UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE JURISPRUDENCIA CIENCIAS SOCIALES Y POLÍTICAS, CARRERA DE DERECHO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADA.

TEMA:

"LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021".

INVESTIGADOR:

BRENDA NARCISA PEÑALOZA JIMENEZ.

TUTOR DEL PROYECTO DE INVESTIGACIÓN:

DR. GONZALO NOBOA LARREA.

GUARANDA

2022

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE JURISPRUDENCIA CIENCIAS SOCIALES Y POLÍTICAS, CARRERA DE DERECHO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADA.

TEMA:

“LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021”.

INVESTIGADOR:

BRENDA NARCISA PEÑALOZA JIMENEZ.

TUTOR DEL PROYECTO DE INVESTIGACIÓN:

DR. GONZALO NOBOA LARREA.

GUARANDA

2022

CERTIFICACIÓN DE AUTORÍA

Yo, **GONZALO ENRIQUE NOBOA LARREA** en mi calidad de Director del Proyecto de Investigación, designado por disposición de Consejo, bajo juramento CERTIFICO: que la señorita: Brenda Narcisa Peñaloza Jiménez, egresada de la Universidad Estatal de Bolívar, Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Escuela de Derecho, ha cumplido con su trabajo de grado previo a la obtención del título de Abogada de los Tribunales y Jugados de la República; con el tema: **"LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021"**, mismo que ha cumplido con todos los requerimientos exigidos por la institución, siendo la misma de su propia autoría, por lo que se aprueba.

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

Atentamente

Dr. Gonzalo Noboa Larrea

iginal
by Turnitin

cument Information

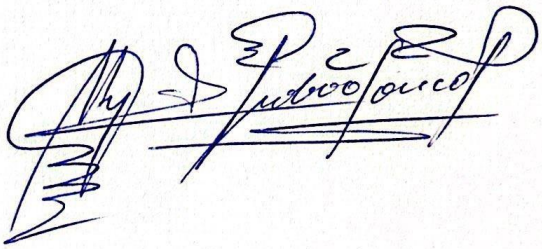
Analyzed document	BRENDA NARCISA PEÑALOZA JIMENEZ.docx (D172068307)
Submitted	7/14/2023 5:34:00 AM
Submitted by	
Submitter email	bpenaloza@mailes.ueb.edu.ec
Similarity	7%
Analysis address	gnoboa.ueb@analysis.urkund.com

ırces included in the report

ire Document

and source - focused comparison, Side by Side

Submitted text	As student entered the text in the submitted document.
Matching text	As the text appears in the source.



13/7/2023

Notaria Tercera del Cantón Guaranda
Msc.Ab. Henry Rojas Narvaez
Notario

....ria

Nº ESCRITURA 20230201003P01693

DECLARACION JURAMENTADA

OTORGADA POR:

BRENDA NARCISA PEÑALOZA JIMENEZ

INDETERMINADA

DI: 2 COPIAS L.L

Factura: 001-001-000013753

En la ciudad de Guaranda, capital de la provincia Bolívar, República del Ecuador, hoy día veinticinco de julio del dos mil veintitrés, ante mi Abogado HENRY ROJAS NARVAEZ, Notario Público Tercero del Cantón Guaranda, comparece la señorita BRENDA NARCISA PEÑALOZA JIMENEZ soltera, de ocupación estudiante, domiciliada en la ciudad de Quito y de paso por esta ciudad de Guaranda, celular número 0968659243, correo electrónico es penalozabrenda49@gmail.com , por sus propios derechos, obligarse a quien de conocerla doy fe en virtud de haberme exhibido sus documentos de identificación y con su autorización se ha procedido a verificar la información en el Sistema Nacional de Identificación Ciudadana; bien instruida por mí el Notario con el objeto y resultado de esta escritura pública a la que procede libre y voluntariamente, advertido de la gravedad del juramento y las penas de perjurio, me presenta su declaración Bajo Juramento declara lo siguientes Previo a la obtención del Titulo de Abogada de los Tribunales y Juzgados de la República, manifestó que los criterios e ideas emitidas en el presente estudio de caso titulado "LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021", es de mi exclusiva responsabilidad en calidad de autora. Es todo cuanto puedo declarar en honor a la verdad, la misma que la hago para los fines legales pertinentes. HASTA AQUÍ LA DECLARACIÓN JURADA. La misma que queda elevada a escritura pública con todo su valor legal. Para el otorgamiento de la presente escritura pública se observaron todos los preceptos legales del caso, leída que le fue a la compareciente por mí el Notario en unidad de acto, aquella se ratifica y firma conmigo se incorpora al protocolo de esta Notaria la presente escritura, de todo lo cual doy fe.-

BRENDA NARCISA PEÑALOZA JIMENEZ
C.C. 1205693825-5

ABOGADO HENRY ROJAS NARVAEZ
NOTARIO PUBLICO TERCERO DEL CANTON GUARANDA

DECLARACIÓN JURAMENTADA DE AUTORÍA

Yo, **Brenda Narcisa Peñaloza Jiménez,** portadora de la cedula N° **120569525-5**, egresada de la carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, bajo juramento declaro de forma libre y voluntaria que el presente trabajo de investigación con el tema **"LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021"** es de mi autoría, con la dirección del tutor **Dr. Gonzalo Noboa Larrea,** docente de la carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, al ser de mi autoría, debo dejar en constancia que las expresiones vertidas en todo el desarrollo del Proyecto de Investigación he realizado bajo la recolección de fuentes bibliográficas, lexigrafías, jurisprudencia y doctrina actualizada que han formado precedentes y demás firmas necesarias para la producción de esta investigación.

Atentamente:

Autor

Brenda Narcisa Peñaloza Jiménez

C.C 120569525-5

UEB | UNIVERSIDAD ESTATAL DE BOLIVAR

DERECHOS DE AUTOR

Yo; **Brenda Narcisa Peñaloza Jiménez.,** portador/r es de la Cédula de Identidad No 1205695255, en calidad de autor y titular / es de los derechos morales y patrimoniales del Trabajo de Titulación:
"LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021". Proyecto de Investigación, de conformidad con el Art. 114 del **CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN**, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

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

Autora

Brenda Narcisa Peñaloza Jiménez.

DEDICATORIA

Este trabajo de investigación va dedicado a las personas más importantes de mi vida y de mi carrera. A mis padres Darwin y Carmita, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo incondicional, por su perseverancia, amor y dedicación para alcanzar este logro. A mis hermanos: Michelle, Fernanda, Mirley, Karelys, Allan, Julián, Domenica, por ser mi apoyo y fortaleza en los días difíciles, A mis tíos, Blanca, Efraín y Patricia, por su apoyo constante, por ser parte importante y fundamental dentro de mi carrera. A mis abuelos: Mery, Blanca y Celso por velar por mi bienestar y siempre darme un consejo cuando lo necesitaba. A mi novio, por ser quien ha estado día a día apoyándome y dándome palabras de aliento cuando ya no podía más. A mis sobrinos, Aurorita, Alessandro y Sofía por ser mi motor en esta carrera. A mis amigas, Jeniffer e Ivette, por ser esas concejeras y ayudarme siempre en los momentos más difíciles.

AGRADECIMIENTO

Los resultados de este trabajo, merecen expresar un profundo agradecimiento, a aquellas personas que de alguna forma son parte fundamental de su culminación, quienes, con su ayuda, apoyo y comprensión me alentaron a lograr. Mi agradecimiento va dirigido A Dios, por su presencia en cada paso y momento de vida. A mis padres, quienes me han apoyado arduamente día tras día. A la Universidad Estatal de Bolívar, especialmente a la facultad de Jurisprudencia, Ciencias Sociales y Políticas, por todas las enseñanzas recibidas en sus aulas. A mis docentes, quienes han impartido sus conocimientos y experiencia para formarme como una profesional. A mis familiares que fueron parte esencial de mi paso por la Universidad, y aportar en mi buenos valores y perseverancia. A mi Tutor de Tesis Dr. Gonzalo Novoa Larrea por su asesoramiento constante, y persistencia en este trabajo de investigación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

Índice de figuras

1. TÍTULO:

“LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021”,

1.1. RESUMEN

La presente investigación sobre los delitos informáticos y en relevancia la especificidad sobre la cadena de custodia en el proceso judicial de delitos cibernéticos, asumí como un propósito para realizar una profunda reflexión sobre las características de la tipificación y aplicación de la ley ecuatoriana a este tipo de delitos; así como también el analizar el sistema de justicia actual en lo concerniente al adecuado tratamiento de las evidencias informáticas; de ahí la relevancia de investigar la forma cómo en el proceso judicial asume el rol de la cadena de custodia en delitos cibernéticos, como también el rol que desempeñan las Instituciones llamadas a proteger el debido proceso y los mecanismos que para aquello utilizan.

La manera de cómo se ha venido tratando esta temática ha hecho que la vulnerabilidad de los ciudadanos se aumente sobre todo con los nuevos mecanismos que utilizan quienes se dedican a estas actividades ilícitas, las mismas que van creciendo directamente proporcional al desarrollo tecnológico, ahí el desafío y el reto de la justicia ecuatoriana para propiciar acciones en pro de encontrar una solución al inadecuado tratamiento de la cadena de custodia en los delitos cibernético.

