UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Trabajo de Titulación para optar al título de Abogada de los Tribunales y Juzgados de la República del Ecuador

Autores:

Curichumbi Cepeda, Lesly Mishell

Changoluiza Fonseca, Kateryn Verónica

Tutor:

Mgs. Nelson Francisco Freire Sánchez

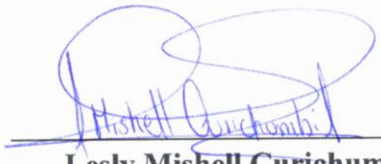
Riobamba, Ecuador. 2024

DECLARATORIA DE AUTORÍA

Yo, **LESLY MISHELL CURICHUMBI CEPEDA**, con cédula de ciudadanía **060609131-2** y **KATERYN VERÓNICA CHANGOLUIZA FONSECA**, con cédula de ciudadanía **060581684-2,** autor (as) del trabajo de investigación titulado**: ALCANCE DE LA NORMATIVA LEGAL ECUATORIANA Y EL IMPACTO DEL MALWARE EN LA SEGURIDAD CIBERNÉTICA**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de nuestra exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de nuestra entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, a los 6 días del mes de noviembre del 2024.



Lesly Mishell Curichumbi Cepeda
C.I .060609131-2

Kateryn Verónica Changoluiza Fonseca
C.I. 060581684-2

ACTA FAVORABLE - INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN

En la Ciudad de Riobamba, a los 22 días del mes de julio del 2024 luego de haber revisado el Informe Final del Trabajo de Investigación presentado por las estudiantes **Lesly Mishell Curichumbi Cepeda** portadora de la cédula de ciudadanía **060609131-2** y **Kateryn Verónica Changoluiza Fonseca** portadora de la cédula de ciudadanía **060581684-2** de la carrera de Derecho y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado ***Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética"***, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

MSc. Nelson Francisco Freire Sánchez

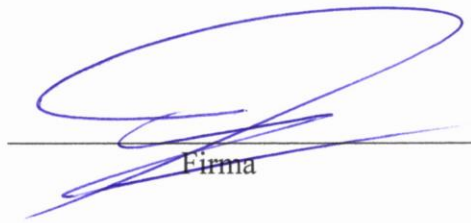
Tutor

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"ALCANCE DE LA NORMATIVA LEGAL ECUATORIANA Y EL IMPACTO DEL MALWARE EN LA SEGURIDAD CIBERNÉTICA",** presentado por Lesly Mishell Curichumbi Cepeda, con cédula de ciudadanía 060609131-2 y Kateryn Verónica Changoluiza Fonseca, con cédula de ciudadanía 060581684-2, bajo la tutoría de Mgs. Nelson Francisco Freire Sánchez; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a los 27 días de noviembre de 2024.

Mgs. Campuzano Llaguno Rosita Elena
PRESIDENTE DEL TRIBUNAL DE GRADO

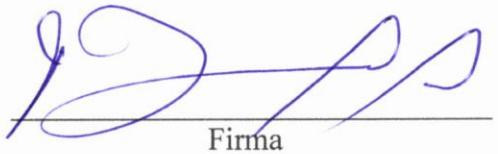


Firma

Mgs. Romero Noboa Wendy Pilar
MIEMBRO DEL TRIBUNAL DE GRADO

Firma

Dr. Montero Chávez Juan Gonzalo
MIEMBRO DEL TRIBUNAL DE GRADO



Firma

CERTIFICACIÓN

Que, Lesly Mishell Curichumbi Cepeda, con CC: 060609131-2 y Kateryn Verónica Changoluiza Fonseca, con CC: 060581684-2, estudiantes de la Carrera de Derecho, Facultad de Ciencias Políticas y Administrativas; ha trabajado bajo mi tutoría el trabajo de investigación titulado "Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética", cumple con el 2%, de acuerdo al reporte del sistema Anti plagio Turnitin, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 6 de noviembre de 2024

Mgs. Nelson Francisco Freire Sánchez
TUTOR

DEDICATORIA

A Dios por guiarme y ser mi fortaleza cada día. A mi padre Basilio, por ser aquel inspirador de seguir adelante y enseñarme que, con sacrificio, esfuerzo respeto, y humildad se puede cumplir todos los sueños que tenga; a mi madre Sara, por enseñarme a confiar en mí y nunca rendirme ante adversidades. El sacrificio y apoyo de ellos ha sido incondicional e importante para poder llegar a cumplir cada una de las etapas de mi vida. A mi hermano, quien ha compartido momentos alegres y tristes, pero siempre alentándome con su constante apoyo. A mis amigos, por formar parte de una experiencia enriquecedora y memorable. Gracias.

Lesly Mishell Curichumbi Cepeda

Dedico este fruto de mi esfuerzo y dedicación a Dios, por conservarme con vida y guiar mi camino bajo la sombra de sus alas, a mis venerados padres por su apoyo incondicional siendo la mayor fuente de inspiración, fortaleza y sabiduría para lograr mis metas con tenacidad, a mis abuelitos, por ser los faros de luz que iluminan mi alma con sus sabios consejos brindándome su apoyo inquebrantable en cada decisión tomada y a mi compañero de risas y sueños, por despertar en mí la confianza en mis capacidades y cultivar una mejor versión de mí misma.

A todos ellos, con gratitud y emoción ferviente dedico este logro reconociendo que su cariño y respaldo han sido elementos sustanciales para mi desarrollo personal y profesional.

Kateryn Verónica Changoluiza Fonseca

AGRADECIMIENTO

Agradezco a Dios, por haberme brindado vida y salud. A mis padres quienes se han sacrificado para yo cumplir mis objetivos. A su vez, como no agradecer a la poderosa Universidad Nacional de Chimborazo, por permitirme formar parte de ella y forjar mis conocimientos; a su planta docente de la Carrera de Derecho por ser aquellos mentores para el desarrollo de mi vida profesional. Agradecer a nuestro tutor de tesis y docente de titulación por su apoyo académico y moral. Por último, agradecer aquellos familiares, amigos, docentes que me han brindado oportunidades de aprendizaje y me han apoyado.

Lesly Mishell Curichumbi Cepeda

Como muestra de reconocimiento expreso mi más profunda gratitud a mis padres, por ser la piedra angular de mi esfuerzo y culminación de mi carrera académica, en especial a mi madre, por haber luchado incansablemente para brindarme los medios y herramientas necesarias para continuar con mis estudios, siendo un verdadero ejemplo de dedicación y perseverancia; a mis entrañables amigas de la facultad, que en medio de risas, sobresaltos y llantos hemos alcanzado la cumbre de la travesía académica; a los docentes de la carrera de Derecho que gracias a su vocación y compromiso han forjado las bases de mi aprendizaje continuo; a nuestro tutor del proyecto de investigación, cuya guía fue fundamental en el desarrollo de este proceso, a los distinguidos profesionales del derecho que con paciencia me brindaron invaluables consejos y contribuyeron a mi crecimiento profesional mostrándome la realidad laboral de esta prestigiosa carrera.

Kateryn Verónica Changoluiza Fonseca

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación se desarrolló con el objetivo de analizar mediante un estudio jurídico analítico, doctrinal y comparativo el alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética para determinar las dificultades en la investigación de delitos informáticos o cibernéticos. El estudio se ha desarrollado a través de un tipo de investigación jurídica descriptiva, pura e histórica jurídica, con un diseño no experimental, que ha tomado como muestra a 4 agentes fiscales de la provincia de Chimborazo y 1 perito informático acreditado por el Consejo de la Judicatura de la ciudad de Quito, se aplicó la técnica de recolección de datos llamada entrevista y se empleó 2 guías de entrevista como instrumento, las cuales han permitido explicar la percepción del agente fiscal sobre la eficacia de la normativa ecuatoriana ante los delitos informáticos cometidos mediante el uso del malware y entender el papel de los peritos informáticos en la investigación del funcionamiento técnico del malware como herramienta para cometer delitos informáticos que afectan a la seguridad cibernética. Además, se llevó a cabo un análisis documental a través de una matriz como instrumento de recolección de datos, por medio de la cual se registró noticias de los medios de comunicación nacionales acerca de los ataques de malware más influyentes en el país. Como resultado de las entrevistas, cuatro de los cinco entrevistados revelan que la normativa ecuatoriana es insuficiente para abordar los delitos informáticos. Se concluye una falta de convenios de cooperación internacional, tipificación específica de las nuevas conductas delictivas en temas de ciberataques e inexistente regulación de manuales y protocolos de procedimientos investigativos entre fiscalía y policía judicial específica para la investigación, guarda y compilación de evidencias digitales en los casos de malware. Por lo tanto, se acepta la hipótesis alternativa y se afirma que la actualización de la norma en materia de ciberseguridad permitirá la efectiva investigación de los delitos informáticos cometidos mediante el malware.

Palabras clave: malware, delito informático, normativa, investigación, seguridad cibernética

ABSTRACT

The present research was developed in the order to understand, through an analytical, doctrinal and comparative legal study, the scope of Ecuadorian legal regulations and the impact of malware on cyber security, to determine the difficulties in the investigation of computer or cybercrimes. The study has been developed through a type of descriptive, pure and historical legal research, with a non-experimental design, which has taken as a sample of four provincial prosecutors of Chimborazo and one computer expert accredited by the "Consejo de la Judicatura" from Quito. The data collection technique called interview was applied and two interview guides were used as instruments, which have allowed to explain the perception of the prosecutor about the effectiveness of the Ecuadorian regulations against computer crimes committed through the use of malware, and to understand the role of computer experts in the investigation of the technical operation of malware as a tool to commit computer crimes that affect cybersecurity. In addition, a documentary analysis was conducted using a matrix as a data collection instrument, through which news from the national media about the most influential malware attacks in the country were recorded. As a result of the interviews, four of the five interviewees revealed that Ecuadorian regulations are insufficient and generalist to address computer crimes. They conclude that there is a lack of international cooperation agreements, specific typification of the new criminal behaviors in cyber-attacks and non-existent regulation of manuals and protocols of investigative procedures between prosecutors and judicial police specifically for the investigation, storage and compilation of digital evidence in malware cases. Therefore, the alternative hypothesis is accepted, and it is affirmed that the updating of the cybersecurity regulation will allow the effective investigation of computer crimes committed with malware.

Key words: malware, cybercrime, regulatory, investigation, cybersecurity.

Reviewed by:
Mgs. Kerly Cabezas
ENGLISH PROFESSOR
I.D. 0604042382

CAPÍTULO I

1. INTRODUCCIÓN

El presente trabajo de investigación analiza el alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética, considerando que el "malware" o software malicioso "está diseñado para realizar un proceso no autorizado que podría tener un efecto adverso en la confidencialidad, integridad o disponibilidad del sistema de información" (Rossinskaya & Ryadovskiy, 2020, p.3).

En el panorama actual, la preocupación global y nacional por los delitos informáticos o cibernéticos va en aumentado debido a la diversidad de estrategias maliciosas empleadas por los cibercriminales, para explotar las vulnerabilidades de la infraestructura digital y el ciberespacio con el fin de cometer diversos tipos de crímenes; en Ecuador, este problema es especialmente notable. A pesar de contar con estrategias y propuestas legislativas, la respuesta sigue siendo insuficiente debido a la falta de agilidad en la adaptación normativa en consonancia con el rápido avance de la tecnología.

La normativa ecuatoriana generaliza a los delitos informáticos los mismos que se encuentran tipificados en el Código Orgánico Integral Penal (COIP); sin embargo, el marco regulatorio no cubre todos los posibles delitos que surgen con el avance de la sociedad y la tecnología. Por lo tanto, es necesario precisarlo y mantenerlo en constante actualización para garantizar la seguridad cibernética, al igual que, es fundamental fomentar la adhesión del país a convenios internacionales que faciliten la investigación transnacional (Fernández & Vázquez, 2022).

En este sentido, la seguridad cibernética se ha visto vulnerada constantemente, por tanto, debe ser tratada como preocupación nacional. En comparación con los países de la región, la calidad de la ciberseguridad en el país es relativamente baja, Ecuador no ha sido inmune a los cambios provocados por la globalización, pero debido a la falta de comprensión de los gobernantes sobre los riesgos en el ciberespacio y la lentitud de las reformas legales, las políticas no están estandarizadas en todas sus entidades constituyentes (Alvarado, 2020).

Con estos antecedentes, la presente investigación tendrá como fin analizar mediante un estudio jurídico analítico, doctrinal, comparativo el alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética para determinar las dificultades investigativas de este tipo de delitos, para ello se determinará el alcance de la normativa jurídica ecuatoriana ante los delitos informáticos, se definirá la naturaleza del malware como nueva herramienta delictiva para cometer delitos informáticos y se establecerá un estudio relacional de la falta de protección de la seguridad cibernética en el Ecuador.

La investigación se estructura conforme a lo establecido en el art.173 numeral 6 del Reglamento del Régimen Académico o reformado de la Universidad Nacional de

Chimborazo, que contempla: introducción, planteamiento del problema, objetivos, estado del arte, metodología, cronograma del trabajo investigativo, materiales de referencia, anexos y visto bueno del tutor.

1.1. PLANTEAMIENTO DEL PROBLEMA

Analizando el eje histórico, "la sustracción de información realizada a través de una computadora es una preocupación desde la década de 1960, cuando las personas intentaban sustraer información almacenada dentro de las computadoras disponibles"(Echevería et al., 2020, p.4) , a partir de este acontecimiento, nace un desafío en la seguridad; por lo tanto, a medida que el número de piratas informáticos incrementa, también crece el número de víctimas potenciales. Desde el siglo XXI el avance de la tecnología ha traído grandes beneficios como desafíos, creando así la necesidad de que el Derecho se amplie para tratar nuevos problemas jurídicos en el campo de la informática.

De la misma manera, existe un problema latente en el sistema de justicia por cuanto, los delitos informáticos no están debidamente actualizados en la norma. Los ataques de las ciber mafias son recurrentes en el país y según un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3 183 delitos informáticos (Diaz et al., 2023). Además, de acuerdo con la Dirección de Estadísticas y Sistemas de la Información desde enero del 2023 a marzo del 2024 se han presentado 1 356 casos de delitos informáticos que siguen en investigación previa.

Las personas que ejecutan este tipo de infracciones tienen la facilidad de encubrir sus actividades ilícitas, ocultarse a través de una pantalla y cubrir su identidad, lo que dificulta recabar elementos de convicción que demuestren la consumación del delito y la responsabilidad del sujeto activo. "Esta es la razón por la que estos delitos son difíciles de demostrar y muchas personas que son víctimas de estos prefieren no denunciar y solo resignarse a la pena de saber que fueron blancos de estos delincuentes" (Aparicio, 2022, p.2).

De tal manera, una de las nuevas modalidades de delitos informáticos, es el uso del malware, el cual se define como un "tipo de ataque cibernético en forma de software malicioso que incluye familiar de criptomonedas, virus, gusanos, softwares espías y gusanos, con el objetivo de sustraer información, efectuar métodos de espionaje o la interrupción de un servicio" (ENISA, 2020, p.2). Es decir, proporciona a los ciberdelincuentes las herramientas necesarias para efectuar ataques dirigidos a la infraestructura digital.

"Los ciberdelincuentes captan la información personal como un medio para perjudicar a su titular o, a su vez, incidir en el ejercicio de sus derechos fundamentales" (Rosas & Pila, 2023, p.10). En tal razón, a futuro, esta modalidad de delito irá en aumento sino se toman medidas correctivas y sancionatorias, a la vez que afectará a los derechos de los usuarios, tales como: el derecho a la protección de datos de carácter personal, a la intimidad personal, a la integridad, a la privacidad, al derecho a la inviolabilidad y el secreto de la correspondencia física y virtual.

Por lo tanto, la jurisdicción ecuatoriana deberá adaptarse a marcos legales, convenios y estrategias actualizadas para abordar adecuadamente estas amenazas cibernéticas, las mismas que implicarán la creación de leyes más específicas y la colaboración internacional, con el fin de combatir la falta de protección de la información que reposa en la nube y en los sistemas informáticos para encontrar el adecuado equilibrio entre una efectiva seguridad digital y el respeto de los derechos individuales de cada usuario (Rosas & Pila, 2023).

Es por ello que, a través de este proyecto de investigación se busca determinar las dificultades que se presentan en la realidad procesal para llevar a cabo la investigación de los delitos informáticos cometidos mediante el malware, estableciendo un análisis normativo e identificando como esta nueva herramienta delictiva logra impactar negativamente en la seguridad cibernética.

1.2. JUSTIFICACIÓN

El presente proyecto investigativo se justifica en la importancia de demostrar que Ecuador, aún mantiene deficiencias en la investigación de los delitos informáticos o cibernéticos. Considerando que el Malware es una nueva amenaza para la seguridad cibernética, el propósito es resolver la necesidad de proteger el espacio digital, la privacidad de los usuarios y la integridad de los datos presentes en un mundo en constante evolución con la tecnología.

Por medio de este estudio, se desea entregar al lector un análisis normativo relacionado a los delitos informáticos e información actualizada sobre la realidad del país frente a los casos de este tipo de delitos cometidos mediante el malware. Con el análisis que se desprende de este estudio se comprende el fenómeno de los delitos cibernéticos en la nueva era y a su vez contribuye al desarrollo del derecho en la búsqueda de estrategias y herramientas que protejan la seguridad en el ciberespacio ante amenazas. Esta investigación es de gran utilidad para estudios futuros relacionados con el tema por su contribución en el aspecto técnico, jurídico y social, por lo que será de gran interés para que la sociedad en general tome conocimiento y se concientice sobre el uso de tecnologías, así como de la cultura de denuncia para que estos hechos no queden en la impunidad.

Esta investigación se dirige directamente a varios beneficiarios clave. En primer lugar, busca ofrecer información crucial al sistema de justicia del país, revelando deficiencias en la investigación de estos crímenes, con la esperanza de mejorar los procesos judiciales relacionados con la ciberseguridad. Además, se beneficia a los profesionales del derecho y estudiantes en formación debido a que encontrarán en este estudio un recurso valioso que les proporcionará un análisis normativo actualizado y estrategias para abordar los delitos informáticos en el ámbito legal.

Al mismo tiempo, este estudio entrega un aporte significativo a los legisladores y responsables del sistema judicial al recibir información que puede contribuir al fortalecimiento de la legislación en materia de seguridad cibernética. Finalmente, se busca

beneficiar a las víctimas directas de los ciberdelitos, de manera que encuentren un amparo eficaz en la justicia ecuatoriana.

1.3. OBJETIVOS

1.3.1. Objetivo General

Analizar mediante un estudio jurídico analítico, doctrinal y comparativo el alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética para determinar las dificultades en la investigación de delitos informáticos o cibernéticos.

1.3.2. Objetivos Específicos

- Determinar el alcance de la normativa jurídica ecuatoriana ante los delitos informáticos.
- Definir la naturaleza del malware como nueva herramienta delictiva para cometer delitos informáticos.
- Establecer un estudio relacional de la falta de protección de la seguridad cibernética en el Ecuador.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ESTADO DEL ARTE

Respecto del tema "Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética" no se han realizados trabajos investigativos iguales; sin embargo, existen algunos similares al que se pretende realizar, cuyas conclusiones más importantes son las siguientes:

Luis Arturo Pérez Maldonado, en el año 2019, en el Instituto Tecnológico Superior "Eloy Alfaro Ecuador" realizó un trabajo investigativo titulado: "Normativa Legal sobre Delitos Informáticos en Ecuador", para la publicación de un artículo científico en la Revista Hallazgos 21 de la Pontificia Universidad Católica del Ecuador, en el cual, mediante un estudio bibliográfico clasifica los delitos informáticos y analiza la normativa legal aplicable, concluye el mismo señalando que:

> Las empresas tanto públicas como privadas del Ecuador no poseen un sistema de seguridad efectivo que les permita enfrentar un ataque informático. Existen verdaderas dificultades para afrontar los delitos informáticos nacionales y transnacionales, debido a la incompatibilidad de las leyes a nivel local y mundial, lo que ha ocasionado grandes problemas como: la revelación ilegal de datos, la disfuncionalidad de los sistemas y sobre todo grandes pérdidas económicas (Ortiz, 2019, pp. 108-109).

