castigar este tipo de comportamientos, los progresos tecnológicos a menudo exceden la capacidad de respuesta de las normativas vigentes. Los ciudadanos y las instituciones están preocupados por esta situación, ya que a menudo se encuentran restringidos para actuar de manera efectiva frente a la perpetración de estos delitos.

Es esencial tener en cuenta que los delitos informáticos impactan no solo el patrimonio económico, sino también la identidad digital, la privacidad y la confianza en los sistemas digitales. En este panorama, es esencial que el sistema jurídico del Ecuador no solo incluya sanciones apropiadas, sino que además asegure su adecuada implementación, robusteciendo las competencias judiciales e investigativas para abordar este fenómeno con más firmeza.

El enfoque principal de este estudio es que el tratamiento legal actual de los delitos cibernéticos en Ecuador no es suficiente ante la rápida evolución de estas amenazas digitales. Para garantizar una respuesta penal efectiva que proteja la seguridad digital de los ciudadanos, es necesario actualizar continuamente la normativa y aumentar la especialización de los operadores de justicia.

En consecuencia, esta investigación sugiere que es necesario fortalecer el marco jurídico y operativo en el que se combaten los delitos cibernéticos en la nación, fomentando reformas a nivel legal, inversión en tecnología forense y campañas de sensibilización entre la ciudadanía. La lucha efectiva contra el cibercrimen y la protección de los derechos individuales en el entorno digital solo se conseguirán a través de una perspectiva integral.

La percepción de inseguridad y desconfianza hacia las instituciones responsables de la protección digital muestra el impacto social. La inseguridad en cuanto a la capacidad de respuesta de las autoridades y a la efectividad de las pesquisas puede hacer que muchas víctimas no solo minimicen el nivel de gravedad de estos crímenes, sino que tampoco denuncien. Por otro lado, las empresas y entidades públicas también sufren pérdidas económicas y daños reputacionales, lo que repercute en el tejido productivo y en la estabilidad institucional del país (Juca Maldonado & Medina Peña, 2023)

1.7 Línea de Investigación Institucional

Sociedad civil, derechos humanos y gestión de la comunicación.

Esta investigación se inscribe dentro de la línea de investigación institucional orientada a la sociedad civil, dado que los delitos cibernéticos afectan directamente a los derechos fundamentales de las personas en un entorno cada vez más digitalizado. La sociedad contemporánea es muy dependiente del empleo de tecnologías para comunicarse, trabajar, comerciar y acceder a servicios, lo que la vuelve susceptible frente a nuevas maneras de crimen que tienen lugar en el ciberespacio.
El propósito de la investigación es examinar el tratamiento legal que se otorga a los

crímenes informáticos en la actualidad, para así establecer si las leyes actuales son adecuadas para resguardar a los ciudadanos ante riesgos como el fraude digital, el hurto de identidad, el ingreso no autorizado a datos personales o financieros y otros delitos que comprometen la privacidad, integridad y seguridad de las personas.

Asimismo, este trabajo pretende generar conciencia sobre la necesidad de actualizar constantemente el marco legal, así como de fortalecer la capacidad de las instituciones públicas para prevenir, investigar y sancionar este tipo de delitos. La sociedad civil es la más expuesta a estas amenazas, y al mismo tiempo, es la que más se beneficia del desarrollo de políticas públicas eficaces y de una legislación moderna que garantice una protección efectiva en el entorno digital.

Esta investigación, a nivel particular, se vincula con la línea académica de Derecho Penal de la Facultad de Jurisprudencia porque examina el análisis legal de comportamientos que constituyen infracciones penales y su efecto en el orden social y la reacción del sistema judicial.

El Derecho Penal, siendo la rama que se encarga de tipificar y castigar las acciones que dañan los bienes jurídicos protegidos, enfrenta el desafío de adecuarse a los nuevos contextos en los que ocurren delitos, particularmente aquellos relacionados con el empleo de tecnologías.

En este marco, el análisis de los crímenes cibernéticos posibilita la detección de carencias legales, obstáculos en la persecución penal y la necesidad de una formación especializada en el campo de la criminalística digital. Asimismo, se analiza la manera en que la legislación penal puede progresar para abordar estas amenazas de forma efectiva, respetando siempre los principios del debido proceso y la legalidad penal.

Esto no solo ayuda a desarrollar teóricamente el Derecho Penal contemporáneo, sino también a robustecer las instituciones en la batalla contra el delito digital organizado y en la protección de los derechos ciudadanos durante la era tecnológica.

CAPÍTULO II
MARCO REFERENCIAL

De acuerdo con Guerrero Álvarez (2021), se evidencia que, aunque el COIP sanciona los ciberdelitos, carece de medidas complementarias efectivas. Por ejemplo, nada impide que un condenado acceda nuevamente a dispositivos digitales, lo que facilita la reincidencia.

Según el estudio realizado por Ochoa Marcillo (2021) muestra que Ecuador enfrenta dificultades tanto en generar políticas de ciberseguridad como en implementar acuerdos internacionales. La autora enfatiza la importancia del Convenio de Budapest en este escenario; se trata del primer acuerdo internacional que trata el cibercrimen de manera exhaustiva. A pesar de que Ecuador no lo ha firmado, se le considera un modelo regulador fundamental para fomentar la colaboración internacional, acelerar los procesos de investigación transnacional y crear un marco común que permita afrontar estos delitos en el ámbito digital.

El estudio de Sarmiento Chamba (2024) señala que el limitado entrenamiento en áreas esenciales como la inteligencia artificial, la ciberseguridad y los métodos forenses digitales restringe considerablemente las habilidades de los jueces y fiscales para investigar y procesar delitos cibernéticos. Asimismo, el análisis alerta que las penas en el COIP son desmedidas o débiles, sobre todo para los delitos que producen un fuerte impacto social y económico.

El trabajo de Posso López (2022) presenta un estudio comparativo entre las leyes en materia de ciberdelincuencia transfronteriza de cuatro países: Ecuador, México, Colombia y Estados Unidos. El análisis muestra que Ecuador afronta serias restricciones, tanto legales como estructurales, para combatir estos delitos, a causa de la ausencia de un marco normativo preciso que incluya las especificidades del cibercrimen internacional y la falta de colaboración efectiva con otras naciones. La autora también pone de relieve la insuficiente capacitación que tienen los operadores judiciales en cuestiones relacionadas con la ciberseguridad, lo que colabora directamente con elevados niveles de impunidad.

El estudio académico realizado por Ordóñez Córdova (2024) examina cómo ha sido la evolución de las normas relacionadas con los delitos informáticos en el país. Es importante señalar que la Ley de Comercio Electrónico, promulgada en el 2002, fue el primer paso en la creación de las normas necesarias para controlar las operaciones electrónicas en Ecuador. Después, en 2014, el Código Orgánico Integral Penal (COIP) incluyó formas penales concretas para los delitos cibernéticos, como la interceptación de datos y el acceso a sistemas sin autorización. La Ley de Protección de Datos Personales, promulgada en 2021, ha fortalecido la seguridad de la información en el área digital. No obstante, el análisis indica que, a pesar de la existencia de un marco legal, hay restricciones para su implementación efectiva por causa de una capacitación en ciberseguridad que no es suficiente y por la ausencia de una infraestructura forense digital apropiada.

2.1 Marco teórico:

2.1.1 Delitos Cibernéticos

Los delitos cibernéticos constituyen un conjunto de conductas ilícitas cometidas mediante el uso de tecnologías de la información y comunicación, especialmente Internet y redes digitales, con el fin de dañar, defraudar o violar la privacidad de personas o instituciones. En Ecuador, se ha registrado un creciente número de casos relacionados con apropiación por medios electrónicos, violación a la intimidad, pornografía infantil y estafas informáticas, con cifras que muestran más de 900 investigaciones en 2022 y una tasa constante en 2023 y 2024, lo que revela una evolución preocupante de estas conductas ilícitas a pesar de las medidas legales existentes (Moncada Chachapoya y Miranda Villacís, 2025)

El aumento de delitos cibernéticos, como la sustracción de datos personales, el fraude en línea, los asaltos digitales a compañías y la sextorsión, demuestra que estas acciones constituyen un peligro constante para la sociedad ecuatoriana. No únicamente marcos legales eficaces, sino también una respuesta técnica que tenga la capacidad de detectar, investigar y castigar de manera adecuada a los perpetradores es lo que este fenómeno necesita. Asimismo, el estudio de tendencias emergentes revela que la falta

de colaboración coordinada entre las entidades gubernamentales, judiciales y los proveedores de servicios digitales agrava los delitos perpetrados en redes sociales como la difusión no autorizada de datos y las estafas electrónicas. Esto demuestra que, más allá de mejorar la legislación, el combate eficaz de los delitos cibernéticos exige un enfoque integral que incluya cooperación institucional y tecnología avanzada.

2.1.2 Principales delitos informáticos

En el periodo 2020 – 2022, se reportaron 3 183 casos, con un incremento notable de estafas en línea, mientras que la violación de la intimidad y los delitos relacionados con pornografía infantil mostraron un alto número de denuncias, lo que demuestra la complejidad y el alcance de la ciberdelincuencia. (Ecuavisa, 2024)

En Ecuador, el phishing es uno de los delitos informáticos más comunes y dañinos, caracterizado por el envío de correos electrónicos, mensajes de texto o de aplicaciones como WhatsApp que imitan instituciones legítimas para extraer datos confidenciales o financieros. Según datos de la Policía Nacional, durante 2024 se reportaron más de 576 denuncias por suplantación de identidad y estafas virtuales vinculadas al phishing. El phishing representa una de las amenazas tecnológicas más comunes y efectivas en el país: correos y mensajes fraudulentos que suplantan entidades reales como bancos o servicios públicos han afectado de forma creciente a usuarios y organizaciones, siendo Ecuador el líder regional en ataques detectados por la firma ESET. (Primicias, 2023)

Por último, el fraude digital abarca medidas más agresivas, como el uso de malware y troyanos bancarios que permiten el robo directo de dinero desde cuentas de usuarios o empresas. En Ecuador, durante la pandemia de COVID-19, se produjeron más ataques, lo que causó un aumento en las denuncias por apropiación fraudulenta y acceso no autorizado a sistemas informáticos. El impacto económico es significativo, afectando a las personas y al sector público y privado; esto pone de manifiesto la necesidad urgente de contar con mecanismos legales y técnicos más robustos para evitar y luchar contra estos delitos.

2.1.3 Regulación legal de los delitos cibernéticos

En Ecuador, la evolución de las normas ha tenido tres hitos relevantes. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue promulgada en el año 2002, que estableció las primeras definiciones y castigos asociados con delitos informáticos, tales como la estafa en línea y el acceso ilegal a sistemas. El Código Orgánico Integral Penal (COIP), que fue promulgado en 2014, supuso un avance significativo al anular las normativas anteriores y definir como delitos ciertas acciones concretas, como son el acceso a datos sin autorización, la interceptación ilegal y la violación de la intimidad, y al establecer penalidades definidas y diferenciadas. (Suárez, 2015)

El siguiente avance normativo fue la Ley Orgánica de Protección de Datos Personales de 2021, que estableció principios como la minimización de datos, la necesidad de consentimiento y la supervisión estatal. Sin embargo, persisten desafíos en su implementación. Solo un 35 % de las empresas ha adaptado sus procesos, y muchos ciudadanos aún desconocen los mecanismos básicos para proteger su información personal (UTPL, 2025)

2.1.4 Convenios internacionales y cooperación jurídica

La adhesión de Ecuador al Convenio de Budapest sobre Ciberdelincuencia, aprobada en julio de 2024, marca un avance significativo en la cooperación internacional para combatir los delitos informáticos. Este tratado, adoptado inicialmente en 2001 por el Consejo de Europa, establece normas comunes para la tipificación de ciberdelitos y promueve mecanismos de asistencia mutua, intercambio de pruebas electrónicas y enlaces 24/7 entre países partes (Noticias Policia, 2024)

Además, Ecuador ha fortalecido su cooperación con organismos internacionales y bloques regionales, como la Unión Europea, con la que mantiene acuerdos para el intercambio de información, asistencia técnica y operaciones conjuntas contra la delincuencia organizada y el narcotráfico, ámbitos que incluyen la ciberdelincuencia como una amenaza creciente. La creación de la Unidad de EUROPOL en la Policía Nacional del Ecuador es un ejemplo concreto de esta colaboración, que permite un

enlace directo para compartir inteligencia y coordinar acciones contra el crimen digital (Unión Europea, 2024)

2.1.5 Impacto social en China

El impacto social de la ciberdelincuencia en China es profundo y multifacético, afectando tanto a la población como a la estabilidad económica y política del país. China enfrenta una "crisis de ciberdelincuencia" que, según Naciones Unidas e Interpol, requiere cooperación internacional urgente para combatirla debido a la sofisticación y escala sin precedentes de estos delitos. Entre los problemas más graves se encuentra la trata de personas para trabajos forzados en fábricas de ciberdelincuencia, afectando a cientos de miles de víctimas, lo que genera un sufrimiento humano considerable y un impacto social negativo (Dixon, 2025)

El uso extendido de sistemas de pago digitales y aplicaciones de chat móvil en China, sumado a la alta integración tecnológica del país, lo vuelve un objetivo atractivo para los ciberdelincuentes que utilizan estas estructuras para perpetrar fraudes y otros crímenes. Esto tiene un impacto negativo en la seguridad que los usuarios sienten al usar plataformas digitales, y causa pérdidas financieras importantes para las empresas y los consumidores.

En contrapartida, la utilización de la ciberdelincuencia como instrumento para espionaje y operaciones apoyadas por el Estado ha socavado la confianza pública y ha desestabilizado servicios fundamentales en China. Los ataques cibernéticos dirigidos a infraestructuras críticas, como la sanidad o las redes eléctricas, no solo causan daños económicos, sino que también ponen en riesgo la seguridad y el bienestar social. Este fenómeno ha llevado a un aumento en la percepción de vulnerabilidad y desconfianza hacia las instituciones encargadas de proteger la seguridad digital (Digital Security, 2025)

2.1.6 Impacto social en Estados Unidos

El impacto social de la ciberdelincuencia en Estados Unidos es significativo y multifacético, afectando tanto a individuos como a sectores críticos de la economía y la infraestructura nacional. En primer lugar, el crecimiento de ataques como el ransomware

ha tenido efectos directos sobre servicios fundamentales. Lo que sucedió en 2024 con incidentes que perjudicaron a proveedores de atención médica y servicios automotrices, provocando interrupciones que afectan la vida cotidiana de millones de individuos, lo demuestra. Estos ataques tienen un impacto en la confianza de la ciudadanía en cuanto a la seguridad de los sistemas digitales, además de generar pérdidas económicas (National Cybersecurity Alliance, 2025)

Además, el hurto de identidad ha progresado hacia modalidades más complejas, empleando tecnologías como la inteligencia artificial para generar identidades sintéticas o eludir sistemas de verificación. Esto hace que los ciudadanos sean más vulnerables y dificulta a las autoridades la protección de la privacidad y de los datos personales. Esta circunstancia produce un efecto social al incrementar la percepción de desconfianza e inseguridad en las plataformas digitales.

2.2 Conceptos Claves:

2.2.1 El Catfishing

El catfishing es una práctica donde una persona crea una identidad falsa en internet, especialmente en redes sociales o aplicaciones para conocer gente, con la intención de engañar a otros. Generalmente, quien hace catfishing busca formar relaciones falsas para aprovecharse emocional o económicamente de la víctima. Este tipo de delito puede causar mucho daño, no solo a nivel emocional, sino también en la reputación y hasta en la economía de quien es engañado.