Los delitos informáticos en el Ecuador han sido tipificados en la Sección Tercera denominados como delitos contra la seguridad de los activos de los sistemas de información y comunicación, pero aun así nuestra legislación penal sigue careciendo de los mecanismos adecuados para este tipo de delitos, y sobre todo para el manejo de las evidencias, puesto que el instructivo para el manejo de indicios y/o evidencia digital es un poco escueto al manifestar el manejo de esta información de evidencias digitales y la responsabilidad que tiene la policía judicial.

Para poder obtener datos directos en esta investigación se procedió a aplicar el instrumento de la encuesta; la muestra obtenida fue efectuada a Jueces, , Fiscales, Policía Judicial, Peritos y Abogados en libre ejercicio de la Provincia Bolívar, resultados que serán analizados e interpretados dando sustento a la problemática planteada como también se dieron hallazgos que

permitieron sustentar la comprobación de la hipótesis planteada, y verificar como la Administración de Justicia cumple con el debido proceso.

ABSTRACT

The present investigation on computer crimes and in relevance the specificity of the chain of custody in the judicial process of cyber-crimes, I assumed as a purpose to carry out a deep reflection on the characteristics of the classification and application of Ecuadorian law to this type of crimes; as well as analyzing the current justice system regarding the proper treatment of computer evidence; Hence the relevance of investigating how in the judicial process it assumes the role of the chain of custody in cybercrimes, as well as the role played by the Institutions called to protect due process and the mechanisms they use for that.

The way in which this issue has been treated has increased the vulnerability of citizens, especially with the new mechanisms used by those who engage in these illegal activities, which are growing directly proportional to technological development, hence the challenge and the challenge of the Ecuadorian justice to promote actions in favor of finding a solution to the inadequate treatment of the chain of custody in cybercrimes.

Computer crimes in Ecuador have been classified in the Third Section as crimes against the security of the assets of information and communication systems, but even so our criminal legislation continues to lack the adequate mechanisms for this type of crime, and on everything for the handling of the evidence, since the instructions for the handling of digital evidence and/or evidence is a bit concise when stating the handling of this digital evidence information and the responsibility of the judicial police.

In order to obtain direct data in this investigation, the survey instrument was applied; The sample obtained was made to Judges, Prosecutors, Judicial Police, Experts and Lawyers in free practice of the Bolívar Province, results that will be analyzed and interpreted, giving support to the problem raised as well as findings that allowed supporting the verification of the hypothesis. raised, and verify how the Justice Administration complies with due process.

GLOSARIO DE TÉRMINOS

Cadena de Custodia

Es el conjunto de procedimientos tendientes a garantizar la correcta preservación de los indicios encontrados en el lugar de los hechos; durante todo el proceso investigativo, y que, dentro de la etapa del juicio, servirá de prueba para que el tribunal de justicia decida sobre la responsabilidad o inocencia del acusado. (Fiscalia General del Estado, 2014)

Custodia

Es el almacenamiento de indicios, muestras y/o evidencias bajo medidas de seguridad y condiciones adecuadas de conservación y preservación. (Fiscalia General del Estado, 2014)

Indicio

Todo objeto, instrumento, huella, marca, señal o vestigio que se usa y se produce respectivamente en la comisión de un hecho; puede ser cualquier cosa, desde objetos enormes hasta partículas microscópicas, que se originaron en la perpetración de un delito y se recogen en la escena del delito o en lugares conexos. (Fiscalia General del Estado, 2014)

Informática forense

Conjunto de métodos que en la actualidad sirven de apoyo a la justicia al momento de determinar y enfrentar la gama de delitos informáticos existentes, recopilando, almacenando y mostrando la información procesada y guardada en un medio informático de manera local o remota (Gutierrez Á. , 2015)

Evidencia Digital

Información o datos, almacenados en un sistema informático, misma que se puede considerar como prueba en una investigación dentro de un proceso judicial.

Criminalidad informática

Como define Davara, “Es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos.” (1990).

Evidencia digital

Casey lo define como, "Cualquier dato que puede establecer que un crimen se ha ejecutado puede proporcionar un vínculo entre un crimen y su víctima o un crimen y su autor." (2011)

Perito Informático

Es aquella persona con conocimiento técnico y analítico, que se encarga de tomar las pruebas respectivas del caso a ser tratado, hallar pistas que ha dejado la intrusión, realiza informes para que sirva de soporte en la declaración ante los tribunales para brindar una gestión más clara al fiscal.

1.2. INTRODUCCIÓN

Hoy en día las nuevas tecnologías han evolucionado formando parte esencial de las actividades de nuestra sociedad, independientemente del tipo de actividad o profesión a las que se dediquen los individuos. Esta realidad ha creado dos dilemas en el campo legal que ameritan una atención especial. El primer dilema, se trata de una inminente migración de los delitos convencionales al campo digital, por consiguiente, el cambio refleja un escenario de delito distinto al habitual y un tipo de prueba diferente, detallada dentro del Artículo 500 del Código Orgánico Integral Penal (COIP) como contenido digital. Un segundo aspecto a considerar, es que en cualquier delito convencional podemos encontrar como evidencias equipos con contenido digital que son usados normalmente para el procesamiento de información como celulares, computadores, Tablet, memorias USB, etc. Con la entrada en vigencia del Código Orgánico Integral Penal, entraron en vigor artículos referentes a la cadena de custodia sobre contenido digital y el tratamiento sobre este elemento probatorio. Al ser considerada como prueba documental, el contenido digital requiere un tratamiento especial y diferente al resto de evidencias por su fragilidad y constante riesgo de ser alterada y contaminada.

Al hablar de la cadena de custodia podemos manifestar que son un conjunto de técnicas y procedimientos que permite mantener la integridad, identidad y conservación de los indicios encontrados en el lugar de los hechos mismas que servirán para que después de su análisis lleguen a ser presentadas en juicios, de forma una impecable y real. La cadena de custodia pretende garantizar la integridad y autenticidad de los elementos de prueba hasta la finalización del juicio, pero al tratarse de contenidos digitales casi siempre están expuestos a recaer en nulidad por una mala práctica procesal que se ve expuesta al no cumplir con lo que dicta el Código Orgánico Integral Penal, o porque el procedimiento que este maneja, no está correctamente explicado para este tipo de pruebas.

De allí que pueden presentarse problemas en el manejo de contenidos digitales durante la incautación inicial de los elementos de prueba, durante el traslado y registros en las bodegas de evidencias o durante los procesos de peritaje, generando de esta forma una falla procesal que puede generar solicitudes de nulidad de la prueba por una de las partes.

1.3. PLANTEAMIENTO DEL PROBLEMA

La cadena de custodia en lo referente a los delitos cibernéticos, es una temática que por muchos años en el Ecuador se le ha restado la importancia y relevancia que necesaria que esta necesita dentro del proceso legal, por parte de las instancias de administración de justicia, acciones estas que muestran la vulnerabilidad de nuestro sistema legal ecuatoriano.

Los delitos informáticos tienen la complejidad del uso de tecnologías lo que ha creado un fenómeno delictivo complejo dando a las ciencias jurídicas un enfoque en el que se interrelacionan varias ciencias y específicamente es el caso de las ciencias forenses las que hoy por hoy cuentan con la rama de la informática forense como un instrumento para cumplir con el acometido de practicar efectivamente la cadena de custodia en delitos relacionados con la seguridad de los sistemas informáticos, su integridad y sobre todo cumplir con los procedimientos para determinar con legalidad y efectividad lo que ha sucedido en cuanto a la supuesta comisión de un delito o infracción.

La cadena de custodia como principio principal pretende garantizar la integridad y autenticidad de los elementos de prueba hasta la finalización del juicio, pero al tratarse de contenidos digitales casi siempre están expuestos a recaer en nulidad por una mala práctica procesal que se ve expuesta al no cumplir con lo que dicta el Código Orgánico Integral Penal, o porque el procedimiento que este maneja, no está correctamente explicado para este tipo de pruebas.

De allí que pueden presentarse problemas en el manejo de contenidos digitales durante la incautación inicial de los elementos de prueba, durante el traslado y registros en las bodegas de evidencias o durante los procesos de peritaje, generando de esta forma una falla procesal que puede generar solicitudes de nulidad de la prueba por una de las partes.

1.4. FORMULACIÓN DEL PROBLEMA

¿Cómo incide el inadecuado tratamiento de la cadena de custodia en los delitos informáticos en el proceso judicial penal ecuatoriano en el año 2021?

1.5. OBJETIVOS DE LA INVESTIGACION

1.5.1. Objetivo General

Analizar el inadecuado tratamiento de la cadena de custodia por la falta de una debida recopilación, procesamiento y almacenamiento de evidencias digitales.

1.5.2. Objetivo Específicos

- Realizar un estudio sobre la cadena de custodia en los delitos informáticos.
- Determinar el grado de incidencia del inadecuado tratamiento de la cadena de custodia en los procesos judiciales sobre delitos informáticos.
- Establecer la falta de celeridad en la recopilación, procesamiento y almacenamiento de las evidencias digitales.

1.6. Justificación

Las normas de procedimiento en la cadena de custodia que utilizan los responsables de la recopilación de evidencias físicas, garantizan la preservación, confiabilidad y registro de las mismas, pues estas personas son las primeras en llegar al reconocimiento del lugar de los hechos y por ende es su deber custodiar las evidencias de una manera responsable.