De lo expuesto se deduce que, en el Ecuador existe una creciente amenaza debido al surgimiento de nuevas formas de ciberdelincuencia que afectan a las empresas. Las mismas que carecen de sistemas de seguridad efectivos para enfrentar ataques informáticos; además, el autor destaca una falta de armonización entre las leyes internacionales lo que dificulta la lucha contra los delitos informáticos, por lo que recomienda la adhesión al convenio de Budapest, la actualización normativa y la capacitación especializada en delitos informáticos.

Viviana Vanessa Aparicio Izurieta, en el año 2022, realizo un trabajo investigativo titulado "Delitos informáticos en Ecuador según el COIP: un análisis documental", cuyo fin es orientar en cuanto a estos delitos informáticos y ofrecer una visión más generalizada sobre los medios y las formas que diversos sujetos manejan para realizar ciberdelitos, concluye el mismo señalando que:

> El avance de la tecnología genera que los delitos informáticos vayan en aumento. Cabe destacar que, estos delitos no requieren de esfuerzos físicos sino más bien intelectuales; cualquier persona puede transformase en creador de un delito informático, por tal razón al existir en estos delitos una causa y efecto debería existir sanciones que establezcan en una balanza dos factores que determinen una igualdad entre la víctima y victimario (Aparicio, 2022, p.3).

Por lo tanto, el desarrollo de la tecnología genera el incremento de los delitos informáticos, cualquier individuo puede convertirse en autor de un delito informático, puesto

que para accionarlo requiere únicamente de esfuerzos intelectuales. Además, es fundamental que existan sanciones proporcionales que equilibren los derechos de las partes.

Alan Eduardo Leyva Méndez, en el año 2021, realizó un trabajo investigativo titulado "Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano", concluye el mismo señalando que:

> El Estado ecuatoriano ha planteado lineamientos simples para tratar la seguridad cibernética, aún requiere un modelo de gobernanza basado en criterios de ciberseguridad que integren los esfuerzos aislados de las instituciones ya que carece de acuerdos técnicos y metodológicos, por ello, es necesario que se fortalezca la gestión tecnológica y se mejore la seguridad de la infraestructura digital crítica del país (Leyva, 2021, p.5).

Dicho de otro modo, se identifica la necesidad de un enfoque integral en ciberseguridad que abarque aspectos jurídicos, técnicos e instructivos. Siendo así que los limitados avances del país en materia de seguridad cibernética y la falta de recursos tecnológicos, capacitación adecuada y cooperación internacional efectiva limitan la capacidad de respuesta ante estos ataques informáticos.

Roxana Cedeño, en el año 2022, realizó un trabajo investigativo titulado: "Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador", para la publicación de un artículo científico en la Revista Tecnológica Ciencia y Educación Edwards Deming, en el cual, mediante un enfoque cualitativo expone la perspectiva de la ciberseguridad en el Ecuador, concluye el mismo señalando que:

> Ecuador, por medio del Ministerio de Telecomunicaciones trabaja en una estrategia nacional de ciberseguridad que tiene como fin robustecer el ciberespacio, generar planificación, estrategias y guías para su desarrollo, sin embargo, es fundamental que la creación y promulgación de leyes se enfoquen en la regulación de todos los aspectos relacionados a la protección de la seguridad cibernética en el país y en las fronteras transnacionales (Villacís, 2022, p.59).

En este sentido, el estudio citado reconoce la necesidad de que el país cuente con medidas de seguridad digital e instaure una legislación idónea que regule cada acto ilegítimo que vulnera los derechos de los usuarios de los medios tecnológicos, sistemas informáticos y navegación web, el Estado debe trabajar de manera permanente desarrollando planes, políticas y acciones urgentes para mitigar el impacto de los ciberataques abordando la problemática desde el punto de vista jurídico.

Rossinskaya y Ryadovsky, en el año 2020, en la Universidad Estatal de Baikal de Rusia, realizó un trabajo investigativo titulado: "El concepto de malware como medio para cometer delitos informáticos: clasificaciones y tecnologías de uso ilegal", para la publicación de un artículo científico en la Revista Panrusa de Criminología, concluye el mismo señalando que:

> Se ha convertido en algo habitual que las redes criminales usen el malware para fines delictivos, es fundamental estudiar estas nuevas tipologías para lograr predecir la evolución de la situación a futuro en el campo de la informática y desarrollar de manera oportuna medidas preventivas y eficaces para contrarrestar este tipo de delitos (Rossinskaya & Ryadovskiy, 2020, p.707).

Por lo tanto, desde la perspectiva del derecho penal y la criminología se destaca que la mayoría de los delitos informáticos que perjudican gravemente la integridad, confidencialidad y disponibilidad de los sistemas informáticos y banco de datos, se efectúan mediante el malware como una herramienta esencial para la consumación del ilícito y a su vez un instrumento para encubrir las huellas y vestigios, dificultando la detección del hecho dañoso. Además, en este estudio el autor subraya la necesidad de actualizar la normativa penal, ya que en muchos casos no contempla la criminalización de ciertos tipos de ciberataques.

Joshua Ojo Nehinbe, en el año 2022, en la editorial IntechOpen realizó un trabajo investigativo titulado: "Modelos de clasificación para prevenir delitos juveniles cometidos con aplicaciones de malware", para la publicación de un capítulo del libro "Malware: detección y defensa", en el cual, mediante la aplicación de entrevistas determinó los elementos genéricos de la delincuencia juvenil respecto a los delitos cometidos por malware, concluye el mismo señalando que:

> Mediante el estudio se ha demostrado que la aplicación del malware tiene motivos intrusivos para la comisión de actividades ilícitas en función de su uso, funciones y programación. Los usuarios y diseñadores de este software malicioso buscan acceder, corromper, eliminar, secuestrar o sustraer datos personales, alterar sistemas informáticos o transferir ilícitamente dinero de las cuentas bancarias de otras personas para su beneficio (Nehinbe, 2022, p.17).

En efecto, el estudio demostró que la capacidad del malware para infiltrarse en los sistemas y causar daños informáticos representa una clara vulneración a los principios de la seguridad cibernética, lo que plantea serios desafíos en el ámbito del derecho penal respecto a que el proceso de investigación se ve obstaculizado por la complejidad técnica inherente al rastreo de la modalidad y origen del ataque, lo que demanda una respuesta inmediata para abordar esta problemática.

2.2. ASPECTOS TEÓRICOS

2.2.1. UNIDAD 1: LA NORMATIVA LEGAL ECUATORIANA ANTE LOS DELITOS INFORMÁTICOS

2.2.1.1. Definición y características de los delitos informáticos o ciberdelitos

Definición

El avance de la tecnología ha dado lugar a nuevas formas de criminalidad. El cibercrimen, también denominado delito informático, es una conducta delictiva que se realiza a través del uso de internet, ordenadores o redes informáticas. Engloba una amplia

gama de actos ilícitos con el fin de dañar el sistema informático o la información almacenada en él, a su vez es una amenaza grave para la seguridad individual, la privacidad y el bienestar social (Frajić, 2020).

El delito informático es un conjunto de actividades ilícitas que se llevan a cabo por individuos que generan interrupciones en los sistemas operativos de red, sustraen datos y documentos confidenciales, hackean cuentas bancarias, entre otros actos. Con la evolución e importancia del Internet para el comercio, el entretenimiento y el gobierno, los ciberdelitos han ido en crecimiento constante siendo así que estos crímenes son ejecutados principalmente por expertos en informática, con el fin de cometer fraude, tráfico de pornografía infantil y apropiación de propiedad intelectual, suplantación de identidad o violación de la privacidad (Goni et al., 2022).

El ciberdelito es una forma de delito que surge debido al uso de la tecnología de Internet. En consonancia con los avances en la tecnología de la información, han surgido varios delitos que a menudo se interpretan como aquellos que son cometidos en el ciberespacio o en áreas informáticas. Además, se lo realiza a través de la ingeniería social, la misma que es una técnica de manipulación que aprovecha el error humano para obtener acceso a información personal o datos valiosos (Sahat Tobing et al., 2023).

Desde un concepto típico el delito informático, constituye una conducta típica, antijurídica y culpable; a su vez, este delito desde un concepto atípico se establece como actitudes ilícitas, siendo así que se lleva a cabo por medio la utilización de computadoras como instrumentos útiles para cometer actos ilícitos (Saltos et al., 2021).

Por ende, estos delitos pueden manifestarse de diversas formas como:

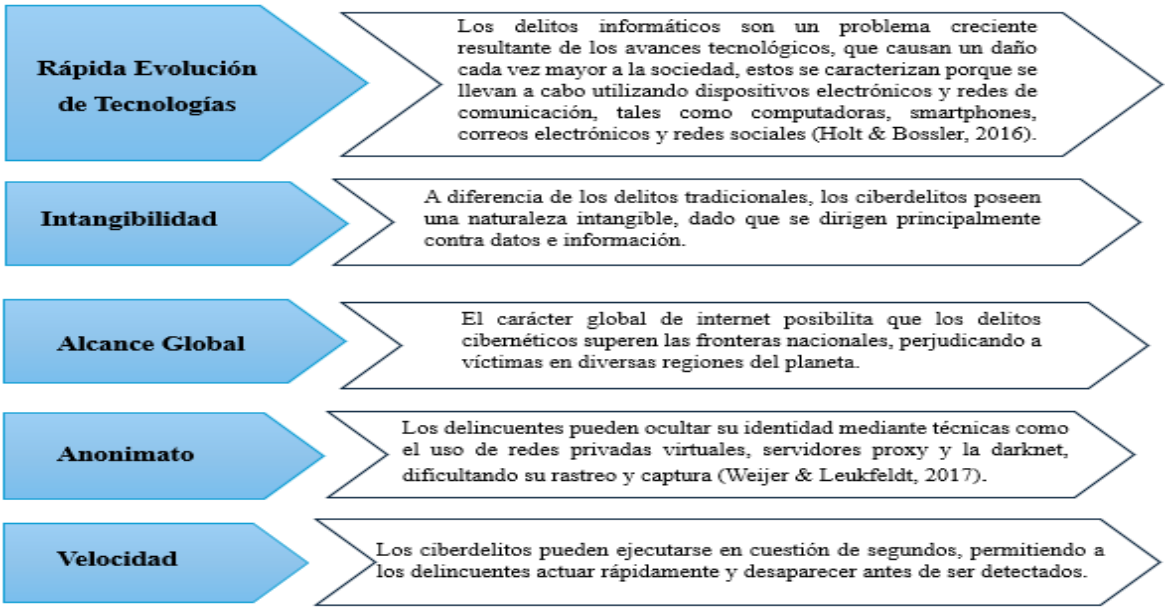
1.- La intrusión en sistemas informáticos, es decir, la obtención de información confidencial o alteración de datos sin ninguna autorización;
2.- Sustracción de información, es la apropiación ilícita de información personal, financiera o de otra índole con fines fraudulentos;
3.- Engaño electrónico, la utilización de medios electrónicos con el objeto de obtener beneficios económicos de cualquier tipo en perjuicio de la víctima;
4.- Programación de software malicioso, es la difusión de programas dañinos con el fin de dañar sistemas informáticos o sustraer información;
5.- coso cibernético, es el hostigamiento o persecución que se lo realiza a través de medios electrónicos, causando en sus víctimas daños emocionales, psicológicos.

Características de los delitos informáticos o ciberdelitos

En el mundo digital actual, los delitos informáticos también denominados ciberdelitos, se han convertido en una amenaza cada vez más preocupante. Estos delitos se perpetran utilizando computadoras, redes o sistemas informáticos, con el fin de vulnerar los derechos, intereses o propiedades de individuos u organizaciones. Cabe destacar que, a diferencia de los delitos tradicionales, los ciberdelitos se caracterizan por su naturaleza transnacional y su capacidad para aprovechar las oportunidades que ofrece el entorno digital,

ya que los delincuentes informáticos pueden alterar o destruir datos, cometer fraudes financieros, todo ello sin fronteras físicas.

Figura 1.
Características de los delitos informáticos o ciberdelitos**.**



Nota: Elaboración propia con Características de los delitos informáticos o cibernéticos adoptado de Cibercrimen en Progreso (2017)

2.2.1.2. Antecedentes y evolución de los delitos informáticos en el Ecuador

Así como el ser humano, a inicios de la prehistoria usó su ingenio para desarrollar herramientas cortopunzantes que facilitaron las labores cotidianas, las mismas fueron usadas por ciertos individuos con intenciones de causar daño físico y atentar contra la existencia de sus semejantes; de manera análoga, el desarrollo continuo de tecnología ha entregado a la sociedad un sinfín de beneficios generando una dependencia cada vez mayor a los sistemas tecnológicos e informáticos en el desarrollo de actividades diarias en el mundo moderno, este hecho ha dado lugar a que varios perpetradores logren incursionarse ilícitamente y causar perjuicios a los usuarios de estos medios.

A nivel mundial, el primer hecho delictivo en materia de delitos informáticos del que se tiene registro es el denominado “phreaking” efectuado por John Draper en 1971, quien hackeo ilegalmente un sistema telefónico con la finalidad de conseguir llamadas a larga distancia de manera gratuita y por medio del uso de la ingeniería social se dedicó a realizar llamadas fraudulentas a los técnicos de las compañías telefónicas reconocidas identificándose como uno de sus compañeros para obtener información reservada (Ruiz, 2022).

Sin embargo, no se puede hablar de un delito informático como tal, sino a partir de 1983 cuando Gerald Wondra a los 22 años accedió ilegalmente a los sistemas informáticos de las entidades bancarias de Estados Unidos y realizó llamadas fraudulentas con fines de

manipulación por lo que fue sentenciado a 24 meses de libertad condicional (Maricruz et al., 2021).

Es así que, el primer país en investigar y juzgar este tipo de delitos fue Estados Unidos, el cual, a partir de 1986 instauró la Ley de Fraude y Abuso de Computadoras, cuerpo normativo en el que precisó la protección de los sistemas informáticos prohibiendo "el acceso no autorizado a los sistemas de computación, la alteración o destrucción de datos, el uso indebido de computadoras para fines delictivos, el fraude informático y la extorción con fines económicos a través de medios tecnológicos" (Ley de Fraude y Abuso de Computadoras, 1986).

En la legislación ecuatoriana, si bien no se tiene registro de los primeros delitos informáticos relevantes de la historia, la regulación de las conductas delictivas relacionadas al uso de medios informáticos es relativamente nueva. El primer paso hacia la búsqueda de la evolución normativa enfocada a la seguridad cibernética inicia en 1990 con el proyecto de Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas conocida como Ley. 67, ley que fue debidamente aprobada en 2002, hasta entonces el país no contaba con una legislación específica en esta materia.

Es así que, la ley mencionada agregó el término de "infracciones informáticas" con un carácter propiamente administrativo que permitió la tipificación de varias conductas con la implementación de una reforma al Código Penal que se encontraba vigente en ese mismo año, en este sentido se reguló el acceso no consentido a un sistema de seguridad informático, la obtención y utilización no autorizada de información, la supresión, destrucción o supresión de documentos contenidos en un sistema informático, la falsificación electrónica, los daños informáticos, apropiación ilícita y demás actos delictivos que impliquen la utilización de medios electrónicos o tecnológicos (Ley de Comercio Electronico, Firmas y Mensajes de Datos, 2002).

Posterior a ello, se promulga la Constitución de la República del Ecuador en 2008, cuerpo constitucional en el que se reconoce el derecho a la protección de datos de carácter personal, el acceso a la información pública, la propiedad intelectual, la intimidad, la inviolabilidad y el derecho al secreto de la correspondencia física y virtual; lo que podría considerarse como un avance significativo en el reconocimiento de los derechos inherentes a la protección de la información y la base de datos (Constitución de la República del Ecuador, 2008).

Como otro dato histórico, para el año 2009, se establece la Secretaría Nacional de Inteligencia (SENAI) como un organismo encargado de coordinar el Sistema Nacional de Inteligencia de las Fuerzas Armadas y la Policía Nacional con la finalidad de llevar a cabo las labores de contrainteligencia a nivel estratégico y operacional, la seguridad interna del presidente de la república y los sistemas de inteligencia encaminados a protección y defensa nacional del Ecuador (Alvarado, 2020).

Para 2014, entra en vigor el Código Orgánica Integral Penal en adelante llamado (COIP) con un nuevo marco normativo que ordena los tipos penales, regula el sistema penitenciario y establece el procedimiento penal en un solo cuerpo jurídico. Es entonces que, a partir de que el COIP entra en vigor el título V de la Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas denominado "Infracciones informáticas" es derogado con sus respectivos artículos del 57 al 64 por la Disposición Derogatoria Novena de la Ley No. 00, publicada el 24 de febrero de 2014 (Código Orgánico Integral Penal[C.O.I.P], 2014).

A partir de 2017, Ecuador entra en un estado crítico y es atacado con mayor fuerza por los cibercriminales quedando en tercer lugar de afectación en América Latina por el virus Wannacry, el cual en 2019 filtró la información perteneciente a 17 millones de ecuatorianos. La empresa de seguridad VPNMentor de Israel determinó que "la falla de seguridad hizo que la información se instaure en un servidor público de Miami, lo que hace que este ataque informático sea catalogado como la más grande filtración de seguridad en América Latina"(Alvarado, 2020, p.21).

En 2019, Ecuador fue víctima de más de 40 millones de ataques de hacking, que en su mayoría afectaron a los portales web de las entidades públicas y causó graves intermitencias en la atención al público; el país paso de ocupar el puesto 56 y alcanzó el puesto 25 en la escala de los países más vulnerables a nivel mundial, hasta este entonces se desconocía sobre el cibercrimen y se veían estos acontecimiento como un evento lejano a la realidad ecuatoriana (Villacís, 2022).

A partir de 2020, las mismas instituciones del Estado, se vieron perjudicadas por los delitos informáticos los cuales se han presentado como un mecanismo de ciberterrorismo o ciberguerra por medio de ataques a la infraestructura de los servicios públicos, infecciones mediante malware, la corrupción de datos y la apropiación fraudulenta de fondos (Salazar et al., 2021).

En respuesta a estos hechos, en el año 2021, la Asamblea Nacional promulga la Ley Orgánica Reformatoria del COIP para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos, por medio de la cual se logra agregar a este código los siguientes tipos penales: revelación de secreto o información personal de terceros, interceptación ilegal de datos, ataque a la integridad de sistemas informáticos, acceso no consentido a un sistema informático, telemático o de telecomunicaciones y falsificación informática (Reforma al Código Orgánico Integral Penal [C.O.I.P], 2021).

A la par de esta actualización normativa, Ecuador presenta la primera Agenda Digital como un instrumento de política pública con el objetivo de impulsar la transformación digital del país enfocada al fortalecimiento de la unión de la ciudadanía digital y el uso adecuado de las herramientas tecnológicas a favor de la educación, el marco jurídico y la sociedad en general. Además, implementa la Ley Orgánica de protección de datos personales con el objetivo de "garantizar el derecho a la protección de datos, el acceso a la información y datos personales, la decisión sobre esta información y su protección comprendiendo los principios,

mecanismo y obligaciones relacionados a la tutela de este derecho" (Ley Orgánica de Protección de Datos Personales, 2021).

