



**UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA**  
**FACULTAD DE CIENCIAS SOCIALES Y SALUD**  
**CARRERA DE DERECHO**  
**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL**  
**TÍTULO DE ABOGADO**

**TÍTULO:**

**ESTUDIO CRIMINOLÓGICO DE LA ESTEGANOGRAFÍA**

**AUTORAS:**

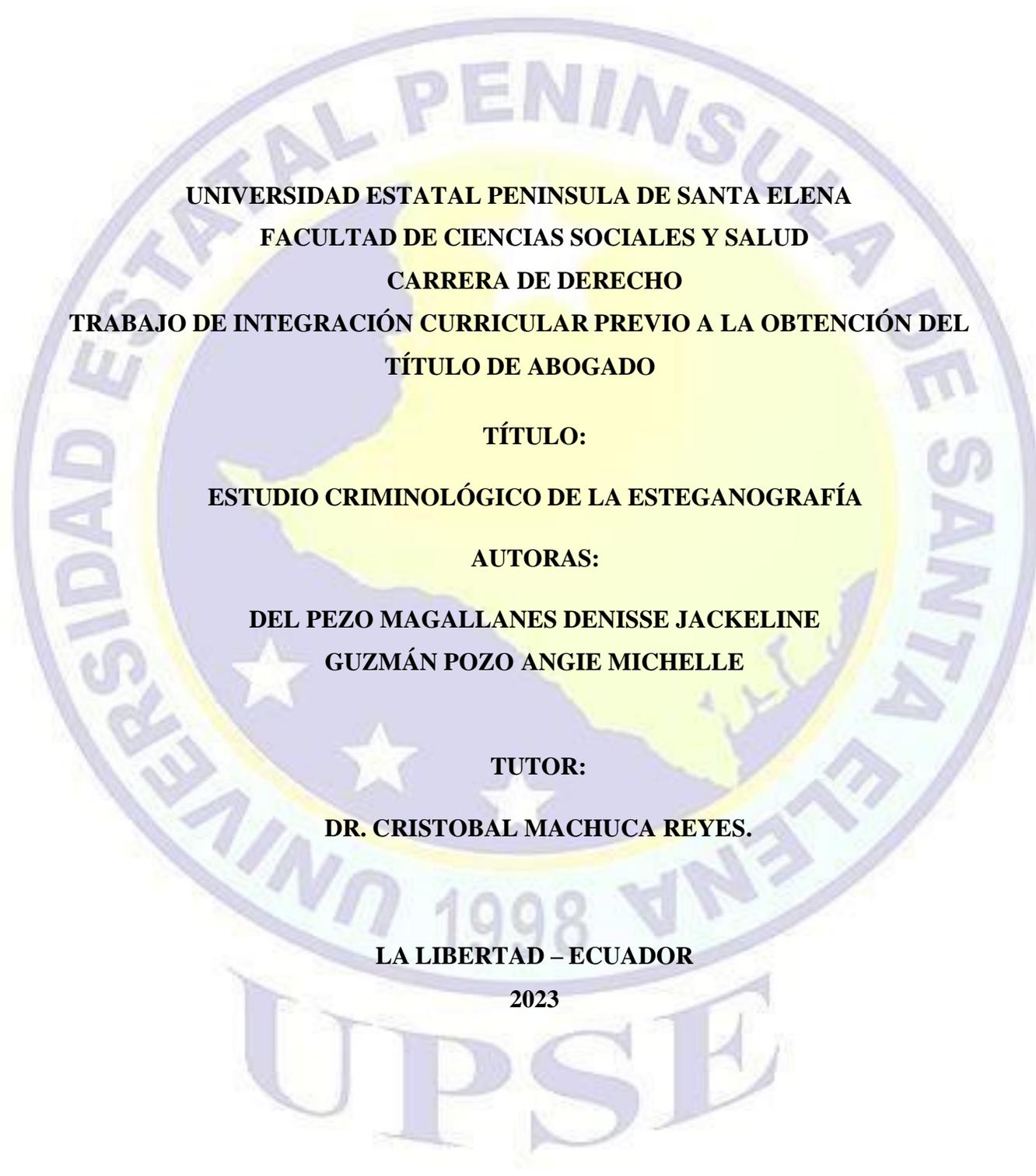
**DEL PEZO MAGALLANES DENISSE JACKELINE**  
**GUZMÁN POZO ANGIE MICHELLE**

**TUTOR:**

**DR. CRISTOBAL MACHUCA REYES.**

**LA LIBERTAD – ECUADOR**

**2023**



**UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA**  
**FACULTAD DE CIENCIAS SOCIALES Y SALUD**  
**CARRERA DE DERECHO**  
**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL**  
**TÍTULO DE ABOGADO**

**TÍTULO:**

**ESTUDIO CRIMINOLÓGICO DE LA ESTEGANOGRAFÍA**

**AUTORAS:**

**DEL PEZO MAGALLANES DENISSE JACKELINE**  
**GUZMÁN POZO ANGIE MICHELLE**

**TUTOR:**

**DR. CRISTOBAL MACHUCA REYES.**

**LA LIBERTAD – ECUADOR**

**2023**

**UPSE**

La Libertad, 24 de julio de 2023

## APROBACION DEL TUTOR

En mi calidad de Profesor Tutor del Trabajo de Integración Curricular de título “estudio criminológico de la esteganografía”, correspondiente a las estudiantes **Del Pezo Magallanes Denisse Jackeline y Guzmán Pozo Angie Michelle** de la Carrera de Derecho, de la Universidad Estatal Península de Santa Elena; declaro que luego de haber orientado científica y metodológicamente su desarrollo el referido proyectó de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la normativa interna, recomendando se inicien los procesos de evaluación que corresponden.

**Atentamente**

Firmado por  
  
CRISTOBAL HOMERO MACHUCA REYES  
EC

.....  
**PROFESOR TUTOR**

## CERTIFICADO DE GRAMATOLOGÍA

La libertad 04 de junio de 2023  
VALIDACIÓN GRAMATICAL Y ORTOGRÁFICA

Lcda. Marcelina Alexandra Pluas Magallanez  
Celular: 096 120 7951  
Correo: [marcelina.pluas.gob.ec](mailto:marcelina.pluas.gob.ec)

Yo, **MARCELINA ALEXANDRA PLUAS MAGALLANEZ**, en mi calidad de **LICENCIADA EN CIENCIAS DE LA EDUCACION Y MAGISTER EN DISEÑO Y EVALUACIÓN DE MODELOS EDUCATIVOS**, por medio de la presente tengo a bien indicar que he leído y corregido el Proyecto de investigación previo a la obtención del título de abogado “**ESTUDIO CRIMINOLOGICO DE LA ESTEGANOGRAFIA**”, de las estudiantes **DEL PEZO MAGALLANES DENISSE JACKELINE Y ANGIE MICHELLE GUZMAN POZO**.

Por tal razón certifico y doy fe que dicho proyecto está redactado con el correcto manejo del lenguaje, claridad en las expresiones, coherencia en los conceptos e interpretaciones, adecuado uso de la sinonimia. Además de haber sido escrito en concordancia con las normas de ortografía y sintaxis vigentes.

Es todo cuanto puedo decir en honor a la verdad, y autorizo a los interesados hacer uso del presente como estimen necesario.



Lcda. Marcelina Alexandra Pluas Magallanez, Mgs.  
**LICENCIADA EN CIENCIAS DE LA EDUCACIÓN.**  
**MAGISTER EN DISEÑO Y EVALUACIÓN DE MODELOS EDUCATIVOS.**  
**NÚMERO DE REGISTRO DE SENECYT 1050-2015-86073107**

## DECLARATORIA DE AUTORIA

Nosotras: **Del Pezo Magallanes Denisse Jackeline y Guzmán Pozo Angie Michelle**, estudiantes de la carrera de Derecho de la Universidad Estatal Península De Santa Elena, habiendo cursado la asignatura Unidad De Integración Curricular declaramos la autoría de la presente propuesta de investigación, de título **estudio criminológico de la esteganografía**”, desarrollado en todas sus partes por los suscritos estudiantes con apego a los requerimientos de la ciencia del Derecho, la metodología de la investigación y las normas que regulan los procesos de titulación UPSE.



**Del Pezo Magallanes Denisse Jackeline**  
C.I. 240034408-7

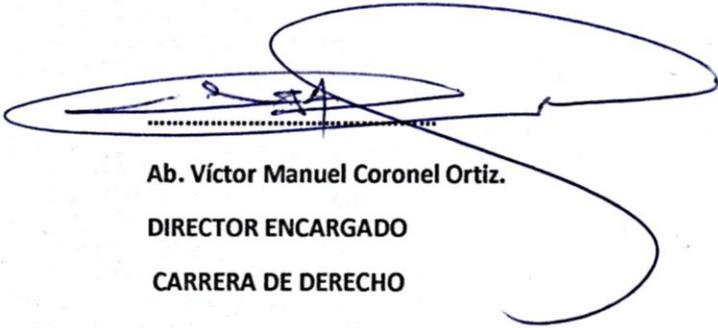
Celular:0960789890  
[denisse.delpozom@upse.edu.ec](mailto:denisse.delpozom@upse.edu.ec)



**Guzmán Pozo Angie Michelle**,  
C.I.0928359421

Celular:0963257651  
[angie.guzmanpozo@upse.edu.ec](mailto:angie.guzmanpozo@upse.edu.ec)

## APROBACIÓN DEL TRIBUNAL



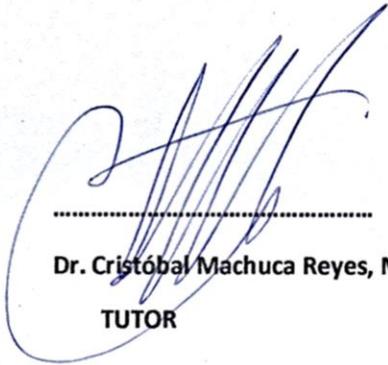
.....

**Ab. Víctor Manuel Coronel Ortiz.**  
**DIRECTOR ENCARGADO**  
**CARRERA DE DERECHO**



.....

**Ab. Esther Viviana Silvestre Ponce**  
**DOCENTE ESPECIALISTA**



.....

**Dr. Cristóbal Machuca Reyes, Mgt.**  
**TUTOR**



.....

**Abg. Brenda Reyes Tomalá, Mgt.**  
**TUTOR DOCENTE GUIA UIC**

## ÍNDICE GENERAL

CONTRAPORTADA	II
APROBACIÓN DEL TUTOR	III
CERTIFICACIÓN GRAMATICAL Y ORTOGRÁFICA	IV
AUTORÍA DEL TRABAJO	V
APROBACIÓN DEL TRIBUNAL	IV
DEDICATORIA	VI
ÍNDICE GENERAL DE CONTENIDOS	VII
ÍNDICE DE TABLAS	X
INDICE DE GRÁFICOS	XI
INDICE DE ANEXOS	XII
RESUMEN	XIII
ABSTRAC	XIV
INTRODUCCIÓN	1
CAPÍTULO I: EL PROBLEMA DE LA INVESTIGACIÓN.....	14
1.1. Planteamiento del Problema .....	14
1.2. Formulación del Problema.....	16
1.3. Objetivos de la Investigación .....	16
1.4. Justificación De La Investigación.....	17
1.5. Variables De Investigación.....	18
1.6. Idea a Defender .....	18
2. CAPÍTULO II: MARCO REFERENCIAL .....	19
2.1. Marco teórico .....	19
2.1.1 Concepto.....	19
2.1.2 Antecedentes .....	19
2.1.3. Teoría del comportamiento criminal y su relación con la esteganografía.....	22
2.1.4. La Esteganografía Como Ciencia En Los Medios Digitales .....	24
2.1.5. Doctrina.....	26
2.2. Marco Legal .....	29
2.2.1. Marco Constitucional y Legal sobre la Protección de Datos.....	29
2.2.2. Análisis Comparativo Entre La Normativa Internacional Sancionadora En La Practica De La Esteganografía Como Método Delictivo Y El Ecuador .....	36

2.3. Marco Conceptual .....	40
2.1.3 Generalidad conceptual .....	40
2.1.4 Definiciones.....	40
CAPITULO III.....	42
MARCO METODOLÓGICO .....	42
3.1. Diseño y Tipo de Investigación .....	42
3.1.2. Tipos de Investigación.....	42
3.1.3. Método de Investigación.....	43
3.1.4. Técnicas de Investigación.....	45
3.2. Recolección de información .....	48
3.3. Tratamiento de Información .....	50
3.4. Operalización de Variables.....	51
CAPITULO IV: RESULTADOS Y DISCUSIÓN .....	53
4.1. Análisis, interpretación y discusión de resultados. ....	53
4.1.1. Encuesta a abogados en libre ejercicio de la provincia de Santa Elena.....	53
4.2. Verificación de la idea a defender .....	77
BIBLIOGRAFÍA .....	81

### ÍNDICE DE GRAFICOS

<b>Tabla 1 Sistematización De Causa, Síntomas, Efectos-----</b>	<b>16</b>
<b>Tabla 2 .....</b>	<b>49</b>
<b>Tabla 3 .....</b>	<b>50</b>
<b>Tabla 4 .....</b>	<b>52</b>

## INDICE DE ANEXOS

<u>1. INDICE DE ANEXOS</u> .....	IX
<u>4.1.2. ENTREVISTA DIRIGIDA A LOS JUECES DE LA UNIDAD JUDICIAL PENAL DEL CANTÓN LA LIBERTAD, PROVINCIA DE SANTA ELENA</u> .....	IX
<u>4.1.3. FECHA: 14 DE JULIO/2023 11:30 am</u> .....	IX
<u>4.1.4 FECHAS: 14 DE JULIO/2023 15:30 pm</u> .....	IX
<u>4.1.5. FECHA: 16 DE JULIO/2023 10:00am</u> .....	IX
<u>4.1.6. FECHA: 17 DE JULIO/2023 11:00 AM, SANTA ELENA</u> .....	IX
<u>4.1.7. FECHA: 17 DE JULIO/2023 3:00 pm LALIBERTAD</u> .....	IX
<u>4.1.8. ENTREVISTA A VARIOS FISCALES</u>	IX

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD  
DE CIENCIAS SOCIALES Y SALUD CARRERA DE DERECHO.**

**ESTUDIO CRIMINOLÓGICO DE LA ESTENOGRAFÍA**

**Autoras: Del Pezo Magallanes Denisse Jackeline  
Guzmán Pozo Angie Michelle**

**Palabras clave:**

**RESUMEN**

La presente investigación de titulación se orienta a la ciudadanía en general que son usuarios digitales que desconocen de los actos criminales cometidos a través de los medios tecnológicos y en especial a la práctica de la esteganografía con fines delictivos, las mismas que están determinadas dentro de la normativa legal vigente penal tipificados como delitos informáticos que producen un daño al patrimonio de la ciudadanía. El objetivo general de la presente investigación es, analizar el estudio criminológico de la esteganografía como modalidad de comportamiento criminal mediante el estudio de los aspectos criminológicos, técnico pericial y doctrina vinculante que permita la caracterización de estas formas de delitos. El desarrollo de la presente investigación implica la fundamentación de temas relevantes como es la investigación científica en delitos informáticos que conllevan al ocultamiento de información dañina o malware que pueden infectar los dispositivos electrónicos vulnerando la seguridad privada y jurídica de los usuarios. Cada capítulo desarrollado dentro de esta investigación cumple a cabalidad las metodologías descritas dentro del marco metodológico respecto a la problemática de la investigación. Siendo importante he de destacar que el trabajo realizado de formapresencial mediante encuestas y las entrevistas sirvieron como base para determinar el comportamiento criminal dentro de la práctica de la esteganografía y como la normativa debe adecuarse para la instauración de una regulación específicas para este tipo de delitos.

## **ASTRACT**

This titling investigation is aimed at the general public who are digital users with no knowledge of criminal practices through technological means and especially the practice of steganography for criminal purposes, the same ones that are determined within the regulations current criminal law such as computer crimes that cause damage to the heritage of citizens. The general objective of the present investigation is to analyze the criminological study of steganography as a modality of criminal behavior through the study of criminological aspects, expert technical and binding doctrine that allows the characterization of these forms of crimes. The development of this research implies the foundation of relevant issues such as scientific research in computer crimes that lead to the concealment of harmful information or malware that can infect electronic devices, violating the private and legal security of users. Each chapter developed within this research fully complies with the methodologies described within the methodological framework regarding the research problem. It is important to highlight the work carried out in person, which was the surveys and interviews that served as a fundamental pillar, to determine criminal behavior within the practice of steganography and how the regulations must be adapted for the establishment of a specific regulation for this type. of crimes.