Se debe tomar en cuenta que cuando una evidencia es desaparecida o no fue tratada correctamente, se está viciando a los elementos de convicción determinantes para comprobar la existencia del delito y la participación del presunto autor, y a su vez, se está violando la garantía del debido proceso y varios principios fundamentales del derecho penal como el de inocencia, duda a favor del reo y objetividad, pues esto podría llevar a que una persona inocente sea sancionado por un delito que no cometió, o caso contrario, que un culpable sea hallado inocente. La cadena de custodia es un conjunto de pasos desarrollados sistemática y prolijamente dentro de una investigación, se realizan para que las evidencias recopiladas no sean alteradas y tampoco destruidas, garantizando de esta manera que lo analizado por los peritos forenses corresponda a lo que se recopiló en el lugar del delito.

Actualmente en el Ecuador, el manejo de la cadena de custodia se ha modificado y mejorado notablemente, aunque se ha de destacar que continúa siendo un procedimiento débil que merece ser observado e investigado, pues sigue siendo ineficaz y consecuentemente genera problemas dentro del procedimiento penal.

De ahí la relevancia e importancia de ésta investigación que pretende fortalecer el desempeño y experticia al momento de manejar las evidencias e indicios digitales con procedimientos y metodología técnica y operativa, con la finalidad de garantizar la validez y confiabilidad del informe posterior al análisis de las evidencias y que brinden al juzgador la certeza y el convencimiento de los hechos y circunstancias materia de la infracción como

también la responsabilidad de la o las personas relacionadas al hecho, quedando claramente determinado su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica y de esta manera alcanzar el valor de prueba

1.7. HIPÓTESIS

El inadecuado tratamiento de la cadena de custodia en los delitos informáticos afecta el debido proceso.

1.8. VARIABLES

1.8.1. Variable Dependiente

cadena de custodia

1.8.2. Variable Independiente

delitos informáticos

2. CAPITULO II MARCO TEÓRICO

2.1. ANTECEDENTES

En los últimos 10 años, Se ha escuchado a través de casos denunciados sobre la tenencia que origina los delitos informáticos en nuestro país y en toda parte del mundo, el alcance y pérdidas que trae como consecuencias estas amenazas. A medida que surgían estos problemas, el país no contaba con leyes necesarias para finalizar a los delincuentes. Por lo tanto cometerlos era un tema que no podían ser sancionados existía muchas partes vulnerables y falencias en las leyes del Ecuador puesto que no existía mucha información acerca de los delitos cibernéticos y peor aún Se desconocía el tratamiento a las pruebas que servirían para determinar la materialidad de la infracción, ya que una falla por parte de las encargadas o encargados de su manejo podría provocar una nulidad, los delitos informáticos también se puede hallar gran cantidad de información de cómo causar daño a través del Internet manuales sitios dedicados donde se pueden aprender diferentes métodos de ataque. El Ecuador ha sufrido muchos incidentes por intromisiones informáticas como son fraudes bancarios violación a la privacidad de datos y extorsiones a través de redes sociales.

Ante la falta de un proceso legal no había una sanción tipificada para estos delincuentes cibernéticos o informáticos, el Ecuador tampoco contaba con los recursos suficientes en tecnologías y personal necesario para llevar a cabo una la indagación respectiva. Actualmente con la entrada en vigencia del código orgánico integral penal contamos con profesionales encargados para realizar estas investigaciones un peritaje informático consiste en precautelar la evidencia digital para que a lo largo de la búsqueda pueda descubrir las pistas necesarias para poder encontrar la información necesaria. Es por ello que las nuevas tecnologías tomen asunto de la seguridad y protección de la información para que la ciudadanía se sienta mayor confianza.

2.2. CRIMINALIDAD INFORMÁTICA

Cómo define Davara, “es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne un tratamiento automático de datos y/o transmisión de datos” (Davara, 1990)

La criminalidad informática es toda acción que implique la utilización indebida de ordenadores o la utilización de cualquier medio de tecnología, herramientas virtuales, con el fin de cometer un perjuicio para obtener toda la información necesaria del usuario comprometiéndolo fácilmente por el atacante, robo de dinero en sus cuentas bancarias, extorsiones a través de publicaciones dolosas y comprometedoras, falsificación, robo de propiedad intelectual.

2.3. CADENA DE CUSTODIA

La cadena de custodia en un proceso judicial es un eje fundamental al momento de buscar un juzgamiento imparcial, real y equitativo, una vez producido el hecho delictivo los agentes que hayan llegado al lugar físico o virtual donde se generaron estos actos punitivos, se da inicio al conjunto de procedimientos previamente establecidos y normados con la finalidad de asegurar la integridad y conservación de los indicios y evidencias.

Cabe resaltar que este conjunto de operaciones siempre debe cumplirse de tal forma que no quepa la menor duda de su validez, y tener la confianza de que los análisis o estudios que se han realizados por los peritos calificados cuenten con el sustento procedimental adecuado y al momento de ser exhibidos en el juicio los mismos sean apreciados como prueba dando al juzgador una apreciación real y contundente de los hechos suscitados.

El en su Artículo 456, manifiesta contenido sobre la Cadena de custodia en la que en la parte pertinente dice: “Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y

conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio" (2014).

Los legisladores ecuatorianos han dado un paso fundamental y progresivo en la definición de contenido digital, lo que da paso al fortalecimiento y tratamiento de los datos digitales; cabe indicar que el antes mencionado artículo en su segundo párrafo se da mayor profundidad en la definición abordando que la cadena de custodia inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Además determina el grado de responsabilidad de su aplicación, al referirse que el personal del sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación, serán responsables de la custodia de los indicios y evidencias hallados.

para el jurista Jorge Badilla es "…el procedimiento de control que se aplica al indicio material relacionado con el delito, desde su localización por parte de una autoridad, hasta que ha sido valorado por los órganos de administrar justicia y deja de ser útil al proceso y que tiene como fin no viciar el manejo de que se haga para evitar alteraciones, daños, sustitución, contaminación, destrucción, o cualquier acción que varíe su significado". (1999)

la Cadena de Custodia en una definición propia: es un conjunto de procedimientos legalmente establecidos por las leyes vigentes, y son aquellos los que permiten realizar una investigación sobre los vestigios y evidencias con el fin de garantizar su validez ante la justicia y que para el efecto no debe quedar la menor duda de su: integridad, originalidad, seguridad y de ser el caso dejando claramente establecido la relación entre el delito cibernético, el lugar del suceso y la persona o persona inculpadas es decir que quede ligado el nexo causal.

2.3.1. Principios de la cadena de custodia

Principios de la Cadena de Custodia Para poder garantizar la legalidad de la Cadena de Custodia deben cumplirse varios principios que deben obligatoriamente cumplir quienes tienen bajo su responsabilidad la custodia de las evidencias e indicios, cuyos procesos son normados legalmente para su aplicación adecuada y oportuna garantizando así el debido proceso enmarcados en los derechos y garantías constitucionales como también del debido proceso penal. Estos principios se abordan a continuación:

1.- Las acciones técnicas y administrativas deben ser ejecutadas de tal manera que se garantice la preservación del lugar de los hechos.

2.- El personal debe tener la pericia necesaria para fortalecer el proceso de esclarecimiento de los hechos suscitados.

3.- Es de gran importancia la rapidez con la que se arriba al lugar de los hechos, lo cual facultara en un análisis efectivo de la escena como en la recolección de evidencias, en el caso de los delitos cibernéticos es de vital importancia realizar la recolección en el menor tiempo posibles evitando de esta manera que los datos volátiles se pierdan.

4.- los funcionarios o ciudadanos que sean responsables o en algún momento se encuentren en el proceso de custodia, velarán por la integridad, seguridad y preservación de los indicios y evidencias, para lo cual deberán conocer los procedimientos establecidos. Las autoridades competentes deberán garantizar que el personal encargado de estas actividades cuente con la experticia necesaria para el efecto.

5.- Toda actividad correspondiente a la Cadena de Custodia debe quedar debidamente registrada sin excepción alguna y las evidencias deben estar en áreas especializadas de ciencias forenses para garantizar su conservación. Las actas de diligencias realizadas deben constar con una descripción completa registrando detalladamente su naturaleza, sitio exacto de donde fue

encontrado, tomado o removido como también contener los datos de la persona o funcionario que realizo esa actividad.

6.- Los análisis periciales deberán constar en acta, como también una descripción detallada de los elementos y las técnicas y procedimientos científicos utilizados. En el centro de acopio o área forense cumplirá con las normas de seguridad necesarias para evitar que se rompa el proceso de Cadena de Custodia.

7.- Se debería contar con un sistema de registro automatizado de los traslados y traspasos de los indicios y evidencias en la que cuente con la identidad de cada uno de los custodios y de las acciones realizadas y así poder contar con un formato estándar de Cadena de Custodia.

8.- Una vez concluida el proceso penal se procederá a devolver las evidencias a las personas correspondientes cumpliendo las normativas legales para el efecto.

2.2.2. Objetivo de la Cadena de Custodia

El objetivo de la cadena de Custodia es que los indicios y evidencias analizadas en el laboratorio y que estas al ser presentadas en el juicio sean las mismas que se recogieron en el lugar de los hechos manteniendo su autenticidad y su valor probatorio.

La Cadena de Custodia, en el proceso penal nos permite saber las acciones realizadas o los datos extraídos y quienes son las personas responsables, el nombre del perito o peritos que intervinieron, las investigaciones realizadas a las evidencias entre otras, cabe indicar que además de las evidencias también hacen parte de la cadena de custodia todos los documentos como actas, fichas identificativas, registros, oficios legales y demás que son parte del procedimiento dando así todas las garantías necesarias demostrando que la posesión de la evidencia la han tenido en todo momento personas autorizadas y que no ha habido intervención de extraños y la han preservado en su estado original y de no ser ese el caso el o los custodios

deberán demostrar su relación de no pretender alterar las evidencias y de existir negligencia tomar las acciones legales pertinentes.

