.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD

CARRERA DE DERECHO

ANTEPROYECTO DE TRABAJO DE TITULACIÓN

TEMA

LA EFICACIA O INEFICACIA DE LA EVIDENCIA DIGITAL COMO ELEMENTO PROBATORIO EN EL JUZGAMIENTO DE LOS DELITOS INFORMÁTICO

AUTORA:

VERA DEL PEZO GERAMY ELIZABETH

LA LIBERTAD – ECUADOR

2023

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD

CARRERA DE DERECHO

PROYECTO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA DEL ECUADOR

TITULO:

LA EFICACIA O INEFICACIA DE LA EVIDENCIA DIGITAL COMO ELEMENTO PROBATORIO EN EL JUZGAMIENTO DE LOS DELITOS INFORMÁTICOS

AUTORIA:

VERA DEL PEZO GERAMY ELIZABETH

TUTOR

ABG. CRISTÓBAL MACHUCA REYES MSc.

LA LIBERTAD – ECUADOR

LA LIBERTAD, **23 DE FEBRERO DEL 2021**

DECLARACIÓN DE AUTORIA

Yo Geramy Elizabeth Vera Del Pezo estudiante del séptimo semestre de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura Unidad de Integración Curricular, declaro la autoría de la presente propuesta de investigación, de título LA EFICACIA O INEFICACIA DE LA EVIDENCIA DIGITAL COMO ELEMENTO PROBATORIO EN EL JUZGAMIENTO DE LOS DELITOS INFORMÁTICOS, AÑO 2022 desarrollada en todas sus partes por la suscritas estudiante con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE.

Atentamente

Geramy Vera Del Pezo

C.C 0923563779

Celular: 0990644132

e-mail: verageramy@gmail.com

La Libertad, septiembre del 2023

APROBACION DEL TUTOR

En mi calidad de Tutor del Proyecto de Investigación: ¨ LA EFICACIA O INEFICACIA DE LA EVIDENCIA DIGITAL COMO ELEMENTO PROBATORIO EN EL JUZGAMIENTO DE LOS DELITOS INFORMÁTICOS, PERIODO 2022 – 2023. Elaborado por VERA DEL PEZO GERAMY ELIZABETH, estudiante de la CARRERA DE DERECHO, FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD perteneciente a la UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, previo a la obtención del Título de ABOGADA, me permito declarar que luego de haber orientado, estudiado y revisado, lo APRUEBO en todas sus partes.

Atentamente.

Dr. Cristóbal Machuca Reyes
TUTOR

APROBACIÓN DEL TRIBUNAL

Ab. Víctor Coronel Ortiz, Mgt.
DIRECTOR DE LA CARRERA
DE DERECHO

Ab. Esther Silvestre Ponce, Mgt.
DOCENTE ESPECIALISTA

Dr. Cristóbal Machuca Reyes, Mgt.
DOCENTE TUTOR

Ab. Brenda Reyes Tomalá, Mgt.
DOCENTE UIC

DEDICATORIA

Dedicado a mi familia que han sido la principal fuente de inspiración en este camino de aprendizaje, en la que he logrado cumplir esta meta y que espero ser también para ellos especialmente para mis hijos, un ejemplo que los motive a conseguir lo que sueñan ser como profesionales.

Geramy Elizabeth Vera Del Pezo

AGRADECIMIENTO

A la comunidad Universitaria UPSE por brindarme la oportunidad de realizar mis estudios y contribuir al desarrollo de mi formación académica y profesional. De manera especial a mis profesores y tutores, quienes me han guiado y orientado con su sabiduría y conocimientos expertos. Agradezco sinceramente sus enseñanzas y la dedicación con la que me han acompañado en este proceso de investigación.

Geramy Elizabeth Vera Del Pezo

ÍNDICE GENERAL

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD

CARRERA DE DERECHO

"LA EFICACIA O INEFICACIA DE LA EVIDENCIA DIGITAL COMO ELEMENTO PROBATORIO EN EL JUZGAMIENTO DE LOS DELITOS INFORMÁTICO"

Autora: Geramy Elizabeth Vera Del Pezo

Tutor: Ab. Cristóbal Machuca

RESUMEN

El presente trabajo de investigación gira en torno a la evidencia digital que es la información utilizada en investigaciones y procesos legales para los casos de delitos informáticos ha sido sometido al análisis documental misma que permitió comprender los principios de donde parte el conocimiento de la evidencia digital en la investigación necesaria y útil para la prueba y de esta manera conocer y comprender cuál será aceptado o no en las cortes. En el tratamiento de la información se consideró el uso de técnicas de instrumentalización como la entrevista, lo que evaluar las respuestas de la muestra probabilística por conveniencia que afirma la idea a defender en la que denota la falta de expertos en la pericia (perito informático) lo que vuelve ineficaz el tratamiento de la evidencia y por ende la determinación de la prueba por ello cuando se denuncia este tipo de acciones antijurídicas, muchos entes del sistema penal no cuenta con el personal capacitado para las investigaciones necesarias, como es el caso de la provincia de Santa Elena, en la no existe una unidad de investigación especializada que se dedique específicamente al estudio de los elementos probatorios derivados de la evidencia digital obtenida por medios informáticos, electrónicos y telemáticos, para que dado el caso sea la información validada como medio de prueba pertinente dentro de los procesos judiciales y en su determinación sancionar a los responsables.

Palabras clave: Delito informático, evidencia digital, perito informático, procesos judiciales

ABSTRACT

Digital evidence is any digital information used in investigations and legal proceedings. It can be a crucial source of evidence in legal cases, but it also presents unique challenges in terms of authentication and data protection. Digital forensic experts play a fundamental role in the recovery and analysis of evidence for its presentation in the legal system. Therefore, it is important to understand the principles underlying the knowledge of digital evidence in the necessary and useful investigation for the trial, and thus understand what will be accepted or not in courts.

The lack of experts in digital forensics makes the treatment of evidence ineffective and consequently impacts the determination of the proof. This is particularly evident when reporting such crimes, as many entities within the penal system lack the appropriate personnel for necessary investigations. For instance, in the province of Santa Elena, there is no specialized investigative unit dedicated specifically to the study of evidence derived from computer, electronic, and telematic means. As a result, when obtaining information, it becomes essential to comply with the corresponding chain of custody, ensuring that it is admitted as relevant evidence in judicial processes and leading to the prosecution of those responsible.

INTRODUCCION

Los delitos que se configuran para causar daño a una persona aumentan cada vez y ahora mucho más de manera “tecnológica”, por ejemplos estafas, acosos, fraudes, falsificación de identidad, y muchos más y todo esto puede darse por parte de personas maliciosas que hacen uso de dispositivos y plataformas tecnológicas como celulares, computadoras, cajeros automáticos, redes sociales y todo lo que gira en el entorno del acceso al internet.

Hoy en día la práctica y desarrollo de varias actividades tecnológicas como fuentes de información e interacción, con diferentes grupos sociales, que si bien es cierto están al alcance de todos los seres humanos a nivel mundial, por ser justamente un tema global, son importantes y necesarios para la comunicación, pero también representan una puerta abierta a la inseguridad de los individuos en general y sobre todo el grupo más vulnerable son los menores de edad y permiten crear escenarios de exposición frente a muchos delitos y generando el daño de un bien jurídico tutelado por el Estado, de los que se puede mencionar la honra y la integridad.

En el Ecuador los delitos informáticos se encuentran tipificados en el Código Orgánico Integral Penal, en donde se distingue cuáles son los tipos y sus respectivas sanciones a estas conductas ilícitas, muchos de los casos denunciados han llegado a sentencia, pero en otros casos no pasa de una simple indagación previa y que por falta de evidencia que determina la prueba se solicita el archivo de las causas, los motivos son varios, depende de algunos factores, entre ellos que no se puede determinar la responsabilidad del infractor, no existe una prueba digital contundente que demuestre la responsabilidad de un determinado sujeto, en otros casos existen evidencias digitales que no fueron recolectadas de la forma debida y las mismas no son válidas dentro del proceso porque al momento de extraerlas la prueba pudo haber sido manipulada, es decir que es frágil y volátil dejando en la impunidad este tipo de delitos informáticos.

Hemos escuchados en medios de comunicación una realidad que se suman cada día muchos casos y que por tales motivos ya ni se denuncian porque se cree no tener la atención merecida, la solución esperada, o la respuesta necesaria de la "justicia" para estos casos.

El interés por este tema se fundamenta en la percepción de estos síntomas que conllevan a la investigación del presente proyecto, lo que permitirá analizarlos para llegar a determinar las razones derivadas de la función judicial y como sus procedimientos son ineficientes además de considerar los argumentos que correspondan para establecer una hipótesis jurídica y aportar con recomendaciones en los casos de personas que se han visto afectadas por estos delitos, así como también evidenciar la falta de especialistas de la pericia informática lo que afecta a la avance de los procesos judiciales y a través de esto ejercer la tutela efectiva a las víctimas de delitos informáticos.

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad la digitalización y el mundo de la tecnología han generado gran impacto y es que desde sus ventajas como la de facilitar la comunicación, relacionarse interculturalmente, esto ha elevado la necesidad de utilizar continuamente los medios tecnológicos lo que ha desplegado un sin número de posibilidades de ejercer o dominar plataformas o dispositivos funcionales para lograr fines de lucro como por ejemplo las ventas en línea, formación educativa, uso de redes sociales entre otras que han logrado acaparar cada vez un gran porcentaje de audiencia indeclinable siendo cada vez más las personas que tienen accesos a estas plataformas poco fiables refiriéndonos a que son manipulables respecto a los datos tanto para acceder a ellos como ya estando suscrito en los mismos; a pesar de que las mismas soliciten permisos por ejemplo la mayoría de edad como uno de los requisitos para sus acceso esta condición no se cumple siendo esta una de las primeras causas en que deriva muchas veces la afectación de la información y posterior la invalidez de la prueba que en su gran mayoría concluyen en el estancamiento de los procesos para el juzgamiento de éstos delitos y que la norma penal prescribe para ser determinados dentro de la ley con sus respectivas sanciones.

Actualmente no existe un consenso a nivel mundial acerca de la conceptualización de un delito informático, pero Hernández Díaz en su libro el "Delito informático", refiere varias definiciones de autores de las que tomaremos en cuenta las siguientes:

> *"Una de las primeras conceptualizaciones fue la aportada por PARKER que definió a los abusos informáticos como "cualquier incidente asociado con la tecnología de los ordenadores, en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio"* (Díaz, 2009, pág. 231)

> *"CAMACHO LOSA consideró que, delito informático es "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma*

activa dispositivos habitualmente utilizados en las actividades informáticas" (Díaz, 2009, pág. 231)

De acuerdo a las definiciones citadas podemos concluir que "Los Delitos Informáticos", son todas aquellas acciones dolosas, cometidas a través de medios digitales, con el fin de causar daño a la integridad moral o económica de una persona o entidad jurídica y así obtener un beneficio de carácter económico o social.

La pandemia por covid-19 que azotó al mundo, no fue una excusa para frenar el aumento de este tipo de delitos, si no, por el contrario, fue un detonante para que otros comunes como la suplantación de identidad, extorción, fraudes, estafas masivas, etcétera, implementando como variante principal el uso de redes sociales o plataformas virtuales para su cometimiento, lo que permitió insertar a estos delitos comunes dentro del grupo de delitos informáticos.

Debido al confinamiento obligatorio al que se sometió la población en general, el uso de transacciones por medios electrónicos para adquirir productos de primera necesidad, la aparición de servicios por medio de páginas web con entregas a domicilios y el sin números de tiendas virtuales o simplemente personas que decidieron emprender un negocio utilizando medios digitales para mejorar su economía, fueron las herramientas perfectas para que personas dedicadas a ejecutar delitos utilizando medios o mecanismos electrónicos establecieran nuevas formas de afectar a la sociedad.

La protección de datos e información digital en Ecuador está regulada de manera dispersa e imprecisa, ya que no existe un Código especializado, ni normativa enfocada a la prevención y en caso de cometimientos de delitos de carácter informático, la sanción para enfrentar los desafíos de la implementación y utilización de las tecnologías de la información, como respuesta ante la inminente problemática acerca de este tipo delitos que se ejecutan a través de medios digitales, encontramos al Código Orgánico Integral Penal, en esta normativa en el vigente hallamos varios tipos de delitos comunes prescritos pero que no son explícitos como referencia se plantea en el Código Orgánico Integral Penal:

> *"Art. 178.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años".* (defensa.gob.ec, 2014)

Generalmente este tipo de acciones antijurídicas quedan en la impunidad por la volatilidad de la información, anteriormente se consideraba un delito común, ya que su cometimiento era realizado en ocasiones de forma directa y personal, en la actualidad la globalización del internet y el anonimato que utilizan los actores para su cometimiento, permiten que cualquier persona con la ayuda de una herramienta informática, cometa acciones en contra de la integridad de otra. Pero que al momento de que la agraviada presenta la denuncia con el fin de protegerse ante una amenaza inminente, el sistema de administración de justicia pone en manifiesto la importancia de la prueba para tratar de localizar a los responsables.

En casos se presentan las pruebas digitales para el esclarecimiento del delito, con las que es posible iniciar una indagación previa para establecer responsabilidades y encontrar a los presuntos infractores, pero como se expone anteriormente, la volatilidad de la información no permite localizar de manera inmediata y en muchas ocasiones resulta imposible vincular al proceso a los responsables, dejando en estado de indefensión a las víctimas o pasando los procesos al archivo.

Otro de los muchos ejemplos es la suplantación de identidad por medios digitales, que es la creación de perfiles falsos para extorsionar o emitir injurias a una determinada persona por medio de redes sociales, en este caso el sujeto activo no obtiene un beneficio económico, sino que lo impulsa un beneficio social y como tiene conocimiento de que el medio que emplea como herramienta para sus actividades ilícitas es idóneo para ellos por el hecho de que es difícil localizarlos. En este tipo de casos la mayoría de las personas desconocen que se pueden amparar con la normativa vigente y no realizan las respectivas denuncias, siendo este tal desconocimiento de la norma otro punto en contra para que se siga cometiendo este tipo de acciones inescrupulosas y evitando a que se dé con el paradero de estos delincuentes.

El presente trabajo de investigación está orientado al estudio de La eficacia de la evidencia digital que se obtiene a través de una herramienta o plataforma digital y si la misma cumple con el debido tratamiento y recolección para que sea admitida dentro de los procesos judiciales que se tramitan en la provincia de Santa Elena, determinando si los medios o mecanismos gubernamentales son eficientes a la hora de investigar diferentes tipos penales que se cometen en la actualidad con el uso y abuso del incremento de las tecnologías de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera afecta la valoración de la evidencia digital como elemento de prueba para en el juzgamiento de delitos informáticos, en relación de su admisibilidad?

1.3 OBJETIVOS GENERAL Y ESPECÍFICOS

OBJETIVO GENERAL

Evaluar los tipos de evidencia digital admitidos e inadmitidos en el procedimiento judicial mediante el análisis de las disposiciones que sobre la materia se encuentran estipuladas en el Código Orgánico Integral Penal y el levantamiento de información de la población involucrada en la problemática para la valoración de la eficacia de la evidencia digital como prueba en el juzgamiento de los delitos informáticos.

OBJETIVOS ESPECÍFICOS

- Enfatizar los delitos informáticos establecidos en la norma penal del Ecuador, su tipificación y sistema procesal para el cumplimiento de la capacidad sancionatoria
- Diagnosticar las falencias del sistema de recolección de evidencia digital de los medios electrónicos para su valoración
- Explicar las fases de la obtención de la prueba digital y su tratamiento según la norma en el Ecuador

- Identificar a las personas o grupos vulnerables de personas que se exponen como víctimas de los delitos informáticos

1.4 JUSTIFICACIÓN

Para justificar este proyecto de investigación y bajo la metodología de Carlos Méndez que radica en el interés que lleva a la realización de una investigación de tres maneras de hacerlo que son la teórica, la metodológica y la práctica; que serán las herramientas para el desarrollo de una investigación que el autor escoge de acuerdo a su interés y que para este es partiendo de un marco teórico que explica los diferentes términos de los temas que se investigan como es la eficacia de la evidencia digital y su admisibilidad en el juzgamiento de los delitos informáticos y de los que se analizaran teniendo en cuenta la vigencia de la normativa legal para su estudio, también fuentes de datos de información recopilados para que sea un aporte al conocimiento que complemente a otros estudios que se direccionan en brindar la posibilidad al lector a extender nuevos proyectos de estudio de investigación respecto al tema que amerita.

Por lo tanto, se justifica este estudio para alcanzar los objetivos de la misma; y defender ideas como es la percepción de ciertas debilidades que acarrea el sistema procesal para sancionar delitos que se imponen en el contexto de las tecnologías, y que la norma ha introducido y especificado para reconocerlos como medios probatorios ante hechos que correspondan al caso y que son admitidos por la constitución, instrumentos internacionales, derechos humanos y otras normas jurídicas.