Según un estudio publicado en Springer, el catfishing implica la creación de un perfil personal falso en un sitio de redes sociales con fines fraudulentos o engañosos. La investigación también destaca que, aunque el término se popularizó con el documental "Catfish" en 2010, la práctica existía mucho antes y ha evolucionado con el tiempo (Fernando, 2023)

2.2.2 Medios Digitales

Los medios digitales se han convertido en un pilar fundamental para la comunicación y el intercambio de información en la sociedad actual. La masificación del acceso a internet y dispositivos tecnológicos ha transformado la forma en que las personas interactúan, acceden a noticias, realizan compras y mantienen relaciones sociales. Este entorno digital también presenta retos importantes en materia de protección de datos personales, privacidad y seguridad, debido a la creciente vulnerabilidad frente a delitos cibernéticos como el fraude electrónico, la suplantación de identidad y el ciberacoso (Castells, 2021)

De acuerdo con la Comisión Interamericana de Derechos Humanos (CIDH), el uso de medios digitales hace posible que la información se difunda rápidamente y que las personas ejerzan derechos esenciales, como la libertad de expresión. No obstante, también advierten acerca de los peligros relacionados con la desinformación, el discurso de odio y la violación de derechos en el ámbito digital. Esto requiere una regulación justa que proteja a los usuarios sin perjudicar la libre comunicación. La CIDH subraya la importancia de fortalecer la cooperación regional para enfrentar estos desafíos y fomentar un uso responsable de las tecnologías.

2.2.3 Ciberdelitos

Los ciberdelitos comprenden una variedad de actividades ilegales realizadas mediante el uso de tecnologías de la información y comunicación, tales como fraudes, ataques a sistemas informáticos, suplantación de identidad y robo de datos personales. Estos delitos presentan una complejidad especial debido a su naturaleza transnacional y el uso de técnicas que dificultan la identificación de los perpetradores. En Ecuador, el marco legal para sancionar los ciberdelitos está contenido en el Código Orgánico Integral Penal (COIP), que ha incorporado tipos penales relacionados con la delincuencia informática. Sin embargo, este marco enfrenta desafíos importantes para mantenerse actualizado frente a las nuevas modalidades delictivas y para fortalecer la capacidad de respuesta de las autoridades (UNODC, 2021)

Asimismo, la cooperación internacional y la formación continua de operadores de justicia son elementos indispensables para combatir eficazmente la ciberdelincuencia. Organismos como Interpol señalan que la rápida evolución tecnológica exige mecanismos legales flexibles y personal especializado para proteger los derechos de los usuarios y garantizar la seguridad en el entorno digital (INTERPOL, 2023)

2.2.4 Phishing

El phishing es una modalidad de delito informático que utiliza técnicas de ingeniería social para engañar a las personas y obtener información confidencial (como contraseñas, datos bancarios o credenciales de acceso) haciéndose pasar por entidades legítimas a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsificados (Kosinski, 2018)

En Ecuador, el phishing ha aumentado de manera preocupante recientemente. Más de 12 millones de ciberataques fueron registrados en el país en 2024, siendo el phishing uno de los métodos más utilizados, y causando un impacto concreto en áreas como la educación, la salud, el gobierno y las finanzas. Las cifras oficiales indican que, entre 2015 y 2025, se registraron más de 25,000 casos de phishing, lo cual demuestra la gravedad del problema en el país. Ecuador, además, es el cuarto país de América Latina con más intentos de infección por minuto. En 2022, se registraron 84 ciberataques por cada minuto en promedio, lo que muestra la gran susceptibilidad ante este tipo de riesgos. (Navarro, 2025)

Los ciberdelincuentes aprovechan la baja cultura digital y los errores humanos, que según estudios representan el origen del 95% de las brechas de seguridad, para ejecutar ataques de phishing con mensajes urgentes o engañosos que inducen a las víctimas a revelar información sensible o descargar malware. Plataformas como WhatsApp, Facebook y el correo electrónico son canales frecuentes para estos ataques, donde se utilizan enlaces falsos o sitios web clonados que imitan a entidades legítimas para captar datos personales o financieros (Bustán, 2025)

La creación de tecnologías como la inteligencia artificial ha llevado a que los ataques de phishing sean más complejos y personalizados, dando lugar al fenómeno conocido como spear phishing, el cual tiene la capacidad de engañar incluso a individuos con conocimientos digitales. Por esa razón, para que la ciberseguridad de Ecuador mejore, no es suficiente con invertir en tecnología. Además, para mejorar la capacidad de defensa frente a estas amenazas, es crucial brindar educación permanente y crear estrategias integrales que incluyan a las empresas, las instituciones y a la sociedad en general.

2.2.5 Malware

El malware es un software malicioso que comprende todo tipo de programas informáticos diseñados con la finalidad de causar daño, alterar el funcionamiento de sistemas, espiar la actividad de usuarios o apropiarse de recursos digitales sin autorización. Normalmente son virus, troyanos, gusanos, ransomware y spyware.

Los virus son programas que se replican y se propagan infectando archivos y sistemas, mientras que los troyanos se ocultan dentro de aplicaciones aparentemente legítimas para acceder de forma oculta a los dispositivos. Los gusanos, en cambio, se duplican automáticamente a través de redes, provocando una sobrecarga y un daño masivo. El ransomware es particularmente amenazante ya que cifra los datos del usuario y requiere de un rescate para liberarlos, perjudicando a personas y organizaciones por igual. El spyware tiene la función de recolectar y vigilar información delicada sin que el usuario se dé cuenta.

En Ecuador, el malware constituye una amenaza que va en aumento a causa de la mayor conectividad y del incremento en el empleo de tecnologías digitales. De acuerdo con informes recientes, el país ha sufrido un aumento de ataques de ransomware y otros tipos de malware que han tenido un impacto en áreas esenciales como la salud, la banca y la administración pública. No solo provocan pérdidas económicas importantes estos ataques, sino que además ponen en riesgo la confidencialidad y la integridad de datos de empresas y personales.

La difusión de malware se produce por medio de varios medios, incluyendo la descarga de software desde páginas web no fiables, la recepción de mensajes de texto infectados, el acceso a enlaces maliciosos en las redes sociales o los correos electrónicos con archivos adjuntos contaminados. La falta de actualización de sistemas operativos y programas, junto con hábitos inseguros de los usuarios, facilita la infección y expansión de estos programas dañinos.

2.2.6 Suplantación de identidad digital

La suplantación de identidad digital consiste en la acción mediante la cual una persona se hace pasar por otra a través de medios electrónicos, con el propósito de engañar, perjudicar o cometer actos ilícitos. Esta conducta puede manifestarse en redes sociales, correos electrónicos, plataformas bancarias, entre otros. Desde el ángulo de la ley, este crimen tiene un impacto directo sobre derechos esenciales como la honra y la privacidad; por lo tanto, su tipificación debe tener en cuenta cuán grave es el daño que causa. Una legislación precisa que posibilite la persecución y sanción apropiadas de estos actos es necesaria debido a la rapidez con que se difunden y a lo complicado que resulta rastrear a los autores.

Asimismo, la usurpación de identidad representa desafíos probatorios importantes para las autoridades que llevan a cabo la investigación, ya que el perpetrador tiende a ocultar su huella utilizando instrumentos tecnológicos sofisticados. Por ello, es fundamental contar con normativas específicas y procedimientos técnicos que permitan identificar y sancionar a los responsables, garantizando a su vez el respeto al debido proceso. La ausencia de una regulación clara genera vacíos legales que dificultan la persecución efectiva de estos delitos.

2.2.7 Ransomeware

El ransomware es una modalidad de software malicioso que bloquea el acceso a la información o sistemas de una víctima hasta que se pague un rescate, generalmente en criptomonedas. Este tipo de ataque ha aumentado de manera exponencial en los años recientes, perjudicando a individuos, empresas e instituciones estatales. Desde el punto de vista legal, se plantea la dificultad de clasificar adecuadamente este

comportamiento y crear protocolos de respuesta que incluyan a las fuerzas del orden y a los expertos en informática forense. La ley debe contemplar castigos duros para quienes son responsables, además de procedimientos que garanticen una recuperación segura de la información.

Los desafíos desde el punto de vista legal no solo incluyen sancionar al autor, sino también implementar procedimientos para salvaguardar a las víctimas y recuperar la información. Además, dado que estos ataques tienden a llevarse a cabo desde territorios foráneos, es fundamental promover la colaboración internacional. Para asegurar que las sanciones sean efectivas y que las víctimas obtengan la protección adecuada, es necesario alinear la legislación con la tecnología forense y con el trabajo de los policías.

2.2.8 Grooming

El grooming es un delito especialmente grave que implica que un adulto se contacte con menores de edad por medios digitales con el fin de ganarse su confianza para cometer abusos sexuales. La vulnerabilidad de los menores en el entorno digital y la facilidad para ocultar estas conductas hacen que este delito requiera un tratamiento legal específico. Las normativas deben incluir medidas preventivas, sanciones penales claras y protocolos para la protección de los menores y la persecución efectiva de los agresores.

Del mismo modo, el análisis de casos de grooming exige procedimientos especializados y personal calificado para abordar a las víctimas y reunir pruebas digitales fidedignas. Para que los colegios y las familias sean capaces de detectar y denunciar comportamientos así a tiempo, es vital que las políticas públicas incorporen protocolos de actuación y campañas educativas. La correcta tipificación y penalización del grooming es una evidencia de la dedicación del Estado a la protección completa de los derechos de los niños.

2.2.9 Ciberacoso

El ciberacoso, también conocido como "cyberbullying", es el proceso de hostigar, acosar o avergonzar a alguien con la ayuda de tecnologías digitales, por lo general de

forma reiterada. Este fenómeno ha cobrado mucha importancia por el efecto psicológico que puede tener sobre las víctimas. Desde el punto de vista del Derecho, es preciso identificar este tipo de comportamientos como delitos o infracciones que requieren ser castigadas y promover campañas pedagógicas que concienticen sobre su prevención.

El ciberacoso, por su parte, supone retos específicos para el sistema judicial a causa de la velocidad con que se propagan los contenidos y de lo complicado que resulta identificar a los culpables. Por esta razón, es necesario que el marco normativo contenga cláusulas que hagan más fácil la adquisición de pruebas digitales y medidas cautelares para salvaguardar a las víctimas de forma inmediata. Para disminuir este tipo de comportamientos, es necesario educar sobre el uso responsable de la tecnología y sensibilizar a la sociedad.

2.2.10 Evidencia digital

La evidencia digital comprende cualquier dato almacenado o transmitido por medios electrónicos que puede ser utilizado como prueba en procesos judiciales. Esto incluye correos electrónicos, registros de navegación, mensajes en redes sociales, entre otros. La correcta obtención, preservación y análisis de esta evidencia es crucial para el éxito en la investigación de delitos cibernéticos. El marco legal debe establecer procedimientos claros que aseguren la integridad y validez de esta información en sede judicial.

Asimismo, la gestión de evidencia digital se enfrenta a diversos desafíos legales, entre los que se incluyen el acceso no autorizado, la manipulación y la cadena de custodia durante las investigaciones. En consecuencia, el marco jurídico debe incluir reglas precisas que regulen estos temas y posibiliten que jueces y fiscales tengan los recursos requeridos para evaluar de manera apropiada este tipo de pruebas. Es fundamental que los operadores de justicia reciban formación constante en temas tecnológicos para utilizar adecuadamente la evidencia digital.

2.2.11 Hacking

El hacking se define como el acceso no autorizado a sistemas informáticos con fines ilegales o malintencionados. Esta conducta puede derivar en la obtención de información confidencial, alteración o destrucción de datos y afectación de servicios digitales. Desde el punto de vista jurídico, el hacking debe estar claramente tipificado y sancionado, considerando las diversas modalidades en que puede manifestarse y su impacto sobre la seguridad de los sistemas y los derechos de las personas.

No obstante, el hacking puede tener distintas modalidades y motivaciones; por lo tanto, la ley debe ser lo suficientemente adaptable para incluir variantes como el hacktivismo, el espionaje cibernético o el sabotaje. Para robustecer la seguridad informática y evitar estos ataques, es fundamental también promover la colaboración entre entidades del sector privado y público. Es fundamental clasificar correctamente el hacking para proteger los sistemas digitales y mantener la confianza en el ambiente tecnológico.

2.2.12 Ingeniería social

La ingeniería social consiste en técnicas utilizadas para manipular a personas con el objetivo de obtener información confidencial, acceso a sistemas o realizar fraudes, mediante engaños o suplantación. A diferencia del hacking tradicional, este delito explota la vulnerabilidad humana más que las fallas técnicas. Es fundamental que la legislación contemple esta modalidad delictiva y que las investigaciones incluyan la identificación de los métodos utilizados para su comisión.

En otra dirección, la ingeniería social supone un desafío particular para la educación y la prevención ya que el eslabón más frágil en la cadena de seguridad es la vulnerabilidad humana. Por lo tanto, además de las sanciones legales, se deben poner en marcha programas de sensibilización orientados a los usuarios, los empleados y los funcionarios con el fin de reducir los riesgos relacionados. Es necesario combinar acciones técnicas y humanas para combatir de manera efectiva este tipo de crímenes.

2.2.13 Protección de datos personales

La protección de datos personales es un derecho fundamental que garantiza que la información privada de los individuos no sea recolectada, almacenada o utilizada sin su consentimiento. La Constitución ecuatoriana reconoce este derecho, y la Ley Orgánica de Protección de Datos Personales establece las obligaciones para quienes manejan datos, así como los mecanismos para que los ciudadanos puedan exigir su respeto. Esta protección se vuelve fundamental para evitar abusos que puedan resultar en crímenes o violaciones graves en el ámbito de la ciberdelincuencia.

Esta regulación, asimismo, establece principios de seguridad, consentimiento informado y transparencia para las entidades que gestionan datos, entre las que se encuentran organismos públicos, empresas e instituciones. Si se quebrantan estos principios, las consecuencias pueden ser civiles, administrativas y penales. En el marco de los delitos cibernéticos, la protección de datos personales constituye una línea fundamental para prevenir abusos y fortalecer la confianza en las tecnologías digitales.

2.2.14 Delitos informáticos transnacionales

Los delitos informáticos transnacionales son acciones ilegales que ocurren en el ciberespacio y cruzan las fronteras nacionales, lo cual hace más complicado su persecución e investigación. La naturaleza global de la red hace posible que los criminales operen desde cualquier parte, perjudicando a víctimas en diversos países. Por lo tanto, es necesario tener acuerdos multilaterales y bilaterales de cooperación internacional que faciliten la colaboración entre las autoridades policiales y judiciales con el fin de combatir estos crímenes de manera efectiva.

Por eso, es fundamental que los países colaboren en acuerdos internacionales, como el de Budapest sobre ciberdelincuencia, para poder coordinar investigaciones, compartir información y llevar a cabo procedimientos judiciales eficaces. Sin una adecuada colaboración, los delincuentes cibernéticos logran esquivar la justicia al explotar los vacíos legales y la ausencia de armonización. Por lo tanto, el robustecimiento de los acuerdos multilaterales y de la legislación nacional son elementos fundamentales en la batalla contra este tipo de crimen.

2.3 Base teórica

2.3.1 Teorías Criminológicas que se aplican a la Ciberdelincuencia:

2.3.1.1 La teoría del Control Social. La teoría del control social, desarrollada por Travis Hirschi, plantea que los lazos que una persona mantiene con instituciones tradicionales como la familia, la educación y el ámbito laboral desempeñan un papel fundamental en la prevención del comportamiento delictivo. Aplicada al contexto de la ciberdelincuencia, esta teoría cobra especial importancia, ya que el entorno virtual puede erosionar o romper dichos vínculos, lo que facilita la participación en actividades delictivas en línea (Aperador)

Los controles sociales tradicionales tienden a ser menos eficaces en el ciberespacio. Por ejemplo, según la teoría del control social, el anonimato y la deslocalización que posibilita internet reducen el impacto de la vigilancia social y la sanción moral, componentes esenciales para prevenir el delito. De este modo, los ciberdelincuentes, en particular los más jóvenes, tienden a tener lazos débiles o nulos con las normas y valores tradicionales, lo cual disminuye la efectividad de los mecanismos de control social y propicia que surjan acciones delictivas en línea.