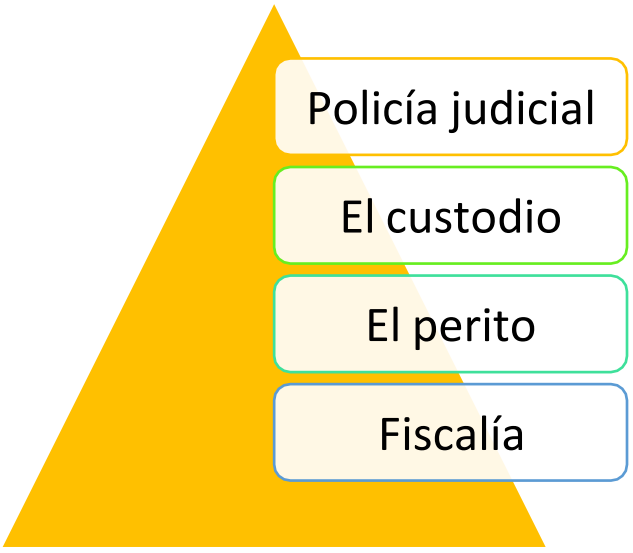
La cadena de custodia destaca por estos tres objetivos:

1.- Recoger indicios y evidencias en el lugar de los hechos, para lo cual se debe cumplir con procedimientos que garanticen la originalidad e integridad fortaleciendo el debido proceso.

2.- Cumplir con los protocolos científicos, para evitar alteraciones, degradaciones, contaminación y destrucción de las evidencias recogidas en el lugar de los hechos, como también registrar las personas que tuvieron contacto, acceso, tiempos que permanecieron en su custodia, como también saber las pericias forenses realizadas, garantizando de esta manera una custodia exitosa.

3.- Presentar en el juicio las evidencias y los informes para su respectiva valoración por la autoridad competente demostrando su autenticidad, integridad, preservación, seguridad, almacenamiento, continuidad y registro.

figura 1 Encargados de la cadena de custodia



Fuente: *elaborado con información recabada de la investigación*.

Autor: *Brenda Peñaloza*

2.4. DELITOS INFORMÁTICOS

Es aquella forma ilícita de destruir y dañar ordenadores, medios electrónicos y redes de internet entre sus características son:

- Obtener las pruebas después del cometimiento del delito es complicado.
- Tienden a expandirse en ataque a sistemas seguros.
- Recuperación de la información.
- Descifrado de claves criptográficas.

2.4.1. Clasificación de los delitos informáticos

Como instrumento o medio: Consiste en temas relacionados como son: la falsificación electrónica, robo, amenazas, muertes, interceptación en redes de información y divulgación.

Con fin u objetivo: Está vinculado con sabotajes, accesos ilícitos, programaciones de ataques, etc.

figura 2 tipos de delitos

FUENTE. *Elaborado por la Fiscalía General del Estado***,** año 2017.

Los ataques de las cibermafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3 183 delitos informáticos. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1 851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650 investigaciones a escala nacional.

Gonzalo García, jefe de la Unidad de Ciberdelitos, dice que este tipo de hechos delictivos ocurren porque las personas tienen más acceso a Internet y redes sociales. Cifras oficiales muestran que el 79,21% de la población ecuatoriana tiene acceso a la web y alrededor de 15,8 millones de personas en el país tienen cuentas en las diferentes redes sociales. (El Comercio, 2022)

2.4.2. La Prueba

El objetivo de la prueba es llegar al juez de una manera ilesa o por lo menos bien valorada para que el de acuerdo a su sana critica pueda valorar si es pertinente, licita y oportuna; mima que no sufra que no sea capaz de ser excluida o peor aún sede de baja el juicio por la no existencia de elementos probatorios.

Según el Art. 453 La prueba tiene por finalidad llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada. (Código Orgánico Integral Penal, 2014)

La prueba dentro de un proceso actúa como dador de vida, tiene la finalidad que el proceso tome forma e intensidad de acuerdo a que prueba y como este manejada llegando así al proceder de la justicia tanto que la prueba en toda materia; y, particularmente en materia penal, debe ser practicada observando fielmente los derechos y garantías consagrados en la

Constitución de la República, así como también considerando la presunción de inocencia de toda persona.

La prueba se divide en tres grandes grupos como son:

- Testimonial
- Documental
- Pericial

El contenido digital entra en el grupo de pruebas documentales.

Las Pruebas Digitales

Eoghan Casey, nos dice que "las pruebas digitales, es un tipo de evidencia que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales."

Otros tratadistas de la materia consideran como pruebas digitales a todos los datos generados o almacenados en medios digitales. (2011)

Medios Digitales

Al hablar de medios digitales hablamos de cualquier dispositivo informático a fin, que tenga capacidad de almacenar información como resultado de algún proceso, por ejemplo, computadoras personales y portátiles, celulares, Tablet, memorias USB, consolas de videos juegos, cámaras fotográficas, GPS, cámaras de video, relojes, drones, memorias de vehículos, etc.

Evidencia Digital

Desde el punto de vista del derecho probatorio, abarca cualquier información en formato digital que pueda establecer una relación entre un documento y su autor. Según los tratadistas como el Dr. Jeimy J. Cano "La evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso" (Cano, 2013)

Contenido Digital

El Código Orgánico Integral Penal en su artículo 500 conceptúa al contenido digital como "todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí".

2.4.3. Enfoque Doctrinario de las Pruebas o Evidencias Digitales

Dentro de la doctrina referente a evidencia o prueba digital encontramos algunos tratadistas que nos hablan de este notable tema. Abordaremos y analizaremos algunos criterios referentes. Dentro de la doctrina existente Miguel López Delgado nos dice que "la evidencia digital es el conjunto de datos en formato binario, esto se comprende en los archivos, su contenido o referencias a éstos, que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático" (2012,p. 14). Podemos mencionar igualmente lo que nos dice Anthony Reyes que se refieren a la evidencia digital como "objetos de datos, en relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento de multimedia, que no son más que cadenas de unos y ceros, es decir de información binaria o digital grabada en un dispositivo magnético (como discos duros o los disquetes), en uno de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD)". (2010,p. 22)

El jurista ecuatoriano Santiago Acuario del Pino menciona a la evidencia digital de la siguiente manera, "La evidencia digital se constituye en todos aquellos datos e información histórica y presente almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia". (2012, p. 33)

Con la definición directo de diferentes tratadistas queda establecido que la evidencia digital es aquel indicio que sirve como guía para la realiza con de diferentes procesos o acciones para que se convierta en pruebe y cabe recalcar que la prueba digital o electrónica nacerá de la evidencia y de su tratamiento y servirá para llevar al juez a la convicción.

2.4.4. El peritaje

Los juristas Dager Aguilar Avilés Dager y Aguilar Avilés manifiestan que por "Peritaje" debe entenderse toda aquella actividad de estudio realizada por una persona o equipo de personas hábiles y prácticos en el tema objeto de peritaje y que poseen acreditación certificada de sus habilidades y conocimientos encaminada a obtener criterios certeros e indubitados útiles para los fines de la actividad procesal. (2010)

Dentro del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses Protocolo del Centro de Acopio se establece el término peritaje: Peritaje. - Es el estudio técnico científico realizado por un perito en determinada materia.

2.4.5. Perito Informático

Es aquella persona con conocimiento técnico y analítico, que se encarga de tomar las pruebas respectivas del caso a ser tratado, hallar pistas que ha dejado la intrusión, realiza informes para que sirva de soporte en la declaración ante los tribunales para brindar una gestión más clara al fiscal, consta de tres etapas como son:

- Toma en contacto
- Desarrollo de la Investigación, elaboración de informes.
- Declaración ante tribunales.

2.4.6. Reglas del área pericial

En el artículo 511del Código Orgánico Integral Penal, están citados los requisitos que deberán cumplir los peritos:

1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.

2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.

3. La persona designada deberá excusarse, si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.

4. Las o los peritos no podrán ser recusados, sin embargo, el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.

5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.

6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.

7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.

2.4.7. Funciones en el área de peritaje informático

- Identificación y recolección de evidencias.
- Análisis forenses en dispositivos.
- Análisis de paquetes de datos.
- Reconstrucción de la escena del crimen.
- Rastros de mensajerías y ficheros

2.4.8. consecuencias legales de la evidencia mal manejada

Como consecuencia de un mal proceder frente a la cadena de custodia en contenido digital se daría como resultado principal la exclusión de la prueba.

Exclusión

Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal. Lo cual hace de un juicio un procedimiento fallido y a su vez que sin prueba no se podría avanzar a y se dictara sobreseimiento o cual sin elementos que vinculen al sospechoso se presumirá tal cual su inocencia a la vez que se ordenara la inmediata libertad.

Tal es hecho si hablamos de consecuencias del mal manejo de la cadena de custodia hablamos de la vulnerabilidad de Estado como justicia se quedaría de lado el debido proceso entonces perdería la capacidad como Estado garantista al ver que los derechos de las personas se vulneran generando fallas gravísimas por la no capacitación oportuna de los miembros operadores de justicia. Al haber exclusión, rechazo o inadmisibilidad de prueba, no habrá suficientes elementos de convicción, y no se podrá concluir con una acusación ya que ha quedado sin efecto todo el proceso de juicio.

