Universidad Tecnológica ECOTEC

Derecho y Gobernabilidad

Título del trabajo:

La aplicación de la cadena de custodia y su incidencia en la prueba digital dentro de los delitos informáticos en la legislación ecuatoriana.

Línea de investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Trabajo de Investigación

Carrera:

Derecho con énfasis en Ciencias Penales y Criminológicas

Título a Obtener:

Abogado

Autor:

Rashell Eilyn Vinces Alaña.

Tutor:

Ab. Jaime Albán Mariscal, Mgtr.

Samborondón, Ecuador

2023

DEDICATORIA

Este trabajo deseo dedicárselo a mis papas quienes son mis bases para seguir adelante, han tomado mi mano en todo el camino, enseñándome que todo lo que vale la pena merece mi esfuerzo. He visto cada sacrificio que ha realizado por mí, es por eso que este logro es también suyo.

A mis pequeños hermanos, Ashley y Liam, porque son mi motivo para alcanzar mis sueños, demostrarles que todo es posible con perseverancia y dedicación. Los amo con todo mi corazón, no habría podido continuar sin ustedes a mi lado.

A mis abuelos, Kleber, Olga, César y Elena, por ser mis segundos papás, he visto el alcance de su amor hacia mí y no me queda más que siempre estar agradecida con cada uno de ustedes. Gracias por siempre estar.

A mi familia, en especial a mis tíos, personas que han depositado su amor y confianza en mí, mucho de lo que soy es por ustedes.

A mi vita Luz, quien estuvo esperando pacientemente que terminara mi carrera universitaria, me llenó de consejos y ánimos siempre que no tenía fuerzas para avanzar; y aunque no estés físicamente junto a mí, sé que me estas cuidando desde el cielo. Te extraño mucho.

A mi enamorado, José Arturo, por ser mi compañero de vida, por ayudarme y darme palabras de aliento cuando todo se tornaba oscuro, gracias por ser luz. Te amo.

Rashell Eilyn Vinces Alaña.

AGRADECIMIENTO

Quiero expresar mis agradecimientos a Dios, por permitirme llegar a este momento, gracias por las fuerzas que colocaste en mí siempre que quise renunciar y por mostrarme otro camino para continuar.

A mi familia, por estar siempre pendiente de cada uno de mis procesos, por festejar mis logros y darme aliento en mis fracasos.

A mis grandes amigos, Jeremías, Gabriela y Pedro, gracias por hacer estos años más amenos, gracias por brindarme su amistad, los quiero mucho.

A mis amigas de carrera, Cristel, Sasha y Anggie, por todo el apoyo y los momentos compartidos. Espero verlas pronto colegas.

Por último quiero agradecer a cada uno de los grandes docentes que tuve, gracias por sus conocimientos y confianza otorgada.

Rashell Eilyn Vinces Alaña.

CERTIFICADO DE REVISIÓN FINAL

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

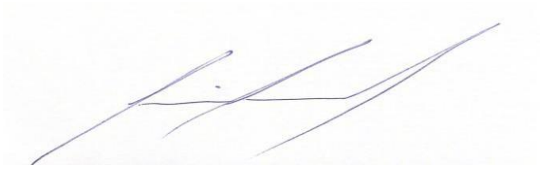
Samborondón, 03 de agosto de 2023

Magíster
Andrés Madero Poveda
Decano(a) de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: *"Aplicación de la cadena de custodia y su incidencia en la prueba digital dentro de los delitos informáticos en la legislación ecuatoriana"* según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **RASHELL EILYN VINCES ALAÑA,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,



Mgtr. Jaime Vicente Albán Mariscal.

Tutor(a)

CERTIFICADO DE PORCENTAJE DE PLAGIO

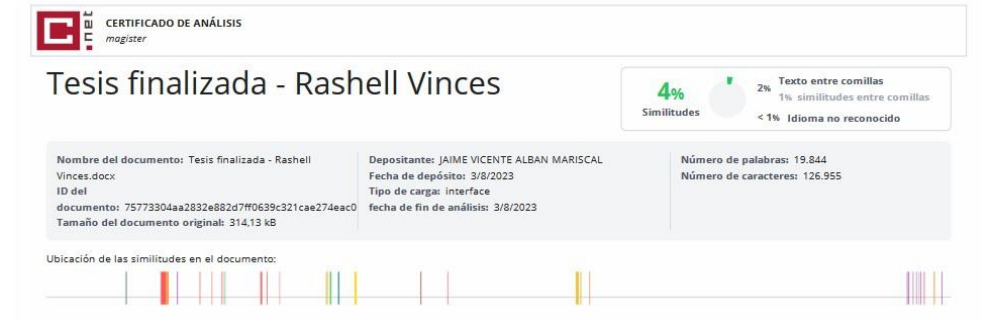
ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado JAIME VICENTE ALBAN MARISCAL, tutor del trabajo de titulación *"Aplicación de la cadena de custodia y su incidencia en la prueba digital dentro de los delitos informáticos en la legislación ecuatoriana"* elaborado por RASHELL EILYN VINCES ALAÑA, con mi respectiva supervisión como requerimiento parcial para la obtención del título de ABOGADO.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias (4%) mismo que se puede verificar en el siguiente link:

https://app.compilatio.net/v5/report/ce69ee23c9c8cc4c6a25c2d3d07729bf8cb84a70/sources. Adicional se adjunta print de pantalla de dicho resultado.



_____

FIRMA DEL TUTOR

JAIME VICENTE ALBAN MARISCAL.

RESUMEN

En el presente trabajo de investigación llamado “La aplicación de la cadena de custodia y su incidencia en la prueba digital dentro de los delitos informáticos en la legislación ecuatoriana”, su objetivo principal es determinar el alcance en el ordenamiento jurídico acerca de la cadena de custodia con respecto a la prueba digital dentro de los delitos informáticos.

Con el fin de cumplir con los objetivos planteados en este proyecto investigativo, se realizó un análisis de alcance descriptivo, exploratorio y explicativo acompañado de un enfoque cualitativo, empleando técnicas como estudio de la información existentes de normativa y doctrina, derecho comparado y el uso de herramientas de recolección de datos como entrevistas.

Para establecer conceptos y generalidades sobre los temas principales a tratar, se inició con el estudio de normativa y doctrina local con la finalidad de indicar si el desarrollo de la normativa ecuatoriana con respecto al resguardo de la prueba digital dentro de la cadena de custodia es efectivo. De manera concisa, se revisó el Código Orgánico Integral Penal, en los articulados donde se menciona la cadena de custodia y la evidencia digital, además de reglamentos internos sobre la Cadena de Custodia. De igual forma, al ser un tema de investigación muy poco abordado, se realizó un estudio de derecho comparado con otras legislaciones para determinar si existe un desarrollo adecuado en el sistema investigativo sobre los delitos informáticos y comprobar la existencia de falencias en el sistema investigativo con respecto a los medios probatorios en el ámbito digital.

Con la información recolectada por medio de la entrevista, se pudo obtener los diferentes puntos de vistas de profesionales del Derecho y Criminalística, en los que se evidencio que la mayor falencia en el sistema investigativo es la falta de una reglamentación detallada sobre los procedimientos de tratamiento de la evidencia

digital dentro de la cadena de custodia, lo que da como resultado que la cadena de custodia no cumpla con su finalidad.

Con los resultados obtenidos de los métodos de investigación y el estudio de la normativa, se concluyó que Ecuador no cuenta con una legislación desarrollada con respecto al sistema investigativo en los delitos informáticos, generando que, en muchos casos, estas evidencias no formen parte del proceso penal por no poder asegurar la cadena de custodia.

Palabras claves: Cadena de custodia, delitos informáticos, evidencias digitales, técnicas periciales.

ABSTRACT

In the present research work called "The application of the chain of custody and its incidence in digital evidence within computer crimes in Ecuadorian legislation", its main objective is to determine the scope in the legal system about the chain of custody with respect to digital evidence within computer crimes.

In order to meet the objectives, set out in this research project, an analysis of descriptive, exploratory and explanatory scope was carried out accompanied by a qualitative approach, using techniques such as the study of existing information on regulations and doctrine, comparative law and the use of data collection tools such as interviews.

In order to establish concepts and generalities on the main issues to be discussed, the study of local regulations and doctrine began with the purpose of indicating whether the development of Ecuadorian regulations regarding the protection of digital evidence within the chain of custody is effective. In a concise manner, the Comprehensive Organic Criminal Code was reviewed, in the articles where the chain of custody and digital evidence are mentioned, as well as internal regulations on the Chain of Custody. In the same way, since it is a research topic that is rarely addressed, a law study was carried out compared with other legislations to determine if there is an adequate development in the investigative system on computer crimes and to verify the existence of shortcomings in the investigative system with regarding the means of evidence in the digital field.

With the information collected through the interview, it was possible to obtain the different points of view of Law and Criminalistics professionals, in which it was evidenced that the greatest flaw in the investigative system is the lack of detailed regulations on treatment procedures. of digital evidence within the chain of custody, resulting in the chain of custody failing its purpose.

With the results obtained from the research methods and the study of the regulations, it was concluded that Ecuador does not have legislation developed regarding the investigative system in computer crimes, generating that, in many cases, this evidence is not part of the criminal process. for not being able to ensure the chain of custody.

Keywords: Chain of custody, computer crimes, digital evidence, expert techniques.

ÍNDICE

INTRODUCCIÓN

La cadena de custodia es un conjunto de procedimientos ordenados y minuciosos, que se encargan de la correcta preservación de los indicios que fueron encontrados y recolectados. La finalidad de este proceso es garantizar la veracidad de la prueba y esto se realizará desde el primer paso que es la recolección de evidencias. Se entiende que bajo este proceso la prueba no debe modificarse y continuará con el grado de validez requerido en un proceso penal.

Esta cadena de custodia es llevada a cabo por el Departamento Policial, esto son los agentes de la Policía Judicial, delegados de la Fiscalía General del Estado.

Actualmente en nuestro Código Orgánico Integral Penal (2014) no existe normas concisas que regulen la cadena de custodia por lo que debemos guiarnos o regirnos en la doctrina del sistema criminalística, lo que genera una aplicación no uniforme del procedimiento y crea falencias el cual afecta la validez de la cadena de custodia.

Los delitos informáticos tienen gran relevancia en el ámbito jurídico debido a que las nuevas tecnologías han revolucionado completamente la sociedad, se considera que se vive en una era completamente digital. El internet es la máxima expresión de desarrollo en esta era y gracias al mismo se han creado nuevas formas para delinquir por medios electrónicos o informáticos.

El Convenio de Ciberdelincuencia del Consejo de Europa (2004) establece que “los delitos informáticos son los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos” (pág. 23)

Como se estudia en la doctrina hay algunos delitos que nacen siendo delitos informáticos, es decir que son delitos que de manera original necesitan a los medios electrónicos para ser utilizado como medio o que esta sea su finalidad. Por otro lado, existen los delitos informáticos que provienen de delitos tradicionales, los

cuales ya habían sido tipificados en la normativa y sólo se modifican debido a que utilizan los medios electrónicos para ejecutar el mismo delito. La evidencia que se recolecta de este tipo de delitos es digital, debido a su propia naturaleza.

La prueba digital se la conoce a cualquier información digital que es producida, almacenada o transmitida por medios digitales, esta información tiene el efecto de poder acreditar hechos en un proceso judicial y se trata de una característica de una prueba tecnológica. Esta prueba tiene la característica de ser intangible, replicable, volátil o mudable, parcial y deleble; y todas estas características son fundamentales para acreditar la autenticidad de las fuentes de las pruebas a través de las reglas de cadena de custodia.

Debido a los avances científicos, desarrollo de la tecnología y en la era de redes sociales en la cual vivimos, es necesario conocer los delitos informáticos, cuál es su conducta punible, sanción, persecución de los autores, sus procedimientos investigativos, jurisdicción y competencia. Todas estas aristas son necesarias para el juzgamiento de los mismos. Por lo que la autora creer conveniente y pertinente abordar el tema de procedimientos investigativos, es decir la aplicación de la cadena de custodia y su incidencia en la prueba digital de los delitos informáticos. Debido a que la información es escasa y muchas veces no actualizada.

En Ecuador, las investigaciones de una infracción penal es un tema que ha sido muy cuestionado o minimizado importancia, por lo que este trabajo de investigación propone el estudio del procedimiento en general de las investigaciones penales y más aún el procedimiento requerido en los casos de delitos informáticos donde la prueba que se maneja es digital.

Con lo antes expuesto el autor determina como problemas o dificultades de la cadena de custodia con respecto a la prueba digital, las que serán detalladas a continuación debido a su relevancia en estos tipos de casos.

- Desconocimiento del procedimiento y protocolos.
- Falta de herramientas adecuadas referentes a software.
- Falta de herramientas adecuadas referente a hardware

- Manejo inadecuado

Por lo que se establece como un tema de investigación relevante debido al desarrollo de tecnologías y el progreso de la sociedad.

El objetivo general de este trabajo de investigación es:

Determinar el alcance en el ordenamiento jurídico acerca de la cadena de custodia con respecto a la prueba digital dentro de los delitos informáticos.

Cumpliendo con los objetivos específicos:

a. Determinar el mecanismo aplicable a la prueba digital de los delitos informáticos.

b. Demostrar las falencias en los procedimientos relacionados a la cadena de custodia con respecto a la prueba digital.

c. Constatar la falta de normativa investigativa penal especializada en los procesos que conforman la cadena de custodia en informática forense.