2.3.1.2 La teoría del Aprendizaje Social. La teoría del aprendizaje social, desarrollada principalmente por Albert Bandura, sostiene que las personas adquieren nuevos conocimientos, habilidades y comportamientos observando e imitando a otros dentro de un contexto social. Según Bandura, el aprendizaje no ocurre únicamente a través de la experiencia directa o el refuerzo, sino que la observación del comportamiento de los demás y las consecuencias que estos reciben desempeñan un papel central en la formación de la conducta (Delgado)

Según Bandura, para que el aprendizaje social sea efectivo, se deben cumplir cuatro procesos fundamentales: atención, retención, reproducción y motivación. Primero, la persona debe prestar atención al comportamiento que observa; luego, debe ser capaz de recordar esa información (retención). Posteriormente, necesita la habilidad para

reproducir la conducta observada y, finalmente, debe estar motivada para hacerlo, generalmente porque percibe una recompensa o quiere evitar un castigo (De la Torre)

Esta teoría subraya lo fundamental que es el ambiente social para el aprendizaje, pues las personas no únicamente aprenden a través de prueba y error, sino también observando cómo se comportan los demás y cuáles son las consecuencias de sus acciones. Por ejemplo, si un alumno ve que otro ha sido castigado por copiar en una prueba, es posible que aprenda a no hacer lo mismo sin tener que vivirlo directamente.

Bandura incorporó en su modelo factores de naturaleza cognitiva y conductual, al aceptar que el aprendizaje supone una constante interacción entre el comportamiento, los procesos mentales y el contexto social. Esto significa que no basta con observar para aprender; también es necesario procesar, recordar y decidir si reproducir o no la conducta observada

2.3.1.3 Argumentos Relacionados. La teoría del aprendizaje social, desarrollada principalmente por Albert Bandura, sostiene que las personas adquieren nuevos conocimientos, habilidades y comportamientos observando e imitando a otros dentro de un contexto social. Según Bandura, el aprendizaje no ocurre únicamente a través de la experiencia directa o el refuerzo, sino que la observación del comportamiento de los demás y las consecuencias que estos reciben desempeñan un papel central en la formación de la conducta

Por un lado, la teoría del control social argumenta que, si se carece o no hay fuerza en los vínculos sociales, como el apego a la familia, el trabajo o la escuela, es más fácil desviarse y cometer delitos, entre ellos el cibercrimen. Cuando estos lazos son débiles, los mecanismos de autocontrol y las sanciones sociales se vuelven ineficaces, lo que aumenta la posibilidad de que un individuo cometa actos delictivos en línea. En los ciberdelincuentes, sobre todo en los más jóvenes, se nota que estos vínculos son a menudo débiles o inexistentes. Esto les posibilita actuar sin percibir las limitaciones sociales que normalmente impiden el delito en el mundo offline (Aperador)

Por otro lado, la teoría del aprendizaje social resalta que se aprende a actuar delictivamente observando, imitando y relacionándose con otros, particularmente en comunidades virtuales. Los criminales pueden aprender y mejorar sus habilidades delictivas en el ciberespacio al ver tutoriales, involucrarse en foros de hacking y colaborar con otros ciberdelincuentes más expertos. Además, estas comunidades no solo difunden saberes técnicos, sino que además fortalecen principios y normas que legitiman y normalizan la conducta delictiva, lo cual hace más sencillo que el cibercrimen se mantenga y crezca (LawBirdie)

Ambas teorías coinciden en que el entorno social, ya sea por la falta de control o por la presencia de modelos delictivos, juega un papel decisivo en la génesis y mantenimiento de la ciberdelincuencia. La interacción entre la debilidad de los controles sociales y la facilidad para aprender conductas desviadas en línea crea un contexto especialmente propicio para la proliferación de delitos informáticos. Por ello, los enfoques preventivos y de intervención deben considerar tanto el fortalecimiento de los lazos sociales y las instituciones de control, como la reducción de la exposición a modelos delictivos y la promoción de contra modelos positivos dentro de las comunidades digitales (Cámara Arroyo)

2.4 Marco Legal:

Este proyecto describe la fundamentación y regulaciones legales de Ecuador, esenciales para luchar contra la ejecución de delitos en el ámbito digital. A continuación, señalamos algunos artículos de legislación nacional relevantes que respaldará esta investigación.

2.4.1 Constitución de la República del Ecuador

La Constitución de 2008 es la norma suprema del país y garantiza explícitamente derechos esenciales en el contexto digital, los cuales son fundamentales para el tratamiento de los delitos cibernéticos. En su artículo 1, establece que el Ecuador es un “Estado constitucional de derechos y justicia”, lo que implica la protección y vigencia de los derechos en todas las esferas, incluida la digital. Además, reconoce los derechos de

libertad, entre ellos el derecho a la protección de datos personales, el secreto de las comunicaciones y la inviolabilidad de la intimidad, lo cual conforma el eje constitucional sobre el que se sustenta la investigación de los ciberdelitos (Constitución de la República del Ecuador, 2008)

Además, el artículo 66, número 21, asegura la inviolabilidad del secreto de las comunicaciones físicas y virtuales. Esto significa que no pueden ser interceptadas sin una orden judicial previa y con la protección de secreto correspondiente.

El Artículo 92, que regula el Habeas Data, establece por su parte que cualquier individuo tiene derecho a saber, entrar, corregir, suprimir o eliminar sus datos de registros públicos o privados sin ningún costo y en formatos tanto físicos como electrónicos. Esta garantía jurídica refuerza el derecho de los ciudadanos a controlar su información personal y proporcionar mecanismos para la defensa ante vulneraciones digitales.

2.4.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002)

La Ley No. 2002-67, conocida como Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, representa la primera normativa ecuatoriana que reconoce las transacciones digitales como válidas legalmente y establece sanciones para las infracciones informáticas. Su capítulo de infracciones tipifica actos como el acceso no autorizado a sistemas, la falsificación electrónica y el fraude informático, imponiendo penas que van desde la prisión de seis meses hasta cinco años y multas de hasta 10 000 USD, según la gravedad del delito (OEA, 2002)

Esta ley sanciona con prisión de seis meses a un año y multas entre 500 y 1 000 USD a quienes “violentaren claves o sistemas de seguridad” para acceder a información protegida, y endurece las penas hasta tres años de prisión si comprometen secretos nacionales o comerciales

2.4.3 Código Orgánico Integral Penal (COIP, 2014)

El COIP, vigente desde febrero de 2014, incluye un capítulo específico en su Título III dedicado a los delitos contra la seguridad de los sistemas de información. El Artículo

229 sanciona con 1–3 años de prisión la revelación ilegal de bases de datos; mientras que el Artículo 230 penaliza con 3–5 años la interceptación ilegal de datos sin orden judicial, incluyendo la creación de malware o dispositivos para acceder a información privilegiada (COIP, 2014)

Además, el Artículo 231 tipifica la “transferencia electrónica de activo patrimonial” es decir, la apropiación no consentida de valores mediante medios digitales imponiendo penas similares de tres a cinco años de prisión (COIP, 2014)

El artículo 178 del Código Orgánico Integral Penal (COIP) de Ecuador tipifica el delito de violación a la intimidad, estableciendo sanciones para quienes, sin consentimiento o autorización legal, accedan, intercepten, retengan, graben, reproduzcan, difundan o publiquen datos personales, mensajes de datos, voz, audio, vídeo, objetos postales, información contenida en soportes informáticos o comunicaciones privadas de otra persona por cualquier medio. La pena prevista para esta conducta es privativa de libertad de uno a tres años.

Este artículo protege la privacidad de las personas y el ámbito privado frente a la violación mediante dispositivos tecnológicos, afirmando que la privacidad es un derecho fundamental que se enfrenta a desafíos importantes en el contexto del avance tecnológico y la digitalización. No obstante, la normativa no se aplica a los que difundan grabaciones en las que participen personalmente o cuando sea información pública según la ley.

El delito de apropiación fraudulenta por medios electrónicos está tipificado en el artículo 190 del Código Orgánico Integral Penal. Esta disposición establece que se incurre en este delito cuando se emplea de manera fraudulenta un sistema informático, redes electrónicas o de telecomunicaciones con el fin de favorecer la apropiación indebida de un bien ajeno o para obtener la transferencia no autorizada de bienes, valores o derechos en detrimento de una persona o de un tercero. Esto implica cambiar, manipular o modificar el desempeño de redes electrónicas, sistemas informáticos, equipos terminales de telecomunicaciones y programas telemáticos.

Esta conducta tiene como sanción una pena privativa de libertad que va de uno a tres años. Asimismo, el artículo determina que la misma pena se aplicará si la infracción se lleva a cabo a través de la inutilización de sistemas de alarma o guardia, el descubrimiento o desentrañamiento de claves secretas o encriptadas, el uso inadecuado de tarjetas magnéticas o perforadas, controles o dispositivos para abrir a distancia, o la violación de seguridades electrónicas, informáticas u otras análogas.

La persona que reprograme o altere la información de identificación de los dispositivos terminales móviles es castigada con pena privativa de libertad de uno a tres años, según el artículo 191 del Código Orgánico Integral Penal. Esta medida tiene como objetivo evitar y sancionar comportamientos vinculados con la manipulación ilegal de datos que identifican los dispositivos móviles, por ejemplo, los teléfonos celulares, conducta que puede favorecer acciones ilegales como la reactivación de equipos que han sido reportados como robados o perdidos.

El Código Orgánico Integral Penal establece en su artículo 212 que aquel que sustituya la identidad de otra persona para obtener un beneficio, ya sea para sí mismo o para otro, a costa de una persona, será castigado con prisión privativa de libertad por un período de uno a tres años. Esta medida pretende salvaguardar a los individuos de actos fraudulentos en los que alguien finge ser otra persona para conseguir beneficios ilegítimos, lo cual compromete la integridad y la seguridad jurídica de las víctimas.

El delito de acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones se menciona en el artículo 234 del Código Orgánico Integral Penal. De acuerdo con esta ley, incurre en este delito quien acceda total o parcialmente a un sistema de telecomunicaciones, telemático o informático sin permiso, o persista en él contra la voluntad de quien tenga el derecho legítimo. También abarca comportamientos como el uso indebido del acceso conseguido, la alteración de portales web, el desvío o la redirección del tráfico de voz o datos, o la prestación de servicios que estos sistemas ofrecen a terceros sin compensar a los proveedores legítimos.

La severidad con que el legislador ecuatoriano considera la violación a la seguridad y a la integridad de los sistemas digitales se refleja en que el castigo para este

crimen es de tres a cinco años de privación de libertad. Además, si la entrada no autorizada interfiere de manera seria o prolongada con sistemas que garantizan funciones sociales esenciales, como la seguridad, la salud, el bienestar económico, las cadenas de suministro o los servicios públicos, se prevé un incremento del castigo en un tercio.

Antecedentes:

A partir de los años 60, la sociedad comenzó un proceso de transformación impulsado por los avances en los medios de comunicación, los cuales no solo facilitaron la interacción entre las personas, sino que también ampliaron el alcance de las relaciones comerciales. Con el paso del tiempo, la aparición de la computadora y el desarrollo del procesamiento masivo de datos a través del internet marcaron un antes y un después. No obstante, estos avances también generaron nuevas oportunidades para que se cometan actos ilícitos en el entorno digital (Breve Aproximación a La Ciberdelincuencia Desde Una Perspectiva Criminológica, 2021).

El internet desempeñó un papel clave en este proceso, ya que permitió no solo organizar sistemas de información complejos, sino también mantenerlos actualizados constantemente. Gracias a ello, las personas podían acceder a datos tanto del pasado como del presente con gran facilidad. Esto impulsó la creación de comunidades virtuales, lo cual derivó en el uso del prefijo “cyber” para referirse a todo lo relacionado con datos, sistemas y entornos tecnológicos (Breve Aproximación a La Ciberdelincuencia Desde Una Perspectiva Criminológica, 2021).

Durante la pandemia por la COVID-19, en Ecuador se evidenció un aumento considerable en el uso del internet por parte de los ciudadanos, lo que trajo consigo un crecimiento del comercio electrónico. Sin embargo, esta situación también fue aprovechada por ciberdelincuentes que suplantaron identidades digitales para aparentar legalidad y obtener ganancias económicas de forma fraudulenta, afectando negativamente la confianza de los usuarios en las plataformas digitales (MQR Investigar, 2024).

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Enfoque de la investigación

La presente investigación adopta un enfoque mixto, que combina métodos cualitativos y cuantitativos para abordar de manera integral el tratamiento legal de los delitos cibernéticos en Ecuador. Este enfoque no solo nos sirve para analizar en profundidad los aspectos normativos, doctrinales y jurisprudenciales mediante técnicas cualitativas como el análisis documental y entrevistas a expertos, sino también para obtener datos cuantificables a través de encuestas dirigidas a funcionarios y ciudadanos, lo que aporta una visión más completa y objetiva del fenómeno estudiado.

El enfoque mixto resulta muy útil en las ciencias jurídicas y sociales porque, por un lado, permite entender a profundidad y en contexto los fenómenos a través de métodos cualitativos, y por otro, aporta datos concretos y medibles gracias a los métodos cuantitativos, lo que ayuda a obtener resultados más completos y aplicables. Según (Mendizábal Anticona,. Et al, 2023), la investigación mixta en derecho facilita la validación cruzada de resultados y la comprensión holística de fenómenos complejos, como la ciberdelincuencia, que involucra tanto dimensiones legales como sociales y tecnológicas.

3.2 Alcance de la investigación

El presente estudio se enmarca en un alcance descriptivo, dado que su objetivo principal es caracterizar y detallar el tratamiento legal de los delitos cibernéticos en Ecuador tal como se presenta.

La investigación descriptiva ayuda a compilar y sistematizar datos que provienen de fuentes doctrinales, empíricas y legales, lo cual favorece la construcción de un marco robusto para futuros análisis o mejoras. En el campo del derecho, este alcance contribuye a aclarar la situación actual de las leyes y su eficacia, lo que hace más fácil detectar vacíos o áreas que necesitan actualización debido al rápido cambio tecnológico.

3.3 Técnica e instrumentos para obtener los datos

Para el desarrollo de esta investigación se emplearán dos técnicas principales de recolección de datos: la encuesta y la entrevista, que permitirán obtener información tanto cuantitativa como cualitativa, acorde con el enfoque mixto adoptado.

La encuesta se utilizará como técnica cuantitativa para recopilar datos estructurados y estandarizados de un grupo representativo de operadores de justicia, funcionarios públicos y ciudadanos relacionados con la temática de los delitos cibernéticos. Este instrumento permitirá medir percepciones, conocimientos y experiencias sobre la aplicación del marco legal, facilitando el análisis estadístico y la identificación de tendencias generales. El cuestionario, diseñado con preguntas cerradas será el instrumento principal para esta técnica.

3.3.1 Entrevista

La entrevista es una técnica cualitativa de recolección de información que permite obtener datos profundos y detallados a partir de la interacción directa con expertos o actores clave. En esta investigación, la entrevista se utiliza para explorar percepciones, experiencias y opiniones sobre el tratamiento legal de los delitos cibernéticos Anexo N1

3.3.2 Encuesta

La encuesta es una técnica cuantitativa de recolección de datos que permite obtener información estructurada y estadísticamente representativa de un grupo determinado. En esta investigación, la encuesta se utiliza para conocer la percepción, conocimientos y experiencias de los usuarios sobre los delitos cibernéticos y el marco legal vigente en Ecuador, facilitando el análisis generalizado y la identificación de tendencias en la población estudiada Anexo N2

3.4 Población y muestra

3.4.1 Entrevista

Para esta investigación se optó por realizar una entrevista a dos personas debido a la disponibilidad limitada de profesionales relacionados con el área legal y el

tratamiento de delitos cibernéticos. Las personas entrevistadas cuentan con experiencia y conocimiento en el ámbito legal que resultan valiosos para aportar una perspectiva fundamentada sobre el tema.