2.5 SUJETOS DEL DELITO CIBERNETICO

Vivimos en una época en que la sociedad ecuatoriana como la del mundo entero se encuentra informatizada incluso en las actividades más básicas del ser humano como es la comunicación. Esta relación tecnología – ser humano en algunos casos muy crónicos se ha convertido en una dependencia a la informática y las nuevas tecnologías de la información y comunicación, pero sin embargo ha hecho de las actividades cotidianas una forma de sistematizar nuestras actividades y servicios como al usar pagos de servicios básicos, pagos en entidades financieras uso de tarjetas de crédito, uso de correo electrónico, sus datos personales

fichados en los registros y archivos nacionales, actividades tributarias, entre otras actividades comerciales y de registros de información.

No hay duda de las generosas ventajas incuestionables que brinda el uso de las tecnologías, pero al mismo tiempo somos muy vulnerables a ser víctimas de actos antijurídicos digitales que se lleven contra estos sistemas o medios informáticos. En el Ecuador la vulnerabilidad de ser víctima de estos actos ilícitos es muy grande y las afectaciones de las transgresiones deben ser enfrentadas por el Estado con las normativas jurídicas acordes a los nuevos tipos penales digitales o crímenes cibernéticos. A continuación, se abordará y profundizara los sujetos que intervienen en los delitos cibernéticos:

Sujeto activo

En los delitos cibernéticos el sujeto activo son aquellas personas que poseen algunas particularidades o características distintas del común de personas es decir que no se enmarcan con el común denominador de los delincuentes ya que los mismos poseen cualidades de experticia en sistemas informáticos además que se encuentra con gran posibilidad de acceder al manejo y manipulación de equipos informáticos ocupando accesos a manejo de información de carácter sensible o a su vez son hábiles al manejar, manipular o ingresar a sistemas informatizados, ya sea por su desenvolvimiento laboral o en muchos de los casos no ejerzan actividades laborales que los relacione directamente con este tipo de delitos.

Sujeto pasivo

Siguiendo con la clasificación de los sujetos que intervienen en el área penal a continuación se abordará al Sujeto Pasivo con enfoque de los delitos cibernéticos para lo cual se iniciará con una definición de sujeto pasivo o víctima del delito, definiendo como tal al sujeto pasivo quien es la víctima del delito, el propietario legítimo del bien jurídico protegido, es decir sobre quien recae la conducta de acción u omisión que realiza el sujeto activo.

En el caso de este tipo de delitos informáticos, las víctimas pueden ser tanto personas naturales o personas jurídicas, instituciones públicas o privadas, Gobiernos Estatales, Provinciales, o Seccionales y todos quienes directa o indirectamente utilicen sistemas informáticos o digitales, que por lo general por necesidades deben conectarse o interconectarse con redes informáticas.

En la configuración de los delitos cibernéticos el papel que juega el sujeto pasivo como en todas las ramas relacionadas a las ciencias penales es de gran relevancia por lo cual en este ha dejado de ser un delito nuevo y convertirse en algo cotidiano y este mecanismo puede determinar las características y componentes de los ilícitos que comenten los delincuentes cibernéticos, que cuyos actos ilícitos en su gran mayoría son revelados por casualidades debido a la complejidad de su modo de operar de los sujetos activos, para lo cual se debe prever el conjunto de estrategias legales y forenses para proteger y precautelas los bienes jurídicos protegidos.

Es por los considerandos expresados anteriormente que para buscar la consecución de la prevención real de la criminalidad cibernética se requiere un análisis objetivo de las diversas necesidades de protección efectiva contra los delitos cibernéticos y sobre todo que las víctimas y potenciales víctimas conozcan los mecanismos, recurso, técnicas y formas de encubrimiento que usan este tipo de delincuencia, con la finalidad de bajar los índices de vulnerabilidad y sobre todo pretender bajar las tasas de impunidad.

Bien jurídico protegido

La manera como se ha venido configurando en la vida del ser humano el uso de la tecnología ha hecho que se produzcan cambios significativos en el comportamiento y actuar de los ciudadanos, dando la configuración de nuevos conceptos y generando la modificación de algunos existentes, y en la gran mayoría fortaleciendo sus concepciones, es así que los nuevos paradigmas que se han replanteado frente a la información en su manejo, almacenamiento y

transmisión de datos, lo cual ha hecho de la comunicación y de quienes tiene la posibilidad de acceder a ella una dinámica social que mueve millones de dólares sin considerar que a la par de aquella se están construyendo imperios de acumulación de poder todo esto enmarcado en el nuevo enfoque que rodea a la información, transformando la manera y forma que tenía su definición tradicional la cual se ha ampliado pretendiendo ser más desarrollada y acorde a la dinámica con la que se genera, como lo expresa la investigadora jurídica Gutiérrez M. Luz, haciendo referencia a la información: "en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico". (Gutiérrez Francés María, 1991).

Es por ello que el analizar este fenómeno investigado y determinar el bien jurídico protegido en los delitos informáticos hace que sea complejo, pero al mismo tiempo apasionante en pro de enmarcar la tipificación de estas nuevas formas delictivas contemporáneas. En la actualidad, la cual se ha catalogado como la era del conocimiento, no resulta suficiente poseer la información, sino a más de eso es necesario tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de ahí que la información deba ser entendida y estudiada como un proceso en el cual se abarque los tres supuestos de la información (almacenamiento, tratamiento y transmisión).

Es por ello que quienes han tenido la posibilidad de comprender estas premisas e invertir en ellas, han solidificado bienes económicos a gran escala, de ahí que por su gran rentabilidad se han convertido en la mayor obsesión de los últimos tiempos, sobre todo de quienes persiguen lucrar u obtener dinero fácil por medio de actividades y acciones ilícitas como es el caso de los delincuentes cibernéticos

Los bienes jurídicos protegidos en el delito cibernético.

Los bienes jurídicos protegidos en los delitos cibernéticos por ser una nueva forma de incriminación penal tienen especificidades propias haciendo parecer una aparente

contradicción con los principios de exclusiva protección de bienes jurídicos del Derecho Penal, entendido como ultima ratio, lo cual debería responder a una racional comprensión del conjunto de respuestas que el Estado considera apropiadas adoptar para hacer frente a conductas causantes de perjuicio social, con el propósito de proteger los intereses y derechos de los ciudadanos como es en el caso de los bienes jurídicos vulnerados en los delitos cibernéticos.

La configuración de los delitos cibernéticos en el ámbito del interés social no implica su acreditación por el simple hecho de ser un bien jurídico penalmente relevante; es de vital importancia para constituirse como tal que reúna los requisitos de merecimiento o importancia social y necesidad de protección tutelar penal y con lo referente a la valoración del merecimiento de protección o importancia social del interés debe tenerse claro que éste se refiere “a la generalidad de los componentes del grupo social y no sólo a la minoría o un sector social determinado; no obstante, la valoración de aquellos intereses que, como la información, tienen un inmanente carácter colectivo, debe abordarse en función a su trascendencia para los individuos, lo que correspondería a los lineamientos propios del modelo de Estado Social y Democrático de Derecho”, (Gutierrez M. , 1991) de esta manera, también lo aborda Mir Puig, señalando que "la valoración de la importancia de un determinado interés colectivo exigirá la comprobación del daño que cause a cada individuo su vulneración", (Puig, 2010)Por lo que para la comprobación del merecimiento no resulta suficiente la protección que el interés social trascienda a la generalidad, va más allá de aquello y precisa que su lesión o puesta en peligro, ostenten identidad para provocar daño recurrente en los individuos integrantes de un grupo social.

Atributos que hoy por hoy los delitos cibernéticos vulneran estos bienes jurídicos que incuestionablemente tienen el merecimiento de protección penal en el interés social denominada “Información”, debido a que este fenómeno informático se encuentra inmerso en todas nuestras sociedades teniendo un interés vital. Cabe indicar que en esta apreciación

doctrinal jurídica la necesidad de tutela penal con relación a la efectividad y eficacia de los demás medios de control social debería calificarse su protección penal cuando los demás instrumentos con los que cuentan las otras ramas del Derecho, hayan fallado en su cometido, pues como lo manifiesta Verdugo, “El Derecho Penal es sólo uno de los tantos instrumentos de control social existentes y posiblemente no sea el más importante de ellos,” Es en esta parte del análisis de los argumentos donde se plantea que la ausencia de protección extra penal, no evidencia por sí sola la falta de protección penal, para lo cual se debe tener en cuenta que al analizar o plantear el legislador la tutela del bien jurídico en los delitos cibernéticos se habría que elevar a la categoría de bien jurídico penal a la “información” dejando sentado que existe la real necesidad de protección punitiva cuando "en el caso concreto no existe ningún otro medio disponible que sea eficaz y menos aflictivo". (2005).

