# ESTADO DEL PERITAJE INFORMÁTICO DE LA EVIDENCIA DIGITAL EN EL MARCO DE LA ADMINISTRACIÓN DE LA JUSTICIA EN COLOMBIA

**VIOLETH LASSO VIVAS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, UNAD**
**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**PALMIRA**
**2017**

# ESTADO DEL PERITAJE INFORMÁTICO DE LA EVIDENCIA DIGITAL EN EL MARCO DE LA ADMINISTRACIÓN DE LA JUSTICIA EN COLOMBIA

**VIOLETH LASSO VIVAS**

**Monografía para optar al título de**
**Especialista en Seguridad Informática**

**Asesor**
**Ing. FRANCISCO HILARION**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, UNAD**
**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**PALMIRA**
**2017**

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Palmira, 28 de noviembre de 2017

## AGRADECIMIENTOS

Agradezco primeramente a Dios por su inmenso amor y guía continua, pues es quien me dio la ayuda necesaria para culminar este trabajo académico, proveyéndome la capacidad intelectual, física y emocional para finalizar la especialización en Seguridad Informática.

A mis padres, porque son quienes que me han dado la oportunidad y el apoyo en cada decisión que he tomado en mi vida, acompañándome en cada momento y dándome su amor, consejos y oraciones.

Al director del Trabajo de Grado Ing. Francisco Hilarion, por su acompañamiento durante el desarrollo de este trabajo, su tiempo y colaboración permitieron que fuese posible la culminación de este proyecto.

A la Universidad, mi alma mater, por haber sido un lugar en el cual me forme profesional y personalmente, brindándome las herramientas para alcanzar un logro más en mi vida.

**CONTENIDO**

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE ANEXOS

## TÍTULO

El título del proyecto es “Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”.

# INTRODUCCIÓN

En Colombia se considera la justicia como uno de los principales fines del Estado, sin embargo, no siempre es bien administrada y dependiendo de quien la dicte puede tomar distintos enfoques tanto en su efectividad como en su alcance, aunque existan leyes específicas establecidas para múltiples casos; no obstante, en una nueva era del conocimiento en la que se multiplica el desarrollo social mediante el uso de la tecnología, pues esta ha brindado un espacio en el que se lleva a cabo interacción humana e intercambios sociales, culturales, económicos, científicos, etc., se hizo necesario el desarrollo de leyes y demás normas jurídicas, con el fin de regular la comunicación a través de medios tecnológicos, de manera que sea segura, confiable y permita la judicialización de cualquier acto delictivo que atente contra en bienestar integral de los ciudadanos. Es así como, quienes integran esta rama del poder actúan en función de resolver los conflictos de forma justa, mediante la implementación y uso de las diferentes instancias y normas jurídicas, empleando la imparcialidad, la autonomía judicial, el sistema jurídico establecido, el juicio, la seguridad jurídica, la doble instancia, la fiscalía y el debido proceso, buscando dirimir los conflictos ocasionados por intereses en pugna a fin de lograr y conservar un orden social; pese a ello, debido a la amplia gama de disposiciones legales, se desconoce, en la mayoría de los casos, la forma en como el peritaje informático y la evidencia digital, tienen lugar dentro de la justicia colombiana; por esta razón, con el fin de definir el estado actual del cómo se lleva a cabo la distribución de la justicia bajo la normatividad establecida en relación al peritaje informático, se hizo necesaria la revisión del marco legal para los casos relacionados con la protección de la información y de los datos, con el fin dar a conocer la situación actual.

El presente trabajo tiene como propósito mostrar el estado actual del peritaje informático en Colombia y su lugar dentro de la justicia en el país, mediante el análisis de los retos que enfrenta y su situación tanto en el escenario internacional como interno, precisando la importancia que tiene la información electrónicamente almacenada en el ordenamiento jurídico colombiano, evidenciando la formación con la que cuentan los jueces en el país en temas de delitos informáticos y su implicación en la administración de la justicia, y por ultimo presentando las consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas en el contexto nacional.

Antes de iniciar el desarrollo de la presente investigación, es pertinente la definición de algunos conceptos claves que serán tratados dentro de este estudio; para lo cual, se recurrirá a una breve explicación que describa de forma sencilla cada uno ellos, de modo que puedan ser entendidos por todos los interesados, incluyendo tanto al personal especializado encargado de realizar la investigación

informática, como aquellos que presentaran el caso ante la justicia, de manera que, se cumpla con las exigencias legales, pues se tiene como fin último proporcionar a la víctima del delito informático, quien en última instancia es el centro y motivo de la presente tarea, la protección y preservación de sus derechos, mediante la consolidación de un trabajo, que muestra de manera clara la situación del peritaje de la evidencia digital en el marco de la administración de la justicia en nuestro país, examinando aspectos importantes que permitirán tener una mejor visión del objeto de estudio.

Es necesario conocer que es el peritaje informático y la importancia que tiene dentro de un proceso judicial, y como la evidencia digital se convierte en el eje fundamental la investigación criminal, pues en ella se basa el dictamen realizado por el perito y es la que finalmente permitirá dirimir un caso específico; e igualmente, conocer la relevancia que tiene el derecho informático en el marco de la distribución de la justicia.

Así pues, como resultado del peritaje informático[1] se obtendrá un dictamen expresado por una persona experta, titulada o no, con conocimientos en temas técnicos de las tecnologías de la información, específicamente en el área de la informática forense, sobre los datos contenidos en medios informáticos; cuyo propósito, es describir el análisis de la evidencia electrónica en cuestión, convirtiéndose en un medio de prueba dentro de un determinado proceso judicial, permitiendo esclarecer ciertos asuntos sensibles surgidos en algunas ocasiones, debido a que los conocimientos del juez pueden llegar a resultar ineficientes respecto a determinados elementos técnicos, volviéndose una herramienta valiosa dentro de un litigio o proceso penal, pues permite tratar la controversia brindando certeza en aquellos temas desconocidos por el juez.

La evidencia digital es un medio probatorio valido en la legislación colombiana[2] y abarca cualquier tipo de información extraída de un medio o dispositivo digital y que será útil para resolver un proceso jurídico, dado que permite obtener convicción de la validez de un hecho en particular. La evidencia digital puede ser de distintos tipos como el contenido de un archivo, metadatos, datos de directorio, datos de configuración, datos de logging, material forense (información que contienen los medios de almacenamiento que no es normalmente visible, como los

---

[1] El peritaje informático y la evidencia digital: conceptos, retos y propuestas. Bogotá, CO: Universidad de los Andes, 2010.

[2] La valoración de la evidencia digital en el Código General del Proceso. https://www.ambitojuridico.com/BancoConocimiento/Procesal-y-Disciplinario/la-valoracion-de-la-evidencia-digital-en-el-codigo-general-del-proceso?CodSeccion=1

archivos eliminados), y las interpretaciones de los expertos[3]. Por último, el derecho informático[4], es la disciplina que estudia y regula las relaciones jurídicas, acciones, procesos y aplicaciones que la informática y las tecnologías de la información y comunicación permiten actualmente, mediante el establecimiento de normas, doctrina y jurisprudencia[5].

Dado los fines que se persiguen con el desarrollo de este trabajo, fue necesario implementar un enfoque cualitativo durante la investigación, que permitió abordar las características del objeto de estudio a partir de distintos ángulos, buscando entender la situación actual, llevándose así un estudio de tipo documental, descriptivo y explicativo.

[3] Torrente, Diego, "Conferencia aeec: en busca de una definición para 'prueba electrónica", en E-Newsletter de Cybex , núm. 27, 2007.

[4] Derecho Informático como rama autónoma del derecho. http://derinformatico.uexternado.edu.co/derecho-informatico-como-rama-autonoma-del-derecho/

[5] Flores Salgado, Lucerito. Derecho informático. México, D.F., MX: Grupo Editorial Patria, 2014. ProQuest ebrary. Web.

# 1 PROBLEMA

## 1.1 DEFINICIÓN DEL PROBLEMA

Determinación del estado actual del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia.

## 1.2 DESCRIPCIÓN DEL PROBLEMA

Colombia al ser un estado democrático, cuenta con un ordenamiento jurídico formado por la Constitución Política, como norma suprema, leyes, y demás normas jurídicas del poder ejecutivo, como decretos, reglamentos y otras regulaciones, las cuales tienen como propósito el establecer justicia mediante la aplicación de la norma, es por ello, que se considera la justicia como uno de los fines principales del Estado, sin embargo, no siempre es bien administrada y dependiendo de quien la dicte puede tomar distintos enfoques tanto en su efectividad como en su alcance, aunque existen leyes específicas establecidas para múltiples casos.

Es aquí donde entra en juego la administración de la justicia en relación a la evidencia digital, fruto de la investigación informática realizada mediante el peritaje, en donde aunque se cuenta con muchas disposiciones legales que permiten la ejecución de las normas jurídicas para casos relacionados con la protección de la información y de los datos, es necesario visualizar de manera clara su aplicación dentro del marco legal para la seguridad de la información, a fin de lograr cumplir con las exigencias legales y proporcionar a la víctima del delito la protección y preservación de sus derechos como ciudadano de una nación democrática y libre, acorde con la leyes y disposiciones jurídicas que intentan velar por la validez jurídica y probatoria de la información electrónica, regular su manejo y protegerla.

La revisión de las leyes y demás disposiciones legales que dictaminan la distribución de la justicia en situaciones donde el peritaje informático pasa a ser una herramienta para la presentación de casos ante la justicia, es una necesidad tanto del personal especializado quien realiza la investigación informática, como de quien presenta el caso ante la justicia colombiana, debido a que juega un papel importante el conocer cómo se debe llevar a cabo el proceso actualmente bajo la normatividad establecida por el gobierno, y cuales consideraciones existen sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas para la presentación de la evidencia digital en un caso presentado ante la justicia colombiana.

## 1.3 FORMULACIÓN DEL PROBLEMA

¿Cuál es el estado actual del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia?.

# 2 JUSTIFICACIÓN

La justicia en Colombia busca, mediante la implantación y uso de las diferentes instancias y normas jurídicas, dirimir los conflictos ocasionados por intereses en pugna a fin de lograr y conservar un orden social, de modo que quienes integran esta rama del poder actúan en función de resolver los conflictos de manera justa, mediante la imparcialidad, la autonomía judicial, el sistema jurídico establecido, el juicio, la seguridad jurídica, la doble instancia, la fiscalía y el debido proceso; siendo así, la justicia no podía ignorar una nueva área del conocimiento que permite el desarrollo social, la tecnología, la cual ha surgido en los últimos años proporcionando un espacio donde se lleva a cabo interacción humana e intercambios sociales, culturales, económicos, científicos, etc., mediante el uso de sistemas de comunicación en donde se ven involucrados dispositivos de todo tipo: alámbricos, inalámbricos, online, offline, etc. Es por ello, que se hace necesario el desarrollo de leyes y demás normas jurídicas, con el fin de regular la comunicación a través de medios tecnológicos, de manera que sea segura, confiable y no sea posible el desarrollo den ningún tipo de abuso o acto delictivo que atente contra en bienestar integral de los ciudadanos.

Debido a la amplia gama de disposiciones legales [6] se desconoce, en la mayoría de los casos, la forma en como el peritaje informático y la evidencia digital, resultado del mismo, tiene lugar dentro de la justicia colombiana; por esta razón, con el fin de definir el estado actual del cómo se lleva a cabo la distribución de la justicia bajo la normatividad establecida en relación al peritaje informático y los estándares de manipulación de pruebas para la presentación de la evidencia digital, se hace necesario la revisión del marco legal para casos relacionados con

[6] Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información.

Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales.

Ley 527 de 1999 – Validez jurídica y probatoria de la información electrónica.

Ley 1581 de 2012 – Ley estatutaria de Protección de datos personales.

Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad.

Ley 962 de 2005 – Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

Decreto 2364 de 2012 – Firma electrónica

Decreto 2609 de 2012 – Expediente electrónico

Decreto 2693 de 2012 – Gobierno electrónico

Decreto 1377 de 2013 – Protección de datos personales

la protección de la información y de los datos, con el fin dar a conocer la situación presente.

Al terminar las actividades de investigación se lograra presentar un trabajo que muestre en amplitud y de manera exacta la situación actual del peritaje en Colombia y su lugar dentro de la justicia en el país, proporcionando una herramienta para todos los interesados en llevar a cabo un proceso de peritaje informático, especialmente, personas particulares o entidades del sector privado, los cuales, debido al temor a generar una mala imagen o desconfianza ante sus clientes, no denuncian los casos de cibercrimen en los que se ven involucrados, con el propósito de que no se haga evidente las falencias que tienen tanto en su infraestructura física como lógica o las pérdidas sufridas después del ataque; los cuales, finalmente, realizaran la contratación de personal especializado para realizar la respectiva investigación informática, en otras palabras, los peritos informáticos, y por supuesto aquellos que presentaran el caso ante la justicia, abogados, de modo que cumpla con las exigencias legales y se pueda alcanzar el fin último de proporcionar a la víctima del delito la protección y preservación de sus derechos como ciudadano, es decir, salvaguardar su derecho a la intimidad, derecho a la igualdad, derecho a la libertad personal, derecho a la libertad de conciencia, culto, expresión e información, búsqueda del conocimiento y expresión artística, derecho a la paz, derecho a la honra, derecho de reunión, manifestación, asociación, y participación, derecho a la protección de la familia, derecho a la protección de los niños, derecho a la protección de los adolescentes, derecho de negociación colectiva, derecho a la protección de la propiedad privada e intelectual, y por último el derecho a la justicia.

# 3 OBJETIVOS

## 3.1 OBJETIVO GENERAL

Determinar el estado actual del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia, mediante la revisión de la normatividad vigente, para finalmente, obtener un documento que sirva como herramienta para la adecuada presentación de las pruebas digitales ante las cortes colombianas.

## 3.2 OBJETIVOS ESPECÍFICOS

Analizar los retos y la situación actual del peritaje informático en el escenario internacional y su realidad en Colombia.

Precisar la importancia que tiene la información electrónicamente almacenada en el ordenamiento jurídico colombiano.

Indagar sobre la formación con la que cuentan los jueces en Colombia en temas de delitos informáticos y su implicación en la administración de la justicia.

Investigar las consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas en el contexto nacional.

# 4 MARCO DE REFERENCIA

## 4.1 ANTECEDENTES

Con el propósito de identificar trabajos relacionados con la propuesta planteada, se tomaron algunas investigaciones y trabajos de grado que proponen temáticas similares a las del presente proyecto, como se muestra a continuación.

El informe de investigación de la ITU denominado "Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica" desarrollado por el Prof. Dr. Marco Gercke en acompañamiento del Departamento de Infraestructura, Entorno propicio y Ciberaplicaciones de la Oficina de Desarrollo de las Telecomunicaciones de la ITU, brinda un panorama muy completo de los temas más importantes en relación a los distintos elementos del ciberdelito, mostrando que a raíz de la capacidad transnacional del cibercrimen, los instrumentos jurídicos empleados en los países en desarrollo e industrializados deberían de ser los mismos, de modo que se cuente con herramientas que permitan la cooperación para dar una contundente respuesta legal en cada una de las facetas de esta actividad ilícita. Su objetivo es brindar apoyo a los distintos Estados que deseen comprender mejor el gran avance del ciberdelito en el mundo y sus gravísimas consecuencias en la estabilidad de los países, pues atenta directamente contra uno de los pilares fundamentales de la sociedad, la seguridad.

La investigación “Aproximación a la informática forense y el derecho informático: ámbito colombiano” desarrollado por la Dra. Ana María Mesa Elneser con el apoyo de la Fundación Universitaria Luis Amigo, plantea referentes teóricos relacionados con algunos aspectos internacionales del ciberdelito y la informática forense, desarrollando una visión jurídica sobre la respuesta legal que ha planteado Colombia en cuanto al cibercrimen y un estudio general a la informática forense en el país. Por otra parte, fruto de la investigación se muestra el análisis de la información recolectada a partir de la compilación de los resultados del trabajo investigativo y por último se plantean algunas consideraciones para la evolución del derecho procesal penal en cuanto a la informática forense.

En el trabajo de grado denominado “Estado del análisis forense digital en Colombia” desarrollado por los estudiantes Diego Alejandro Jaramillo Arciniegas y Martha Liliana Torres Moncada de la Universidad Militar Nueva Granada – los autores desarrollan el estudio en base a la revisión de documentos, archivos y otra información recolectada proporcionando un panorama completo de los avances del análisis forense que han tenido lugar en Colombia, ampliando aspectos importantes tales como sus principios, casos de éxito, informática forense,

evidencia digital y la legislación existente para todo lo concerniente a los ciberdelitos.

## 4.2 MARCO CONTEXTUAL

La gran variedad de los sistemas de información que se requieren, adquieren o se encuentran disponibles en las organizaciones, en conjunto con el cambio permanente de las tecnologías de la información y las comunicaciones, ha llevado a grandes cambios y avances en los procesos que se llevan a cabo dentro de las mismas, modificando en muchas ocasiones inclusive las condiciones dadas comúnmente para tener éxito. Estos grandes avances y por ende múltiples cambios han permitido que las empresas, mercados y el mundo en general observen y disfruten de grandes trasformaciones con ventajas incalculables tanto para las personas del común como para las grandes compañías y organizaciones; sin embargo, esto ha traído consigo grandes riesgos y amenazas en escenarios tan utilizados como el internet y las redes de comunicación.

A través de los años se ha evidenciado que los ataques a dispositivos de almacenamiento y procesamiento de información se hacen con más frecuencia y causando un mayor impacto, haciendo uso de las vulnerabilidades existentes que estos presentan, muchas veces inclusive desde su fabricación, provocando que una gran cantidad de datos con un alto valor personal, organizacional, académico, financiero, científico o gubernamental quede expuesto, causando graves daños en el patrimonio de las personas y de las organizaciones, al punto de afectar tanto su dignidad, como honra e inclusive su vida. Por lo cual, se considera que el avance de la tecnología, debido a su gran influencia en casi todas las áreas de desarrollo humano, además de brindar grandes beneficios trae consigo como efecto adverso el surgimiento de comportamientos ilícitos, comúnmente llamados delitos informáticos, los cuales abarcan un gran campo de estudio debido al inminente riesgo que representan.

Este riesgo, es decir, cualquier situación vista como una amenaza que posiblemente pueda derivar en un ataque informático, se incrementó cada vez más a causa del uso extendido de las redes y en especial de internet, pues esta facilita que personas, cuyo propósito es afectar de manera negativa a un tercero, viajen por medios virtuales y realicen todo tipo de actividades ilegales, tales como: La piratería informática, el acceso sin autorización a sistemas de información, la estafa, el sabotaje informático, y muchas otras acciones delictivas que tocan todos los ámbitos de la sociedad, y que afectan tanto a personas particulares de todas las edades como a los entes estatales.

Bajo esta situación distintas compañías a nivel mundial que trabajaban en los escenarios informáticos, iniciaron el desarrollo de instrumentos de sanción y control para evitar que de manera inescrupulosa se empleara la informática para delinquir; sin embargo, en algunos países esta reacción ha tomado más tiempo del esperado, causando que se lleven a cabo situaciones que comprometan de manera importante la información y algunos sistemas vitales. Es por ello, que se convirtió con el paso del tiempo en una necesidad el hacer frente a la delincuencia informática, haciendo que varios países dispusieran de un sistema judicial especializado que permitiera procesar estas acciones ilegales y castigar a quienes las practican.

En el año 2009 Colombia se unió al grupo de países que cuentan con disposiciones legales que permiten judicializar los diferentes delitos informáticos; esto sucedió el 5 de enero de ese año, cuando el Congreso de la República de Colombia promulgó la Ley 1273 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”-, lo cual permitió mediante medios legales preservar integralmente los sistemas que utilizan tecnologías de información y comunicación. Esta ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, lo cual, hizo necesario que las empresas y/o usuarios de los servicios de comunicación conocieran las implicaciones y alcances de la misma para blindarse jurídicamente protegiendo sus derechos y a la vez evitando incurrir en alguno de los delitos establecidos.