1.5 VARIABLES DE LA INVESTIGACIÓN

VARIABLE DEPENDIENTE

Juzgamiento de los delitos Informáticos

VARIABLE INDEPENDIENTE

La evidencia digital y su admisibilidad.

1.6 IDEA A DEFENDER

En los casos en donde se tiene la evidencia digital como prueba, no son suficientes para el juzgamiento de infracciones o delitos informáticos debido a la falta de especialistas para la práctica pericial sobre estos delitos, lo que concluye en el anquilosamiento del proceso judicial y posterior el archivo de las causas.

CAPITULO II: MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 EVIDENCIA DIGITAL

Para Sánchez Garrido, “Las evidencias digitales son información de valor probatorio en un juicio, que no hay que confundir con la recuperación de datos. La evidencia digital es cualquier información de valor probatorio que se almacena o transmite en forma digital (datos en binario a bajo nivel). Se trata de entender y contestar preguntas referidas a cómo, cuándo y desde dónde se produjo el incidente, así como cuál fue su impacto y a qué afectó.” (Sanchez, 2021)

La evidencia digital se refiere a cualquier tipo de información digital que se utiliza en investigaciones o procesos legales. Esto puede incluir datos electrónicos, documentos, imágenes, videos, registros de actividad en línea, correos electrónicos, mensajes de texto y otros tipos de contenido digital. La evidencia digital se ha vuelto cada vez más importante en los últimos años debido al crecimiento de la tecnología y el aumento de la actividad en línea.

La evidencia digital puede ser utilizada en una amplia gama de casos legales, como delitos informáticos, fraude, espionaje, acoso en línea, casos de propiedad intelectual, disputas laborales, casos de divorcio y muchas otras situaciones legales. La evidencia digital puede proporcionar pruebas críticas en estos casos, ya que puede ser difícil de manipular y puede proporcionar un registro detallado de eventos. Sin embargo, la evidencia digital también plantea desafíos únicos, puede ser fácilmente alterada o eliminada, lo que requiere técnicas y herramientas especiales para preservarla y autenticarla correctamente. Además, la privacidad y la protección de datos también son consideraciones importantes al tratar con evidencia digital, ya que puede contener información sensible.

Los expertos forenses digitales son profesionales capacitados en la recuperación, análisis y presentación de evidencia digital. Utilizan herramientas y técnicas especializadas para extraer y examinar datos digitales de manera forense, asegurándose de que la evidencia se maneje de manera legal y ética.

La evidencia digital es un elemento de un caso que se analiza o se estudia el cual debe ser confiable y determinante para su valoración, como antecedentes sabemos que todo dispositivo digital en la actualidad genera información pudiendo ser esta personal o institucional la misma que sirve como evidencia para investigaciones de casos de cibercrimen o ataques informáticos o cualquier actividad ilícita de la que pueda tener valor probatorio para resolverlos, el problema radica en la obtención de la misma es decir, desde el punto de partida, la recolección, la preservación, su análisis a veces no resultan correctos o viables para ser considerados como tal, para que esto suceda deben utilizarse métodos de aplicación de tratamiento de la evidencia bajo el proceso de la informática forense; en este término se permitirá obtener, analizar, recuperar y presentar información referente que después de su procesamiento se almacenaran en un sistema informático para luego ser usados como evidencia.

2.1.2 PRESERVACIÓN DE LA EVIDENCIA DIGITAL

En cuanto a la preservación de la evidencia es un aspecto particular e importante para los procesos judiciales ya sean estos actuales, o futuros o también como antecedente. Por ejemplo, las instituciones tienen obligación de preservar cualquier información que puede llegar a determinarse como evidencia para algún caso y o proceso judicial, pero ¿qué es la preservación de la información?… para Ferreira es *"la capacidad de asegurar que la información digital se mantiene con las cualidades accesibles y suficientes de autenticidad, que se pueden interpretar en el futuro con uso de una plataforma tecnológica diferente utilizado al momento de su creación"* (Ciencia Digital, 2019)

Es decir, la preservación de la evidencia se debe asegurar al máximo y ante cualquier intento de vulnerabilidad digital para que garantice su autenticidad, sea integra y confiable para su posterior uso como información de valor probatorio legal que se utiliza o puede ser utilizada para un procedimiento de un caso judicial que será admitida o no admitida cumpliendo así relativamente con el paso a paso de sistematización, obtención, investigación pericial, examinación, de coherencia, previa su presentación.

Según Vivian Neptune Rivera Catedrática de la Escuela de Derecho de la Universidad de Puerto Rico; en su artículo publicado "Reglas de admisibilidad de prueba digital" quien en búsqueda de la admisibilidad de la evidencia como un medio probatorio en Latinoamérica se obtiene que solo en países como Estados Unidos se adoptaron reglas para su admisión y valoración como pruebas y estas se consideran Reglas de la evidencia" en Puerto Rico particularmente estas Reglas se aprobaron en 1979 pero se reforman en 2009 y se integran las reglas con tratamiento de la información de la evidencia electrónica y digital y según su análisis en derecho probatorio se encontró que Canadá y Singapur eran los únicos Países que abarcaba un código de derecho probatorio tratante específicamente sobre la evidencia electrónica o digital, este código comprende todo información de cómo se genera, crea, conserva o comparte en dispositivos electrónicos o digitales, también se recomienda el análisis de las maneras de autenticar las páginas de Internet, correos electrónicos, mensajería de audio, de texto, entre otros tipos de evidencia electrónica y digital.

A si también en el Capítulo X sobre contenido de escritos, grabaciones y fotografías, etc. Basado en este código se escoge 3 requisitos básicos de admisibilidad de la prueba evidencia que se cumplen como Reglas de Evidencia; Estos son: La autenticación, la regla de la mejor evidencia, y la prueba de referencia. Sobre la autenticación, toda prueba documentada y de objeto tiene que ser autentificada antes de ser admisible sin embargo no es determinante *"La autenticación es condición necesaria pero no suficiente para la admisibilidad"* (Rivera, PDF, 2021)

Es decir, es un paso previo a ser considerada pertinente según el Juez y en términos de pertinencia se considera el impacto material y la relevancia de los elementos que constituyen al delito, los elementos de causa de la acción, y la credibilidad del o los testigos. En este artículo también se hace mención de que en el Sistema Probatorio de EEUU la cantidad de evidencia para determinar la autenticidad de un documento electrónico digital, foto y video es mínimo y suficiente incluso menor que el estándar de preponderancia de la prueba que es cincuenta más uno.

En ese mismo artículo también se menciona acerca de la regla 902 en la que haciendo uso del parafraseo se enumeran los la autenticación de probatoria del hecho base : *"(a) documentos reconocidos; (b) documentos públicos bajo sello oficial; (c) documentos públicos firmados por funcionarios; (d) documentos públicos extranjeros; (e) copias certificadas de récords y documentos públicos; (f) publicaciones oficiales; (g) periódicos o revistas; (h) etiquetas comerciales; (i) papeles comerciales y documentos relacionados; (j) presunciones según las leyes; (k) récords certificados de actividades que se realizan con regularidad o récords de negocios, y (l) récord electrónico*" (Rivera, 2021) se indica también que no se menciona a los mensajes de texto porque hasta el momento de elaboración del código no se usaban con la dimensión que se usa actualmente

2.1.3 DELITOS INFORMÁTICOS

DEFINICIÓN Y CONCEPTO

Los delitos informáticos, también conocidos como ciberdelitos o delitos cibernéticos, son actividades criminales que se llevan a cabo utilizando tecnología informática o redes de comunicación electrónica. Estos delitos involucran el uso ilegal o malicioso de dispositivos electrónicos y sistemas de información para llevar a cabo actividades ilegales. Los delitos informáticos pueden tener graves consecuencias tanto para individuos como para empresas. Los perpetradores pueden enfrentar sanciones legales, incluyendo multas y penas de prisión. Para combatir estos delitos, muchas jurisdicciones tienen leyes específicas de ciberdelitos y unidades especializadas en delitos informáticos dentro de las fuerzas del orden.

Las leyes sancionatorias para delitos informáticos, también conocidos como ciberdelitos o delitos cibernéticos, varían según el país y la jurisdicción. Sin embargo, en muchos casos, las leyes se han actualizado para abordar los delitos cometidos a través de medios electrónicos o relacionados con tecnologías de la información. A continuación, mencionaré algunos aspectos comunes que suelen abordarse en este tipo de legislación:

1. Acceso no autorizado a sistemas informáticos: Prohibición de acceder, de forma intencionada y sin autorización, a sistemas informáticos, redes, bases de datos o cualquier otro tipo de sistema electrónico protegido.

2. Interceptación ilegal: Penalización de la interceptación no autorizada de comunicaciones electrónicas, como el acceso no autorizado a correos electrónicos, mensajes de texto o comunicaciones telefónicas.

3. Fraude informático: Castigo de actividades fraudulentas que involucran el uso de sistemas informáticos, como estafas en línea, phishing, robo de identidad o manipulación de datos para obtener beneficios ilegales.

4. Daños a sistemas informáticos: Sanción de acciones que causen daños a sistemas informáticos, incluyendo la introducción de virus informáticos, la destrucción de datos, el sabotaje de redes o el bloqueo de servicios en línea.

5. Pornografía infantil en línea: Establecimiento de medidas estrictas para combatir la producción, distribución, posesión o promoción de material pornográfico que involucre a menores de edad.

6. Delitos relacionados con la propiedad intelectual: Prohibición de la infracción de derechos de autor, la piratería informática, la distribución ilegal de software o el robo de información confidencial.

7. Delitos informáticos contra la privacidad: Protección de la privacidad y penalización de la violación de la misma, como el acceso no autorizado a información personal, el espionaje informático o la divulgación ilegal de datos privados.

Es importante tener en cuenta que estas son solo algunas categorías comunes y que las leyes pueden variar en cada país. Además, las sanciones y penas asociadas a los delitos informáticos también pueden diferir según la gravedad de la infracción y las leyes específicas de cada jurisdicción. Es recomendable consultar la legislación vigente en tu país para obtener información más precisa y actualizada sobre las leyes sancionatorias para delitos informáticos.

ANTECEDENTES DEL DELITO INFORMÁTICO EN EL ECUADOR

Los delitos informáticos en el Ecuador, al igual que en otros países, han evolucionado con el rápido desarrollo de la tecnología y el aumento de la conectividad en línea. Aunque los primeros casos de delitos informáticos pueden remontarse a la década de 1990, fue a principios de los años 2000 cuando se comenzaron a tomar medidas más significativas para abordar estos problemas en el país. Algunos antecedentes históricos relevantes incluyen:

Años 1990: Durante esta década, la informática y la tecnología de la información empezaron a adquirir mayor relevancia en la sociedad ecuatoriana, lo que también abrió nuevas oportunidades para cometer delitos informáticos.

Ley de Comercio Electrónico: En el año 2002, Ecuador aprobó la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Esta legislación fue un paso importante para establecer un marco legal que regule las transacciones electrónicas y establezca sanciones para ciertos tipos de delitos informáticos.

Crecimiento del uso de Internet y redes sociales: Con el aumento del acceso a Internet y el uso generalizado de las redes sociales, surgieron nuevos delitos relacionados con la suplantación de identidad, el acoso en línea y la difusión de contenido ilegal.

Respuesta legislativa: El gobierno ecuatoriano ha ido adaptando su legislación para abordar los delitos informáticos y la ciberseguridad. En 2014, se promulgó el Código Orgánico Integral Penal (COIP), que incluye disposiciones para sancionar delitos informáticos y cibernéticos específicos.

Cooperación internacional: Ecuador ha buscado colaborar con otros países y organizaciones internacionales para enfrentar los desafíos de la ciberdelincuencia a nivel global.

Es importante tener en cuenta que la evolución tecnológica y la naturaleza de los delitos informáticos hacen que esta sea una problemática en constante cambio, y es probable que hayan ocurrido eventos adicionales después de mi fecha límite de

conocimiento. Si deseas información más actualizada sobre los antecedentes históricos del delito informático en el Ecuador, te sugiero consultar fuentes más recientes y autorizadas.

En Ecuador se contemplan disposiciones específicas relacionadas con los delitos informáticos establecidas en el Código Orgánico Integral Penal (COIP). Estos delitos se refieren a actividades ilícitas que se cometen a través de medios electrónicos o informáticos, como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de comunicaciones, el fraude informático, entre otros.

Los delitos informáticos contemplados en el COIP ecuatoriano: Acceso ilegítimo a un sistema informático, Interceptación ilegal de comunicaciones, pornografía infantil, estafas y fraudes informáticos, sabotaje informático; Estos son solo algunos ejemplos de los delitos informáticos contemplados en el COIP ecuatoriano. Es importante tener en cuenta que las leyes y regulaciones pueden cambiar con el tiempo, por lo que siempre es recomendable consultar la legislación de actualidad.

PERSONAS VULNERABLES DE LOS DELITOS INFORMÁTICOS

Las personas más vulnerables a los delitos informáticos varían dependiendo de diversos factores, pero generalmente incluyen a aquellos que pueden tener menos conocimiento y experiencia en tecnología, así como menos recursos para protegerse adecuadamente. Algunos grupos que suelen ser más vulnerables a los delitos informáticos son:

Personas mayores: Los adultos mayores a menudo tienen menos experiencia con la tecnología y pueden ser más propensos a caer en estafas en línea o ser víctimas de phishing.

Niños y adolescentes: Los jóvenes, especialmente aquellos que son muy activos en línea y en redes sociales, pueden ser víctimas de acoso cibernético, grooming o abuso en línea.

Personas con poca experiencia tecnológica: Aquellos que no están familiarizados con el uso seguro de computadoras e Internet pueden ser presa fácil para los delincuentes informáticos.

Personas con discapacidades: Aquellos con discapacidades físicas o cognitivas pueden tener dificultades para protegerse en línea o pueden ser víctimas de estafas dirigidas específicamente a ellos.

Personas con recursos financieros limitados: Los individuos que no pueden permitirse implementar medidas de seguridad avanzadas pueden ser más vulnerables a ataques cibernéticos.

Empleados de empresas poco capacitados: Los empleados sin una formación adecuada en seguridad informática pueden ser la puerta de entrada para ataques dirigidos a las empresas.

Grupos minoritarios y marginados: En algunos casos, los delincuentes informáticos pueden dirigirse a grupos minoritarios y marginados debido a su situación social, política o cultural.

Personas que confían fácilmente: Aquellos que tienden a confiar en exceso o que son demasiado crédulos pueden ser más susceptibles a caer en trampas en línea.

Es esencial que todos, independientemente de su perfil, estén informados y tomen medidas para protegerse contra los delitos informáticos, como mantener sus dispositivos actualizados, utilizar contraseñas seguras, evitar hacer clic en enlaces sospechosos o proporcionar información personal sensible a desconocidos. La educación y la conciencia sobre la seguridad en línea son cruciales para protegerse contra las amenazas cibernéticas.

LA OEA Y LA ONU FRENTE A LOS DELITOS CIBERNÉTICOS

La Organización de los Estados Americanos (OEA) ha mostrado una preocupación creciente por los delitos cibernéticos y ha adoptado diversas posturas y acciones para abordar esta problemática en la región de las Américas reconociendo que los delitos cibernéticos representan una amenaza significativa para la seguridad y el desarrollo de los países de la región. Por lo tanto, ha tomado iniciativas para promover la

cooperación y el fortalecimiento de las capacidades nacionales para enfrentar este tipo de delitos. Algunas de las posturas y acciones de la OEA frente a los delitos cibernéticos incluyen:

La Convención Interamericana contra el Cibercrimen. En el año 2001, la OEA sostiene esta convención, conocida también como la Convención de Budapest, que es un instrumento jurídico que busca establecer medidas para prevenir y combatir los delitos cibernéticos en la región.

Programas de capacitación y cooperación técnica. La OEA ha desarrollado programas de capacitación y cooperación técnica para los Estados miembros con el objetivo de fortalecer sus capacidades para abordar los delitos cibernéticos. Estos programas incluyen entrenamiento para el personal encargado de hacer cumplir la ley y la promoción de mejores prácticas en seguridad cibernética.

Fomento de políticas de seguridad cibernética. La OEA ha alentado a los países miembros a establecer políticas y marcos legales sólidos en materia de seguridad cibernética, así como a promover la conciencia pública sobre la importancia de protegerse contra los delitos cibernéticos.

Colaboración con otras organizaciones y actores internacionales. La OEA ha trabajado en conjunto con otras organizaciones internacionales, como la Unión Internacional de Telecomunicaciones (UIT) y la INTERPOL, para coordinar esfuerzos y mejorar la lucha contra los delitos cibernéticos a nivel global.