## INTRODUCCIÓN

En el presente trabajo de investigación se desarrolla en base a la normativa regulatoria de los delitos informáticos, para ello se propuso establecer un tema base de la presente investigación, la que lleva por nombre de **“ESTUDIO CRIMINOLÓGICO DE LA ESTEGANOGRAFÍA”** misma que está elaborada a base de instrumentos de recolección de información considerados como entrevistas, encuestas, doctrina, bibliografía documental y digital correspondiente a la materia de estudio y sus afines.

Dentro de este contexto planteado, debemos destacar con precisión la importancia del tema de estudio, la que abarca detenidamente los institutos jurídicos penales, constitucionales e internacionales, de la criminología y su relación estrecha con la normativa vigente para la correcta aplicación de una justicia adecuada en delitos informáticos, como es la esteganografía, comprendiendo de forma analítica mediante análisis jurídico conceptual de los delitos a través de los medios informáticos y como la norma no regula de forma específica una sanción y una detenida determinación de los elementos básicos necesarios que puedan demostrar y esclarecer los hechos facticos y su relación con la normativa sancionadora.

Ahora, empezamos desde el capítulo uno donde se comprende la parte inicial de esta investigación, en el que se desarrollan temas importantes y esenciales como son, la determinación del problema tanto práctico como jurídico, siendo este, determinar el uso de la esteganografía con fines delictivos y su normativa sancionadora, para lo que se formula un problema esencial a investigar, seguido de objetivos específicos y general, así mismo su respectiva justificación de la importancia de la presente investigación, además de la univariable a determinada y la idea principal que se corroborara al final de esta investigación.

En lo respectivo al segundo capítulo de la presente investigación se basa al desarrollo conceptual, normativo y doctrinario de los elementos de investigación aportados a esta, siendo el desarrollo de subtemas y los temas principales correspondientes a este capítulo, determinando la perspectiva de varios autores literarios relacionado a la temática de la criminalística y su uso a través de los medios electrónicos en los delitos relacionados con la esteganografía.

Siguiendo la secuencia de ideas a desarrollar, también se ha determinado la forma metodológica

en la que se elaboró la presente investigación correspondiente al capítulo número 3, donde se especifican los diseños, tipos de investigación, utilizadas para el desarrollo de esta, obteniendo un enfoque cualitativo, mediante una metodología exploratoria documental; en este orden de ideas, también se determinaron instrumentos de recolección de información los que están determinados como encuestas y entrevistas, para luego procesarla a través del análisis técnico y determinando los resultados correspondientes.

Consiguiente al anterior capítulo corresponde a los resultados obtenidos de los instrumentos de recolección de información, con su respectiva interpretación y saneamiento de los resultados obteniendo la verificación de la idea principal a defender.

Para finalizar la presente investigación se determinaron las conclusiones y recomendaciones respectivas que comprende un aporte necesario e importante para la implementación de medios adecuados para la sanción y protección del usuario, las misma que se adjuntan bibliografía correspondiente y evidencias del trabajo realizado.

## CAPÍTULO 1: EL PROBLEMA DE LA INVESTIGACIÓN

### 1.1. Planteamiento del Problema

Actualmente, el derecho informático se ha vuelto una rama fundamental del derecho, la cual permite determinar cuáles son los medios tecnológicos que llevan a cometer un delito; ahora si nos enfocamos en el derecho informático, el presente trabajo pretende indagar sobre los estudios criminológicos especializados en determinar cómo es la práctica inadecuada e ilegal de la técnica de esteganografía, esta permite adjuntar información de dudosa procedencia a cualquier tipo de archivo, sin que estos puedan ser detectados por un analizador antivirus o por cualquier otra medida de seguridad que esta se pueda tomar. sin embargo, dentro de nuestras legislaciones no existe una ley que ampare a este tipo de delito y que cuya finalidad es que se pueda establecer una normativa que permita darle sanción a cualquier tipo de comportamiento ya mencionado.

Si bien es cierto se reconoce que, dentro de las técnicas para cometer delitos, se encuentra la esteganografía, esta trata de enviar información oculta por cualquier canal inseguro de información (redes sociales, programas de comunicación como el correo electrónico), en si esta puede pasar totalmente desapercibida ya que muy pocas personas conocen de esta técnica; A pesar de que este tema no es actual ni nuevo dentro de las tecnologías de información. Ante esta realidad, surge la informática criminalística como parte de las especialidades que integran la técnica, que hasta la fecha es la de más reciente creación y que tiene sus orígenes en el año 2001.

Esta versión digital de ocultamiento de información fue descubierta por series de malwares de ciber espionaje para robar información de cuentas bancarias en varios países junto con la venta de pornografía infantil mediante esta técnica, es así como se la detecto principalmente en delitos financieros y de carácter sexual. En los últimos años uno de los delitos de mayor auge es la pornografía infantil, la cual a través de la utilización de esta técnica podría pasar totalmente desapercibida, ya que, al enviar contenido oculto dentro las imágenes, los antivirus ya sea en versiones gratuitas o de pago no realizan el análisis de estos. ***“Se insertan datos en un archivo sin afectar la representación (reproducción visual o de audio) de los datos, aunque se produce un incremento en su tamaño”*** (ciberseguridad, 2022).

La esteganografía utiliza un medio digital como archivos de texto, audio, imagen y video que son utilizados como un archivo de transporte, para ocultar la información. A este medio se le conoce como contenedor o cubierta y tiene la característica de que ser un contenedor aparentemente inocente que no despierte ninguna sospecha. De igual manera el mensaje secreto o la información a ocultar puede ser cualquier medio digital descrito anteriormente. Aquí cuando el mensaje secreto es ocultado en el contenedor a través de una técnica esteganografía se obtiene un estenograma que contendrá el mensaje oculto en el archivo de transporte o cubierta. (Velasco Bautista, López Hernández, & Nakano Miyatake, & Pérez Meana, 2020)

Hoy en día dentro de otros países la esteganografía ya se encuentra regulada, estos son: Estados Unidos y Países de la Unión Europea; En la Ley Orgánica de Protección de Datos que está vigente desde el 25 de mayo del 2018 con sanciones de hasta 20 millones de euros. Pueden ser utilizada para fines delictivos, filtración de datos, estafas entre otras, esta técnica esta conmocionando a diversos países que se están viendo afectados por esta innovación tecnológica, si bien es cierto la finalidad de la creación de esta modalidad fue con el fin de que empresas grandes o personas particulares puedan ocultar su información para evitar ser robada y mal utilizada.

En el Ecuador en los últimos 10 años se ha visto un aumento de usuarios que manifiestan haber sido víctimas de la esteganografía, y otros que denuncian páginas web que aparentan ser inofensivas y venden material inapropiado y de carácter sexual de menores, por lo tanto, es necesario su estudio y análisis al ser un tema actual y no obstante este aporta innovación en la rama de derecho puesto que las tecnologías han tomado un gran auge a nivel mundial.

Según el Universo (2015), “Diariamente se envían más 350 millones de fotos por Facebook, 300 millones por Dropbox y 58 millones por Instagram aproximadamente basándose en un sondeo realizado en Estados Unidos en el primer trimestre del 2015”, siendo así podemos observar la facilidad con la cual se pueden enviar y recibir imágenes junto con videos aparentemente inocentes que poseen en gran parte contenido ilícito.

Por lo cual sería una forma segura de transmitir información perjudicial a través de canales totalmente inseguros donde este pase información y además pueda convertirse en viral y nadie sepa de su existencia, permitiendo a las personas distribuir este tipo de contenido sin que tenga el

conocimiento de la información que en el archivo se encuentra oculto.

La presente investigación pretende identificar y analizar esta técnica como un medio de transmisión de información con fines delictivos, siendo parte del estudio de las ciencias criminalistas, ya que como se mencionó anteriormente, se puede adjuntar cualquier tipo de información a una imagen (videos, bases de datos, archivos de Excel, etc.) y esta ser distribuida por cualquier canal de información electrónica.

**Tabla 1 Sistematización De Causa, Síntomas, Efectos.**

SÍNTOMAS	CAUSAS	EFFECTOS
Vacío legal en la normativa referente a los delitos Informáticos	Desprotección y desamparo del sujeto pasivo.	El sujeto pasivo en estado vulnerabilidad ante la delincuencia cibernética
Ineficacia de la sanción de delitos informáticos en el COIP específicamente para evitar la vulneración del patrimonio	Vulneración de la seguridad patrimonial e integral	Alto índice de casos de robo cibernético
Ineficiencia del delito tipificado como pornografía infantil	El cometimiento del delito de pornografía infantil por esteganografía	Daño psicológico y físico al menor violentado y aumento del pederasta al tener acceso al contenido
Baja sanción para los delitos informáticos	Sujeto activo reincidente sin rehabilitación	Aumento de potenciales delincuentes

Elaborado por: Del Pezo Denisse, Guzmán Angie

## 1.2. Formulación del Problema

¿Cómo la esteganografía posibilita nuevas formas de delitos?

## 1.3. Objetivos de la Investigación

### Objetivo General

Analizar el estudio criminológico de la esteganografía como modalidad de comportamiento criminal mediante el estudio de los aspectos criminológicos, técnico pericial y doctrina vinculante que permita la caracterización de estas formas de delitos.

### Objetivos Específicos

- ✚ Analizar los estudios criminológicos enfocados en la sanción penal de la práctica delictiva de la esteganografía.
- ✚ Examinar la normativa internacional de Latinoamérica y Nacional sobre la práctica especializada por criminólogos en el campo de la esteganografía para determinar sus

métodos y fines delictivos.

- ✚ Analizar si los estudios de criminológicos han planteado la necesidad de una aplicación de sanciones establecidas en los delitos informáticos es específica en la práctica de la esteganografía.

#### **1.4. Justificación De La Investigación**

En la actualidad existen diversas ideas que permiten tener una comunicación secreta a través de medios tecnológicos, por tal razón, las nuevas técnicas que permite proteger la información confidencial tienden a tener una vulnerabilidad cibernética e informática.

La técnica esteganografía forma parte de la problemática social e informática a tal punto de ser parte de la intervención del estado y sus diversas instituciones reguladoras de orden tales como la inteligencia criminológica, policial y civiles en el que opera camuflando información relevante como datos personales o protegiendo alguna señal privada y confidencial mediante textos, audios, videos e imágenes dependiendo del fin que se quiera cumplir. Se debe recalcar que no es una forma de codificar algún dato como lo hace la criptografía.

Ante lo anteriormente expuesto, se determina que la presente investigación se enfocara en la revisión, análisis y comparación de los diversos estudios criminológicos que han permitido determinar, encontrar e identificar, las diversas técnicas de esteganografía usadas para el cometimiento de hechos delictivos, que rara vez pueden ser detectados por los usuarios o victimas que sufren de las consecuencias de la práctica indebida de la misma.

Sin embargo, cabe destacar que, para la investigación realizada, no solo se determinara la importancia del estudio criminológico de la esteganografía, sino, además como a través de la criminología se ha aportado una gran cantidad de información relevante del uso y medios de utilización de las técnicas informáticas para la importación de información, tanto como códigos de seguridad, código de cerrojos, códigos digitales, códigos binarios, códigos cartageninos, etc.

Con la presente investigación se pretende estudiar, comprender y a su vez explicar cómo los estudios criminológicos sobre la informática y los nuevos medios de comunicación han progresado para facilitar la comunicación entre los medios humanos y digitales, si no, además de

determinar sus usos prácticos e ilegales, los mismos que la ley imputa por ser violadores de derechos como la intimidad, seguridad, y privacidad.

La finalidad de la presente investigación se justifica en el estudio documentado de la criminalística con el fin de sancionar la práctica de la esteganografía con fines delictivos y la falta de claridad en la normativa penal vigente al momento de sancionar esta práctica de forma específica en su uso indebido e ilegal.

### **1.5. Variables De Investigación**

Para la operacionalización de variables se ha tomado en cuenta el título de la investigación y se procedió a descomponer una sola variable, revisando su concepto, y relacionando las características de sus dimensiones, aplicando la variable cualitativa de la información por medio de sus indicadores, para medir los elementos que son propios de las variables.

**UNIVARIABLE:** Estudio criminológico de la Esteganografía.

### **1.6. Idea a Defender**

La técnica de esteganografía es un soporte para el cometimiento de delitos.

## 2.

## **CAPÍTULO II: MARCO REFERENCIAL**

### **2.1. Marco teórico**

#### **2.1.1 Concepto**

La esteganografía proviene del vocablo griego steganos el mismo que lo define como lo cubierto o lo que se ocultase y de graphos que en su traducción textual del griego corresponde al significado de escritura, si se toma como punto de partida histórico de la aplicación de la esteganografía. Se tiene que remontar de forma continua a los años 440 A. C., cuando la antigua Grecia se escribían mensajes en madera a su vez se cubrían con cera, lo que permitía enviar mensajes encriptados a través de un medio de cobertura.

#### **2.1.2 Antecedentes**

Siguiendo esta línea histórica sobre las practicas más inusuales de la esteganografía como medio de comunicación oculta, podemos remontar hacia la segunda guerra mundial en donde esta práctica tuvo una evolución histórica sofisticada, por el hecho de que en este periodo los militantes, agentes secretos, y diplomáticos de prestigio utilizaban la esteganografía a través de micro puntos en los que se contenían mensajes en clave que solo aquellos capacitados para descifrarlo lograban detectar esta práctica.

Continuando con la era moderna, la práctica de la esteganografía se convirtió en unas de las obras más complejas al adaptarse a las nuevas tecnologías, convirtiéndolo en patrones numéricos y alfanuméricos, fuente de datos y texto combinándolos y encriptándolos, dando un margen mayor de facilidad de ocultamiento y aún más segura para los datos ocultos, puede considerarse una de las practicas más complicadas, sin embargo se puede comprender con mayor facilidad con ejemplos prácticos de la siguiente forma en varios pasos:

Primero: Tomamos una imagen tipo Bit map, en mi caso uso una de Pokémon donde esconderé un mensaje, para ejemplificar se usará el software Xiao Stenography.

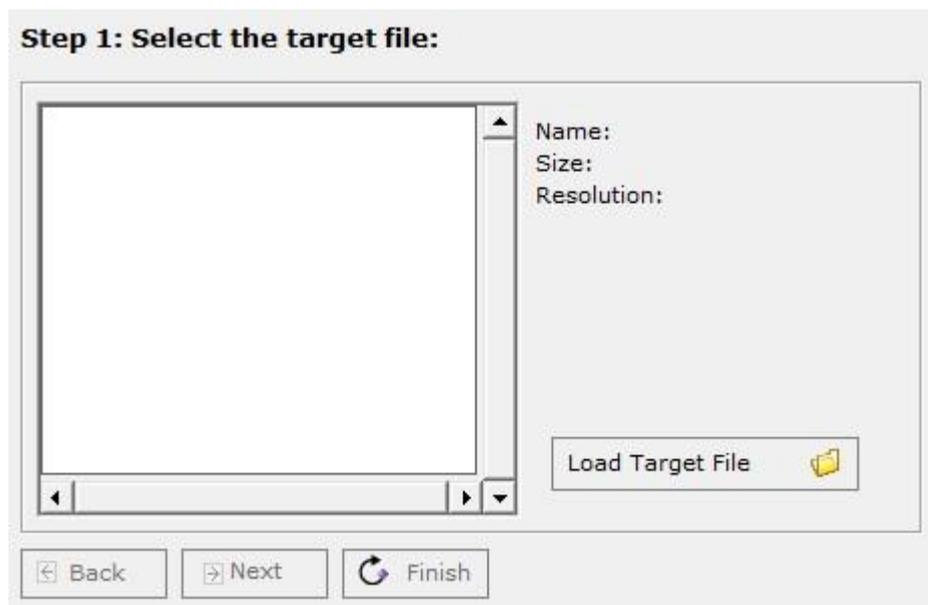
**Ilustración 1**



(MANRIQUE, 2021)

Segundo: cargamos la imagen de Pokémon pulsando en Load Target File

**Ilustración 2**



(MANRIQUE, 2021)

Tercero: Seleccionamos la imagen y next.