Para 2022, mediante la Resolución No. 34 FGE-2022 se establecieron las directrices, atribuciones y designaciones para la conformación de la Unidad Nacional Especializada en Investigación de Ciberdelito, la cual fue creada con la finalidad de investigar los delitos informáticos que se encuentran tipificados en el COIP en el apartado de los delitos contra la seguridad de los activos de los sistemas de información y comunicación, la cual se integra en su sede única en la ciudad de Quito con un ámbito legislativo a nivel nacional, con la posibilidad de extenderse a futuro a otras provincias por necesidad institucional (Resolución No. 34 FGE-2022, 2022).

Dicha resolución establece que la Unidad Nacional Especializada en Investigación de Ciberdelito está conformada por un agente fiscal coordinador, agentes fiscales, secretarios y asistentes. Dentro de las atribuciones asignadas a esta unidad se encuentran: coordinar y orientar las investigaciones de los delitos informáticos en el territorio nacional; asesorar y dar seguimiento a las actuaciones de las demás unidades especializadas; y dirigir las actuaciones de las instituciones encargadas de la prevención contra el fenómeno criminal.

Cabe destacar que, para la asignación de las noticias del delito a esta unidad, previo a la apertura de la investigación previa o durante la misma, se lleva a cabo un análisis preciso para determinar que se cumplan con los siguientes parámetros: que se trate de un crimen organizado transnacional, que afecte gravemente a la seguridad del Estado o paralice un servicio público. Una vez que se identifique uno o varios de estos parámetros el fiscal general del Estado de manera motivada asignará la noticia del delito a la Unidad Nacional Especializada en Investigación de Ciberdelito, caso contrario será devuelto a la fiscalía de origen para que continúe con la investigación (Resolución No. 34 FGE-2022, 2022).

Finalmente, la siguiente tabla muestra una recopilación de datos sobre el número de denuncias receptadas desde el año 2017 a mayo de 2024 referente a los delitos informáticos.

Tabla 1.

Estadística de los delitos informáticos en Ecuador

Art. COIP	Tipo Penal	2017	2018	2019	2020	2021	2022	2023	2024
229	Revelación ilegal de la base de datos	22	44	34	30	23	63	29	20
230	Interceptación ilegal de datos	63	41	86	73	67	79	61	40
231	Transferencia electrónica de activo patrimonial	54	37	50	76	212	117	163	83
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	125	200	174	112
233	Delitos contra la información pública reservada legalmente	14	12	5	5	8	5	5	0

234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	419	354	490	370
234.1	Falsificación informática	-	-	-	-	-	24	67	53
190	Apropiación fraudulenta por medios electrónicos	959	1448	1744	2280	5235	3136	3447	1562
	Total	**3432**	**3922**	**4291**	**4874**	**8110**	**6000**	**6459**	**2240**

Nota: La tabla muestra datos con datos proporcionados por el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado sobre los delitos informáticos desde el año 2017 hasta mayo de 2024. Autoría propia (2024)

2.2.1.3. Realidad procesal en la investigación de los delitos informáticos

Cuando se habla sobre la realidad procesal y los principales obstáculos tanto teóricos como prácticos para llevar a cabo una adecuada investigación e imputación de los delitos informáticos en un sentido amplio se debe tomar en cuenta que las nuevas tecnologías han desafiado los conceptos jurídicos tradicionales, de manera que, las conductas delictuales se han vuelto más complejas, menos predecibles e incluso indetectables (Nadareishvili et al., 2022).

Los desafíos que deben considerarse son: la desactualización normativa, el exceso de información y mínima intervención en el tratamiento de datos de las entidades públicas y privadas, la falta de mecanismos de regulación en el procesamiento de datos, el exceso de confianza del usuario y titular de la información al entregar el consentimiento informado de sus datos de manera desmedida consecuencia de la no lectura de las políticas de privacidad y las sanciones insuficientes de las conductas que vulneran la protección de datos (Rosas & Pila, 2023).

En relación a ello, la Fiscalía del Estado ecuatoriano enfrenta diferentes retos para combatir los delitos informáticos como: la normativa ecuatoriana desactualizada en materia de delitos informáticos y el tratamiento de la evidencia digital, la falta de capacitación del personal que interviene en la investigación de este tipo de delitos, la poca instrucción a la ciudadanía sobre las leyes y protocolos que contrarrestan el delito informático, la falta de recursos tecnológicos y la infraestructura adecuada para la investigación y la ausencia de tratados internacionales y convenios que permitan la investigación de los delitos transnacionales (Ortiz, 2019).

Con estos antecedentes, uno de los principales retos que enfrenta el Ecuador relacionados a los ciberdelitos es la falta de información trascendente y confiable acerca de la problemática, las investigaciones, detenciones, juicios y sentencias lo que dificulta cuantificar el impacto real de este tipo de delitos en la sociedad ecuatoriana (Ortiz, 2019). Sin embargo, se puede hablar de otros retos significativos como los que se describen a continuación:

Falta de conocimientos técnicos informáticos. Se debe tomar en cuenta que la investigación de este tipo de delitos requiere un alto nivel de conocimientos en el mundo de la informática por lo que este hecho es el principal obstáculo que vive el Ecuador debido a

que las tecnologías de la información y comunicación son complejas y normalmente desconocidas en el campo de la justicia penal tradicional. El desconocimiento y poca experiencia de los servidores del sistema policial y fiscal referente a las modalidades delictuales en espacios digitales dificulta la capacidad de investigación forense digital requerida para la admisibilidad de la prueba en los tribunales (Tamayo & Delgado, 2023).

Más del 70% del cuerpo policial no ha recibido capacitación orientada al procedimiento investigativo de este tipo de delitos sobre el acompañamiento a víctimas para efectuar la respectiva denuncia e incluso a las entidades que debe acudir; además, el 90% de este no ha recibido información sobre el tratamiento y preservación de la evidencia digital, lo que revela que el personal policial parece estar poco preparado para responder a incidentes informáticos (Tamayo & Delgado, 2023).

Mal manejo de la evidencia digital. Por la naturaleza volátil de la evidencia digital, esta es susceptible de eliminación, supresión y alteración, de manera que si no existe dominio científico de las técnicas de obtención, conservación, recuperación y resguardo digital o no se lleva a cabo una cadena de custodia impecable no se podrá preservar esta información e incluso la escena del delito. En este sentido, las malas prácticas durante la producción de la prueba son comunes en el proceso investigativo, por lo que uno de los problemas más frecuentes es la falta de selección adecuada de la evidencia digital como prueba para el juicio oral, la cual muchas veces no es practicada en su totalidad a causa de la renuncia expresa de las partes (Salazar et al., 2021).

Falta de estrategias metodológicas. Las estrategias metodológicas facilitan la creación de principios y criterios por medio de técnicas, métodos y sobre todo procedimientos que describen una secuencia de pasos ordenados y planificados para cumplir un fin en común. En la realidad que vive el país no existen estrategias metodológicas que faciliten la búsqueda, obtención, recolección y preservación de la evidencia digital de los delitos cibernéticos cometidos mediante el malware; esta deficiente planificación compromete la capacidad de presentar pruebas sólidas y asegurar un peritaje técnico-científico correcto dentro de la materia de estudio (Salazar et al., 2021).

En este sentido, la ausencia de la planificación en la investigación judicial en el ámbito de los delitos cibernéticos es indiscutible. La ausencia de cooperación interdisciplinaria y colaboración efectiva entre diferentes áreas de expertos, como la ingeniería, el derecho y la informática forense entorpece la comprensión del delito, la recolección de evidencia y la construcción de un caso sólido (Salazar et al., 2021).

Transnacionalidad del delito. Los delitos informáticos ocurren en el espacio digital, de manera que el perpetrador tiene la facilidad de realizar sus actos a pesar de encontrarse en un lugar físico distinto al de la víctima incluso llegando a atravesar fronteras internacionales, además, suele usar seudónimos o encubrir su identidad, lo que complica la investigación y la identificación del actor del hecho delictivo en la búsqueda de la asociación de la dirección IP del dispositivo de la persona física (Salazar et al., 2021).

Desactualización normativa. El crimen informático plantea retos importantes para la legislación. La incapacidad de las leyes tradicionales para adaptarse a las nuevas modalidades delictivas en el campo digital crea una problemática a nivel mundial en la "la interpretación subjetiva de las leyes y la brecha de conocimiento en torno a los delitos cibernéticos" (Diaz et al., 2023).

Se puede afirmar con certeza que la legislación ecuatoriana, en muchos casos no prevé tipos penales específicos, sino que los sanciona con la tipología de otros delitos parecidos. En este sentido, de acuerdo con Lanas y Cárdenas (2022) las actividades de: pharming, phishing, sexting, grooming, baiting, redes trampa, email spoofing y malware (virus, troyano, spyware, ransomware, gusano, adware); no se contemplan como tipos penales autónomos y específicos.

Las modalidades delictivas avanzan y la legislación no logra seguir su paso. La normativa procesal no determina que las personas naturales y las entidades tanto públicas como privadas entreguen inmediatamente a las autoridades judiciales su información, banco de datos y sistemas informáticos a partir de los cuales se pudo haber infiltrado la información o se generó la posible comisión del delito e incluso lo almacenen por cierto tiempo con fines investigativos (Salazar et al., 2021).

La ausencia de un marco regulatorio sobre la recolección, mantenimiento, preservación y admisibilidad de la prueba electrónica genera dificultades en el juzgamiento de los sospechosos de ilícito creando una falta de prueba útil, pertinente y conducente para determinar la responsabilidad y la materialidad del delito y por ende no se obtiene una sentencia condenatoria ni la reparación de la víctima (K Malik & Choudhury, 2020).

2.2.1.4. Alcance de la normativa jurídica ecuatoriana en los delitos informáticos

Considerando el orden jerárquico de las normas jurídicas ecuatorianas, la norma suprema del Estado es "la constitución", en la cual se reconoce a ciertos derechos como: el derecho al acceso universal a las tecnologías de la información y comunicación (Art. 16), el derecho a la protección de datos personales de carácter personal que comprende el acceso, recolección, determinación, archivo, procesamiento, difusión y protección de la información personal (Art. 66, n.19) y el derecho a la intimidad personal y familiar (Art. 66, n.3) (C.R.E., 2008).

En relación con los convenios internacionales Ecuador mantiene vínculos con el convenio de Berna y el convenio de París relacionados a los derechos de autor, el convenio internacional de telecomunicaciones y protocolos adicionales para la solución de conflictos. Sin embargo, el Ecuador es uno de los pocos países que no ha suscrito el convenio de Budapest, lo cual ha limitado la lucha con el cibercrimen y la cooperación internacional en la investigación y persecución este tipo de delitos (Ortiz, 2019).

Por otra parte, el COIP dedica el capítulo tercero (delitos contra los derechos del buen vivir), en la sección tercera (los delitos contra la seguridad de los activos de los sistemas

de información y comunicación) comprendiendo los artículos 229, 230, 231, 232, 233 y 234 para tratar sobre los delitos informáticos, los cuales son descritos a continuación en la tabla 2; sin embargo, no tratan la conducta del malware de manera directa y específica.

Esto sucede debido a que, los artículos mencionados se refieren directamente a la manipulación directa o acceso no consentido a los sistemas informáticos, sin prever el uso de un software malicioso como una herramienta autónoma que facilita la comisión de varias acciones malintencionadas aprovechando el desconocimiento y vulnerabilidad de los usuarios. Los tipos penales existentes no abordan técnicas de ataques de malware como: el cifrado de datos y documentos electrónicos; anuncios, códigos y archivos maliciosos; ataques directos a la privacidad mediante las técnicas de spyware o adware; clonación de páginas web y aplicaciones legítimas; suplantación y falsificación de direcciones IP; y softwares de vigilancia de actividades de navegación, ubicación o comunicación sin consentimiento.

Tabla 2.
Delitos informáticos reconocidos en el COIP

Art. COIP	Tipo Penal	Pena Privativa de Libertad
229	Revelación ilegal de la base de datos	1 a 3 años
230	Interceptación ilegal de datos	3 a 5 años
231	Transferencia electrónica de activo patrimonial	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	3 a 5 años
233	Delitos contra la información pública reservada legalmente	5 a 7 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años
234.1	Falsificación informática	3 a 5 años
190	Apropiación fraudulenta por medios electrónicos	1 a 3 años

Nota: La tabla muestra los delitos informáticos que se encuentran reconocidos por el COIP a partir de la reforma de 2021. Autoría propia (2024)

Cabe destacar que el COIP no tipifica ni hace mención a los nuevos delitos informáticos como el ciberbulling, ciberataques, venta ilegal en internet, subastas electrónicas y uso ilícito de las inteligencias artificiales (Ortiz, 2019). Además, se evidencia una falta de reconocimiento de las categorías delictivas perpetradas mediante softwares maliciosos, debido a que estos están fuera del alcance de la aplicación del derecho penal, al no ser contemplados en la normativa jurídica (Rossinskaya & Ryadovskiy, 2020).

Siguiendo con el orden piramidal jerárquico del estudio y aplicación de la normativa ecuatoriana, se considera a la ley de Comercio Electrónico, Mensaje de datos y Firmas Electrónicas, la cual tiene como fin de regular todo lo concerniente al comercio electrónico por lo que se fundamenta en establecer un marco legal dirigido a la contratación electrónica

y telemática, servicios electrónicos, firmas electrónica, la comunicación de datos y la protección de los usuarios de estos sistemas; de manera que, su promulgación dio un paso gigantesco en el reconocimiento de la necesidad de que Ecuador se preocupe por la regulación del espacio digital, la seguridad cibernética y el cibercrimen (Fernández & Vázquez, 2022).

Finalmente cabe destacar, que el país no cuenta con manuales y protocolos específicos para llevar a cabo los procedimientos investigativos entre la Fiscalía y la Policía Judicial en los delitos informáticos cometidos mediante la herramienta del malware. Además, existe la ausencia de manuales de evidencias digitales para entornos informáticos, dando como resultado una significativa laguna jurídica en el marco normativo nacional. Esto se refleja en los Manuales de Protocolos Instructivos de Medicina Legal y Ciencias Forenses, donde dentro de los manuales presentados se limitan a tratar temas de medicina legal pero no se trata la informática forense a pesar de ser una rama de las ciencias forenses. La ausencia de estos protocolos deja a los peritos informáticos sin guías claras y estandarizadas para la recolección, preservación y análisis de evidencias digitales en casos de malware (Carrers & Aguilar, 2020).

En el país existe una latente necesidad de adecuar los procesos que efectivicen la recolección y conservación de evidencia digitales. Además, que requiere reconocer lazos de cooperación que permita la formación y capacitación del recurso humano en tema de delitos informáticos, esa falta de manuales y protocolos acerca de la cadena de custodia de la evidencia digital da como consecuencia "la ineficacia de la norma" pues al no existir elementos de convicción para acusar o no a un sujeto, "la impunidad será el día a día de la justicia" (Carrers & Aguilar, 2020, p.8).

2.2.2. UNIDAD 2: EL MALWARE EN EL ECUADOR

2.2.2.1. Definición y tipología del malware

Definición

El Malware es un tipo de software malicioso que esta creado por piratas informáticos, con el fin de dañar los recursos de la computadora, sustraer información importante y tener acceso completo a la máquina de destino. Este tipo de ataque busca para inyectar códigos maliciosos al sistema, de tal forma que lo infecte para continuar con su tarea. Siendo así que los piratas informáticos utilizan servidores o páginas web que presentan vulnerabilidades en sus sistemas, para distribuir malware a los usuarios y así acceder a la información (Toapanta et al., 2020).

Malware es un tipo de ciberataque en forma de software malicioso. Las familias de malware incluyen virus, ransomware, gusanos y software espía. Sus fines comunes son la sustracción de información, suplantación de identidad, el espionaje y la interrupción del servicio (Agencia de Ciberseguridad de la Unión Europea [ENISA], 2020).

La mayoría de los métodos de delitos informáticos se basan en el acceso no autorizado a la computadora, instalaciones y sistemas obtenidos a través de malware que, de hecho, actúa como arma criminal. Los delincuentes se esfuerzan por ocultar al usuario la descarga, instalación y actividad del malware que no puede auto propagarse. Actualmente no existe malware cuyas funciones incluyan solo un tipo especifico de acciones, la mayoría contiene una combinación de varios tipos de acciones implementadas a través de una arquitectura de módulos, lo que ofrece a los delincuentes amplias oportunidades para manipular la información (Rossinskaya & Ryadovskiy, 2020).

Tipos de Malware

Hay que considerar que el Malware se presenta de diferentes formas, haciendo de cada una muy específica en su intención maliciosa.

- **Virus:** es un tipo de malware que infecta directamente archivos ejecutables o sectores de arranque del sistema, generando un comportamiento distinto a su propósito previsto. Siendo así que se replica adjuntando su código a otros archivos ejecutables, programando la infección a distintos sistemas cuando el archivo infectado se comparte o transfiere (Radu, 2023).
- **Gusano:** los gusanos son un tipo de malware autorreplicable que se propaga a través de redes, aprovechando las vulnerabilidades del sistema para expandirse de una computadora a otra. Cabe destacar que, el virus se diferencia del gusano ya que estos no requieren un programa anfitrión para propagarse, sino que pueden replicarse y propagarse de forma autónoma. Además, los gusanos pueden causar congestión en la red y ralentizar los sistemas informáticos al consumir recursos del sistema, y también pueden usarse para sustraer información confidencial de los sistemas infectados (Radu, 2023).
- **Troyano:** también se lo denomina caballo de troya, este tipo de malware tiene apariencia de programa legítimo para engañar a los usuarios para que lo descarguen o instalen. Una vez instalado, el troyano puede brindarle al atacante acceso remoto al sistema infectado, por lo cual le permite sustraer datos confidenciales, instalar otro malware o utilizar el sistema infectado como parte de una botnet (ordenadores o dispositivos). Cabe destacar que el método clave para distribuir este tipo de malware es el envío masivo de correos electrónicos con archivos adjuntos disfrazados de contenido útil. La clasificación de los programas maliciosos según su forma y método de programación (virus, gusanos, troyanos) (Radu, 2023).
- **Ransomware:** este tipo de malware, es aquel que cifra los archivos de la víctima, haciéndolos inaccesibles hasta que se pague un rescate al atacante. Se puede distribuir a través de archivos adjuntos de correo electrónico, sitios web infectados o ataques de ingeniería social. Cabe destacar que los ataques de ransomware dirigidos al sector público aumentaron en 2019 debido a su capacidad de pagar rescates más altos (Radu, 2023).

  El ransomware es la amenaza cibernética más predominante en la infraestructura digital. Estos ataques utilizan diferentes técnicas para secuestrar los archivos y recursos de los usuarios u organizaciones y exigir un rescate a cambio de liberar los datos o recursos cifrados. Aunque existen muchos ataques de malware, el

ransomware se considera el más peligroso, creando desafíos para rastrear al atacante o las redes de los atacantes (Reshmi, 2021).

- **Adware:** es un tipo de malware, que se muestra en anuncios no deseados en el ordenador de la víctima, normalmente en forma de ventanas emergentes o banners. Además, puede ralentizar la computadora de la víctima, consumir ancho de banda y rastrear la actividad en internet del usuario (Radu, 2023).
- **Spyware:** es un tipo de malware que se monitorea en secreto la actividad informática de la víctima y recopila información confidencial, como credenciales de inicio de sesión, información bancaria y datos personales. Se lo considera como el software espía, puede utilizarse para la suplantación de identidad, el fraude financiero y el espionaje. A su vez, puede distribuirse a través de sitios web infectados, archivos adjuntos de correo electrónico o ataques de ingeniería social (Radu, 2023).