Sin embargo, aunque Colombia cuenta con un sistema establecido para castigar las acciones delictivas cometidas mediante el uso de medios de comunicación, el país aún presenta una baja calificación en seguridad en muchos aspectos en comparación con otros países de la región, debido a la poca importancia que se le da a la seguridad informática en la industria en general, mayoritariamente las pyme, y en algunos sectores del gobierno en donde no se refleja el nivel de preocupación necesario para implementar sistemas de protección o políticas de seguridad, lo que ha hecho que el país viva un proceso más lento de lo esperado en cuanto a la implementación de este tipo estrategias.

A lo largo de los años y a partir de las muchas experiencias a nivel mundial con situaciones de delitos informáticos, se ha podido identificar dos grupos específicos de delincuentes que operan en el ciberespacio, en el primero se encuentran, tanto aquellos que saben cómo emplear la tecnología y usan este conocimiento para llevar a cabo acciones ilícitas, como aquellos que no son expertos en este campo y, sin embargo, saben cómo hacer uso de las vulnerabilidades que presentan las plataformas corporativas aprovechándolo para obtener algún tipo de beneficio, y el segundo grupo lo conforman las personas que, por lo general, son empleados de las organizaciones afectadas, conocidos como insiders, cuyas acciones están

enmarcadas dentro de actos delictivos como el robo, borrado o daño de la información sensible de la víctima.

Ante este panorama, como se había mencionado, en Colombia el Congreso de la Republica sancionó la Ley de la Protección de la información y de los datos, a partir de la cual se logró establecer un marco regulatorio que permite sancionar las conductas delictivas relacionadas con la tecnología o que son llevadas a cabo desde medios informáticos. Sin embargo, los expertos en este materia concuerdan que el avance de la tecnología va mucho más rápido que el desarrollo de la legislación, es por ello, que mientras se disponen de normatividades para sancionar las diferentes acciones delictivas existentes, aparecen nuevas y mejores tecnologías diseñadas para pasar por alto las normas establecidas, de lo cual sacan ventaja los ciberdelincuentes; aparte de ello, la poca capacitación y entendimiento en este campo por parte de las entidades y organismos judiciales hacen que el problema se acreciente, por lo que como bien lo dirían "La legislación colombiana de delitos informáticos es suficiente, el problema es de conocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial", según Andrés Guzmán, CEO de la firma Adalid Corp.

En Colombia, actualmente no se cuenta con fiscales ni jueces especializados en delitos informáticos, es decir, si se llegase a presentar algún tipo de situación delictiva la víctima no podría acudir a una Fiscalía especializada en delitos informáticos, por ejemplo; por lo que el reto está en hacer que los jueces comprendan las leyes establecidas en la actualidad y que lo fiscales logren documentar adecuadamente los casos, identificando acorde con la normatividad vigente si las conductas investigadas entran dentro de la tipificación de delitos informáticos.

Para el abogado especialista en Derecho de Telecomunicaciones, Iván Darío Marrugo, el proceso de investigación y peritaje informático es la principal dificultad para procesar este tipo de acciones delictivas, tal como lo manifiesta: "Solo desde hace unos años tenemos una Ley de procedimiento administrativo (Ley 1437 de 2011) y el Código General del Proceso (Ley 1564) que abrió la posibilidad de admitir pruebas electrónicas en este tipo de juicios"; lo cual, abre campo para establecer que el Estado colombiano se encuentra con el deber de capacitar a los distintos organismos judiciales, con el fin de sensibilizarlos y proporcionarles el conocimiento necesario para la apropiación de las temáticas relacionadas con el manejo y uso de las pruebas electrónicas provenientes del uso de las tecnologías de la información.

Dado que el peritaje informático es la herramienta principal que emplea la informática forense para, junto con el derecho, buscar realizar la compensación a la víctima de los daños causados por los criminales, y un adecuado procesamiento judicial de los mismos, proporcionando una vía para su persecución, y la posterior creación y aplicación de las medidas necesarias para la prevención de estos casos, se cuenta con mecanismos empleados a nivel internacional y aceptados actualmente en las cortes colombianas para la presentación de las pruebas, con el propósito de que la manipulación de las mismas se lleve a cabo acorde con las medidas cautelares y disciplinarias para que puedan ser admitidas como pruebas validas dentro de un juicio permitiendo la prosecución criminal, litigación civil, investigaciones, gestión de asuntos relacionados con las corporaciones o el mantenimiento de la ley, dependiendo de las necesidades explicitas de los involucrados.

En Colombia, las compañías que realizan actividades de peritaje informático, cuentan con asignaciones o capacidades específicas para la extracción segura de información y toma de las evidencias digitales, mediante el desarrollo de distintos métodos, tales como: La reconstrucción de los elementos informáticos, la autenticación de la información de los sistemas operativos, la revisión de los datos residuales y la autenticación de los dispositivos con memoria informática, como discos duros, GPS, cámaras, memorias USB, etc.; lo cual permite que, a través de la utilización de un equipo técnico, legal e investigativo, se realice además del análisis pertinente de la evidencia digital la asesoría sobre la viabilidad y pertinencia de las pruebas electrónicas, de modo que, el interesado no mal gaste ni tiempo ni dinero en pruebas innecesarias. Para estas tareas se emplean laboratorios forenses especializados que facilitan el análisis de la evidencia recopilada, los cuales cuentan con equipos y herramientas de última tecnología, ayudando a que la cadena de custodia cumpla con parámetros estrictos, definidos en los formatos internacionales de manejo y presentación de evidencia digital dentro de un litigio judicial, cuyos procesos son soportados y avalados por la Cámara de Comercio, proporcionando así la capacidad de alcanzar altos estándares de seguridad manteniendo la integridad, confiabilidad y validez de las pruebas.

## 4.3 MARCO TEÓRICO

### 4.3.1 Historia del Peritaje Informático

#### 4.3.1.1 El peritaje informático en el mundo

Los inicios del peritaje informático tuvieron lugar en los Estados Unidos en el estado de la Florida, en el año de 1978 cuando se aceptó la informática

forense como una disciplina dentro de la ciencia de la criminología, para reconocer ciertos delitos realizados a través de los sistemas informáticos.

Cuatro años después, en 1982, se desarrolló Copy II PC de Central Point Software, una herramienta que permitía la copia exacta de los disquetes, protegiéndolos de la piratería. Un año más tarde, Peter Norton creo una herramienta para la recuperación de archivos borrados por accidente, entre otras aplicaciones, que se convertirían en pioneras dentro de la informática forense. En 1984, se estableció el Programa de Medios Magnéticos del FBI, conocido actualmente como el equipo de respuesta y análisis de informática CART (Computer Analysis and Response Team).

Más tarde para la década del 90, en el año de 1993, se celebró la primera conferencia sobre la recopilación de pruebas de los equipos, y dos años más tarde nació la organización internacional de evidencia informática IOCE (International Organization on Computer Evidence), cuyo propósito fue convertirse en un punto de encuentro para que expertos de todo el mundo pudieran compartir sus prácticas, permitiendo aunar los avances y esfuerzos alcanzados en esta materia, y mediante la creación de congresos anuales se realizaran intercambios de herramientas, experiencia e información. Durante los años 90, debido a que los computadores pasaron a estar cada vez más en los hogares, los delincuentes empezaron a utilizar estos equipos para cometer delitos, surgiendo así conceptos como el de 'hacker' o 'pirata informático' para denominar a este tipo de criminales. Sin embargo, no fue sino hasta 1994 cuando la informática forense y el perito informático aparecieron como figuras determinantes dentro de un proceso judicial, en el juicio de O. J. Simpsom, que fue uno de los más mediáticos y llamativos de los Estados Unidos, durante el cual hubo muchas contradicciones, puesto que no se contaba con un protocolo único para el tratamiento de la evidencia digital.

En 1996, la INTERPOL se unió para formar parte de la historia, mediante la realización de eventos para el intercambio de conocimientos con otras agencias de investigación, y es así como al año siguiente, se celebró un simposio sobre informática forense.

En 1997, por medio de un comunicado del G7 se reconoció que los funcionarios encargados de hacer cumplir la ley debían tener conocimiento en la forma en que se adquiere la evidencia digital, ocasionando esto, que se desarrollara en el año de 1998, una serie de principios aplicables a la metodología empleada por los peritos de informática forense, de modo que se garantizara la confiabilidad, objetividad e imparcialidad que exigen

los tribunales de justicia en relación con las pruebas presentadas. Es así como, a lo largo de los años se fue perfeccionando la metodología de estudio que se emplea para hacer admisible la evidencia digital en una corte, haciendo que el peritaje informático contara con procesos aceptados a nivel internacional para la presentación de las pruebas electrónicas en un juicio.

Los casos asignados para investigación al grupo CART continúo creciendo, y para el año de 1999, se reportó que el programa abordó 2000 casos individuales, analizando alrededor de 17 terabytes de datos, sin embargo, para el año 2003 el grupo llego a examinar 782 terabytes de datos sólo en ese año, dejando de manifiesto cómo se multiplico no solo el uso de la tecnología para cometer delitos, sino también el avance que se ha experimentado en materia de peritaje informático.

#### 4.3.1.2 El peritaje informático en Colombia

El Colombia el peritaje informático inicio haciendo reflexiones sobre la realidad vivida en otros países, de los cuales Estados Unidos fue uno de los grandes referentes, y es así como en el año 2004 aparece dentro del ordenamiento jurídico colombiano la denominación de perito informático o experto en informática forense, tal como se manifiesta en el artículo 236 del Código de procedimiento penal colombiano. En este mismo año, apareció por primera vez la informática forense como una ciencia de apoyo para las investigaciones judiciales que realiza la Policía Nacional, pues debido al incremento de los delitos informáticos, evidenciado en los problemas de seguridad informática de las empresa y las grandes pérdidas financieras del sector privado, surge el Gabinete de Informática Forense, conocido actualmente como la Dirección de Investigación Criminal e Interpol (DIJÍN), con el fin de brindar apoyo a las labores investigativas forenses, desarrolladas por la Policía, dedicadas específicamente a los medios informáticos. Sin embargo, durante este año no solo se fundó la DIJIN sino que la Contraloría delegada para investigaciones, juicios fiscales y jurisdicción coactiva de la Contraloría General de la Nación decidió crear su propio laboratorio de informática forense, con el propósito de investigar las acciones delictivas cometidas contra el patrimonio del Estado, convirtiéndose así en la primera entidad latinoamericana que contaba con estos instrumentos de investigación elevando su nivel de desarrollo investigativo al igual que organizaciones como la CIA, el FBI, la INTEPOL, y la Agencia de Seguridad Israelí, entre otras.

### 4.3.2 Peritaje Informático

#### 4.3.2.1 Definición

El Peritaje Informático es el estudio e investigación orientado a la obtención de una prueba o evidencia electrónica de aplicación en un asunto judicial o extrajudicial que servirá para decidir sobre la culpabilidad o inocencia de una de las partes.

Los Peritajes Extrajudiciales se dan cuando se requieren para un arbitraje o para un particular, ya sea para aclarar un litigio con otra persona, para conocer más sobre una materia o como consultoría previa antes de presentar una demanda.

El Peritaje Judicial es la investigación orientada a obtener pruebas para presentarlas en un juicio[7].

#### 4.3.2.2 Quien lo realiza

Existen diferentes disciplinas interesadas en la extracción de las evidencias digitales, las cuales se pueden dividir en dos enfoques: Aquellas orientadas en conocer (Peritaje extrajudicial) y las que se centran en probar (Peritaje judicial), la primera de ellas se centran en la obtención de las pruebas únicamente con el propósito de saber, es decir, su punto principal es brindar la información que el interesado desea conocer de una situación específica, como: Que sucedió?, como sucedió?, cuando sucedió?, que perdidas se tuvieron?, si es posible la recuperación, que se puede hacer al respecto?, etc.; la otra, pretende probar una hipótesis mediante la sustentación de un caso frente una corte, por lo que se extreman las medidas de precaución en la captura y tratamiento de la información, de modo que se minimice la posibilidad de que la prueba sea repudiada durante el proceso judicial.

Ahora bien, dependiendo de lo que se pretenda realizar con la obtención de la evidencia digital, es posible que una persona experta, titulada o no, con conocimientos en temas técnicos de las tecnologías de la información,

---

[7] EVIDENCIAS INFORMÁTICAS [online]. Peritaje Informático. Update 2012. [citado 11 mayo 2017]. Available from World Wide Web: URL <http://www.evidenciasinformaticas.com/index.asp?IdContenido=3>.

específicamente en el área de la informática forense, realice actividades de peritaje informático, sin embargo, si lo que se busca es la admisibilidad de la evidencia en una corte, es pertinente recurrir a entidades especializadas en esta tarea. Actualmente, existen diferentes organizaciones encargadas de realizar esta actividad, en el sector privado, para las compañías y particulares en general, hay empresas especializadas en realizar peritaje informático, tanto para quienes solo desean conocer como para aquellos que afrontaran un caso judicial, y en sector público, el encargado de realizar la investigación es la fiscalía, quien junto con el Centro Cibernético Policial (CCP) de la Dirección de Investigación Criminal e Interpol (DIJÍN) se encarga del desarrollo de las actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos en Colombia.

#### 4.3.2.3 Fases del peritaje informático

El peritaje informático cuenta con cinco fases claramente definidas:

1. **Planificación:** Se define lo que se desea conocer y la forma en la que estará orientada la investigación, mediante el establecimiento de los requerimientos del cliente y la evaluación de la pertinencia de la información que será analizada.

2. **Recuperación de la información:** Se recopila toda la documentación existente relacionada con el caso, mediante un reconocimiento pericial, sometiendo a revisión técnica todos los elementos informáticos en cuestión, con el fin de obtener detalles técnicos y datos de comportamiento, a través de la identificación, validación y preservación de los datos adquiridos.

    i. Identificación: Se definen las características físicas del elemento objeto de estudio, mediante el desarrollo de mapas y planos.
    ii. Validación y preservación de los datos adquiridos: Se inicia la cadena de custodia, asegurándose que se conserven altos estándares de calidad (integridad de la información), a través de medidas estrictas de seguridad, mediante la realización de la copia exacta de la información que posiblemente contenga la evidencia digital.

3. **Análisis de los datos:** Se analiza y se busca información a partir de los datos recolectados, mediante el uso de software de análisis forense y equipos especializados.

4. **Desarrollo del informe pericial:** Se desarrolla el informe pericial, tanto en un lenguaje sencillo (para ser interpretado por personas sin conocimientos en informática forense) como en un lenguaje técnico, que mostrara de forma clara los hallazgos fruto de la investigación, mediante la redacción de la interpretación de evidencia obtenida.

5. **Sustentación del informe pericial:** Se lleva a cabo la discusión o defensa del informe, mediante la comparecencia del perito frente al juez, con el objetivo de dar a conocer el trabajo realizado y los resultados obtenidos.

#### 4.3.2.4 Herramientas empleadas

Para la realización del peritaje de la evidencia digital se emplean técnicas de informática forense, las cuales son un conjunto de métodos destinados a adquirir, preservar y presentar la información valiosa extraída de los distintos dispositivos que manejan memoria informática, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta[8].

Los estándares de manipulación son la manera de manipular las pruebas digitales halladas en los análisis forenses, los cuales establecen unas reglas comunes, con el fin de conseguir tratar las evidencias digitales de manera que puedan ser usadas como pruebas válidas dentro de una investigación[9]; para ello, se hace uso de laboratorios de informática forense especializados, los cuales emplean tecnología de punta para la recuperación, procesamiento y almacenamiento de la información que posteriormente será utilizada como evidencia. Estos laboratorios están compuestos por equipos de hardware bastante robustos, que cuentan con chasis redundante, discos duros de estado sólido a la medida, varios procesadores por equipo (alrededor de 12 o más), y una capacidad de

---

[8] POROLLI, Matías. ¿En qué consiste el análisis forense de la información? [online]. Update 12 august 2013. [citado 11 mayo 2017]. Available from World Wide Web: <https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/>.

[9] BARRIO, Marta. Estándares de manipulación de pruebas digitales: RFC 3227 [online]. Update 20 june 2014. [citado 11 mayo 2017]. Available from World Wide Web: <http://wh0s.org/2014/06/20/estandares-de-manipulacion-de-pruebas-digitales-rfc-3227/>.

más de 120 TB de procesamiento, que son combinados con poderosos software forense como FTK, Encase, Nuix, X-ways, Autopsy y Cellebrite, los cuales en conjunto con una red de fibra de última generación (10 Gb Ethernet, actualmente la más rápida existente en el mercado), permiten el tratamiento de grandes cantidades de información disminuyendo el tiempo invertido.

### 4.3.3 Cadena de Custodia

#### 4.3.3.1 Definición

La cadena de custodia es el conjunto de actividades que se despliegan con el fin de verificar la ocurrencia de una posible conducta punible e iniciar la recopilación de la información general para su confirmación; en un caso de peritaje informático, la información que se recopila es conocida como evidencia digital.

Inicia con la recepción de la información, lo cual es desarrollado por la primera autoridad que llega al lugar o lugares de los hechos y personas relacionadas con la ocurrencia del hecho y finaliza con el procedimiento de aseguramiento del lugar de los hechos[10].

#### 4.3.3.2 Evidencia digital

La evidencia digital es uno de los medios probatorios validos en la legislación colombiana[11] y abarca cualquier tipo de información extraída de un medio o dispositivo digital y que será útil para resolver un proceso jurídico, dado que permite obtener convicción de la validez de un hecho en particular.

---

[10] FISCALÍA GENERAL DE LA NACIÓN [online]. Manual de Procedimientos para Cadena de Custodia. [Bogotá D.C., Colombia]. ISBN 958-97542-8-7. Available from World Wide Web: <http://www.fiscalia.gov.co/en/wp-content/uploads/2012/01/manualcadena2.pdf>.

[11] La valoración de la evidencia digital en el Código General del Proceso. https://www.ambitojuridico.com/BancoConocimiento/Procesal-y-Disciplinario/la-valoracion-de-la-evidencia-digital-en-el-codigo-general-del-proceso?CodSeccion=1

La evidencia digital puede ser de distintos tipos, tales como: el contenido de un archivo, metadatos, datos de directorio, datos de configuración, datos de logging, material forense (información que contienen los medios de almacenamiento que no es normalmente visible, como los archivos eliminados), e interpretaciones de los expertos.

## 4.4 MARCO CONCEPTUAL

A continuación, se definen tres de los criterios o variables de la seguridad informática que se aplican a la presente investigación.

### 4.4.1 Integridad

Este trabajo será desarrollado en base a estudios, investigación, e información en general del tema a tratar, la cual estará sustentada por entidades reconocidas como: Universidades, grupos de investigación estatales o empresas privadas de seguridad informática, y que serán debidamente citadas o recopiladas dentro de la bibliografía, garantizando que la información que contiene el documento no ha sido alterada y tiene un respaldo solido reconocido.

### 4.4.2 Disponibilidad

La investigación contara con información actual en relación al peritaje informático dentro del contexto legal colombiano, y se publicara en el repositorio de la universidad, siendo provista como material de consulta para todo el que desee iniciar un proceso de peritaje con implicaciones legales para ser presentado frente a una corte, de modo que pueda ser consultada y utilizada a expensas de las necesidades de los interesados.

### 4.4.3 Trazabilidad

La investigación se desarrollará en orden a obtener una monografía que condense el estado actual del peritaje de la evidencia digital en el marco de la administración de la justicia en Colombia, mostrando los avances correspondientes durante el tiempo previsto para el desarrollo de la misma, acorde con el cronograma de trabajo, en el foro especifico definido por la universidad para la interacción del alumno con el director de proyecto, de forma que cualquier modificación o mejora podrá ser revisada desde su origen.

## 4.5 MARCO LEGAL

Ley 527 de 1999, sobre la validez jurídica y probatoria de la información electrónica, por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación además de dictarse otras disposiciones.

La ley estatutaria 1266 de 2008, en la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, y se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley estatutaria 1581 de 2012 en la cual se dictan disposiciones generales para la protección de datos personales efectuado en territorio colombiano o cuando al responsable del tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Ley 594 de 2000, ley general de archivos y criterios de seguridad, la cual da a conocer los conceptos sobre los distintos tipos de archivos, permitiendo comprender la función archivística, exponiendo la elaboración del documento hasta su eliminación o conservación permanente, además de ello regula el proceder de los funcionarios en relación a cómo se deben archivar y que se debe hacer con los documentos que se generen dentro de una entidad u empresa.