Es importante mencionar que, debido a la naturaleza en constante evolución de los delitos cibernéticos, la OEA ha tenido que adaptarse continuamente para hacer frente a nuevas amenazas y desafíos en el ámbito digital de la nueva era.

Por otra parte, Organización de las Naciones Unidas (ONU) ha expresado su preocupación y ha reconocido la ciberdelincuencia como un desafío global que requiere una respuesta coordinada y cooperativa por parte de los Estados miembros y la comunidad internacional. La ONU ha adoptado una serie de enfoques y acciones para abordar la ciberdelincuencia y promover un ciberespacio seguro. A continuación, se mencionan algunas de las formas en las que la ONU enfrenta la ciberdelincuencia:

Resoluciones y declaraciones: La Asamblea General de la ONU y otras agencias especializadas que dentro de la organización han emitido resoluciones y declaraciones que reconocen la importancia de abordar la ciberdelincuencia y el ciberespacio seguro. Estos documentos alientan a los Estados miembros a fortalecer la cooperación internacional y adoptar medidas para prevenir y combatir los delitos informáticos.

Convenciones y tratados internacionales: La ONU ha respaldado la Convención de Budapest sobre Ciberdelincuencia, que es el único tratado internacional vinculante específicamente enfocado en la ciberdelincuencia. Esta convención tiene como objetivo establecer un marco legal común y promover la cooperación entre los países en la lucha contra la ciberdelincuencia.

Programas de asistencia técnica: La ONU, a través de sus diversas agencias y programas, ofrece asistencia técnica y capacitación a los Estados miembros para fortalecer sus capacidades en la prevención, investigación y respuesta a la ciberdelincuencia.

Grupos de trabajo y foros: La ONU facilita grupos de trabajo y foros para que los Estados miembros puedan intercambiar conocimientos y mejores prácticas en el ámbito de la ciberseguridad y la lucha contra la ciberdelincuencia.

Promoción de normas y principios: La ONU aboga por la promoción de normas y principios de comportamiento responsable en el ciberespacio, incluyendo la protección de los derechos humanos en línea, la privacidad y la seguridad de la información.

Sensibilización y educación: La ONU promueve la sensibilización y la educación sobre la ciberdelincuencia y la seguridad cibernética, tanto entre los Estados miembros como entre el público en general.

Es importante destacar que la ciberdelincuencia es un desafío en constante evolución y que la ONU sigue trabajando en colaboración con otros organismos internacionales, organizaciones no gubernamentales y actores relevantes para fortalecer la seguridad cibernética y proteger el ciberespacio.

Además, la ONU insta a los Estados miembros a adoptar un enfoque integral y multidisciplinario para abordar los delitos cibernéticos, fomentando la cooperación internacional para enfrentar este problema global.

EL TRATADO DE BUDAPEST SOBRE EL CIBERCRIMEN

También conocido como el Convenio sobre Ciberdelincuencia, es un tratado internacional diseñado para abordar y combatir el cibercrimen y otros delitos relacionados con la tecnología de la información y las comunicaciones. Aquí hay información importante sobre el Tratado de Budapest:

El tratado fue adoptado el 23 de noviembre de 2001 en Budapest, Hungría, bajo los auspicios del Consejo de Europa. Entró en vigor el 1 de julio de 2004.

Objetivo Principal: El principal objetivo del tratado es proporcionar un marco legal internacional para la cooperación entre los países en la lucha contra el cibercrimen. Busca establecer normas comunes y herramientas de investigación para combatir delitos informáticos y proteger la seguridad de la información en el contexto de una creciente digitalización.

Ámbito de Aplicación: El tratado abarca una amplia gama de delitos informáticos, que incluyen la interferencia ilegal en sistemas informáticos, el acceso no autorizado a datos, el fraude informático, la pornografía infantil en línea y otros delitos relacionados con tecnología.

Contenido Clave: El tratado establece una serie de disposiciones y principios para la cooperación internacional en la investigación y persecución de delitos cibernéticos. Incluye medidas relacionadas con la legislación nacional, la protección de datos, la obtención de pruebas electrónicas, la cooperación transfronteriza y la formación de las fuerzas del orden.

Cooperación Internacional: El tratado promueve la cooperación entre los países en la investigación y persecución de delitos cibernéticos. Los países firmantes se comprometen a establecer procedimientos y canales para la asistencia mutua en la

obtención de pruebas, la identificación de infractores y otros aspectos relacionados con la cooperación internacional.

Convención abierta: Además de los estados miembros del Consejo de Europa, el tratado también está abierto a la adhesión de otros estados y organizaciones internacionales. Esto ha llevado a una amplia participación y adhesión en todo el mundo.

Comité de Vigilancia: Se estableció un Comité de Vigilancia del Tratado de Budapest, encargado de supervisar su implementación y promover la cooperación entre los estados partes.

Importancia Global: El Tratado de Budapest es uno de los instrumentos legales más importantes en la lucha contra el cibercrimen a nivel internacional. Ha sido adoptado por numerosos países y ha contribuido a la armonización de las leyes y los enfoques en la investigación y persecución de delitos cibernéticos.

En resumen, el Tratado de Budapest es un acuerdo internacional crucial que busca abordar el cibercrimen mediante la promoción de la cooperación internacional, la armonización legal y la adopción de medidas para combatir eficazmente los delitos cibernéticos en una era digital en constante evolución.

2.1.4 DELITOS QUE SE COMETEN EN MEDIOS INFORMÁTICOS, TELEMÁTICOS, ELECTRÓNICOS Y RED SOCIAL

PORNOGRAFÍA INFANTIL

Incluye la producción, distribución, almacenamiento o posesión de material pornográfico que involucre a niños, niñas o adolescentes. La pornografía infantil se describe como una representación visual en donde un menor de edad conserva una conducta sexualmente explícita, también a una persona real que participa en actos

sexuales explícitos, aparentando ser menor de edad y/o imágenes realistas de un menor inexistente que mantiene una conducta sexualmente explícita.

Ésta es una problemática que ha evolucionado a través del tiempo, caracterizada por la vulnerabilidad de los derechos de niños, niñas y adolescente alrededor del mundo, dejando como consecuencia daños físicos y psicológicos en sus víctimas, además afectando hogares de diversas formas y en muchos casos quedando en la impunidad.

La Pornografía Infantil es un delito tipificado en el código Orgánico Integral Penal en la que establece una sanción de pena privativa de libertad de entre trece a dieciséis años, y se forma de acción es por vías telemáticas haciendo uso de red internet y artefactos tecnológicos como video cámara fotográficas, cámaras pc, cámaras web con esto se produce la explotación sexual comercial, ya que se utilizan fotos o videos con fines lucrativos, vulnerando la integridad física y psicológica de un sin número de víctimas.

Existe un caso en particular que permitió que el Estado implemente una alerta para localizar a niños, niñas o adolescentes desaparecidos; este es el caso de Emilia Benavides, una niña de 9 años quien desapareció el 15 de diciembre de 2017 al salir de su escuela en la ciudad de Loja. Tras una exhaustiva búsqueda, dentro y fuera de la ciudad, justo después de 4 días desde su desaparición, fue hallada desmembrada e incinerada en una quebrada.

Gracias a unas cámaras de seguridad lograron encontrar a su captor, José Nero, quien confesó llevar a Emilia a un lugar con el fin de tomar fotos y videos pornográficos para una red que se dedicaba a la trata de personas y pornografía infantil a nivel mundial, denominada Inocentes 10.

José Nero, Manuel A. y Tania R. fueron detenidos y a las pocas horas, Nero fue encontrado sin vida. Acusados por pornografía infantil, trata de personas y violación, la Fiscalía sentenció a 34 años y 8 meses por el delito de femicidio.

Después de este trágico suceso, el Ministro del Interior de entonces, César Navas, suscribió un convenio con ICMEC, International Center for Missing and Exploited

Children, para activar dicha alerta y en honor a Emilia Benavides obtuvo el nombre de Alerta Emilia en Ecuador.

Con la pandemia de la COVID –19, los niños, niñas y adolescentes no retrasaron su educación y siguieron sus clases de manera virtual, las personas trabajaban para evitar un mayor daño en la economía y el uso del internet se convirtió en la única forma de contacto entre personas. Sin embargo, esto logró que los menores tengan curiosidad y la usen con más frecuencia, abriendo las puertas a la facilidad del cometimiento de *Child Grooming* que es un delito que se da a través medios tecnológicos o por internet, en donde el victimario, por lo general un adulto, manipula y engaña al menor para obtener contenido sexual o contacto sexual.

VIOLACIÓN DEL DERECHO A LA INTIMIDAD

La tecnología al evolucionar con el tiempo, ha llegado a complementarse con un conjunto de aplicaciones denominadas redes sociales, estas herramientas facilitan la interacción y relaciones interpersonales entre dos o más personas, sin embargo, su mal uso ha influido de manera negativa como un instrumento para divulgar hechos íntimos que violan la integridad del individuo, puesto que los datos personales son de libre acceso en estas plataformas, o están sujetos a un manejo inadecuado en el que su almacenamiento, tratamiento y recuperación son posibles en cualquier tiempo, espacio y dispositivo.

Estos actos conllevan consecuencias que legalmente se convierten en delitos tales como: secuestros, extorsión, fraudes, acoso, violación de intimidad, hackeos de sitios web para capturar datos personales, entre otros delitos que en más de una ocasión provocan un déficit financiero y causan daños psicológicos y psicosociales en las personas afectadas.

El Estado a través de la Constitución, garantiza el completo goce de los derechos fundamentales del ciudadano entre estos, el derecho a la intimidad personal y familiar, el derecho a la protección de datos de carácter personal, entre otros.

Según el Dr. José García Falconí, analista, menciona: "*el derecho a la intimidad detenta un carácter autónomo, como tal no está supeditado al ejercicio de otro para que sea respetado, este derecho es contenido del derecho a la personalidad, mismo que tutela la dignidad humana por lo cual debe de ser objeto de garantía"* (Falconí, 2015)

Por lo que dicho autor, refiere que el derecho a la intimidad puede manifestarse en estas áreas:

Tabla 1. Derecho a la intimidad según García Falconi.

INTIMIDAD FÍSICA	**INTIMIDAD PSICOLÓGICA**
Al desarrollar funciones fisiológicas	Situaciones que el individuo considere vergonzosas
Al desempeñar actividades con representación sexual	Declaraciones que involucre su vida amorosa
Las limitaciones físicas	Creencias religiosas, opiniones, ideologías políticas, que el individuo pueda detectar
La muerte y nacimiento del individuo	Los momentos de consternación y zozobra que sufra el individuo
	El desarrollo y mantenimiento de relaciones patento-filiales
	Datos que el sujeto considere que deben ser ocultos, siempre que estos no sean contrarios a la ley o lesionen derechos de terceros

Tomado de (UNIANDES, 2018)

Si bien es cierto que el artículo 178 del COIP tipifica el delito de violación a la intimidad., y en esencia, se refiere a la grabación u obtención, y publicación de información de una persona sin su autorización y cuya sanción es la privación de libertad de entre uno a tres años. Sin embargo, según abogados y gremios periodísticos, más allá de proteger a víctimas de violencia digital, estas reformas limitan las investigaciones periodísticas y penaliza potenciales pruebas en casos de corrupción. (PRIMICIAS, 2021)

FRAUDE INFORMÁTICO

Para Calderón “El fraude informático a menudo suele relacionarse con el phishing y en algunos casos con el haming, e incluso confundirlos. Sin embargo, en términos generales, el fraude informático implica la provocación de un daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos”. (Mayer Lux & Calderón, 2020)

Existen tres tipos de fraudes penalizados por la ley ecuatoriana:

1. Manipulación de datos de entrada

También conocido como sustracción de datos, simboliza el delito informático más común a realizar, ya que es fácil de cometer y difícil de descubrir, puesto no demanda vastos conocimientos técnicos en informática y puede ejecutarlo cualquier persona que tenga acceso a funciones normales de procesamiento de datos en la fase de obtención de los mismos.

2. Manipulación de programas

Difícil de descubrir y frecuentemente no es percibido o captado, debido a que el desarrollo de este delito es complejo. Consiste en modificar los programas existentes en el sistema de computadoras o en instalar nuevos programas, nuevas rutinas o virus.

3. Manipulación de datos de entrada

Se comete al establecer un objetivo en el funcionamiento del sistema informático.

Un ejemplo claro y común, es el fraude a través de los cajeros automáticos; sucede cuando se falsifica las instrucciones en la computadora en la fase de obtención y verificación de datos. En tiempo antaño, esos fraudes se realizaban a base de tarjetas bancarias robadas. Sin embargo, en la actualidad se utiliza equipos y programas especializados en la decodificación de información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias de débito y crédito.

Según el artículo 190 del COIP, se sentencia este delito a la pena de privativa de libertad de entre tres a cinco años. (Saltos Salgado, Robalino Villafuerte, & Pazmiño Salazar, 2021)

INTERCEPTACIÓN DE COMUNICACIONES

La Real Academia de la Lengua define a la intercepción de comunicaciones como "*una disposición establecida por ley y adoptada por una autoridad judicial con la facultad de apoderarse, obstruir e interrumpir un medio de comunicación*". (RAE, 2023) Este delito refiere a la captación, grabación o divulgación de comunicaciones privadas a través de medios informáticos sin la autorización de las partes involucradas.

La Fiscalía General del Estado con el respaldo de la Constitución (Art. 194, 195 y 226) y el apoyo de entidades como la Secretaría Nacional de Inteligencia (SENAIN), el Subsistema de Interceptación de Comunicaciones o Datos Informáticos (SICOM) y la Fiscalía Especializada en Delincuencia Organizada Transnacional e Internacional (FEDOTI), han logrado desarticular organizaciones delictivas mediante la interceptación de voz y de mensajes de texto (de SMS) de números telefónicos de personas que se encuentren bajo sospecha de estar relacionados con algún ilícito tales como: homicidios, asesinatos, trata y tráfico de personas; además de lavado de activos, asociación ilícita, cohecho, concusión, plagio, robo agravado, extorsión, tenencia, posesión y tráfico ilícito de sustancias estupefacientes y psicotrópicas.

Es necesario resaltar que, cada interceptación no debe ser por más de 90 días y la información recabada se mantiene bajo cadena de custodia, con respecto a la información que no sea útil o de relevancia, esta será eliminada, desechada y descartada de manera permanente de los sistemas de almacenamiento de todas las instituciones involucradas en dicha investigación, según la reforma vigente. (FGE, 2022)

Por otra parte, el interceptar las vías de comunicación no solo está al alcance de instituciones gubernamentales, sino que también pueden ser desarrolladas por ciudadanos intelectualmente aptos y capacitados en cualquier parte del mundo con la finalidad de obtener algún beneficio de su víctima.

REVELACIÓN ILEGAL DE INFORMACIÓN DE BASES DE DATOS

La "Revelación ilegal de información de bases de datos" se refiere a una situación en la cual se divulga, comparte o expone información confidencial o protegida almacenada en bases de datos sin la autorización adecuada o sin un propósito legítimo.

Este delito generalmente implica el acceso no autorizado a una base de datos o sistemas informáticos que contienen información sensible, y posteriormente la divulgación o distribución de esa información a terceros sin el consentimiento del titular de los datos o la entidad que almacena la información.

Las bases de datos pueden contener datos personales, información financiera, secretos comerciales, propiedad intelectual, entre otros tipos de información confidencial. La revelación ilegal de información de bases de datos puede tener graves consecuencias, tanto para los individuos cuyos datos fueron expuestos como para las organizaciones o entidades que sufren la violación de seguridad.

Este tipo de delito suele ser perseguido por la ley, y dependiendo de las jurisdicciones y las leyes aplicables, las personas involucradas en la revelación ilegal de información de bases de datos pueden enfrentar sanciones penales y civiles, incluyendo multas y penas de prisión.

No cabe duda que el incremento de los delitos informáticos se debe gracias a los avances tecnológicos y de acuerdo con estadísticas del Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU), agencia de la Organización de las Naciones Unidas (ONU); los ataques cibernéticos en Latinoamérica han aumentado entre un 30 y 40% en el periodo 2017 – 2020. Lamentablemente, Ecuador no queda exento de dicha estadística, colocándose en el puesto 119 de 182 países participantes, sumándose así a Brasil, Argentina, Colombia, México y Perú, como uno de los países latinos más golpeados por los delitos informáticos. (ONU, 2020)

En síntesis, este tipo de delito se produce cuando “el titular o un tercero revelan datos e información almacenada en ficheros, archivos, o bases de datos personales que se encuentran en instituciones públicas o privadas, hacia algún sistema electrónico, informático, telemático o de telecomunicaciones, violentando intencionalmente la

privacidad del individuo, empresas y microempresas públicas y privadas con fines lucrativos". (Coronel Añazco, 2020)

Fiscalía conoció un hecho que gracias a una denuncia presentada por el entonces director general del Centro de Inteligencia Estratégica sentenció, en la cuidad de Loja (Loja), el 03 de marzo de 2023, a dieciséis meses de prisión a Diego R. quien creó una aplicación que permitía realizar consultas automatizadas a través de un sistema Chatbot, que promocionó en la red social "Acuabot".

