# DIFICULTADES EN EL MANEJO DE LA EVIDENCIA DIGITAL EN EL PROCESO PENAL COLOMBIANO

**John Rodrigo Londoño Naranjo**[1]

*"El uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado. De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo.*

*La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica3, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas4. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil.*
*Trabajar en temas de ciberseguridad y ciberdefensa implica un compromiso del Gobierno Nacional por garantizar la seguridad de la información. Por ello, si bien este documento busca sentar las bases de política para los tópicos de ciberseguridad y ciberdefensa en particular, las entidades involucradas tendrán la responsabilidad de desarrollar estas bases y generar mecanismos que permitan garantizar la seguridad de la información a nivel nacional. Para lo anterior, se tendrán en cuenta las normas técnicas y los estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad…"*

*CONPES 3701 DE 2011*

[1] Abogado, especialista en derecho Penal, candidato a Magister en Derecho Penal y Teoría del Delito, monografía realizada bajo la tutoría del profesor César Alejandro Osorio Moreno, correo electrónico: jrgarfiel@gmail.com

## TABLA DE CONTENIDO

**RESUMEN**

Para el desarrollo de este tema se nos hace necesario distinguir entre datos e información, pues si bien es cierto entre ambos hay una gran diferencia, hablar de datos es hablar de símbolos, códigos, números, etc. Que estos por si solos como un hecho aislado no dice nada, pero cuando estos se concatenen unos entre otros podemos decir que ya hay información, la cual puede ser o no relevante al proceso o lo que se busca, pero algo muy importante a tener en cuente al momento de buscar estos datos que nos suministren información, es el tener el tacto suficiente y la prudencia necesaria para no incurrir en actos contrarios a la ley, como sería el caso de la violación a la intimidad de las personas, la dignidad humana entre otros, no menos graves.

Es de esta forma que analizamos desde nuestra propia legislación como de una forma u otra se ha venido preocupando por el tema, toda vez que se ha legislado sobre el mismo y se han hecho algunas reformas, como lo podemos detectar en nuestro código penal con la reforma del código al ser insertado en el artículo 269A y S.S., llamados delitos informáticos y todo lo que tiene que ver con los mismos, pero a modo de critica vemos que el legislador se quedó corto toda vez que solo se preocupó por algunos delitos contra el patrimonio económico, sin tener en cuenta que en esta nueva modalidad de delincuencia también se ven afectados otros tipos penales no menos importantes y que también son tutelados, las amenazas, la extorción, el chantaje, la injuria, la falsedad, la estafa. En cada uno de estos tipos penales se observa que claramente cumple con los requisitos antes mencionadas, encajan perfectamente en los verbos rectores, cuentan con un sujeto activo y uno pasivo, hay una lesión, circunstancias de modo, tiempo y lugar.

A estos tipos penales teniendo en cuenta el medio que se utiliza para cometer el acto, se hace necesario hablar de una análisis forense, para lo que se requiere que nos sea cualquier persona, sino una persona debidamente capacitada y con la formación debida para realizar este tipo de investigaciones, en el análisis forense,

se detectan los tipos de ataques perpetuados, que herramientas fueron utilizadas y como sería su posible solución esto en cuanto a los virus, o trampas creadas, no solo para la prevención, sino para poder detectar los posibles responsables y poder finalmente obtener una condena por los actos contrarios a la ley cometidos.


## PALABRAS CLAVES:

Pruebas - Delitos informáticos - Proceso penal colombiano



**SUMMARY**

For the development of this topic it is necessary to distinguish between data and information, because although it is true between both there is a big difference, talking about data is talking about symbols, codes, numbers, etc. That these alone as an isolated event does not say anything, but when these are concatenated among others we can say that there is already information, which may or may not be relevant to the process or what is sought, but something very important to have in count when looking for these data that provide us with information, is having the sufficient tact and the necessary prudence not to commit acts contrary to the law, as would be the case of the violation of the privacy of the persons, the human dignity between others, no less serious.

It is in this way that we analyze from our own legislation how one way or another has been concerned about the issue, since it has legislated on it and some reforms have been made, as we can detect in our criminal code with the reform of the code to be inserted in article 269A and SS, called computer crimes and everything that has to do with them, but by way of criticism we see that the legislator fell short whenever he only cared for some crimes against the economic wealth, without taking into account that in this new form of crime are also affected other criminal types no less important and that are also protected, threats, extortion, blackmail, insult, falsehood, fraud. In each of these criminal types it is observed that clearly meets the

requirements mentioned above, fit perfectly in the governing verbs, have an active and a passive subject, there is an injury, circumstances of manner, time and place. To these criminal types taking into account the means used to commit the act, it is necessary to speak of a forensic analysis, for which it is required that we are any person, but a person duly trained and with the necessary training to perform this type of investigations, in the forensic analysis, the types of attacks perpetuated are detected, which tools were used and how would its possible solution be in terms of viruses, or created cheats, not only for prevention, but also to be able to detect possible responsible and finally be able to obtain a conviction for acts contrary to the law committed.

## Key Words:

Evidence - Computer crimes - Colombian criminal process

## 1. PLANTEAMIENTO PRELIMINAR

Para abordar el tema se hace necesario tener claro algunos de los términos que utilizaremos a lo largo del desarrollo temático, en este aparte are una pequeña reseña, en el cual doy a conocer la temática, los objetivos, el método utilizado y el planteamiento del problema, que fue el factor fundamental para el desarrollo del tema.

En el planteamiento de la problemática propuesta, es necesario definir que es una evidencia digital (Cano Martínez, 2009), la cual no es otra cosa que aquella información o rastro hallado en un medio informático de la tecnología y la comunicación, el cual puede ser utilizado dentro de un proceso legal como medio probatorio, siendo esta la materia prima, para demostrar la existencia o inexistencia de un hecho, el cual puede estar inmerso en alguna de sus categorías (Bogota Prieto & Moreno Peña, s.f.) Como:

- Registros almacenados (correos electrónicos)

- Registros generados por el mismo equipo (eventos)
- Registros parcialmente generados y almacenados (visitar parciales)

El término “Evidencia Digital” abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal.

Por ejemplo, el elemento material probatorio seria el documento.

Pero ahora, ese medio probatorio que llamamos materia prima del proceso, tiene una exigencia desde la misma norma, que han tratado de regular de una forma muy amplia, escueta y sin profundizar en la misma, como es el caso de la ley 527/99, la cual hace alusión a la conservación y tratamiento que se le debe dar a algunos aspectos en cuenta al comercio electrónico (Republica, Congreso de la, 1999), pero su principal enfoque lo hace desde la óptica jurídica del derecho civil y comercial, pero poco hace frente a otra áreas del derecho, como es el penal y es aquí donde debemos poner más atención, ya que están en juego los derechos fundamentales, como el derecho a la libertad, a la intimidad, la dignidad humana, entre otros. En este caso se enfatiza más en las bases de datos que en la evidencia digital.

Se debe tener en cuenta que hablar de evidencia digital, nos refiera a un aspecto muy importante que es la tecnología, cuya principal característica es que es demasiado cambiante, evolutiva y dinámica, lo que conlleva a que en esta materia debamos hacer un mayor esfuerzo y a ser muy cuidadosos, pues en materia probatoria, se caracteriza por ser volátil, anónima, duplicable, alterable, modificable y eliminable (Cano Martínez, 2009).

Si hacemos un pequeño símil de lo analizado hasta el momento, podemos decir que para el momento el elemento material probatorio es el documento, pero la evidencia digital a la que nos referimos son los rastros cambiantes como las direcciones IP, las cuales son cambiantes y dinámicas (las conexiones o direcciones de conexión) o en otro caso, las memorias RAM que son volátil (memoria de inicio y de procesamiento de una CPU).

Características estas, que a su vez se convierte en un verdadero desafío en quienes sopesan dicha carga, pues finalmente pueden afectar el desarrollo del proceso en su parte probatoria, esto si no se hace un adecuado manejo a esos rastros o evidencias halladas, las cuales deben ser recolectadas en debida forma por el personal idóneo, con herramientas adecuadas, cumpliendo unos protocolos estandarizados y, sobre todo, ajustado a las normas legales e internacionales.

Para que, de esta forma, pueda estar garantizada la integridad, el análisis detallado, recolección rápida y oportuna, al igual que la preservación y la idoneidad en la presentación con su resultado.

Dado que no existen investigaciones iguales, no es posible definir un procedimiento único para adelantar un análisis en Informática forense. Pero, si sería posible definir una aproximación metodológica que permita el manejo adecuado de la evidencia digital, que minimice la posibilidad de cometer errores en su manejo y que, en alguna medida, garantice la admisibilidad de la misma en situaciones jurídicas.

La evidencia digital debe ser cuidadosamente recopilada y manejada, para posteriormente cumplir con los requisitos de admisibilidad de un medio probatorio. Independiente de una legislación particular, es esencial garantizar la confiabilidad e integridad de la evidencia.

Debe tenerse en cuenta que cada delito en particular mientras tenga intervención de un medio tecnológico informático o de comunicación en la ruta del esclarecimiento de los hechos, se pretende un acervo probatorio, el cual va a estar delimitado por la eficiencia física y en caso concreto, evidencia digital y que para este, se debe tener un tacto especial gracias a sus características; además de que es muy importante la forma para su recolección, demostrar la mismidad, continuidad, conservación, análisis y presentación.

# 2. **DELIMITACIÓN DEL EJERCICIO DE INVESTIGACIÓN**

## 2.1. **Metodología**

Para alcanzar el objetivo propuesto en esta investigación, pretendí realizar dicha investigación utilizando una metodología, que considero la más apropiada para demostrar las necesidades y falencias que se encuentran dentro de nuestro ordenamiento jurídico y por parte de los operadores jurídicos.

La metodología a utilizar y que ofrezco para el desarrollo de esta, es la deductiva por inducción incompleta (CARVAJAL, 2013), la cual no es otra que "Es el razonamiento que, partiendo de casos particulares, se eleva a conocimientos generales. Este método permite la formación de hipótesis, investigación de leyes científicas, y las demostraciones."; bajo este postulado, se pretende mantener una posición analítica frente a los postulados de aquellos que han abordado temas similares y una valoración crítica frente a los operadores judiciales.

Es así pues que desde la misma casuística y gracias a mi labor y al conocimiento que he podido adquirir dentro de la Unidad de Delitos Informáticos de la Fiscalía General de la Nación, pretendo demostrar la problemática existente frente al planteamiento problemático y la necesidad de poder ofrecer una solución al mismo; es por esto que dicha metodología es abordada desde el análisis de casos concretos, abonado a nuestras experiencias como servidor judicial, situación que nos puede llevar a ofrecer unas conclusiones probables; gracias a la veracidad de la información desde una experiencia, no solo vivida, sino aplicada desde el campo laboral, llevándonos así a aportar unas conclusiones al campo experimental.

Es entonces que el método a seguir para el desarrollo de este trabajo es el método de inducción incompleta por la simple conclusión probable, basándonos desde el desarrollo y aplicación de la caustica, con la que pretendo demostrar que el planteamiento es lógico, razonable y probable, además de la necesariedad del desarrollo del mismo o su aplicabilidad, ante los operadores judiciales, el cual hace parte de la conclusión.

## 2.2. **Objetivos A Desarrollar Para Alcanzar La Propuesta Temática**

Es establecer y demostrar al interior del proceso penal colombiano, las dificultades que se presentan en el manejo de la evidencia digital, no solo para los operadores judiciales, sino para todas y cada una de las personas que se ven afectadas por estos delitos llamados "de nueva generación". Una vez conocido los conceptos y temimos más comunes dentro de la temática a tratar, analizamos la normatividad del proceso penal colombiano, en relación a la evidencia digital, como se aplica a lo

largo de cada proceso interpuesto a modo de experiencia en cada despacho judicial, el tratamiento del mismo y como es el tratamiento en la actualidad. Lo que nos lleva a determinar los efectos procesales que tienen el desconocimiento o la falta de un adecuado tratamiento de la evidencia digital, además de qué forma se puede ver afectado no solo el proceso, sino cada uno de los intervinientes.

