compAS

Grupo de capacitación e investigación pedagógica

La relación de las ciencias jurídicas y las ciencias forenses

Abg. María Soledad Murillo Ortiz, Mgtr.
Lic. Rosa Andrea Portero Ortiz, Mgtr
Ab. Ambar Murillo Mena. Mgtr.

La relación de las ciencias jurídicas y las ciencias forenses

Abg. María Soledad Murillo Ortiz, Mgtr.
Lic. Rosa Andrea Portero Ortiz, Mgtr
Ab. Ambar Murillo Mena. Mgtr.

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad científica del mismo.

Guayaquil - Ecuador
compasacademico@icloud.com
https://repositorio.grupocompas.com

Murillo, M., Portero, R., Murillo, A. (2024) La relación de las ciencias jurídicas y las ciencias forenses. Editorial Grupo Compás

Compiladora
Abg. Carlos Alcívar Trejo. Mgtr

ISBN: 978-9942-33-781-8

Índice

CAPÍTULO I 5

La seguridad informática y las ciencias forenses con visión jurídica 5

Introducción 5

LA SEGURIDAD INFORMÁTICA Y SUS RELACIONES CON LAS CIENCIAS FORENSES Y JURÍDICAS 7

LA DOCUMENTOLOGÍA, COMO CIENCIA AUXILIAR DEL DERECHO 13

CONCLUSIONES 18

BIBLIOGRAFÍA 20

CAPÍTULO II 26

LA SEGURIDAD JURÍDICA DE LOS MENSAJES DE DATOS 26

INTRODUCCIÓN 26

EL USO DE LAS FIRMAS ELECTRÓNICAS EN DOCUMENTOS PRIVADOS Y PÚBLICOS UTILIZANDO LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC), A TRAVÉS DE MEDIOS ELECTRÓNICOS DE TRANSMISIÓN Y ALMACENAMIENTO DE DATOS. 28

EL MENSAJE DE DATOS-DOCUMENTOS ELECTRÓNICOS ..35

LA PROTECCIÓN DE DATOS EN EL ECUADOR-SEGÚN SU REGULACIÓN NORMATIVA 38

CONCLUISIONES 43

BIBLIOGRAFÍA 44

CAPÍTULO III 51

LOS DELITOS INFORMÁTICOS EN EL ECUADOR-SU RELACIÓN CON LA CRIMINALÍSTICA Y SU TIPIFICACIÓN 51

Introducción 51
LOS DELITOS INFORMÁTICOS Y SUS TIPOS 52
TIPOS DE DELITOS INFORMÁTICOS Y LA INVESTIGACIÓN FORENSE 56
CONCLUSIONES 62
BIBLIOGRAFÍA 64

CAPÍTULO I
La seguridad informática y las ciencias forenses con visión jurídica

Introducción

Acorde a lo señalado por varios autores lograremos revisar cierta literatura que nos permitirá lograr analizar la importancia de la seguridad informática, sus relaciones con las ciencias forenses y el campo jurídico desde los delitos informáticos. Dicho esto, logramos enfocarnos y relacionar, que el análisis forense informático, se podría decir que es "la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística a la tecnología digital, con el fin de apoyar a la justicia en su lucha contra la delincuencia y el crimen, o como recurso especializado en esclarecimiento de incidentes de seguridad informática". (López Delgado, 2007)

De tal manera logramos entender que toda la evidencia digital es cualquier tipo de información que se puede obtener en el lugar del crimen que tenga valor probatorio almacenada o trasmitida de forma digital.

De acuerdo a esto, señalaremos unas definiciones más exactas, que nos permiten vincular con mayor precisión, la importancia del análisis forense, que es un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en

un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad. (Helena Rifà Pous, 2009). De tal manera relacionamos que el uso de las tecnológicas, logran también y permiten realizar los procesos de preservación, colección, análisis y presentación de evidencia digital, de acuerdo a procedimientos técnico-legales preestablecidos, como apoyo a la administración de justicia en la resolución de un caso legal. De esta manera contemplamos que la seguridad informática es importante tener en cuenta que la posibilidad de ver ciertos datos no significa necesariamente que esta exista en verdad; de acuerdo con esto, se puede asegurar que toda información puede provenir de muchos otros sitios, acorde a lo señalado por. (Hidalgo Cajo, 2014).

Al utilizar la informática forense es posible investigar (incluso cuando Internet permite el anonimato y el uso de nombres falsos) quién es el dueño de algún sitio Web, quiénes son los autores de determinados artículos y otros documentos enviados a través de alguna red o publicados en la misma. El rastreo que se realiza trata de indagar quién es y cómo es que realizó el ataque o cualquier otra acción ilícita.

La Informática forense es una rama de las ciencias forenses, que involucra la aplicación de la metodología y la ciencia para

identificar, preservar, recuperar, extraer, documentar e interpretar (Zdziarski, 2008) evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos encontrados en la escena del crimen. (Reith, 2002). Así como también debemos señalar que, el FBI, considera que la Informática forense es la ciencia que se encarga de adquirir, preservar, analizar y presentar los datos que han sido procesados electrónicamente y almacenados en medios electrónicos aplicando técnicas científicas y analíticas, utilizando hardware y software especializado para realizar la tarea. (Noblett M. G., 2000).

LA SEGURIDAD INFORMÁTICA Y SUS RELACIONES CON LAS CIENCIAS FORENSES Y JURÍDICAS

La ciberdelincuencia o Cybercrimen engloba cualquier acto criminal que trata con las computadoras y redes (llamado hacking). Esto incluye los delitos tradicionales realizados a través de Internet. Por ejemplo; los crímenes de odio, el telemarketing, el fraude en Internet, el robo de identidad, y robo de la cuenta de tarjeta de crédito son considerados como delitos cibernéticos cuando las actividades ilegales se cometen mediante el uso de una computadora y el Internet.

En este contexto los elementos informáticos que se disponen en los celulares, las computadoras o los dispositivos de almacenamiento como imágenes, mensajes de texto,

conversaciones de WhatsApp, videos, ubicación, etc. constituyen las evidencias necesarias para resolver diferentes tipos de casos judiciales, en este contexto los elementos informáticos que se disponen en los celulares, las computadoras o los dispositivos de almacenamiento como imágenes, mensajes de texto, conversaciones de WhatsApp, videos, ubicación, etc. constituyen las evidencias necesarias para resolver diferentes tipos de casos judiciales. Por estos motivos se considera que las telecomunicaciones conforman uno de los sectores de más grande desarrollo tecnológico en el planeta. Las novedosas tecnologías brindan grandes ventajas para las comunidades, pero también pueden ser medios para que diversas personas tengan la posibilidad de hacer diferentes tipos de fraudes, mismos que afectan a usuarios.

Cabe señalar que la seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital. Este desarrollo tiene aparejado consigo una serie de problemas, dentro de ellos, se encuentra el uso inadecuado de las tecnologías de la comunicación para cometer delitos (Rifa Pous, 2009), ya que las mismas están presentes en casi todas las actividades del ser humano, así como en instituciones públicas y privadas.

Podríamos definir a la ciencia forense digital, como el uso de principios y métodos científicos, aplicados sobre evidencia

obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal, de tal manera definamos que la extracción de una evidencia digital se realizará a partir de una utilización amplios recursos, por medio de software, hardware o herramientas para este propósito. De este modo, la extracción de una evidencia puede ser realizada a través de los más variados métodos. (Taborda, 2017). Con esta definición citada, podemos citar que es la aplicación de prácticas científicas dentro del proceso legal. Esencialmente esto se traduce en investigadores altamente especializados o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios. (Trejo, 2018).

De esta misma manera debemos ser observadores de como ya se anunció en el presente capítulo, las redes sociales se desarrollan en un ritmo muy fuerte, por lo tanto ya esto es una situación global, por lo tanto y debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la “Teoría del delito”, por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas. (Acevedo Esparza, 2010).

De tal manera y por los avances, debemos identificar que la conducta del ser humano, también va en proyección al igual que el internet y los avances tecnológicos, por lo tanto, concebimos que existen nuevas tendencias, tipos de comportamientos, los cuales provocan que la criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. (C. Alcívar Trejo., 2015).

Por tanto, el término forense lleva implícito el concepto de la defensa de un acto supuestamente delictivo, como medio de prueba legal y como una categoría de exposición pública, por lo cual La ciencia forense es una ciencia aplicada, basada en el estudio de la prueba pericialoindicio1 y fundamentada en principios científicos de otras ciencias. De tal manera los sistemas forenses pueden ser muy variados alrededor del mundo, pudiendo ser muy avanzados en algunos países, y prácticamente no existir, en otros. Es así como encontramos las relaciones de las ciencias forenses, socio-jurídicas, entre otras ya que le permite a un científico de las ciencias forenses, quien puede interpretar datos tales como: lo que halló en la escena del hecho, la causa aparente, cuándo sucedió, o cuáles

fueron las consecuencias de la violencia desenfrenada; un científico forense puede documentar y dar su opinión solamente sobre lo que ha visto, puede determinar si un acto está de acuerdo con la evidencia encontrada o con los testimonios, pero lo que no puede esperarse es que una persona que no sea un científico forense, o que no tenga esa calidad, pueda emitir un informe firme y certero, sin que su opinión resista el escrutinio de abogados y de jueces en el tribunal.

