UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

"Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos".

Trabajo de Integración Curricular previo a la Obtención del Título de Abogado.

AUTOR:

Wilman Daniel Romero Sánchez

DIRECTOR:

Dr. Guílber René Hurtado Herrera, Mg. Sc.

Loja – Ecuador

2024

Universidad Nacional de Loja

1859

Sistema de Información Académico Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, **Hurtado Herrera Guilber Rene**, director del Trabajo de Integración Curricular denominado **DESAFÍOS LEGALES EN LA PERICIA INFORMÁTICA EN ECUADOR: ANÁLISIS DE LA EFECTIVIDAD DEL INFORME PERICIAL EN CASOS DE DELITOS INFORMÁTICOS**, perteneciente al estudiante **WILMAN DANIEL ROMERO SANCHEZ**, con cédula de identidad N° **0706107588**.

Certifico:

Que luego de haber dirigido el **Trabajo de Integración Curricular**, habiendo realizado una revisión exhaustiva para prevenir y eliminar cualquier forma de plagio, garantizando la debida honestidad académica, se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Integración Curricular**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Integración Curricular del mencionado estudiante.

Loja, 20 de Febrero de 2024

Firmado electrónicamente por: GUILBER RENE HURTADO HERRERA

F) .....

DIRECTOR DE TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Wilman Daniel Romero Sánchez**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del misma. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Integración Curricular, en el Repositorio Digital Institucional- Biblioteca Virtual.

Firma: 

Cédula de identidad: 0706107588

Fecha: 15 de febrero del 2024

Correo electrónico: wilman.romero@unl.edu.ec

Teléfono: 0992253607

Carta de autorización por parte del autor, para la consulta, reproducción parcial o total y/o publicación electrónica del texto completo, del Trabajo de Integración Curricular.

Yo, **Wilman Daniel Romero Sánchez**, declaro ser el autor del Trabajo de Integración Curricular denominado: **"Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos"**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 15 días del mes de febrero de dos mil veinticuatro, firma el autor.

Firma: 

Autora: Wilman Daniel Romero Sánchez

Cédula: 0706107558

Dirección: Calle Manuel Zambrano entre John F. Kennedy y Abraham Lincoln.

Correo electrónico: wilman.romero@unl.edu.ec

Teléfono: 0992253607

DATOS COMPLEMENTARIOS:

Director del Trabajo de Integración Curricular: Dr. Guílber René Hurtado Herrera, Mg. Sc.

Dedicatoria

Quiero dedicar la culminación del presente Trabajo de Integración Curricular y toda mi carrera universitaria, primeramente, a Dios por guiarme y darme el conocimiento para lograr este objetivo muy anhelado de mi formación profesional.

A mi familia quiénes han sido mi fuente constante apoyo, amor y aliento a lo largo de toda mi carrera.

Wilman Daniel Romero Sánchez.

Agradecimiento

Una vez finalizado el presente Trabajo de Integración Curricular, expreso mis más sinceros agradecimientos a la Universidad Nacional de Loja y de manera muy especial a mi director de Trabajo de Integración Curricular Dr. Guílber René Hurtado Herrera, Mg. Sc. Por su dirección en todo el proceso de la realización de esta investigación.

Wilman Daniel Romero Sánchez.

Índice de Contenidos

1. Título

“Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos”.

2. Resumen

El presente trabajo de integración curricular previo a optar el Título de Abogado se titula: “Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos”. La cual propone un análisis jurídico y doctrinario de los informes periciales en delitos informáticos, considerando la acelerada globalización y la creciente incidencia de ciberdelitos en Ecuador. Puesto que, el fenómeno de la ciberdelincuencia se presenta como una consecuencia directa de la globalización, afectando tanto a individuos como a entidades jurídicas. Es por ello que el presente trabajo de integración curricular destaca la necesidad de adaptación a los avances tecnológicos y de comunicación para competir efectivamente en el entorno globalizado actual.

En el contexto de la ciberdelincuencia en Ecuador, se señala un aumento significativo de los delitos informáticos, lo que subraya la necesidad de actualizar las normativas y protocolos legales, especialmente en lo que respecta a los informes periciales. Dado que, aunque la legislación ecuatoriana regula las actividades del perito judicial, existe la preocupación de que las normativas sobre informes periciales estén desactualizadas y carezcan de metodologías internacionales para guiar el proceso de creación de dictámenes periciales informáticos. Asimismo, se destaca la necesidad de aplicar estándares internacionales, como UNE 197010:2015, en la elaboración de informes periciales informáticos para garantizar su calidad y validez.

Durante el desarrollo de este proyecto de integración curricular, se utilizaron una variedad de recursos, tales como: metodologías y técnicas de investigación, los cuales fueron explicados en la propuesta respectiva. Esto incluyó la realización de entrevistas y encuestas dirigidas a profesionales en el ámbito legal. Los objetivos de la investigación incluyen determinar la aplicabilidad del estándar internacional UNE 197010:2015 en informes periciales de delitos informáticos, y demostrar la insuficiencia de la metodología del Consejo de la Judicatura. Finalmente, este Trabajo de Integración Curricular busca contribuir como referencia para futuras investigaciones y proporcionar material de apoyo para profesionales del derecho y partes procesales en casos de ciberdelincuencia.

Palabras clave: ciberdelito, pericia, informática, globalización, normativas.

2.1 Abstract.

Before pursuing a law degree, the student authored the following paper: “Legal Challenges in Computer Expertise in Ecuador: An analysis of the Effectiveness of the Expert Report in Cases of Computer Crimes”. It proposes a legal and doctrinal analysis of expert reports in computer crimes, considering accelerated globalization and the growing incidence of cybercrimes in Ecuador. As a consequence of globalization, cybercrime has become a widespread phenomenon affecting individuals and legal entities alike. Thus, the following work of curriculum integration emphasizes the importance of adapting to technological and communication advances in order to compete effectively in today's globalized world.

As regards cybercrime in Ecuador, there has been a significant increase in computer crimes, which highlights the need for updated legal regulations and protocols, particularly concerning expert reports. Despite Ecuadorian legislation regulating legal experts' activities, there are concerns that the regulations governing expert reports are outdated and lack international methodologies for guiding the creation of computer expert opinions. It also highlights the need to apply international standards, such as UNE 197010:2015, in the preparation of computer expert reports to ensure their quality and validity.

During the development of this curricular integration project, a variety of resources were used, such as: research methodologies and techniques, which were explained in the respective proposal. This included conducting interviews and surveys with legal professionals. The purpose of the research is to determine whether the international standard UNE 197010:2015 can be applied in computer crime expert reports, as well as to demonstrate the inadequacy of the Judiciary Council's methodology. Additionally, this Curricular Integration Work is intended to serve as a reference for future research and as support material for legal professionals and procedural parties involved in cybercrime cases.

Keywords: cybercrime, expertise, computer science, globalization, regulations.

3. Introducción

Dentro del amplio panorama de la globalización, la población cuenta con la facilidad de conectarse con el mundo exterior al presionar simplemente el botón izquierdo del mouse, seleccionar la tecla aceptar o utilizar dispositivos como computadoras, tabletas y teléfonos móviles que deben contar con conexión a internet y tener instaladas aplicaciones o programas. Todo esto con el propósito de recibir resultados en un plazo de tiempo razonable.

No obstante, a pesar de que la tecnología facilita la vida de las personas, también conlleva riesgos de índole informático, especialmente cuando los usuarios no navegan de manera responsable por sitios web o carecen de conocimientos en seguridad informática. En estas circunstancias, pueden convertirse en víctimas o potenciales víctimas para los ciberdelincuentes, quienes pueden cometer delitos tanto en la ciudad de origen como en cualquier parte del mundo. Los ciberdelincuentes aprovechan la falta de políticas estatales relacionadas con la ciberseguridad o la falta de adhesión a tratados transnacionales diseñados para abordar estos delitos.

En el contexto ecuatoriano, la globalización es la vía que permite a las empresas exportar sus productos o servicios, siempre y cuando sus procesos estén alineados con los estándares del país receptor. La única manera internacional de garantizar o certificar la calidad óptima de los trabajos o servicios ofrecidos es si las empresas han seguido las pautas de cumplimiento y regulación de ciertos estándares de calidad internacionales, como son los Estándares de Normalización ISO, por mencionar un ejemplo.

En un mundo donde los ciberdelincuentes son una realidad, es inevitable encontrarse con la perpetración de delitos informáticos. En caso de querer denunciar ser víctima de un ciberdelincuente, la única prueba admisible en un juicio es el informe pericial elaborado por un experto en informática. Este informe, considerado como prueba documental, se utiliza en el proceso legal con el fin de permitir al juez descubrir la verdad de los hechos y tomar una decisión respecto a la existencia o ausencia de violaciones de derechos.

Dada la importancia legal y el impacto social significativo del informe pericial, ya que de él depende la eficacia probatoria de la evidencia examinada y el juez lo toma en cuenta al emitir su sentencia, este estudio destaca la necesidad de contemplar la incorporación de estándares internacionales en la elaboración de informes sobre delitos informáticos. Esto es relevante incluso cuando se realizan actividades previas a la elaboración de estos informes,

como la identificación de la prueba digital, el manejo seguro de la evidencia, la metodología aplicada para su adecuada preservación y la cadena de custodia, a pesar de que estos aspectos no sean el enfoque principal del análisis.

Este trabajo de Integración curricular, titulado: "Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos", se centra en el análisis de la metodología utilizada por los peritos informáticos al elaborar informes periciales en casos de ciberdelitos, siguiendo la normativa ecuatoriana vigente. Asimismo, este trabajo se encuentra estructurado de manera clara en la cual se establece los elementos clave, como el planteamiento del problema visualizado desde varios enfoques, ya sea a nivel, regional nacional y mundial. Además, presenta los objetivos, delimitaciones, justificación y variables del estudio.

Del mismo modo, en cuanto al Marco Teórico, se aborda generalidades, conceptos doctrinarios propiciados por autores clásicos y contemporáneos, y su respectivo análisis encaminado al contexto ecuatoriano, derecho comparado y, proporcionando una comprensión completa. Posteriormente se detalla la metodología empleada, incluyendo enfoque, métodos y técnicas, con un formato de encuestas dirigido a profesionales del derecho cuyos conocimientos son importantes para el desarrollo de la investigación, y las entrevistas realizadas a expertos y en la materia judicial e informática.

Con respecto a la Propuesta, se presenta la justificación de la misma, antecedentes, objetivos y alcance, desarrollando propuestas basadas en respuestas de los expertos entrevistados. Finalmente, se realiza las respectivas conclusiones y recomendaciones, evaluando la necesidad de reformas en el Sistema Pericial Integral de la Función Judicial, en relación con la elaboración de informes periciales en delitos informáticos.

Es importante señalar que este estudio no abarca las actividades preliminares que debe llevar a cabo el perito judicial antes de elaborar el informe pericial. Dichas actividades están relacionadas con el análisis de la prueba digital, abarcando aspectos como su manejo adecuado, cadena de custodia, administración y la ejecución meticulosa de procedimientos. El propósito de estas acciones es redactar de manera organizada y detallada los descubrimientos encontrados en el informe pericial informático, el cual será presentado tanto a las partes en litigio como al juzgador del caso. Este documento, una vez aprobado por el Honorable Tribunal de Grado, estará disponible para los estudiosos del Derecho como fuente de consulta.

4. Marco teórico

4.1. El delito.

El delito, según el Diccionario Panhispánico del Español Jurídico (2017), se caracteriza como una acción típica, antijurídica y culpable, siendo normalmente punible. Esta definición sugiere que un delito es una conducta común, ilícita por infringir normativas legales y que implica culpabilidad en la acción.

Eugenio Raúl Zaffaroni, (1981) en su Manual de Derecho Penal Tomo III, aborda la definición de delito según el código penal argentino. Señala que el código penal no ofrece una definición clara de delito, empleando términos como acto, conducta y hecho de manera imprecisa. La precisión del lenguaje jurídico distingue entre delito stricto sensu y delito lato sensu, abordando en este trabajo solo el primero, que implica una conducta típica, antijurídica y culpable.

José María Márquez destaca dos términos esenciales para comprender el delito: el dolo, referido a la intención de causar daño, y la imprudencia, que no se considera en la culpabilidad. Menciona que, al cometer un delito, la imprudencia no es relevante, subrayando así la culpabilidad en la ejecución de un acto antijurídico (Márquez, 2016). Según el autor, el delito se centra en la finalidad del agresor, destacando la importancia del dolo, ya que, aunque los delitos no siempre se consuman, la intención de cometerlos es importante tomarlos en cuenta desde la intencionalidad. Es decir, para Márquez, el delito no se centra en la injusticia objetiva del hecho, sino en la intención del agresor al cometerlo, resaltando la importancia del dolo.

Es menester hacer mención que, en épocas antiguas, ya se observaban actos de violencia entre individuos o comunidades, lo que llevó a la imposición de sanciones para estos eventos (Fernández, 2017) sostiene que el delito, en sus primeras etapas humanas, se configuraba por ataques a intereses o bienes, siendo inicialmente considerado común. A medida que el tiempo avanzaba, se documentaban los delitos y las posibles sanciones. En estas etapas, la falta de normativas contribuía al aumento de la violencia, destacando la ausencia de la ciencia del derecho penal.

Desde otra perspectiva; (Iglesias, 2017) describe el delito como un proceso que nace, vive y muere, destacando la comisión, existencia durante el proceso legal y la consumación. Las legislaciones de varios países han buscado adelantar la intervención penal mediante estudios previos a la transgresión del bien jurídico protegido, permitiendo sancionar conductas

que, aunque no lesionen dicho bien, representen peligro para la integridad física o la vida humana.

Los delitos, según lo expresado, son conductas prohibidas por la ley y sancionadas por el sistema penal estatal. Pueden ser cometidos por individuos o grupos, causando daño a otras personas, la colectividad o al Estado, infringiendo derechos y justificando la intervención del derecho penal para regular y sancionar. La legislación española, por ejemplo, define delitos como acciones u omisiones dolosas o imprudentes, castigadas por la ley y establece penas, ya sea civiles o penales, según la intencionalidad de la conducta. Mientras que, en la legislación ecuatoriana, el Código Orgánico Integral Penal (2014) utiliza el término "infracción penal" en lugar de "delito", definiéndolo como una “conducta típica, antijurídica y culpable” (Asamblea Nacional , 2023) sancionada por dicho código.

En este contexto, el derecho penal no solo protege derechos, sino que también aborda procedimientos y garantías procesales para asegurar un juicio justo, desempeñando un papel trascendental. Relacionando esto con el derecho informático, más adelante se procederá a abordar los ciberdelitos, delitos cometidos en el ámbito digital, que pueden afectar la integridad y seguridad de las personas y sociedades, exigiendo respuestas normativas y sanciones adecuadas en este entorno tecnológico.

4.1.1 Elementos del delito.

El pensador (Blanco, 2005) destaca que la teoría del delito experimenta una constante evolución científica y constituye la parte esencial del derecho penal, influyendo de manera significativa en la determinación de la acción punible. Subraya que esta teoría se basa en conceptos abstractos, empleados para analizar los elementos inherentes a cualquier delito, independientemente de su naturaleza, y se centra principalmente en el estudio de elementos comunes aplicables a todos los delitos, como la tipicidad, antijuricidad y culpabilidad.

En el contexto de este planteamiento, se puede decir que los delitos son acciones o conductas prohibidas por la ley, sujetas a sanciones conforme al sistema penal de cada Estado. Los delitos pueden ser perpetrados por individuos o grupos, causando daño a otras personas, a la colectividad o al Estado, siendo su factor principal la afectación de un derecho, lo que justifica la intervención del derecho penal para regular y sancionar. Estas acciones intencionales (dolosas) y no intencionales (imprudentes) están prohibidas y son objeto de sanciones, ya sea de índole civil o penal, con posibilidad de privación de la libertad.

4.1.1.1 Acto

El concepto de acto, según (Albán, 2004) constituye el primer elemento esencial del delito, representando la manifestación material y perceptible de la figura jurídica. Para que se configure un delito, resulta crucial establecer la corporeidad del acto, seguido de su correspondiente descripción conforme a la tipicidad establecida por la ley. Luego, se evalúa desde la perspectiva del juicio de valor objetivo, conocido como antijuricidad, y finalmente se examina la culpabilidad, que junto a los demás elementos conforman la estructura del delito.

Con esta definición se puede conceptualizar al acto como la conducta llevada a cabo por una persona que resulta en la comisión de una acción tipificada como delito. Para que este acto sea considerado delictivo, debe cumplir con varios requisitos, entre ellos, la voluntariedad, antijuricidad, culpabilidad y la punibilidad. En este contexto, la voluntariedad implica que la conducta del autor debe ser consciente y deliberada, destacando la importancia de la intencionalidad en la realización del acto delictivo.

4.1.1.1.1 Modalidades del acto

En el ámbito del derecho penal, las modalidades del acto, a saber, la acción y la omisión, desempeñan un papel fundamental al dirigirse hacia la comisión de un delito, donde la conducta del individuo determina si es o no penalmente relevante, poniendo en peligro o generando resultados lesivos.

Según (Albán, 2004) la acción se destaca como la modalidad característica predominante en la mayoría de los delitos, manifestándose a través de los movimientos externos del ser humano y dando lugar a un resultado dañoso premeditado por la intención de llevar a cabo el acto. En términos simples, la acción implica la ejecución de una conducta tipificada por una norma y considerada como delito según la ley penal. Se fundamenta en la realización positiva de un acto por parte del individuo con la intención de cometer el hecho delictivo.

Respecto a la omisión, el mismo autor aborda esta modalidad destacando la falta de voluntariedad para la realización de un delito. En este contexto, se refiere a la omisión como la condición en la cual un individuo no lleva a cabo una acción que estaba legalmente obligado a realizar, y dicha omisión genera un resultado tipificado como delito. En otras palabras, la omisión se produce cuando un individuo incumple con la realización de una acción que estaba

legalmente prescrita, dando lugar a un resultado que está normativamente considerado como delito.

4.1.1.2 La Tipicidad

Según la definición proporcionada por el experto (Navas, 2003), la tipicidad se refiere a la adecuación de una conducta a un tipo penal. En términos sencillos, implica que la conducta de un individuo debe ajustarse a lo que la ley establece como un delito. Es decir, para que una acción sea considerada como delito, debe estar claramente descrita y definida como tal en la ley, y la conducta del autor debe coincidir con lo que la ley establece como un comportamiento típico.

En este sentido, la tipicidad se convierte en un elemento esencial del delito, ya que garantiza que la conducta que se está juzgando y, eventualmente, sancionando, esté previamente establecida en la ley como delictiva. Asegura que la acción del autor se ajuste a lo que la ley considera como un comportamiento típico. En ausencia de tipicidad, una conducta no puede ser reconocida como delito y, por lo tanto, no puede ser objeto de sanciones penales.

4.1.1.2.1 Elementos que conforma la tipicidad:

Núcleo

Dentro de los elementos que constituyen la tipicidad, es esencial destacar el núcleo, según lo expresado por (González, 2018). Este autor describe el núcleo como la acción que se precisa mediante modalidades desarrolladas en diversas formas, con el fin de ofrecer una descripción clara del acto cometido. En términos sencillos, el núcleo detalla la conducta que está prohibida en el ámbito penal, siendo el componente central que describe la acción realizada.

Es fundamental destacar que la descripción del núcleo del tipo penal debe ser lo suficientemente clara y precisa para que las personas puedan entender qué está prohibido y así evitar sanciones injustas. En este contexto, el núcleo se considera como el verbo principal, indicando la acción fundamental que se llevará a cabo. Por ejemplo, en el delito de sicariato, el núcleo sería "matar a otra persona", reflejando la acción que se ejecutará y que tendrá como objetivo o beneficio un rédito económico para la persona principal que lo realiza o para terceras personas.

Sujeto Activo:

Según (Laffite, 1989) el sujeto activo es el perpetrador del delito, es decir, la persona que lleva a cabo la conducta prohibida por la ley. En algunas circunstancias, la legislación penal establece que solo ciertas personas pueden ser consideradas sujetos activos; por ejemplo, en el delito de cohecho, solo un funcionario público puede ser configurado como sujeto activo, mientras que, en el homicidio, cualquier persona puede ser catalogada como tal. La identificación del sujeto activo es crucial para imputar la responsabilidad penal por la conducta prohibida.

En el contexto de los delitos cibernéticos, el sujeto activo se refiere al individuo o entidad que lleva a cabo acciones delictivas en el ámbito digital. Por ejemplo, un hacker que realiza un ataque informático para acceder ilegalmente a datos confidenciales podría considerarse un sujeto activo en el ámbito de los delitos cibernéticos. En este caso, la legislación penal relacionada con la ciberseguridad podría establecer restricciones específicas y considerar solo a ciertas personas como sujetos activos, como aquellos que realizan actividades ilegales en línea.

Sujeto Pasivo:

Siguiendo las palabras de (Cruz, 2020), el sujeto pasivo se refiere al titular del bien jurídico protegido, es decir, la persona o entidad que sufre las consecuencias de la conducta delictiva, siendo la víctima del delito. Este elemento esencial en la tipicidad del delito implica que el tipo penal no solo debe describir la conducta prohibida, sino también a quién se le prohíbe dicha conducta y sobre quién recae la acción cometida por el sujeto activo o actor. Es crucial tener en cuenta que el sujeto pasivo no siempre es un individuo, ya que, en ciertos casos, las personas jurídicas pueden ser víctimas de acciones delictivas, dependiendo del tipo penal y la conducta prohibida.

Con respecto al sujeto pasivo en delitos cibernéticos, este sería el titular del bien jurídico protegido en el ámbito digital. Podría ser un individuo, una empresa o una entidad que sufre las consecuencias de un ataque cibernético. Por ejemplo, en el caso de un ataque de ransomware o (secuestro de datos), la entidad cuyo sistema informático es secuestrado y sus datos son cifrados sería el sujeto pasivo. También, en el ámbito de los delitos cibernéticos, las personas jurídicas, como empresas o instituciones, pueden ser víctimas, dependiendo del tipo de delito

y la conducta prohibida, como la violación de la privacidad en línea o el robo de propiedad intelectual.

Tiempo, Lugar y Espacio

En el contexto de los delitos cibernéticos, las circunstancias de tiempo, lugar y espacio adquieren una dimensión digital. (Vega, 2016) destaca la importancia de ubicar geográficamente la conducta penal realizada por un individuo en el ámbito digital. En el ciberespacio, las descripciones de cómo, cuándo y dónde se originó el delito son cruciales para establecer la tipicidad. Evaluar el entorno físico en el mundo digital, como la red o plataforma utilizada, se vuelve esencial para atribuir la responsabilidad y determinar la gravedad del delito.

Objeto Material:

Vega, (2016) también menciona el objeto material en la comisión de delitos, y en el ámbito cibernético, este se relaciona con el bien jurídico transgredido. En el caso de los delitos cibernéticos, el objeto material puede ser tanto una persona (el sujeto pasivo) como datos, sistemas informáticos o incluso redes completas. La transgresión de bienes jurídicos en el entorno digital puede tener un impacto directo en la privacidad, la propiedad intelectual o la integridad de la información.

4.1.1.2 La Antijuricidad:

Con respecto a los ciberdelitos, (Welzel, 2004) destaca la antijuricidad como la oposición de la ejecución del tipo de una norma vetada con el ordenamiento jurídico en su totalidad. En el contexto digital, esto implica que una conducta será considerada antijurídica si va en contra de las normas o leyes que rigen la ciberseguridad y el uso responsable de la tecnología.

Antijuricidad y Causas de Justificación:

La antijuricidad no siempre conlleva la ilegalidad de una conducta en el ámbito cibernético. (Silva Sánchez, 1987) sugiere que, aunque una acción pueda considerarse antijurídica, la presencia de causas de justificación o eximentes de responsabilidad penal puede alterar esta evaluación. En delitos cibernéticos, esto podría aplicarse, por ejemplo, si la acción se realizó con el consentimiento del propietario del sistema informático o si existen circunstancias que justifican la intrusión.

Enfoque Legal en la Legislación Ecuatoriana:

En la legislación ecuatoriana, específicamente en el COIP (Código Orgánico Integral Penal), el artículo 29 establece que “una acción será considerada antijurídica si amenaza o

lesiona un bien jurídico protegido sin justificación" (Asamblea Nacional , 2023). Este enfoque legal enfatiza la importancia de evaluar la conducta en términos de su impacto en los bienes jurídicos relevantes, un aspecto crucial en delitos cibernéticos donde la protección de la información y la privacidad es esencial.

4.1.1.2 La Culpabilidad:

(Zambrano, 2019) establece que la culpabilidad se manifiesta como el juicio de reproche dirigido al responsable de un acto típicamente antijurídico, es decir, un delito. Este juicio se desglosa en dos momentos valorativos: el primero evalúa el acto como violatorio de una norma jurídica y, por ende, antijurídico; el segundo, denominado juicio de reprochabilidad, señala al autor del acto como responsable por no haber evitado la acción, a pesar de tener la capacidad de hacerlo según la norma.

En el ámbito de los delitos cibernéticos, la culpabilidad implica que el autor debe tener la capacidad de comprender la ilicitud de su conducta y la intención o conocimiento de llevarla a cabo. La evaluación subjetiva de la culpabilidad se centra en determinar si el autor era consciente de la antijuridicidad de sus acciones y si podría haber actuado de manera diferente.

Causas de Inimputabilidad:

Dentro de las causas de inimputabilidad que (Albán, 2004) destaca, como la minoría de edad, perturbación mental, trastorno mental, sordomudez, embriaguez, toxicomanía y drogadicción, es esencial considerar su aplicabilidad en el entorno digital. Por ejemplo, la embriaguez puede manifestarse en delitos cibernéticos relacionados con el acceso no autorizado a sistemas informáticos bajo la influencia de sustancias.

El Código Orgánico Integral Penal, en su artículo 34 enfatiza que, para considerar a alguien culpable, debe ser imputable y tener conocimiento de la naturaleza ilícita de sus acciones (Asamblea Nacional , 2023). Esto se conecta directamente con el segundo elemento de la teoría del delito, la antijuricidad, indicando que el autor, al cometer el acto, está consciente de que está prohibido.

4.1.2 Tipos de delitos.

La clasificación de los delitos en el Derecho Penal de nuestro país se fundamenta en diversos criterios relevantes, Asimismo, existen muchas y variadas clasificaciones, no obstante, se

explicará tomando en cuenta nuestro Código Orgánico Integral Penal; se detalla la clasificación según algunos de estos criterios:

1. **Por la forma de acción:**

- **Omisión:** Implica que la persona activa no permite que se realice la conducta prohibida u ordenada por la ley.
- **Comisión:** La persona es directamente responsable de llevar a cabo el delito. Por ejemplo, en casos de robo, homicidio o lesiones, donde el individuo ejecuta la acción delictiva de manera directa.
- **Omisión propia:** Puede ser cometida por cualquier persona, ya que se refiere a actos que la ley exige a la sociedad en general. Un ejemplo es no detenerse para auxiliar a las víctimas de un accidente de tráfico.
- **Omisión impropia:** Solo puede ser realizada por personas que actúan como garantes en relación con las víctimas, como cuando los padres no pagan las pensiones alimenticias a sus hijos.

2. **Por calidad del sujeto:**

- **Propios o comunes:** Delitos que, según la ley, pueden ser cometidos por cualquier persona.
- **Impropios o especiales:** Delitos expresamente designados por la ley, indicando que solo ciertas personas pueden llevarlos a cabo. Ejemplos incluyen los delitos de malversación o prevaricación.

3. **Según los sujetos intervinientes:**

- **Cooperador:** Aquel que brinda al autor del delito una ayuda indispensable.
- **Inductor:** Quien incita a cometer un delito.
- **Autoría:** Aquellos que realizan por sí mismos el hecho delictivo.