Esta entrevista complementará la información obtenida a través de las encuestas, enriqueciendo el análisis cualitativo y aportando elementos relevantes para comprender mejor la problemática estudiada.

3.4.2 Encuesta

La población objetivo de esta investigación está compuesta por personas adultas residentes en Ecuador que utilizan medios electrónicos para realizar actividades cotidianas, como transacciones bancarias, compras en línea y uso de redes sociales. Este grupo es especialmente relevante porque representa a los usuarios más expuestos a los delitos cibernéticos, como estafas electrónicas, suplantación de identidad y apropiación fraudulenta, que son los ilícitos informáticos con mayor incidencia en el país.

Según datos oficiales, aproximadamente el 79% de la población ecuatoriana tiene acceso a internet y alrededor de 15,8 millones de personas usan redes sociales, lo que amplía considerablemente el universo de usuarios vulnerables a la ciberdelincuencia (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022)

Para determinar el tamaño de la muestra necesaria para la aplicación de encuestas, se consideró un nivel de confianza del 95% y un margen de error del 10%, parámetros que servirán para obtener resultados confiables y útiles, dada la naturaleza y alcance de esta investigación.

El cálculo del tamaño de muestra se realizó utilizando la siguiente fórmula de estimación:

$$n = \frac{Z^2.p.q}{e^2}$$

Donde:

Z = 1.96 (Valor correspondiente al 95% de nivel de confianza)

p = 0.5 (Proporción esperada)

q = 0.5 (1 – p)

e = 10% (Margen de error aceptable)

Cálculo:

$$n = \frac{1.96^2 \times 0.5 \times 0.5}{10\%^2} = 96.04$$

Tamaño de la muestra n = 96

Para calcular el tamaño de la muestra se usó la fórmula básica que se aplica cuando la población es muy grande o prácticamente infinita. Esto se debe a que en este estudio la población está formada por cerca de 15,8 millones de usuarios de medios electrónicos en Ecuador, un número amplio que no es necesario hacer ajustes especiales.

La fórmula que corrige el tamaño de muestra según el tamaño real de la población se usa cuando el número total de personas es pequeño o moderado, pero en este caso, como la población es tan grande, esa corrección no afecta casi nada. Por eso se prefirió usar la fórmula básica, que es más simple y adecuada para este tipo de estudios.

3.5 Tipos de Muestra en investigación cualitativa

Para la selección de la muestra, se aplicará un muestreo probabilístico, enfocándose en usuarios activos de plataformas digitales en ciudades con alta incidencia de ciberdelitos, como Guayaquil, Quito y otras provincias con reportes significativos. Se prevé encuestar a un grupo representativo de estos usuarios para obtener datos cuantitativos sobre su experiencia, percepción y conocimiento respecto a la seguridad digital y el marco legal vigente.

CAPÍTULO IV
PROPUESTA O INFORME

4.1 Presentación y análisis de resultados

En este capítulo se presentan los resultados obtenidos a partir del desarrollo de la investigación, conforme al marco metodológico y los objetivos planteados desde el inicio del trabajo. A lo largo del proceso investigativo y mediante la recopilación de datos relevantes, ha sido posible identificar ciertas falencias, dudas e incluso molestias por parte de la ciudadanía ecuatoriana frente al tratamiento legal de los delitos cibernéticos. Esto evidencia la necesidad de revisar el marco jurídico actual y buscar mecanismos más eficaces que garanticen una mejor protección de los derechos del entorno digital.

4.1.1 *Análisis de encuestas*

A partir de este apartado, se presentan y analizan los resultados obtenidos en las encuestas aplicadas durante el proceso de investigación, con el fin de identificar la percepción de la ciudadanía.

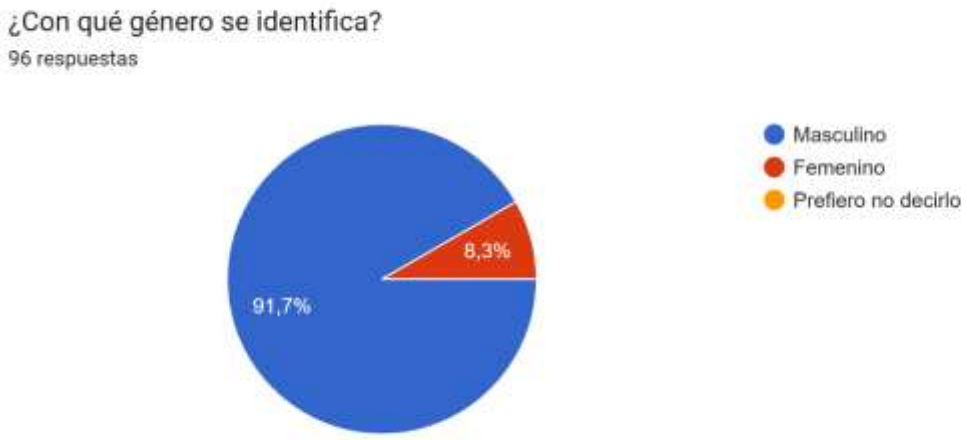
Preguntas demográficas

Tabla 1 Género

Género	Frecuencia	Porcentaje
Masculino	88	91,7%
Femenino	8	8,3%
Total	96	100,0%

Elaborado por: Bárcenas (2025)

Figura 1 Género



Elaborado por: Bárcenas (2025)

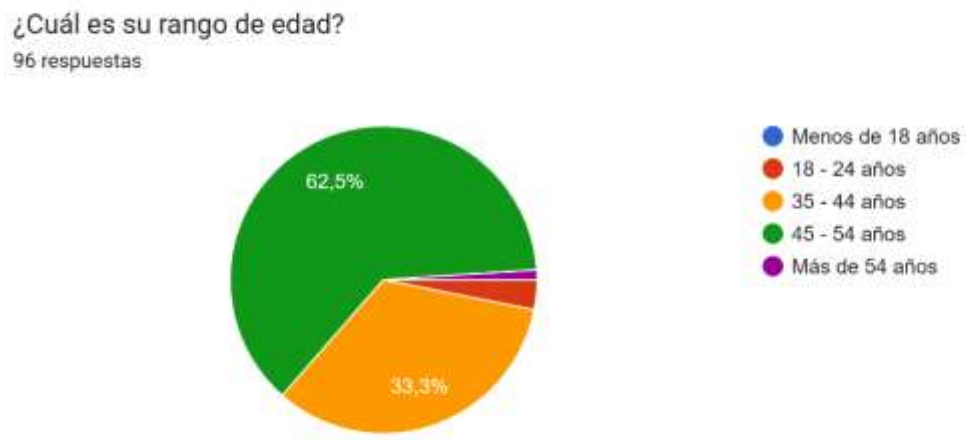
A través de esta primera pregunta se visualiza que el 92% de los encuestados responden al género masculino, mientras que el 8% corresponden al género femenino.

Tabla 2 Edad

Concepto	Frecuencia	Porcentaje
Menos de 18 años	0	0%
18 - 24 años	3	3,1%
35 - 44 años	32	33,3%
45 - 54 años	60	62,5%
Más de 54 años	1	1%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 2 Edad



Elaborado por: Bárcenas (2025)

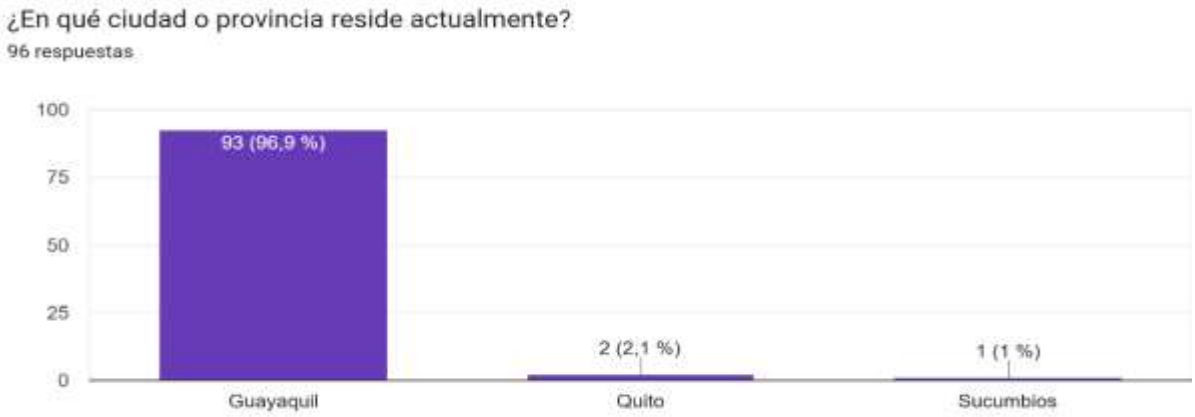
La mayoría de los encuestados tienen entre 45 y 54 años (62,5 %), seguidos por el grupo de 35 a 44 años (33,3 %). Esto indica que la percepción principal sobre los delitos cibernéticos proviene de personas adultas. Los jóvenes y adultos mayores estuvieron poco representados, y no se registraron respuestas de menores de 18 años.

Tabla 3 Ciudad de Residencia

Concepto	Frecuencia	Porcentaje
Guayaquil	93	96,9%
Quito	2	2,10%
Sucumbíos	1	1%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 3 Ciudad de Residencia



Elaborado por: Bárcenas (2025)

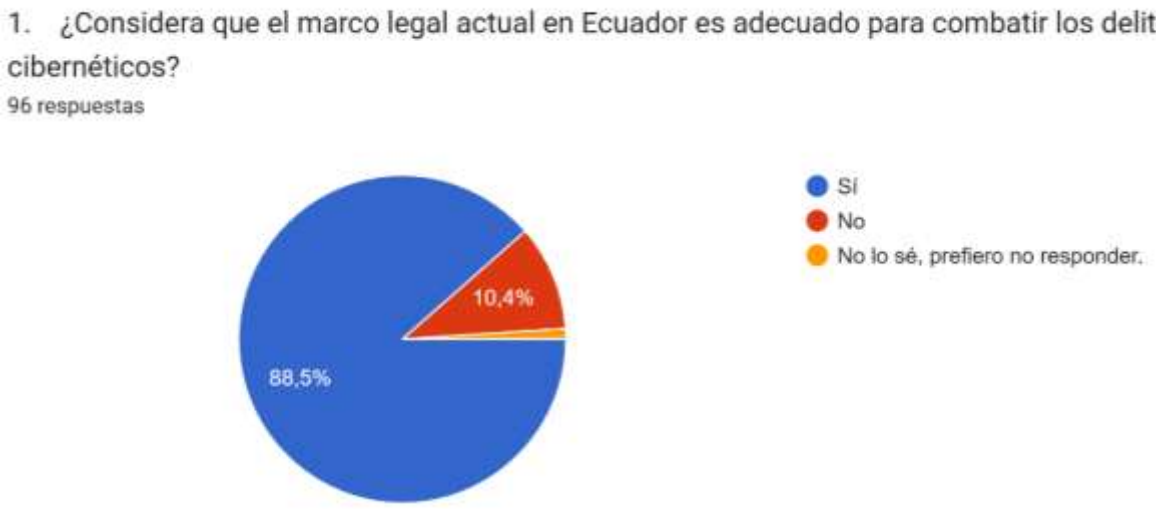
La mayoría de los encuestados reside en Guayaquil (96,9 %), mientras que solo un pequeño porcentaje corresponde a Quito (2,1 %) y Sucumbíos (1 %). Esto refleja que los resultados están centrados principalmente en la realidad de la ciudad de Guayaquil.

Tabla 4 Opinión sobre el marco legal actual

Concepto	Frecuencia	Porcentaje
Sí	85	88,5%
No	10	10,4%
No lo sé, prefiero no responder	1	1%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 4 Opinión sobre el marco legal actual



Elaborado por: Bárcenas (2025)

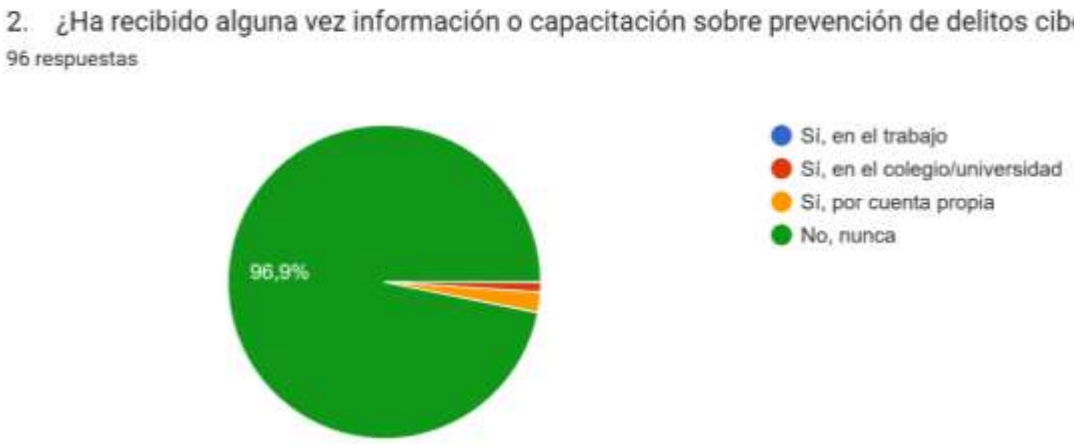
El 88,5 % de los participantes en la encuesta sostiene que el marco jurídico vigente en Ecuador es apropiado para luchar contra los delitos cibernéticos. El 1 % optó por no responder, mientras que el 10,4 % consideró que no es apropiado. Esto indica que, a pesar de que la mayor parte tiene confianza en la normativa vigente, todavía hay una minoría de personas críticas o inseguras acerca de su eficacia.

Tabla 5 Capacitación Delitos Cibernéticos

Concepto	**Frecuencia**	**Porcentaje**
Sí, en el trabajo	0	0%
Sí, en el colegio/universidad	1	1%
Sí, por cuenta propia	2	2,1%
No, nunca	93	96,9%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 5 Capacitación Delitos Cibernéticos



Elaborado por: Bárcenas (2025)

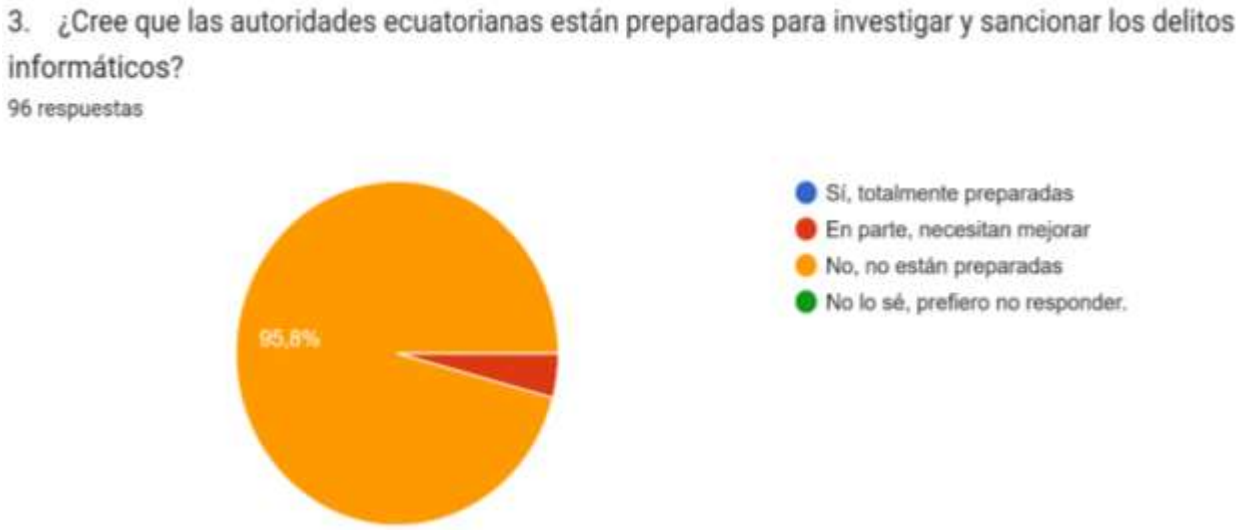
El 96,9 % de los participantes en la encuesta reportó que nunca ha sido capacitado en prevención de delitos cibernéticos. El 1 % de ellos solamente obtuvo información en la escuela o en la universidad, mientras que el 2.1 % se ha informado por sí mismo. Este hallazgo revela de manera evidente una falta de educación en la ciudadanía en relación con estos delitos, lo cual es un riesgo considerable en el entorno digital.