De igual manera hayamos las relaciones desde la Criminalística, como ciencia, descansa sobre los medios y métodos especiales para el descubrimiento, recolección, análisis, investigación y apreciación de las pruebas, con el fin de esclarecer las manifestaciones delictivas; estudia procesos, regularidades, fenómenos y hechos con criterio jurídico, (E., 2010) y se encarga del descubrimiento de los autores de tales hechos y la determinación del valor probatorio de determinadas huellas mediante el análisis integral del suceso, para lograr el esclarecimiento del delito. (C, 2010).

Las telecomunicaciones remotas mutan a una velocidad vertiginosa, dando paso a un nuevon paradigma crítico social desde lo endógeno a la propia comunidad internacional,de tal manera la novísima Red tecnológica 5G y su incidencia en el campo de las ciencias jurídicas, desde el foco del Derecho

penal, constituye un avance sin parangón en la humanidad, dada las connotaciones de ubicuidad en los sistemas de información y comunicación activos que envuelven los hardware y software directamente a los componentes tecnológicos. (Andrés, 2023) Por tales motivos ya citados contemplamos que el término criminalística fue introducido en la obra titulada "El Manual del Juez Instructor", publicada en 1892, en Gratz Australia, por eldoctor en derecho Hanns Groos, a quien se le reconoce como el Padre de la Criminalística.

(MONTIEL SOSA, 2002). De tal manera analizamos la relación entre las ciencias, tanto como la criminología y las ciencias forenses se basan en los mismos principios aplicados por las disciplinas científicas y tienen como fin buscar la verdad de los hechos. Por tales motivos consideramos que la investigación forense "es el conjunto de conocimientos teóricos y herramientas metodológicas dirigidas a solucionar los cuestionamientos planteados por el derecho" (Rodas Andrade, 2014). De tal manera que la informática forense ha permitido avances en la investigación de los cyber-crimenes y de las diversas acciones ilícitas que se cometen por medio de la red informática o el internet, y de sus aportaciones se centra en la implementación de la infografía forense, la cual a través de equipo tecnológico, permite la recreación de escenas del crimen y de los hechos que allí surgieron, los cuales tienen

como objetivo ilustrar al juez para poder dictar una sentencia absolutoria o condenatoria.

LA DOCUMENTOLOGÍA, COMO CIENCIA AUXILIAR DEL DERECHO

Las ciencias forenses son un eje transversal para el derecho, por lo tanto, definamos que. La acepción de la palabra documentoscopia posee una formación dual, sus raíces provienen de la locución latina documentum, que significa enseñar, mostrar, informar, testimoniar; y del griego Skopein, que significa observar, examinar, inspeccionar. De tal manera esta ciencia experimental, no sólo analiza un documento y sus medidas de seguridad (Abel Lluch, 2010), sino también se dedica al estudio de todos aquellos textos que contienen manuscritos, incluida las firmas y sus rúbricas, tal y como analiza la grafoscopia. Esta rama de la criminalística, se exige, que la figura del perito o experto tenga la capacidad o competencia en un determinado sector científico (Robles Llorente M. &., 2009). Así como también lo definen: (Del Picchia, 1993) cuya definición se concibe como “la disciplina relativa a la aplicación práctica y metódica de los conocimientos científicos, teniendo como objetivo verificar la autenticidad o determinar la autoría de los documentos”, de igual manera. (Méndez Baquero, 1994), quien define la documentoscopia como “la técnica que trata de establecer,

mediante una metodología propia, la autenticidad de escritos y documentos y determinar, cuando sea posible, la identidad, tal como lo definen varios autores":

De acuerdo a lo señalado por (Serrano García, 1988), la Documentología es el conjunto de estudios referentes a la observación y análisis de los escritos, de igual manera según lo señalado por (Barberá, 1988), quien señala y nos permite descubrir como la ciencia de la documentología se convierte en interdisciplinar y obtenemos a la documentoscopia como "La parte de la Policía Científica que estudia, analiza e investiga mediante metodología e instrumental adecuado, todo tipo de documentos para determinar su autenticidad o falsedad.

Así como también debemos señalar que estas ciencias son utilizadas, tanto por otras ciencias como lo jurídico, así como de igual manera como la criminalística y de hecho parte de esto se logra obtener resultados Constituye un capítulo de la criminalística, con el objetivo específico de verificar la autenticidad o determinar la autoría de los documentosonsiste ésta, así como de las alteraciones y manipulaciones sufridas. (Parra Qujjano, 1987).

Aunque la voz documentoscopia sigue empleándose y poco a poco tiende a sustituírsele por la de documentología, nombre de alcance más amplio, que se considera más apropiado y que también ha sido adoptado por la Organización Internacional

de Policía Criminal, INTERPOL, para distinguir en general los peritajes sobre documentos cuestionados.

Podemos señalar que la documentología facilita durante todo el proceso de la investigación científica la gestión de la información y la documentación interna del proyecto. Aunque esta actividad ha sido realizada tradicionalmente por los propios científicos, a medida que los equipos de investigación crecen y la actividad científica se institucionaliza y se organiza en redes de trabajo amplias y cohesivas, requiere cada vez más la concurrencia de profesionales especializados.

Cabe señalar que las relaciones de estas ciencias son aplicables, basando La Técnica Criminalística, que utiliza por necesidad, los recursos que a través del progreso científico-técnico han estado disponibles y han sido aplicables para esta ciencia. Así, la revolución científico-técnica ha permitido examinar el aspecto relacionado con la adaptación de los medios y métodos de las ciencias naturales, técnicas y otras a la lucha contra el delito.

Considerando por tanto que la Criminalística es “la disciplina que aplica fundamentalmente los conocimientos [...] de las ciencias naturales en el examen del material sensible y significativo relacionado con un presunto hecho delictuoso. (Moreno, 1997). Epistemológicamente, reaviva un esquema que es coherente con la mirada naturalista-empirista de la

ciencia social, en el que se intenta aplicar el modelo de las ciencias naturales al ámbito del mundo social. (Palma, 2012)

Por lo tanto, concebimos que la relación de las ciencias, en este caso la de la Criminalística, la Documentología y el derecho, se basan en la aplicación de la Criminalística, ya que se advierte que éste tiene una clara preponderancia, dado que el principal propósito de la disciplina es aportar a la resolución de un hecho delictivo. Su importancia es tal que tanto el ámbito de innovación y el de evaluación están subsumidos en la praxis profesional. (Streuli, 2018).

De tal manera esto nos permite reconfirmar y llegar a unas primeras conclusiones de las relaciones de estas ciencias, considerando que la diversidad de situaciones en las que incursiona esta disciplina, precisa de un abordaje que recupere múltiples aristas de la actividad científica. En este sentido, resulta útil la noción de (Echeverría, 1995), de que toda actividad científica se sustancia en cuatro contextos: educación, innovación, evaluación y aplicación. En el primero se desarrollan los procesos de enseñanza y aprendizaje. El segundo y el tercero refieren a la producción y validación de los descubrimientos e invenciones en la ciencia respectivamente. El cuarto implica el uso y adecuación de las innovaciones para generar una transformación en el medio.

Es así como varios autores analizan los desafíos educativos de diversas disciplinas dedicadas al estudio del delito, con la relación de estas ciencias, tal es el caso como lo definen. En Argentina,

(Bruquetas Correa, 2019)analiza la formación en una de las áreas de la Criminalística, la Documentología, y destaca que tiene una importante orientación técnica. Desde la tesis de los contextos de la actividad tecnocientífica, la autora describe un contexto de educación dedicado, principalmente, a la formación de sujetos para el contexto de aplicación.

Así se ratifica en este capíyulo y lo citado que la Documentología se aboca al estudio de los documentos en tanto estos puedan suscitar una problemática de índole jurídica. Así como la Criminalística, fundamenta parte de sus intervenciones a través de las ciencias naturales, sin embargo, incorpora entre sus técnicas el estudio de la escritura, principalmente con el fin de identificar al autor de un manuscrito. En este sentido, (Robles Llorente M. A., 2015), hace una revisión integral de estos tipos de análisis, la mayoría implica la detección de peculiaridades inherentes a la grafía que permiten vincularla con un sujeto en específico. El abordaje se distancia de las técnicas de la Química y la Física para tomar su propia impronta, una que tiene por objeto un fenómeno humano difícil de reducir (quizás imposible) a categorías naturalista.

CONCLUSIONES

- La Documentología es una ciencia social con una demarcada estructura interdisciplinar.
- El contexto de aplicación se presenta como dominante de las prácticas disciplinares en la Documentología.
- La documentonomología viene a auxiliar a la propia documentoscopia, considerándosela como parte integrante de ésta.
- La reflexión es indispensable en la construcción del conocimiento científico, debemos considerar desde una mirada superadora, que no se detenga en la cuestión técnica. El dato que se genera responde a una finalidad social, tiene valor porque los sujetos o la comunidad tienen un interés en él.
- La documentonomología – utiliza métodos propios, que divergen de la definición que nos aporta la doctrina científica respecto a la documentoscopia, en cuanto que esta última, únicamente, tiene como objetivo la detección de un documento falsificado por medio del análisis de las divergencias existentes en sus medidas de seguridad, comparadas con las de uno auténtico. En este sentido, consideramos indispensable este neologismo que subsana, dilata y perfecciona, con mayor concreción, esta área de la criminalística.