2.3. **Planteamiento De La Problemática Objeto De Investigación**.

Para mí la pregunta principal, y que me llevo a desarrollar este planteamiento temático es: ¿Qué tipo de dificultades podemos encontrar en el manejo de la evidencia digital en el Proceso Penal Colombiano?, ya que desde mi experiencia personal y laborar, es nuestra mayor dificultar para el manejo y tratamiento de estos delitos llamados “de nueva generación”, pues no son ni nuevos, ni son de esta generación, como lo veremos a lo largo del desarrollo temático, es solo la evolución y adaptación de todos y cada uno de los delitos a unos medios diferentes.

2.4. **Instrumentos Empleados Que Coadyuvaron En El Desarrollo Del Tema**.

Si bien es cierto, que gracias a mi labor personal, profesional y laboral, como servidor de la fiscalía general de la nación, al interior de la unidad de delitos informáticos, pude hacer una recopilación no solo de conocimiento si no de material académico y que fui plasmando en una base de datos para luego ir depositando o extrayendo la información a las unas plantillas o fichas las cuales me sirvieron de mucha ayuda para demostrar la certeza y las dificultades que se tienen a la fecha, no solo al interior de las instancias judiciales, sino, de todos los operadores judiciales, además de la sociedad en general, que se ven afectadas y tan vulnerables día, a día, esto gracias a la falta de conocimiento y capacitación e incluso a la de información.

**FICHA DE ANALISIS DE CASOS EN DELITOS INFORMATICOS No.**

| **Datos generales** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Radicado | | Fecha Denuncia | | Fecha Hechos | | Fecha Asignación | |
| | | | | | | | |
| Denunciante - Victima | | P. Natural | | Afectación | P. Natural | | |
| | | P. Jurídica | | | S. Financ. | | |
| Sexo | Edad | Residencia | | Lugar Hechos | | | |
| | | | | | | | |
| **Etapas del Proceso** | | | | | | | |
| **Indagación** | | | | | | | |
| Narración Fáctica: | | | | | | | |
| Modus Operandi | | Tipo Penal | | | | | |
| | | | | | | | |
| Elementos Obtenidos con Vocación Probatoria | | | | | | | |
| Con la Denuncia | | Después de la Denuncia | | | | | |
| | | | | | | | |
| ¿Qué otras conductas penales concursan?: | | | | | | | |
| Indiciado | | | | Sexo | Edad | | |
| | | | | | | | |
| Actos investigación | Si | | No | | Cuales? | | |
| | | | | | | | |
| Archivado | | Motivo de Archivo | | | | | |
| Si | No | Sin Sujeto Activo | | Sujeto activo sin identificar | | Sin EMP* | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| Captura en flagrancia | | Captura con orden | | |
| Legalización captura | Si | | Medida aseguramiento | Si | |
| | No | | | No | |
| Motivo Medida | | | | | |
| **Investigación** | | | | | |
| Imputado | | | Escrito acusación | Si | |
| | | | | No | |
| Terminación anticipada | Si | | Aceptación cargos | | |
| | No | | preacuerdos | | |
| **Juicio** | | | | | |
| Acusado | | | Presente | Contumaz | |
| | | | | | |
| Pruebas | | | | | |
| Testimonial | Si | | No | | ¿Quienes? | |
| | | | | | | |
| Documental | Si | | No | | ¿Cuales? | |
| | | | | | | |
| Pericial | Si | | No | | ¿Quienes? | |
| | | | | | | |
| Sentencia | Si | | Absolutoria | | Tiempo | |
| | No | | Condenatoria | | | |
| Sentido del fallo: | | | | | | |

*EMP (Elemento Materiales Probatorios)

*Fuente: autoría propia.

Capítulo 1

# 1. APROXIMACIÓN A LOS REFERENTES CONCEPTUALES CON RELACION A LOS DELITOS INFORMATICOS

He considerado que para el desarrollo y una buena comprensión de este trabajo se hace necesario tener una serie de conceptos bastante claros y delimitados ya que son términos, que a lo largo del mismo se van a enunciar y en algunos se casos se van a repetir, pues son términos estrictamente necesarios respecto al tema a tratar, razón por la cual se expone el siguiente glosario de términos y definiciones.

## 1.1. Glosario

DATO: No es otra cosa que una información aislada que por sí solo tal vez no signifique nada, ya que hablar de datos es decir una serie de elementos tales como símbolos, códigos, letras números, etc. (Sanchez, 2016)

INFORMACION: Es la recopilación de todos los datos que de una forma sistemática dan referencia de algo en este caso ya no podemos decir que son datos aislados sin, que son la sumatoria de cada uno de ellos para obtener un resultado. (Sanchez, 2016)

DATOS INFORMATICOS: Es la sumatoria de unos datos convertidos en información expresados a través de un medio tecnológico.

BIEN JURIDICO: Desde la órbita que pretendemos abordar, este concepto hace referencia no solo al bien sino al medio utilizado para su consumación o afectación. (Stalin, 2013)

DELITO INFRMATICO: Estamos enfrentados a unas conductas que se cometen utilizando esos medios informáticos existentes y que pueden ser computadores

portátiles, teléfonos inteligentes, computadores de oficina, todos ellos sí, con una conexión obligatoria a la red de datos conocida como Internet. Medios estos que, aunados a los conocimientos especiales de los autores, son utilizados para apropiarse de los activos de sus víctimas. (Stalin, 2013)

SEGURIDAD INFORMATICA: Puede ser definida como aquellos programas eficaces diseñados e implementados en los servidores de las empresas o entidades bancarias, que busca limitar el ingreso o acceso a un sistema. (Stalin, 2013)

SISTEMA INFORMATICO: Conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales. (Stalin, 2013) “designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos. (Republica, Congreso de la, 2018)

SISTEMA DE AUTENTICACION: Aquel proceso de verificación de la identidad digital de quien remite una comunicación como una petición para conectarse. El usuario remitente puede ser una persona, un computador o un programa elaborado bajo un lenguaje especial y enviado desde el computador o dispositivo de comunicación. (Stalin, 2013)

SISTEMA DE AUTORIZACION: Es un proceso digital por el cual una red de datos autoriza a un usuario previamente identificado a acceder a determinados recursos de la misma. (Stalin, 2013)

ANALISIS FORENCE: Es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad. (Rifa Pous Helena, 2009)

“Surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades.
Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales”. (Pino A. d., 2009)

INCIDENTES DE SEGURIDAD: Es cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, extorsión, posesión de pornografía infantil, envío de correos electrónicos ofensivos, fuga de información confidencial dentro de la organización. (Rifa Pous Helena, 2009)
“Cualquier evento anómalo que pudiese afectar la Seguridad de la Información, que comprende la pérdida de la disponibilidad, integridad o confidencialidad de la misma”. (Torres Moncada Martha Liliana, 2016)

PROGRAMAS MALICIOSOS: Es una serie de archivos ejecutables que desempeñan acciones dañinas al reproducirse o activarse, dentro de un ordenador sin consentimiento previo. (Rifa Pous Helena, 2009)

HASH: Es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito, generalmente menor (un subconjunto de los números naturales, por ejemplo). Una propiedad fundamental del *hashing* es la que dicta que, si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son. (Rifa Pous Helena, 2009)

DELITO CIBERNETICO EN SENTIDO ESTRICTO: Todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y de los datos procesados por ellos. (Rincon Rios Jarvey, 2011)

DELITO CIBERNETICO EN SENTIDO LATO: Todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos (Rincon Rios Jarvey, 2011)

EVIDENCIA DIGITAL: Aquella información o rastro hallado en un medio informático de la tecnología y la comunicación el cual puede ser utilizado dentro de un proceso legal como medio probatorio, siendo esta la materia prima para demostrar la existencia o inexistencia de un hecho. (Cano Martinez, 2009)
"Es la información contenida dentro del Hardware" (Pino A. d., 2009)

EVIDENCIA ELECTRONICA: Se obtiene del elemento material de un sistema informático o Hardware. (Pino A. d., 2009)

HARDWARE: Son los componentes físicos de un equipo de cómputo o telemático.

SOFTWARE: Conjunto de programas y rutinas que permiten el desarrollo operativo de ciertos equipos tecnológicos.

DELINCUENTES INFORMATICOS: Son una nueva generación de criminales qué, Utilizando sus técnicas naturales en el mundo físico renuevan y afianzan las mismas para producir acciones punibles de mayor Impacto utilizando un medio tecnológico. (Cano Martinez, 2009)

TEST DE DAUBERT: Es un conjunto de reglas extraídas de la Corte Suprema de Justicia estadounidense, en el caso de Daubert versus Merrell Dow Pharmaceutics, inc., 509 U.S. 579 de 1993, donde se clarifican los estándares que los jueces federales deben tener en cuenta a la hora de admitir o no la evidencia entregada por los expertos del caso, si bien no es un estándar universalmente sugerido, si en muchas iniciativas normativa sobre el tema a nivel internacional. (Cano Martinez, 2009)

TECNICAS FORENSES: Protocolos de estandarización y ajustes que fortalecen las herramientas y técnicas utilizadas en favor de la administración de justicia. (Cano Martinez, 2009)

CIBERTERRORISMO: Es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas. (Cano Martinez, 2009)

CIBERSEGURIDAD: Consiste en proteger contra el acceso no autorizado y la manipulación y destrucción de recursos y activos esenciales de la información y la materialización de la delincuencia, en medios electrónicos. Desafío de un atacante anónimo. (Cano Martinez, 2009)

ARCHIVOS CIFRADOS: Una de las técnicas más utilizadas por los atacantes, como parte de sus actividades delictivas, es cifrar la información (Casey y Stllatos 2008) reciente en el dispositivo de almacenamiento con algoritmos de cifra conocidos, utilizando llaves de cifrado generalmente largas (512,1024, 2048 bits), que limiten un ataque de fuerza bruta que intente descifrar lo se encuentra allí. (Cano Martinez, 2009)

MEMORIA VOLATIL: Es información almacenada dentro de un procesador la cual se conserva solo durante el tiempo que este procese la información también llamada información volátil. Altamente sensible. (Cano Martinez, 2009)

EVIDENCIA VOLATIL: Es aquella que se encuentra alojada temporalmente en la memoria RAM o en el CACHE, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado. (Pino A. d., 2009)

BACK UP: Proporciona los parámetros básicos para la recuperación dela información necesaria. (Pino A. d., 2009)

PRINCIPIO DE TRANSFERNCIA: ya que el trabajo criminal de un delincuente exige su presencia física y por lo tanto deja rastro; el trabajo criminal es digital, no existe presencia física del sujeto sino transmisiones de datos, emisiones electromagnéticas, impulsos eléctricos, entre otros. (Maria, 2013)

FORENSE INFORMÁTICO: Disciplina que se encarga de la investigación sobre medios informáticos se le conoce con variadas denominaciones, siendo las más frecuentes investigaciones digitales, forense digital, computación forense, informática forense, entre otras. (Maria, 2013)

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. (Republica C. d., 2012)

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de Tratamiento. (Republica C. d., 2012)

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Republica C. d., 2012)

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Republica C. d., 2012)

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Republica C. d., 2012)

TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento. (Republica C. d., 2012)

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Republica C. d., 2012)

DATOS SENSIBLES: Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Republica C. d., 2012)

FIRMA DIGITAL: es la que es impuesta por parte del usuario autorizado en los documentos que reposan en el SAE tendrá la misma fuerza y efectos que el uso de una firma autógrafa. (Republica C. G., 2014)
“Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador.” (Republica, Congreso de la, 1999)

TOKEN: Es el dispositivo que contiene la información correspondiente al certificado de firma necesario para acceder a la plataforma. (Republica C. G., 2014)

MENSAJE DE DATOS: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax. (Republica, Congreso de la, 1999)

COMERCIO ELECTRÓNICO: Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. (Republica, Congreso de la, 1999)

ENTIDAD DE CERTIFICACIÓN: Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos. (Republica, Congreso de la, 1999)

INTERCAMBIO ELECTRÓNICO DE DATOS (EDI): La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto. (Republica, Congreso de la, 1999)

SISTEMA DE INFORMACIÓN: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. (Republica, Congreso de la, 1999)

PRESTADOR DE SERVICIO: Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, trate almacene datos informáticos para ese servicio de comunicación o sus usuarios. (Republica, Congreso de la, 2018)

DATOS DE TRÁFICO: designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último. (Republica, Congreso de la, 2018)

DELITO INFORMATICO: Toda conducta punible, señalada por el legislador; haciendo uso indebido de la información y de cualquier medio informático empleado para su manejo o de la tecnología electrónica o computarizada, como método, medio o fin, que ponga en riesgo el bien jurídico de la información y de los datos u otros bienes jurídicos. (Cortes Botero , Ballen Rojas, & Duque Montes, 2015).