Tabla 6 - Percepción sobre la preparación de autoridades

Concepto	**Frecuencia**	**Porcentaje**
Sí, totalmente preparadas	0	0%
En parte, necesitan mejorar	4	4%
No, no están preparadas	92	95,8%
No lo sé, prefiero no responder	0	0%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 6 Percepción sobre la preparación de autoridades



Elaborado por: Bárcenas (2025)

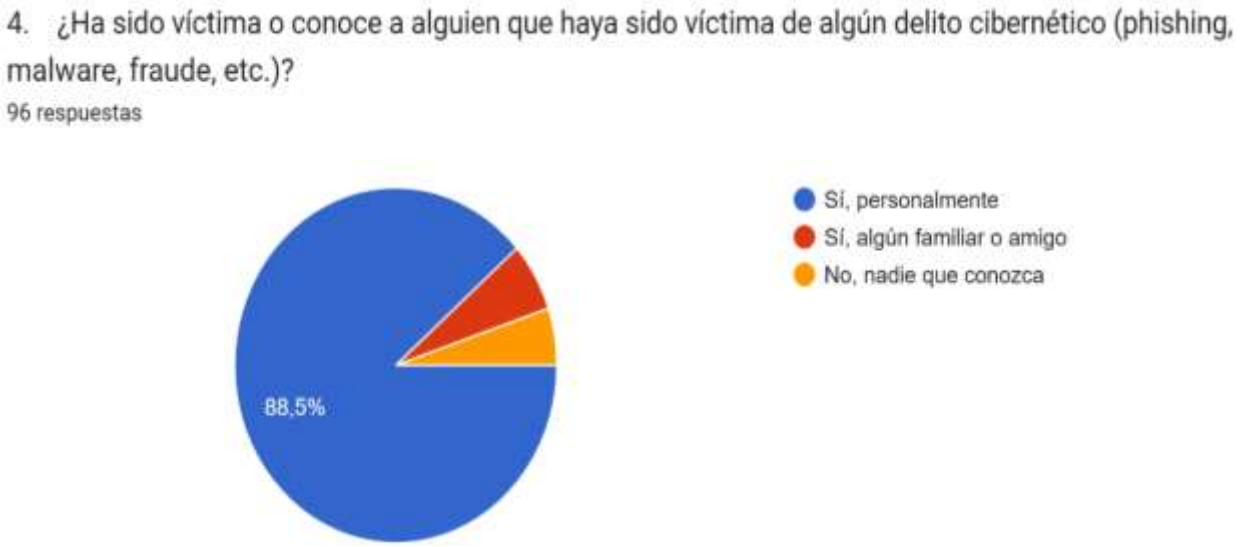
El 95,8 % de los encuestados cree que las autoridades de Ecuador no están capacitadas para investigar y castigar los crímenes informáticos. Un 4 % considera que están preparadas parcialmente, pero ninguno de los encuestados piensa que estén completamente capacitadas. Este resultado indica que los ciudadanos tienen una gran desconfianza en la capacidad de las instituciones para combatir el cibercrimen.

Tabla 7 Víctima de delitos cibernéticos

Concepto	**Frecuencia**	**Porcentaje**
Sí, personalmente	85	88,5%
Sí, algún familiar o amigo	6	6,3%
No, nadie que conozca	5	5%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 7 Víctima de delitos cibernéticos



Elaborado por: Bárcenas (2025)

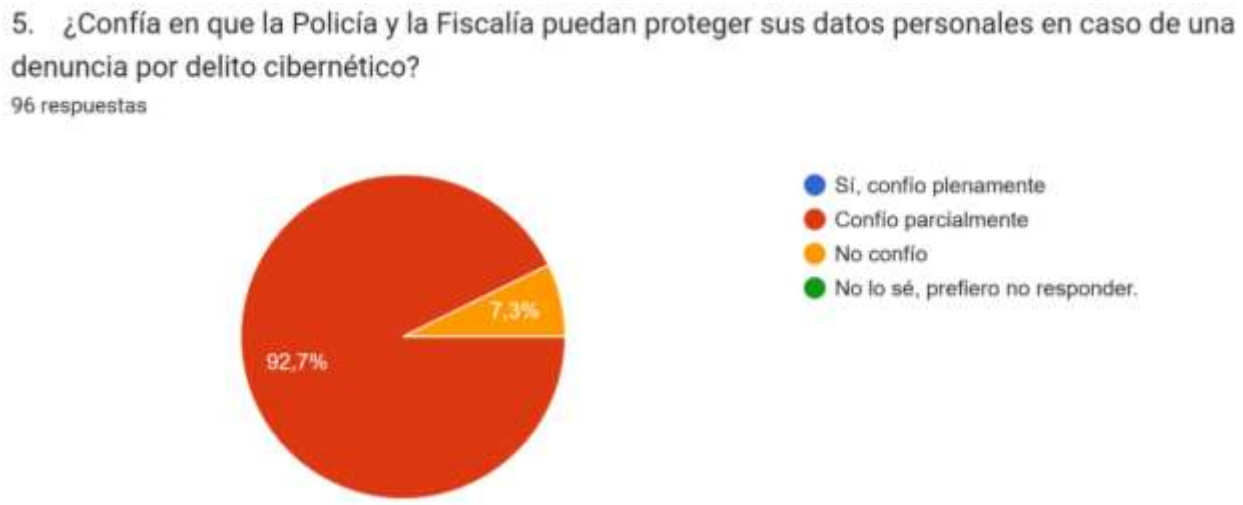
El 88,5% de los participantes en la encuesta afirmó que ha sufrido directamente algún crimen cibernético. Asimismo, el 6,3 % declaró que un amigo o familiar próximo se vio afectado. El 5 % de los encuestados afirmó no conocer a ninguna víctima. Estos datos muestran la elevada frecuencia de este tipo de delitos en la población, lo que subraya la importancia de optimizar la prevención y el abordaje legal en estas situaciones.

Tabla 8 Confianza en la protección de datos personales

Concepto	**Frecuencia**	**Porcentaje**
Sí, confío plenamente	0	0%
Confío parcialmente	89	92,7%
No confío	7	7,3%
No lo sé, prefiero no responder	0	0%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 8 Confianza en la protección de datos personales



Elaborado por: Bárcenas (2025)

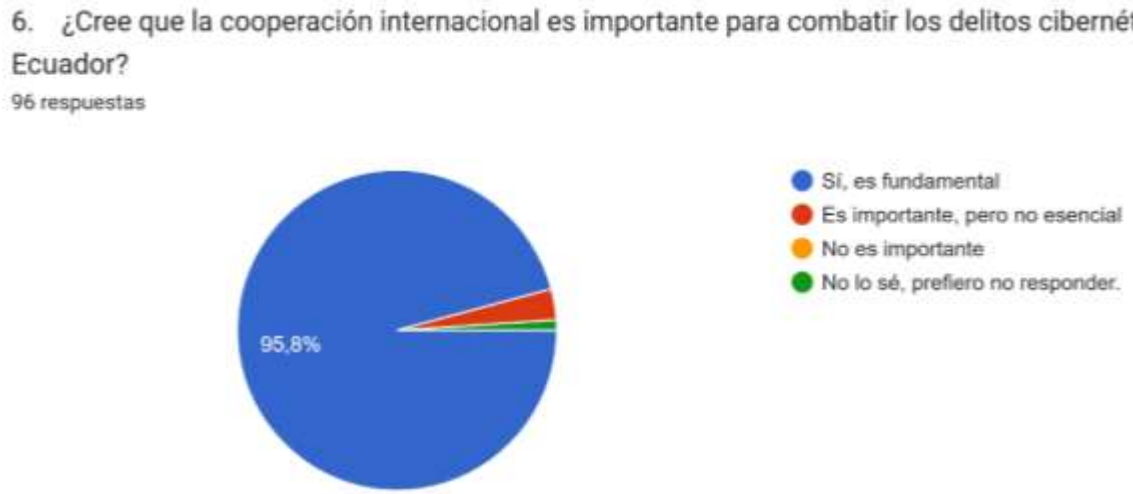
El 92,7 % de los encuestados manifestó que tiene confianza parcial en que sus datos personales se resguardarán si denuncian un delito cibernético. El 7,3 % de los encuestados expresó desconfianza, y nadie reveló confianza total. Este hallazgo indica que se percibe inseguridad sobre el manejo de información personal por las autoridades, lo que podría afectar la voluntad de denunciar este tipo de crímenes.

Tabla 9 Opinión sobre la cooperación internacional

Concepto	**Frecuencia**	**Porcentaje**
Sí, es fundamental	92	95,8%
Es importante, pero no esencial	3	3,1%
No es importante	0	0%
No lo sé, prefiero no responder	1	1%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 9 Opinión sobre la cooperación internacional



Elaborado por: Bárcenas (2025)

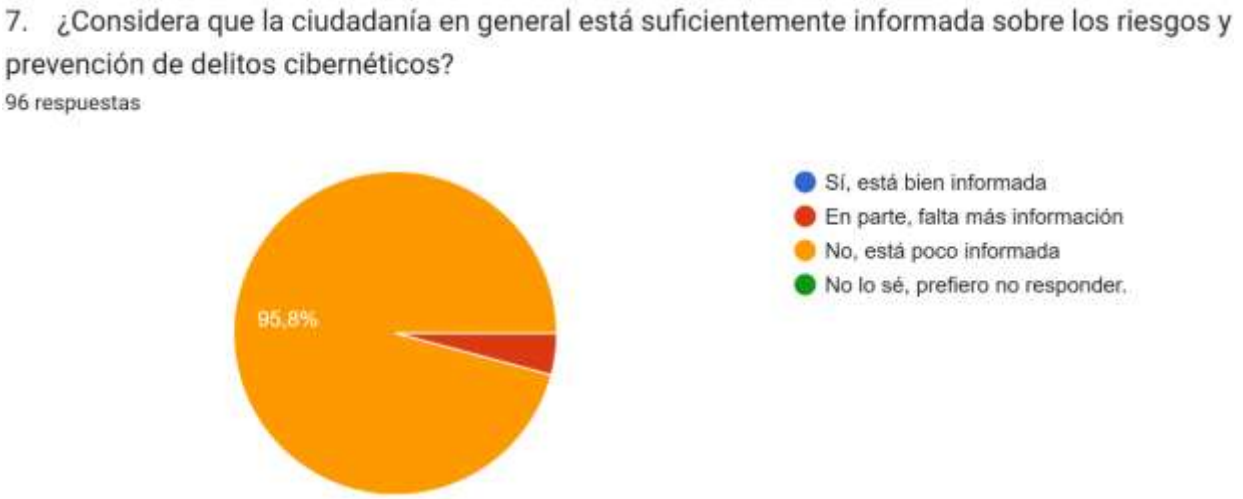
En Ecuador, el 95,8 % de los encuestados sostiene que es esencial la colaboración internacional para luchar contra la delincuencia cibernética. El 3,1 % sostiene que es importante pero no esencial, y el 1 % solo optó por no contestar. Estos resultados evidencian un amplio consenso entre los ciudadanos acerca de la importancia de colaborar con otros países para combatir la ciberdelincuencia de manera efectiva.

Tabla 10 Nivel de información ciudadana

Concepto	**Frecuencia**	**Porcentaje**
Sí, está bien informada	0	0%
En parte, falta más información	4	4,2%
No, está poco informada	92	95,8%
No lo sé, prefiero no responder	0	0%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 10 Nivel de información ciudadana



Elaborado por: Bárcenas (2025)

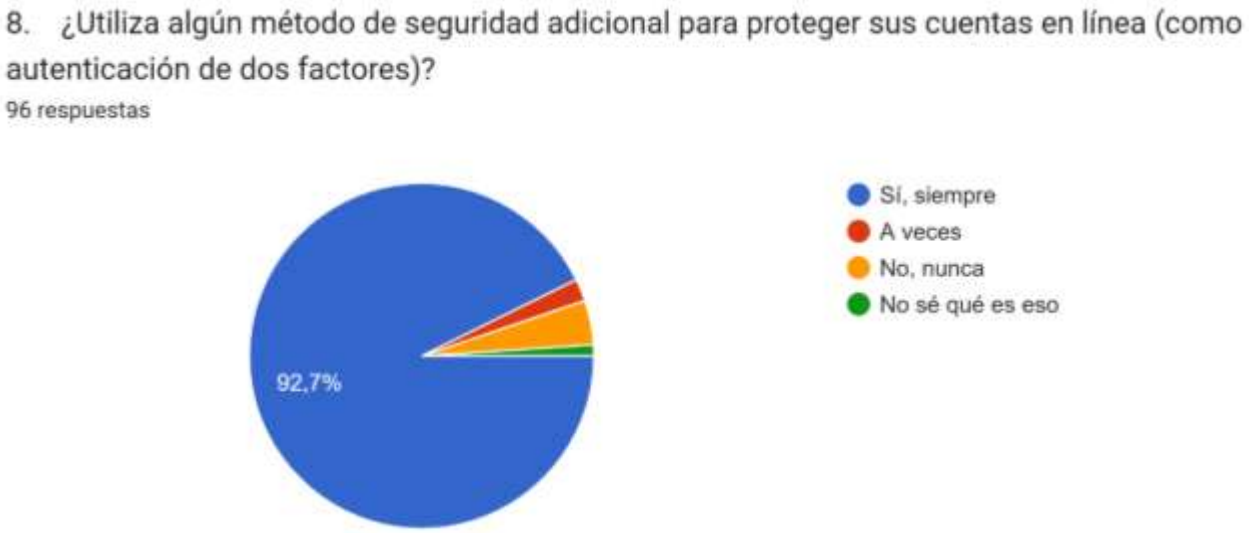
El 95,8 % de los encuestados considera que la ciudadanía está poco informada sobre los riesgos y la prevención de delitos cibernéticos. Un 4,2 % cree que hay cierta información, pero que aún es insuficiente. Nadie considera que esté bien informada, lo cual evidencia una gran necesidad de campañas educativas y mayor difusión sobre este tipo de riesgos digitales.