4. **Por la forma procesal:**

- **Públicos:** Delitos que cualquier persona puede denunciar, como asesinato o hurto.
- **Semipúblicos:** La denuncia solo puede ser presentada por el agraviado, el ministerio fiscal o el representante legal. Ejemplos incluyen delitos de acoso o revelación de secretos.
- **Privados:** Solo pueden ser denunciados por el perjudicado o su representante legal, como delitos por injurias y calumnias.

5. **Por la forma de ejecución:**

- **Instantáneos:** El delito se consuma en el momento de la acción, como en el robo o homicidio.
- **Permanentes:** El delito se consuma con la acción, pero continúa desarrollándose después, como en el caso del secuestro.
- **Continuados:** Se comete una serie de delitos de manera continua hasta consumar el delito final, como suministrar veneno gradualmente.
- **Conexos:** Los delitos se llevan a cabo en tiempos y lugares diversos, pero con un objetivo común, como romper una ventana y luego robar algo de la casa.
- **Flagrantes:** Los delitos se cometen públicamente, como ladrones descubiertos rompiendo una ventana.

6. **Según el bien afectado:**

- **Simple:** El delito afecta solo un aspecto legal, como en el caso del homicidio.
- **Complejo:** Implica afectar múltiples aspectos legales, como violar y luego cometer homicidio.

7. **Según la culpabilidad:**

- **Doloso:** Cometido con plena conciencia de causar daño.
- **Imprudente:** Se comete sin intención de causar daño.
- **Preterintencional:** Se inicia con intención de cometer el delito, pero los daños resultan ser mayores.

8. **Por el daño causado:**

- **De lesión:** Requiere una lesión específica.
- **De peligro:** No necesita una lesión; basta con que haya riesgo, como en la conducción temeraria.

9. **Por el resultado:**

- **Formales:** Sancionados por el comportamiento, como el falso testimonio.
- **Materiales:** Exigen un resultado concreto, como en los delitos de lesiones.

10. **Por gravedad:**

- **Leves:** Castigados con penas más suaves, como amenazas o hurtos.
- **Graves:** Infracciones con penas más severas, como asesinato, tráfico de drogas o secuestro.
- **Menos graves:** Delitos con penas menos severas, como dañar bienes públicos. (Mora, Pérez, & Rodríguez, 2014)

Esta clasificación de los delitos según distintos criterios en el marco del Derecho Penal, especialmente basándose en el Código Orgánico Integral Penal, pretende explicar la complejidad y diversidad de situaciones que el ámbito legal debe abordar para comprender y juzgar las conductas delictivas.

La primera clasificación según la forma de acción destaca entre la omisión y la comisión, proporcionando ejemplos claros, como el robo o las lesiones, para ilustrar la responsabilidad directa del individuo en la ejecución del delito. Además, se diferencian las omisiones propia e impropia, agregando una capa de complejidad al considerar el deber legal de la sociedad y los casos donde ciertas personas actúan como garantes. La clasificación por calidad del sujeto distingue entre delitos propios o comunes y delitos impropios o especiales, agregando una dimensión adicional a quiénes pueden ser responsables de ciertos actos ilícitos. La introducción de los sujetos intervinientes, como el cooperador, inductor y autoría, añade matices a la participación de individuos en la comisión del delito.

Del mismo modo, La segmentación por la forma procesal, que diferencia entre delitos públicos, semipúblicos y privados, refleja la complejidad del proceso legal y cómo diferentes actores pueden desencadenar denuncias. La clasificación por la forma de ejecución proporciona una visión sobre el desarrollo temporal y la naturaleza de los delitos, incluyendo situaciones instantáneas, permanentes, continuadas, conexas y flagrantes. Además, se consideran otras clasificaciones, como aquellas relacionadas con el bien afectado, la culpabilidad, el daño causado, el resultado y la gravedad del delito, ofreciendo una comprensión integral de las diversas facetas que pueden surgir en el ámbito legal.

Con respecto a los ciberdelitos, también conocidos como delitos informáticos o ciberataques, encuentran su clasificación dentro de diversas categorías legales. Estos engloban desde estafas en línea y fraudes con tarjetas de crédito, considerados delitos contra la propiedad y el patrimonio, hasta acciones como acceso no autorizado y difusión de malware, que se catalogan como delitos contra la seguridad informática. La violación de datos y el acoso en línea se incluyen en la categoría de delitos contra la privacidad y la integridad de la información, mientras que la piratería de software y la violación de derechos de autor en línea entran en la clasificación de delitos contra la propiedad intelectual.

Además, actividades como el ciberterrorismo, que amenaza la seguridad nacional, son consideradas delitos contra el orden público. Por último, los ciberdelitos también pueden abordar aspectos relacionados con la libertad sexual, como el ciberacoso sexual. La

clasificación específica de estos delitos responde a la necesidad de adaptar la legislación a la rápida evolución tecnológica y abordar eficazmente los desafíos únicos que presentan en términos de investigación y enjuiciamiento. A continuación, se detallará más sobre los delitos informáticos.

4.2 Delitos informáticos

Definir la naturaleza de los delitos informáticos puede ser complicado, pero en líneas generales se refieren a acciones intencionales que causan daño a personas o entidades utilizando dispositivos típicamente relacionados con la informática, como lo señalan (Mata & Martín, 2003) Incorporando conceptos sugeridos por (Mora, Pérez, & Rodríguez, 2014) surgen cuatro posturas doctrinarias que abordan esta problemática.

La primera postura considera el uso de la informática como medio y fin del delito, mientras que la segunda centra la protección en la información o datos procesados. La tercera postura cuestiona la existencia de un nuevo tipo de delito, mientras que la cuarta, una teoría ecléctica, abarca cualquier conducta ilícita sancionada por el ordenamiento jurídico que involucre el uso indebido de computadoras como instrumento. Estos actos ilícitos, que involucran el uso del ordenador, en esencia son similares a los delitos tradicionales, como los perpetrados a lo largo de la historia contra la persona, el honor, la seguridad pública y el patrimonio nacional. Además, algunos los denominan cibercrimen o ciberdelito.

Según (Posada, 2017), esto abarca cualquier comportamiento que afecte la seguridad de los sistemas informáticos, incluso poniendo en riesgo otros bienes legales. Estos delitos difieren de los comunes debido a su complejidad técnica, su capacidad de dañar bienes intangibles y su ubicuidad en el ciberespacio.

Los delitos informáticos se vinculan con acciones ilícitas establecidas por la ley, siendo definidos como "actos ilícitos realizados a través del uso inadecuado de la tecnología, que afectan la privacidad de la información de terceros al dañar o extraer datos almacenados en servidores o dispositivos electrónicos" (Acosta, Benavides, & García, 2020). En este contexto, los delitos informáticos abarcan diversas conductas ilegales sancionadas legalmente, independientemente del ejercicio de la acción penal.

Sin embargo, se caracterizan por la necesidad de utilizar dispositivos tecnológicos como medio para perpetrar el delito, con el objetivo de afectar cualquier bien jurídico protegido por las normativas legales estatales. Este enfoque destaca la conexión intrínseca entre las acciones

delictivas y la tecnología, subrayando cómo la comisión de estos actos ilícitos depende crucialmente del uso indebido de herramientas tecnológicas, lo que refuerza la importancia de la regulación y legislación en este ámbito emergente (Acosta, Benavides, & García, 2020)

Estos autores destacan la evolución de los delitos informáticos en el entorno digital actual, subrayando su definición como actos ilícitos perpetrados a través de la tecnología para comprometer la privacidad y la seguridad de los individuos. Además, resaltan la necesidad de una legislación actualizada que comprenda la complejidad de estos delitos, los cuales requieren una comprensión profunda de los avances tecnológicos y un enfoque innovador para su prevención y combate, evidenciando así la intersección entre la tecnología y la ley en la lucha contra el crimen cibernético.

El delito informático se define como cualquier acción punible que involucre el uso de dispositivos informáticos, ya sea que se realice directamente a través de una computadora o que afecte el funcionamiento de sistemas informáticos en general (Suárez Sánchez, 2016). Este concepto abarca tanto las conductas perpetradas mediante computadoras como aquellas cuyo objetivo esté relacionado con la tecnología informática. Para que un delito informático se concrete, el perpetrador debe emplear programas o equipos informáticos, ya sea de forma directa o indirecta, como se menciona en la normativa legal del país.

En Ecuador, la legislación penal ha ido evolucionando para abordar estos delitos, reconociendo la importancia de proteger la seguridad y la integridad de la información en el ámbito digital. Por lo tanto, la materialización de un delito informático en el país implica que el perpetrador utilice programas o equipos informáticos de manera directa o indirecta, con el objetivo de cometer acciones ilícitas tipificadas como antijurídicas dentro del marco normativo nacional.

4.2.1 Tipos de delitos informáticos

Los delitos informáticos han surgido en un contexto donde los sistemas legales no estaban preparados para enfrentarlos, pero en años recientes se han establecido leyes y normativas para controlar y perseguir estas acciones. A pesar de los esfuerzos legales, a veces resulta difícil identificar a los responsables de estos actos delictivos, aunque la existencia de leyes proporciona cierta protección a las víctimas (García, 2018).

Este autor destaca la evolución de los delitos informáticos en un contexto inicialmente desafiante para los sistemas legales, pero resalta el progreso mediante la implementación de leyes y normativas específicas. Se puede decir que, aunque estas medidas ofrecen cierta

protección a las víctimas, persiste la dificultad para identificar a los responsables debido a la naturaleza anónima y global de muchos ataques, así como a las habilidades técnicas avanzadas de los perpetradores.

Asimismo, se puede destacar que, estos delitos no son estáticos; cambian y se adaptan a medida que evolucionan las circunstancias y surgen nuevas tecnologías. Cada año surgen nuevos tipos de ciberdelitos y se desarrollan métodos innovadores para cometer los ya existentes. Entre los más comunes se encuentran las estafas, que han aumentado con el uso de las Tecnologías de la Información y la Comunicación (TIC), donde es común recibir mensajes sospechosos con el fin de engañar a las personas (Martínez, 2017). El jurista en mención destaca el constante surgimiento de nuevos tipos de ciberdelitos y el desarrollo de métodos innovadores para cometer los ya existentes. Resaltando especialmente el aumento de las estafas, facilitadas por el uso de Tecnologías de la Información y la Comunicación (TIC), donde los individuos pueden ser engañados a través de mensajes sospechosos.

El robo de datos es otro delito informático común, especialmente preocupante para instituciones gubernamentales y empresas, ya que existen programas diseñados para acceder a información confidencial (Sánchez, 2019). Además, las amenazas en línea, tanto por parte de desconocidos como de personas conocidas, son una extensión de los delitos tradicionales y representan un riesgo significativo en el entorno digital (Pérez, 2020). El robo de datos es especialmente preocupante para instituciones gubernamentales y empresas, dado que existen programas diseñados para acceder a información confidencial, lo que subraya la importancia de fortalecer las medidas de seguridad cibernética. Por otro lado, las amenazas en línea, provenientes tanto de desconocidos como de personas conocidas, representan una extensión de los delitos tradicionales y plantean un riesgo significativo en el entorno digital, evidenciando la necesidad de una mayor conciencia y precaución al interactuar en línea.

Los delitos informáticos engloban una serie de acciones ilegales perpetradas a través de las tecnologías de la información y la comunicación (TIC). A parte de los mencionados anteriormente se puede destacar algunos de los más preocupantes hoy en día, estos son:

4.2.1.1 Abuso a menores y pornografía infantil:

Las TIC se han convertido en el medio principal para difundir contenidos de abuso a menores y pornografía infantil, facilitando la acción de mafias y redes dedicadas a estos delitos. Las autoridades policiales han establecido unidades especializadas para perseguir y eliminar este tipo de contenido de la red (Iglesias, 2017).

Sabotajes informáticos:

Los sabotajes informáticos, dirigidos principalmente contra administraciones públicas en España, buscan interrumpir la actividad de empresas o instituciones con el fin de causar perjuicios económicos o productivos. La identificación de los perpetradores suele ser difícil en la mayoría de los casos (Pérez, 2020).

Ataques a la intimidad:

Estos ataques ocurren al extraer información íntima de dispositivos o al difundir datos privados de personas sin su consentimiento. Son especialmente frecuentes entre la población joven, que muchas veces no comprende las consecuencias de compartir ciertos contenidos (Pérez, 2020).

Phishing y carding:

El phishing consiste en obtener información bancaria mediante engaños, a menudo haciéndose pasar por entidades bancarias legítimas. Por otro lado, el carding implica la duplicación u obtención de datos de tarjetas bancarias para acceder fraudulentamente a fondos (Pérez, 2020).

Fraude de identidad en línea:

Los delincuentes aprovechan Internet para robar la identidad de sus víctimas y llevar a cabo acciones como la firma de créditos o la compra de productos en línea utilizando información personal ajena (Pérez, 2020).

Extorsión:

Grandes empresas y organismos públicos pueden ser blanco de extorsión por parte de ciberdelincuentes, quienes exigen un beneficio a cambio de no atacar sus sistemas informáticos o divulgar información confidencial (Pérez, 2020).

En el contexto ecuatoriano, la ciberdelincuencia representa una preocupación creciente debido al aumento de la dependencia de la tecnología y la conectividad digital en todos los aspectos de la vida cotidiana. Si bien Ecuador ha tomado medidas para abordar estos desafíos, como la creación de unidades especializadas dentro de las fuerzas de seguridad, aún enfrenta obstáculos significativos en la lucha contra estos delitos. La falta de conciencia pública sobre las amenazas cibernéticas y la necesidad de una educación más amplia sobre seguridad digital son áreas que requieren atención urgente. Además, la cooperación internacional y la adopción de medidas de seguridad cibernética más sólidas son cruciales para proteger los datos y la privacidad de los ciudadanos ecuatorianos en un entorno digital cada vez más complejo y peligroso.

4.2.2 Clasificación de delitos informáticos

La Policía Nacional Española ha clasificado diferentes tipos de delitos que pueden ocurrir en el ámbito digital, reflejando así la gravedad de las amenazas en línea. Estos delitos abarcan una amplia gama de acciones, desde la violación de la privacidad y la propiedad intelectual hasta el sabotaje informático, la estafa en línea, las amenazas y la difamación, así como la explotación infantil a través de la pornografía.

Es importante destacar que estos delitos tienen repercusiones significativas tanto a nivel individual como societal. Por ejemplo, la divulgación de información privada puede causar daños emocionales a las personas afectadas, además de socavar la confianza en la seguridad de la información en línea (Martínez, 2017). Por otro lado, la violación de los derechos de autor y la propiedad intelectual no solo perjudica a los creadores y propietarios legítimos, sino que también puede tener un impacto negativo en la innovación y el desarrollo económico. Los sabotajes informáticos pueden interrumpir servicios vitales y causar pérdidas económicas significativas para empresas e instituciones. Asimismo, las estafas en línea pueden afectar la confianza del público en el comercio electrónico y las transacciones en línea, lo que tiene consecuencias en la economía digital.

Además, las amenazas, la difamación y la distribución de pornografía infantil representan un grave problema social, ya que contribuyen a crear un entorno en línea tóxico y perjudicial para la sociedad en su conjunto. Estas actividades pueden causar un gran daño emocional y psicológico a las víctimas, especialmente a los niños y a las personas vulnerables.

La Organización de las Naciones Unidas (ONU) ha identificado y clasificado varios tipos de delitos informáticos que abarcan una amplia gama de actividades ilícitas en el ámbito digital.

1. **Fraudes cometidos mediante manipulación de computadoras:** En esta categoría se incluyen diversas acciones, como la manipulación de datos de entrada, la modificación de programas informáticos y la manipulación de datos de salida. Según lo indicado por la (ONU, 2012), este tipo de fraude puede manifestarse de varias maneras, como la extracción de datos, la inserción de nuevos programas o la alteración de la información de salida, como en el caso de los cajeros automáticos.
2. **Manipulación de datos de entrada:** Este tipo de delito puede tener dos objetivos: alterar directamente los datos de una información computarizada o utilizar las computadoras como medio para la falsificación de documentos. (Martínez, 2017)

3. **Daños o modificaciones de programas o datos computarizados:** Aquí se incluyen actividades como el sabotaje informático, donde se elimina o modifica sin autorización funciones o datos de una computadora para obstaculizar su funcionamiento. Además, se menciona el acceso no autorizado a servicios y sistemas informáticos, que puede tener motivaciones diversas como la curiosidad, el espionaje o el sabotaje (Posada, 2017)

La Asamblea Nacional del Ecuador plantea que los delitos informáticos no son realmente nuevos; más bien, lo que diferencia al ciberdelincuente del delincuente tradicional es que el primero utiliza medios digitales para cometer sus actos punibles. Esto se traduce en la materialización de los delitos informáticos a través de medios digitales.

En cuanto a la clasificación de estos delitos, se destaca el fraude digital, el cual se divide en tres categorías, una de las cuales es la estafa. Esta se define como el acto de engañar a otra persona con el propósito de obtener un beneficio económico, ya sea simulando hechos falsos, deformando la verdad u ocultando información veraz. Se establece que quien cometa este tipo de estafa podría enfrentar una pena privativa de libertad de cinco a siete años. Además, se especifica que la pena máxima se aplicará a aquellos que cometan fraude utilizando tarjetas de crédito, débito u otros dispositivos electrónicos de manera ilegal, como la alteración, clonación o duplicación sin consentimiento del propietario legítimo (Asamblea Nacional , 2023).

4.2.3 Delitos de naturaleza informática

Los delitos de naturaleza informática abarcan acciones realizadas con el uso de medios tecnológicos que vulneran la intimidad de otra persona o que implican la suplantación de identidad, tal como se estipula en los artículos 178 y 212 del Código Orgánico Integral Penal (Asamblea Nacional , 2023). Este tipo de delitos se encuentran subdivididos en tres categorías según la legislación vigente.

La primera subdivisión, identificada en los artículos 229 al 234.1 del COIP, se enfoca en los "Delitos contra la seguridad de los activos de los sistemas de información y comunicación" según la clasificación propuesta por el asambleísta en el año 2014. Estos delitos están relacionados con acciones que amenazan la integridad y seguridad de los sistemas de información y comunicación, como el acceso no autorizado a datos sensibles o la interrupción del funcionamiento normal de los sistemas informáticos.

La segunda subdivisión, establecida en los artículos 173 y 174 del COIP, aborda las conductas contrarias a la integridad reproductiva y sexual, denominadas como "Delitos contra la integridad sexual y reproductiva" por el legislador. Estos delitos incluyen acciones como el acoso sexual en línea, el grooming y otros actos que atentan contra la integridad sexual y reproductiva de las personas en el entorno digital.

Finalmente, la tercera subdivisión, contemplada en el artículo 103 del COIP, se refiere a una forma específica de explotación humana relacionada con la pornografía infantil, identificada como "Pornografía con utilización de niñas, niños o adolescentes" en la ley. Esta categoría penaliza la producción, distribución y posesión de material pornográfico que involucre a menores de edad, y busca proteger a los niños y adolescentes de la explotación sexual en línea.

4.3. Delincuencia

La comprensión de la delincuencia es un desafío considerable debido a su naturaleza multifacética, que se manifiesta en diversos contextos sociales como una respuesta al rechazo o la insatisfacción, reflejando una descomposición social que requiere medidas correctivas para restaurar la estabilidad jurídica de los individuos afectados (Ortiz, 2020). Este fenómeno, conocido como delincuencia, constituye un comportamiento desviado que viola las normas establecidas por la sociedad (Castell & Carballo, 1999). Se presenta en diferentes formas, desde una simple inadaptación social hasta conductas que contravienen abiertamente la ley.

Estos autores analizan a la delincuencia como un fenómeno multifacético, enraizado en diversos contextos sociales y motivado por el rechazo o la insatisfacción. Reconociendo a la delincuencia como un reflejo de la descomposición social, subrayando la necesidad de medidas correctivas para restaurar la estabilidad jurídica y social. Es decir, definen a la delincuencia como un comportamiento desviado que viola las normas sociales establecidas, manifestándose en una variedad de formas, desde la inadaptación social hasta la transgresión de la ley. Enfatizando la importancia de comprender la delincuencia en su diversidad, sugiriendo un enfoque más allá de lo punitivo, hacia intervenciones rehabilitadoras y preventivas.

Según (Torre Campo, 1996), los individuos que participan en la delincuencia son aquellos que exhiben una conducta antisocial definida como delito por la ley, a menudo en una etapa crítica de desarrollo personal, con habilidades sociales deterioradas debido a su naturaleza disruptiva. Asimismo, propone una tipología de comportamiento socialmente

irregular que incluye la inadaptación social, caracterizada por la desviación de la norma sin necesariamente infringir la ley, la conducta desviada, que implica acciones que contravienen las normas sociales establecidas, y finalmente, la conducta delincuente, que es sancionada por la ley como una transgresión penal.

Este jurista, ofrece una perspectiva sobre la delincuencia centrada en la conducta antisocial definida como delito por la ley, señalando que quienes participan en ella suelen encontrarse en una etapa crítica de desarrollo personal, con habilidades sociales deterioradas debido a su naturaleza disruptiva. Este enfoque sugiere una comprensión escalonada de la delincuencia, desde formas menos severas de desviación hasta aquellas que son penalizadas legalmente, destacando la importancia de considerar el contexto y la gravedad de la conducta en el análisis del fenómeno delictivo.

La delincuencia, según Eduardo García Maynez, "se origina cuando un individuo no logra ajustarse a las expectativas de su entorno social" (García Maynez, 1951); mientras otros autores la definen como un fenómeno social surgido de transgresiones a las normas básicas de convivencia en un contexto específico. Manuel herrero la describe como "cualquier acto ilegal realizado por individuos o grupos espontáneos" (Herrero Herrero, 2005). En términos generales, se entiende como los crímenes observables en una sociedad y momento histórico dados.

Tanto la delincuencia como el delincuente se definen en relación con la ley penal y la reacción social ante su violación dentro de un grupo social. El enfoque sociológico es fundamental para comprender las interacciones entre individuos y las normas en una sociedad.

Jurídicamente, un delincuente es aquel que comete un delito, ya sea como autor, cómplice, encubridor o en cualquier función punible. Diversos factores están asociados con la delincuencia, como el género (con más hombres que mujeres implicados), habilidades cognitivas (conexiones entre bajo coeficiente intelectual y delincuencia), síndrome hiperquinético en la infancia, egocentrismo y clase social marginal. El entorno familiar también desempeña un papel crucial, con padres ausentes o abusivos como predictores de comportamiento delictivo, especialmente cuando hay una ruptura temprana entre padres e hijos.

La delincuencia es un fenómeno complejo que abarca una amplia gama de comportamientos y contextos sociales. Para comprender mejor este fenómeno, es importante analizar las diversas perspectivas y definiciones proporcionadas por expertos en el campo.

Hilda Marchiori, destaca que la delincuencia no solo se limita a la comisión de un delito específico, sino que también implica la calidad del individuo que lo comete y la frecuencia o extensión de los delitos en un determinado lugar o tiempo (Marchiori, 2005, pág. 322). Esta noción resalta la diversidad y dinamismo de la delincuencia, que puede manifestarse de diversas formas y escalas.

Por otro lado, Eduardo García Maynez subraya la relación entre el delito y la ley, señalando que el delito es una violación de la normativa legal que conlleva sanciones establecidas por la sociedad (García Maynez, 1951). Esta definición resalta la importancia del marco jurídico en la comprensión y regulación de la conducta delictiva. Al verlo desde una perspectiva sociológica se puede explicar que la delincuencia surge del fracaso del individuo para adaptarse a las normas y expectativas sociales. Esto sugiere que la delincuencia no es simplemente un acto aislado, sino el resultado de factores sociales, económicos y culturales más amplios que influyen en el comportamiento humano.

El comunicado del Consejo Europeo de Tampere amplía aún más esta visión al incluir una variedad de comportamientos punibles, que van desde delitos graves hasta acciones antisociales menos serias. Esta inclusión reconoce la complejidad de la delincuencia y la necesidad de abordarla de manera integral, considerando sus diversas manifestaciones y causas subyacentes. En cuanto a la organización de la delincuencia, se reconoce que los delitos pueden ser tanto premeditados como espontáneos, y pueden llevarse a cabo de manera individual o en grupos organizados. Esta distinción entre delincuencia menor y organizada refleja la diversidad de estrategias y niveles de sofisticación que pueden estar presentes en la actividad delictiva.

4.3.1 Ciberdelincuencia

En nuestra sociedad contemporánea, la tecnología es un componente vital en nuestras rutinas diarias, y la delincuencia se ha adaptado a este entorno dinámico. Los avances tecnológicos han dado paso a nuevas formas de perpetrar crímenes, como la invasión de la privacidad y la utilización de sistemas tecnológicos para actividades ilícitas (Marchiori, 2005).

Por otro lado, el Convenio sobre la Ciberdelincuencia, adoptado en Budapest en 2001, define la ciberdelincuencia como cualquier actividad criminal dirigida a socavar la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos (Convenio sobre la Ciberdelincuencia, 2001). Esta forma de delito se centra en atacar sistemas informáticos específicos, datos y tecnologías de la información y la comunicación.

Al analizar estas definiciones, se puede comprender, en primer lugar, la importancia fundamental de la tecnología en nuestras vidas diarias, lo que refleja su omnipresencia en la sociedad contemporánea. Esta integración tecnológica proporciona oportunidades tanto para el progreso como para la criminalidad, ya que los avances tecnológicos han permitido nuevas formas de cometer delitos.

La referencia a la invasión de la privacidad y el uso indebido de sistemas tecnológicos para actividades ilícitas subraya cómo la tecnología puede ser aprovechada por los delincuentes para perpetrar crímenes de manera más sofisticada y encubierta. Esta adaptación de la delincuencia al entorno tecnológico demuestra la necesidad de una comprensión más profunda de los riesgos y desafíos asociados con el uso de la tecnología en la sociedad moderna.

Lo preocupante es que la ciberdelincuencia carece de fronteras geográficas, lo que implica que los delincuentes pueden atacar cualquier infraestructura en cualquier parte del mundo. Estos criminales pueden operar de manera individual, formar parte de organizaciones delictivas o recibir respaldo financiero de ciertos países (Reyes & López, 2021). La globalización y la interconexión digital han ampliado las oportunidades para cometer estos delitos, lo que requiere una cooperación internacional para abordar eficazmente este problema.

En nuestra vida cotidiana, la tecnología abarca una amplia gama de actividades, desde la gestión de datos personales hasta las compras en línea y la interacción en redes sociales. Esta diversidad de información, que incluye aspectos culturales, religiosos, políticos y educativos, entre otros, está constantemente en riesgo ante posibles ciberdelincuentes, quienes la consideran valiosa.

En la era actual de la información, cada dato se vuelve significativo, siendo el llamado Big Data más valioso que los recursos minerales. El Big Data consiste en analizar e interpretar grandes volúmenes de datos, utilizados por empresas para la toma de decisiones y la personalización de la publicidad dirigida a clientes potenciales, entre otros propósitos. Este recurso se considera el "oro" del futuro, debido a su capacidad para impulsar el desarrollo y la eficacia de diversas organizaciones, tanto públicas como privadas.

4.4 La prueba

El término "prueba" tiene su origen en el latín "probatio o probationis", proveniente de "probus", que significa bueno (Morillo, 2011). Esta raíz sugiere que el acto de presentar una prueba implica hacer algo considerado como positivo o válido. Ahora bien, desde la perspectiva

doctrinal, se han ofrecido diversas definiciones de "prueba". Bentham, citado por (Morillo, 2011) la concibe como un "hecho supuestamente verdadero que se presume debe servir de motivo de credibilidad sobre la existencia o inexistencia de otro hecho". En otras palabras, la prueba es un medio utilizado para verificar la veracidad de un hecho.