## 2. Fundamento Conceptual Para El Referente Probatorio

Para poder adentrarnos en el tema que nos atañe, debemos tener muy claro cuál es fundamento, o pilar conceptual que nos sirve de referente, dentro de un acervo probatorio y para esto debemos dar cuenta de que un dato, el cual no es otra cosa que una información aislada que ello por si solo tal vez no signifique nada, ya que hablar de datos es decir una serie de elementos tales como símbolos, códigos, letras números, etc. pero si la unimos unos con otros, estos datos se convierten en información.

Decimos que los datos son una construcción del ser humano, pero que su mayor definición es que deben ser aislados el uno del otro.

Es por esta razón que no podemos decir que los datos es información, ya que la información es la recopilación de todos los datos que de una forma sistemática dan referencia de algo en este caso ya no podemos decir que son datos aislados sin, que son la sumatoria de cada uno de ellos para obtener un resultado llamado información, ejemplo: decir que en la escena de un crimen encontramos un cuerpo sin vida, un arma de fuego, un computador, el cual esta encendido, en el cual se encuentra una nota al parecer dejada por la persona que está en el piso, donde hace alusión a una traición, pero además observamos en el pc, imágenes intimas de una pareja en la cual no está el sujeto que esta tirado en el piso.

Si observamos cada hecho de forma aislada esta solo son datos, pero si los analizamos de forma conjunta nos está dando una información valiosa para el esclarecimiento del hecho o herramientas para la investigación (Sanchez, 2016).

Por otro lado, es importante observar la postura jurídica desde la carta de navegación jurídica. Nuestra constitución política, la cual nos hace referencia a una serie de derechos y deberes dentro de los cuales nos refiere como un derecho muy importante es el derecho a la intimidad y así muchos más como la libertada de

expresión, donde todos y cada uno de ellos, si los relacionamos unos con otros en el tema de la información, nos van a regular el manejo y tratamiento que del mismo. Es así como llegamos a comprender el concepto de bien jurídico en el delito informático, pues la información que se tiene es personalísima y nuestros legisladores, aunque se han quedado un poco cortos en el desarrollo profundo de la misma, si han tratado de regular el manejo, desarrollo y protección de la información de los ciudadanos, en las diferentes fuentes jaricas, esto se vivencia desde la ley ya mencionada de “la protección de datos” (Republica C. d., 2012).

Pero porque esto es importante, y es precisamente porque debemos tener en cuenta que la información no solo puede ser tomada como un objeto sino que también debe vista como un medio de delito, toda vez que así como lo mencionaba antes que los datos sumados unos con otros nos pueden llevar a una información relevante, la cual puede ser convertida en un objeto, como son el caso de las fotos intimas, la carta al parecer dejada por la víctima, así sucesivamente, pero estos a su vez son los medios que me pueden ayudar a demostrar no solo la existencia del hecho sino que también me ayudan a esclarecimiento de los hechos e identificar el posible responsable.

Como un aporte muy importante del estado para el manejo y sobre todo la regulación que se hace tan necesaria, ya que como lo mencionamos anteriormente los datos informáticos y la información que estos suministran, no pueden estar al libre albedrío y se hace necesario que tenga una regulación y alguien que responda o este al pendiente de la misma no solo de la regulación, sino del manejo, ya que este debe ser regulado y controlado, pues de lo contrario esto se puede convertir en lo que hoy por hoy conocemos delitos informáticos (Cano Martinez, 2009).

## 3. Aportes De Nuestra Legislación, Para Mitigar La Problemática Latente.

Gracias a la exigencia y preocupación de los legisladores, se han hecho una clasificación a mi parecer muy somera de algunos delitos informáticos. Digo que

algunos puesto que a mi parecer se están quedando muy cortos ya que como evoluciona la tecnología a pasos agigantados la norma debe evolucionar en la misma velocidad ya que se debe estar muy atento a ese crecimiento y desarrollo para así tratar de prever maniobras fraudulentas, pues esa es la tendencia a nivel mundial ya los delitos no se cometen de forma “directa”, sino que el medio para cometer el fin es la tecnología, pero es de abonarle al legislador que se preocupó por hacer una clasificación (Rincón Ríos & Naranjo Duque, 2011) de algunos delitos teniendo en cuenta el objeto, sujeto, medio y fin.

Pero para poder realizar dicha clasificación se hace no menos necesario identificar y diferenciar el significado de que es un bien jurídico (Grisales Pérez, 2013) y cuál es el bien que finalmente se está afectando en estos tipos penales, nos debemos remitir al medio que se utiliza para la consumación o afectación del mismo, como es el caso de la tecnología y los medios de comunicación. Por otra parte esto nos permite evidenciar que los actores en este tipo de casos o eventos no son cualquier persona, sino que son personas con mucho conocimiento y personas que un buen patrimonio económico, pues si bien nuestro ordenamiento jurídico por ahora solo está tratando bajo este entendido los delitos contra el patrimonio económico a través de los medios tecnológicos, pero podemos darnos cuenta que no solo estos son los que se ven afectados día a día, razón por la cual considero que nuestros legisladores deben evolucionar y comenzar a legislar enfocando otro tipos penales para la protección de más bienes jurídicamente protegidos, pues la tecnología es el medio que evoluciona al mismo ritmo del conocimiento, además de la regulación respecto al acceso de la misma, razones que por eso hoy en día vemos como los tipos penales concurren unos con otros y se nos da la disyuntiva, bajo cual tipo penal, es más conveniente procesar determinadas actuaciones, como es el caso del hurto calificado y agravado que a su vez puede ser visto como un hurto por medios informático el cual también puede ser agravado.

### 4. La Necesidad De Un Análisis Forense.

Pero para poder abordar este tema se hace necesario para comprender que es un análisis forense, (Rifà Pous, Sierra Ruiz, & Rivas López, 2009) y por qué la necesidad del mismo; aunque este tema será abordado en varios apartes, a que tipos de ataques estamos expuestos al momento de utilizar los ordenadores, la tecnología y las comunicaciones, pero adicional a esto también vemos que existen algunas formas y herramientas para evitar caer en las trampas de aquellas personas que migraron su forma de delinquir a este medio que aparente mente para ellos es un poco más seguro y que obviamente tiene menos riesgos físicos para ellos.

Encontraremos algunas ayudas para enfrentar este flagelo, además como una de las principales herramientas es desconfiar y poner en conocimiento de las autoridades lo que está sucediendo, pero esto también debe ser acompañado de una serie de cuidados al manipular el medio de ataque para evitar se pierda la prueba.

## 2. EVOLUCIÓN DE LOS DELITOS COMUNES A DELITOS DE LA NUEVA GENERACIÓN.

Es así como se conocemos de forma común, los delitos comunes, pero a lo largo del estudio, nos podemos dar cuenta que no solo son los delitos contra el patrimonio económico los que siempre están afectados bajo esta nueva figura del derecho penal como bien se observa a lo largo del artículo 269A bis (Rincón Ríos & Naranjo Duque, 2011), pero poco hace referencia a estos nuevos tipos penales a los que se hace referencia, pues bien es tratado los delitos contra la libertad sexual el constreñimiento, la calumnia etc. Los cuales también son afectados o atacados a través de los medios tecnológicos y de las comunicaciones, su importancia está basada en la forma que se trata cada tipo penal, que sujetos y de que formas los integran, cuales son los verbos rectores y como a través de esta nueva figura se ven alterados, así de esta forma podemos darnos cuenta de las falencias que se tienen en el acervo probatorio (Maria, 2013).

Ya que en el mismo se da un gran desarrollo en el campo de la investigación forense y de la recolección de las pruebas.

### 2.1. Dificultades Comunes En El Manejo Del Tema

Si bien es cierto en el campo de la investigación forense se hace necesario ciertos temas gracias a las dificultades existentes, entre ellas nos indican la necesidad de capacitar y de tener personas expertas en el área de la investigación forense, propiamente en el área de la informática, sin ser necesarios ingenieros, pero lo más importante es la capacitación constante y la actualización permanente ya que este es un medio que evoluciona constantemente y se actualiza de forma constante y permanente.

Es muy importante tener en cuenta las cantidades de software libre como otros licenciados que nos ayudan de forma constante y poder estar a la vanguardia con los ataques cibernéticos producido por unas personas que de igual forma aprovechan la facilidad del sistema.

Referirnos de los tipos de atacantes es como nos hace una breve mención a que tipos de atacantes nos enfrentamos, pues bien no son ni los más expertos, pero tampoco son los más ingenuos, puesto que la tecnología es un medio en el cual no cualquier persona puede acceder y más con el fin de cometer actos delictivos es por esto que son personas que tiene la firme intención y por esta razón ellos se capacitan buscan y escudriñan los vacíos o abismos en el ciberespacio (lo que llaman puertas traseras), para poder ingresar y cometer los actos delictivos.

Es por esto que me parece muy importante la propuesta que muchos autores plantean como las escuelas o centros de capacitación para investigadores (Cano Martínez, 2009) que pretendan hacer este de investigaciones y quienes deben ser los tipos de capacitadores, además de los programas donde se debe enfatizar, ya que debemos recordar que esta es la modalidad de delincuencia y que todas las grandes empresas criminales están accesando, ya que es muy difícil dejar rastros y más difícil aun que los encuentren.

Por qué se insiste en la capacitación de los investigadores, dentro de muchas necesidades algunas ya mencionadas también es de tener en cuenta la necesidad de conservar y proteger la evidencia pero no solo esto es también lo más importante, su recolección, vale decir que esto no puede ser de cualquier forma ya que los sistemas de información manejan una memorias, las cuales son muy volátil (Pino A. d., 2009), algunas más que otras, es por esto que se debe tener sumo cuidado en la extracción de la información, además, es importante saber o conocer que partes de un equipo es la que contiene la información y que se hace necesario de ella, para evitar perjuicios y desgaste innecesario.

Por otro lado, no debemos ser ajenos y pensar que este tipo de situaciones solo se dan en las películas, No. Esto se da en la vida real y no es otra cosa que el Ciberterrorismo, delitos que son impulsados por grandes potencias o delincuencia organizada que opera a nivel mundial, y nosotros no podemos ser ajenos a esta problemática e irnos actualizando además de capacitando para enfrentar esta problemática, no debemos seguir pensando como un país tercermundista y creer que eso no nos va a pasar a nosotros o seguir con el cuento que eso solo se ve en las películas.