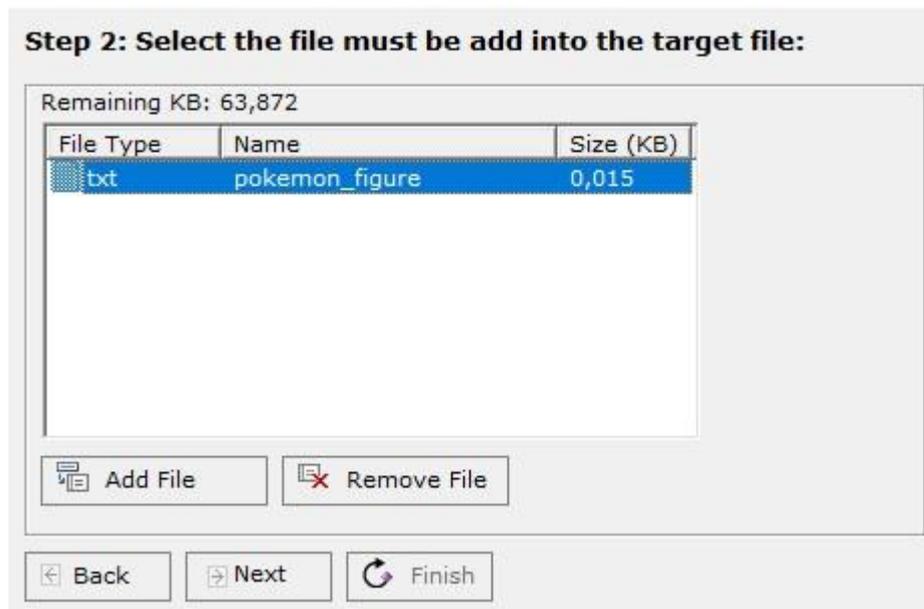
**Ilustración 3**



(MANRIQUE, 2021)

Cuarto: Cargamos el fichero que contendrá el nombre del Pokémon y next.

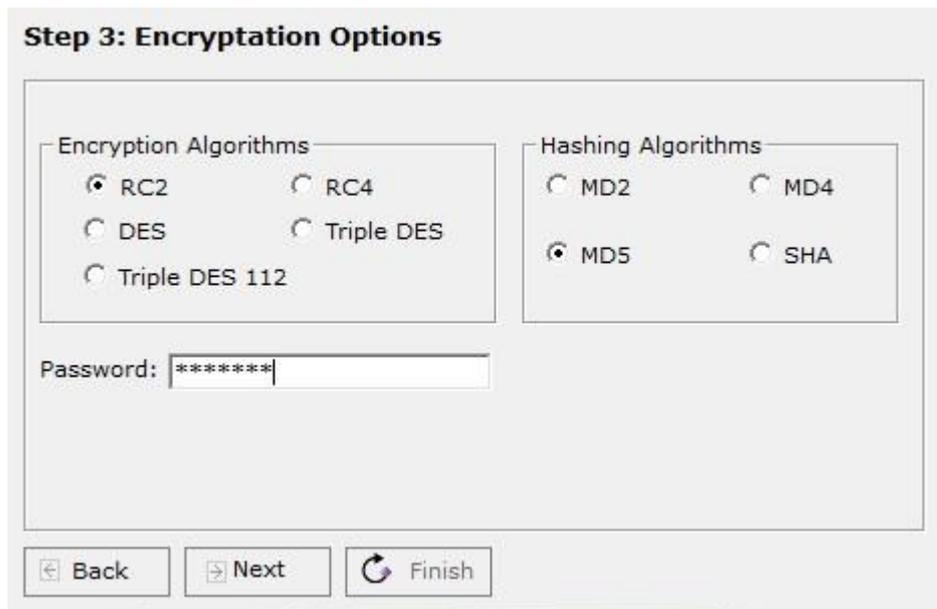
**Ilustración 4**



(MANRIQUE, 2021)

Quinto: Seleccionamos el tipo de encriptado y el hasing, así como la password para poder desenscriptarlo.

**Ilustración 5**



(MANRIQUE, 2021)

Sexto: guardamos la imagen con el texto en la ruta deseada.

De esta forma se puede ejemplificar como la práctica de esteganografía puede llegar a ocultar archivos diferentes a los que están programados para ser observados a simple vista.

Siendo así que actualmente esta práctica a tornado un rumbo más sofisticado al usarse equipos especializados para este tipo de tareas con softwares implementados que permiten con mayor facilidad la aplicación de la esteganografía.

Aquí es donde el derecho sujeto de la rama del estudio criminológico de la esteganografía, se complementan para determinar tanto su uso práctico, con fines delictivos conllevando a una sanción, siempre que esta práctica afecte a los datos personales de terceras personas e incluso causando vulnerabilidades a su seguridad cibernética, comprendiendo una actividad de alto riesgo para quienes desconocen sobre este tipo de práctica.

### **2.1.3. Teoría del comportamiento criminal y su relación con la esteganografía.**

La criminología, es la diversidad de estudios que conforman unos determinados parámetros establecidos, que se vinculan al comportamiento criminal y la caracterización de este ámbito regulatoria a la normativa penal, Sergio Cámara Arroyo lo conceptualiza de la siguiente forma:

La Criminología, entre una de las conceptualizaciones posibles, puede ser definida como la ciencia empírica, de carácter inter y multidisciplinar holística del fenómeno criminal. Asumimos que, cuando se pretende hablar de conocimiento “holístico” del objeto de estudio de una ciencia, se va demasiado lejos. La aspiración de la criminología de estudiar y conocer cada realidad atinente al crimen, al delincuente, la víctima (ahora objeto de la Victimología, como ciencia autónoma), su prevención, control y tratamiento de forma interrelacionada y como un todo distinto de la suma de las partes que lo componen. (Arroyo, 2020)

En las últimas décadas, la teoría científica del comportamiento criminal estaba completamente fundamentada en la relación causal objetiva. es decir, las concurrencias de las conductas penalmente relevantes como el hurto, robo, etc., las mismas que han ido evolucionado con desarrollo doctrinario y analítico como lo es la imputación objetiva.

Sin embargo, también hay que tomar en cuenta la protección de los bienes jurídicos inmateriales, como, por ejemplo, la propiedad intelectual, la propiedad personal de usuarios, información codificada con uso personal a través de sistemas informáticos, mismo que tienen su auge a partir del siglo XX, entre ellos se establecen los delitos informáticos y cibernéticos que dañan de forma dolosa datos informáticos e infraestructura digital.

Configurándose a partir de este punto, un ámbito de conductas punibles relacionados a un comportamiento criminal, que tienen como lugar de hechos un sitio llamado ciberespacio o web, la misma que es implementada a través de las redes digitales de información, misma que a pesar de demostrar un desarrollo futurista y actualizada, también puede conllevar a los riesgos actuales de la delincuencia criminalizada e organizada, los mismos que se caracterizan por ser autónomos, descentralizados, técnicos y masivos que dejan de lado la criminalidad tradicional, el mismo que debe tener una analogía mas compleja para determinar el comportamiento criminal a través del uso de los medios digitales.

Ricardo Posada Maya, plantea que la categoría de la ciberdelincuencia debe ser planteado y desarrollada más allá del análisis valorativo y normativo, si no, además, que debe tener un desarrollo resolutivo del comportamiento criminal a través de la teoría de la tipicidad analógica, en el que se determina ajustándose a las nuevas tendencias de la delincuencia - criminalidad,

siendo este análisis de la siguiente manera:

No resulta convincente construir la categoría del cibercrimen a partir de una noción ontológico-normativa pura, que si bien tiene un cierto rendimiento en el análisis valorativo y normativo de la imputación de delitos clásicos, en realidad no permite explicar todo lo que existe o sucede en una realidad simulada, pues, no solo incluye todas las posibles formas de objetos y métodos lógicos, sino también, porque no permite resolver de forma hábil y práctica todos los problemas que se producen a partir de la informática en la realidad criminal. (Maya, 2017)

Dicho lo anterior, el presente texto busca plantear algunas inquietudes que surgen al momento que se observa, es decir, cómo la teoría de la tipicidad “analógica” trata de explicar y ajustarse a estos nuevos paradigmas de criminalidad, bien o mal, propios del nuevo derecho penal; en el sentido de un derecho que nace como producto de complejas transferencias tecnológicas que marcan nuevas relaciones sociales e individuales en el marco de un mundo simulado y virtual, que tiende a la globalización. De esta manera, en la segunda parte se precisan algunos elementos centrales del cibercrimen respecto a la teoría de la tipicidad, comenzando por su concepto y las particularidades que lo distinguen de los delitos tradicionales y los delitos informáticos en sentido amplio. (Maya, 2017)

#### **2.1.4. La Esteganografía Como Ciencia En Los Medios Digitales**

La esteganografía, es una ciencia practica del uso de información a través de medio digitales que operan como base para archivar información personal, de alta confidencialidad, debo recalcar que esta técnica es utilizada por maliciosos malwares, en otras palabras, son programas altamente infecciosos que roban información personal de usuarios con acceso a la red informática global.

Los desarrolladores de malwares normalmente configuran sus programas con códigos ocultos, ejecutándolo para que establezca una conexión automática; una vez que la víctima reciba o de clic en el archivo infectado se roba la información de sus datos confidenciales. este es un método delictivo que se utiliza operando dentro de archivos de video, música, jpg, tex, documentos.

También podemos comprender varias de las formas o técnicas de esteganografía digital como son:

**La técnica de dominio espacial:** esta metodología de ocultamiento se realiza directamente a los valores que son atribuibles a los píxeles determinado en un archivo de imagen, logrando compactar varios archivos debajo de un solo archivo a través de su capacidad de tamaño, fuente y carga o de la siguiente manera:

Se refiere a métodos en el ocultamiento de los datos se realiza directamente en el valor de píxel de la imagen de portada, de tal manera que el efecto del mensaje no sea visible en la imagen de portada. Los métodos de dominio espacial se clasifican de la siguiente manera: LSB, diferencia de valor de píxeles y BPC. (ayudaleyprotecciondatos.es, 2020)

**Método basado en la inserción:** este método es utilizado mediante la inclusión de información en forma de bloques informáticos, contenidos a través de datos ajenos o adicionales al original que se desea apreciar, es decir:

Es la inserción trabajan a través de la inserción de bloques de datos dentro de un archivo publicable. El dato es insertado en el mismo punto en cada archivo. Este tipo de técnica trabaja encontrando lugares que pueden ser modificados en un archivo, sin tener un efecto fácilmente apreciable sobre el archivo publicable. (ayudaleyprotecciondatos.es, 2020)

**Método basado en algoritmos:** como lo establece el mismo nombre es la creación de algoritmos informáticos capaces de encontrar las vulnerabilidades de un archivo, ubicándose de forma predeterminada dentro del archivo original sin afectar al mismo, es decir, ocultar información sin destruir el archivo original o de una forma más sencilla de comprender su utilización sería la siguiente:

Las técnicas esteganografías basadas en algoritmos utilizan alguna clase de algoritmo para decidir dónde se debería ocultar un mensaje dentro de un archivo de datos. Esta técnica usualmente no inserta los datos en los mismos puntos en cada archivo, por ello puede ocurrir que se degrade la calidad del archivo encubridor. Comparando el archivo original con el que contiene datos ocultos, es posible ver o escuchar la modificación del archivo. (ayudaleyprotecciondatos.es, 2020)

**El método gramático:** en este tipo de metodología no existe la necesidad de formar parte del

archivo en sí, sino, que lo puede generar incluso cuando los archivos están cargados en la red, simplemente basándolos en una gramática predefinida que hace de soporte, por ejemplo:

sí se quisiera que una porción de texto suene o tenga la apariencia como una sección de clasificado del Washington Post, se podría recolectar una gran cantidad de material de la sección clasificados y producir un mensaje que mantenga los patrones estadísticos observados. (ayudaleyprotecciondatos.es, 2020)

### **2.1.5. Doctrina**

Es interesante plantear preguntas antes de comenzar a analizar la criminología dentro la naturaleza científica ¿Qué hace que algunos conocimientos y aplicaciones técnicas sean considerados científicos y otros no? ¿Qué es una ciencia? ¿Es la Criminología una ciencia? El filósofo de la Ciencia Karl Popper (1967) expreso que: *una teoría científica debe basarse en enunciados observacionales que se hacen públicos, y son susceptibles de ser comprobados y falsados.*

La criminología si bien es cierto se trata de una ciencia empírica debido a que esta se basa en la observación, es decir, observa lo que ocurre dentro de la sociedad, actualmente la criminología dispone de conocimientos sobre delincuentes, víctimas y métodos del control social recordando que cada una varía según la época y la sociedad, este estudio empírico no solo afecta a los delitos y a sus autores, también influye a las víctimas y a la actividad. Otro filósofo de la ciencia, Thomas Kuhn (2006), diferenció entre dos tipos de investigación que denominó, respectivamente, “ciencia normal” y “revolución científica”.

En este aspecto de la naturaleza científica se puede analizar la criminalística actualmente es un hecho francamente indiscutible, no obstante, su interpretación a través del tiempo ha ido teniendo cambios drásticos en cuanto a su propio conocimiento y la ciencia en general, es decir, de ser un simple conjunto de reglas prácticas, empíricas, hasta convertirse en un conglomerado heterogéneo de diversos conocimientos tomados de la mano de otras ciencias para lograr sus objetivos y finalidades y esto también incluye en cuanto a las investigaciones de delitos y de los respectivos delincuentes.

Sutherland definió la Criminología como el cuerpo de conocimientos relativos a la delincuencia en cuanto fenómeno social, lo que incluiría el análisis de los procesos de creación de las leyes, de su quebrantamiento, y, también, de las reacciones sociales que siguen a las infracciones. (Sutherland, 2012)

Esto quiere decir que serían objetos de interés criminológico, los delitos, los delincuentes, las víctimas y los sistemas de control social en donde estos principales factores serían áreas importantes para el estudio de la criminología a continuación veamos las áreas prioritarias de la criminología mencionado en este texto.

El profesor Alemán ROXIN, establece que el delito es una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena. Es la ley la que establece que hechos son delitos, es la ley la que nombra que hecho va a ser considerado como delito, es la ley la que designa y fija caracteres delictuales a un hecho, si en algún momento esta ley es abrogada, el delito desaparece.

Entonces al analizar aquí el delito es importante señalar que el derecho establece y define al delito como una conducta penalmente relevante, esto quiere decir que puedan producir un daño inminente y peligroso cabe resaltar lo que establece el Código Orgánico General de Procesos de la siguiente manera:

Art. 22.- Conductas penalmente relevantes. - Son penalmente relevantes las acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables.

No se podrá sancionar a una persona por cuestiones de identidad, peligrosidad o características personales indeterminadas. (NACIONAL, 2017)

En el transcurso de dos siglos de investigación científica dentro de la criminología se encuentran dos factores importantes acerca de la naturaleza que encierra a la delincuencia que tienen implicaciones ontológicas sobre la propia concepción y definición de la disciplina. Entre estos factores el primero es que la delincuencia es un problema real que a lo largo del tiempo a intervenido en varios tipos de delitos es importante señalar que los diferentes tipos de delitos han

conllevado a que se creen sanciones para con la sociedad, donde cada vez que han surgido nuevos delitos con las leyes y normas se ven en la obligación y el deber de ir reformándose y ajustándose a la realidad social en la que nos encontremos, ahora bien, varios individuos utilizan la fuerza física o el engaño para conseguir sus propios objetivos afectando así a otros individuos o a un grupo de personas, por otra parte el segundo factor es que la delincuencia es también, un fenómeno construido a partir de la reacción social de rechazo que suscita entre la ciudadanía.

Por ende, en base a estos dos factores mencionados anteriormente se puede analizar que la criminología es la ciencia que estudia los comportamientos delictivos y las reacciones sociales frente a ello, es decir, que la criminología se ocupa de un conjunto muy amplio que tiene que ver con los diferentes comportamientos humanos y a la vez las reacciones sociales en cuanto al rechazo, es importante mencionar que algunas conductas humanas delictivas dañan gravemente a otras personas entre esos daños por ejemplo se encuentra el homicidio o la violación entre otros delitos. Si bien es cierto, existen otros mecanismos de control social en cuanto al delito estos son los informales ( familias, amigos, el vecindario, o los medios de comunicación), entonces se puede expresar que la criminología es un intercambio de senderos en las que se encuentra diferentes conductas humanas, las delictivas y a su vez las relaciones sociales frente a diversas conductas, a continuación un gráfico donde la confluencia de estas dos dimensiones principales encuadra el espacio científico dentro de la criminología:

**Ilustración 6**



Dentro del gráfico se encuentra como punto inicial el comportamiento delictivo este referente tiene sin duda alguna expresa la ley penal lo cual define los distintos delitos penales estos son los delitos contra las personas, delitos contra la propiedad, delitos contra la libertad sexual, delitos contra la salud pública entre otros.... dentro de este análisis no solo se enfoca en los delitos establecidos por la ley penal, por lo contrario, también es la necesidad de comprender el origen de los comportamientos delictivos dentro de la criminología.