En mi análisis personal, encuentro fascinante cómo el concepto de prueba ha evolucionado a lo largo del tiempo, desde su raíz etimológica hasta sus diversas interpretaciones en el ámbito doctrinal. La prueba no solo es un aspecto fundamental en el derecho y la justicia, sino que también tiene implicaciones más amplias en términos de cómo establecemos la verdad y la confiabilidad en diferentes contextos. Este análisis me lleva a reflexionar sobre la importancia de la evidencia y la argumentación en la toma de decisiones y la construcción del conocimiento en diversas disciplinas.

Por su parte, (Taruffo, 2008), la describe como "el instrumento que las partes utilizan desde hace siglos para demostrar la veracidad de sus afirmaciones, y del cual se sirve el juez para decidir respecto a la verdad o falsedad de los enunciados fácticos". Además, Taruffo destaca otros aspectos relacionados con la prueba, como su función como medio de conocimiento y su capacidad para persuadir.

Según el autor, la prueba no solo es un instrumento utilizado por las partes involucradas para demostrar la veracidad de sus afirmaciones, sino que también es una herramienta esencial para el juez en su proceso de discernir la verdad o falsedad de los enunciados fácticos. Además, Taruffo subraya otros aspectos importantes relacionados con la prueba, como su papel como medio de conocimiento. Esto sugiere que la presentación y evaluación de pruebas no solo sirven para establecer hechos concretos en un caso legal, sino que también pueden contribuir al entendimiento más amplio de los eventos y circunstancias involucradas.

La prueba, según (Taruffo, 2008) desempeña dos roles fundamentales en el proceso judicial. Por un lado, actúa como un instrumento de conocimiento al proporcionar información sobre los hechos que deben ser determinados en el proceso. Esto implica que los enunciados pueden ser considerados verdaderos o falsos en función de las pruebas presentadas, ya que cualquier conclusión del juez depende de las pruebas incorporadas en el proceso. Por otro lado, la prueba también funciona como un instrumento de persuasión, donde su objetivo principal no es determinar la verdad de los hechos, sino convencer al juez sobre la validez de un enunciado, ya sea con o sin fundamento.

Desde una mirada analítica, se observa que la prueba no solo se concibe como un medio para establecer la verdad de los hechos, sino también como una herramienta de persuasión en el proceso judicial. El primer aspecto resaltado es el papel de la prueba como un instrumento de conocimiento. Aquí, se enfatiza su función para proporcionar información relevante sobre los hechos en cuestión, lo que permite al juez tomar decisiones informadas y basadas en evidencia. Por otro lado, se explora la dimensión de la prueba como un instrumento de persuasión; sugiriendo que, más allá de su función informativa, la prueba también se utiliza para influir en la opinión del juez y convencerlo sobre la validez de ciertos enunciados

En cuanto al ámbito legal del Derecho Penal ecuatoriano, la prueba se establece en el Título IV del COIP, como se detallará en la parte correspondiente a las bases legales.

4.4.1 Medios de prueba

El término "medio de prueba" se refiere al procedimiento a través del cual el juez o el órgano de prueba revela y registra el objeto de la evidencia, según lo indica Florián, citado por (Morillo, 2011) Es importante entender dos conceptos adicionales: el objeto de prueba y el órgano de prueba.

El objeto de prueba se refiere al tema sobre el cual se centra la actividad probatoria, es decir, los hechos relevantes para determinar la posible ocurrencia de un delito. Este concepto responde a preguntas como qué se debe probar, dónde, cómo, quién y por qué. Por otro lado, el órgano de prueba se refiere a la persona o personas a través de las cuales se presenta ante el juez y las partes interesadas el objeto de prueba. Actúan como intermediarios entre el objeto de prueba y el tribunal, proporcionando conocimientos e información sobre dicho objeto. Además, es relevante conocer el término "sujeto de prueba", que engloba a todas las personas involucradas en la actividad probatoria, incluyendo a quienes solicitan la prueba, quienes la reciben y terceros que participan como peritos o testigos.

(Plascencia, 1995), define el medio de prueba como la evidencia misma utilizada en un proceso judicial. Destaca que el nivel de "medio" lo adquiere la prueba cuando es ofrecida y admitida dentro del proceso. En la legislación ecuatoriana, se reconocen como medios de prueba el documento, el testimonio y la pericia. Plascencia también diferencia entre medio de prueba y fuente de prueba. Mientras que la fuente de prueba existe independientemente del proceso penal y es ajena a él, el medio de prueba es un concepto procesal posterior, que surge cuando la fuente de prueba es ofrecida, admitida y desahogada dentro del proceso penal.

4.4.1.1 Elementos de prueba

Algunos de los aspectos fundamentales de la prueba, según (Artavia, 2018) que incluyen:

a. El objeto de la prueba, que se refiere a los hechos o circunstancias relevantes que pueden ser demostrados durante el proceso.
b. La fuente de la prueba, que es de donde se extrae la evidencia, como documentos, testimonios de testigos o informes periciales.
c. La carga de la prueba, que establece quién tiene la responsabilidad de probar ciertos hechos durante el juicio.
d. Los medios de prueba, que son los métodos o instrumentos utilizados para obtener la evidencia necesaria para respaldar los argumentos de las partes en el juicio.
e. El procedimiento de la actividad probatoria, que determina cuándo y dónde se llevará a cabo la recolección y presentación de pruebas durante el proceso judicial.
f. El producto final del proceso de prueba, que son los elementos de evidencia obtenidos y presentados durante el juicio y que influyen en la decisión final del tribunal.

4.4.1.2 prueba electrónica

La prueba digital o electrónica se define como un medio de reproducción y almacenamiento de palabras, sonidos e imágenes, así como de datos y operaciones matemáticas relevantes para el proceso, según lo expuesto por Muñoz, citado por (Rodríguez, 2018). En este contexto, la legislación española, establece que el soporte material que contenga datos o narraciones relevantes y tenga eficacia probatoria y relevancia jurídica, constituye una prueba digital.

Por otro lado, (Borges, 2018) aporta una definición que integra los conceptos de prueba, medio y fuente. Según este autor, la prueba digital abarca toda información de valor probatorio transmitida o contenida en medios electrónicos. La fuente de prueba se refiere específicamente a esta información, mientras que el medio de prueba es la manera en que se introduce en el proceso, ya sea como prueba documental, pericial o testimonial. En el contexto legal del Derecho Penal ecuatoriano, la prueba digital se considera parte de la prueba documental, como se detalla en el artículo 500 del COIP.

En el ámbito del Derecho Penal ecuatoriano, se establecen vías procesales para la introducción de medios de prueba como herramientas estratégicas en un juicio, sustentadas en el principio de libertad probatoria contemplado en el COIP (Asamblea Nacional , 2023), específicamente en el artículo 454 numeral 4. Este principio permite demostrar hechos y circunstancias pertinentes según el caso, siempre y cuando el medio de prueba no contravenga la Constitución, los instrumentos internacionales ratificados por el Estado y otras normativas legales.

Además del principio de libertad probatoria, existen otros principios que rigen el anuncio y la práctica de la prueba en el Derecho Probatorio Penal en Ecuador. Estos incluyen la oportunidad, inmediación, contradicción, pertinencia, exclusión y garantía de igualdad de oportunidades para la prueba. Estos principios serán ampliados en la sección correspondiente a Bases Legales. Es importante destacar que la prueba y sus elementos deben guardar relación directa con la infracción y la persona acusada, evitando basarse en meras presunciones y priorizando hechos reales respaldados por medios de prueba (Asamblea Nacional , 2023).

Para garantizar la autenticidad, manejo, análisis y conservación de los elementos probatorios, se establece la aplicación de la cadena de custodia, según lo establecido en el Artículo 456 del COIP. Esto implica que el servidor público que entre en contacto con la escena del crimen asume la responsabilidad de su manejo hasta que llegue el personal especializado.

4.4.2 Peritaje

Según Ortega (2007), la palabra "pericia" tiene su origen en el latín perita, que se refiere a una persona con un profundo conocimiento en un campo específico. Este término se descompone en dos partes: "periens", que denota algo probado, y "ia", que indica una cualidad. La pericia se lleva a cabo con el propósito de ayudar al juez a resolver incertidumbres relacionadas con ciertos acontecimientos. El autor destaca cómo la pericia se utiliza para esclarecer incertidumbres y ayudar al juez a tomar decisiones informadas. Esta función destacada en el ámbito legal resalta la relevancia crucial de la pericia no solo en la búsqueda de la verdad, sino también en la administración de justicia.

La pericia, “se refiere a la habilidad, conocimiento y experiencia en un campo específico” (Flores, Prueba pericial. Consideraciones sobre la prueba pericial y su valoración en la decisión judicial. , 2005). Esta competencia la posee un individuo llamado perito, quien es consultado habitualmente para resolver disputas. En el contexto judicial, una pericia puede consistir en un estudio realizado por un perito, designado por un juez, tribunal u otra autoridad,

que resulta en la elaboración de un informe pericial o dictamen pericial. Este informe puede convertirse en evidencia en el proceso legal y contribuir a la emisión de una sentencia.

El contenido de un informe pericial siempre incluye una descripción minuciosa del objeto, persona o situación bajo estudio, así como una lista detallada de todas las operaciones realizadas durante la pericia y sus resultados. Además, se enumeran los métodos científicos y técnicos empleados para elaborar el informe, junto con las conclusiones derivadas de estos hallazgos. Por ejemplo, existen casos donde el resultado de una pericia afecta directamente las decisiones judiciales, como la detención de un sospechoso, la liberación de un individuo debido a la evidencia pericial que demuestra su inocencia, o la evaluación de la validez de las pruebas basadas en la escena del crimen. En resumen, se resalta la importancia de la pericia en el proceso legal y su influencia en la determinación de la verdad en los casos judiciales.

En un proceso legal, pueden intervenir dos tipos de peritos: los peritos de parte, propuestos por alguna de las partes involucradas en el litigio, y los peritos judiciales, designados por el juez. Según (López, 2006), los informes periciales se presentan bajo juramento y se basan en las pruebas recopiladas por el perito, quien está prohibido de hacer suposiciones o emitir opiniones.

El jurista Garberí Llobregat, (2003) define el dictamen de peritos como un medio de prueba en el cual se aporta al proceso un informe elaborado por un experto en una disciplina específica, acompañado, en algunos casos, de la posibilidad de que el autor comparezca en el juicio para responder preguntas y aclaraciones solicitadas por las partes y el tribunal. El propósito es demostrar hechos relevantes legalmente para el caso, que requieren conocimientos especializados en ciencia, arte, técnica o práctica.

4.4.3 Perito

La palabra "perito", derivada del latín "Perítus", se refiere a alguien con conocimientos especiales en un área específica. Según la (Real Academia Española, 2019) un perito es una persona que posee un título oficial conferido por el Estado o que, teniendo conocimientos teóricos o prácticos especiales, proporciona información al juez sobre asuntos litigiosos relacionados con su expertise, bajo juramento. Mientras que para (Cassrino Viterbo, 1954) un perito no necesariamente tiene certificaciones formales de instituciones educativas, sino que destaca su dominio y competencia en una materia específica, permitiéndole ofrecer una opinión autorizada sobre los aspectos dentro de su campo de competencia.

En primer lugar, se destaca la etimología de la palabra y su definición según la Real Academia Española, lo que nos lleva a entender al perito como alguien con conocimientos especializados, ya sea a través de un título oficial o de experiencia práctica, que proporciona información relevante al juez en casos legales. Asimismo, la perspectiva de Cassrino Viterbo añade un matiz interesante al señalar que la certificación formal no es necesariamente un requisito para ser considerado perito, sino que lo crucial es el dominio y la competencia en un área específica. Esto sugiere que la experiencia y el conocimiento práctico pueden ser igualmente valiosos para desempeñar el papel de perito en un proceso judicial.

En línea con esta perspectiva, (Silva, 1991) considera al perito como un profesional que asiste al juez, destacando que no es parte en el proceso judicial, sino un tercero que colabora con el tribunal en asuntos específicos que requieren conocimientos especializados en ciencia, arte u oficio. La visión de Silva destaca el papel del perito como un colaborador imparcial del tribunal, enfatizando su función de proporcionar conocimientos especializados sin estar directamente involucrado en el litigio. Esta perspectiva resalta la importancia de la neutralidad y la imparcialidad en el trabajo del perito dentro del sistema legal.

En nuestra legislación, para que un profesional pueda actuar como perito judicial, es necesario que obtenga la calificación correspondiente del Consejo de la Judicatura y cumpla con las normativas establecidas en el COGEP y en el Reglamento SPIFJ. Según el artículo 4, inciso 1 del (SPIFJ, 2014) se establece que, para ser considerado perito, es requisito previo estar calificado por el Consejo de la Judicatura de acuerdo con el Código Orgánico General de Procesos y este Reglamento. Sin embargo, el reglamento SPIFJ contempla una excepción a esta regla en el artículo 4, inciso 2, que permite que expertos que no residen en Ecuador y sean designados como peritos para un juicio no necesiten la calificación obligatoria por parte del Consejo de la Judicatura (2014).

Esta disposición está alineada con la normativa del (COGEP, 2015) , que define al perito como personas debidamente acreditadas por el Consejo de la Judicatura, autorizadas para emitir informes periciales, intervenir y declarar en el proceso, según lo establecido en el artículo 221, inciso 2.

Según las definiciones proporcionadas en las normativas legales ecuatorianas, el estado garantiza a la sociedad que los peritos judiciales poseen amplios conocimientos y una experiencia sólida en las áreas periciales en las que han sido calificados. Esta garantía asegura

que los peritos estén debidamente capacitados para ofrecer análisis especializados y opiniones fundamentadas dentro del ámbito profesional.

Además, el estado ecuatoriano establece que los peritos son profesionales judiciales cuyo rol principal es auxiliar al juez en el proceso probatorio, como lo indica el artículo 22, inciso 1, del reglamento (SPIFJ, 2014) Esto implica que los peritos calificados tienen la responsabilidad de brindar asistencia al sistema judicial mediante la presentación de informes periciales y la intervención en el proceso legal, contribuyendo así a la búsqueda de la verdad y a la administración de justicia de manera imparcial y eficiente.

El rol del perito forense en el ámbito judicial ha cobrado una importancia creciente en diversos campos, especialmente en casos civiles y penales donde se involucran pruebas digitales o delitos informáticos. Según el nuevo código orgánico integral penal, se establecen requisitos obligatorios para quienes actúan como peritos:

a. Deben ser profesionales expertos en el área, titulados o con experiencia y especialización acreditada por el Consejo de la Judicatura.
b. Su designación es obligatoria y deben aceptar el cargo notificado.
c. Deben excusarse si se encuentran en alguna de las causales de inhabilitación establecidas por el COIP.
d. No pueden ser recusados, pero si presentan motivos de inhabilidad o excusa, su informe carecerá de validez.
e. Deben presentar informes dentro de plazos establecidos y ampliarlos si es requerido por las partes.
f. Los informes periciales deben incluir detalles como lugar y fecha, identificación del perito, descripción del objeto peritado, técnica utilizada, fundamentación científica, ilustraciones y conclusiones.
g. Deben comparecer a la audiencia de juicio para sustentar oralmente sus informes y responder a los interrogatorios.
h. El sistema pericial a nivel nacional está a cargo del Consejo de la Judicatura, quien determina los honorarios por estas diligencias.

4.4.4 Idoneidad del Perito

El proceso de calificación de los peritos judiciales recae exclusivamente en el Pleno del Consejo de la Judicatura, tal como se establece en el Código Orgánico de la Función Judicial,

artículo 264, numeral 9. Este órgano jurisdiccional tiene la responsabilidad de sistematizar un registro de peritos autorizados y reconocidos como idóneos, asegurando que estén debidamente calificados y cuenten con la experiencia y profesionalización necesarias. El Sistema Pericial Integral, administrado por el Pleno del Consejo de la Judicatura, no solo incluye sistemas para registrar y conservar las actividades realizadas, sino también a profesionales, entre ellos los peritos judiciales, cuyo trabajo contribuye a los objetivos de este organismo estatal.

Para que un perito judicial pueda certificarse como profesional idóneo, debe asegurarse de que su desempeño esté alineado con los principios establecidos en el reglamento (SPIFJ, 2014). Este reglamento, en su artículo 2, establece que el Sistema Pericial Integral de la Función Judicial se guiará por principios como legalidad, transparencia, credibilidad, alternatividad, igualdad, probidad, no discriminación, publicidad, méritos, independencia, imparcialidad, especialidad, autonomía, responsabilidad, entre otros, conforme a lo dispuesto en la Constitución de la República del Ecuador y en el Código Orgánico de la Función Judicial.

El artículo mencionado por el Pleno del Consejo de la Judicatura, al incluir la expresión "entre otros" en la lista de principios que rigen a los profesionales del Sistema Pericial Integral, deja abierta la posibilidad de evaluar diversos aspectos del desempeño de los peritos en todo momento. Este enfoque permite considerar situaciones hipotéticas como la de un perito con problemas de alcoholismo o dependencia de sustancias controladas, cuyos peritajes podrían ser técnicamente correctos pero cuya conducta personal podría plantear interrogantes sobre su idoneidad para formar parte del sistema pericial.

En efecto, existen principios y normativas de vida que van más allá de los conocimientos técnicos y se relacionan con el comportamiento y el compromiso ético de un profesional. En el caso hipotético mencionado, la presencia de problemas de alcoholismo o adicción podría afectar la objetividad, la imparcialidad y la responsabilidad del perito, elementos esenciales para el adecuado desempeño en el Sistema Pericial Integral.

El reglamento del SPIFJ establece claramente las obligaciones generales que deben cumplir los peritos judiciales, incluyendo la aplicación de principios de actuación como objetividad, imparcialidad, independencia, responsabilidad, entre otros. Se espera que el trabajo del perito se enmarque en todo momento en la ética, presentando criterios técnicos y especializados libres de juicios de valor. Esto subraya la importancia de la integridad y la honestidad en el ejercicio de la función pericial, asegurando la confianza y la credibilidad del sistema judicial en su conjunto.

El proceso para calificarse como perito judicial es detallado en un documento disponible en el sitio web de la (Consejo de la Judicatura, 2023), el cual presenta varias secciones, incluida una que explica las funciones del perito judicial. Según este documento, el perito judicial tiene varias responsabilidades:

- Asistir obligatoriamente cuando es convocado en un proceso judicial.
- Exponer su informe durante la audiencia correspondiente y responder a las preguntas formuladas por el juez, las partes o el fiscal, enfocándose en aspectos técnicos contenidos en el informe.
- Abstenerse de emitir juicios de valor a favor o en contra de alguna de las partes; su alcance se limita estrictamente a lo técnico (Consejo de la Judicatura, 2023).

Sin embargo, se observa que la aplicación de estándares internacionales para la elaboración de informes periciales de carácter informático no se menciona como una función específica del perito judicial informático en este documento. Este enfoque destaca la importancia de la imparcialidad y la objetividad en el trabajo del perito judicial, asegurando que sus informes se basen únicamente en aspectos técnicos y no en opiniones personales. Sin embargo, podría plantearse la necesidad de incluir la aplicación de estándares internacionales en el ámbito informático como parte de las funciones del perito judicial especializado en esta área, con el fin de garantizar la calidad y la relevancia de sus informes en casos relacionados con la tecnología.

4.4.5 Perito informático

El peritaje informático es un proceso mediante el cual se extrae, analiza y recopila información de dispositivos electrónicos como computadoras, tablets, teléfonos móviles, entre otros, con el fin de obtener pruebas válidas que puedan presentarse ante un tribunal en un proceso judicial (Flores, 2015). Dado que los jueces carecen de la formación y conocimiento necesarios para verificar la autenticidad y la integridad de las pruebas tecnológicas, y los abogados no tienen la capacidad de obtenerlas por sí mismos, los peritos informáticos juegan un papel crucial en este ámbito.

Es importante mencionar que, el peritaje informático se lleva a cabo cuando existen evidencias o sospechas de que ha ocurrido un incidente de seguridad informática que involucra un uso indebido de los dispositivos electrónicos o que estos se han utilizado para cometer algún tipo de delito (Molina, 2019). Entre los casos típicos en los que se suele recurrir al peritaje

informático se incluyen el espionaje industrial, la filtración de información sensible o confidencial, la violación de la privacidad de las personas, el uso inapropiado de los equipos informáticos y el fraude electrónico.

La importancia del peritaje informático radica en su capacidad para proporcionar pruebas sólidas y verificables en casos donde la tecnología está involucrada, ayudando así a garantizar la imparcialidad y la integridad del proceso judicial. Además, su intervención es fundamental para esclarecer hechos complejos relacionados con el uso de la tecnología, lo que contribuye a la administración de justicia de manera eficaz y equitativa.

El proceso inicial de un peritaje informático comienza con un análisis detallado de la situación para determinar el alcance del peritaje y comunicar al cliente la naturaleza y el costo del proceso. Una vez establecida la magnitud del impacto, se inicia la obtención de información de los dispositivos pertinentes, como ordenadores, tablets, teléfonos móviles y servidores. Para garantizar la integridad de la información recopilada, es común realizar la extracción ante notario y depositar los equipos en la notaría, asegurando así la custodia tanto de los dispositivos como de la información contenida en ellos (Ibáñez, 2015). Esta información será la base sobre la cual se sustenten las pruebas tecnológicas presentadas ante el tribunal.

Posteriormente, la información obtenida de los dispositivos se somete a un análisis exhaustivo para determinar las causas y consecuencias del incidente de seguridad de la información o para recabar evidencia de un posible uso inapropiado de los equipos (Molina, 2019). Este análisis implica investigar aspectos como la información almacenada en los dispositivos, los registros de acceso o modificación, la presencia de datos borrados o eliminados, la existencia de copias en dispositivos externos, así como eventos y registros de actividad. A partir de estos hallazgos, se construye una línea de tiempo que documenta los eventos y acciones identificados.

Finalmente, las evidencias recopiladas se documentan en un informe pericial, redactado de manera clara, concisa y comprensible, con el fin de presentarlo ante el tribunal como prueba de los hechos investigados (Ibáñez, 2015). Este informe pericial cumple un papel fundamental en el proceso judicial al proporcionar una descripción detallada y fundamentada de los eventos analizados, lo que contribuye a la toma de decisiones judiciales informadas y justas.

El Reglamento del Sistema Pericial Integral de la Función Judicial, compuesto por cuarenta y un artículos, cuatro disposiciones transitorias, dos disposiciones derogatorias y dos disposiciones finales, es una normativa creada por el Pleno del Consejo de la Judicatura. Su

última modificación se realizó el 23 de junio de 2022. Este reglamento, según el artículo 1, tiene como objetivo regular todos los aspectos relacionados con la calificación, gestión, administración y disciplina de los peritos de la Función Judicial a nivel nacional (2014).

Para asegurar que los peritos judiciales sean profesionales competentes en el área y especialización en la que desean desempeñarse, este reglamento establece en su artículo 2 los principios que rigen esta normativa. Estos principios incluyen la legalidad, transparencia, credibilidad, alternatividad, igualdad, probidad, no discriminación, publicidad, méritos, independencia, imparcialidad, especialidad, autonomía, responsabilidad, entre otros, los cuales están en consonancia con lo establecido en la Constitución de la República del Ecuador y en el Código Orgánico de la Función Judicial.

Este enfoque basado en principios garantiza que la selección y el desempeño de los peritos judiciales se realicen de manera justa, imparcial y competente, lo que fortalece la integridad y la confianza en el sistema judicial. Además, al alinearse con las disposiciones constitucionales y legales, se asegura que el trabajo de los peritos esté en línea con los estándares éticos y profesionales más altos.

4.5 Informes periciales

Como hemos podido constatar, independientemente del campo de especialización, un informe pericial se caracteriza por dos aspectos fundamentales: en primer lugar, no tiene carácter vinculante para el juez que preside el proceso judicial; y, en segundo lugar, su propósito principal es presentar de manera clara y comprensible al juez y a las partes involucradas los hallazgos obtenidos, sin utilizar un lenguaje técnico excesivo (Silva, 1991).

De acuerdo con la definición proporcionada por Silva, el informe pericial es "el análisis que el perito realiza sobre los temas presentados por las partes o por el tribunal, y que proporciona una opinión autorizada que ayuda al juez a tomar una decisión definitiva". Esto resalta la importancia del informe pericial como un recurso fundamental para el juez en la resolución del caso. Puesto que, el informe pericial contiene afirmaciones o negaciones que respaldan las argumentaciones de las partes, respaldadas por pruebas periciales basadas en los hallazgos documentados. En resumen, el informe pericial desempeña un papel crucial en el proceso judicial al proporcionar al juez información detallada y fundamentada sobre los aspectos técnicos relevantes del caso, lo que contribuye a una administración de justicia justa y equitativa.

El Informe Pericial es un elemento crucial en el sistema legal ecuatoriano, como lo establece el Código Orgánico Integral Penal. En el artículo 498 de este código se enumeran tres medios de prueba: el documento, el testimonio y la pericia. Esto destaca la importancia otorgada a la pericia como un medio válido para la presentación de pruebas en los procesos judiciales.

El legislador, en el artículo 511 del mismo cuerpo legal, detalla ocho reglas que los peritos deben cumplir. Estas reglas incluyen requisitos específicos para el contenido mínimo de un informe pericial. Entre estos requisitos se encuentra la necesidad de incluir información detallada sobre el lugar y la fecha en que se realizó el peritaje, la identificación del perito, una descripción completa del objeto o persona peritada, la técnica utilizada en el peritaje, así como la fundamentación científica que respalda las conclusiones del informe (Asamblea Nacional , 2023). Además, se menciona la inclusión de ilustraciones gráficas cuando sea pertinente.

Estos requisitos son fundamentales para garantizar la calidad y la validez de los informes periciales presentados ante los tribunales. Al exigir un contenido mínimo aceptable, se busca proporcionar al juez y a las partes involucradas información precisa y detallada que les permita comprender adecuadamente los hallazgos del peritaje. Esto contribuye a la transparencia y la imparcialidad en el proceso judicial, al tiempo que fortalece la credibilidad de la evidencia presentada.

4.5.1 El informe pericial en el COGEP

El Código Orgánico General de Procesos (COGEP, 2015) regula varios aspectos relacionados con la prueba pericial, incluyendo el contenido del informe pericial, los procedimientos para solicitar informes periciales y quiénes están autorizados para hacerlo. Sin embargo, ni el COGEP ni el Reglamento del SPFJ especifican las metodologías que debe utilizar el perito para elaborar correctamente el informe pericial, independientemente de si la prueba pericial es de naturaleza informática o no.

En cuanto a la prueba pericial, el COGEP tipifica varios aspectos relacionados con ella. Por ejemplo, el artículo 221 define quién es considerado perito, el artículo 222 establece el procedimiento para la declaración de los peritos, y el artículo 223 enfatiza la imparcialidad como requisito fundamental para la actuación del perito judicial. En lo que respecta al informe pericial, el artículo 224 del (COGEP, 2015) establece los requisitos mínimos que se espera en su contenido. El artículo 225 determina quiénes tienen la facultad de solicitar una pericia, mientras que el artículo 226 establece que, en caso de pericias contradictorias entre las partes,

el juez puede solicitar una pericia adicional para resolver mejor el caso. Por último, el artículo 227 aborda la finalidad y el contenido de la prueba pericial en general.

Estos aspectos regulados por el COGEP garantizan un marco legal sólido para la utilización de la prueba pericial en los procesos judiciales, asegurando que se cumplan los requisitos mínimos de calidad y que se respeten los principios fundamentales de imparcialidad y objetividad en la actuación de los peritos. Sin embargo, la falta de especificación sobre las metodologías a utilizar puede dejar cierta discrecionalidad en manos de los peritos, lo que destaca la importancia de la formación y la ética profesional en este campo.