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO 1: MARCO TEÓRICO

1. Cadena De Custodia

Todo delito o acción delictiva deja indicios o vestigios en el lugar del cometimiento de este acto, por lo que estos indicios quedan como objetivos de las investigaciones posteriores, es decir, el estudio de los mismos, la reconstrucción de los hechos, y entre otros mecanismos que ayudan a alcanzar la verdad de lo que ocurrió. Así que se entiende que la finalidad principal en el proceso penal es demostrar la verdad o no, de los hechos que son imputados y su grado de responsabilidad para que se aplique una pena proporcional al cometimiento del delito. Para que el proceso penal llegue a esta instancia, se debió seguir el conjunto de procedimientos para resguardar los medios probatorios y lograr ser válidos en el proceso penal.

A este conjunto de procedimiento o al procedimiento se le llama “Cadena de Custodia”, y se ha entendido como el conjunto de procedimientos de tratamiento de evidencias desde su recolección hasta su utilización como prueba dentro del proceso penal.

La autora Hermoza (2007) realiza un análisis en el Manual de Cadena de Custodia, en el que define a la cadena de custodia como el conjunto de procedimientos que garantizan la correcta y adecuada preservación de los indicios que fueron encontrados en el lugar de los hechos y a lo largo del proceso investigativo posterior.

> El autor López en su libro de Proceso Penal ha mencionado lo siguiente:
>
> Se puede afirmar que la cadena de custodia es un procedimiento establecido por la normatividad jurídica, que tiene el propósito de garantizar la integridad, conservación e inalterabilidad de elementos materiales como documentos, muestras (orgánicas e inorgánicas), armas de fuego, proyectiles, vainillas, armas blancas, estupefacientes y sus derivados, etc. entregados a los laboratorios criminalísticas y forenses por la autoridad

> competente a fin de analizar y obtener por parte de los expertos, técnicos o científicos, un concepto pericial. Su importancia reside en que garantiza el manejo idóneo de los elementos materiales de prueba desde su identificación en el lugar de los hechos, pasando por los diferentes laboratorios, hasta el envío del resultado pericial a la autoridad correspondiente (López, 2022, pág. 137).

Integrando más conceptos de autores se menciona que “La cadena de custodia importa, por lo tanto, que se mantenga la evidencia en un lugar seguro, protegida de todo factor o persona que puedan alterarla y que no se permita el acceso a la evidencia a personas que no estén autorizadas” (Donna et al., 2011, pág. 190).

Conforme a los conceptos mencionados anteriormente, se puede indicar que la cadena de custodia es el procedimiento ordenado y minucioso de todas los indicios y evidencias las cuales puede ser físicas o digitales, que son recolectadas en la escena en la que se produjo el cometimiento del delito y serán resguardadas hasta cuando sean presentadas ante el juzgador.

Estos indicios y evidencias deben ser vigiladas y protegidas de manera constante, porque el objetivo es que se mantengan en el estado en que se las encontró y así cumplir con varios principios establecidos en la Constitución, por ejemplo, el principio de legalidad, el cual es el más fundamental debido a que si no se cumple con lo que está establecido la prueba será rechazada, por lo que es necesario no irrumpir la cadena de custodia para que el medio probatorio no quede invalidado.

Para la autora es relevante mencionar algunos conceptos de Cadena de custodia, de entidades que se encargan de su manejo y control.

Policía Nacional del Ecuador (Manual de Cadena de Custodia de la Policia Nacional, 2007), entiende a la cadena de Custodia como el informe, que debe ser

firmado por el jefe de la Sala de Guardia, que detalla las evidencias halladas en una escena de delito o en posesión de algún sospechoso.

La Policía Técnica Judicial del Ecuador, indica que la Cadena de custodia es el documento de manejo de las evidencias, el cual consiste en enumerar y detallar los objetos o sustancias que fueron halladas como evidencia dentro de la escena del delito.

La Fiscalía General del Estado, establece que es un formulario o formato donde se establecen las consignas de las evidencias con todas sus características que forman parte de un sumario.

1.1. Antecedentes de la Cadena de Custodia.

A lo largo de la historia las normas penales han ido surgiendo en cada una de las sociedades, desarrollando sus características particulares y corrientes en el derecho. Estas normas surgen debido a que en todas las épocas se ha necesitado la creación de ellas para solucionar conflictos, sancionar conductas de las personas y reparar las lesiones que fueron causadas por estas conductas penalmente sancionadas, es la finalidad primordial del Derecho Penal.

Los procesos de investigación penal y como el Derecho Penal han tenido avances significativos debido al desarrollo de las sociedades, estos avances permiten el ejercicio y el respeto a los derechos y garantías para los ciudadanos.

Anteriormente no existía un proceso definido para la correcta aplicación de las diferentes prácticas investigativas que se realizaban posterior al cometimiento de una infracción que vulnerara algún bien jurídico protegido. En ese tiempo lo que existía eran prácticas primitivas, criterios empíricos e interpretaciones cuestionables e ilógicas por parte de los administradores de justicia.

Y es gracias a los inicios de la Criminalística, que dio origen a la terminología Cadena de Custodia debido a que se reconoció la importancia de proteger las

evidencias de las infracciones delictivas para un posterior análisis en el proceso penal. Es así que, en el año 1894, Hans Gross conocido como el padre de la Criminalística público su obra llamada “Manual del Juez”, en el que se mencionó por primera vez a los métodos o procedimiento de la investigación criminal y estableció que su elemento primordial eran las evidencias que posteriormente se convertirían en prueba en el proceso.

Luego de este hito, todo lo relacionado a la Cadena de Custodia empieza a tener relevancia, los elementos que se obtienen en el cometimiento del delito, este proceso de resguardo de la prueba comienza a ser solicitada y utilizada con mayor frecuencia, dado que determinan la eficacia y certeza en la validez de la información obtenida.

1.2. Principios de la Cadena de Custodia.

Se conoce que todo lo relacionado con el Derecho se rige por principios básicos los cuales no deben ser omitidos. El Derecho Penal como ciencia de estudio tiene una variedad de principios fundamentales, así también la Criminalística cuenta con principios que rigen su aplicación y dado que la Cadena de Custodia es un procedimiento que tiene inferencia de las dos ciencias, se entiende que también cuenta con sus propios principios que ayudan a su aplicación.

Colombia a través de su normativa (Reglamento de la Cadena de Custodia de elementos materiales, evidencias y administración de bienes incautados , 2006) establece entre los principios más importantes de la Cadena de Custodia se tiene los siguientes:

1. Que se realicen todas las acciones que permitan la preservación y el resguardo del lugar de los hechos, estas acciones son de carácter administrativo y técnico.

2. Acudir con la mayor prontitud al lugar del cometimiento del delito, también llamado lugar de los hechos, esto ayudará a que se realice un análisis efectivo de la escena y se proteja la evidencia.

3. Tienen el deber de velar por la preservación, integridad y seguridad, de todos los funcionarios que intervengan en el proceso de Cadena de Custodia.

4. Todos los funcionarios que intervengan en el proceso de Cadena de Custodia deben conocer los procedimientos tanto generales como específicos.

5. Se debe levantar actas de diligencias al momento de recolectar el material probatorio, con su respectiva descripción, sitio donde fue hallado y la persona encargada que lo recolectó.

6. Los análisis periciales también deberán estar en constancia en acta, con la descripción detallada de los procedimientos y técnicas utilizadas.

7. El centro de acopio de la Policía Judicial debe cumplir con los lineamientos de seguridad personal e industrial, para que el proceso de Cadena de Custodia no se rompa.

8. Cuando se termine el proceso penal, es decir cuando la cadena de custodia haya sido efectiva y las pruebas hayan servido como medio prueba se regresará las evidencias físicas a las personas que le correspondan.

1.3. Características de la cadena de Custodia.

La característica principal de la Cadena de Custodia es que los indicios y evidencias que fueron encontradas en el lugar de los hechos, analizadas por los laboratorios y que fueron presentadas en el proceso penal, mantenga su validez y nivel probatorio (Gúzman, 2018).

Guzmán en su obra (El examen de la escena del crimen.) indica que las siguientes características son las más relevantes:

1. Recoger evidencias en él lugar de los hechos garantiza un proceso completamente válido y su valor probatorio queda intacto.

2. Se debe determinar un listado de quien ha intervenido en algún momento dentro del proceso.

3. Se debe presentar en etapa penal es decir en etapa probatoria para que sea valorada por la autoridad competente.

4. Se debe evitar que el medio probatorio se altere, contamine, destruya o cualquier que altere a las evidencias recolectadas.

5. Que esté libre de vicios para que se tenga una custodia exitosa.

Todas estas características ayudan a que la Cadena de Custodia se mantenga resguardada, así ayudan a probar o descartar el cometimiento de un delito. Este proceso, nos ayuda a conocer, las personas encargadas, los peritos que intervienen y las investigaciones realizadas.

1.4. Procedimiento de la cadena de custodia

Es necesario para esta investigación conocer el protocolo o procedimiento correcto de la Cadena de Custodia. Con respecto a esta necesidad se puede indicar una estructura al momento de iniciar la cadena de custodia.

En el Manual de Cadena de Custodia de la Policía Nacional (2007) se presenta la siguiente estructura de la Cadena de Custodia:

1. Protección del lugar de la escena.
2. Observación del lugar de la escena.
3. Recolección, embalaje, rotulación y traslado de indicios al centro de acopio de evidencia.
4. Ingreso y custodia de los indicios en el centro de acopio de evidencia.
5. Solicitud de remisión de Indicios del centro de acopio de evidencias.
6. Ingreso, custodia y análisis de indicios en el Laboratorio de Criminalística.

A continuación, se desarrollará cada uno de los pasos de la cadena de custodia.

1.4.1. Protección del lugar de la escena.

Se conoce a este concepto en la ciencia Criminalística como la escena del crimen. Es por eso que se debe indicar la importancia que tiene el lugar del cometimiento del delito.

Para el auto Hans Gross, en su obra Manual del juez de Instrucción como Sistema de Criminalística, indicó que “El término nace cuando consideré como parte del Procedimiento de la Inspección Ocular la denominada Descripción de Lugar”, la cual tenía como actividad fundamental la descripción del ambiente alrededor al cuerpo, la descripción de las prendas o lo que se encontró en ellas, y es por eso la

conceptualización que le dio Hans Gross al término escena del crimen, de ahí su origen y denominación (Gross, 1892).

La Policía Nacional del Ecuador, denomina a la escena del delito como el lugar donde se presume que se ha cometido un delito y en la que amerita una investigación policial.

Para Aton en su obra (Cadena de Custodia, 2009) detalla como características de la escena del delito las siguientes:

- **Acto calificado como delito. -** esto quiere decir que el examen o análisis de la escena debe ser consecuencia de una conducta criminal, por lo que debe estar tipificado en la ley.
- **Tipo de evidencias. -** con respecto a este tema, se entiende que hay ciertos delitos que no dejan evidencia física, por lo que el tratamiento de la evidencia digital también es importante.
- **Debe contar con un espacio. -** se entiende que el acto criminal fue cometido o llevado a cabo en un lugar determinado, puede ser una pequeña área o un ambiente extenso.
- **Escenas concentradas o no concentradas. -** Este tipo de escena o ambiente puede ser limitada o no, eso quiere decir una habitación, cuarto, departamento, algo con límites superficiales, pero existen otros tipos de delitos, como los delitos informáticos que comprenden áreas sumamente extensas, debido a que este tipo de delitos no tienen territorialidad, en donde el concepto de "espacio" puede apartarse de la jurisdicción y competencia de un país.

En la obra (Investigación criminal y criminalística., 2010), establece que la escena del delito se puede clasificar en abierto, cerrado, mixto y móvil.

a. **Escena del delito abierto. -** Es denominado así porque el espacio no tiene límites establecidos y no tiene protección con los factores ambientales tales como el viento, luz solar, lluvia, polvo, entre otros.

Es necesario tener mayor cuidado en este tipo de escena debido a la contaminación de la evidencia por los factores antes mencionados.

b. **Escena del delito cerrado. -** es denominado así porque son aquellos espacios que se encuentran delimitados y tienen alguna protección de los factores ambientales.

Este tipo de escenas tienen ventajas como la facilidad de establecer límites físicos en el lugar de los hechos, no se contamina la escena con mucha facilidad y eso permite la investigación.

c. **Escena del delito mixto. -** es llamado de este modo, debido a que se encuentra compuesto por dos o más lugares, estos lugares tienen las características de una escena abierta y cerrada.

En este tipo de escena deben mezclarse las aplicaciones de métodos diversos que ayuden en la investigación de indicios.

d. **Escena del delito móvil. -** se denomina así al espacio que tiene la característica de estar en movimiento.

Es toda escena o espacio que pueda moverse de un lugar. En este tipo de escena se le da el tratamiento o procedimiento de una escena del delito mixto.

Precauciones para proteger la escena del delito.

- Llegar con brevedad al lugar.
- Comprobar el cometimiento de algún delito.
- Verificar si hay algún herido.
- Proteger la escena del delito.
- Identificar, localizar evidencias.
- No tocar, ni alterar nada.

Que la investigación sea exitosa, depende de la adecuada seguridad que se le dio al lugar donde ocurrieron los hechos, con el fin que no se altere o pierda indicios para que exista una correcta valoración de la evidencia.

La cadena de custodia comienza en el lugar del cometimiento del delito, los encargados de dar inicio a la cadena de custodia son los agentes del SIOT (Sección de Inspección Ocular Técnica), son aquellos que ingresan a la escena del cometimiento de los hechos y realizan el levantamiento de huellas, armas, búsqueda de evidencias, toman fotografías. Los agentes del SIOT tienen la responsabilidad de realizar la noticia técnica y el informe, luego trasladar todos los indicios y el acta al Centro de Acopio de evidencias de Criminalística.