Esta realidad del fracaso de los medios de control social y el daño social propio de este tipo de conductas delictivas hacen más que necesaria la regulación punitiva de comportamientos que afecten el bien jurídico de la información. Dejando sentado las discrepancias con el sector doctrinal que siguen considerando aun que detrás del delito cibernético no existe un bien jurídico específico, y que solo se trata de diversas formas recurrentes de acciones de delitos que transgreden tipos penales ya establecidos confundiendo a los delitos cibernéticos con comunes delitos computacionales ya que estos tratan como lo manifiesta el Jurista Herrera Bravo que no solo se trata de "ilícitos convencionales que ya están regulados en el Código Penal sino de nuevas conductas delictivas que por su singular naturaleza no se subsumen en la descripción típica de los delitos convencionales" (Herrera, 1999). Aseveración que es adoptada y validada en los últimos años donde se acepta con total apertura la existencia de estos nuevos tipos penales que acorde a los cambios y la dinámica social requieren atención inmediata en pro de fortalecer la seguridad de los nuevos bienes protegidos.

3. CAPÍTULO III MARCO METODOLÓGICO

3.1. Método de Investigación

para ejecución de la presente investigación sobre LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021, se encamino considerando las características del fenómeno investigado determinando su condición de proyecto social, su carácter epistemológico se fundamentó en teorías pre establecidas, las mismas que fueron producto del análisis de diversas fuentes formales del Derecho, especialmente en los estudios Socio-jurídicos de Doctrina y jurisprudencia referente a la temática de la Cadena de Custodia en los delitos cibernéticos, como también del estudio de fuentes Constitucionales y del Código Orgánico Integral Penal ecuatoriano.

3.2. Tipo de Investigación

El diseño de la Investigación sobre la cadena de custodia en el proceso judicial de delitos cibernéticos fue Bibliográfico y de Campo.

Investigación Bibliográfico:

Porque me he valido en este diseño para realizar la investigación documental, ya que se realizó a partir del análisis de textos, tratados, Doctrina, jurisprudencia, enciclopedias, revistas, folletos, y también de publicaciones y artículos de internet; para lo cual se aplicó el método analítico- sintético el que me permitió seleccionar y procesar adecuadamente la información obtenida.

Investigación de campo:

En la investigación utilice este diseño porque se realizó un proceso de recolección de información in situ como también en el levantamiento de documentación referente al tema con las instituciones y personal involucrado en la temática abordada ya que se tomó muestras a Jueces, Fiscales, peritos, Abogados en libre ejercicio profesional y ciudadanos, sobre la temática de la cadena de custodia en el proceso judicial en lo referente a delitos informáticos.

Para el tipo de investigación se utilizó el tipo Transversal, y por la configuración del fenómeno investigado se utilizó el Método Descriptivo porque el mismo me permitió tener una observación actual de los hechos jurídicos, sociales y de casos lo cual permitió sustentar la interpretación racional y el análisis detallado de todos los componentes que conforman este fenómeno investigado.

3.3. TÉCNICA DE RECOLECCIÓN DE DATOS

Para la recolección de datos en la presente investigación utilice el instrumento de la encuesta, mediante la cual se logró la consecución de hallazgos producto de la recolección de información cuantitativa. La encuesta que se planteó para esta investigación me permitió consultar criterios, vivencias, argumentos y formas de abordar la problemática referente 61 a los delitos cibernéticos en especial a lo investigado que es sobre la cadena de custodia en el proceso judicial ecuatoriano. Esta encuesta tuvo como población objetivo a Jueces, Fiscales, Policía Judicial, Peritos, Abogados en libre ejercicio profesional de la provincia Bolívar, para lo cual se elaboró un cuestionario cumpliendo parámetros investigativos y metodológicos que garanticen la validez de este instrumento como también de los hallazgos encontrados, por lo que el cuestionario consto de preguntas cerradas y abiertas, que fueron dirigidas estadísticamente a la población investigada.

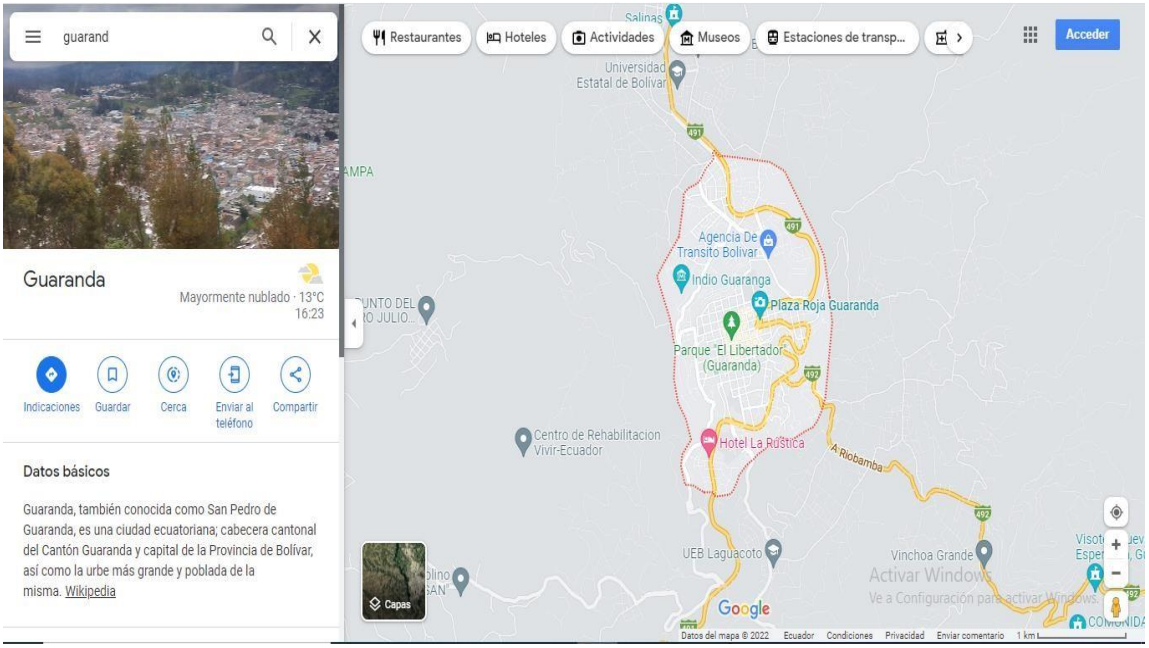
3.4. POBLACIÓN Y MUESTRA

La investigación sobre la cadena de custodia en el proceso judicial de delitos cibernéticos tuvo como población objetivo a Jueces, Fiscales, Peritos, Policía Judicial, Abogados en libre ejercicio profesional de la provincia Bolívar. La misma que se detalla a continuación:

Composición de la población	
Jueces	3
Fiscales	4
Policía judicial	5

Abogados en libre ejercicio	20
Peritos	5
Total	37

Localización geográfica del estudio



Este proyecto de investigación se realizará en el cantón Guaranda, provincia de Bolívar, Ecuador.

4. PROCESAMIENTO Y ANÁLISIS

En la presente investigación el procesamiento y análisis de datos se lo realizo cumpliendo parámetros y normas investigativos los cuales fueron resultado de la aplicación de la encuesta cuya información extraída de la población objetivo se tabuló mediante el programa Microsoft Excel utilizando el tipo de estadística descriptiva.

La escala a la que pertenecen las variables es la escala ordinal y nominal porque me permitió clasificar datos obtenidos de la encuesta.

Los datos obtenidos como resultado de la aplicación del instrumento de la encuesta se procesaron mediante la utilización de cuadros estadísticos calculando de esta manera las frecuencias y los porcentajes de cada una de los datos obtenidos por preguntas.

La tabulación de los datos de la encuesta se realizó por medio de cuadros, gráficos estadísticos y a través de los cuales se dedujo los resultados y hallazgos de la investigación, la tabulación me permitió confirmar la problemática planteada como también comprobar la hipótesis planteada.

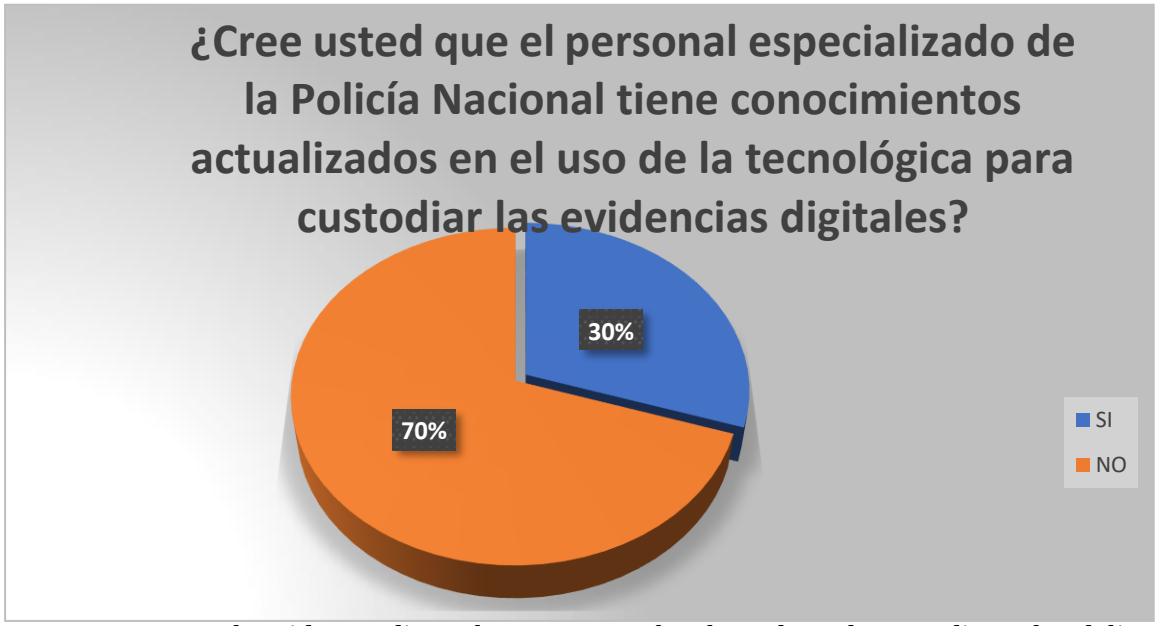
1. **¿Cree usted que el personal especializado de la Policía Nacional tiene conocimientos actualizados en el uso de la tecnológica para custodiar las evidencias digitales?**

Tabla 1 custodia digital

RESPUESTAS	FRECUENCIA	%
SI	11	30%
NO	26	70%
TOTAL	**37**	**100%**

Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Gráfico No. 1 custodia digital



Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Análisis

Por medio de la encuesta realizada a los diferentes conocedores del derecho se ha podido evidenciar que el 70% manifiesta que el personal especializado de la Policía Nacional no tiene conocimientos actualizados en el uso de la tecnológica para custodiar las evidencias digitales, lo que impide el adecuado uso de la justicia.