4.6 Derecho comparado

4.6.1 Convenio de Budapest

El 23 de noviembre de 2001, los Estados europeos adheridos al Consejo de Europa y los firmantes del Convenio de Budapest elaboraron un documento que consta de 48 artículos y un preámbulo, el cual establece las regulaciones para los actos ilegales realizados por ciberdelincuentes que constantemente buscan vulnerar las protecciones de los datos personales y financieros almacenados en medios electrónicos (Convenio sobre la Ciberdelincuencia., 2001)

Este convenio, conocido como el Convenio sobre la Ciberdelincuencia, aunque no tiene carácter vinculante para los ciudadanos ecuatorianos, resulta relevante para esta investigación debido a que pone de manifiesto la ausencia de normativas legales con enfoques técnicos en Ecuador. Estas normativas tendrían como objetivo identificar conductas punibles que amenacen el funcionamiento adecuado de las redes informáticas, así como la integridad y disponibilidad de la información electrónica.

En relación con los delitos informáticos, los Estados Miembros del Consejo de Europa argumentan que es necesario prevenir acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos. Esto incluye el abuso de dichos sistemas y redes, y se propone tipificar como delito estas acciones, tal como se definen en el Convenio (Convenio sobre la Ciberdelincuencia, 2001). Además, se plantea la necesidad de otorgar poderes suficientes para combatir eficazmente estos delitos, facilitando su detección, investigación y sanción a nivel nacional e internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y confiable.

Es menester destacar la importancia de abordar los delitos informáticos de manera integral y colaborativa, tanto a nivel nacional como internacional, para garantizar la seguridad y protección de los sistemas de información y la información electrónica en un entorno cada vez más digitalizado y conectado.

El Convenio de Budapest establece directrices que los países miembros o adheridos deben seguir para dos propósitos principales. En primer lugar, busca definir, mediante el uso de terminología técnica informática, qué conductas deben ser consideradas como delitos informáticos (Consejo de Europa). Esto implica tipificar acciones como el acceso ilícito a datos, la interceptación de señales o datos de manera ilegal, ataques informáticos que comprometan la integridad de los datos y el funcionamiento adecuado de los sistemas, así como la falsificación y el fraude informático, entre otros (2001).

En segundo lugar, el Convenio de Budapest establece procedimientos procesales que los estados deben seguir para hacer cumplir las leyes y sanciones relacionadas con los delitos informáticos. Estos procedimientos normalizan tareas específicas relacionadas con la informática, como se describen en los artículos del 14 al 22 (Convenio sobre la Ciberdelincuencia, 2001). Estas tareas incluyen la rápida conservación de datos almacenados en sistemas informáticos, la conservación y revelación parcial rápida de datos relativos al tráfico, el registro y confiscación de datos almacenados, la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido.

Este enfoque del Convenio de Budapest busca proporcionar un marco legal sólido para abordar los delitos informáticos, no solo identificando claramente las conductas punibles, sino también estableciendo procedimientos claros y efectivos para garantizar la aplicación de la ley en el ámbito digital.

El Convenio de Budapest, en su sección que va desde el artículo 23 hasta el 34, aborda una serie de principios clave relacionados con la cooperación internacional y la aplicación de la ley en contextos transfronterizos. Estos principios engloban aspectos como la colaboración entre los estados firmantes, los procesos de extradición, la ayuda mutua entre los estados, la transferencia de datos confidenciales, la protección de la confidencialidad de esta información y las restricciones sobre su uso (2001). Una disposición destacada en este acuerdo es la referida al acceso transfronterizo a datos almacenados, ya sea con consentimiento o cuando dichos datos sean accesibles públicamente.

Es crucial destacar que el Convenio de Budapest tiene un alcance global, lo que implica que aborda situaciones donde los delitos cibernéticos traspasan las fronteras nacionales. Por este motivo, el artículo 22 del convenio establece cómo se distribuye la jurisdicción entre los países firmantes o adherentes, incluso en casos donde los delitos informáticos ocurren en buques o aeronaves en movimiento. Asimismo, contempla escenarios donde el delito cibernético se comete en un país diferente al de registro del medio de transporte utilizado por el delincuente.

4.6.2 Estándares Internacionales

La UNE, conocida por sus siglas de la Asociación Española de Normalización, es el principal Organismo de Normalización en España, autorizado por el gobierno y reconocido por la Comisión Europea. Actúa como representante de estándares europeos y nacionales, incluyendo normativas como el estándar internacional UNE, información que encuentro muy relevante para esta presente investigación.

El estándar de normalización UNE abarca un conjunto de normas técnicas que sirven como guía para las empresas que desean implementar Sistemas de Gestión de Calidad basados en estándares internacionales, como la ISO 9001 (UNE, ISO 9001. (2023). [Norma internacional]., 2024). La aplicación de estos estándares asegura la uniformidad en los procesos de las empresas que optan por adoptarlos, lo que conlleva a una mejora en la eficiencia y la calidad de los productos y servicios ofrecidos. Los estándares de normalización, en general, son desarrollados para abordar los desafíos que surgen entre el progreso de la sociedad y la protección del medio ambiente y los seres vivos. Estos estándares promueven procesos competitivos a nivel internacional, lo que facilita la interoperabilidad y la armonización de prácticas a nivel global.

La política de calidad de la UNE, tal como se describe en su sitio web, se centra en el desarrollo de la normalización y la cooperación internacional para impulsar la competitividad y la seguridad de las empresas, así como para mejorar el control de los riesgos empresariales y promover el buen gobierno corporativo. Además, se enfoca en la inclusividad, la protección del medio ambiente y el bienestar de la sociedad, alineándose con los Objetivos de Desarrollo Sostenible. Esto evidencia el compromiso de la UNE con la excelencia empresarial y el beneficio social a través de la aplicación de estándares de calidad y seguridad.

El contenido del informe pericial sigue un estándar para registrar los hallazgos, independientemente de la naturaleza del peritaje. Por ejemplo, en informes médicos, el formato

puede ser estático, ya que las partes del cuerpo humano son constantes y no evolucionan anatómicamente (Cabrera, 2018). Sin embargo, en informes periciales informáticos, el contexto es diferente debido al constante avance tecnológico y las innovaciones digitales desarrolladas por ciberdelincuentes. En este sentido, el perito informático debe seguir los lineamientos establecidos por estándares internacionales para garantizar la precisión y validez de su informe (Ruiz, 2020).

Es importante que el perito informático utilice herramientas y metodologías reconocidas internacionalmente para la elaboración de su informe. Esto asegura que el dictamen esté respaldado por prácticas reconocidas en la comunidad internacional y minimiza la posibilidad de sesgos basados únicamente en la experiencia y conocimientos individuales del perito.

4.6.3 Norma UNE 197001:2019

La normativa española, la cual se encuentra dirigida a los peritos establece pautas generales obligatorias para la elaboración de informes periciales en diversos ámbitos, dejando espacio para la aplicación de normativas más específicas según la evaluación del perito. Su alcance se centra en definir la estructura de los informes periciales, sin especificar los métodos y procesos específicos para su elaboración (UNE, 2019).

Es importante tener en cuenta que esta normativa no es adecuada como referencia cuando la pericia se basa principalmente en pruebas de naturaleza tecnológica o de comunicación. El estándar español aborda aspectos que no están contemplados en el Formato de Informe Pericial establecido por el Consejo de la Judicatura, como, por ejemplo, la inclusión de los datos del solicitante del informe pericial y la sección para registrar posibles tachas del perito. Por ejemplo, en el formato establecido por el estándar español, se requiere incluir los datos completos del solicitante del informe pericial, ya sea el juez o alguna de las partes involucradas en el proceso judicial, junto con su número de identificación legal (UNE, 2019). Además, se contempla una sección para registrar cualquier objeción o cuestionamiento relacionado con el perito, como expedientes administrativos abiertos o procesos judiciales en su contra, que podrían afectar su imparcialidad.

En contraste, el Formato de Informe Pericial establecido por el Consejo de la Judicatura incluye una sección de declaración juramentada, que enfatiza la independencia del perito en la elaboración del informe. Esta sección asegura que el dictamen pericial se base únicamente en

la experiencia y conocimientos profesionales del perito, sin verse influenciado por opiniones o intereses de terceros, independientemente de su posición laboral o relación con el perito (Consejo de la Judicatura, 2023).

El estándar internacional establece que el perito debe declarar bajo juramento su imparcialidad durante la elaboración del informe pericial, una indicación de suma importancia que busca eliminar cualquier sesgo que pueda existir y que podría pasar desapercibido durante el proceso de calificación como perito judicial. Esta medida contribuiría a garantizar la imparcialidad y la neutralidad del perito en la presentación de sus hallazgos, evitando así cualquier predisposición que pudiera influir en el contenido del informe pericial (UNE, 2019).

Es crucial resaltar que la imparcialidad está estrechamente relacionada con la ausencia de predisposiciones a favor o en contra de alguna de las partes involucradas en el litigio, lo cual puede influir en los hallazgos periciales. Aunque el (COGEP, 2015) y el Pleno del (Consejo de la Judicatura, 2023) regulan la imparcialidad del perito y su objetividad al realizar la pericia asignada, el estándar internacional destaca la importancia de incluir la declaración juramentada de imparcialidad en el Formato Estándar de Informe Pericial, una medida que no se contempla en dichos documentos.

En este sentido, es esencial que el perito desempeñe su labor con objetividad e imparcialidad, tal como lo establece la ley en sus respectivas regulaciones. Sin embargo, la inclusión de la declaración juramentada de imparcialidad en el Formato Estándar de Informe Pericial podría fortalecer aún más la credibilidad y la confianza en los informes periciales, al proporcionar una garantía adicional de neutralidad por parte del perito durante todo el proceso.

4.6.3 Norma UNE 197001:2015

El propósito y la aplicación de esta norma son establecer los requisitos formales que deben cumplir los informes y dictámenes periciales en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC), sin entrar en detalle sobre los métodos y procesos específicos para su elaboración (UNE, 2015). La elaboración de esta normativa se fundamenta en la norma genérica "Criterios generales para la elaboración de informes y dictámenes periciales" la cual fue anulada posteriormente para ser reemplazada por la normativa (UNE, 2019), que se detalló en la sección anterior.

Es así como la Asociación Española de Normalización, conocida como AENOR, una empresa reconocida por sus servicios de certificación internacional, publica esta normativa que establece la estructura documental y el contenido adecuado para la redacción, organización y

presentación de informes periciales exclusivamente en el ámbito informático. Esta norma específica define los "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)" (UNE, 2015).

Según (Flores Galea, 2019), la normativa UNE 197010:2015 establece principios que deben ser respetados por el perito informático durante la elaboración de informes periciales:

En su introducción, la norma enumera los siguientes principios aplicables durante la selección, obtención, presentación y almacenamiento de evidencias, tanto físicas como digitales:

1. **Relevancia**: Se refiere a la importancia y el valor que tienen las evidencias en el informe pericial, resaltando aquellas que son más trascendentales para el caso.
2. **Fiabilidad**: Esta propiedad implica que los resultados obtenidos del proceso puedan ser reproducidos consistentemente por diferentes investigadores independientes, a partir de las mismas evidencias.
3. **Suficiencia**: Se refiere a que las evidencias presentadas sean adecuadas y proporcionadas al objeto que se busca demostrar en el informe pericial, asegurando su representatividad.
4. **Oportunidad**: La evidencia presentada debe ser relevante para las circunstancias y el momento temporal del caso, de manera que sea trascendente en el juicio (Flores Galea, 2019)

El principio de relevancia destaca la importancia de identificar y resaltar las evidencias más significativas para el caso en cuestión, lo que ayuda a centrar la atención en los aspectos más relevantes de la investigación. La fiabilidad se refiere a la consistencia y reproducibilidad de los resultados obtenidos, lo que es esencial para asegurar la validez y la credibilidad del informe pericial. La suficiencia garantiza que las evidencias presentadas sean adecuadas y proporcionadas para respaldar las conclusiones del informe, evitando la inclusión de información innecesaria o irrelevante. Finalmente, el principio de oportunidad enfatiza la importancia de presentar las evidencias en el momento adecuado y dentro del contexto del caso, lo que aumenta su relevancia y su impacto en el juicio.

Es menester, recalcar que, estos principios son fundamentales para garantizar la integridad y la calidad de los informes periciales informáticos, ya que proporcionan una guía

clara y objetiva para los peritos durante el proceso de elaboración de los informes. Al seguir estos principios, los peritos pueden asegurar que sus informes sean completos, precisos y pertinentes, lo que contribuye a la justicia y la equidad en el sistema legal. Además, estos principios promueven la transparencia y la confianza en el trabajo de los peritos informáticos, lo que es crucial en un campo tan técnico y especializado.

5. Metodología

5.1 métodos

En este estudio se emplearon los siguientes enfoques de investigación:

Método Inductivo: Este enfoque se caracteriza por pasar de lo específico a lo general, lo que implica analizar casos individuales para obtener conclusiones que se puedan aplicar de manera generalizada. Es un proceso sistemático que se basa en la observación de hechos particulares para desarrollar teorías más amplias.

Método exploratorio: se emplea para abordar problemas poco estudiados o desconocidos, como la existencia y aplicación de estándares internacionales en la elaboración de informes periciales informáticos en el Sistema Integral Pericial ecuatoriano. Este tipo de investigación permite identificar y comprender mejor la problemática en cuestión, sirviendo como un primer paso para explorar e indagar sobre el tema (Escobar & Bilbao, 2020). Además, se aplica cuando se necesita obtener una visión aproximada de un objeto de estudio poco conocido o para el cual existen pocas investigaciones previas.

Método descriptivo se centra en especificar las propiedades importantes de personas, grupos, fenómenos, etc., delimitando los hechos que constituyen el problema de investigación. En este estudio, se busca comprender y describir tanto el informe pericial informático como a los peritos que lo elaboran, lo que justifica el uso de este tipo de investigación.

Método de investigación documental: se basa en la recopilación de información de diversas fuentes como libros, sitios web, datos estadísticos y tesis, con el objetivo de elaborar un marco teórico sólido y delimitar con precisión el objeto de estudio. Esto permite al investigador evitar duplicar esfuerzos al resolver problemas que ya han sido abordados previamente, así como establecer la importancia y relevancia de su estudio en comparación con otros similares (Rodríguez, 2019).

Método Deductivo: Contrariamente al método inductivo, este enfoque parte de lo general para llegar a conclusiones específicas. Se complementa con el método analítico y consiste en inferir

conclusiones a partir de principios generales, lo que ayuda a abordar problemas específicos desde un contexto más amplio.

Método Analítico: Este método implica descomponer un fenómeno o problema en sus partes constituyentes para analizarlas de manera detallada. Se centra en el estudio de las partes que conforman un todo, lo que facilita el establecimiento de nuevas teorías o conclusiones.

Método Exegético: Se trata de un enfoque que se basa en una interpretación literal de las disposiciones legales, buscando comprender el significado que el legislador les dio. Este método es relevante en la investigación al analizar diversas normas jurídicas en relación con el tema de estudio y buscar su interpretación desde su origen y contexto.

Método Hermenéutico: Este enfoque se centra en la interpretación de textos, especialmente textos jurídicos, con el fin de comprender su significado. Se busca encontrar la esencia de la ley a través de la interpretación de sus disposiciones.

Método Mayéutico: Este método implica hacer preguntas que guíen a una reflexión profunda, permitiendo descubrir conceptos que pueden no ser evidentes inicialmente. En la investigación, este enfoque facilita la dinámica de preguntas y respuestas para llegar a una comprensión más profunda del tema.

Método Estadístico: Se refiere a un conjunto de procedimientos para la recolección, análisis y presentación de datos cualitativos y cuantitativos. Implica seleccionar la población adecuada y diseñar técnicas para recopilar la información necesaria.

Método Sintético: Consiste en resumir los aspectos más relevantes de todo el proceso investigativo, destacando las conclusiones más importantes.

Método Comparativo: Este enfoque implica comparar y contrastar legislaciones para identificar similitudes y diferencias entre ellas. En este estudio, fue útil para comparar las leyes relacionadas con la repatriación y el indulto en varios países como España, México y Colombia.

5.2 Técnicas y Estrategias.

Para la recolección de datos, se emplearon diversas técnicas que se dividen en dos categorías principales:

5.2 Procedimientos y Técnicas.

Técnicas de acopio teórico documental: con el fin de recolectar de todas las identificaciones posibles tales como: datos bibliográficos, fichas bibliográficas, fichas nemotécnicas.

Técnicas de acopio empírico: También conocidas como técnicas de campo, se tiene las siguientes:

Observación Documental: Estudios de documentos fidedignos que aportan y respaldan la investigación

Encuesta: se elaboró un cuestionario que contiene preguntas claras y concretas para obtener respuestas con la finalidad de recolectar datos y una vez tabulados, se podrá conocer la opinión pública sobre la problemática planteada. Que en este caso será la aplicación de 30 encuestas a profesionales del derecho de la provincia de Loja.

Entrevista: esta técnica se realizó mediante un dialogo entre el entrevistador y el entrevistado sobre aspectos puntuales de la problemática de estudio y se realizó a 5 personas especialistas conocedoras de la problemática.

Materiales y Herramientas.

Herramientas: Grabadora, cuaderno de apuntes, fichas, retroproyector, cámara, computadora.

Materiales: Libros, diccionarios jurídicos, manuales, leyes.

Los resultados que se obtengan a través de la aplicación de los diferentes métodos y técnicas se presentarán con la ilustración de tablas, barras o gráficos y de forma pormenorizada a través del análisis de los criterios y datos concretos, que sirven para la construcción del marco teórico, verificación de los objetivos, y finalmente para determinar las conclusiones y recomendaciones referentes a la solución del problema investigado

6. Resultados

6.1 Resultados de las Encuestas

La presente técnica fue aplicada a treinta profesionales del Derecho de la ciudad de Loja, de quienes se obtuvo las siguientes respuestas:

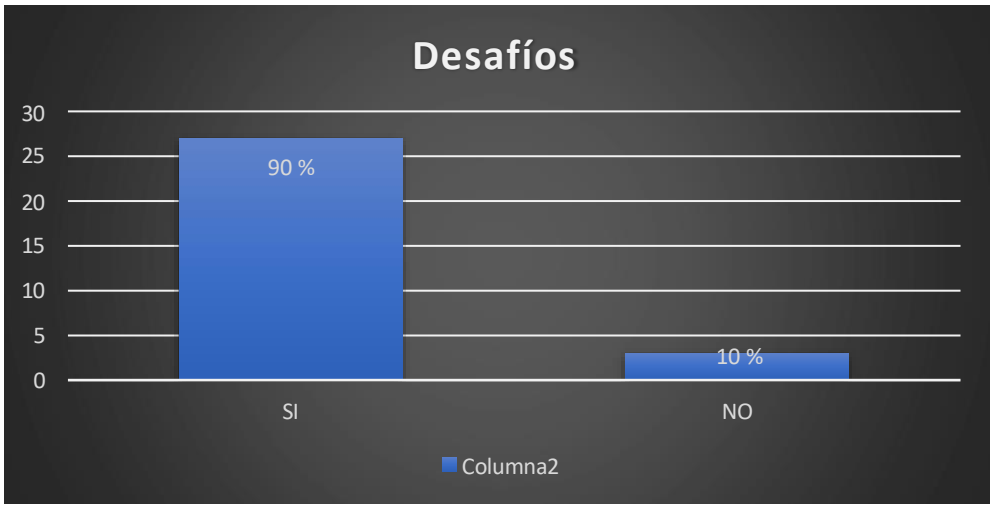
Primera pregunta: La Norma UNE 197010:2015 respecto del informe pericial sobre delitos informáticos determina la estructura y aplicabilidad de la siguiente forma: Título, Estructura Básica, Paginación, Contenido, Declaración de Tachas, Juramento o Promesa y por último Índice General. ¿Está usted de acuerdo en que en nuestro país se establezcan estos requisitos mínimos que debe contener el informe pericial sobre delitos informáticos?

Tabla N° 1.

Indicadores	Variables	Porcentaje
Si	27	**90%**
No	3	**10%**
Total	**30**	**100%**

Fuente: Profesionales del Derecho de la ciudad de Loja.
Autor: Wilman Daniel Romero Sánchez

Figura 1.



Interpretación:

En la presente pregunta se obtuvo una respuesta favorable, pues el 90% de los encuestados, es decir, veintisiete de treinta personas, están a favor de establecer los requisitos mínimos para los informes periciales sobre delitos informáticos, según la Norma UNE 197010:2015. Esto indica un amplio respaldo a la adopción de estos estándares en el país. Mientras que el 10% restante, que corresponde a tres personas de treinta encuestados, no están a favor de establecer los requisitos mínimos para los informes periciales sobre delitos informáticos, según la Norma

UNE 197010:2015, esto entendiendo que algunos de los profesionales desconocen de dicha normativa propuesta, además de que se pronunciaron con cuestionamientos sobre su eficacia para abordar los desafíos de los delitos informáticos, preocupaciones sobre la rigidez normativa, o desconfianza en el proceso de estandarización.

Análisis:

Comparto la opinión de la mayoría de los encuestados; en primer lugar, la adopción de requisitos mínimos para los informes periciales sobre delitos informáticos, basados en la Norma UNE 197010:2015, proporcionaría una guía clara y uniforme para los peritos en informática forense, lo que aumentaría la calidad y fiabilidad de los informes presentados en procesos judiciales. Además, establecer estándares mínimos podría mejorar la eficacia del sistema judicial en la investigación y resolución de delitos informáticos al proporcionar un marco sólido y consistente para la evaluación de pruebas. Del mismo modo, la adopción de estos estándares podría promover la confianza del público en el sistema judicial al garantizar que los informes periciales sean realizados de manera profesional y siguiendo pautas reconocidas internacionalmente.

Segunda pregunta: En nuestra legislación se determina como metodología para presentar informes periciales considerando los siguientes aspectos: Datos completos del perito, Información sobre la profesión, oficio o actividad especial ejercida por el perito, Número de acreditación otorgado por el Consejo de la Judicatura y la declaración de su vigencia, Explicación de los hechos u objetos analizados, Detalle de los exámenes, métodos y prácticas aplicadas en el análisis y por último Razonamientos y deducciones que condujeron a las conclusiones.

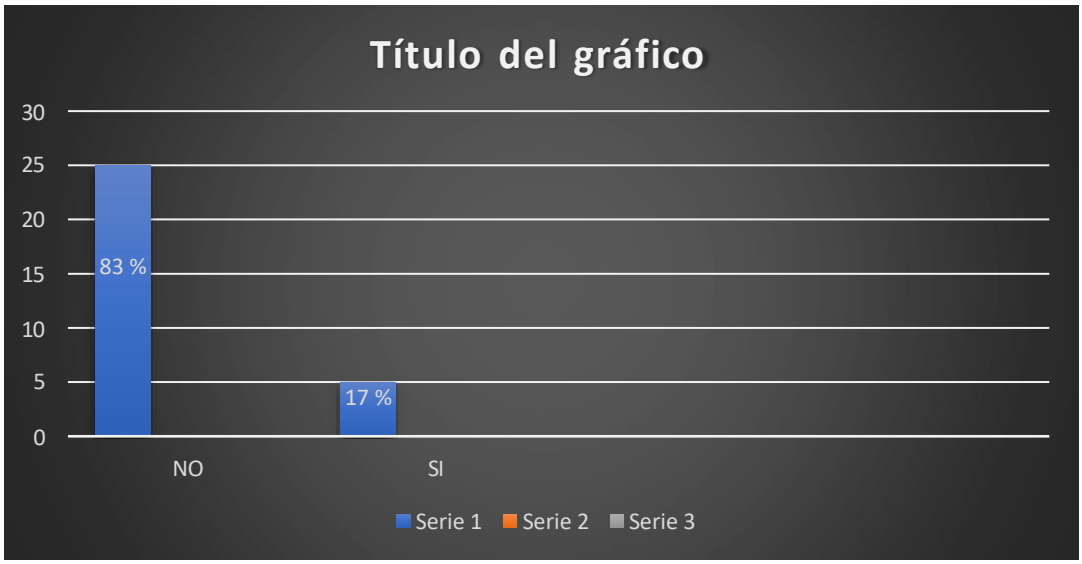
¿Cree usted que esta metodología es suficiente para la correcta administración de justicia?

Tabla N° 2.

Indicadores	Variables	Porcentaje
Si	5	**17%**
No	25	**83%**
Total	**30**	**100%**

Fuente: Profesionales del Derecho de la ciudad de Loja.
Autor: Wilman Daniel Romero Sánchez

Gráfico N° 2.



Interpretación:

En la presente pregunta se obtuvo una respuesta favorable conforme a la propuesta diseñada, puesto que el 83.33% de los encuestados, es decir, veinticinco de treinta personas, mencionan que la metodología actual en nuestro sistema de informes periciales no es suficiente. Este alto porcentaje de respaldo indica una fuerte aceptación hacia la metodología establecida en la legislación para garantizar la calidad y transparencia en la administración de justicia.

Mientras que, el 16.67% de los encuestados no está de acuerdo con la metodología propuesta para presentar informes periciales debido a posibles preocupaciones sobre su insuficiencia en abordar todos los aspectos relevantes, dudas sobre la transparencia en su aplicación, la necesidad de flexibilidad para adaptarse a casos específicos, experiencias previas negativas con metodologías similares, o simplemente por desconocimiento o falta de comprensión sobre su alcance y beneficios potenciales.

Análisis:

En mi análisis personal, estoy totalmente de acuerdo con la mayoría de los encuestados que respaldan la metodología propuesta para presentar informes periciales. Pues considero que esta alta proporción de apoyo refleja una clara necesidad y reconocimiento de la importancia de contar con una metodología robusta y detallada en nuestro sistema de informes periciales. La legislación establecida proporciona una guía clara y transparente para los peritos en la

presentación de informes, lo que garantiza la calidad y transparencia en la administración de justicia.

En cuanto al 16.67% de los encuestados que expresaron desacuerdo, entiendo que sus preocupaciones son válidas y deben ser consideradas. Sin embargo, creo firmemente que la metodología propuesta aborda adecuadamente estas preocupaciones al proporcionar un marco sólido y flexible para la presentación de informes periciales, promoviendo así la confianza en el sistema judicial y la efectividad en la resolución de casos.

Tercera pregunta: Las normas internacionales para estructurar informes periciales respecto a delitos informáticos aplicables internacionalmente son la Norma Une 19701: 2019 y la Norma Une 19701: 2015.

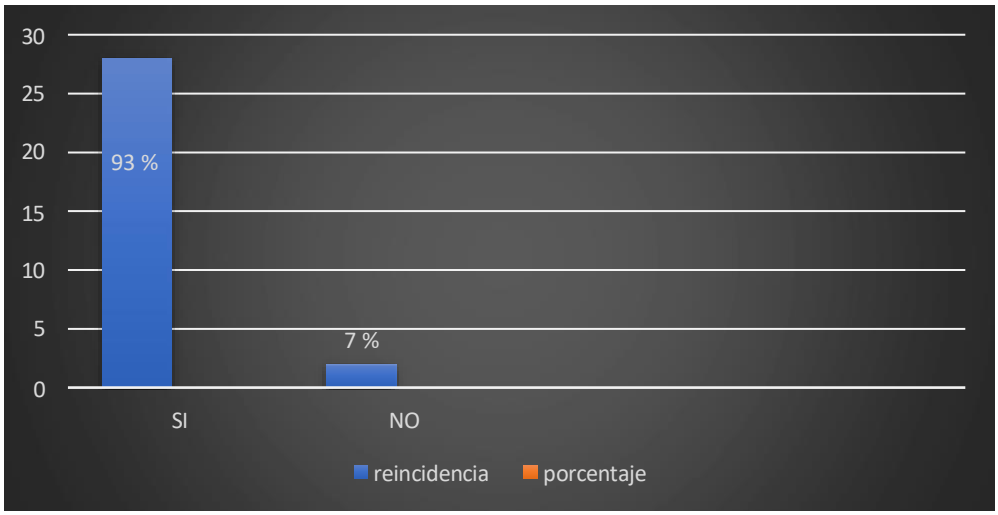
¿Está usted de acuerdo en su aplicación para efecto de estructura mínima en cuanto a informes periciales de delitos informáticos?