## 3. LA ADAPTACIÓN DE LAS CIENCIAS A LA EVOLUCIÓN CRIMINAL Y LA EVIDENCIA DIGITAL.

Para la ciencia forense, frente a la investigación criminal, se hace necesario referirnos a un principio esencial que es el de la trasferencia (Maria, 2013), el cual consiste en que se hace necesaria la presencia del sujeto activo, al momento de cometer un hecho, frente a los ciberdelitos, se genera una gran duda si este principio se aplica o no, pero la respuesta está dada en la necesidad de la presencia del mismo sujeto activo, ya no de forma física, sino de la misma forma virtual, pues lo que se pretende es encontrar los rastros dejados él, ya sea de forma física o virtual, por eso decimos que el principio de trasferencia se aplica en ambos casos pues este solo refiere a los rastros dejados por el sujeto activo de la conducta punible.

Nuestra legislación regula ciertos medios probatorios, con los cuales se pretende estar un paso delante frente a la evolución social (Republica, Congreso de la, 1999), condicionados a la no violación de los derechos humanos, en el caso concreto como lo manifiesta la norma “evidencia física” y que para nuestro caso la expresión más adecuada es de evidencia digital; se hace necesario la combinación de tres medios de prueba como son la prueba documental, la prueba pericial y la prueba testimonial En relación a la prueba pericial, regulado en nuestro ordenamiento exige, que sea una persona competente, que pueda acreditar no solo su experiencia, sino que además la certifique, en relación al tema, ya que la falta de técnica no solo puede generar la exclusión de la prueba sino también la nulidad.

Frente a la prueba testimonial, se hace necesaria, toda vez que es de esta forma que a través del principio de contradicción el perito podrá dar a conocer las herramientas utilizadas y los protocolos aplicados para el caso en concreto, además de darle a conocer de una forma adecuada al juez, el contenido de su informe.
La prueba documental no es otra que el soporte de todo lo actuado o analizado por el experto, además de todos los hallazgos o rastros dejados.

Con el devenir de los tiempos, se ha dado una gigantesca evolución en el medio de la delincuencia lo que antes era presencial ya no se hace necesario, y para esto también evoluciona el medio probatorio así como la forma de preserva y conservas los EMP y EF, para nuestro caso la evidencia digital, en la cadena de custodia, para poder presentarla en juicio y esta tenga su valoración necesaria de acuerdo con la trazabilidad, confidencialidad, integridad, disponibilidad, privacidad, autenticidad, usabilidad, confiabilidad.

Es por esta razón que vemos que muchas partes en el mundo se han preocupado por este tema y están crenado una serie de protocolos al igual que herramientas, para la conservación y tratamiento de este tipo de evidencia la cual no es tan común y que requiere un tratamiento muy especial. De igual forma se hace referencia a

una serie de equipos de trabajo, la cual debe tener una serie de limitaciones o en su mejor entendido una serie de roles, cada uno con unas habilidades específicas. Vale decir que este tipo de roles y de actividades en nuestro país es desarrollada por entidades públicas y privadas encargadas de hacer el tratamiento a las bases de datos de una forma casi que confidencial, clasificada y reservada, desconociendo incluso los estándares y protocolos internacionales, adaptándolo a una conveniencia institucional.

También es cierto que existen laboratorios en todo el mundo dispuestos a prestar sus servicios y a capacitar en temas referentes, pero por sus altos costos y poco interés por parte de las entidades, sumado a esto la falta de convicción en relación al tema, no se están aprovechando o mejor incentivando de manera adecuada. Se hace necesario, en un futuro inmediato, la normalización y estandarización de los laboratorios con el objetivo de unificar los criterios; promovida bajo los lineamientos de la Convención de Budapest.

A través de una serie de métodos de calificación (Maria, 2013), se pudo hacer un muestreo del grado de conocimiento y de aplicación en relación al tema en cuestión, entre una un grupo de personas pertenecientes a una comunidad específica, destacando así su grado de conocimiento, de aceptación y la aplicabilidad dentro de la misma. De igual forma se realiza una forma de hacer un rastreo del conocimiento y bajo el entendido de la medición cuantitativa, la cual evidencia con una serie de valores porcentuales el cual no es muy distante de la medición cualitativa.

Una forma, que también nos permite evidenciar lo que hemos venido referenciando, es como el tribunal supremo (Alfonso, 2015), en España, confirma que todo medio de prueba es una comunicación bidireccional, e incluso los me dios de mensajería instantánea, pero de igual forme es consiente que este puede ser manipulado o alterado, razón por la cual traslada la carga probatoria a la parte que la presenta, sin dejar de lado la necesidad de ser acompañada por otro medio probatorio para poder demostrar su autenticidad como todo medio probatorio.

El alto tribunal supremo viene reconociendo la extinción del papel, en sus procesos, toda vez que en los procesos penales se incorpora como una realidad fática, el papel como soporte y la escritura como unidad de significación, la cual, final mente llevaría a la convicción del juzgador, pero no se puede perder el rumbo de lo que se pretende ya que intención, es la evolución del sistema donde el papel pierda su mayor importancia y se pueda transformar en otra forma de evidenciar la prueba que se pretende y de igual forma llevar al mismo convencimiento del juzgador.

Es de esta forma que aparece la necesidad de aplicar la evidencia electrónica como un medio probatorio, desde correos electrónicos, pantallazos, sms, el log transaccional, las direcciones IPs, e incluso los mensajes enviados a través del WhatsApp, los cuales se convierten en evidencia digital, la cual está llamada a ser más operante en nuestro sistema penal, razón por la cual se insiste en la necesidad dentro de la actividad probatoria la necesidad de incluir la evidencia digital como medio probatorio, para demostrar la existencia de un hecho, donde la carga probatoria esta en cabeza de quien la ofrezca sin perjuicio de aportar otras pruebas que ayuden a su sustento para demostrar la autenticidad de la misma.

Como se ha manifestado en distintas ocasiones la era de la globalización nos exige un cambio y una transformación en nuestras formas de operar al igual que nuestro sistema penal, pero para ello se hace necesario la capacitación, pues vemos que la tecnología o los medio telemáticos e informáticos avanzan cada día al igual que la sociedad se transforma y se vincula a la misma, pues de esto damos cuenta cuando vemos las transacciones comerciales que cada día se ven más, tema al que aremos referencia un poco más adelante cuando de forma somera, al tocar la ley 5277 de 1999 (Republica, Congreso de la, 1999).

Continuando con el análisis forense y la evidencia digital, la gran mayoría de autores convergen en la definición de AFD (Torres Moncada Martha Liliana, 2016), el cual no es otro que el estudio sistemático, extensivo y profundo, de un equipo, medio

informático o telemático, con el propósito de extraer la información que allí repose, aplicando una serie de protocolos, esto con el mismo fin de encontrar unos patrones, huellas o rastros dejados en el sistema por el autor o autores y quienes finalmente son responsables del hecho investigado.

Podemos decir que evidencia digital son aquellas huellas o rastros dejados al interior de un medio magnético, trasmitida, procesada y trasmitida electrónicamente, información que debe ser plasmada en un informe pericial, para ser presentada ante el juez con el propósito de darle claridad al proceso que se adelanta.

Es de anotar que este análisis forense cuenta con unas ventajas, pues cumple con una función preventiva inicialmente, además nos da a conocer las falencias del sistema, al momento de hacer un rastreo, se puede detectar, no solo el daño generado, recopila la evidencia electrónica, detecta el origen del ataque, al igual que las alteraciones realizadas, sin dejar de lado las nuevas tendencias de la violación a equipos móviles, esto gracias a su similitud o semejanza con los equipos de cómputo.

De igual forma tiene unas desventajas, como, la necesidad de contar las herramientas adecuadas para poder hacer dicho análisis tales como buenos equipos de cómputo, los cuales deben ser bien robustos, con muy buena capacidad de procesar la información, abonado a esto se hace necesario contar con unos buenos programas (software), en este mismo orden de ideas se debe contar con un personal altamente capacitado en el tema. Ya que dichos operadores se convierten en peritos expertos, los cuales deben aplicar unos protocolos para el análisis forense, paso a paso, en la identificación, recolección, adquisición y preservación. Pero lo más importante es la presentación del informe, el cual dentro de su información suministre algunas características como autenticidad, confiabilidad y suficiencia.

Algunos autores refieren a una clasificación de la evidencia digital:

- Registros no generados en el computador, pero guardado en este.
- Registros generados en el computador
- Registros generados en el computador y archivados en el mismo.

## 3.1. La Globalización Criminal Y La Evidencia Digital.

Como flagelo mundial y cuando nos adentramos en este tema, el cual nos da a conocer una problemática para la aceptación de la evidencia digital como tal. Como es la carencia de normatividad en materia sustancial y procesal, la falta de técnica y la inaplicación de los protocolos internacionales en esta materia, sin dejar de lado lo ya antes mencionado como es el tema de la capacitación a los operadores judiciales para que de esta forma puedan hablar el mismo idioma del tipo penal (el principio de la Congruencia), al igual que fortaleces la cooperación nacional e internacional.

En aras de la "globalización" (Alejandra, 2010), decimos que el mundo vive una enorme transformación y de igual forma nuestra legislación, la cual es llamada legislación moderna, la cual de una u otra forma viene viviendo una transformación en este siglo, gracias a los avances técnicos y tecnológicos, al igual que la electrónica y la telecomunicación.

Esta transformación o cada uno de estos avances nos ha llevado a que la forma de delinquir también se transforme y que tomen como herramientas todos y cada uno de estos instrumentos que surgen y de ahí que aparezca una nueva legislación.

Nuestra legislación no ha sido ajena a estos cambios y ha tratado de adecuar la misma a estos nuevos tipos penales. Como es el caso de los documentos electrónicos (Republica C. G., 2014) y la forma como deben ser no solo aportados, sino su valoración por parte de los operadores judiciales, ya que muchos de ellos no aceptan o mejor aún son muy temerosos de reconocerlo como un medio de prueba convencional (documento escrito), e incluso desconociendo la adaptación

de nuestro ordenamiento jurídico a estos cambios, ya que reconoce el documento electrónico como otro medio de prueba. Su aceptación no solo es al interior de los entes estatales sino al interior de las empresas privadas; ya que los documentos electrónicos, como los mensajes de datos, están en capacidad de brindar la misma seguridad jurídica que un documento convencional, en cuanto a confianza y validez, además de guiar al juez en una convicción de lo ocurrido con la misma certeza.

Situación está que nos permite aseverar e insistir que el problema está más en la falta de capacitación de los operadores jurídicos que le brinde la seguridad jurídica necesaria al proceso, que en la creación de nuevas herramientas. Si bien es cierto, en la práctica se ha logrado identificar, la existencia de soporte jurídico para la adaptación de este tipo de medios de prueba, pero una gran parte de los operadores jurídicos desconocen las técnicas y los medios que le permitan su aplicación, valoración y aceptación, dentro de un proceso, la información que este contiene.

Muy a pesar de existir medios de prueba idóneos con los cuales puedo llevar al juez a un verdadero conocimiento del hecho y de forma más precisa, desafortunadamente a las pruebas electrónicas no le han dado la suficiente valoración y por ende pierde su fuerza probatoria, degradándola al concepto de indicios. Pero podemos decir que esto se debe gracias al desconocimiento por parte del juez y el temor a explorar en nuevos mecanismos o alternativas, la inseguridad del operador jurídico se convierte en una inseguridad para el sistema.

En el ordenamiento civil existe un principio llamado equivalencia funcional el cual está contenido en la ley 527 de 1996, el cual no es una forma de valoración de la prueba electrónica, sino que, presenta unos parámetros para que se circunscriba en el equivalente funcional; además para ahondar en estas garantías el estado cuenta con unas entidades encargadas de validar parte de la información y brinda algunas garantías como es el de certificar, de esta forma se puede hablar de autenticidad y veracidad de la información contenida; Es el caso de las cámaras de comercio.