Ahora con respecto a la dimensión y reacción social, analizando este segundo punto aquí su enfoque es que abarca desde la desaprobación y el control paterno de algunas conductas infantiles, juveniles inapropiadas.

Existe una diferencia entre la criminología y el derecho penal, la criminología no se halla conjuntamente vinculada a concretas acciones delictivas en cuanto a las sanciones impuestas en el código penal más bien la criminología se encarga de estudiar el comportamiento humano de una manera más amplia debido a que cada acción no necesariamente tiene que ser delictiva pues componen otros factores que se expondrán más adelante. Por el contrario, el derecho penal este se enfoca únicamente a aquellos comportamientos concretos tipificado como delitos puesto a que las acciones cometidas son confrontadas a un tipo delictivo que este tipificado dentro de la norma penal establecidas para sancionar aquellas conductas delictivas.

Criminalística es la ciencia auxiliar del derecho penal que utiliza o emplea los recursos técnico-científicos en la búsqueda y análisis de los elementos materiales de prueba, a fin de establecer si hubo un delito, otorgando a los investigadores y al criminalista bases científicas sobre el análisis del lugar de los hechos y determinar las posibles causas o móviles de lo sucedido. (López et al, 2000, págs. 148-149)

## **2.2. Marco Legal**

### **2.2.1. Marco Constitucional y Legal sobre la Protección de Datos**

La esteganografía es una práctica informal y vulnerable para adaptarse al uso indebido, ilegal en prácticas deshonestas con el fin de infectar y destruir información valiosa de los usuarios e incluso a infectar con otro tipo de archivos maliciosos que no solo pueden conllevar a la destrucción de información, sino, además a la sustracción de la información personal.

En base a aquello la normativa legal, internacional, nacional, y códigos orgánicos se han adaptado

a través del tiempo para la protección de los medios digitales y su información personal, correspondiendo al adecuado cumplimiento de la normativa.

Dentro de la constitución de la república del Ecuador determina que se protegerán todos los datos personales de los ciudadanos y la difusión de estos con las respectivas autorizaciones de los involucrados este lo determina en el artículo 66:

### **Capítulo sexto**

#### **Derechos de libertad**

##### **Art. 66.- Se reconoce y garantizará a las personas:**

**19.** El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (nacional, 2008)

Consecuentemente el estado debe optar por medios adecuados para la protección de datos e información personal de todos los ciudadanos y la accesibilidad de instrumentos de justicias para la defensa de estos derechos tal como lo establece en su artículo 75:

### **Capítulo octavo**

#### **Derechos de protección**

**Art. 75.-** Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley. (nacional, 2008)

En este orden de ideas también debemos reconocer que la protección de datos, no solo comprende volver inaccesible la información sino también establecer parámetros a cumplirse para que el ciudadano común pueda acceder a ellos y no se les restrinja el acceso a sus propios datos, por lo tanto, la constitución establece acciones constitucionales que garanticen el libre acceso a estas tal como lo es la acción de acceso a la información pública y la habeas data que se determina como una garantía jurisdiccional en los artículos 91 y 92:

### **Sección cuarta**

#### **Acción de acceso a la información pública**

**Art. 91.-** La acción de acceso a la información pública tendrá por objeto garantizar el acceso

a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley. (nacional, 2008)

## **Sección quinta**

### **Acción de hábeas data**

**Art. 92.-** Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (nacional, 2008)

Siguiendo el hilo de ideas concebidas para las normativas debemos establecer que, fueron surgiendo nuevas normas, leyes orgánicas que, de forma especial, se enfoquen en la protección de datos personales e informáticos entre estas tenemos a la ley de protección de datos personales que tiene por objetivo lo siguiente:

**Art. 1.-Objeto y finalidad.** -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

(nacional a. , 2021)

La misma normativa determina que para que los datos personales y digitales que correspondan al ciudadano deben ser usado de forma responsable, legítimo y de forma lícita para ello determina una serie de condiciones que deben ser de estricto cumplimiento que son las siguientes:

**Art. 7.-Tratamiento legítimo de datos personas.** -El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

- 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas;
- 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal; 3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente ley;
- 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;
- 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;
- 6) Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad;
- 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,
- 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma. (nacional a. , 2021)

En cumplimiento estricto de esta normativa legal, también corresponde a observar que cada ciudadana que sea objeto de tratamiento de su informacional personal, en cualquier base de datos

debe ser informado de manera eficaz y transparente sobre el uso, almacenamiento, duración, y recolección de su información para ello se comprende dentro de sus articulados el siguiente:

**Art. 12.-Derecho a la información.** -El titular de datos personales tiene derecho a ser informado

conforme los principios de lealtad y transparente por cualquier medio sobre:

- 1) Los fines del tratamiento;
- 2) La base legal para el tratamiento;
- 3) Tipos de tratamiento;
- 4) Tiempo de conservación;
- 5) La existencia de una base de datos en la que constan sus datos personales;
- 6) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
- 7) Otras finalidades y tratamientos ulteriores;
- 8) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá:  
dirección del domicilio legal, número de teléfono y correo electrónico;
- 9) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, número de teléfono y correo electrónico;
- 10) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
- 11) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
- 12) El efecto de suministrar datos personales erróneos o inexactos;
- 13) La posibilidad de revocar el consentimiento;
- 14) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
- 15) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
- 16) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos y la Autoridad de Protección de Datos Personales, y;

17) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. (nacional a. , 2021)

En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal.

Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el titular deberá ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas.

La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección. (nacional a. , 2021)

Siendo de esta forma aquellos que mantengan acceso a la información personal de otros, responsables directo de su cuidado, seguridad, alcance, tratamientos de los datos, y de realizar las respectivas evaluaciones del nivel de riesgo a las que pueden sujetarse los datos personales de los ciudadanos por lo que este cuerpo legal establece el siguiente capítulo dirigido a la protección de datos, que se determina de la siguiente manera:

## **CAPÍTULO VI**

### **SEGURIDAD DE DATOS PERSONALES**

**Art. 37.-Seguridad de datos personales.** -El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos. (nacional a. , 2021)

El responsable o encargado del tratamiento de datos personales, deberá implementar un

proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales. (nacional a. , 2021)

El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados. Entre otras medidas, se podrán incluir las siguientes;

- 1) Medidas de anonimización, seudonomización o cifrado de datos personales;
- 2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y
- 3) Medidas dirigidas a mejorar la residencia técnica, física, administrativa, y jurídica.
- 4) Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales. (nacional a. , 2021)

De la misma forma se promulgaron más leyes que prevalecen en el factor común de la protección de datos informáticos y protección de los usuarios que utilizan los medios electrónicos como medios de comercio, intercambio y contratación, facilitando una regulación singular llamada ley de comercio electrónico, firmas y mensajes de datos la que tiene por objetivo el siguiente:

## **LEY DE COMERCIO ELECTRONICO, FIRMAS**

### **ELECTRONICAS Y MENSAJES DE DATOS**

#### **TITULO PRELIMINAR**

**Art. 1.- Objeto de la ley.** - Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. (LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS, 2002 )

Al igual que toda normativa legal tiene su principio pertinente de protección de datos el mismo

que la utilización de los datos personales, su forma de uso, trasmisión, y recopilación que se determina de la siguiente forma:

**Art. 9.- Protección de datos.** - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo. (LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS, 2002 )

### **2.2.2. Análisis Comparativo Entre La Normativa Internacional Sancionadora En La Practica De La Esteganografía Como Método Delictivo Y El Ecuador.**

La normativa legal vigente establece sanciones penales en las diferentes formas de cometer algún tipo de delito informático, sin embargo, en el ámbito internacional ha realizado una cooperación entre varios países para combatir este tipo de delitos.

A pesar de la constante cooperación por contener y erradicar este tipo de acciones informáticas que terminan convirtiéndose en delitos cibernéticos internacionales, debemos comprender que la normativa legal tiene sus limitantes y restricciones, entre ellas está la competencia y la jurisdicción, esto quiere decir que, aunque exista una cooperación esta debe radicar la competencia

de quien le corresponde resolver el acto delictivo, cuando existe un delito practico ejemplo:

Un hombre de edad joven realiza una práctica de esteganografía enviando archivos maliciosos a los servidores web de una institución pública de un país vecino, estando dentro del territorio ecuatoriano, generando una vulnerabilidad a los datos privados de miles de usuarios robando y borrando esta información, el mismo es detenido por el servicio de inteligencia de protección de datos.

El juzgamiento del mismo tiene dos lugares de cometimiento del delito, el primero en el ecuador desde donde infecto y accedió a los datos privados, y el segundo donde se cometió el delito que es el país vecino donde fueron vulnerados los datos.

Desde aquí se nos genera varias interrogantes ¿cuál es la adecuada forma de regular esta acción delictiva? ¿se debería juzgar al actor del delito con la legislación local o con las regulaciones internacionales? ¿las regulaciones internacionales de cooperación son eficientes para reducir el cometimiento de delitos informáticos?

Al determinar en un contexto internacional sobre la cooperación entre diversos países para la reducción y control de los delitos informáticos que vulneran los sistemas de información tanto públicos como privados han conlleva a que se generen convenios tales como del grupo G7 y el convenio sobre la ciberdelincuencia en el mismo establecen una variedad de principio entre los más importantes como:

Art 23.- Principios generales relativos a la cooperación internacional: las partes cooperaran entre sí en la mayor parte posible de conformidad con las disposiciones del presente capitulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal , de los acuerdos basados en legislación uniforme o reciproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos. (ciberdelincuencia, 2001)

Este principio relativo nos establece la cooperación entre dos estados en la intervención y recolección de información necesaria para el juzgamientos de los antisociales, es decir la recolección de pruebas digitales que conllevan a una carga probatoria que pueda conlleva la

fiscalía competente en el caso para poder determinar una responsabilidad penal y determinar una responsabilidad material sobre el objeto de la infracción, un ejemplo similar a una cooperación dentro de nuestro ámbito territorial, se estructuraría de la siguiente manera, fiscalía realiza una investigación pero para obtener una prueba contundente requiere de la extracción de información de un dispositivo móvil, en este caso la fiscalía oficia a una unidad de criminalística especializada en el área informático para obtener la información dentro del dispositivo teniendo una cooperación eficaz entre estos dos organismo, uno es la fiscalía y el otro es la unidad de criminalística especializada, siendo una cooperación relativa y determinadas para la obtención de una prueba de cargo.

Art 24.- extradición: el presente artículo se aplicara a la extradición entre las partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente convenio, siempre que sean castigados por las legislaciones de las dos partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave. (ciberdelincuencia, 2001)

Desde el punto de vista jurisprudencial no se puede sancionar más de dos veces por el mismo delito a una persona por que se vulneraria el principio de legalidad, y de no bis in ídem, lo cual es una garantía ciudadana básica, en la que no es correcto sancionar a una persona por los mismos hechos, mismos elementos , mismas prueba y el mismo delito por más de una vez, sin embargo dentro de la cooperación internacional se propone dar una sanción mayor o con cierto límite mínimo para la gravedad, está involucrándola como una agravante al hecho.

Art 25.- principios generales relativos a la asistencia mutua: las partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito. (ciberdelincuencia, 2001)

Al igual que en párrafos anteriores se propone, pero de una forma en específico auxiliarse entre su organismo de control e investigación en mutuo acuerdo entre los mismos delimitándose a la aportación necesaria de pruebas contenidas dentro de los instrumentos informáticos en los que tuvieron participación o fueron herramientas de utilidad para el cometimiento del hecho delictivo

informático.

Art 26.- información espontanea: dentro de los límites de su derecho interno y sin que exista demanda previa, una parte podrá comunicar a otra parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha parte en virtud del presente capítulo. (ciberdelincuencia, 2001)

De forma explícita se puede comprender en el anterior artículo, que no necesariamente debe haber una solicitud previa de una de la partes interesadas al momento de obtener cierta información útil para los procedimientos investigativos que se realizan durante los periodos de instrucciones previas, sino que, al haber cierta cooperación mutua entre estados estos pueden dirigirse de forma espontánea, libre y voluntaria a aportar información que pueda esclarecer el hecho cometido que produjo la presente investigación.

Art 28.- confidencialidad y restricción de uso: en ausencia de asistencia mutua o de acuerdo basado en legislación uniforme o reciproca en vigor entre la parte requirente y a la parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo. (ciberdelincuencia, 2001)

Dentro de este principio es importante recalcar que la información que se obtenga o está al alcance de una parte ya sea la requirente o la requerida según este convenio, para aquellos países que no formen parte de este o que no estén sujetas a un convenio para atender asuntos internacionales de esta naturaleza, el requirente deberá seguir las regulaciones nacionales e internas del requerido, es decir, sujetarse a sus procedimientos internos para poder obtener esta información importante dentro de la investigación, siendo de esta una condición de suma importancia que es la confidencialidad de la misma, esta información no puede ser usada para otros fines y menos en investigaciones ajenas para la que se le requirió.

De esta forma se compone los principios importantes en un convenio internacional en la

cooperación mutua en contra de la ciberdelincuencia y su uso inadecuado para la obtención de información privada y personal que puedan afectar a los usuarios y cibernautas.

## **2.3. Marco Conceptual**

### **2.1.3 Generalidad conceptual**

Dentro de la presente investigación se desarrollaron variaciones de términos técnicos correspondiente a la investigación planteada y su problemática, debiendo indicar de forma general sus significados, sin embargo, de debe puntualizar cada significado de los términos técnicos utilizados para la comprensión del lector en general.

Para ello se emplea un marco conceptual en la que se determina los conceptos básicos y específicos de los tecnicismos utilizados, este mismo se puede determinar desde la perspectiva, doctrinaria, jurídica, relacionado a la información aportada a la presente investigación.

la importancia del marco conceptual que sustenta a la investigación, partiendo de la postura del investigador, por lo que se describen algunas características que favorecen el desarrollo de un buen estudio. Se sugiere realizar un análisis de la literatura existente sobre el tema que se investigará, tomando en cuenta diversas perspectivas: lo señalado por la(s) teoría(s) que pretenden explicar el problema, referidas a la educación, la enseñanza y el aprendizaje del tema, habilidad o competencia en cuestión; el diseño más adecuado para poner a prueba el modelo de enseñanza que se propone; la estrategia de evaluación del aprendizaje más adecuado al contenido y objetivos; y el análisis de los datos recabados que permitan aceptar o rechazar la(s) hipótesis establecidas en el estudio, que se pretende llevar a cabo. (Reidl-Martínez, 2012)

### **2.1.4 Definiciones**

**Esteganografía:** se produce durante la practica informática de ocultar información sobre otra en los medios digitales, haciéndola imperceptible a los usuarios cibernéticos, por ejemplo, se puede ocultar una imagen sobre otra sin ser detectada e incluso sin alterar el archivo original.

**Cibercrimen:** se determina como una actividad ilícita que se dispone a realizarse a través de los

medios digitales dentro de la red informática, los más comunes en realizar estos actos son llamados hackers, crackers.

**Criminología:** ciencia auxiliar al derecho que estudias las causas del delito, sus formas, su manejo, y las consecuencias de este, también se realizan estudios varios con el fin de evitar más víctimas de los ciberdelincuentes.

**Seguridad informática:** está relacionado estrechamente con la esteganografía, por especializarse en la prevención y protección del cibernauta sobre su propiedad digital, sistemas, redes y programas que amenacen la seguridad del usuario, realizando prevenciones de diferentes tipos de riesgos en la web.

**Ley de protección de datos:** La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes.

**Criptografía:** Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

**Códigos binarios:** El código binario es el sistema de codificación usado para la representación de textos, o procesadores de instrucciones de computadora, utilizando el sistema binario. En informática y telecomunicaciones, el código binario se utiliza en la codificación de datos, tales como cadenas de caracteres, o cadenas de bits.