- No podemos obviar y más bien relacionar que la Documentología, nos permite identificar y aplicar otras ciencias, acorde a el término documento, ya que es empleado en su sentido más amplio, ya que en él, además de expresarse manifestaciones de voluntad o compromisos con efectos dentro del tráfico jurídico fiduciario, pueden derivarse consecuencias jurídicas. (Toledano Toledano, 2008)
- Por esto observamos que el empleo de la documentonomología seremos capaces de detectar documentos falsos y falsificados, documentos robados en blanco, fotocopias falsificadas; e incluso conocer el tratamiento jurídico de documentos de fantasía, ficticios y/o manipulados, así también como de los permisos de conducir provisionales de otros países; y, con ello, y tras su exhibición por parte de un individuo a los miembros de las fuerzas y cuerpos de seguridad, por ejemplo, estar en disposición de detectar un delito de falsedad documental o uno contra la seguridad vial.
- Es evidente las relaciones que existen de estas ciencias que aportan desde lo social, lo jurídico y la aplicación de justicia para el Estado.

BIBLIOGRAFÍA

Abel Lluch, X. (2010). *Estudios prácticos sobre los medios de prueba*. Barcelona : Bosh.

Acevedo Esparza, P. J. (2010). Tecnología e Informática. *Colegio Técnico Industrial José Elias Puyanaarea*, Puyo.

Andrés, C. B. (2023). La red 5G y su impacto en las ciencias jurídicas desde la perspectiva penal. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas. Año VIII. Vol. VIII. Nº 15.*, 22-37.

Barberá, F. A.-D. (1988). *"Manual de técnica policial"*. Valencia: Ed. Tirant Lo Blanch.

Bruquetas Correa, E. (2019). *Un debate acerca del estatus Epistemológico y Metodológico de la Documentología*. Universidad Nacional del Nordeste. Resistencia. .

C, G. (2010). *Manual de criminalística*. BUENOS AIRES: Ediciones La Rocca.

C. Alcívar Trejo., A. G. (2015). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. *AVANCES, 41*, 41.

Carrascosa, J. y. (1991). *Introducción al Derecho Internacional*. MADRID: Editorial Comares.

CEPAL. (2011). *El gobierno electrónico en la Gestión Pública*. Santiago de Chile: Naciones Unidas.

Chaum, D. (1985). Security without Identification: Card Computers to make Big Brother Obsolete. *Communications of the ACM, 28(10),*, 1030-1044.

Del Picchia, J. &. (1993). *Tratado de documentoscopia*. Buenos Aires : La Rocca.

Docusign. (2021). *¿Es posible falsificar una firma electrónica?* MÉXICO: https://www.docusign.com/es-mx/blog/falsificar-una-firma.

E., L. (2010). *Manual de técnica policíaca*. Valladolid: Maxtor.

Echeverría, J. (1995). *Filosofía de la Ciencia*. AKAL.

Font, A. (2000). *Seguridad y certificación en el comercio electrónico*. Madrid.: Fundación Retevisión.

Helena Rifà Pous, J. S. (2009). *Análisis forense de sistemas informáticos.* . Barcelona.

Hidalgo Cajo, I. (2014). *Análisis Preliminar y diseño de una Herramienta de toma de decisiones como soporte para*

las tareas de Análisis Informático Forense. Tarragona: Información de Tecnología.

Humanos, C. I. (1948). *Declaración Americana de los Derechos y Deberes del Hombre*. Humanos, C. I.

Jara-Grau, J. (2012). Embracing electronic signatures - myths, benefits and tips. *Revista del IX Congreso Internacional de comercio electrónico*. .

Justice, N. I. (2021). *Electronic Crime Scene Investigation Guide: A Guide for First Responders*. NY: United States Department of Justice Office of Justice, 93.

Kent, K. C. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. The National Institute of Standards and Technology.

López Delgado, M. (2007). Análisis Forense Digital. *Journal of Chemical Information and Modeling*, 2,32.

Méndez Baquero, F. (1994). *Documentoscopia. Estudios de policía científica, división de formación y perfeccionamiento de la D.G.P*. Madrid: Ministerio del Interior. Madrid.

MONTIEL SOSA, J. (2002). *Criminalística", Tomo I, Duodécima reimpresión, México*. México: Limusa, S. A.

Moreno, R. (1997). *La criminalística: concepto, objeto, método y fin. En R. Moreno (Ed.), Introducción a la criminalística*. México: Porrúa.

NACIONAL, A. (2008). *CONSTITUCIÓN DEL ECUADOR* . QUITO: CEP.

NACIONAL, A. (2008). *Ley del Sistema Nacional de Registro de Datos Públicos,*. QUITO: CEP.

NACIONAL, A. (2014). *Código Orgánico Integral Penal*. QUITO: CEP.

Nacional, C. (2002). *Ley No. 2002-67*. Quito: CEP.

Nacional., C. (2002). *Ley de comercio electrónico, firmas y mensajes de datos [Ley 67]*. . QUITO: Registro Oficial Suplemento 557 del 17 de abril de 2002. https://bit.ly/3vRrn4A .

Noblett M. G., P. M. (2000). *"FBI"*. New York: "FBI".

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. . *Revista Economía y Política, XIV(28),*, 35–46. .

Palma, H. y. (2012). *Epistemología de las Ciencias Sociales*. Biblos.

Parra Qujjano, J. (1987). *Tratado de la prueba judicial" Tomo III,* . Bogóta: Ed. Librería del Profesional.

Pásara, L. (2006). *El uso de los instrumentos internacionales de derechos humanos en la administración de justicia*. QUITO.

Reith, M. C. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence,Air Force Institute of Technology, Volume 1*, 3.

Rico Carrillo, M. (2005). *Comercio electrónico, internet y Derecho. Segunda*. Bogotá-Colombia.: Legis.

Rifa Pous, H. S. (2009). *Análisis Forense de los Sistemas Informáticos*. Eureca Media.

Robles Llorente, M. &. (2009). *Grafoscopia y pericia caligráfica forense*. Barcelona: Bosh.

Robles Llorente, M. A. (2015). *La escritura y la firma manuscrita como elementos coadyuvantes de la seguridad documental.* Barcelona: Universidad Autónoma de Barcelona.

Rodas Andrade, V. (2014). *La investigación forense en Costa Rica,*.

Serrano García, P. (1988). *Manual de documentoscopia o examen y peritaje de documentos*. MADRID: Imprenta de Justo López.

Streuli, S. (2018). *Construcción y validación de un dispositivo metodológico para la investigación criminalística del lugar del hecho en delitos de narcotráfico*. Universidad Nacional del Nordeste. Resistencia.

Szabo, N. (1994). *The idea of smart contracts*.

Taborda, K. B. (2017). El uso de la informática en la pericia criminal y sus herramientas. *Revista Espacios. Vol. 38, Año 2017. Número 51*, 25.

Toledano Toledano, J. (2008). *Introducción a la documentoscopia, Escola de Prevenció i Seguretat integral,*. Barcelona: Universitat Autònoma de Barcelona.

Trejo, C. A. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *REVISTA ESPACIOS Vol. 39 (Nº 42)* , 15.

Unidas, N. (2015). *Declaración Universal de los Derechos del Hombre*. ONU.

Zdziarski, J. (2008). *iPhone Forensics, Recovering Evidence, Personal Data &*. O‘‘Reilly Media, Inc.

CAPÍTULO II
LA SEGURIDAD JURÍDICA DE LOS MENSAJES DE DATOS

INTRODUCCIÓN

En los últimos años la necesidad de ajustar las situaciones jurídicas de la sociedad a soluciones ágiles y efectivas han puesto a las tecnologías de la información y comunicación a solventar mediante herramientas mejoras en varios aspectos. A lo largo de la historia la celebración de actos jurídicos ha sido un punto contradictorio por alteraciones o modificaciones que puedan sufrir los documentos esto implica la creación de mecanismos de seguridad, que con el tiempo s Las innovaciones en los procesos de formación con TIC`s pasan por definir y utilizar metodologías y técnicas pedagógicas (y de construcción de conocimiento) que desafían y estimulen a los participantes a indagar, investigar, colaborar, tomar decisiones, argumentar, tomar posición, inventar proyectos; reforzando sus capacidades y conocimientos previos y desarrollando las competencias que le servirán para la vida, la ciudadanía activa, la generación de opinión, el emprendimiento y la realización.

Las innovaciones en los procesos de formación con TIC`s pasan por definir y utilizar metodologías y técnicas pedagógicas (y de construcción de conocimiento) que desafían y estimulen a los participantes a indagar, investigar, colaborar, tomar decisiones, argumentar, tomar posición, inventar proyectos; reforzando sus capacidades y conocimientos previos y desarrollando las competencias que le servirán para la vida, la ciudadanía activa, la generación de opinión, el emprendimiento y la realización.

Entendemos que la seguridad jurídica es la previsibilidad de entender los derechos y obligaciones, aquella certeza que tiene la sociedad respecto a sus normativas y autoridades donde el estado garantiza lo consagrado en el marco constitucional.

En referencia a esto una de las problemáticas de la sociedad es la constante falsificación de documentos públicos, acorde a la Fiscalía General del Estado (2021) existen 22.254 denuncias respecto a falsificación y uso de documentos falsos en el Ecuador, sobre este mismo aspecto en el año 2020, existieron 18.916 denuncias. Uno de los elementos más importantes para la validez de un acto jurídico es la voluntad de las partes que se refleja con la firma de los contrayentes en cualquier documento, más en el caso de documentos públicos las firmas son un elemento sine qua non para validez de los mismos tanto

de los contrayentes como de la autoridad que da fe pública a dichos documentos.