Tabla 11 Métodos de seguridad en línea

Concepto	**Frecuencia**	**Porcentaje**
Sí, siempre	89	93%
A veces	2	2,1%
No, nunca	4	4,2%
No sé qué es eso	1	1%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 11 Métodos de seguridad en línea



Elaborado por: Bárcenas (2025)

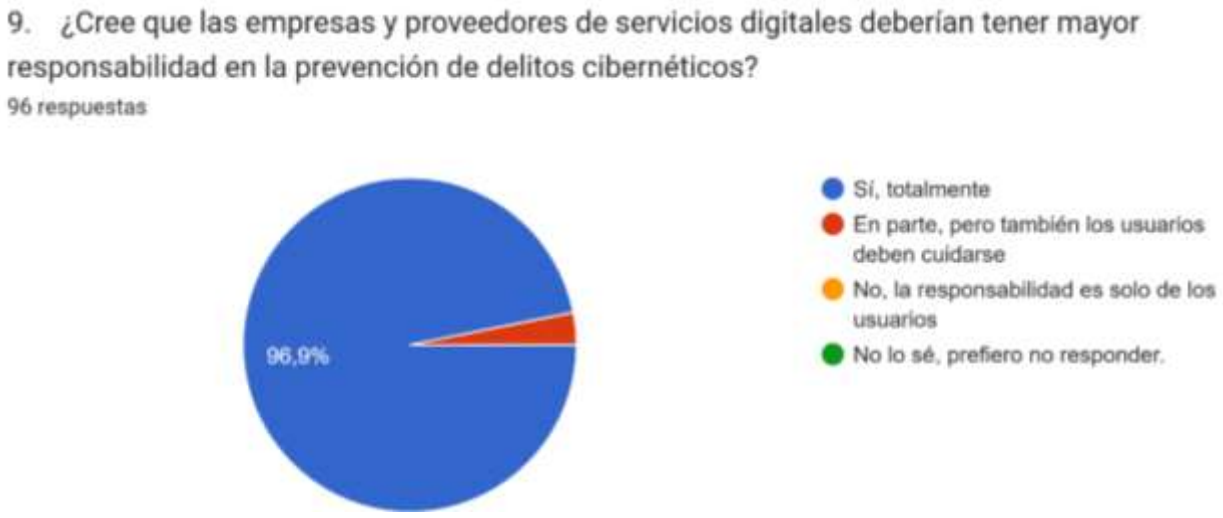
El noventa y tres por ciento de los encuestados declaró que, para salvaguardar sus cuentas en línea, emplean siempre métodos de seguridad extra, como la autenticación de dos factores. El 2,1 % lo utiliza de manera ocasional, en cambio el 4,2 % no lo emplea nunca. Además, el 1% afirmó no saber qué es esta clase de medida. Aunque todavía hay una pequeña parte de la población que necesita más orientación acerca de la seguridad digital, esto evidencia un buen comportamiento en la mayoría de los usuarios.

Tabla 12 Responsabilidad de empresas y proveedores digitales

Concepto	**Frecuencia**	**Porcentaje**
Sí, totalmente	93	96,9%
En parte, pero también los usuarios deben cuidarse	3	3,1%
No, la responsabilidad es solo de los usuarios	0	0,0%
No lo sé, prefiero no responder	0	0%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 12 Responsabilidad de empresas y proveedores digitales



Elaborado por: Bárcenas (2025)

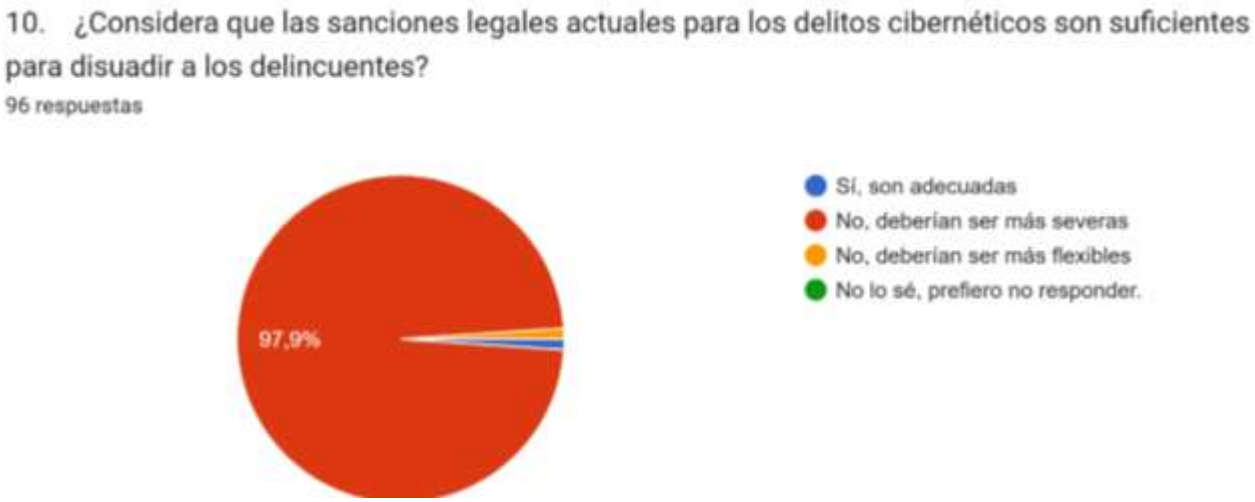
El 96,9 % de los encuestados considera que las empresas y proveedores de servicios digitales deben asumir mayor responsabilidad en la prevención de los delitos cibernéticos. Un 3,1 % cree que la responsabilidad debe ser compartida con los usuarios, mientras que nadie considera que sea responsabilidad exclusiva del usuario. Este resultado muestra una clara demanda ciudadana de mayor compromiso por parte de las plataformas digitales frente a la ciberseguridad.

Tabla 13 Opinión sobre las sanciones legales

Concepto	**Frecuencia**	**Porcentaje**
Sí, son adecuadas	1	1,0%
No, deberían ser más severas	94	97,9%
No, deberían ser más flexibles	1	1%
No lo sé, prefiero no responder	0	0%
Total	96	100%

Elaborado por: Bárcenas (2025)

Figura 13 Opinión sobre las sanciones legales



Elaborado por: Bárcenas (2025)

El 97.9 % de los encuestados cree que las sanciones legales vigentes no son suficientemente estrictas como para desalentar a los criminales cibernéticos. Solo un 1 % considera que son apropiadas y otro 1 % sostiene que deberían tener más flexibilidad. Estos datos evidencian una percepción intensa de debilidad en el sistema sancionador, lo que fortalece la necesidad de examinar y posiblemente hacer más severas las penas contempladas en el COIP para este tipo de delitos.

4.1.2 Análisis de entrevista

Para complementar la información obtenida a través de las encuestas, se realizaron dos entrevistas a profesionales con experiencia directa en el tema de delitos cibernéticos. El objetivo fue conocer sus opiniones y perspectivas desde el campo práctico y técnico, y así enriquecer el análisis de la investigación.

El primer entrevistado fue el teniente coronel Gonzalo García – jefe de la Unidad Nacional de ciberdelitos de la Policía Nacional del Ecuador. Durante la entrevista, el teniente coronel reveló información relevante acerca de las labores que lleva a cabo la unidad de ciberdelitos. Dijo que, a pesar de que luchan por combatir con eficacia este tipo de delitos, se encuentran con una serie de restricciones en sus operaciones que obstaculizan su trabajo cotidiano. La ausencia de tecnología adecuada y la necesidad de equipos más avanzados para seguir y estudiar con mayor exactitud las pruebas digitales fueron limitaciones que sobresalieron. Asimismo, hizo hincapié en que la formación continua del personal es esencial, porque los delitos cibernéticos están en constante cambio y necesitan de conocimientos específicos que no siempre son accesibles.

Además, subrayó la necesidad de que se lleven a cabo reformas jurídicas para poder reaccionar de manera más rápida y decidida ante estos comportamientos delictivos. De acuerdo con su experiencia, en numerosas ocasiones las leyes actuales no se han ajustado del todo a las nuevas circunstancias tecnológicas, lo cual provoca obstáculos y demoras en los procedimientos judiciales. Por ello, consideró que es imprescindible fortalecer tanto el marco legal como los recursos humanos y técnicos de la unidad, para garantizar que la ciudadanía reciba la protección adecuada y que los responsables de ciberdelitos sean sancionados de manera efectiva y oportuna.

La segunda entrevistada fue la Ab. Elena Ferrín – Especialista en Métodos Alternos de Solución de Conflictos, quien compartió una perspectiva jurídica profundamente reflexiva sobre cómo el sistema puede fortalecer la prevención y resolución de los delitos cibernéticos. Desde su experiencia profesional, subrayó la imperiosa necesidad de trabajar en la educación digital de las personas, no únicamente

desde el punto de vista técnico, sino también desde la preparación en derechos y obligaciones y su prevención. De acuerdo con su opinión, muchas personas ignoran los verdaderos peligros a los que se enfrentan en línea, lo cual las hace más susceptibles a potenciales amenazas. Asimismo, indicó que dentro de las instituciones públicas todavía no se ha cultivado una auténtica cultura digital, lo que restringe su capacidad para reaccionar ante estos delitos.

En cuanto al tratamiento legal, explicó que, si bien en algunos casos podrían evaluarse métodos alternativos de solución de conflictos, sobre todo en situaciones menos complejas o cuando no exista daño grave, la mayoría de delitos informáticos requieren de un abordaje penal riguroso. Para ella, estos delitos afectan derechos fundamentales como la privacidad, la seguridad y la integridad, por lo tanto, deben ser tratados con firmeza y desde una estructura legal que permita no solo sancionar, sino también prevenir con políticas claras y personal capacitado. Enfatizó que la justicia restaurativa no tiene que ser confundida con impunidad y que el mayor reto es conseguir que la legislación progrese al mismo compás que la tecnología.

El Dr. Juan Gabriel, un profesor universitario especializado en temas penales, fue el tercer entrevistado. Él proporcionó una perspectiva académica y práctica sobre cómo se abordan los delitos cibernéticos en Ecuador. Durante la entrevista, destacó que es fundamental que los profesionales del Derecho, como jueces, fiscales, colegios de abogados y agentes de la policía, se capaciten continuamente. Indicó que muchos todavía no están adecuadamente preparados para hacer frente a esta clase de criminalidad. Resaltó además que, a pesar de que la legislación ecuatoriana ha progresado en gran medida, sobre todo por la inclusión de acuerdos internacionales como el de Budapest, todavía hay deficiencias en la implementación, principalmente debido a los prolongados periodos requeridos para los procesos de cooperación internacional y a una insuficiencia de recursos. Asimismo, destacó que la inteligencia artificial, a pesar de ser un avance tecnológico, ha colaborado indirectamente en el aumento de delitos como la suplantación de identidad y la falsificación de documentos digitales. En cuanto a las medidas de prevención, señaló la necesidad urgente de

concientizar a la población y reforzar la seguridad digital en instituciones que manejan información sensible, como bancos y organismos públicos.

Ambas entrevistas coinciden en que el marco legal actual presenta ciertos vacíos y que tanto las autoridades como la ciudadanía aún no están completamente preparadas para enfrentar los retos que plantea la ciberdelincuencia. Esta información sirve de base para sustentar la propuesta presentada en este capítulo.

Entrevista 1

¿Cómo calificaría el marco legal actual en Ecuador para la prevención, investigación y sanción de los delitos cibernéticos?

Actualmente la legislación que Ecuador posee es una actualización bastante acorde a las tendencias mundiales, y esto es gracias a un proyecto trabajado con diferentes instituciones gubernamentales como fiscalía nacional, Policía Nacional, Cancillería, Ministerio de Comunicaciones. Al Ecuador le tomo alrededor de 5 años trabajando para poder adherirnos al convenio de Budapest, luego de varias reformas al COIP que se exigía como requisito para formar parte a este convenio que, en sí, es la convención contra la ciberdelincuencia a nivel mundial.

Bastante actualizada y a la par de otros países.

¿**Considera que este marco legal es suficiente o requiere reformas?**

En el tema tecnológico, nunca un marco legal va a ser suficiente por la propia modalidad de esta temática ya que el tema tecnológico va evolucionando día a día, por esa razón considero que la normativa siempre estará un paso atrás de la evolución que tenga la tecnología. Entonces por lo general en los países lo que se trata es que dependiendo de la evolución que tengan estas tendencias delictivas pues las normas tendrán que ir preparando su actualización.

¿Cuáles son las principales dificultades que enfrentan los operadores de justicia fiscales, policías y administradores de justicia para combatir los casos de ciberdelincuencia?

Entre los principales nudos críticos que tenemos están:

No hay autoridades formadas en estas actividades ilícitas, en Ecuador solo contamos con un señor fiscal especializado en ciberdelincuencia, existiendo sola una fiscalía competente para todo el país, entonces necesitamos muchas más fiscalías y así mismo más señores fiscales especializados en esta área.

Segundo también al nivel de jueces, no hay jueces especializados en ciberdelincuencia, las investigaciones de ciberdelitos son netamente técnicas, las audiencias se trata terminología técnica muy específica y muchas veces las autoridades no entienden o no saben de lo que se está hablando.

¿Qué mecanismos legales existen para la preservación y obtención de pruebas electrónicas en investigaciones de delitos cibernéticos?

La convención de Budapest es la actual norma que nos rige a nivel internacional, es la que Ecuador ya es parte junto a otros 76 Estados miembros.

Pero también el Ecuador ha sido parte de la creación de la Convención de Naciones Unidas, la cual también ha generado una lucha contra la ciberdelincuencia y el uso inadecuado de las tecnología y telecomunicaciones., donde yo personalmente fui parte de la delegación de Ecuador y participamos alrededor de dos años elaborando esta convención en New York , pues se tiene ya lista una norma creada por Naciones Unidas que se está planificando para que Ecuador en el transcurso de este año 2025 se suscriba y ser adeptos a dicha convención.

¿Cómo se maneja la cooperación internacional en casos de delitos cibernéticos que involucran a más de un país?

La cooperación internacional es vital en este tipo de delitos , para esto Ecuador a través de su unidad de ciberdelitos de la policial nacional cuenta con una sección que

se conoce como el Punto 24/7 sección perteneciente Budapest, justamente fue creada para esto , para tener un contacto directo con los 77 Estados miembros de Budapest donde a través de un correo electrónico , inclusive tan rápido con una llamada telefónica o mensajes de texto tenemos los puntos de contacto de todos estos Estados miembros donde nos es posible obtener información o requerimientos sin necesidad de hacer tanta tramitología.

¿Qué estrategias o programas de capacitación se ofrecen a los funcionarios encargados de combatir la lucha contra la ciberdelincuencia?

El Ecuador hace dos años ya cuenta con el Comité Nacional de Ciberseguridad, conformado por el Ministerio de Telecomunicaciones, Ministerio de defensa, ministerio del interior, cancillería, centro estratégico de inteligencia y la Presidencia de la Republica. Este comité es quien da las políticas para la lucha y protección para los ciudadanos en contra la ciberdelincuencia y también emitir políticas de ciberseguridad.

Constantemente estamos haciendo campañas de prevención, en las cuales les compartimos información valiosa a través de trípticos con medidas para evitar que la comunidad sea víctimas de delitos como el famoso Fishing.

¿Cuáles son las recomendaciones que daría usted para fortalecer el marco legal y operativo en Ecuador para enfrentar eficazmente la ciberdelincuencia?

Reforzar a nuestros legisladores en materia de ciberdelitos, tengan claridad en lo relacionado a la terminología usada en esta sección, de igual manera que se formen en las academias peritos como por ejemplo en informática forense.

Seguir adelante con nuestro proyecto para este año 2025 en la creación de tecnólogos de los miembros de la Policía Nacional, ya vamos a tener especialistas en investigaciones de ciberdelitos.

Las empresas públicas y privadas no tienen que considerar a la inversión de actualización de software y de equipos de seguridad como un gasto, pues la

actualización de estos son precisamente los que permiten dar una seguridad a esa información tan delicada propia de su institución.

Entrevista 2

¿Qué rol cumple la educación y la concienciación en la prevención de los delitos cibernéticos?

Aunque actualmente nos encontramos en una era digital, considero que en relación con la educación y la concientización existe bastante desconocimiento por parte de la población en relación con este tipo de delitos, es verdad que se han hecho y se están haciendo campañas para crear concientización en la gente, pero aun así no basta porque el ciberdelito a diferencia de otros delitos evoluciona más rápido, constantemente sale una tendencia nueva o modalidad de infracción a través de estos medios.

¿Considera que el marco legal de Ecuador para la prevención e investigación del ciberdelito es suficiente o requiere reformas?