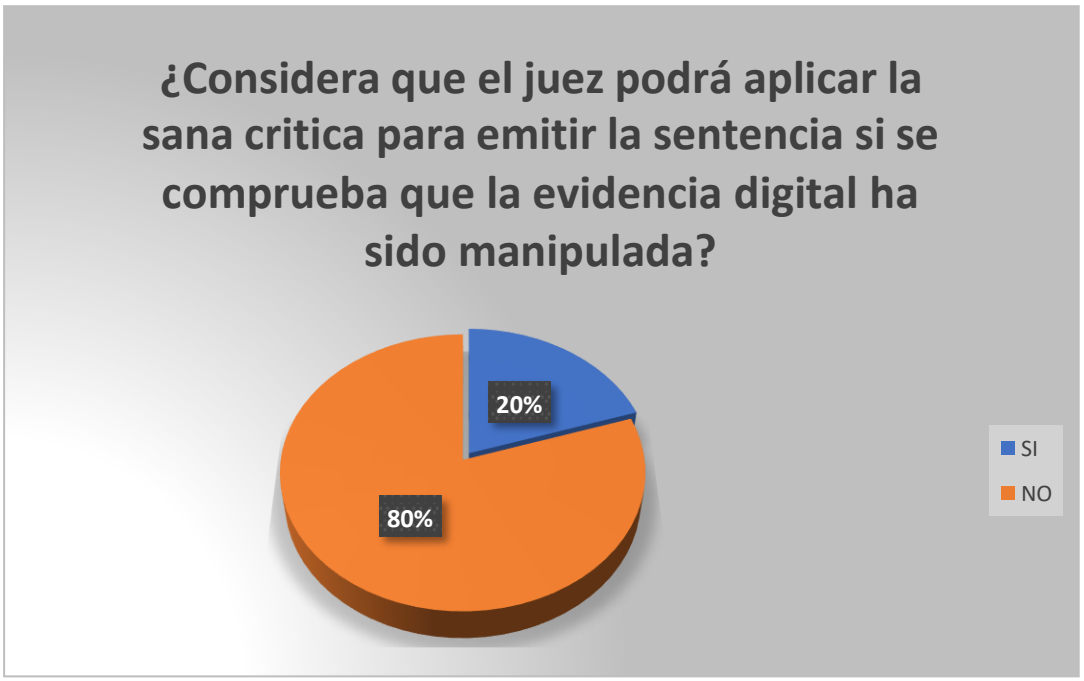
2. **¿Considera que el juez podrá aplicar la sana critica para emitir la sentencia si se comprueba que la evidencia digital ha sido manipulada?**

Tabla 2 Evidencia Digital

RESPUESTAS	FRECUENCIA	%
SI	7	20%
NO	30	80%
TOTAL	**37**	**100%**

Fuente: *Fuente: Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Gráfico No. 2 Evidencia Digital



Fuente: *Fuente: Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Análisis

Por medio de la encuesta realizada a los diferentes conocedores del derecho se ha podido evidenciar que el 80% manifiesta que, no se podría aplicar la sana critica para emitir una sentencia si se verifica que la evidencia digital ha sido manipulada, constituyéndose este factor en elemento determinante del alto grado de errores al momento de determinar la responsabilidad de la persona procesada.

3. ¿Cuál es su grado de conocimiento respecto a las características de las herramientas tecnológicas sobre informática forense?

Tabla 3 Herramientas Tecnológicas

RESPUESTAS	FRECUENCIA	%
Alto	7	19%
Medio	12	32%
Bajo	15	41%
Ninguno	3	8%
TOTAL	**37**	**100%**

Fuente: Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Gráfico No. 3 Herramientas *Tecnológicas*

Fuente: *Fuente: Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Análisis

Por medio de la encuesta realizada a los diferentes conocedores del derecho se ha podido evidenciar que es alarmante el 41% manifiesta que su grado de conocimiento está en un punto bajo y que la necesidad de lineamientos claros que procuren mejorar los conocimientos

respecto al uso de las herramientas tecnológicas sobre informática forense es una realidad tenida muy en cuenta por los involucrados en el trabajo de control y preservación de la evidencia digital.

4. **¿Considera que la manipulación sin protocolos de seguridad de los indicios identificados, deriva en la modificación de la prueba?**

Tabla 4 Modificación de la Prueba

RESPUESTAS	FRECUENCIA	%
SI	23	60%
NO	14	40%
TOTAL	**37**	**100%**

Fuente: Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Gráfico No. 4 Modificación de la Prueba

Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Análisis

Por medio de la encuesta realizada a los diferentes conocedores del derecho se ha podido obtener un 60% mismo que evidencia que la percepción mayoritaria de los encuestados es que la manipulación sin protocolos de seguridad de los indicios identificados, deriva en

la modificación de la prueba provocando una inminente contaminación de la misma y la comparan con la teoría del árbol de la fruta envenenada.

5. **¿Califique usted con qué tipo de conocimiento se procede a manejar la cadena de custodia realizada por los operadores de Justicia?**

Tabla 5 Operadores de justicia

RESPUESTAS	FRECUENCIA	%
Experiencia	10	26%
Conocimientos simples	12	32%
Inexperiencia	16	42%
TOTAL	**38**	**100%**

Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Gráfico No. 5 Operadores de justicia

Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021.*

Análisis

En relación a los conocimientos de los conocedores del derecho en cuanto al proceder del manejo de la cadena de custodia, tomando en cuenta la muestra el 32% concuerda con que se maneja con conocimientos simples, más sin embargo el 42% manifiesta de una inexperiencia en cuanto a conocimiento, pero también existe en 26% que afirma que hay experiencia.

Lo que nos da un indicativo de que la mayor parte de la muestra sostiene los conocimientos sobre el manejo de la cadena de custodia es básico.

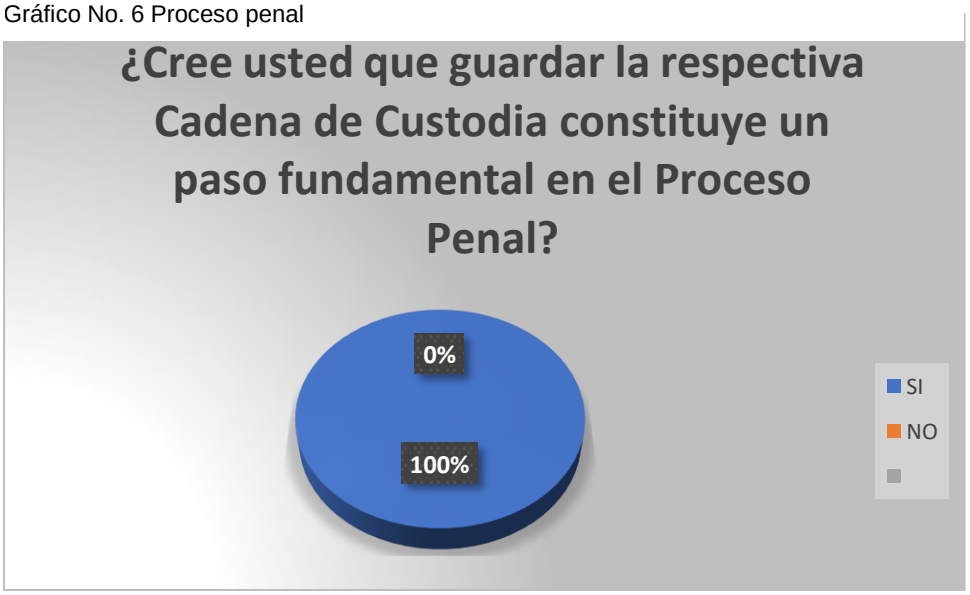
6. ¿Cree usted que guardar la respectiva Cadena de Custodia constituye un paso fundamental en el Proceso Penal?

Tabla 6 proceso penal

RESPUESTAS	FRECUENCIA	%
SI	37	100%
NO	0	0%
TOTAL	**37**	**100%**

Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021*

Gráfico No. 6 Proceso penal



Fuente: *Datos obtenidos mediante la encuesta sobre la cadena de custodia en los delitos informáticos en el año 2021*

ANALISIS

El respectivo proceso que lleva consigo la cadena de custodia en los delitos informáticos, si constituye un pilar fundamental en el proceso, puesto que la inexperiencia y la falta de herramientas necesarias puede causar perjuicio para los sujetos procesales, es por ello que se concluyo que es fundamental en el proceso, por que es prueba fundamental para determinar la infracción.