**Malwares:** Un programa malicioso, también conocido como programa maligno, programa malintencionado o código maligno, es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

## **CAPITULO III:**

### **MARCO METODOLÓGICO**

#### **3.1. Diseño y Tipo de Investigación**

La presente investigación contiene un enfoque cualitativo por estar basado en el análisis, interpretación y la conclusión de pretender determinar la existencia de una oscuridad legal dentro de la normativa Ecuatoriana dentro de su normativa penal en los delitos específicos tales como la estenografía cuyo fin es el ocultamiento de información a través de los medios, telemáticos e informáticos con fines ilícitos, por lo tanto dentro de la misma se realiza una redacción tanto normativa, doctrinaria, sobre la normativa sancionadora y la oscuridad legal que mantiene en la impunidad este tipo de delito, la presente investigación pretende analizar estos vacíos legales y manifestarlos a través de un análisis interpretativo cuyo fin es evidenciar la falta de claridad en la norma al momento de sancionar este tipo de acciones.

El enfoque cualitativo tiene por finalidad la búsqueda de información, exploración y análisis con el fin de conllevarla a una interpretación basándose en las teorías preliminares o perfeccionadas a través de la recolección de información, así como lo interpreta Roberto Hernández Sampieri en su libro metodología a la investigación:

En la búsqueda cualitativa, en lugar de iniciar con una teoría y luego “voltar” al mundo empírico para confirmar si ésta es apoyada por los datos y resultados, el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa, dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). (sempieri r, 2014)

#### **3.1.2. Tipos de Investigación**

El presente trabajo de investigación se presenta como un tipo de investigación exploratoria, siendo un hecho puntual la búsqueda de información normativa, doctrinaria, informativa, y recolección de información por otros medios de exploración, aportando un contenido bibliográfico sobre la esteganografía como medio delictivo, el mismo que dentro de la normativa legal vigente tiende a

ser llamado un delito informático, conteniendo una oscuridad legal, que no sanciona con claridad este tipo de práctica, por ende la presente investigación, explorara a través de la información normativa y doctrinaria, con la finalidad de demostrar la existencia de esta oscuridad legal.

Al ser una investigación de tipo exploratorio, conlleva a recabar un sinnúmero de información para posterior ser procesada y estudiada de forma específica con relación al planteamiento del problema estudiado, tal como lo define Paulina Salinas Meruane y Manuel Cárdenas Castro en su libro Métodos de Investigación Social:

Los estudios Exploratorios sirven para familiarizarse con un fenómeno relativamente desconocido. Son importantes ya que nos entregan datos importantes sobre la posibilidad de desarrollar investigaciones más profundas o dirigidas a un contexto en particular. (Castro, 2009)

### **3.1.3. Método de Investigación**

#### **METODO ANALITICO**

El método analítico se utilizará en la presente investigación, consiste en la interpretación y análisis de estudios criminológicos relacionas a la materia informática en específico la esteganografía, la misma que consiste en el análisis de las diferentes tesis de investigación criminalista que comprenden la experticia y pericia de la rama estratigráfica e instrumentos utilizados en esta práctica.

El método analítico es aquel método de investigación que consiste en la desmembración de un todo descomponiéndolo en sus partes o elementos para observar las causas, naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. (COCA, 2017)

#### **MÉTODO EXEGÉTICO**

Se trata, en síntesis, de un método en el que partiendo de un sistema de conceptos teorías (un modelo teórico), siguiendo luego procedimientos deductivos y de Observación del texto de determinadas normas y su análisis dialéctico en relación con otros factores y condiciones económicas, sociales, políticas y otras, arribar a un diagnóstico sobre la calidad técnica de las normas e instituciones jurídicas, posibilitando identificar las deficiencias tanto de forma (gramaticales, de léxico) como de fondo (lagunas, colisiones, su pertinencia objetiva y subjetiva,

etc.) y que pudieran ser causa de problemas en su interpretación y aplicación. (DERECHO, 2022) En base a la cita anterior, se puede comprender que la metodología de la investigación exegética trata dilucidar desde las problemas de interpretación como de aplicación de la norma teniendo en consideración un análisis deductivo, sobre las afectaciones y los probables consecuencias ocurridas a través del error de interpretación jurídica, por ello en la presente investigación se utiliza el método exegético para determinar la oscuridad legal dentro de la aplicación de sanciones a la práctica ilícita de la esteganografía.

## **MÉTODO DE SÍNTESIS**

Este método implica netamente la relación entre las variables obtenidas, los elementos recabados a través de la investigación, implicando la interrelación entre estos elementos con el fin de relacionarlos con el problema de investigación, es decir, en el presente trabajo de investigación se recolectan los elementos que componen un delito y como estos conforman la falta de claridad y la oscuridad legal, al no ser específicos en que practicas exactas se deben sancionar. En conclusión, la síntesis relaciona los elementos y componentes que conforman el problema estudiado, creando escenarios con explicaciones y soluciones planteadas a partir del estudio de este.

Dentro del libro de Carlos Mendoza en su libro metodología de la investigación establece los siguiente:

La síntesis implica que a partir de la interrelación de los elementos que identifican su objeto, cada uno de estos puede relacionarse con el conjunto en la función que desempeña con referencia al problema de investigación. Que en consecuencia la síntesis complementa el estudio analítico del problema. (alvarado, 2011)

## **MÉTODO DEDUCTIVO**

El método deductivo es un procedimiento de investigación que utiliza un tipo de pensamiento que va desde un razonamiento más general y lógico, basado en leyes o principios, hasta un hecho concreto. Es decir, es un método lógico que sirve para extraer conclusiones a partir de una serie de principios. (Aspasia, 2021)

Esta metodología presupone, por lo tanto, que dentro de los propios principios de los que parte se encuentra la solución a la que se quiere llegar y que, finalmente, se extrae a partir de un análisis o desglose de los primeros, adquiriendo una deducción a fin al problema de investigación planteado, contemplando hechos concretos comprendido por los resultados del razonamiento investigativo dentro del ámbito relacionado.

#### **3.1.4. Técnicas de Investigación**

Las técnicas de investigación comúnmente son realizadas en varios tipos, entre las cuales se determinan, técnicas analíticas, técnica bibliográfica o documental, de observación, etnográfica, fundamental, y de estudio de casos.

Dentro del libro de métodos y técnicas de investigación de Esther maya, analiza que la técnica de investigación es una búsqueda lógica y comprensible del conocimiento científico y de los hechos que lo comprenden siendo determinado de esta forma en la siguiente cita:

Las técnicas de investigación comprenden un conjunto de procedimientos organizados sistemáticamente que orientan al investigador en la tarea de profundizar en el conocimiento y en el planteamiento de nuevas líneas de investigación. Pueden ser utilizadas en cualquier rama del conocimiento que busque la lógica y la comprensión del conocimiento científico de los hechos y acontecimientos que nos rodean. (sempieri r, 2014)

Las técnicas de investigación permiten obtener datos precisos a través de la revisión, valoración y análisis documental y bibliográfico, permitiendo no solo el análisis fundamental de un problema a investigar, sino, además permite la apertura de nuevas perspectivas y teorías de análisis conceptual y que son obtenido a través de la información concedida, permitiendo una base sólida en la que se pueden demostrar las posibles soluciones al problema de investigación.

#### **TÉCNICA DE ENTREVISTAS**

Dentro de la presente investigación se realizará un debido proceso de entrevistas hacia los funcionarios públicos habilitados a ejercer cargos como son fiscales, jueces y abogados a quienes se recabo información necesaria con cuestionarios previamente detallados sobre la información a obtener.

Tanto como lo describe Bernal en su libro metodología de investigación es un proceso previamente planteado y detallado para el estudio del problema planteado, o descrito de la siguiente manera por el mismo autor:

la entrevista es una técnica que consiste en recoger información mediante un proceso directo de comunicación entre entrevistador(es) y entrevistado(s), en el cual el entrevistado responde a cuestiones, previamente diseñadas en función de las dimensiones que se pretenden estudiar, planteadas por el entrevistador. (bernal, 2010)

## **TÉCNICAS DE ENCUESTAS**

Bernal dentro de su libro metodología de investigación detalla lo siguiente:

El cuestionario es un conjunto de preguntas diseñadas para generar los datos necesarios, con el propósito de alcanzar los objetivos del proyecto de investigación. Se trata de un plan formal para recabar información de la unidad de análisis objeto de estudio y centro del problema de investigación. (bernal, 2010)

Este instrumento se utiliza con el fin de recabar información que permita dilucidar si la problemática planteada en el desarrollo de la presente investigación, esto es determinar si la práctica de la esteganografía es una modalidad de trabajo con fines delictivos.

## **TÉCNICA DOCUMENTAL**

La técnica documental nos permite la implementación de fundamentos teóricos, analíticos, jurídicos y jurisprudenciales, sobre la práctica de la esteganografía como comportamiento criminal y sus diversos estudios caracterizando este tipo de práctica, que dentro de la presente investigación se propone como técnica de investigación, con el fin de recabar tanto normativa, como doctrina, y de criminólogos en el estudio de la practica esteganografía que permitan el desarrollo de la presente investigación.

La investigación documental consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio. (bernal, 2010)

### **3.1.5. INSTRUMENTOS DE INVESTIGACIÓN**

#### **GUIA DE ENTREVISTAS**

Dentro de la presente investigación se realiza un debido proceso de entrevistas hacia los funcionarios públicos habilitados a ejercer cargos como son fiscales, jueces y abogados a quienes se recabo información necesaria con cuestionarios previamente detallados sobre la información a obtener.

Tanto como lo describe Bernal en su libro metodología de investigación es un proceso previamente planteado y detallado para el estudio del problema planteado, o descrito de la siguiente manera por el mismo autor:

la entrevista es una técnica que consiste en recoger información mediante un proceso directo de comunicación entre entrevistador(es) y entrevistado(s), en el cual el entrevistado responde a cuestiones, previamente diseñadas en función de las dimensiones que se pretenden estudiar, planteadas por el entrevistador. (bernal, 2010)

#### **CUESTIONARIO**

Bernal dentro de su libro metodología de investigación detalla lo siguiente:

El cuestionario es un conjunto de preguntas diseñadas para generar los datos necesarios, con el propósito de alcanzar los objetivos del proyecto de investigación. Se trata de un plan formal para recabar información de la unidad de análisis objeto de estudio y centro del problema de investigación. (bernal, 2010)

Este instrumento se utiliza con el fin de recabar información que permita dilucidar si la problemática planteada en el desarrollo de la presente investigación sobre la práctica de la esteganografía como comportamiento criminal y sus diversos estudios caracterizando este tipo de práctica, que dentro de la presente investigación se propone como técnica de investigación, con el fin de recabar tanto normativa, como doctrina y criminología basada en el tema planteado.

#### **FICHAS**

Las fichas dentro de la presente investigación son utilizadas como referencias bibliográficas idóneas además de ser un instrumento que requiere de una valoración adecuado para el procesamiento de información necesaria con el fin de aportar firmeza y claridad al momento de identificar las fuentes y su valoración pertinente, que en este caso son los estudios de la criminología en el ámbito informático específicamente la estenografía.

Las fichas bibliográficas constituyen un instrumento imprescindible en el proceso de investigación, particularmente en la fase inicial de consultar los libros o fuentes principales que forman la base del análisis y argumentación del trabajo. La función de una ficha bibliográfica consiste en identificar las fuentes de información que se van a examinar o estudiar para escribir el trabajo: los libros, folletos, leyes, artículos de revistas y periódicos, documentos gubernamentales, tesis, fuentes audiovisuales, etc. (RABELL, 2008)

### **3.2. Recolección de información**

#### **POBLACIÓN**

La población es aquella cantidad de personas o para ser exactos el lugar donde se realizara la investigación, dentro de la cual se buscarán analizar tantas las variables planteadas y por supuesto su respectiva valoración, la población sirve como el conjunto de ciudadanos que estén relacionado con el tema de investigación, es decir, con los que esté relacionado la investigación.

Según los libros de metodología la población no solo aborda una cantidad especifica de personas que estén relacionadas acordes a la investigación, sino, también una sección poblacional que se ve afectada por la problemática planteada, es decir, ejemplo, una provincia, un cantón, un barrio, etc. Siendo delimitada la población acorde a las necesidades la de investigación y sus recursos.

Así como se define en el libro de Briceida Carnacho de Báez la población está determinada, en un lugar, espacio y tiempo determinado para la investigación:

Una vez definida la unidad de análisis, se delimita la población que va a ser estudiada y

sobre la cual se pretende generalizar los resultados. La población corresponde a todos los sujetos u objetos que pueden intervenir en el experimento, es decir, todas las unidades (personas, animales, objetos, sucesos etc.) que forman parte de un grupo. Se define como el conjunto de todos los casos que concuerdan con una serie de especificaciones. (C., 2008)

Dentro de la presente investigación se toma referente a la Provincia de Santa Elena con el fin de hacer abordajes con las personas vinculadas al tema de la esteganografía en el ámbito de criminológico para acceder al criterio de magister y otros profesionales del derecho y personal pericial y la fiscalía General Del Estado.

**Tabla 2**

<b>POBLACIÓN</b>	<b>N</b>
<b>JUECES PENALES DE LA PROVINCIA DE SANTA ELENA</b>	5
<b>FORO DE ABOGADOS DE LA PROVINCIA DE SANTA ELENA</b>	864
<b>PERITOS DE LA PROVINCIA DE SANTA ELENA CON SEDE EN EL CANTON DE LA LIBERTAD.</b>	1
<b>FISCALES DE LA PROVINCIA DE SANTA ELENA</b>	16
<b>TOTAL</b>	<b>883</b>

## **MUESTRA**

El objetivo general de todo muestreo es llegar a conocer determinadas características de una población, a partir de una selección de unidades de ésta, con el menor coste posible en dinero, tiempo y trabajo Mediante las técnicas estadísticas, las leyes probabilísticas y los diseños muestrales basados en varios métodos de muestreo, podemos aproximarnos al conocimiento de estas características sin necesidad de tener que obtener la información exhaustiva de toda la población. (López-Roldán, 2015)

Tal como se define en la cita anterior la muestra tiene el fin de determinar las características de la investigación determinando una unidad de trabajo sobre la que se determinara la investigación y se realizara la determinada recolección de datos idóneos y específicos.

El tipo de muestra que se utilizara dentro de la presente investigación, es la muestra no probabilística por no conveniencia siendo este tipo de muestra una de las más factibles para el investigador, toda vez que recurre a una investigación que se caracteriza por definir la muestra por parámetros determinados que faciliten la disponibilidad, física, económica e informativa del investigador, es decir, se adapta a las posibilidades del investigador de recolectar información precisa y necesaria en base de parámetros establecidos o características de la investigación.

Es un tipo de muestreo en el que las unidades están disponibles y son fáciles de localizar, tienen un carácter de representatividad de la población que se quiere analizar, pero se hace una selección conveniente de varias unidades con el objetivo de constituir grupos reducidos y controlados en el contexto de diseños de tipo experimental. Así se configuran grupos de control y experimentales a partir de la elección aleatoria de unos cuantos individuos que los forman. (López-Roldán, 2015)

**Tabla 3**

<b>MUESTRA</b>	<b>N°</b>
<b>JUECES PENALES DE LA PROVINCIA DE SANTA ELENA CON SEDE EN EL CANTON DE LA LIBERTAD.</b>	3
<b>ABOGADOS REGISTRADOS EN EL FORO DE LA PROVINCIA DE SANTA ELENA.</b>	50
<b>PERITOS DE LA PROVINCIA DE SANTA ELENA CON SEDE EN EL CANTON DE LA LIBERTAD.</b>	1
<b>FISCALES DE LA PROVINCIA DE SANTA ELENA</b>	7
<b>TOTAL</b>	61

### **3.3. Tratamiento de Información**

### **3.4. Operalización de Variables**

Para la operacionalización de variables se ha tomado en cuenta el título de la investigación y se procedió a descomponer una sola variable, revisando su concepto, y relacionando las características de sus dimensiones, aplicando la variable cualitativa de la información por medio de sus indicadores, para medir los elementos que son propios de las variables.

UNIVARIABLE: Estudio criminológico de la Esteganografía.