Lo que nos lleva a establecer como objeto de esta investigación la seguridad jurídica de los documentos públicos. Estableciendo como objetivo general analizar los distintos tipos de firmas y la seguridad jurídica que aporta el uso de los mismos en documentos públicos. Con la finalidad de abordar este objetivo se plantean los siguientes objetivos específicos: Describir los distintos tipos de firmas; Identificar en la normativa en la legislación ecuatoriana respecto el uso de los distintos tipos de firmas en documentos públicos; y Caracterizar los niveles de seguridad de dichas firmas para la suscripción de documentos públicos.

EL USO DE LAS FIRMAS ELECTRÓNICAS EN DOCUMENTOS PRIVADOS Y PÚBLICOS UTILIZANDO LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC), A TRAVÉS DE MEDIOS ELECTRÓNICOS DE TRANSMISIÓN Y ALMACENAMIENTO DE DATOS.

Las redes mundiales de información están transformando al mundo y acercando más a la gente a través de la innovación de las comunicaciones, lo cual posibilita cambios en todos los ámbitos de la actividad humana como la competitividad, el empleo y la calidad de vida de las naciones. Con las nuevas

tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos pueden dirigirse a una audiencia masiva o a un pequeño grupo de expertos y buscar un alcance mundial o meramente local.

Los documentos electrónicos, que hoy día sirven de vía, fundamento y eje de una cada vez más creciente clase de actividades negóciales, comunicacionales, intelectuales, contractuales y de toda índole de las que usa la sociedad contemporánea y que han pasado a ser, por tanto, reconocidas y reguladas por las normas programáticas y especiales de los países.

Conforme a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002) la firma electrónica es la representación de la persona, tal y como la firma de puño y letra, pero emitida por dispositivos electrónicos y que dan fe de los dichos y hechos emitidos en el documento que se suscribe identificando al titular. En otras palabras, el mensaje firmado electrónicamente se vincula directamente con una persona específica teniendo el mismo valor que un documento firmado manuscritamente.

Internet es un medio de comunicación global, que permite el intercambio de información entre los usuarios conectados a la red y que conecta a unos 8 millones de servidores encargados de servicios de información y de todas las operaciones de

comunicación y de retransmisión; llega hasta unos 250 millones de usuarios en más de 100 países. Internet ofrece una oportunidad única, especial y decisiva a organizaciones de cualquier tamaño. La rápida difusión y el gran interés en el mundo de la informática, ha permitido la creación de tecnología Internet/Web, una herramienta fundamental para redes de computadoras y sus usuarios. Internet ofrece un nuevo mercado que define la "economía digital". Los productores, proveedores de bienes/servicios y usuarios logran tener acceso y transmisión mundial de la información y esparcimiento en forma sencilla y económica, sean con fines comerciales o sociales. La apertura de mercados es fundamental para el rápido crecimiento del uso de nuevos servicios y la asimilación de tecnologías nuevas. En la práctica, las empresas están comenzando a usar Internet como un nuevo canal de ventas, sustituyendo las visitas personales, correo y teléfono por pedidos electrónicos, ya que gestionar un pedido por Internet cuesta 5% menos que hacerlo por vías tradicionales. Nace entonces el comercio electrónico, como una alternativa de reducción de costos y una herramienta fundamental en el desempeño empresarial. La organización mundial de Comercio destaca la necesidad de contar con un marco previsible con normas claras que permitan generar confianza en los instrumentos y medios utilizados en el comercio electrónico.

La firma electrónica según (Jara-Grau, 2012), surge como un mecanismo de seguridad en la transmisión de los mensajes de datos en el que implica el uso de tecnologías para firmar un mensaje de datos. Estos mensajes de datos que son vinculados a una persona con su identidad se lo realizan a través de un certificado de firma electrónica, mismo que ofrece las garantías de autenticidad, integridad, no repudio y confidencialidad hasta su extinción.

Sobre la seguridad de la firma electrónica (Docusign., 2021), menciona que utiliza un sistema de protección digital y herramientas como la criptografía, que permite codificar los mensajes de manera que solo el emisor y el remitente tengan acceso. Es así que el artículo 51 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (Ley de comercio electrónico, firmas y mensajes de datos [Ley 67]. , 2002), menciona el valor de equivalencia funcional de la firma electrónica tiene el mismo valor jurídico de los documentos tradicionales a través de los mensajes de datos conferidos, autorizados y expedidos por y ante autoridad competente.

En el Ecuador, se encuentra regulado por. La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es la encargada de acreditar este tipo de firmas por medio de entidades como el Banco Central, Consejo de Judicatura, Security Data, ANF AC, UANATACA, Dirección General de

Registro Civil, Identificación y Cedulación; y ECLIPSOFT S.A. dentro de la misma norma en el artículo.

Art20.- Certificado de firma electrónica. - Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

El certificado electrónico al ser un mensaje de datos, se lo emite mediante archivo digital o token.

Por lo tanto nos ceñiremos, acorde a lo señalado por: (Carrascosa, 1991), quienes exponen que la firma como signo distintivo y personal, reúne los siguientes elementos funcionales, aplicables también a las firmas electrónicas:

1. La identificación: La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. Este elemento conduce al autor de la firma, y es un proceso pasivo por cuanto dicha función puede hacerse a posteriori o incluso sin el consentimiento del autor.

2. La autentificación: En contraposición a la anterior función, ésta consiste en un proceso activo según el cual el autor expresa su consentimiento sobre un acto jurídico. Es el acto que materializa el consentimiento en los actos jurídicos solemnes. Esto supone un vínculo material entre el escrito y la firma y un vínculo intelectual entre la firma y el texto del documento.

De igual forma y citando a (Rico Carrillo, 2005), que: “Dentro de los componentes básicos de un sistema de certificación electrónica encontramos tres elementos:

(1) el uso de la firma electrónica,

(2) la presencia de un tercero de confianza –el prestador de servicios de certificación, comúnmente conocido por las siglas PSC– y

(3) la emisión de un documento que respalde esa firma; el certificado electrónico”.

Por su parte, (Font, 2000), quien expone que “un certificado digital es una credencial electrónica emitida y firmada (digitalmente) por una Autoridad de Certificación. El certificado digital contiene la clave pública de una determinada persona o identidad a la que queda vinculada”.

Por su parte, las legislaciones europeas han definido al certificado electrónico de la siguiente manera: en primer lugar, España en la Ley 59/2003 de 19 de diciembre sobre firma electrónica, lo define en el artículo 6, así: “Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad”.

Por su parte, en la legislación francesa, en el Decreto Nº 2001-272 del 30 de marzo de 2001, es definida esta institución como: "Article 1: Ausens du présent décret, on entend par: 9. Certificat Électronique: un document sous forme électronique attestant du lien entre les dones de vérification de signatura électronique et un signataire" (Artículo 1: En el sentido del presente decreto, entendemos por: 9. Certificado Electrónico: un documento bajo forma electrónica que atestigua del vínculo entre los dones de comprobación de la firma electrónica y un signatario).

En este mismo sentido, España en la Ley 59/2003, de 19 de diciembre sobre firma electrónica, define al certificado electrónico en el artículo 6, del modo siguiente: "Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad". Asimismo, la Unión Europea en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, define en el artículo 2 a los certificados electrónicos de la siguiente manera: "A los efectos de la presente directiva se entenderá por: 9) Certificado: la certificación electrónica que vincula unos datos

de verificación de firma a una persona y confirma la identidad de ésta".

EL MENSAJE DE DATOS-DOCUMENTOS ELECTRÓNICOS

El mensaje de datos también llamado documento electrónico, tanto desde el punto de vista tecnológico, como desde el punto de vista jurídico, implica la emisión de información la cual puede ser de ciencia, de conocimiento o de voluntad.

Fuera de su definición legal, para los efectos prácticos, el mensaje de datos es un concepto final que agrupa a todos los componentes del documento electrónico, ya que al referirnos al mensaje de datos nos referimos a varios elementos. Un mensaje de datos, por lo tanto, puede estar compuesto por datos en particular, (que a su vez se subdividen en bit y bytes), los mismos se organizan en segmentos, que a su vez se estructuran en un todo comprensible denominado texto, siendo éste el elemento clásico que contiene toda la información de un documento en soporte papel, (tal como la hora, fecha, nombre de empresa, etc.), y finalmente, el anexo de un dato identificador o firma digital."

Los Documentos Electrónicos, representan ser Toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogida en cualquier tipo de

soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Por lo tanto su validez jurídica de los documentos electrónicos, se desarrolla conforme al incremento del uso del Internet, en especial para la celebración de Contratos van surgiendo controversias y conflictos los mismos que requieren de intervención judicial para llegar a un acuerdo entre las partes La mayoría de legislaciones no establecen los contenidos de Ley de comercio electrónico, por lo que las restricciones para la validez jurídica de los documentos electrónicos son estricta o taxativas a los medios de prueba, y en considerando el carácter novedoso y reciente de las nuevas tecnologías de la información y comunicación, en especial el comercio Electrónico. Obviamente no contemplan entre sus medios de prueba a los documentos electrónicos. El problema se acrecienta al recordar el retraso tecnológico en el poder Judicial de muchos países. Así que dificulta enormemente la utilización de los documentos electrónicos como medio de prueba, debido a que los funcionarios no tienen, en la mayoría de las ocasiones la más mínima preparación técnica para optar computadoras y consiguientemente, trabajar con este tipo de documentos.