1.4.2. Observación del lugar de la escena

Cuando ya se ha protegido y valorado el lugar del cometimiento del delito, procede el siguiente paso que es la observación. Este paso consiste en examinar atentamente, es decir realizan un examen detallado y minucioso de los detalles de la escena del delito y sobre los indicios recolectados.

El autor Luis Kvitko, quien en su obra “Escena del Crimen” afirma que la observación “…consiste en practicar el examen completo, meticuloso, metódico y sistemático de la totalidad del lugar del hecho, y no limitarse estrictamente al cadáver y lo que está ubicado inmediatamente alrededor del mismo” (Kvitko, 2006).

Es correcto indicar que la observación es un acto de investigación de campo, debido a que corre por iniciativa propia de la Policía Judicial o por una denuncia previa, esta observación debe ser llevada a cabo en el lugar de la escena del delito. La finalidad de la observación es imaginar cómo es el espacio en el que se produjo el delito.

Dentro del proceso de observación, existe un mecanismo denominado fotografía judicial, se estableció para promover la seguridad del estado original de

las cosas. La importancia de esto es que las fotografías ayudan a mostrar el estado original de la escena, quedando como un registro permanente del lugar.

1.4.3. Recolección, embalaje, rotulación y traslado de indicios al centro de acopio de evidencia.

Con respecto a esta etapa del proceso de Custodia, es necesario tenerlo en cuenta como el principio del estudio. Es relevante que el funcionario sepa cómo puede obtener la evidencia para posteriormente conservarla, manejarla, recolectarla y producirla en el proceso.

Es por eso que en el Manual de Cadena de Custodia (2007) indica los siguientes parámetros técnicos:

1.4.3.1 Recolección

Cuando se recolectan las evidencias del lugar de la escena se utiliza una técnica diferente debido al tipo de indicios que desea recolectar, para evitar que se destruya o se altere. Es en esta fase donde el conocimiento y la experticia de los funcionarios encargados de este paso juega un rol sumamente importante en el resguardo de la cadena de custodia.

1.4.3.2. Embalaje

Este paso tiene como finalidad clasificar e individualizar los indicios según el caso, este embalaje garantiza la integridad del indicio. Otro beneficio es que este proceso imposibilita que terceros puedan alterar voluntaria o involuntariamente el índice.

1.4.3.3. Rotulación

Este procedimiento también se lo conoce como el etiquetado y en el que la evidencia se le otorgará una etiqueta con el que se deberá diferenciar o caracterizar el matera probatorio.

1.4.3.4. Traslado de indicios al centro de acopio de evidencia

En último lugar tenemos al traslado de estos indicios ya rotulados al centro de acopio de evidencia, esto es la bodega de evidencia en el departamento de policía judicial,

1.4.4. Ingreso y custodia de evidencias en el centro de Acopio.

Este ingreso al Centro de Acopio lo realizará la persona que hizo el levantamiento en la escena del delito. Son ingresadas por parte policial en el cual se determina las características de la evidencia, para esto es importante el etiquetado o rótulo donde se establezca el tipo de embalaje y el contenido de la evidencia.

1.4.5. Solicitud de Remisión de evidencia del Centro de acopio.

Para la salida de cualquier evidencia del centro de acopio, es necesario la solicitud de remisión con una justificación de salida, donde se explica el motivo y también deberá ser justificada por el jefe de área en la Cadena de Custodia.

Este garantiza la validez de las pruebas en el proceso penal, debido a que existen registros de las condiciones de la evidencia.

1.4.6. Ingreso, custodia y análisis de evidencia al laboratorio de Criminalística.

Para el completo análisis de las evidencias, deben ser trasladadas al laboratorio de criminalística acompañada con su debida autorización de los responsables o encargados de esa cadena de custodia.

Se conoce que todos los elementos que son encontrados en el lugar de la escena del crimen o la escena del delito, su destino final es dispuesto por el Fiscal o el Juez competente.

La relación de la cadena de custodia con la evidencia es implícita debido a que lo que resguarda, protege y cuida la cadena de custodia es la evidencia que se encuentra para el proceso, todo esto hablando de la cadena de custodia en evidencia de delitos que no son informáticos.

1.5. Cadena de custodia en el ámbito digital

Como se ha mencionado anteriormente el proceso de la cadena de custodia es sumamente relevante para el resguardo de las evidencias de los actos delictivos tradicionales. Y a medida que se desarrolla la sociedad y las tecnologías, la criminalidad también se acopla a los nuevos medios para delinquir. Es aquí donde entran en escena los delitos informáticos, la prueba digital y cómo se relaciona con la cadena de custodia.

Cadena de custodia de evidencias digitales

En países aledaños, establecen normativas o lineamientos que ayudan al procedimiento de cadena de custodia en ámbitos digitales. Colombia tiene lineamientos establecidos para la informática forense, donde se establece los pasos a seguir para la prueba digital, desde el paso de manipulación hasta que se determine la validez de la información contenía esos medios probatorios o la originalidad de los medios probatorios digitales.

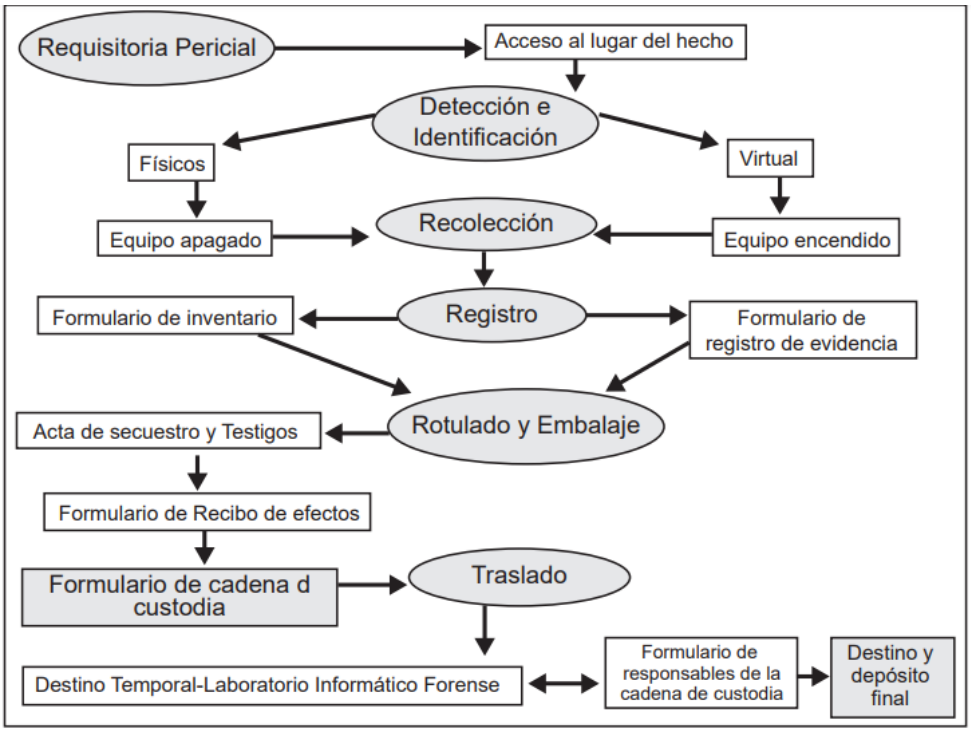


Figura 1. Nota: Protocolo para la cadena de custodia en informática forense. Tomado de (Arellano & Castañeda, 2012).

Tal como se ha mencionado anteriormente el principal objetivo es conservar la evidencia, que la prueba tenga validez y se podrá demostrar la veracidad de los hechos. Esta figura demuestra el protocolo que debe seguir para que la cadena de custodia no se rompa en pruebas digitales es decir en informática forense.

2. Los Delitos Informáticos.

Debemos establecer en primer lugar el concepto de delito en general antes de abordar el tema de delitos informáticos. El concepto de delito se encuentra en la misma legislación ecuatoriana en el Código Orgánico Integral Penal (COIP), establece lo siguiente “Delito es la conducta, típica, antijurídica y culpable, cuya sanción se encuentra prevista en este código.” (Código Orgánico Integral Penal, 2014, pág. 20).

Es importante aclarar que el concepto de delito informático no se encuentra estipulado en la legislación ecuatoriana, pero si ha llegado a ser desarrollado por doctrina.

Para el autor Efraín Chávez (2002), el delito informático:

> “Es toda acción o comportamiento ilícito, antijurídico y doloso, en donde el computador es el instrumento, medio o fin para cambiar, borrar, copiar, alterar o manipular información protegida que se almacena o procesa en un computador y/o redes informáticas o páginas webs pertenecientes a una persona natural o jurídica” (pág. 78).

Los delitos informáticos son aquellos que se realizan o materializan con la utilización de medios electrónicos, por lo que, según los autores Mendoza y Urdaneta (2005) establece que “la facilidad con la cual puede ser accedida cual red, ha hecho posible la aparición de comportamientos antijurídicos, no éticos o no autorizados, relacionados con el procesamiento y la tramitación de datos” (p. 125). Ante lo manifestado se puede colegir que las personas suministran información de carácter personal para poder hacer uso de programas o páginas digitales, los mismos que pueden ser utilizados de forma ilegítima por un tercero para la comisión de ciertos ilícitos punibles.

Las pruebas digitales son aquellas obtenidas a través de medios electrónicos.

2.1. Antecedentes

Con el desarrollo de los medios tecnológicos en los años 70 se producen una diversidad de problemas informáticos, tanto así que desde la creación de una página y su suscripción provoca que las personas puedan estar o proporcionar información de índole personal hacia una red que no es del nada seguro, información que puede

ser de fácil acceso para aquellas personas que tienen conocimientos avanzados y técnicos por medios electrónicos.

Históricamente se puede determinar cómo apogeo de los delitos informáticos La Segunda Guerra Mundial, sin embargo, un hecho histórico en este tema data específicamente en 1970 y es aquella ocurrida mediante llamadas telefónicas, sin embargo, se considera que no existió un delito real hasta 1980. En 1981 se determinó que un sujeto A había hackeado la computadora de un sujeto B, sacando información de índole personal, mismo que mediante proceso fue declarado culpable, el nombre de ésta personas es Ion Murphy.

2.2. Antecedentes de los delitos informáticos en Ecuador

Los delitos informáticos entran en relevancia en Ecuador en el año 1999 a partir de la propuesta de la Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas, que posteriormente fue aprobada y entró en vigencia en el año 2002, esta ley tiene la finalidad de regular los mensajes de datos y comercio electrónico, protegiendo a los usuarios en línea.

Es en el año 2014 con la creación del Código Orgánico Integral Penal (COIP), el cual recoge todas la normativa penal y procesal penal. Reunió todos los delitos con su conducta y pena, estableció normas procesales penales y normas sustantivas penales.

Como se mencionó anteriormente en el Código Orgánico Integral Penal (COIP), no se establece la definición de delito informático, tampoco existe un apartado dentro del código que reúna todos los delitos informáticos, sino que están dispersos por toda la normativa penal, ubicados según el bien jurídico que protegen.

2.3. Definición

El autor Davara (1990) delimita que los delitos informáticos son aquella "realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular del elemento informático" (p.10). Como lo manifiesta el autor Davara los delitos informáticos son aquellos que se producen por medios electrónicos y que afectan directamente a las personas a las que le roban su información personal Para la comisión de algún ilícito punible.

Según el diccionario Significados (2023) "los delitos informáticos son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades".

La autora puede definir a los delitos informáticos como aquella conducta que reúne la calidad de delito y lo comete por medios electrónicos o que su objetivo es dañar un sistema informático.

2.4. Generalidades de los delitos informáticos

Ahora bien, corresponde analizar los componentes jurídicos que determina la comisión del posible hecho punible, tanto así que es importante delimitar el sujeto pasivo, el sujeto activo, el bien jurídico protegido y otras características relevantes dentro del presente análisis, mismo que es relevante para para *ius puniendi*.

Es importante recalcar que el bien jurídico cumple una de las funciones primordiales para saber que podría existir la comisión de un posible delito, sin embargo, se puede establecer que el bien jurídico podría ser una persona o algo material, adicionalmente se debe de considerar lo que mencionaba el autor Mayer (2017) al decir que "sabido es que los bienes jurídicos pueden ser individuales o

colectivos. Los bienes jurídicos individuales son de titularidad o sirven a una persona determinada o a un grupo" (p. 236).

Con la manifestado se puede hacer una clara idea de que tiene que existir la individualización concreta o abstracta de que debe existir una persona o algo material que se protege, conforme a aquello también se debe de delimitar que nuestro cuerpo normativo o Código Orgánico Integral Penal (COIP) describe dentro de sus diversos articulados, mismos que serán analizados en partes posteriores de este trabajo.

2.5. Elementos de los delitos informáticos.

Los elementos del delito informático son los mismos que los delitos tradicionales, estos son: sujetos del delito, acción del delito, bien jurídico del delito, y los demás estipulado en el art. 18 del COIP.

En los delitos existen dos tipos de sujetos, el sujeto activo y el sujeto pasivo. El sujeto activo es aquel que comete la infracción o la conducta delictiva. Aterrizándolo en el ámbito informático, el sujeto activo "En el delito informático viene a ser cualquier persona que tenga conocimiento en programas y sistemas informáticos que cometa uno o más de los delitos sancionados en el Código Orgánico Integral Penal" (Riofrío, 2016, pág. 119).

Y el sujeto pasivo es la persona que sufre la infracción, es decir la víctima de delito informático, puede tener esta calidad personas naturales, instituciones, corporaciones, gobiernos o cualquiera que utilice Internet o sistemas electrónicos.