Esta aplicación recopilaba, almacenaba y revelaba información de cualquier ciudadano y con el pago de 5 dólares americanos, podía acceder –sin autorización– a distintos sistemas informáticos de fuentes gubernamentales, como el Servicio de Rentas Internas /SRI), Registro Civil, Agencia Nacional de Tránsito (ANT), Sistema de Inteligencia del Centro de Inteligencia Estratégica (CIES), Sistema Integrado Informático de la Policía Nacional del Ecuador (SIPNE), Servicio Ecuatoriano de Capacitación Profesional (SECAP), entre otros. (FGE, 2023)

PHARMING Y PHISHING

El phishing y el pharming son dos de las técnicas de delitos informáticos más usuales que existen en internet. Ambas representan una amenaza, ya que por medio de estas los hackers intentan robar datos personales para hacer mal uso de ellos.

"Phishing, en su traducción al español, significa "pescar, pescando incautos". Esta es una técnica que se basa en intentar engañar al usuario, por lo general a través de un correo electrónico fingiendo ser una empresa o institución verificada, diciéndole que pulse en un determinado enlace, para validar sus claves y datos por uno u otro motivo, redirigiéndolos a una página online que simula ser oficial". (Garea, 2022)

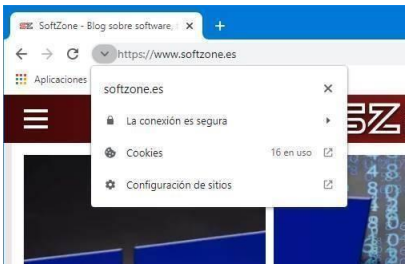
Existen casos en que el Phishing, los remitentes fijen ser de algún banco donde solicitan completar formularios y además ingresar a tu cuenta. Probablemente, al ser de un banco en específico, hacerlo se vuelve necesario, más que todo por seguridad financiera, sin embargo, al aceptar este enlace, lo único que hacen los "incautos" es entregar datos bancarios a un ciberdelincuente.

En otro caso, una institución policiaca advierte sobre acciones legales en contra del usuario, donde solicita por correo electrónico una explicación por verse involucrado en la difusión de contenidos sexuales, acto cuya finalidad es obtener información personal y confirmar que es una cuenta activa en donde en un futuro podrían realizar alguna estafa.

Cabe recalcar que cuando la víctima de phishing abre o descarga algún archivo adjunto en estos correos, esta acción puede ser acompañada con la descarga de algún virus o malware, con el cual podrían manipular la computadora o dispositivo electrónico de forma remota y así también robar datos personales y bancarios.

Por tal motivo, es necesario considerar llamar o visitar a las entidades involucradas y solicitar más información acerca del correo, claro está, que no se debe llamar a los números proporcionados en el correo electrónico. Y también, observar detenidamente la página, ya que existen métodos para comprobar rápidamente su veracidad de esta tales como:

Tabla 2. Métodos para mostrar la veracidad de una página

La URL comienza con https://	La aparición de un candado al principio o al final de la URL.
	

Tomado de (Garea, 2022)

Por su parte, Pharming resulta un poco más peligrosa, ya que es más difícil de identificar. “Resultando de la combinación de los términos phishing y farming, este último haciendo referencia al trabajo agrícola, tiene como fin redirigir a la víctima a una dirección IP falsa, mostrando un sitio web oficial, pero no lo es”. (BANCO PICHINCHA, 2021)

Los hackers pueden hacerlo posible con ayuda de las denominadas “granjas de servidores”, estas son un grupo de ordenadores que están conectados de forma conjunta, haciendo posible realizar cosas que pueden resultar difíciles o imposibles de hacer por un solo servidor ya que toda la carga de trabajo es distribuida entre múltiples componentes de los servidores. Este delito puede ser provocado por la redirección a un enlace, enviado a un correo electrónico o como ya se mencionó con anterioridad, redirigirnos a la página falsa del banco bosquejada por los raptores de forma automática, es decir, sin que nosotros necesitemos pulsar ningún enlace.

En los sistemas Windows, existe una forma de agilizar el trabajo de los servidores DNS, ahorrándole algo de tiempo a nuestro proveedor del servicio de internet. El servicio DNS (Resolución de Nombres), no es nada más que la misma dirección IP, traducida a un lenguaje que podamos entender, el lenguaje de palabras; mientras que una dirección IP está formada por 4 números, separados por un punto (.) y cada uno de ellos puede tener un valor de 0-255. Por ejemplo, si se escribe en el navegador www.elmundo.es o también http://193.110.128.212 iremos al mismo sitio web, puesto que solo se trata de una traducción. Al delinquir estas personas utilizan un fichero del sistema llamado HOSTS. Cada vez que se escribe una dirección en el navegador, lo primero que hace el sistema es comprobar si esa dirección (ese "host", en términos informáticos) está en el fichero hosts, y si es así, el ordenador lee la dirección IP que le corresponde y nos enviará allí.

Por lo tanto, los estafadores se pueden meter en nuestro ordenador para modificarnos este fichero a través de un virus o malware. De esta forma, cuando escribamos en nuestro navegador una dirección, estaremos yendo a otra sin saberlo. Un claro ejemplo, lo datamos en el 2007, donde se produjo un ataque de pharming a nivel global contra más de 50 entidades bancarias, lastimosamente, hubo millones de afectados, principalmente en Estados Unidos y Europa; A pesar de que es complejo detectar una página pharming, es posible considerar ciertas características para corroborar la veracidad de la misma, dichas características son compartidas con la técnica de estafa phishing, es decir:

- URL de la página web: comprobar que comienza por https:// y no por http://

- Revisar la URL completa: no debe existir guiones inusuales o algún cambio (letra o palaba añadida) en la dirección habitual
- Examinar el diseño de la web: Revisa detalladamente la composición de la página. Fíjate en el color, la disposición de los elementos o los botones de inicios.

Tabla 3. Cuadro comparativo entre Pharming y Phishing

PHARMING	PHISHING
• Más difícil de identificar • Múltiples objetivos al mismo tiempo • Código malicioso instalado en el ordenador • Dirige automáticamente sin que los usuarios tengan que clicar	• Más fácil de identificar • Un objetivo cada vez • Email malicioso enviando a la bandeja • Requiere que los usuarios hagan clic para activar el código

Obtenido de: (Panda Security, 2022)

En Ecuador, los delitos informáticos se vienen sancionando con moderación desde el 2009, sin embargo, a raíz del confinamiento gracias al COVID-19 los casos aumentaron considerablemente, llegando a sumar más de 600 casos en el último estudio realizado del año 2020-2021, según (EL UNIVERSO, 2021).

SABOTAJE INFORMÁTICO

Es el Ataque A La Integridad De Sistemas Informáticos y Consiste en interferir, dañar o interrumpir el funcionamiento de un sistema informático con el propósito de causar perjuicio, generalmente es conocido como sabotaje informático o delito de daños informáticos, este consiste en borrar, suprimir o modificar sin autorización algunas o todas las funciones o datos de un sistema informático (S.I.) con intención de obstaculizar y alterar el funcionamiento normal del mismo.

En otras palabras, se trata de una acción dolosa que tiene como objetivo comprometer la exactitud y confidencialidad de los registros digitales sin importar la entidad afectada, sea esta pública o privada.

"Cuando se habla de un Sistema Informático, en esencia se refiere a un conjunto de elementos físicos y lógicos capaces de recibir, guardar y procesar información, para posteriormente otorgar resultados solicitados a partir de ello, la parte física se adjudica al hardware, es decir, todo lo tangible, mientras que la parte lógica alude al software, es decir, todo lo intangible. Según otros autores, es posible incluir al personal informático dentro del sistema, puesto que son aquellas personas encargadas de manejar a los ordenadores, haciéndolo también parte fundamental de la estructura". (Chavez, 2023)

Uno de los últimos casos conocidos por la ciudadanía y relacionados a este delito en Ecuador tenemos al que sucedió en las instalaciones de la Agencia Nacional de Tránsito (ANT). Un 22 de octubre del 2021, la Policía y Fiscalía allanaron la oficina central de la ANT en Quito, con la finalidad de conseguir más información y localizar a los responsables de ese ataque cibernético. Los agentes decomisaron tres discos duros y dos teléfonos pertenecientes a funcionarios de la entidad.

Este hecho, es decir la vulneración al sistema informático, impidió que los usuarios realicen sus trámites de licencias y matrículas vehiculares.

La ANT explicó que este ataque se produjo 24 horas después de establecer medidas de seguridad informática para evitar ilícitos con la entrega de licencias; además de ejecutar procesos regulatorios para anular "el alza fraudulenta de puntos, la entrega ilícita de licencias profesionales y no profesionales y la baja de 100 000 procesos de matriculación vehicular entregados sin el pago de las multas correspondientes" ((ANT), 2021)

DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVADA LEGALMENTE

Esta infracción penaliza a aquella persona, sea o no un servidor público que acceda, destruya o inutilice información pública almacenada en los diferentes sistemas informáticos, utilizando algún medio electrónico o tecnológico, para llevar a cabo dicho delito.

ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES

Consiste en ingresar sin autorización a un sistema informático protegido, ya sea por violación de medidas de seguridad o mediante el uso de contraseñas o credenciales obtenidas de manera ilícita. En el Artículo 234 del COIP indica que la persona que sin autorización previa acceda completa o parcialmente a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificando un portal web, desviando o redireccionando el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.

Actualmente, el término telemático se usa para hacer referencia a soluciones utilizadas en los vehículos de flota comercial; en otras palabras, son software especializado en la gestión de flotas, cuyo fin es coordinar los vehículos disponibles y tener una visión general y en conjunto del estado, la rentabilidad y la productividad de toda la flota. Los sistemas telemáticos incluidos en los vehículos cuentan con un dispositivo de seguimiento que envía, recibe y almacena datos de telemetría, estos datos pueden ser: ubicación, la velocidad, los tiempos muertos, la aceleración o las frenadas bruscas, el consumo de combustible, los fallos en los vehículos, etc.; dichos datos utilizan una comunicación a través de la red inalámbrica que se realiza gracias a un módem a bordo, el dispositivo recoge la información y los transmite a un servidor centralizado vía GPRS (servicio de paquetes vía radio), 4G u otra tecnología de telefonía móvil o redes de comunicaciones por satélite. El servidor interpreta los datos y los muestra al usuario final en sitios web seguros o aplicaciones optimizadas para teléfonos móviles y tabletas.

Por otra parte, al hablar de Sistemas de Telecomunicaciones, hace referencia a una comunicación a grandes distancias utilizando señales eléctricas u ondas electromagnéticas a través de un conjunto de nodos y enlaces que proporcionan conexiones entre dos o más puntos definidos, un claro ejemplo, tenemos el uso de teléfonos celulares o computadoras.

2.1.5 SOBRE INFORMÁTICA FORENSE

Concepto y generalidades

La Informática Forense, también conocida como Forense Digital o Ciencia Forense Computacional, es una disciplina que se ocupa de la recolección, análisis y preservación de evidencia digital con el fin de investigar y prevenir delitos cibernéticos. Consiste en aplicar técnicas y metodologías especializadas para descubrir, recolectar, examinar y presentar pruebas digitales en un contexto legal.

El objetivo principal de la Informática Forense es recopilar evidencia digital de manera forense, es decir, siguiendo métodos científicos y legales para asegurar la integridad y confiabilidad de la evidencia. Esto implica el uso de herramientas y técnicas especializadas para extraer información de dispositivos electrónicos, redes, sistemas informáticos y cualquier otro medio digital.

La Informática Forense se aplica en una amplia variedad de delitos y situaciones legales, incluyendo: Delitos informáticos, Investigación de ataques cibernéticos, intrusiones en sistemas, fraudes electrónicos, robo de información, ciber espionaje, entre otros.

Delitos con evidencia digital: Recopilación y análisis de pruebas digitales en casos de pornografía infantil, acoso en línea, difamación, extorsión, entre otros.

Análisis de dispositivos digitales: Examinar computadoras, teléfonos móviles, discos duros, dispositivos de almacenamiento, dispositivos IoT, para identificar y recuperar evidencia digital.

Análisis de redes y tráfico de datos: Investigar actividades sospechosas en redes, identificar intrusiones y analizar el tráfico de datos para recopilar pruebas.

Análisis de malware: Estudiar programas maliciosos para comprender su funcionamiento, su propósito y el impacto que han tenido en un sistema o red.

Recuperación de datos: Utilizar técnicas especializadas para recuperar información borrada o dañada de dispositivos digitales.

IMPORTANCIA DE LA INFORMÁTICA FORENSE

La Informática Forense es fundamental en el ámbito legal, ya que proporciona pruebas digitales que pueden ser utilizadas en investigaciones criminales, procesos judiciales, juicios y peritajes. Además, contribuye a garantizar la integridad y validez de la evidencia digital, así como a proteger los derechos y la privacidad de las personas involucradas en los casos. En el proceso penal es de suma importancia debido a la creciente presencia de la tecnología en nuestra sociedad y su impacto en delitos y actividades ilícitas. Esta disciplina se enfoca en la recolección, análisis y preservación de evidencia digital para su uso y su relevancia radica en varios aspectos:

Identificación y recolección de pruebas digitales: La Informática Forense permite identificar, recolectar y asegurar pruebas digitales que podrían ser cruciales en un caso penal. Esto incluye datos almacenados en computadoras, teléfonos móviles, discos duros, dispositivos de almacenamiento y en la nube.

Pruebas sólidas y admisibles en el tribunal: La manipulación incorrecta de evidencia digital puede invalidarla como prueba en un juicio. Los especialistas en Informática Forense están capacitados para seguir procedimientos rigurosos y garantizar que la evidencia digital se recolecte y analice de manera forense, asegurando su admisibilidad en el tribunal.

Resolución de casos complejos: Muchos delitos modernos involucran tecnología, como el cibercrimen, el fraude electrónico, el robo de identidad, el acoso en línea y más. La Informática Forense permite investigar y resolver casos complejos que de otra manera serían difíciles de esclarecer.

Prevención y disuasión del delito: La capacidad de recuperar pruebas digitales y utilizarlas en juicios ayuda a disuadir a los delincuentes, ya que saben que es más probable que sean capturados y condenados.

Protección de los derechos individuales: La Informática Forense se realiza siguiendo estrictos protocolos legales y éticos para garantizar que la recolección de datos digitales no viole los derechos de privacidad de las personas.

Recuperación de información eliminada: Los delincuentes informáticos pueden intentar ocultar sus actividades eliminando datos o utilizando técnicas avanzadas para borrar su rastro digital. Los expertos en Informática Forense pueden recuperar información eliminada o escondida, proporcionando una visión completa de los hechos.

Apoyo a la justicia y equidad: La utilización de la Informática Forense en el proceso penal busca garantizar una justicia más equitativa y precisa, permitiendo la identificación de los verdaderos responsables y evitando la condena errónea de personas inocentes.

En resumen, la Informática Forense es crucial en el proceso penal porque proporciona las herramientas necesarias para lidiar con la complejidad y sofisticación de los delitos informáticos, asegura la integridad de la evidencia digital y contribuye a un sistema de justicia más eficiente y justo en la era digital.

SUJETOS DEL DELITO INFORMÁTICO

Si bien se ha considerado que los delitos informáticos y ciberdelitos son aquellos que se cometen utilizando tecnologías de la información y las comunicaciones como medios para llevar a cabo actividades ilícitas. Los sujetos activos, sujetos pasivos y bienes jurídicos protegidos pueden variar según el tipo específico de delito informático. A continuación, proporcionaré algunos ejemplos comunes:

SUJETO ACTIVO

En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación pudiendo ser por ejemplo hackers, crackers, spammers, phishers, entre otros individuos o grupos con habilidades técnicas para acceder ilegalmente a sistemas informáticos

SUJETO PASIVO

Son las personas o entidades que sufren el daño o la afectación como resultado del delito informático. Estos pueden ser particulares, empresas, instituciones gubernamentales o cualquier entidad con sistemas de información vulnerables.