Ley 962 de 2005 por medio de la cual se realiza la simplificación y racionalización de trámite, y se establecen los atributos de seguridad en la información electrónica de entidades públicas.

Decreto 2364 de 2012 sobre la firma electrónica, por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones, en relación al uso del mecanismo de firma electrónica, su creación, métodos empleados y el firmante.

Decreto 2609 de 2012 sobre el expediente electrónico, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 2693 de 2012 sobre gobierno electrónico, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Decreto 1377 de 2013 sobre la protección de datos personales, por el cual se reglamenta parcialmente la Ley 1581 de 2012 y se dictan disposiciones generales para la protección de datos personales, relacionadas con el tratamiento de datos en el ámbito personal o doméstico.

# 5 DISEÑO METODOLÓGICO

## 5.1 METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo de esta investigación se implementara un enfoque cualitativo, con el cual, se abordaran las cualidades del fenómeno planteado, correspondiente a: El estado actual del peritaje informático dentro de la administración de la justicia colombiana, pues se busca entender la situación presente, teniendo en cuenta sus propiedades; por esta razón, se llevaran a cabo distintas tareas, tales como la verificación, revisión y replicación, puesto que el interés es propiamente la cualificación y descripción del fenómeno de estudio.

### 5.1.1 TIPO DE INVESTIGACIÓN

La investigación que se llevara a cabo es de tipo documental, descriptiva y explicativa.

- Documental, es decir, se realizará el análisis de los datos e información recopilada concerniente al tema, con el propósito de comprender el objeto de estudio, para finalmente desarrollar construcciones con sentido a partir del material documental que será sometido a análisis.

- Descriptiva, es decir, se llevará a cabo la interpretación de los contenidos analizados, trabajando sobre realidades de hecho cuyo propósito final es la presentación de una interpretación correcta.

- Explicativa, es decir, se busca dar razón del porqué de los fenómenos, donde la principal preocupación está en determinar las causas u orígenes de los mismos, con el propósito de responder al porque ocurre o que determina la situación actual del fenómeno objeto de estudio.

Las propiedades que se manejaran durante la investigación son la fiabilidad, la sensibilidad, y la validez.

### 5.1.2 POBLACIÓN Y/O MUESTRA

La población es la normatividad y bibliografía sobre el peritaje informático y la presentación de la evidencia digital en las distintas cortes a nivel mundial.

La muestra sobre la cual se llevará a cabo la investigación es la documentación específica, es decir, las leyes y demás dictámenes legales que propenden la protección de la información y de los datos, investigaciones sobre el peritaje, y el proceso de la justicia para los casos en los que interviene el peritaje informático, documentos de actualidad jurídica y procesos de peritaje informático, que aplique para Colombia.

### 5.1.3 TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE DATOS

Dado que la investigación es de enfoque cualitativo conforma una propuesta que empleara técnicas de análisis tales como la exploración, la inducción y la descripción.

## 5.2 METODOLOGÍA DE DESARROLLO

El proceso metodológico que se implementara para el desarrollo se define en tres fases diferenciadas, las cuales se describen a continuación.

1. Fase descriptiva: Se identifica el área problema. Se parte de la lectura del mayor número posible de documentos que presenten explicaciones sobre el fenómeno en estudio. Se busca abordar los diferentes tipos de estudios que se han efectuado, sus referentes disciplinares y teóricos, las poblaciones y muestras, las delimitaciones temporales y contextuales en las que se han desarrollado.

2. Fase interpretativa: Se establece el diálogo entre saberes. Se establecen relaciones entre los argumentos, teorías, tendencias y resultados mostrados en cada documento. No solamente describe los hallazgos, sino que hace interpretaciones de estos. Crea sistemas de hipótesis, elabora categorías y relaciones y da lugar a la construcción de una nueva coherencia teórica en términos estructurales.

3. Fase de construcción: Se expresa una comprensión del área del saber en estudio. Esta fase corresponde a un balance teórico global, en el que se evidencian los vacíos, limitaciones, dificultades, tendencias, posturas y logros en el tema abordado, lo que permite, en primera instancia, conocer su estado actual, señalar nuevos interrogantes para la investigación, formular propuestas, orientar nuevas líneas de investigación, etc.

# 6 RESULTADOS Y DISCUSIÓN

## 6.1 SITUACIÓN ACTUAL Y RETOS DEL PERITAJE INFORMÁTICO

### 6.1.1 Aclaraciones

#### 6.1.1.1 Peritaje Informático

El peritaje informático es un instrumento de investigación empleado dentro de procesos penales e investigaciones privadas con el propósito de recabar pruebas, mediante el uso de herramientas de informática forense, que sean de aplicación en un procedimiento judicial o sirvan para aclarar una hipótesis o conocer más sobre un asunto en particular. Esta investigación centrará su enfoque en el peritaje informático con aplicación a un proceso judicial.

El peritaje informático abarca distintos criterios para cumplir con el objetivo de servir como instrumento para facilitar un veredicto en un juicio, que van desde el procedimiento para la obtención, conservación, análisis y presentación de las pruebas, hasta la admisibilidad de la evidencia digital en los tribunales de justicia.

#### 6.1.1.2 Evidencia Electrónica vs. Evidencia Digital

La Evidencia electrónica, conocida también como prueba electrónica, y la evidencia digital se diferencian entre sí por su rango de cobertura; la primera de ellas abarca la evidencia obtenida mediante el uso de medios análogos y medios digitales, en otras palabras, la evidencia electrónica está constituida por información de cualquier tipo que haya sido almacenada o transmitida por algún medio electrónico ya sea en formato analógico o digital; y, la evidencia digital es aquella almacenada o transmitida de forma digital o binaria, es decir, en formato lógico. Por lo cual, todo lo concerniente a la evidencia electrónica aplica igualmente para la evidencia digital pues esta última se encuentra incluida.

### 6.1.2 En el Escenario Internacional

El delito informático constituye uno de los más grandes desafíos de la justicia penal en el mundo, pues aunque el cibercrimen es claramente una seria amenaza para la sociedad de la información, su diversa y compleja estructura,

maniobrabilidad, y rápido desarrollo, han dificultado la creación de una legislación penal que contemple tan grande estructura criminal y su variado abanico de posibilidades, desarrollándose así una ineficacia en la distribución de las condenas y por supuesto la impunidad junto con la violación de los derechos humanos de las víctimas. Por ello, las fuerzas policiales, órganos fiscales y tribunales penales de todo el mundo han intentado responder a estos nuevos tipos de delito, buscando adecuar la legislación penal existente, en procura de lograr clarificar a partir del modo en cómo son cometidos, su alcance e impacto, con la mira en poder sentenciar un fallo que castigue con el rigor de la ley todo tipo de acción delictiva, que afecte a todos los entes de la sociedad en general; es aquí, donde el peritaje informático juega un papel crucial, pues permite la revisión y el análisis de las pruebas digitales, haciendo posible no solo dirimir un caso particular, sino también crear un precedente que permita determinar un juicio en futuros procesos penales y el desarrollo de una legislación informática que reúna leyes, normas, reglas y procedimientos para lidiar con ellos.

Revisar la situación actual del peritaje de la evidencia digital en los principales países y regiones del mundo se constituye en una necesidad con el fin de entrar en contexto con los retos que enfrenta actualmente esta actividad de manera global, la cual tiene como propósito principal presentar el análisis de la evidencia digital en un juicio, con el objetivo de lograr eliminar la impunidad y brindar la posibilidad de un veredicto que falle a favor de la víctima y condene al perpetrador.

La situación del peritaje informático se puede observar desde dos perspectivas a nivel internacional, tanto dentro de las organizaciones internacionales con carácter universal como dentro de las organizaciones internacionales con carácter regional, distinguiéndose la una de la otra por su tendencia, ya sea hacia la participación abierta de todos los Estados en el mundo, en el primer caso, o hacia una participación restringida de un número limitado de Estados.

Entre las organizaciones internacionales con enfoque universal se encuentra el G7[12] (The Group of Seven, El Grupo de los Siete), compuesto por Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido, igualmente las Naciones Unidas[13] (UN, United Nations), conformada por 193 Estados, y la INTERPOL[14], las cuales son organizaciones que han planteado la necesidad de crear medidas y adoptar métodos o procedimientos de operación para combatir el delito informático, ya sea mediante principios, planes de acción y creación de redes de cooperación 24/7 en el caso del G7 o mediante resoluciones adoptadas

[12] The Group of Seven (G7). https://www.cfr.org/backgrounder/group-seven-g7

[13] Naciones Unidas (UN). http://www.un.org/es/index.html

[14] INTERPOL. https://www.interpol.int/en/

por la Asamblea General de las Naciones Unidas, sin embargo, muy poco se ha acordado de forma conjunta sobre los aspectos relacionados con el peritaje informático, entre los que se encuentran los procedimientos para la obtención de las evidencias digitales, o las regulaciones para que las pruebas sean admitidas en los tribunales.

Entre las organizaciones internacionales de enfoque regional se encuentran la Unión Europea[15] (UE, European Union), el Consejo de Europa[16] (CoE, Council of Europe), la Organización de Cooperación y Desarrollo Económico[17] (OECD, Organization for Economic Co-operation and Development), el Foro de Cooperación Económica Asia-Pacífico[18] (APEC, Asia-Pacific Economic Cooperation), la Commonwealth[19] (Commonwealth of Nations, Mancomunidad de Naciones), la Unión Africana[20] (AU, African Union), la Comunidad de Desarrollo del África Meridional[21] (SADC, Southern African Development Community), la Liga Árabe[22] (AL, Arab League), el Consejo de Cooperación del Golfo[23] (CCASG, Cooperation Council for the Arab States of the Gulf), y la Organización de los Estados Americanos[24] (OAS, Organization of American States).

Aparte de las organizaciones internacionales algunos países han desarrollado de forma independiente procedimientos que son aceptados en las cortes en cuanto a la obtención de la evidencia digital, y solo algunos han establecido un marco jurídico que contemple su admisibilidad.

Aunque las dificultades en cuanto a la aceptación de la evidencia digital, resultado del peritaje informático, en las cortes de todo el mundo son similares pese a los diferentes sistemas jurídicos, y la informática y las tecnologías de red son las herramientas empleadas para cometer los ilícitos de manera internacional, aún no se han establecido de forma armonizada normas jurídicas vinculantes, por lo que

---

[15] La Unión Europea (EU). https://europa.eu/european-union/index_es

[16] Consejo de Europa (CoE). https://www.coe.int/en/web/portal/home

[17] Organización de Cooperación y Desarrollo Económico (OECD). http://www.oecd.org/

[18] Foro de Cooperación Económica Asia-Pacífico (APEC). https://www.direcon.gob.cl/apec/

[19] Commonwealth. http://thecommonwealth.org/

[20] Unión Africana (AU). https://au.int/

[21] Comunidad de Desarrollo del África Meridional (SADC). http://www.sadc.int/

[22] Liga Árabe (AL). http://www.arableagueonline.org/

[23] Consejo de Cooperación del Golfo (CCASG). http://www.gcc-sg.org/

[24] Organización de los Estados Americanos (OAS). http://www.oas.org/es/

se adolece de instrumentos de procedimiento en lo que respecta a la evidencia digital a escala mundial.

Hasta el momento son escasos los países que han iniciado el proceso de actualización de sus legislaciones, con el fin de que las pruebas digitales se consideren de forma directa en los tribunales de justicia, tal como sucede con la evidencia tradicional. Por esto, el presente trabajo se enfocará en organizaciones internacionales, regiones del mundo y Estados específicos que de alguna manera han logrado determinar aspectos concretos y de relevancia sobre el peritaje informático.

#### 6.1.2.1 Organizaciones Internacionales

**Naciones Unidas (UN)**

Las Naciones Unidas es la organización internacional más grande que existe en la actualidad, está compuesta por 193 Estados, los cuales se encuentran representados en el órgano deliberante conocido como Asamblea General. Esta entidad fue fundada con el propósito de tomar decisiones sobre las dificultades que enfrenta la humanidad en relación a aspectos como el mantenimiento de la paz, los derechos humanos, asuntos humanitarios, el desarrollo, y el derecho internacional.

Esta entidad dispone de distintos órganos con el fin de cumplir los objetivos planteados, entre los que se encuentran la Asamblea General, el Consejo de Seguridad, el Consejo Económico y Social, el Consejo de Administración Fiduciaria, la Corte Internacional de Justicia y la Secretaría, los cuales constituyen los seis órganos principales[25]; además de estos, cuenta con organismos especializados[26], que se vinculan a la organización mediante acuerdos de cooperación, por medio del Consejo Económico y Social, entre los que se encuentra la ITU[27] (International Telecommunication Union, Unión Internacional de Telecomunicaciones), que es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC, y quien ha establecido especificaciones sobre políticas y legislación modelo en cuanto a la evidencia electrónica.

---

[25] Órganos Principales de las UN. http://www.un.org/es/sections/about-un/main-organs/index.html

[26] Órganos Especializados de las UN. http://www.un.org/es/aboutun/uninbrief/institutions.shtml

[27] Unión Internacional de Telecomunicaciones (ITU). https://www.itu.int/es/about/Pages/default.aspx

La ITU al ser un organismo autónomo comprometido con conectar a la población mundial, protege y apoya el derecho fundamental de todos de comunicarse, y en miras de cumplir a cabalidad con su labor ha desarrollado distintos proyectos para el Grupo de Estados de África, el Caribe y el Pacífico (ACP), financiados por la Unión Europa y la misma organización, los cuales buscan apoyar la elaboración de políticas y de una legislación, teniendo en cuenta las diferentes prioridades, necesidades y acontecimientos de cada región, es por ello que se promovieron tres subprogramas regionales: el HIPSSA[28] (Harmonization of ICT Policies in Sub-Saharan Africa, Armonización de Políticas TIC en el África subsahariana), el HIPCAR[29], (Harmonization of ICT Policies, Legislation and Regulatory Procedures, Armonización de las políticas de TIC, legislación y procedimientos reglamentarios en el Caribe), y el ICB4PAC[30] (Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries, Creación de capacidades y marcos político, reglamentario y legislativo en materia de TIC para los Estados insulares del Pacífico); de los cuales el HIPCAR nos compete, pues en él se tratan asuntos relacionados con el evidencia digital.

El HIPCAR definió nueve esferas de trabajo, las cuales fueron evaluadas, elaboradas y finalizadas en forma de legislación modelo, directrices o recomendaciones que pueden ser implementadas por cada país individualmente y por la región a nivel mundial, entre las cuales se desarrolló la concerniente a las pruebas por medios electrónicos. En el informe desarrollado por equipos de expertos regionales e internacionales se evaluó la legislación existente en los países beneficiarios que ya hubieran promulgado leyes o resoluciones sobre la evidencia electrónica, entre los cuales se encuentran solo 6 de los 15 países participantes en el estudio, que son: Barbados, Belice, Jamaica, San Vicente y las Granadinas, Trinidad y Tobago, y las Bahamas, información que fue comparada con las mejores prácticas a nivel internacional, y a partir de la cual, se desarrollaron modelos de directrices para políticas y textos legislativos en relación a la prueba por medios electrónicos.

---

[28] Proyecto HIPSSA. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

[29] Proyecto HIPCAR. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx

[30] Proyecto ICB4PAC. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx

Inicialmente se plantearon las directrices que deben seguir los países como modelo para desarrollar las políticas en relación a las pruebas electrónicas, las cuales son:

1) Establecer las interpretaciones comunes necesarias para los términos clave relacionados con la prueba por medios electrónicos.
2) Establecer el marco necesario para definir el origen público o privado y las funciones de las partes encargadas de recopilar y/o gestionar la prueba electrónica.
3) Definir los mandatos jurídicos y las normas a que debe someterse la prueba por medios electrónicos.
4) Proporcionarán una protección adecuada a la prueba por medios electrónicos.
5) Establecer al mismo tiempo el marco de la prueba por medios electrónicos y las políticas públicas sobre los asuntos conexos.[31]

En relación a la admisibilidad de la prueba electrónica, se instituyo lo siguiente:

- Se estableció la no modificación de ninguna disposición fundamentada en el common law[32] o el derecho positivo[33], derechos empleados en los diferentes sistemas jurídicos de los países beneficiarios, en cuanto a la aceptación de los registros[34], excepto por la autenticación de los mismos y la regla de la mejor prueba.

---

[31] La prueba por medios electrónicos: Modelos de directrices para políticas y textos legislativos. HIPCAR Project, ITU. 2012. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/SPANISH%20DOCS/e-evidence_mpg-sp.pdf

[32] Common law. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/common-law/common-law.htm

[33] Derecho positivo. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/derecho-positivo/derecho-positivo.htm

[34] Por “registro”' se entiende cualquier información grabada que ha sido recopilada, creada o recibida durante el inicio, proceso o finalización de una actividad y que cuenta con suficiente contenido, contexto y estructura como para dar cuenta o servir de prueba de dicha actividad o de una transacción, que está inscrita, almacenada o conservada de otro modo en un medio tangible o almacenada en un medio electrónico o de otro y tipo y que es accesible a través de la percepción. (ITU, 2012).

- Se podrá tener en cuenta los principios de admisibilidad de los registros electrónicos[35] establecidos en la ley de cada país.
- Se estableció que la aplicación de la regla de la mejor prueba será considerada solo si se demuestra la integridad del computador en el cual se encontraron almacenados los datos, sin embargo, a menos que se muestre lo contrario se presume como cierta la integridad del mismo.
- Se estableció el principio de aceptación general de las pruebas, puesto que no se puede denegar la admisibilidad de las mismas por el hecho de estar en formato electrónico.
- Se estableció el acuerdo sobre la admisibilidad de la prueba, por lo que un registro electrónico será admisible, sin recelo de lo que decida el tribunal, a menos que otra ley haya dispuesto con anticipación otra cosa.
- Se estableció la carga de probar la autenticidad de la prueba por medios electrónicos por parte de quien introduce el registro electrónico en un procedimiento jurídico, sin embargo, en caso de que se involucre a personas más vulnerables, como los consumidores y los niños, y exista una legislación especial para protegerlos, esta legislación tendrá prioridad.
- Con el fin de determinar si un registro electrónico es admisible, se da lugar a la presentación de pruebas sobre el procedimiento o practica que se empleó para su obtención.
- Se podrá presentar la prueba en forma de declaración jurada[36].
- Se establecieron técnicas y procedimientos alternativos para la presentación de pruebas por medios electrónicos tales como: la certificación por notarios públicos, jueces de paz u otras autoridades competentes, la informática forense en el transcurso del proceso, y la grabación del registro en un soporte que no pueda modificarse.
- Se estableció la admisibilidad de registros electrónicos de otros países.
- Se estableció el reconocimiento de firmas y documentos electrónicos extranjeros.
- Se estableció la interpretación de la ley acorde con los principios internacionalmente aceptados. [37]

[35] Por “registro electrónico” se entiende un conjunto de datos creado, generado, grabado, almacenado, tratado, enviado, comunicado y/o recibido, en cualquier soporte físico, por un ordenador/computador u otro dispositivo similar, y que una persona puede leer o percibir por medio de un sistema informático u otro dispositivo similar, en una pantalla, una versión impresa u otra forma de presentación de esos datos. (ITU, 2012).

[36] Declaración jurada. Definición. 2017. https://definicion.de/declaracion-jurada/

Aunque durante esta etapa del proyecto, se elaboraron políticas modelo y directrices para textos legislativos en relación a la prueba por medios electrónicos, no obstante, la aplicación del mismo se dejó a disposición de cada Estado; además de ello, no se abordó ningún aspecto concerniente a establecer un procedimiento general aceptado para llevar a cabo la obtención de la evidencia.

**INTERPOL**

La INTERPOL es la segunda organización internacional más grande del mundo, conformada por 192 naciones, las cuales componen la mayor organización de policía internacional. Esta institución trabaja en conjunto con los países miembros en la lucha contra el crimen internacional brindando vigilancia, conocimientos y capacidades, y apoyo a tres programas principales de delitos: contraterrorismo, delitos informáticos, y delincuencia organizada y emergente, haciendo uso de una infraestructura de alta tecnología de soporte técnico y operativo que proporciona la capacidad necesaria para enfrentar los crecientes desafíos contra la delincuencia.