Cuando analizamos el bien jurídico del delito, establecemos que es lo que desea la ley proteger, como la vida, la seguridad, libertad sexual, entre otros. Son diferentes los bienes jurídicos que protegen los delitos informáticos, en algunos son los derechos de autor, la seguridad del Estado, integridad sexual, propiedad, identidad, entre otros.

A continuación, se detalla algunos análisis de artículos para establecer los elementos de los delitos informáticos.

El artículo 190 del COIP tipifica como delito la apropiación fraudulenta por medios electrónicos al determinar el que, mediante la alteración, manipulación o modificación del funcionamiento de redes electrónicas, programas, sistemas informáticos y telemáticos y terminales de telecomunicación, procure la transmisión no consentida de bienes, valores o derechos en perjuicio de aquél o de un tercero, en beneficio propio o ajeno, o utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno, se sancionará con una pena privativa de libertad de uno a tres años. Si el delito se comete inutilizando sistemas de alarma o de vigilancia, encontrando o interpretando claves secretas o cifradas, utilizando tarjetas magnéticas o perforadas, utilizando mandos o herramientas de apertura a distancia, o vulnerando sistemas electrónicos, informáticos u otros similares, se aplicará la misma pena (Código Orgánico Integral Penal, 2014).

En este delito se puede determinar que el sujeto activo y sujeto pasivo son indeterminados**,** el verbo rector que se utiliza en este tipo de delitos es utilizar**,** los elementos del delito es el uso de la información personal de otra a través de medios informáticos, la pena privativa de libertad es de 1 a 3 años, dependiendo de la forma como haya operado el mismo o si la persona procesada ayuda con la consecución de la causa.

El mismo COIP en su artículo 191 determina que en caso de que exista alguna reprogramación o modificación de información de equipos terminales móviles será sancionada con una pena de 1 a 3 años. Conforme al análisis, el bien jurídico protegido es indeterminado, el verbo rector es reprogramar o modificar, la pena privativa de libertad es de 1 a 3 años.

En el artículo 192 se establece que se impone una multa de hasta tres años de cárcel a quien sea sorprendido comercializando, comprando o intercambiando

bases de datos que contengan los datos de identidad de equipos terminales móviles (Código Orgánico Integral Penal, 2014). Del análisis se puede establecer que el sujeto activo y pasivo son indeterminados, en cuanto al verbo rector existen tres y son intercambiar, comercializar y comprar, y la pena es de uno a tres años de privación de la libertad.

El artículo 195 del COIP (Código Orgánico Integral Penal) delimita que el siguiente contenido legal y es que se impondrá una multa de hasta tres años de cárcel a quien se encuentre en posesión de la infraestructura, software, herramientas, bases de datos o etiquetas que permitan reprogramar, cambiar o alterar los datos de identidad de un dispositivo terminal móvil. No existe ningún tipo de delito asociado a la apertura de bandas para el funcionamiento de equipos terminales móviles.

En este artículo se puede observar que va direccionado a otras características que no son materia de la Litis en este trabajo, sin embargo, hay una parte fundamental en la que se hace referencia al uso de información almacenada en una base de datos, aquello quiere decir que hace uso de diversas herramientas tecnológicas para obtener información de un tercero, información que al hacer un mal uso de ellas podrían provocar daños colaterales para las personas afectadas.

Los autores Ojeda, Rincón, Arias y Daza (2010) en su obra “Delitos informáticos y entorno jurídico vigente” manifiestan que al igual que la tecnología y sus avances han influido en casi todos los aspectos de la actividad humana a lo largo de la historia, la dependencia tecnológica actual se centra más en los fenómenos de la informática, la información y la comunicación. Con el tiempo se descubrió que este descubrimiento trae consigo una serie de nuevos peligros como impacto retardado (p. 44).

Con lo manifestado por estos autores se puede determinar que verídicamente este tipo de delitos surgen con la evolución misma de los seres humanos, aquello quiere decir que a medida que se va avanzando se va creando

nuevas fuentes de información, información que al estar dentro de una plataforma o de una fuente de archivos electrónicos puede ser hurtada o robada.

2.6. Características de los delitos informáticos

Los delitos informáticos tienen características específicas que las diferencian de los otros tipos de delitos tradicionales. Entre las más relevantes tenemos los sujetos activos del delito, el bien jurídico que protegen y los medios que emplean para ejecutarlos. A continuación, se detallará las características más relevantes:

- Son delitos de cuello blanco. Esto significa que los que cometen estos delitos son personas con poder, conocimientos especializados y estatus social.
- Son delitos dolosos. La mayoría de los delitos informáticos son dolosos, significa que hay la intención de causar daño. Por otro lado, existe una pequeña cantidad de delitos que pueden ser culposos.
- Pérdidas para las víctimas. Estos delitos siempre provocan pérdidas para los afectados, pueden ser perdidas de información personal, ingresos económicos, entre otros.
- Delitos de oportunidad. Se aprovecha de una oportunidad creada o de una ocasión donde se encuentre en desventaja el sistema económico y tecnológico.
- Delitos difíciles de evidenciar. Se requiere de expertos en este caso de programadores o profesionales tecnológicos para que encuentren el rastro del sujeto activo. Por otro lado, las
- pruebas que puedan tener, son intangibles y muchas veces son borradas así que no existe medios probatorios que validen que en realidad se cometió un ciberdelitos.

2.7. Caso práctico

Dentro de la causa No. 2062-20-EP se puede denotar un caso práctico sustanciado por uno de los grandes juristas del territorio ecuatoriano de nombres Ramiro Ávila Santamaría, el cual dentro de sus establece que el señor Carlos Alfredo Caiza Quillupangui presenta una denuncia en contra del señor Ramiro Baldeón por presumir que él mismo había accedido al contenido personal a través de sistemas informáticos. Con posterioridad aquellos el 20 de noviembre de 2015 se realizó la respectiva audiencia de formulación de cargos, posteriormente el 22 de febrero del 2018 se realizó la audiencia de evaluación y preparatoria de juicio, misma que fue acogido por la suscrita jugadora conocedora del proceso y dio paso al inicio de la instrucción fiscal encuentra el señor denunciado. En el año 2019 se realiza la audiencia de juicio por los magistrados del Tribunal de Garantías Penales con Sede en el Cantón Quito y se ratifica el estado de inocencia del procesado. Posteriormente se presenta el recurso de apelación ante la decisión adoptada por este tribunal para que tenga conocimiento la Corte Provincial de Pichincha, misma que confirma el estado de inocencia del denunciado. En diciembre de 2019 se da paso el recurso de casación interpuesto por el denunciado y fue sustanciado por la Sala de lo Penal de la Corte Nacional, sin embargo, es inadmitido el 9 de noviembre del 2020.

Mediante la garantía jurisdiccional de acción extraordinaria de protección, que tiene como finalidad prioritaria el amparo directo de los derechos constitucionales y el debido proceso en autos definitivos sentencias y resoluciones, misma que planteada en contra del auto de inadmisión que emite la Corte Nacional de Justicia. Ahora bien, del análisis realizado en esta sentencia se desprende que dicha acción fue presentada dentro del término legal correspondiente conforme lo determina el artículo 61, 62 y 63 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, de la misma manera se establece que la demanda cumple con los requisitos formales determinados en el artículo 59 y 61 de la LOGJCC.

De los hechos narrados se desprende que él accionante plantea que se declare la vulneración del derecho a la tutela judicial efectiva, a la seguridad jurídica y que se deje sin efecto el auto de admisión del auto que inadmite el recurso de casación, Así mismo considera que al no declararse de maliciosa y temeraria la denuncia se ha vulnerado el derecho a la seguridad jurídica.

Del análisis complejo realizado por el juzgador sustanciador de esta causa se delimita que se debe realizar un análisis exhaustivo de los requisitos formales o no para que proceda este recurso, por lo que se conforme a lo que determina el artículo 62 se puede colegir que el accionante no realiza o no fundamenta su acción en el contenido de la misma, es decir, de la relación circunstancial de los hechos no se desprende que exista realmente una vulneración a derechos constitucionales por lo que se declara de inadmisible la presentación de este recurso.

A pesar de que haberse declarado la inadmisibilidad de la presente acción se puede determinar qué en el territorio ecuatoriano existe la figura jurídica o de derechos que tienen todas las personas sobre su información personal, información que no puede ser utilizada por terceros a través de diversos medios, en este caso medios electrónicos.

3. La prueba digital

3.1. Definición

La sociedad va avanzando y se incrementa el uso de las redes de comunicación, y hoy en día se utilizan en actividades cotidianas que requieren el uso de la tecnología. Para poder definir lo que es una prueba digital se debe entender lo que es una prueba tradicional y luego aterrizar al ámbito digital.

La palabra prueba proviene del término latín Probatio, y este nace del vocablo probus, que significa buena, honrado, auténtico. Para los doctrinarios que han desarrollado el concepto de prueba, tenemos el de Bentham citado por (Morillo &

Herrero, 2011), la conceptualiza como “hecho supuestamente verdadero que se presume debe servir de motivo de credibilidad sobre la existencia o inexistencia de otro hecho (…) la prueba es un medio que se utiliza para establecer la verdad de un hecho” (pág. 7).

Entonces se entiende que aquella información que se utiliza para probar algo, pueden ser huellas dactilares, mensajes, cartas, un sin número de información. Adentrándonos más a la materia se conoce que existe la prueba digital o evidencia digital. Es aquella evidencia que tiene como característica que se encuentra en el ámbito digitalizado y son los resultados del cometimiento de los delitos informáticos.

El autor Arrabal (2019) delimita a la prueba digital como los archivos informáticos, o impulsos electrónicos, pueden almacenarse en cualquier lugar del planeta, transmitirse a otra parte del mundo en cuestión de segundos, modificarse o duplicarse rápidamente, almacenarse en lugares secretos en servidores ajenos y cifrarse mediante un procedimiento (p. 41).

En la legislación ecuatoriana la prueba digital se encuentra dentro de la prueba documental y el contenido de la prueba digital se encuentra en el art. 500 del COIP. El art. 500 del Código Orgánico Integral Penal (2014) establece el siguiente concepto:

Se denominan contenidos digitales todos los datos informáticos que representan hechos, información o nociones de la realidad que se almacenan, procesan o transfieren utilizando un método técnico que permite el tratamiento informático, incluidos los programas creados para equipos tecnológicos independientes, conectados o vinculados.

La investigación debe seguir las siguientes pautas

1. Deben utilizarse técnicas forenses digitales para el examen, evaluación, recuperación y presentación del material digital almacenado en dispositivos o sistemas informáticos.

2. Se utilizarán técnicas forenses digitales para recopilar el contenido digital in situ y en tiempo real, manteniendo su integridad. Se utilizará la cadena de custodia, lo que permitirá su posterior valoración y examen de contenido. Esto es válido para el material digital que se guarda en ordenadores frágiles, memorias volátiles u otras piezas de hardware moderno que son esenciales para las infraestructuras vitales tanto del sector público como del privado.

3. La recogida debe realizarse utilizando técnicas forenses digitales para preservar la integridad de los datos digitales cuando se almacenan en soportes no volátiles. También deben seguirse los procedimientos de cadena de custodia.

4. Cada soporte físico que almacene, procese o transmita contenido digital que se descubra durante una investigación, registro o redada debe identificarse e inventariarse específicamente, su ubicación exacta debe documentarse con fotos y un plano del lugar, debe protegerse utilizando técnicas forenses digitales y debe transferirse mediante cadena de custodia a una instalación creada a tal efecto.

3.2. Generalidades

La prueba digital se encuentra coligada de forma estrecha con el ámbito informático o electrónico, obviamente sin hacer alegación alguna de que existan otras formas de denominaciones en el ámbito del derecho probatorio. La prueba digital puede ser analizada desde dos vertientes, la primera es aquella que se encuentra delimitada por la modalidad de la prueba, que no es otra cosa que aquella que es propia y que se proporciona a través de fuentes digitales; y, la segunda relación versa en aquel orden o categoría probatoria.

El Código Orgánico Integral Penal establece que la prueba tiene como fin que el juzgador tenga la certeza de que los hechos son verídicos y que por lo tanto existe la comisión de una infracción. El anuncio práctico de las pruebas debe de regirse

por los principios de oportunidad, inmediación, contradicción, libertad probatoria, pertinencia, exclusión y de igualdad de oportunidades.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece en su artículo 2 que los mensajes de datos poseen el mismo valor probatorio que los documentos escritos, siempre y cuando cumpla con ciertos requisitos formales que la misma normativa de forma taxativa exige. De la misma manera se reconoce que dicha información verídica, siempre y cuando, sea ha remitido por el órgano competente (Asamblea Nacional del Ecuador, 2002).

Es importante destacar que el mismo cuerpo normativo delimita a dos principios fundamentales que priman en la base de datos, esto es, el principio de confidencialidad y reserva, aquello lo hace en razón de que se proteja todas forma, medio o intención con la que se utilice dicha prueba.

En el artículo 20 dice que el mensaje que certifique la vinculación de datos debe pasar por un filtro para confirmar la identidad de la persona que firma electrónicamente dicho contenido, asimismo es importante determinar que las entidades pueden emitir y certificar información de índole electrónica, mismas que están autorizadas por el Consejo Nacional de telecomunicaciones. Las empresas unipersonales o personas jurídicas que de una u otra manera emitan certificados electrónicos están obligadas a certificar dicha información (Asamblea Nacional del Ecuador, 2002).