2.2.2.2. Evolución y modus operandi del malware

Las armas cibernéticas fueron reconocidas entre 2010 y 2012, donde los primeros tipos de malware se presentaron en forma de virus informáticos como Stuxnet, Flame, Duqu y Gaus, identificados principalmente en Irán y posterior a ello se expandieron a diferentes países del mundo adquiriendo nuevas modalidades y variaciones. Para finales de 2011 inicia la aparición de troyanos como Wiper, el cual llegó a destruir gran cantidad de bases de datos de varias empresas internacionales sin la posibilidad de ser recuperados (Márquez Díaz, 2017).

Para los siguientes años, se produjo en aumento significativo de la creación, desarrollo y actualización de los distintos tipos de malware. Posteriormente, para 2019 el 94% de los tipos de malware comenzaron a distribuirse a través de correo electrónico, siendo este medio el principal punto de entrada; en consecuencia, durante los últimos años la evolución del software malicioso ha incrementado la posibilidad de la corrupción de datos, el secuestro de información y la producción de otros delitos cibernéticos mediante el ataque progresivo de malware (Aboaoja et al., 2022).

En Ecuador, se conoce sobre el malware a partir de 2020, cuando la empresa de seguridad ESET reportó que país ocupa el sexto lugar de posición entre los países latinoamericanos con más indicios cibernéticos producidos por malware después de Brasil, México, Argentina, Colombia y Perú (Ávila, 2022). Pero para 2024, según estudios de la empresa de seguridad Check Point, el país se encuentra en una posición preocupante frente a amenazas cibernéticas dirigidas mediante malware, de manera que presenta un riesgo de 51,9%, ubicándose como el tercer país más vulnerable a estos ataques después de Perú y Colombia (El Universo, 2024).

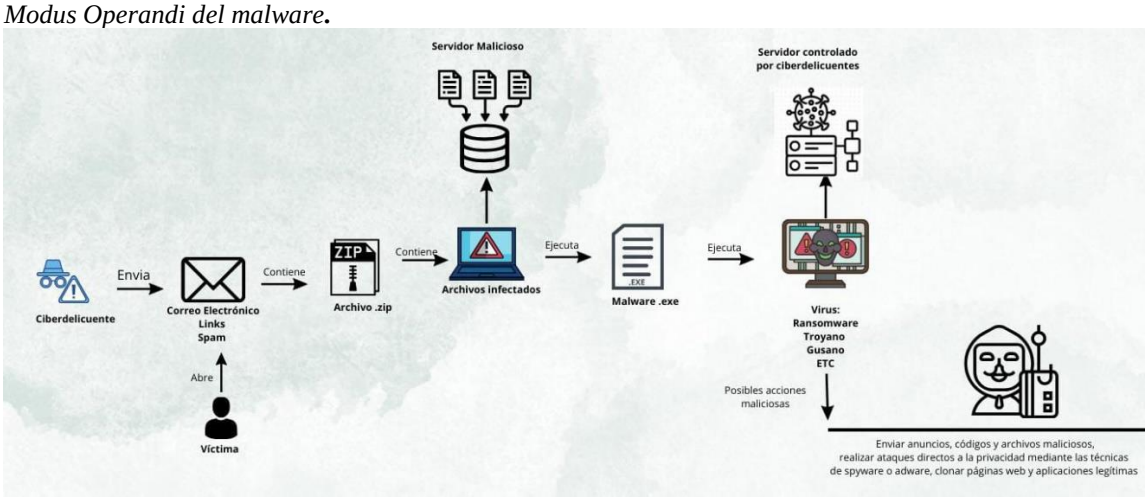
En efecto, el malware es considerado como la mayor amenaza para la ciberseguridad por su clasificación en categorías que incluyen los gusanos, troyanos, ransomware y demás virus que operan causando daño directo a los sistemas informáticos o sustrayendo información reservada. A partir de 2022 este tipo de ataque informático es el más común en

los dispositivos, por lo que ha tenido un incremento del 22,9% en comparación a otros años (Aboaoja et al., 2022).

En el pasado, el malware se producía para efectuar una sola operación con fines simples y sencillos de detectar, sin embargo, el malware moderno utiliza técnicas más destructivas y es más complicada su detección llegando incluso a esquivar los softwares de protección y antivirus. Para tal efecto, el modus operandi del malware actual combina las técnicas del malware original para efectuar múltiples procesos y persistir en el sistema creando accesos dirigidos y combinando varias tipologías durante la ejecución de un ataque informático (Aslan & Samet, 2020).

En tal razón, el malware pone en peligro la seguridad de los sistemas informáticos y puede actuar de diferentes formas para infiltrarse en ellos de acuerdo a su tipo. Entre las acciones más comunes son: el acceso ilegítimo a un sistema informático; la sustracción de datos, contraseñas e información personal y financiera; el secuestro de la información o archivos (ransomware), la vigilancia o espionaje del dispositivo (spyware), extorción y denegación del servicio; sin embargo, todos los tipos de malware siguen un modus operandi que inicia con la descarga o instalación de un software malicioso de manera involuntaria que implica abrir un archivo o enlace infectado de un correo electrónico, mensaje o de una página web para luego actuar de acuerdo a su tipología y funcionalidad, como se describe en la figura 2 (Belcic, 2023).

Figura 2.
Modus Operandi del malware.



Nota: La figura describe el modus operandi del malware en una computadora. (Guía de Ciberataques, 2020)

El software malicioso permite que el infractor como usuario no legítimo ingrese a un sistema sin ser reconocido como intruso. Algunas veces está infiltrado en las imágenes digitales lo que le permite hacer varias actividades, desde recopilar información hasta ejecutar un ataque de denegación del servicio (Alodat, 2022). Además, existen aplicaciones de malware que están compitiendo fuertemente en el mercado con aplicaciones legítimas y legales, lo que hace que estas tengan mayor apertura de anuncios que encubren la ejecución del malware y mediante esta modalidad sustraer información y las credenciales bancarias por medio de enlaces maliciosos camuflados (Nehinbe, 2022)(McAfee, 2021).

Sin embargo, el malware también se puede ejecutar sin la necesidad de emplear archivos adjuntos evadiendo los filtros de seguridad más comunes con mayor probabilidad de éxito. Por consiguiente, este tipo de malware se inyecta por medio de un código malicioso en un software existente y confiable para producir sus efectos, ya sea al instalar un aplicativo o al descargar un documento. Este tipo de ataques imperceptibles ha incrementado un 65% a partir de 2019 (ENISA, 2020).

Conforme a ello, el malware tiene canales de programación definidos, los cuales se clasifican en pasivos y activos. Los canales pasivos hacen que este se propague a través de una flash o USB, mientras que, la intrusión directa del malware se efectúa mediante la vulnerabilidad de la misma red, por medio de correo electrónico, archivos adjuntos maliciosos, códigos java, páginas web infectadas, publicidades, navegadores, etc. Esto indica que el malware busca aprovechar cualquier medio para vulnerar la seguridad de cualquier tipo de sistema informático (Márquez Díaz, 2017).

Pero el modus operandi más común de malware es el que distribuye sus aplicaciones por medio de mensajes o enlaces en sitios populares de las redes sociales. También, es muy común el uso de malwares bancarios los cuales se insertan en las aplicaciones de banca móvil o enlaces dirigidos encubiertos por medio de los cuales el infractor tiene acceso total al dispositivo, accede a los datos del usuario y contraseña de los servicios bancarios e incluso descarga más componentes. Esta modalidad de malware se resume en la funcionalidad y operación de los troyanos bancarios que mediante un mecanismo de mensajes alerta al usuario de una actualización de una aplicación conocida con el fin de infiltrarse en la descarga e instalación de la misma (McAfee, 2021).

2.2.2.3. Naturaleza del malware como herramienta delictiva para cometer delitos informáticos

Considerando que un arma modificada puede emplearse para fines ilícitos, es decir un programa legal adaptado puede aplicarse debido a su funcionalidad a aportar a la delincuencia las oportunidades para alcanzar sus objetivos; el malware se presenta como una herramienta modificada a favor de la delincuencia informática, la cual brinda una serie de oportunidades a los ciberdelincuentes para llevar a cabo su comisión delictiva (Rossinskaya & Ryadovskiy, 2020).

Desde luego, el malware se ha considerado como una amenaza persistente avanzada (APT) siendo catalogada internacionalmente como una de las primeras armas cibernéticas capaces de comprometer gravemente la infraestructura digital de uno o más países; es así que por sus características y potencialidades puede atacar cualquier sistema informático convirtiéndose un arma potencialmente inteligente en manos de criminales informáticos (Márquez Díaz, 2017).

De este modo, en su mayoría los delitos informáticos se fundamentan en la acción típica del acceso no autorizado a una plataforma digital, sistemas informáticos o infraestructura digital, hecho que se logra por medio del malware (Rossinskaya & Ryadovskiy, 2020). En

tal razón, las aplicaciones de malware se han creado con fines propiamente intrusivos o criminales, sus creadores los han desarrollado para utilizarlos para estafar, sustraer, eliminar o corromper sistemas y bases de datos (Nehinbe, 2022).

El acceso no autorizado a los sistemas informáticos mediante el uso de malware se efectúa por medio de un código malicioso que puede ser considerado como un instrumento para la comisión del delito informático. La metodología y naturaleza de este tipo de delitos suele ser estructurada de manera que se logra reconocer las fases de preparación, ejecución y ocultamiento del mismo (Rossinskaya & Ryadovskiy, 2020).

Para ejemplificar, se puede hablar de un delito informático de malware aquel que se realiza mediante una aplicación de malware para ingresar de manera ilícita a un sistema informático de una persona natural o jurídica con la finalidad de sustraer, modificar, corromper o eliminar la información del mismo (Nehinbe, 2022).

La naturaleza del malware como una nueva herramienta delictiva puede ejecutarse por medio de un correo electrónico que infecta con un virus malicioso con el objetivo de alterar un sistema informático borrando, falsificando o destruyendo datos (Salazar et al., 2021). Este método que distribuye las infecciones de malware es más común en la actualidad por lo que se insiste a la ciudadanía que evite o rechace totalmente efectuar acciones imprudentes, no abra un archivo adjunto no deseado, no ingrese a correos electrónicos desconocidos y no ingrese a enlaces sospechosos (Rossinskaya & Ryadovskiy, 2020).

En tal sentido, es importante señala que, un delincuente cibernético que tiene por objetivo ejecutar un hecho ilícito que implique la vulneración de un sistema informático con fines lucrativos lo lleva a cabo consciente o inconscientemente un proceso que inicia con el análisis de la víctima a quien irá dirigido el ataque, el desarrollo de la creación del código malicioso o el mecanismo de ataque, la propagación planificada del malware mediante una interacción con el usuario que por lo general se resume un hecho de ingeniería social, la infección y la recolección de datos (Jumbo, 2017). Este proceso se resume en la figura 3 titulada como “Ciclo de un ataque de malware”.

Figura 3.
Ciclo de un ataque de malware

Nota: La figura muestra el ciclo de un ataque informático de malware. Jumbo (2017)

En este contexto, el malware como una herramienta que contribuye al crimen permite el acceso y manipulación de la información que reposa en los bancos de datos y programas perjudicando los intereses y patrimonio de la víctima. Además, debido a su naturaleza resulta difícil averiguar el autor del hecho delictivo si este ha utilizado estrategias sofisticadas para encubrir su identidad y sus actividades ilícitas, de manera que la obtención de elementos de convicción que permitan determinar la materialidad del ilícito y la responsabilidad o individualización del sospecho dentro de un proceso penal resulta ser un asunto complejo (Salazar et al., 2021).

En este caso, el uso del malware para fines ilícitos puede ser considerado dentro del ámbito penal como una herramienta para la comisión de delitos, pero también como un delito en sí mismo. Por un lado, se califica al malware como una herramienta delictiva cuando el software dañino resulta ser el componente esencial que permite el cometimiento del delito, es decir, sin su aplicación, no existiría el delito; mientras que, también se debe considerar al malware como un delito, aunque no produzca un daño informático, es decir, cuando se cree, adquiera, importe o facilite a terceros un programa o código malicioso adaptado para cometer este tipo de delitos informáticos (Peláez, 2022).

2.2.2.4. Bienes jurídicos lesionados con el impacto del malware

La aparición del malware en la actualidad ha llevado a convertirse en un campo crucial para la ciberseguridad, ya que opera en un entorno de confrontación en el que los ataques evolucionan constantemente en sus tácticas. Siendo así que la naturaleza de malware implica que el impacto puede ser de manera amplia, afectando tanto a personas naturales, jurídicas, instituciones u organizaciones (Me et al., 2023). Los bienes jurídicos lesionados por el impacto del malware son:

Confidencialidad de la información. La confidencialidad de la información es la protección de la información contra el acceso no autorizado. El malware, troyanos y el spyware, pueden infiltrarse en los sistemas y acceder a datos sensibles sin el consentimiento del propietario. De acuerdo con investigaciones actuales, el 58% de los sucesos de malware resultan en la exhibición de información confidencial (Mazurczyk & Caviglione, 2015).

Integridad de la información. El malware es una amenaza para la integridad de la información, ya que estos ataques pueden alterar o destruir datos, comprometiendo su fiabilidad, exactitud y completitud. A su vez es la precisión, la coherencia y confiabilidad de los datos dentro de un sistema y al mismo tiempo defenderse contra diversas amenazas maliciosas como es el ransomware, la corrupción de datos y los ataques internos(Cawthra et al., 2020).

Disponibilidad de la Información. Los ataques a través del malware, específicamente en el ransomwore pueden cifrar datos y sistemas impidiendo el acceso hasta que se cancele por el pago, cabe destacar que la disponibilidad asegura que la información este accesible cuando sea necesario. El malware, utiliza técnicas de ocultación de información para encubrir su existencia, haciendo más difícil de detectar. Además, hay que

destacar (ransomware) que puede permanecer oculto durante un largo periodo de tiempo, mientras que de manera lenta y continua sigue filtrando datos confidenciales de los usuarios (Mazurczyk & Caviglione, 2015).

Privacidad. El malware que infringe la privacidad es una clase cada vez mayor de aplicaciones maliciosas que intentan sustraer datos confidenciales y filtrados a terceros. Siendo así que, la actividad común realizada por el malware que viola la privacidad es el registro de teclas, es decir, la escucha, recolección y filtración de las pulsaciones de teclas emitidas por el usuario. La capacidad de ejecutarse, facilita su implementación y distribución, lo que pone de relieve la necesidad de contar con técnicas de detección eficaces (Ortolani et al., 2010).

Propiedad Intelectual. El malware puede también afectar a la propiedad intelectual, incluyendo secretos comerciales y datos de investigación, lo que resulta pérdidas económicas. Las aplicaciones de software malicioso, o también denominando malware es la causa principal de muchos problemas de ciberseguridad. Estas aplicaciones maliciosas, intencionalmente manipuladoras, intentan realizar actividades no autorizadas en nombre de sus creadores en las máquinas host por diversas razones, como la apropiación de tecnologías avanzadas y propiedades intelectuales, actos gubernamentales de venganza y manipulación de información confidencial, por nombrar algunos (Me et al., 2023).

2.2.3. UNIDAD 3: LA SEGURIDAD CIBERNÉTICA EN EL ECUADOR FRENTE AL IMPACTO DE NUEVAS MODALIDADES DELICTIVAS

2.2.3.1. Definiciones y antecedentes de la ciberseguridad frente a delitos informáticos

El término ciberseguridad o seguridad cibernética tiene un origen reciente como resultado de un proceso de globalización e innovación tecnológica que ha generado la necesidad de proteger la información y los datos personales de los usuarios de internet. Es así que, se instaura como un conjunto de operaciones destinadas a proteger la información de individuos y organizaciones que interactúan en el ciberespacio (Villacís, 2022). En otras palabras "la ciberseguridad se refiere a la preservación de la información en el espacio digital de manera íntegra, disponible y confidencial" (Rodríguez, 2021, p.20).

La ciberseguridad llega a postularse como un método de protección de los datos contra ataques, daños o accesos no autorizados por medio de estrategias, procesos y técnicas. Considerando que por medio de las redes informáticas se puede ser víctima de distintos tipos de delitos, se ha generado preocupaciones legales debido a que la interconexión de las actividades humanas cotidianas con recursos tecnológicos representa una vulnerabilidad considerable y constituye una amenaza constante de mala conducta, fraude, estafa y demás delitos informáticos en general (Sunil et al., 2021).

En Ecuador, a partir de 2021, la ciberseguridad se planteó como tendencia en los medios de telecomunicaciones por los constantes ataques informáticos a las empresas privadas y a las instituciones públicas, lo que hizo que se lo reconozca como un blanco fácil

para la ciberdelincuencia (Heredia, 2021). Desde entonces el país se encuentra en el puesto 82 del ranking National Cyber Security Index (NCSI) siendo calificado como un país con ciberseguridad deficiente (Alvarado, 2020).

Bajo esta perspectiva, Ecuador llega a definir a la ciberseguridad como la capacidad del Estado para proteger a los usuarios del ciberespacio y a su información frente a riesgos y amenazas existentes, además, se acoge al concepto entregado por la Unión Internacional de Telecomunicaciones (UIT) para entender a la seguridad cibernética como el conjunto de estrategias, herramientas, directrices, políticas y métodos aplicados para proteger los activos digitales de las personas naturales o jurídicas (Política Nacional de Ciberseguridad, 2021).

En tal sentido, la ciberseguridad está enmarcada como uno de los deberes constitucionales del Estado ecuatoriano y bajo la política nacional de Ciberseguridad incluye criterios y principios relacionados a la ciberdefensa y ciberinteligencia (Política Nacional de Ciberseguridad, 2021). Así también, define a la seguridad digital como el conjunto de "principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permiten preservar la confidencialidad, integridad, disponibilidad de la información en los entornos digitales manejados por las entidades públicas" (Reforma Norma Técnica Que Regula El Proyecto de Gobierno Electrónico, 2024, p.4).

Sin embargo, a pesar de que el país ha efectuado un esfuerzo por comprender la problemática de la ciberseguridad, aún no ha llevado a cabo un estudio determinante sobre la eficiencia de la normativa actual sobre los delitos informáticos que contempla el COIP y otras leyes relacionadas, así como el análisis del cumplimiento de estándares internacionales en la protección de derechos en el mundo digital. Además que, no cuenta con un marco regulatorio que integre a nivel nacional los requerimientos de la ciberseguridad, ciberdefensa y ciber inteligencia (Ávila, 2022).

Finalmente, es posible afirmar que el país cuenta con bajos niveles de madurez de las capacidades de ciberseguridad como se detalla en un diagnóstico de las capacidades de ciberseguridad efectuado por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, el Comité Nacional de Ciberseguridad y el Banco Mundial en 2022, donde se describen 5 dimensiones de estudio: estándares y tecnologías, políticas y estrategias de ciberseguridad, cultura cibernética y sociedad, desarrollo de conocimiento y capacidades en ciberseguridad , marcos legales y regulatorios. De estas dimensiones cabe recalcar que los factores que cuentan con un nivel de madurez inicial comprendido como muy bajo se encuentran: la respuesta a incidentes, la protección de la infraestructura digital, la investigación e innovación en ciberseguridad, marcos legislativos relacionados, capacidad y competencia legal y regulatoria, marcos de cooperación para combatir la delincuencia y controles de seguridad (Ávila, 2022).

2.2.3.2. Estrategias nacionales e internacionales sobre la seguridad cibernética ante el impacto de nuevas modalidades delictivas

Las estrategias de ciberseguridad nacionales o internacionales tienen una gran relevancia a la hora de abordar el panorama cambiante de las ciber amenazas, por ello los países de todo el mundo se centran cada vez más en mejorar su preparación para la ciberseguridad mediante el desarrollo de estrategias nacionales integrales de ciberseguridad. Con el fin de delinear los valores, objetivos y acciones fundamentales para mitigar la ciberdelincuencia (Shackelford & Kastelic, 2014).

Nacional

Estrategia Nacional de Ciberseguridad del Ecuador.