Tabla 4

TITULO	UNIVARIABLE	CONCEPTO	DIMENSIONES	INDICADORES	ITEMS	INSTRUMENTOS
ESTUDIO CRIMINOLÓGICO DE LA ESTEGANOGRAFÍA	ESTUDIO CRIMINOLÓGICO DE LA ESTEGANOGRAFÍA	La esteganografía utiliza un medio digital como archivos de texto, audio, imagen y video que son utilizados como un archivo de transporte, para ocultar la información.	<ul style="list-style-type: none"> <li>• Antecedentes de la estenografía</li> <li>• Bienes jurídicos lesionados en el delito de la estenografía.</li> <li>• Análisis comparativo en la práctica de la esteganografía y entre otras legislaciones</li> </ul>	<ol style="list-style-type: none"> <li>1 Datos históricos.</li> <li>2 Realidad jurídica.</li> <li>3 Lesiones.</li> </ol> <ol style="list-style-type: none"> <li>1 Propiedad personal o privada.</li> <li>2 Intimidad</li> <li>3 patrimonio</li> </ol> <ol style="list-style-type: none"> <li>1 legislaciones internaciones.</li> <li>2 tipos de esteganografía.</li> <li>3 técnicas de esteganografía.</li> </ol>	<p>¿Usted sabe que la esteganografía puede ser utilizado para cometer un delito? ¿Usted sabe reconocer como se transmite información oculta a través de medios digitales?</p> <p>Dentro de nuestro país, ¿considera usted necesario establecer una sanción específica para la práctica ilícita de la estenografía ¿Usted considera que la normativa penal es clara al momento de sancionar la estenografía?</p> <p>¿Usted considera que sus derechos son vulnerados a través de los medios digitales? ¿Usted conoce que la normativa penal sanciona al delito de la esteganografía de forma individual?</p>	Entrevista

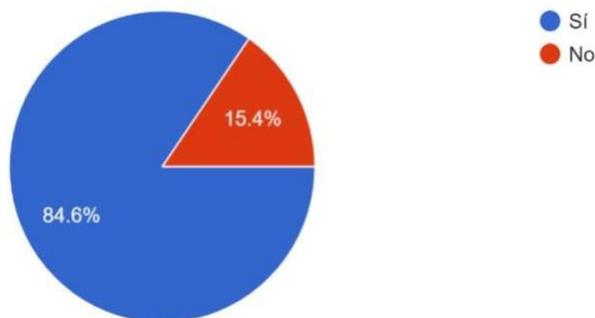
## CAPITULO IV: RESULTADOS Y DISCUSIÓN

### 4.1. Análisis, interpretación y discusión de resultados.

#### 4.1.1. Encuesta a abogados en libre ejercicio de la provincia de Santa Elena

##### Encuesta ítem 1

1. ítem: ¿Reconoce usted a la práctica de la esteganografía como un comportamiento criminal y que deber ser sancionado?



**Fuente:** encuesta dirigida a los abogados de la provincia de santa Elena

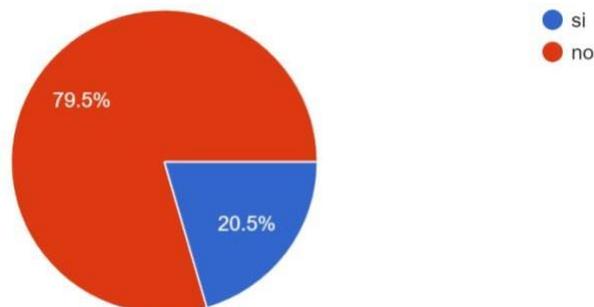
**Elaborado por:** Del Pezo Magallanes Denisse Jackeline; Guzmán Pozo Angie Michelle.

**Descripción del ítem:** dentro del interrogante elaborado en el primer ítem, se pregunta si se reconoce a la esteganografía como una practica criminal y la relación que se le da a la interpretación jurídica de los abogados con la normativa sancionadora.

**Análisis e interpretación:** con esta interrogante realizada a los abogados en libre ejercicio se pretende determinar si reconocen a la práctica de la esteganografía como un comportamiento criminal con fines delictivos y como resultados de la encuesta, que un 84,6% si reconoce esta practica como un comportamiento criminal, y un 15,4% no lo reconocía, dando un resultado favorable para validar las preguntas continuas.

## Encuesta ítem 2

2. **Ítem 2:** En su experiencia ¿ha conocido casos relacionados con la práctica de la esteganografía como delito sancionado?



**Fuente:** encuesta dirigida a los abogados de la provincia de santa Elena

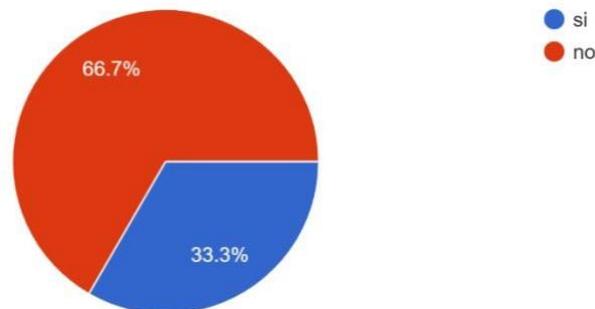
**Elaborado por:** Del Pezo Magallanes Denisse Jackeline; Guzmán Pozo Angie Michelle.

**Descripción del ítem:** dentro del segundo ítem se pregunto sobre el conocimiento práctico de la mayoría de abogados en este tipo de comportamiento criminal como es la práctica de la esteganografía, para determinar su experiencia en este ámbito practico.

**Análisis de ítem:** la presente pregunta corresponde a determinar la cantidad de profesionales del derecho que han tenido participación en delitos relacionados con la practica de la esteganografía determinando que la mayoría en un 79,5% no han tenido casos relacionados, y un 20,5% si han tenido practica y experiencia en casos relacionados a este ámbito.

### Encuesta ítem 3

3. **Ítem 3:** Según su criterio, ¿usted considera que la esteganografía está justificada y tipificada en el Código Orgánico Integral Penal cómo delito?



**Fuente:** encuesta dirigida a los abogados de la provincia de santa Elena

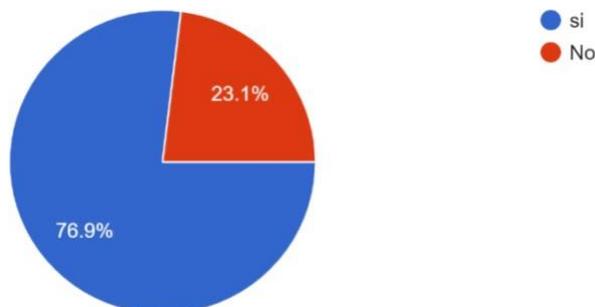
**Elaborado por:** Del Pezo Magallanes Denisse Jackeline; Guzmán Pozo Angie Michelle.

**Descripción del ítem:** dentro de la presente interrogante se pretende determinar si del conocimiento jurídico, y análisis normativo que realizan los abogados en libre ejercicio, lograban determinar si la normativa penal establecía y tipificaba el motivo sancionador de la practica de la esteganografía.

**Análisis de ítem:** los resultados que proporciono la encuesta fue realmente concordante tanto con las entrevistas realizada, como la investigación del presente proyecto, es decir, un 66,7% de los encuestados determinaron que no esta justificado y mucho menos tipificado esta práctica, mientras otro 33,3% que si por estar relacionado con los delitos informáticos.

#### Encuesta ítem 4

4. Ítem 4: Usted considera ¿Que los estudios criminológicos sobre la esteganografía son bases doctrinarias para determinar un comportamiento criminal?



**Fuente:** encuesta dirigida a los abogados de la provincia de santa Elena

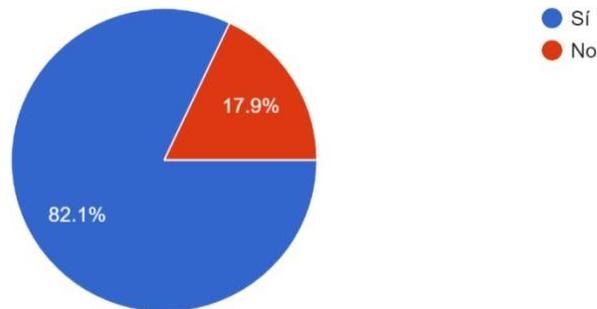
**Elaborado por:** Del Pezo Magallanes Denisse Jackeline; Guzmán Pozo Angie Michelle.

**Descripción del ítem:** dentro del presente ítem se pretendía determinar si aquellos estudios realizados a base de la criminología como ciencia del derecho son suficientes para comprobar un comportamiento criminal en el uso y práctica de la esteganografía.

**Análisis de ítem:** la mayoría de los abogados determinó que las investigaciones científicas basadas en estudios del derecho y dirigidas a determinar un comportamiento criminal, también son una base doctrinaria que pueden ser valoradas para determinar un comportamiento criminal a falta de normativa expresa, arrojando un resultado de 76,9% a favor y un 23,1% en negativo.

### Encuesta ítem 5

5. Ítem 5: En su experiencia, ¿Considera usted que deben realizarse estudios enfocados en el comportamiento criminal que se interrelacione tanto los delitos informáticos con la práctica de la esteganografía?



**Fuente:** encuesta dirigida a los abogados de la provincia de santa Elena

**Elaborado por:** Del Pezo Magallanes Denisse Jackeline; Guzmán Pozo Angie Michelle.

**Descripción del ítem:** dentro de la presente interrogante se pretendió realizar una correlación entre los delitos informáticos tipificados en la normativa penal y la practica de la esteganografía, tratando de hacer énfasis en la relación dentro del ámbito criminal y la investigación científica entre los dos.

**Análisis de ítem:** existen varias investigaciones dirigidas al comportamiento criminal dentro del ámbito informático, sin embargo la mayoría de estas investigaciones son exclusivas a la generalidad del ámbito informático, por lo que se requieren que este tipo de investigaciones se determinen exclusivamente a la práctica de la esteganografía, por eso se determino esta interrogante, dando resultados favorable en un 82,1% con un sí, y solo en contra un 17,9% justificando que los delitos informáticos engloban estas prácticas.

**4.1.2. ENTREVISTA DIRIGIDA A LOS JUECES DE LA UNIDAD JUDICIAL PENAL DEL CANTÓN LA LIBERTAD, PROVINCIA DE SANTA ELENA.**

**FECHA: 14 DE JULIO/2023 10:00am**

**LUGAR: DESPACHO**

**LA ESTEGANOGRAFÍA COMO MODALIDAD DE COMPORTAMIENTO CRIMINAL.**

**1. - De acuerdo con su criterio, ¿Qué pericia surgiere como válida para determinar un comportamiento criminal con el uso de la estenografía al momento de juzgar?**

-Pericia informática en la que se demuestre:

1. el cifrado del mensaje
2. el contenido del mensaje
3. quien es el remitente
4. quien sería el posible presunto receptor de este mensaje para establecer la cadena de quien difunde el mensaje y quien se va a beneficiar de ese mensaje

**2.- ¿Cuáles son los criterios de valoración de la prueba, en los delitos que se cometen a través de la esteganografía?**

Determinar la cadena de custodia de la información es decir el origen, desde donde es obtenida de que base de datos se obtuvo, además el perito debe determinar la credibilidad del origen en caso de que sea entregada a través de un medio magnético o un disco Cd donde se encuentre la raíz de la información, aunque sea difícil determinar de qué forma se obtuvo ejemplo:

Si se trata de una información propia de una entidad bancaria debería por lo menos determinarse de que agencia fue obtenida esta información bancaria o si fue hackeada a través de una página web o alguna forma de determinar algo más específico de que equipo fue obtenida dicha información. habría de acreditar el contenido de medio magnético para determinar qué tan autentica es la información o si se puede facilitar la descripción del sistema descifrado ya que también podría tratarse de información que no sea reservada.

También valorar la gravedad de la conducta es decir la intensión dolosa y de qué manera se puede reservar dicha información, si el funcionario que la obtuvo estaba habilitado para obtener esta información o si estaba facultado para transmitir esta información y con qué propósito se obtuvo la información. Además, la valoración probatoria puede variar dependiendo cada caso específico

**3.- Según su criterio, ¿Qué indicios considera que son suficientes para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía al iniciar un proceso penal?**

1. que la información sea de circulación restringida que no sea de acceso público
2. haya sido obtenida de manera ilícita
3. Que se determine que efectivamente el mensaje se encuentra hackeada con algún propósito criminal
4. Se determine el propósito

**4.- En sus funciones como juez, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

No ha conocido casos en delitos informáticos con relación a la esteganografía.

**5.- En su experiencia, cuando fiscalía le presenta los indicios para determinar un comportamiento criminal en delitos relacionados a la esteganografía ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad?**

Relaciona este criterio con la tercera pregunta.

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tiene un fin delictivo?**

En lo procesal atacar la cadena de custodia la forma de obtención para que de esta manera se desacredite el contenido, es decir, si no justificas que eso se obtuvo de un registro que no es de

acceso público, que no es de circulación restringida no podría establecer su origen ilícito.

Justificar que a pesar de que se obtuvo esa información de manera ilícita no tenía un propósito criminal es decir de vender esa información o compartirla con personal no autorizado, por ejemplo:

Ejemplo 1. El banco no me quiere dar información y yo hackeo de manera ilícita esa información para conocer de un estado financiero propio, pero como el banco no me lo quiere dar, yo un ser humano rebelde lo obtengo de manera ilícita, podría justificarse dentro del proceso que no tenía fin doloso que a pesar de no ir por los trámites correspondientes no significa que se iba a utilizar para fines delictivos o para afectar al banco o a terceros.

Ejemplo 2. Yo como trabajador de banco utilizo esta información únicamente para efectos propios es decir tenía que presentar un informe de gestión y resulta que no podía obtener información dentro del departamento y tenía que entregar este informe de gestión que podría afectar a mi situación laboral entonces de manera ilícita o inapropiada obtengo la información de la base de datos hackeo el mensaje cifrado lo guardo en un pendrive oculto ese mensaje para que nadie se dé cuenta que fui yo quien accedió a la base de datos pero no era tampoco para afectar al banco si no para presentar un informe de gestión del cual necesitaba justamente esos datos estadísticos.

El proceso penal debe ser el fin múltiple situaciones que se pueden solucionar de otra manera en este caso atreve es de una vía no penal si no una vía laboral.

**7.- En experiencia como juzgador me puede indicar ¿Cuál es la dificultad que normalmente se presenta cuando se trata valorar los elementos de convicción presentados en la fiscalía para sostener un comportamiento criminal en los delitos relacionados a la esteganografía?**

La deficiencia en cuanto a la insuficiencia de peritos experto en esta materia ya que en Ecuador no tenemos los expertos técnicamente preparados para determinar todos los parámetros con anterioridad mencionados las fuentes las famosas IP de qué manera están cifrados por ende se debería formar más peritos en los tipos de la materia en criminalísticas informáticas.

**4.1.3. FECHA: 14 DE JULIO/2023 11:30 am**

**LUGAR: DESPACHO**

**1.- De acuerdo con su criterio, ¿Qué pericia surge como válida para determinar un comportamiento criminal con el uso de la estenografía al momento de juzgar?**

Pericia informática, documentológica, y pericia de los hechos y evidencias eso lo hace la fiscalía de acuerdo con sus atribuciones constitucionales y legales conferidas en el artículo 195 de la carta magna

**2.- ¿Cuáles son los criterios de valoración de la prueba, en los delitos que se cometen a través de la esteganografía?**

De acuerdo con la normativa la esteganografía no está tipificado en el Código Orgánico Integral Penal, sin duda en otras legislaciones si están, pero aquí lo que tenemos es si en cuestiones de delitos son delitos informáticos establecidos desde el artículo 173 al 174 que se refieren al acoso sexual, la oferta de servicios sexuales contra menores de edad y a medios electrónicos en el coip desde artículo 190- 194 tipifica la prohibición fraudulenta también está el artículo 191 también.

**3.- Según su criterio, ¿Qué indicios considera que son suficientes para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía al iniciar un proceso penal?**

Los indicios son los recaba la policía experta en estas materias de delitos cibernéticos o ciberdelitos de la policía nacional del Ecuador indicios que se infieren en algún operativo policial los computadores, el modem, las memorias USB entre otras se fijan a través en el departamento de criminalísticas esos indicios vienen hacer elementos de convicción al momento de formular cargos fiscalía los presenta ante los jueces de penales.

**4.- En sus funciones como juez, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

No existe el delito aquí en el país hay delitos informáticos.

**5.- En su experiencia, cuando fiscalía le presenta los indicios para determinar un comportamiento criminal en delitos relacionados a la esteganografía ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad?**

Los indicios se recogen en el momento de hacer un allanamiento o en delito flagrante va al departamento de criminalística y se fijan los indicios, estos indicios al momento de formular cargos fiscalía se convierten en elementos de convicción todo atreves de los peritajes.