BIEN JURÍDICO PROTEGIDO

"El bien jurídico cumple funciones de gran relevancia para las ciencias penales. Entre ellas, la afectación de un bien jurídico permite fundamentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito ineludible para el ejercicio del ius puniendi". (Revista chilena de derecho, 2017)

Bienes jurídicos protegidos: Son los intereses o valores que la ley busca salvaguardar y proteger mediante la tipificación de los delitos informáticos. Algunos bienes jurídicos protegidos en este contexto pueden incluir:

- Integridad de datos y sistemas informáticos: Proteger la información y los sistemas de computadoras de accesos no autorizados, alteraciones o destrucción.

- Confidencialidad: Salvaguardar la privacidad de la información almacenada y transmitida a través de sistemas informáticos.
- Disponibilidad: Garantizar que los sistemas y datos estén disponibles para su uso legítimo y no sean objeto de denegación de servicio u otros ataques que los inhabiliten.
- Propiedad intelectual: Proteger los derechos de autor, patentes y marcas registradas relacionadas con software, obras digitales y otros activos intelectuales en línea.
- Privacidad y datos personales: Resguardar la información personal de los individuos y prevenir su mal uso o divulgación no autorizada.

Es importante tener en cuenta que las legislaciones varían entre países y pueden tener definiciones y alcances diferentes

2.1.6 LA PRUEBA DIGITAL

ANTECEDENTES DE LA PRUEBA DIGITAL

Los antecedentes de la prueba digital se remontan a la popularización de las tecnologías de la información y la comunicación (TIC) en la sociedad. A medida que el uso de computadoras, internet y dispositivos electrónicos se ha vuelto más común, también ha aumentado la relevancia de la información digital como evidencia en casos legales.

Los primeros casos de prueba digital estuvieron relacionados con delitos informáticos, como el hacking y el fraude informático, que requirieron la presentación de pruebas electrónicas para establecer la responsabilidad de los acusados.

Con el tiempo, la evolución de las TIC ha llevado a la creación de nuevos tipos de pruebas digitales, como registros de actividad en línea, mensajes de texto, correos electrónicos, imágenes y videos digitales, datos de ubicación de dispositivos móviles, historiales de navegación web, entre otros.

EVOLUCIÓN DE LA PRUEBA DIGITAL

La evolución de la prueba digital ha estado influenciada por el rápido desarrollo tecnológico y los cambios en la forma en que las personas almacenan, comparten y acceden a la información.

En el pasado, las pruebas digitales se basaban principalmente en registros de actividad en sistemas informáticos y correos electrónicos. Sin embargo, con la proliferación de las redes sociales, los dispositivos móviles y las aplicaciones de mensajería, las pruebas digitales han adquirido una mayor variedad y complejidad.

Además, el aumento en la cantidad de datos digitales generados por individuos y organizaciones ha hecho que la gestión y autenticación de las pruebas digitales sean aspectos críticos en el proceso legal.

CARACTERÍSTICAS DE LA PRUEBA DIGITAL

Sobre la prueba digital se exponen las siguientes características:

Volatilidad: La prueba digital puede ser fácilmente alterada o eliminada, lo que requiere medidas específicas para preservar su integridad y autenticidad.

Autenticidad: Es fundamental asegurar que la prueba digital proviene de la fuente alegada y no ha sido manipulada para garantizar su validez en el juicio.

Rastreabilidad: Se debe poder rastrear el origen y las manipulaciones realizadas a la prueba digital desde su creación hasta su presentación en el tribunal.

Complejidad técnica: La gestión y presentación de pruebas digitales pueden requerir conocimientos técnicos especializados y la participación de expertos forenses digitales.

Privacidad: Algunas pruebas digitales pueden contener información sensible o privada, por lo que se debe tener en cuenta la protección de datos durante el proceso legal.

Cadena de custodia: Es esencial mantener una cadena de custodia adecuada para asegurar que la prueba digital no se altere ni se contamine desde el momento de su obtención hasta su presentación en el tribunal.

FASES DE LA PRUEBA DIGITAL

Las fases de la prueba digital en el contexto de un proceso judicial implican una serie de etapas bien definidas para garantizar la autenticidad, integridad y validez de la evidencia digital presentada. A continuación, describiré cada una de estas fases:

INCORPORACIÓN DE LA PRUEBA DIGITAL

Una vez que la prueba digital ha sido debidamente obtenida, tratada y su cadena de custodia se ha documentado correctamente, puede ser incorporada al proceso judicial. La presentación de la evidencia digital puede ocurrir durante distintas etapas del juicio, como audiencias previas, juicio oral o presentaciones escritas, y debe realizarse de acuerdo con los procedimientos y reglas establecidos por el sistema legal aplicable.

OBTENCIÓN, TRATAMIENTO, INCORPORACIÓN DE LA PRUEBA DIGITAL

La primera fase implica la recopilación de la evidencia digital relevante para el caso. Esto puede incluir registros de actividad en sistemas informáticos, correos electrónicos, mensajes de texto, imágenes, videos, archivos digitales u otros datos electrónicos pertinentes. La obtención debe realizarse siguiendo procedimientos legales y garantizando que se preserven las características originales de la prueba para evitar cualquier alteración o contaminación.

Tratamiento. Una vez que se ha obtenido la evidencia digital, es necesario realizar su tratamiento adecuado para garantizar su integridad. Esto puede implicar la creación de copias forenses de la prueba original para evitar daños accidentales o modificaciones. El tratamiento también puede incluir la eliminación de datos irrelevantes o duplicados para simplificar el análisis y presentación de la evidencia.

CADENA DE CUSTODIA DE LA PRUEBA DIGITAL

La cadena de custodia es un componente crítico en la gestión de pruebas digitales. Consiste en mantener un registro detallado y documentado de todos los pasos tomados desde la obtención hasta la presentación de la prueba en el tribunal. Esto incluye información sobre quién tuvo acceso a la evidencia, cuándo y con qué propósito, para garantizar que no se produzcan alteraciones o manipulaciones durante el proceso. Mantener una cadena de custodia adecuada es esencial para asegurar la admisibilidad de la prueba en el juicio.

CARGA DE LA PRUEBA DIGITAL EN EL PROCESO JUDICIAL

En algunos sistemas legales, la carga de la prueba recae en la parte acusadora o demandante para demostrar la culpabilidad o sustentar sus reclamaciones. En este sentido, la parte que presenta la prueba digital debe asegurarse de que se cumplan los requisitos de autenticidad, integridad y relevancia para demostrar su caso de manera convincente.

Es importante destacar que la gestión de pruebas digitales puede ser compleja y, en muchos casos, requerir la participación de expertos en informática forense para garantizar que se cumplan los estándares legales y técnicos necesarios. La presentación efectiva de pruebas digitales puede tener un impacto significativo en el resultado de un caso judicial, por lo que es fundamental seguir procedimientos adecuados y proteger la integridad de la evidencia digital en todo momento.

2.1.7 EFICACIA PROCESAL DE LA PRUEBA

La eficacia procesal de la prueba se refiere a la capacidad de la evidencia presentada en un proceso judicial para influir en la decisión final del tribunal. Es fundamental para garantizar un juicio justo y objetivo. La prueba debe cumplir con ciertos principios y requisitos para ser considerada válida y admisible en el proceso judicial.

PRUEBA JUDICIAL

La prueba judicial es el conjunto de elementos o medios utilizados para demostrar los hechos en un caso ante un tribunal. Estos elementos pueden ser documentos, testimonios de testigos, peritajes, pruebas físicas o cualquier otra evidencia que ayude a establecer la verdad sobre los hechos en disputa.

PRINCIPIOS DE LA PRUEBA JUDICIAL

- Principio de pertinencia: La prueba debe estar directamente relacionada con los hechos en disputa y ser relevante para la resolución del caso.
- Principio de contradicción: Las partes tienen el derecho de confrontar y cuestionar las pruebas presentadas por la otra parte, lo que permite asegurar la imparcialidad y la veracidad de la evidencia.
- Principio de publicidad: Las pruebas deben presentarse en audiencias públicas para garantizar la transparencia del proceso judicial.
- Principio de inmediación: El tribunal debe presenciar directamente la presentación de las pruebas para poder evaluar su credibilidad y valor probatorio.
- Principio de unidad de acto: La valoración de la prueba debe realizarse de manera integral, considerando todas las pruebas presentadas, y no de forma aislada.

NECESIDAD DE LA PRUEBA

La necesidad de la prueba radica en la premisa de que los tribunales deben basar sus decisiones en hechos probados y no en conjeturas o suposiciones. La evidencia es esencial para establecer la verdad sobre los acontecimientos en disputa y proporciona una base sólida para la toma de decisiones justas y equitativas.

ELEMENTOS PROBATORIOS

Los elementos probatorios son los distintos medios o tipos de pruebas que se pueden presentar en un juicio para demostrar la verdad de los hechos. Algunos ejemplos de elementos probatorios incluyen:

- Testimonios de testigos presenciales o expertos.
- Documentos, como contratos, facturas, registros médicos, entre otros.
- Pruebas físicas, como armas, drogas u otros objetos relacionados con el caso.
- Pruebas digitales, como correos electrónicos, mensajes de texto, registros de actividad en línea, etc.

ADMISIBILIDAD E INADMISIBILIDAD DE LA PRUEBA

La admisibilidad de la prueba se refiere a la capacidad de la evidencia para ser aceptada por el tribunal y considerada como válida para su valoración. La inadmisibilidad, por otro lado, se refiere a la exclusión de una prueba, ya sea por no cumplir con ciertos requisitos legales o por haber sido obtenida de manera ilegal o inapropiada.

Las reglas de admisibilidad varían según las leyes y procedimientos legales de cada jurisdicción. Algunos motivos comunes para la inadmisibilidad de la prueba pueden incluir:

- Falta de pertinencia o relevancia.
- Obtención de la prueba de manera ilícita, como violando el derecho a la privacidad o sin autorización legal.
- Pruebas obtenidas bajo coacción o mediante tortura.
- Pruebas que son demasiado especulativas o con poca fiabilidad.

Es responsabilidad de las partes en el juicio y del tribunal garantizar que la evidencia presentada cumpla con los principios y requisitos de admisibilidad para que pueda ser considerada en la toma de decisiones.

La evolución constante de la tecnología seguirá influyendo en la forma en que se recopilan, presentan y evalúan las pruebas digitales en el ámbito legal. Los sistemas legales de todo el mundo están trabajando para adaptarse a estos cambios y

desarrollar marcos regulatorios y procesos adecuados para abordar los desafíos que presentan las pruebas digitales en los casos judiciales.

2.2 MARCO LEGAL

- **Constitución de la República del Ecuador** (449 R. o., 2008)

Primera Constitución: El 11 de agosto de 1830, Ecuador se separó de la Gran Colombia y se convirtió en una república independiente. Ese mismo año, se promulgó la primera Constitución del país, que estableció la estructura básica del gobierno y los principios políticos y legales. A lo largo del siglo XIX, Ecuador experimentó una serie de gobiernos y constituciones que reflejaban la inestabilidad política y las luchas internas entre diferentes facciones políticas y regiones.

La Constitución de 1906: Esta constitución estableció un sistema de gobierno conservador y centralizado, otorgando amplios poderes al presidente y restringiendo las libertades civiles.

La Constitución de 1929: Esta constitución buscó abordar algunos de los problemas sociales y políticos del país, estableciendo derechos laborales y sociales.

La Revolución Liberal de 1944: Un movimiento popular llevó al derrocamiento del gobierno conservador y la promulgación de una nueva constitución en 1945, que incluyó disposiciones progresistas y democráticas.

La Constitución de 1978: Tras varios períodos de inestabilidad política, se promulgó una nueva constitución que estableció un gobierno democrático y representativo.

La Constitución de 1998: En 1998, se aprobó una nueva constitución que otorgó mayor reconocimiento a los derechos indígenas y promovió la descentralización del poder.

La Constitución de 2008: La actual Constitución de Ecuador o la denominada carta magna que establece las bases fundamentales del país, fue aprobada en 2008 y marcó un cambio significativo en la estructura política y legal del país. Esta constitución ha sido objeto de enmiendas y reformas a lo largo de los años como también esta constitución reconoció a Ecuador como un Estado Plurinacional e incluyó

disposiciones progresistas sobre derechos humanos, derechos de la naturaleza, participación ciudadana, y descentralización, entre otros.

En la función ejecutiva, su máxima autoridad preside en El presidente de la República es el jefe del Estado y de gobierno, y es elegido por voto popular. Su mandato tiene una duración de cuatro años, pudiendo ser reelegido una sola vez de manera consecutiva. La Función Legislativa responde al poder legislativo que recae en la Asamblea Nacional, conformada por asambleístas elegidos por voto popular.

La Asamblea es responsable de la elaboración y aprobación de leyes. La administración de justicia está a cargo de la Función Judicial, que garantiza la independencia y autonomía del sistema judicial. Existe un Consejo de la Judicatura encargado de la designación y evaluación de jueces y demás funcionarios judiciales.

Es importante mencionar que la Constitución de la República del Ecuador ha sido objeto de cambios a lo largo del tiempo, mediante enmiendas y reformas constitucionales, lo que ha influido en la evolución de su contenido y aplicación.

Artículo 9: Establece el deber del Estado de promover la interculturalidad, la plurinacionalidad y el respeto a la diversidad étnica y cultural del país.

Artículo 66: Reconoce el derecho a la seguridad social, incluyendo la salud, la educación, la vivienda, el agua potable, el saneamiento y el ambiente sano, y garantiza el acceso universal a estos servicios.

Artículo 86: Establece que toda persona tiene derecho a un ambiente sano y a vivir en un ambiente libre de contaminación. Además, se establece el deber del Estado y de los ciudadanos de proteger el medio ambiente.

Artículo 103: Establece la independencia y autonomía de la Función Judicial y del Consejo de la Judicatura, garantizando un sistema de justicia transparente, imparcial y eficiente.

Artículo 194: Se refiere a la función de control político que ejerce la Asamblea Nacional sobre el Ejecutivo y otros órganos del Estado, con el fin de garantizar la transparencia y la rendición de cuentas.

Artículo 195: Establece la autonomía y funciones del Consejo de Participación Ciudadana y Control Social, cuyo objetivo es garantizar la participación ciudadana en los procesos de designación y control de autoridades.

Artículo 226: Establece el derecho a la comunicación y la libertad de expresión, garantizando la diversidad y pluralismo informativo. Se establecen regulaciones para evitar la concentración de medios de comunicación.

Artículo 393: Se refiere a la Corte Constitucional, estableciendo su función como intérprete máxima de la Constitución y sus atribuciones para garantizar la supremacía constitucional.

Artículo 442: Establece el derecho de participación de los ciudadanos, incluyendo la participación en la formulación, ejecución y control de políticas públicas, así como el derecho a la revocatoria del mandato.

Artículo 443: Regula el derecho a la resistencia, estableciendo que este derecho puede ser ejercido por los ciudadanos en defensa de sus derechos e intereses.

Artículo 444: Se refiere a la transparencia y acceso a la información pública, estableciendo el derecho de las personas a acceder a la información en posesión de las instituciones del Estado y a recibir una respuesta oportuna.

- **Código Orgánico Integral penal** (COIP_act_feb-2021.pdf, 2014)

Los antecedentes del Código Orgánico Integral Penal (COIP) del Ecuador se remontan a la necesidad de actualizar y modernizar el sistema penal ecuatoriano para adecuarlo a los cambios sociales, culturales y jurídicos del país. A continuación, se presentan los principales hitos en la evolución del COIP:

Código de Procedimiento Penal de 1998: Antes de la promulgación del COIP, el sistema penal ecuatoriano estaba regido principalmente por el Código de Procedimiento Penal de 1998. Este código regulaba principalmente los procedimientos y garantías procesales, pero no abordaba de manera integral los tipos penales y las sanciones.

Asamblea Nacional Constituyente de 2008: En 2008, se llevó a cabo una Asamblea Nacional Constituyente con el propósito de redactar una nueva Constitución para el país. La nueva Constitución de la República del Ecuador, aprobada en ese mismo año, estableció la base para la reforma integral del sistema penal y la creación del COIP.

Reforma Constitucional de 2011: En 2011, se llevó a cabo una reforma constitucional que introdujo importantes cambios en el sistema de justicia penal, como la adopción del enfoque garantista y el reconocimiento de los derechos de las víctimas.

Anteproyecto del COIP: A partir de 2012, se inició un proceso de trabajo para redactar el anteproyecto del COIP. Se contó con la participación de expertos en derecho penal, juristas, académicos y representantes de la sociedad civil.

Aprobación y Promulgación del COIP: El 10 de febrero de 2014, la Asamblea Nacional de Ecuador aprobó el Código Orgánico Integral Penal. El 19 de febrero del mismo año, el presidente Rafael Correa lo sancionó y fue publicado en el Registro Oficial.