Este documento es fundamental porque garantiza la protección del ciberespacio en el Ecuador, tendiendo a relacionarse con los aspectos globales, a su vez, asegurando la seguridad ciudadana y estatal con relación a la era digital. Esta estrategia se basa en seis ejes fundamentales como lo es: gobernanza y coordinación nacional, resiliencia cibernética, prevención y combate a la delincuencia, ciberdefensa, habilidades y capacidades de ciberseguridad, y cooperación internacional. Con esta estrategia se busca establecer un marco integral de gobernanza, a su vez mejorar la gestión de riesgos y crisis cibernéticas, actualizar el marco legal en ciberdelincuencia, fortalecer las capacidades de ciberdefensa del Estado, también mejorar la concienciación y habilidades en ciberseguridad (Estrategia Nacional de Ciberseguridad Del Ecuador, 2022).

Internacional

Convenio de Budapest

La norma internacional más completa hasta la fecha, que proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica es el Convenio sobre la Ciberdelincuencia denominado Convenio de Budapest, fue firmado en el año del 2001 por los Estados miembros del Consejo de Europa y entro en vigor en el 2004; sirve como guía para los países que deseen desarrollar la legislación nacional acerca de ciberdelitos y a su vez como un marco para la cooperación internacional. En este convenio forman parte 93 Estados, ellos participan como miembros es decir como partes o también participan como observadores, es decir como signatarios o invitados dentro del comité del Convenio sobre la ciberdelincuencia. Cabe destacar que dentro de este convenio existen 22 países invitados a adherirse, entre ellos esta Ecuador (Consejo de Europa, 2024).

El Convenio de Budapest al ser un instrumento jurídico fundamental para la lucha contra la delincuencia informática, ha permitido dar pasos importantes en los países que se han suscrito, ya que afrontan los nuevos retos y desafíos garantizando una respuesta eficaz, coordinada. Cabe destacar que este convenio tiene un Comité denominado Cybercrime Convention Committee, el cual se encarga del debate de las mejoras y actualizaciones del texto, esta actualización se basa en el artículo 46 del Convenio, generando así un espacio de intercambio de información. Además, dentro de la estructura del convenio se encuentra la red 24/7, el cual tiene como fin establecer un canal de asistencia para las investigaciones con

relación a crímenes cibernéticos a su vez la recolección de las pruebas electrónicas (Martins, 2022).

Este convenio se ha desarrollado con el fin de cubrir la necesidad de los Estados parte de poseer una política penal común que tenga por objetivo la protección de los ciudadanos ante la ciberdelincuencia por medio de la cooperación internacional y la creación de protocolos específicos. En este sentido, el convenio entrega una clasificación de varios tipos penales, establece las disposiciones comunes, instaura las reglas de la jurisdicción, considera las reglas de la tentativa y complicidad en los delitos informáticos y configura los principios generales de la cooperación internacional como la asistencia mutua, la información espontánea y la confidencialidad de la información; incluso hace referencia a la creación de un punto de contacto en cada legislación que será accesible y localizable las 24 horas del día los 7 días a la semana, lo que facilita la asistencia de las investigaciones relacionadas a delitos que vulneren la seguridad de los sistemas informáticos y la obtención de pruebas de manera inmediata y en formato digital (Consejo de Europa, 2024).

Beneficio para los Estados parte

Una de las ventajas de formar parte de este convenio, es el marco legal para la cooperación internacional en relación con la ciberdelincuencia que impliquen pruebas electrónicas. Este convenio esa conformado por partes el primero es relativo a la penalización de actos de carácter racista y xenófobo, en el segundo protocolo se abrió el 12 de mayo de 2022 que es adicional al convenio se proporciona herramientas adicionales y aceleradas con el fin de mejorar la cooperación y divulgación de pruebas electrónicas. Todos los Estados que forman el convenio pueden constituir parte del Comité del Convenio sobre la Ciberdelincuencia, con el fin de obtener una cooperación confiable y eficiente. Hay que resaltar las ventajas que existen para las partes, ya que mediante su adhesión permitirá una cooperación expedita en situaciones de emergencia, equipos conjuntos de investigación e investigaciones conjuntas (Consejo de Europa, 2024).

Los principales motivos del convenio se establecen en la armonización de leyes, los países que forman se comprometen a adaptar sus leyes para tipificar como delitos las actividades relacionadas con la ciberdelincuencia. Además, mediante la cooperación internacional existe una facilidad de colaboración entre países para la investigación y persecución de los delitos informáticos. A su vez, establece procedimientos comunes para la recopilación y preservación de las pruebas digitales. Cabe destacar a través de este convenio se busca garantizar que las investigaciones respeten los derechos fundamentales, como la privacidad y la protección de datos (Estrasburgo, 2024).

2.2.3.3. Impacto del malware en la seguridad cibernética del Ecuador

El malware representa una amenaza importante para la ciberseguridad en el Ecuador, porque afecta a las organizaciones públicas y privadas a pesar de que puedan contar con una adecuada infraestructura (Toapanta et al., 2020). Actualmente, la abrumadora cantidad de delitos informáticos, relacionados con el acceso no autorizado a instalaciones y sistemas informáticos, se lleva a cabo mediante software maliciosos y, en este sentido, pueden

considerarse instrumentos para cometer actos ilícito o delitos, el crecimiento constante de usuarios de Internet y la prestación de servicios en línea, como los servicios bancarios y de compras, brindan a los delincuentes piratas informáticos un entorno adecuado para realizar sus delitos cibernéticos, lo que conduce a un aumento en los gastos que se pagan para proteger los sistemas (Reshmi, 2021).

El Malware se considera la mayor amenaza para la ciberseguridad, representa el tipo más frecuente de ataques a sistemas, computadoras, redes o usuarios para causar daño o sustraer información confidencial. En los últimos años, el número de software ha aumentado un 22,9%, lo que representa un ataque alarmante de las amenazas a los ordenadores (Rossinskaya & Ryadovskiy, 2020).

A nivel de Latinoamérica, Ecuador ha sido uno de los países más atacados por incidentes informáticos de malware, resultando ser uno de los problemas frecuentes en el espacio digital. Los delincuentes informáticos han aprovechado la pandemia para expandir sus redes mediante softwares maliciosos, diseñando nuevas modalidades de ataque y proliferación. Es así que, entre el 60 y 70% de las empresas ecuatorianas han reportado la vulneración a sus sistemas a partir del año 2019, desde entonces, esta problemática no ha cesado (Uiolibre, 2024). En el periodo de julio de 2023 a julio de 2024 los sectores más afectados fueron "el gobierno (19,49%), la manufactura de procesos (21,61%), la agricultura y silvicultura (9,23%) y el comercio (8,73%)" (Assoline, 2024, p.1).

El impacto que genera un ataque de malware en la seguridad cibernética del Ecuador comprende una vulneración en la infraestructura digital y múltiples pérdidas financieras de productividad, gastos de recuperación de incidentes, pérdida de ventajas competitivas, gastos por falta de conformidad legal, pérdida de reputación y gastos por remplazo de sistemas de información. En este contexto, varias instituciones y municipalidades del país han sufrido ataques de malware con grandes pérdidas financieras lo que ha demostrado que este tipo de ciberataque ha logrado vulnerar los sistemas informáticos de dichas entidades impactando negativamente en su desarrollo e incluso perjudicado la credibilidad de las mismas (Enríquez, 2022).

En este sentido, varios medios de comunicación han reportado el impacto que ha causado los ataques de malware en Ecuador, puesto que, en varias ocasiones los ciberatacantes han enviado falsos correos suplantando la identidad de instituciones públicas con el fin de espiar y sustraer información, para realizar acciones maliciosas como capturas de pantallas, revelación ilegal de credenciales y contraseñas o incluso manipulación de los registros de Windows. Además, cabe destacar que a través de la suplantación de identidad de las instituciones los ciberatacantes envían a las víctimas supuestas demandas judiciales e infracciones de tránsito falsas (Primicias, 2023). Estos incidentes se detallan en la matriz de análisis documental.

2.2.3.4. La inseguridad cibernética en la normativa ecuatoriana: un estudio relacional frente al malware

Considerando que, la delincuencia en el ciberespacio ha incrementado de manera alarmante en los últimos tiempos con un impacto notablemente trágico sobre la economía del país; dentro de los últimos veinte años, los usuarios poco éticos mediante la manipulación del internet han causado inseguridad personal y social, tendencia que ha cobrado fuerza y exige una respuesta inmediata (Sunil et al., 2021).

En la era digital, los riesgos que enfrenta Ecuador respecto a la seguridad cibernética se reflejan en amenazas relacionadas con la pérdida de control de la titularidad, distribución y destino del tratamiento de información personal que se traduce en el padecimiento de varios delitos informáticos como la sustracción o revelación ilegítima de bases de datos tanto de carácter público como privado lo que ha generado diversos perjuicios económicos y sociales. Frente a esta realidad, varios sectores exigen la creación inmediata de un sistema de protección de datos que cumpla y se certifique bajo estándares internacionales para salvaguardar los derechos fundamentales de los ciudadanos (Rosas & Pila, 2023).

En el país, las medidas de ciberseguridad no se encuentran establecidas de forma clara, hasta el momento se desconoce del propósito de las organizaciones de control a nivel nacional, aún no se han identificado a las entidades encargadas de conocer incidentes informáticos y tampoco se han identificado los daños que podría generar un ataque informático masivo. Los indicadores de ciberseguridad en Ecuador son muy bajos en comparación con otros países y considerando que la sociedad no se ha resistido a los cambios provocados por la globalización tecnológica, se palpa una lentitud en la creación de reformas jurídicas y una falta de comprensión de las constantes amenazas que se viven en el ciberespacio (Alvarado,2020).

En el área de la seguridad informática, las políticas no están claramente estandarizadas en todas las entidades públicas, el tema de la ciberseguridad aún no es discutido en la política exterior ecuatoriana, los peligros en la red no son tomados en serio para prevenir ataques a la infraestructuras digital de las instituciones y no existen suficientes herramientas disponibles para certificar una ciberseguridad adecuada (Alvarado, 2020).

En este sentido, enfatizando el análisis relacional frente al malware, no existe norma que incluya esta terminología como una herramienta delictiva ni pretenda regular esta conducta, únicamente llega a definirse en la reforma al reglamento de políticas de seguridad de la información, donde de manera general se entiende al malware como un código malicioso que tiene el objetivo de dañar un sistema, sustraer información o malograr su funcionamiento; haciendo alusión a sus tipos: troyanos, gusanos y ransomwares (Reforma Reglamento de Políticas de Seguridad de La Información, 2023).

Para complementar, se conoce que el proyecto de Ley de Seguridad Digital propuesta por el ex legislador Juan Carlos Yar en 2019, impulsada por el ex asambleísta Rodrigo Fajardo en 2021 y presentada por José Luis Vallejo Ayala con la finalidad de que el país

cuente con una normativa regulatoria referente al fortalecimiento de la infraestructura digital fue archivada el 6 de junio de 2024 tras un mínimo debate parlamentario por el pleno de la Asamblea Nacional del Ecuador con cinco legisladores interventores, un breve discurso y poco apoyo por parte de los legisladores (Debate Sobre El Proyecto de Ley de Seguridad Digital, 2024).

Al respecto, en los primeros 6 meses del 2024, se cree que la Asamblea no ha llevado a cabo un debate oportuno para considerar la problemática que aqueja al país, considerando que incluso entre sus manos está la revisión de la adhesión del Ecuador al convenio de Budapest, convenio al que ha sido invitado el país desde 2019 (Carrillo, 2024).

Este proyecto de ley en su mismo cuerpo normativo establece: "constituye una urgencia para el Ecuador, el que se elabore textos normativos que creen normas que permitan actuar y mitigar los delitos que se pretenden ejecutar desde la red" (Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, 2024). De manera que intentó aportar en la tarea de contrarrestar los hackeos e incidentes informáticos en el Ecuador bajo los principios de ciberseguridad, ciberinteligencia y ciberdefensa.

Los puntos claves de este proyecto fueron establecer un sistema de seguridad digital, plantear la creación de un sistema nacional de seguridad digital, determinar las funciones de las instituciones parte, disponer las reglas de la conformación de dicho sistema; así como, planificar la creación de un subsistema de seguridad digital, un sistema de ciberdefensa y uno de ciberinteligencia; disponer las funciones del Ministerio de Gobierno del Subsistema de Ciberseguridad, del Ministerio de Telecomunicaciones y de la Sociedad de la Información y del Ministerio de Defensa y Comando Conjunto de las Fuerzas Armadas; finalmente hizo un esfuerzo por determinar las funciones de la Fiscalía del Estado y el Consejo de la Judicatura como organismos auxiliares del sistema macro (Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, 2024).

El principal argumento de la Asamblea para archivar este proyecto de ley fue la ambigüedad de los términos de "soberanía digital", "infraestructura crítica digital" y "control geográfico", además que se pretendía cambiar la entidad rectora entregando el poder del Ministerio de Telecomunicaciones y Sociedad de la Información al Ministerio del interior, lo que supuestamente implicaría entregar un poder considerable a la policía acerca de la gobernanza del internet y la revisión de contenidos de los usurarios en nombre de la protección a la seguridad cibernética, bajo el argumento de que no se pueden crear barreras o limitantes en el alcance del internet por su carácter internacional este proyecto fue archivado totalmente por el poder legislativo (Durán, 2024).

Conforme a ello, se evidencia una falta de conciencia generalizada sobre los riesgos relacionados con el uso de la tecnología haciendo que la seguridad cibernética no sea reconocida como un tema prioritario en el país, lo que implica que no se lleven a cabo medidas proactivas para contrarrestar las amenazas y vulnerabilidades a la infraestructura

digital y no se implementen buenas prácticas de ciberseguridad (Política Nacional de Ciberseguridad, 2021).

A pesar de los pocos esfuerzos, Ecuador no trabaja de manera sistemática en la ciberseguridad y no cuenta con un plan de acción fructífero para las entidades gubernamentales limitando el potencial institucional en la creación de una estructura digital protegida (Ávila, 2022). El país debería contar con una entidad enfocada en la protección cibernética, desarrollar políticas y acoger estándares internacionales para mejorar sus capacidades de perfeccionamiento de la seguridad digital (Alvarado, 2020).

CAPÍTULO III

3. METODOLOGÍA

3.1. Técnicas e instrumentos de investigación

Las técnicas de recopilación de la información que se utilizaron fueron la entrevista y una matriz de análisis documental; los agentes fiscales de la provincia de Chimborazo y peritos informáticos fueron entrevistados con ayuda de una guía de entrevista dirigida a su especialidad, debidamente validada como instrumento de investigación, con el objetivo de conocer su percepción sobre la eficacia normativa ecuatoriana relacionada a la investigación de los delitos informáticos, conocer el procedimiento investigativo y determinar la implicación del malware en este tipo de delitos; una vez recopilada la información se llevó a cabo el respectivo tratamiento y análisis de datos.

Por otra parte, el análisis documental como técnica de recolección de datos se efectuó mediante una matriz, como instrumento para la descripción sistemática del contenido de publicaciones de diversas fuentes secundarias con el objetivo de interpretarlas; fue elaborada y validada con la finalidad de sintetizar la información de casos registrados por medio de noticias sobre el uso del malware para la comisión de delitos informáticos, la cual fue interpretada mediante un análisis cualitativo.

3.2. Unidad de análisis

El presente proyecto de investigación titulado "Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética" se llevó a cabo en la provincia de Chimborazo, específicamente en el cantón Riobamba, donde se analizó las dificultades que se presentan en la investigación de los delitos informáticos perpetrados mediante el malware.

3.3. Métodos

La presente investigación, para abordar la problemática jurídica empleó los siguientes métodos de estudio:

Método jurídico-analítico: "Es el método propio del Derecho Anglosajón que se basa en un análisis de la normativa jurídica por medio de la comprensión de diferentes conceptos, enunciados y contextos en los que se instauró su aplicación" (Witker, 2021, p.29). Por medio de la aplicación de este método se analizó el alcance y sentido de las normas jurídicas relacionadas a los delitos informáticos y la seguridad cibernética permitiendo identificar, evaluar e interpretar las leyes dentro del contexto social, político y económico en el que fueron desarrolladas.

Método jurídico-doctrinal: "Se refiere al estudio de las propuestas interpretativas planteadas por los académicos con el objetivo de aclarar las fuentes del derecho en categorías de conceptos y principios o simplemente se refiere a la investigación académica de un problema jurídico" (Brito, 2023, p.10). Con la aplicación de este método el presente estudio

se enfocó en profundizar la doctrina jurídica y las interpretaciones de los expertos en la materia con el fin de crear conclusiones científicamente válidas acerca de los desafíos de la ciberseguridad en el Ecuador.

Método jurídico comparativo: "Representa el criterio de interpretación valorada en los hallazgos empíricos y teóricos relacionados a la realidad social y política de un país en base a la información de naturaleza cualitativa y cuantitativa sustentada a través de la comparación lógica" (Barquera, 2020, p.58). El empleo de este método facilitó relacionar el estudio teórico y el empirismo basándose en el análisis estadístico, histórico y cualitativo del objeto materia de la presente investigación jurídica.

3.4. Enfoque de investigación

Por las características que posee la investigación, se asumió un enfoque de investigación cualitativo.

3.5. Tipo de investigación

De acuerdo con el objetivo de la investigación y los métodos seleccionados para el estudio del problema jurídico se utilizó los siguientes tipos de investigación:

Investigación jurídica descriptiva. "Tiene como objetivo estudiar y comprender los fenómenos jurídicos describiéndolos en su entorno natural, interpretando las realidades sociales y evaluando políticas basadas en los sentimientos, percepciones y experiencias de las personas" (Disemadi, 2022, p.1). Por tal razón, a través de la investigación jurídica descriptiva se pudo especificar los problemas jurídicos actuales en la investigación de los nuevos delitos informáticos en el país.

Investigación pura. "Tiene como objetivo comprender principios y conceptos jurídicos sin influencias externas como la moralidad u observaciones empíricas" (Gorban & Gruzdev, 2022, p.1). La aplicación de este tipo de investigación facilitó el análisis claro y amplitud de conocimiento teórico relacionado a los delitos informáticos.

Investigación histórica jurídica. "Implica estudiar el desarrollo histórico de los sistemas jurídicos, las leyes y los principios jurídicos a lo largo del tiempo. Este tipo de investigación profundiza en los orígenes, la evolución y las transformaciones de los marcos legales, proporcionando información sobre las conexiones entre las prácticas legales pasadas y los sistemas legales contemporáneos" (Majeed, 2023, p.1). De este modo, mediante la utilización de este tipo de investigación se comprendió la importancia de la evolución histórica de los delitos informáticos en el Ecuador y el desarrollo de las instituciones jurídicas encargadas de la investigación de los nuevos delitos informáticos.

3.6. Diseño de investigación

Considerando la complejidad de la investigación, los objetivos planteados, los métodos y tipo de investigación a emplearse, el estudio del problema jurídico se construyó a partir de un diseño no experimental.

3.7. Población y muestra

3.7.1. Población

La población se centra en la provincia de Chimborazo, específicamente en el cantón Riobamba, donde se analizó las dificultades que se presentan en la investigación de los delitos informáticos perpetrados mediante el malware. La población seleccionada incluye 5 agentes fiscales de la provincia de Chimborazo y 2 peritos informático acreditado por el Consejo de la Judicatura de la ciudad de Quito, considerando que, dentro de la georreferenciación de la población, en Chimborazo, no se cuenta con estos especialistas en la materia.

3.7.2. Muestra

De la población descrita, se obtuvo una muestra intencional no probabilística por conveniencia bajo los siguientes criterios de selección: que acepten libre y voluntariamente la participación en la presente investigación; de manera que, se logró la participación de 4 agentes fiscales de la provincia de Chimborazo y 1 perito informático acreditado por el Consejo de la Judicatura de la ciudad de Quito.