Tabla N° 3.

Indicadores	Variables	Porcentaje
Si	28	**93%**
No	2	**7%**
Total	**30**	**100%**

Fuente: Profesionales del Derecho de la ciudad de Loja.
Autor: Wilman Daniel Romero Sánchez

Gráfico N° 3.



Interpretación:

En la esta pregunta se obtuvo una respuesta positiva, ya que el 93.33% de los encuestados, equivalente a veintiocho de treinta personas, menciona que están de acuerdo con la aplicación de las normas internacionales, como la Norma Une 19701:2019 y la Norma Une 19701:2015, para estructurar informes periciales sobre delitos informáticos. Este alto grado de aceptación refleja un sólido respaldo hacia la adopción de estándares internacionales en el ámbito local, lo que puede contribuir a mejorar la calidad y consistencia de los informes periciales en casos de delitos informáticos.

Mientras que el 6.67%, lo que equivale a dos de los encuestados, no están de acuerdo con la aplicación de las normas internacionales para estructurar informes periciales sobre delitos informáticos. Esta minoría cuenta con ciertos argumentos reflejados en preocupaciones de que en nuestro país si existen las características suficientes para aplicar correctamente los informes periciales y no se necesita de otras normas extranjeras; sin embargo, entendemos su desacuerdo, pero la gran mayoría respalda la adopción de estándares internacionales en este ámbito.

Análisis:

Mi análisis personal refleja un fuerte respaldo hacia la aplicación de normas internacionales para estructurar informes periciales sobre delitos informáticos, respaldado por la mayoría de los encuestados que comparten esta misma perspectiva. Pues considero que, esta alta proporción de apoyo indica una amplia aceptación y reconocimiento de la importancia de establecer estándares internacionales en el ámbito local. Creo firmemente que la adopción de estas normas proporcionaría una serie de beneficios significativos.

En primer lugar, comparto con la adopción de estas normas, porque ofrecen una guía clara y consistente para los peritos, lo que garantizaría la calidad y transparencia en la administración de justicia. Además, al seguir estándares internacionales reconocidos, se promueve la coherencia y comparabilidad en los informes periciales, facilitando la cooperación y el intercambio de información a nivel internacional. Además, la adopción de estas normas podría ayudar a fortalecer el sistema judicial local al elevar los estándares y prácticas en el ámbito de la informática forense. En definitiva, estoy plenamente convencido de que la aplicación de estas normas internacionales es fundamental para mejorar la calidad y efectividad de los informes periciales sobre delitos informáticos, y estoy de acuerdo con la mayoría de los encuestados en este aspecto.

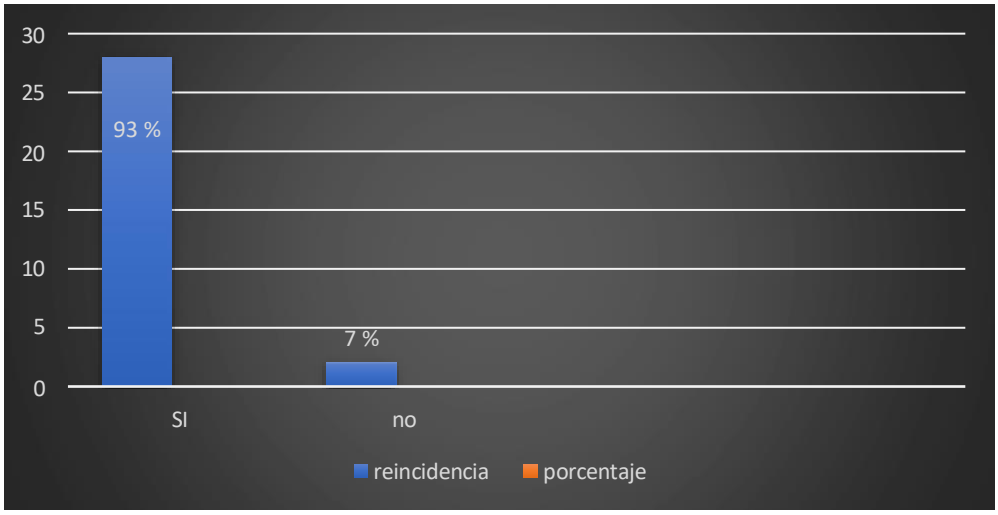
Cuarta pregunta: ¿Está usted de acuerdo en presentar un proyecto de reforma en torno al informe pericial sobre delitos informáticos para una adecuada administración de justicia?

Tabla N° 4.

Indicadores	Variables	Porcentaje
Si	28	**93%**
No	2	**7%**
Total	**30**	**100%**

Fuente: Profesionales del Derecho de la ciudad de Loja.
Autor: Wilman Daniel Romero Sánchez

Gráfico N° 4.



Interpretación:

Con respecto a la cuarta pregunta, se plantea si se está de acuerdo en presentar un proyecto reformatorio sobre el informe pericial en delitos informáticos para una administración de justicia adecuada. Los resultados obtenidos nos muestran, un enfoque favorable, puesto que 28 de 30 profesionales, lo que corresponde al 93.33% de los encuestados está a favor, mientras que el 6.67% está en desacuerdo. Desde una perspectiva jurídica, este alto nivel de acuerdo indica un reconocimiento generalizado de la importancia de establecer lineamientos claros y específicos para la elaboración de informes periciales en casos de delitos informáticos.

Esta propuesta reformatoria podría contribuir a mejorar la calidad y consistencia de los informes presentados ante los tribunales, lo que a su vez fortalecería el proceso judicial al

proporcionar una base sólida para la toma de decisiones. Del mismo modo, la adopción de esta reforma podría promover la transparencia y confianza en el sistema judicial, al establecer estándares reconocidos y aceptados para la evaluación de pruebas en casos de delitos informáticos. En conclusión, desde una perspectiva jurídica, el alto nivel de acuerdo con la propuesta de presentar un proyecto de reforma refleja un consenso en torno a la necesidad de mejorar y estandarizar los procesos relacionados con la presentación de informes periciales en el ámbito de los delitos informáticos en nuestro país.

Análisis:

Comparto con la opinión de la mayoría de los encuestados porque considero que establecer reformas en torno al informe pericial sobre delitos informáticos es fundamental para garantizar una administración de justicia adecuada en este ámbito. La elaboración de este proyecto reformatorio proporcionaría una guía clara y consistente para los peritos, lo que garantizaría la calidad y transparencia en la presentación de informes periciales ante los tribunales. Además, estas reformas podrían contribuir a mejorar la eficiencia y efectividad del proceso judicial al establecer estándares reconocidos y aceptados para la evaluación de pruebas en casos de delitos informáticos. En sí, estoy de acuerdo con la propuesta de presentar un proyecto reformatorio, ya que considero que es un paso importante hacia la mejora del sistema judicial en la investigación con respecto a los avances del peritaje informático.

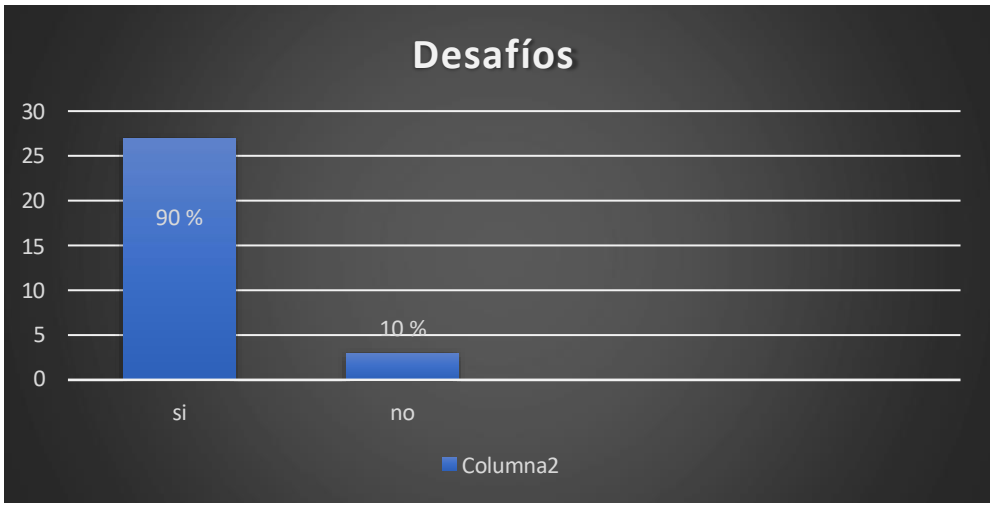
Pregunta 5: ¿Considera usted que nuestro sistema de justicia debería mejorar el formato de los informes periciales, especialmente en casos de delitos informáticos?

Tabla N° 5.

Indicadores	Variables	Porcentaje
Si	27	**90%**
No	3	**10%**
Total	**30**	**100%**

Fuente: Profesionales del Derecho de la ciudad de Loja.
Autor: Wilman Daniel Romero Sánchez

Gráfico N° 4.



Interpretación:

Esta quinta pregunta plantea si se considera que el sistema de justicia en nuestro país debería mejorar el formato de los informes periciales, especialmente en casos de delitos informáticos. La tabla muestra que el 90% de los encuestados está de acuerdo con esta afirmación, mientras que el 10% está en desacuerdo. Desde una perspectiva jurídica, este alto nivel de acuerdo indica un reconocimiento generalizado de la necesidad de mejorar el formato de los informes periciales en el ámbito de los delitos informáticos.

Este tipo de delitos suelen implicar aspectos técnicos y complejos que pueden no ser adecuadamente abordados con los formatos tradicionales de informes periciales. Por lo tanto, mejorar el formato de estos informes podría contribuir a una mejor comprensión de la evidencia por parte de los jueces, fiscales y demás actores del sistema judicial, lo que a su vez podría mejorar la calidad y eficacia de la administración de justicia en casos de delitos informáticos. Es por ello que, desde una perspectiva jurídica, considero que el alto nivel de acuerdo con la necesidad de mejorar el formato de los informes periciales en casos de delitos informáticos refleja un consenso en torno a la importancia de adaptar los procedimientos judiciales a las particularidades de este tipo de delitos.

Análisis:

Concuerdo con la mayoría de los encuestados debido a que reconocen la necesidad imperante de mejorar el formato de los informes periciales en casos de delitos informáticos. Es evidente que este tipo de delitos presenta desafíos técnicos y complejidades que no pueden abordarse adecuadamente con los formatos tradicionales de informes periciales. Mejorar el formato de estos informes permitiría una presentación más clara y comprensible de la evidencia ante los

tribunales, lo que facilitaría la toma de decisiones por parte de los jueces, fiscales y demás actores del sistema judicial. Además, una mayor claridad en la presentación de la evidencia contribuiría a una administración de justicia más eficaz y justa en casos de delitos informáticos. Por lo tanto, estoy de acuerdo en que es crucial adaptar los procedimientos judiciales para abordar adecuadamente las particularidades de los delitos informáticos y asegurar una respuesta efectiva por parte del sistema de justicia.

6.2 Resultado de las Entrevistas

La presente técnica de entrevistas fue aplicada a cinco profesionales del Derecho con especialización en derecho Penal y Derecho Informático, de quienes se obtuvo las siguientes respuestas:

Primera pregunta: La Norma UNE 197010:2015 respecto del informe pericial sobre delitos informáticos determina la estructura y aplicabilidad de la siguiente forma: Título, Estructura Básica, Paginación, Contenido, Declaración de Tachas, Juramento o Promesa y por último Índice General.

¿Está usted de acuerdo en que en nuestro país se establezcan estos requisitos mínimos que debe contener el informe pericial sobre delitos informáticos?

Respuestas:

Primer entrevistado:

Como profesional, en derecho informático, con base a lo que me ha comentado, puedo señalar que la Norma UNE 197010:2015 establece una serie de pautas y requisitos para la elaboración de informes periciales sobre delitos informáticos. Estos requisitos son fundamentales para garantizar la calidad, claridad y consistencia de los informes presentados en procesos legales relacionados con la informática y la ciberseguridad.

En cuanto a si estoy de acuerdo con el establecimiento de estos requisitos mínimos en nuestro país, puedo afirmar que la adopción de estándares como la Norma UNE 197010:2015 puede ser beneficiosa para el sistema legal y para los profesionales del derecho informático. Porque considero que, estos requisitos proporcionan una guía clara y uniforme para la elaboración de informes periciales, lo que puede mejorar la eficiencia de los procesos judiciales, facilitar la comprensión de la evidencia digital por parte de los jueces y garantizar la calidad y credibilidad

de la prueba pericial presentada ante los tribunales. Por lo tanto, en general, estoy a favor de la adopción de estándares como la Norma UNE 197010:2015 en nuestro país, siempre y cuando se adapten adecuadamente a las particularidades de nuestro sistema legal y se promueva su aplicación de manera efectiva en los procesos judiciales relacionados con delitos informáticos.

Segundo entrevistado:

Desde mi perspectiva, considero que la adopción de requisitos mínimos para los informes periciales sobre delitos informáticos, conforme a la Norma UNE 197010:2015, es un paso fundamental hacia la estandarización y la calidad en la presentación de evidencia digital en procesos legales. Lo digo porque, estos requisitos nos pueden proporcionar una estructura clara y coherente para la elaboración de informes periciales, lo que facilita la comprensión y evaluación por parte de los jueces y demás partes involucradas en el proceso judicial.

Además, el establecimiento de pautas específicas contribuye a la profesionalización de la labor pericial en el ámbito de la informática forense, garantizando que los informes presentados sean rigurosos, completos y objetivos. Asimismo, al seguir estos estándares, se promueve la transparencia y la confianza en el sistema legal, ya que se asegura que la evidencia digital sea tratada de manera adecuada y conforme a criterios reconocidos internacionalmente. Por ello, no me opondría a que se establezcan estos requisitos mínimos en nuestro país, ya que contribuyen a mejorar la calidad y la fiabilidad de la prueba pericial en casos de delitos informáticos, fortaleciendo así el Estado de derecho y la protección de los derechos de las partes involucradas.

Tercer entrevistado:

Considero que esta Norma de la que me habla, la norma UNE 197010:2015 ofrece una guía valiosa y a mi parecer más completa para la elaboración de informes periciales sobre delitos informáticos. La estructura detallada y los requisitos específicos establecidos en esta norma pueden contribuir significativamente a la claridad, coherencia y calidad de la evidencia presentada ante los tribunales. Es por eso que la adopción de estos requisitos mínimos en nuestro país podría representar un avance importante en la estandarización de la práctica pericial en el ámbito de la informática forense, porque al seguir estas directrices, los expertos en el campo pueden garantizar que sus informes sean exhaustivos, objetivos y comprensibles para todas las partes involucradas en el proceso judicial.

Del mismo modo, considero que, la aplicación de la Norma UNE 197010:2015 puede ayudar a mejorar la eficiencia y la efectividad de los procedimientos legales relacionados con delitos informáticos, al proporcionar una estructura sólida para la presentación de evidencia digital. Entonces, considero que, esto puede contribuir a una administración de justicia más justa y transparente en nuestra sociedad.

Cuarto entrevistado:

Como profesional del derecho, reconozco la importancia de establecer pautas claras y precisas para la elaboración de informes periciales en casos de delitos informáticos. Y según lo que me ha explicado, con esta norma internacional, como es la Norma UNE 197010:2015, pues veo que nos ofrece un marco estructurado que puede ayudar a garantizar la consistencia y la calidad de la evidencia presentada ante los tribunales en este ámbito tan especializado. Por lo tanto, adoptar estos requisitos mínimos en nuestro país puede fortalecer la credibilidad y la confianza en el proceso judicial, al proporcionar un estándar reconocido para la evaluación de la evidencia digital. Por ello, pienso que sería buena idea la implementación de dicha norma en nuestro país, ya que puede contribuir a mejorar la calidad y la fiabilidad de la prueba pericial en casos de delitos informáticos, lo que a su vez fortalece el Estado de derecho y garantiza los derechos fundamentales de todas las partes involucradas en el proceso judicial.

Quinto entrevistado.

Desde mi punto de vista, considero que la adopción de estándares internacionales, como la norma UNE 197010:2015, para la elaboración de estos informes periciales sobre delitos informáticos, es una medida positiva que puede beneficiar nuestro sistema legal de diversas maneras. Por ejemplo, al aprovechar los estándares internacionales, nuestro país puede alinearse con las mejores prácticas reconocidas a nivel global en el campo de la informática forense. Y esto no solo garantiza la calidad y la consistencia de los informes periciales presentados ante los tribunales, sino que también facilita la cooperación y el intercambio de información con otras jurisdicciones en casos transnacionales de ciberdelitos. Entonces, es una idea que se debería considerar conforme a lo que permite nuestra legislación, desde luego.

Comentario del autor:

Estoy de acuerdo con los entrevistados y con la propuesta planteada porque considero que la adopción de estándares internacionales, como la Norma UNE 197010:2015, para la elaboración de informes periciales sobre delitos informáticos, representa un avance significativo en la

mejora de nuestro sistema legal en el ámbito de la ciberseguridad. En primer lugar, comparto con los comentarios, porque estos estándares ofrecen una guía clara y completa para la elaboración de informes periciales, lo que garantiza la calidad, claridad y consistencia de la evidencia digital presentada ante los tribunales. Esto es crucial para una correcta administración de justicia en casos de delitos informáticos, donde la complejidad de la evidencia digital requiere un enfoque especializado y riguroso.

Además, la adopción de estándares internacionales promueve la profesionalización de la labor pericial en el ámbito de la informática forense, alineándonos con las mejores prácticas reconocidas a nivel global. Esto no solo fortalece la credibilidad y la confianza en nuestro sistema legal, sino que también facilita la cooperación y el intercambio de información con otras jurisdicciones en casos transnacionales de ciberdelitos. Asimismo, considero que la implementación de estos estándares contribuiría a una administración de justicia más eficiente y transparente en el ámbito de la ciberseguridad, promoviendo la protección de los derechos fundamentales de todas las partes involucradas en el proceso judicial. Por ello, estoy de acuerdo con los entrevistados y con la propuesta planteada porque considero que la adopción de estándares internacionales para la elaboración de informes periciales sobre delitos informáticos es un paso positivo hacia la mejora de nuestro sistema legal en este ámbito tan importante.

Segunda pregunta: En nuestra legislación se determina como metodología para presentar informes periciales considerando los siguientes aspectos: Datos completos del perito, Información sobre la profesión, oficio o actividad especial ejercida por el perito, Número de acreditación otorgado por el Consejo de la Judicatura y la declaración de su vigencia, Explicación de los hechos u objetos analizados, Detalle de los exámenes, métodos y prácticas aplicadas en el análisis y por último Razonamientos y deducciones que condujeron a las conclusiones.

¿Cree usted que esta metodología es suficiente para la correcta administración de justicia?

Respuestas:

Primer entrevistado:

Primeramente, debo reconocer que la metodología para presentar informes periciales establecida en nuestra legislación, sí aborda ciertos aspectos importantes que deben ser considerados para garantizar la validez y la eficacia de la evidencia digital en los procesos

judiciales. Sin embargo, es necesario reconocer que la calidad de las pericias informáticas en nuestro país puede ser deficiente en algunos casos.

Como segundo punto, la metodología propuesta incluye elementos esenciales, como la identificación completa del perito, su experiencia y acreditación, así como una explicación detallada de los métodos utilizados en el análisis y las deducciones que conducen a las conclusiones. Estos aspectos son fundamentales para que los informes periciales sean claros, comprensibles y confiables para los jueces y demás partes involucradas en el proceso judicial. No obstante, la suficiencia de esta metodología para la correcta administración de justicia depende en gran medida de la calidad de la ejecución de los informes periciales por parte de los expertos en informática forense. En muchos casos, la falta de formación especializada, recursos adecuados y supervisión puede resultar en informes periciales deficientes que no cumplen con los estándares necesarios para respaldar una decisión judicial justa y precisa.

Por lo tanto, yo creo que, si bien la metodología establecida en nuestra legislación es un paso en la dirección correcta, diría que, es necesario fortalecer los mecanismos de capacitación, supervisión y control de calidad en el ámbito de la informática forense para garantizar que los informes periciales cumplan con los más altos estándares de integridad y fiabilidad. Solo así se podrá asegurar una correcta administración de justicia en los casos que involucren evidencia digital.

Segundo entrevistado:

Yo considero que la metodología establecida en nuestra legislación para la presentación de informes periciales sobre evidencia digital es un primer paso hacia la correcta administración de justicia en casos que involucren delitos informáticos. Sin embargo, es importante reconocer que la mera adopción de una metodología no garantiza la calidad de los informes periciales. En muchos casos, la falta de recursos, capacitación especializada y supervisión adecuada puede resultar en informes periciales deficientes que no cumplen con los estándares necesarios para respaldar una decisión judicial precisa y justa.

Entonces, se podría decir que, aunque la metodología establecida en nuestra legislación proporciona un marco útil para la presentación de informes periciales, es importante que los peritos en informática cuenten con los recursos y el apoyo necesarios para realizar su trabajo de manera efectiva. Esto incluye capacitación continua, acceso a herramientas y tecnologías adecuadas, así como supervisión y revisión por parte de colegas y expertos en el campo. Solo así se podrá garantizar que la evidencia digital presentada ante los tribunales sea confiable y

pueda contribuir de manera significativa a la administración de justicia en casos de delitos informáticos.

Tercer entrevistado

Yo veo a la metodología que nuestra legislación establece para los informes periciales sobre delitos informáticos como una buena señal. Es como una especie de guía que nos ayuda a presentar la evidencia digital de manera más ordenada y comprensible ante los tribunales. Entonces, los detalles que menciona la metodología, como identificar bien al perito, explicar cómo se hicieron los análisis y cómo llegamos a nuestras conclusiones, son como los ingredientes esenciales para preparar una buena receta. Sin ellos, el informe pericial podría ser un poco confuso y poco convincente.

Pero, es importante entender que la calidad de estos informes depende mucho de la habilidad y la experiencia de los peritos. Es como cuando tienes la receta perfecta, pero si no sabes cocinar, el resultado no será el mejor. Por eso, para que todo funcione como debe ser, es crucial que los peritos estén bien preparados y tengan acceso a las herramientas adecuadas. En sí, la metodología es la que nos guía en el proceso de presentar la evidencia digital ante los tribunales, pero para que realmente funcione, necesitamos peritos bien entrenados, buenas herramientas y una supervisión adecuada. De esa manera, podremos contribuir a una administración de justicia más eficiente y precisa en el ámbito de los delitos informáticos.

Cuarto entrevistado:

Los requisitos presentados en nuestra legislación para los informes periciales están bien porque proporcionan una estructura clara y detallada que guía a los peritos en informática en la presentación de evidencia digital ante los tribunales. La completa identificación del perito, la explicación detallada de los métodos utilizados en el análisis y las conclusiones derivadas de estos procesos son elementos fundamentales que garantizan la integridad y la credibilidad de la evidencia presentada. Además, estos requisitos ayudan a asegurar que los informes periciales sean comprensibles para los jueces y otras partes involucradas en el proceso judicial, lo que contribuye a una toma de decisiones más informada y justa. Al seguir esta metodología, se promueve la consistencia en la presentación de la evidencia digital, lo que es crucial para la correcta administración de justicia en casos de delitos informáticos, pero si los estándares internacionales nos aportan con métodos y requisitos más estrictos sería óptimo para mejorar la eficiencia y credibilidad en nuestra administración de justicia.

Quinto entrevistado:

Creo que sería beneficioso adoptar las normas internacionales en nuestro país para los informes periciales sobre delitos informáticos. Lo digo, porque generalmente, estas normas tienden a ser más completas y detalladas, lo que podría mejorar la calidad y la consistencia de la evidencia digital presentada ante los tribunales. Además, al alinearnos con estándares internacionales reconocidos, podríamos facilitar la cooperación y el intercambio de información con otras jurisdicciones en casos transnacionales de ciberdelitos. Esto sería especialmente útil en un mundo cada vez más interconectado donde los delitos informáticos pueden tener repercusiones globales.

Otro aspecto a considerar es que seguir normas internacionales puede ayudar a fortalecer la credibilidad y la confianza en nuestro sistema legal, tanto a nivel nacional como internacional; esto porque, los estándares internacionales suelen ser desarrollados por expertos de diferentes países y representan las mejores prácticas en el campo de la informática forense.

Comentario del autor:

Comparto con la mayoría de los entrevistados porque refleja una necesidad importante de mejorar la calidad y la consistencia de los informes periciales sobre delitos informáticos en nuestro país. Como se ha señalado, la metodología establecida en nuestra legislación aborda ciertos aspectos cruciales para garantizar la validez y la eficacia de la evidencia digital en los procesos judiciales relacionados con la informática y la ciberseguridad. Sin embargo, es necesario reconocer que la calidad de las pericias informáticas puede ser deficiente en algunos casos, lo que resalta la importancia de fortalecer los mecanismos de capacitación, supervisión y control de calidad en este ámbito. Además, la adopción de estándares internacionales, como la Norma UNE 197010:2015, podría mejorar significativamente la calidad y la consistencia de la evidencia presentada ante los tribunales, alineándonos con las mejores prácticas reconocidas a nivel global en el campo de la informática forense.

Por otro lado, seguir normas internacionales también puede facilitar la cooperación y el intercambio de información con otras jurisdicciones en casos transnacionales de ciberdelitos, lo que es crucial en un mundo cada vez más interconectado. Además, esto contribuiría a fortalecer la credibilidad y la confianza en nuestro sistema legal, tanto a nivel nacional como internacional. Por lo antes expuesto, estoy de acuerdo en que la adopción de estándares

internacionales y el fortalecimiento de los mecanismos de calidad en la elaboración de informes periciales sobre delitos informáticos son pasos necesarios para mejorar nuestra administración de justicia en este ámbito tan especializado y relevante en la era digital.

Tercera pregunta:

Las normas internacionales para estructurar informes periciales respecto a delitos informáticos aplicables internacionalmente son la Norma Une 19701: 2019 y la Norma Une 19701: 2015.

¿Está usted de acuerdo en su aplicación para efecto de estructura mínima en cuanto a informes periciales de delitos informáticos?

Respuestas:

Primer entrevistado:

Reconozco la importancia de contar con normas internacionales que establezcan pautas para la estructuración de informes periciales respecto a delitos informáticos. Como me comenta, estas normas UNE 19701:2019 y UNE 19701:2015 son ejemplos de tales normativas y ofrecen una base sólida para la elaboración de informes periciales en este ámbito.

Entonces, estoy de acuerdo en su aplicación para establecer una estructura mínima en cuanto a informes periciales de delitos informáticos. Porque, estas normas proporcionan una guía clara y detallada sobre los aspectos que deben incluirse en dichos informes, desde la identificación del perito hasta la explicación de los métodos utilizados en el análisis de la evidencia digital y las conclusiones derivadas de estos procesos.

Segundo entrevistado:

Considero que, al adoptar estas normas internacionales, se promueve la uniformidad y la consistencia en la presentación de evidencia digital en procesos judiciales relacionados con delitos informáticos, lo que facilita la comprensión y evaluación por parte de los jueces y demás partes involucradas en el proceso judicial. Además, al alinearnos con estándares internacionales reconocidos, podemos mejorar la calidad y la credibilidad de la evidencia presentada ante los tribunales, lo que contribuye a una administración de justicia más efectiva en el ámbito de la ciberseguridad. Por ello, considero que la aplicación de las normas UNE 19701:2019 y UNE 19701:2015 para establecer una estructura mínima en cuanto a informes periciales de delitos informáticos es fundamental para garantizar la integridad y la eficacia de la evidencia digital en los procesos judiciales, y, por lo tanto, estoy de acuerdo en su aplicación.