El COIP entró en vigencia el 10 de agosto de 2014 y representa un cambio significativo en la legislación penal del país. Incorpora nuevos tipos penales, reconoce derechos de las víctimas, promueve una justicia restaurativa y busca adecuar el sistema penal a los principios y valores establecidos en la Constitución de 2008. Además, el COIP refleja el compromiso del Ecuador en la lucha contra la criminalidad y la promoción de la justicia social.

ANÁLISIS DEL ARTÍCULO 178 COIP:

Este artículo trata sobre el delito de estafa y define las acciones que constituyen esta conducta delictiva. Establece que comete estafa quien, mediante engaño o astucia,

induzca o mantenga a alguien en error, con el fin de obtener un provecho económico indebido para sí o para un tercero. También se tipifican otras formas de estafa, como el uso de tarjetas de crédito falsas o alteradas, o la manipulación de sistemas informáticos para obtener beneficios económicos.

Art. 186.- Estafa. - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario. 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

Análisis del artículo 186 trata sobre el delito de fraude informático y otros delitos relacionados con tecnologías de la información y la comunicación. Establece que comete este delito quien, con el propósito de obtener un beneficio económico para sí o para otro, acceda, intercepte, interfiera, altere o modifique datos informáticos, sistemas o redes informáticas sin autorización. También se incluyen acciones como la falsificación de documentos electrónicos o la utilización de programas informáticos para defraudar.

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura

a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Análisis del artículo 190 se refiere al delito de acceso no autorizado a un sistema informático o a una base de datos. Establece que comete este delito quien acceda a un sistema informático o base de datos sin autorización, incluso cuando no medie el propósito de obtener un beneficio económico. La pena será más grave si el acceso no autorizado causa daño o perjuicio a los datos o al sistema.

2.3 MARCO CONCEPTUAL

Bien Jurídico. - Todo bien o valor de la vida de las personas que es protegido por la ley. Se trata de algo, ya sea tangible o intangible, considerado valioso a un nivel que merece una garantía legal de no ser quebrantado por la acción de un tercero.

Delito. - Infracción penal; Acción o conducta típica, antijurídica y culpable que, por ello, es normalmente punible.

Delito Informático. - Es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática

Eficacia Procesal. - Del orden jurídico consiste en el hecho de que generalmente los individuos a quienes **se** dirigen las normas **se** conforman **con** ellas y en caso de incumplimiento, **se** aplican también generalmente las sanciones previstas para tales supuestos.

Evidencia. - Del lat. *evidentia*. *Es la* Certeza clara y manifiesta de la que no se puede dudar. Prueba determinante en un proceso.

Evidencia Digital. - La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación

Integridad de datos. - La integridad de los datos se refiere a la información almacenada en cualquier tipo de base de datos o centro de datos que sea precisa, completa, consistente y confiable, sin importar cuánto tiempo se almacene o con qué frecuencia se acceda a ella.

Pericia. - La Pericia es el medio probatorio con el cual se intenta obtener, para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o la valoración de un elemento de prueba.

Perito informático. - Es una persona con formación de la disciplina criminalística del ámbito de la informática y sistemas computacionales, con alto nivel de capacitación, conocimientos y experiencia en un ámbito técnico, p cuyo testimonio puede ayudar en la resolución de casos de delitos afines

Proceso Judicial. - Der. Conjunto de actos y trámites seguidos ante un juez o tribunal, tendentes a dilucidar la justificación en derecho de una determinada pretensión entre partes y que concluye por resolución motivada.

Propiedad Intelectual. - Es el derecho que se confiere a la persona sobre las creaciones de su mente. Quien tiene es el titular exclusivo sobre la utilización de su obra por un plazo determinado o indeterminado.

Prueba digital. - "Toda aquella información digital acreditativa de la realidad de un hecho afirmado por las partes y que resulta relevante para el objeto del proceso judicial" (Aguilar, 2019)

Prueba judicial. - Devis Echandía define las pruebas judiciales como «el conjunto de reglas que regulan la admisión, producción, asunción y valoración de los diversos medios que pueden emplearse para llevar al juez la convicción sobre los hechos que interesan al proceso»

Sistema informático. - Es un sistema que nos permite almacenar y procesar información mediante una serie de partes interrelacionadas, como el hardware, el software y el personal. De hecho, estos son sus tres componentes fundamentales.

CAPÍTULO III:

MARCO METODOLÓGICO

3.1 DISEÑO Y TIPO DE INVESTIGACIÓN

3.1.1 ENFOQUE DE LA INVESTIGACIÓN

Para entender un proyecto de investigación a lo largo del tiempo y en varias etapas de ellas se debe tener claro que en todas comparten una similitud y una relación en ambos métodos Cualitativo y Cuantitativo como lo explica el libro de Hernández, Fernández y Baptista en donde explica que ambas llevan a cabo la observación y evalúan fenómenos y que a partir de ellas establecen ideas y suposiciones mismas que se deben fundamentar y probar para permitir proponer nuevas observaciones que fundamentar nuevas ideas.

Por lo tanto, este proyecto de investigación está orientado al análisis teórico proveniente de estadísticas proporcionadas de las instituciones públicas del estado en este caso, la fiscalía general del Estado, las mismas que nos permitirán realizar una interpretación amplia de la problemática actual de nuestro objeto de estudio “La Eficacia O Ineficacia De La Evidencia Digital Como Elemento Probatorio En El Juzgamiento De Los Delitos Informáticos

Eficacia o Ineficacia de la Evidencia digital como elemento probatorio pericial y la admisibilidad en delitos informáticos dentro de los procesos judiciales” por medio de los métodos de investigación que se detallan de la siguiente manera:

Teniendo en cuenta a los autores que describen lo siguiente “el enfoque cualitativo permite utilizar técnicas para recolección de datos, como la observación no estructurada, entrevistas abiertas, revisión de documentos, evaluación de experiencias personales… Será la modalidad que determine la estructura de este proyecto para obtener de manera directa la información necesaria por lo tanto por serán las entrevistas de campo a profesionales del derecho tales como: jueces, fiscales, miembros de la policial judicial y abogados en libre ejercicio; recolección de datos estadísticos obtenidos de las bases de datos de la Función Judicial; y a través del análisis interpretativo de las fuentes obtenidas la aportación que permitirá

demostrar la hipótesis planteada dentro del proyecto de investigación. Para el estudio de la información se aplicará el método analítico, el mismo que ayudará a establecer los fenómenos concretos que generan el problema.

3.1.2 TIPO DE INVESTIGACIÓN

Para el referido tema La eficacia de la evidencia digital y su admisibilidad en el juzgamiento de los delitos informáticos el tipo de investigación en que se presentará este trabajo es de tipo exploratorio en la que se evaluara una situación latente y actual que determina un fenómeno que se vive a diario y expone a muchos ciudadanos y al mundo entero enfrentar problemas de seguridad con respecto a los delitos informáticos y que sin duda no se puede obviar pues la globalización acentúa la necesidad de mantener conexiones tecnológicas, electrónicas y de redes sociales que difícilmente irán quedando atrás sino, por el contrario ira en aumento por lo que es importante conocer la normativa que protege los derechos de los ciudadanos como usuarios de los medios tecnológicos. Así también bajo este mismo tipo de estudio exploratorio se podrá conocer las sanciones de los tipos penales que están tipificados como delitos y el procedimiento que se lleva para determinar la eficacia de la norma y la admisibilidad de la evidencia digital que sirve como prueba para el juzgamiento de estos delitos que se describirán con sus respectivas características.

Por lo tanto, el tipo de investigación exploratoria promueve la comprensión de la realidad determinada en herramientas conceptuales y prácticas de las que se levantara la información necesaria para cumplir con los objetivos del mismo y para ello debemos involucrar todo en cuanto al sistema teórico, formal y metodológico que permita alcanzar los resultados planteados. Así lo plantea el tesista Carlos Mendez,20111 en la siguiente definición "*Cuando el investigador construye un marco de referencia teórico y práctico puede decirse que este primer nivel de conocimiento es exploratorio, el cual puede complementarse con el descriptivo, según lo que quiera o no el investigador". (pag.230)*

3.1.3 RECOLECCIÓN DE LA INFORMACIÓN

POBLACIÓN Y MUESTRA

POBLACIÓN

Dentro de la presente investigación se tomará en consideración a un determinado grupo de operadores de justicia que se encuentran inmersas dentro de la problemática objeto de estudio, y quienes validan las pruebas el procesos judiciales y representados los cuales mencionaremos como por ejemplo: Jueces de garantías penales; Fiscales, defensores públicos, Abogados en libre ejercicio y el análisis documental de un caso por ser uno de los puntos clave del procedimiento que se lleva ante el juzgamiento de los delitos informáticos. Esta selección se produce a partir de la siguiente cita del libro de Metodología de Carlos Méndez "*La población está constituida por el número total de personas o elementos que son miembros del grupo, empresa, región, país, u otra forma de asociación humana que se constituye objeto de conocimiento en la investigación* (Mendez C. E., 2011)

Tabla 4 Población

Tabla 5. Descripción de la población

DESCRIPCIÓN	POBLACIÓN
Jueces de garantías penales	8
Fiscales	17
Defensores públicos	8
Abogados en libre ejercicio (Colegiatura)	137
TOTAL	**161**

Elaborado por: Geramy Vera

MUESTRA

La muestra escogida de la población está determinada en un representativo que permite seleccionar la unidad de aplicación de parámetros de estimación de obtención de información necesaria para la comprobación de la idea defendible por lo que la técnica de muestreo es por conveniencia, esta técnica permitirá recoger la información que proporcionaran los datos que aportaran a este proyecto y de la que también esta técnica avala como la selección de los elementos para el cuestionario de la entrevista a elección del investigador y entrevistador por lo que para el presente trabajo de investigación, para efectos de la misma se detallan a continuación.

Tabla 6 Muestreo

Tabla 7. Descripción del muestreo

DESCRIPCIÓN	POBLACIÓN
Jueces de lo penal	1
Fiscales	3
Defensores públicos	1
Abogado en libre ejercicio	1
TOTAL	**6**

Elaborado por: Geramy Vera

3.1.4 MÉTODOS DE INVESTIGACIÓN

MÉTODO ANALÍTICO - DEDUCTIVO

Basándonos en el método que permitirá analizar las variables de este proyecto a partir de la observación de los fenómenos que han llevado al estudio cada una en sus partes como lo expresa el autor Ramón Ruiz

"Aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos.

Así que, mediante el método deductivo, ya que parte de la observación de casos sobre situaciones reales se hará un importante análisis para despejar el banco de interrogantes que el tema permite, así como también alcanzar los objetivos generales y específicos.

Por lo que el presente proyecto de Investigación partirá desde el estudio y análisis de estadísticas generales a nivel nacional otorgadas por la Fiscalía General del Estado, tomando en cuenta que este método deductivo permite realizar el estudio del objeto de investigación desde características generales hasta aspectos muy particulares, en este caso nos permitirá deducir los indicadores principales que conllevan al desarrollo de problemáticas y que se convierten en objeto de estudio dentro de este proyecto de investigación cómo es los delitos informáticos y la

eficacia de la norma en la admisibilidad de la prueba digital para luego relacionarlos y de acuerdo a abordaje de la bibliografía referencial en la que elaboraremos fichas nemotécnicas para direccionar la misma teniendo en cuenta las características de este método por ejemplo que puede ser progresiva y auto correctiva es decir, ira avanzando como también modificándose para que determine la conceptualización de los temas de interés y que en las evidencias del estudio determinar los objetivos así como la comprobación de las variables.

3.1.5 TÉCNICAS E INSTRUMENTACIÓN DE INVESTIGACIÓN

Las técnicas que se utilizaran como instrumento para la recolección de información, permitirá establecer de manera empírica y directa varios fenómenos, los mismos que conlleva a demostrar o no la hipótesis y objetivos planteados dentro de este proyecto de investigación entre ellos describimos los siguientes:

Análisis documental – esta técnica permite que el investigador haga uso sistemático de sus sentidos a través de la revisión de la información documental que se recoge de fuentes primarias y secundarias en dependencia de la utilización y de los datos que el investigador necesite como los de casos existentes, libros, materiales documentales, trabajos de grado, artículos de relevancia informativa, diccionarios, entre otros; en concreto que servirán para conocer aspectos relevantes del objeto de investigación además servirá para presentar los objetivos planteados.

La Entrevista. – mediante este sistema de recolección de información formal y previamente estructurada, orientada directamente a profesionales del derecho y funcionarios de la Función Judicial, permitirá obtener la información estandarizada, sencilla y objetiva requerida para el estudio del objeto de investigación.

3.1.6 TRATAMIENTO DE LA INFORMACIÓN

El presente trabajo de investigación usa métodos de recolección de información a través del análisis de documentación accesible sobre el tema de evidencia digital, y delito informático en el Ecuador y mediante la adquisición de información de libros y artículos científicos que estudian a mayor profundidad el tema en cuestión. Así también se da a conocer la importancia de recopilar los comentarios a través de las entrevistas que permiten conocer la opinión del Juez y fiscales cuyos resultados de la recopilación de información serán plasmados con las respectivas evidencias fotográficas para ser analizado y brindar sustentación al proyecto.

Tabla 4 Operacionalización de Variables

VARIABLES	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS	INSTRUMENTOS
DEPENDIENTE Juzgamiento de los delitos Informáticos	L**os** delitos informáticos son aquellas acciones u omisiones realizadas a través de medios informáticos y electrónicos que son penados por la Ley. (Díaz, 2009)	➢ Normativa ➢ Medidas preventivas ➢ Proceso judicial ➢ Practica tecnológica ➢ Organismos competentes	✓ Código Orgánico Integral Penal ✓ Cautelares, prisión preventiva ✓ Índice de Denuncias ✓ Procesos abiertos ✓ Sentencias ✓ Acreditación de hechos en un proceso judicial ✓ Fiscalía	✓ ¿Qué porcentaje de denuncias existen sobre delitos Informáticos? ✓ ¿Qué causas se han determinado como principales para llevar a un individuo al cometimiento de estos delitos? ✓ ¿Cuántos Procesos llegan a la sentencia?	➢ Guía de Entrevista Estructurada ➢ Observación documental
INDEPENDIENTE La evidencia digital y su admisibilidad	Prueba digital es toda aquella información digital acreditativa de la realidad de un hecho afirmado por las partes y que resulta relevante para el objeto del proceso judicial. (Díaz, 2009)..	➢ Delitos ➢ Medio ➢ Prueba ➢ Infracciones ➢ Consecuencias	✓ Hecho fatico (casos existenciales) ✓ Uso de instrumentos tecnológicos volátiles ✓ La pericia – Nexo Causal ✓ Elementos de afirmación procesal ✓ No identificación del sujeto activo	✓ ¿Con qué frecuencia suceden estos tipos de delitos? ✓ ¿Cuál es el tipo de sanción a los infractores de estos delitos? ✓ ¿La volatilidad de la evidencia producen que los delitos no lleguen en su mayoría a la culminación de los procesos quedando en la impunidad?	➢ Consulta Bibliográfica de la norma penal del Ecuador ➢ Recursos estadísticos

Elaborado por: Geramy Vera

Tabla 8. Operacionalización de Variables

Sistematización

Síntomas	Causas	Efecto
Aumento de delitos informáticos	Fragilidad de los Sistemas Informáticos, telemáticos, electrónicos etc.	Por la volatilidad de la información de contenido digital muchas veces no es posible la identificación del infractor (a)
Manipulación y alteración de la evidencia digital.	No se pude comprobar la integridad del contenido digital	Violación al principio de garantía de la Cadena de custodia.
No se logra identificar la pertinencia y la autenticidad de la evidencia digital	Falta de peritos informáticos calificados	Dilación de los procesos judiciales
Falta de elementos para preservar la evidencia	Falla en la cadena de custodia	Inadmisibilidad de la prueba
Evidencia obtenida sin autorización	Falta de Autorización por autoridades competentes para la explotación y exploración de medios electrónicos para la recolección de la Evidencia digital.	Nulidad del Proceso Judicial

Tabla 9. Sistematización

Elaborado por: Geramy Vera

CAPÍTULO IV: RESULTADOS Y DISCUSIÓN

4.1 ANÁLISIS, INTERPRETACIÓN Y DISCUSIÓN DE RESULTADOS

ENTREVISTA AL DR. JUAN CARLOS AYAR, JUEZ EN LA UNIDAD JUDICIAL PENAL CON SEDE EN EL CANTÓN LA LIBERTAD DE LA PROVINCIA DE SANTA ELENA

1.- ¿De su experiencia como juzgador que referencias tiene acerca de unidades o entidades que están encargadas específicamente de investigar o perseguir delitos informáticos?