Para Colombia a pesar que es un país donde no se ha avanzado mucho en el tema, si cuenta con una legislación y con una capacidad de afrontar el tema desde el punto de vista forense, estados unidos a través de su agencia de investigación inicia el proceso en lo referente a la investigación y la evidencia digital en el año 1984 y para nosotros esto no es ajeno, hemos dado grandes avances, pero también es cierto que la delincuencia en nuestro país viene avanzando a pasos agigantados además que estos son delitos transnacionales en su gran mayoría.

Dentro del análisis forense no solo se procura por la autenticidad de la información recopilada sino también por el contenido del mismo, su lugar de almacenamiento, el tratamiento recibido, entre otras, ya que de esta forma podemos referirnos a la autenticidad, si la información fue alterada, o si es veraz o no. Dentro de dicho análisis de decantan una serie de terminología que debe ser amplia mente conocida por los operadores judiciales, donde no solo basta con saber que es un software o un hardware, las partes de computador, sino que también se hace necesario conocer términos como Bit, archivos MTF o FAT, logaritmos de HASH, dirección IP, Log transaccional, entre otras (Alejandra, 2010).

Es por esta razón que se insiste en la capacitación a los operadores judiciales y al público en general para que podamos hablar un mismo idioma y se le dé el tratamiento justo y necesario a cada proceso, de acuerdo con lo que nos arroje la investigación y las pruebas con sus evidencias electrónicas.

## 3.2. Cuál Ha Sido La Postura De Otros Países Referente Al Tema.

Si bien podemos evidenciar este temas, no solo nos preocupan a nosotros ya que de esta misma forma lo vivencian en otros países con otra legislaciones como es el caso de Ecuador (Pino A. d., 2009), quienes manifiestan que, Si bien es cierto la prueba es de suma importancia dentro del proceso penal ya que con ella se afianza o se desvirtúa la hipótesis del proceso, en tratándose de delitos informáticos, debemos tener en cuenta, no solo la capacidad del investigador en la recolección

sino en la conservación de la misma y que en la mayoría de los casos en los delitos informáticos tales como el frade informático, desviación de fondos, entre otros son cometidos desde adentro de la misma organización o de una que tiene relación virtual con la misma es decir que esta electrónicamente conectada.

A pesar de que normativamente estén tipificadas muchas o la gran mayoría de conductas, también se hace necesario no solo la parte procedimental sino la capacitación de los agentes que intervienen el proceso, contar con buenas herramientas para el análisis de la información obtenida, para que de esta forma se pueda tener unas buenas decisiones judiciales.

Es importante tener en cuenta que jurídicamente de manera sustancial existen muchos mecanismos para enfrentar este tipo de infracciones, como lo es la ley de comercio electrónico, código de penal y de procedimiento penal vigente en este país, pero se hace necesario poder otorgarle plena validez a la evidencia electrónica (Alfonso, 2015) y darle un mejor tratamiento al mismo, dentro de la sana critica tener en cuenta la valoración de la misma y el aporte que esta le brinda al proceso en aras de proteger los bienes jurídicos legales.

Para encaminar de forma adecuada una investigación se hace necesario tener una serie de conceptos muy claros, ya que como se refiere no es lo mismo adelantar una investigación por homicidio donde se vea involucrado en la parte probatoria un elemento electrónico, que investigar un fraude, donde esté involucrado un equipo electrónico o la misma red.

Refiere a que se hace necesario categorizar para poder distinguir entre el elemento material de un sistema informático (evidencia electrónica) contenida en el hardware y la información contenida dentro de esta (llamada evidencia digital) (Pino A. d., 2009).

Es importante tener claro que el hardware puede ser elemento de delito, cuando este sea el objeto de comercio ilegal por ejemplo o un medio para cometer el delito, cuando este sea el instrumento utilizado para tal fin como es el caso del disco duro.

Se dice que es una evidencia electrónica ya que ella es el contenedor o el mismo elemento producto del ilícito.

Decimos que la información es ilegal cuando se trata el contenido que esta lleva consigo el caso de la pornografía infantil, pero es diferente cuando la información es utilizada para lograr cometer un acto ilícito como es el caso de los correos electrónicos engañosos.

Sirve como evidencia digital en la medida que deje rastros de la persona que utilizo dicha información.

También es cierto que estos elementos deben ser analizados no solo por separado sino en conjunto y con la ayuda de expertos en el análisis forense digital.

Existen muchas definiciones de evidencia digital, donde todos convergen en que es un sistema binario conservado en un dispositivo llamado ipods, celular, Tablet, memorias extraíbles, Etc. Donde podemos conservar imágenes, documentos, música entre otros. Pero todo esto se conserva mediante archivos, denominados metadatos, pero estos archivos pueden ser fragmentados en el evento que se sobre escriba la información, la cual queda almacenada en la memoria RAM.

La evidencia digital se puede clasificar en 3 grupos.

- Sistema de computación abierto: son los equipos de cómputo personales o portátiles
- Sistema de comunicación: sistemas de redes de comunicación.
- Sistemas convergentes de computación: son todos los sistemas tecnológicos diferentes al computador, pero operan igual a estos

Es importante aclarar que la tecnología evoluciona y esto lo deben tener claro los investigadores al igual que los operadores jurídicos y el público en general, pues con la evolución del tiempo nos hemos dado cuenta que hay información que se almacena en los equipos tecnológicos como el disco duro almacenamiento de forma permanente en los archivos creados, pero también es cierto que hay información llamada volátil que solo se almacena de forma temporal en la memoria RAM o en el CACHE, información que solo se puede extraer mientras el equipo esté en funcionamiento una vez se apague esta se pierde, esta evidencia se perdería y este es uno de los problemas que presenta este tipo de evidencia y por ende se convierte en una prueba poco confiable para aquellos operadores que conocen poco de esto. Por otra parte, la evidencia digital tiene una dinámica de acción la cual es llamada por algunos autores y conocedores del tema como el principio de intercambio o el Locard, el cual tiene una semejanza con la bitácora o el Log transaccional (Alfonso, 2015) en el cual se evidencia la actividad registrada por el agente que realiza el ataque.

La dinámica de la evidencia se puede alterar de múltiples formas, para las cueles el investigador debe estar lo suficientemente preparado para enfrentar estas situaciones y lograr la mayor parte de evidencia digital que le sé a posible recolectar y preservar, sin que sufra alteración o deterioro.

## 4. SEGURIDAD INFORMÁTICA.

Es importante anotar que cuando nos referimos a la seguridad informática se debe tener en cuenta inicialmente, quienes son las personas encargadas de dicha seguridad, además de una serie de requisitos que debe tener en cuenta para poder aplicar la misma, como seguridad física en relación a los equipos, de los datos, recuperación de los mismos, disponibilidad y seguridad normativa, por último la capacidad de análisis forense, una capacidad suficiente para evitar que la evidencia en el momento de ser presentada en juicio no sea susceptible de ser excluida.

Razón por la cual que podemos decir que se hace necesario, un procedimiento de operaciones estándar, el cual no es otra cosa que una serie de pasos o procedimientos que se deben realizar de forma ordenada, al momento de recolectar, asegurar, analizada y filtrada de la evidencia digital con el fin de que cada opinión por separada tenga la misma conclusión, por eso se hace necesario un protocolo, con el cual se pueda certificar todas y cada una de las actuaciones de los expertos, quienes fungirían como peritos expertos, esto sin desconocer que cada caso tiene su complejidad en su esencia.

Razón por la cual nuestros legisladores muestran gran preocupación, al referente, lo vemos reflejado con la ley 1581 de 2012 (Republica C. d., 2012), podemos decir que su objeto es desarrollar el derecho que tenemos todos los ciudadanos a conocer, ratificar y actualizar toda la información que se tenga sobre nosotros en bases de datos, su aplicación en dichas bases ya sea en entidades públicas o privadas. El tratamiento de los datos personales le será aplicable al responsable del tratamiento dentro del territorio colombiano o aquellas personas que no estén dentro del territorio nacional pero que la legislación le sea aplicable al mismo.
En que eventos no es necesario el tratamiento de datos; cuando sean bases personales, cuando sea por seguridad o defensa nacional, de inteligencia o contra inteligencia, información periodística, los censos de población y vivienda nacional.

Por otra parte, nos da a conocer las categorías de los datos, como los sensibles, los cuales no son otros que afectan la intimidad de las personas dueña de la información, el tratamiento para estos datos, es la prohibición de los mismos con algunas excepciones; el titular autorice; que la información se vital, cuando se trate por parte de una fundación o una ONG, en ejercicio o defensa de un derecho del procesado, tenga finalidad histórica con la suspensión de la identidad del titular.

En razón a los derechos de los niño, niñas y adolescentes: debe prevalecer los derechos de los mismos, salvo los datos de naturaleza pública y el estado debe

garantizar la capacitación necesaria para sus tutores frente a los riesgos de la información de sus prodigados privados e íntimos dejados al azar.

Que derechos tiene el titular:

- Conocer, actualizar y ratificar sus datos personales, frente al responsable de sus datos.
- Solicitar prueba de autorización otorgada.
- Ser informando sobre el uso efectuado.
- A elevar queja, cuando sienta que su información no fue tratada correctamente.
- Revocar la autorización cuando el encargado allá incurrido en una falta
- Acceder a sus datos de forma gratuita.

El tratamiento de los datos (Republica, Congreso de la, 2018) requiere autorización previa por parte del mismo, la cual puede ser obtenida por cualquier medio, y esto también vincula a los mensajes de texto o correos electrónicos.

Cuando no es necesaria dicha autorización:

- La información sea requerida por una entidad en ejercicio de sus funciones legales u orden judicial.
- De naturaleza pública.
- Por urgencia médica o sanitaria
- Para fines históricos

La información puede ser suministrada por cualquier medio, de fácil lectura y sin barreras técnicas.

Se debe informar al titular:

- A que tratamiento será sometido sus datos y la finalidad.
- Las respuestas a las preguntas hechas son facultativas.
- Sus derechos
- La identificación completa del responsable.

Que personas pueden acceder a esta información:

- Titulares, causahabientes o representantes
- Entidades con orden legal u orden judicial.
- Los que este autorice.

Frente a los responsables del tratamiento cumplen con los siguientes deberes.

- Garantizar el hábeas data
- Solicitar y conservar las autorizaciones.
- Informar al titular los derechos que le asisten.
- Conservar la información bajo medidas de extrema seguridad.
- Garantizar la veracidad de la información
- Ratificar, cuando se incorrecta.
- Exigir al encargado del tratamiento la discrecionalidad con la información.
- Tramitar en los términos señalados
- Garantizar el adecuado cumplimiento de la ley.
- Informa de manera oportuna cuando se presente violación a la seguridad de la misma y que esto genere un riesgo.

## 4.1. La Colaboración Internacional Y Protocolos Nacionales

En razón de la seguridad informática se hace necesario mencionar la colaboración y que clase de protocolos son determinados por la comunidad internacional, ya que su principal exigencia como norma de seguridad es que se prohíbe la trasferencia de datos personales a otros países, que no cumplan con los estándares que exige la súper intendencia de industria y comercio sobre la materia, entre otras, para poder cumplir con dichos estándares de seguridad y a los cuales nosotros le debemos apuntar.

Así mismo respecto al tema se ha referido en la resolución reglamentaria de la contraloría general de la nación 277 de 2014 (Republica C. G., 2014), por medio del cual implementan una herramienta tecnológica denominada SAE (sistema de aseguramiento Electrónico) tiene por objeto adoptar dicha herramienta con el fin de

conservar, administrar, emitir información, regular el funcionamiento, alimentación de los expedientes electrónicos, entre otros, el cual es aplicable a toda la contraloría general de la nación.

Se crea una distribución de responsabilidades de acuerdo a las funciones relacionadas con el manejo de la herramienta tecnológica. Tal es el caso de la oficina de sistemas quien es la responsable de administrar, gestionar, implementar procesos y procedimientos, mantenimiento, administración de la seguridad de la plataforma, mantenimiento del software, realizar los respaldos necesarios del sistema, realizar los ajustes necesarios.