3.3. Características de la prueba digital

Este tipo de pruebas presenta una variedad de características que la diferencia de las pruebas documentales, aunque forme parte de ellas con una clasificación. Castañeda y Arellano establecen las siguientes características en su obra (La cadena de custodia informático-forense, 2012):

- Esta prueba se basa en indicios digitales, esto quiere decir que se encuentra en un espacio digital normalmente almacenados ahí.
- En relación a lo establecido anteriormente hay una clasificación en la presentación de la prueba digital, se puede encontrar almacenada, en desplazamiento o en proceso.
    - Almacenada: significa que se encuentra guardada en un almacenamiento, esto quiere decir que se tiene acceso a ella.
    - En desplazamiento: quiere decir que se esta evidencia digital se encuentra moviéndose o se está transportando por algún medio físico y debe acceder por medio de dicho medio.
    - En proceso: este se considera el estado más complejo, debido a que no hay una finalización de la prueba. Al usarse el equipo se entiende que esta información está en proceso, eso quiere decir que se puede modificar, alterar, actualizar.
- Se entiende que algunas de las evidencias digitales son volátiles, esto quiere decir que es temporal, la evidencia que no se encuentra almacenada cuenta con esta característica.

3.4. Tipos de pruebas digitales

Como se mencionó la prueba digital forma parte de la prueba documental, por lo que su tratamiento se entiende que va encaminado a la generalidad de la prueba documental, con sus modificaciones y especialidades al ser una prueba digital.

Contamos con distintos tipos de prueba digital, en los cuales tenemos:

- Comunicación por medios de correos.
- Llamadas telefónicas.
- Comunicación por redes sociales.

Comunicación por medios electrónicos

Este tipo de prueba digital tiene un tratamiento jurídico especial, se considera un documento privado y sigue sus reglas, pero al igual que el documento público, tendrá la misma fuerza vinculante. Esta prueba se debe presentar con un informe pericial que demuestre que el contenido es original y no ha sufrido alguna modificación, es decir la validez de la prueba (Chiluiza, 2017).

Llamadas telefónicas

El Código Orgánico Integral Penal (2014), en su art. 476 establece que cuando existan pruebas pertinentes para los objetivos de la investigación y la medida sea adecuada, necesaria y proporcionada, de acuerdo con requisitos específicos, el juzgador ordenará la interceptación de comunicaciones o datos informáticos en respuesta a una petición justificada del fiscal, y enumera en casos se dará esta intercepción.

Por lo que se entiende que se podrá interceptar las comunicaciones y la información recolectada puede ser un medio de prueba digital que ayude a esclarecer los hechos y se llegue a la verdad.

Comunicación por redes sociales.

Son admitidas las publicaciones en redes sociales por medio de pruebas digitales. La forma más común de aportar estas pruebas es mediante capturas de pantalla, materializando los documentos y adjuntando un informe pericial, demostrando la eficacia del medio probatorio (Lacalle, 2018).

3.5. Sistema probatorio general en Ecuador

Es importante mencionar que en el territorio ecuatoriano existe una diversidad de normas jurídicas que regulan el debido proceso, proceso que es determinado o que tiene asidero legal en la norma constitucional.

Luego de haber realizado esta inferencia se debe tener en cuenta que nuestro sistema procesal se encuentra dividido hoy en materia penal y en materia no penal. Diferencia al sistema no penal podemos determinar que nuestro sistema procesal existe el Código Orgánico General de Procesos, el mismo que describe la forma y los medios en los que se puede solicitar, anunciar y reproducir las pruebas; en cambio, en el sistema penal existe el Código Orgánico Integral Penal, el cual dentro de cada tipo de procedimiento determina las vertientes por la cual debe de regirse valga la redundancia el proceso penal.

El artículo 202 del Código Orgánico General de Procesos determina que aquellos documentos que hayan sido producidos de forma electrónica deben ser considerados con categoría de original, hola aduciendo que tendrán la misma fuerza probatoria dentro del proceso, por lo que, deberá admitirse como prueba y se respetará su contenido en su integralidad. Importante mencionar que toda prueba, ya sea física o digital, puede ser impugnada al momento de presentar la contestación a la demanda o como también en la reconvención, siempre y cuando no cumple con los requisitos formales exigidos por la misma (2015).

3.6. Relación de la prueba digital con los delitos informáticos

Conforme este enunciado se debe de indicar que las pruebas dentro de un proceso deben ser: en primer lugar, en el ámbito penal en la denuncia y contestación a la denuncia para que puedan ser reproducidas en la etapa procesal oportuna, ahora bien, es importante mencionar qué, a pesar de que las pruebas sean digitales deberán ser presentadas de forma física para que consten dentro del expediente o

cuaderno procesal, es importante mencionar que las pruebas digitales deben de cumplir ciertos requisitos formales para que sean consideradas como pruebas válidas dentro del proceso.

Unos de los puntos relevantes de las pruebas digitales es que, como ya se ha manifestado, cumplen una serie de requisitos formales para que sean consideradas como válidas dentro de un proceso. Conforme a lo manifestado se recalca que con el uso de la informática y los medios electrónicos hace factible que algunas personas puedan suministrar información falsa o que sean de dudosa procedencia, por lo que, al momento de que el suscrito juzgador se percate de aquello podría ordenar que se realice una investigación penal por fraude procesal en contra de aquellas personas involucradas.

CAPÍTULO 2: METODOLOGÍA DEL PROCESO DE INVESTIGACIÓN

2.1. Conceptualización

Según la revisión documental revisada para la investigación, autores como Arias (2012) definen al marco metodológico como el conjunto de técnicas, métodos, procesos y pasos que son requeridos para la solución de un problema, además teniendo en cuenta que con la ejecución de este método se pretende describir y analizar la problemática (pág. 16).

2.2. Enfoque de la Investigación

Dentro de la metodología de investigación existen tres enfoques, los cuales tienen diferentes procedimientos para poder responder a la problemática planteada. Tenemos el enfoque cualitativo, cuantitativo y mixto.

El autor para el presente trabajo de investigación decidió implementar el enfoque cualitativo, debido a que este enfoque implica que la recolección de datos y el análisis del mismo no sea numérico o estadístico. Se analiza las opiniones, conocimientos y conceptos interpretativos de las personas y los resultados de este enfoque se presentan en palabras (Hernández-Sampieri, 2018).

El autor al elegir este enfoque, iniciará su proceso de investigación con la revisión de trabajos anteriores, doctrina relacionada al tema de la problemática y demás información relevante para plantear su hipótesis.

Posteriormente debido al enfoque elegido, se establecerá la herramienta adecuada para poder ejecutar su investigación dentro del marco del enfoque cualitativo, la cual podría ser entrevista, grupos focales, análisis de documentos, entre otros.

2.3. Tipo de Investigación

Debido al tema del proyecto de investigación, el autor considera necesario que en el presente trabajo se implementan tres tipos de investigación, el Exploratorio, Explicativo y Descriptivo.

Para Sampieri (2018) el tipo de investigación exploratorio se debe implementar cuando la problemática es nueva, muy poco abordada en el campo de estudio o desconocida. Se eligió el tipo de investigación exploratorio dado que el problema o el fenómeno es muy poco estudiado, del cual surgen muchas dudas y la información es escasa o muy vaga. Este tipo de enfoque ayudará a que se obtenga más información y así lograr una investigación más completa y eficaz (págs. 106 - 107).

Según Sampieri (2018) la investigación descriptiva es aquella que tiene la finalidad de recolectar datos sobre conceptos, aspectos, características y generalidades determinantes del problema de investigación (págs. 108 - 109). Y es por eso que el autor considera necesario utilizar este tipo de investigación debido a que los temas abordados no han sido estudiados por completo y requiere de una detallada conceptualización de los términos referidos para la comprensión del tema.

El tipo de investigación explicativo es el que tiene como finalidad establecer la causa de la problemática o fenómeno de estudio, así lo explica Sampieri (2018, págs. 110 - 111). Con este tipo de investigación el autor pretende determinar cuál es el origen del problema esto es, las falencias en la cadena de custodia con respecto a la prueba digital, para de esta manera proporcionar un mayor entendimiento del fenómeno.

2.4. Periodo y lugar en donde se desarrolla la Investigación

Esta investigación se desarrolla en la ciudad de Guayaquil, provincia de Guayas. Es en esta ciudad donde se realizan las entrevistas a los profesionales de la materia, revisión de documentos, recolección de datos y análisis de los mismos.

El periodo en el cual se desarrolla esta investigación es desde septiembre del dos mil veintidós hasta agosto del presente año.

2.5. Universo y muestra de la Investigación

En el presente trabajo lo que se pretende brindar es información útil y eficaz sobre la cadena de custodia en las evidencias digitales dentro de los delitos informáticos, por lo que nuestro universo será definido en la población del territorio nacional, debido a que los delitos informáticos son cometidos de manera general en el Ecuador y por ende la aplicación de la cadena de custodia está presente en todo el territorio ecuatoriano.

Se conoce que una muestra es una pequeña parte de la población, es decir un subgrupo y esta pequeña parte de la población es de la cual se recolectarán la data y se entiende que es representativo para generar y analizar datos (Hernández-Sampieri, 2018).

Para este trabajo investigativo la muestra escogida son abogados expertos en derecho penal y agentes investigativos especializados en diferentes ramas de la criminología, en donde se aplicará el método para la recolección de datos en la investigación.

2.6. Método empleado

Se estableció como método para recolectar información el uso de entrevistas. Las cuales se encuentran ubicadas en el enfoque cualitativo.

Como lo define Sampieri (2018) para las entrevistas, el entrevistador aplica un cuestionario a los entrevistados que tengan conocimiento o experticia para brindar mayor información en la investigación (págs. 268 - 269).

Se realizaron entrevistas a profesionales especializados en la rama de Criminalística y Derecho. Dentro de esta entrevista se realizó un banco de

interrogantes, la cual cuenta con seis preguntas relacionadas a la problemática. Estas preguntas fueron dirigidas a cinco abogados y tres agentes investigativos criminalísticos, los cuales dieron su criterio sobre la realidad del manejo de la evidencia digital en la cadena de custodia dentro de los delitos informáticos.

2.7. Procesamiento y análisis

Dentro de la investigación se realizaron siete entrevistas direccionadas a dos grupos especializados. El banco de preguntas fueron las mismas para los dos grupos debido a que quería establecer cuál era el grado de eficacia de la cadena de custodia en las evidencias digitales. El primer grupo estuvo compuesto por cinco profesionales de Derecho y el segundo grupo fue conformado por tres profesionales de la rama de Criminalística.

Esta entrevista está compuesta por seis preguntas, de las cuales la primera interrogante está direccionada a establecer si existe o no un adecuado desarrollo de la normativa ecuatoriana en relación a los derechos informáticos y a partir de esta se extiende cuatro preguntas más las cuales están relacionadas al tratamiento de la evidencia digital y la aplicación de la cadena de custodia, para terminar con la entrevista la última se enfocó en que si la solución de estas falencias demostradas en la investigación pueden ser resueltas estableciendo una normativa detallada para la aplicación de la cadena de custodia en evidencias digitales dentro de los delitos informáticos.

CAPÍTULO 3: ANÁLISIS DE RESULTADOS

Investigación

3.1. Resultados de la Investigación.

Como se mencionó anteriormente en el marco metodológico, se realizaron entrevistas a diferentes profesionales de las áreas de Derecho y Criminalística, con el objetivo de recabar información sobre el tema base de este proyecto de investigación, es decir, la evidencia digital en la cadena de custodia ecuatoriana. Estas entrevistas fueron resueltas por cuatros profesionales de la rama de Derecho y tres profesionales de Criminalística.

Las preguntas elaboradas por el autor son dirigidas a ambos grupos de profesionales y son las siguientes:

1. **Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología, dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?**
2. **¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?**
3. **¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?**
4. **¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?**
5. **¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?**

6. **¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa y no sea válida en el proceso penal?**

3.1.1. Primer grupo de profesionales - Entrevistas a abogados

Estas entrevistas fueron realizadas a cinco abogados para que brinden sus conocimientos, experiencia y sobre todo que expongan la realidad sobre los procedimientos de la cadena de custodia en relación con la prueba digital. Este grupo de abogados está conformado por dos fiscales, una jueza y dos abogados en libre ejercicio.

Las respuestas que se obtuvieron a las preguntas antes detalladas son las siguientes:

Entrevista 1

Entrevistado: Mgtr. César Suarez Pilay, Fiscal.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

En nuestra normativa vigente específicamente en el código orgánico integral penal, existen tipos penales que prevén sanción para los delitos informáticos, tipos penales que han sido incorporados de acuerdo a las realidades que existen en la sociedad ecuatoriana, considerando que el mismo si es eficaz toda vez que permite investigarlos al estar debidamente tipificado en el COIP.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

En cuantos al tratamiento de la evidencia existen diferentes forma de realizar la física de la digital, por ejemplo en una evidencia física el perito va se traslada hasta el lugar, la fija, la embala y luego ingresa al centro de acopio a diferencia de la digital que el perito debe de seguir otros protocolos a efectos de preservar esta evidencia, así por ejemplo tenemos que en el caso de los teléfonos celulares debemos de poner el mismo en modo avión para posteriormente poder extraer la información o si se trata de un servidor esta evidencia debe de ser fijada desde el respectivo equipo.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

Las cadenas y protocolos de evidencia son elaborados acorde al tratamiento que se le debe de dar a cada una de ellas, por lo que considero que en la obtención de su procedimiento pueden existir falencias, ya que a recopilación de las evidencias digitales aún se corre riesgo de que éstas pierdan su validez, ya que no se aplica un procedimiento adecuado de control recurrente de todas las muestras de evidencia recolectadas, mismas que, por no estar a buen recaudo en depósitos idóneos de preservación que en la actualidad están bajo responsabilidad de la Policía Judicial para su custodia sin aplicar los protocolos sugeridos.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Si queremos entender lo que es la cadena de custodia dentro de la informática, lo primero que debemos saber es que necesita un conjunto de datos obtenidos de un análisis inicial.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

Por supuesto que es necesario ya que así tendremos conocimiento de la técnica que utilizaron.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Claro que sí, esto mejorará los respectivos procedimientos en cuanto al manejo de la cadena de custodia, siendo esta de mucha relevancia.