El Código Orgánico Integral Penal, ya crea un sistema especializado en investigación, que están a cargo de la Fiscalía, y que ellos pueden realizar técnicas de investigación, o sea que no necesitan ser solicitadas a un juez, sino que directamente al fiscal ordena y ellos hacen estas técnicas de investigación. Obviamente, en derecho, va avanzando y existen nuevas conductas que no están calificadas, por ejemplo, los ciberdelitos o delitos informáticos, que están tipificados de cierta manera, pero no están bien estructurados y todavía no hay la eficacia para poder nosotros, determinar una responsabilidad de quiénes son las personas que cometen este tipo de delitos, entonces sí existe una unidad de delitos informáticos, está creada en la Fiscalía, pero todavía es incipiente, no ha despuntado por ciertos factores.

2.- ¿Considera usted la necesidad de crear o adoptar un instrumento normativo que pueda tipificar todas estas acciones?

El problema es que nosotros no hemos firmado el convenio de Budapest; es justamente el convenio para la para luchar contra los ciberdelitos. Entonces, como no tenemos firmado, a nosotros nos cuesta a todo el sistema de Justicia para poder luchar contra la ciberdelincuencia. Mire que ahora nosotros la las WebDark, que son buscadores como Google, pero estos se buscan para hacer comercios ilícitos, se puede contratar desde pornografía infantil hasta un sicariato. Entonces la pregunta es. ¿Quién es responsable de subir esa información o de dar ese servicio? Si cuando yo puedo contratar hago un

pago por estas nuevas tecnologías, por ejemplo, por PAYPAL o hago una transferencia A X persona o uso western unión, y solo ejecutan el acto o simplemente estas estafas, por ejemplo, a usted le dicen "sabe qué, se le vende un iPhone, en tal cantidad de dinero". Usted cree en esa persona, deposita y pues no le entregan; Pero ¿cuál es el problema de nosotros limitamos? Justamente por esto, porque este protocolo - convenio protocolo de Budapest. ¿Qué es lo que hace? Vamos al ejemplo de que le vendo a usted en un celular, entonces sí, está mi foto, pero ese Facebook fue clonado o fue realizado por otra; Lo máximo que hacen nuestra policía investigativa es solo darle el IP. Este simplemente es en donde se generó información, pero no me dicen a quién pertenece esa cuenta, no me dicen quién creó esa cuenta. Actualmente se oficia a Facebook, preguntando por el link de cuenta y a quién pertenece. Pero ellos dicen, no respondemos porque ustedes no pertenecen al convenio de Budapest o no respondemos y eso se queda ahí, en investigación previa que después se va al archive. En cambio, si nosotros tuviéramos firmado este convenio, este protocolo, ellos mandan toda la información, nos dicen con detalle el lugar donde se creó, quién la creó, porque inclusive nosotros cuando firmamos estas aceptaciones de Facebook e Instagram, todas estas redes sociales nosotros vamos dándole la oportunidad a estas redes de que maneje nuestros datos; Tanto es así, que cuando usted sube fotos usted se está dando una autentificación de su rostro y existe ahorita compañías que venden estos datos de su rostro. Inclusive la FBI ha comprado esta información. Entonces, ellos ya pueden darle toda esta información que necesita de esta cuenta, no pertenece a Juan Carlos Aguilar, pero la creó Pepito Pérez, y le dan toda la información de la descarga y todo lo demás. Entonces, como no tenemos jugado este tipo de convenio es imposible luchar contra delitos informáticos.

3.-Para el convenio de Budapest, el país ha sido invitado para firmarlo, pero ¿de qué depende que Ecuador no se haya adherido?

Bueno, eso ya es un problema que tiene que tomar la Presidencia de la República y también la asamblea que podrían determinar por qué no se firma o nos adherimos el tratado que es muy importante porque se está prolongando la delincuencia acá y la delincuencia ahorita está afectando más al promedio de informáticos. Hay muchos delitos de estafas y que no sabemos a quién sancionar, inclusive si ya afirmamos este protocolo de Budapest. ¿Qué pasa con nosotros? ¿Cómo determinamos quién es el responsable de los delitos que se hagan por esta WEB dark? Si no conozco a esta

persona contra quien me voy. Entonces, pues también tenemos que tener una normativa; si no firmamos esto, por más normativa que creemos, no vamos a poder tener elementos e indicios de comisión para poder juzgar estos delitos y saber quién es el actor directo o actor mediato que hace cometer estos delitos. Y, por ende, también los especialistas en el peritaje. O sea, nosotros podemos tener especialistas del peritaje. Ellos pueden ir, por ejemplo, van a especializarse en Israel, pero al momento de solicitar información a Facebook a WhatsApp no les dan nada. ¿Entonces, de qué sirve que tengamos una plantilla especializada si no tenemos en ese convenio para consignar? Un ejemplo, es como que nosotros no tuviéramos firmado un convenio con Registro Civil. ¿Quiero los datos biométricos de Juan Carlos Vera y no responde nunca, ¿por qué? Porque no tenemos firmado el convenio, así de simple.

4.- ¿Cuáles serían las medidas que usted considera que serían eficaces en la lucha contra estas acciones ilícitas?

Primero, Firmar en los convenios. Segundo, hacer una tipificación real de cómo deberían hacerse a los delitos. Pasa que nosotros tenemos una calificación normativa que es muy ambigua, por ejemplo, le pongo el delito de homicidio, estipula que es la persona que mata a otra, y se acabó. Entonces debe ser más singularizada y especialmente en delitos informáticos; deben estar expertos informáticos al lado de los asambleístas para que en la normativa digan que debe ser detallada de esta manera y que no existan vacíos o lagunas legales que permitan evadir a la justicia y que quede en la impunidad.

6.- ¿El estado ofrece la capacitación a los funcionarios responsables de la aplicación de la legislación contra el delito informático Cibernético y para la obtención de pruebas digitales y electrónicas?

Claro, la normativa esta, es como si tuviera una licencia de conducir, pero no tiene vehículo, entonces de qué le sirve la licencia si no cuenta con el vehículo.

7**.- ¿Cuáles serían sus recomendaciones que usted daría al lector interesado en referente al tema de estudio acerca de la exposición latente que nos encontramos los ciudadanos ante esta problemática?**

No tenemos todavía doctrina especializada en delitos informáticos, no tenemos la doctrina que nos digan cómo determinar la autoría o participación en un delito. Por

ejemplo, nosotros tenemos la teoría del autor mediato o el hombre de atrás, sea por instigación, el flujo cíclico. Entonces por instigación, yo le digo que A mate a B. Yo soy el autor mediato, necesito un instrumento, la persona A. Ahora si logro determinar qué A es instrumento mío y que actuó como instrumento con instigación y mato a B. A no tiene responsabilidad y la responsabilidad es mía. Entonces para culpabilidad existen dos teorías, la teoría del dominio de derecho y la teoría de infracción de deber. Por eso se creó esta teoría para los juicios de newbern para poder condenar a estas personas. Pero el problema es. ¿Cómo aplicamos la teoría del dominio del derecho? Sí, si no sabemos quién es el que subió esa información o quién hizo esa estafa. Sí y, además, esta web dark es oculta. Usted tiene que saber buscar y llegar a mí. ¿Cómo aplico la teoría de infracciones que deber?, o sea ninguna de las dos teorías podría aplicar. Entonces tendríamos que normativamente ver y crear alguna forma u otra teoría para poder juzgar a estas personas que están detrás de estas redes ocultas que no dan la cara y saber cómo poder sancionar.

ENTREVISTA A FISCALES

ENTREVISTA AL AB. WAGNER SAMUEL ZAMBRANO – FISCALIA 1

1.- Señor fiscal por la experiencia que le amerita ¿conoce usted acerca de los casos del informático que se han suscitado en la localidad y de por ende en esta Fiscalía?

Aquí el delito informático existe poco, ya que esta provincia no tenemos peritos en el Consejo de la altura ni la Policía Nacional que se han realizado en esa área. Pero si podemos solicitar peritos informáticos de otras localidades como Guayaquil o en Quito o cualquier parte del territorio ecuatoriano que puedan realizar aquella pericia informática en casos de ser necesario.

2.- ¿Cuáles serían las medidas que usted considera que serían eficaces en la lucha contra los delitos informáticos?

Obtener una información, la base del disco duro donde se haya grabado la información, en cuanto el IP de la computadora, porque siempre se haya un registro de un de un equipo electrónico donde se ha realizado aquella transacción económica o aquel envío de las fotografías de las redes sociales, ahí podría entrar el perito informático donde podría determinar a qué computadora o teléfono celular corresponde ese email o ese IP.

3**.- En cuanto a la evidencia, considerando que la información-evidencia, siendo volátil y vulnerable, ¿cómo es el tratamiento de la misma?**

En primicia se tiene que incautar el equipo tecnológico para de esa manera, evitar que sea manipulado y pues, y de esa manera ser periciado para obtener información requerida, ya sea a través de la unidad de análisis financiero, la wifi, a través de la unidad especializada con las conductas, la pornografía, trata de personas para delito de sustracción de bienes públicos o privados a través de las redes sociales, entre otras cosas. Pues para precautelar el hecho, tendríamos que incautar el equipo tecnológico.

4**.- Si partimos del Principio del Derecho Romano "No hay Crimen, no hay pena, sin previa ley" y considerando que las técnicas que se utilizan para el cometimiento de los delitos informáticos varían y cada vez son nuevos; ¿Considera usted que nuestra legislación es suficiente para el juzgamiento de estos delitos?**

Hay muchos que no están tipificados literalmente, pero hay otros delitos que subsumen, como, por ejemplo, está el artículo 186, que habla de la estafa, el numeral sexto, sino más bien recuerdo, que establece sobre una situación a través de una parte electrónica; está ya subsumiendo el delito de utilización de medios tecnológicos.

5.- **¿Considera que es necesario un nuevo instrumento normativo que tipifique todas las acciones dolosas y hechos punibles referentes al delito informático y cibercrimen que dañan el bien o bienes jurídicos?**

Necesitamos personal capacitado, en primera instancia para poder determinar cuáles son ahorita que pueden este originarse de un hecho en sí. Porque un delito o un hecho realizado por una persona puede acarrear uno o varios delitos que primero tiene que ser analizada por personal capacitado y especializado, para luego determinar la creación de un nuevo instrumento normativo.

6.- **¿Y, basado en su experiencia como jurista, conoce usted la existencia de jurisprudencia sobre la admisibilidad de la evidencia digital o electrónica que haya aportado alguna resolución en el caso de delitos?**

En doctrina ecuatoriana desconozco, en doctrina internacional, existen varias por cuanto la legislación en otro país es tan diferente y mucho más avanzada en la parte de tipificación o analizando delitos.

7.- **Con el convenio de Budapest, el cual Ecuador no se ha adherido todavía. ¿Considera que debería adherirse?**

Exactamente, deberíamos de adherirnos por cuanto sería beneficioso, no solamente para los estudiantes de derecho, para la persona de derecho, sino para la ciudadanía en general quiénes se beneficiarían de los conocimientos que ya han partido de otras sociedades y han servido de experiencia para poder tipificar el delito en sí.

8.- **¿Cuáles serían sus recomendaciones para el lector interesado en referente al tema de estudio acerca de la exposición latente que se encuentra en los ciudadanos ante esta problemática?**

Capacitación personal para poder realizar pericias inherentes a este delito.

ENTREVISTA AL AB. CARLOS SANTIAGO CARGUA CARPIO - FISCALÍA 3

1.- **Con la experiencia que le amerita, ¿Conoce usted casos de delitos informáticos que se hayan suscitado en esta localidad?**

No, no conozco

2.- **¿Considera usted que es necesario la creación de un nuevo instrumento normativo que tipifique todas estas acciones dolosas a profundidad o hechos punibles de referente al delito que dañen un bien jurídico?**

Primero se debería capacitar y que existan los peritos expertos que puedan determinar de que ese tipo de conductas revestidas de dolo, en conciencia y voluntad, tiende de alguna forma lesionar un bien jurídico; entonces, luego de que se haga ese tipo de capacitación, debería incluirse en el catálogo de delitos algunos de esos especiales a los que usted refiere, porque de lo contrario si se hace al revés, tendríamos un tipo penal pero en realidad no tendríamos la capacidad física, pericial para poder demostrar que esa conducta es típica, es antijurídica y también la culpabilidad.

3**.- ¿Cuál es su opinión acerca de la falta de especialistas en herramientas en investigación y recuperación de información para los delitos informáticos en el Ecuador?**

Es un problema específico del Estado; es el Estado ecuatoriano que debería encargarse de capacitar a profesionales en ese tipo de áreas específicamente; No existe, usted dice, es muy, muy escaso, es limitado.

4.- **Y basado en su experiencia como jurista ¿conoce la existencia de jurisprudencia sobre la admisibilidad de evidencia digital o electrónica que hayan aportado alguna resolución y para los casos de delitos informáticos que hemos mencionado?**

Muy poco, muy poco se ha visto que en esa especificidad de los temas que usted refiere.

5.- **Para el lector interesado, referente al tema que el ciudadano se encuentra esta problemática. ¿Cuáles serían sus recomendaciones acerca de esta problemática?**

Ser un poco más celoso respecto del acceso que uno permite al público, de la información personal de uno. Debe ser celoso respecto de lo que uno tiene, lo que uno hace, los lugares que frecuenta, o hacer saber las personas que son más cercanas al núcleo familiar; esa información es la aprovechada por la delincuencia para poder cometer algún tipo de extorsión, algún tipo de ilícitos; entonces, mi recomendación al lector es esa, ser un poco más celoso como la información de uno, que siendo personal decide a veces hacerla pública en redes sociales. Eso no debe ocurrir.

ENTREVISTA AL AB. JOHN TIPANTASI TAIPE – FISCALÍA 5

¿Señor fiscal por su experiencia, conoce usted algún caso de derecho informático que se ha solicitado en esta localidad?

Sí, en efecto, fiscalía como titular la Acción Penal Pública es dueña de la investigación, según un mandato constitucional del artículo 194 de la carta magna, la Fiscalía tiene el deber de investigar los delitos que se cometen en esta jurisdicción, que son competencia más que todo de la Fiscalía de la provincia de Santa Elena. Y efectivamente, sí se han conocido varios casos de delitos informáticos, sobre todo en los delitos de sustracción de dineros a través de cuentas corrientes, a través de hackeo de cuentas o a veces también por la información que los mismos usuarios o clientes de las instituciones bancarias les proveen a personas que se encuentran dedicadas a estas actividades. Y eso ha sido básicamente uno de los mayores casos en ese sentido de delitos informáticos. Por ejemplo, también un delito psicopático se puede considerar también lo de los que se realizan a través de creación de perfiles falsos, para parecer como una persona que no es...

¿Cómo se da el delito de suplantación de identidad estipulado en el COIP referente al uso de medios electrónicos e informáticos?

Podría entender como una suplantación de una identidad, haciendo que estas personas ofrecen servicios de carácter sexual o servicios como préstamos bancarios, cosas así. Entonces, hay otros que también, como, por ejemplo, suelen crear todos perfiles falsos para subir imágenes con contenido sexual de personas que tienen algún conflicto entre ellos y obviamente, pues la única evidencia que queda es de los IP, de dónde se crea

estas cuentas. Y ha sido un poco complicado esto en el avance de la investigación, porque la única quien debe de proveer de esta información, en la que nosotros remitimos, es a la misma cuenta o red de plataforma social, en este caso, usualmente es Facebook, que queda en Estados Unidos, entonces hay que hacerlo a través de un correo y entiendo que a nivel mundial vendrán tantos casos, entonces es bastante complicado recibir una respuesta de parte de ellos, porque en esa información que se solicita se tiene que pedir el IP, el nombre de la persona, lugares quizás de donde se crearon estos perfiles

¿Considera usted que la información que se obtiene en estos medios es volátil, pudiendo originar el anquilosamiento en cuanto al proceso que se lleva para el juzgamiento de este delito?

Obviamente, porque usualmente la mayoría de estos casos no es que la persona presta voluntariamente en su imagen un contenido íntimo para que le suban a una red social, sino que más bien muchas veces son mal utilizadas, mal utilizadas por personas que tienen acceso a ellos. Por ejemplo, en el caso de una relación extra marital, la esposa le encuentra en el teléfono las imágenes de su pareja y en represalia a esta relación, la suena efectiva. Otra puede ser el que, a través de una sustracción de un aparato electrónico en un celular, obviamente tienen acceso a imágenes que tienen las personas de manera íntima o personal para el uso de ello, pero se hacen virales cuando tienen acceso, obviamente.

Y si una denuncia, que aquí pueden, obtiene la denuncia, ¿No?, ¿Verdad?, denuncia y ya para el proceso, ya para llegar al momento, toda esa información, ¿se vulneras, se borra, se elimina? ¿Cómo resuelven esos casos de sangre? ¿Qué sería necesario?