El cibercrimen se ha convertido en un área de rápido crecimiento debido a algunas características tales como el anonimato, la velocidad y la comodidad que ofrece internet para la realización de gran cantidad de delitos tanto físicos como virtuales, sin restricciones de frontera, causando un enorme impacto alrededor del mundo y afectando a millones de personas y entidades de todo tipo, generando grandes costos en la economía mundial debido a las enormes e innumerables perdidas que ascienden a miles de millones de dólares. Hoy en día, surgen continuamente nuevas tendencias de delito, a tal punto que existen redes de ciberdelincuencia altamente complejas, conformadas por personas de todo el mundo, unidas para comentar delitos a una escala sin precedentes, maximizando sus ganancias en poco tiempo gracias a las facilidades que ofrece internet. Es aquí donde la INTERPOL en su lucha contra el cibercrimen se asocia con las distintas entidades encargadas de administrar la ley para investigar este tipo de delitos, trabajando de la mano con la

[37] La prueba por medios electrónicos: Modelos de directrices para políticas y textos legislativos. HIPCAR Project, ITU. 2012. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/SPANISH%20DOCS/e-evidence_mpg-sp.pdf

industria privada[38], para proporcionar la inteligencia cibernética necesaria para hacer frente a las distintas formas que existen de perpetrar delitos informáticos transgrediendo la ley.

En cuanto al peritaje informático esta organización a partir del programa sobre Ciberdelincuencia brinda apoyo para el soporte operacional e investigativo, inteligencia cibernética y análisis forense digital, creación de capacidades y revisión nacional sobre el cibercrimen, desde el Complejo Global de Innovación (IGCI, Global Complex for Innovation) ubicado en Singapur e inaugurado en 2014, para la investigación y desarrollo de vanguardia, utilizando tanto la experiencia cibernética mundial de las fuerzas del orden como la ayuda proporcionada por los socios del sector privado, generando resultados basados en modelos de investigación mundialmente aceptados, los cuales son ajustados a la legislación y procedimientos aprobados por las cortes de cada uno de los países miembros.

En el complejo Mundial de INTERPOL para la innovación se halla el centro Cyber Fusion, en donde se encuentra un laboratorio forense digital, un centro de innovación y se congregan varias de las partes interesadas con el propósito de hacer uso de las capacidades policiales de esta organización, ajustando las líneas de acción del programa de Ciberdelincuencia a los otros dos programas mundiales con el objetivo de garantizar un enfoque congruente en la lucha contra las distintas formas de delitos transnacionales. Entre las cinco líneas de acción de este programa dos de ellas se relacionan directamente con el peritaje informático:

- Acceso y Explotación de los Datos Digitales No Procesados. El propósito de INTERPOL es facilitar el acceso a los datos, herramientas y socios, para posibilitar la recopilación de la información y agilizar su explotación.
- Gestión de pruebas Electrónicas. El propósito de INTERPOL es brindar las herramientas forenses digitales y realizar la coordinación mundial para la investigación y enjuiciamiento, a partir de la recopilación legal, conservación y presentación de la evidencia de modo que sea admisible para el sistema judicial.

[38] INTERPOL Y KASPERSKY LAB INTERCAMBIARÁN DATOS PARA COMBATIR EL CIBERCRIMEN. ANTPJI. (2017). https://www.antpji.com/antpji2013/index.php/1131-interpol-y-kaspersky-lab-intercambiaran-datos-para-combatir-el-cibercrimen

Aunque el principal ámbito de acción del programa sobre Ciberdelincuencia de INTERPOL está enfocado a la ciberdelincuencia pura, es decir, a los delitos cometidos contra los equipos y sistemas de información en donde la meta es denegar el acceso a un usuario legítimo o acceder sin autorización a un dispositivo, no obstante, se admite la importancia de actuar contra los delitos cibernéticos en donde el uso de los equipos y sistemas de información se hace para amplificar el delito, como el uso con fines terroristas de las redes sociales y el fraude financiero.

Mediante la investigación proactiva de los delitos emergentes, las últimas técnicas de capacitación, el desarrollo de nuevas herramientas policiales innovadoras, y la combinación de insumos a nivel mundial, esta entidad fortalece las capacidades de investigación de los Estados miembros innovando los resultados y ofreciendo herramientas para detectar y prevenir la comisión de más delitos digitales.

**Consejo de Europa (CoE)**

El Consejo de Europa es una organización ajena a la Unión Europea, conformada por la totalidad de las naciones europeas con excepción de Bielorrusia, empeñada en abogar por la libertad de expresión y de los medios de comunicación, la libertad de reunión, la igualdad y la protección de las minorías, teniendo como principios fundamentales la defensa de los derechos humamos, la democracia y el estado de derecho. El Consejo de Europa ayuda a los Estados miembros a luchar contra la corrupción y el terrorismo y emprender las reformas judiciales necesarias. Su grupo de expertos constitucionales, conocido como la Comisión de Venecia[39], ofrece asesoramiento legal a países de todo el mundo.

Entre las muchas reuniones que se han llevado a cabo desde el Consejo de Europa se han elaborado recomendaciones, directrices, y decisiones de marco en relación a cómo se debería tratar la ciberdelincuencia, llevando a cabo el 23 de noviembre de 2001 la firma del convenio sobre la ciberdelincuencia, conocido como el Convenio de Budapest[40], que en materia de derecho se reconoce como el único acuerdo internacional en relación a disposiciones penales informáticas, el cual se ha constituido en un instrumento importante en la lucha contra el delito informático. Sin

[39] Comisión de Venecia. http://www.venice.coe.int/webforms/events/

[40] Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001. Council of Europe. http://www.oas.org/juridico/english/cyb_pry_convenio.pdf

embargo, a pesar de contar con tal herramienta, que busca la cooperación de los Estados firmantes con el fin de crear una política penal común, mediante la admisión de una legislación adecuada y la colaboración internacional, aún no se ha logrado una definición de común acuerdo sobre el procedimiento que debería seguir el peritaje informático a fin de que la evidencia digital sea admisible en los tribunales de Europa y los Estados que han sido invitados a adherirse al convenio; ni siquiera se cuenta aún con un concepto común sobre lo que constituye una prueba digital, por lo tanto, se ha tenido que recurrir a las definiciones y procedimientos establecidos de forma independiente por los distintos países, y que más se acercan a un mecanismo apropiado que se ajusta a las técnicas con las que actualmente se cuenta para la recolección de la evidencia digital y presentación de la misma ante la autoridad judicial.

El convenio de Budapest si bien no plantea la definición de la terminología, ni establece las medidas que deberían adoptarse en relación al peritaje informático, si lo hace en cuanto al derecho procesal[41], estableciendo políticas que incluyen sanciones y tipos de penas a imponer para preservar las garantías[42] de la persona que está siendo sindicada o procesada por la comisión de un delito informático, y para los Estados, en relación a la preservación de los datos de tráfico guardados en los servidores que son propiedad de los IPS[43] (Internet Service Provider, Proveedores de Servicios de Internet), a los cuales se les confiere la potestad de administrar el tiempo, la manera en que serán conservados y sus criterios de divulgación; en el titulo 3 de la sección de derecho procesal del este convenio, en relación a la evidencia digital se incluye una disposición como mandato de comunicación, pues se crea para los países la capacidad de regular las facultades de los ISP sobre los servidores de su propiedad, ante un incidente informático si es necesaria la apertura de los logs[44], preservando el derecho a la intimidad y a la información; en el titulo 4, se articulan las

---

[41] Por “Derecho procesal” se entiende a una rama del derecho civil o del derecho penal, etc., destinada a dar efectividad a los derechos subjetivos reconocidos por aquellas disciplinas.

[42] Garantía. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/garant%C3%ADa/garant%C3%ADa.htm

[43] Proveedor de Servicios de Internet (ISP). Ministerio de Tecnologías de la Información y las Comunicaciones, MICTIC. http://www.mintic.gov.co/portal/604/w3-article-5879.html

[44] Por “log” se entiende al registro oficial de eventos durante un determinado periodo de tiempo, que es empleado por los profesionales en seguridad informática para conocer los datos e información sobre que, quien, cuando, donde y porque ocurrió un evento para una aplicación o dispositivo en particular.

políticas dirigidas a que cada Estado establezca de manera legal la autorización que se otorgara a la autoridad competente para ingresar a los sistemas informáticos y dispositivos de almacenamiento con el fin de recabar la evidencia digital de un suceso informático que está siendo investigado. Igualmente, se reglamentó la facultad de los distintos países para realizar políticas que permitan interceptar el tráfico de datos, sin que se incurra en la violación de derecho a la persona investigada.

Finalmente, al ser un tratado desarrollado en común acuerdo por varios países y al que se han adherido nuevos Estados, se establecieron principios para la cooperación internacional dirigidos hacia la capacidad de investigar asuntos relacionados con incumplimiento de la ley vinculada a sistemas o datos informáticos, y a la obtención de evidencias electrónicas de cualquier acción delictiva que infrinja el derecho penal[45], posibilitando la interceptación de las comunicaciones, captura y almacenamiento de datos de tráfico, conservación de la confidencialidad, comunicación y acceso con o sin el consentimiento del propietario de los datos, mediante una autorización judicial, ya sea en territorio nacional o transfronterizo, puesto que la naturaleza del delito informático es expansiva.

**La Commonwealth**

La Commonwealth es una asociación conformada por 52 Estados soberanos independientes e iguales, la cual participa en distintas actividades como: brindar ayuda a los países con negociaciones comerciales, construir el sector de las pequeñas empresas, apoyar la participación de los jóvenes y proporcionar expertos para redactar leyes, promoviendo la democracia, el Estado de derecho, los derechos humanos, el buen gobierno y el desarrollo social y económico.

Actualmente, aunque muchos países han desarrollado disposiciones de derecho penal sustantivo[46] en relación a los delitos informáticos más comunes, con el propósito de definir el delito, determinar a quien se

[45] Derecho penal. Enciclopedia Jurídica. www.enciclopedia-juridica.biz14.com/d/derecho-penal/derecho-penal.htm

[46] Por “Derecho penal sustantivo” se entiende a la configuración en conjunto tanto del Derecho penal subjetivo como del objetivo, el cual se contrapone al Derecho procesal penal, y se consagra en el Código Penal, reuniendo las normas o leyes concerniente a los delitos, penas y medidas de seguridad que el Estado posee como herramientas para suprimir cualquier actuación antisocial.

considerara como delincuente y establecer las penas que se le impondrán, muy poco se ha abordado sobre los aspectos concretos relacionados con el peritaje informático, creando un faltante de normatividad jurídica a escala internacional. Sin embargo, la Commonwealth como organización internacional estableció en el año 2002 la Ley modelo sobre evidencia electrónica; ley que surgió como resultado del grupo de trabajo acordado de conformidad con la Law Ministers of Small Commonwealth Jurisdictions en el año 2000, cuyo propósito fue elaborar una legislación sobre la evidencia electrónica. Esta ley se encuentra basada en las legislaciones de Singapur y Canadá, y en su redacción se constató la conclusión principal del grupo de trabajo, después de realizar el análisis comparativo legislativo, la cual manifiesta que en cuanto a la admisibilidad de la evidencia digital se le da mayor importancia a la fiabilidad del sistema a partir del cual se crea la prueba que a la evidencia misma; igualmente, se trataron las características más significativas de la evidencia digital en relación con los Estados cuyo sistema jurídico se basa en el Common Law, tales como la integridad y la aplicación de la norma de la mejor evidencia. La sección 3 plantea la disposición sobre la admisibilidad general de la evidencia electrónica, de modo que esta no sea inadmisible en una corte por el hecho de tratarse de un registro de naturaleza electrónico, y aunque durante esta sección se proporciona el soporte para la utilización de la evidencia digital en un tribunal, su admisibilidad no se garantiza solo por ser digital, sino que se requiere que la prueba digital cumpla con las normas de la evidencia tradicional.

Debido a que algunos principios sobre la admisibilidad de la evidencia digital pueden contender con los criterios de la admisibilidad de la evidencia tradicional, se hizo pertinente el desarrollo de la regla de la mejor prueba, pues su propósito es disminuir los riegos de testimonios equívocos sobre el contenido de los documentos, la transcripción errónea y cualquier manipulación que no haya sido descubierta. Es de esta forma como la Commonwealth ha aportado al desarrollo de la normatividad que regula algunos de los aspectos referentes al peritaje informático, sin embargo, aún no se ha especificado un procedimiento general aceptado por las naciones que la conforman para llevar a cabo la investigación de los sistemas informáticos involucrados en una actividad ilegal.

#### 6.1.2.2 Regiones y Países

**Europa**

Debido a la gran cantidad de delitos informáticos cometidos actualmente, cuyo alcance va en aumento año tras año, generando un costo muy alto para las empresas y organizaciones en toda Europa[47], atentando contra los derechos humanos, se hace necesario contar con un elemento legal que permita tratar estas acciones delictivas con el fin de esclarecer los actos perpetrados mediante el uso de los dispositivos digitales, en otras palabra lo que se conoce como evidencia o prueba digital.

Entre las revisiones de las disposiciones legales encontradas en el marco europeo correspondientes a la legislación informática se abarcan múltiples aspectos que contemplan desde la protección del tratamiento automatizado de los datos personales[48], la protección jurídica de programas de ordenador[49], los derechos de autor[50], aspectos jurídicos del intercambio electrónico de datos [51], la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación[52], hasta otras muchas regulaciones concernientes con aspectos relacionados al comercio electrónico, tráfico de datos, proveedores de servicio, y en general múltiples aspectos referentes a la normatividad en general de las tecnologías de la electrónica, de la informática y de las comunicaciones, haciendo extensa su estructura jurídica, dada la gran cantidad de legislación y doctrina para todos los asuntos relacionados con la informática; por esta razón, para términos del presente trabajo, se enfocará su revisión en el atributo judicial en materia penal concerniente al peritaje de la evidencia digital y su admisibilidad en la cortes europeas.

Para conocer la legislación con la que cuentan los países europeos en relación al peritaje informático, se han desarrollado investigaciones que han permitido analizar la forma en como está regulado el procedimiento para la

---

[47] Ponemon 2016 HPE Cost of Cyber Crime GLOBAL REPORT ESE. Ponemon Institute. 01 de septiembre 2017.

[48] Recomendación 81/679/CEE, de la Comisión de 29 de julio de 1981 (DOCE nº L 246 de 29 de agosto de 1981).

[49] Directiva 91/250/CEE, del Consejo, de 14 mayo 1991 (DO L 122 de 17.5.1991, p. 42-46).

[50] Directiva 93/83/CEE del Consejo, de 27 de septiembre de 1993 (DO L 248 de 6.10.1993, p. 15/21).

[51] Recomendación 94/820/CE de la Comisión, de 19 de octubre de 1994 (DO L 338 de 28.12.1994, pp. 98-117).

[52] Recomendación 95/4 (Adoptada por el Comité de Ministros el 7 de febrero de 1995, durante la 528ª reunión de los Delegados de los Ministros).

obtención de la evidencia electrónica y su admisibilidad en los tribunales de justicia. Estudiando de forma minuciosa estas legislaciones en 16 Estados, y siguiendo un mismo criterio se analizaron 48 normas, y sin embargo, no se encontró una definición específica de prueba electrónica, pero sí referencias legislativas en relación al documento electrónico, firma electrónica, prueba tradicional y medios de prueba, las cuales son aplicables por correlación a la prueba electrónica.

#### *6.1.2.2.1.1 Reino Unido y Bélgica*

Para el procedimiento de la obtención, conservación y presentación de la evidencia digital ante los tribunales, al no contarse con un mecanismo específico que lo regule "los países aplican por analogía la regulación del procedimiento general de la prueba tradicional"[53], sin embargo, países como Reino Unido y Bélgica cuentan con las normas que más se asemejan a un procedimiento adecuado para la obtención de la prueba digital. El Consejo Nacional de Jefes de Policía de Reino Unido[54] (NPCC, National Police Chiefs Council) recomienda ajustarse a un procedimiento forense estandarizado compuesto normalmente de cuatro etapas[55], el cual se encuentra dentro del Código sobre la Policía y la Prueba Penal vigente, cuyas fases son:

1) *Etapa de Recolección*: Durante esta fase se realiza la búsqueda, identificación, obtención y la documentación de la evidencia.
2) *Etapa de Examinación*: En esta parte del proceso se documenta el contenido y el estado de la evidencia recolectada, separando aquella que sea útil para la investigación, explicando su origen y alcance.
3) *Etapa de Análisis*: En esta fase se estudia la evidencia que fue señalada como útil para el proceso de investigación, verificando su relevancia y valor probatorio.

---

[53] INSA MERIDA, Fredesvinda; LAZARO HERRERO, Carmen y GARCIA GONZALEZ, Nuria. Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad.: Un proyecto europeo. Enlace [online]. 2008, vol.5, n.2, pp. 139-152. Disponible en: <http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152008000200009&lng=es&nrm=iso>. ISSN 1690-7515.

[54] Consejo Nacional de Jefes de Policía (NPCC). http://www.npcc.police.uk/

[55] England, Wales and North Ireland Association of Chief Police Officers, Good Practice Guide for Computer based Electronic Evidence.

4) *Etapa de Declaración*: En este último paso se desarrolla el reporte, en el cual se debe explicar el proceso de examinación que se llevó a cabo sobre la evidencia y la información útil que fue separada como resultado del mismo. También debe contener el análisis del investigador enfocado en el procedimiento de examinación y la información obtenida.

La NPCC resalta la necesidad de que todas las observaciones realizadas por el investigador se preserven para efectos testimoniales, teniendo presente que durante el procedimiento judicial el investigador podría ser llamado a testificar. Por otra parte, se recalca la importancia de la elección de los elementos se software y hardware que serán empleados para llevar a cabo la investigación, de manera que la información original no termine siendo comprometida.[56]

#### *6.1.2.2.1.2 Austria, Dinamarca, Suecia, Finlandia y otros países*

En cuanto a la admisibilidad de la evidencia digital, en algunos países de Europa, además del juez o del tribunal se entiende como máxima autoridad en casos particulares al fiscal general. Actualmente, en cada Estado de la Unión Europea se requiere el cumplimiento de ciertos requerimientos para la aceptación de las pruebas digitales, coexistiendo dos paradigmas, el primero de ellos se basa en la decisión autónoma de juez al aprobar o no la evidencia digital como material probatorio, estableciendo dentro de la tradición jurídica extensos principios de admisibilidad, criterio que es practicado en países como Austria, Dinamarca, Suecia y Finlandia; el conjunto restante de países comparte el segundo modelo, el cual exige el cumplimiento de ciertos requisitos de orden legal, que rigen las causantes por las que una prueba puede llegar a ser rechazada o desestimada dentro de un proceso judicial, los cuales contemplan los siguientes atributos: legalidad, respeto por los derechos fundamentales, fiabilidad, proporcionalidad y efectividad, originalidad y enfoque (directa o indirecta).[57] La observancia de la cadena de custodia es fundamental para la

---

[56] El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, CO: Universidad de los Andes, 2010. p.108.

[57] INSA MERIDA, Fredesvinda; LAZARO HERRERO, Carmen y GARCIA GONZALEZ, Nuria. Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad.: Un proyecto europeo. *Enlace* [online]. 2008, vol.5, n.2, pp. 139-152. Disponible en: <http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152008000200009&lng=es&nrm=iso>. ISSN 1690-7515.

admisibilidad de las pruebas recolectadas, de manera que no se pueda cuestionar su validez frente a un estrado judicial, es por ello que, durante la investigación tanto la policía como la fiscalía son los encargados de la custodia de la evidencia, y durante el juicio, el encargado de la custodia pasa a ser el órgano judicial; sin embargo, en uno u otro caso influye en gran medida el hecho de quien estuvo a cargo de la obtención de la evidencia, dando mayor validez a la manipulación de la prueba si esta es realizada por expertos, por lo que la mayoría de los juristas europeos tienden a "preferir a los fiscales y policías como los expertos en informática forense por excelencia, otorgándoles a éstos la responsabilidad de obtener la prueba digital y de manipularla adecuadamente"[58].

