UNIVERSIDAD METROPOLITANA DEL ECUADOR

FACULTAD DE CIENCIAS SOCIALES, HUMANIDADES Y EDUCACIÓN.

CARRERA: DERECHO.

SEDE: QUITO.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA.

TEMA: **“VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS”**

AUTORA

XIMENA VALERIA CANTOS MESTANZA.

ASESOR

DR. HERMES GILBERTO SARANGO AGUIRRE.

QUITO – 2021

CERTIFICACIÓN DEL ASESOR

Dr. Hermes Gilberto Sarango Aguirre, en calidad de Asesor de Trabajo de Titulación por la Dirección de la Escuela de Derecho, certifico que la señorita **XIMENA VALERIA CANTOS MESTANZA** ha cumplido el trabajo de investigación con el tema: **"VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS"**, quien ha cumplido con todos los requisitos legales exigidos, por los que se aprueba la misma.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso de la presente, así como también se autoriza la presentación para la evaluación por parte del jurado respectivo.

Atentamente.

Dr. Hermes Gilberto Sarango Aguirre.

CERTIFICACIÓN DE AUTORÍA DE TRABAJO DE TITULACIÓN

Yo, **XIMENA VALERIA CANTOS MESTANZA**, estudiante de la Universidad Metropolitana del Ecuador “UMET”, carrera de Derecho, declaro en forma libre y voluntaria que el presente trabajo de investigación que versa sobre la ¨**VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS**¨, con todas las expresiones vertidas en el mismo, son de mi autoría, las cuales se han realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la investigación y el cuidado debido al referirme a las fuentes bibliográficas respectivas para fundamentar válidamente su contenido.

Atentamente:

Firmado electrónicamente por:
XIMENA VALERIA CANTOS MESTANZA

XIMENA VALERIA CANTOS MESTANZA.

C.I. 2300260995

Autora.

CESIÓN DE DERECHOS DE AUTOR

Yo**, XIMENA VALERIA CANTOS MESTANZA** , en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación, ¨**VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS**¨, modalidad proyecto de investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, cedo a favor de la Universidad Metropolitana del Ecuador una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Metropolitana del Ecuador para que realice la digitalización y publicación de este trabajo de titulación en el repositorio virtual que se cree para tales efectos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Declaro que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
XIMENA VALERIA CANTOS MESTANZA

XIMENA VALERIA CANTOS MESTANZA

CI: 2300260995

DEDICATORIA

¡A toda mi familia!

Especialmente para mi pequeño trípode familiar que conformamos mi mami Marce, quien me enseño constantemente que todo lo que se empieza se debe terminar, a mi hermano Ángel, quien con su ejemplo de profesionalismo me enseñó a no rendirme en el transcurso de los años de formación y a mi persona, por mis esfuerzos durante toda la formación académica.

Finalmente dedico mi tesis con mucho afecto a mis abuelos Ángel y Anita.

Con mucho cariño Valeria.

AGRADECIMIENTO

Quiero agradecer a Dios por sus infinitas bendiciones, a la mujer que en todo momento me impulsó a estudiar, a mi mayor ejemplo a seguir, quien formó a sus dos hijos como profesionales, si, a ti mamá, mi hermosa Marcelita Mestanza.

Agradezco a la familia Avila, en especial a mi gran amiga Sol Avila por estar presente en buenas y malas durante los cinco años de formación profesional, siendo un soporte fundamental en el transcurso de mi carrera, formándonos como un excelente equipo académico.

Mis más sinceros agradecimientos a mi amiga y compañera de aventuras Darling, a mi gran amigo Alejandro Romero, por apoyarme en absolutamente todo a lo largo de la formación profesional.

Agradezco a mi tutor, mentor y profesor, el Dr. Hermes Sarango Aguirre por su constante apoyo en el desarrollo de mi trabajo previo a titulación.

Con mucho cariño Valeria.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

“Dónde la ley es incierta, no existe ley”

Proverbio.

RESUMEN

Tener un derecho exigible porque así lo establezca la ley y no poderlo probar, es tan grave como no tenerlo. Muchos tipos de prueba, como: las documentales, testimoniales y periciales, son ampliamente reconocidos por la doctrina y la legislación ecuatoriana ha recogido muchos de ellos, regulándolos y aplicándolos para su valoración en la administración de justicia. Ahora bien, la prueba digital sigue siendo una prueba documental, sólo que, el legislador ecuatoriano parece haberla apartado de los demás tipos de pruebas posiblemente por sus características de intangibilidad y novedad. Sin embargo, el Código Orgánico Integral Penal contempla la regulación de los delitos informáticos y en la mayoría de ellos, se deberá recurrir a la prueba digital para comprobarlos y alcanzar la verdadera justicia. En esta investigación, de tipo teórico-descriptiva y de enfoque mixto, se ha determinado que los criterios de valoración probatoria en general establecidos, así como otros componentes para la aplicación de la prueba digital adolecen de suficiente claridad como para poder dirigir el criterio del juzgador en una línea coherente, racional y equilibrada, produciéndose inseguridad jurídica a la hora de su promoción, evacuación y valoración. En aras de resolver esta problemática, se presenta una propuesta de redefinición de la prueba digital y las disposiciones legales que la disponen y reglamentan.

Palabras Clave: prueba, digital, intangibilidad, valoración, discrecionalidad judicial.

ABSTRACT

Have an enforceable right because it is established by law and not being able to prove it is as serious as not having it. Many types of evidence, especially material or physical documentaries as well as testimonials, are widely recognized by the doctrine and Ecuadorian legislation has collected many of them, regulating and applying them with the aid of judicial discretion for their assessment. Now, the digital evidence is still a documentary evidence, only that the Ecuadorian legislator seems to have separated it from the other types of evidence, possibly due to its characteristics of intangibility and novelty. However, the Comprehensive Organic Criminal Code contemplates the regulation of computer crimes and in most of them, digital evidence must be used to verify them and achieve true justice. In this research, of a theoretical-descriptive type and with a qualitative approach, it has been determined that the evidentiary evaluation criteria in general established, as well as other components for the application of the digital test, lack sufficient clarity to be able to direct the judgment of the judge in a coherent, rational, and balanced line, producing legal uncertainty at the time of its promotion, evacuation and evaluation. To solve this problem, a proposal is presented to redefine the digital evidence and the legal provisions that provide and regulate it.

Keywords: evidence, digital, intangibility, valuation, judicial discretion.

INTRODUCCIÓN

En la era digital, y especialmente con ocasión de la pandemia por COVID-19, las personas están utilizando las tecnologías de la información y de la comunicación para muchos actos de comercio, para relaciones interpersonales, para gestiones jurídicas entre un sinfín de actividades necesarias para el desarrollo social. Todas estas actividades se realizan a través de plataformas digitales, las cuales tienen un componente físico referido a equipos electrónicos y un componente digital, relacionado a las redes, internet y conectividad; ambos sometidos a riesgo de vulneración por delitos informáticos.

El Código Orgánico Integral Penal (en lo adelante COIP) desde el año 2014 tipifica en su contenido lo relativo a los principales delitos contra la seguridad de los activos de los sistemas de información y comunicación (mejor conocidos como delitos informáticos) que pudieran cometerse en el país. Entre ellos, se encuentran: la revelación ilegal de bases de datos (Art. 229), la interceptación ilegal de datos (Art. 230), la transferencia electrónica no consentida de activo patrimonial (Art. 231) el ataque a la integridad de sistemas informáticos (Art. 232), los delitos contra la información pública reservada legalmente (Art. 233) y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones (Art. 234).

Aunque el Código Orgánico Integral Penal describe cada una de estas modalidades delictivas, no ha establecido una forma clara para la demostración de estos dentro del respectivo procedimiento. Es decir, se encuentra en el referido Código una descripción de posibles medios probatorios y de unos criterios de valoración para dichos medios en general, pero la realidad es, que la principal prueba necesaria en tales casos, que sería la prueba documental de contenido digital, aparece tan restringida que podría dejar en estado de indefensión a las partes afectadas o víctimas de los delitos informáticos.

Esa indefensión es el principal problema que pretende tratar esta investigación, al contrastar lo regulado para la prueba de contenido digital con lo referente a los criterios de valoración de la prueba establecidos en el COIP porque, al parecer, la

aplicación práctica de los preceptos que lo contienen (Arts. 500 y 457) no es congruente ni garantiza la valoración de algunos medios probatorios. De esta hipótesis parte el investigador, planteando como formulación del problema la siguiente interrogante: ¿Cómo establecer criterios de valoración idóneos para regular la prueba de contenido digital mediante el uso de los criterios establecidos en el art. 457 del COIP en los procedimientos de delitos informáticos?

Los criterios de valoración de la prueba establecidos en el artículo 457 antes mencionado, no presentan mayores problemas cuando se trata de los medios probatorios más utilizados como serían la prueba documental no solo contemplada en el COIP y como fuente supletoria contemplada en el art. 193 y siguientes del Código Orgánico General de Procesos, la prueba testimonial y la prueba pericial porque las mismas tienen un mejor desarrollo en el Código, en la doctrina y en la jurisprudencia nacional a pesar de que los criterios de valoración hayan sido escuetamente presentados por el legislador. Sin embargo, en cuanto a la prueba de contenido digital, pueden encontrarse discrepancias en el texto normativo que llegarían a hacer ineficaz la promoción de dicha prueba y con ello, lesionar el derecho a la defensa de las partes.

La idea de la investigación es descubrir si la prueba documental de contenido digital que regula el artículo 500 del Código Orgánico Integral Penal, por su conformación y consideraciones, guarda la suficiente coherencia con las disposiciones referidas a otros medios de prueba en general y muy especialmente, si los criterios de valoración existentes en la ley pueden aplicarse de la misma manera que se haría con medios probatorios de otro tipo de contenido.

La investigación se realizará bajo el diseño no experimental, obedeciendo las formalidades de un estudio de tipo teórico-documental, con enfoque mixto a través de los métodos de la investigación jurídica, tales como el análisis comparativo, el deductivo, y la interpretación objetiva de los datos.

La investigación se realizará bajo el diseño no experimental, obedeciendo las formalidades de un estudio de tipo teórico-documental, con enfoque mixto a través de

los métodos de la investigación jurídica tales como el análisis comparativo, el deductivo, y la interpretación objetiva de los datos.

El objetivo general de la investigación se concreta en establecer la idoneidad de los criterios de valoración legal existentes en el Código Orgánico Integral Penal para la prueba documental de contenido digital en los procedimientos de delitos informáticos. Se pretende alcanzar este propósito mediante los siguientes objetivos específicos:

1. Caracterizar jurídica y doctrinalmente los delitos informáticos del COIP.
2. Identificar el sistema de valoración de la prueba existente en el COIP para la prueba de contenido digital.
3. Presentar directrices de ampliación del sistema de valoración de la prueba de contenido digital en comparación con otros medios de prueba.

La estructura capitular de la tesis ha sido realizada con un capítulo correspondiente al marco teórico, el cual reúne los contenidos conceptuales, doctrinarios y legales en los cuales se fundamentará el análisis de los resultados. Seguidamente, se presenta el segundo capítulo con la metodología de la investigación, esto es, los pasos que se han seguido para realizar el trabajo de responder a los objetivos trazados para la construcción del conocimiento científico. En un tercer capítulo se presentan los resultados, propuesta y finalmente, las conclusiones y sugerencias en favor de la solución de la problemática.

Se trata así, de un trabajo innovador que contrapone los criterios considerados por el propio legislador para valorar cualquier medio de prueba frente a la disposición del artículo 500 que, al parecer, es tan restringido que puede hacer inefectiva su propia aplicación afectando en gran medida los procedimientos de delitos informáticos en los que las pruebas mayormente presentadas son documentales de contenido digital.

CAPÍTULO I

MARCO TEÓRICO

El marco teórico contiene los elementos necesarios para soportar documentalmente los resultados, en ellos se encuentran las bases del análisis deductivo y para este proyecto está comprendido por los siguientes títulos:

1.1. Antecedentes

Los antecedentes de una investigación sirven de referencia para desarrollar el tema objeto de estudio, mediante la exposición de trabajos que hasta el momento han expuesto el tema tratado.

En el año 2017, Vargas Eduardo, realizó un Proyecto de Investigación previo al título de Abogado, en la Pontificia Universidad Católica del Ecuador (Sede Ambato), titulado: Los criterios de valoración de la cadena de custodia en el procedimiento penal ecuatoriano. El objetivo de este estudio se centró en analizar el criterio de valoración de custodia para unos casos específicos, para lo cual determinó los criterios de valoración legal para la efectividad de la cadena de custodia, comprobó las circunstancias presentadas bajo las cuales se violenta la cadena de custodia y estableció los criterios de los jueces penales para el efectivo uso del criterio de valoración legal (Vargas, 2017).

El logro de estos objetivos fue posible gracias a su enfoque cualitativo, a la aplicación de un método deductivo, universal, histórico y dogmático y al empleo de la entrevista a un experto en el área, fichas nemotécnicas y el estudio de caso como técnicas de investigación.

Como principales conclusiones del estudio se encuentran: que los criterios de valoración de la cadena de custodia se ciñen rigurosamente a lo expresado en el Código Orgánico Integral Penal (COIP), en su artículo 457, sin que exista la posibilidad de que los Jueces expresen razonamientos ajustados a su sana crítica; la cadena custodia no debe estar estructurada solo en un Manual, sino que debe existir al menos

un Reglamento y su valoración no debe ser *“in integrum”*, sino singularizada, ya que cada prueba guarda cada hecho, cada paso realizado por el infractor para cometer su ilícito, por lo que no debe ser cuidada por los auxiliares de Fiscalía, sino por un personal idóneo, preparado y sobre todo, técnico.

Esta investigación es de relevancia para el trabajo en estudio, ya que brinda información sobre el tratamiento que se le ha dado al criterio de valoración: cadena de custodia, en casos propios de la realidad ecuatoriana, dado que forma parte del objeto de estudio de esta investigación.

Hidalgo (2018), elaboró un trabajo de titulación previo a la obtención del título Abogado de los tribunales y juzgados de la República, en la Universidad Católica de Santigo de Guyaquil, el cual tiene por nombre: Los delitos informáticos y su afectación sobre los bienes jurídicos, cuyo objetivo fue analizar el bien jurídico como una consagración constitucional y social y su incidencia en los delitos informáticos, con el propósito de dedicar la importancia de un estudio apropiado de éste, y en el caso de que se trate de un delito.

Aun cuando no se refleja en el estudio, se puede observar que fue de tipo documental, con las siguientes conclusiones producto de su análisis: se observa la constante ascensión de cuestiones informáticas frente al derecho de forma general, a consecuencia de su desarrollo tecnológico e inclusión en los medios y actividades sociales, acompañado de demandas populares que presionan a legisladores a crear políticas de forma rápida, pero ineficientes, al ejercer su función de proteger cierto bien público. Hay gran preocupación por el desarrollo de la tecnología, pero se dejan de lado regulaciones en cuanto a su trato, métodos y leyes que busquen frenar la nueva onda delictiva.

Por ello, el estudio recomienda una mayor cautela y consideración de los legisladores en la tipificación de los delitos informáticos, pues ésta muchas veces ocurre sin el debido estudio del tema y de los bienes a ser protegidos, a modo de evitar la no criminalización de conductas que deberían serlo, o en un tratamiento que no lleva a la protección efectiva y eficaz de tales delitos. Se defiende que antes de la

criminalización de las conductas relacionadas con la informática, se haga un estudio acerca del bien jurídico, con base en la Constitución de la República y en lo que es reclamado por la sociedad, como de la parte técnica de la reforma, a fin de que la ley o el tipo penal se hagan de manera más precisa y clara, facilitando su aplicación y el alcance de su fin.

Esta investigación es de relevancia para el trabajo en estudio, ya que sus aportes analíticos sobre el concepto de bien jurídico enfocado en los delitos informáticos, son valiosos al caracterizar jurídica y doctrinalmente dichos delitos para el caso investigativo que concierne este estudio.

Con el título: Valor probatorio de la prueba documental de contenidos digitales durante la etapa de juicio del Derecho Procesal Penal Ecuatoriano, (Dunn, 2019) desarrolló su trabajo de titulación previo a la obtención del grado de Abogada de los Tribunales y Juzgados del la República del Ecuador, en la Universidad Católica de Santigo de Guayaquil, cuyo objeto versa sobre la prueba documental, específicamente la que contenga contenido digital, para observar que en la valoración de ésta también surge la necesidad de su sometimiento a cadena de custodia y el incumplimiento de la misma, produce tal nivel de afectación que conllevaría a tildar de ineficaz a su validez probatoria.

Mediante dicha investigación, de tipo documental, se trataron los siguientes temas: proceso penal, la prueba dentro del proceso penal ordinario, la prueba en el COIP, la prueba documental, documentos digitales y valor probatorio de un documento digital, de lo cual se concluyó que la parte denunciante, la víctima o terceros, no pueden aportar documentos desmaterializados provenientes de páginas web, puesto que carecerían de suficiencia probatoria, por ser considerados copias certificadas y no poder ser sometidos a la cadena de custodia. La vía correcta es solicitar al titular de la acción penal, que a su vez solicite al Juez de garantías penales la intercepción de las comunicaciones o datos informáticos, ya que sólo por esa vía quedarían subsanados los obstáculos de cosentimiento y cadena de custodia.

Esta investigación es de relevancia para el trabajo en estudio, ya que tanto su componente teórico como sus señalamientos sobre la importancia de llevar un correcto procedimiento de cadena de custodia a la prueba digital, enriquecen el estado del arte asociado a esta investigación.

(Zumba, 2015), en la Universidad de Cuenca, elaboró una monografía titulada: "Delitos contra la seguridad de los activos de los sistemas de información y comunicación: delitos a través de las redes sociales", con el objetivo de dar a conocer los delitos informáticos que pueden cometerse, quienes lo hacen, las víctimas de estos delitos, y la pertinencia e introducción de la prueba al proceso en este tipo de delitos.

El contenido que abarca esta investigación documental, está conformado por los aspectos: generalidades acerca de las redes sociales, el delito informático, los delitos tipificados en el COIP, y la prueba pericial informática en la legislación ecuatoriana, de cuyo desarrollo, (Zumba, 2015) concluye: el gran avance tecnológico en materia de comunicación, presenta tanto ventajas como desventajas, ya que la variedad de servicios que presta la red de internet, es aprovechada por sujetos como herramienta para causar daño, ya sea por diversión o por un interés personal o a favor de un tercero, violentando derechos fundamentales reconocidos y garantizados en la Constitución y tratados internacionales. Además, aun cuando se cuenta con cuerpos normativos que regulen conductas de esta índole, no resultan suficientes para combatir la cyberdelincuencia, aunado a que el seguimiento a los delitos informáticos se torna complejo ante la existencia mínima de peritos calificados (por el Consejo de la Judicatura del Azuay) y la facilidad que brinda la misma informática para borrar toda clase de evidencia.