Ahí va a ser imposible, por ejemplo, si sabemos que estas imágenes, porque según las víctimas, dicen no, sí, esas, efectivamente, yo esas imágenes tenía en mi teléfono, pero se me perdió, se me robaron, pero al no haber, en este caso, el teléfono, no se puede, por ejemplo, levantar una calle en la custodia, en relación a de dónde salieron estas imágenes, sino que únicamente nuevamente se remiten a donde reposaban o de donde reposan, que es usualmente un usuario de Facebook.

4.2 VERIFICACIÓN DE LA IDEA A DEFENDER

Sobre la idea planteada en el presente trabajo de investigación y habiendo usado los instrumentos de análisis documental y la entrevista para la recopilación de la información necesaria de la que en respuesta se comprueba la hipótesis que determina que falta de expertos en pericia digital genera un problema que afecta la eficacia del tratamiento de la evidencia en el sistema penal. Esto implica que en muchos casos en los que se suscita una acción típica y antijurídica respecto al tema no las víctimas no realizan las respectivas denuncias o si lo hacen ante los entes de justicia penal, éstas no cuentan con personal capacitado para realizar las investigaciones necesarias, afectando de esta manera el derecho de las personas que puedan garantizar el manejo adecuado de la prueba y su admisión eficaz en los procedimientos judiciales.

CONCLUSIONES

La falta de peritos acreditados en herramientas de recuperación de información para los casos de delitos informáticos en el Ecuador puede tener varios impactos negativos en el proceso de investigación y en la resolución de estos casos

Que existe dificultad en la recolección y preservación de evidencia: Los delitos informáticos suelen dejar una huella digital, pero sin peritos capacitados, la recolección adecuada y la preservación de la evidencia digital pueden verse comprometidas. Esto podría llevar a la pérdida de pruebas cruciales y dificultar la identificación y captura de los perpetradores.

Que los peritos en informática forense están capacitados para analizar y examinar la evidencia digital de manera forense. Sin su conocimiento y experiencia, las pruebas digitales pueden no ser examinadas adecuadamente, lo que lleva a conclusiones inexactas o incompletas.

Que la evidencia digital debe ser presentada adecuadamente en un tribunal para ser considerada válida y admisible. Sin peritos acreditados en herramientas de

recuperación de información y análisis forense, la defensa podría impugnar la validez de la evidencia, lo que afectaría la fuerza del caso.

Que la falta de expertos en informática forense podría dificultar la identificación y persecución de los delincuentes digitales. Esto podría llevar a un aumento de la impunidad en los casos de delitos informáticos, ya que los culpables no logran ser detectados ni responsabilizados.

Que, sin peritos capacitados, las investigaciones de delitos informáticos podrían prolongarse innecesariamente, lo que retrasaría la resolución de los casos y frustraría a las víctimas y a la sociedad en general.

RECOMENDACIONES

Es fundamental asegurar la integridad de la evidencia digital desde el momento de su obtención hasta su presentación en el tribunal. La cadena de custodia debe estar debidamente documentada, indicando quién tuvo acceso a la prueba, cuándo y con qué propósito. Esto asegura que la evidencia no sea alterada o contaminada y permite establecer su autenticidad, pero toda esta información se obtiene bajo un debido sistema especializado y capacitado para el uso de las técnicas y herramientas que concluyan la resolución de los casos de sanciones de los delitos tipificados en la normativa vigente, por lo tanto, se realiza las siguientes recomendaciones:

Utilización de técnicas forenses, importante que la obtención y el análisis de la evidencia digital se realicen mediante técnicas forenses adecuadas. Esto implica utilizar herramientas y métodos específicos para preservar la evidencia sin modificarla y garantizar la obtención de resultados precisos y confiables. Es esencial establecer la autenticidad de la evidencia digital presentada. Esto puede lograrse mediante la identificación y validación de la fuente de la evidencia, asegurando que no haya sido manipulada o alterada.

La evidencia digital presentada debe ser relevante y pertinente para el caso en cuestión. Debe estar directamente relacionada con los hechos bajo investigación y ser capaz de demostrar o refutar la existencia de un delito informático.

La evidencia digital debe ser obtenida de manera legal y respetando los derechos y garantías de los individuos involucrados. La obtención de pruebas mediante actividades ilícitas o violatorias de la privacidad puede hacer que la evidencia sea inadmisible.

Y por ende la actualización constante del área de la tecnología y las técnicas forenses digitales evolucionan constantemente. Es esencial que los profesionales involucrados en la gestión de pruebas digitales se mantengan actualizados en cuanto a las últimas tendencias y avances en el campo. Esto puede posibilitarse a través de la firma de convenios o tratados de cooperación internacional, luego, tener un personal capacitado que pueda determinar el tipo de delito que se pueda originar de un hecho en sí; es decir, capacitar para que existan peritos expertos que puedan determinar que un tipo de conductas revestidas de dolo que a conciencia y voluntad tiende de alguna forma lesionar un bien jurídico.

Al seguir estas recomendaciones, se puede aumentar significativamente la probabilidad de que la evidencia digital sea admitida como prueba en el juzgamiento de los delitos informáticos, lo que contribuye a un proceso judicial más justo y efectivo.

ANEXOS – evidencias fotográficas

Imagen 1. Entrevista al Dr. Juan Carlos Ayar, juez en la Unidad Judicial Penal con sede en el cantón La Libertad de la provincia de Santa Elena

Imagen 2Entrevista al Ab. John Tipantasi Taipe – Fiscalía 5.

Imagen 3. Entrevista al Ab. Wagner Samuel Zambrano – Fiscalía 1

Imagen 4 Entrevista al Ab. Santiago Cargua – Fiscalía 3.

INSTRUMENTO DE ENTREVISTA DIRIGIDA AL DR. JUAN CARLOS AYAR, JUEZ EN LA UNIDAD JUDICIAL PENAL CON SEDE EN EL CANTÓN LA LIBERTAD DE LA PROVINCIA DE SANTA ELENA

1.- ¿De su experiencia como juzgador que referencias tiene acerca de unidades o entidades que están encargadas específicamente de investigar o perseguir delitos informáticos?

2.- ¿Considera usted la necesidad de crear o adoptar un instrumento normativo que pueda tipificar todas estas acciones?

3.-Para el convenio de Budapest, el país ha sido invitado para firmarlo, pero ¿de qué depende que Ecuador no se haya adherido?

4.- ¿Cuáles serían las medidas que usted considera que serían eficaces en la lucha contra estas acciones ilícitas?

6.- ¿El estado ofrece la capacitación a los funcionarios responsables de la aplicación de la legislación contra el delito informático Cibernético y para la obtención de pruebas digitales y electrónicas?

7.- ¿Cuáles serían sus recomendaciones que usted daría al lector interesado en referente al tema de estudio acerca de la exposición latente que nos encontramos los ciudadanos ante esta problemática?

INSTRUMENTO DE ENTREVISTA DIRIGIDA A LOS SRES. FISCALES DE SANTA ELENA

1.- Señor Fiscal, por la experiencia que le amerita, ¿Conoce usted casos de delitos informáticos que se hayan suscitado en esta localidad?

2.- **¿**Considera usted que es necesario la creación de un nuevo instrumento normativo que tipifique todas estas acciones dolosas a profundidad o hechos punibles de referente al delito que dañen un bien jurídico?

3**.-** ¿Cuál es su opinión acerca de la falta de especialistas en herramientas en investigación y recuperación de información para los delitos informáticos en el Ecuador?

4.- Si partimos del Principio del Derecho Romano "No hay Crimen, no hay pena, sin previa ley" y considerando que las técnicas que se utilizan para el cometimiento de los delitos informáticos varían y cada vez son nuevos; ¿Considera usted que nuestra legislación es suficiente para el juzgamiento de estos delitos?

5.- Y basado en su experiencia como jurista ¿conoce la existencia de jurisprudencia sobre la admisibilidad de evidencia digital o electrónica que hayan aportado alguna resolución y para los casos de delitos informáticos que hemos mencionado?

6.- ¿Considera usted que la información que se obtiene en estos medios es volátil, pudiendo originar el anquilosamiento en cuanto al proceso que se lleva para el juzgamiento de este delito?

7.- Para el lector interesado, referente al tema que el ciudadano se encuentra esta problemática. ¿Cuáles serían sus recomendaciones acerca de esta problemática?

BIBLIOGRAFÍA

(ANT), A. N. (Octubre de 2021). Fiscalía investiga ataque cibernético a sistema informático de la ANT. *Actualidad*. (A. Rosero, Entrevistador) QUITO: EL COMERCIO. Obtenido de https://www.elcomercio.com/actualidad/seguridad/fiscalia-investigacion-ataque-cibernetico-ant.html

180, R. O. (2014). *Codigo Orgánico Integral Penal.* Quito, Ecuador.

(19 de Septiembre de 2019). Obtenido de Primicias.ec: https://www.primicias.ec/noticias/tecnologia/estos-delitos-informaticos-mas-recurrentes-ecuador/

449, R. o. (2008). Quito.

449, R. O. (2008). *Constitución de la República del Ecuador.* Quito, Ecuador.

544, R. O. (2009). *Código Orgánico de la Función Judicial.* Quito, Ecuador.

BANCO PICHINCHA. (Abril de 2021). *Ciberseguridad , Riesgos de seguridad , Estafa*. Obtenido de Pharming: qué debes hacer cuando los ciberdelincuentes se convierten en "granjeros": https://www.pichincha.com/portal/blog/post/ataque-pharming

Cabanellas, G. (1993). *Diccionario Jurídico Elemental* . Editorial Heliasta S.R.L .

Chavez, J. (Febrero de 2023). ¿Qué es un Sistema informático? Componentes, características y ejemplos. Obtenido de https://www.ceupe.com/blog/sistema-informatico.html

Ciencia Digital. (enero - marzo de 2019). Obtenido de file:///C:/Users/Acer/Downloads/364-Texto%20del%20art%C3%ADculo-1493-4-10-20190318.pdf

COIP_act_feb-2021.pdf. (10 de febrero de 2014). Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Consejo de la Judicatura del Ecuador. (2008). En *Codigo Organico Integral Penal del Ecuador.*

Coordinadores: Ricardo Oliva león, Sonsoles Valero Barceló. (2016). *La prueba Electronica, Validez y Eficacia Procesal.* Obtenido de Juristas futuro.com: https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf

Coronel Añazco, M. D. (2020). *"LA REVELACIÓN ILEGAL DE BASE DE DATOS EN EL DERECHO COMPARADO".* Universidad Catolica de Cuenca, UNIDAD ACADÉMICA DE CIENCIAS SOCIALES, La Troncal. Obtenido de https://dspace.ucacue.edu.ec/handle/ucacue/9978

defensa.gob.ec. (10 de Febrero de 2014). Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Delgado, M. L. (2da Edicion, 2007). *Analisis Forense Digital.* GNU Free Documentation License.

Delito Informatico. Procedimiento Penal en Ecuador. (2016). *Revista Científica*, 12. Obtenido de https://dominiodelasciencias.com/ojs/index.php/es/article/viewFile/159/pdf

Dialnet. (2022). Sitio Web del derecho a la privacidad y a la intimidad en el contexto de la interceptación de las comunicaciones en el Ecuador. En G. H. Sarmiento Vallejo. Serie Científica de la Universidad de las Ciencias Informáticas. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8590735

Díaz, L. H. (2009). *El Delito Informático.* San Sebastián: EGUZKILORE.

El Diario.ec. (09 de Julio de 2017). Obtenido de https://www.eldiario.ec/noticias-manabi-ecuador/440641-4-delitos-informaticos-causan-alerta/

el telegrafo. (16 de 08 de 2016). Obtenido de el telegrafo: https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

El Telégrafo, Ecuador. (16 de Marzo de 2001). Obtenido de https://www.eltelegrafo.com.ec/noticias/judicial/12/en-guayas-39-personas-fueron-victimas-de-delitos-informaticos

EL UNIVERSO. (Mayo de 2021). EL UNIVERSO. *Más de 600 denuncias por delitos cibernéticos*. Obtenido de https://www.eluniverso.com/noticias/seguridad/mas-de-600-denuncias-por-delitos-ciberneticos-se-han-registrado-en-ecuador-en-lo-que-va-del-2021-nota/

el universo.com. (27 de septiembre de 2020). Obtenido de https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador/

Falconí, G. (2015). *El tiempo.com.ec*.

FGE. (2022). *RESOLUCION N. 61 - FGE2022.* FISCALIA GENERAL DEL ESTADO, QUITO. Obtenido de https://www.fiscalia.gob.ec/transparencia/2022/octubre/a3/RESOLUCION-061-FGE-2022.pdf

FGE. (MARZO de 2023). *FISCALIA GENERAL DEL ESTADO - BOLETINES*. Obtenido de Fiscalía obtiene sentencia por los delitos de acceso no consentido a un sistema informático, telemático o de telecomunicaciones y revelación ilegal de base de datos: https://www.fiscalia.gob.ec/fiscalia-obtiene-sentencia-por-los-delitos-de-acceso-no-consentido-a-un-sistema-

informatico-telematico-o-de-telecomunicaciones-y-revelacion-ilegal-de-base-de-datos/

Garea, E. (Octubre de 2022). *Conversia*. Obtenido de ¿SABES LO QUE ES EL PHARMING Y EN QUÉ SE DIFERENCIA DEL PHISHING?: https://www.consultoria-conversia.es/ciberseguridad/sabes-lo-que-es-el-pharming-y-en-que-se-diferencia-del-phishing/

Hernandez, R., Fernandez, C., & Baptista, P. (2010). *Metodología de la Investigación.* México: Interamericana Editores S.A. DE C.V.

Imbaquingo Narváez, I. E. (2019). *Derecho Informatico y Nuevas Tecnologias de la Información.* Ibarra, Ecuador: UTN (Universidad Tecnica del Norte).

Mayer Lux, L., & Calderón, G. O. (2020). *El delito de fraude informático: concepto y delimitación.* Pontificia Universidad Católica de Valparaíso. Santiago: Revista Chilena de Derecho y tecnología. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

Méndez, C. (s.f.). p.231.

Mendez, C. (2011). *Metodología de la Investigación.* Mexico: LIMUSA.

Mendez, C. E. (2011). Metodología, Diseño y desarrolo del proceso de investigacion. México D.F.: Limusa S.A.

Miguel, L. D. (2da Edición 2007). *"Analisis Forense Digital".* Obtenido de https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

ONU, U. I.-S. (2020). *ITUPublicaciones.* Obtenido de Índice Mundial de Ciberseguridad: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

Panda Security. (Septiembre de 2022). *Mobile News - Security*. Obtenido de ¿Qué es el pharming? Definición y formas de prevenirlo: https://www.pandasecurity.com/es/mediacenter/seguridad/pharming/#:~:text=Mientras%20que%20el%20phishing%20implica,web%20falsos%20sin%20siquiera%20saberlo.

Peñaranda Quintero, H. R. (2002). Nociones generales acerca de la cibern{etica y la iuscibernética. *revista Chilena de Derecho Informático N°1*.

Peñaranda Quintero, H. R. (2002). Nociones generales acerca de la cibernética y la iuscibernética. *Revista Chilena de Derecho Informatico*.

PRIMICIAS. (Mayo de 2021). *Primicias - Política*. Obtenido de Protección de la intimidad o censura: polémica por reformas al COIP: https://www.primicias.ec/noticias/politica/proteccion-intimidad-censura-reformas-coip/

RAE. (2023). *Diccionario Panhispanico del español juridico*. Obtenido de Interceptación de comunicaciones: https://dpej.rae.es/lema/interceptaci%C3%B3n-de-comunicaciones

Revista chilena de derecho. (abril de 2017). *Revista chilena de derecho*. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011

Rivera, V. I. (11 de octubre de 2021). Obtenido de https://sistemasjudiciales.org/wp-content/uploads/2021/10/11.-SJ24.-Neptune-Rivera.pdf

Rivera, V. I. (11 de 10 de 2021). *PDF*. Obtenido de PDF: (https://sistemasjudiciales.org/wp-content/uploads/2021/10/11.-SJ24.-Neptune-Rivera.pdf

Ruiz, R. (2007). Obtenido de https://es.slideshare.net/recursostics/el-mtodo-cientfico-y-sus-etapas-ramn-ruiz-mxico-2007-9039882

Sain, G. R. (2012). *Delito y nuevas tecnologías Fraude, narcotráfico y lavado de dinero por Internet* . Editores del Puerto.

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). *Análisis conceptual del delito informático en Ecuador.* Universidad Regional Autónoma de Los Andes. Ecuador. Scielo. Obtenido de http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext

Sanchez, C. (20 de octubre de 2021). Obtenido de https://www.sanchezgarridoabogados.com/evidencias-digitales-forenses/

UNIANDES. (2018). LA VIOLACIÓN A LA INTIMIDAD SEGÚN EL CÓDIGO ORGÁNICO. En S. BRAVO URRUTIA. Babahoyo. Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/9178