**América**

América no ha sido ajena a los grandes cambios producidos por el avance de la tecnología, la cual ha permitido que los sistemas de comunicación se expandan y sean más robustos, fortaleciendo las capacidades del ser humano para comunicarse sin que existan barreras de distancia. Sin embargo, al igual que sus grandes beneficios, junto con los avances han llegado nuevas formas de delito, posibilitadas gracias a la infraestructura de comunicación con la que cuenta el mundo en la actualidad. Por esta razón, muchos países americanos han aunado esfuerzos en procura de hacer frente a la ciberdelincuencia, de lo cual se ha dejado constancia en las distintas regulaciones expedidas que manifiestan la importancia que empieza a tomar el peritaje informático y la evidencia digital en el marco de la administración de la justicia a nivel regional.

Organizaciones como la OEA (Organización de los Estados Americanos), que reúne a los 35 países independientes del continente americano, ha venido desarrollando una serie de reuniones con el propósito de estudiar activamente lo referente al ciberdelito en la región, la cual se conoce como la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA)[59], en donde se ha realizado una serie de recomendaciones que incluyen: la creación de un Grupo de Expertos Intergubernamental sobre el Ciberdelito, la elaboración de la Estrategia interamericana para hacer frente a las amenazas cibernéticas, el llamado a los Estados miembros a revisar los mecanismos que se tienen para hacer

[58] El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, CO: Universidad de los Andes, 2010. p.108.

[59] Departamento de Cooperación Jurídica, OEA. Portal Interamericano de Cooperación en materia de Delito Cibernético. http://www.oas.org/juridico/spanish/cybersp.htm

frente al ciberdelito de modo que se facilite una cooperación amplia y eficaz, el llamado a estudiar el desarrollo de la capacidad técnica y jurídica para incorporarse a la Red 24/7 del G7, evaluar la conveniencia de aplicar los principios del Convenio de Budapest sobre la Ciberdelincuencia y estudiar la posibilidad de incorporarse a dicho Convenio, el llamado a los Estados miembros para que examinen su ordenamiento jurídico y adopten la legislación necesaria en relación con el derecho procesal, la evidencia electrónica y los juicios penales, entre otras recomendaciones. Sugerencias a las que han intentado responder gran parte de los Estados americanos con el fin de avanzar en la lucha contra los delitos informáticos, desarrollando mecanismos y disposiciones legales para regular principalmente lo concerniente con la aceptación de la evidencia digital en los tribunales de justicia.

#### *6.1.2.2.1.1 Estados Unidos*

La intervención de los Estados Unidos es relevante en relación a la legislación sobre el peritaje informático y todo lo que se deriva de este, puesto que es el país de origen de la Internet, del comercio electrónico, y el lugar donde se identificó el primer delito informático en el mundo. Es así como el gobierno de los Estados Unidos participa de forma activa en la colaboración internacional contra la criminalidad informática, puesto que además de ser el pionero en el uso de la internet también es el país en donde se registra el mayor índice de ciberdelincuencia.

En Estados Unidos debido a la costumbre del desarrollo de jurisprudencia[60] y al enorme valor que esta tiene dentro de su sistema jurídico, se ha generalizado la aceptación de la evidencia digital dentro de los procesos judiciales, lo cual se encuentra establecido en las Reglas Uniformes de Evidencia[61] (URE, Uniform Rules of Evidence) y en las Reglas Federales de Evidencia[62] (FRE, Federal Rules of Evidence), de las cuales la segunda regula la introducción de la evidencia en los procedimientos judiciales llevados a cabo en cortes federales.

Se han promulgado leyes en relación a la importancia que tienen los derechos fundamentales en el proceso de búsqueda y recolección de la

---

[60] Jurisprudencia. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/jurisprudencia/jurisprudencia.htm

[61] Uniform Rules of Evidence. https://www.law.cornell.edu/uniform/evidence

[62] Federal Rules of Evidence. https://www.law.cornell.edu/rules/fre

evidencia electrónica, lo cual ha sido consignado en la cuarta enmienda a la Constitución estadounidense, de modo que se proteja el derecho a la privacidad y no se llegue a ser víctima de apoderamiento o búsqueda arbitraria. En Estados Unidos las cortes han considerado que, con el fin de no violar la privacidad, en el caso en el que la evidencia digital este de por medio, se debe obtener un consentimiento judicial expreso para realizar la actividad de búsqueda o apoderamiento del material probatorio.

En cuanto al procedimiento para la obtención de la evidencia el Manual del Departamento de Justicia admite que el marco legal para este proceso es el mismo que el que rige las investigaciones convencionales, por lo que se hace necesario recurrir a los estándares y buenas prácticas[63] para la realización del peritaje informático, pues en este se lleva a cabo la manipulación de pruebas electrónicas cuyo manejo difiere de la evidencia tradicional debido a la naturaleza de la misma, que incluye algunas características como la volatilidad. Y con el fin de que la evidencia digital sea admisible el Manual del Departamento de Defensa plantea que esta debe cumplir con tres criterios: Integridad, Autenticidad y superación del Anonimato, con el objetivo de ser aceptada en la corte.

#### *6.1.2.2.1.2 México*

En la legislación mexicana actualmente se han definido distintas cuestiones en la búsqueda de responder legalmente a los nuevos desafíos que presenta la ciberdelincuencia, entre estas leyes se encuentran aquellas que reglamentan aspectos relacionados con los documentos electrónicos, la firma electrónica y la certificación de la misma[64], el mercado de valores[65], los derechos de autor[66], los delitos informáticos[67], y el comercio electrónico[68].

---

[63] Para más información sobre buenas prácticas en los Estados Unidos, se puede acceder a la página del Centro Nacional de Ciencias Forenses: https://ncfs.ucf.edu/

[64] Reglamento de la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma. Núm. 181.- Santiago, 9 de julio de 2002.

[65] Ley de Mercado de Valores de 1990.

[66] Ley Federal del Derecho de Autor de 1996.

[67] Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de Fuero Federal.

[68] DECRETO por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal

Aunque México no cuenta con una ley de evidencia electrónica, el gobierno mexicano empezó desde el 2003 los primeros pasos legislativos con la reforma del Código de Comercio pues se adiciono el artículo 89 bis[69], en donde se estableció que no se negaría la validez, fuerza obligatoria y los efectos jurídicos a todo tipo de información por el hecho de estar en forma de mensaje de datos. Se reconoció como prueba a la información generada o transmitida por medios electrónicos, ópticos o de cualquier otro tipo mediante la adición del artículo 210-A al Código Federal de Procedimientos Civiles, en donde además se indica que tendrá mayor valor probatorio la información recabada dependiendo de la fiabilidad del método con el que fue generada, recibida, guardada o comunicada. Además de ello, en el año 2007 se estableció la legislación sobre la protección de los datos[70] mediante modificaciones constitucionales que establecieron que el derecho a la información será garantizado por el Estado e igualmente se definieron los principios y bases sobre los cuales se llevará acabo el acceso a la información por parte de la Federación, los Estados y el Distrito Federal, en la esfera de sus respectivas competencias, cuando sea necesario para el desarrollo de una investigación judicial.

#### *6.1.2.2.1.3 Barbados*

Barbados no ha promulgado una ley separada en relación con la evidencia electrónica. Sin embargo, la Ley de Evidencia contiene algunas disposiciones que se refieren a la información registrada o almacenada por medio de un computador u otro dispositivo. Esta ley definió el término "documento" para incluir información registrada o almacenada en un computador. También suprime la regla de la mejor evidencia con el efecto de que la evidencia electrónica no se excluiría por el hecho de que no es el documento original. La ley de Barbados también toma en cuenta la evidencia producida por máquinas, dispositivos o procesos. Esta ley especifica que cuando sea razonable encontrar el dispositivo o proceso, a

---

de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor, publicado en el Diario Oficial de la Federación de 29 de Mayo del 2000.

[69] Diario Oficial de la Federación el 29 de Agosto de 2003, con la entrada en vigor con el Artículo Primero Transitorio del Decreto que modifica el Código.

[70] Acuerdo por el que se Adiciona el diverso por el que se determinan las atribuciones, funciones, organización y circunscripción de las delegaciones y Subdelegaciones Federales y Oficinas de Servicios de la Secretaría de Economía, publicado en el Diario Oficial de la Federación el 28 de Marzo de 2007.

partir del cual se obtuvo la evidencia digital, si se utiliza adecuadamente, este normalmente hará lo que afirma que hace quien presenta la prueba, por lo que se presumirá que al producir el documento (a menos que se demuestre lo contrario) el dispositivo o proceso hizo lo que la parte que lo presento afirma haber hecho[71].

#### *6.1.2.2.1.4 Belice*

Belice es el único estado de los países del Caribe que ha desarrollado una Ley de Evidencia Electrónica que sigue completamente la Ley Modelo de la Commonwealth sobre Evidencia Electrónica. Esta ley define "registro electrónico" como los datos grabados o almacenados en cualquier medio en o por un sistema informático u otro dispositivo similar y que pueden ser leídos o percibidos por una persona o un sistema informático u otro dispositivo similar e incluye una pantalla, imprimir u otro resultado de esa información. El término "computador" no está definido en la ley. Las disposiciones más destacadas de la ley incluyen la admisibilidad general de los registros electrónicos, cuestiones de autenticación, aplicación de la regla de la mejor prueba, presunción de integridad, normas, prueba de declaración jurada, acuerdo sobre la admisibilidad de los registros electrónicos y la admisibilidad de las firmas electrónicas[72].

#### *6.1.2.2.1.5 Jamaica*

Jamaica no ha promulgado una legislación autónoma de evidencia electrónica, pero sí cuenta con una Ley de Evidencia con disposiciones mínimas relacionadas con la admisibilidad de los documentos electrónicos. El término "documento" se define en la ley para incluir (a) cualquier mapa, plan, gráfico o dibujo; (b) cualquier fotografía; (c) cualquier disco, cinta, pista de sonido u otro dispositivo en el que los sonidos u otros datos (que no sean imágenes visuales) estén incorporados de modo que sean capaces (con o sin la ayuda de algún otro equipo) de reproducirse a partir de ellos; (d) cualquier película (incluyendo microfilm), negativo, cinta u otro dispositivo en el que una o más imágenes visuales estén incorporadas para ser reproducidas (con o sin la ayuda de algún otro equipo). La ley también establece en la sección 31 la admisibilidad de la evidencia informática que

[71] Electronic Evidence: Assessment Report. 2013. Establishment of Harmonized Policies for the ICT Market in the ACP countries. ITU. Pág. 21.

[72] Ibíd., Pág. 21.

constituye rumores, así como la admisibilidad de la evidencia informática que no constituye un testimonio indirecto[73].

#### *6.1.2.2.1.6 San Vicente y las Granadinas*

En San Vicente y las Granadinas la Ley de transacciones electrónicas contiene disposiciones mínimas en cuanto a la admisibilidad de las pruebas electrónicas. Esta ley establece la no discriminación contra la información electrónica y especifica que no se le denegará la validez o aplicación de la información, solo por el hecho de que está en formato electrónico. El término "sistema de información" significa un sistema para generar, enviar, recibir, almacenar, visualizar o procesar de otro modo los mensajes de datos e incluye las comunicaciones de protocolos de aplicaciones inalámbricas e Internet.

La ley también establece que, en los procedimientos por un delito contra una ley, el hecho de que se alegue que se ha cometido el delito de interferir con un sistema de información y que las pruebas se han generado a partir de ese sistema de información, no impiden que la evidencia sea admisible. La firma electrónica está prevista en esta ley. La disposición especifica que una firma electrónica no carece de validez y efecto simplemente por el hecho de que está en formato electrónico[74].

#### *6.1.2.2.1.7 Trinidad y Tobago*

Trinidad y Tobago no tiene una ley de evidencia electrónica, pero si cuenta con algunas disposiciones relacionadas con la admisibilidad de los documentos electrónicos, las cuales se encuentran en la Ley de Evidencia, Cap. 7:02. El término "computador" se define en la ley como cualquier dispositivo para almacenar o procesar información. El término "documento" también se define en esta ley e incluye cualquier disco, cinta, pista de sonido u otro dispositivo en el que los sonidos u otros datos, que no sean imágenes visuales, estén incorporados de manera que sean capaces (con o sin la ayuda de otro equipo) de ser reproducidos desde allí. Esta ley establece la admisibilidad en los procesos civiles de las declaraciones producidas por computadores, así como la admisibilidad de ciertos registros

[73] Ibídem, Pág. 21.

[74] Ibídem, Pág. 22.

comerciales. La ley también define la admisibilidad de los registros informáticos en casos penales[75].

#### *6.1.2.2.1.8 Las Bahamas*

Las Bahamas no tiene específicamente una ley de evidencia electrónica, pero si ha desarrollado algunas disposiciones relacionadas con la admisibilidad de documentos electrónicos, y que se encuentran en la Ley de Transacciones y Comunicaciones Electrónicas de 2003, en la Parte II sobre el Reconocimiento legal y equivalencia funcional de comunicaciones electrónicas, firmas, contratos y asuntos relacionados, en la parte III sobre Intermediarios y proveedores de servicios de comercio electrónico, y en la parte IV sobre el Consejo asesor de comercio electrónico. Estas partes de la ley se centran en la responsabilidad civil y penal de los proveedores de servicios de Internet, la aceptación de los documentos electrónicos por parte del tribunal y la creación de un consejo para asesorar al Ministerio de Telecomunicaciones sobre estos asuntos. La ley también proporciona varias definiciones, conceptos y normas aplicables a distintas cuestiones relacionadas con la evidencia electrónica[76].

#### *6.1.2.2.1.9 Argentina*

Argentina al igual que otras naciones ha dispuesto leyes que permitan un adecuado manejo de la tecnología, iniciando en 1968 con la reforma del Código Civil en el cual se estableció que la energía eléctrica y magnética contenida en forma de información en un soporte digital es semejante a una cosa[77], la protección de bases de datos y software[78], los derechos de autor[79] y la protección de datos[80], entre otras muchas disposiciones de ley. Sin embargo, aunque no cuenta con una ley específica sobre evidencia

---

[75] Ibídem, Pág. 22.

[76] Ibídem, Pág. 22.

[77] Ley 17.711 de 22 de abril de 1968, Artículo 2311 del Código Civil.

[78] Decreto 165/94 del 8 de febrero de 1994, establece que los programas de ordenador sean incluidos dentro del artículo 1 de la Ley 11.723 como obras protegidas.

[79] Ley 25.036 de 14 de octubre de 1998, que modifica la Ley 11.723 de propiedad intelectual.

[80] El 8 de marzo de 1999, se reformó el Art.º 67. Amparo informativo (corpus data), del Código Procesal.

Constitucional.

electrónica, dispone de normas sobre el valor y la eficacia de los documentos digitales remitidos a la Comisión Nacional de Valores, las cuales se encuentran establecidas en el Decreto 677/2001 de 22 de marzo de 2001. El Código Procesal Civil y Comercial de la Nación en el artículo 378 establece que los documentos electrónicos poseen valor probatorio e igualmente el Proyecto de Código Civil de 1998 en sus artículos 263 y 264 denomina a los documentos electrónicos como instrumentos particulares.

#### *6.1.2.2.1.10 Chile*

Chile al igual que otros países no cuenta con una ley de evidencia electrónica, sin embargo, ha desarrollado algunas disposiciones en cuanto a la admisibilidad de los documentos electrónicos en un juicio, las cuales se encuentran en la Ley 19.799, en donde se establece que estos documentos pueden ser empleados durante un proceso judicial, y en el caso de que se busque hacerlos valer como medios de prueba, se deberá seguir el esquema tradicional previsto en la ley común. El tratamiento probatorio de los documentos electrónicos que hace la ley remite al Código Civil, indistintamente de cual fuere la situación a tratar, sea que fuere un documento electrónico privado o público, y si se encuentra reconocido o no[81].

### 6.1.3 En Colombia

El avance de las tecnologías de la información y la comunicación han cambiado no solo la forma de concebir el mundo, sino que también, han permitido el desarrollo acelerado de todo tipo de crímenes mediante el uso de dispositivos tecnológicos, que incluyen tanto los delitos cuyo accionar se ejecuta a través de las redes, como los delitos que se encuentran estrechamente vinculados con la información y los datos, e incluso los delitos tradicionales que encuentran en la tecnología la facilidad para ampliar su accionar, haciéndose en muchos casos imperceptibles o quedando en el anonimato, pues el desarrollo de la tecnología proporciona al delincuente la capacidad de ocultar tanto su identidad como el registro de sus acciones, haciendo en ocasiones imposible la individualización del mismo. Es así como, la recabación de la evidencia digital resulta ser muy compleja para probar los delitos informáticos, debido a las muchas facilidades que ofrece la tecnología actualmente, dificultando la recolección de los datos que se encuentran almacenados o fueron transmitidos mediante equipos informáticos.

---

[81] EL VALOR PROBATORIO DE LA INFORMACIÓN ELECTRÓNICA EN EL JUICIO EN LÍNEA. 2014. TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA. Pág. 239-241.

Frente a este panorama, se hizo necesario que los mecanismos de respuesta de los poderes públicos fueran novedosos e innovadores, administrando y poniendo en funcionamiento las normas y el poder judicial requerido para la situación actual, por esta razón en Colombia se ha visto como una necesidad la creación de legislaciones e instrumentos jurídicos que acojan los principios de la International Organization on Computer Evidence, con el fin de lograr obtener y tratar la evidencia digital de manera que se garantice su veracidad, integridad y correcto tratamiento de forma segura.[82]

La evidencia digital es un medio probatorio válido en la legislación colombiana desde la expedición de la Ley 527 de 1999, aunque anteriormente, se admitían como prueba las evidencias digitales que fueran útiles para el convencimiento del juez y que estuvieran relacionadas en el artículo 175 del Código de Procedimiento Civil. Actualmente, en Colombia se cuenta con elementos legales definidos dentro del Código de Procedimiento Penal, Ley 906 de 2004, para la presentación de las pruebas que involucren evidencia digital, y aunque no cuenta con una ley de evidencia electrónica ha desarrollado disposiciones relacionadas con la admisibilidad de documentos electrónicos y del peritaje informático dentro de un proceso judicial.

## 6.2 LA INFORMACIÓN ELECTRÓNICAMENTE ALMACENADA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO

### 6.2.2 Aclaraciones

#### 6.2.2.1 Información Electrónicamente Almacenada (ESI)

La información electrónicamente almacenada (ESI, Electronically Stored Information) es toda aquella información y datos que se crean, manipulan, almacenan, transmiten y utilizan en forma digital. Se necesita de hardware, software y redes para utilizar la ESI. Esta información es empleada dentro de los procesos judiciales como evidencia con el propósito de obtener información que permita esclarecer ciertos asuntos sensibles y la tratar la controversia brindando certeza en aquellos temas desconocidos por el juez.

[82] Declaración de Barranquilla de 1 de junio de 2013. HACIA LA UNIFICACIÓN DE CRITERIOS E INSTRUMENTOS JURÍDICOS PARA LA PROTECCIÓN DE LA PRIVACIDAD.

La información electrónicamente almacenada se puede encontrar en dos tipos de formato: Tangible y no tangible. La ESI se divide en cinco clases, las cuales requieren de una medida diferente de esfuerzo y costo para acceder a ella.

1) Información electrónicamente almacenada que ha sido creada, procesada o recibida de forma rápida y a la que se accede con frecuencia. Se encuentra en discos duros, servidores de red, etc. Es razonablemente accesible.
2) Información electrónicamente almacenada en medios extraíbles o a la que se accede a través de sistemas de almacenamiento automatizados o robóticos. La velocidad de acceso es variable. Se encuentra en memorias USB, discos ópticos, etc. Igual que la anterior es razonablemente accesible.
3) Información electrónicamente almacenada que es enviada a un deposito o almacenamiento. A esta ESI se accede de forma manual. Se encuentra en memorias, discos ópticos, RAID, JBOD. También es razonablemente accesible.
4) Información electrónicamente almacenada utilizando la compresión de datos. La información es almacenada como copia de seguridad para la recuperación frente a un desastre, y no está organizada para la recuperación de archivos o mensajes específicos. Requiere que se restaure para acceder a la información. En este caso se hace necesario probar que tanto la pertinencia como la necesidad de la información que se busca es mayor que los costos de recuperación y procesamiento. Está información no es razonablemente accesible, pues se requiere de un gran esfuerzo y mayores costos para recuperarla.
5) Información electrónicamente almacenada que ha sido borrada, sobrescrita, fragmentada (rota y almacenada en partes) o corrupta (dañada por virus informáticos, o un mal funcionamiento del hardware o software). Existe la posibilidad de que sea imposible recuperar esta información, en caso contrario se necesitara de un procesamiento significativo para acceder a ella. Igual que la anterior no es razonablemente accesible.