Unidad de seguridad y aseguramiento tecnológico e informático, los deberes, las obligaciones y perfiles necesarios, velar por el buen uso de la herramienta, la administración lógica de los certificados, esto a través de un dispositivo denominado TOKEN (Republica C. G., 2014).
Unidad de archivo y correspondencia se encarga de: velar por los expedientes y digitalizarlos, brindar los soportes necesarios.

La oficina de capacitación, producción de tecnología y cooperación técnica internacional, será la responsable de: implementar programas de capacitación, lo relacionado y pertinente con la elaboración de documentos o manuales necesarios para la capacitación de dicho sistema. La oficina de planeación será la responsable de: producir y aprobar los manuales.

La dependencia de usuarios de la plataforma, de acuerdo a los roles: de primera instancia, con permiso de todo e incluso con firma digital. Sustanciador de primera instancia, responsable del proceso administrativo, solo conoce de los asuntos que son encomendados, usuario líder de grupo, revisa las decisiones del sustanciador.

Sustanciador de segunda instancia, encargado de revisar los procesos tales como quejas o apelaciones. Usuario de revisión de segunda instancia. Usuario

competente de secretaria común, el encargado de los trámites de notificación o comunicación de los actos administrativos.

La unidad de gestión documental se encargará de garantizar el expediente electrónico y todo lo que a ella le atañe como es la elaboración de la firma digital, alimentar los expedientes electrónicos.

Frente a la autenticidad de la firma digital (Republica, Congreso de la, 1999) por parte del sujeto responsable mientras este inmerso en el sistema SAE (Republica C. G., 2014), la firma se reputará de auténtica.

Tanto el trámite de notificación como los expedientes y la expedición de copias se reputarán de auténticas mientras su contenido este acompañado de la firma digital del responsable del remite., las mismas serán entregadas por medio magnético, sin menoscabo de su validez.

Lo atinente al dispositivo que contiene toda la información correspondiente a las firmas necesarias para acceder a la plataforma y todo lo que esta contiene, llamado TOKEN, es suministrado a cada servidor responsable de la unidad y encargada de alimentar los expedientes y plasmar su firma electrónica.

Pero finalmente vemos como apenas se está adentrando en esta materia, muy a pesar que ya se tenía referencia del mismo, pero no se había visto la necesidad y aun el avance como vemos es poco, pues to lo podemos analizar desde la ley 527 de 1999 reglamenta el uso y acceso de los mensajes de datos, del comercio electrónico y la firma digitales, al igual que las entidades que las certifican (Republica, Congreso de la, 1999).

De una manera muy amplia la ley define mensaje de datos como toda información procesada por medios electrónicos o telemáticos tales como intercambio electrónico

de datos (es la trasmisión electrónica de datos de un equipo a otro), mensajes electrónicos, correo electrónico telegramas, télex, entre otros.

Los mensajes de datos a partir de esta ley tienen plena valides, con carácter vinculante y legal.

Requisito de originalidad de un documento, el cual pude ser un mensaje de datos, si cumple con unas condiciones tales como: garantice que se ha conservado la integridad desde que se generó, se pueda presentar, la cual se constituye en obligación si es exigida por la norma o como forma de prevenir, se presume enviado por la persona que lo elaboro, cuando el que lo recibe tiene comunicación con el mismo o cuando que haya autorizado su representación

Dicha ley es aplicable a todo tipo de información a través de mensajes de datos, pero establece algunas excepciones como: las obligaciones contraídas por los convenios o tratados internacionales y las descritas en las obligaciones legales.

Comercio electrónico es toda transacción comercial realizada a través de un sistema electrónico como mensaje de datos o cualquier otro medio similar.

Firma (Republica C. G., 2014), es un valor numérico (logaritmos) que se le da un texto, para su autenticidad; si es establecida como exigencia de la misma e indica la aprobación para una obligación o para prevenir posibles consecuencias, además denota la intención de acreditación, como la firma manuscrita, cumpliendo con unos atributos especiales.

La entidad que certifica es aquella encargada de emitir las certificaciones necesarias de las personas que posean las firmas digitales.
Sistema de información es aquel utilizado para enviar, recibir, archivar y procesar los mensajes.

Los mensajes de datos a partir de esta ley tienen plena valides, con carácter vinculante y legal.

Requisito de originalidad de un documento, el cual pude ser un mensaje de datos, si cumple con unas condiciones tales como: garantice que se ha conservado la integridad desde que se generó, se pueda presentar, la cual se constituye en obligación si es exigida por la norma o como forma de prevenir.

La norma refiere que los mensajes de datos tienen una fuerza probatoria, y así se acepta, una vez se demuestre con criterios científicos o incluso des de la misma sana crítica del operado judicial, al momento de dar su valoración.

Se tiene la obligación de conservar los mensajes de datos o archivos cuando estos contengan información sensible, que se conserve en el formato generado y que permita determinar origen, destino, fecha y hora y podrán ser conservadas por terceros.

Se regula las entidades prestadoras del servicio de acreditación, las cuales pueden ser organismos del estado o privadas siempre y cuando realicen unas actividades encargadas y cumplan con unas obligaciones, para poder certificar.

### 4.2. El Gran Logro De Colombia Respecto A La Política De Seguridad, Referente Al Cibercriminalidad.

De una forma muy grata puedo decir que, nuestro gran paso en lo ateniente al tema, está en la ley 1924 de 2018 (Republica, Congreso de la, 2018) por la cual se aprueba el convenio de Budapest para Colombia, un gran paso, El presente convenio, el cual es suscrito inicialmente por algunos países europeos, con el fin de contrarrestar, el avance y la aceleración desbordada de los delitos a través de la tecnología y las redes, donde se vulnera la confidencialidad, integridad y disponibilidad de los sistemas informáticos, las redes y datos informáticos, además de abuso a estos. Preocupados por esto y en aras de velar por la protección d los

derechos humanos, la libertad de expresión, la intimidad de las personas entre otros, no menos fundamentales, se crea el presente convenio, el cual recoge una seria de convenios y tratados, siempre con el objeto de proteger el derecho de los datos personales, de esta creciente oleada de crímenes mutados.

El presente convenio hace una tipificación efectiva de algunas infracciones penales las cuales de una u otra forma enmarcan la gran mayoría de los delitos que se cometen a través de los sistemas informáticos como son: acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad de un sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, lo relativo a la pornografía infantil, atentados contra la propiedad intelectual y derechos afines, esto a modo de prevención, siendo muy reiterativos además de respetuosos al presentar la expresión “Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno”.

Me genera una gran admiración ya que dicho convenio fue adoptado creado se adelantaron a muchas situaciones, que cualquiera pensaría que no eran aun previsibles, como es el hecho de referirse a la tentativa y la complicidad, más aún a la sanción de las personas jurídicas, cuando en nuestro país apenas a la fecha 17 años después, se está analizando la posibilidad de dichas sanciones. En nuestro país aún es difícil el manejo del delito como acción consumada y hablar de complicidad mucho más, puesto que en lo relativo a la parte probatoria se nos ha hecho difícil de mostrar la autoría d un hecho punible, gracias a la falta de valoración probatoria, gracias al desconocimiento del manejo del mismo.

En relación a la aplicación, procura que todos los estados firmantes adopten las medidas legislativas y necesarias que estime conveniente para instaurar los poderes y procedimientos para los efectos de las investigaciones o procedimientos penales específicos, situación que en lo personal considero necesario y pertinente

ya que a la fecha vemos que estamos en un estado muy garantista más que para la víctima, está en favor del victimario.

Como condiciones y garantías esta en velar por la puesta en funcionamiento y aplicación de los procedimientos y poderes previstos para el cumplimiento y protección de los deberes del hombre, además del principio de proporcionalidad, manteniendo la supervisión judicial o cualquier otra medida que cumpla con la misma; así mismo imponer las medidas necesaria para la conservación y protección de los datos electrónicos y el tráfico de los mismos, en medios idóneos.

Asegurar de igual forma la divulgación de los datos electrónicos que se encuentren el poder de los prestadores de servicio autorizados en tiempo real, a las autoridades competentes cuando lo estimen necesario.

Dentro de estos mismos poderes debe existir la posibilidad que las autoridades competentes puedan exigir al prestador del servicio los datos llamados por nuestra legislación “sensibles”. E incluso con la posibilidad de registro y decomiso, sin la necesidad de solicitar una orden ante el juez de control de garantías (competente), sin desconocer que esta actividad debe ser realizada por personal altamente calificado e idóneo en la materia.

Este personal debe tener las condiciones y capacidad necesaria para recolectar o grabar mediante herramientas adecuadas con el fin de que la información se conserve de forma idónea.

Este poder que se otorgue a los representantes del estado es muy necesario que se le permita la posibilidad de exigir y ordenar a los prestadores de servicio o aquellas personas encargadas de conservar los datos electrónicos, el suministro de los mismos, sin ningún tipo de reserva, ya que esto es una situación que los operador judiciales que representan el estado se encuentran con las manos atadas, ya que los prestadores de estor servicio se niegan a entregar dicha información

hasta tanto no se solicita una audiencia de búsqueda selectiva en bases de datos, ante un juez de control de garantías, desconociendo la representación del estado y su competencia, apoyados en los vacíos de las normas.

Es muy importante resaltar el compromiso, entre los estados firmantes, respecto a la colaboración mutua sin perjuicio de que un estado demande la ayuda y el otro estado solicitado pueda negarse a prestar dicha ayuda, siempre y cuando cumpla con unos protocolos establecidos para tal situación; igual forma se debe cumplir con mantener la confidencialidad de la información e incluso de acuerdo con la legislación de cada estado y decidan no someterse.; además existe la posibilidad del estado requirente de la información a demandar y a imponer medidas cautelares, frente a la información solicitada o los datos electrónicos (Sanchez, 2016).

En tratándose de un flagelo, que afecta a todos los países del mundo, se hace necesario la integración de los mismos para poder atacar y contrarrestar esta actividad delictiva, si bien es cierto las personas que operan en este ámbito son personas altamente capacitadas y gracias a la misma tecnología pueden estar en cualquier parte del mundo y afectar un país por más distante que este, Colombia no es ajeno a dicha situación más a un que cada día incrementan los delitos cometidos por este medio, razón por la cual se hace necesario que este inmerso en este tipo de convenios o tratados para el fortalecimiento, gracias a la colaboración mundial.

Así de esta forma se pueda atacar los delitos electrónicos, los cuales no son otra cosa que: todo tipo de acción o conducta punible que pone en peligro o genera un riego de un bien jurídico protegido, cuyo medio de empleo son los medios técnicos, tecnológicos o de las comunicaciones, obteniendo provecho para sí o para otro. Creo que de esta forma se abarca la totalidad de la expresión en términos generales.

Es importante hacer el análisis que plantea el autor frente a la criminología, ya que no es posible hablar de un delincuente común que ejecuta un tipo de ordinario, aquel

que tiene una función especial dentro de una organización y más aún, frente aquella persona que tiene unos conocimientos especiales y que no son del común, como es el caso de los delitos informáticos, razón por la cual es cierto que debe tener un tratamiento especial, en todos los sentidos de la palabra, e incluso para el desarrollo de la investigación, como al momento de ser juzgado, a modo personal considero que la persona que se atreva a investigar y juzgar estos tipos penales, debe estar un paso adelante del autor o responsable del hecho punible.

Así como a medida que evoluciona, el tiempo, evoluciona la tecnología, de igual manera evolucionan las acciones del hombre contra el mismo hombre, situación que no es ajena frente al tema en cuestión, cada que evoluciona la tecnología y/o los medios, evoluciona el conocimiento, consiente e inconsciente de hacer daño, pues no todos lo hacen de forma dolosa, pues algunos llegan a esto por nuestra propia culpa, al dejar puertas abiertas y es aquí donde se puede aplicar una frase de los abuelos “el ladrón lo hace la ocasión”. Pues estas personas solo con el afán de conocer o explorar llegan a lugares desconocidos y aprovechan la situación, pero también es cierto que si como hay personas que llegan a ser daño sin una intención inicial, hay otras personas que dolosamente aprovechan, no solo el conocimiento, sino los avances y los medios para cometer actos delictivos cada vez más graves o de mayor envergadura.