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tiene un fin delictivo?**

Como defensor público que fui para demostrar que mi patrocinador no es autor cómplice de la infracción q se le acusa fiscalía debe probar fervientemente con los peritajes correspondientes que efectivamente en mi domicilio donde hubo el allanamiento efectivamente desde ahí fue que se cometió el delito si la fiscalía no hace el seguimiento de que computadora IP se produjo para mí, no tendría consistencia la acusación fiscal lógicamente que no hallan los elementos suficientesde convicción que es actos cómplice del hecho lógicamente al juez le tocara sobreseer.

**7.- En experiencia como juzgador me puede indicar ¿Cuál es la dificultad que normalmente se presenta cuando se trata valorar los elementos de convicción presentados en la fiscalía para sostener un comportamiento criminal en los delitos relacionados a la esteganografía?**

Dicho delito como ya mencionado anteriormente no hay en el Ecuador hay otros tipos de delitos como delitos sexuales delitos a la intimidad, estafa atreves de WhatsApp o medios electrónicos, pero si lo hubiera esto tiene que probarse a través de la fiscalía a través de las pericias correspondientes. Caso contrario como juez tendría que sobreseer por falta de elementos de convicción.

**4.1.4 FECHAS: 14 DE JULIO/2023 15:30 pm**

**LUGAR: DESPACHO**

**1.- De acuerdo con su criterio, ¿Qué pericia surgiere como válida para determinar un comportamiento criminal con el uso de la estenografía al momento de juzgar?**

Nosotros para asuntos de delitos que son por redes sociales o que se distribuye por redes sociales, el Ecuador, no puede tener una eficiente investigación ya que no hemos formados el convenio el Estambul este convenio no está firmado con Ecuador al no tener esto a nosotros nos limita por ejemplo el día de mañana se difunde algún tipo de información o quieren o realizan delitos como el de estafa nosotros tenemos que pedir la fuente de la información por ejemplo ustedes tienen un mensaje o una imagen de WhatsApp o de Facebook presentan en la fiscalía y la fiscalía tiene que decir a Facebook o WhatsApp sabe que quiero que me de la información idónea de esa persona no del IP porque el IP lo único que nos dice es esa información se grabó en la computadora de tal pero no nos dice quién es el dueño es decir el titular de esa cuenta es por eso que se pueden crear cuentas falsas y sencillo a mi clonaron la cuenta pero no sabemos quién clono esa cuenta pero cuando ustedes crean una cuenta tanto de WhatsApp como Facebook le piden datos personales entonces como no se tiene ese convenio de Estambul no van a responder por qué no tienen la obligación de responder, la información de Facebook o de WhatsApp pero si este convenio fuera firmado sería más fácil saber de quien fue ese perfil creado incluso Facebook, nosotros no tenemos una política criminal en el país lamentablemente nosotros solamente copiamos los tipos penales de otros países. Entonces son impedimentos legales porque no tenemos una política criminal para determinar que comportamiento criminal encontramos tenemos que ver en qué sociedad estamos, pero nosotros solo copiamos un código y la adaptamos supuestamente a nuestra realidad.

**2.- ¿Cuáles son los criterios de valoración de la prueba, en los delitos que se cometen a través de la esteganografía?**

Como juez lo que se valora son las pericias técnicas, pero para tener acceso a una pericia técnica tenemos que ir a fuente de donde salió esa información como mencione anterior si no vamos a Facebook pues Facebook no nos va a responder la mayoría de personas van a una notaría la hacen

registrar y presentar, pero esto sirve como una prueba documental no como una prueba pericial que nos diga donde se originó esa información de esa fuente.

**3.- Según su criterio, ¿Qué indicios considera que son suficientes para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía al iniciar un proceso penal?**

Estos indicios sirven para establecer si vamos a tener a futuro un proceso penal después de estos indicios se van a convertir en prueba y actuado en una audiencia de juicio y en etapa probatoria van hacer elementos de convicción entonces estos indicios tienen que pasar primero por una serie de mecanismos y de protocolos que tienen que actuar la policía especializada para combatir en elementos de convicción necesitamos de las pericias y las pericias no las tenemos estos tipos de delitos se comente en la web Dark.

**4.-En sus funciones como juez, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

Aquí en la provincia de Santa Elena No.

**5.- En su experiencia, cuando fiscalía le presenta los indicios para determinar un comportamiento criminal en delitos relacionados a la esteganografía ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad?**

La experticia, es decir, en donde se encuentra el dispositivo, pero por falta de pericia no se puede ir más halla debido a que no haya convenio con el Estambul, la mayoría de delitos informáticos se quedan sin ser resueltos.

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tiene un fin delictivo?**

En las redes sociales tienen ciertas restricciones por ejemplo una página donde publican que hubo un sicariato o asesinato o si es una información sensible ustedes pueden reportar esa información para q se bloquee esa publicación, pero para dé hay para determinar un hecho delictivo no tendríamos en este momento indicios de procesados que digan que esta página pero la IP solo me

da la ubicación de donde subieron eso pero no me dice quién está detrás de todo eso y pues no tengo una pericia que me indique que persona estaba en el computador .

**7.- En experiencia como juzgador me puede indicar ¿Cuál es la dificultad que normalmente se presenta cuando se trata valorar los elementos de convicción presentados en la fiscalía para sostener un comportamiento criminal en los delitos relacionados a la esteganografía?**

Las pericias normales por reconocimiento facial pueden decirme que esa misma persona en la red, pero no me dice que fue creado por la persona por ejemplo creo un WhatsApp y como sé que ese WhatsApp lo utilizo la persona para un delito no hay detalles de eso.

**4.1.5. FECHA: 16 DE JULIO/2023 10:00am**

**LUGAR: CRIMINALISTICA**

**1.- De acuerdo con su experiencia ¿Cuál es la información que se requiere para determinar un comportamiento criminal?**

Dentro de la criminología se tiene las formas de pensar de cada uno de los presuntos delincuentes, nosotros como criminalística realizamos el análisis criminológico en base a las pruebas en este caso indicios que nosotros obtenemos de una determinada escena, estos indicios nos permiten tener una hipótesis de un caso en específico puede ser un femicidio, sicariato o inclusive dentro de las mismas escenas también tenemos hipótesis no tan acertadas dentro de un caso en específico.

**2.- De acuerdo con su opinión ¿Dentro de los procesos de investigación de pericias que ha realizado, usted ha encontrado si la esteganografía se asocia a otro tipo de delitos?**

Por lo general están asociados a los delitos cibernéticos en la mayor parte de los casos que hemos tenido, tenemos igual casos en los cuales han ocultado información dentro de otra información, entonces esta situación nos ayuda a comprender un poco más la delincuencia en el sentido que ya no son solamente los tipos de delitos que antes se realizaron como un robo una estafa ahora utilizan lo que son los medios informáticos y tecnológicos para poder realizar estas clases de delitos.

**3.- En su experiencia ¿Qué técnicas de investigación utiliza para determinar el comportamiento criminal en sus pericias dirigidas a los delitos vinculantes con la esteganografía?**

Todo lo que son técnicas forenses en base a lo que es enmarcado directamente en el COIP tenemos en el artículo 500 está enmarcado lo que es la evidencia digital entonces todo lo que tiene que ver con evidencia digital entonces todo lo que tiene que ver con evidencia digital es el tratamiento constatación, materialización, fijación y la materialización de esta información obtenemos información a lo que son resultados a los que son arrojados por los programas forenses en este caso el gobierno nos provee y con eso nosotros realizamos la investigación

**4.- Según su criterio ¿Qué pericia técnica es la más común para identificar aquellos delitos que son asociados con la esteganografía?**

La informática forense por lo general como mencione anteriormente los delincuentes ahora están optando nuevas maneras y métodos para poder coger una información dentro de una información

es decir si yo a usted le envié una imagen puede ser que dentro de esa imagen este camuflada alguna otra información entonces es por eso que nosotros utilizamos los programas forenses con el fin de poder extraer esa información y lograr de alguna u otra manera tratar de cifrar todo eso porque antes era fácil mandaba un mensaje y dice “tienes que matarle al jefe de criminalística” poniendo un ejemplo, pero estaba escrito pero ahora no yo le puedo mandar una serie de imágenes pero no va a tener ningún sentido pero dentro de esas imágenes están codificado un mensaje es porque aquí enlazamos todas las herramientas forenses tratar de descifrar esa imagen con respecto a la información y dar a conocer este caso a la fiscalía que son los entes rectores que nos dirigen a nosotros en la investigación poder realizar una correcta investigación dentro de un determinado caso.

**5.- De acuerdo con su conocimiento ¿Qué otras pericias consideran usted que son necesarias para determinar un comportamiento criminal en estos tipos de delitos?**

Dentro de lo que es la informática forense también tenemos la psicología forense que están enmarcada directamente en lo que es la criminología entonces teniendo lo que son estas bases tenemos lo que son los indicios levantados en la escena, la información que podemos obtener de los equipos tecnológicos que viene hacer lo que es informática forense y la psicología forense que directamente está enfocada en la búsqueda de actitudes directamente desarrolladas en un ámbito criminal.

**6.- De acuerdo con su criterio ¿Cuáles son los medios digitales más comunes en los que ha realizado una pericia dentro de estos casos de delitos vinculantes a la esteganografía?**

La red social Facebook es una de las más usadas al igual que el WhatsApp, entonces por lo general las personas o los delincuentes han optado el hecho de enviar imágenes o fotografías, audios, y videos encriptados a las diferentes personas, en el caso a las víctimas y dentro de eso al realizar la materialización de esa información obtenemos otra información aparte de la que nosotros ya tenemos que son unas imágenes que a las víctimas envían directamente a un Facebook o WhatsApp, entonces nosotros con los programas forenses obtenemos más información de la que nosotros observamos a simple vista entonces hay ingresaría la localización de los medios forenses con el fin de poder materializar esa información en un informe y emitirlo directamente a la fiscalía.

**7.- En su experiencia al momento de sustentar su pericia en una audiencia ¿Qué preguntas son las más comunes que le han realizado al momento de sustentar su pericia los sujetos**

## **procesales?**

La acreditación por lo general al momento que realizamos una pericia tenemos que estar legalmente posesionado y también certificados por el consejo de la judicatura, no cualquier persona puede realizar una pericia siempre hay que tener en cuenta que debe está debidamente acreditada por el consejo de la judicatura, en este caso si el consejo de la judicatura dice usted va hacer perito en informática forense yo puedo realizar las pericias de informática forense pero si hay otro compañero que es en inspección ocular técnica ellos están encargado de realizar el levantamiento de todos los indicios y evidencias encontradas en el sitio, entonces este no puede realizar una pericia técnica como la perito informática forense realiza y es igual en el caso de audio y video y esta es la pregunta más frecuente que realizan al momento de realizar una audiencia “Señor perito usted está acreditado”.

**4.1.6. FECHA: 17 DE JULIO/2023 11:00 AM, SANTA ELENA**

**LUGAR: DESPACHO**

**1.- De acuerdo con su criterio, ¿Qué pericia surge como válida para determinar un comportamiento criminal con el uso de la esteganografía al momento de acusar?**

Sugiero que la pericia adecuada para poder determinar el comportamiento criminal sería una pericia de audio y video.

**2.- ¿Cuáles son los criterios de valoración de la prueba que usted determina en los delitos que se cometen a través de la esteganografía?**

En este caso la credibilidad del perito radica básicamente en el tiempo de experticia que tiene respecto de la realización de audio y video considero es la más idónea para determinar ese tipo de delitos.

**3.- Según su criterio, ¿Qué indicios considera que son necesarios para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía?**

Los indicios que identifiquen información que siendo reservada este siendo compartida por medio de audio, fotografía, video o cualquier otro medio digital sin autorización de la persona que aparece ser dueño de esa información.

**4.- En su cargo como fiscal, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

En mi experiencia como fiscal no existe, no he visto en esta provincia el ocultamiento de información en ningún medio digital.

**5.- En su experiencia como fiscal ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad para determinar un comportamiento criminal en el uso de la esteganografía o relacionado a delitos informáticos?**

Los indicios que principalmente aparecen, es decir, los más comunes son los de audio, fotografías, grabaciones de video.

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tienen un fin delictivo?**

La defensa técnica de una persona procesada debe orientarse en su defensa a intentar destruir o demostrar la inexistencia del dolo en la conducta de su defendido debería demostrar que no ha tenido la intención de compartir o hacer pública en medios digitales.

**7.- En su amplia experiencia como fiscal me puede indicar ¿Cuál es la dificultad que normalmente se le presenta cuando los elementos de convicción recabados no pueden justificar un comportamiento criminal en los delitos relacionados a la esteganografía?**

Si no existen elementos de convicción suficientes para saber que existe una infracción y en este caso relacionado con el ocultamiento de información de un medio digital sin duda alguna eso es una dificultad extrema y por mandato constitucional y siendo un deber ser del fiscal ser objetivo al no existir un elemento de convicción fuerte que demuestre ese comportamiento criminal se debe desistir de la acusación y aquello deriva de que el juez dicte un sobre seguimiento.

**4.1.7. FECHA: 17 DE JULIO/2023 3:00 pm LALIBERTAD**

**LUGAR: DESPACHO**

**1.- De acuerdo con su criterio, ¿Qué pericia surge como válida para determinar un comportamiento criminal con el uso de la esteganografía al momento de acusar?**

En este caso es relevante contar con una pericia técnica de orden informático, una pericia informática, efectos a determinar mediante peritos especializados en este caso cuyas conclusiones se deba determinar justamente que se ha utilizado o se ha vulnerado las barreras tecnológicas para cometer delitos informáticos a través de la aplicación de la esteganografía que en este caso vendría ser la ocultación de mensajes encriptados pero técnicamente el perito es el llamado a realizar y determinar bajo sus conclusiones ese comportamiento criminal.

**2.- ¿Cuáles son los criterios de valoración de la prueba que usted determina en los delitos que se cometen a través de la esteganografía?**

La valoración de la prueba evidentemente corresponde al juzgador al momento en que la fiscalía procesa oportunamente su acusación fiscal con base a elementos de convicción que se hayan señalado en una audiencia propiamente dicha y de esta valoración nace primero de la idoneidad del perito de la capacidad, preparación y sobre todo de la forma de sustentar sus pericia, en este caso según las pericias informáticas para cuyas conclusiones deban llevarle al juzgador a la certeza absoluta, no solamente de su idoneidad de pericia sino que cuyas conclusiones se aparejan a la verdad histórica, a la verdad procesal respecto al comportamiento delictual en este caso un delito informático.

**3.- Según su criterio, ¿Qué indicios considera que son necesarios para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía?**

Evidentemente los indicios de un delito flagrante o dentro del marco de una investigación debe advertir que estén asociados al tema evidentemente informático a la modalidad de la conducta, es decir, que el sujeto activo utilice estos medios informáticos tecnológicos a través de enlaces para poder engañar y llegar al sujeto pasivo a la víctima y poder configurarse el delito como tal. Ejemplo abrir un enlace cuya finalidad tenga encriptado un mensaje malicioso del cual pueda ocasionar daños en varios sistemas informáticos u otras clases de delitos que se pueda determinar, entonces estos son los indicios vinculantes o relevantes que luego pues se convertirá en elementos de convicción y luego a una etapa de juicio alcanzarán su valor probatorio.

**4.- En su cargo como fiscal, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

En la actualidad No, hasta este momento no.

**5.- En su experiencia como fiscal ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad para determinar un comportamiento criminal en el uso de la estenografía o relacionado a delitos informáticos?**

Evidentemente el uso de herramientas tecnológicas sea a través de dispositivos móviles, a través de también de correos electrónicos que son dirigidos a las presuntas víctimas al sujeto pasivo del delito en quien recae la lesividad del hecho delictual

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tiene un fin delictivo?**

En este caso la defensa técnica siempre ha desvirtuar los elementos de cargo o de convicción de cargo que la fiscalía demuestre técnicamente y al hablar ya propiamente de delitos de orden informáticos, deberá desvirtuar mediante la práctica de diligencias de esta naturaleza en la que se puedan contraponer o cuestionar que las conclusiones del perito que determina cierta modalidad de conducta que se ha evidenciado mediante un enfoque pericial, que no es adecuado o no es correcto desacreditar de cierta forma eso sería desacreditar básicamente la argumentación que tendría la defensa técnica para sostener a favor de su defendido en este caso tratándose de delito informático cuyas pericias principal son de orden técnico informático.