Reconozco que hay un avance en la legislación ecuatoriana respecto a esta modalidad, pero aun así yo creería que debería ampliarse más y por ende darle la prioridad que requieren estos temas. Actualmente es a través de estos medios digitales donde se han registrado un aumento de infracciones.

¿Cuáles son los tipos de delitos cibernéticos más comunes en Ecuador?

Uno de los más comunes es el denominado Phishing, el cual está relacionado con mensajes que se hacen pasar por entidades bancarias y te solicitan datos personales con el fin de manipular la cuenta del usuario en este caso la víctima.

Otro caso común es el de compras no autorizadas, pues este consiste en que el usuario realiza una compra en línea y resulta que solo con el hecho de ingresar sus datos, le reflejan en el pago otros gastos adicionales que el usuario no ha autorizado.

¿Cuáles son las consecuencias legales en relación con los delitos cibernéticos?

Las penas por estos delitos podrían variar, todo va a depender según qué tan grave sea la infracción que se haya cometido, en nuestro marco legal ecuatoriano el COIP señala penas que van desde los 3 a 5 años. Al igual de la existencia de sanciones privativa de libertad, también viene consigo la respectiva multa por la infracción.

¿Cuál es el proceso que se lleva a cabo en lo que respecta a estos delitos?

Lo primero es realizar una denuncia.

Se lleve una investigación por parte de fiscalía

Se abra una investigación previa

A consideración del fiscal se formulen cargos a quien esté cometiendo la infracción

Una vez formulados los cargos, se procede con el juicio

¿Cómo se puede mejorar la legislación ecuatoriana para hacer frente a los nuevos desafíos planteados por los delitos cibernéticos?

Considero que nuestro código penal debería mantener esa constante evolución que ha demostrado respecto al ciberdelito, además sumaría mucho mantener activo en los convenios internacionales para estar a la altura de otros países.

¿Considera que ha habido un progreso notable del ciberdelito en el Ecuador?

Yo considero que en la última década las infracciones en este tipo de delitos han aumentado en un 20%, y el aumento va a seguir debido a que ahora lo que está en tendencia son las compras en línea.

Entrevista 3

¿Qué medidas considera más adecuadas a tomar para evitar ser víctima de ciberdelitos?

• Considero que la población tendría que concientizar y capacitarse sobre el tema citado, así sea de forma empírica, porque es lo que predomina actualmente.

• Sería de gran ayuda que instituciones, como por ejemplo las bancarias, ya sea a través de bancas virtuales, correos o cualquier medio que éstas utilicen para transmitir información a sus usuarios, eduquen a los mismos respecto a la ciberdelincuencia.

• También considero que estas instituciones que manejan datos e información importante de sus usuarios opten por contratar, justamente, seguridad especializada para evitar estos delitos en perjuicio de la ciudadanía.

¿De qué manera perjudican los delitos cibernéticos a las víctimas, tanto a nivel individual como a nivel empresarial?

Generalmente afectan de la misma manera en ambos casos, ya que lo que comúnmente se da son las estafas, suplantaciones de identidades; pero lo que podría diferenciarlos es que muchas veces las empresas o corporaciones tienen un mejor control, filtro y, a su vez, personas preparadas para combatir cualquier ataque de esta naturaleza, a comparación de una persona natural, dependiendo del contexto.

¿Cómo se puede mejorar la formación de los profesionales involucrados en la investigación y persecución de ciberdelitos?

La capacitación juega un papel muy importante, sobre todo en cuestión de funcionarios públicos como Fiscalía, jueces, Consejo de la Judicatura, Escuela de Fiscales.

A mi consideración, lo que es la forma de capacitación en este campo va enrutado directamente a la preparación de estas instituciones. En los casos de los abogados que están o no asociados, tienen que proveerse también estas campañas que van a mejorar

el desenvolvimiento de los mismos como profesionales, ya sea los Colegios de Abogados y gremios relacionados directamente a estas incumbencias. Tampoco debemos olvidar capacitar a nuestros agentes policiales, de los que vienen del servicio urbano, para establecer justamente la cadena de custodia respectiva.

¿Cuáles son los problemas que pueden generarse en las instituciones a la hora de combatir el ciberdelito?

Recursos, falta de capacitación y ente humano.

Indudablemente, uno de los mayores problemas son los recursos, esto en razón de que los programas que se requieren para ejercer un mejor control tecnológico, sobre todo en caso de control de magnitud a escala nacional, muchas veces no son tan accesibles económicamente hablando.

Desde mi perspectiva, hay muchas cuestiones envueltas aquí, desde infraestructura y talento humano. En cuanto a la parte jurídica, no podemos negar que sí ha habido un avance significativo; sin embargo, no muchos profesionales están capacitados en relación a este tipo de delitos.

¿Cómo de efectiva es la legislación ecuatoriana actual (COIP y otras leyes) para abordar los delitos cibernéticos?

Yo creo que muy buena actualmente, pues a través del tiempo nuestra legislación ha tenido sus actualizaciones y, a mi criterio, puedo decir que sí se ha adecuado desde el punto de vista procesal y sobre técnicas investigativas al amparo de este tipo de medidas. Además, hoy contamos con ayuda de convenios internacionales; ahí está Budapest, convenio al cual Ecuador recientemente adaptó su presupuesto, aquello para internacionalmente ayudar a combatir el ciberdelito.

¿Qué tan efectiva es la cooperación internacional en la lucha contra el ciberdelito en Ecuador?

A mi criterio, la cooperación internacional sí ayuda, pero no es tan eficaz; es muy protocolaria. Tiene que pasar directamente del ente, primero por Fiscalía, luego se envía a una unidad especializada en la ciudad de Quito, que está centralizada. Luego, esta información pasa a un canal diplomático para otro país; en el mismo sentido, aquel país manda la destitución requerida, esta puede ser de ejercicio público o privado. En conclusión, la normativa existe, pero los tiempos de espera son muy extensos.

¿Considera que la IA indirectamente ha ayudado para que este tipo de delitos aumente?

A opinión personal, por supuesto que podría aportar a la comisión de estos delitos. Creo que la tecnología ha avanzado tanto que, hoy en día, es posible sacar de contexto las opiniones que emite una persona o las intervenciones de los usuarios en plataformas digitales. Entre los delitos que podrían cometerse en este contexto estarían la suplantación de identidad, cometer algún tipo de engaño o falsedad de documentos que se puedan generar.

4.2 Propuesta (opcional)

Con base en los resultados obtenidos durante la investigación, se propone fortalecer el tratamiento legal de los delitos cibernéticos en Ecuador a través de reformas normativas, estrategias institucionales y campañas de concienciación ciudadana.

Hoy en día, a pesar de que entre los artículos 232 y 233 el COIP considera algunos delitos informáticos, estos son insuficientes ante la creciente complejidad de las amenazas digitales. La legislación de Ecuador no clasifica de manera concreta delitos como el acoso a través de medios electrónicos, el grooming digital (hostigamiento a menores de edad por medio de medios digitales), la suplantación de identidad con propósitos fraudulentos en redes sociales o la utilización de software dañino como el ransomware. Esta falta produce lagunas jurídicas que obstaculizan una respuesta penal apropiada y a tiempo.

Por esta razón, se sugiere establecer un capítulo dedicado dentro del COIP para compilar y desarrollar con más profundidad los delitos cibernéticos, incluyendo nuevas figuras delictivas que se ajusten a la realidad digital presente. Esto ya lo han hecho naciones como Colombia, México y Chile.

Se sugiere, además, promover la inclusión de Ecuador en el Convenio de Budapest acerca de ciberdelitos; esto posibilitaría la actualización del marco legal del país y el fortalecimiento de la cooperación a nivel mundial para perseguir estos crímenes.

Además, se recomienda que la Policía Nacional y la fiscalía general del Estado fortalezcan sus unidades dedicadas a los crímenes informáticos mediante una mayor inversión financiera, tecnología moderna y formación continua de su personal.

Para terminar, se propone la puesta en marcha de campañas educativas que aborden el uso responsable de la tecnología, la prevención de delitos cibernéticos y los métodos para denunciar, poniendo énfasis en colectivos vulnerables como son las mujeres que sufren violencia digital, así como los niños y adolescentes.

CONCLUSIONES

La investigación permitió evidenciar que, si bien en Ecuador existe una normativa básica sobre delitos cibernéticos dentro del COIP, esta resulta limitada frente a las nuevas formas de ciberdelincuencia que se presentan con rapidez y complejidad creciente. A través del análisis documental, encuestas y entrevistas, se comprobó que la legislación actual no abarca de manera integral todos los tipos de delitos digitales que afectan a la ciudadanía, cumpliéndose así el objetivo de evaluar el marco legal vigente y su efectividad. Esta falta de regulación causa vacíos jurídicos que obstaculizan la persecución y la penalización de nuevas formas delictivas, lo que deja a las víctimas en una situación de vulnerabilidad.

Los hallazgos muestran una situación alarmante, ya que la mayor parte de los ciudadanos ha sido víctima directa de algún delito cibernético y no confía del todo en las entidades encargadas de proteger sus datos o castigar a los culpables. Asimismo, hay una evidente escasez de formación en la población acerca de cómo prevenir estos delitos, lo que aumenta la exposición a riesgos y disminuye la eficacia de las medidas de protección. Este contexto demuestra que el sistema legal e institucional ecuatoriano aún no está preparado para afrontar de forma eficiente el crecimiento de la ciberdelincuencia, lo que demanda un esfuerzo conjunto y urgente de actualización, formación y equipamiento.

La propuesta presentada en este trabajo busca fortalecer el tratamiento legal de los delitos cibernéticos a través de reformas al COIP, la adhesión plena y efectiva al Convenio de Budapest, el fortalecimiento institucional con mayor dotación de recursos tecnológicos y humanos, y la implementación de campañas educativas dirigidas tanto a la ciudadanía como a funcionarios encargados de la justicia. Su valor se basa en que atiende directamente las necesidades identificadas en la investigación y se respalda con puntos de vista de expertos, los cuales están de acuerdo en que es urgente una intervención coordinada e integral para contrarrestar esta problemática.

La propuesta, además, presenta soluciones concretas y factibles en el contexto ecuatoriano, lo que le confiere un carácter innovador y provechoso para el progreso del sistema de justicia ante los retos del entorno digital. Es importante mejorar la infraestructura tecnológica para que los procesos de investigación y judiciales se agilicen, además de incluir capacitación especializada en ciberdelitos para jueces, fiscales y policías. Además, se destaca la importancia de reforzar la colaboración internacional para abordar la naturaleza transnacional de estos crímenes.

Para concluir, este estudio no solo alcanzó los objetivos establecidos, sino que también ayuda a hacer visibles las carencias actuales y sugiere un camino factible para que Ecuador pueda ajustarse a las demandas de un mundo en creciente digitalización. El tratamiento legal de los delitos cibernéticos requiere de un enfoque dinámico, integral y participativo que garantice la protección efectiva de los derechos de la ciudadanía y la sanción oportuna de los responsables, asegurando así un entorno digital más seguro y confiable para todos.

RECOMENDACIONES

Se recomienda realizar una reforma al Código Orgánico Integral Penal (COIP) con el fin de actualizar su contenido en materia de delitos cibernéticos. Para ofrecer una respuesta más eficaz ante las amenazas del entorno digital, esta reforma tendría que contener un capítulo específico que clasifique nuevos delitos penales, como el grooming, el ciberacoso, la suplantación de identidad en línea, el fraude digital y la utilización de software malicioso.

Igualmente, es imprescindible robustecer las habilidades de los organismos encargados de la indagación y persecución de estos crímenes, como es el caso de la Fiscalía y la Policía Nacional. Para lograrlo, es necesario invertir en tecnología especializada, formar a los técnicos y abogados, y crear unidades que se ocupen exclusivamente de la ciberdelincuencia, capaces de actuar con eficacia y celeridad.

Es importante que Ecuador se adhiera al convenio de Budapest sobre ciberdelincuencia, lo cual posibilitaría la armonización de su legislación con estándares globales y el mejoramiento de la colaboración técnica y legal con otras naciones. Esto es crucial debido a la naturaleza transnacional de estos delitos.

Se recomienda además poner en marcha campañas de educación digital orientadas a la población, con el objetivo de prevenir y reconocer riesgos, así como actuar correctamente ante incidentes cibernéticos. Estas medidas deben incorporarse en programas formales de educación y en áreas comunitarias, particularmente en zonas vulnerables.

Asimismo, es crucial instaurar normativas que exijan a las plataformas digitales y las empresas adoptar un papel más participativo en la prevención de delitos informáticos, a través de la salvaguarda eficaz de los datos personales de los usuarios, la comunicación de incidentes y el trabajo conjunto con las autoridades pertinentes.

Finalmente, se recomienda fomentar la investigación académica y jurídica sobre la evolución de los delitos cibernéticos, para que desde las universidades y centros

especializados se propongan soluciones innovadoras que permitan enfrentar con mayor preparación los desafíos del entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Aperador, M. (2024, 25 de septiembre). Análisis del perfil criminológico de los ciberdelincuentes. Lisa News. https://www.lisanews.org/criminologia/analisis-del-perfil-criminologico-de-los-ciberdelincuentes/

Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica. (2021). Revista Ruptura. http://www.revistaruptura.com/index.php/ruptura/article/view/85/40

Bustán, J. (2025, 31 de marzo). Ecuador es uno de los principales objetivos de los ciberataques en América Latina. Zona Libre. https://www.revistazonalibre.ec/2025/03/31/ecuador-es-uno-de-los-principales-objetivos-de-los-ciberataques-en-america-latina/

Cámara Arroyo, S. (2020, 4 de abril). [Título del artículo]. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=7524987

Castells, M. (2021). La sociedad red: una visión global. Editorial Alianza.

Ciencia Latina. (2024). Criminología relacionada con los delitos cibernéticos y la falta de punibilidad de conductas, 8(6). https://ciencialatina.org/index.php/cienciala/article/view/14605

COIP. (2014, 3 de febrero). [Título del artículo]. Wipolex. https://wipolex-res.wipo.int/edocs/lexdocs/laws/es/ec/ec097es.html

Comisión Federal de Comercio. (2022). Cómo reconocer y evitar las estafas de phishing. https://consumidor.ftc.gov/articulos/como-reconocer-y-evitar-las-estafas-de-phishing

ComputerWeekly.es. (2024). ¿Qué es un ciberdelito y cómo prevenirlo? https://www.computerweekly.com/es/definicion/Que-es-un-ciberdelito-y-como-prevenirloConstitución de la República del Ecuador. (20 de 10 de 2008).