## 5. VEAMOS A MODO DE RESEÑA COMO A EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS EN ALGUNAS REGIONES DE NUESTRO PAÍS.

Respecto a las denuncias, podemos ver lo que tanto hemos insistido con relación al tema en, no es otra cosa que el desconocimiento, si bien es cierto en el parágrafo anterior mencionamos que así como la tecnología avanza los delincuentes lo hacen de igual forma, pero las investigaciones y las condenas no o son iguales o disminuyen, pero esto no es gracia a una acción efectiva por parte del estado, esto realmente me atrevo a decir que es gracias al desconocimiento del tema y el manejo

frente al mismo, es increíble que en el 2011 en la ciudad de Villavicencio (Sanchez, 2016) existan un número indeterminado de denuncias por distintos delitos, pero para el 2013, solo se estén tipificando 3 tipos de delitos, y para la fecha cuantos delitos podremos mencionar?, los organismos del estado cuantos delitos investigan diariamente?, si bien es cierto nuestra legislación solo ha tenido en cuenta los delitos informáticos, pero que afectan directamente el patrimonio, pero desconoce la existencia de delitos que el medio para causar o llegar al fin es la tecnología y violentan la vida, la salud, el libre desarrollo de la personalidad, entre otros. Ana lisis que se debe hace por cada región, en este caso mostrare unas estadísticas de la policía metropolitana de Antioquia, Sijín Meval unidad de investigaciones tecnológicas (imágenes anexas).

Se presentan múltiples discusiones alrededor del tema, si existe las herramientas necesarias para contrarrestar la acción criminal de los ciberdelincuente, si está en aumento, si se cuenta con la normatividad necesaria y suficiente, para tal fin, pero se ha dejado de lado, sin desmeritar todo el trabajo que las grandes entidades del estado han realizado como por ejemplo el COMPES, pero no se han preocupado por la aplicación e desarrollo procedimental el cual debe ir a la par de la norma sustancial, el cual debe recibir un tratamiento igual de especial como quienes en ellos intervienen, debemos aprender de los países que son potencia mundial, en razón a su practicidad al crear las normas y la aplicación de las mismas, no es de legislar por legislar y llenarnos de normas que finalmente no se aplican., a modo de ejemplo que ha pasado con algunas de las recomendaciones realizadas por el COMPES, las cuales, considero que si se le diera la aplicación, habrían más resultados positivos frente al flagelo de la ciberdelincuencia.

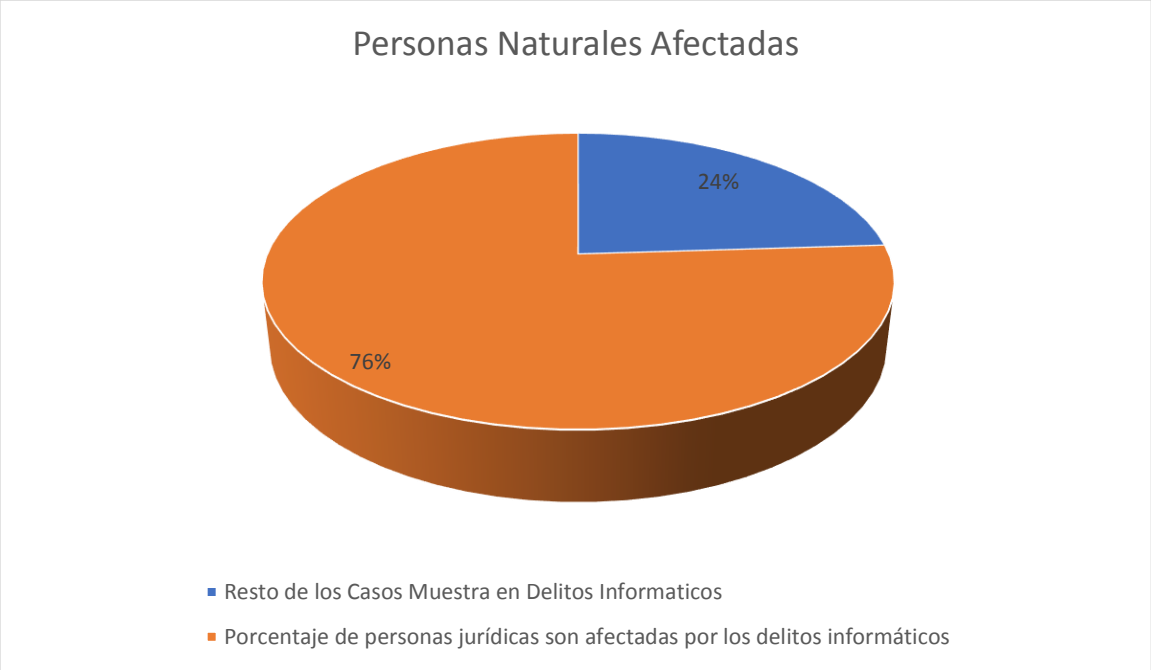
Capítulo 2

## 1. INFORME Y ANÁLISIS DE CASOS, COMO FORMA ESTADÍSTICA.

Una de las primeras estadísticas que debemos conocer no es otra a la cantidad de denuncias que ingresan diariamente a la sala de denuncias DE LA FISCALAIA GENERAL DE LA NACION SECCIONAL MEDELLIN, las cuales posterior mente son procesadas en la oficina de asignaciones, luego son repartidas en las diferentes unidades y grupos de trabajo, despachos fiscales, vale decir que para el mes de septiembre del año 2018 ingresaron solo por la sala de denuncias de la fiscalía de la seccional Medellín 4.242, de las cuales 220 correspondieron y fueron asignadas al grupo de fiscales de la unidad de delitos informáticos de esa seccional, todos sin indiciado conocido.

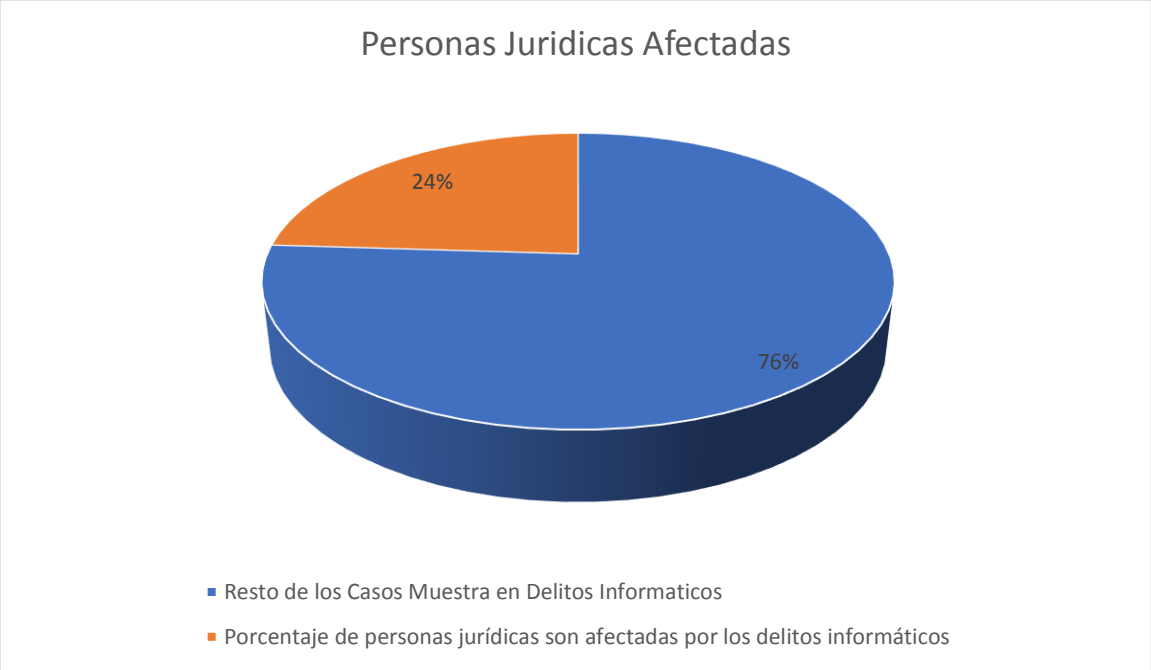

De acuerdo con el análisis de los casos observados vamos a sacar una serie de estadísticas en las cuales reflejare sus resultados y posteriormente hare un comentario a cada uno de estos resultados.

1. Porcentaje de personas naturales son afectadas por los delitos informáticos
   38 de 50



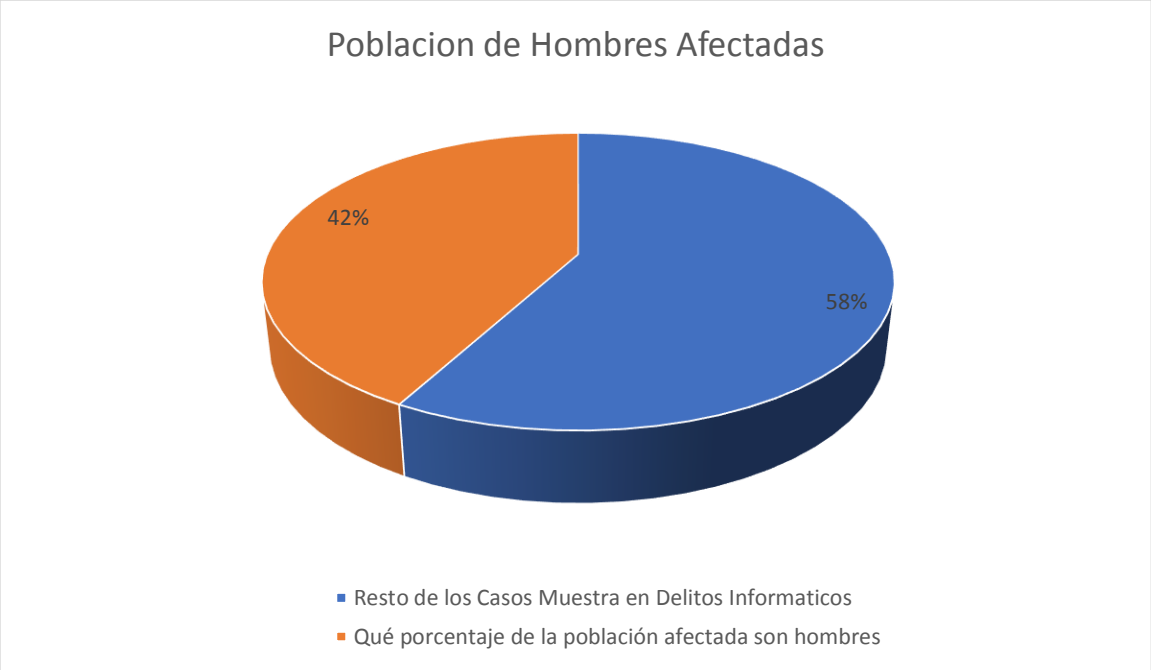

Con la presente grafica quiero indicar que de una muestra determinada de denuncias que se escogieron, el 76% de ellas, son personas naturales las que resultan afectadas por los delitos relacionados con los delitos informáticos, son delitos que afectan directamente a las personas ya sea en su patrimonio o cual quiera otro derecho fundamental, como la intimidad.