**7.- En su amplia experiencia como fiscal me puede indicar ¿Cuál es la dificultad que normalmente se le presenta cuando los elementos de convicción recabados no pueden justificar un comportamiento criminal en los delitos relacionados a la esteganografía?**

En la praxis como fiscal son escasos este tipo de delito de comportamiento criminal en cuanto al delito informático en la que esté relacionado a la esteganografía.

#### **4.1.8. ENTREVISTA A VARIOS FISCALES**

##### **1.- De acuerdo con su criterio, ¿Qué pericia surgiera como validad para determinar un comportamiento criminal con el uso de la esteganografía al momento de acusar?**

Es muy nuevo para nosotros como operadores de justicia esta modalidad de comportamiento criminal a través de la esteganografía, siendo objetivo a este tema a ciencia cierta como para tomarlo como prueba para este delito como es la esteganografía, en nuestras legislaciones no detallan algo vinculante como este tipo de delito. **sim embargo, estamos hablando de una cuestión psicológica quizás un análisis forense para estar enfocándonos del** comportamiento criminal que lo puede tener en cualquier tipo de modalidades del cometiendo de este delito y no solo de aquello, normalmente en delitos informáticos lo que hacemos en la práctica que se oficie a un perito especializado de las plataformas de redes sociales para que recaben la información Facebook para seguir a la persona que creo esos perfiles falsos más aun de tratar de ocultar o borrar la información a través de la esteganografía.

la pericia denominada informática esta es practicada a través de un software que no la tiene una institución a más que la fiscalía general de estado directamente en la unidad de investigación. mediante ese software se puede comprobar que los delitos ocultos se puedan borrar o ocultar la información, entonces a través de ese software es donde se puede recuperar toda la información es una pericia importantísima en un caso informático.

##### **2.- ¿Cuáles son los criterios de valoración de la prueba que usted determina en los delitos que se cometen a través de la esteganografía?**

delitos que se encuentran tipificado como es la esteganografía aún no está tipificado como delito, entonces no se podría determinar. pero al momento en el que se valora la prueba es hacia donde el tribunal se presente.

reitero, no he tenido casos en nuestra practica y no podría dar mi criterio de una valoración de prueba sobre todo que no es común.

En los procesos penales en la actualidad son pocos los abogados de libre ejercicio que solicita las pruebas pertinentes porque hay que solicitar las pruebas para estos casos. entonces al momento de valorar esa prueba tiene que ser precisa en donde se pueda determinar la materialidad y la responsabilidad de la persona que adecue su conducta a este futuro delito penal porque aún no se

encuentra establecido lo que si existe son otros delitos informáticos en el COIP, pero no de esta naturaleza.

**3.- Según su criterio, ¿Qué indicios considera que son necesarios para determinar, si existe un comportamiento criminal en delitos cometidos con la esteganografía?**

si hablamos de indicios estamos hablando de una flagrancia. a mi criterio es un delito continuado ya que el delito se comete a través de dispositivos electrónicos como es la computadora(informática).

el comportamiento criminal que existe no habría ninguna diferenciación porque la esteganografía es una modalidad de una conducta es la misma que utilizan todas las personas que infringen o adecuan su conducta a un tipo penal considerando a los en delitos informáticos básicamente. pero no está establecido un estudio criminológico del comportamiento de estas personas si hablamos de eso contienen un sin número de factores sociales, psicológicos y eso lo han establecido muchos factores en tantas obras como la sitti radian.

en la adecuación de la conducta los indicios tendrían que ser las direcciones del IP para poder determinar el usuario del lugar donde está ubicado aquel equipo informático que se pueda ver iniciado o ejecutado este tipo de delito de esta naturaleza.

**4.- En su cargo como fiscal, ¿Usted ha conocido casos de delitos informáticos cometidos a través de la esteganografía en la provincia de Santa Elena?**

como fiscal en la provincia de santa elena, aún no he conocido casos de delitos informáticos. pero en la provincia del Guayas sí.

directamente como delitos informáticos no, pero como delito de estafa si. porque para poder llevar a una estafa es donde se oculta la información.

**5.- En su experiencia como fiscal ¿Cuáles son los indicios más comunes que se le han presentado a vuestra autoridad para determinar un comportamiento criminal en el uso de la esteganografía o relacionado a delitos informáticos?**

Básicamente, relacionados a delitos informáticos que podría ser el conjunto de todas estas modalidades entendemos que hay otras formas de delitos informáticos. por ejemplo, los hackers que crean o tienen información los mismos usuarios o que aquellos mismos solicitan en hackear las cuentas de ahorro con el fin de realizar trasferencias electrónicas de las víctimas. es la experiencia que tenemos aquí en fiscalía tenemos las comunes como un robo o estafa. ya que hay víctimas que no manejan bien los dispositivos informáticos, en la pornografía infantil a través de los mensajes mediante redes sociales.

**6.- ¿Qué elementos técnicos debe demostrar la defensa del procesado, para sostener que estos tipos de conductas vinculantes a la esteganografía no tiene un fin delictivo?**

solicitar la pericia de explotación de información de aquel dispositivo informático.

De manera general se utilizarían técnicas de delitos que se necesitan para el sospechoso o que conoce la materia de informática, si la defensa técnica llega a demostrar que no tiene una grave preparación, no tiene un título académico a fin a este tipo de actividades informáticas. obviamente no podría demostrar que es una persona preparada para utilizar esta modalidad como es la esteganografía.

a veces consideran que es parte de su profesión y piensan que ha desconocimiento de las demás personas y por eso adecuan su conducta. justificándola de esa manera. como únicos entendidos en la materia piensan que la información no va a ser revelada.

**7.- En su amplia experiencia como fiscal me puede indicar ¿Cuál es la dificultad que normalmente se le presenta cuando los elementos de convicción recabados no pueden justificar un comportamiento criminal en los delitos relacionados a la esteganografía?**

al momento que no existen las licencias en criminalísticas para ser las explotaciones para intersecciones

este tipo de conducta es bastante complicado, se podría analizar bajo un análisis o un estudio para visualizar que delito informático sería, lo que mayormente la fiscalía conoce como delitos informáticos es la sustracción de dinero los elementos de convicción que normalmente tenemos es primero s demostrar la materialidad de la infracción, es decir, demostrar que existe una cuenta en donde fue debitado los valores en donde se creó esta cuenta o en donde existe. demostrando la responsabilidad de la persona y que como demostrar el nexo causal a prueba a favor el IP.

para que hablemos de convicción ya no son indicios ya son elementos que van a hacer valorados como prueba, ya estamos hablando de que hay una certeza de la infracción. entonces no hay una justificación que pueda justificar un comportamiento criminal de esa manera.

## **6. ANALISIS GENERAL DE ENTREVISTAS.**

De acuerdo a las entrevistas realizadas a jueces, fiscales, y perito, al tema de esta tesis titulado como “estudio criminológico de la esteganografía “se llega al análisis que la esteganografía se relaciona con otros tipos de delitos que el código orgánico integral penal establece, pero sin embargo a pesar que esta práctica no se encuentra tipificado como un delito en nuestro país se pone aplica en relación con otros delitos, debido a que la esteganografía es el ocultamiento de información a través de imágenes, audios y videos, para los jueces la pericia en casos de delitos informáticos presentados en la península son muy pocos además manifestaron que hace falta peritos que puedan validar las respectivas pericias para que sea válida como prueba.

Para los fiscales la esteganografía, indicaron que es nuevo este comportamiento criminal, además que es relevante contar con una pericia técnica de orden informático, efectos que se determina a través de peritos especializados en este caso.

Para el perito de acuerdo a su experiencia este tipo de comportamiento criminal se vincula con delitos informáticos, además dentro de la criminología es importante estudiar y analizar las formas en las que los delincuentes piensan, los peritos como criminalística realiza análisis criminológicos en base a pruebas es decir indicios que les permita tener una hipótesis de un caso en específicos una de las técnicas más común para identificar los delitos que se asocian con la esteganografía es a través de la informática forense y también la psicología forense ya que están vinculadas a la criminología.

#### **4.2. Verificación de la idea a defender**

La presente investigación tiene el fin de determinar si la practica de la esteganografía en el uso de los medios informáticos, es un soporte para el cometimiento de delitos informáticos, que conllevan a un comportamiento criminal que debería ser sancionado por su práctica en específico con aporte de doctrina vinculante, y mediante una tipificación sancionadora sobre su práctica delictiva.

Para ello se realizó de forma metodológica una investigación de carácter bibliográfico, documentológico, con técnicas de investigación como la recolección, encuestas y entrevistas a aquellos servidores judiciales, peritos, y abogados en libre ejercicio con el fin de determinar si la practica de la esteganografía en el ámbito penal.

Dentro de la investigación planteada y ejecutada se logro determinar que para que la práctica de la esteganografía logre determinarse como un comportamiento criminal deben influir varios factores que deben ser sometidos a una valoración determinada entre estos parámetros encontramos, el uso que le den a la esteganografía, es decir, si es usada para ocultar información se valor y confidencial cumple con ser un acto violatorio de la normativa, otro parámetro el fin de la práctica, es decir, que el ocultamiento de la información enviada a través de imágenes tenga como fin vulnerar el patrimonio de una persona o un tercero, y por ultimo parámetro, la confidencialidad de la información, es decir, si una información es de uso reservado y una tercera persona con acceso restringido a esa información utiliza la esteganografía para filtrar aquella información reservada ocultándola sobre otra información de ámbito público, se determina que hay un uso inadecuado de una información reservada y que se está filtrando a través del uso metódico de la esteganografía, se determina como un acto criminal el cual debe ser sancionado.

Por lo que la idea principal a defender dentro de la presente investigación es acepta, determinando que el uso de la esteganografía, si es un soporte para el cometimiento de delitos, sin embargo, este esta determinados bajo parámetros específicos como ya se determinó, su uso, su fin, y la confidencialidad de la información que se somete a esta práctica.

Adicionalmente, se logro determinar que la normativa legal debe establecer una sanción sobre la forma específica del usos inadecuado de la esteganografía, dado que la normativa legal vigente solo determina de forma general sanciones a los delitos informáticos, siendo un hecho que la

practica de la esteganografía necesariamente debe cumplir ciertos parámetros para determinarse como un acto criminal.

## CONCLUSIONES

En conclusión a la investigación realizada se lograron determinar varios puntos importantes que se deben analizar detenidamente para la aplicación de una normativa eficaz en el uso de los medios informáticos, el Ecuador ha evolucionado constantemente a treves del tiempo y reformas y demás aplicaciones legales dentro del ámbito informático, sin embargo esta normativa actualmente se enfrasca detenidamente en la protección de datos, dejando en oscuridad legal cuales son las practicas y usos constantes de los actos criminales a través de los medios electrónicos.

Deben determinarse estudios específicos con apoyo de los estudios criminológicos en base a los delitos informáticos que vallan correlacionado los diversos ámbitos de aplicación informática y practica inadecuada con fines delictivos de los medios electrónicos, ejemplo la presente investigación el uso de la esteganografía como apoyo al cometimiento de actos delictivos.

El código orgánico integral penal debe adecuarse debidamente a las nuevas formas de uso delictivo de los medios informáticos, toda vez que los medios de información tienen usos restringidos y poco perceptibles a la interpretación normativa vigente, con lo que se dificulta poder determinar los parámetros adecuados de un medio informático con fin delictivo.

El Ecuador debe ratificar aquellos convenios y tratados internacionales, que agilitan los medios adecuados para la incorporación de nuevas prácticas de investigación en la política criminal del país, siendo que es uno de los sectores mas vulnerables del derecho al estar limitados por no tener los medios adecuados para la aplicación investigativa en el ámbito criminológico.

## **RECOMENDACIONES**

Se recomienda que se realicen estudios criminológicos que tengan con fin de determinar los parámetros que conllevan a un comportamiento criminal en el uso de la práctica de la esteganografía como soporte del cometimiento de delitos con relación a los delitos informáticos.

Se recomienda a la asamblea nacional y a función judicial el análisis e implantación de una política criminal en base a los estudios criminológicos y su contramedida con la ciberdelincuencia que usas los medios electrónicos como herramienta de apoyo.

Se recomienda a los legisladores que determinen y establezcan parámetros adecuados de investigación científica en el ámbito normativo penal, que sirvan de apoyo en las investigaciones criminales a través de los medios electrónicos.

Se recomienda al presidente de la republica del ecuador que se ratifique con los tratados y convenios internacionales adecuados que sirvan de apoyo internacional, para la política criminal del país, y así incorporar los medios adecuados de investigación criminal en los delitos como el uso inadecuado de la esteganografía.

## BIBLIOGRAFÍA

- alvarado, c. e. (2011). *METODOLOGIA*. . mexico: EDITORIAL LIMUSA S.A.
- Aspasia, G. (2021). *grupoaspasia.com*. Obtenido de grupoaspasia.com:  
<https://grupoaspasia.com/es/glosario/metodo-de-investigacion-deductivo/#:~:text=El%20m%C3%A9todo%20deductivo%20es%20un,de%20una%20serie>
- ayudaleyprotecciondatos.es*. (13 de 5 de 2020). Obtenido de ayudaleyprotecciondatos.es:  
<https://ayudaleyprotecciondatos.es/2020/05/13/esteganografia/#:~:text=El%20primer%20uso%20de%20la,se%20usaron%20luz%20o%20calor>
- bernal, C. A. (2010). *METODOLOGIA DE LA INVESTIGACION*. BOGOTA: Pearson Educación de Colombia Ltda.
- C., B. B. (2008). *metodologia de la investigacion cientifica*. repositorio.uptc.edu.com.
- Castro, P. S. (2009). *metodos de investigacion social*. quito: quipus.
- ciberdelincuencia, c. s. (2001). *oas.org*. Obtenido de oas.org:  
[https://www.oas.org/juridico/english/cyb\\_pry\\_convenio.pdf](https://www.oas.org/juridico/english/cyb_pry_convenio.pdf)
- ciberseguridad*. (2022). Obtenido de ciberseguridad: <https://ciberseguridad.com/guias/esteganografia/>
- COCA, I. G. (2017). *www.uaeh.edu.mx*. Obtenido de [www.uaeh.edu.mx](http://www.uaeh.edu.mx):  
[https://www.uaeh.edu.mx/docencia/P\\_Presentaciones/b\\_huejutla/2017/Metodo\\_Analitico.pdf](https://www.uaeh.edu.mx/docencia/P_Presentaciones/b_huejutla/2017/Metodo_Analitico.pdf)
- DERECHO, L. M. (2022). *ava.upse.edu.ec*. Obtenido de [ava.upse.edu.ec](http://ava.upse.edu.ec):  
[https://ava.upse.edu.ec/pluginfile.php/437317/mod\\_resource/content/1/LAINVESTIGACION](https://ava.upse.edu.ec/pluginfile.php/437317/mod_resource/content/1/LAINVESTIGACION)
- López et al, 2. p.-1. (2000).
- López-Roldán, P. &. (2015). *metodologia de la investigacion social cuantitativa*. barcelona - españa: Bellaterra (Cerdanyola del Vallès) .
- MANRIQUE, F. (4 de 11 de 2021). *trentia.net*. Obtenido de [trentia.net](http://trentia.net):  
<https://www.trentia.net/evolucion-de-la-estenografia-desde-sus-origenes-hasta-la-era-digital/>
- NACIONAL, R. D. (2017). *codigo organico integral penal*. quito: lexisfinde.
- RABELL, D. L. (2008). *GUÍAS PARA ELABORAR FICHAS BIBLIOGRÁFICAS EN LA REDACCIÓN DE ENSAYOS, MONOGRAFÍAS Y TESIS*. . puerto rico.
- Reidl-Martínez, L. M. (2012). *Marco conceptual en el proceso de investigación*. mexico: ELSEVIER.
- sempieri r, h. (2014). *Metodologia a la investigacion 6ta edicion*. MEXICO: MCGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.
- Sutherland, C. y. (2012).
- Velasco Bautista, López Hernández, & Nakano Miyatake, & Pérez Meana. (2020). estudio sobre la esteganografia.

# ANEXOS

ENTREVISTA A LOS JUECES DE LA UNIDAD PENAL EN LA PROVINCIA DE SANTA ELENA.



ENTREVISTA A LOS FISCALES DE LA PROVINCIA DE SANTA ELENA.





ENTREVISTA AL PERITO DE LA PROVINCIA DE SANTA ELENA.