3.8. Técnicas para el tratamiento de información

De la información obtenida por medio de la aplicación de los instrumentos de investigación se efectuó un proceso minucioso para su tratamiento. En primer lugar, se usó el programa Pinpoint para realizar la transcripción de las cinco entrevistas grabadas en formato mp3 y mp4, transformándolas en texto, seguidamente se efectúo una revisión meticulosa para evitar errores en el registro de la información.

En segundo lugar, los datos fueron analizados en base a cada una de las respuestas adquiridas tras aplicar las 2 guías de entrevista; de este modo, se codificó cada sección organizando la información y estructurando el estudio por medio de etiquetas atribuidas a cada respuesta, las cuales fueron: “alcance normativo”, “delitos informáticos”, “dificultades en la investigación”, “impacto del malware”, “procedimiento de investigación” y “seguridad cibernética”.

Una vez codificadas las respuestas, se organizó, interpretó y analizó los resultados, lo que facilitó la observación de tendencias, perspectivas y criterios; así como la elaboración de un estudio de categorías por código que permitió cumplir los objetivos planteados para este apartado de la investigación.

Por otra parte, para la construcción de la matriz de análisis documental se desarrolló una indagación oportuna sobre los casos registrados en las noticias de los diarios y medios de comunicación nacionales acerca de los ataques de malware más influyentes dentro del país, de manera que, la información fue seleccionada y clasificada dentro de la matriz en apartados categorizados denominados: “tipo de documento”, “fuente”, “título”, “fecha”, “enlace”, “tipo de ataque” y “resumen”. Una vez clasificada la información, se elaboró un

análisis cualitativo que explica la finalidad de la tabla y las conclusiones más trascendentales.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Resultados

4.1.1. Análisis del alcance de la normativa jurídica ecuatoriana ante los delitos informáticos.

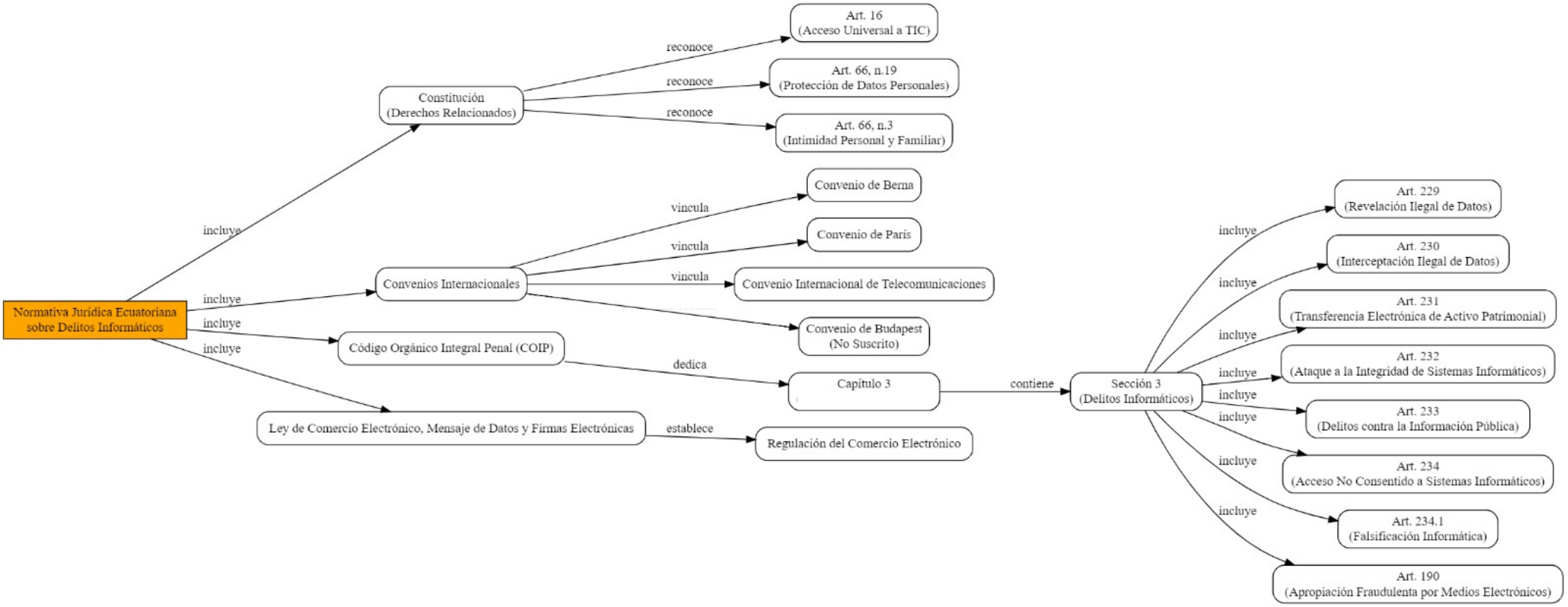
A partir del estudio teórico de la problemática, se creó un mapa conceptual presente en la figura 4 donde se resume el análisis alcance de la normativa jurídica ecuatoriana en materia de delitos informáticos, como se puede observar en el gráfico, del tema central se desglosan 4 componentes, iniciando por la constitución, como norma suprema del Estado, la cual establece derechos relacionados al ámbito informático digital, en este sentido, se menciona al derecho al acceso universal a las tecnologías de la información y comunicación, el derecho a la protección de datos de carácter personal y el derecho a la intimidad personal y familiar; los cuales son un punto de partida indirecto para el fortalecimiento de la creación de normativa relacionada a la protección de los entornos digitales y la ciberseguridad.

A posterior, se describen los convenios internacionales ratificados por el Ecuador, entre ellos el convenio de Berna y el convenio de Paris, que hacen hincapié en los derechos de autor y las telecomunicaciones; y se hace alusión a la falta de ratificación del convenio de Budapest, que trata sobre cooperación internacional y la lucha contra el ciberdelito. El cuarto apartado del mapa considera a los delitos reconocidos en el COIP contra la seguridad de los activos de los sistemas de información y comunicación y el delito de apropiación fraudulenta por medios electrónicos. Finalmente se menciona a la Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas con un marco regulatorio apegado al comercio electrónico y la protección a sus usuarios.

En este sentido, cabe aclarar que en la normativa actual no se tipifican las nuevas conductas delictivas en temas relacionados con la informática, no se reconocen las acciones delictivas perpetradas por medio del malware y se evidencia un déficit en la normativa relacionada a las directrices, manuales y protocolos del procedimiento de investigación de este tipo de delitos. Es decir, la legislación no desarrolla manuales y protocolos necesarios para cumplir el proceso de peritaje informático, desde la obtención y guarda de las evidencias digitales para garantizar la autenticidad de los elementos de convicción recabados y con ello resguardar el valor probatorio dentro de los procesos investigativos.

Figura 4.

*Análisis del alcance de la normativa jurídica ecuatoriana ante los delitos informático**s***



Nota: La figura muestra un análisis del alcance de la normativa jurídica ecuatoriana ante los delitos informáticos. Autoría propia (2024)

4.1.2. Naturaleza del malware como nueva herramienta delictiva para cometer delitos informáticos.

4.1.2.1. Análisis de entrevistas

Entrevistado 1.
Agente Fiscal de la Unidad de Patrimonio Ciudadano I,
Doctor en Jurisprudencia,
Docente de Posgrado de la Universidad Nacional de Chimborazo.

El entrevistado destaca que la normativa actual en Ecuador para abordar delitos informáticos necesita mejoras, especialmente en la clasificación y regulación de ciertos tipos penales. Señala que existen lagunas jurídicas que requieren mayor regulación para mejorar la persecución de estos delitos. Propone adaptar la legislación a estándares internacionales y fortalecer el enfoque en la lesividad de las conductas. Explica el procedimiento típico de investigación y acusación de delitos informáticos, resaltando la importancia de la cadena de custodia para preservar la integridad de las evidencias digitales.

Destaca los desafíos en la práctica diaria de investigar y acusar delitos informáticos, incluyendo la necesidad de recursos y peritos especializados. Considera que la pericia informática es crucial en casos de delitos informáticos, ya que ayuda a determinar si existió manipulación o acceso indebido a equipos mediante georreferenciación de direcciones IP. La competencia para investigar estos delitos se determina según las reglas establecidas en el COIP, considerando la transnacionalidad del delito.

En Ecuador, la capacidad de las instituciones para detectar y procesar delitos informáticos que incluyen malware es limitada sin tecnología y expertos especializados. La cooperación internacional no es efectiva para perseguir estos delitos; y, los bienes jurídicos protegidos más afectados en los delitos informáticos incluyen la intimidad, la propiedad y la seguridad nacional.

Entrevistado 2.
Agente Fiscal de la Unidad de Patrimonio Ciudadano III,
Magister en Derecho Constitucional,
Magister en Derecho Penal y Criminología,
Especialista en Derecho Penal y Justicia Indígena,
Doctora en Jurisprudencia y Abogada de los Tribunales y Juzgados de la República.

La especialista sugiere fortalecer la normativa actual en Ecuador para abordar los delitos informáticos cometidos con malware, estableciendo convenios de cooperación internacional y tratando cada conducta de manera exclusiva. Menciona la importancia de mejorar las relaciones con entidades financieras y de manejo de datos, así como la cadena de custodia de evidencias digitales para asegurar la integridad en la investigación y acusación de estos delitos.

También destaca la necesidad de contar con expertos informáticos para enfrentar los desafíos diarios al investigar y acusar estos delitos. Refiere sobre la importancia de la informática para la detección de softwares maliciosos y cómo los peritos informáticos ayudan a identificar el alcance de estos. Destaca desafíos en la investigación de delitos informáticos, como la dificultad para rastrear el malware y la escasez de recursos. Además, que, indicó las deficiencias en la capacidad técnica de las instituciones ecuatorianas para detectar y procesar delitos informáticos, así como la repercusión en los bienes jurídicos protegidos, especialmente en el patrimonio.

Entrevistado 3.
Agente Fiscal de la Unidad de Soluciones Rápidas III,
Abogado de los Tribunales y Juzgados de la República,
Doctor en Jurisprudencia en Derecho Penal.

El entrevistado considera que la normativa ecuatoriana sobre delitos informáticos es efectiva, pero destaca la falta de peritos informáticos en algunas jurisdicciones. Propone la necesidad de mejorar las leyes y la importancia de la creación de tipos penales específicos. Destaca desafíos en la investigación de delitos informáticos como la cooperación internacional y la falta de tecnología adecuada para abordar de manera más efectiva el impacto del malware en el país. Finalmente, alude que el bien jurídico más afectado por los delitos informáticos es el derecho al patrimonio.

Entrevistado 4.
Agente Fiscal de la Unidad Especializada de Delincuencia Organizada, Transnacional e Internacional I,
Abogado de los Tribunales y Juzgados de la República.

La entrevistada considera que la normativa legal ecuatoriana actual es general y no aborda específicamente los delitos informáticos, lo que genera lagunas jurídicas y la necesidad de una mayor regulación. Propone la creación de un procedimiento específico para abordar estos delitos, así como tipificarlos adecuadamente en la ley. También destaca la importancia de la capacitación de los agentes encargados de investigar estos casos y la colaboración de las entidades financieras para obtener la información necesaria. Indica la importancia de la cadena de custodia para preservar la integridad de las evidencias digitales. Además, destaca los desafíos que existen en la investigación de estos delitos, especialmente debido a la falta de recursos tecnológicos y la necesidad de una mayor cooperación internacional. Los bienes jurídicos más afectados en los delitos informáticos son el derecho al patrimonio, al buen nombre y al secreto empresarial.

Entrevista 5.
Perito Informático Forense Acreditado por el Consejo de la Judicatura
Ingeniero en informática e inteligencia digital

El perito en informática forense se refiere a la naturaleza y características técnicas del malware. Destaca el impacto en la seguridad cibernética del Ecuador y la relevancia del análisis forense. Según este experto, el malware es una amenaza porque se encuentra en un sistema operativo, un archivo y la información que contienen. El experto hace hincapié en que el trabajo de la detección y análisis de malware requiere una adecuada herramienta y un procedimiento exigente y jurídico. Además, afirma que la legislación ecuatoriana no responde eficazmente a las características los delitos informáticos y la tendencia a su aumento. Por lo tanto, recalca la relevancia de la cooperación internacional para sancionar a los autores de este tipo de delitos que usan el malware como modo de ataque.

Análisis por categorías de códigos

Alcance normativo

Se destaca que en la normativa legal ecuatoriana existe la ausencia de procedimientos específicos dentro del COIP para manejar delitos informáticos. El marco legal actual es visto como muy general y carece de directrices explícitas sobre cómo proceder en estos casos, lo cual dificulta la labor investigativa. Además, se destaca la falta de capacitación y preparación adecuada para enfrentar la particularidad de estos delitos, que a menudo tienen una dimensión transnacional.

Se resalta la necesidad de una mayor precisión y tipificación de los delitos informáticos dentro del marco legal. Existe una carencia de figuras penales específicas para ciertos delitos cibernéticos, como el virus, guanos, ransomware, Spyware, entre otros tipos de malware y se subraya la importancia de adaptar la legislación a las normativas y mejores prácticas internacionales. Además, un tratamiento pormenorizado de cada tipo penal es visto como un paso necesario para abordar las diversas modalidades y elementos que caracterizan estos delitos, asegurando así una mejor protección y sanción de las conductas ilícitas en el ámbito digital.

La falta de estos convenios limita significativamente la capacidad de las autoridades ecuatorianas para resolver casos complejos que involucran actores y recursos fuera del país. Se subraya la necesidad de fortalecer las relaciones internacionales y establecer marcos de cooperación más sólidos para mejorar los resultados en la lucha contra los delitos cibernéticos. La calidad de las leyes existentes es criticada, se señala que la corrupción impide el progreso y la creación de leyes efectivas, prácticas. Estos problemas estructurales deben ser abordados para asegurar que las reformas legales no solo se promulguen, sino que también se apliquen de manera eficaz y justa, contribuyendo así al fortalecimiento de la ciberseguridad en Ecuador.

Delitos informáticos

Se destaca que se han incorporado nuevos tipos penales al Código Orgánico Integral Penal (COIP), como la revelación ilegal de bases de datos, la interceptación ilegal de datos, y la transferencia electrónica de activos patrimoniales. Sin embargo, a pesar de estos avances, hay consenso entre los expertos sobre la necesidad de mejorar el tratamiento y

desarrollo de estos tipos penales para hacer frente a los desafíos que presentan las tecnologías.

Se destaca que los delitos informáticos en Ecuador están en constante evolución, ya que los ciberdelincuentes demuestran habilidades avanzadas y la capacidad de operar desde cualquier lugar del mundo. Existen varios casos en donde el panorama es desafiante y destaca la necesidad urgente de actualizar, reforzar la normativa legal para enfrentar estos delitos de manera efectiva. Este problema evidencia la necesidad de establecer marcos de colaboración internacional más sólidos y efectivos para combatir los delitos informáticos transnacionales de manera eficiente.

Además, la dependencia de expertos informáticos y la falta de equipos especializados dentro de las instituciones representan una tendencia preocupante, esta deficiencia limita la capacidad de respuesta y resalta la necesidad de invertir en capacitación continua y en la creación de equipos especializados para enfrentar estas amenazas. Los delitos informáticos actuales son vistos como insuficiente, y se requiere una mejor tipificación y adaptación de la legislación a las normativas internacionales.

Dificultades en la investigación

El análisis de las dificultades en la investigación de este tipo de delitos resalta el desafío de obtener cooperación penal internacional con otros países, en la realidad, la solicitud de asistencia penal internacional es un proceso engorroso y lento, que a menudo no produce resultados eficaces a tiempo para rastrear a los culpables o recuperar fondos perdidos.

Es preciso resaltar la limitación de recursos y capacidades técnicas dentro del país. Los expertos mencionan que muchas unidades de investigación carecen de los recursos necesarios para realizar investigaciones complejas de ciberdelitos. La falta de tecnología avanzada y personal capacitado en peritaje informático limita la capacidad de respuesta y resolución de estos delitos.

Asimismo, se observa una tendencia hacia la centralización de los recursos en las grandes ciudades, lo que deja a las provincias con capacidades limitadas para investigar ciberdelitos; esta centralización provoca demoras en las investigaciones y permite que los delincuentes escondan o eliminen rastros de sus actividades antes de ser detectados. Los expertos sugieren que cada provincia debería contar con una unidad de investigación de ciberdelitos para mejorar la eficiencia y la capacidad de respuesta local.

Procedimiento de investigación

La norma carece de un procedimiento específico en tema de delitos informáticos, lo que obliga a los fiscales a adaptar el procedimiento general para estos casos; esto implica cumplir la fase de investigación previa y las etapas de procedimiento penal (instrucción fiscal; evaluación y preparatoria de juicio; y, juicio). En este sentido, el proceso inicia determinando la competencia enfocada en el lugar donde se produjo el daño, lo que ya resulta

ser un desafío considerando la transaccionalidad del delito y la dificultad para seguir el camino del delito en los sistemas informáticos y la web.

Es destacable la necesidad de establecer protocolos para el manejo de evidencias digitales diferentes a los procedimientos tradicionales. Para este tipo de casos se debe llevar a cabo una impecable cadena de custodia de las evidencias digitales encontradas, para ello es importante contar con la autorización judicial para obtener la apertura de los dispositivos (teléfonos, tablets, computadoras, discos duros, etc.), la cual se realiza por medio de una audiencia privada con la participación de un perito especializado, el fiscal y el abogado defensor.

Dentro de este apartado se destacan las dificultades procesales en la investigación por cuanto existen desafíos importantes al momento de rastrear los delitos cometidos con tecnología avanzada y transacciones electrónicas complejas. Para efectivizar este proceso, es crucial la colaboración de las entidades financieras en la recolección de información transcendental y la labor de los peritos especializados en informática forense, de los cuales se toma en cuenta tanto su informe físico como su testimonio pericial dentro de la audiencia de juicio.

Impacto del malware

El malware es un software sofisticado y complejo que trae consigo desafíos significativos en la seguridad cibernética para las instituciones públicas y privadas, así como para las personas naturales. El uso del malware como herramienta delictiva para cometer delitos informáticos va en aumento y cada vez utiliza modalidades más técnicas e indetectables, lo que dificulta la investigación de estos crímenes. La capacidad de los delincuentes para encubrir sus actividades y operar a nivel mundial utilizando herramientas avanzadas complica aún más los esfuerzos de las autoridades encargadas de investigar el delito y acusar a los presuntos infractores.

La normativa ecuatoriana no está adaptada para contemplar los desafíos específicos de la investigación de los delitos cometidos por medio del malware, lo que dificulta la acusación y la obtención de pruebas contundentes. Con certeza se puede afirmar que existe una falta de recursos tecnológicos para combatir el malware de manera efectiva, muchas de las instituciones no tienen sistemas de seguridad adecuados, incluso la misma Fiscalía General del Estado y los grandes bancos han recibido amenazas de estos ataques cibernéticos lo que subraya una necesidad urgente de protección de la ciberseguridad del país.

Seguridad cibernética

Según los expertos, incidentes como los sucedidos en el municipio de Riobamba, donde hubo una transferencia ilegal de 13 millones de dólares y las constantes amenazas a la seguridad destacan la vulnerabilidad de las instituciones frente a la tecnología avanzada utilizada por los delincuentes informáticos, lo que acentúa la necesidad de fortalecer las medidas de ciberseguridad en la normativa actual.

La falta de inversión en seguridad digital y estrategias de ciberseguridad en las instituciones públicas y privadas es un factor clave que contribuye a la vulnerabilidad de los sistemas ante ataques de malware, así como la falta de capacitación en ciberseguridad son tendencias preocupantes que requieren atención urgente para proteger el patrimonio y la información sensible de las instituciones.