4.1. Beneficiarios

4.1.1. Beneficiarios Directos.

Los beneficiarios directos del presente proyecto serán las autoridades, docentes y estudiantes de la carrera de Derecho de la Universidad Estatal de Bolívar, quienes tendrán acceso directo al presente proyecto.

4.1.2. Beneficiarios Indirectos.

Los beneficiarios indirectos del presente proyecto serán los profesionales del derecho y estudiantes que podrían tener interés en utilizar los resultados generados con el presente proyecto de investigación, aunque no participen directamente en el desarrollo del mismo.

4.2. Impacto de la investigación

La cadena de custodia aplicada de una manera y correcta dentro de un delito informático sirve como prueba fundamental en el desarrollo del mismo, ya que un manejo inadecuado o descuidado como actualmente se lo lleva puede generar que el sujeto procesal que contaba con la prueba se quede sin poder materializarla y obtener una sentencia desfavorable.

4.3. Transferencia de resultados

Con la investigación realizada mediante las encuestas aplicadas se obtuvo resultados fehacientes y se verificó los sujetos responsables del manejo de evidencias digitales no se encuentran cien por ciento capacitados para este tipo de delitos que ha dejado de ser nuevo para volverse en algo cotidiano en el Ecuador y el resto del mundo.

Los resultados de la investigación realizada serán en primer lugar transferida en la respectiva defensa de grado, consecutivamente con la publicación de este proyecto de investigación en el repositorio digital de la Universidad Estatal de Bolívar, los resultados serán compartidos a la sociedad en general, para que los hallazgos encontrados en esta investigación puedan ser utilizados para nuevas investigaciones.

5. Capítulo V conclusiones y recomendaciones

5.1. CONCLUSIONES

1. La manera cómo la Fiscalía General del Estado en la Unidad Operativa de la provincia Bolívar en la actualidad está manejando la cadena de custodia en lo concerniente a delitos cibernéticos, no es la adecuada debido a que carece de herramientas tecnológicas forenses y mucho menos cuenta con un laboratorio de informática forense.
2. La cultura informática en nuestra sociedad ha jugado un rol desatinado a la hora de enfrentar la vulneración de los bienes jurídicos protegidos en los delitos cibernéticos, debido a que la ciudadanía ecuatoriana aun no se encuentra preparada para asimilar su corresponsabilidad al asumir la utilización de nuevas tecnologías de la información y comunicación, sumado a esto el negligente accionar en el proceso judicial de estos delitos que ha hecho que prime la impunidad.
3. El manejo de custodia sobre contenido digital que presenta en COIP, no es suficientemente claro para, lo que generara un problema en la interpretación y en el análisis de procedimientos que permitieron verificar el estado original de una prueba digital duran el proceso investigativo
4. Los profesionales del derecho descuidan su interacción con las nuevas tecnologías, visto como medios de prueba, esto les crea dificultad para llevar una causa legal en donde intervienen estos medios probatorios, tomando o dejando a este tipo de evidencia en segundo plano.

5.2. RECOMENDACIONES

1. Se recomienda la ejecución de la propuesta del diseño de una Área de Informática Forense, en la Fiscalía General del Estado en la Unidad Operativa de la provincia Bolívar, que cuente con una guía de Cadena de Custodia en delitos cibernéticos lo que permitirá mejorar el proceso judicial penal, dando sostenimiento y apoyo a la justicia ecuatoriana en el esclarecimiento de los delitos cibernéticos.
2. Reformar el artículo 500 del código orgánico integral penal, generando un nuevo inciso que permita aclara los requisitos mínimos para la presentación de un contenido digital.
3. Generan una socialización sobre las técnicas digitales forense a jueces y fiscales que les permita afrontar medios documentales de prueba, generadas por la profundización regulatoria de los contenidos digitales en el artículo 500 del COIP.
4. Capacitar a investigadores, peritos informáticos en el manejo de técnicas digitales forenses para que sus hallazgos sean presentados acorde a lo dispuesto por el COIP.

Bibliografía

Fiscalia General del Estado. (2014). *sistema especializado integral de investigación, de medicina legal y ciencias forenses protocolo del centro de acopio*. Obtenido de https://www.fiscalia.gob.ec/wp-content/uploads/2014/08/files_archivos%20AC_COIP%20073%20FGE_Area%20de%20Cadena%20de%20Custodia_14_Protocolo_del_Centro_de_Acopio.pdf

Acurio, S. (2012). *Libro Derecho y Nuevas Tecnologías.*

Anbar. (1998). *Diccionario Juridico con Legislacion Ecuatoriana* (Vol. IV). Ecuador, Cuenca : fondo de cultura ecuatoriana. Recuperado el 2022

Asamblea Nacional del Ecuador . (2008). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR.* Corporación de Estudios y Publicaciones, .

Avilés, D. A., & Dager Aguilar Avilés . (2010). *El peritaje en el proceso penal* . España: Málaga.

Badilla, J. (1999). *Manual del Curso de administración y procesamiento de la Escena del Crimen.* Cosa Rica: secion de capacitacion.

Cabanellas, G. (1998). *Diccionario Jurídico Elemental* (1 ed., Vol. 1). Eliasta. Recuperado el 20 de 08 de 2022

Cano, J. (2013). *Libro La inseguridad Informática.*

Casey, E. (2011). *Digital Evidence and Computer Crimen.* Elsevier.

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* (A. N. Ecuador, Ed.) Ecuador .

conceptosjuridicos.com. (2 de 06 de 2022). *conceptosjuridicos.com.* Obtenido de Razón Social de una empresa: concepto y ejemplos de razón social.: https://www.scribbr.es/citar/generador/folders/3BRxRuwnslM6tqQjtXxGWV/lists/2LjStjJvwOJQ0nb4jCPn1m/

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

El Comercio. (25 de 07 de 2022). Actualidad. *3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. Obtenido de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Enciclopedia-juridica. (S/F). *Enciclopedia-juridica*. Recuperado el 07 de 10 de 2022, de Enciclopedia-juridica: http://www.enciclopedia-juridica.com/d/empleador/empleador.htm

Enciclopedia-juridica.com. (s/f). *Enciclopedia-juridica.com*. Obtenido de Enciclopedia-juridica.com.: https://www.scribbr.es/citar/generador/folders/3BRxRuwnslM6tqQjtXxGWV/lists/2LjStjJvwOJQ0nb4jCPn1m/

Fundacion Tomas Moro . (2001). *Diccionario Juridico Espasa.* Espasa Calpe.

Gomez, B. (2005). *Derecho Penal de la Democracia vs Seguridad Pública.* España.

Gutierrez, Á. (2015). *Manual de Ciencias Forenses y Criminalistica.* Mexico: Trillas.

Gutierrez, M. (1991). *Fraude Informático y Estafa.* Salamanca.

Herrera, R. (1999). *Derecho Informático.* Chile.

Jurídico, D. (s/f). *Diccionario Jurídico*. Recuperado el 10 de 2022, de Diccionario Jurídico: http://diccionariojuridico.mx/definicion/imprescriptible/

López, M. (2012). *Libro análisis forense digital.*

Moran , M., Ortega , I., Arguello, Y., & Sanchez , V. (2015). *Tipos de Investigacion* . Universidad Nacional Experiental Francisco Miranda.

Puig, S. M. (2010). *Seguridad Pública ante el Derecho Penal.* España.

Reyes, A. (2010). *Cyber Crime Investigations.*

Rombola, N., & Reiboras, L. (2004). *Diccionario de Ciencias Jurídicas y Sociales,* (Vol. I). Buenos Aires , Argentina: Ruy Díaz.

ANEXO

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

Tema: "LA CADENA DE CUSTODIA EN LOS DELITOS INFORMATICOS EN EL AÑO 2021".

El proyecto busca analizar la cadena de custodia en los delitos informáticos en el año 2021, y por medio de esta encuesta obtendremos una información clara para una compresión más precisa sobre este tema.

Objetivo: Recolectar información clara y precisa acerca del manejo o cadena de custodia en los delitos informáticos.

Indicación: Solicitamos su colaboración para el llenado de la siguiente encuesta, marcando con una x la respuesta de su elección, en las preguntas con múltiples opciones pueden ser marcadas más de una opción

1. **¿Cree usted que el personal especializado de la Policía Nacional tiene conocimientos actualizados en el uso de la tecnológica para custodiar las evidencias digitales?**

   SI ☐ **NO** ☐

2. **¿Considera que el juez podrá aplicar la sana critica para emitir la sentencia si se comprueba que la evidencia digital ha sido manipulada?**

   SI ☐ **NO** ☐

3. **¿Cuál es su grado de conocimiento respecto a las características de las herramientas tecnológicas sobre informática forense?**

   ALTO ☐

   MEDIO ☐

   BAJO ☐

   NINGUNO ☐

4. **¿Considera que la manipulación sin protocolos de seguridad de los indicios identificados, deriva en la modificación de la prueba?**

   SI ☐ **NO** ☐

5. **¿Califique usted con qué tipo de conocimiento se procede a manejar la cadena de custodia realizada por los operadores de Justicia?**

   SI ☐ **NO** ☐

6. **¿Cree usted que guardar la respectiva Cadena de Custodia constituye un paso fundamental en el Proceso Penal?**

   SI ☐ **NO** ☐

ANEXOS