Esta investigación es de relevancia para el trabajo en estudio, ya que expone aspectos relacionados con la sección tercera del COIP: delitos contra la seguridad de los activos de los sistemas de información y comunicación, y su pertinencia en la resolución de casos inherentes, lo cual contribuye en el tratamiento de los objetivos específicos de esta investigación.

Como apoyo a los estudios de Corte Nacional, se han encontrado los siguientes de origen internacional, los cuales se incorporan al estudio por incluir temas que aportan al análisis que se realizará.

(Rodríguez, 2018), realizó en España un trabajo de fin de máster titulado: La prueba digital en el proceso penal, con el objetivo de estudiar la prueba digital en el proceso penal, y la necesidad, en muchas ocasiones, de recurrir a la pericial informática para acreditar la autenticidad de la misma.

En este estudio de corte documental, (Rodríguez, 2018) enfatizó en el análisis de las fases de la prueba digital, su obtención y vulneraciones de Derechos Fundamentales que pueden producirse y que darán lugar a una prueba digital ilícita; la incorporación de la fuente de prueba al proceso, así como su valoración en el mismo; el examen de la cadena de custodia y las consecuencias de la manipulación y posterior aportación de esta tipología de pruebas al proceso.

Como principales conclusiones, el estudio arrojó que en el país de realización no hay un concepto legal para la prueba digital; son numerosas las ocasiones en que la jurisprudencia, ante una inmisión policial sin autorización judicial, justifica que pudiera haber quebrantado el derecho a la intimidad, el cual siempre cede, ya que éste no precisa necesariamente de autorización judicial y en muchos casos esta premisa escuda la aprehensión de dispositivos electrónicos para el visionado de su contenido; la obtención de la prueba digital a través del registro remoto del dispositivo electrónico, plantea problemas relativos a su acreditación.

Otras conclusiones advierten que los casos que requieran de una pericial informática presentan dificultades para llegar a buen fin en el marco de un proceso, para quien no puede asumir los costos de la realización de un informe pericial que dictamine sobre la veracidad de la misma; en ocasiones la jurisprudencia ha otorgado valor de prueba de cargo con aptitud para desvirtuar la presunción de inocencia, a pruebas cuya custodia ha sido deficiente por no haber sido preservada íntegramente la cadena de custodia; Quizás se lograse la observancia de dichas garantías técnicas premiando y promoviendo la utilización de normas para la recopilación de evidencias

que den indicaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales.

Esta investigación es de relevancia para el trabajo en estudio, ya que resalta la importancia de que se explicite en la ley el tratamiento de la prueba digital, en conjunto con un adecuado protocolo de preservación de la evidencia digital, información de utilidad en la presentación de directrices de mejora al sistema de valoración de la prueba digital, como parte del desarrollo de esta investigación.

Finalmente, (Morillo & Herrero, 2011), elaboró en Costa Rica una tesis titulada: La prueba ilícita y la cadena de custodia en el Ordenamiento Jurídico Costarricense. Alcoholemias y pruebas con alcoholímetro, con el objetivo de analizar y estudiar el concepto de la prueba ilícita, para determinar la importancia de la cadena de custodia y sus implicaciones en el procedimiento de alcoholemias y de pruebas con alholímetro.

Dicho trabajo se apoyó metodológicamente en un análisis doctrinario, jurisprudencial y en una investigación de campo, cuyas más relevantes conclusiones para el tema de estudio fueron: la prueba debe cumplir con los requisitos de objetividad, legalidad, relevancia, pertinencia, integridad e identidad; en Costa Rica rige el sistema de la libre convicción o la sana crítica racional, mediante el cual el juzgador valora las pruebas con base en las reglas de la psicología, la lógica y la experiencia; la aplicación de excepciones a las reglas de exclusión de valoración de la prueba obtenida ilícitamente, revitaliza los derechos y garantías del imputado, dando paso a confundir el respeto de los derechos procesales con impunidad.

De igual manera, (Morillo & Herrero, 2011) concluyó que no existe en el país del estudio, una norma especializada que trate con profundidad el tema de la cadena de custodia, por lo que encuentra su fundamento en la protección constitucional que se le da garantía al Debido Proceso y al Derecho de Defensa y en los principios básicos de Dignidad Humana y Libertad; al existir esta laguna legal sobre el tema de cadena de custodia, existe también un desconocimiento importante por parte de los sujetos procesales encargados, lo que dificulta la debida protección de los elementos

probatorios y puede generar la ilicitud de la prueba recabada en un escenario del crimen, con la consecuente impunidad del sujeto culpable.

Pese a que el tema sobre Alcoholemia y pruebas con alcoholímetro se escapa del interés para esta investigación, el trabajo de (Morillo & Herrero, 2011), es de relevancia para la investigación en estudio, pues podría aportar en cuanto a que se detallan meticulosamente aspectos en torno a la prueba, principios y medios, producto de análisis jurisprudencial, definir posibles lagunas legales que podrían mitigarse con la presentación de propuestas de ajuste a la normativa jurídica pertinente al tema objeto de estudio.

1.2. Terminología básica

1.2.1. Delitos informáticos

Aun cuando resulta difícil universalizar un concepto de delitos informáticos, se puede definir en un sentido general, como “Toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas” (Mata y Martín, 2003), como el computador.

Resulta conveniente incorporar unos conceptos que (Mora, y otros, 2014) señalaron, como producto de cuatro posturas doctrinarias:

Tabla 1. Posturas doctrinarias de los delitos informáticos

Postura 1: Uso de la informática como método y fin	Postura 2: la información o datos procesados como bien protegible	Postura 3: no existencia de un nuevo tipo de delito	Postura 4: Teoría ecléctica
Toda conducta ilícita sancionada por el ordenamiento jurídico, que hace uso indebido de las computadoras como medio o instrumento	Toda conducta que involucre características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el	Son hechos ilícitos que se cometen mediante el empleo del computador, siendo en principio los mismos que desde hace miles de	Todo comportamiento ilícito que atente contra los sistemas de procesamiento de información o los datos procedentes de

para la comisión de un delito.	soporte lógico de un sistema de procesamiento de información, el cual se distingue de los delitos computacionales o tradicionales informatizados.	años fueron castigados: contra la persona, el honor, la seguridad pública y de la nación hurtos, entre otros.	éstos, que pueda ser tipificado y sancionado por el Derecho Penal.

Fuente: (Mora, y otros, 2014)

Otras posturas también lo llaman como Cibercrimen o Ciberdelito. Bajo este término, (Posada, 2017) lo define como todo comportamiento que atenta contra la seguridad de las funciones informáticas, e incluso puede poner en peligro otros bienes jurídicos, rompiendo toda dinámica probatoria propia de los delitos comunes, dada su riqueza técnica, su virtualidad, el daño a objetos intangibles y su deslocalización en el ciberespacio (pp.81-82).

1.2.2. Prueba

La palabra prueba, “deriva del término latín *probatio* o *probationis*, que a su vez procede del vocablo *probus* que significa bueno” (Morillo & Herrero, 2011), de lo que se puede inferir, que el acto de hacer una prueba es hacer algo bueno.

Desde la doctrina, se pueden encontrar diversas definiciones del concepto “prueba”: Bentham, citado por (Morillo & Herrero, 2011), la define como un “hecho supuestamente verdadero que se presume debe servir de motivo de credibilidad sobre la existencia o inexistencia de otro hecho (…) la prueba es un medio que se utiliza para establecer la verdad de un hecho” (p.7).

(Taruffo, 2008), la define como “el instrumento que utilizan las partes desde hace siglos para demostrar la veracidad de sus afirmaciones, y del cual se sirve el juez para decidir respecto a la verdad o falsedad de los enunciados fácticos” (p.59). Destacan otros conceptos también aportados por (Taruffo, 2008): La prueba como un instrumento de conocimiento y la prueba como un instrumento de persuasión.

Como instrumento de conocimiento, ofrece informaciones referentes a hechos que deben ser determinados en el proceso: es un instrumento que da información relacionada con el contenido de un enunciado y su contexto, con el efecto de que dicho enunciado puede ser verdadero o falso en función de la(s) prueba(s) que a él refieren; un hecho ha sido conocido por pruebas que demuestran la veracidad de un enunciado correspondiente; en el proceso no existen verdades absolutas, pues cualquier conclusión del Juez producto del análisis de las pruebas, dependerá de aquellas que se incorporaron en el proceso (Taruffo, 2008).

Como instrumento de persuasión, la prueba no tendría nada que ver con el conocimiento de los hechos, por lo que no serviría para decretar si un enunciado es verdadero o falso o para aportar algún conocimiento. Sólo serviría para convencer al Juez, acerca de un enunciado con o sin fundamento. Bajo este concepto, en el juicio prevalecen los discursos y narraciones realizadas en el proceso, con lo cual un enunciado se podría definir como verdadero si el Juez está persuadido, y en esta situación, cualquier cosa está probada. Por lo tanto, resulta difícil analizar las características y estructura de la prueba, en el marco de esta concepción, dado que implica una concepción irracional de la prueba judicial. No vale ni siquiera la discusión de si el Juez tiene una posición correcta o equivocada, ya que ello supondría recurrir a una explicación descriptiva o normativa de la prueba, mientras que las persuasiones no son correctas o equivocadas, verdaderas o falsas: sólo existen o no ante un Juez. (Taruffo, 2008)

En el ámbito legal del Derecho Penal ecuatoriano, la prueba se establece en el Título IV del COIP, aspecto que se abordará en la parte concerniente a las bases legales.

1.2.3. Medios probatorios

El medio de prueba es el acto mediante el cual el juez u órgano de prueba revela y consigna el objeto de prueba afirma Florián, citado por (Morillo & Herrero, 2011).

De este concepto es importante tener claro dos términos más: el objeto de prueba y el órgano de prueba.

Se entiende por objeto de prueba, el tema sobre el cual se desarrolla la actividad probatoria; hechos relevantes para establecer la posibilidad o no de realización de un hecho delictivo. Es la respuesta a las preguntas: ¿Qué ha de probarse? ¿Qué, dónde, ¿cómo?, ¿quién?, ¿por qué? (Morillo & Herrero, 2011).

Por otro lado, órgano de prueba es la persona(s) por medio de la cual se da a conocer ante el Juez y demás sujetos procesales un objeto de prueba. Fungen de intermediarios entre el objeto y el ente juzgador, aportando conocimientos e información acerca de dicho objeto de prueba. (Morillo & Herrero, 2011)

De igual manera, es pertinente conocer el término sujeto de prueba, referido a la persona(s) que interviene(n) en el desarrollo de la actividad probatoria. Este concepto engloba a todos los involucrados en el proceso: quien solicita la prueba, quien la recibe, así como terceros intervinientes en calidad de peritos o testigos. (Morillo & Herrero, 2011)

(Plascencia, 1995), se refiere a medio de prueba como la prueba en sí, pero utilizada en un proceso judicial, es decir, el nivel de “medio” es adquirido por la prueba cuando ésta es ofrecida y admitida dentro de dicho proceso judicial. Son elementos con los cuales se prueba en un proceso y en la legislación ecuatoriana se reconocen como: el documento, el testimonio y la pericia.

Destaca también, la distinción que (Plascencia, 1995) hace entre medio de prueba y fuente de prueba, dado que ampos se encuentran en niveles y momentos completamente distintos. La fuente de prueba es preexistente y extraña al proceso penal, a diferencia del medio de prueba, el cual es un concepto procesal, posterior a la fuente de prueba, pero que existe porque la fuente de prueba ha sido ofrecida, aceptada y desahogada como tal en el proceso penal.

En el ámbito legal del Derecho Penal ecuatoriano, los medios de prueba se detallan en el Capítulo Tercero del COIP, aspecto que se abordará en la parte concerniente a las bases legales.

1.2.4. Elementos de prueba

Si bien esto es objeto de la teoría general del proceso, conviene repasar brevemente algunos elementos básicos de la prueba, como todo lo relativo a:

a) Que puede ser probado – objeto de la prueba
b) De donde debe extraerse la prueba – fuente de prueba
c) Quien debe confirmar – carga de la prueba
d) Como ha de hacerse la prueba – medios de prueba
e) Cuando y donde ha de hacerse la actividad probatoria – procedimiento de la confirmación
f) Cuál es el producto final del procedimiento – elementó de prueba (Artavia & Picado , 2018)

1.2.5. Prueba digital o electrónica

De acuerdo con Muñoz, citado por (Rodríguez, 2018), la prueba digital es un medio de reproducción de la palabra, sonido e imagen e instrumento para archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas, relevantes para el proceso.

Como el soporte material que incorpore datos, hechos o narraciones, que tenga eficacia probatoria y relevancia jurídica, lo establece la legislación española, citada por (Pérez J. , 2014).

Un concepto que integra los términos vistos sobre prueba, medio y fuente, es el aportado por (Borges, 2018), quien la define como toda información de valor probatorio que se encuentra o transmite por un medio electrónico. La fuente de prueba es precisamente esa información contenida o transmitida por medios electrónicos y el

medio de prueba vendría a ser la manera cómo se incorpora al proceso, ya sea como prueba documental, pericial o testifical (p.541).

En el ámbito legal del Derecho Penal ecuatoriano, la prueba digital se incorpora dentro de la documental, y el contenido digital está definido en el artículo 500 del COIP, como se detallará en el punto relativo a Bases Legales.

1.2.6. Sistema de Derecho Penal del Ecuador

El Sistema de Derecho Penal ecuatoriano lo conforma el conjunto de normas e instituciones relativas a los temas delito y pena, como un aparato de control social, cuyo ordenamiento jurídico es aplicado para la concreción de situaciones en las que se comete un delito.

El procedimiento para el juzgamiento de las personas en tales situaciones, está establecido en el Código Orgánico Integral Penal (COIP), además de tipificar las infracciones penales, promover la rehabilitación social y la reparación integral de las víctimas (Ecuador, Asamblea Nacional, 2014).

En su dinámica, el sistema penal se encuentra con el dilema de combatir la impunidad y garantizar los derechos de los sospechosos de haber cometido una infracción penal; de proteger a las personas cuando han sido gravemente lesionadas, y restringirles excepcionalmente sus derechos, cuando una persona vulnera los derechos de otras y justifica la aplicación de una sanción. (Ecuador, Asamblea Nacional, 2014)

1.2.7. Sistema de Derecho Probatorio Penal en Ecuador

En el Derecho Penal ecuatoriano, existen vías procesales para incorporar un medio de prueba como instrumento para el manejo estratégico de un juicio, sustentado por el principio de libertad probatoria incluido en el COIP (Ecuador, Asamblea Nacional, 2014), artículo 454 numeral 4, el cual señala la posibilidad de probar hechos y circunstancias pertinentes según sea el caso, siempre que el medio no sea contrario a la Constitución, instrumentos internacionales ratificados por el Estado y demás normas jurídicas.

Otros principios que rigen el anuncio y práctica de la prueba en el Derecho Probatorio Penal en Ecuador son: oportunidad, inmediación, contradicción, pertinencia, exclusión y garantía de igualdad de oportunidades para la prueba, los cuales serán detallados en el punto correspondiente a Bases Legales.

De igual manera, se toma en cuenta que la prueba y sus elementos deben guardar correspondencia entre la infracción y la persona procesada, pues su fundamento no puede basarse en presunciones, sino en hechos reales introducidos a través de un medio de prueba. (Ecuador, Asamblea Nacional, 2014)

La garantía de autenticidad, manejo, análisis y conservación de los elementos materia de prueba, se otorga mediante la aplicación de cadena de custodia, fundamentado en el Art. 456 del COIP. Por su parte, el servidor público que entre en contacto con la escena del hecho, será el responsable de su participación, hasta contar con la presencia del personal especializado. (Ecuador, Asamblea Nacional, 2014)

1.2.8. Criterios de valoración probatoria en la doctrina

Una de las cuestiones más importantes del derecho probatorio, es la etapa de valoración de la prueba una vez practicada, con la finalidad de dictar sentencia. Para ello, la doctrina señala la existencia de dos sistemas teóricos de valoración de la prueba: el sistema de prueba legal y el de valoración libre (Pardo, 2006).

El sistema de prueba legal tiene las siguientes características, establecidas por (Pardo, 2006):

- El ordenamiento jurídico comprende en forma legal un conjunto de “máximas de experiencia”, bajo los cuales se establecen los hechos como probados, independientemente del convencimiento del juez.
- La ley establece el valor que tiene cada medio probatorio, lo que implica que el juez no es libre de emitir una apreciación, sino que le deberá atribuir a la prueba el valor indicado por ley.

El sistema de valoración libre, de acuerdo con (Pardo, 2006), se caracteriza por lo siguiente:

- El juez determina en atención a la “sana crítica”, qué valor otorgar a cada una de las pruebas practicadas, lo que no quiere decir que este criterio le confiera discrecionalidad en la decisión.
- La libre valoración supone una deducción lógica, sobre la base de datos certeros, de una evaluación analítica de los hechos, y de una apreciación crítica de los medios de prueba, lejos de subjetividades, sino de un conocimiento objetivo.
- Se trata de una apreciación lógica de la prueba, que no está libre de pautas y lineamientos objetivos. “Valoración en conciencia no puede, en ningún caso, ser sinónimo de arbitrariedad” (p.82).

A fin de evitar una libre valoración, se recurre a la fijación de criterios que deberá seguir el juez para no caer en la arbitrariedad. La libertad de convicción de un juez se establece respecto de reglas legales de prueba, mas no de condiciones de racionalidad en el conocimiento de la realidad. (Pardo, 2006)

1.2.9. Criterios de valoración probatoria en el COIP

El Código Orgánico Integral Penal establece claramente los criterios de valoración probatoria, en su Art. 457. A tales efectos, la valoración de la prueba se desarrollará bajo los criterios de legalidad, autenticidad, sometimiento a cadena de custodia y grado de aceptación científica y técnica de los principios bajo los cuales se fundamentan los informes periciales. (Ecuador, Asamblea Nacional, 2014)

Otro aspecto que incorpora el mencionado artículo, es el referente a la demostración de la autenticidad de elementos probatorios que no son sometidos a cadena de custodia, cuya responsabilidad queda a cargo de la parte que los presenta.

Es conveniente señalar, la falta de detalle en la presentación de los criterios, ya que no se precisa el alcance de cada uno de ellos, lo que aportaría mayor información al momento de evaluar y valorar la prueba mostrada.