De la Torre, S. (2024, 4 de septiembre). Teoría del aprendizaje social de Bandura. iSeazy. https://www.iseazy.com/es/blog/teoria-del-aprendizaje-social-de-bandura/

Delgado, P. (2019, 9 de diciembre). Teoría del aprendizaje social. Instituto para el Futuro de la Educación. https://observatorio.tec.mx/teoria-del-aprendizaje-social/

Digital Security. (2025, 13 de febrero). Crece el uso de grupos y tácticas de ciberdelincuencia por parte de los estados-nación. Digital Security. https://www.itdigitalsecurity.es/actualidad/2025/02/crece-el-uso-de-grupos-y-tacticas-de-ciberdelincuencia-por-parte-de-los-estadosnacion

Dixon, W. (2025, 23 de abril). ¿Pueden Occidente y China cooperar en el ciberespacio? World Economic Forum. https://es.weforum.org/stories/2025/04/pueden-occidente-y-china-cooperar-en-el-ciberespacio/

Ecuavisa. (2024, 15 de octubre). Ciberdelitos: tipos más frecuentes en Ecuador. https://www.ecuavisa.com/noticias/seguridad/ciberdelitos-tipos-mas-frecuentes-ecuador-EF8153574

Emergentes, Revista Científica. (2024). El ciberacoso en Ecuador: análisis comparado con la legislación española, 4. https://pdfs.semanticscholar.org/fffb/614bd006ead80b440c6e3dfedf7be927e439.pdf

FAC By Verdian. (2024, 4 de noviembre). Qué es la ciberdelincuencia: tipos de delitos financieros. Financial Crime Academy. https://financialcrimeacademy.org/es/que-es-la-ciberdelincuencia-tipos-de-delitos-financieros/

Fernando, J. (2023, 23 de abril). Catfishing. Investopedia. https://www.investopedia.com/terms/c/cat-fishing.asp

Guerrero Álvarez, D. E. (2021, 10 de octubre). [Título del artículo]. Repositorio Digital UNIANDES. https://dspace.uniandes.edu.ec/bitstream/123456789/12207/1/ACTFMDDP013-2021.pdf

INTERPOL. (2023). *Cybercrime*. https://www.interpol.int/en/Crimes/Cybercrime

Juca Maldonado, F., & Medina Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social: panorama actual y futuras perspectivas. *Revista científica Portal de la Ciencia, 4*(3), 325-337. https://doi.org/10.51247/pdlc.v4i3.394

Kosinski, M. (2018). Phishing. IBM. https://www.ibm.com/mx-es/think/topics/phishing

LawBirdie. (2024, 15 de abril). Teoría del aprendizaje social y su aplicación en la criminología. https://lawbirdie.com/es/teoria-del-aprendizaje-social-y-su-aplicacion-en-la-criminologia/

LISA News. (2024, 25 de septiembre). El perfil psicológico de los ciberdelincuentes. https://www.lisanews.org/criminologia/analisis-del-perfil-criminologico-de-los-ciberdelincuentes/

Luris Dictio. (2018). La necesidad de incorporar el agente encubierto en la legislación ecuatoriana, 22. https://revistas.usfq.edu.ec/index.php/iurisdictio/article/view/1127

Malwarebytes. (2025). *Malwarebytes*. https://www.malwarebytes.com/es/malware

Mendizábal Anticona, W. J., Huanca Frías, J. O., Huanca Frías, R. E., & Quispe Ticona, I. L. (2023). Investigación cualitativa y mixta en derecho: tipología y aplicación del metaanálisis cualitativo. *Revista de Climatología*. https://doi.org/10.59427/rcli/2023/v23cs.256-269

Ministerio de Defensa. (2008, 20 de octubre). Constitución de la República del Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia nacional de ciberseguridad del Ecuador. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Moncada Chachapoya, J. Z., & Miranda Villacís, A. D. (2025, enero). La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la legislación en

Ecuador. ResearchGate. https://www.researchgate.net/publication/387635762_La_influencia_de_las_redes_sociales_en_los_delitos_ciberneticos_y_los_desafios_para_la_Legislacion_en_Ecuador

MQR Investigar. (2024). Análisis jurídico del catfishing en transacciones de comercio telemático en Ecuador: desafíos y soluciones en el contexto de la seguridad cibernética. Revista Multidisciplinaria Arbitrada de Investigación Científica, 8(4). https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1866

National Cybersecurity Alliance. (2025, 7 de enero). Cybersecurity predictions for 2025: Challenges and opportunities. https://www.staysafeonline.org/es/articles/cybersecurity-predictions-for-2025-challenges-and-opportunities

Navarro, V. (2025, 6 de agosto). Cómo protegerse de estafas digitales. Lupa Media. https://lupa.com.ec/explicativos/protegerse-estafas-digitales/

Noticias Policía. (2024, 4 de julio). Ecuador ratifica su adhesión al Convenio de Budapest sobre ciberdelincuencia. https://noticias.policia.gob.ec/ecuador-ratifica-su-adhesion-al-convenio-de-budapest-sobre-ciberdelincuencia/

Ochoa Marcillo, A. C. (2021). [Título del artículo]. Repositorio Universidad Andina Simón Bolívar. https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Organización de los Estados Americanos (OEA). (2002). Departamento de cooperación jurídica. https://www.oas.org/juridico/spanish/cyb_ecu.htm

Ordóñez Córdova, L. A. (2024, junio). El marco legal de los delitos cibernéticos en Ecuador. ResearchGate. https://www.researchgate.net/publication/381380145_El_Marco_Legal_de_los_Delitos_Ciberneticos_en_Ecuador

Periodismo de Investigación en Ecuador. (2023). Análisis de prácticas de seguridad digital desde 2017, 7.

https://www.semanticscholar.org/reader/401da2d7ccf5083d8dc3166fb9289e4e29fb7783

Posso López, D. F. (2022, agosto). [Título del documento]. Repositorio Digital UNIANDES. https://dspace.uniandes.edu.ec/bitstream/123456789/14938/1/UA-MMP-EAC-046-2022.pdf

Primicias. (2023, 7 de noviembre). Ecuador: detección de ataques phishing. https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-phishing/

Redilat, Latam. (2023). Las nuevas tecnologías frente al Código Orgánico Integral Penal, 4(4). https://latam.redilat.org/index.php/lt/article/view/1202

Reincisol. (2024). [Título del artículo], 3(5). https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

RICEd. (2025). La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la legislación en Ecuador. https://revistasfiecyt.com/index.php/riced/article/view/2

Sain, G. (2015). *Pensamiento penal*. Gustavo Sain. https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

Sarmiento Chamba, J. A. (2024, 27 de julio). [Título del artículo]. Revista Multidisciplinaria Arbitrada de Investigación Científica. https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1552/5076

Southern New Hampshire University. (2025). Medios digitales: ¿Qué son y cuáles son los tipos? https://es.snhu.edu/blog/cuales-son-los-tipos-de-medios-digitales

Suárez, K. (2015, 1 de noviembre). El Código Orgánico Integral Penal (COIP) y los delitos informáticos. APEspol. https://apespol.ec/el-codigo-organico-integral-penal-coip-y-los-delitos-informaticos/

Unión Europea. (2024, 9 de julio). *Unión Europea*. https://www.eeas.europa.eu/delegations/ecuador/ecuador-y-la-uni%C3%B3n-europea-refuerzan-su-cooperaci%C3%B3n-en-seguridad_es

UNIR. (2021). *¿Qué es la teoría del control social desde el punto de vista de la criminología?* https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

Universidad Internacional de la Rioja. (2024, 15 de febrero). *Delitos cibernéticos*. https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

UNODC. (2021). *Naciones Unidas*. https://www.unodc.org/unodc/en/cybercrime/home.html

Usal Revistas. (2024). *Ciberseguridad vs ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. Propuestas para una más eficaz represión de los ciberdelitos*, 182. https://revistas.usal.es/cuatro/index.php/2254-0326/article/view/31962

UTPL. (2025, 15 de enero). *Innovación tecnológica para la protección de datos personales en Ecuador*. https://noticias.utpl.edu.ec/innovacion-tecnologica-para-la-proteccion-de-datos-personales-en-ecuador?utm_source=chatgpt.com

Voces y Saberes. (2024). *Revista Voces y Saberes*. https://vocesysaberes.aragon.unam.mx/index.php/RAVS/article/view/86

ANEXOS

Anexo N° 1 Preguntas Entrevista

Nombre del funcionario: **Tiempo de trabajo:** • Menos de 1 año • De 1 a 3 años • Más de 3 años	**Respuesta**
¿Cómo calificaría el marco legal actual en Ecuador para la prevención, investigación y sanción de los delitos cibernéticos?	
¿Considera que este marco legal es suficiente o requiere reformas?	
¿Cuáles son las principales dificultades que enfrentan los operadores de justicia fiscales, policías y administradores de justicia para combatir los casos de ciberdelincuencia?	
¿Qué mecanismos legales existen para la preservación y obtención de pruebas electrónicas en investigaciones de delitos cibernéticos?	
¿Cómo se maneja la cooperación internacional en casos de delitos cibernéticos que involucran a más de un país?	
¿Qué estrategias o programas de capacitación se ofrecen a los funcionarios encargados de combatir la lucha contra la ciberdelincuencia?	
¿Cuáles son las recomendaciones que daría usted para fortalecer el marco legal y operativo en Ecuador para enfrentar eficazmente la ciberdelincuencia?	

Anexo N° 2 Preguntas encuesta

Estimado/a participante:

Le invitamos a formar parte de esta encuesta que tiene como objetivo conocer la percepción y experiencia de los usuarios respecto a los delitos cibernéticos y el marco legal vigente en Ecuador. Su participación es muy importante para obtener información valiosa que contribuya al análisis y mejora de las políticas y acciones destinadas a la prevención y sanción de estos delitos.

La encuesta es completamente anónima y sus respuestas serán tratadas con estricta confidencialidad, utilizándose únicamente con fines académicos y de investigación. Le agradecemos de antemano el tiempo que dedique para responder con sinceridad y atención.

¡Muchas gracias por su colaboración!

Preguntas demográficas

¿Con qué género se identifica?

Masculino

Femenino

Otro / Prefiero no decir

¿Cuál es su rango de edad?

Menos de 18 años

18-24 años

25-34 años

35-44 años

45-54 años

Más de 54 años

¿En qué ciudad o provincia reside actualmente?

Preguntas

1. ¿Considera que el marco legal actual en Ecuador es adecuado para combatir los delitos cibernéticos?

Sí

No

No sabe / No responde

2. ¿Ha recibido alguna vez información o capacitación sobre prevención de delitos cibernéticos?

Sí, en el trabajo

Sí, en el colegio/universidad

Sí, por cuenta propia

No, nunca

3. ¿Cree que las autoridades ecuatorianas están preparadas para investigar y sancionar los delitos informáticos?

Sí, totalmente preparadas

En parte, necesitan mejorar

No, no están preparadas

No sabe / No responde

4. ¿Ha sido víctima o conoce a alguien que haya sido víctima de algún delito cibernético (phishing, malware, fraude, etc.)?

Sí, personalmente

Sí, algún familiar o amigo

No, nadie que conozca

Prefiero no responder

5. ¿Confía en que la Policía y la Fiscalía puedan proteger sus datos personales en caso de una denuncia por delito cibernético?

Sí, confío plenamente

Confío parcialmente

No confío

No sabe / No responde

6. ¿Cree que la cooperación internacional es importante para combatir los delitos cibernéticos en Ecuador?

Sí, es fundamental

Es importante, pero no esencial

No es importante

No sabe / No responde

7. ¿Considera que la ciudadanía en general está suficientemente informada sobre los riesgos y prevención de delitos cibernéticos?

Sí, está bien informada

En parte, falta más información

No, está poco informada

No sabe / No responde

8. ¿Utiliza algún método de seguridad adicional para proteger sus cuentas en línea (como autenticación de dos factores)?

Sí, siempre

A veces

No, nunca

No sabe qué es eso

9. ¿Cree que las empresas y proveedores de servicios digitales deberían tener mayor responsabilidad en la prevención de delitos cibernéticos?

Sí, totalmente

En parte, pero también los usuarios deben cuidarse

No, la responsabilidad es solo de los usuarios

No sabe / No responde

10. ¿Considera que las sanciones legales actuales para los delitos cibernéticos son suficientes para disuadir a los delincuentes?

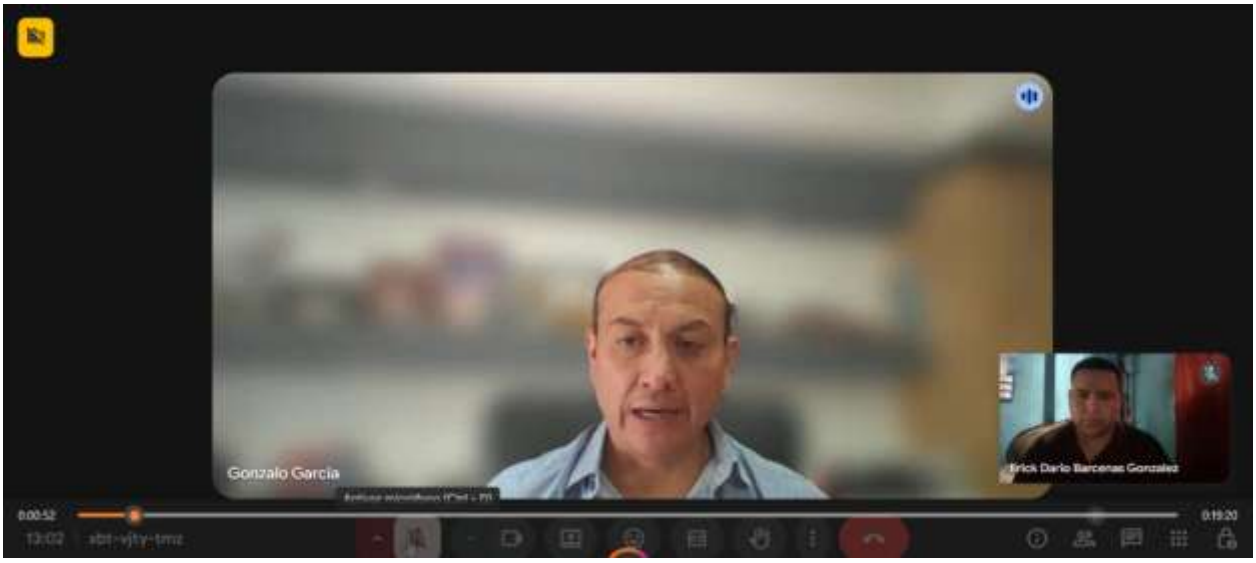
Sí, son adecuadas

No, deberían ser más severas

No, deberían ser más flexibles

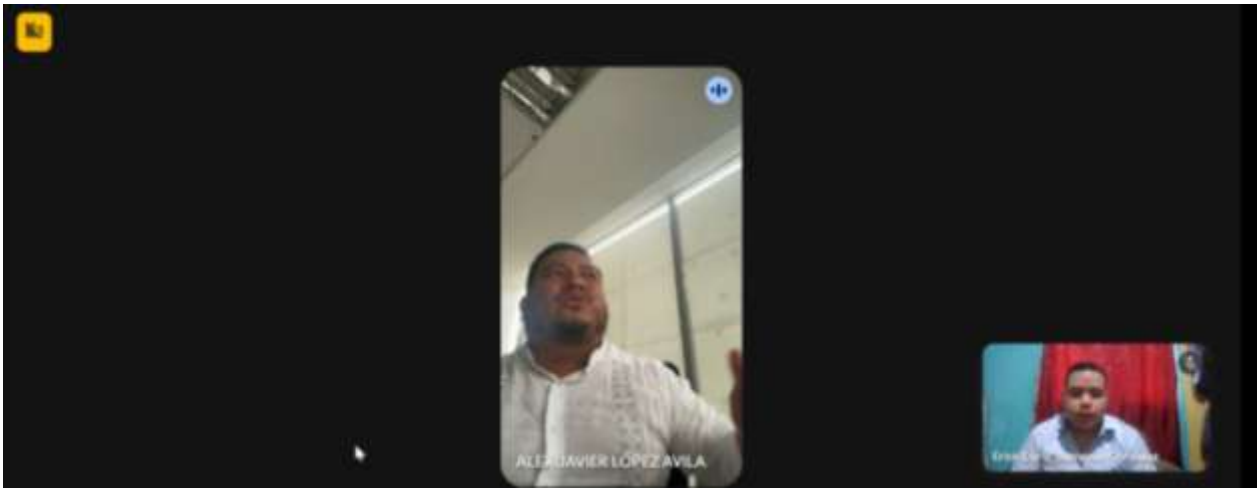
No sabe / No responde

Anexo N° 3 Entrevista 1



Link de acceso: https://drive.google.com/file/d/12CKn1MT6Hvz7NpFgfllhct-_dO1w--TR/view?usp=drive_link

Anexo N° 4 Entrevista 2



Link de acceso:
https://drive.google.com/file/d/1v7jRdFF1JWVcS8ENnuH1enQ48dVF83C-/view?usp=drive_link