Finalmente, cabe destacar que, el Ecuador aún mantiene un importante índice de analfabetismo digital y falta de conciencia de buenas prácticas en uso de dispositivos, internet y sistemas informáticos, lo que facilita la propagación de softwares maliciosos que evidentemente quebrantan la seguridad cibernética.

4.1.3. Estudio relacional de la falta de protección de la seguridad cibernética en el Ecuador.

4.1.3.1. Análisis de la matriz de análisis documental

La matriz de análisis documental revela un panorama preocupante de la seguridad cibernética en el país. En primer lugar, de la información recopilada se destaca la prevalencia de diversidad de ataques cibernéticos incluyendo al pishing, malware, troyanos y ransomware, estos ataques han afectado tanto a ciudadanos como a instituciones, lo que demuestra la vulnerabilidad del país frente a las amenazas cibernéticas.

Bajo este estudio documental de fuentes secundarias se ha descubierto nuevas campañas de malware como “la Operación Pulpo Rojo” y el ataque “BlackCat” lo que demuestra como los delincuentes cibernéticos utilizando su ingenio han logrado atacar a los sistemas informáticos del mismo gobierno y servicios nacionales buscando tener un beneficio económico, sustraer información y espiar datos sensibles.

A través de este análisis se ha determinado el riesgo del país a significativos ataques informáticos, el cual cuenta con grandes desafíos legales y de ciberseguridad que deben ser tratados con urgencia. Se constata una necesidad imperante de fortalecer las políticas y la infraestructura digital, un ajuste constante de la normativa y estrategias educativas para combatir de manera eficaz la ciberdelincuencia.

Tabla 3.
Matriz de análisis documental

Tipo de documento	Fuente (Autor)	Título	Fecha	Enlace	Tipo de ataque	Resumen
Informativo	El Comercio (diario en línea)	Ciberdelincuentes operan de cuatro formas en el Ecuador	11 de enero de 2022	https://www.elcomercio.com/actualidad/seguridad/ciberdelincuencia-ecuador-organizaciones-delictivas-victimas.html	Phishing, malware, sitios web fraudulentes y hackeo de cuentas de redes sociales	Durante la pandemia Covid-19, la policía alertó un aumento de las operaciones de las ciber mafias. Se logró identificar 4 tipos de ataque más comunes: phishing, malware, sitios web fraudulentes y hackeo de cuentas de redes sociales. El caso de Marcia fue el más relevante, debido a que por medio de un ataque de malware, en noviembre de 2021, recibió un correo electrónico notificándole que se efectuó una transferencia no consentida de USD 350 a la cuenta de un desconocido (El Comercio, 2022).
Informativo	El Universo (diario en línea)	Ecuador es el tercer país con las mayores amenazas cibernéticas en América Latina, según Check Point	3 de mayo de 2024	https://www.eluniverso.com/noticias/ecuador/ecuador-enfrenta-un-creciente-riesgo-de-ciberataques-en-el-2024-nota/	Malware	Según un informe de ciberseguridad de Check Point, el país registra un riesgo de 51,9% ante los ataques informáticos, de manera que la principal amenaza que ha sido identificada es el malware multipropósito, tanto CNT en 2021 y el Municipio de Quito en 2022 fueron víctimas de este tipo de ataque (El Universo, 2024).
Informativo	Fernando Tavella (página Web)	Operación Pulpo Rojo: campaña de malware dirigida a organismos de alto perfil de Ecuador	30 de agosto de 2022	https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/	Malware (troyano)	El malware está siendo utilizado para espiar y sustraer información a entidades gubernamentales por medio de la distribución de una campaña de malware tipo troyano con acceso remoto. El 90% de la distribución de esta campaña afectó a Ecuador y su distribución se efectuó por medio de Google, Drive y Discord (Tavella, 2022).

Informativo	Vistazo (diario en línea)	Hackers al acecho: Esto se sabe sobre una campaña de malware dirigida a Ecuador que utiliza correos sobre demandas judiciales falsas	2 de agosto de 2023	https://www.elcomercio.com/actualidad/negocios/ecuador-cuarto-pais-latino-con-intentos-ataque-cibernetico-por-minuto.html	Malware (troyano)	Se identificó una campaña de malware dirigida a entidades públicas y privadas que difundía contenido malicioso por medio de un malware tipo troyano que se distribuyó por medio de correos electrónicos, en los que suplantando la identidad de la Fiscalía General del Estado enviaban notificaciones de denuncias faltas contra la víctima con la finalidad de implantar este troyano y tener acceso a las credenciales, espiar la pantalla, etc (Vistazo, 2023).
Informativo	Mercedes Onofa (página Web)	Ataques cibernéticos amenazan seguridad en Ecuador	30 de junio de 2022	https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/	Malware (ransomware)	Ecuador se encuentra entre uno de los países más vulnerable antes los delitos informáticos principalmente por ataques de malware. Desde 2021, el Banco Pichincha y el Ministerio de Finanzas de Ecuador fueron víctimas de este tipo de ataques y a partir de 2022, los ataques de ransomware aumentaron un 25% al año anterior (Onofa, 2022).
Informativo	El Comercio (diario en línea)	BlackCat, el ataque multinivel que amenaza a la ciberseguridad del Municipio de Quito	22 de abril de 2022	https://www.elcomercio.com/actualidad/blackcat-ataque-hackers-municipio-quito.html	Malware (ransomware)	El malware tipo ransomware denominado Black Cat inhabilitó varios servicios informáticos del municipio de quito, este tipo de malware actúa encriptando la información para ser ocultada o revelada a cambio de una prestación monetaria de la víctima. En los casos más recientes los ciberdelincuentes han llegado a pedir hasta USD 14 000 000 para restaurar la información y el sistema (El Comercio, 2022).

Informativo	Agencia de Regulación y Control de las Telecomunicaciones (Centro de Respuesta a incidentes informáticos del Ecuador)	Alerta de Seguridad	16 de enero de 2023	https://www.ecucert.gob.ec/wp-content/uploads/2023/01/AL-2023-003-malware-zoom-rev.1-FAHA-160123-1.pdf	Malware (troyano)	Se identificó una campaña de malware dirigida a la aplicación de ZOOM, reconocido como un troyano bancario que facilita a los cibercriminales sustraer credenciales bancarias de las víctimas. La modalidad empleada fue crear una página parecida a la de ZOOM para engañar a los usuarios y descargar el malware IceID, para a partir de ello, efectuar actividades maliciosas (Centro de Respuesta a incidentes informáticos del Ecuador, 2023).
Informativo	¿Cómo funcionan las estafas por mensaje de texto en Ecuador?	Ecuavisa	16 de julio de 2024	https://www.ecuavisa.com/noticias/seguridad/como-funcionan-las-estafas-por-mensaje-de-texto-en-ecuador-FA7673887	Smishing	Los ataques informáticos ahora también se ejecutan a través de mensajes de texto de WhatsApp. La modalidad de smishing para obtener datos del usuario está registrando varias formas de engañar a sus víctimas entre ellas se evidencia: la falsa alerta bancaria, engaños por delivery, falso servicios al cliente, ofertas irregulares del portal chino Shein. Cada día se reporta entre 300 000 y 400 000 ataques de este tipo alrededor del mundo según la empresa de seguridad Proofpoint, quien asegura que estos ataques irán en aumento (Ecuavisa, 2024).

Nota: La tabla muestra una matriz documental que recopila noticas de diarios nacionales sobre los ataques más comunes de malware. Autoría propia (2024)

4.2.Discusión de resultados

Los resultados del estudio documental y las entrevistas realizadas para el presente trabajo de investigación indican que la normativa actual en Ecuador se considera insuficiente para abordar específicamente los delitos informáticos cometidos mediante el malware. Según Carrers y Aguilar (2020) el Ecuador presenta normativa ambigua que no comprende manuales y protocolos para la investigación, compilación y guarda de evidencias digitales, por lo que surge una necesidad imperante en la creación de los mismos debido a que este tipo de ataques requieren un procedimiento especial para recabar elementos de convicción necesarios para esclarecer la materialidad, responsabilidad y nexo causal en estos crímenes con lo que se garantizará el debido proceso.

A partir del análisis realizado se demuestra que, el avance de la tecnología ha sido de gran importancia para la sociedad, pero también ha constituido grandes desafíos para la misma. Autores como Aslan, Samet, Belic, Méquez Díaz y Jumbo concuerdan con el presente trabajo de investigación, ya que los modos delictivos a través de los sistemas informáticos cada día van en aumento y las estrategias que los ciberdelincuentes utilizan también son más sofisticadas, de esta manera, afirman que el malware es una de las nuevas herramientas para cometer delitos, la misma que posee nuevas modalidades más técnicas, generando dificultades en la investigación y obtención de pruebas para sancionar a los responsables.

María Sanz (2022) considera que el impacto del malware en Ecuador no solo afecta a las personas naturales, sino que extiende sus redes a las empresas, organizaciones, instituciones y a los mismos gobiernos creando graves amenazas a la ciberseguridad nacional y mundial. En este contexto, los resultados obtenidos concuerdan con los estudios preliminares de varios autores como Ortiz, Aparicio y Leyva referente a que, Ecuador, no posee un sistema de seguridad efectivo que le permita enfrentar los ataques cibernéticos de cualquier tipo, en especial los efectuados mediante el malware; menos aún posee tecnología, infraestructura y sistemas efectivos de investigación informática.

De manera que, de las entrevistas realizadas a 4 agentes fiscales de la provincia de Chimborazo y 1 perito informático acreditado por el Consejo de la Judicatura de la ciudad de Quito, 4 de ellos determinaron que: se debería mejorar la cooperación internacional; impulsar las relaciones con entidades financieras y de manejo de datos; fortalecer el enfoque en la lesividad de las conductas; incrementar expertos informáticos para enfrentar los desafíos diarios en la investigación. Además, destacaron la importancia de la pericia informática, el buen manejo de la cadena de custodia de la evidencia digital y el uso de sistemas y herramientas técnicas que coadyuben a profundizar la identificación e investigación de estas conductas delictivas.

Es así como se ha corroborado las dificultades planteadas en el marco teórico afirmando que en el proceso investigativo se evidencia una falta de conocimientos técnicos informáticos, mal manejo de la evidencia digital, falta de estrategias metodológicas, desactualización normativa y complejidad transnacional del delito.

Tal como lo señala Rossinskaya y Ryadoysky (2020) en su obra “El concepto de malware como medio para cometer delitos informáticos: clasificaciones y tecnologías de uso ilegal”, los entrevistados destacaron la complejidad de la investigación de los delitos informáticos cometidos mediante el malware debido a que suelen estar completamente estructurados desde su preparación, ejecución, ocultamiento y encubrimiento.

En tal sentido, los resultados de las entrevistas confirman en gran escala lo planteado respecto a: la complejidad investigativa de los delitos informáticos cometidos mediante esta modalidad, las dificultades que presenta el sistema especializado de medicina legal y ciencias forenses y demás instituciones. Por tanto, podemos indicar que la hipótesis sustentada en la presente investigación es certera, ya que la actualización de la norma, estrategias, convenios en materia de ciberseguridad, permitirá la efectiva investigación de los delitos informáticos cometidos mediante el malware.

Además, al realizarse el análisis respectivo de las entrevistas se identificó que los expertos en la materia coinciden en la falta de convenios de cooperación internacional, tipificación de las nuevas conductas delictivas en temas de ciberataques e inexistente regulación de manuales y protocolos de procedimientos investigativos entre la Fiscalía y la Policía Judicial específica para la investigación, guarda y compilación de evidencias digitales en los casos de malware lo que acertadamente apoya la hipótesis planteada; no obstante uno de ellos sugirió que el problema no radica en la falta de normativa sino en la insuficiente adaptación de la misma a estándares internacionales.

Finalmente, a través del análisis documental, los resultados han demostrado que los medios de comunicación como El Comercio, El Universo, Vistazo y Ecuavisa dieron a conocer que, Ecuador ocupa uno de los países latinoamericanos con mayor amenaza en la ciberseguridad argumentando que existe un alto índice de analfabetismo digital y falta de conciencia en el uso de redes sociales, tecnologías, sistemas informáticos generando que el impacto del malware a través de la difusión de softwares maliciosos demuestre una gran afectación en la seguridad cibernética del país.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Después del respectivo análisis jurídico analítico, doctrinal y comparativo del alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética para determinar las dificultades en la investigación de delitos informáticos o cibernéticos se concluye lo siguiente:

La normativa jurídica en el Ecuador es insuficiente para abordar específicamente los delitos informáticos debido a la falta de tipificación específica de las nuevas conductas delictivas en temas de ciberataques, la falta de convenios de cooperación internacional e inexistente regulación de manuales y protocolos de procedimientos investigativos entre la fiscalía y la policía judicial específica para la identificación y análisis de malware, así como para investigación, guarda y compilación de evidencias digitales en estos casos. Esto se suma a que en la realidad investigativa los peritos y fiscales enfrentan varias dificultades como: la falta de conocimientos técnicos informáticos, mal manejo de la evidencia digital, falta de estrategias metodológicas y transnacionalidad del delito.

El malware es un software malicioso, que se constituye como una herramienta delictiva capaz de perjudicar seriamente la ciberseguridad; vulnerando la confidencialidad, integridad, privacidad y disponibilidad de los sistemas de información. Sin embargo, a pesar de su rol predominante en: el cifrado de datos y documentos electrónicos; envío de anuncios, códigos y archivos maliciosos; ejecución de ataques directos a la privacidad mediante las técnicas de spyware o adware; clonación de páginas web y aplicaciones legítimas; suplantación o falsificación de direcciones IP; colocación de softwares de vigilancia de actividades de navegación, ubicación o comunicación sin consentimiento. No existe una tipificación específica dentro de la normativa penal que sancione claramente su desarrollo, ejecución, adquisición, distribución y posesión como un delito autónomo.

Finalmente, a través del análisis relacional, se ha identificado que el país carece de los mecanismos necesarios para enfrentar las crecientes amenazas cibernéticas. La falta de un debate serio por parte de los legisladores sobre la importancia de la seguridad cibernética y la insuficiente capacitación especializada de los agentes investigadores destacan una falta de preocupación sobre importancia de la seguridad cibernética en el Ecuador.

5.2. Recomendaciones

Se recomienda fortalecer la estructura jurídica y técnica del país, adherirse a tratados internacionales como el convenio de Budapest y elaborar un Manual de Informática Forense en el que se determine las directrices específicas y los protocolos de actuación para la identificación y análisis de malware, así como para investigación, guarda y compilación de evidencias digitales; lo que permitirá enfrentar las dificultades presentes en la investigación de los delitos informáticos perpetrados mediante el malware.

Se recomienda considerar la siguiente propuesta reformatoria al artículo 232 del Código Orgánico Integral Penal, para agregar el siguiente numeral que tipifique la conducta de ataques de malware añadiendo lo siguiente:

> ***Art.232.1.-Ataques de malware****: la persona que desarrolle, ejecute, adquiera, distribuya o posea un software malicioso con el propósito de dañar, destruir, interferir, alterar, sustraer información de sistemas informáticos, cifrar datos y documentos electrónicos, enviar anuncios, códigos y archivos maliciosos, realizar ataques directos a la privacidad mediante las técnicas de spyware o adware, clonar páginas web y aplicaciones legítimas, suplantar o falsificar direcciones IP, enviar softwares de vigilancia de actividades de navegación, ubicación o comunicación sin consentimiento será sancionado con pena privativa de libertad de tres a cinco años.*
>
> *La pena se agravará en un tercio si la infracción es cometida mediante un software malicioso para afectar la infraestructura crítica del Estado destinada a la seguridad nacional del país.*

Se recomienda a los legisladores ejercer una vigilancia crítica sobre los marcos legales y retomar debates que integren los temas de ciberseguridad, ciberdefensa y ciberinteligencia. Así como, instruir constantemente a los agentes investigadores sobre conocimientos informáticos que ayuden al esclarecimiento del proceso investigativo de las conductas delictivas cometidas mediante el malware.

REFERENCIAS

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware Detection Issues, Challenges, and Future Directions: A Survey. *Applied Sciences (Switzerland)*, *12*(17). https://doi.org/10.3390/app12178482

Agencia de Ciberseguridad de la Unión Europea (ENISA). (2020). *MALWARE*.

Alodat, I. (2022). Malware: Detection and Defense. *Intech*, *11*(tourism), 13. https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics

Alvarado, J. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. *Revista Científica Aristas*, *2*(1), 18–27. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

Aparicio, V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(1), 1057–1063. https://doi.org/10.51798/sijis.v3i1.284

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

Assoline, F. (2024). *Amenazas en Ecuador: malware, phishing y el rol de la inteligencia de amenazas*. https://itahora.com/2024/09/03/amenazas-en-ecuador-malware-phishing-y-el-rol-de-la-inteligencia-de-amenazas/

Ávila, Ó. (2022). *Diagnóstico de las capacidades de ciberseguridad*.

Barquera, S. (2020). Antologías para el estudio y la enseñanza de la ciencia política. *Analytical Biochemistry*, *11*(1), 1–5. http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/

Belcic, I. (2023). *¿Qué es el malware y cómo funciona?* https://www.avast.com/es-es/c-malware

Brito, F. (2023). Metodología doctrinal en el derecho administrativo de la UE: reaccionar frente a la "impronta estatal." *Revista de Derecho Público: Teoría y Método*, *8*(2021), 7–69. https://doi.org/10.37417/rdp/vol_8_2023_1953

Carrers, F., & Aguilar, M. (2020). Guía integral de empleo de la informática forense en el proceso penal del Ecuador. *Revista Científica de La Universidad de Cienfuegos*, 1–14.

Carrillo, P. (2024). *La seguridad digital se hunde en el pantano político*. https://www.labarraespaciadora.com/ciberespacio/la-seguridad-digital-se-hunde-en-el-pantano-politico/

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & John, S. (2020). *Data Integrity : Detecting and Responding to Ransomware and Other Destructive*.

Centro de Respuesta a incidentes informáticos del Ecuador. (2023). Alertas de seguridad. *Agencia de Regulación y Control de Las Telecomunicaciones*, 1–11. https://web.pharmacyboardkenya.org/safety-alerts/

Consejo de Europa. (2024). *Budapest Convenio sobre la Ciiberdelincuencia*. 8–11.

Constitución de La República Del Ecuador (2008).

Debate Sobre El Proyecto de Ley de Seguridad Digital, 1 (2024).

Diaz, I., Ojeda, P., Cajas, C., & Cabrera, E. (2023). *Desafios legales en Ecuador frente a los delitos informáticos, importacia de su prevención*. 746–754.

Disemadi, H. (2022). Lensa Penelitian Hukum: Esai Deskriptif tentang Metodologi Penelitian Hukum. *Jurnal of Judicial Review*, *24*(2), 289–304. http://dx.doi.org/10.37253/jjr.v

Durán, S. (2024). *Ley de Seguridad Digital en Ecuador preocupa a la industria*. https://dplnews.com/ley-de-seguridad-digital-en-ecuador-preocupa-a-industria/

Echevería, M., Garaycoa, M., & Tusev, A. (2020). *¿Están preparados los millennials ecuatorianos contra un ataque informático? 2020*, 73–86.