1.2.10. Seguridad jurídica

Al respecto la Corte Constitucional para el periodo de transición en sentencia No 021 10 SEP CC de fecha 11 de mayo del 2010 indica

> Es la necesidad de certeza y seguridad jurídica uno de los principios que alimentan el núcleo duro del deber ser de las formalidades y solemnidades que caracterizan a los procesos en derecho, sin embargo, la seguridad jurídica no se agota en las meras formas, pues en muchos casos dichas formalidades y solemnidades podrían ser el mecanismo de perpetuación de una injusticia o un sin razón jurídico. (Ecuador, Corte Constitucional, 2010)

La Constitución de la República del Ecuador, en su artículo 82 consagra el derecho a la seguridad jurídica, así textualmente dice “El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas claras públicas y aplicadas por las autoridades competentes” (Ecuador, Asamblea Constituyente, 2008). Al respecto la Corte Constitucional para el periodo de transición en sentencia No 021 10 SEP CC de fecha 11 de mayo del 2010 indica

> Es la necesidad de certeza y seguridad jurídica uno de los principios que alimentan el núcleo duro del deber ser de las formalidades y solemnidades que caracterizan a los procesos en derecho, sin embargo, la seguridad jurídica no se agota en las meras formas, pues en muchos casos dichas formalidades y solemnidades podrían ser el mecanismo de perpetuación de una injusticia o un sin razón jurídico. (Ecuador, Corte Constitucional, 2010)

Pese a la dificultad de encontrar un concepto claro, Rincón, citado por (Arrázola, 2014), como:

> la expectativa que tiene todo operador jurídico de que el marco legal es y será confiable, estable y predecible y como tal, es por sí sola fundamento esencial de la construcción del Estado y del adecuado funcionamiento de la Administración Pública, lo que implica que su consolidación y garantía constituyan uno de los imperativos de actuación para la administración pública de cualquier Estado (p. 6).

De acuerdo con (Ugartemendía, 2006), la Seguridad Jurídica en el ordenamiento constitucional español es un principio general y un mandato dirigido a los poderes públicos, “la suma de certeza y legalidad, jerarquía y publicidad normativa, irretroactividad de lo no favorable e interdicción de la arbitrariedad” (p.20).

Otras condiciones son incorporadas por (Pérez A. , 2000), cuando define Seguridad Jurídica como un valor ligado al Estado de Derecho a través de los componentes: corrección estructural (referente a la existencia de normas jurídicas adecuadamente formuladas), corrección funcional (garantía de cumplimiento del Derecho), y el subjetivo de certeza del derecho (proyección personal de garantías estructurales y funcionales de la seguridad objetiva) (p.28).

De estos conceptos destaca que la seguridad jurídica involucra como elementos esenciales:

- La previsibilidad de la actuación por parte del Estado.
- La suma de principios que promueven la justicia, la igualdad en libertad.
- La certeza de garantía de adecuada formulación y cumplimiento de la norma jurídica.

1.2.11. Debido proceso

El debido proceso, consagrado en el artículo 76 de la Constitución de la República, constituye un derecho de protección elemental, siendo el conjunto de derechos y garantías, así como las condiciones de carácter sustantivo y procesal, que deben cumplirse en procura de que quienes son sometidos a procesos en los cuales se determinen derechos y obligaciones, gocen de las garantías para ejercer su derecho de defensa y obtener de los órganos judiciales y administrativos un proceso exento de arbitrariedades. Dentro del artículo 76 numeral 4 ibídem, se establece como una garantía del debido proceso que: "Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria". (Ecuador, Asamblea Constituyente, 2008)

La Constitución de la República ecuatoriana incorpora este concepto, al ordenar la determinación de derechos y obligaciones de cualquier orden, como en el caso de los procesos penales, para asegurar garantías tanto para la persona procesada (de defensa), como para las víctimas, canalizadas a través de la ley penal; es decir, garantías del debido proceso. (Ecuador, Asamblea Nacional, 2014)

1.2.12. Tutela Judicial Efectiva

La tutela judicial efectiva, es el derecho, de carácter autónomo, de acudir ante el órgano jurisdiccional del Estado, por una respuesta con respecto a una pretensión determinada, dirigida a través de una demanda, la cual no necesariamente es positiva. Este derecho faculta a una persona a solicitar un servicio de administración de justicia por parte del Estado, y obtener una sentencia, goce o no de derecho material (Aguirre, 2010).

Sin embargo, el concepto de tutela judicial efectiva no abarca solo el hecho de que las personas tengan la potestad de acudir a los órganos judiciales en busca de la tutela de su derecho, sino que garantiza que la sentencias dictada por la autoridad correspondiente en el momento, sea justa y no arbitraria. Es así como “el derecho a la tutela judicial efectiva se configura, fundamentalmente, como la garantía de que las pretensiones de las partes que intervienen en un proceso serán resueltas por los órganos judiciales con criterios jurídicos razonables” (Cevallos & Alvarado , 2018).

En la norma jurídica ecuatoriana, se consagra la tutela judicial efectiva como un derecho de protección del Estado ecuatoriano para los ciudadanos, disposición que todas las personas tienen para acceder a una justicia equitativa en la que primen las garantías constitucionales de un proceso justo. (Ecuador, Asamblea Constituyente, 2008)

1.3. Bases contextuales de la investigación

1.3.1. Principales espacios e instrumentos de los que pueden obtenerse medios de prueba digital.

La prueba puede obtenerse, ya sea por las partes involucradas, quienes aporten al proceso o por medio de las autoridades policiales como parte de una investigación. En este último caso, se precisará autorización judicial si con tal obtención pudieran resultar vulnerados derechos fundamentales del sujeto que está siendo investigado. (Rodríguez, 2018)

(Zambrano, Dueñas, & Macías, 2016), definen “Tratado sobre Delito Informático, como un instrumento de ámbito internacional que abarca los delitos cometidos mediante el uso del Internet y las redes informáticas, comprende los siguientes” (p. 207):

- Violación por derechos de autor. Si bien el Internet le ha permitido a los autores generar múltiples ganancias, al facilitar la distribución de sus obras, no le permite controlar la cantidad de copias o reproducciones que se hacen de su obra. La difusión legal de contenidos en la red está conformada principalmente por 3 modelos: las redes P2P, la centralización de contenidos para los cuales no poseen licencia de distribución) y la agregación de enlaces sostiene Moisés, citado por (Ortiz, 2019).
- Estafas informáticas por internet. “consiste en la manipulación informática /para conseguir/ una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero” (Ortiz, 2019). Entre éstas se pueden encontrar:
    - El phising, consistente en la obtención de datos personales o financieros de la víctima, a través de el envío masivo de correos electrónicos que incluyen enlaces de páginas web falsas de entidades financieras o bancarias;
    - El pharming, referido a la manipulación de direcciones DNS para redireccionar al usuario hacia la navegación de sitios web falsos que han sido creados con el fin de defraudar;

- Money-mules, phishing-mules o pharming-mules, creados con el fin de poner a disposición de los estafadores, el dinero obtenido a través del phishing o pharming. (Ortiz, 2019)

- Pornografía infantil. Se refiere al material audiovisual conteniente de exhibición sexual explícita de menores (<18 años para el caso de Ecuador). De este comportamiento se derivan los delitos: producción de pornografía infantil con difusión por medio de sistemas informáticos; adquisición de pornografía infantil mediante un sistema informático, para una o más personas; posesión de pornografía infantil en sistemas informáticos. (Ortiz, 2019)
- Ciberterrorismo. Conjunto de acciones sobre la información, sistemas, programas, datos, que se planifican para coaccionar, intimidar, ofender, gobiernos, estados, poblaciones, y así generar fuertes impactos psicológicos.
- Delitos de odio, calumnias e injurias. Ocurre cuando un individuo se extralimita en el ejercicio de su libertad de expresión, al procurar insultos y difamaciones para causar daños a su víctima, que se profundizan al ser expuestos públicamente a través de internet.

> El Tratado de Delito Informático busca establecer una política penal para la protección de la sociedad contra el cibercrimen, a través de la creación de leyes especializadas y de cooperación internacional. Abarca situaciones relacionadas con el derecho procesal, tales como la preservación expeditiva de los datos almacenados, y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. De igual manera, cuenta con una disposición específica sobre el acceso transfronterizo a los datos informáticos almacenados, que no requieren asistencia mutua, para lo que se prevé la creación de una red mediante la que se garantiza una asistencia rápida entre las partes colaboradoras (Zambrano, Dueñas, & Macías, 2016, pág. 208).

En el COIP, la forma en que se obtienen los medios de prueba digital se establece en el Art. 500, los cuales se definen como contenido digital, que se detallarán en el punto Bases Legales. (Ecuador, Asamblea Nacional, 2014)

1.3.2. Tesis del fruto del árbol envenenado

> Dada la complejidad en torno al tema de la ilicitud de la prueba, surge el concepto de eficiacia refleja de la prueba ilícita, concretamente como producto de un caso de la jurisprudencia norteamericana surgido en 1920: el caso Silverthorne Lumber Co. Vs. Estados Unidos, en el cual, el Tribunal Supremo Federal decretó que las pruebas ilícitas no sólo no eran utilizables, sino que tampoco eran admitidas las pruebas obtenidas o logradas a partir de ella. (Fernández, 2017)

Esta doctrina es conocida como Teoría del fruto del árbol envenedado, pues hace alusión a las palabras de San Mateo en su evangelio, capítulo 7, versículos 17-20:

Así todo árbol da buenos frutos, pero el árbol malo da frutos malos. No puede el buen árbol dar malos frutos ni el árbol malo dar frutos buenos. Todo árbol que no da buen fruto, es cortado y echado en el fuego. Así que por su fruto lo conoceréis.

Su origen se relaciona con el caso Silverthorne Lumber Company contra Estados Unidos, pues éste tiene las siguientes características (Fernández, 2017).

Los Agentes del Gobierno allanaron las instalaciones de la empresa del Sr. Silverthorne, con la obtención de pruebas que lo inculpaban, relativas a libros de contabilidad, pero esta prueba fue declarada ilícita y anulada, por violar un derecho fundamental, pues la entrada fue realizada sin orden judicial.

Al efectuar una comparación con las palabras de San Mateo, el árbol sería la fuente de prueba, es decir, las instalaciones de Silverthorne; al ser éstas vulneradas mediante un allanamiento, la fuente se corrompe (árbol envenenado), por lo tanto toda consecuencia de dichas pruebas (los frutos del árbol) también se corromperá.

Sin embargo, existen exclusiones a la mencionada teoría, ante situaciones en que es factible permitir una prueba secundaria, pese a que la primaria fue declarada ilegal (Quintero, 2013):

Tabla 2. Exclusiones a la aplicación de la Teoría del fruto del árbol envenenado

Limitación de la fuente independiente	Limitación del nexo causal atenuado	Limitación del descubrimiento inevitable
La obtención ilegal de datos, no necesariamente son intocables o inaccesibles. Si el conocimiento de los hechos proviene de una fuente independiente, pueden ser utilizados.	La doctrina de la atenuación, surge como punto intermedio entre "el fruto del árbol envenenado" y la limitación de "la fuente independiente", en los casos en que la primera resulta excesiva e iría en contra del interés social de castigar al culpable. En casos en los que la prueba ilícita sólo sea utilizada como enfoque de dirección de la investigación en una persona concreta, que luego se le castigue por otras pruebas auténticas e independientes de aquella, sería excesivo el efecto de la nulidad de la nueva prueba, pues haría a esa persona inmune al castigo.	Analiza si la prueba encontrada por medios ilícitos, inevitablemente, de cualquier forma, hubiera sido hallada por vías legales.

Elaborado por: Valeria Cantos

1.4. Bases legales

Las bases legales están conformadas por la jurisprudencia vinculante al tema objeto de estudio. Esta se apoya principalmente en la Constitución de la República y en el Código Orgánico Integral Penal.

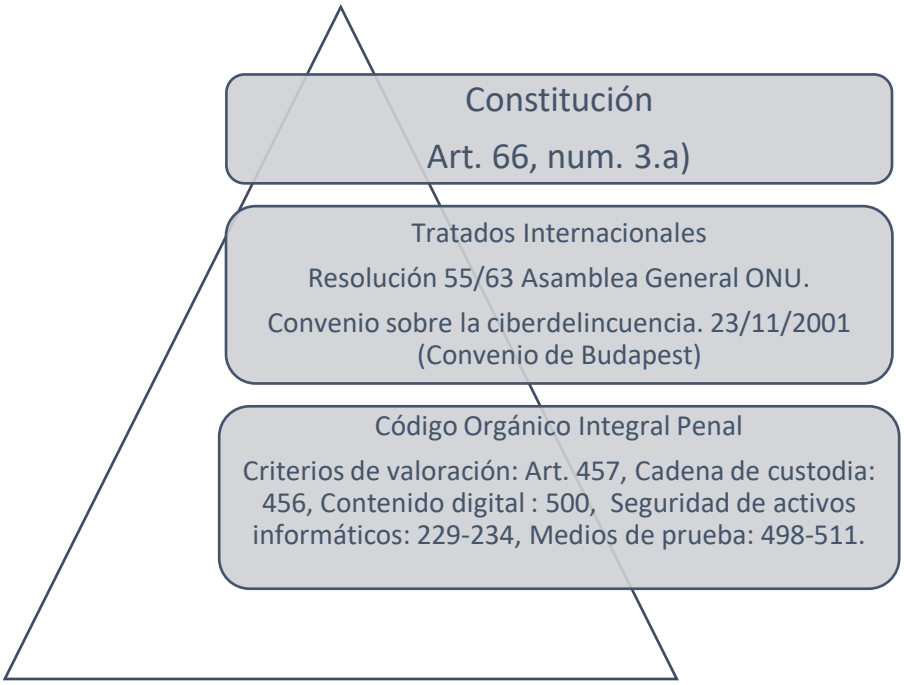

Figura 1. Marco legal entorno a los delitos informáticos (Estilo pirámide Kelseniana)
Elaborado por: Valeria Cantos

En las siguientes tablas se detallan los aspectos generalizados en la pirámide anterior.

Tabla 3. Aspectos de la Constitución de la República del Ecuador, pertinentes al objeto de estudio

Constitución de la República del Ecuador	
Artículo	Aspectos
66. Numeral 3 a)	Reconocimiento y garantía del derecho a la integridad física, psíquica, moral y sexual.

Elaborado por: Valeria Cantos

Tabla 4.Aspectos de Tratados internacionales, pertinentes al objeto de estudio

Tratado internacional	**Aspectos principales**
Resolución 55/63 Asamblea General de la Organización de las Naciones Unidas (ONU): Lucha contra la	Lucha por la eliminación de “refugios seguros” para los delincuentes informáticos. Cooperación entre Estados para la vigilancia del cumplimiento de la Ley y la investigación sobre delitos informáticos en el plano

utilización de la tecnología de la información con fines delictivos.	internacional. Capacitación y equipo adecuado, por parte del personal encargado de hacer frente a los delitos informáticos. Protección del carácter confidencial, integridad y disponibilidad de datos por parte de los sistemas jurídicos. Soluciones que tengan en cuenta tanto la protección de las libertades individuales como la preservación de la capacidad de los gobiernos para combatir los delitos informáticos.
Convenio sobre la ciberdelincuencia. 23/11/2001	Cada parte del convenio adoptará medidas necesarias para tipificar como delitos: El acceso deliberado e ilegítimo a todo o parte de un sistema informático. La intercepción deliberada e ilegítima de datos informáticos en transmisiones no públicas dirigidas a un sistema informático. Todo acto deliberado que dañe, borre, deteriore, altere o suprima datos informáticos. La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático. La producción, venta, obtención para su utilización, importación, difusión de dispositivos o programas informáticos, contraseñas, códigos de acceso, que sean utilizados para cometer delitos informáticos. Perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos, con la intención dolosa o delictiva de obtener de forma ilegítima un beneficio económico. La producción de pornografía infantil a través de un sistema informático. Infracciones de la propiedad intelectual que defina la legislación.

Fuente: (Organización de las Naciones Unidas, 2001); (Consejo de Europa, 2001).

Tabla 5. Aspectos del Código Orgánico Integral Penal, pertinentes al objeto de estudio

Código Orgánico Integral Penal	
Artículo	Aspectos
457.-Criterios de valoración de la prueba	Legalidad Autenticidad Sometimiento a cadena de custodia

	Grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales. La demostración de autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, queda a cargo de la parte que los presente.
456.- Cadena de custodia	Se aplica tanto a elementos físicos como contenido digital materia de prueba, para garantizar su autenticidad. Acredita su identidad y estado original, las condiciones, personas que intervienen en la recolección, envío, manejo, análisis y conservación de los elementos y se incluirán los cambios hechos en ellos por cada custodio. Inicia en el lugar donde se obtiene el elemento de prueba. Finaliza por orden de la autoridad competente. Son responsables de su aplicación: El personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses. El personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos. El personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación.
500. Contenido digital	Concepto. El contenido digital es todo acto informático representado por hechos, información, conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, Interconectado o relacionados entre sí. Reglas generales de investigación: 1. El análisis, valoración, recuperación y presentación del Contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses. 2. La recolección del contenido digital almacenado en sistemas y memorias volátiles o equipos tecnológicos del sector público o privado, se realizará en el lugar y en tiempo real, con técnicas Digitales forenses para preservar su integridad, cadena de custodia y se facilitará su posterior valoración y análisis de contenido. 3. La recolección del contenido digital almacenado en medios no volátiles, se realizará con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

	4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.
229.-Revelación ilegal de base de datos	Sanción con pena privativa de libertad de uno a tres años. Sanción con pena privativa de libertad de tres a cinco Años, si la conducta es cometida por un servidor público. Implica: Revelación de información registrada, contenida en bases de datos o medios semejantes, mediante sistemas informáticos y otros, con materialización voluntaria de la violación de la intimidad de las personas, para provecho propio.
230.- Interceptación ilegal de datos	Sanción con pena privativa de libertad de tres a cinco Años. Implica: Intercepción de datos informáticos sin orden judicial previa para obtener información en provecho propio o de un tercero. Diseño de plataformas financieras que induzcan a la persona a ingresar a una dirección web diferente a la que quiere acceder. Clonación de información contenida en dispositivos electrónicos soportados en tarjetas de crédito, débito o similares, así como la fabricación de materiales para la comisión de dichos delitos.
231.-Transferencia electrónica de activo patrimonial	Sanción con pena privativa de libertad de tres a cinco años. Implica: Alteración del funcionamiento de medios informáticos para la transferencia o apropiación no consentida de activos patrimoniales de terceros, sin consentimiento de éstos. Proporción de datos de cuentas bancarias propias para obtener activos patrimoniales de forma ilegítima.
232.- Ataque a la integridad de los sistemas	Sanción con pena privativa de libertad de tres a cinco años. Implica: Destrucción, alteración, supresión de datos, sistemas o componentes electrónicos. Diseño, ejecución, venta o distribución de dispositivos o sistemas informáticos maliciosos para causar estos ataques. Destrucción o alteración de infraestructura tecnológica utilizada para

	transmitir, receptar o procesar información. Sanción con pena privativa de libertad de cinco a siete años, si las implicaciones anteriores se desarrollan sobre bienes informáticos destinados a la prestación de servicios públicos.
233.-Delitos contra la información pública reservada legalmente.	Sanción con pena privativa de libertad de cinco a siete años. Implica: Destrucción o inutilización de información clasificada conforme a la ley. Sanción con pena privativa de libertad de tres a cinco años. Implica: Obtención de información clasificada de conformidad con la ley, por parte de un servidor público, con el uso de medios electrónicos o informáticos. Sanción con pena privativa de libertad de siete a diez años e inhabilitación del ejercicio de la función pública por seis meses. Implica: Revelación sin autorización, de información reservada, que compromete gravemente la seguridad del Estado.
234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	Sanción con pena privativa de la libertad de tres a cinco años. Implica: Acceso a sistemas telemáticos o informáticos o permanencia en éste sin el consentimiento de quien tenga el legítimo derecho, con el fin de su explotación ilegítima: modificación del portal web, desvío de tráfico de dato o voz, oferta de servicios que posee el sistema, sin pagarlos a sus proveedores.
498.- Medios de prueba	Los medios de prueba son: El documento El testimonio La pericia
499.- El documento. Reglas generales	6 reglas generales por las cuales se rige la prueba documental, en cuanto al reconocimiento del documento por parte de la persona procesada, requerimiento de informes por parte del Fiscal, uso de los documentos agregados al proceso, la obtención de copias certificadas de documentos que forman parte de otro proceso, no uso de documentos que no tienen relación con el proceso, admisión como prueba de contenidos digitales, conforme con las normas del COIP.
501.- El testimonio	Medio de conocimiento de las personas involucradas con los hechos del cometimiento de la infracción penal.