#### 6.2.2.2 Ordenamiento Jurídico

El ordenamiento jurídico es el conjunto de normas que permiten guiar la justicia en un momento y espacio determinado. Surge como resultado de aquello que la comunidad considera una necesidad para que la vida en sociedad se desarrolle de forma adecuada y que posteriormente es puesto en palabras y en práctica.

Colombia cuenta con un ordenamiento jurídico formado por la Constitución Política, como norma suprema, las leyes, y demás normas jurídicas del poder ejecutivo, como decretos, reglamentos y otras regulaciones; las cuales tienen como propósito establecer justicia mediante la aplicación de la norma.

#### 6.2.2.3 Tipos de Ciberdelitos

Actualmente no existe una definición universal de ciberdelito, comúnmente conocido como “delito informático”, sin embargo, se han planteado distintas clasificaciones de los ciberdelitos. La aplicación de la ley generalmente realiza la distinción entre dos tipos principales de delitos, que reúnen todas las clasificaciones que puedan asignarles cualquier entidad privada o pública, los cuales se describen a continuación.

**Delitos de Alta Tecnología**

Los delitos de alta tecnología considerados por INTERPOL como “Cibercrimen avanzado” o “Ciberdelincuencia pura”, son todos aquellos ataques sofisticados contra el hardware y software de los computadores y sistemas de información, donde el principal objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo.

Según la legislación colombiana, ley 1273 de 2009[83], se establecen estos delitos como los “Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”, en donde las distintas conductas ilícitas vulneran el Bien Tutelado de la Información y el Dato.

Entre los delitos de alta tecnología encontramos:

- Según la ley colombiana.
    - ❖ Artículo 269A: Acceso abusivo a un sistema informático.
    - ❖ Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
    - ❖ Artículo 269C: Interceptación de datos informáticos.

[83] Ley 1273 DE 2009. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- ❖ Artículo 269D: Daño Informático.
- ❖ Artículo 269E: Uso de software malicioso.
- ❖ Artículo 269F: Violación de datos personales.
- ❖ Artículo 269G: Suplantación de sitios web para capturar datos personales.

- Según el Convenio de Ciberdelincuencia del Consejo de Europa[84].

  - ❖ Acceso ilícito a sistemas informáticos.
  - ❖ Interceptación ilícita de datos informáticos.
  - ❖ Interferencia en los datos informáticos.
  - ❖ Interferencia en el funcionamiento de un sistema informático.
  - ❖ Abuso de dispositivos que faciliten la comisión de delitos.

**Delitos Habilitados Mediante el Uso de la Informática**

Los delitos habilitados mediante el uso de la informática considerados por la INTERPOL como “Crimen amplificado” o “Crimen habilitado” por la cibernética, son todos aquellos delitos 'tradicionales' o ya tipificados que toman lugar mediante el uso de computadores y sistemas de información, como los delitos contra los niños, los delitos financieros e incluso el terrorismo.

Según la legislación colombiana, ley 1273 de 2009[85], se establecen estos delitos como los “Atentados informáticos y otras infracciones”, en donde se vulnera el Bien Tutelado de la Información y el Dato.

Entre los delitos habilitados mediante el uso de la informática encontramos:

- Según la ley colombiana.

  - ❖ Artículo 269I: Hurto por medios informáticos y semejantes.
  - ❖ Artículo 269J: Transferencia no consentida de activos.

- Según el Convenio de Ciberdelincuencia del Consejo de Europa[86].

---

[84] Convenio sobre la Ciberdelincuencia Budapest, 23.XI.2001. https://rm.coe.int/16802fa41c

[85] Ley 1273 DE 2009. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- ❖ Falsificación informática mediante la introducción, alteración o borrado de datos informáticos.
- ❖ Fraude informático mediante la introducción, supresión o borrado de datos informáticos, o interferencia en sistemas informáticos.

#### 6.2.2.4 Evidencia vs. Prueba

La evidencia constituye la esfera que engloba la certeza sobre un asunto particular exponiendo la verdad o realidad de algo, es decir, es aquello que permite demostrar un echo especifico sin dejar lugar a la duda, y la prueba es el medio que facilita mostrar una verdad o realidad determinada, es decir, es la herramienta, recurso, o mecanismo empleado para dar a conocer los resultados encontrados a partir de la investigación, en otras palabras, da a conocer la evidencia.

### 6.2.3 Pruebas Empleadas en un Caso Penal – Ley 906 de 2004

En la escena del cibercrimen se manifiestan los desafíos a los que se enfrenta la ciencia forense, en este caso específicamente la informática forense, pues la actividad criminal es desarrollada de forma digital haciendo posible que no haya presencia física del delincuente, por lo que no hay un rastro físico a seguir, sino que se cuenta únicamente con datos de transmisiones, impulsos eléctricos, emisión electromagnética, etc., por lo que la investigación científica tiende a variar dada la naturaleza de la evidencia a estudiar.

Dentro de los tipos de pruebas que son empleadas en un caso penal que involucra medios digitales se cuenta con: La prueba pericial, la prueba documental y la prueba testimonial. Dichas pruebas se tratarán con mayor amplitud a continuación.

#### 6.2.3.1 Prueba Pericial

La prueba pericial se ratifica junto con el uso de los otros dos tipos de prueba, pues la prueba de tipo documental permite reforzar el informe del perito forense digital y la prueba testimonial permite sustentar el informe pericial ante el juez de control de garantías y el juez de conocimiento. Esta prueba se encuentra regulada en la Ley 906 del 2004 correspondiente al

---

[86] Convenio sobre la Ciberdelincuencia Budapest, 23.XI.2001. https://rm.coe.int/16802fa41c

Estatuto Procesal Penal en el tercer libro, cuarto título, tercer capítulo sobre la práctica de la prueba, en la tercera parte, desplegándose desde el articulo 405 hasta el 423.

Se incluye la evidencia digital de forma implícita en el Código de Procedimiento Penal, pues al hablar de la procedencia, articulo 405, se instituye que la prueba pericial es aceptable siempre y cuando se hayan requerido conocimientos científicos o técnicos especializados para realizar una valoración en particular, dando lugar a la realización de la investigación a partir de la utilización de herramientas de informática forense para el estudio de la evidencia digital.

Acorde con el artículo 406, se valida explícitamente la legitimidad de la prueba pericial presentada por los peritos informáticos forenses privados, aprobando tanto el informe pericial como el laboratorio donde se desarrolló la investigación. Sin embargo, se requiere, con el fin de que la prueba no sea excluida del proceso judicial, que el perito cuente con las capacidades profesionales necesarias, evitando de esta forma no solo la exclusión sino, en el peor de los casos, la nulidad de la prueba por falta de bases científicas o el uso inadecuado de la técnica empleada.

No existe una limitación para el numero de peritos que pueden participar en las investigaciones que se llevaran a cabo, durante el proceso, lo cual se encuentra estipulado en el artículo 407. Igualmente se determina que la prueba pericial puede ser fruto de la cooperación de expertos, titulados o no, dejando lugar para la participación en la investigación de los peritos de informática forense que no cuenten con un título legalmente reconocido, según el artículo 408.

Un informe pericial tendrá validez y fuerza probatoria siempre y cuando el perito que lo realizo cuente con la certificación profesional o de experiencia que lo acrediten como una persona idónea para llevar a cabo esta tarea, asunto que se encuentra descrito en el artículo 413.

En el artículo 414 se entrelaza la prueba pericial con la prueba testimonial, pues se establece que el perito deberá presentarse en la audiencia con el propósito de sustentar los resultados de la investigación desarrollada.

Se valida la existencia del informe pericial, el cual debe ser sustentado en juicio de modo que sea admisible como evidencia, en donde se documentara el proceso forense digital que se desarrolló para la obtención

de la evidencia y el posterior manejo de la misma, con el fin de esclarecer lo ocurrido mediante la comprobación de los hechos, tal como lo define la ley en el artículo 415

Los artículos 417, 420 y 423, muestran que la admisibilidad de la prueba pericial depende de la pertinencia de lo que se demuestra a partir de ella, y que su nivel de aceptación dependerá de la comprobación de la idoneidad profesional y moral del perito, estableciendo que este debe poseer un amplio conocimiento en cuanto a todo lo referido al uso de la informática forense.

Los demás artículos que describen el manejo de este tipo de prueba hacen referencia a otros aspectos particulares en cuanto a la presentación de la misma durante el juicio, sin embargo, no se refieren o tratan alguna cuestión específica relacionada con la evidencia digital.

#### 6.2.3.2 Prueba Documental

Esta prueba se encuentra regulada en la Ley 906 del 2004 del Estatuto Procesal Penal en el tercer libro, cuarto título, tercer capítulo sobre la práctica de la prueba, en la cuarta parte, extendiéndose desde el articulo 424 hasta el 434.

Entre los documentos descritos como prueba documental en el artículo 424, se encuentran aquellos que sirven para dar soporte al informe pericial, tales como las grabaciones computacionales, textos manuscritos o impresos, discos de todo tipo que contengan grabaciones, grabaciones magnetofónicas, videos, mensajes de datos, télex, telefax y similares y cualquier otro objeto similar a los 15 elementos que se definen.

Se tratan aspectos sobre la autenticidad de la prueba, artículo 425, donde se establece que esta será considerada autentica si se demuestra que se tienen conocimiento sobre la persona que la elaboro. En el artículo 426 se definen los mecanismos que serán empleados para establecer la autenticidad e identificación del documento, los cuales incluyen la identificación de la persona que lo elaboro, reconocimiento del documento por la parte contraria, certificación del documento por una entidad certificadora de firmas digitales, y el hecho de que el informe pericial fue desarrollado por una persona experta.

Los artículos 427 y 428 tratan sobre aspectos relacionados con la prueba documental cuando esta proviene del extranjero, estableciendo la autenticidad de la misma a menos que se demuestre lo contrario.

La apreciación de la prueba será evaluada por el juez en base a criterios que incluyen tanto la integridad del documento como la pertinencia de la información que contiene y la forma clara y sencilla como se expone, lo cual está establecido en el artículo 432.

Los demás artículos que describen el manejo de este tipo de prueba hacen referencia a otros aspectos particulares en cuanto a la presentación de la misma durante el juicio, sin embargo, no se refieren o tratan alguna cuestión específica relacionada con la evidencia digital.

#### 6.2.3.3 Prueba Testimonial

La prueba testimonial se encuentra regulada en la Ley 906 del 2004, del Estatuto Procesal Penal en el tercer libro, cuarto título, tercer capítulo sobre la práctica de la prueba, en la segunda parte, extendiéndose desde el articulo 383 hasta el 404, facultando a las partes procesales, en este caso el juez, para admitir, excluir o anular el informe presentado por el perito informático forense.

### 6.2.4 Valoración de la Evidencia Digital en el Marco Legal

Colombia es un país que no ha sido ajeno a la vehemente necesidad de actualizar su legislación con el fin de hacer frente a la ciberdelincuencia, la cual opera de muchas formas haciendo uso de las tecnologías de información para perpetrar acciones ilícitas causando enormes daños en los bienes de las víctimas. El estudio de este fenómeno, denominado comúnmente delincuencia o criminalidad informática, y la motivación de contar con una capacidad de respuesta legal adecuada, ha permitido que se dé solución jurídica a muchos de los aspectos concernientes al cibercrimen tanto desde el Derecho Penal[87] como desde el Derecho Procesal Penal[88], vinculándose el manejo ilícito de la informática con la

[87] Derecho penal. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/derecho-penal/derecho-penal.htm

[88] Derecho procesal penal. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/derecho-procesal-penal/derecho-procesal-penal.htm Derecho penal.

protección de lo que se ha denominado bien jurídico tutelado de la información y de los datos mediante la expedición de la ley 1273 de 2009.

En Colombia muchas personas y organizaciones han resultado afectadas por las diferentes modalidades de cibercrimen, entre algunos de los casos más significativos y que han llegado a enjuiciamiento están el caso del hacker Andrés Sepúlveda[89] y el caso del robo de LifeMiles perpetrado a Avianca[90]. Sin embargo, existen muchas otras personas particulares, organizaciones privadas e instituciones gubernamentales que han sido víctimas de estos delitos cuyos procedimientos judiciales están en tránsito o han finalizado sin un juicio que aplique un castigo ejemplar.

De acuerdo con las cifras del Informe del Cibercrimen en Colombia para los años 2016-2017[91] realizado por la Dirección de Investigación Criminal e INTERPOL (DIJIN) con su Centro Cibernético Policial (CCP) y en alianza con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), en el país durante el 2016 se incrementaron los ataques de malware un 114.4% en relación al año inmediatamente anterior, e igualmente hubo un aumento de ataques de ransomware del 500% en comparación con el año 2015, además según el CCP se recibieron 15.565 incidentes informáticos por medio de las plataformas disponibles, y durante los años 2014, 2015, 2016 y hasta marzo del 2017 se recibieron 13.774 denuncias por violación a la ley 1273 de 2009, reflejando estas una disminución significativa del 35% del total de incidentes atendidos en los que estaban involucrados ciudadanos del común y un aumento del 28% en los reportes atendidos que afectan al sector empresarial, ver figura 1. Es así como surge la inminente necesidad de contar con un ordenamiento jurídico que responda de forma adecuada a la cibercriminalidad, no solamente desde la identificación de los delitos cometidos y el establecimiento de penas sino también desde el procedimiento penal admitido para dar solución a las investigaciones en las que se vea involucrada evidencia digital.

---

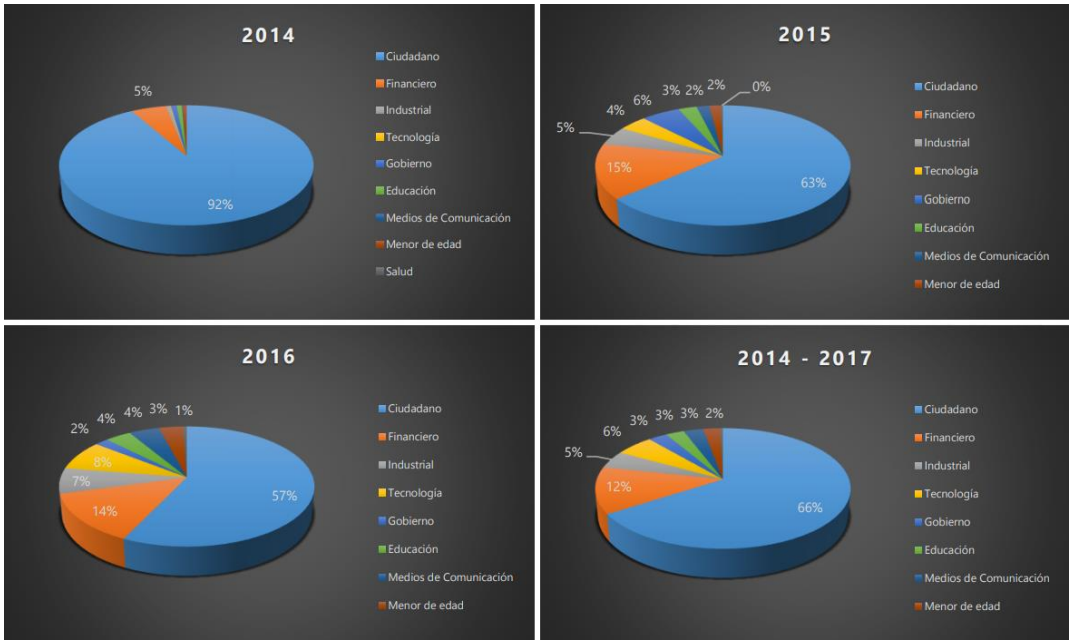
Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/derecho-penal/derecho-penal.htm

[89] Caso Andrés Sepúlveda. https://es.wikipedia.org/wiki/Caso_Andr%C3%A9s_Sep%C3%BAlveda

[90] El ciberdelincuente que viajó por el mundo con millas de los famosos. http://www.eltiempo.com/archivo/documento/CMS-16006809

[91] Informe Amenazas del Cibercrimen en Colombia 2016-2017. Centro Cibernético Policial, 2017. https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Figura 1. El cambio en la selección de las víctimas de la ciberdelincuencia




Fuente: Centro Cibernético Policial (CCP)

En Colombia existen soportes constitucionales, el Derecho al Debido Proceso consagrado en el artículo 29 de la Constitución mediante la Sentencia C-980/10, y legales, Ley 527 de 1999[92] y la Ley 906 de 2004[93] en donde se expide el Código de Procedimiento Penal, que permiten contar con herramientas para la presentación de la evidencia digital durante un proceso judicial, aunque también dan a conocer la urgencia de la mejoría del Estatuto Procesal Penal de modo que sea suficiente y su interpretación y aplicación no sea incongruente.

#### 6.2.4.1 Ley 527 de 1999

La ley 527 de 1999 se convirtió en el fundamento para darle validez jurídica a la evidencia digital en Colombia, pues en ella se reconoció el valor jurídico de los mensajes de datos, en otras palabras, podían ser admitidos como medios de prueba en una corte, lo cual quedo establecido en los artículos 10 y 11 referentes a la *Admisibilidad y fuerza probatoria de los mensajes de*

---

[92] Ley 527 de 1999. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[93] Ley 906 de 2004. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C.http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787

*datos* y al *Criterio para valorar probatoriamente un mensaje de datos,* respectivamente.

En esta ley se reconoce el hecho de que no se le negara validez jurídica a la información presentada como prueba por el hecho de estar en forma de mensaje de datos. También se establecen los criterios que se deben garantizar para que un mensaje de datos tenga valor probatorio:

- Confiabilidad en la manera en que se produjo.
- Confiabilidad en la forma en cómo se conservó.
- Confiabilidad en la manera en cómo se identificó al autor.

#### 6.2.4.2 Ley 906 de 2004 del código de Procedimiento Penal

La ley 906 de 2004 además de regular los distintos tipos de pruebas que pueden ser empleadas en un procedimiento penal donde interviene la evidencia digital, los cuales fueron descritos con anterioridad, establece los principios a seguir en relación a los organismos a los que le compete la actividad investigativa y como se debe llevar a cabo este procedimiento acorde con la ley, para la preservación de los derechos de los involucrados.

En el artículo 14 se instituyen los elementos y actividades que deben ser investigados solo con una orden escrita del Fiscal General de la Nación o su delegado, refiriendo aspectos relacionados con la intimidad.

Se describen las actividades de la fiscalía, planteando tanto las facultades que posee como el deber que le corresponde en los artículos 114 sobre Atribuciones y 142 sobre Deberes específicos de la Fiscalía General de la Nación.

Se definen los órganos de investigación penal encargados de la interceptación de los datos informáticos, los cuales se encuentran descrito en el artículo 200, y se establecen las responsabilidades de la Fiscalía General de la Nación, artículo 142, el cual es un organismo altamente cualificado acreditando los conocimientos necesarios para realizar esta actividad.

El artículo 235 sobre Interceptación de comunicaciones telefónicas y similares. Modificado por el art. 15, Ley 1142 de 2007, Modificado por el

art. 52, Ley 14 de 2011, muestra los elementos y actividades que pueden ser investigados sin autorización previa de un juez.

#### 6.2.4.3 Desde la perspectiva de los involucrados

Acorde con la investigación realizada desde la academia por la Fundación Universitaria Luis Amigo sobre la Aproximación a la informática forense y el derecho informático en el ámbito colombiano[94], se constataron los resultados de la encuesta realizada a los tres actores principales involucrados en los procesos judiciales en los que la evidencia digital es presentada como prueba, los cuales se presentan a continuación, y en donde se describe el concepto que cada uno de ellos posee en relación a la evidencia digital dentro del marco jurídico colombiano.

**Juez**

Desde la perspectiva de los jueces, siguiendo el modelo del derecho sustancial procesal, para asignarle valor probatorio a la prueba que recaba la evidencia digital de un caso particular se debe garantizar la integridad y autenticidad del documento, pues acorde con los artículos 430 y 431 de la Ley 906 de 2004 sino se logra individualizar al autor del documento se convierte en un documento anónimo y por ende no debe ser admitido como prueba. La evidencia digital debe dar cumplimiento a todos los requisitos legales que se estipulan preservando las garantías y los derechos fundamentales.