Tercer entrevistado:

Por como veo, estas normativas nos ofrecen una guía útil y reconocida internacionalmente para la elaboración de informes periciales en el ámbito de la informática forense, lo que puede contribuir a mejorar la calidad y la consistencia de la evidencia presentada ante los tribunales en casos relacionados con delitos informáticos. Además, al seguir estándares internacionales, se facilita la comparación y la cooperación con otros países en asuntos de ciberseguridad y delitos informáticos, lo que es crucial en un mundo cada vez más interconectado.

Sin embargo, es importante tener en cuenta que estas normas deben adaptarse adecuadamente a las particularidades de nuestro sistema legal y a las necesidades específicas de los casos de delitos informáticos en nuestro país. Además, la aplicación de estas normas no debe limitar la discrecionalidad y el juicio del perito en la elaboración de informes periciales, ya que cada caso puede presentar sus propias complejidades y peculiaridades.

Cuarto entrevistado:

Considero que, si bien estas normativas que me presenta, nos ofrecen una guía sólida y reconocida a nivel internacional para la elaboración de informes periciales en el ámbito de la informática forense, es importante tener en cuenta que cada jurisdicción tiene sus propias particularidades legales y procedimentales. Por lo tanto, la aplicación de estas normas debe realizarse con precaución y adaptarse adecuadamente a las leyes y prácticas locales.

Entonces, por ello es crucial considerar que la tecnología y las prácticas en el campo de la informática forense están en constante evolución. Por lo tanto, las normativas internacionales pueden quedarse obsoletas o no abordar completamente los avances más recientes en el campo. En este sentido, es necesario mantener una actualización constante de las normativas y adaptarlas según sea necesario para garantizar su relevancia y eficacia. Pero sí, considero que estas metodologías, de informes periciales son más completas y sería importante tomarlos en cuenta.

Quinto entrevistado:

Considero que la aplicación de normas internacionales para estructurar informes periciales de delitos informáticos podrían ser una opción interesante, aunque con algunos matices que considerar. Estas normativas ofrecen una especie de "manual de instrucciones" reconocido a

nivel global para elaborar informes periciales en el campo de la informática forense. Es como tener una hoja de ruta que guía a los peritos en el proceso de presentar evidencia digital en casos judiciales.

Sin embargo, es importante recordar que cada país tiene sus propias leyes y formas de aplicarlas, por lo que estas normas internacionales no son una talla única que sirva para todos. Se deben adaptar a la realidad local y a las particularidades de cada caso. Además, la tecnología avanza a pasos agigantados, lo que significa que estas normas pueden quedarse un poco rezagadas si no se actualizan con regularidad. Por lo tanto, es importante mantener un ojo en las últimas tendencias y ajustar las normativas según sea necesario. Pero fuera de ello, me parece que serían un paso interesante, si están enfocadas en mejorar la credibilidad de los informes periciales en nuestro sistema de justicia.

Comentario del autor:

Comparto con los entrevistados la opinión de que la aplicación de normas internacionales para estructurar informes periciales de delitos informáticos puede ser beneficiosa por varias razones. En primer lugar, porque estas normativas proporcionan una guía sólida y reconocida a nivel global para la elaboración de informes periciales en el ámbito de la informática forense, por ello, al seguir estas normas, se promueve la consistencia y la calidad en la presentación de evidencia digital ante los tribunales, lo que facilita la comprensión y evaluación por parte de los jueces y demás partes involucradas en el proceso judicial.

Además, la aplicación de normas internacionales puede facilitar la cooperación y el intercambio de información con otras jurisdicciones en casos transnacionales de ciberdelitos, lo que es crucial en un mundo cada vez más interconectado. Por otro lado, se reconoce la importancia de adaptar estas normativas a las particularidades de nuestro sistema legal y a las necesidades específicas de cada caso y jurisdicción. Es crucial mantener una actualización constante de estas normas para reflejar los avances tecnológicos y las nuevas tendencias en el campo de la informática forense. Por lo antes expuesto estoy de acuerdo con los entrevistados en que la aplicación de normas internacionales para estructurar informes periciales de delitos informáticos puede ser beneficiosa para mejorar la calidad y la consistencia de la evidencia digital presentada ante los tribunales, siempre y cuando se realice de manera cuidadosa y adaptada a las circunstancias locales.

Cuarta pregunta: ¿Está usted de acuerdo en presentar un proyecto de reforma en torno al informe pericial sobre delitos informáticos para una adecuada administración de justicia?

Respuestas:

Primer entrevistado:

Sí, estoy de acuerdo en presentar una propuesta reformatoria en torno al informe pericial sobre delitos informáticos si se busca garantizar una adecuada administración de justicia. Establecer pautas claras y precisas para la elaboración de informes periciales en este ámbito es fundamental para asegurar la calidad, la consistencia y la fiabilidad de la evidencia digital presentada ante los tribunales.

Esta propuesta reformatoria puede ayudar a mejorar la eficiencia y la efectividad de los procesos judiciales relacionados con delitos informáticos, al proporcionar una estructura sólida y reconocida internacionalmente para la presentación de evidencia digital, finalmente, contribuirían a fortalecer el Estado de derecho y a garantizar los derechos fundamentales de todas las partes involucradas en el proceso judicial.

Segundo entrevistado:

Sí, concuerdo con esa propuesta, porque la presentación de un proyecto de reforma en torno al informe pericial sobre delitos informáticos sería interesante para garantizar una adecuada administración de justicia en un contexto cada vez más digitalizado. Lo digo porque este tipo de propuestas proporcionan una estructura clara y coherente para la elaboración de informes periciales, lo que ayuda a los peritos en informática forense a presentar evidencia digital de manera consistente y comprensible ante los tribunales. Además, se puede considerar que estas pautas contribuyen a la profesionalización de la labor pericial en el ámbito de la informática forense, asegurando que los informes periciales sean rigurosos, completos y objetivos. Al seguir estos estándares, se promueve la transparencia y la confianza en el sistema legal, ya que se asegura que la evidencia digital sea tratada de manera adecuada y conforme a criterios reconocidos internacionalmente.

Tercer entrevistado:

Si, concuerdo con su propuesta, sería útil y oportuno más que nada porque una propuesta o proyecto reformatorio puede ayudar a mejorar la eficiencia y la efectividad de los procedimientos legales relacionados con delitos informáticos, al proporcionar una estructura sólida para la presentación de evidencia digital. Esto puede resultar en una administración de

justicia más justa y transparente, protegiendo así los derechos de todas las partes involucradas en el proceso judicial. Entonces, como decía, la presentación de una ley reformatoria en torno al informe pericial sobre delitos informáticos es fundamental para garantizar la calidad, la consistencia y la fiabilidad de la evidencia digital presentada ante los tribunales, así como para fortalecer el Estado de derecho y proteger los derechos fundamentales de todas las partes involucradas.

Cuarto entrevistado:

Por supuesto, estoy a favor de presentar el respectivo proyecto de reforma a la norma pertinente, en torno al informe pericial sobre delitos informáticos. Primeramente, porque estas pautas son cruciales para establecer un marco claro y coherente que guíe a los peritos en informática forense en la presentación de evidencia digital ante los tribunales. Al proporcionar directrices claras sobre la estructura, contenido y metodología de los informes periciales, se mejora la calidad y la consistencia de la evidencia presentada, lo que a su vez fortalece la credibilidad del proceso judicial en casos de delitos informáticos.

Asimismo, estos proyectos de investigación con propuestas de reforma pueden contribuir de cierta manera a la actualización y profesionalización del campo de la informática forense al alinear las prácticas periciales con los estándares internacionales reconocidos. Esto garantiza que los informes periciales sean rigurosos, completos y objetivos, lo que aumenta la confianza en la integridad del proceso judicial.

Quinto entrevistado:

Comparto con esta propuesta; yo considero interesante la presentación de proyectos de reformas a la norma en torno al informe pericial sobre delitos informáticos. Puesto que, estas cosas nos ofrecen una especie de "hoja de ruta" para los peritos en informática forense, proporcionando directrices claras sobre cómo estructurar y presentar la evidencia digital ante los tribunales. Entonces, al seguir estos lineamientos, se mejora la calidad y la coherencia de los informes periciales, lo que a su vez fortalece la integridad del proceso judicial en casos de delitos informáticos.

Además, al proporcionar un marco comúnmente aceptado, estos proyectos reformatorios facilitan la comprensión y la evaluación de la evidencia por parte de los jueces y otras partes involucradas en el caso. Entonces, se podría decir que, la presentación de lineamientos propositivos en torno al informe pericial sobre delitos informáticos es esencial para garantizar

un proceso judicial justo y transparente en un mundo cada vez más digitalizado. Sobre todo, porque estos lineamientos proporcionan una base sólida para la presentación de evidencia digital, promoviendo así la equidad y la confianza en el sistema legal.

Quinta pregunta:

¿Qué sugerencias daría usted frente al problema planteado?

Respuestas:

Primer entrevistado:

Desde mi perspectiva, yo sugiero la implementación de medidas para estandarizar los formatos de los informes periciales informáticos en Ecuador con el objetivo de fortalecer la credibilidad en el sistema de justicia. Esta sugerencia se fundamenta en varios aspectos cruciales que afectan directamente la eficacia y la confianza en los procesos judiciales relacionados con delitos informáticos. Primero, la estandarización de formatos brinda una guía clara y uniforme para la presentación de la información en los informes periciales. Esto permite una organización coherente de los datos, facilitando su comprensión tanto para los jueces como para las partes involucradas en el proceso judicial. Al contar con secciones claramente definidas para la descripción de los hechos, los métodos utilizados en el análisis, las conclusiones alcanzadas y las recomendaciones pertinentes, se evitan confusiones y se mejora la evaluación de la evidencia digital.

Además, la estandarización fomenta la consistencia en la presentación de los informes periciales, lo que contribuye a la equidad y la imparcialidad en el proceso judicial. Al seguir un formato común, se minimiza la posibilidad de sesgos o interpretaciones subjetivas, garantizando así una evaluación objetiva de la evidencia por parte de los jueces y demás actores judiciales. Otro punto relevante es que la estandarización facilita la comparación y el análisis de múltiples informes periciales. Los profesionales del derecho y los peritos en informática forense pueden revisar y contrastar los informes de manera más eficiente cuando siguen un mismo formato, lo que agiliza el proceso de toma de decisiones judiciales y aumenta la confianza en la calidad de la evidencia presentada.

Segundo entrevistado

Desde mi perspectiva profesional, puedo sugerir a la formación especializada de los peritos informáticos, porque este rol juega un papel crucial en la mejora del sistema de justicia en

Ecuador en lo que respecta a los informes periciales informáticos. La capacitación de los peritos en informática forense es fundamental para mantenerlos actualizados sobre las últimas técnicas y herramientas disponibles en el campo. Esta formación les permite enfrentar los desafíos cambiantes de la tecnología y realizar análisis más precisos y completos de la evidencia digital.

Además, considero que, es importante fomentar la colaboración entre expertos en derecho penal y en informática forense. La integración de conocimientos y perspectivas de ambas disciplinas garantiza la integridad y la precisión de los informes periciales. Los expertos en derecho penal pueden proporcionar orientación sobre las implicaciones legales de la evidencia digital, mientras que los peritos en informática forense pueden ofrecer su experiencia técnica para interpretar y analizar la evidencia de manera adecuada. Esta colaboración interdisciplinaria contribuye a la calidad y la fiabilidad de los informes periciales, fortaleciendo así la credibilidad del sistema de justicia en Ecuador. Además, promueve una comprensión más completa y precisa de la evidencia digital por parte de los jueces y demás actores judiciales, lo que facilita la toma de decisiones informadas y justas en casos de delitos informáticos.

Tercer entrevistado

Yo podría recomendar, a parte de su propuesta en torno a los lineamientos propositivos de adopción de la norma internacional, es importante asegurar la transparencia y la objetividad en los informes periciales informáticos para fortalecer la credibilidad del sistema de justicia en Ecuador. Los informes deben ser claros y transparentes en cuanto a los métodos utilizados y los resultados obtenidos, evitando cualquier sesgo o interpretación subjetiva que pueda afectar la imparcialidad de la evaluación.

Asimismo, Considero que, para garantizar la objetividad de los peritos, es importante implementar medidas que promuevan la divulgación de posibles conflictos de interés. Esto implica que los peritos deben revelar cualquier relación o interés personal que puedan tener con las partes involucradas en el caso, lo que ayuda a prevenir cualquier influencia indebida en el proceso de análisis y evaluación de la evidencia digital.

La transparencia y la objetividad son pilares fundamentales para la integridad y la confianza en los informes periciales, ya que aseguran que la evaluación de la evidencia se realice de manera imparcial y basada en criterios objetivos. Porque creo que, al implementar estas

medidas, se puede fortalecer la credibilidad del sistema de justicia en Ecuador y se garantiza una evaluación justa y precisa de los casos relacionados con delitos informáticos.

Cuarto entrevistado

Mi recomendación sería, que el Estado ecuatoriano tome acción en la implementación de un proceso de revisión y supervisión de los informes periciales en el ámbito de la informática forense, para garantizar su calidad y fiabilidad en el sistema de justicia ecuatoriano. Establecer un mecanismo de revisión por parte de colegas o comités especializados en esta área permite identificar posibles errores o inconsistencias en los informes presentados, lo que contribuye a fortalecer la integridad del proceso judicial.

Es importante tomar en cuenta estas medidas, puesto que, la revisión y supervisión de los informes periciales nos ofrecen una capa adicional de control de calidad, asegurando que la evidencia digital presentada ante los tribunales sea precisa y confiable. Los colegas o comités especializados en informática forense tienen el conocimiento y la experiencia necesarios para detectar posibles fallos en los análisis realizados, así como para evaluar la coherencia y consistencia de las conclusiones alcanzadas. Además, este proceso de revisión promueve la transparencia y la confianza en el sistema de justicia, al demostrar un compromiso con la excelencia y la objetividad en la presentación de la evidencia digital. Los informes periciales revisados y supervisados inspiran mayor confianza tanto en los jueces como en las partes involucradas en el proceso judicial, lo que contribuye a una toma de decisiones más informada y justa.

Quinto entrevistado

La propuesta planteada con respecto a la adopción de las normas y protocolos internacionales me parece muy buena, ahora ante eso yo recomendaría desde mi perspectiva, que la actualización constante de los formatos y prácticas relacionadas con dichos informes periciales es un aspecto fundamental en el contexto de la informática forense en Ecuador. Esto porque el rápido avance de la tecnología exige que los procedimientos y estándares utilizados en la elaboración de informes periciales se adapten continuamente para reflejar los últimos desarrollos en este campo especializado.

La evolución constante de la tecnología plantea nuevos desafíos y oportunidades en la investigación y análisis de evidencia digital. Por lo tanto, es esencial que los peritos en

informática forense se mantengan actualizados sobre las últimas herramientas, técnicas y metodologías disponibles para realizar análisis precisos y completos. Del mismo modo, la actualización regular de los formatos de informes periciales permite incorporar nuevas secciones o elementos que sean relevantes para la evaluación de la evidencia digital. Esto asegura que los informes sean exhaustivos y aborden adecuadamente los aspectos clave de la investigación, lo que aumenta su utilidad y credibilidad ante los tribunales.

Entonces, en este contexto, sí recomendaría la actualización constante también porque refleja un compromiso con la excelencia y la mejora continua en la práctica de la informática forense. Al mantenerse al día con los avances tecnológicos y las mejores prácticas en el campo, los peritos pueden ofrecer un servicio de mayor calidad y relevancia para la administración de justicia en Ecuador.

Comentario del autor:

Desde mi punto de vista, comparto plenamente las sugerencias y opiniones expresadas por los entrevistados en relación con la mejora de los informes periciales informáticos en Ecuador. La estandarización de formatos propuesta por algunos entrevistados es fundamental para proporcionar una estructura clara y coherente en la presentación de la evidencia digital ante los tribunales. Además, estoy de acuerdo en que la formación especializada y la colaboración interdisciplinaria entre expertos en derecho penal e informática forense son elementos esenciales para garantizar la calidad y la objetividad de los informes periciales.

Del mismo modo, considero relevante la sugerencia de establecer un proceso de revisión y supervisión de los informes periciales por parte de colegas especializados, ya que esto contribuiría a detectar posibles errores o inconsistencias, mejorando así la integridad del sistema judicial. La necesidad de una actualización constante de los formatos y prácticas relacionadas con los informes periciales también coincide con mi opinión, dado el rápido avance tecnológico y la importancia de mantenerse al día con las últimas tendencias en el campo de la informática forense.

Personalmente, sugiero la adopción de la Norma UNE 197010:2015 en Ecuador porque considero que proporciona un marco estructurado y detallado para la elaboración de informes periciales sobre delitos informáticos. Considero oportuna esta sugerencia porque esta norma

internacional ofrece pautas claras y específicas que pueden mejorar la calidad y la consistencia de la evidencia digital presentada ante los tribunales.

Cabe recalcar que, esta Norma UNE 197010:2015 establece requisitos mínimos para la elaboración de informes periciales que abordan aspectos importantes como la identificación del perito, la descripción de los métodos utilizados en el análisis y las conclusiones alcanzadas. Al adoptar esta norma, se promueve la estandarización de las prácticas periciales en el ámbito de la informática forense, lo que facilita la comprensión y evaluación de la evidencia digital por parte de los jueces y demás partes involucradas en el proceso judicial.

Finalmente considero que, la adopción de la Norma UNE 197010:2015 podría contribuir a alinear las prácticas periciales en Ecuador con estándares internacionales reconocidos, lo que fortalecería la credibilidad del sistema de justicia en el país. Al seguir esta norma, se fomenta la transparencia, la objetividad y la calidad en la presentación de evidencia digital, aspectos fundamentales para garantizar una administración de justicia justa y efectiva en casos de delitos informáticos.

6.3 Estudio de casos

Caso No. 1

1. Datos Referenciales:

- Juicio Nro: 0928620146178
- Victima: J.V.
- Demandado: Banco Pichincha
- Acción: Contravenciones a la ley orgánica de defensa del consumidor
- Juzgado: UNIDAD JUDICIAL NORTE 2 PENAL CON SEDE EN EL CANTÓN GUAYAQUIL, PROVINCIA DEL GUAYAS
- Fecha: Guayaquil, miércoles uno de febrero del dos mil veinte y tres.

2. Antecedentes

En marzo de 2020, en Guayaquil, se llevó a cabo una audiencia judicial relacionada con un caso de defensa del consumidor contra el Banco Pichincha. El proceso inició en 2018 con una

apelación a la resolución de un juez de la Unidad Judicial Norte No. 2 de Guayaquil. Por lo que, el Juez de Contravenciones declara su competencia para conocer y juzgar las infracciones contempladas en la Ley Orgánica de Defensa del Consumidor. Se destaca la importancia de administrar justicia conforme a la Constitución, los derechos humanos y la ley.

La denuncia presentada por J.V, representante legal de la compañía Austro Distribuciones Austrodis, Cía. Ltda., por un servicio defectuoso del Banco Pichincha. Se menciona un fraude electrónico, la falta de respuesta del banco y la apelación de la sentencia inicial que declaró con lugar la denuncia. Pues, durante el proceso, se discuten temas como la responsabilidad del banco, la implementación de medidas de seguridad, y se destaca la falta de cumplimiento de normativas. La parte denunciante busca una indemnización y acusa al banco de vender un servicio defectuoso.

Posteriormente la audiencia de apelación y la presentación de argumentos tanto de la defensa del Banco Pichincha como del denunciante, continua con que, la parte denunciante solicita la ratificación de la sentencia que declaró culpable al banco por prestar un mal servicio. La decisión del juez se considera crucial para establecer jurisprudencia en casos similares de usuarios perjudicados por el sistema bancario. El denunciante mantiene una relación proveedor-usuario con el Banco Pichincha, específicamente utilizando el servicio "Cash Management" para transferencias electrónicas; por lo que alega una transferencia no autorizada desde su cuenta, generando un perjuicio económico.

Ante este hecho, se invoca a la Ley Orgánica de Defensa del Consumidor, destacando los derechos fundamentales del consumidor, incluyendo la reparación e indemnización por servicios defectuosos. Por su parte, el Banco Pichincha argumenta que fue víctima de la delincuencia común, desvinculándose de responsabilidad.

Por tal motivo, la evidencia técnica se centra en utilización de peritajes informáticos donde se investigó la dirección IP utilizada para la transferencia fraudulenta, señalando discrepancias entre la ubicación habitual de la empresa y la dirección IP de Perú asociada al fraude. La perita informática destacó la falta de personalización y medidas de seguridad según la normativa.

Por su parte, el juzgador subraya las debilidades del sistema del banco, haciendo énfasis en la falta de respuesta a eventos fraudulentos y la posibilidad de prevenir el fraude electrónico. Concluyendo que el Banco Pichincha prestó un mal servicio al no cumplir con las normativas de seguridad, respaldando la posición de la denunciante y destacando las deficiencias tecnológicas que permitieron el fraude informático. Posteriormente, la resolución destaca que

el Banco Pichincha incumplió con las normativas de seguridad al no implementar medidas de personalización, lo que habría evitado la transferencia ilegal. La falta de adecuación a la dirección IP habitual de la empresa y la carencia de alarmas ante eventos fraudulentos señalan debilidades y vulnerabilidades en los sistemas de seguridad del banco. Por lo tanto, la conclusión es que el Banco Pichincha proporcionó un servicio administrativo defectuoso y un producto "Cash Management" inadecuado a la Compañía Austro Distribuciones.

3. Resolución

Por lo anteriormente expuesto, el infrascrito Juez de esta Unidad Judicial Penal Norte 2 de Guayaquil, ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR, POR AUTORIDAD DE LA CONSTITUCION Y LAS LEYES DE LA REPUBLICA, declara con lugar la denuncia presentada por J.V, por los derechos que representa de Austro Distribuciones Austrodis C. Ltda, en contra del Banco Pichincha C. A, a quien de conformidad con el Art. 75 de la Ley Orgánica de Defensa del Consumidor, le impone la multa de quinientos dólares de los Estados Unidos de América, condenándolo, además, a pagar los daños y perjuicios.

Por cuanto la parte denunciada, en la audiencia de juzgamiento interpuso recurso de apelación de la sentencia, de conformidad con el Art. 86 de la ley de la materia, se lo concede, debiendo por Secretaría remitirse el expediente a la Oficina de Sorteo, a fin de que conozca el juez de garantías penales de primer nivel que le corresponda por el sorteo reglamentario. Con costas. Notifíquese y cúmplase. -

Por las consideraciones que anteceden, Administrando justicia, en nombre del pueblo soberano del Ecuador, y por autoridad de la constitución y leyes de la república, el suscrito juez, ratifica en todas sus partes la sentencia venida en grado dictada por el juez a quo, Dr. V.M, para que, dentro de la denuncia presentada por J.V; representante legal de la empresa Austro Distribuciones Austrodis, cía. Ltda., desechando el recurso de apelación interpuesto por la Ab, S.A, defensora autorizada del Banco Pichincha.- Ejecutoriado este fallo, devuélvase el expediente al juzgado de origen, para el cumplimiento del mismo. Queda de esta forma atendido el escrito presentado por el accionante. - Continúe actuando la Abg. E.S, en calidad de secretaria encargada del despacho. - Cúmplase y Notifíquese.

4. Comentario del autor:

El caso presentado es en base a un litigio entre la empresa Austro Distribuciones Austrodis, Cía. Ltda., representada por J.V, y el Banco Pichincha, relacionado con un presunto servicio defectuoso. Por ello, la resolución del juez me parece pertinente, pues recae en la importancia de administrar justicia conforme a la Constitución, los derechos humanos y la ley. En este sentido, se aborda la utilización de informes periciales, particularmente en el ámbito de la peritación informática.

En primer lugar, la denuncia se basa en un fraude electrónico, y la evidencia técnica se centra en peritajes informáticos para investigar la dirección IP utilizada en la transferencia fraudulenta. La perita informática encargada de esta misión, destaca la falta de personalización y medidas de seguridad, señalando discrepancias entre la ubicación habitual de la empresa y la dirección IP de Perú asociada al fraude. Por lo que, este análisis pericial resulta crucial para establecer la conexión entre el presunto mal servicio del banco y las deficiencias tecnológicas que permitieron el fraude informático.

Es por esta razón que, la resolución del juez refleja la valoración de la evidencia técnica presentada por la perita informática. Entonces se muestran las debilidades del sistema del banco, haciendo hincapié en la falta de respuesta a eventos fraudulentos y la posibilidad de prevenir el fraude electrónico mediante la implementación de medidas de seguridad adecuadas. La resolución dictada, concluye que el Banco Pichincha prestó un mal servicio al no cumplir con las normativas de seguridad, respaldando así la posición de la denunciante.

Por otra parte, la ratificación de la sentencia inicial y el desecho del recurso de apelación indican que el juez considera concluyentes los argumentos presentados y respaldados por la evidencia pericial. La resolución dada, refuerza la importancia de los informes periciales en la correcta administración de justicia, destacando su papel en la evaluación de aspectos técnicos y tecnológicos que pueden influir en la resolución del caso. Por ello es tan importante la utilización adecuada de estos informes periciales porque contribuye a una toma de decisiones fundamentada y justa en el ámbito judicial.

Caso No. 2

1. **Datos Referenciales:**

- Juicio Nro. 01283201603612
- Victima: J. CH.
- Demandado: J.B.

- Acción: 396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1
- Juzgado: SALA ESPECIALIZADA DE LO PENAL, PENAL MILITAR, PENAL POLICIAL Y TRÁNSITO DE LA CORTE PROVINCIAL DE JUSTICIA DE AZUAY.
- Fecha: Cuenca, jueves 20 de junio del 2019

2. Antecedentes:

La señora Jueza de la Unidad Judicial Penal de Cuenca, Dra. P.B, en fecha 20 de junio del 2019, emite sentencia por escrito, en la cual declara a J.B, autor de la contravención de cuarta clase tipificada y sancionada en el artículo 396, numeral 1 del Código Orgánico Integral Penal, imponiéndole las penas y la reparación integral descrita en la sentencia que se trata. Llevada a cabo la Audiencia, oral, pública y contradictoria de fundamentación del Recurso de Apelación conforme a las normas del artículo 563 del Código Orgánico Integral Penal y dada a conocer la resolución en forma oral desechando el recurso interpuesto, acorde a lo señalado en el artículo 652, numeral 3 ibídem, la misma se reduce a escrito para lo cual se considera: En primer lugar, establece la jurisdicción y competencia de la sala para conocer un recurso de apelación. Se verifica la legalidad del proceso y se admite a trámite el recurso. Luego, se presentan los antecedentes de un caso en el que el ofendido denunció insultos y difamaciones proferidos por el acusado a través de redes sociales.

El defensor del acusado JB. Argumenta que se ha afectado el principio de congruencia y el derecho a la defensa, señalando que la prueba presentada por el denunciante se adecua a un delito de calumnia en lugar de injuria. Además, menciona una resolución de la Corte Nacional de Justicia sobre la calumnia. La sala analiza las alegaciones, concluyendo que la prueba presentada por el denunciante es consistente con el delito de injuria. Posteriormente, la prueba presentada por ambas partes, incluyendo documentos y testimonios. La sala realiza un análisis, indicando que las expresiones proferidas por J.B. afectaron el honor del denunciante. Por ello, se discute el principio de congruencia y se concluye que la alegación del defensor carece de sustento jurídico. Se destaca que la experticia y la prueba testimonial son válidas para probar la injuria. Finalmente, se establece que J. B. actuó con dolo y se confirma la existencia del delito de injuria gracias al informe pericial.