502.- Reglas generales	9 reglas generales por las cuales se rigen la prueba y los elementos de convicción obtenidos mediante declaración, en cuanto a la valoración del testimonio, el tratamiento del testimonio de personas con condiciones que les impiden comparecer a la audiencia de juicio, el procedimiento de comparecencia de personas que están en el extranjero, el no llamado a declarar a familiares o cónyuges, la forma de declaración de niños, niñas y adolescentes, la declaración de personas que no hablen castellano, el testimonio de personas sordomudas o que no saben escribir, las interrupciones al testimonio, el tratamiento a declarantes en situación de riesgo, el lugar donde se practicará el testimonio, el testimonio de servidores públicos con fuero de Corte Nacional, la forma de declaración del testimonio y los datos que se deben proporcionar, el tipo de preguntas que pueden ser formuladas.
503.- Testimonio de terceros	5 reglas que rigen este testimonio, en cuanto a : obligación de comparecencia, personas con secreto de profesión, la declaración de los peritos, comparecencia cuando hay más de veinte testigos y peritos, la forma de recibir varios testimonios o peritos para una misma causa.
504.- Versión o testimonio de niños, niñas o adolescentes, personas con discapacidad y adultos mayores	Derecho de comparecencia adecuado a su situación y desarrollo evolutivo.
505.- Testimonio de peritos	Sustentación oral del resultado de sus peritajes, con respuesta a interrogatorio y contrainterrogatorio.
506.- Detención de testigos por falso testimonio y perjurio	Remisión de lo pertinente para su investigación.
507.- Reglas de testimonio de la persona procesada	6 reglas para rendir este testimonio, en cuanto a: el carácter de medio de defensa, la no obligación a rendir, forma de declaración en caso de que decida dar testimonio, derecho de contar con un defensor público o privado, la instrucción sobre sus derechos, la nulidad del acto.
508.-Versión de la persona investigada o procesada	3 reglas para rendir esta versión, en cuanto a: el carácter voluntario de la rendición, sin coacciones, el derecho de contar con un defensor y asesoría, disposición de ampliación de la versión, de ser el caso.
509.- No liberación de práctica de prueba	Aun con la declaración de autoría de la infracción, el fiscal no queda libre de demostrar dicha responsabilidad.
510.- Reglas para el	5 Reglas para la recepción de este testimonio, en cuanto a: la

testimonio de la víctima	posibilidad de solicitud sin contacto visual con la persona procesada, el cerciorarse de la identidad de la persona que rinde el testimonio, disposición de medidas especiales para facilitar el testimonio de la víctima, el evitar hostigamiento o intimidación a la víctima, acompañamiento de la víctima en crisis, por parte de personal capacitado.
511.- La pericia. Reglas generales	8 Reglas en cuanto a: las credenciales de los peritos, el desempeño obligatorio de su función, situaciones en que deberán excusarse, valor del informe de peritos inhabilitados o excusados, plazo de presentación del informe, contenido del informe, cancelación del monto de diligencias judiciales y procesales, procedimiento en caso de no contar con perfiles para peritos o casos de mala práctica pericial, intervención de peritos internacionales.

Elaborado por: Valeria Cantos

En la Constitución nacional, si bien se establece que las personas tienen derecho a opinar y expresar libremente sus manifestaciones, éste no debe confundirse con pretender tener carta abierta para difamar en público a otros, con el consecuente atentado a su integridad física y moral.

A pesar de la existencia de los tratados internacionales, en la práctica persiste la falta de cooperación internacional para procesar los delitos informáticos y las iniciativas que han surgido para mitigar esta situación, como es el caso del Convenio de Budapest, aún no cuentan con la inclusión de Ecuador.

1.5. Bases doctrinales

1.5.1. Aspectos generales y comunes de los delitos informáticos

Para complementar la información que al respecto se señaló en la terminología básica, se expondrán puntos comunes de delitos informáticos tipificados según la Organización de las Naciones Unidas (Acurio, 2016):

Tabla 6. Aspectos generales y comunes de los delitos informáticos

Delito informático	**Aspectos generales del delito**	**Aspectos comunes entre los delitos informáticos**
Los fraudes	Datos engañosos: introducción de datos falsos a un computador, para lograr movimientos falsos en transacciones de una empresa. Manipulación de programas o “caballos de troya”, consistente en alterar programas informáticos para que a la par a sus funciones normales, realicen otras no autorizadas. La técnica del salami: se llama así, por la extracción repetida de una cuenta a otra, de “rodajas muy finas”, apenas perceptibles, de transacciones financieras. Falsificaciones informáticas. Alteración de datos de documentos digitales. Manipulación de datos de salida. Uso de equipos informáticos para codificar información falsificada en bandas magnéticas de tarjetas bancarias.	Manipulación ilegal de datos informáticos, con fines dañinos.
Sabotaje informático	Modificar o suprimir, sin autorización, datos informáticos para obstaculizar el normal funcionamiento de los sistemas. Bombas lógicas. Especie de bomba de tiempo, con una destrucción programada de datos en un momento futuro. Gusanos. Cuya fabricación se realiza al tiempo que el virus informático, para así infiltrarlo en programas de procesamiento de datos, con el fin de modificarlos o destruirlos, sin posibilidad de regeneración. Virus informáticos y malware. Elementos informáticos con tendencia a la reproducción y extensión dentro del sistema que penetran, susceptibles de destrucción con el uso de antivirus, aunque algunos desarrollan resistencia a éstos. Ataques de denegación de servicio. Empleo de recursos del sistema objetivo, impidiendo su acceso, lo que perjudica la actuación del sistema, en especial si éste es de uso masivo.	Inhabilitación permanente de las funciones de los sistemas informáticos, lo que perjudica gravemente el acceso y ejercicio de actividades de diferentes tipos, por parte de los usuarios.
Espionaje informático y	Fuga de datos. Sustracción de información confidencial de una empresa. Por esta razón, se	Sustracción y reproducción no

robo o hurto de software	recurre a la criptografía. Reproducción no autorizada de programas informáticos de protección legal, con una consecuente pérdida económica sustancial para los propietarios legítimos.	autorizada de información confidencial, para la explotación económica personal o de terceros.
Robo de servicios	Hurto del tiempo del computador. Apropiación de informaciones residuales. Aprovechamiento de información recogida de papeleras virtuales que la han enviado allí como residuo de trabajos previos y por lo tanto no tienen protección. Parasitismo informático y suplantación de personalidad. Suplantar identidades con artimañas y engaños, para cometer otros delitos informáticos.	Sustracción de información no protegida, suplantación de identidad.
Acceso no autorizado a servicios informáticos	Las puertas falsas. Interrumpir procesos lógicos de los programas, "…con el objeto de chequear en medio de procesos complejos si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante"(p.29). La llave maestra. Programa informático que abre cualquier archivo del computador. Pinchado de líneas. Interferir líneas telefónicas para acceder a información que circula por ellas. Piratas informáticos o hackers. Delincuentes que acceden a sistemas informáticos desde un lugar exterior, aprovechando la falta de rigor en las medidas de seguridad o haciéndose pasar por usuarios legítimos del sistema.	Acceso ilegal a los sistemas para sustraer información con fines de explotación o suplantar identidades.
Extorsión	Es una práctica maliciosa en la que un criminal accede a información personal y amenaza con exponerla públicamente, a no ser que la persona titula de la información sensible le otorgue una cierta cantidad de dinero a cambio del silencio. Ransomware. Es un software malicioso que se utiliza para ejercer esta práctica de extorsión, al infectar a un equipo informático y secuestrar sus datos, para solicitar un pago de rescate a los mismos recursos secuestrados. Es un malware que busca lucro a través de la extorsión, dada la referencia que hace su término: ransom= rescate, ware, mercancía (Martínez & Moo, 2016, p.38).	Acceso ilegal a los sistemas para sustraer información con fines de explotación

Delitos sexuales	Son aquellos que vulneran la intimidad sexual de una persona, por medio de su exposición en en el ciberespacio, especialmente en redes sociales, mediante dispositivos electrónicos. El objetivo es atacar el honor, la intimidad, libertad e integridad sexual del sujeto pasivo, haciendo posible las prácticas como extorsión, acecho, amenazas, entre otros. Sexting. Proviene de la unión entre las palabras sex (sexo en inglés) y texting (envío de mensajes de texto). Se refiere a la exposición de material sexual mediante mensajería instantánea, usualmente entre parejas con relación estable u ocasional, tanto de manera voluntaria o en contra de la voluntad de alguna de las partes. Stalking. Significa acechar y perseguir maliciosa y obsesivamente a un sujeto, quien funge de blanco u objetivo de su acechador, a través de plataformas informáticas. Se produce mediante el "stalkeo"permanente de las redes sociales del sujeto pasivo, haciendo un seguimiento exhaustivo de la rutina de la víctima. Sextortion. Consiste en el chantaje, amenaza o extorsión sexual hacia la víctima, quien previamente fue filmada o fotografiada en situaciones sexuales explícitas, con el fin de no exponerlas públicamente, a cambio de dinero o de la exigencia de más fotografías en similares condiciones. Revenge porn (Porno venganza). Es el acto o amenaza de publicar fotografías, audios o videos sexuales, cometidos por la ex pareja de la víctima, sin su consentimiento, como consecuencia del daño ocasionado por ésta al finalizar la relación, mediante la degradación pública y con ello la satisfacción del agravio recibido (Águila, 2019, pp.12-17).	

Fuente: (Acurio, 2016); (Martínez García, Moo Medina, & Chuc Us, 2016), (Águila, 2019)

Ya sea información financiera, íntima o informática, los delitos electrónicos llevan inmersos la manipulación de datos, tanto para alterar los sistemas que los incorporan, como para acceder y hacer uso de ellos, un uso no consentido por quienes son propietarios de los datos vulnerados.

1.5.2. Hechos digitales relevantes y no relevantes penalmente.

En este punto conviene partir de las conductas relevantes y no relevantes definidas en los artículos 22 al 24 del COIP, para luego contrastar con lo estipulado en materia de prueba digital.

En cuanto a conductas penalmente relevantes, éstas son acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables. (Ecuador, Asamblea Nacional, 2014)

Las modalidades de conducta punible son: la acción y la omisión. (Ecuador, Asamblea Nacional, 2014)

En cuanto a conductas no penalmente relevantes, éstas son resultados dañosos o peligrosos que resultan de: fuerza física irresistible, movimientos reflejos o estados de plena inconciencia, debidamente comprobados. (Ecuador, Asamblea Nacional, 2014)

De acuerdo con estas características de las conductas penales o no penalmente relevantes, se pueden extraer ejemplos de hechos digitales penalmente relevantes, en los cuales ha intervenido la fiscalía general del Estado (Ecuador, Fiscalía General del Estado, 2012):

- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. Esto se pudo evidenciar gracias a una fotografía encontrada en el dispositivo celular del actor de la conducta.
- Pornografía infantil, con presencia de varios menores de entre 8 y 10 años de edad. En las evidencias constan celulares, dispositivos electrónicos de almacenamiento de datos, entre otros, que se encuentran en cadena de custodia en la Policía Judicial.
- Apropiación fraudulenta por medios electrónicos. Su presunto modo de operar consistía en utilizar números de tarjetas y códigos robados en Estados Unidos y Europa, para comprar cuentas de streaming y mercadería en plataformas virtuales, para luego venderlos, a través de redes sociales, a la mitad del precio real.

- Utilización de claves de acceso a los correos personales de altos funcionarios públicos sin su consentimiento, para acceder a su información.
- Adulteración de datos en el sistema de matriculación vehicular para entregar certificados presuntamente fraudulentos.

1.5.3. Delitos informáticos y sus características

De acuerdo con Téllez, citado por (Mora, y otros, 2014), se pueden caracterizar los delitos informáticos de la siguiente manera:

- Su ejecución puede provocar fuertes pérdidas económicas.
- Se ejecutan en su mayoría, con un alto margen de efectividad.
- Ya sea por falta de regulación o desconocimiento de la población, los casos denunciados son un porcentaje muy bajo con relación a los casos ejecutados.
- No son fáciles de comprobar, ameritan de la inspección o peritaje por parte de expertos.
- Su grado de sofisticación, permite que se utilicen para ataques militares o contra la seguridad de los Estados.
- Permanecen en el tiempo, ya que evolucionan con los avances tecnológicos.
- Pueden ser perpetrados contra personas e instituciones de carácter público o privado.
- Ofrecen facilidades de tiempo y espacio, al poder cometerse en milésimas de segundo sin necesidad de presencia física.
- Son de difícil comprobación, dado su carácter técnico.
- Pueden ser dolosos o culposos.
- Comúnmente son cometidos por personas con conocimientos especiales.

1.5.4. Sujetos del delito informático

Como se señaló en el punto de terminología básica, en la comisión de un delito confluyen sujetos que pueden ser activos y pasivos.

En cuanto al sujeto activo, definido como aquel individuo que realiza toda o parte de una acción, se pueden encontrar los siguientes:

1.1.1.1 Hacker.

A diferencia del significado peyorativo que le han dado, el término hacker se refiere a todo individuo que muestra interés y disfruta de aprender a programar y ampliar sus capacidades, sólo por el gusto de hacerlo, sin sentirse obligado (Sandoval & Vaca, 2013).

Según el objetivo de accionar, se pueden encontrar diversos tipos de hacker:

Hacker de sombrero negro o crackers. Son los hackers maliciosos, capaces de violar la seguridad de una computadora, red o crear un virus para éstas, optando por caminos de menor resistencia, ya sea por vulnerabilidad, un error humano, un nuevo método de ataque. Su objetivo de accionar es en su mayoría, el dinero. (Sandoval & Vaca, 2013)

Hacker de sombrero blanco. Hacker quienes hacen uso de su experticia para contribuir con compañías y organizaciones en la protección a los sistemas, de los hackers de sombrero negro, con la creencia de que es importante examinar la propia red de la manera en que lo haría un cracker para entender sus puntos fuertes y débiles. Su objetivo de accionar es defensivo. (Sandoval & Vaca, 2013)

Hacker de sombrero gris. Son aquellos hackers quienes no adoptan una posición fija en cuanto a sus objetivos, ya que unas veces pueden trabajar con fines ofensivos y otros defensivos, es decir, en ocasiones pueden traspasar los límites de la legalidad. (Sandoval & Vaca, 2013)

Ethical hacker. Son profesionales de la informática, con sólidos conocimientos en programación, hardware, sistemas operativos, quienes tienen la responsabilidad de la seguridad informática de una compañía, por lo que manejan información sensible para ésta, lo cual le exige que tenga además de profesionales, altos niveles éticos, alto grado de paciencia y serenidad para soportar extensas jornadas de trabajo, dentro y

fuera de las reglamentarias, ya que los delincuentes pueden esperar días e inclusos semanas para esperar una oportunidad de descuido y perpetrar en los sistemas. (Sandoval & Vaca, 2013)

1.1.1.2 Lamers Script kiddies

A diferencia del hacker, quien goza de altos conocimientos informáticos, los lamers carecen de ellos, aunque comparten su interés por perpetrar acciones de hacking, por lo que, sin serlo, se autodenominan como tales. Representan un gran peligro para las redes y sistemas, ya que ponen en práctica cuanto software de hacking descarguen de internet, sin entender su funcionamiento o los conocimientos técnicos empleados en su desarrollo. Su objetivo de accionar es molestar o ganar notoriedad y popularidad en su grupo de amigos, a partir de la ejecución de programas creados por otros. (Salcedo, Fernández, & Castellanos, 2012)

1.1.1.3 Neófito o newbie

Son aspirantes a hacker, quienes comienzan a aprender hacking con herramientas que consiguen en la web. Son inofensivos al comienzo, mientras aprenden lentamente, y según su paciencia, tenacidad e inteligencia, con el tiempo pueden llevar a ser hackers. Su objetivo de accionar es aprender sobre informática, computadoras, redes y TIC, e ir superando retos. (Salcedo, Fernández, & Castellanos, 2012)

1.1.1.4 Piratas informáticos.

Son personas que no tienen conocimientos informáticos como los hackers, aun cuando a menudo los confunden con ellos. Su objetivo de accionar es la venta ilícita de copias que ellos mismos realizan y reproducen ilegalmente, de software, música, textos, películas. (Salcedo, Fernández, & Castellanos, 2012)

1.1.1.5 Phreakers.

Son llamados crackers de las redes de telefonía y comunicaciones, por sus altos conocimientos autodidactas de dichos temas. Emplean procedimientos y técnicas

diversos, para utilizar sin pagar los servicios de las empresas de telecomunicaciones, mediante el uso de hardware y software.