Cabe señalar que el avance exponencial de las Tecnologías de la Información y Comunicación, en adelante TIC, en los

patrones de comportamiento, hábitos de consumo de los ciudadanos y políticas públicas, genera una oportunidad de crecimiento económico e inclusión social para los países de la región, donde el conocimiento en base a la información se fortalece como el eje transversal de desarrollo, bienestar, progreso, institucionalidad y democracia.

Sin embargo, de esto, el Plan parte de la definición de la Organización de Naciones Unidas (ONU) acogiendo los 7 principios establecidos por la Carta Iberoamericana de Gobierno Electrónico del año 2007 y ampliando estos a 12; propone un modelo que define las cuatro formas principales de relación Gobierno-Ciudadano (G2C), Gobierno-empresa (G2B), Gobierno-Gobierno (G2G) y Gobierno-Servidores Públicos (G2E). Adicionalmente precisa cuatro etapas de maduración definidas por la ONU, que son: emergente, provee información básica en línea; avanzada, incorpora mayores servicios de información y comunicación bidireccional entre el gobierno y el ciudadano; transaccional, permite llevar aplicaciones interactivas y transacciones financieras; conectada, admite la interoperabilidad total entre el gobierno, el ciudadano, la empresa y el mismo gobierno. (CEPAL., 2011), La Comisión Interamericana de Derechos Humanos (1948) indica que, en la Declaración Americana de Derechos y Deberes del Hombre, en su artículo 5 establece que “toda

persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar", hace referencia también a la inviolabilidad del domicilio y la correspondencia. (Humanos, 1948)

Declaración Universal de los Derechos del Hombre (2015) en su artículo 12 "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni ataques a su honra o reputación. Toda persona tiene el derecho a la protección de la ley contra tales ataques o injerencias" (Unidas, 2015).

LA PROTECCIÓN DE DATOS EN EL ECUADOR- SEGÚN SU REGULACIÓN NORMATIVA

La protección de datos personales surge como un mecanismo jurídico para proteger el derecho a la vida privada de las personas en la era de las tecnologías de la información. Sus objetivos principales son: definir a los datos personales; determinar quién es el responsable del tratamiento de datos; regular cuestiones esenciales del tratamiento de datos, tales como la conservación, el acceso, la seguridad, la confidencialidad; y determinar el nivel de protección adecuado para la transferencia de datos personales a otros países.

Son muchos los países del mundo que regulan la protección de datos personales para proteger los derechos de sus ciudadanos,

y fomentar el desarrollo de empresas de servicios, cuyo objeto de negocios es la información.

Las décadas de los ochenta y noventa marcaron el origen en la creación de programas informáticos, expertos como (Chaum, 1985) y (Szabo, 1994), anunciaron al público la creación de un sistema informático de pago, cuyas condiciones se pactan mediante la desmaterialización de un documento al que denominarían años más tarde smart contract. Es en el 2008, cuando se crea, en Estados Unidos, la primera especie de moneda digital, llamada bitcoin, una moneda utilizada al margen del gobierno o banco central, cuyo objetivo sería fundamentalmente la transacción de bienes y servicios. Mientras tanto en Ecuador, es en el año 2002, en el que se publica mediante Registro Oficial Suplemento 557 la Ley de Comercio Electrónico, firmas y mensajes de datos, que regularía por primera vez la contratación electrónica, señalando entre sus artículos, el siguiente: Art. 45 Validez de los contratos electrónicos. -Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos. (Nacional., 2002)

La protección de datos personales en Ecuador está regulada de manera dispersa, imprecisa, y no está enfocada en los desafíos

que presentan las tecnologías de la información. A continuación, revisaremos las normas jurídicas sobre protección de datos personales que existen en Ecuador: Constitución de la República del Ecuador La Constitución instituye la protección de datos personales: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (NACIONAL, CONSTITUCIÓN DEL ECUADOR , 2008), de igual forma lo declara el Art. 66.- Se reconoce y garantizará a las personas: 20) El derecho a la intimidad personal y familiar. (NACIONAL, CONSTITUCIÓN DEL ECUADOR , 2008). Si bien el derecho en principio no ha sido modificado, podemos decir que la legislación que se sustenta en este mismo artículo ha ido permitiendo legislar sobre datos, metadatos además de su uso, también es importante mencionar que se aprecia una independencia formal del derecho, dándole un carácter de autonomía del derecho a la honra y buen nombre. Esto se relaciona con lo declarado por: (Pásara, 2006), quien expresa que las personas tenemos la libertad como derecho, esto permite al hombre elegir su modo de vida, sus opciones políticas y religiosas, creencias, identidad moral, intelectual, física y mental, este poder de elección es en

el que se apoya la democracia. Dentro del ordenamiento jurídico ecuatoriano tenemos garantías jurisdiccionales que garantizan la eficacia del derecho como: La acción de protección, junto con Hábeas Data, que protege específicamente los datos personales, existe otra garantía que sirve para garantizar a las personas su derecho a la intimidad. El Art 88 de la constitución establece el objetivo de este mecanismo de protección: "La acción de protección tendrá por objeto el amparo directo y eficaz de los derechos reconocidos en la Constitución, y podrá interponerse cuando exista una vulneración de derechos constitucionales, por actos u omisiones de cualquier autoridad pública no judicial; contra políticas públicas cuando supongan la privación del goce o ejercicio de los derechos constitucionales; y cuando la violación proceda de una persona particular, si la violación del derecho provoca daño grave". (NACIONAL, CONSTITUCIÓN DEL ECUADOR , 2008)

Así mismo las leyes conexas en el Ecuador, como lo son:

- Ley de comercio electrónico, firmas electrónicas y mensajes de datos Esta ley provee la única definición sobre datos personales existente en la legislación ecuatoriana: "Datos personales: son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley". Como

podemos apreciar, es un concepto que no define de manera apropiada los datos personales. (Nacional, 2002)

- Ley del sistema nacional del registro de datos públicos Esta ley no define los datos personales, pero es muy importante considerarla como parte del engranaje donde tendrá que acoplarse la futura ley ecuatoriana referente a esta materia. Según esta ley, datos públicos son aquellos que constan en los registros de datos públicos, sin hacer una diferencia con datos personales protegidos.
- Art. 13.- De los registros de datos públicos. - Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes. (NACIONAL, Ley del Sistema Nacional de Registro de Datos Públicos,, 2008),
- En nuestro Código Orgánico Integral penal Como norma conexa, cabe mencionar que el Código Orgánico Integral Penal tipifica el delito de violación a la intimidad: La persona que, sin contar con el

consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. (NACIONAL, Código Orgánico Integral Penal, 2014).

CONCLUISIONES

- La transformación y cambio tecnológico forma parte del comportamiento cotidiano de las personas y en especial en el ámbito de la justicia, lo cual exige que los profesionales del Derecho, sean como operadores de justicia, servidores públicos, y de libre ejercicio, se especialicen en esta rama, vertiente, tendencias de aplicación de delitos y acciones públicas y privadas.
- Debe existir una preparación de jueces, funcionarios judiciales, y abogados litigantes respecto al uso de este tipo de medios probatorios ya que la prueba electrónica en la actualidad debe ser fácil acceso, ya que la misma en un futuro cercano debe ser la más utilizadas en la actualidad.

- Ante el inminente avance de los nuevos escenarios en materia contractual se vuelve necesario volver siempre a los principios generales que regulan los derechos inter partes, entre los que prevalecen el de autonomía de la voluntad, buena fe y equivalencia o proporcionalidad entre las partes.
- El desconocimiento de que es y para que se utiliza la firma electrónica, así como también su validez jurídica dentro de los procesos judiciales.

BIBLIOGRAFÍA

Abel Lluch, X. (2010). *Estudios prácticos sobre los medios de prueba*. Barcelona : Bosh.

Acevedo Esparza, P. J. (2010). Tecnología e Informática. *Colegio Técnico Industrial José Elias Puyanaarea*, Puyo.

Andrés, C. B. (2023). La red 5G y su impacto en las ciencias jurídicas desde la perspectiva penal. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas. Año VIII. Vol. VIII. Nº 15.*, 22-37.

Barberá, F. A.-D. (1988). *"Manual de técnica policial"*. Valencia: Ed. Tirant Lo Blanch.

Bruquetas Correa, E. (2019). *Un debate acerca del estatus Epistemológico y Metodológico de la Documentología*. Universidad Nacional del Nordeste. Resistencia. .

C, G. (2010). *Manual de criminalística*. BUENOS AIRES: Ediciones La Rocca.

C. Alcívar Trejo., A. G. (2015). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. *AVANCES, 41*, 41.

Carrascosa, J. y. (1991). *Introducción al Derecho Internacional*. MADRID: Editorial Comares.

CEPAL. (2011). *El gobierno electrónico en la Gestión Pública*. Santiago de Chile: Naciones Unidas.

Chaum, D. (1985). Security without Identification: Card Computers to make Big Brother Obsolete. *Communications of the ACM, 28(10),*, 1030-1044.

Del Picchia, J. &. (1993). *Tratado de documentoscopia*. Buenos Aires : La Rocca.

Docusign. (2021). *¿Es posible falsificar una firma electrónica?* MÉXICO: https://www.docusign.com/es-mx/blog/falsificar-una-firma.

E., L. (2010). *Manual de técnica policíaca*. Valladolid: Maxtor.

Echeverría, J. (1995). *Filosofía de la Ciencia*. AKAL.

Font, A. (2000). *Seguridad y certificación en el comercio electrónico*. Madrid.: Fundación Retevisión.

Helena Rifà Pous, J. S. (2009). *Análisis forense de sistemas informáticos.* . Barcelona.