**Experto Forense**

Desde la perspectiva de los expertos forenses en la legislación colombiana solo se han modificado los tipos penales y las sanciones que se les imponen, pero al código de procedimiento penal no se le ha realizado ningún cambio, por lo que no está regulado el procedimiento que se debe seguir para realizar la investigación que constituye el peritaje informático de modo que la evidencia digital sea admisible en la corte, dejando todo a la libre interpretación del juez que esté al frente del caso.

---

[94] Aproximación a la informática forense y el derecho informático: Ámbito Colombiano. 2013. Ana María Mesa Elneser. Fundación Universitaria Luis Amigo. Medellín, Colombia. http://www.funlam.edu.co/uploads/fondoeditorial/84_Aproximacion_a_la_informatica_forense.pdf

**Abogado**

Desde la perspectiva de los abogados mientras la evidencia digital cumpla con las características de integridad y autenticidad, las cuales se garantizan a partir del manejo adecuado de la firma digital (Dos de claves: una publica y otra privada), esta se puede hacer equivalente a un documento. A excepción de algunos casos como los cheques y las escrituras públicas, la ley no acepta documentos electrónicos. No se requiere de mucha experiencia para la extracción de la evidencia si se cuenta con una firma electrónica.

## 6.3 FORMACIÓN DE LOS JUECES EN COLOMBIA EN TEMAS DE DELITOS INFORMÁTICOS Y SU IMPLICACIÓN EN LA ADMINISTRACIÓN DE LA JUSTICIA

Debido a la amplia gama de ciberdelitos y la capacidad operacional con la que se cuenta para la realización de estas actividades criminales hoy en día, las cuales no tienen limitaciones fronterizas ni exclusión de ningún actor de la sociedad, se ha hecho necesario y urgente el desarrollo de instrumentos tanto internacionales como nacionales para hacer frente al cibercrimen, con el fin de proporcionar seguridad y contar con mecanismos de ciberdefensa.

Entre los instrumentos internacionales con los que se cuenta actualmente en materia de ciberseguridad y ciberdefensa se pueden mencionar el Convenio sobre Ciberdelincuencia del Consejo de Europa, conocido como el Convenio Budapest, la Resolución AG/RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos, la Decisión 587 de la Comunidad Andina, el Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU) en el seno de Naciones Unidas, y la Resolución 64/25 “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional” de la Asamblea General de las Naciones Unidas, entre muchos otros que buscan brindar herramientas y capacidades para responder de forma efectiva a la situación actual de los Gobiernos frente al cibercrimen.

### 6.3.1 Marco Legal Colombiano

En Colombia como respuesta a esta grave situación también se han realizado esfuerzos en materia normativa, con el fin de crear una legislación que proporcione las capacidades legales para afrontar la ciberdelincuencia, garantizando la seguridad de los sistemas, proporcionando herramientas de

defensa y una adecuada implementación de la justicia. Es así como se cuenta con los siguientes instrumentos legales relacionados con la ciberdelincuencia, ciberseguridad y ciberdefensa, los cuales se encuentran explicados por orden cronológico de expedición.

#### 6.3.1.1 Normatividad expedida entre 1900 – 1999

Ley 527 de 1999, conocida como la ley del Comercio Electrónico, es la norma en donde se define y se reglamenta lo relacionado con el uso y el acceso del comercio electrónico, los mensajes de datos y las firmas digitales, e igualmente se definen las entidades de certificación.

#### 6.3.1.2 Normatividad expedida entre 2000 – 2009

Ley 599 de 2000, es la norma mediante la cual se expide el Código Penal.

Ley 594 de 2000, es la ley general de archivos y criterios de seguridad, la cual da a conocer los conceptos sobre los distintos tipos de archivos, permitiendo comprender la función archivística, exponiendo la elaboración del documento hasta su eliminación o conservación permanente, además de ello regula el proceder de los funcionarios en relación a cómo se deben archivar y que se debe hacer con los documentos que se generen dentro de una entidad u empresa.

Ley 906 de 2004, es la norma mediante la cual se expide el Código de Procedimiento Penal.

Ley 962 de 2005, es la norma donde se desarrolla la racionalización y simplificación de los trámites, incentivando el uso de medios tecnológicos para reducir los tiempos y costos de su realización y estableciendo las características de seguridad de la información electrónica en las entidades públicas.

Ley 1150 de 2007, aquí se establecen las disposiciones para la contratación con recursos públicos, introduciendo las medidas para la transparencia y eficiencia, definiendo además la posibilidad de que se expidan actos administrativos y se hagan notificaciones a través de medios electrónicos, vislumbrando el desarrollo del Sistema Electrónico para la Contratación Pública (Secop).

Circular 052 de 2007 de la Superintendencia Financiera de Colombia, es donde se establecen los requerimientos mínimos de calidad y seguridad en el manejo de información a través de canales y medios de distribución de productos y servicios para clientes y usuarios.

Ley estatutaria 1266 de 2008, es la norma mediante la cual se regula el manejo de la información contenida en bases de datos personales, principalmente la financiera, comercial, crediticia, de servicios y la proveniente de otros países, e igualmente se establecen las dispones legales relacionadas con el hábeas data.

Ley 1273 de 2009, es conocida como la ley de los delitos informáticos, en donde se modifica el Código Penal y se crea un nuevo Bien Jurídico Tutelado de la Protección de la Información y de los Datos.

Ley 1341 de 2009, es la norma en la cual se establecen los conceptos y principios de la sociedad de la información, la organización de las TIC y la creación de la Agencia Nacional de Espectro.

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009, en donde se establecen las obligaciones de los proveedores de redes y servicios de telecomunicaciones en relación a la seguridad de la información y la inviolabilidad de las comunicaciones.

#### 6.3.1.3 Normatividad expedida entre 2010 – Año presente 2017

Ley estatutaria 1581 de 2012, es la norma por medio de la cual se definen las disposiciones para la protección de datos personales, ya sea dentro del territorio colombiano o cuando al responsable del manejo de esta se le apliquen las normas colombianas en virtud de tratados internacionales.

Decreto 2364 de 2012, en donde se tratan aspectos relacionados con la firma electrónica, reglamentando el artículo 7° de la Ley 527 de 1999 sobre la firma electrónica, igualmente se establecen disposiciones en relación al uso de la firma electrónica, su creación, métodos empleados y el firmante.

Decreto 2609 de 2012, aquí se tratan aspectos relacionados con el expediente electrónico, reglamentando el Título V de la Ley 594 de 2000, y parcialmente los artículos 58 y 59 de la Ley 1437 de 2011, fijando por ultimo las disposiciones en cuanto a la gestión documental para las organizaciones del Estado.

Decreto 2693 de 2012, en donde se desarrollan los temas concernientes al gobierno electrónico, estableciendo los lineamientos generales de la Estrategia de Gobierno en Línea, y reglamentando de forma parcial las Leyes 1341 de 2009 y 1450 de 2011.

Decreto 1377 de 2013, es donde se definen las disposiciones sobre la protección de datos personales, reglamentando parcialmente la Ley 1581 de 2012, e igualmente define otras disposiciones relacionadas con el tratamiento de datos en el ámbito personal o doméstico.

De todas las disposiciones legales presentadas la Ley 1273 de 2009 y Ley 906 de 2004 son empleadas para la administración de la justicia en un caso donde interviene como medio probatorio la evidencia digital.

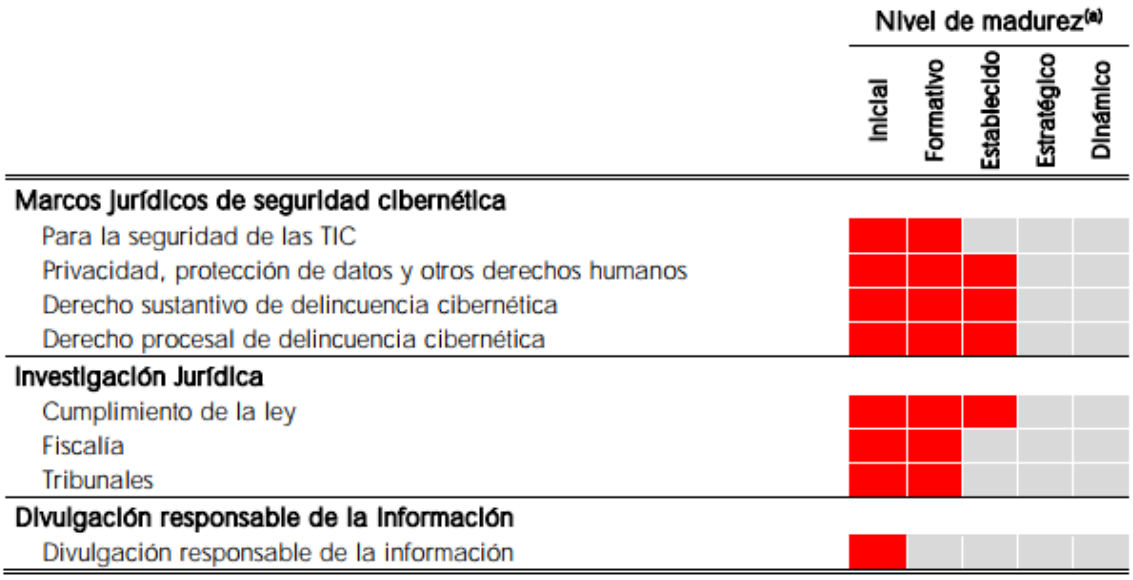
### 6.3.2 Capacitación de los Operadores Jurídicos

Para ver de forma la clara la respuesta que ha tenido el sistema judicial en Colombia frente a la administración de la justicia en los casos relacionados con los delitos informáticos, como comúnmente se les conoce a los ciberdelitos, sea hace particularmente necesario añadir el resultado de la evaluación desarrollada por el CONPES[95] (Consejo Nacional de Política Económica y Social) en relación a la política nacional de seguridad digital, la cual fue divulgada en el documento CONPES 3854[96] en abril del 2016, y en donde se refleja el nivel de madurez de la legislación colombiana frente a los distintos aspectos de seguridad cibernética en el país, véase la figura 2.

Figura 2. Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia.

[95] El Consejo Nacional de Política Económica y Social, CONPES. Departamento Nacional de Planeación - DPN. https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

[96] CONPES 3854. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Consejo Nacional de Política Económica y Social, Departamento de Planeación. República de Colombia. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf




Fuente: CONPES 3854

La grafica muestra claramente que, aunque se ha avanzado en el desarrollo de la normatividad colombiana está aún no se encuentra en un nivel estratégico, indicando que, pese a que existe la legislación para tratar múltiples aspectos concernientes a los ciberdelitos no es posible garantizar su efectividad. Esto se debe a distintos factores entre los que se encuentra el desconocimiento de la conducta criminal informática por parte de los administradores de justicia, en este caso específicamente los jueces, lo cual causa que se disminuyan sus capacidades para ejercer sus funciones acorde con las nuevas políticas.

Tal como lo manifiesta Alexander Díaz, quien redactó el proyecto y ahora Ley 1273 de 2009, no es que haga falta tipificación de las conductas informáticas delictivas, conocidas como ciberdelitos, en Colombia, sino que hay un pronunciado desinterés por parte del aparato judicial para difundir información entre la rama al respecto. Por lo tanto, debido a la poca capacitación de los jueces en esta materia, se hace imposible dar viabilidad a las leyes que hacen frente al ciberdelito, causando que se tramiten las conductas delictivas informáticas como delitos tradicionales conllevando consigo graves consecuencias jurídicas, pues se juzga el delito entendiéndose como una forma novedosa de llevar a cabo delitos tradicionales, entorpeciendo el juzgamiento de los crímenes cometidos bajo esta modalidad, pues estos terminan siendo procesados como crímenes tradicionales.

Para comprender con mayor amplitud la situación actual del conocimiento que los jueces poseen en materia de ciberdelitos y el trámite que se debe llevar a cabo en estos procedimientos judiciales que los involucran, se recurre a los resultados de la investigación realizada por la Dra. Ana María Mesa Elneser con apoyo de la

Fundación Universitaria Luis Amigo, donde se desarrolló una consulta mediante el instrumento de encuesta cerrada proponiendo una serie de interrogantes frente al reconocimiento, interpretación, divulgación, suficiencia y redacción de los ciberdelitos; la cual fue llevada a cabo sobre la muestra poblacional circunscrita a los municipios que integran el Área Metropolitana del Valle de Aburra y Envigado para un total de 30 jueces consultados.

Se evaluaron cinco objetivos específicos que son:

1) **Presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.**

   En donde solo el 50% de los jueces entrevistados reconocieron el conjunto de tipos penales informáticos vigentes en la legislación colombiana.

   Y en relación a la pregunta sobre si creía que los tipos penales consagrados en la ley colombiana son suficientes para procesar las diferentes conductas delictivas que se desarrollan en el campo cibernético el 57% de los jueces manifestaron no saber o no respondieron, el 25% estuvieron parcialmente de acuerdo, 15% estuvieron de acuerdo, y 3% en desacuerdo

2) **Listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuales son o se pueden presentar como evidencia digital y física en relación con un tipo penal informático.**

   En donde el 70% de los jueces entrevistados compartieron que es clara la caracterización de la prueba para la defensa en un juicio sobre delitos informáticos, y el 30% manifestaron lo contrario.

   Y en relación a la pregunta sobre si estimaban valido que los medios probatorios existentes en la ley 906 de 2004 pudieran ser empleados como evidencia física o digital en un proceso sobre delitos informáticos, el 57% de los jueces no supieron o no respondieron, el 25% estuvieron de acuerdo, el 15% estuvieron parcialmente de acuerdo y el 3% manifestaron estar totalmente de acuerdo.

3) **Identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.**

En donde el 90% de los jueces manifestaron desconocer los protocolos forenses que se deben aplicar en Colombia para la investigación de los ciberdelitos, y solo el 10% dijeron conocerlos.

Y en relación a la pregunta sobre si conoce la formación profesional, capacidades y certificación que debe tener un experto en informática forense para la obtención de las pruebas y realización del informe pericial el 90% de los entrevistados manifestó desconocerlos y solo el 10% dijo tener conocimiento sobre este aspecto.

4) **Verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis post mortem de un incidente en Colombia.**

   En donde el 87% de los jueces entrevistados manifestaron desconocer el protocolo de la cadena de custodia para el análisis de los dispositivos electrónicos que almacenan información, y solamente el 13% dijeron conocerlo.

   Y en relación a la pregunta sobre si conoce los requisitos materiales y formales que se deben verificar del elemento material probatorio (EMP) en el manejo del laboratorio forense, con el fin de que la evidencia digital sea aceptada como prueba electrónica, el 80% manifestó desconocerlos y solo el 10% dijo conocerlos.

5) **Analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal.**

   En donde el 87% de los jueces entrevistados manifestaron desconocer el procedimiento que realiza la Dirección de Investigación Criminal e Interpol (DIJÍN) para la recepción, análisis de los elementos materiales de prueba y posterior entrega del informe y de los elementos materiales de prueba, y solo el 13% dijeron conocerlo.

   Y en relación a la pregunta sobre si el procedimiento efectuado por la DIJIN permite la aplicación de protocolos inapropiados en el manejo del elemento material probatorio en el laboratorio forense, el 90% manifestó que no y el 10% restante respondió de forma afirmativa.

Lo anterior deja ver las falencias que poseen los jueces debido al desconocimiento de los delitos informáticos e inclusive la falta de interpretación jurídica sobre el alcance y aplicabilidad de los tipos penales, evidenciándose la falta de capacitación, profesionalización y actualización en esta materia. Es así como se hace necesario tomar medidas en cuanto a la divulgación de la normatividad relacionada con la ciberdelincuencia dentro de la rama judicial y la capacitación o

actualización de la interpretación de las normas jurídicas por parte de los jueces, de modo que se pueda avanzar de forma efectiva en la investigación de estas conductas delictivas durante el procedimiento judicial, manejando de forma adecuada todo lo concerniente al proceso probatorio durante el juicio, mejorando así la judicialización de estos delitos y permitiendo que la justicia se administre con total contundencia.

## 6.4 CONSIDERACIONES SOBRE EL PERITAJE INFORMÁTICO Y LOS ESTÁNDARES DE MANIPULACIÓN DE PRUEBAS EN COLOMBIA

Dentro de las consideraciones iniciales para la correcta ejecución del peritaje informático, en el cual se desarrolla la identificación, recolección, manipulación y análisis de la evidencia digital, es importante tener presente algunas medidas antes de iniciar este procedimiento, de modo que se planifique de forma adecuada y certera la realización de las actividades de investigación. Estas medidas se definen a continuación:

1) Confirmar que haya tenido lugar un incidente informático.
2) Revisar si es necesario o pertinente el desarrollo del análisis forense al incidente informático reportado.
3) Definir lo que se quiere conocer y la forma en la que estará orientada la investigación.

Después de que se haya realizado la verificación de las medidas iniciales se procede al desarrollo de las fases que componen el procedimiento del peritaje informático.

### 6.4.1 Metodología General del Procedimiento del Peritaje Informático de la Evidencia Digital

La metodología general del procedimiento del peritaje informático de la evidencia digital se compone de cinco fases principales acorde con la Guía No. 13[97] desarrollada por el MINTIC[98] (Ministerio de Tecnologías de la Información y las

[97] Guía No. 13. Evidencia Digital. Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), 2016. https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

[98] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). http://www.mintic.gov.co/portal/604/w3-channel.html

Comunicaciones), como referencia al Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea[99]. Esta guía fue desarrollada en base a la norma técnica colombiana NTC ISO/IEC 27035[100] vigente, y la NIST SP 800-86[101] (Guide to Integrating Forensic Techniques into Incident Response).

Figura 3. Diagrama del Proceso del Peritaje Informático de la Evidencia Digital


Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)

#### 6.4.1.1 Aislamiento de la escena

Una vez que se confirma el incidente de seguridad se procede a restringir el ingreso a la zona en donde se produjo. Lo ideal es que alguna autoridad competente como el Centro Cibernético Policial (CCP) o el Grupo de Respuesta a Emergencias Cibernéticas (COLCERT) realice el aislamiento de la escena, sin embargo, dada la urgencia y necesidad de asilar este espacio a la mayor brevedad, se puede realizar por personal especializado, como un ingeniero forense, el cual debe contar con la capacidad necesaria

[99] Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las Comunicaciones. http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

[100] NTC ISO/IEC 27035. ICONTEC. https://tienda.icontec.org/wp-content/uploads/pdfs/GTC-ISO-IEC27035.pdf

[101] NIST SP 800-86. NIST. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875

para describir de forma detallada los procedimientos empleados y realizar la captura de la evidencia.

Aquí se inicia la cadena de custodia la cual es el procedimiento que tiene como objetivo garantizar que la evidencia es auténtica e integra al momento de presentarse ante el tribunal penal o el comité disciplinario. La información mínima que se debe manejar en una cadena de custodia es la siguiente:

- *Una hoja de ruta:* En donde se describe la evidencia, indicando las fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega.
- *Recibos personales:* En donde están datos similares a los de la hoja de ruta y que guarda cada custodio.
- *Etiquetas*: Que van pegadas en los empaques de las evidencias, ya sean bolsas plásticas, sobres de papel, cajas, frascos, etc.
- *Libros de registro de entradas y salidas:* Los cuales se deben llevar en los laboratorios y en los despachos de los fiscales e investigadores.[102]

Para este fin la fiscalía desarrolló un procedimiento oficial llamado “Manual Único de Cadena De Custodia”, el cual describe de forma completa los pasos para para asegurar la evidencia desde que es recolectada hasta su disposición final.

#### 6.4.1.2 Identificación de fuentes de información

En esta fase se identifican las posibles fuentes de información de donde se podría obtener la evidencia, entre las cuales las más comunes son: Los computadores portátiles o de escritorio, servidores, dispositivos USB, Firewire, CD/DVD, PCMCIA, discos duros, Memorias SD y MicroSD, entre otros medios internos y externos de almacenamiento de información, igualmente dispositivos celulares, PDAs, cámaras digitales y grabadoras de audio. También se pueden considerar otras fuentes de información como: Logs de dispositivos de seguridad informática (IDS, Firewalls, plataformas

[102] Guía No. 13. Evidencia Digital. Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), 2016. https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

antispam y Proxy), Logs de dispositivos de red (Switch o Router), y Logs de proveedores de servicio, los cuales solamente se pueden extraer bajo órdenes judiciales.