1.1.1.6 Sneakers, snuffer.

Son espías informáticos, quienes utilizan sus conocimientos informáticos para este fin. Los snuffer solo se limitan a identificar claves de acceso a sistemas y describir errores en los programas. (Salcedo, Fernández, & Castellanos, 2012)

1.1.1.7 Sujeto pasivo en el delito informático.

Es el titular del bien jurídicamente protegido, sobre el cual recae la acción delictiva de naturaleza informática, la víctima del sujeto activo. Puede ser persona natural o jurídica, pública o privada, nacional o extranjera. (Zumba, 2015)

En este tipo de delitos comúnmente no es una sola la víctima, pues el ataque afecta masivamente, según el fin que persiga el sujeto activo, por lo que en algunos casos pueden resultar adolescentes los agravados, en otros, entidades financieras y demás personas jurídicas.

1.6. Tipos de pruebas digitales

1.6.1. Comunicaciones por medios de correos

Estas formas de mensajería virtual tienen un tratamiento jurídico, como un documento privado, sujeto a las reglas generales detalladas en el COIP (desarrollados en las bases legales de este documento), y tendrán la misma fuerza vinculante que un documento público, en caso de no ser impugnado por la parte contraria. Sobre la parte que presentó esta prueba en el tribunal, recae la carga de la prueba. Se debe acompañar esta prueba con un informe pericial técnico, en el cual se detalle: “el contenido original del mensaje, la identidad del equipo que lo emitió y recibió, la fecha y hora de esa comunicación y la cadena de custodia del correo (…) los servidores de correo, los logs de acceso” (Chiluiza, 2017). La integridad de esta prueba se evidencia de acuerdo con la conclusión del perito en su informe.

1.6.2. Redes sociales

Las publicaciones en redes sociales pueden ser admitidas como un medio de prueba digital, así como también conversaciones por mensajería instantánea, siempre y cuando su consignación sea a través del medio probatorio adecuado en conjunto con los medios necesarios para su reproducción.

Las formas comunes de aportar estas pruebas son mediante capturas de pantalla de conversaciones efectuadas a través de aplicaciones como WhatsApp, o de publicaciones en las diferentes redes sociales. Resulta entonces un medio útil para demostrar, por ejemplo, la existencia de una relación (laboral, afectiva, entre otras); un comportamiento sancionable, entre otros; siempre y cuando se hayan obtenido de forma lícita, sin violar derechos fundamentales o libertades públicas (Lacalle, 2018).

1.6.3. Llamadas telefónicas

- El COIP en su artículo 472, señala 9 reglas para la intercepción de comunicaciones o datos informáticos, si se percata de la existencia de indicios relevantes para la investigación, las cuales rigen:
- El tiempo de intercepción de la comunicación, el cual no debe exceder de noventa días, prorrogables por noventa días más, con la salvedad de investigaciones sobre delitos de delincuencia organizada, cuya intercepción puede ser hasta por seis meses prorrogables por igual período.
- El carácter secreto de la información sobre la infracción obtenida de la comunicación interceptada.
- El procedimiento a realizar cuando se conozca del cometimiento de otra infracción en el transcurso de la intercepción y también para el caso de delitos flagrantes.
- La forma de intercepción y registro de los datos informáticos en transmisión, la cual se realizará a través de telefonía fija, satelital, móvil e inalámbrica, con servicios de llamadas de voz, mensajes SMS, MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros.

- Las prohibiciones de interceptación de comunicaciones.
- La parte de las comunicaciones interceptadas que se incluirán en el proceso.
- La obligación de guardar reserva del contenido interceptado, por parte del personal encargado de ello.
- El medio de almacenamiento de la información interceptada.
- La prohibición de interceptación de comunicaciones que vulneren los derechos de niños, niñas y adolescentes.

1.6.4. La discrecionalidad judicial

Como discrecionalidad jurídica se puede entender, lo que Peralta (2017) concluye:

> aquel margen de libertad en la toma de decisiones de la autoridad judicial; entendida como la facultad que el ordenamiento jurídico otorga a la autoridad judicial para que decida según los estándares que considere justificadamente ante la indeterminación o el carácter abierto de la norma jurídica a ser aplicada (pág. 25)

1.1.1.8 La debida motivación.

La importancia de una debida motivación, tanto en un auto, como en un decreto o sentencia, depende del razonamiento de cada administradores de justicia, que pueden exteriorizar para llegar a la conclusión de un proceso judicial.

Para Cantón, citado por (Solís, 2015), la motivación es: “la exteriorización por parte del juez o tribunal de la justificación racional de determinada conclusión jurídica” (p. 48).

Por otro lado, De la Rúa, citado por (Solís, 2015) la define como “un elemento intelectual, de contenido crítico, valorativo y lógico, que consiste en el conjunto de razonamientos de hecho y de derecho en que el juez apoya su decisión” (p.48).

Zavala, citado por (Solís, 2015) señala:

> La motivación constituye un juicio lógico que se desarrolla alrededor de la pretensión. El juez al momento de sentenciar debe exponer, a las partes y a la sociedad, las razones que han tenido para resolver en la forma constante en la parte dispositiva de la sentencia… Para estimar o desestimar la pretensión punitiva, el juez debe ponerla en relación con el derecho objetivo… Pero, además, en el caso que el juez estimare la pretensión punitiva, la motivación o parte lógica de la sentencia debe comprender también las causas de la calidad y de la cantidad de la pena, es decir, las razones por las cuales se impone el máximo o no se admite la variación o, en su defecto, se atenúa la pena. Por otro lado, si se estima la pretensión, se debe incorporar en la motivación el fundamento para establecer la calidad de la pena, o en su caso, la razón para que proceda la imposición de ciertas medidas de seguridad proyectadas inclusive para el tiempo posterior al de la ejecución de la condena (p. 48-49).

Es entonces la motivación, una herramienta para el juez, quien implanta su voluntad al otorgar la razón a una de las partes procesales, al ser garante de derechos, y obedientes al debido proceso. La motivación forma parte de los principios procesales establecidos en el COIP Art.5, numeral 18, y es importante ya que cada decisión tomada puede dinamizar el trámite, en el cual las partes procesales tendrán la obligación de cumplir con lo ordenado en la sentencia.

1.1.1.9 La verificación de los principios de inmediación, contradicción, legalidad, comunidad, igualdad y publicidad.

Uno de los principios fundamentales de un sistema procesal oral por audiencias es la inmediación que implica al juez interactuar en la recepción de la prueba, permitiéndole tomar una decisión basada en la información de calidad proporcionada por las partes, testigos y peritos. A través de la inmediación se logra que el juez extraiga su convicción sobre la prueba actuada en audiencia. Las Resoluciones dictadas por la Corte Nacional de Justicia del Ecuador, en caso de ausencia de alguno de los jueces, que intervinieron en el juicio oral y que por cualquier circunstancia no pudieron suscribir la sentencia, vulneran el principio de inmediación, por cuanto, no permiten que el juez interactúe en la misma, ni dicte una sentencia formando su

convicción. Tomar una decisión judicial sin haber intervenido en una audiencia por parte de los juzgadores, es hacer referencia a un sistema escrito, en donde el juzgador debe extraer sus conclusiones sobre lo constante en actas o en la escucha del audio o video. (Gallegos, 2019)

El Principio de Contradicción estipulado en Código Orgánico Integral Penal artículo 5 numeral 13 establece: “los sujetos procesales deben presentar en forma verbal las razones o argumentos de los que se crean asistidos; replicar los argumentos de las otras partes procesales; presentar pruebas, y contradecir las que se presenten en su contra”. (Ecuador, Asamblea Nacional, 2014)

Este principio es una base de la naturaleza jurídica de la prueba, para contradecir y refutar la verdad de los hechos o de su búsqueda. Para Cabanellas, citado por (Tercero, 2017), “el principio de Contradicción en lo procesal obliga a las partes a facilitar al tribunal los hechos o medios de prueba necesarios para la resolución” (p.33).

Es así como el principio de contradicción hace posible que las partes cuestionen preventivamente todo lo que pueda influir en la decisión final, y como tal presupone la paridad de acusación y defensa en el proceso. Su eficacia es posible sólo si los contendientes tienen la misma fuerza o poderes. Es la posibilidad de refutación de la contraprueba, el derecho a la igualdad ante la ley procesal, para contar con las mismas oportunidades de convencer al juzgador. (Tercero, 2017)

El principio de legalidad constituye la cualidad que distingue por excelencia el estado de derecho. Implica que, en el interior de una organización política, prevalece la voluntad de la ley por sobre la de los gobernantes. El concepto de legalidad no está referido a una ley en particular, sino a cualquier norma incluida en el ordenamiento jurídico”. Es una característica del estado de derecho, en la cual la constitución funge como norma suprema sobre la cual se basa el desarrollo de preceptos jurídicos que constituyen la base de la organización pública, sobre la cual se establecen directrices que norman las actuaciones de los individuos, de éstos con el estado y el poder

público. El principio de legalidad se apoya en el acatamiento a las normas jurídicas y su efectiva administración por parte de la autoridad. (Coello, 2015)

El principio de publicidad permite la existencia de garantía de que el desarrollo de todas las diligencias de prueba sucede en audiencias públicas; es interna porque se desarrolla en presencia e intervención de las partes, y externa, cuando se orienta al control por la sociedad de la actividad jurisdiccional. Este principio está limitado, cuando se trata de secretos de Estado, orden público o asuntos de menores. (Chumi, 2017)

El principio de igualdad garantiza que a las partes se les conceda idénticas oportunidades para presentar o pedir pruebas, refutarlas o contradecirlas, de modo que ninguna tenga privilegios o ventajas. Esta igualdad difiere de oportunidades la igualdad en la distribución de la carga de la prueba para las partes, ya que ésta es un principio que incluye contiene reglas de conducta, tanto para el juzgador (imperativa, aplicada ante la falta de prueba y debe fallar de fondo sin que pueda abstenerse) como para las partes (facultativa, con poder para alegar la prueba y/o libertad para no hacerlo, con el consecuente efecto de su inactividad). (Chumi, 2017)

CAPÍTULO II

2. MARCO METODOLÓGICO

El marco metodológico presenta las acciones que describen y analizan el problema planteado, las técnicas de observación y recolección de datos.

2.1. Metodología utilizada y enfoque de la investigación

Esta investigación integra sistemáticamente los métodos cuantitativo y cualitativo.

El postulado central de los métodos mixtos radica en la retroalimentación de los métodos cuantitativo y cualitativo dentro de una perspectiva metodológica única y coherente, que permitiría un nivel de comprensión del objeto investigativo (y, por ende, de los resultados) más cercana a la complejidad de fenómeno. (Nuñez, 2017)

Esta investigación es mixta, porque para el desarrollo del objetivo general, se recurre a dos recursos: el cualitativo, producto del análisis de los criterios de valoración de la prueba digital y su relación con otros medios de prueba, desde la base de la doctrina y el marco legal relacionado directamente con el objeto de estudio, y el cuantitativo porque se hace uso de instrumentos de recolección de datos para obtener información de una muestra de individuos y analizar las frecuencias de mención de aspectos que servirán de soporte a la conclusión sobre la suficiencia de los criterios de valoración en la prueba digital.

2.2. Métodos aplicados

La estructura empleada para clasificar los métodos aplicados en esta investigación, es la propuesta por (Morán & Alvarado, 2010):

2.2.1. Según los medios

2.2.1.1. Documental.

Esta investigación se basa fundamentalmente en información acumulada en documentos de corte legal, teórico, extraído de:

- Textos jurídicos
- Leyes, Códigos
- Sitios web oficiales de entidades públicas (Fiscalía General del Estado)
- Tesis universitarias de tercer y cuarto nivel
- Teorías básicas clásicas

2.2.1.2. No experimental.

No se busca propiciar la realización de fenómenos mediante manipulación de variables, sino que se recurrió a la observación de las cosas, de la conducta de personas, situaciones, sin intervenir en su comportamiento.

2.2.2. Por los conocimientos que se adquieren

2.2.2.1. Descriptiva.

En esta investigación se especificaron detalladamente, características de las variables objeto de estudio: los criterios de valoración de la prueba digital, las pruebas en el proceso penal, los delitos electrónicos, los sujetos activos y pasivos en torno a este tipo de delitos, entre otros aspectos sometidos a análisis.

2.2.2.2. Explicativa.

Esta investigación no solo describe las variables de análisis señaladas en el punto anterior, sino que también se dirigió a encontrar las posibles causales de la suficiencia o insuficiencia de los criterios de validación para la prueba digital en contraste con otros medios de prueba.

2.2.3. Métodos que predominan en la búsqueda del conocimiento científico

2.2.3.1. Método deductivo.

En esta investigación se aplicó el método deductivo, pues se parte de un precepto general, con formado por los criterios de validación de las pruebas, establecidos en el Art. 457 del COIP, para obtener explicaciones particulares, con relación al procedimiento de delitos informáticos.

2.2.3.2. Método analítico-sintético.

Para este estudio, se hizo uso de este método, ya que se estudiaron los hechos a partir de la descomposición del objeto de estudio (los criterios de validación de prueba y los medios de prueba penal) en cada una de sus partes, para estudiarlas en forma individual y luego se integraron dichas partes para estudiarlas de manera holística, en el momento en que se compararon analíticamente los criterios de validación de los diferentes medios de prueba.

2.3. Técnicas de investigación

Para el desarrollo de este punto, se consultó la estructura propuesta por (Maya, 2014)

2.3.1. La búsqueda de material

Las principales fuentes de trabajo científico fueron:

Fuentes primarias:

- Constitución de la República
- Leyes y decretos
- Tratados internacionales
- Resultados de Tesis de Licenciatura y Maestría
- Revistas electrónicas especializadas
- Libros electrónicos

Fuentes secundarias:

- Referencias doctrinales y conceptuales reflejadas en tesis de grado
- Conceptos referenciados en artículos especializados.
- Interpretaciones de la ley reflejadas en tesis de grado.

2.3.2. El resumen

Esta técnica se aplicó para extraer las ideas de las fuentes consultadas y rehacerlas de manera fiel al texto leído, evitando en lo posible utilizar la escritura fiel del autor, salvo los casos de conceptos muy especializados, en los cuales es necesario recurrir a la cita textual.

2.3.3. La encuesta

La técnica de la encuesta fue utilizada, ya que permite la rápida y eficaz obtención y elaboración de datos, a partir de la interrogación sistemática de un grupo de individuos para conocer su opinión acerca del sistema de valoración de la prueba digital, en comparación con otros medios de prueba.

2.4. Población y Muestra

La población objeto de esta investigación está conformada por los abogados de la República de Ecuador, en libre ejercicio.

Para la elección de la muestra, se extrajo de la población de interés, dada su accesibilidad y fácil disponibilidad, haciendo uso del muestreo no probabilístico por conveniencia.

El muestreo no probabilístico por conveniencia se refiere al que obtiene a personas o unidades convenientemente disponibles para el investigador. Es la técnica de muestreo no probabilística más común, dada su velocidad, costo, efectividad y facilidad de disponibilidad de la muestra. (Zikmund & Babin , 2009)

Es así como la muestra a la cual se aplicaron las encuestas, está conformada por 10 abogados especialistas en el tema de delitos informáticos. Cabe destacar que, mediante una forma de consentimiento informado, a solicitud de los encuestados se les fue protegida su identidad.

2.5. Instrumentos de recolección de datos

Para el análisis del tema objeto de estudio y el desarrollo de los objetivos de esta investigación, se aplicaron dos tipos de instrumentos: uno de tipo documental, en correspondencia con el medio 3.2.1.1 descrito, y la encuesta, en correspondencia con la técnica 3.3.3 descrita.

2.5.1. Matriz analítica

Este instrumento de análisis documental, se utilizó con el fin de extraer del COIP los aspectos vinculados a los criterios de valoración que se detallan y no se detallan, en relación a la prueba digital, a diferencia de otros medios de prueba, con el fin de contar con insumos para concluir el nivel de suficiencia de los criterios de valoración para la prueba digital en procesos de delitos informáticos.

Tabla 7. Formato Matriz analítica

Componente (Criterio de valoración)				
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		

Elaborado por: Ximena Cantos.

El llenado del formato anterior presentado, se incorpora a continuación:

Tabla 8. Matriz analítica con la información recopilada

Componente (criterio de valoración)	**Legalidad**			
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		
Se refiere a la forma de obtención de la prueba y cómo es incorporada al conjunto de elementos probatorios	X		Documentales físicas o materiales, testimonio, pericia y de contenido digital.	Se establece como criterio de valoración en el artículo 457 del Código Orgánico Integral Penal (COIP), pero no se define en este.
Se relaciona con el principio de exclusión que establece que toda prueba o elemento de convicción obtenidos con violación a lo establecido en la Constitución, en los convenios internacionales o en la Ley, carecerán de eficacia probatoria y por tanto, se excluyen de la actuación procesal.	X		Documentales físicas o materiales, testimonio, pericia y de contenido digital.	Se define en el artículo 454 literal 6 del COIP y es general para "Toda Prueba"
Establece taxativamente las reglas por las cuales se rige la presentación del medio de prueba	X		Documentales físicas o materiales, testimonio, pericia y de contenido digital.	En el caso de la prueba documental de contenido digital, están estictamente establecidas en el artículo 500 del COIP.

Elaborado por Ximena Cantos.

Tabla 9. Matriz analítica con la información recopilada

Componente (criterio de valoración)	**Autenticidad**			
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		
Está referido a la inalteración de la prueba por ninguna circunstancia externa o interna, desde su creación u origen hasta su evacuación en el proceso.		X	Documentales, testimoniales y periciales.	Se establece como criterio de valoración en el artículo 457 del Código Orgánico Integral Penal (COIP), pero no se define en este.
Únicamente puede ser garantizada por la cadena de custodia		X	Documentales, testimoniales y periciales.	Por mandato del artículo 456 del Código Orgánico Integral Penal (COIP)
Se exige acreditación por otros medios		X	Exhibición de documentos para la exhibición de vídeos, grabaciones u otros	Contenida en el art. 616 del Código Orgánico Integral Penal (COIP)

Elaborado por Ximena Cantos

Tabla 10. Matriz analítica con la información recopilada

Componente (criterio de valoración)	**Cadena de custodia**			
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		
Debe iniciar en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente	X		Todo tipo de prueba de contenido físico o digital	Establecido en el artículo 456 del COIP
Es exigible como garantía de autenticidad para la prueba de contenido digital	x			Descripción del elemento para la fase investigativa
No requiere de acompañamiento pericial	X		Solo en la de exhibición para la prueba digital es diferente	Contenida en el art. 616 del Código Orgánico Integral Penal (COIP)

Elaborado por Ximena Cantos

Tabla 11. Matriz analítica con la información recopilada

Componente (criterio de valoración)	**Grado de aceptación científica y técnica de los principios de los informes periciales**			
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		
Se exige el elemento de actualidad científica del perito		X	Todos los medios de prueba distintos al procedimiento investigativo para la de contenido digital	Para la prueba de contenido digital no se establece o define cuál o cómo debe medirse el grado de aceptación científica y técnica. Ese grado es únicamente de libre valoración judicial. Discrecional.
Principios en que se fundamenten los informes periciales		X	Ninguno	No se definen ni mencionan cuáles deben ser tales principios

Elaborado por Ximena Cantos

Tabla 12. Matriz analítica con la información recopilada

Componente (criterio de valoración)	**Elementos probatorios y evidencia física no sometidos a cadena de custodia**			
Contenidos mínimos	Tratado en el COIP para la prueba específica de contenido digital (Art. 500)		Tipos de pruebas en las que sí se desarrollan los contenidos mínimos	Observaciones
	Sí	No		
El enunciado está definido en el COIP		X	Para la acumulación de indicios en caso de personas desaparecidas	Es un artículo inequitativo y excluyente. Solo para el caso que expresamente menciona.