Entrevista 2

Entrevistado: Mgtr. Nino Cassanello Fognini, Abogado en libre ejercicio.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

En agosto de 2021, se agregó al Código Orgánico Integral Penal, la sección de delitos contra la seguridad de los activos de los sistemas de información y comunicación.

Sin embargo, y pese a haber añadido ciertos delitos informáticos, no deja de ser cierto que ciertas situaciones informáticas no encajan en algunas. Además de ello, el problema se suscita realmente en la investigación como tal, tanto en la etapa pre procesal como en la etapa procesal.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

No realmente. Suele entrar por cadena de custodia el dispositivo que originalmente contiene la información. El departamento pericial especializado en la pericia pertinente procede a realizar la pericia ordenada.

En caso de no poder acceder al equipo en el que se ha originado la información, **creería que** la información pertinente, debería ser copiada a otra memoria, iniciando en la transferencia de información la pertinente cadena de custodia.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

No he tenido un caso en estas circunstancias, pero teniendo en consideración que la integridad de la cadena de custodia de evidencia en muchos casos es violada, lo más probable es que se presenten falencias con la prueba digital.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

No tengo conocimiento de esto, pero a más de las herramientas, dada a la novedad de los delitos, me preocupa también la respectiva educación del personal especializado en la obtención, recolección y explotación de este tipo de evidencias.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

Sí. Totalmente. Al igual que en cualquier otro tipo de informe pericial, la técnica que es aplicada en el análisis de la evidencia es crucial. De hecho, es lo mínimo que debe contener en concordancia con lo establecido en el Art. 511, número 6 del COIP. Es crucial para poder analizar, defender, objetar o impugnar la referida prueba por las partes, como elemento de cargo o descargo.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Sí, evidentemente, establecer una normativa detallada respecto al procedimiento minimizará los riesgos de viciar la cadena de custodia de la evidencia digital.

Entrevista 3

Entrevistado: Abg. Irma Gómez Medina, Jueza.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

La ley de fecha 7 de febrero de 2023, en algo ayuda, pero hay ausencia de tipicidad de los delitos transnacionales, porque ahora, el ciberespacio es donde se comete y está fuera del alcance de nuestra legislación.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Por supuesto, la diferencia más obvia es la ubicación, un lugar que es intangible, indeterminado; a diferencia de la física que ocupa un espacio determinado (lugar específico) por lo que las personas que son víctimas de éstos delitos, y más aún las que ignoran la tecnológica y su modo de uso, por desconocimiento, no acuden a las autoridades competentes.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

Si considero que existen falencias en la aplicación, muchas de estas son por el escaso personal capacitado, por la multiplicidad de éstas infracciones penales y su forma de obtención que las debe hacer profesionales en esa área. Considero que se vuelve una odisea practicar correctamente la cadena de custodia.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Tengo conocimiento que la policía criminalística maneja este tipo de herramientas, pero desconozco si son lo suficientemente eficientes, pero insisto con que la falta de normativa y el escaso personal capacitado es el problema.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

Por supuesto es muy importante indicar porque forma parte de la defensa, acceder cuál fue la técnica a usarse. Y en realidad eso es el debido proceso

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Los reglamentos deben auxiliar a la ley, por lo que en mi opinión si es importante detallar una normativa que detalle el procedimiento para la aplicación de la cadena de custodia. Pero también creo que es importante que Ecuador forme parte del convenio de Budapest, donde ellos son pioneros para combatir delitos, respetando el debido proceso.

Entrevista 4

Entrevistado: Abg. Diego Paredes Paredes.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

No, Ecuador está totalmente atrasado frente a la problemática de los delitos informáticos. Además, la tecnología para contrarrestar dichos delitos es caduca, y muchas veces inexistente en nuestro país.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Si existen, ya que el cuidado para que estás no se contaminen son con protocolos distintos, la cadena de custodia para el uno es más portátil y manual, la de digitales puede ser a través de la red.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

Creería que sí ya que muchas veces los operadores de justicia no solicitan cadena de custodia desde un principio, siendo esto necesario para el debido proceso y al ser extemporáneo la cadena de custodia la misma ya pudo haber sido contaminada.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

En realidad, conozco muy pocas, más que las de respaldos de IP y demás tecnologías a través de la explotación, ejecutado con la autorización de la autoridad competente.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

No creo necesario, como dije la explotación de equipos tecnológicos son los únicos que conocemos actualmente, no se dé la existencia de software o hackers de contrainteligencia para verificar que no se cambie datos por la red cuando se custodia empresas digitales.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Absolutamente, considero importantísimo que se cree un reglamento donde se detalle el procedimiento de cada una de las técnicas para la custodia de las evidencias digitales, más aún si no estamos a la vanguardia de cómo proteger datos y normativa interna para resguardar los mismos.

Entrevista 5

Entrevistado: Mgtr. Marcos Ordeñana Baldeón, Fiscal.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

Como sabemos, efectivamente el avance de la sociedad es ínsito al desarrollo de las tecnologías y por lo mismo el aparecimiento de nuevas formas de criminalidad que el legislador ha tenido que tipificar como conductas penalmente relevantes. Así, los tipos penales como la estafa, la extorsión, la pornografía infantil, etc. han emigrado a los espacios cibernéticos.

Sin embargo, pese al esfuerzo del órgano legislativo en adecuar dichas conductas a los ordenamientos jurídicos en materia criminal, sigue produciéndose un fenómeno en torno a la comisión de los mismos: la impunidad. Eso evidencia que el desarrollo del marco normativo de los delitos informáticos o de los delitos cometidos a través de medios informáticos definitivamente no ha tenido un desarrollo eficaz, tanto en lo sustantivo como en lo adjetivo. En lo sustantivo por la obvia incapacidad del Estado en advertir las conductas delictivas que se avecinan en torno al aparecimiento de las nuevas tecnologías, o incluso de las que ya se

están desarrollando, pues la ciberdelincuencia constituye una conducta que no corresponde solamente al ámbito de la individualidad de un hacker por ejemplo, sino en verdadera estructura criminal organizada que opera desde la extraterritorialidad, lo que complica el aspecto procesal de aplicación de una normativa interna que carece los ribetes necesarios para hacer frente a este monstruo invisible.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Los elementos físicos consisten en los objetos materiales que en el trayecto de la investigación criminal y proceso penal deben ser materia de recolección, envío, manejo, análisis y conservación, a fin de que se garantice su autenticidad desde que son encontrados en el lugar de los hechos hasta que sean presentados como prueba en el juicio, según el caso. Por ello objetos o materiales biológicos como armas, huellas, pelos, fluidos, frecuentemente relacionados con delitos contra la inviolabilidad de la vida o la integridad sexual, entre otros, se constituyen en elementos físicos a los que necesariamente deben someterlos a cadena de custodia.

Existen delitos en los que en forma directa o indirecta se utilizan medios tecnológicos para su comisión. Por ser dichas infracciones de tipo informáticas o encontrarse relacionada su comisión por medios informáticos, se requiere de evidencia o prueba digital para poderlas probar. Por lo tanto, registros como correos electrónicos, archivos e imágenes almacenados en equipos tecnológicos deben ser objeto de cadena de custodia para que tengan validez jurídica al momento de ser presentados en el juicio.

En consecuencia, desde lo estrictamente normativo, no existe una diferencia en el tratamiento de la evidencia física y la digital, en lo que a cadena de custodia se refiere.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

En el lugar de los hechos siempre quedan indicios relacionados al delito, los cuales en muchas ocasiones se constituyen en la punta del ovillo que se genera para el esclarecimiento de las investigaciones.

Por esa razón la ley regula un mecanismo para poder identificar los indicios encontrados en la escena del crimen, desde que son recogidos hasta que son presentados como prueba en el juicio, siendo aquel mecanismo la cadena de custodia.

Esto se aplica tanto a la evidencia física como a la digital. Sin embargo, en la práctica apreciamos que existen marcadas diferencias al momento de iniciar la cadena de custodia en uno o en otro. En el caso de la evidencia física no existen complicaciones mayores. El problema se presenta en las evidencias digitales, donde existen falencias en el procedimiento especialmente relacionado con la cadena de custodia, en unos casos, por desconocimiento en cuanto a su tratamiento, en otros, por la falta de medios técnicos adecuados para su obtención.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Estamos atravesando por un momento de un correcto manejo de la política criminal que repercute en carencia de necesidades básicas para la investigación preprocesal o procesal penal como la falta de logística e insumos en cada una de sus áreas técnico-científicas, por ejemplo, la carencia de reactivos en las pruebas de alcotest en los casos de tránsito o psicosomáticas en casos de drogas.

Si en esos casos comunes no existen las condiciones adecuadas para la práctica de ciertas pruebas indispensables para el esclarecimiento de los hechos,

imagínense en los delitos informáticos que revisten una complejidad técnica de mayor profundidad como podrían ser por ejemplo equipos de alta capacidad o de punta.

Ello demuestra que definitivamente no existen las herramientas adecuadas para dar inicio a la cadena de custodia, como cuando en un equipo de grabación privada se ha registrado un hecho delictivo común también, y no se cuenta siquiera con un CD para levantar la información en el mismo lugar de los hechos. Es decir, la cadena de custodia se rompe desde el inicio de su tratamiento, puesto que generalmente cuando la Fiscalía requiere tal información días después por no haberla podido levantar in situ, la misma ya ha sido eliminada de la memoria de los equipos por falta de espacio, ya que los registros recientes reemplazan a los antiguos, perdiéndose la oportunidad de recabar indicios digitales necesarios para el esclarecimiento de los hechos.

A todo ello se suma, la falta de personal especializado en delitos informáticos, tanto a nivel de la policía como de la fiscalía, que como se sabe, son los entes responsables de la investigación, ya que los que hay, son insuficientes ante la vorágine delictiva de delitos informáticos o de delitos en los que se usan los medios informáticos.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

En el sistema procesal acusatorio que rige nuestro sistema de administración de justicia penal emergen principios como el de contradicción, inmediación y publicidad que garantizan la transparencia de cada una de las actuaciones del juicio, entre ellas la de la actividad probatoria.

En ese contexto el análisis digital forense tiene por objetivo principal la extracción de datos digitales relacionados con las pruebas electrónicas que conllevan a una conclusión en base a la cual el juez tomará una decisión. Por lo

tanto, es indispensable que se detalle el tipo de técnica digital empleada en la práctica y conclusión de la pericia, sobre lo cual incluso así lo exige el Art. 511 numeral 6 del Código Orgánico Integral Penal, que exige que el informe debe de contener entre otros aspectos “la técnica utilizada”.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

En el Código Orgánico Integral Penal no existe una normativa específica para el tratamiento de evidencia digital. Apenas en el Art. 456 se hace referencia a que se aplicará cadena de custodia tanto a los elementos físicos como digitales. Así en forma general y sin ninguna diferenciación técnica o conceptual.

Para tratar de regular esta ineficiencia procesal, se emite una resolución en el cual se expide un manual enfocado en las áreas indispensables en la investigación penal.

Sin embargo, la problemática persiste, por lo cual efectivamente considero que ante la falta de una diferenciación técnica y conceptual existente en nuestra legislación actual sobre la cadena de custodia que se le da tanto a las evidencias físicas como a las digitales, resulta indispensable establecer una normativa adecuada para el procedimiento específico en relación al tratamiento de los indicios recabados a propósito de los delitos informáticos o de los delitos que se ejecutan con el empleo de medios informáticos, a fin de que la misma no queden en simples directrices institucionales o manuales técnicos sino que formen parte de nuestro ordenamiento positivo.

3.1.2. Análisis del primer grupo de profesionales (Abogados)

Los resultados de estas entrevistas arrojan por unanimidad que el desarrollo de la normativa ecuatoriana en relación a los delitos informáticos no es apropiado para la época de evolución tecnológica que existe, es decir que se encuentra atrasada en esta área del derecho cibernético. Los profesionales de Derecho consideran que las evidencias digitales si tienen diferente tratamiento a las evidencias físicas por lo que creen necesario que se usen correctamente las herramientas, se especifique y se conozca el tipo de técnica utilizada para la valoración de la misma. Asimismo, indican que algunos de los problemas son la falta de personal profesional altamente capacitado para la correcta aplicación de la cadena de custodia a causa de que no se ha implementado una normativa que establezca los procedimientos de manera detallada para el tratamiento de la evidencia digital en los delitos informáticos.

3.1.3. Segundo grupo de profesionales – Entrevistas a expertos en Criminalística.

Estas entrevistas dirigidas a tres profesionales de Criminalísticas, tienen el objetivo de demostrar si el desarrollo normativo de la cadena de custodia en Ecuador logra su propósito, el cual es resguardar la prueba en su integridad para que posteriormente pueda ser válida en un proceso penal. Fue seleccionado para este grupo de profesionales a un perito en criminalística, perito en balística forense y un perito en informática.

Las respuestas que se obtuvieron a las preguntas antes detalladas son las siguientes:

Entrevista 1

Entrevistado: Lcdo. Alberto Stalin Gutiérrez Tigse, Perito en balística forense.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

Como docente de la carrera de criminalística, puedo decirte que el crecimiento de los delitos informáticos es una preocupación creciente en el contexto de la evolución tecnológica y la sociedad digital. En cuanto a la normativa ecuatoriana en relación a los delitos informáticos, es importante analizar su eficacia para abordar esta problemática.