3. Resolución

Por lo expuesto, la suscrita Jueza de la Unidad Judicial Penal de Cuenca, “ADMINISTRANDO JUSTICIA, EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR

AUTORIDAD DE LA CONSTITUCIÓN Y LEYES DE LA REPÙBLICA", declara a J.B, ecuatoriano, divorciado, chofer, mayor de edad, con cédula de ciudadanía Nro.*******, con domicilio en esta ciudad de Cuenca, como autor de la contravención de cuarta clase tipificada y sancionado en el artículo 396 numeral 1 del Código Orgánico Integral Penal, esto es, por proferir expresiones en descrédito y deshonra.

No se han justificado circunstancias atenuantes ni agravantes, por lo que se le impone la pena definitiva de QUINCE DIAS DE PRIVACION DE LIBERTAD, que la cumplirá en el Centro de Rehabilitación Social Regional Centro Sur Turi, y con fundamento en el artículo 70 numeral 1 ibídem, se le impone la multa de noventa y un dólares con cincuenta centavos (91,50 usd). De ejecutoriarse esta resolución el sentenciado deberá presentarse voluntariamente para el cumplimiento de la pena, en el plazo de tres días, caso contrario se oficiará a la Policía Nacional con el fin de que procedan a su captura.

La Constitución de la República garantiza en el artículo 78, que las víctimas de infracciones penales tendrán derecho a una protección especial, y a que se adopten mecanismos para una reparación integral. La REPARACION INTEGRAL (restitutio in integrum) implica el restablecimiento de la situación anterior y la eliminación de los efectos que la violación ha producido. Por su parte, el artículo 78 consagra el deber del Estado, para el cumplimiento de este derecho, ahora bien esta juzgadora al establecer la reparación integral, no puede realizarla en virtud de criterios subjetivos; al contrario, se debe propender a la objetivación de los métodos para el cálculo de las indemnizaciones, lo cual solo se conseguirá a través de la actividad probatoria de los sujetos procesales. Los elementos constitutivos de la reparación integral, contenidos en el artículo 78 del Código Orgánico Integral Penal, pueden extraerse del artículo 63 numeral 1 de la Convención Americana de Derechos Humanos.

1- Derecho a la verdad. En la causa se ha garantizado el acceso a la tutela judicial efectiva, imparcial y expedita. (Art. 75 de la Constitución de la República), primando el debido proceso, en la que se ha establecido la existencia la violación de un derecho, identificación del responsable, a través de un proceso justo, en igualdad de condiciones, y a través de la valoración de la prueba legalmente obtenida que han permitido alcanzar esta resolución.

2. INDEMNIZACION. La CIDH, ha definido a la indemnización, de la siguiente manera: "La indemnización corresponde en primer término a los perjuicios sufridos por la parte lesionada, y comprende, como esta Corte ha expresado anteriormente, tanto el daño material como el moral". Señala, la CIDH que se han seguido los criterios generales determinados por el derecho

de daños, debiendo, por tanto, considerar el daño emergente y el lucro cesante. En el caso que nos ocupa, dada la naturaleza del bien jurídico protegido, la honra, no es posible determinar de modo objetivo, un monto económico que corresponda a la indemnización.

3. MEDIDAS DE SATISFACCION O SIMBÓLICAS. Presupuesto de una justicia restauradora, que se traduce en actos u obras de alcance o repercusión pública, que buscan la recuperación del bien jurídico violado. Para ello esta juzgadora dispone: las disculpas públicas que deberá realizar el ciudadano Julio Bermeo Bermeo al señor Juan Marcos Chumbi Jadán, en un medio impreso (periódico) de mayor circulación de la ciudad de Cuenca, a su costa, dentro del plazo de quince días a partir de la ejecutoria de esta resolución, cuyo texto deberá ser aprobado por la juzgadora en forma previa a la publicación. Con costas. Se fija en dos salarios básicos unificados del trabajador en general como honorarios a favor de los abogados que patrocinaron a la víctima. Los principios, normas constitucionales y legales aplicables, se encuentran insertas en el fallo. Notifíquese y Cúmplase.

4. Comentario del autor:

El presente caso judicial hace mención a que la señora Jueza de la Unidad Judicial Penal de Cuenca emite una sentencia contra J.B. por la comisión de una contravención de cuarta clase, tipificada y sancionada en el artículo 396, numeral 1 del Código Orgánico Integral Penal. Posteriormente, se lleva a cabo una Audiencia de Recurso de Apelación, en la cual se desecha el recurso interpuesto por J.B.

Ahora bien, en relación con la eficiencia del informe pericial, se observa que se menciona que la sala concluye que J.B. actuó con dolo GG Sin embargo, el informe no proporciona detalles específicos sobre el contenido y la extensión del informe pericial ni señala si ha sido completo o detallado. Por lo tanto, no se puede evaluar directamente la eficiencia del informe pericial a partir de la información proporcionada.

Ante esto, se recalca que, la eficiencia de un informe pericial depende de varios factores, como la exhaustividad de la investigación, la claridad en la presentación de los hallazgos y la relevancia de la información proporcionada. Puesto que, si el informe pericial en este caso no ha sido completo o detallado, podría plantearse un cuestionamiento sobre la validez de las conclusiones alcanzadas por la sala con base en dicho informe. Por tal razón sería necesario contar con más detalles sobre el contenido específico del informe pericial y cualquier argumento adicional relacionado con su falta de completitud para realizar un análisis más preciso sobre la eficiencia del mismo y su impacto en la resolución del caso.

Caso No. 3

1. **Datos Referenciales:**

- Juicio Nro. 05254201700211
- Victima: K.E.
- Demandado: E.C
- Acción: CONTRAVENCIONES PENALES
- Juzgado: UNIDAD JUDICIAL MULTICOMPETENTE PENAL CON SEDE EN EL CANTÓN LA MANÁ, PROVINCIA DE COTOPAXI
- Fecha: La Mana, lunes 3 de septiembre del 2018
-

2. **Antecedentes:**

En la denuncia presentada por la ciudadana, K.E en contra de la ciudadana E.C, por la contravención penal de cuarta clase tipificada en el numeral 1 del Art. 396 del Código Orgánico Integral Penal, en adelante COIP, ha tenido lugar la audiencia de Juzgamiento en procedimiento expedito. Siendo el estado procesal de la causa el de dictar sentencia, se realizan las siguientes consideraciones:

PRIMERO. - INSINUACIÓN DE CONCILIACIÓN: En aplicación del Art. 190 de la Constitución de la República y Art. 130 número 11 del Código Orgánico de la Función Judicial, se insinúa a las partes a que establezcan un acuerdo conciliatorio que ponga fin a la acción judicial, y que garantice en el futuro el respeto mutuo entre las personas intervinientes. En respuesta, la denunciada E.C, expresa que no está de acuerdo con aplicar ninguna conciliación.

SEGUNDO. - JURISDICCIÓN Y COMPETENCIA: En razón de las disposiciones constantes en el Art. 404, numeral 1 del COIP, en concordancia con el Art. 171 del Código Orgánico de la Función Judicial, COFJ, así como por el contenido de las Resoluciones No. 143-2013 y 98-2017, expedidas por el Pleno del Consejo de la Judicatura, el juez es competente como Jueza titular de la Unidad Judicial Multicompetente Penal con sede en el cantón La Maná, para conocer, sustanciar y resolver la presente causa.

TERCERO. - VALIDEZ PROCESAL: La causa ha sido sometida al trámite de procedimiento expedito establecido en el Art. 642 del COIP, habiéndose cumplido los requisitos y condiciones que contempla esta disposición legal. Se han respetado las reglas del debido proceso contenidas en el Art. 76 de la Constitución de la República, y no se ha vulnerado el derecho a la defensa de las partes procesales.

CUARTO. - IDENTIFICACIÓN DE LA PROCESADA: La persona que ha sido sometida a procedimiento contravencional en el presente caso responde a los nombres de: E.C de nacionalidad ecuatoriana, portadora de la cédula de ciudadanía No. 0503300915, de 31 años de edad, de estado civil casada, con grado de instrucción secundario, de ocupación comerciante, domiciliada en el cantón La Maná, provincia de Cotopaxi.

QUINTO. - HECHO ILÍCITO ACUSADO: La ciudadana K.E ha presentado con fecha miércoles 20 de diciembre del 2017, denuncia en contra de la ciudadana E.C. La denuncia consta a folios seis y seis vueltas del expediente.

SÉPTIMO. -Pruebas

El caso presentado, presenta testimonios y pruebas relacionadas con un caso de difamación en redes sociales. La denunciante, K.E, menciona que ha sido objeto de comentarios difamatorios en Facebook, donde la acusan de ser una "zorra" y "quita maridos". Esto ha tenido un impacto negativo en su vida personal y laboral. Se menciona que la publicación provino de la cuenta de C.E, quien posteriormente admitió haber realizado la publicación, pero se negó a disculparse.

Testimonios de N.C, T.L, D.T. y W.J respaldan la versión de K.E y muestran cómo la difamación ha afectado a su familia y entorno social. Además, se incluyen testimonios de expertos en psicología y peritajes informáticos que respaldan el impacto emocional y la difamación sufrida por K.E.

Posteriormente, el debate planteado se centra en la presunta comisión de un delito relacionado con la difamación a través de redes sociales. La defensa de la víctima argumenta que se ha probado que la denunciada publicó expresiones difamatorias en Facebook, lo que causó un daño emocional significativo a la víctima. Solicitan una sanción penal y una reparación económica. Por otro lado, la defensa de la denunciada argumenta que se debe declarar la nulidad procesal debido a la falta de realización del peritaje del lugar de los hechos, lo que no cumple con los requisitos legales establecidos. Además, impugnan la imparcialidad del perito informático y cuestionan la validez de las pruebas presentadas. En la réplica, la defensa de la víctima refuta los argumentos de nulidad procesal y enfatiza en la importancia de proteger los derechos de la víctima. Por otro lado, la defensa de la denunciada insiste en la aplicación de la ley para declarar sin lugar la demanda.

La argumentación se centra en establecer si se han cumplido los elementos del delito de difamación, como la existencia del hecho, el ánimo de injuriar y el perjuicio causado a la

víctima. Se concluye que la conducta de la denunciada se ajusta al tipo penal establecido y que actuó con pleno conocimiento de su ilicitud, por lo que se justifica la imposición de una sanción penal.

3. Resolución

En razón de los argumentos analizados y expuestos, de acuerdo a la información proporcionada en la audiencia, y que luego de la valoración efectuada de la prueba incorporada, éstas han cumplido la finalidad establecida en el Art. 453 del COIP; esto es, se ha permitido a la juzgadora llegar al convencimiento de los hechos, más allá de toda duda razonable, sobre la infracción tipificada y sancionada por el 396, numeral 1 del COIP, así como de la participación y responsabilidad de la denunciada; por lo que, en mi condición de Jueza titular de la Unidad Judicial Multicompetente Penal con sede en el cantón La Maná, de acuerdo a lo establecido por los Arts. 621 y 622 del COIP, ADMINISTRANDO JUSTICIA, EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, dicto SENTENCIA CONDENATORIA, en contra de la ciudadana E.C, cuyos datos se encuentran singularizados en el ordinal cuarto de la presente sentencia, a quien se le impone la pena privativa de la libertad QUINCE (15) DÍAS DE PRIVACIÓN DE LA LIBERTAD, en razón de no haberse verificado la existencia de las circunstancias atenuantes que permitan su modificación.-

MULTA: Conforme lo dispuesto por el numeral 1 del Art. 70 del COIP, se condena además a la ciudadana, E.C al pago de una multa del VEINTE Y CINCO POR CIENTO 25% DE UN SALARIO BÁSICO UNIFICADO DEL TRABAJADOR EN GENERAL, esto es, la suma de USD. 96,50, que deberán ser depositados en la cuenta No. 3001109468, sublínea No. 170499 otras multas a nombre del Consejo de la Judicatura de Cotopaxi, en BAN ECUADOR, de manera íntegra e inmediata una vez que la sentencia quede ejecutoriada. -

REPARACIÓN INTEGRAL: En virtud de que en la audiencia no se practicó prueba que haya permitido a esta juzgadora la cuantificación de los perjuicios ocasionados y a fin de cumplir con lo dispuesto por el Art. 78 de la CRE; Art. 1; 11, numeral 2 y 52 del COIP, se dispone, como Reparación Integral de la Víctima, de acuerdo a lo establecido en el numeral 4 del Art. 78 del COIP, lo siguiente: 4.- Medidas de satisfacción y simbólicas: Dada la naturaleza de la infracción, la sentenciada E.C, deberá expresar disculpas públicas a través del mismo medio, esto es la página Facebook utilizando su usuario a la víctima K.E, en el plazo de siete días contados a partir de que se ejecutoríe esta sentencia, considerándose así un mecanismo de

reparación de la dignidad y reputación de la víctima.- Continúe actuando como secretaria encargada de este despacho, la Dra. E.T.- NOTIFIQUESE y CÚMPLASE.

4. Comentario del Autor:

Con respecto a este caso, se puede apreciar como el peritaje informático desempeña un papel fundamental en la resolución de casos judiciales que involucran evidencia digital, como en el caso de difamación en redes sociales mencionado anteriormente. Sin embargo, es evidente que, en muchos países, incluido el nuestro, el peritaje informático no siempre es eficiente y puede presentar deficiencias significativas que obstaculizan de cierta forma la administración de justicia de manera efectiva. Por ello, el caso planteado de difamación en redes sociales ejemplifica los desafíos asociados con el peritaje informático deficiente. A lo largo del proceso, se evidenció la importancia de contar con un peritaje sólido y más completo para analizar la evidencia digital, como los comentarios difamatorios en Facebook. Sin embargo, se debe recalcar un hecho importante en el caso, que es justamente, que, la defensa cuestionó la imparcialidad del perito informático y la validez de las pruebas presentadas, lo que resalta la necesidad de directrices más claras y completas en esta área.

Del mismo modo, se debe recalcar que, la falta de regulación adecuada y estándares claros para el peritaje informático puede conducir a disputas legales sobre la validez de la evidencia digital presentada en casos judiciales. Por lo tanto, en este caso, la defensa de la denunciada argumentó la nulidad procesal debido a la falta de realización del peritaje del lugar de los hechos y cuestionó la imparcialidad del perito informático. Por ende, estos aspectos reflejan la necesidad de una mayor capacitación y recursos en el campo del peritaje informático para garantizar la eficiencia y la imparcialidad en la administración de justicia.

Finalmente, considero necesario mencionar que, la falta de recursos y expertos cualificados en peritaje informático puede obstaculizar la correcta evaluación de la evidencia digital, como se observa en este caso donde el perito informático no pudo completar la pericia debido a la eliminación de la cuenta de Facebook de la denunciada; por lo tanto, esto destaca la necesidad de una mayor inversión en capacitación y recursos en este campo para mejorar la calidad y confiabilidad del peritaje informático en casos judiciales en nuestro país.

7. Discusión

7.1 Verificación de los Objetivos

Los objetivos propuestos en el Trabajo de Integración Curricular aprobado son los siguientes: un objetivo general y cuatro objetivos específicos que se describirán a continuación:

7.1.1 Verificación de objetivo general

El objetivo general legamente aprobado en el proyecto de integración curricular es el siguiente: **"Realizar un Análisis jurídico y doctrinario de los informes periciales relacionados con delitos informáticos"**

El presente objetivo general se logra verificar a través del desarrollo del marco teórico, donde se profundizan los conceptos doctrinarios proporcionados por autores especializados en la intersección del derecho penal y la informática. Es así como en este análisis, se abordan aspectos fundamentales del derecho penal, tales como el concepto del delito, sus elementos constitutivos y diversos tipos delictivos. Además, la comprensión se extiende hacia el ámbito específico de los delitos informáticos, explorando categorías particulares, su clasificación, así como la distinción entre delincuencia convencional y ciberdelincuencia. Demostrando que, este enfoque no solo aborda la teoría, sino también se adentra en la relevancia práctica, destacando la necesidad de examinar rigurosamente la prueba en el ámbito de los delitos informáticos.

Del mismo modo, la investigación abarca también los medios de prueba, destacando el papel crucial del peritaje informático y la figura del perito. En este apartado, se examina la idoneidad del perito y se analiza el proceso de peritaje informático, así como la correcta elaboración de informes periciales. Por ello, la incorporación del informe pericial en el contexto del COGEP (Código Orgánico General de Procesos) proporciona un vínculo directo con el marco legal nacional, resaltando la conexión esencial entre la teoría y la aplicación práctica en el sistema judicial ecuatoriano. Además, desde una perspectiva más amplia, se incorpora un análisis de derecho comparado, destacando la relevancia del Convenio de Budapest y la adopción de estándares internacionales en la materia. La inclusión de normativas específicas, como la Norma UNE 197001:2019 y la Norma UNE 197001:2015, destacando de esta manera el compromiso con la necesidad de la adopción de prácticas internacionales en el ámbito de la seguridad informática en nuestro país.

El estudio jurídico se sitúa en el marco normativo vigente en Ecuador, abarcando normativas fundamentales como la Constitución de la República del Ecuador, los estándares

internacionales de derechos humanos, el Código Orgánico Integral Penal y demás leyes vinculadas al derecho informático. Dado que, este enfoque garantiza una base sólida en la legislación nacional para la exploración de cuestiones jurídicas relativas al ámbito digital. Adicionalmente, se llevó a cabo una exhaustiva comparación con el derecho internacional, considerando específicamente las normas UNE 197001:2019 y la Norma UNE 197001:2015. Puesto que, estas normativas, las cuales establecen pautas y requisitos para la correcta elaboración de informes periciales, han sido adoptadas como estándares en países como España y otros que aplican estas normas y tienen mejores resultados. Es importante mencionar que, esta comparación proporciona una perspectiva global y destaca la importancia de armonizar prácticas periciales en el ámbito informático, facilitando la comprensión y aplicación de estas normas en el contexto legal ecuatoriano.

En sí, se puede afirmar que, la inclusión de estándares internacionales refuerza la perspectiva del estudio jurídico, mostrando un compromiso no solo con la normativa local, sino también con las mejores prácticas y estándares reconocidos internacionalmente en el ámbito del derecho informático para de esta manera mejorar el sistema de justicia en nuestro país. Valorando que, esto no solo fortalece la validez y relevancia del estudio, sino que también permite una contextualización global de las cuestiones abordadas, enriqueciendo así el análisis y los objetivos planteados inicialmente.

7.1.2 Verificación de Objetivos específicos

1. El primer objetivo específico es: **Determinar la estructura y aplicabilidad del estándar internacional UNE 197010:2015 en los informes periciales relacionados con delitos informáticos, para garantizar la correcta administración de justicia.**

El primer objetivo específico se logra alcanzar mediante la investigación planteada en el marco teórico, puesto que es aquí donde analiza detenidamente la estructura y la aplicabilidad del estándar internacional UNE 197010:2015, la cual tiene como objetivo establecer los requisitos formales para informes y dictámenes periciales en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC). Por lo que es importante destacar, que esta normativa específica, denominada "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)" es la que establece la estructura documental y el contenido apropiado exclusivamente para informes periciales en el ámbito informático.

Al analizar detenidamente dicha la normativa, se puede evidenciar que esta, establece los principios cruciales que deben ser respetados por los peritos informáticos durante la elaboración de informes periciales. Estos principios son: relevancia, fiabilidad, suficiencia y oportunidad. El primero, destaca la importancia de identificar y resaltar las evidencias más significativas para el caso, centrando la atención en los aspectos más relevantes de la investigación. Por su parte, la fiabilidad se refiere a la consistencia y reproducibilidad de los resultados, esencial para la validez y credibilidad del informe. La suficiencia garantiza que las evidencias respalden adecuadamente las conclusiones del informe, evitando la inclusión de información innecesaria. Y finalmente el principio de oportunidad enfatiza la importancia de presentar las evidencias en el momento adecuado y dentro del contexto del caso.

De manera análoga, la verificación de este objetivo se respalda mediante la actividad realizada a través de entrevistas a profesionales en derecho penal e informático. En particular, se centró en la pregunta 3 del cuestionario, que indaga sobre la aplicación de normas internacionales para estructurar informes periciales en el ámbito de delitos informáticos, específicamente la Norma Une 19701: 2015. La totalidad de los entrevistados y el 83% de los encuestados expresaron su acuerdo con la relevancia y utilidad de estas normativas, subrayando que su implementación fortalecería la credibilidad del sistema pericial ecuatoriano.

Esta aceptación generalizada se justifica en la percepción predominante entre los entrevistados de que, estas normas son indispensables para salvaguardar la integridad y calidad de los informes periciales informáticos. De igual manera, ellos destacan que sirven como una guía objetiva para los peritos, asegurando que sus informes sean exhaustivos, precisos y pertinentes. Por lo que, este cumplimiento de principios contribuye significativamente a la promoción de la justicia y la equidad dentro del sistema legal. Además, se enfatiza que estas normativas fomentan la transparencia y confianza en el desempeño de los peritos informáticos, los cuales son aspectos cruciales en un ámbito tan técnico y especializado como el de los delitos informáticos. En definitiva, la adopción de estas normas internacionales se presenta como un factor clave para fortalecer la validez y fiabilidad de los informes periciales en nuestro sistema de justicia.

2. El segundo objetivo específico es: **Demostrar que la metodología establecida por el Consejo de la Judicatura para la elaboración de informes periciales no es suficiente para una correcta administración de justicia.**

El segundo objetivo específico se logra verificar a través de la implementación de encuestas, focalizándose especialmente en las respuestas obtenidas a la segunda pregunta, la cual plantea la metodología actualmente establecida en la legislación para la presentación de informes periciales. Dicha metodología aborda aspectos como los datos completos del perito, información sobre la profesión o actividad especial ejercida, número de acreditación otorgado por el Consejo de la Judicatura y su vigencia, explicación de los hechos u objetos analizados, detalle de los exámenes y prácticas aplicadas, así como los razonamientos y deducciones que condujeron a las conclusiones.

Las respuestas revelaron que 25 de los 30 encuestados consideran insuficiente esta metodología en comparación con la Norma Une 19701:2015, argumentando la carencia de requisitos específicos que garanticen la completitud de los informes periciales. En las entrevistas con profesionales del derecho, la mayoría opinó que, si bien los requisitos de la legislación local son adecuados, podrían ser considerados incompletos. Además, muchos de ellos sugirieron la posibilidad de adoptar estándares internacionales, como la Norma Une 19701:2015, argumentando que estos sí ofrecen un análisis más exhaustivo y podrían ser más efectivos en la administración de justicia. Por tal motivo, este objetivo destaca la percepción generalizada de que la metodología vigente en la legislación local podría beneficiarse al incorporar estándares internacionales, mejorando de esta manera, la calidad y exhaustividad de los informes periciales. Por ende, la consideración de estándares más abarcadores y completos, se postula como una opción viable para fortalecer el sistema de administración de justicia en el ámbito pericial.

Este objetivo también se logra verificar con el estudio de casos, pues en ellos podemos observar la deficiencia de los informes periciales aplicados o no aplicados correctamente; por ello radica la importancia de la calidad y objetividad en los informes periciales se pone de manifiesto al analizar estos tres casos específicos, donde cualquier deficiencia en su elaboración o interpretación puede socavar la integridad del proceso judicial. Por ejemplo, al revisar detenidamente el tercer caso, se observa la falta de claridad y la posible parcialidad en el informe pericial presentado, lo que cuestiona la imparcialidad del perito y deja en entredicho la validez del caso. Deduciendo de esta manera, que estos informes son pilares fundamentales en la toma de decisiones judiciales, proporcionando información especializada para determinar hechos relevantes. Por tal motivo, garantizar la calidad y objetividad de estos informes es necesario para fortalecer la integridad del sistema de justicia, asegurando que las decisiones se basen en evidencia confiable y equitativa.

3. El tercer objetivo específico es: **Identificar los estándares internacionales relevantes que rigen la correcta elaboración de informes periciales.**

Con respecto al tercer objetivo específico se logra verificar gracias a la minuciosa indagación llevada a cabo en el marco teórico. Puesto que, al examinar detenidamente los estándares internacionales y compararlos con los informes periciales empleados actualmente en nuestra legislación, se evidencia que la Norma Une 19701:2015 se destaca por su notable exhaustividad y detalladas especificaciones. Este análisis teórico resalta las diferencias significativas entre los estándares internacionales y los procedimientos vigentes en la legislación local, subrayando de esta manera la necesidad de considerar la adopción de normativas más completas y rigurosas para fortalecer la calidad y la integridad de los informes periciales en nuestro país.

Del mismo modo, el estudio a profundidad de esta norma destaca las pautas esenciales para la elaboración de informes periciales "TIC". Principalmente, se enfatiza la importancia del título en la identificación clara del proceso de investigación y se especifica una estructura básica que incluye identificación, índice, cuerpo del informe y anexos. Además, en esta norma se detallan elementos cruciales como la declaración de imparcialidad, juramento o promesa, conclusiones, firma y visado. Por consiguiente, la paginación uniforme y la inclusión de información detallada sobre el perito, solicitante, letrado y procurador son destacadas como requisitos esenciales en el contenido inicial del informe.

Con respecto al cuerpo del informe, se establecen secciones específicas, como objeto, alcance, antecedentes, consideraciones preliminares, documentos de referencia, terminología y abreviaturas, análisis, conclusiones y anexos. Es por esta razón que, la claridad y comprensibilidad del informe son resaltadas, así como la necesidad de incluir la interpretación técnica de manera inequívoca. Y finalmente es importante identificar y paginar correctamente los anexos existentes. En conclusión, esta norma nos brinda una guía detallada para garantizar la calidad y coherencia en la presentación de informes periciales TIC y poder así mejorar con los informes periciales y obtener una mayor credibilidad en nuestro sistema de justicia.

4. El cuarto objetivo específico es: **presentar proyecto de reforma en torno al informe pericial sobre delitos informáticos para una adecuada administración de justicia.**

Este cuarto objetivo específico se puede verificar mediante la aplicación de encuestas, particularmente mediante las respuestas obtenidas en la cuarta pregunta, en la cual se indaga sobre la disposición de los profesionales para presentar una propuesta de reforma en relación con los informes periciales sobre delitos informáticos, con el propósito de mejorar la administración de justicia. Un notable 93.33% de los encuestados, es decir, 28 de 30 profesionales, expresaron su apoyo a esta medida, destacando la oportunidad de proponer directrices que enfoquen la mejora de los formatos de los informes periciales, contribuyendo así a una administración de justicia más efectiva en el país.

Del mismo modo, en las entrevistas realizadas, se observa un consenso general entre los entrevistados a favor de la propuesta de establecer una propuesta de reforma en relación con la adopción de la Norma Une 19701:2015. Por tal motivo, este respaldo se fundamenta en la percepción de que esta norma, al ser más completa, tiene el potencial de ofrecer resultados más sólidos y confiables, asegurando de esta manera, la efectividad del sistema de justicia. Esta alineación de opiniones refuerza la importancia de considerar la implementación de la respectiva propuesta de reforma, especialmente con lo relacionado a la adopción de estándares internacionales, con la finalidad de mejorar la calidad y confiabilidad de los informes periciales en el ámbito de delitos informáticos en nuestro sistema de justicia.

8. Conclusiones:

Una vez desarrollado el marco teórico y la investigación de campo se procede a presentar las siguientes conclusiones:

1. La mayoría de encuestados y entrevistados están de acuerdo en establecer los requisitos mínimos según la Norma UNE: 197010:2015 en informes periciales sobre delitos informáticos en el país. Dado que la adopción de estos estándares se percibe como una medida que brindaría claridad, uniformidad y calidad en los informes, mejorando la eficacia del sistema judicial.
2. De la investigación de campo se desprende que existe insuficiente metodología actual para presentar informes periciales en el sistema legal. Lo que significa que, este fuerte respaldo sugiere una clara demanda de una metodología más detallada y completa con el fin de garantizar la calidad y transparencia en la administración de justicia.
3. Los profesionales del derecho están a favor de la aplicación de normas internacionales, específicamente la Norma Une 19701:2015, en la estructuración de informes periciales

sobre delitos informáticos. Concluyendo así que este alto grado de aceptación indica un fuerte respaldo hacia la adopción de estándares internacionales, destacando así la importancia de mejorar la calidad y consistencia de los informes periciales en el ámbito nacional.