Principios en los cuales se fundamente o su definición		X		Los indicios son importantes en todo procedimiento y deberían emplearse también en los de delitos informáticos, ya que por su naturaleza, estos pueden contribuir a reconstruir la secuencia digital delictiva.
Admite prescindir de la cadena de custodia		X	Solo en casos de personas desaparecidas, documentales materiales o físicos, testimoniales y periciales	Es necesario que la prueba digital prescinda de la cadena de custodia al menos en la fase originaria y de recolección, pues cuando se origina, es imposible que haya un perito presente o que se ocupe de recoger la prueba.

Elaborado por Ximena Cantos.

2.5.2. Encuesta

La Encuesta aplicada es de tipo estructurada, conformada por cuatro preguntas cerradas que tien por objeto conocer la opinion de abogados especialistas en delitos informaticos sobre la regulacion de la prueba de conteido digital mediante el uso de criterios establecidos en el articuo 457 del COIP . A continuación se presenta el modelo. Los datos recolectados de las encuestas, fueron codificados con el uso de hojas de cálculo de Microsoft Excel y las herramientas de gráficos fueron empleadas para la presentación de los resultados.

2.6. Validez y confiabilidad del Instrumento de recolección de datos

Para conocer el grado en que el instrumento aplicado, en este caso, la encuesta, puede obtener los datos que pretende recolectar (Validez), así como también el grado en que su repetida aplicación genera resultados similares (Confiabilidad), se realizó una prueba piloto, que consistió en aplicar la encuesta, previamente, a un grupo de tres abogados de cualquier especialidad, con el fin de: 1) Observar cómo éstos realizaron el llenado de la encuesta, si tuvieron algunas dudas o algún tipo de incomodidad; 2) Recoger impresiones y observaciones sobre la encuesta respondida. Los resultados se presentan en la siguiente tabla:

Tabla 13.Resultados de la aplicación prueba piloto

Ítem 1. Observación
El grupo de abogados quienes voluntariamente aceptaron colaborar con la prueba piloto se mostró accesible y participativo en el proceso de llenado de la encuesta. Algunos manifestaron tener algunas dificultades para comprender las preguntas 2 y 4 del instrumento, sin embargo, todos pudieron dar respuesta a éste en su totalidad.
Ítem 2. Impresiones y observaciones de los encuestados.
Abogado 1. Manifestó que el instrumento estaba bien redactado y guardaba una correspondencia lógica en la distribución de las preguntas. Sugirió incorporar opciones en la pregunta número 4, sugerencia que fue atendida y ajustada.
Abogado 2. Manifestó que no tenía mayores observaciones al documento, al menos de forma, ya que de fondo señaló que no manejaba el tema con propiedad.
Abogado 3. Manifestó que el instrumento le pareció entendible, sencillo y suficiente para recoger la información requerida. Cabe destacar que este abogado es especialista en delitos informáticos.

Elaborado por: Ximena Cantos.

Luego de la aplicación de la prueba piloto, se incorporaron los ajustes sugeridos, para proceder con la aplicación definitiva del instrumento validado, lo cual es analizado e interpretado en el capítulo siguiente.

CAPÍTULO III

3. ANÁLISIS DE LOS RESULTADOS Y PROPUESTAS

Este capítulo refiere los resultados derivados de los hallazgos de la investigación en cuanto a las matrices analíticas derivadas del método teórico-documental en conjunto con la técnica de la encuesta, debidamente validadas en la forma descrita en el capítulo anterior, así como con los aportes realizados por la autora de esta para poder presentar un informe detallado, argumentado y con el carácter científico requerido.

Siguiendo la metodología propuesta, se han estructurado los resultados con base en los objetivos de la investigación por lo que, brevemente, se presentan los planteamientos teóricos que responden la interrogante formulada como problema la cual era ¿Existe seguridad jurídica en la valoración de la prueba de contenido digital mediante el uso de los criterios establecidos en el art. 457 del COIP en los procedimientos de delitos informáticos? tal y como pudo señalarse en la primera parte del estudio relacionada con la problemática, esto es, en la introducción.

Concretamente la respuesta a dicha pregunta resultó ser que no hay seguridad jurídica para las partes interesadas en promover alguna prueba de contenido digital cuando, en la investigación, ésta no ha sido obtenida conforme al procedimiento descrito en el artículo 500 del Código Orgánico Integral Penal pues, al contrastar esto, con la disposición que orienta la valoración judicial de la prueba, las mismas presentarían un vicio en su elemento de legalidad pues por lo general no pueden ser obtenidas conforme estrictamente lo dispone el mencionado artículo.

Así mismo la autenticidad podría criticarse por el no seguimiento de la cadena de custodia en manos de peritos especializados tal y como dispone el legislador y el juzgador dejaría sin valoración la prueba de contenido digital en los delitos informáticos.

Como se presenta detalladamente en este capítulo, se realizó un análisis de las encuestas y matrices de análisis deductivo, para poder realizar una descripción suficiente de los hallazgos y mediante un desglose de información y métodos de

saturación e interpretación, examinar la calidad de la información a los fines de la investigación.

Tabla 14. Análisis de Resultados Teóricos derivados de la matriz para la identificación del sistema de valoración de la prueba existente en el artículo 457 del COIP para la prueba de contenido digital utilizable en los procedimientos de delitos informáticos.

Criterio de Valoración analizado	**Resultados en lo que respecta a la prueba de contenido digital**	**Considerado para la propuesta (Si o No)**	
Legalidad	Es un elemento relacionado directamente con la eficacia probatoria exigible por mandato de las disposiciones del artículo 454 del COIP. El desacato a las indicaciones expresadas en el artículo 500 para la investigación que logra encontrar la prueba de contenido digital anula la prueba por afectación del criterio de legalidad. No existe otra forma en el COIP por la que sea realmente posible garantizar que la prueba digital que desde su origen no haya estado bajo cadena de custodia en los términos indicados, vaya a ser valorada por el sentenciador a los efectos de su veredicto, quedando los administrados afectados en estado de vulnerabilidad e indefensión.	Sí	
Autenticidad	Es el elemento directamente relacionado con la verdad y exacta coincidencia de un medio probatorio con los hechos. La prueba de contenido digital requiere necesariamente de la cadena de custodia desde su origen para demostrar autenticidad por mandato del legislador. Al referirse a la exhibición de documentos digitales, el artículo 616 del COIP hace el requerimiento de autenticidad de nuevo ratificándose lo que exige el artículo 500 pero con ello, deja claro, que no podrá valorarse la prueba con apego a lo que ordena el artículo 457 del mismo código.	Sí	
Cadena de Custodia	Se entiende por la doctrina que es la secuencia de pasos que deben seguirse en la fase de recopilación, traslado y resguardo de una prueba que será utilizada en un procedimiento judicial, sin embargo, el legislador no la define, no la detalla en cuanto a sus pasos y exige obligatoriedad de cumplimiento para los medios de contenido digital. Además de se confiere la acreditación de autenticidad del medio probatorio a esta secuencia. Es el caso que la prueba de contenido digital al no ser de tipo tangible, los delitos se producen de	Sí	

	manera asíncrona con el conocimiento de la víctima y mucho menos con el de algún perito especializado por lo que se concluye que el procedimiento establecido en el artículo 500 del COIP es en la mayoría de casos, irrealizable de manera exacta, con lo cual, el legislador al aplicar los criterios de valoración del artículo 457, entendería que, sin cadena de custodia no puede haber autenticidad y mucho menos legalidad en la obtención de la prueba, vulnerando la carta magna en cuanto al derecho a la defensa de los beneficiarios de la ley.		
Grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales	Está relacionado con el nivel de conocimientos actualizados en la pericia aplicada en un procedimiento sobre algún tipo de prueba promovida. La ley no define este requerimiento de valoración, aunque el término “actual” conduce a pensar que el juez tiene la responsabilidad de verificar si el perito seleccionado está recientemente capacitado en las últimas técnicas científicas y demás novedades en su materia, sin embargo, esto es solamente una inferencia cuando lo correcto es que el legislador explique lo que se precisa para valorar de manera inequívoca un informe pericial. Tampoco se establecen cuáles son los principios en los que debería fundamentarse dicho informe por lo que, como resultado de la presente investigación, está claro que este elemento también exigible para la obtención de la prueba de contenido digital según el artículo 500 del COIP, es atentatorio contra la seguridad jurídica y el derecho a la defensa.	Sí	
Excepción a la cadena de custodia	Aparece como un enunciado en el primer aparte del artículo 457 permitiendo que, bajo su responsabilidad, la parte pueda probar la autenticidad de una prueba no sometida a esta secuencia de pasos, sin embargo, aunque no lo diga expresamente, esta excepción no está permitida para la recolección y procesamiento de la prueba digital pues de hacerlo, la misma estaría viciada de ilegalidad y falta de autenticidad por su origen, este resultado es producido en la investigación al contraponer los artículos expresamente analizados, es decir, 456, 457 y 500 del COIP.	Sí	

Elaborado por: Ximena Cantos.

Es importante tomar en cuenta que los criterios de valoración de la prueba son incluyentes, es decir, que la ausencia determinada de uno solo de ellos afectaría la validez de la misma de tal forma que esta quedaría sin efecto. Por otra parte, una cosa es la investigación que se realiza bajo las directrices legales y otra cosa es la legalidad de la prueba en su forma de obtención, sin embargo, el legislador ha mezclado ambos elementos al plantear la investigación que busca obtener una prueba de contenido digital, lo cual, puede apreciarse en el artículo 500 del COIP suficientemente explicado a lo largo de la presente investigación.

Esta mezcla de elementos deja de manos atada a los beneficiarios de la ley en lo que respecta a la prueba de contenido digital que se ha obtenido fuera de la propia investigación, esto es lo que comúnmente sucede, de hecho, cuando se verifica la acción tipificada como delito es porque la víctima se percata en equipos y comunicaciones personales, que efectivamente sus derechos han sido vulnerados.

Si los criterios de valoración son incluyentes, como en efecto lo son, se tendrían casos en los que, aunque la prueba haya sido obtenida conforme al procedimiento de ley y observación de la cadena de custodia, pero esté viciada por algún defecto en su autenticidad o en los principios tomados en cuentas por el perito, especialmente tomando en cuenta que ninguno de ellos está definido por el legislador.

Otro resultado de relevancia es que, en comparación con otros medios de prueba, la de contenido digital no puede hacer uso del primer aparte del artículo 457 referido a la posibilidad de demostrar un hecho aun cuando la prueba no se haya sometido a la cadena de custodia, en virtud de que eso significaría que la prueba no ha sido obtenida conforme a la legalidad que exige el artículo 500.

Así como está explicada la cadena de custodia en el artículo 456 del COIP (2014), que se cita:

> Art. 456 Cadena de custodia. **Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad**, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la

> recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio. (Ecuador, Asamblea Nacional, 2014)
>
> **La cadena inicia en el lugar donde se obtiene**, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación. (Ecuador, Asamblea Nacional, 2014)

No es suficiente para comprenderla y aplicarla porque no se entiende lo que realmente es la cadena de custodia sin el auxilio de la doctrina, lo cual conlleva a infinitas interpretaciones y da cabida a una discrecionalidad judicial prácticamente ilimitada; cuanto menos entendibles son así, los otros criterios ni siquiera mencionados de forma aparte al mismo artículo 457.

Tampoco el legislador parece haber considerado el principio de libertad de prueba según el cual, cualquier medio probatorio (refiriéndose al tipo de medio) que sirva para esclarecer la verdad de los hechos, debe ser validado por él en sentencia siempre que las pruebas sean pertinentes, idóneas, conducentes y por supuesto, legales y legítimas. Con las exigencias descritas en el artículo 500, la prueba de contenido digital no sometida a cadena de custodia siempre será vista como ilegal o ilegítima en su obtención. No tiene garantía de validez, porque esa es la finalidad no negociable de la cadena de custodia como ya se ve en el artículo 456.

Es preciso que el cuerpo jurídico normativo, sea lo suficientemente específico en cuanto a explicar las definiciones, delimitaciones, fases y procedimientos que deben seguirse para dar por entendido cada criterio de valoración y se pueda garantizar la seguridad jurídica mediante los principios del derecho a la defensa y al debido proceso, pues de lo contrario, se estaría vulnerando la propia Constitución de la República.

La finalidad de la justicia es que ningún delito quede impune pero las máximas de experiencia y las reglas de la sana crítica, no garantizan nada por encima de la ley y

por ello, muchas pruebas de contenido digital pueden ser mal valorada o declaradas ineficaces por un asunto de formalidad y de legalidad exigibles en el procedimiento penal.

El legislador le ha conferido igualmente a la cadena de custodia una carga de suma importancia como es garantizar la autenticidad de la prueba de contenido digital, pero, al omitir en qué consiste o la manera en cómo debe realmente aplicarse, ha cercenado tanto al juez como a las partes, la forma de utilizar aquellas que solo pueden formar parte de esa cadena cuando, mucho tiempo después de originadas, se suman al procedimiento especialmente de delitos informáticos. Si los delitos se producen a través de una nube de datos, valdría preguntarse cómo y desde donde debe comenzar a regir la cadena de custodia.

Según los datos proyectados por la Fiscalía General del Estado al cierre del ejercicio del año 2019, los principales delitos informáticos cometidos en el país fueron el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, el ataque a la integridad de sistemas informáticos, la interceptación ilegal de datos y la revelación ilegal de base de datos, tal como puede apreciarse en el siguiente gráfico:

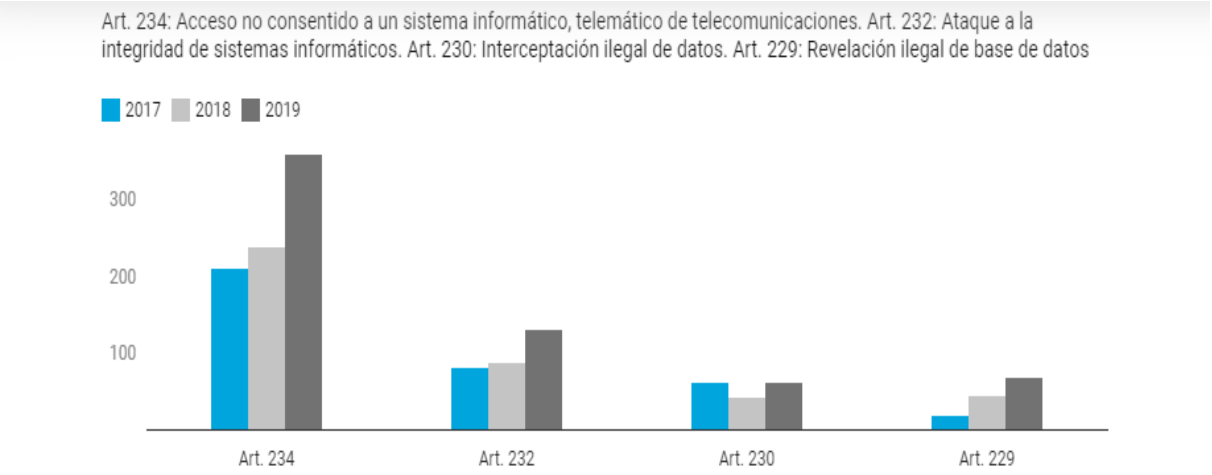

Figura 2. Acceso no consentido a un sistema informático
Fuente: (Primicias, 2019)

Todos estos delitos ameritan de la prueba de contenido digital y de la valoración correcta del juez para que haya sentencias justas por encima de unas estadísticas de

denuncias mal resueltas en la mayoría de las veces y con razón ya que el legislador no ha sabido dar a estas, las directrices adecuadas en su regulación.

Resultados de la encuesta realizada:

A continuación, se procede a presentar los resultados de las encuestas aplicadas mediante el acuerdo de confidencialidad descrito en el capítulo anterior de esta investigación. Se hace énfasis en que, de acuerdo a las instrucciones del cuestionario, los encuestados podían seleccionar más de una opción de respuesta para las preguntas números 2 y 4.

Pregunta 01. ¿Ha detectado deficiencias en los criterios de valoración para la prueba digital no sometida a la cadena de custodia, conforme al artículo 457 del COIP?

Tabla 15. Pregunta 1

Opciones	Respuesta	Porcentaje
SÍ	9	29%
No	1	71%

Elaborado por: Ximena Cantos.

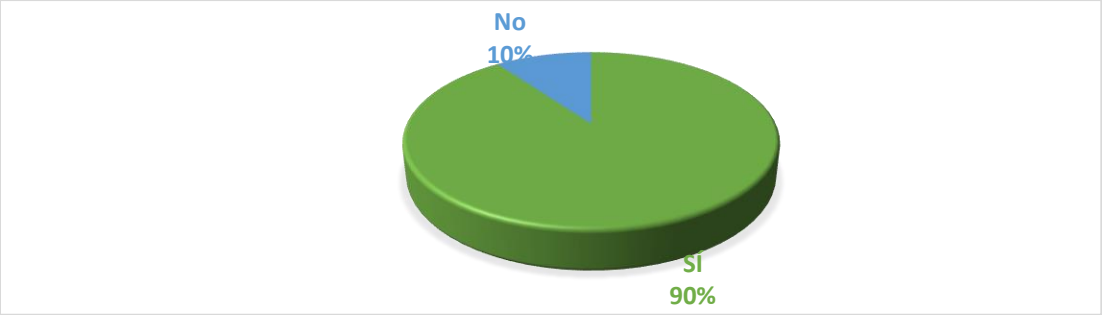

Figura 3.¿Ha detectado deficiencias en los criterios de valoración para la prueba digital no sometida a la cadena de custodia, conforme al artículo 457 del COIP?
Elaborado por Ximena Cantos.