Hidalgo Cajo, I. (2014). *Análisis Preliminar y diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Informático Forense*. Tarragona: Información de Tecnología.

Humanos, C. I. (1948). *Declaración Americana de los Derechos y Deberes del Hombre*. Humanos, C. I.

Jara-Grau, J. (2012). Embracing electronic signatures - myths, benefits and tips. *Revista del IX Congreso Internacional de comercio electrónico.* .

Justice, N. I. (2021). *Electronic Crime Scene Investigation Guide: A Guide for First Responders*. NY: United States Department of Justice Office of Justice, 93.

Kent, K. C. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. The National Institute of Standards and Technology.

López Delgado, M. (2007). Análisis Forense Digital. *Journal of Chemical Information and Modeling*, 2,32.

Méndez Baquero, F. (1994). *Documentoscopia. Estudios de policía científica, división de formación y perfeccionamiento de la D.G.P.* Madrid: Ministerio del Interior. Madrid.

MONTIEL SOSA, J. (2002). *Criminalística", Tomo I, Duodécima reimpresión, México.* México: Limusa, S. A.

Moreno, R. (1997). *La criminalística: concepto, objeto, método y fin. En R. Moreno (Ed.), Introducción a la criminalística.* México: Porrúa.

NACIONAL, A. (2008). *CONSTITUCIÓN DEL ECUADOR* . QUITO: CEP.

NACIONAL, A. (2008). *Ley del Sistema Nacional de Registro de Datos Públicos,.* QUITO: CEP.

NACIONAL, A. (2014). *Código Orgánico Integral Penal.* QUITO: CEP.

Nacional, C. (2002). *Ley No. 2002-67.* Quito: CEP.

Nacional., C. (2002). *Ley de comercio electrónico, firmas y mensajes de datos [Ley 67].* . QUITO: Registro Oficial Suplemento 557 del 17 de abril de 2002. https://bit.ly/3vRrn4A .

Noblett M. G., P. M. (2000). *"FBI".* New York: "FBI".

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. . *Revista Economía y Política, XIV(28),*, 35–46. .

Palma, H. y. (2012). *Epistemología de las Ciencias Sociales*. Biblos.

Parra Qujjano, J. (1987). *Tratado de la prueba judicial" Tomo III,* . Bogóta: Ed. Librería del Profesional.

Pásara, L. (2006). *El uso de los instrumentos internacionales de derechos humanos en la administración de justicia*. QUITO.

Reith, M. C. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence,Air Force Institute of Technology, Volume 1*, 3.

Rico Carrillo, M. (2005). *Comercio electrónico, internet y Derecho. Segunda*. Bogotá-Colombia.: Legis.

Rifa Pous, H. S. (2009). *Análisis Forense de los Sistemas Informáticos*. Eureca Media.

Robles Llorente, M. &. (2009). *Grafoscopia y pericia caligráfica forense*. Barcelona: Bosh.

Robles Llorente, M. A. (2015). *La escritura y la firma manuscrita como elementos coadyuvantes de la*

seguridad documental. Barcelona: Universidad Autónoma de Barcelona.

Rodas Andrade, V. (2014). *La investigación forense en Costa Rica,.*

Serrano García, P. (1988). *Manual de documentoscopia o examen y peritaje de documentos.* MADRID: Imprenta de Justo López.

Streuli, S. (2018). *Construcción y validación de un dispositivo metodológico para la investigación criminalística del lugar del hecho en delitos de narcotráfico.* Universidad Nacional del Nordeste. Resistencia.

Szabo, N. (1994). *The idea of smart contracts.*

Taborda, K. B. (2017). El uso de la informática en la pericia criminal y sus herramientas. *Revista Espacios. Vol. 38, Año 2017. Número 51*, 25.

Toledano Toledano, J. (2008). *Introducción a la documentoscopia, Escola de Prevenció i Seguretat integral,.* Barcelona: Universitat Autònoma de Barcelona.

Trejo, C. A. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *REVISTA ESPACIOS Vol. 39 (Nº 42)* , 15.

Unidas, N. (2015). *Declaración Universal de los Derechos del Hombre*. ONU.

Zdziarski, J. (2008). *iPhone Forensics, Recovering Evidence, Personal Data &*. O‟Reilly Media, Inc.

CAPÍTULO III
LOS DELITOS INFORMÁTICOS EN EL ECUADOR- SU RELACIÓN CON LA CRIMINALÍSTICA Y SU TIPIFICACIÓN

Introducción

Los delitos informáticos son aquellas actividades ilícitas que: (a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos). (C. Alcívar Trejo., 2015)

El delito informático es toda actividad ilícita cometida mediante el uso de sistemas informáticos u otros dispositivos de comunicación o que tenga como finalidad el robo de información, apropiación del patrimonio económico o intelectual, el fraude financiero, la pornografía infantil, etc., es decir, desde el enfoque del derecho, los delitos informáticos se los puede catalogar como toda conducta típica, antijurídica y culposa que afecta la confidencialidad, integridad, patrimonio, acceso o disponibilidad de los datos de los sistemas informáticos y/o redes de telecomunicación. (Chávez, 2021). El delito informático tiene una característica transnacional cuya naturaleza se constituye de grupos delictivos organizados

radicados en una jurisdicción específica quienes cometen actos ilícitos en otra mientras que los bienes protegidos sustraídos terminan en una tercera (Sviatun, 2021).

LOS DELITOS INFORMÁTICOS Y SUS TIPOS

Consideremos que para partir de que existan las acciones punibles, del individuo y de la sociedad, debemos definir que, para efectos de entender los delitos informáticos, partimos del precepto desde la definición, a lo cual considerando ser, la informática es la ciencia responsable de ordenar, organizar, guardar y custodiar la información. Por lo tanto, la importancia que presta la informática, la ha llevado a estar relacionada con otras áreas de conocimiento como, por ejemplo: la medicina, la arquitectura, la arqueología, la educación, entre otras (Vázquez Gómez, 2012). Por tal motivo considerando que el avance informático ha permitido implementar y utilizar sistemas de información para ejecutar tareas que antes se realizaban manualmente (Acurio Del Pino, 2006).

La ciencia forense digital, como el uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop

DFRWS). La extracción de una evidencia digital se realizará a partir de una utilización amplios recursos, por medio de software, hardware o herramientas para este propósito. De este modo, la extracción de una evidencia puede ser realizada a través de los más variados métodos. (Taborda, 2017)

Según, (C. Alcívar Trejo., 2015), el términose utilizópor primera vez a finales de los añosnoventa del pasado siglo XX. En la medida que el uso de Internet se extendía, también surgían nuevos delitos que se cometían a través delas redes informáticas. Estos delitos se han convertido en un fenómeno global que afecta a todos los países, lo que representanimportantes desafíos para la seguridad de la información y la privacidad de las personas. (Choo, 2011).

Según, (Juca-Maldonado, 2023). En respuesta a este problema, se han desarrollado diversas estrategias para prevenir y combatir los ciberdelitos. Estas estrategias incluyen la mejora de la seguridad de los sistemas informáticos, la educación y concientización de los usuarios sobre los riesgos de seguridad en línea, el fortalecimiento de la cooperación internacional para la persecución de delitos transnacionales y la mejora de la legislación en materia de ciberdelitos.

La tipificación del delito informático en la ley penal responde a elementos tales como el sujeto o autor de la conducta ilícita o delictiva; el medio, el sistema informático; y el objeto, el bien

que produce el beneficio económico o ilícito. (Zambrano Mendieta, 2016).

Considerando que el Derecho surge para dar respuesta a los múltiples problemas relacionados con el empleo de las tecnologías en la informática y la comunicación, así como en su desarrollo (Saltos, 2021).

Entre los delitos reconocidos por las Naciones Unidas, están los fraudes cometidos mediante la manipulación de computadoras, falsificaciones informáticas, daños o modificaciones de programas o datos computarizados, el acceso no autorizado a servicios y sistemas informáticos. En esta línea, es necesario mencionar los delitos de acceso a servicios y sistemas informáticos (Hernández, 2021).

Desde un marco general, En el marco legal internacional, la norma más relevante para establecer la jurisdicción de los delitos informáticos es el Convenio sobre la Ciberdelincuencia conocido también como "Convenio de Budapest", esta normativa proporciona un marco integral y coherente en contra del delito informático y la evidencia electrónica. Esta norma ha sido utilizada como guía para la elaboración de diferentes legislaciones a nivel local sobre el delito informático y también como marco de cooperación internacional entre los países miembros ([COE]., 2022)

Por otro lado, existen otros delitos que también se han cometido en el Ecuador, entre ellos están: la interceptación ilícita, accesos no autorizados, ataques a la integridad de datos y sis-temas, abuso de dispositivos, falsificación y fraude informático, delitos contra la propiedad intelectual y la pornografía infantil. Además, también se han cometido ilícitos la modalidad Skimming y Phishing. (hora., 2014).

De tal manera con lo descrito, podemos indicar la relación, e importancia de la Informática forense en estos procesos, ya que es el conjunto de métodos que en la actualidad sirven de apoyo a la justicia al momento de determinar y enfrentar la gama de delitos informáticos existentes, recopilando, almacenando y mostrando la información procesada y guardada en un medio informático de manera local o remota, (Gutierrez, 2015), de tal manera y tomando la definición de *Davara,* entendemos que existe la criminalidad informática, como "Todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos." (Davara, 1990).