Se debe decidir hasta qué punto se está en capacidad de realizar la recolección y análisis de la evidencia, por lo que se aconseja contactar al CCP o el COLCERT con el fin de recibir instrucciones para la realización de estos procedimientos, y así poder continuar con el desarrollo de las demás fases del peritaje informático.

#### 6.4.1.3 Recolección y examinación de información

La secuencia general para la recolección de la información incluye 3 etapas, los cuales se describen a continuación:

1) Planificación de la recolección de los datos: Se especifican las fuentes de información de las que se extraerán los datos y el orden en que se va a proceder, teniendo en cuenta la volatilidad y complejidad de la información contenida.
2) Recolección de los datos: Se emplean herramientas de informática forense para obtener la información que será utilizada como evidencia. Este proceso puede variar dependiendo si el acceso a la información es local o a través de la red.
3) Verificación de la integridad de los datos recolectados: Se emplea herramientas de Hash o funciones de resumen, las cuales generan un valor que debe ser igual en la copia y en la fuente original. Esta verificación se realiza con efectos legales, con el fin de asegurar que la evidencia no ha sido modificada y es auténtica.

Se debe extremar el cuidado en la manipulación de las fuentes de información y de los datos si la evidencia obtenida va a emplearse con fines legales, por lo que se aconseja llevar a cabo la cadena de custodia adecuadamente, registrando cada una de las acciones que se desarrollaron en la recolección y almacenamiento de la evidencia.

La secuencia específica a seguir para la recolección y examinación de la información incluye las siguientes actividades:

1) Creación del archivo ‘bitácora de hallazgos’, para la cadena de custodia.
2) Generación de la imagen de datos.

3) Verificación de integridad de la imagen.
4) Creación de una copia de la imagen suministrada.
5) Aseguramiento de la imagen original suministrada.
6) Revisión antivirus y verificación de la integridad de la copia de la imagen.
7) Identificación de las particiones actuales y anteriores.
8) Detección de información en los espacios entre las particiones.
9) Detección de un hpa (host protected area).
10) Identificación del sistema de archivos.
11) Recuperación de los archivos borrados.
12) Recuperación de información escondida.
13) Identificación de archivos existentes.
14) Identificación de archivos protegidos.
15) Consolidación de archivos potencialmente analizables.
16) Determinación del sistema operativo y las aplicaciones instaladas.
17) Identificación de información de tráfico de red.
18) Depuración de archivos buenos conocidos.
19) Consolidación de archivos sospechosos.
20) Realización de la primera clasificación de archivos.
21) Realización de la segunda clasificación de archivos.

#### 6.4.1.4 Análisis de la información

En esta fase se realiza el análisis de la información que fue seleccionada en la etapa anterior después de los diferentes procesos de depuración, llevándose a cabo las siguientes actividades:

1) Análisis de la información prioritaria: Cuyo nivel de importancia depende se la relevancia que tenga en relación al caso y del criterio del investigador.
2) Generación del listado de archivos comprometidos con el caso: Se listan los archivos que hacen parte de la evidencia.
3) Obtención de la línea de tiempo de la evidencia: Se realiza la reconstrucción de los hechos en una línea de tiempo, teniendo en cuenta las fechas de modificación, acceso y creación de los archivos.
4) Generación de informe final: Se desarrolla el informe de los hallazgos encontrados, realizando una descripción detallada.

#### 6.4.1.5 Reporte

Se realiza el reporte en el cual se presenta toda la información y la evidencia obtenida en la fase de análisis. Este documento debería contener lo siguiente:

- El resultado de los análisis.
- La explicación del cómo y por qué fueron utilizadas las diferentes herramientas forenses.
- Definición de las acciones a tomar.
- Definición de las recomendaciones y otras observaciones en relación al proceso forense.

### 6.4.2 Presentación del Informe Pericial

En Colombia, el informe pericial no tiene una estructura establecida por ley, sin embargo, se sugiere considerar algunos elementos de modo que la veracidad del procedimiento sea verificable en un corte, los cuales se mencionan a continuación:

I. Encabezado. El cual permitirá identificar: el código del caso, la solicitud efectuada, el nombre de los investigadores, los participantes, y la clasificación de la información.
II. Introducción. Describe la conducta o hechos que se investigan, el objetivo de los análisis y los alcances del peritaje que se llevara a cabo.
III. Verificación de la cadena de custodia. Define de forma específica las fuentes de información que se reciben y sus características, en qué fecha, de quién, sus marcas y seriales, los peritos que las reciben y el identificador del caso, entre otros aspectos.
IV. Preparación de la evidencia. Se detalla el proceso forense, especificando las herramientas que serán empleadas, la preparación de los medios que se analizarán, los detalles de los análisis que se desarrollarán y las verificaciones del caso.
V. Análisis de la evidencia. Detalla la forma en cómo fueron empleadas las herramientas forenses para el análisis de las copias autenticadas de la evidencia recogida.
VI. Hallazgos obtenidos como resultado de la aplicación de las herramientas de informática forense. Se realiza la definición general de los archivos, información recuperada, sitios en los medios, entre otros aspectos.
VII. Conclusiones. Tratan los hechos investigados, sin juicios de valor, basadas en los hechos y datos recolectados a partir del uso de las herramientas forenses.
VIII. Firma del perito. La cual permitirá certificar los hallazgos y procedimientos aplicados sobre el material probatorio entregado.

### 6.4.3 Estándares de Manipulación de Pruebas

En el mundo existe una innumerable cantidad de estándares de manipulación de pruebas, los cuales se han dado a conocer mediante publicaciones de entidades de investigación reconocidas. Sin embargo, aunque en Colombia no existe un estándar propiamente definido, se han desarrollado iniciativas gubernamentales, que se han plasmado en el documento CONPES 3701[103], que trata sobre los Lineamientos de política para Ciberseguridad y Ciberdefensa, y los cuales se listan a continuación:

1) NIST SP 800-61 – Computer Security Incident Handing Guide
2) NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response
3) RFC 2350 – Expectations for Computer Security Incident Response
4) RFC 3227 – Guidelines for Evidence Collection and Archiving
5) ISO/IEC 17015:2005 – Requisitos generales para la competencia de laboratorios de ensayo y calibración
6) ISO/IEC TR 18044:2004 Gestión de Incidentes de Seguridad de la Información
7) Electronic Crime Scene Investigation: A Guide for Fisrt Responders, Second Edition
8) Digital Evidence in the Courtroom: A Guide for Law Enforcement Prosecutors
9) Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability Version 2.0
10) Incident Management Mission Diagnostic Method, version 1.0
11) Incident Management Capability Metrics Version 0.1
12) Creating a Computer Security Incident Response Team: A Process for Getting Started
13) First Responders Guide to Computer Forensics: Advanced Topics
14) Handbook for Computer Security Incident Response Teams (CSIRTs) version 2
15) CSIRT Services
16) A Common Language for Computer Security Incidents
17) Homeland Security - Legal Division Handbook
18) Best Practices For Seizing Electronic Evidence v. 3. A Pocket Guide for First Responders

[103] CONPES 3701. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Consejo Nacional de Política Económica y Social, Departamento de Planeación. República de Colombia. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

El uso de uno o varios de estos estándares no propende el cumplimiento de alguna normatividad, sino que se desarrolla en base al criterio individual del investigador.

# 7 DIVULGACIÓN Y RECOMENDACIONES

La divulgación de esta monografía se realizará mediante la publicación del trabajo de grado en el repositorio institucional de la biblioteca de la Universidad Nacional Abierta y a Distancia (UNAD).

Este trabajo estará disponible para todos los interesados, dirigiéndose tanto al personal especializado encargado de realizar el peritaje de la evidencia digital, mediante el uso de técnicas de informática forense, como el personal encargado de presentar el caso ante la justicia colombiana, en el cual se muestra el estado actual del peritaje informático en Colombia y su lugar dentro de la justicia en el país, mediante el análisis de los retos que enfrenta y su situación tanto en el escenario internacional como interno, e igualmente se precisa la importancia que tiene la información electrónicamente almacenada (ESI) en el ordenamiento jurídico colombiano, evidenciando la formación con la que cuentan los jueces en el país en temas de delitos informáticos y su implicación en la administración de la justicia, y por último se presentan las consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas en el contexto nacional.

# 8 CONCLUSIONES

Teniendo en cuenta la información que se recolecto en el proceso del desarrollo de la presente investigación y los distintos temas que se derivaron del mismo, se realizó un análisis en donde se identificaron aspectos positivos y negativos dando lugar a las siguientes conclusiones.

El peritaje informático es una actividad de investigación que ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales donde interviene la evidencia digital, a raíz del aumento de los ciberdelitos, pues permite esclarecer los hechos ocurridos en un caso específico, brindando las herramientas para dirimir y lograr la impartición de la justicia de manera adecuada.

En Colombia se cuenta con un marco legal que abarca muchos aspectos relacionados con la ciberdelincuencia, la ciberseguridad y la ciberdefensa, en el cual se tratan aspectos concernientes principalmente a la admisibilidad de la evidencia digital en las cortes, sin embargo, no se encuentra definido de forma clara muchas características de la presentación y aceptación de la evidencia digital en el Código del Procedimiento Penal, sino que su definición está implícita.

En cuanto a los demás aspectos del peritaje informático concernientes al proceso de investigación, no está definido dentro del marco legal los estándares de manipulación de pruebas válidos, sino que se deja al libre criterio del investigador, dejando vacíos jurídicos que pueden influir posteriormente en la decisión del juez de aceptar o no las pruebas presentadas.

El órgano judicial en Colombia cuenta con un marco jurídico amplio en relación a los aspectos concernientes a la ciberdelincuencia, pero debido al desconocimiento por parte de los jueces, la impartición de la justicia flaquea y en ocasiones se pierde, dañando la confianza que la sociedad deposita en la justicia como medio para proteger sus derechos y castigar con rigor toda conducta ilícita.

## BIBLIOGRAFÍA


ACUÑA G., José Y SOTELO V., Diego A. La política criminal en los menores adolescentes en Colombia [en línea]. Revista Iter Ad Veritatem, vol. 14, 2016. ISBN 1909-9843. [citado el 28 octubre 2017], pp.181-193. Disponible en Internet: <http://revistas.ustatunja.edu.co/index.php/iaveritatem/article/view/1339/1242>

BARRIO, Marta. Estándares de manipulación de pruebas digitales: RFC 3227 [en línea]. Actualizado el 20 junio 2014. [citado el 11 mayo 2017]. Disponible en Internet: <http://wh0s.org/2014/06/20/estandares-de-manipulacion-de-pruebas-digitales-rfc-3227/>.

CAMELO, Leonardo. Marco legal de Seguridad de la Información en Colombia [en línea]. Actualizado el 23 febrero 2010. [citado el 11 mayo 2017]. Disponible en Internet: <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html>.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL [en línea]. Lineamientos de política para Ciberseguridad y Ciberdefensa. [Bogotá D.C., Colombia]: Departamento Nacional de Planeación, 2011. [citado el 11 mayo 2017]. Disponible en Internet: <https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>.

EVIDENCIAS INFORMÁTICAS [en línea]. Peritaje Informático. Actualizado el 2012. [citado el 11 mayo 2017]. Disponible en Internet: <http://www.evidenciasinformaticas.com/index.asp?IdContenido=3>.

FERREYRO, A., Y LONGHI, A. D. Metodología de la investigación [en línea]. [Córdoba, Argentina]: Encuentro Grupo Editor, 2014. [citado el 11 mayo 2017]. Disponible en Internet: <http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=847674&lang=es&site=eds-live>.

FISCALÍA GENERAL DE LA NACIÓN [en línea]. Manual de Procedimientos para Cadena de Custodia. [Bogotá D.C., Colombia]. ISBN 958-97542-8-7. [citado el 11 mayo 2017] Disponible en Internet: <http://www.fiscalia.gov.co/en/wp-content/uploads/2012/01/manualcadena2.pdf>.

FUENTES A., Yolfaris N. DERECHO INFORMÁTICO [en línea]. [Medellín, Colombia]: Corporación Universitaria Remington, 2016. [citado el 28 octubre 2017], Cuarta Edición. Disponible en Internet: <http://imagenes.uniremington.edu.co/moodle/M%C3%B3dulos%20de%20aprendizaje/Derecho%20informatico/Derecho%20informatico_2016.pdf>

GANDINI, Isabela. Y ISAZA, Andrés. Y DELGADO, Alejandro. Ley de Delitos Informáticos en Colombia [en línea]. Actualizado el 2016. [citado el 11 mayo 2017]. Disponible en Internet: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>.

GERCKE, Marco. Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica [en línea]. [Ginebra, Suiza]: ITU, 2014. ISBN 978-92-61-15643-5. [citado el 28 octubre 2017]. Disponible en Internet: <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf>

GERENCIA TÉCNICA DEL CPAU [en línea]. Costos de un proyecto para tener en cuenta. Actualizado el 25 junio 2013. [citado el 11 mayo 2017]. Disponible en Internet: <https://www.clarin.com/arq/arquitectura/Costos-proyecto-tener-cuenta_0_rkgGuALiDXl.html>.

JARAMILLO A., Diego A. Y TORRES M., Martha L. ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA [en línea]. [Bogotá, D.C., Colombia]: Universidad Militar Nueva Granada, 2016. [citado el 10 noviembre 2017]. Disponible en Internet: <http://repository.unimilitar.edu.co/bitstream/10654/14401/1/TorresMoncadaMarthaLiliana2016.pdf>

LERMA, H. D. Metodología de la investigación: Propuesta, Anteproyecto y Proyecto [en línea]. [Bogotá, D.C., Colombia]: Ecoe ediciones, 2009. [citado el 11 mayo 2017]. Disponible en Internet: <http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=483354&lang=es&site=eds-live>.

MESA E., Ana M. Aproximación a la Informática Forense y el Derecho Informático: Ámbito Colombiano. [en línea]. [Medellín, Colombia]: Fondo Editorial Funlam, 2013. ISBN 978-958-8399-67-6. [citado el 28 octubre 2017]. Disponible en Internet: <http://www.funlam.edu.co/uploads/fondoeditorial/84_Aproximacion_a_la_informatica_forense.pdf>

OJEDA P., Jorge E. Y RINCÓN R, Fernando. Y ARIAS F., Miguel E. Y DAZA M., Libardo A. Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. [en línea]. 2010, vol.11, n.28 [citado el 11 mayo 2017], pp.41-66. Disponible en Internet: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&nrm=iso>. ISSN 0123-1472>.

PÉREZ G., Camilo. ¿En Colombia se investigan los delitos informáticos? [en línea]. Actualizado el 1 mayo 2013. [citado el 11 mayo 2017]. Disponible en Internet: <https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html>.

POROLLI, Matías. ¿En qué consiste el análisis forense de la información? [en línea]. Actualizado el 12 agosto 2013. [citado el 11 mayo 2017]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/>.

MARTIN M., Raúl. Introducción al Derecho Informático [en línea]. [citado el 11 mayo 2017]. Disponible en Internet: <https://www.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf>.

RINCÓN C., Erick. Instrumentos Normativos de Ciberseguridad [en línea]. [Colombia]: Certicamara, 2014. [citado el 11 mayo 2017]. Disponible en Internet: <https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

RUIZ O., J. I. Metodología de la investigación cualitativa [en línea]. [Bilbao, España]: Universidad de Deusto, 2012. [citado el 11 mayo 2017]. Disponible en Internet: <http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=edsebk&AN=869656&lang=es&site=eds-live>.

# ANEXOS

## ANEXO A. RESUMEN ANALÍTICO ESPECIALIZADO RAE

| | |
|---|---|
| **Título de Documento** | ESTADO DEL PERITAJE INFORMÁTICO DE LA EVIDENCIA DIGITAL EN EL MARCO DE LA ADMINISTRACIÓN DE LA JUSTICIA EN COLOMBIA |
| **Autor** | Violeth Lasso Vivas |
| **Palabras Claves** | • Peritaje informático<br>• Cadena de custodia<br>• Análisis forense<br>• Estándares de manipulación<br>• Presentación de pruebas<br>• Justicia en Colombia |
| **Descripción** | Este documento es una monografía que describe el estado actual del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia. |

**Resumen**

En Colombia se considera la justicia como uno de los principales fines del Estado, sin embargo, no siempre es bien administrada y dependiendo de quien la dicte puede tomar distintos enfoques tanto en su efectividad como en su alcance, aunque existan leyes específicas establecidas para múltiples casos; no obstante, en una nueva era del conocimiento en la que se multiplica el desarrollo social mediante el uso de la tecnología, pues esta ha brindado un espacio en el que se lleva a cabo interacción humana e intercambios sociales, culturales, económicos, científicos, etc., se hizo necesario el desarrollo de leyes y demás normas jurídicas, con el fin de regular la comunicación a través de medios tecnológicos, de manera que sea segura, confiable y permita la judicialización de cualquier acto delictivo que atente contra en bienestar integral de los ciudadanos. Es así como, quienes integran esta rama del poder actúan en función de resolver los conflictos de forma justa, mediante la implementación y uso de las diferentes instancias y normas jurídicas, empleando la imparcialidad, la autonomía judicial, el sistema jurídico establecido, el juicio, la seguridad jurídica, la doble instancia, la fiscalía y el debido proceso, buscando dirimir los conflictos ocasionados por intereses en pugna a fin de lograr y conservar un orden social; pese a ello, debido a la amplia gama de disposiciones legales, se desconoce, en la mayoría de los casos, la forma en como el peritaje informático y la evidencia digital, tienen lugar dentro de la justicia colombiana; por esta razón, con el fin de definir el estado actual del cómo se lleva a cabo la distribución de la justicia bajo la normatividad establecida en relación al peritaje

informático, se hizo necesaria la revisión del marco legal para los casos relacionados con la protección de la información y de los datos, con el fin dar a conocer la situación actual.

El presente trabajo muestra el estado actual del peritaje informático en Colombia y su lugar dentro de la justicia en el país, mediante el análisis de los retos que enfrenta y su situación tanto en el escenario internacional como interno, precisando la importancia que tiene la información electrónicamente almacenada en el ordenamiento jurídico colombiano, evidenciando la formación con la que cuentan los jueces en el país en temas de delitos informáticos y su implicación en la administración de la justicia, y por ultimo presentando las consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas en el contexto nacional.

**Metodología**

Inicialmente se identificó el área problema, y se partió de la lectura del mayor número posible de documentos que presentan explicaciones sobre el fenómeno en estudio, buscando abordar los diferentes tipos de investigaciones que se han efectuado, sus referentes disciplinares y teóricos, las poblaciones y muestras, las delimitaciones temporales y contextuales en las que se han desarrollado.

Posteriormente, se establecieron las relaciones lógicas entre los argumentos aportados por cada uno de los textos en estudio, asimilando las teorías, tendencias y resultados mostrados en cada documento, describiendo no solamente los hallazgos, sino realizando una interpretación de estos, dando lugar a la construcción del presente documento.

Por último, se estableció la comprensión de los diversos temas que se estudiaron, realizando un balance teórico global, en el que se evidenciaron los vacíos, limitaciones, dificultades, tendencias, posturas y logros en el tema abordado, lo cual permitió conocer su estado actual y determinar los distintos factores que abarca, con el fin de consolidar un trabajo que abordara los temas previstos a ser tratados.

**Conclusiones**

El peritaje informático es una actividad de investigación que ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales donde interviene la evidencia digital, a raíz del aumento de los

ciberdelitos, pues permite esclarecer los hechos ocurridos en un caso específico, brindando las herramientas para dirimir y lograr la impartición de la justicia de manera adecuada.

El órgano judicial en Colombia cuenta con un marco jurídico amplio en relación a los aspectos concernientes a la ciberdelincuencia, pero debido al desconocimiento por parte de los jueces, la impartición de la justicia flaquea y en ocasiones se pierde, dañando la confianza que la sociedad deposita en la justicia como medio para proteger sus derechos y castigar con rigor toda conducta ilícita.