Análisis del resultado de las encuestas

Se observa que, del total de los encuestados, la mayor parte de los abogados especialistas en delitos informáticos (90%), han detectado deficiencias en los criterios

de valoración para la prueba digital, no sometida a cadena de custodia, frente a un 10% (comprendido por un especialista) quien expresó no haber detectado tales deficiencias.

Pregunta 02. ¿Cuáles deficiencias?

Tabla 16. Opciones pregunta 2

Opciones	Total respuestas	Porcentaje
a) No concordancia con el artículo 500 del COIP.	10	100%
b) Incongruencia con el criterio de autenticidad.	8	80%
c) Imposibilidad de la pericia en el origen de la prueba.	9	90%
d) Inexactitud en la definición de los criterios.	8	80%

Elaborado por: Ximena Cantos

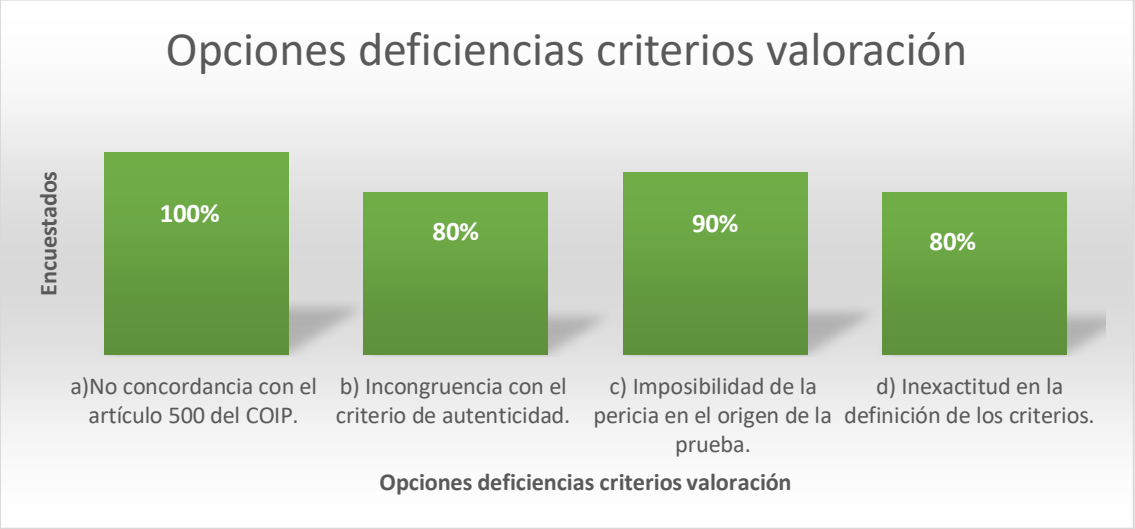

Figura 4. Porcentajes respuestas a la pregunta 2
Elaborado por Ximena Cantos.

Análisis del resultado de las encuestas

Se puede observar que cada opción fue escogida por un porcentaje mayor o igual al 80% de los encuestados, lo que sugiere que todas las deficiencias propuestas son reconocidas como tales por los especialistas encuestados y al alcanzar tales porcentajes, se detecta la existencia de la necesidad de corregir la ley.

Pregunta 03. ¿Considera necesaria una mejor regulación legal para la valoración de la prueba digital por parte del juzgador en los procedimientos de delitos informáticos?

Tabla 17. Pregunta 3

Opciones	Respuesta	Porcentaje
SÍ	8	80%
No	2	20%

Elaborado por: Ximena Cantos.

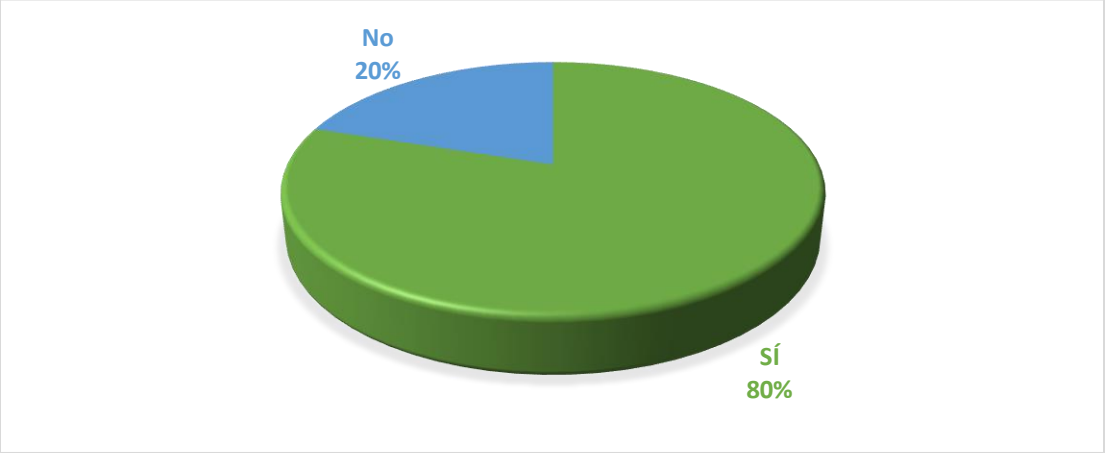

Figura 5. Porcentajes respuestas a la pregunta 3
Elaborado por Ximena Cantos.

Análisis del resultado de las encuestas

Del resultado se observa que el 80% de los encuestados considera necesaria una mejor regulación legal para la valoración de la prueba digital por parte del juzgador en los procedimientos de delitos informáticos, a diferencia de un 20% que afirma no considerar necesario dicho procedimiento.

Pregunta 04. ¿Cuáles contenidos mínimos debe incluir la Ley para ofrecer seguridad jurídica frente a la valoración judicial de la prueba digital?

Tabla 18. Pregunta 4

Opciones	Respuestas	Porcentaje
a) Definición y delimitación de cada criterio de validación	10	100%
b) Valoración de la prueba digital no sometida a cadena de custodia	7	70%
c) Establecer otras formas de garantía de autenticidad	7	70%
d) Considerar las particularidades de la prueba de contenido digital	10	100%

Elaborado por: Ximena Cantos.

Figura 6. Porcentajes respuestas a la pregunta 4
Elaborado por Ximena Cantos.

Análisis del resultado de las encuestas

Se puede observar que cada opción fue escogida por un porcentaje mayor o igual al 70% de los encuestados, lo que sugiere que todas las propuestas de contenidos mínimos en materia de valoración de la prueba digital que debe incluir la Ley son identificadas y avaladas como necesarios por los especialistas encuestados.

Al relacionar los resultados obtenidos en la matriz de análisis documental como los que corresponden a las encuestas, es preciso indicar que ambas fuentes de datos son análogos en cuanto a sus posturas y como resultados integrales de la presente investigación se obtuvo, con altos porcentajes de respuestas, que existen deficiencias en los criterios de valoración cuando son aplicados a la prueba digital que no es sometida a la cadena de custodia, conforme lo exige el artículo 457, ya que este no guarda concordancia con el artículo 500.

Por otra parte, hay incongruencia con el criterio de autenticidad y todos los demás criterios de valoración; se hace imposible la aplicación de pericia en el origen de la prueba de contenido digital y hay una manifiesta necesidad de determinar con exactitud la definición de los criterios de valoración respecto a todos los tipos de prueba y más aún, con la naturaleza de la prueba de contenido digital.

Por tales razones, los encuestados sugirieron con la opinión compartida de esta investigadora que dentro de las posibles reformas a la normativa del COIP, debe considerarse:

Primero: la definición, delimitación y procedimiento de validación de cada criterio, es decir, de lo que debe entenderse por legalidad, autenticidad, cadena de custodia, actualidad científica de la prueba pericial y la posibilidad de validar pruebas no sometidas a cadena de custodia como es el caso de la mayor parte de las de contenido digital necesarias en los procedimientos de delitos informáticos.

Segundo: la valoración de la prueba digital no sometida a cadena de custodia, es decir, que se permita y se regule.

Tercero: establecer otras formas de garantía de autenticidad que no sea únicamente la cadena de custodia desde el origen del hecho delictivo y de la prueba.

Cuarto: considerar las particularidades de la prueba de contenido digital y establecer para su obtención y valoración un mecanismo especial, más adaptado a la realidad de las circunstancias actuales de proliferación de las actividades digitales.

Es un hecho necesario la revisión y modificación del Código Orgánico Integral Penal en lo que respecta a la prueba de contenido digital y debe hacerse de forma urgente ya que, la necesidad de todas las gestiones cotidianas, comerciales y jurídicas de la ciudadanía, especialmente por la pandemia, se están realizando a través del uso de medios digitales, por lo cual, esta autora presenta la siguiente propuesta.

Propuesta

Título de la Propuesta: Directrices para consideración en el proceso de seguimiento y evaluación de la ley por parte de la Unidad Técnica Legislativa de la Asamblea Nacional del Ecuador, caso: Código Orgánico Integral Penal.

Objetivo: Someter a consideración de la Unidad Técnica Legislativa de la Asamblea Nacional del Ecuador directrices generales y específicas observables en el proceso de seguimiento y evaluación de la ley en el caso del Código Orgánico Integral Penal.

Alcance: para establecer el alcance de esta propuesta se siguió el método SMART, cuyo significado de traduce de las iniciales del inglés como a continuación se describe:

S (specific) – Alcance específico.

M (measurable) – Medible, ya sea en sus datos o en su impacto.

A (achievable) – Posible. Referido a su realización.

R (real) – Factible, es decir, que, conforme a los recursos y tiempo disponibles, se lleve a cabo.

T (time-related) – Se refiere a la fijación del tiempo de elaboración.

Como alcance específico esta propuesta pretende hacerse llegar a la Unidad Técnica de la Asamblea Nacional para que sea parte del próximo proceso de

seguimiento y evaluación de la ley en el caso del Código Orgánico Integral Penal como competencia de aquella.

La Unidad Técnica de la Asamblea Nacional tiene entre sus funciones mantener la vinculación con la comunidad académica para viabilizar el análisis de los temas legislativos de interés social a través de diferentes procesos entre los cuales, se destaca el de seguimiento y evaluación de leyes ya aprobadas con la finalidad de revisar su eficacia y necesidad de actualización según sea determinado por ésta.

La Unidad Técnica es quien emite las asesorías técnicas en materia de construcción y perfeccionamiento sobre la calidad de los proyectos de ley o de reformas de ésta. Todo conforme a lo establecido en el artículo 30 de Ley Orgánica de la Función Legislativa que establece:

> **Artículo 30.-** Unidad de Técnica Legislativa.- Se crea la Unidad de Técnica Legislativa con el objeto de acompañar el proceso de creación de la norma y proveer a las comisiones especializadas y al Pleno de la Asamblea de un informe no vinculante sobre los siguientes temas: 1. Normas legales vigentes que se verían afectadas o deberían derogarse o reformarse con la aprobación de la norma propuesta; 2. Lenguaje utilizado en la norma y revisión de lenguaje no discriminatorio; 3. Impacto de género de las normas sugeridas; y, 4. Estimación del costo que podría provocar la implementación de la norma. Quienes integran esta comisión multidisciplinaria serán profesionales hombres y mujeres, altamente calificados para el tratamiento de estos temas. (Ecuador, Asamblea Nacional, 2009, pág. 10)

> **Art. 31.-** Codificación por la Unidad de Técnica Legislativa. - Por decisión expresa del Pleno de la Asamblea Nacional, la Unidad de Técnica Legislativa podrá preparar proyectos de codificación de diversas leyes, que serán puestos a conocimiento de la respectiva comisión especializada permanente para que ésta realice el informe correspondiente en un plazo máximo de sesenta días. (Ecuador, Asamblea Nacional, 2009, pág. 10).

En cuanto al aspecto de medible, el impacto de esta propuesta será cuantificable una vez que sea sometida a consideración de la Unidad antes referida y de la comisión permanente correspondiente.

Es una propuesta perfectamente posible, al dirigirse mediante oficio al Dr. Paulo César Gaibor quien preside la respectiva Unidad. Conforme a los recursos y tiempo disponibles en este trabajo de investigación, la propuesta será efectivamente enviada. El tiempo de elaboración de la propuesta fue de 10 días durante los cuales se elaboró el capítulo de esta investigación correspondiente a los resultados.

Limitaciones: Dentro de las limitaciones que esta propuesta puede encontrar deben considerarse en primer lugar, las prioridades de agenda de la Unidad Técnica Legislativa para la consideración de los requerimientos ciudadanos como beneficiarios de la ley. En segundo lugar, la transición gubernamental que se está realizando producto del cambio de mandato presidencial que podría incluir algunas reformas de actuación de la referida unidad.

Fundamento fáctico: como fundamentos de hecho de esta propuesta se señalan los hallazgos y resultados de la investigación titulada: **VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS** de la autoría de Ximena Valeria Cantos Mestanza.

Fundamentos legales: Dentro de estos se encuentran las disposiciones de la Constitución de la República referidas a la Participación Ciudadana y Control Social: Art. 11 Núm. 3, Art. 66 Núm. 23, Art. 127, 134, 204, 206, 384, entre otros. Artículos 30 y 31 de la Ley Orgánica de la Función Legislativa.

Vale aquí indicar que únicamente cuando algún proyecto de ley o reforma de una se encuentra bien redactado, “desde un punto de vista técnico y sistemático, pueden realizarse las modificaciones de contenido deseadas … sin que se produzca una ley oscura o contradictoria” (García-Escudero, 2010, p. 10).

Contenido: Directrices Generales y específicas.

Como directrices generales para la modificación del Código Orgánico Integral Penal se sugieren:

1. Revisar exhaustivamente el fundamento fáctico de esta propuesta, es decir, revisar el análisis de datos y resultados a los que se llega en la investigación **VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS**, a objeto de verificar los hallazgos encontrados que dieron lugar a la presente iniciativa.
2. Relacionar los artículos 456, 457 y 500 del Código Orgánico Integral Penal a los fines de detectar las incongruencias que existen entre ellos y que limitan el derecho a la defensa de la parte que pretende servirse de la prueba de contenido digital.

Como directrices específicas deben considerarse las siguientes:

1. Revisar el artículo 500 del Código Orgánico Integral Penal (2014) del que textualmente dice:

Contenido digital. El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. (Ecuador, Asamblea Nacional, 2014)

En la investigación se seguirán las siguientes reglas:

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.

2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto (Ecuador, Asamblea Nacional, 2014).

Motivado en que este artículo dictamina la línea de investigación en el caso de medios probatorios de contenido digital sin considerar que en la mayoría de los casos de delitos informáticos contemplados en el mismo código, las pruebas en su origen, no pueden materialmente estar sometidas a cadena de custodia, de manera que la posibilidad de que la parte que los presente tenga a su cargo la demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, contemplada en los criterios de valoración establecidos dentro del artículo 457 del mismo COIP, limitaría el derecho a la defensa de los interesados y esto, vulnera los preceptos fundamentales de la Carta Magna.

2. Revisar el artículo 457 del Código Orgánico Integral Penal que textualmente dice:

> Criterios de valoración. La valoración de la prueba se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales. La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente (Ecuador, Asamblea Nacional, 2014, pág. 72).

En el caso de delito de desaparición involuntaria, la acumulación de indicios servirá de nexo causal vinculante siempre y cuando dichos indicios se relacionen con el

hecho o circunstancia a probar y sean inequívocos respecto del hecho o circunstancia controvertida.

Debido a que se detectan las siguientes deficiencias que son necesarias para garantizar el derecho a la defensa de los beneficiarios de la ley:

a) No existe definición expresa en el cuerpo normativo de lo que debe entenderse por legalidad ni por autenticidad de la prueba, dejando al arbitrio del legislador la consideración de la doctrina según la cual puedan apreciarse tales criterios, así como la temporalidad a partir de la cual deban apreciarse, esto es, momento de presentación de la prueba o momento en el cual aquella se originó;
b) En lo que se refiere a dejar a cargo de la parte que la presente, la prueba no sometida a cadena de custodia; este parágrafo excluye la prueba de contenido digital porque la ley no concede para este tipo de medio, durante su etapa de investigación, la posibilidad de excluir la cadena de custodia. De manera que la parte que consiga la prueba fuera de dicha cadena, pero se someta a ella luego de presentar la prueba en el procedimiento, quedaría en indefensión, es decir, su prueba sería ineficaz por falta de legalidad.
c) En cuanto a la acumulación de indicios, la forma de valoración probatoria es inequitativa frente a otros procedimientos para los cuales también pudiera ser necesaria como es el caso de los delitos contra la seguridad de los activos de los sistemas de información y comunicación también conocidos como delitos informáticos.
d) Se sugieren como contenidos mínimos que debe incluir la Ley para ofrecer seguridad jurídica frente a la valoración judicial de la prueba digital una definición y delimitación clara de cada criterio de validación, especificar los pasos de la cadena de custodia, la posibilidad de valoración de la prueba digital no sometida a cadena de custodia, el establecimiento de otras formas de garantía de autenticidad distintas a la cadena de custodia y por último, considerar las particularidades exclusivas de la prueba de contenido digital.

Conclusión:

En definitiva, se somete a conocimiento de la Unidad Técnica Legislativa de la Asamblea Nacional, la necesidad de relacionar y modificar con amplitud, a partir de un discernimiento normativo y crítico, los artículos antes presentados para garantizar la seguridad jurídica de los beneficiarios de la ley especialmente vinculados a procedimientos en los que la prueba principal promovida será, por su naturaleza, la de contenido digital, tal como sucede con otros medios de prueba tales como la documental material, la testimonial y la pericial.

Oficio que acompaña a la propuesta:

Quito; 27 de mayo de 2021

Dr. Paulo César Gaibor
Director de la Unidad Técnica Legislativa de la Asamblea Nacional
Su despacho.

Señor Director según lo dispuesto en los artículos 30 y 31 de la Ley Orgánica de la Función Legislativa presento a usted, en mi calidad de beneficiaria de la ley y en ejercicio de mi derecho de petición y de participación consagrados en la Constitución de la República, una propuesta para incluirse en el proceso de seguimiento y evaluación de la ley en el caso del Código Orgánico Integral Penal que lleve a cabo su respectivo despacho para que sea analizada por los especialistas de su unidad, remitida a la comisión correspondiente, difundido a los asambleístas y de ser posible, a la ciudadanía a través del portal web con la previa revisión técnica para informe no vinculante correspondiente.

Atentamente;

Ximena Valeria Cantos Mestanza, Abg.
Ciudadana Ecuatoriana.
Se adjunta Tesis de Grado de mi autoría, aprobada por la Universidad Metropolitana (UMET) en la que se soportan científicamente las directrices propuestas.

Elaborado por: Ximena Cantos.