Los delitos informáticos tienen la complejidad del uso de tecnologías lo que ha creado un fenómeno delictivo complejo dando a las ciencias jurídicas un enfoque en el que se interrelacionan varias ciencias y específicamente es el caso de las ciencias forenses las que hoy por hoy cuentan con la rama

de la informática forense como un instrumento para cumplir con el objetivo de esclarecer las acciones punibles en delitos relacionados con la seguridad de los sistemas informáticos, su integridad y sobre todo cumplir con los procedimientos para determinar con legalidad y efectividad lo que ha sucedido en cuanto a la supuesta comisión de un delito o infracción.

La delincuencia informática, se apoya en la manipulación de equipos informáticos o equipos inteligentes y que, aprovechando las redes de conexiones telemáticas y la interconexión de las computadoras como el internet se pueda realizar el cometimiento de un delito. (Acurio, 2007)

Los ciberdelitos afectan a cualquier persona,pero, los gruposmás vulnerables son los niños y adolescentes, quienes utilizan con mayor frecuencia las redes sociales y otras plataformas en línea. Además, las empresas y entidades públicas también son objetivos frecuentes de los ciberdelincuentes. (Castillo-González, 2017).

TIPOS DE DELITOS INFORMÁTICOS Y LA INVESTIGACIÓN FORENSE

La Investigación Forense tiene las siguientes guías a nivel internacional:

- RFC 3227
- IOCE

- DoJ1 y DoJ2
- Hong Kong
- Las herramientas de Software que son las más utilizadas para realizar la investigación
- forense digital son:
- Winhex,
- Hélix,
- Encase

Así de igual forma debemos definir varios conceptos de relación de las ciencias forenses y la norma jurídica:

- Ciberterrorismo: Nye, (De la Corte Ibáñez, 2014), define al ciberterrorismo como acciones ofensivas que se planifican y realizan tomando como blanco gobiernos, estados, sectores de población o poblaciones enteras con el fin de coaccionar e intimidar o generar un profundo impacto psicológico.
- Pornografía infantil: el convenio de Budapest define como pornografía infantil a todo material pornográfico que contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que aparezca con un menor comportándose de una forma sexualmente explicita; imágenes realistas que representan a un menor

comportándose de una forma sexualmente explícita. De tal manera (Ruiz Larrocha, 2017), afirma que hoy en día la pornografía infantil es uno de los negocios que genera más dinero en la red, pues el Internet ha permitido su fácil expansión y ha limitado la identificación y localización de los responsables de este hecho delictivo.

- Delitos Contra la Propiedad Intelectual: La propiedad intelectual se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Las legislaciones protegen a la propiedad intelectual a través de las patentes, el derecho de autor y las marcas (Intelectual., La OMPI por dentro, 2018).
- Delitos de calumnias e injurias: el Internet proporciona la difusión universal de difamaciones, calumnias e injurias. Injuriar y calumniar en Internet supone dar "publicidad" a los insultos, lo cual agrava la calificación de los mismos, puesto que el daño causado a la víctima es mayor que si se lleva a cabo en un ámbito acotado o privado. "Cuando alguien se excede en el ejercicio de su libertad de expresión entramos en el ámbito del delito" (García, 2015). Por tales motivos entendemos que la criminalidad informática es toda acción que implique la utilización indebida de ordenadores o la utilización de

cualquier medio de tecnología, herramientas virtuales, con el fin de cometer un perjuicio.

figura 2 tipos de delitos

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

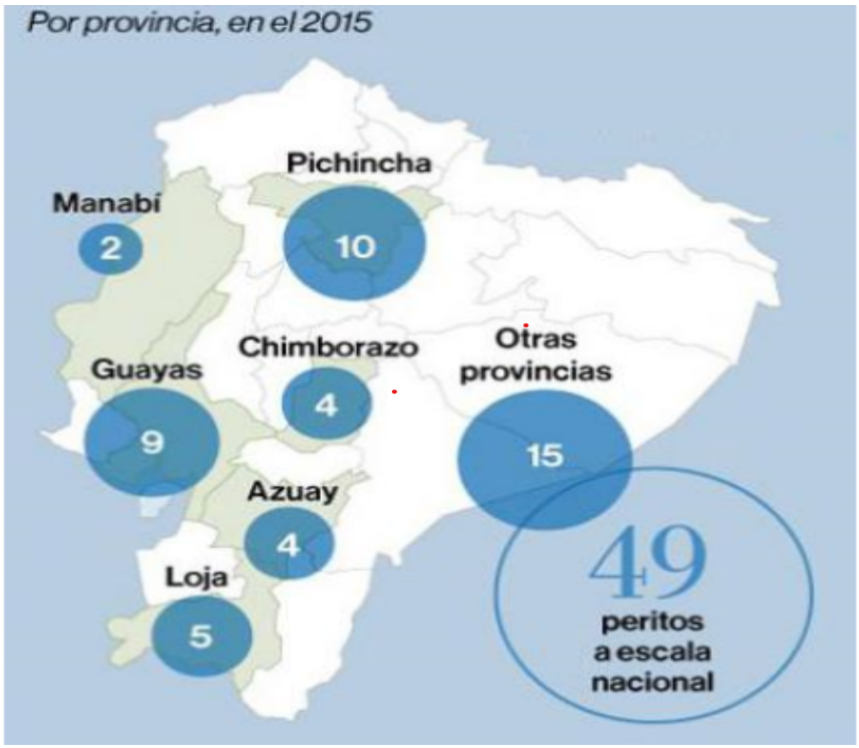
El Código Orgánico Integral Penal en su artículo 500 conceptúa al contenido digital como "todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los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

Orgánico Integral Penal, COIP, 2024). En relación con este tipo de delitos, la legislación penal ecuatoriana, es decir, el Código Orgánico Integral Penal (COIP) establece varios tipos penales que corresponden a delitos informáticos, a partir del Art. 190. Por tanto, es necesario realizar un análisis de la tipicidad subjetiva y la tipicidad objetiva con respecto al Art. 190 del Código Orgánico Integral Penal que trata sobre la apropiación fraudulenta por medios electrónicos, en donde la una hablando de manera general es la conducta del sujeto quien ha logrado vulnerar el derecho a la propiedad y si las mismas han sido realizadas con dolo o culpa, en cambio otra se encuentra el bien jurídico protegido, la acción típica, los sujetos, la relación de casualidad, la imputación objetiva y los elementos descriptivos y normativos. El mencionado artículo 190, tiene como título apropiación fraudulenta por medios electrónicos, esta norma permite entender que cualquier conducta debe cumplir una serie de características para ser calificada como apropiación fraudulenta por medios electrónicos. (NACIONAL, Código Orgánico Integral Penal, 2014).

En el Ecuador el Consejo de la Judicatura (CJ), acredita a los peritos que no solo requieren de conocimientos en informática, sino también en leyes o viceversa. Deben buscar evidencias de un delito y redactar informes técnicos forenses, sin establecer

responsables sin embargo existe déficit de este tipo de profesionales algunas provincias del Ecuador y según estadísticas del CJ a nivel nacional son pocos los peritos registrados. (Trejo, 2018)

Estadísticas de peritos informáticos en Ecuador



Fuente: Consejo de la Judicatura del Ecuador

En términos estadísticos, según el Informe de Amenazas de Seguridad de Internet de Symantec del año2021, se detectaron más de 5,6 mil millones de ataques cibernéticos en todo el

mundo en el 2020, esto representa un aumento del 40% en comparación con el año anterior. (Juca-Maldonado, 2023).

Asimismo, según el mismo informe, los ataques de ransomware aumentaron un 62% en el 2020 respecto al año 2019 y se registraron más de 304 millones de intentos de phishing. (Symantec, 2021).

En cuanto a las medidas que se están tomando, para prevenir y combatir los ciberdelitos en Ecuador, se han implementado una serie de iniciativas y políticas públicas que buscan fortalecer la seguridad digital en el país. (Juca-Maldonado, 2023).

CONCLUSIONES

- La investigación de los ciberdelitos es compleja, debido principalmente al desconocimiento de técnicas en la investigación en los funcionarios públicos y la falta de coordinación interinstitucional del sector a cargo de las telecomunicaciones.
- Los delitos informáticos se han venido desarrollando con el avance de la tecnología y esto hace mucho más complejo poder llegar con los responsable, tanto en estados unidos como en otros de países estos han tenido mucho más auge, teniendo un impacto en los ciudadanos, afectándolos ya sea económicamente

trayendo consigo responsabilidades enormes en cuanto se refiere a deudas con las instituciones, pero no solo así muchos de ellas también han tenido que liderar con la crítica social porque algunas intimidades han sido reveladas. (C. Alcívar Trejo., 2015).

- Implementar capacitaciones, de concientización legal-informático-legal, para el uso seguro y responsable de las nuevas tendencias tecnologías.
- Como sabemos el Derecho al igual que las ciencias forenses, como ciencias no son estáticas, por aquello, su evolución será acorde a los actos del ser, y la sociedad, por aquello, la seguridad de la información juega un papel fundamental en el desarrollo social y económico del país, es hoy por hoy el activo más valioso con el que cuentan las organizaciones, es por ello que los mecanismos, leyes y políticas para el aseguramiento de los derechos y de los derechos vulnerados.
- Entender que el correcto uso de las redes sociales es responsabilidad de todos y esto se logra a través del conocimiento que cada persona.

BIBLIOGRAFÍA

[COE]., C. d. (2022). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia:*. Budapest.