Ecuavisa. (2024). *¿Cómo funcionan las estafas por mensaje de texto en Ecuador?*

El Comercio. (2022a). *BlackCat, el ataque multinivel que amenaza a la ciberseguridad del Municipio de Quito - El Comercio*. https://www.elcomercio.com/actualidad/blackcat-ataque-hackers-municipio-quito.html

El Comercio. (2022b). *Ciberdelincuentes operan de cuatro formas en el Ecuador - El Comercio*. https://www.elcomercio.com/actualidad/seguridad/ciberdelincuencia-ecuador-organizaciones-delictivas-victimas.html

El Universo. (2024). *Ecuador es el tercer país con las mayores amenazas cibernéticas en América Latina, según Check Point*. https://www.eluniverso.com/noticias/ecuador/ecuador-enfrenta-un-creciente-riesgo-de-ciberataques-en-el-2024-nota/

ENISA. (2020). Malware. *European Union Agency for Cybersecurity*, *April*, 24. https://www.enisa.europa.eu/publications/malware

Enríquez, L. (2022). *Hacia una cultura de "Valor al Riesgo" en la ciberseguridad del Ecuador - Observatorio Ciberderechos y Tecnosociedad*. https://www.uasb.edu.ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/

Estrasburgo, F. (2024). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios*. 8–11.

Estrategia Nacional de Ciberseguridad Del Ecuador, Ministerio de Telecomunicaciones y de la Sociedad de la Información 30 (2022). https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Fernández, D., & Vázquez, M. (2022). Main types of computer crimes existing in Ecuador. *Journal of Social Problems Research*, *1*(1), 50–59. https://doi.org/10.54216/jspr.010106

Franjić, S. (2020). Cybercrime is very dangerous form of criminal behavior and cybersecurity. *Emerging Science Journal*, *4*(Special Issue), 18–26. https://doi.org/10.28991/esj-2020-SP1-02

Goni, O., Md. Haidar Ali, Showrov, Md. Mahbub Alam, & Md. Abu Shameem. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2), 16–24. https://doi.org/10.56556/jtie.v1i2.113

Gorban, V. S., & Gruzdev, V. S. (2022). Sobre la diversidad de doctrinas jurídicas puras. *Sergeevich, Gorban Sergeevich, Gruzdev*, *11*, 32–43. https://doi.org/10.7256/2454-

0706.2022.11.39415
Guía de Ciberataques, Gobierno de España (2020).
Heredia, J. (2021). *Ciberseguridad en Ecuador y Latinoamérica*.
Jumbo, T. M. (2017). Metodología para el análisis de malware en un ambiente controlado. *Universidad Politécnica Salesiana Sede Cuenca*. http://dspace.ups.edu.ec/handle/123456789/14202
K Malik, Jitender, & Choudhury, D. S. (2020). Illegal Access to a Computer System: White Collor Crime in India. *Scholars Bulletin*, *6*(12), 262–268. https://doi.org/10.36348/sb.2020.v06i12.003
Leyva, A. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. *Polo*, *56*(3), 1229–1250. https://doi.org/10.23857/pc.v6i3.2431
Majeed, N. (2023). *On historical and historical - legal research : forms , challenges and methodologies*. *07*, 4–7.
Maricruz, J., Zambrano, L., Adrián, J., Peralta, P., Arturo, M., & Argudo, A. (2021). *Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación uruguaya desde un enfoque de ciberseguridad y delitos informáticos*. *669*.
Márquez Díaz, J. E. (2017). Armas cibernéticas. Malware inteligente para ataques dirigidos. *Ingenierías USBMed*, *8*(2), 48–57. https://doi.org/10.21500/20275846.2955
Martins, B. (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina*.
Mazurczyk, W., & Caviglione, T. L. (2015). *Information Hiding as a Challenge for Malware Detection*.
McAfee. (2021). Temores pandémicos y banca movil son objetivos populares del malware. *McAfee Móvil*.
Me, U., Sharath, R., Sujith, S., & Vasanth, K. (2023). *Detección de intrusos en la red mediante el uso de la máquina Aprendiendo*. 1–8.
Nadareishvili, I., General, F., & Kakulia, G. S. (2022). *Análisis de problemas procesales en las investigaciones de delitos cibernéticos*. *2022*, 131–145.
Nehinbe, J. (2022). Classification Models for Preventing Juvenile Crimes Committed with Malware Apps. *ICT Security Solutions*, *W/Africa *Address*, *i*(tourism), 13. https://doi.org/http://dx.doi.org/10.5772/57353
Onofa, M. (2022). *Ataques cibernéticos amenazan seguridad en Ecuador - Diálogo Américas*. https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/
Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Estuarine, Coastal and Shelf Science*, *2020*(1), 473–484.
Ortolani, S., Giuffrida, C., & Crispo, B. (2010). *Profiling Memory Usage Patterns for Keylogging Detection*. *217*(Raid), 2010.
Peláez, F. (2022). *El Malware en el fenómeno de la ciberdelincuencia*. https://www.economistjurist.es/articulos-juridicos-destacados/el-malware-en-el-fenomeno-de-la-ciberdelincuencia/
Política Nacional de Ciberseguridad (2021).
Primicias. (2023). *Ciberatacantes usan correos falsos de demandas judiciales en Ecuador*. https://www.primicias.ec/noticias/tecnologia/ciberataque-correos-demandas-

judiciales/

Radu, A. (2023). *Métodos para detectar malware mediante estático y dinámico y análisis híbrido*. *X*, 258–265.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Resolución No. 34 FGE-2022 (2022).

Rodríguez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. *Revista UIS Ingenierías*, *20*(3), 19–45. https://doi.org/10.18273/revuin.v20n3-2021002

Rosas, G., & Pila, G. (2023). La protección de datos personales en Ecuador. *Revista Cálamo*, *13*, 6–33. https://doi.org/10.61243/calamo.13.156

Rossinskaya, E., & Ryadovskiy, I. (2020). The Concept of Malware as a Means of Committing Computer Crimes: Classification and Methods of Illegal Use. *Russian Journal of Criminology*, *14*(5), 699–709. https://doi.org/10.17150/2500-4255.2020.14(5).699-709

Ruiz, F. (2022). *La ingeniería social y el phishing*. *8*.

Sahat Tobing, M., Wulandari, U., & Sari Sihotang, M. (2023). Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime. *Jurnal Hukum Dan Sosial Politik*, *1*(2), 60–67.

Salazar, D., Posada, R., Del Pino, S., Llumiquinga, G., & Chávez, F. (2021). Ciberdelitos. *Revista Científica de Ciencias Jurídicas, Criminológicas y Seguridad*, *11*(1), 1–5. http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/

Saltos, M., Robalino, J., & Pazmiño, L. (2021). *Análisis conceptual del delito informático en Ecuador*. http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Sanz, M. (2022). *Alcance del constructo*. https://typeset.io/papers/alcance-del-constructo-analogia-2hcoryl1zz

Shackelford, S., & Kastelic, A. (2014). *¿Hacia una paz cibernética centrada en el Estado? Análisis del papel de las estrategias nacionales de ciberseguridad en la mejora de la ciberseguridad globa*.

Sunil, C., Pawar, C., Mente, S., Bapu, R., & Chendage, D. (2021). Cyber Crime, Cyber Space and Effects of Cyber Crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3307*, 210–214. https://doi.org/10.32628/cseit217139

Tamayo, S., & Delgado, M. (2023). Preparación policial para responder al delito informático en Ecuador. *Podium*, *44*, 17–36. https://doi.org/10.31095/podium.2023.44.2

Tavella, F. (2022). *Campaña de malware dirigida a organismos de alto perfil de Ecuador*. https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/

Toapanta, M., Mera, H., Naranjo, B., & Mafla, L. (2020). Analysis of security mechanisms to mitigate hacker attacks to improve e-commerce management in Ecuador.

Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, 242–250. https://doi.org/10.1109/ICICT50521.2020.00044

Uiolibre. (2024). *Ecuador, una de las naciones más atacadas por los 'hackers.'* https://www.uiolibre.com/ecuador-una-de-las-naciones-mas-atacadas-por-los-hackers/

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*, 50–62. https://doi.org/10.37957/rfd.v6i1.88

Vistazo. (2023). *Hackers al acecho: Esto se sabe sobre una campaña de malware dirigida a Ecuador que utiliza correos sobre demandas judiciales falsas*. https://www.vistazo.com/actualidad/nacional/hackers-campana-de-malware-dirigida-a-ecuador-DK5693335

Witker, J. (2021). Metodología de la Investigación Jurídica. In *Jurnal Sains dan Seni ITS* (Vol. 6, Issue 1). http://repositorio.unan.edu.ni/2986/1/5624.pdf%0Ahttp://fiskal.kemenkeu.go.id/ejournal%0Ahttp://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1

Legislación

Constitución de La República Del Ecuaor (2008).

Código Orgánico Integral Penal (2014).

Ley de Comercio Electronico, Firmas y Mensajes de Datos, 1 (2002). https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf?fbclid=IwAR2PhfFJMvEU4S0R_nYNE2--YV9mjaGvZ-eTb0efkBpKn5QEgmnrIwJeGMA

Ley de Fraude y Abuso de Computadoras (1986).

Ley Orgánica de Protección de Datos Personales (2021).

Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, 1 (2024).

Reforma Código Orgánico Integral Penal, COIP (2021).

Reforma Norma Técnica Que Regula El Proyecto de Gobierno Electrónico (2024).

Reforma Reglamento de Políticas de Seguridad de La Información (2023).

ANEXOS

Guía de entrevista aplicada los agentes fiscales de la provincia de Chimborazo

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLITICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

GUIA DE ENTREVISTA

Fecha: _____ **Hora**: _____

Lugar (ciudad y sitio específico): _____

Entrevistado (a): _____

Objetivo: Determinar la percepción del agente fiscal sobre la eficacia de la normativa ecuatoriana relacionada a la investigación preprocesal y procesal penal ante los delitos informáticos cometidos mediante el uso de malware comprendiendo el procedimiento legal.

Consentimiento informado:

Estimado entrevistado/a, antes de iniciar con la entrevista, es relevante mencionar que la misma está diseñada como parte de un estudio de investigación titulado " **Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética**". Por ello, aseguramos que sus respuestas serán tratadas con estricta confidencialidad y solo serán utilizadas con fines de investigación académica, de manera que garantizamos la confidencialidad de sus respuestas en todo momento. Para ello, requerimos su consentimiento informado sobre su participación en esta entrevista, ya que esta es completamente libre y voluntaria ¿está de acuerdo con participar en esta entrevista?

Preguntas:

Dimensión 1: Marco legal

Objetivo: Evaluar la adecuación de la normativa vigente para abordar delitos informáticos cometidos mediante el malware y si cubre todos los aspectos necesarios para una persecución efectiva.

1. ¿Cómo evalúa usted la efectividad de la normativa actual en Ecuador para abordar los delitos informáticos cometidos mediante el malware?
2. ¿Considera que existen vacíos legales o áreas que requieren mayor regulación para mejorar la persecución de estos delitos?
3. Desde su punto vista, ¿Qué mejoras legislativas podrían fortalecer la investigación de nuevos delitos informáticos?

Dimensión 2. Prácticas y Procedimientos

Objetivo: Evaluar las prácticas y procedimientos actuales utilizados en la investigación y acusación de delitos informáticos y su efectividad.

4. ¿Existe un procedimiento establecido en la norma para la investigación y acusación en cuanto a los delitos informáticos?
5. Desde su experiencia ¿Cómo se lleva a cabo la cadena de custodia para asegurar la integridad de las evidencias digitales relacionadas con delitos informáticos?
6. ¿Considera que existen desafíos en la práctica diaria al investigar y acusar delitos informáticos cometidos con malware?
7. Bajo su experiencia, ¿Cuáles son los elementos convicción relevantes para demostrar la materialidad y responsabilidad en los delitos informáticos cometidos a través del uso del malware?

8. Considerando la transnacionalidad del delito, ¿Cómo se determina la competencia para la investigación de los delitos informáticos?

Dimensión 3. **Eficacia institucional y estrategias en ciberseguridad**
Objetivo: Evaluar la capacidad técnica y la efectividad de las instituciones ecuatorianas en la implementación y ejecución de estrategias de ciberseguridad.

9. ¿Cómo evalúa la capacidad de las instituciones ecuatorianas para detectar, investigar y procesar los delitos informáticos que involucran malware?
10. ¿Qué tan efectivo considera que es el marco de cooperación internacional para la persecución de delitos informáticos?

Dimensión 4: **Delitos informáticos y el impacto en los bienes jurídicos protegidos**
Objetivo: Analizar cómo los delitos informáticos, específicamente los ataques de malware afectan a los bienes jurídicos protegidos y evaluar si la normativa legal actual proporciona una protección adecuada.

11. En base a su criterio, en los delitos informáticos ¿Cuáles son los bienes jurídicos protegidos que se ven afectados?

Guía de entrevista aplicada al perito informático

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

GUIA DE ENTREVISTA

Fecha: _____ **Hora:** _____

Lugar (ciudad y sitio específico): _____

Entrevistado (a): _____

Objetivo: Entender como los peritos informáticos definen el malware y describen su funcionamiento técnico como herramienta para cometer delitos informaticos afectando a la seguridad cibernética.

Consentimiento informado:

Estimado entrevistado/a, antes de iniciar con la entrevista, es relevante mencionar que la misma está diseñada como parte de un estudio de investigación titulado " **Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética"**. Por ello, aseguramos que sus respuestas serán tratadas con estricta confidencialidad y solo serán utilizadas con fines de investigación académica, de manera que garantizamos la confidencialidad de sus respuestas en todo momento. Para ello, requerimos su consentimiento informado sobre su participación en esta entrevista, ya que esta es completamente libre y voluntaria ¿está de acuerdo con participar en esta entrevista?

Preguntas:

Dimensión 1: Naturaleza del malware

Objetivo: comprender las características técnicas del malware como herramienta para cometer delitos informáticos.

1. Desde su punto de vista, ¿Cómo actúa el malware y cuáles son sus características funcionales?
2. ¿Podría explicar qué tipos de malware ha identificado con mayor frecuencia en la comisión de delitos informáticos?
3. ¿Qué particularidades técnicas hacen que el malware sea efectivo para cometer delitos informáticos?

Dimensión 2: Análisis Forense de Malware

Objetivo: Explorar las técnicas y herramientas utilizadas para detectar y analizar el malware en investigaciones forenses.

4. ¿Cómo aborda usted el uso de técnicas y herramientas fundamentales para el análisis forense de malware?
5. Según su experiencia, ¿Cuáles son los desafíos más comunes en la detección de malware durante una investigación?
6. De acuerdo a su experticia, ¿Qué evidencia digital considera que es relevante para demostrar el uso de malware en un delito informático?

Dimensión 3: Evaluación Técnica de la Normativa Legal
Objetivo: Determinar la percepción técnica de los peritos sobre la adecuación y aplicabilidad de la normativa ecuatoriana en la lucha contra el malware.

7. ¿Cómo evalúa la normativa ecuatoriana actual en términos de especificidad técnica para abordar delitos de malware, existen manuales para la investigación de este tipo de delitos?
8. ¿Qué tan efectivo considera que es el marco de cooperación internacional para la persecución de delitos informáticos?

Validación del instrumento

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Francisco Freire

Especialidad: Penal

Titulo de la investigaciòn: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir): Determinar la percepción del agente fiscal sobre la eficacia de la normativa ecuatoriana relacionada a la investigación preprocesal y procesal penal ante los delitos informáticos cometidos mediante el uso de malware comprendiendo el procedimiento legal.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓			✓	✓		✓			
2	✓		✓			✓	✓		✓			
3	✓		✓			✓	✓		✓			
4	✓		✓			✓	✓		✓			
5	✓		✓			✓	✓		✓			
6	✓		✓			✓	✓		✓			
7	✓		✓			✓	✓		✓			
8	✓		✓			✓	✓		✓			
9	✓		✓			✓	✓		✓			
10	✓		✓			✓	✓		✓			
11	✓		✓			✓	✓		✓			

Firma de Validador

Nombre: Francisco Freire

Cèdula: 0602469991

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Francisco Freire

Especialidad: Penal

Titulo de la investigaciòn: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir):

Entender como los peritos informáticos definen el malware y describen su funcionamiento técnico como herramienta para cometer delitos informáticos.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓			✓	✓		✓			
2	✓		✓			✓	✓		✓			
3	✓		✓			✓	✓		✓			
4	✓		✓			✓	✓		✓			
5	✓		✓			✓	✓		✓			
6	✓		✓			✓	✓		✓			
7	✓		✓			✓	✓		✓			
8	✓		✓			✓	✓		✓			

Firma de Validador

Nombre: Francisco Freire

Cèdula: 0602464441

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Edison Bonilla

Especialidad: Metodología de la Investigación

Titulo de la investigaciòn: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir): Determinar la percepción del agente fiscal sobre la eficacia de la normativa ecuatoriana relacionada a la investigación preprocesal y procesal penal ante los delitos informáticos cometidos mediante el uso de malware comprendiendo el procedimiento legal.

Preguntas	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	Simplificar las preguntas
1	✓		✓			✓	✓		✓			
2	✓		✓			✓	✓		✓			
3	✓		✓			✓	✓		✓			
4	✓		✓			✓	✓		✓			
5	✓		✓			✓	✓		✓			
6	✓		✓			✓	✓		✓			
7	✓		✓			✓	✓		✓			
8	✓		✓			✓	✓		✓			
9	✓		✓			✓	✓		✓			
10	✓		✓			✓	✓		✓			
11	✓		✓			✓	✓		✓			

Firma de Validador

Nombre: Edison Bonilla

Cèdula: 0602037269

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Edison Bonilla

Especialidad: Metodología de la Investigación

Título de la investigación: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir):

Entender como los peritos informáticos definen el malware y describen su funcionamiento técnico como herramienta para cometer delitos informáticos.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún item)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓			✓	✓		✓			INCLUIR PREGUNTA SOBRE SANCIONES LEGAL.
2	✓		✓			✓	✓		✓			
3	✓		✓			✓	✓		✓			
4	✓		✓			✓	✓		✓			
5	✓		✓			✓	✓		✓			
6	✓		✓			✓	✓		✓			
7	✓		✓			✓	✓		✓			
8	✓		✓			✓	✓		✓			

Firma de Validador

Nombre: Edison Bonilla

Cèdula: 0602073264

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Luis Zurita

Especialidad: Constitucional.

Tìtulo de la investigaciòn: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir): Determinar la percepción del agente fiscal sobre la eficacia de la normativa ecuatoriana relacionada a la investigación preprocesal y procesal penal ante los delitos informáticos cometidos mediante el uso de malware comprendiendo el procedimiento legal.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	/		/			/	/		/			
2	/		/			/	/		/			
3	/		/			/	/		/			
4	/		/			/	/		/			
5	/		/			/	/		/			
6	/		/			/	/		/			
7	/		/			/	/		/			
8	/		/			/	/		/			
9	/		/			/	/		/			
10	/		/			/	/		/			
11	/		/			/	/		/			

Firma de Validador

Nombre: Luis Antonio Zurita Avalos

Cèdula: 0604411249

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Luis Zurita

Especialidad: Constitucional.

Titulo de la investigaciòn: Alcance de la normativa legal ecuatoriana y el impacto del malware en la seguridad cibernética

Objetivo del instrumento (Que pretende medir):

Entender como los peritos informáticos definen el malware y describen su funcionamiento técnico como herramienta para cometer delitos informáticos.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓			✓	✓		✓			
2	✓		✓			✓	✓		✓			
3	✓		✓			✓	✓		✓			
4	✓		✓			✓	✓		✓			
5	✓		✓			✓	✓		✓			
6	✓		✓			✓	✓		✓			
7	✓		✓			✓	✓		✓			
8	✓		✓			✓	✓		✓			

Firma de Validador

Nombre: Luis Antonio Zurita Avalos

Cèdula: 0604411249

Matriz de análisis documental

MATRIZ DE ANÁLISIS DOCUMENTAL

Tipo de documento	Fuente (Autor)	Título	Fecha	Enlace	Tipo de ataque	Resumen

Elaborado por: Zambrano et. Al (2021)