CONCLUSIONES

Caracterizar jurídica y doctrinalmente los delitos informáticos del Código Orgánico Integral Penal, sirvió para explorar en ellos la necesidad de la prueba de contenido digital con la finalidad de tener un debido proceso y finalmente, obtención de justicia. De nada sirve la tipificación de un delito, el establecimiento de una posible pena y la responsabilidad penal si no existen criterios de valoración judicial adaptados al tipo de prueba para que puedan exigirse y defenderse los derechos de las partes, lo cual, conllevó a la necesidad de comparar con otros medios y concluir que deben hacerse algunas adecuaciones legales.

Al identificar el sistema de valoración de la prueba existente en el artículo 457 del COIP para la prueba de contenido digital, fue posible concluir que este no es compatible con la descripción que el mismo legislador hace en el artículo 500 puesto que se ha establecido un procedimiento de obtención para ella que exige el sometimiento a la cadena de custodia pericial en cada etapa y esto no se corresponde con la realidad práctica ya que muchas veces, en el momento de producirse el hecho delictivo la prueba está fuera del alcance, incluso de la propia víctima.

De ser así lo anterior, al momento de presentarse la prueba dentro del procedimiento, se determinará que no se ha cumplido con lo establecido en la ley, de manera, que a la hora de valorarla, según el artículo 457 se verá afectada de ilegalidad, falta de autenticidad, estará fuera de la cadena de custodia, entre otros y esto la convierte en ineficaz conforme al fin para el cual ha sido considerada y principalmente, para su uso en los procedimientos de delitos contra la seguridad de los activos de los sistemas de información y comunicación también llamados delitos informáticos.

Por las anteriores razones, la propuesta de presentar directrices de ampliación del sistema de valoración de la prueba de contenido digital en comparación con otros medios de prueba, encontró su justificación y pertinencia para cerrar esta investigación concluyendo que los criterios de valoración legal existentes en el Código Orgánico Integral Penal para la prueba documental de contenido digital en los procedimientos de

delitos informáticos no es la más idónea para los beneficiarios de la ley y la garantía de su derecho de prueba y por tanto a la defensa y el debido proceso.

RECOMENDACIONES

A la Unidad Técnica Legislativa de la Asamblea Nacional del Ecuador se sugiere la revisión de hallazgos presentados como resultados de esta investigación con la finalidad de mejorar la ley y ofrecer mayor seguridad jurídica en los procedimientos de delitos informáticos.

A la Comisión Especializada de Derechos en lo Penal de la Asamblea Nacional del Ecuador, se sugiere la presentación de un proyecto de ley reformatoria del Código Orgánico Integral Penal previo informe no vinculante de la Unidad Técnica Legislativa producto del proceso de seguimiento y evaluación de la ley para el cual es expresamente competente atendiendo a las directrices propuestas en la presente investigación.

A las facultades de Ciencias Jurídicas y Políticas de las diferentes casas de estudio, reforzar las mallas curriculares en materia de Derecho Parlamentario y técnica legislativa con la finalidad de que, desde estas, puedan vincularse de manera directa proyectos de leyes reformatorias al trabajo de la Asamblea Nacional.

A todos los beneficiarios de la ley (Código Orgánico Integral Penal) para que impulsen la reformatoria del COIP en virtud de la necesidad de proteger la información y actividades jurídicas que cada día son más necesarias y están vulnerables de numerosos hechos delictivos, pues frente a ellos, quedarían en estado de indefensión.

Bibliografía

Acurio, S. (2016). *Delitos informáticos: generalidades.* Recuperado el 3 de abril de 2021, de Organización de Estados Americanos : https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Águila, F. (2019). *Delitos sexuales informáticos.* Recuperado el 4 de abril de 2021, de Universidad Siglo 21: https://repositorio.uesiglo21.edu.ar/handle/ues21/16689

Aguirre, V. (2010). *El derecho a la tutela judicial efectiva: una aproximación a su aplicación por los tribunales ecuatorianos.* Recuperado el 31 de marzo de 2021, de https://revistas.uasb.edu.ec/index.php/foro/article/download/387/382/

Arrázola, F. (2014). *El concepto de seguridad jurídica, elementos y amenazas ante la crisis de la ley como fuente del derecho.* Recuperado el 31 de marzo de 2021, de https://dialnet.unirioja.es/servlet/articulo?codigo=4760108

Artavia , S., & Picado , C. (noviembre de 2018). *La Prueba en General.* Recuperado el 2 de abril de 2021, de Punto Jurídico: https://www.masterlex.com/descargas/PuntoJuridico/2018/Noviembre/Capitulo_19_La_prueba_genereal.pdf

Borges, R. (enero de 2018). *La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea.* Recuperado el 30 de marzo de 2021, de http://www.scielo.org.bo/pdf/rbd/n25/n25_a18.pdf

Cevallos , G., & Alvarado , Z. (2018). *Tutela judicial efectiva y la relación con el principio de inmediación.* Recuperado el 31 de marzo de 2021, de http://rus.ucf.edu.cu/index.php/rus

Chiluiza, E. (16 de septiembre de 2017). *El correo electrónico como prueba digital*. Recuperado el 4 de abril de 2021, de El Universo: https://www.eluniverso.com/opinion/2017/09/16/nota/6382855/correo-electronico-como-prueba-judicial/

Chumi, A. (2017). *El deber judicial de admisión de los medios probatorios y la vulneración al derecho a la prueba en relación con el derecho a la defensa .* Recuperado el 4 de abril de 2021, de Universidad Andina Simón Bolívar : https://repositorio.uasb.edu.ec/bitstream/10644/5633/1/T2285-MDP-Chumi-El%20deber.pdf

Coello, A. (2015). *Los principios de legalidad y principio de proporcionalidad en el derecho penal.* Recuperado el 4 de abril de 2021, de Universidad Regional Autónoma de los Andes : https://dspace.uniandes.edu.ec/handle/123456789/1546

Consejo de Europa. (23 de noviembre de 2001). *Convenio sobre la ciberdelincuencia.* Recuperado el 2 de abril de 2021, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Dunn, M. (12 de marzo de 2019). *Valor probatorio de la prueba documental de contenidos digitales durante la etapa de juicio en el Derecho Procesal Penal Ecuatoriano.* Recuperado el 29 de marzo de 2021, de Universidad Católica Santiago de Guayaquil: http://repositorio.ucsg.edu.ec/handle/3317/13130

Ecuador, Asamblea Constituyente. (20 de octubre de 2008). *Constitución de la República del Ecuador.* Recuperado el 5 de abril de 2021, de Registro Oficial No. 449: https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Ecuador, Asamblea Nacional. (27 de julio de 2009). *Ley Orgánica de la Función Legislativa.* Recuperado el 9 de abril de 2021, de Registro Oficial Suplemento No. 642: https://www.oas.org/juridico/PDFs/mesicic4_ecu_org5.pdf

Ecuador, Asamblea Nacional. (10 de febrero de 2014). *Código Orgánico Integral Penal.* Recuperado el 4 de abril de 2021, de Registo Oficial Suplemento No. 180: https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Ecuador, Corte Constitucional. (11 de mayo de 2010). *Sentencia No. 021 10 SEP CC.* Recuperado el 6 de abril de 2021, de https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=021-10-SEP-CC

Ecuador, Fiscalía General del Estado. (2012). *Perito informático rindió versión en caso juez Paredes*. Recuperado el 3 de abril de 2021, de https://www.fiscalia.gob.ec/perito-informatico-rindio-version-en-caso-juez-paredes/

Fernández, R. (2017). *La nulidad de la prueba: la teoría de los frutos del árbol envenenado.* Recuperado el 1 de abril de 2021, de Universidad Pontificia Comillas : http://hdl.handle.net/11531/12260

Gallegos, R. (2019). El principio de inmediación y la actividad probatoria en la normativa procesal ecuatoriana. *Innova, 4*(2), 120-131. Recuperado el 4 de abril de 2021, de https://repositorio.uide.edu.ec/bitstream/37000/3802/3/document%20%289%29.pdf

García-Escudero, P. (2010). *Técnica legislativa y seguridad jurídica: ¿hacia el control constitucional de la calidad de las leyes?* Pamplona: Aranzadi Thomson Reuters.

Hidalgo, J. (22 de febrero de 2018). *Los delitos informáticos y su afectación sobre los bienes jurídicos.* Recuperado el 29 de marzo de 2021, de Universidad Católica Santiago de Guayaquil: http://repositorio.ucsg.edu.ec/handle/3317/10643

Lacalle, A. (2018). El impacto de las redes sociales y de la mensajería instantánea en la fase probatoria laboral. *IUS Labor*(1), 232-252. Recuperado el 5 de abril de 2021, de https://dialnet.unirioja.es/servlet/articulo?codigo=6443221

Martínez García, H., Moo Medina, M., & Chuc Us, L. (2016). Origen y evolución del cryptovirus Ransomware. *Revista del Centro de Graduados e Investigación del Instituto Tecnológico de Mérida, 31*(62), 38-43. Recuperado el 4 de abril de 2021, de https://www.researchgate.net/publication/312490181_ORIGEN_Y_EVOLUCION_DEL_CRYPTOVIRUS_RANSOMWARE

Mata y Martín, R. (2003). *Delincuencia informática y Derecho Penal.* Managua: Hispamer.

Maya, E. (2014). *Métodos y técnicas de investigación.* México , México: Universidad Nacional Autónoma de México. Recuperado el 5 de Abril de 2021, de

http://www.librosoa.unam.mx/bitstream/handle/123456789/2418/metodos_y_tecnicas.pdf?sequence=3&isAllowed=y

Mora, E., Araujo, A., Bravo, V., Sumoza, R., Contreras , J., & Quintero , D. (2014). *Seguridad Informática y la identidad digital. Fundamentos y aportes.* Mérida, Venezuela: Cenditel. Recuperado el 29 de Marzo de 2021, de https://www.cenditel.gob.ve/portal/wp-content/uploads/biblioteca/2014/siidfa/siidfa.pdf

Morán, G., & Alvarado, D. (2010). *Métodos de investigación.* México: Pearson Educación. Recuperado el 5 de Abril de 2021, de https://mitrabajodegrado.files.wordpress.com/2014/11/moran-y-alvarado-metodos-de-investigacion-1ra.pdf

Morillo, M., & Herrero, A. (septiembre de 2011). *La prueba ilícita y la cadena de custodia en el Ordenamiento Jurídico Costarricense. Alcoholemias y pruebas con alcoholímetro.* Recuperado el 29 de marzo de 2021, de Universidad de Costa Rica: http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/La-prueba-ilicita-y-la-cadena-de-custodia-en-el-Ordenamiento-Juridico.pdf

Nuñez, J. (2017). Los métodos mixtos en la investigación en Educación: Hacia un uso reflexivo. *Cadernos de Pesquisa, 47*(164), 632-649. Recuperado el 5 de abril de 2021, de https://www.scielo.br/pdf/cp/v47n164/1980-5314-cp-47-164-00632.pdf

Organización de las Naciones Unidas. (22 de enero de 2001). *Lucha contra la utilización de la tecnología de la información con fines delictivos.* Recuperado el 2 de abril de 2021, de https://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf

Ortiz, N. (2019). *Normativa legal sobre delitos informáticos en Ecuador.* Recuperado el 1 de abril de 2021, de https://revistas.pucese.edu.ec/hallazgos21/article/view/336/234

Pardo, V. (2006). La valoración de la prueba penal. *Revista Boliviana de Derecho*(2), 75-86. Recuperado el 31 de marzo de 2021, de https://www.redalyc.org/pdf/4275/427539902005.pdf

Peralta, F. (2017). La Discrecionalidad Judicial y la Sanción. *Revista Jurídica Derecho, 5*(6), 23-29. Recuperado el 6 de abril de 2021, de http://www.scielo.org.bo/scielo.php?script=sci_abstract&pid=S2413-28102017000100003&lng=es&nrm=iso

Pérez, A. (2000). *La seguridad jurídica: una garantía del derecho y la justicia.* Recuperado el 31 de marzo de 2021, de https://core.ac.uk/download/pdf/61482516.pdf

Pérez, J. (3 de julio de 2014). *La prueba electrónica: consideraciones.* Recuperado el 30 de marzo de 2021, de Universitat Oberta de Catalunya: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf

Plascencia, R. (1995). Los medios de prueba en materia penal. *Boletín mexicano de derecho comparado*(83), 711-743. Recuperado el 30 de marzo de 2021, de https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3361/3890

Posada, R. (2017). *El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual.* Recuperado el 29 de marzo de 2021, de https://dialnet.unirioja.es/descarga/articulo/6074006.pdf

Primicias. (19 de septiembre de 2019). *Los cuatro delitos informáticos más recurrentes en Ecuador.* Recuperado el 8 de abril de 2021, de https://www.primicias.ec/noticias/tecnologia/estos-delitos-informaticos-mas-recurrentes-ecuador/#:~:text=Los%20cuatro%20delitos%20inform%C3%A1ticos%20con,art%C3%ADculo%20230)%20y%20la%20revelaci%C3%B3n

Quintero, S. (2013). *Prueba en el proceso penal ecuatoriano.* Recuperado el 1 de abril de 2021, de Universidad del Azuay : http://dspace.uazuay.edu.ec/handle/datos/2510

Rodríguez, M. (2018). *La prueba digital en el proceso penal.* Recuperado el 29 de marzo de 2021, de Universidad de la Laguna: https://riull.ull.es/xmlui/bitstream/handle/915/7290/LA%20PRUEBA%20DIGITAL%20EN%20EL%20PROCESO%20PENAL.pdf?sequence=1

Salcedo, O., Fernández, C., & Castellanos, L. (2012). Hackers en la sociedad de la información. Análisis de su dinámica desde una perspectiva social. *Visión electrónica, 6*(1), 115-125. Recuperado el 4 de abril de 2021, de https://dialnet.unirioja.es/descarga/articulo/4234868.pdf

Sandoval, L., & Vaca, A. (2013). *Implantación de técnicas y administración de laboratorio para investigación de ethical hacking.* Recuperado el 4 de abril de 2021, de Escuela Politécnica del Ejercito: http://repositorio.espe.edu.ec/handle/21000/6483

Solís, G. (2015). *La adecuada motivación como garantía en el debido Proceso de Decretos, Autos y Sentencias.* Recuperado el 4 de abril de 2021, de Universidad Central del Ecuador : http://www.dspace.uce.edu.ec/handle/25000/6204

Taruffo, M. (2008). *La prueba, artículos y conferencias.* Santiago de Chile: Metropolitana. Recuperado el 29 de Marzo de 2021, de https://letrujil.files.wordpress.com/2012/01/la-prueba-michele-taruffo.pdf

Tercero, J. (2017). *El prinicipio de contradicción y el dereho a la defensa consagrada en la Constitución de la República del Ecuador en contraposición a la prueba no solicitada oportunamente.* Recuperado el 4 de abril de 2021, de Universidad Regional Autónoma de los Andes : https://dspace.uniandes.edu.ec/handle/123456789/7288

Ugartemendía, J. (2006). El concepto y alcance de la seguridad jurídica en el Derecho constitucional español y en el Derecho comunitario europeo: un estudio comparado. *Cuadernos de Derecho Público*(28), 17-54. Recuperado el 31 de marzo de 2021, de https://core.ac.uk/download/pdf/61482516.pdf

Vargas, E. (2017). *Los criterios de valoración de la cadena de custodia en el Procedimiento Penal Ecuatoriano.* Recuperado el 29 de marzo de 2021, de Pontificia Universidad Católica del Ecuador: https://repositorio.pucesa.edu.ec/handle/123456789/1859

Zambrano, J., Dueñas, K., & Macías, L. (2016). Delito informático: Procedimiento penal en Ecuador. *Dominio de las Ciencias, 2*(2), 204-215. Recuperado el 31 de marzo de 2021, de https://dominiodelasciencias.com/ojs/index.php/es/article/viewFile/159/pdf

Zikmund , W., & Babin , B. (2009). *Investigación de mercados.* México: Cengage Learning.

Zumba, C. (2015). *Delitos contra la seguridad de los activos de los sistemas de información y comunicación: delitos a través de las redes sociales.* Recuperado el 29 de marzo de 2021, de Universidad de Cuenca: http://dspace.ucuenca.edu.ec/handle/123456789/21976

ANEXOS

Modelo de Encuesta aplicada a una muestra de Abogados especialistas en delitos informáticos

1.- ¿Ha detectado deficiencias en los criterios de valoración para la prueba digital no sometida a la cadena de custodia, conforme al artículo 457 del COIP?

Sí ____ No ____

2.- ¿Cuáles?

a) No concordancia con el artículo 500 del COIP _____

b) Incongruencia con el criterio de autenticidad _____

c) Imposibilidad de la pericia en el origen de la prueba _____

d) Inexactitud en la definición de los criterios _____

3.- ¿Considera necesaria una mejor regulación legal para la valoración de la prueba digital por parte del juzgador en los procedimientos de delitos informáticos?

Sí ____ No ____

4.- ¿Cuáles contenidos mínimos debe incluir la Ley para ofrecer seguridad jurídica frente a la valoración judicial de la prueba digital?

a) Definición y delimitación de cada criterio de validación _____

b) Valoración de la prueba digital no sometida a cadena de custodia ____

c) Establecer otras formas de garantía de autenticidad ____

d) Considerar las particularidades de la prueba de contenido digital _____

Modelo de Consentimiento Informado

Universidad Metropolitana de Ecuador

Consentimiento informado

Acuerdo de confidencialidad

Declaro que la información contenida en el Trabajo de Titulación denominado "**VALORACIÓN DE LA PRUEBA DIGITAL EN LOS DELITOS INFORMÁTICOS**" que realizo para optar al título de Abogada de los Tribunales de Justicia del Ecuador, la mantendré como Información Confidencial, y me comprometo a no revelar, directa o indirectamente, ni a utilizar en beneficio propio o de terceros esta información bajo forma alguna. La presente obligación es exigible inclusive en el evento de haber concluido mi contrato de trabajo por cualquier causa o motivo.

Para los efectos de este acuerdo, se entiende por "Información Confidencial", todos los antecedentes, conocimientos y/o datos, escritos o verbales, contenidos en documentos, informes, bases de datos, registros, soportes informáticos, telemáticos u otros materiales, y en general, todo soporte y/o vehículo apto para la incorporación, almacenamiento, tratamiento, transmisión y/o comunicación de datos de manera gráfica, sonora, visual, audiovisual, escrita o de cualquier tipo, a los cuales he tenido acceso, directa o indirectamente, por cualquier medio en virtud de mi interacción con el encuestado.

Cualquier información considerada Información Confidencial dejará de ser Información Confidencial al momento en que se divulgue en literatura publicada o esté disponible de otra manera para la industria o el público.

NOMBRE, FIRMA del Encuestador

Quito, xxxxxxxx 2021