En términos generales, la efectividad de la normativa ecuatoriana en relación a los delitos informáticos depende de diversos factores. Es necesario evaluar la claridad y amplitud de las leyes existentes, así como su capacidad para abordar las formas emergentes de delincuencia cibernética. Además, es importante considerar la capacidad de aplicación y cumplimiento de las normas, así como los recursos destinados a la investigación y persecución de estos delitos.

En el ámbito internacional, existen estándares y convenios que buscan armonizar la legislación en materia de delitos informáticos. Ecuador, como parte de la comunidad global, ha trabajado en la implementación de instrumentos internacionales y ha promulgado leyes para enfrentar este tipo de delincuencia. Sin embargo, es fundamental evaluar la adecuación de estas leyes a los desafíos específicos que plantea el panorama de los delitos informáticos.

Para determinar la eficacia de la normativa ecuatoriana, es recomendable analizar casos emblemáticos, investigaciones y resultados judiciales relacionados con delitos informáticos en el país. Asimismo, se deben considerar las opiniones y análisis de expertos en el campo de la ciberseguridad y el derecho digital.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Sí, existen diferencias notables en el tratamiento de las evidencias digitales en comparación con las evidencias físicas. A continuación, te mencionaré algunas:

Tienen características diferentes, las evidencias digitales son intangibles y se encuentran almacenadas en dispositivos electrónicos o en redes informáticas. Por otro lado, las evidencias físicas son objetos concretos, como armas, huellas dactilares, sustancias químicas, entre otros.

Sus métodos de obtención también son diferentes ya que, para obtener evidencias digitales, se requiere el uso de herramientas y técnicas específicas para el análisis forense digital, como la extracción de datos de dispositivos electrónicos o el análisis de metadatos. En contraste, las evidencias físicas se obtienen a través de inspecciones, recolección y preservación de objetos físicos en el lugar del delito.

Otra diferencia radica en que las evidencias digitales pueden ser altamente complejas y voluminosas, ya que incluyen archivos digitales, registros de actividad, comunicaciones en línea, entre otros. Esto hace que se requiera de habilidades técnicas especializadas para su manejo y análisis. En comparación, las evidencias físicas suelen ser más tangibles y su análisis puede implicar técnicas más tradicionales, como análisis de huellas o análisis químicos.

Su forma de rastreo y la trazabilidad también tienen diferencias, las evidencias digitales pueden ser más fácilmente rastreadas y tienen un alto potencial para dejar registros electrónicos de su manipulación. Por otro lado, las evidencias físicas pueden ser más difíciles de rastrear y su trazabilidad puede depender de las circunstancias y características particulares de cada caso.

Lo anterior se encuentra estrechamente relacionado con los factores de vulnerabilidad y manipulación de las evidencias mientras las digitales son más susceptibles a la manipulación, la alteración o la destrucción involuntaria, ya que

pueden ser modificadas fácilmente mediante acciones en los sistemas informáticos, las evidencias físicas en cambio suelen ser más resistentes a la manipulación, aunque también es posible que sufran daños o alteraciones.

Es importante destacar que estas diferencias no implican que el tratamiento de las evidencias digitales sea más importante o menos importante que el de las evidencias físicas. Ambos tipos de evidencias son fundamentales en las investigaciones criminales y requieren un enfoque riguroso y especializado en cada caso, teniendo en cuenta las particularidades de cada uno.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

En general, puedo decir que, en el ámbito de los delitos informáticos, la aplicación de la cadena de custodia de las pruebas digitales puede presentar ciertas falencias o desafíos específicos. Por ejemplo, te puedo mencionar algunos aspectos que podrían considerarse como posibles falencias en el procedimiento de obtención de la prueba digital:

1. La preservación de la integridad de las pruebas digitales ya que es fundamental para garantizar su validez y admisibilidad en un proceso judicial. Sin embargo, las pruebas digitales pueden ser fácilmente modificadas, eliminadas o corrompidas si no se toman las precauciones adecuadas. Esto puede plantear desafíos adicionales en comparación con las pruebas físicas, donde la manipulación suele ser más evidente.
2. La obtención de pruebas digitales requiere técnicas especializadas y herramientas forenses digitales apropiadas por lo que es esencial asegurarse de que las pruebas sean recolectadas y extraídas de manera adecuada, siguiendo los protocolos establecidos y evitando la alteración accidental o intencional de la evidencia. La falta de

conocimientos o recursos especializados en el manejo de pruebas digitales puede ser una posible falencia en el proceso de obtención.

3. La trazabilidad y la autenticidad de las pruebas digitales, como dije anteriormente, son aspectos esenciales para establecer su validez y confiabilidad. El seguimiento de la cadena de custodia digital y la garantía de que las pruebas no hayan sido manipuladas o alteradas durante su recolección y análisis pueden resultar más desafiantes en comparación con las pruebas físicas.

4. En mi experiencia puedo afirmar que la colaboración interdisciplinaria puede llegar a representar una falencia debido a que los delitos informáticos suelen requerir una colaboración estrecha entre expertos en diferentes áreas como la informática forense o el derecho digital. La falta de coordinación efectiva y comunicación entre estas disciplinas puede generar falencias en el proceso de obtención de pruebas digitales y su posterior análisis.

Cabe destacar que las falencias en el procedimiento de obtención de la prueba digital pueden variar dependiendo de los recursos disponibles, el nivel de capacitación del personal encargado y las particularidades de cada caso. Es esencial que las autoridades competentes promuevan la formación continua y el uso de buenas prácticas en la obtención y manejo de pruebas digitales para minimizar las falencias y garantizar la validez y confiabilidad de las evidencias en los delitos informáticos.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Desconozco, dado que mi área de especialización es otra (balística forense) no podría establecer si existen las herramientas y menos aún si son las adecuadas.

Esta es una pregunta muy específica del área por lo que sugiero consultar a un perito especializado en la materia.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

Sí, al igual que en todas las disciplinas forenses detallar el tipo de técnica o metodología que el perito utiliza en sus análisis es una parte fundamental de su trabajo ya que le permite demostrar de forma científica, categórica y fehaciente sus resultados ante el órgano judicial competente. En este sentido la obtención y análisis de la prueba digital no es ajena a este principio de trabajo y abarca una amplia gama de técnicas y metodologías que se aplican para su investigación y recolección.

Una premisa básica del trabajo forense es precisamente la elección de la técnica adecuada que dependerá del tipo de delito, el contexto de la investigación y la naturaleza de la prueba en cuestión. Al detallar el tipo de técnica utilizada, se proporciona una base sólida para el análisis y la evaluación de la prueba, y también permite a los expertos y profesionales en el campo comprender mejor el enfoque utilizado y la validez de los resultados obtenidos.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Sí, considero que establecer una normativa detallada al respecto puede ser beneficioso y contribuir a disminuir el riesgo de que dicha cadena se rompa.

Teóricamente la cadena de custodia se define como uno de los procesos cruciales dentro de la investigación criminalística, su fin es asegurar la integridad, autenticidad y trazabilidad de las evidencias durante su recolección, almacenamiento, transporte y presentación en un proceso judicial. En el caso de las

evidencias digitales, donde la manipulación o alteración accidental o intencional es más factible, resulta especialmente importante establecer pautas claras y específicas.

Al establecer una normativa detallada, se brinda un marco de referencia claro para todos los actores involucrados en la gestión de evidencias incluyendo investigadores, peritos, agentes de la ley y profesionales del derecho promoviendo una mayor uniformidad en los procedimientos y reduciendo el riesgo de que se cometan errores o se incurra en prácticas inadecuadas que puedan comprometer la integridad de la cadena de custodia.

Sin embargo, es importante tener en cuenta que la normativa por sí sola no es suficiente. También se requiere una cultura de cumplimiento, capacitación continua y recursos adecuados para implementar y mantener efectivamente los procedimientos establecidos.

Entrevista 2

Entrevistado: Lcda. Mayra Arias, Licenciada en Informática.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

Considero que el avance que ha tenido Ecuador en cuanto a su normativa ha sido significativo, reconocemos una gran variedad de delitos informáticos, pero lo que falta es incentivar a la socialización y conocimiento de las normas legales.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Si existen diferencias, son muy obvias que pueden darse por irrelevantes. Las evidencias físicas sólo son tangibles, mientras que las evidencias digitales son las intangibles, aunque por lo general debemos obtenerlas de un objeto tangible. Pero si tuviera que decir que en el tratamiento existen diferencias notorias entre las dos evidencias, diría que no.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

Entendería que las falencias provienen del desconocimiento del personal profesional encargado y este desconocimiento se da básicamente por dos causas, falta de especificación en la normativa en relación a los procedimientos y la falta de capacitación para los encargados de criminalísticas sobre estas normativas.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Como profesional en esta área puedo decir que existen las herramientas para poder realizar un tratamiento, pero no descarto la idea que si tuviéramos herramientas más adecuadas y avanzadas sería mejor. Con respecto al uso, repito falta capacitación para los profesionales.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

En mi opinión si es necesario detallar el tipo de técnica así le da validez a la prueba. En los modelos de informes que sirven para presentar la prueba a la Fiscalía y a CJ en uno de sus puntos se pide detallar el tipo de técnica.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Si considero importante la existencia de esta normativa, quiero indicar que, si existe, abarca temas importantes en cuestión de la cadena de custodia en la evidencia digital, pero aún así no es lo suficientemente detallada por lo que creo importante se establezcan y se profundicen algunos procedimientos para que estos sean aplicados correctamente por los profesionales y así resguardar la evidencia digital.

Entrevista 3

Entrevistado: Juan Carlos Pintag Jiménez, Perito en Criminalística.

Actualmente el cometimiento de los delitos informáticos ha tenido un crecimiento significativo debido al desarrollo de la sociedad junto a la tecnología dado que se crean nuevos modos de delinquir por el uso de los medios informáticos. ¿Usted considera que el desarrollo que ha tenido la normativa ecuatoriana en relación a los delitos informáticos es eficaz?

No, debido a que día a día, los modos de delinquir son más modernos debido al uso de la tecnología, por lo que los delitos informáticos van tomando fuerza y las legislaciones no son vigentes no son suficientes.

¿De acuerdo a su conocimiento existe una diferencia notoria en el tratamiento de las evidencias digitales y las físicas? ¿Cuáles serían?

Si existen diferencias porque las características de la evidencia física son visibles y la evidencia digital es necesario de un equipo o software para verificar el contenido de la prueba como tal.

¿Considera usted que al momento de aplicar la cadena de custodia se presentan falencias en el procedimiento de la obtención de la prueba digital dentro de los delitos informáticos?

Sí porque se debe proteger la información in situ y al no tener un personal capacitado conociendo el protocolo porque no contamos con un reglamento donde se especifique los procedimientos a seguir en las evidencias digitales, existe un caos al momento de obtener la prueba.

¿Conoce si existen las herramientas adecuadas o que el uso es el correcto al momento de llevar a cabo la cadena de custodia de la prueba digital dentro de los delitos informáticos en el Ecuador?

Honestamente no tengo conocimiento si tenemos las herramientas adecuadas, pero sí podría decir que no estamos preparados de manera tecnológica para resguardar y evaluar estos tipos de evidencias. La tecnología evoluciona y Ecuador no tiene un desarrollo como los países de primer mundo. Además, como he mencionado, no hay un personal profesional altamente capacitado.

¿Cree que es necesario detallar el tipo de técnica digital forense que es utilizada en la prueba digital dentro de los delitos informáticos?

Es necesario conocer el tipo de técnica que es utilizada en la prueba digital, conocer el procedimiento y sobre todo estar consciente que esa técnica es la propicia para evaluar la evidencia digital.

¿Usted considera que establecer una normativa detallada del procedimiento adecuado para la aplicación de la cadena de custodia en evidencias digitales disminuiría el riesgo de que la misma se rompa?

Efectivamente el crear una normativa, ya sea un reglamento, protocolo o manual en el que se describen los procedimientos, es decir los pasos a seguir,

generaría que haya una disminución en los casos en los que la prueba digital se ve viciada.

3.1.4. Análisis del segundo grupo de profesionales (Expertos en Criminalísticas)

Las entrevistas a este grupo de expertos fueron con la finalidad de palpar la realidad sobre la aplicación de la cadena de custodia, expusieron sus conocimientos tanto teóricos como prácticos para establecer sus criterios sobre el tema principal. Los peritos explicaron que aún falta por desarrollar normativa en relación a los delitos informáticos; es más indicaron que la inexistencia o vaga normativa sobre los procedimientos de la cadena de custodia con respecto a la evidencia digital, crea ineficacia en el procedimiento penal debido al mal empleo de este medio para obtener, resguardar, valorar las pruebas.

3.2. Análisis.

Los resultados que fueron obtenidos por medio de las entrevistas ayudaron a demostrar que los entrevistados consideran escaso el desarrollo de la normativa ecuatoriana en relación a la ciberdelincuencia o delitos informáticos, desconocen si el uso de las herramientas es el adecuado y consideran de suma importancia que se especifique el tipo de técnica que se utiliza en cada prueba digital.

Todos los entrevistados indicaron que existen falencias en el tratamiento de la cadena de custodia en las evidencias digitales. De hecho, se estableció que la falencia principal es que no existe o es muy vaga una normativa (reglamento, manual, protocolo) que detalle los diferentes procedimientos a seguir en relación a resguardar la evidencia digital. Sin embargo, se considera otro problema latente que el personal profesional no esté capacitado, la cual tiene mucha lógica que esta dificultad sea una consecuencia de la falta de normativa.