Abel Lluch, X. (2010). *Estudios prácticos sobre los medios de prueba*. Barcelona : Bosh.

Acevedo Esparza, P. J. (2010). Tecnología e Informática. *Colegio Técnico Industrial José Elias Puyanaarea*, Puyo.

Acurio Del Pino, S. (2006). *Delitos Informáticos*. Generalidades. Ecuador.: Generalidades. Ecuador.

Acurio, S. (2007). *Delitos Informáticos: Generalidades*. . ECUADOR: OAS.

Andrés, C. B. (2023). La red 5G y su impacto en las ciencias jurídicas desde la perspectiva penal. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas. Año VIII. Vol. VIII. N° 15.*, 22-37.

Barberá, F. A.-D. (1988). *"Manual de técnica policial"*. Valencia: Ed. Tirant Lo Blanch.

Bruquetas Correa, E. (2019). *Un debate acerca del estatus Epistemológico y Metodológico de la Documentología*. Universidad Nacional del Nordeste. Resistencia. .

C, G. (2010). *Manual de criminalística*. BUENOS AIRES: Ediciones La Rocca.

C. Alcívar Trejo., A. G. (2015). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. *AVANCES, 41*, 41.

Carrascosa, J. y. (1991). *Introducción al Derecho Internacional*. MADRID: Editorial Comares.

Castillo-González, G. (2017). *Plan de continuidad del negocio basado enservicios en la nube para el área de tecnología*. Guatemala: Universidad Galileo.

CEPAL. (2011). *El gobierno electrónico en la Gestión Pública*. Santiago de Chile: Naciones Unidas.

Chaum, D. (1985). Security without Identification: Card Computers to make Big Brother Obsolete. *Communications of the ACM, 28(10),*, 1030-1044.

Chávez, F. (2021). Ciberdelitos: una primera aproximación y proyección institucional. *Perfil criminológico,*, 55-61.

Choo, K. K. (2011). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3(1),*, 37-59.

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

De la Corte Ibáñez, L. &. (2014). *Seguridad nacional, amenazas y respuestas*. España: : LID .

Del Picchia, J. &. (1993). *Tratado de documentoscopia*. Buenos Aires : La Rocca.

Docusign. (2021). *¿Es posible falsificar una firma electrónica?* MÉXICO: https://www.docusign.com/es-mx/blog/falsificar-una-firma.

E., L. (2010). *Manual de técnica policíaca*. Valladolid: Maxtor.

Echeverría, J. (1995). *Filosofía de la Ciencia*. AKAL.

Font, A. (2000). *Seguridad y certificación en el comercio electrónico*. Madrid.: Fundación Retevisión.

García, N. N. (2015). *Cómo actuar si sufres calumnias e injurias en Internet*.

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

Helena Rifà Pous, J. S. (2009). *Análisis forense de sistemas informáticos.* . Barcelona.

Hernández, L. (2021). El delito informático. . *Eguzkilore,* , 227-243.

Hidalgo Cajo, I. (2014). *Análisis Preliminar y diseño de una Herramienta de toma de decisiones como soporte para*

las tareas de Análisis Informático Forense. Tarragona: Información de Tecnología.

hora., L. (2014). *Tasa_de_crecimiento_en_Ecuador_en_el_uso_y_acceso_a_Internet*. Guayaquil: La Hora.

Humanos, C. I. (1948). *Declaración Americana de los Derechos y Deberes del Hombre*. Humanos, C. I.

Intelectual., O. M. (2018). *La OMPI por dentro*.

Intelectual., O. M. (2018). *La OMPI por dentro*.

Jara-Grau, J. (2012). Embracing electronic signatures - myths, benefits and tips. *Revista del IX Congreso Internacional de comercio electrónico*. .

Juca-Maldonado, F. &.-P. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Revista Portal de la Ciencia, 4(2),*, 325-337.

Justice, N. I. (2021). *Electronic Crime Scene Investigation Guide: A Guide for First Responders*. NY: United States Department of Justice Office of Justice, 93.

Kent, K. C. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. The National Institute of Standards and Technology.

López Delgado, M. (2007). Análisis Forense Digital. *Journal of Chemical Information and Modeling*, 2,32.

Méndez Baquero, F. (1994). *Documentoscopia. Estudios de policía científica, división de formación y perfeccionamiento de la D.G.P.* Madrid: Ministerio del Interior. Madrid.

MONTIEL SOSA, J. (2002). *Criminalística", Tomo I, Duodécima reimpresión, México.* México: Limusa, S. A.

Moreno, R. (1997). *La criminalística: concepto, objeto, método y fin. En R. Moreno (Ed.), Introducción a la criminalística.* México: Porrúa.

NACIONAL, A. (2008). *CONSTITUCIÓN DEL ECUADOR* . QUITO: CEP.

NACIONAL, A. (2008). *Ley del Sistema Nacional de Registro de Datos Públicos,.* QUITO: CEP.

NACIONAL, A. (2014). *Código Orgánico Integral Penal.* QUITO: CEP.

NACIONAL, A. (2024). *Código Orgánico Integral Penal, COIP.* QUITO: CEP.

Nacional, C. (2002). *Ley No. 2002-67.* Quito: CEP.

Nacional., C. (2002). *Ley de comercio electrónico, firmas y mensajes de datos [Ley 67].* . QUITO: Registro Oficial Suplemento 557 del 17 de abril de 2002. https://bit.ly/3vRrn4A .

Noblett M. G., P. M. (2000). *"FBI"*. New York: "FBI".

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. . *Revista Economía y Política, XIV(28),*, 35–46. .

Palma, H. y. (2012). *Epistemología de las Ciencias Sociales*. Biblos.

Parra Qujjano, J. (1987). *Tratado de la prueba judicial" Tomo III,* . Bogóta: Ed. Librería del Profesional.

Pásara, L. (2006). *El uso de los instrumentos internacionales de derechos humanos en la administración de justicia*. QUITO.

Reith, M. C. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence,Air Force Institute of Technology, Volume 1*, 3.

Rico Carrillo, M. (2005). *Comercio electrónico, internet y Derecho. Segunda*. Bogotá-Colombia.: Legis.

Rifa Pous, H. S. (2009). *Análisis Forense de los Sistemas Informáticos*. Eureca Media.

Robles Llorente, M. &. (2009). *Grafoscopia y pericia caligráfica forense*. Barcelona: Bosh.

Robles Llorente, M. A. (2015). *La escritura y la firma manuscrita como elementos coadyuvantes de la seguridad documental*. Barcelona: Universidad Autónoma de Barcelona.

Rodas Andrade, V. (2014). *La investigación forense en Costa Rica,*.

Ruiz Larrocha, E. (2017). *Nuevas tendencias en los sistemas de información*. BUENOS AIRES: Editorial Centro de Estudios Ramon Areces SA.

Saltos, M. R. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado, 17(78)*, 343-351.

Serrano García, P. (1988). *Manual de documentoscopia o examen y peritaje de documentos*. MADRID: Imprenta de Justo López.

Streuli, S. (2018). *Construcción y validación de un dispositivo metodológico para la investigación criminalística del lugar del hecho en delitos de narcotráfico*. Universidad Nacional del Nordeste. Resistencia.

Sviatun, O. G. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions On Environment And Development, 18*, 751-762.

Symantec. (2021). *nternet Security Threat Report* .

Szabo, N. (1994). *The idea of smart contracts.*

Taborda, K. B. (2017). El uso de la informática en la pericia criminal y sus herramientas. *Revista Espacios. Vol. 38, Año 2017. Número 51*, 25.

Toledano Toledano, J. (2008). *Introducción a la documentoscopia, Escola de Prevenció i Seguretat integral,.* Barcelona: Universitat Autònoma de Barcelona.

Trejo, C. A. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *REVISTA ESPACIOS Vol. 39 (Nº 42)* , 15.

Unidas, N. (2015). *Declaración Universal de los Derechos del Hombre*. ONU.

Vázquez Gómez, J. B. (2012). *Introducción a la Informática*. México DF: ED TERCER MILENIO .

Zambrano Mendieta, J. E. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las ciencias,* , 204-215.

Zdziarski, J. (2008). *iPhone Forensics, Recovering Evidence, Personal Data &*. O‟Reilly Media, Inc.

Abg. María Soledad Murillo Ortiz, Mgtr.
Abogada de los Tribunales y Juzgados (Ecuador)
Magister en Derecho Notarial y Registral (Ecuador)
Coordinadora Académica de la Carrera de Derecho y Docente
Tiempo Completo de la Facultad de Derecho y Gobernabilidad
De la Universidad Tecnológica ECOTEC, Samborondón, Ecuador
mmurilloo@ecotec.edu.ec
https://orcid.org/0000-0001-6272-5478

Lic. Rosa Andrea Portero Ortiz, Mgtr
https://orcid.org/0000-0001-6272-5478
Coordinadora Académica de la Carrera de Criminalística y Docente
tiempo completo de la Facultad de derecho y Gobernabilidad
Universidad Tecnológica Ecotec, Samborondón,Ecuador,
rportero@ecotec.edu.ec

Ab. Ambar Murillo Mena. Mgtr.
Coordinadora Académica y Docente Titular Tiempo completo de la
Facultad de Derecho y Gobernabilidad de la Universidad
Tecnológica ECOTEC
Phd. (C) Universidad de Córdoba España, en Ciencias Sociales y
Jurídicas
amurillo@ecotec.edu.ec.
Orcid.org/0000-0001-9967-0634

compÁs
Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com