4. La mayoría de los encuestados y entrevistados están de acuerdo en la presentación de una propuesta de reforma en torno al informe pericial sobre delitos informáticos. Concluyendo así que, este alto nivel de acuerdo refleja un consenso generalizado entre los profesionales del Derecho encuestados y entrevistados sobre la importancia de establecer directrices claras y específicas para la elaboración de informes periciales en casos de delitos informáticos.
5. La mayoría de encuestados y entrevistados estiman que el sistema de justicia en el país debería mejorar el formato de los informes periciales, especialmente en casos de delitos informáticos, concluyendo de esta manera, que es importante y necesario adaptar los procedimientos judiciales internacionales y técnicas específicas con respecto a los delitos informáticos.
6. En cuanto al estudio de los casos analizados, se concluye la importancia central de los informes periciales en la administración de justicia, donde su eficacia resulta determinante para respaldar denuncias y confirmar la existencia de delitos; puesto que en el segundo caso señala una preocupación sobre la falta de detalles específicos en el informe pericial, resaltando la necesidad de una mayor claridad en estos documentos; por lo que resulta imperante la necesidad de informes periciales más eficientes y detallados, que proporcionen una base sólida para decisiones judiciales justas y precisas, contribuyendo así a una mejor aplicación de la justicia.
7. Con respecto al derecho comparado, se puede observar la falta de normativas legales con enfoques técnicos en Ecuador para abordar los delitos informáticos. Además, se evidencia la necesidad de regulaciones específicas que identifiquen conductas punibles y establezcan procedimientos para la aplicación de la ley en el ámbito digital. Por tal motivo, la colaboración internacional y la aplicación de estándares, como los definidos por la UNE, son importantes para abordar los delitos informáticos de manera integral.

9. Recomendaciones

Con base en las conclusiones obtenidas, se recomienda implementar las siguientes medidas jurídicas para abordar la problemática existente en el sistema penitenciario ecuatoriano

1. Al Consejo de la Judicatura se recomienda, tomar en consideración la implementación de requisitos mínimos basados en la Norma UNE 19701:2015 para informes periciales sobre delitos informáticos en el país, puesto que, no solo garantizará claridad y uniformidad, sino también mejorará la calidad y eficacia del sistema judicial al proporcionar estándares reconocidos y aceptados.
2. Al Consejo de la Judicatura, se sugiere desarrollar una metodología más detallada y completa para la presentación de informes periciales en el sistema legal; porque esto atenderá la demanda clara de los profesionales del Derecho, mejorando así la calidad, transparencia y eficacia en la administración de justicia.
3. A los operadores de justicia, se recomiendo la aplicación efectiva de normas internacionales, en particular la Norma UNE 19701:2015, para estructurar informes periciales sobre delitos informáticos.
4. A los estudiantes de las Carreras de Derecho, seguir investigando en torno al informe pericial en torno al informe pericial sobre delitos informáticos, considerando los consensos generalizados entre los profesionales del Derecho; dado que, estos lineamientos proporcionarán directrices claras y específicas para mejorar la elaboración de informes periciales en casos de delitos informáticos.
5. A los peritos informáticos mejorar el formato de los informes periciales, especialmente en casos de delitos informáticos, para adaptar los procedimientos judiciales y técnicas específicas, puesto que esto asegurará una presentación más clara y comprensible de la evidencia, facilitando así una administración de justicia más efectiva y justa.
6. A la presidencia de la República se sugiere promover la colaboración internacional y la adopción de estándares, como los definidos por la UNE, para abordar integralmente los delitos informáticos en Ecuador; debido a que estos estándares proporcionarán una guía sólida y objetiva, asegurando la aplicación efectiva de la ley en el ámbito digital y mejorando de esta manera nuestro sistema de justicia.
7. A la Universidad Nacional de Loja continuar con investigaciones exhaustivas con el objetivo de perfeccionar los informes periciales relacionados con los delitos informáticos; con el fin de que ayuden a fortalecer la confianza en nuestro sistema de justicia en el ámbito de las cuestiones informáticas; recalcando que la investigación debe enfocarse en identificar las mejores prácticas, metodologías y estándares

internacionales aplicables a la elaboración de informes periciales en casos de delitos informáticos.

9.1 Proyecto de Reforma.

Que: "el artículo 178 inciso segundo de la Constitución de la República del Ecuador, así como el artículo 254 del Código Orgánico de la Función Judicial, disponen que el Consejo de la Judicatura es el órgano de gobierno, administración, vigilancia y disciplina de la Función Judicial."

Que: "el artículo 177 de la Constitución de la República del Ecuador, prescribe: "La Función Judicial se compone de órganos jurisdiccionales, órganos administrativos, órganos auxiliares y órganos autónomos. La ley determinará su estructura, funciones, atribuciones, competencias y todo lo necesario para la adecuada administración de justicia."

Que: "el artículo 181 numerales 1 y 5 de la Constitución de la República del Ecuador, determina: Serán funciones del Consejo de la Judicatura además de las que determine la ley: 1. Definir y ejecutar las políticas para el mejoramiento y modernización del sistema judicial; […] y, 5. Velar por la transparencia y eficiencia de la Función Judicial."

Que: "el artículo 14 del Código Orgánico de la Función Judicial, preceptúa: PRINCIPIO DE AUTONOMÍA ECONÓMICA, FINANCIERA Y ADMINISTRATIVA. -La Función Judicial goza de autonomía económica, financiera y administrativa. Administrativamente se rige por su propia ley, reglamentos y resoluciones, bajo los criterios de descentralización y desconcentración."

Que: "el Pleno del Consejo de la Judicatura (periodo 2013-2018), mediante Resolución 040-2014, de 10 de marzo de 2014, expidió el "REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL", reformado con resoluciones: 009-2015, de 27 de enero de 2015; 327-2015, de 14 de octubre de 2015; 067-2016, de 25 de abril de 2016; 126-2016, de 28 de julio de 2016; 068-2017 de 10 de mayo de 2017, 75A-2018, de 19 de septiembre de 2018; y, 147-2022, de 23 de junio del 2022."

Que: "el artículo 264 numerales 9 y 10 del Código Orgánico de la Función Judicial, dispone como facultades del Pleno del Consejo de la Judicatura: "9. Fijar y actualizar: […] así como organizar el sistema pericial a nivel nacional. […] y sistematizar un registro de los peritos

autorizados y reconocidos como idóneos, cuidando que estos sean debidamente calificados y acrediten experiencia y profesionalización suficiente.”

En ejercicio de sus atribuciones constitucionales y legales, por unanimidad.

RESUELVE:

APROBAR LA REFORMA AL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL.

ARTICULO 1:

CONTENIDO DEL INFORME PERICIAL

En el artículo 29 agregase el siguiente inciso:

En los informes periciales relacionados con delitos informáticos, se deberá incluir una sección de referencia bibliográfica que respalde:

a. La base científica aplicada en el contenido del informe.
b. La base científica en la que se fundamenta el dictamen pericial.
c. El estándar internacional utilizado para la elaboración del informe pericial.

ARTÍCULO SEGUNDO

En el artículo 30 agréguese el siguiente inciso:

En caso de que el informe pericial se refiera a delitos informáticos, la estructura documental y redacción deberán ajustarse a los lineamientos de estándares internacionales diseñados para garantizar uniformidad en los requisitos formales que deben cumplir los informes y dictámenes periciales en el ámbito informático.

ARTÍCULO TERCERO (Alcance de la capacitación)

Sustitúyase el artículo 40 por el siguiente:

Las y los peritos calificados estarán obligados a completar con éxito un Curso Básico para Peritos, organizado por la Escuela de la Función Judicial. Este curso se centrará en profundizar en temas contemplados en el presente Reglamento, abordando las obligaciones integrales y los deberes de las y los peritos, así como la normativa relevante constante en el Código Orgánico de la Función Judicial y demás leyes aplicables. Además, se enfocará en el análisis y

comprensión de los formatos a utilizarse para la emisión de los informes periciales, asegurando el cumplimiento de sus requisitos.

Disposición Derogatoria:

Derogase todas las disposiciones reglamentarias q se opongan a la siguiente reforma.

Disposición final:

Esta resolución entrará en vigencia a partir de su aprobación, sin perjuicio de su publicación en el registro oficial.

Dado en el Distrito Metropolitana de Quito, en la Sala de Sesiones del Consejo de la Judicatura, a los 15 días del mes de febrero de 2024.

…… **…..……**

Dr. Álvaro Román Márquez **Abg. Carolina Martínez Ríos**

Presidente del C.J **Secretaria General del C.J**

CERTIFICO: QUE EL PLENO DEL CONSEJO DE LA JUDICATURA APROBÓ ESTA RESOLUCION A LOS 19 DIAS DEL MES DE FEBRERO DEL 2024.

……...

Abg. Carolina Martínez Ríos

Secretaria del C.J

10. Bibliografía

Acosta, M., Benavides, M., & García, N. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios.* . Redalyc.org.

Albán, E. (2004). *Manual de derecho penal ecuatoriano: parte general.* . Quito, Ecuador.: Ediciones Legales. .

Artavia, S. &. (2018). *La prueba en el proceso civil costarricense.* . San José: Editorial Juricentro.

Asamblea Nacional . (2023). *Código Orgánico Integral Penal.* Quito: Registro oficial.

Blanco, J. (2005). *Teoría del delito.* Valencia, España.: Editorial Tirant lo Blanch.

Borges, A. (2018). *La prueba digital en el proceso penal.* . Lima: Ara Editores.

Cassrino Viterbo, J. (1954). *La prueba pericial.* . Buenos Aires, Argentina: Ediciones Jurídicas Europa-América.

Castell, R., & Carballo, M. (1999). *Psicología de la delincuencia.* Madrid: Editorial Síntesis.

COGEP, C. O. (2015). *Código Orgánico General de Procesos (COGEP).* Quito, Ecuador: Asamblea Nacional.

Consejo de Europa. (23 de noviembre de 2001.). *Convenio sobre la ciberdelincuencia.* Budapest.

Consejo de la Judicatura. (28 de diciembre de 2023). *Consejo de la Judicatura. Proceso de calificación de peritos judiciales.* Obtenido de https://www.funcionjudicial.gob.ec/: https://www.funcionjudicial.gob.ec/

Convenio sobre la Ciberdelincuencia. (23 de noviembre de 2001). *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*. Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Convenio sobre la Ciberdelincuencia. (2001). *Convenio sobre la Ciberdelincuencia.* Consejo de Europa.

Cruz, M. (2020). *Manual de derecho penal ecuatoriano: parte general.* Quito, Ecuador.: Ediciones Legales.

Fernández, J. (2017). La evolución histórica del delito. . *Revista Derecho Penal*, 1(2), 23-34.

Flores Galea, J. (2019). *El informe pericial informático.* . Madrid: Editorial Reus.

Flores, M. (2005). Prueba pericial. Consideraciones sobre la prueba pericial y su valoración en la decisión judicial. . *Revista IIDH*, 45, 127-140.

Flores, M. (2015). Prueba pericial. Consideraciones sobre la prueba pericial y su valoración en la decisión judicial. *Revista IIDH, ,* 45, 127-140.

Garberí Llobregat, J. (2003). *La prueba pericial en el proceso civil.* . Barcelona, España: Editorial Bosch.

García Maynez, E. (1951). *Derecho penal. Parte general.* . México : Editorial Porrúa.

García, L. (2018). *Delitos informáticos: Tipificación y jurisprudencia.* . Marcial Pons.

González, R. (2018). *Manual de derecho penal ecuatoriano: parte general.* . Quito, Ecuador.: Ediciones Legales. .

Herrero Herrero, M. (2005). *Criminología.* Madrid: Editorial Dykinson.

Ibáñez, J. (2015). *Peritaje informático forense.* . Madrid, España: Editorial Dykinson.

Iglesias, J. (2017). El delito como proceso. *Revista de Derecho Penal*, 2(1), 15-22.

Laffite, H. (1989). *Derecho Penal. Parte General.* Bogotá, Colombia.: Editorial Temis.

López, P. (2006). *Investigación criminal y criminalística.* . Bogotá, Colombia.: Editorial Temis, S.A, .

Marchiori, H. (2005). *Personalidad del Delincuente, sexta Edición.* Mexico: Porrúa.

Márquez, J. M. (2016). *El delito. Aspectos Criminológicos y jurídicos* . Valencia, España.: Editorial Tirant lo Blanch.

Martínez, M. (2017). *Ciberdelitos: Prevención y actuación.* . Tirant lo Blanch.

Mata, J. A., & Martín, G. (2003). *Delitos informáticos.* . Madrid: Editorial Dykinson.

Molina, J. (2019). *Peritaje informático: aspectos técnicos y jurídicos.* . Madrid, España: Editorial Díaz de Santos.

Mora, J. M., Pérez, A., & Rodríguez, J. (2014). *Delitos informáticos.* . Madrid: Editorial Aranzadi.

Morillo, M. &. (2011). *La prueba en el proceso civil.* . Madrid: Thomson Reuters Aranzadi.

Navas, A. (2003). *Tipicidad y Derecho Penal.* México: Editorial Porrúa.

ONU, O. d. (2012). *Recomendación No. 85 del Consejo Económico y Social sobre la delincuencia informática.* Naciones Unidas.

Ortiz, E. (2020). La delincuencia como expresión de la descomposición social. . *Revista de Ciencias Sociales*, 26(1), 1-15.

Pérez, M. (2020). *Ciberamenazas: Prevención y protección.* . Lex Nova.

Plascencia, S. (1995). *La prueba en el proceso penal.* . Quito: Corporación de Estudios y Publicaciones.

Posada, L. (2017). *El cibercrimen.* . Bogotá: Editorial Temis.

Real Academia Española. (2019). *Definición de perito. Diccionario de la lengua española.* Madrid.

Reyes, A., & López, M. (2021). La ciberdelincuencia: un reto para la seguridad internacional. . *Revista de Derecho*, 52(1), 189-214.

Rodríguez, M. (2018). *La prueba digital en el proceso penal.* . Barcelona : Atelier.

Sánchez, J. (2019). *Robo de datos informáticos: Prevención y persecución.* . Aranzadi.

Silva Sánchez, J. M. (1987). *Aproximación al Derecho penal contemporáneo.* . Madrid, España.: Editorial Civitas. .

Silva, A. (1991). *La prueba pericial.* . Buenos Aires, Argentina: Ediciones Jurídicas Europa-América.

SPIFJ. (2014). *Reglamento del Sistema de Peritaje Judicial del Ecuador (SPIFJ).* . Quito, Ecuador: Consejo de la Judicatura.

Suárez Sánchez, M. (2016). *Delitos informáticos: Aspectos jurídicos y criminológicos.* . Editorial Tirant lo Blanch.

Taruffo, M. (2008). *La prueba.* . Madrid: Marcial Pons Ediciones Jurídicas y Sociales.

Torre Campo, J. (1996). *Introducción a la criminología.* Madrid: Editorial Dykinson.

UNE, A. E. (2015). *UNE 197010:2015. Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).* . Madrid: UNE.

UNE, A. E. (2019). *UNE 197001:2019. Criterios generales para la elaboración de informes periciales.* . Madrid: UNE.

UNE, A. E. (20 de enero de 2024). *ISO 9001. (2023). [Norma internacional]*. Obtenido de Asociación Española de Normalización: https://www.iso.org/iso-9001-quality-management.html

Vega, J. (2016). Delitos cibernéticos: una aproximación desde el derecho penal. . *Revista de Derecho Penal*, 2(1), 1-15.

Welzel, H. (2004). *Derecho penal. Parte general.* Granada, España.: Editorial Comares.

Zaffaroni, E. R. (1981). *Manual de Derecho Penal Tomo III* . Buenos Aires, Argentina.: Editorial Ediar.

Zambrano, M. (2019). *Derecho penal. Parte general.* Quito, Ecuador.: Ediciones Legales.

11. Anexos

11.1 Anexo 1

FORMATO DE ENCUESTA A PROFESIONALES DEL DERECHO.

Estimado(a) Abogado(a): por motivo que me encuentro realizando mi Trabajo de Integración Curricular titulado: **"Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos",** solicito a usted de la manera más comedida sírvase dar contestación al siguiente cuestionario, resultados que permitirán obtener información para la culminación de la presente investigación.

Instrucción:

La presente encuesta asociada al proyecto de integración curricular tiene como propósito evaluar la efectividad de los informes parciales específicamente en relación con los delitos informáticos en nuestro país. Además, busca informar sobre la posibilidad de incorporar la norma UNE 197010:2015 al "Reglamento del Sistema Pericial Integral de la Función Judicial". Dicha norma, tiene como objetivo establecer los requisitos formales que deben cumplir los informes y dictámenes periciales en el ámbito de las Tecnologías de la Información y la Comunicación (TIC). Esta medida también proporciona criterios generales para la elaboración de informes y dictámenes periciales, con el fin de garantizar una aplicación más completa y efectiva de los mismos.

CUESTIONARIO:

1. ¿Considera usted que, en nuestro país, la aplicación de los informes periciales en cuanto a delitos informáticos es eficiente?

- Sí
- No

¿Por qué?.....

2. ¿Ha considerado usted que la implementación de estándares reconocidos internacionalmente puede mejorar la credibilidad, reputación y posición de la imagen

corporativa de una organización, al tiempo que ayuda a optimizar procesos y genera ahorros significativos?

- Sí
- No

¿Por qué?.....

3. ¿Está familiarizado con el estándar internacional UNE 197010:2015, diseñado para establecer los requisitos formales de informes y dictámenes periciales en el ámbito de las TIC, sin especificar los métodos y procesos exactos para su elaboración?

- Sí
- No

¿Por qué?.....

4. ¿Considera usted que el Consejo Judicial debería mejorar el formato de los informes periciales, especialmente en casos de delitos informáticos?

- Sí
- No

¿Por qué?.....

5. Si el Consejo Judicial decidiera adoptar el estándar internacional UNE 197010:2015 para la elaboración de informes periciales informáticos, ¿estarías dispuesto a recibir capacitación al respecto?

- Sí
- No

¿Por qué?.....

11.2 Anexo 2

FORMATO DE ENTREVISTA A PROFESIONALES DEL DERECHO.

Estimado(a) Abogado(a): por motivo que me encuentro realizando mi Trabajo de Integración Curricular titulado: **"Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos",** solicito a usted de la manera más comedida sírvase dar contestación al siguiente cuestionario, resultados que permitirán obtener información para la culminación de la presente investigación.

Instrucción:

La presente encuesta asociada al proyecto de integración curricular tiene como propósito evaluar la efectividad de los informes parciales específicamente en relación con los delitos informáticos en nuestro país. Además, busca informar sobre la posibilidad de incorporar la norma UNE 197010:2015 al "Reglamento del Sistema Pericial Integral de la Función Judicial". Dicha norma, tiene como objetivo establecer los requisitos formales que deben cumplir los informes y dictámenes periciales en el ámbito de las Tecnologías de la Información y la Comunicación (TIC). Esta medida también proporciona criterios generales para la elaboración de informes y dictámenes periciales, con el fin de garantizar una aplicación más completa y efectiva de los mismos.

CUESTIONARIO:

6. ¿Qué opinión tiene sobre la importancia de evaluar la efectividad de los informes parciales en relación con los delitos informáticos en nuestro país?

7. ¿Cuál es su percepción sobre cómo la incorporación de la norma UNE 197010:2015 al "Reglamento del Sistema Pericial Integral de la Función Judicial" podría impactar positivamente en la calidad y fiabilidad de los informes y dictámenes periciales en el ámbito de las TIC?

8. ¿Cree usted que la adopción de estándares internacionales como la norma UNE 197010:2015 podría contribuir a una mayor profesionalización y estandarización de los procedimientos periciales en el ámbito de las tecnologías de la información?

9. ¿Qué beneficios considera usted que podría traer consigo la mejora del formato de los informes periciales, especialmente en casos de delitos informáticos, tanto para los actores judiciales como para la sociedad en general?

10. ¿Cómo piensa que la capacitación en la aplicación del estándar internacional UNE 197010:2015 podría mejorar las habilidades y competencias de los peritos informáticos en la elaboración de informes periciales?

11.3 Anexo 3

Documentos referentes a Norma UNE 197010:2015 Obtenida a través del servicio de la Biblioteca de la UPV.Base de datos en Aenormás

norma española

UNE 197010

Septiembre 2015

TÍTULO Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Requisitos Generales Del Informe Pericial - UNE 197010:2015

Sección	Detalle del Contenido por Sección
1.Título, es imprescindible y debe identificar de forma clara e inequívoca el proceso de investigación.	
2.Estructura básica, donde se especifica los contenidos mínimos que debe tener todo informe pericial	• Identificación. • Índice. • Cuerpo del informe. • Anexos (si corresponde).
3.Además de la estructura básica, todo informe pericial TIC debe contener:	• Declaración de imparcialidad. • Juramento o promesa (si procediera). • Conclusiones. • Firma. • Visado (cuando proceda).
4.Paginación, en todas las páginas debe figurar la identificación del informe, el número de página y el total de páginas.	
5.Contenido, la información con la que debe iniciarse el informe es:	• título y su código o referencia de identificación, • nombre del organismo/s a los que se dirige y número de expediente, • nombre y apellidos del perito, su titulación, colegio o entidad a la que pertenece, DNI, domicilio profesional, teléfono y correo electrónico, • nombre, apellidos y documento de identificación del solicitante o representante, • en caso de que se contemple un emplazamiento geográfico concreto, debe indicarse dirección y población y si fuera necesario coordenadas UTM (Universal Transverse Mercator), • nombre y apellidos del letrado y del procurador del solicitante (si procede), • la fecha de emisión del informe o dictamen pericial, • competencia y capacidades del perito o peritos, deben figurar la titulación, formación y experiencia correspondiente a la materia objeto del informe o dictamen, • firma del perito o peritos, si se proporciona el informe en soporte digital, este debe ir firmado digitalmente
6. Declaración de tachas, cuando proceda el perito puede aplicar el sistema de tachas o hacer constar su imparcialidad.	
7. Juramento o promesa, cuando proceda, el perito manifiesta bajo juramento o promesa decir la verdad, que actúa con veracidad y con objetividad y que conoce las sanciones penales en que puede incurrir.	
8. Índice general, este tiene como misión facilitar la localización de todos y cada uno de los capítulos y apartados del informe o dictamen	

norma española

UNE 197010

Septiembre 2015

TÍTULO

Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Sección	Detalle del Contenido por Sección
9. Cuerpo del informe o dictamen pericial, debe ser claramente comprensible por los interesados, especialmente en lo referente a sus objetivos, las investigaciones y las razones que conducen a las conclusiones	• Objeto, indicar la finalidad, esta debe de ser especificada por el solicitante. • Alcance, debe indicar cuestiones planteadas por el solicitante y el ámbito del mismo. • Antecedentes, hay describir los hechos, sucesos o asuntos que se hayan producido anteriormente. • Consideraciones preliminares, se deben enumerar todos los aspectos necesarios para comprender la investigación, así como, la metodología empleada. • Documentos de referencia, este capítulo debe recoger las normas, la buena práctica profesional y la bibliografía citada en el informe. • Terminología y abreviaturas, relación de definiciones técnicas, así como, el significado de las siglas utilizadas en el informe. • Análisis, deben describir los datos de partida y bases establecidas por el solicitante, y los que se deriven de la legislación aplicable, de la investigación realizada, de las referencias, documentos, procedimientos y conservación de las mismas que puedan dar fundamento a las conclusiones del informe. En el próximo apartado se describen los contenidos mínimos de los informes periciales TIC según cada caso. • Conclusiones, describir de manera inequívoca la interpretación técnica y experta resumida. Si el solicitante plantea preguntas concretas, se deberán incluir tanto las preguntas como las respuestas. • Anexos, estos deben ser identificados de manera correlativa y paginados de forma inequívoca.

Fuente: Norma UNE 197010:2015 Obtenida a través del servicio de la Biblioteca de la UPV. Base de datos en Aenormás

norma española

UNE 197010

Septiembre 2015

TÍTULO

Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Contenido Técnico del Informe Pericial Informático - UNE 197010:2015

La norma enumera las evidencias digitales mínimas que deben contener los informes o dictámenespericiales TIC, según su tipología:

1. **Sistemas de Información**
   - Descripción del sistema de información analizado.
   - Gestión de la cadena de custodia.
   - Fecha y hora de intervención.
   - Condiciones de funcionamiento del sistema
   - Medidas que se han tomado para salvaguardar el sistema de información.
   - Procedimiento y documentación.
   - Política de seguridad de la instalación donde está operando el equipo, incluyendo copias deseguridad.
   - Identificación del personal con acceso al equipo, como mínimo el administrador el sistema.
   - Topología de red, cortafuegos, NAT (Network Address Translation), VPN (Virtual Prívate Network),enlaces a internet, entre otros.
   - Normativa aplicada en la instalación afectada.
2. **Autenticación del correo electrónico**
   - Valorar la seguridad del mecanismo de firma electrónica del correo.
   - Si no va firmado, hacer análisis de la cabecera o ver si existe un tercero con copia del mensaje.
   - Cotejo de las cabeceras del correo electrónico con los históricos de los servidores utilizados.
   - Informe del proveedor de internet, si procediera.
3. **Delitos contra la propiedad intelectual e industrial en formato digital. Identificación, manipulación o utilización de:**

- componentes hardware,
- elementos software,
- documentos digitales, películas, vídeos, música y juegos,
- patentes y propiedad intelectual relacionadas con las TIC.

4. **Utilización e identificación de metadatos encontrados en:**
   - correos electrónicos,
   - fotografías y documentos gráficos,
   - documentos electrónicos de texto.

5. **Contenido web**
   - captura de la pantalla en modo gráfico,
   - acta testimonial del contenido,
   - acceso a la página web en cuestión.

6. **Soporte de almacenamiento digital (discos duros, pendrives, memorias SD, etc.) o inventario del contenido,**
   - si se ha iniciado o continuado la cadena de custodia,
   - si se ha realizado copia forense del componente original,
   - si se ha aplicado las claves HASH11 al elemento original y a la copia.

Mg. Yanina Quizhpe Espinoza
Licenciada en Ciencias de Educación mención Inglés
Magister en Traducción y mediación cultural

Celular: 0989805087
Email: yaniqes@icloud.com
Loja, Ecuador 110104

Loja, 6 de julio de 2024

Yo, Lic. Yanina Quizhpe Espinoza, con cédula de identidad 1104337553, docente del Instituto de Idiomas de la Universidad Nacional de Loja, y con master en Traducción, con registro 724187576 en la Senescyt, certifico:

Que tengo el conocimiento y dominio de los idiomas español e inglés y que la traducción del resumen del Trabajo de Integración Curricular **"Desafíos Legales en la Pericia Informática en Ecuador: Análisis de la Efectividad del Informe Pericial en Casos de Delitos Informáticos"**., cuya autoría del estudiante Wilman Daniel Romero Sánchez, con cédula 0706107588, estudiante de la Carrera de Derecho de Facultad Jurídica, Social y Administrativa, perteneciente a la Universidad Nacional de Loja, es verdadero y correcto a mi mejor saber y entender.

Atentamente

YANINA BELEN QUIZHPE ESPINOZA
Firmado digitalmente por YANINA BELEN QUIZHPE ESPINOZA
Fecha: 2024.07.06 20:21:49 -05'00'

Mg. Yanina Quizhpe Espinoza.

Traductora freelance