Una de nuestras expertas en Criminalísticas detalla en su intervención que, a pesar de la existencia de una normativa para los procedimientos de la evidencia digital, considera que no se ha profundizado ni detallado los procedimientos, por lo que cree importante que se amplíe la información de manera más detallada, además que se actualice debido a que está en constante fluctuación porque está sujeta al avance de la tecnología. Es importante establecer esta normativa para tener un tratamiento eficaz de la evidencia digital desde su obtención hasta su validación en el proceso penal.

CAPÍTULO 4: PROPUESTA

Propuesta

Título de la Propuesta

Creación de Reglamento especial para la aplicación de la cadena de custodia en evidencia digital dentro de los delitos informáticos.

Objetivo

Proponer que se cree un reglamento, manual o instructivo que especifique todos los procedimientos y pasos a seguir para resguardar la evidencia digital; debido a que la finalidad de la cadena de custodia es preservarla para que se válida en el proceso penal.

Justificación

Ecuador se encuentra atrasado en la normativa relacionada a la ciberdelincuencia, ciberdelitos y demás temas relacionados. Se conoce que uno de los muchos problemas característicos que presentan los ciberdelitos o delitos informáticos, son que las pruebas pueden ser alteradas, ocultadas, modificadas con mucha facilidad y por lo tanto genera una mala eficacia en el sistema investigativo. El problema en mención no es solamente para Ecuador, también se considera una dificultad para todos los países incluso los países suscritos al Convenio de Ciberdelincuencia de Budapest.

Como se puede evidenciar en la investigación, el tema cadena de custodia como tal no ha sido objeto de mucho estudio en el ámbito legal, debido a que se considera que este tema es más doctrinario; y mucho menos con relación a un enfoque nuevo como lo es la evidencia digital. En toda la legislación ecuatoriana son muy pocos los artículos donde se menciona a la cadena de custodia, como por ejemplo en el art. 500 del Código Orgánico Integral Penal (COIP). Por lo que se deja a toda esta información en doctrina, conocimientos a base de experiencia y en

directrices internas de ciertas instituciones, creando falencias para la ejecución de la misma.

Está comprobado por los expertos que una causa relevante para la admisibilidad de las pruebas no es admitida puesto que se rompió la cadena de custodia y perdieron veracidad o integridad. Y esto se incrementan en las evidencias digitales porque gracias a su naturaleza son pruebas que pueden ser alteradas y destruidas fácilmente, por lo que tener descrito el procedimiento a seguir en este sistema para resguardar la prueba beneficiaria a la aplicación de la misma.

Viabilidad

Esta propuesta dirigida a proponer la creación de reglamento especial a la aplicación de la cadena de custodia en evidencias digitales para el personal investigativo, es viable debido a que es un reglamento interno y especial, esto significa un conjunto de normas o reglas cuya finalidad es regular las actividades de una comunidad en particular. Este reglamento ayudará a establecer un adecuado sistema para la protección de esta prueba.

Beneficiarios

Se podría establecer que existen dos tipos de beneficiarios a raíz de esta propuesta; beneficiarios directos e indirectos.

Los beneficiarios directos de esta propuesta son las víctimas, es decir personas a las que se le ha generado un daño o afectación, del cometimiento de un delito informático.

Los beneficiarios indirectos son el sistema especializado de investigación, abogados, debido a que recibirán mejores herramientas, capacitaciones técnicas/teóricas y una base legal para la ejecución de sus trabajos.

Descripción de la propuesta

Con la implementación de este reglamento, lo que se busca es que existan reglas especiales donde se detalle procesos, técnicas y procedimientos que ejecutan los agentes investigativos para el resguardo y la valoración del material probatorio.

Debido a la naturaleza de estas evidencias, es decir que proviene de delitos informáticos, se entiende que este reglamento en casi la totalidad del contenido, será técnico, lo que significa que para consolidar este reglamento necesitaremos personal experto en constante actualización en informática y delitos informáticos. Esta información que será obtenida de estos profesionales, será plasmada en este reglamento que será publicado para que sea de conocimiento público.

En conjunto a esta propuesta escrita, se deberá capacitar al personal profesional. Esta capacitación deberá ser tanto teórica, es decir tener el conocimiento de las reglas y procesos establecidos por el reglamento; y práctica, decir en la ejecución de los procesos para que exista una eficacia en la labor investigativa.

Este reglamento deberá contener información actualizada de:

- Procedimientos respectivos para cada tipo de evidencia digital.
- Procedimiento para manejar la escena. (Observación del lugar de los hechos)
- Procedimiento de obtención de la evidencia digital.
- Procedimiento de embalaje de la evidencia digital.
- Procedimiento de sellado y rotulación de la evidencia digital.
- Procedimiento de traslado de evidencia digital al centro de acopio.
- Procedimiento de ingreso de la evidencia digital al centro de acopio.
- Detalle de las diferentes técnicas periciales sobre la evidencia digital.
- Procedimiento con el uso adecuado de las herramientas en las diferentes técnicas periciales.

- Demás temas relevantes para asegurar la eficacia de la cadena de custodia.

Conclusiones

De este trabajo de investigación hemos obtenido las siguientes conclusiones:

- De las investigaciones sobre la normativa se puede establecer que la legislación ecuatoriana en el campo de delitos informáticos no ha sido desarrollada de manera eficaz, permitiendo que en el proceso penal existan dificultades prácticas.
- Con respecto a los estudios de doctrina y de legislaciones de otros países, se concluye que es de suma importancia establecer una reglamentación dirigida al tratamiento de las evidencias digitales, por lo que no pueden ser tratadas de la misma manera que una evidencia física, debido a su naturaleza y características.
- Por medio de la ejecución del método de la entrevista, se evidenció que no existe la aplicación adecuada debido a la reglamentación desactualizada sobre el manejo de las evidencias digitales con respecto a los delitos informáticos, este manejo abarca desde los procedimientos de obtención, tratamiento de protección, técnicas periciales y demás métodos para resguardar la integridad de la evidencia hasta que ingrese al proceso penal.
- Las opiniones expuestas por medio de las entrevistas también arrojaron que es la falta de conocimiento y la ausencia de personal capacitado en el área, lo que genera que exista problemas en el resguardo y tratamiento de la evidencia digital.
- Por último, las investigaciones dieron como resultado que Ecuador no se encuentra suscrito al Convenio de Ciberdelincuencia de Budapest, ni a ningún otro convenio que coopere de manera internacional con respecto a los delitos informáticos; siendo el primero un convenio internacional importante para que exista una cooperación con respecto a los delitos informáticos tanto en el ámbito normativo como investigativo.

Recomendaciones

Las recomendaciones del presente proyecto de investigación son las siguientes:

- Se recomienda tener presente esta propuesta para el ámbito jurídico/digital, con la finalidad que, en el futuro, cuando la tecnología siga avanzando y existan más modos de delinquir acoplados a los avances de tecnológicos, se busque evitar inconsistencias e irregularidades en el resguardo de las evidencias digitales dentro de los delitos informáticos.
- Se recomienda que se empiece el proceso de adhesión al Convenio de Budapest sobre Ciberdelincuencia.
- Se recomienda que el Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses realice constantes actualizaciones en los protocolos o instructivos creados, con la finalidad de desarrollar eficazmente la normativa procesal penal.
- Se recomienda que el Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses mediante charlas, programas o capacitaciones, instruya al personal encargado del sistema investigativo en la cadena de custodia de evidencias digitales con respecto a los procedimientos establecidos en la normativa.
- Se recomienda establecer una normativa especial para los derechos informáticos, esta normativa contará con la parte sustantiva y adjetiva.

Referencias bibliográficas

Arellano, L., & Castañeda, C. (2012). La cadena de custodia informático-forense. *ACTIVA*, 67-81.

Arias, F. (2012). Proyecto de investigación: introducción a la metodología científica. *Caracas: Espíteme*, 16.

Arrabal, P. (2019). *Tratamiento procesal de la prueba tecnológica .* Universidad Miguel Hernández.

Asamble Nacional del Ecuador. (2015). *Código Orgánico General de Procesos.*

Asamblea Naciona del Ecuador. (2014). *Código Orgánico Integral Penal.*

Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito : Registro Oficial Sumplemento 180 de 10 de febrero de 2014.

Asamblea Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.*

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador.*

Aton. (2009). *Cadena de Custodia.* Arequipa, Peru.

Bujosa, L., Bustamente, M, & Toro, L. (2021). La prueba digital produto de la vigilancia secreta: obtención, adminisibilidad y valoración en el proceso penal en España y Colombia. *Deireito Processual Penal*, 1347 - 1384.

Cantos, X. (2021). *Valoración de la prueba digital en los delitos informáticos.* Quito: UMET.

Chávez, E. (2002). Comentarios a la Ley de Comercio Electrónico. Quito, Ecuador.

Chavez, E. (2013). *La cadena de custodia en el Sistema Procesal Penal.* Quito, Ecuador: Universidad Internacional Del Ecuador.

Chiluiza, E. (16 de Septiembre de 2017). *El correo electrónico como prueba digital.* Obtenido de El Universo: https://www.eluniverso.com/opinion/2017/09/16/nota/6382855/correo-electronico-comoprueba-judicial/

Christen, G., & Kirschner, A. (2022). *Teoria crítica do processo.* Belém,: Rfb.

Colombiana, F. d. (2006). *Reglamento de la Cadena de Custodia de elementos materiales, evidencias y administración de bienes incautados .* Colombia.

Consejo de Europa. (2004). *Convenio de Ciberdelincuencia .* Budapest.

Davara, M. (1990). Análisis de la Ley de Fraude Informático. *evista de Derecho de UNAM*.

Decreto Ejecutivo 1651. (2001). *Reglamento de la Policia Judicial.*

Donna, Edgardo, & Ledesma. (2011). La Investigación Penal Preparatoria. *Revista de Derecho Procesal Penal*, 190.

Fiscalia General Del Estado. (2014). *MANUALES, PROTOCOLOS, INSTRUCTIVOS Y FORMATOS DEL SISTEMA ESPECIALIZADO.*

Fiscalia General Del Estado. (s.f.). *Protocolo del Centro de Acopio.*

Gross, H. (1892). *Manual del Juez de Instrucción como Sistema de Criminalística.* Bolivia.

Guimaraes, D., Moller, G., & Kirschner, A. (2022). *Teoria Crítica do Processo.* RFB Editora.

Gúzman, C. (2018). *El examen de la escena del crimen.* Buenos Aires: Julio Cesar Faira.

Hermoza, P. (2007). *La Cadena de Custodia en el nuevo Proceso Penal.* Lima: La Reforma.

Hernández-Sampieri, R. (2018). *Metodología de la Investigación. .* Ciudad de México: McGraw-Hill Interamericana Editores.

Jimenez, J. (s.f.). *La escena del Crimen en el criminal profiling. .*

Kvitko, L. (2006). *Escena del Crimen.* Buenos Aires, Argentina: La Rocca.

Lacalle, A. (2018). *El impacto de las redes sociales y de la mensajería instantánea en la fase probatoria laboral.* Obtenido de Ius Labor.

López, P. (2022). *Investigación Criminal y Criminalística.* Bogotá: TEMIS S.A.

Lopez, P., & Gómez, P. (2010). *Investigación criminal y criminalística.* Colombia: Editorial Temis.

Manosalvas, C. (2019). *La cadena de custodia en el proceso penal.* Otavalo: Universidad de Otavalo.

Manual de Cadena de Custodia de la Policia Nacional. (2007). Quto, Ecuador: Registro Oficial N°.156.

Marin, J., & García, G. (2014). Problemas que enfenta la prueba digital en los Estados Unidos de Norteamerica. *Estudios de la Justicia*, 75-91.

Martinez, G. (2022). Prblematica juridica de la prueba digital y sus implicaciones en los principios penales. *Revista Electronica de Ciencia Penal y Criminología*.

Mayer, L. (2017). El bien juríco protegido en los delitos informáticos . *Revista Chilena de Derecho, vol. 44, núm. 1*, 235-260.

Mendoza, E., & Urdaneta, E. (2005). La telemática y los delitos informáticos en Venezuela. *élématique, vol. 4, núm. 1,*, 124-140.

Morillo, M., & Herrero, A. (2011). *La prueba digital y la cadena en el Ordenamiento Jurídico Costarrincense. Alchoholemiow y prueba con alcoholimetro.* Costa Rica.

Nalvarte, G. (2016). *APLICACIÓN DE TÉCNICAS EN EL ESTUDIO SISTEMÁTICO DE INDICIOS BIOLÓGICOS RECOGIDOS EN LA ESCENA DEL CRIMEN .* Lima, Peru: UNIVERSIDAD INCA GARCILASO DE LA VEGA ESCUELA DE POSGRADO .

Nicomedes, E. (s.f.). *Tipos de Investigación.*

Ojeda, J., Rincón, F., Arias, M., & Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, vol. 11, núm. 28*, 41-66.

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a travéz de internet.* Chimborazo: UNC.

Parra, D. (2019). *Requisitos jurídicos para la validez jurídica de la prueba digital. .* Colombia: Universidad Católica de Colombia.

Ramirez, D., & Castro, E. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informaticos mediante cadena de custodia.* Villavicencio: UNAD.

Riofrío, J. (2016). *Los Delitos Informáticos y su tipificación en la legislacion Ecuatoriana.* Ecuador: UNL.

Significados. (03 de Junio de 2023). Obtenido de Que son los delitos informáticos: https://www.significados.com/delitos-informaticos/

Villacrés, K. (2012). *Estudio Jurídico de la importancia de la cadena de custodia en los procesos penales.* Cotopaxi, Ecuador: Universidad Técnica de Cotopaxi.

Zamora, J. (2020). *Los delitos informáticos y el derecho a la intimidad en el Código Orgánico Integral Penal.* Ambato: UTA.