2. Porcentaje de personas jurídicas son afectadas por los delitos informáticos
   12 de 50



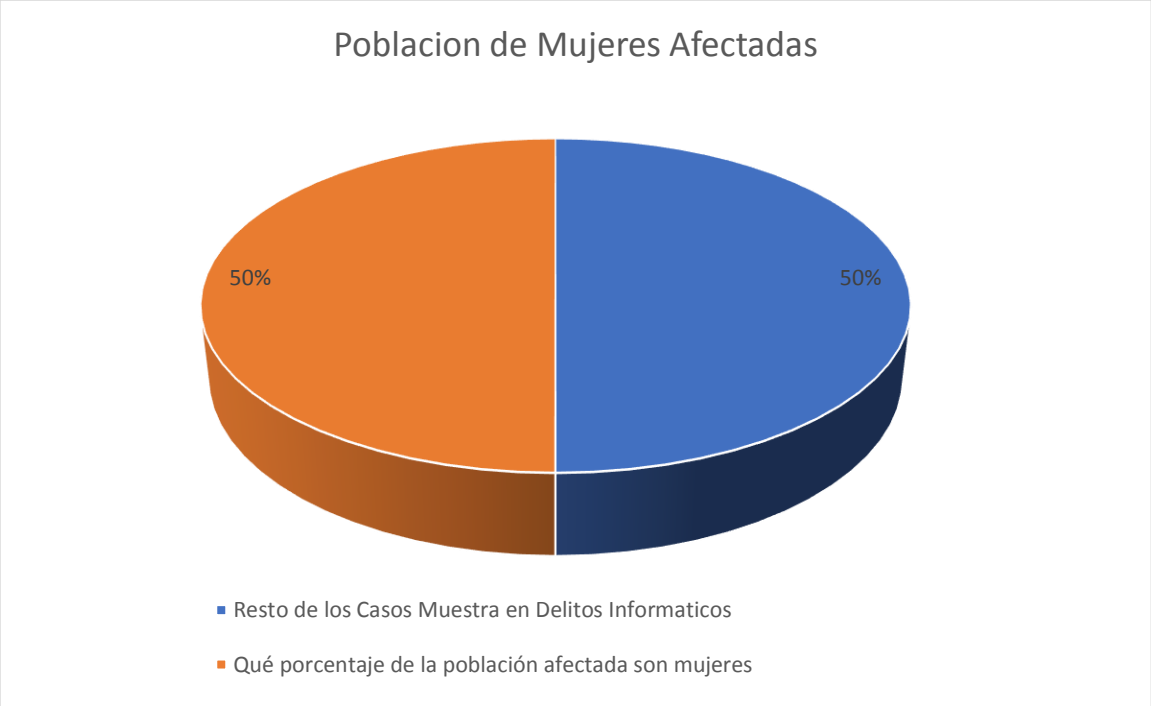

En este aparte encontramos a diferencia de la anterior, ya que, de la muestra tomada de denuncias, solo el 24% de la muestra, son personas jurídicas las afectadas, de las cuales la gran mayoría de este porcentaje son empresas privadas y un pequeño porcentaje de la misma corresponden a entidades financieras, muy a pesar de que ellas sean el medio, razón por la cual en la gráfica anterior se ve un porcentaje más alto la afectación de las personas naturales.

3. Qué porcentaje de la población afectada son hombres 21 de 50



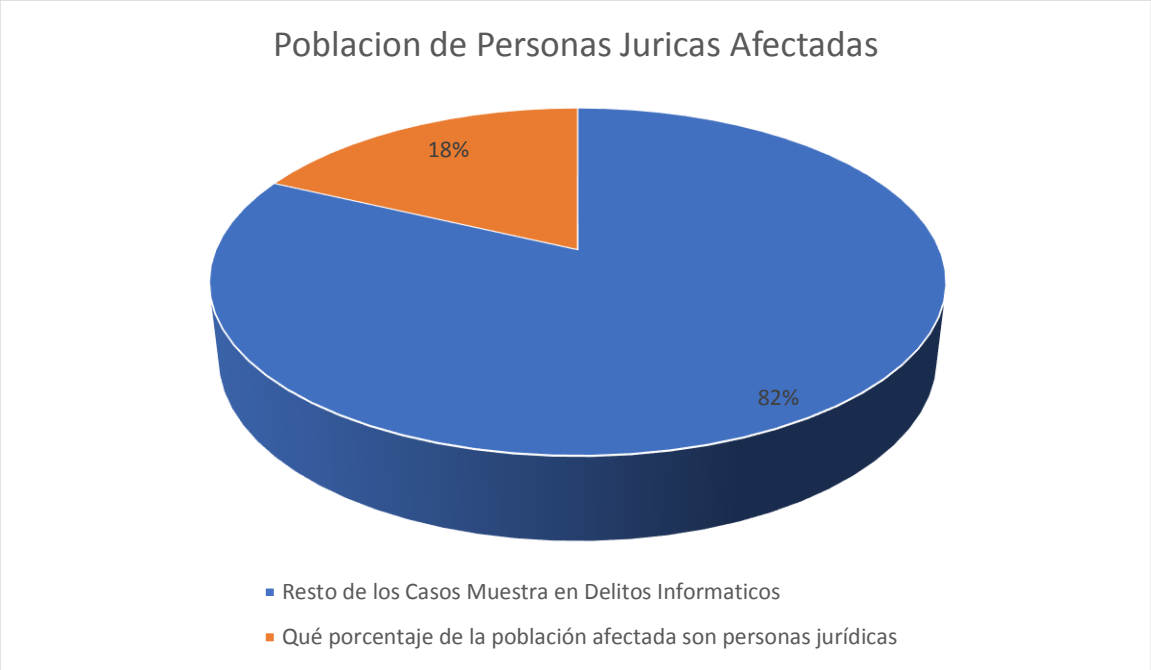

A través de esta grafica quiero demostrar que, de la muestra tomada de denuncias con relación a los delitos tecnológicos, el 42% son hombres, quienes se ven afectados, con delitos como compras por internet, extorción, estafa, entre otros.

4. Qué porcentaje de la población afectada son mujeres 25 de 50



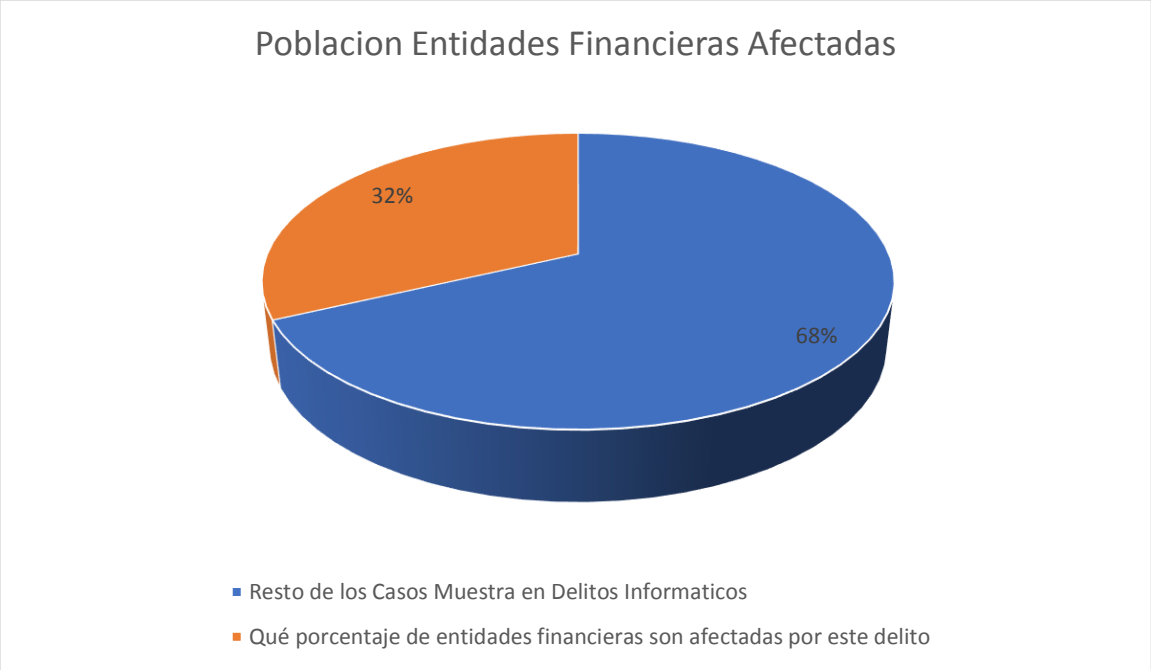

Con esta grafica se observa claramente que la diferencia entre personas naturales afectadas no siempre son las mujeres, pues es el 50% de la muestra son mujeres, el resto se divide entre el grupo de hombres y personas jurídicas, desafortunadamente lo que ha hecho que las mujeres sean un blanco perfecto para aquellos sujetos activos que operan es este tipo d delitos, es gracia a la confianza que ellas depositan, en sus operaciones o transacciones comerciales.

5. Qué porcentaje de la población afectada son personas jurídicas 9 de 50



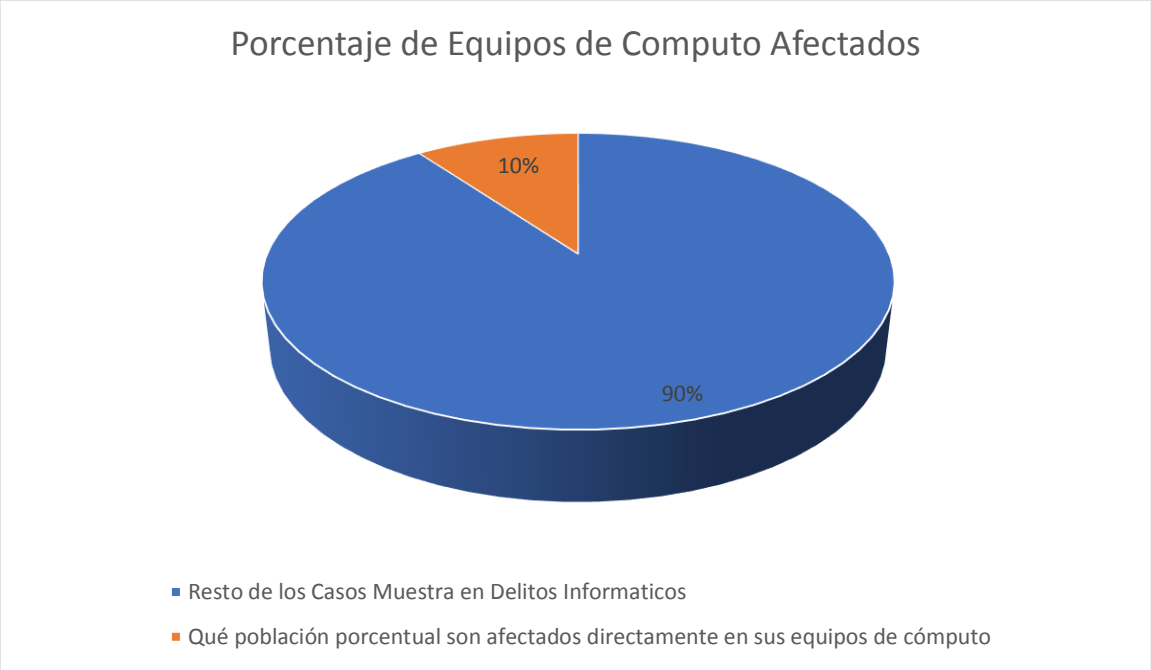

En la gráfica anterior se hizo el comentario con relación al porcentaje de personas jurídicas que se ven afectas por este tipo d delitos del cual se tomó una muestra de denuncias instauradas en la fiscalía general de la nación seccional Medellín y solo el 18% de la población representa a las personas jurídicas y básicamente esto sucede gracias a que no utilizan medios de protección segura, como por ejemplo un buen antivirus o por el hecho que los equipos de cómputo son utilizados sin bloqueos a paginas desconocidas.

6. Qué porcentaje de entidades financieras son afectadas por este delito 16 de 50



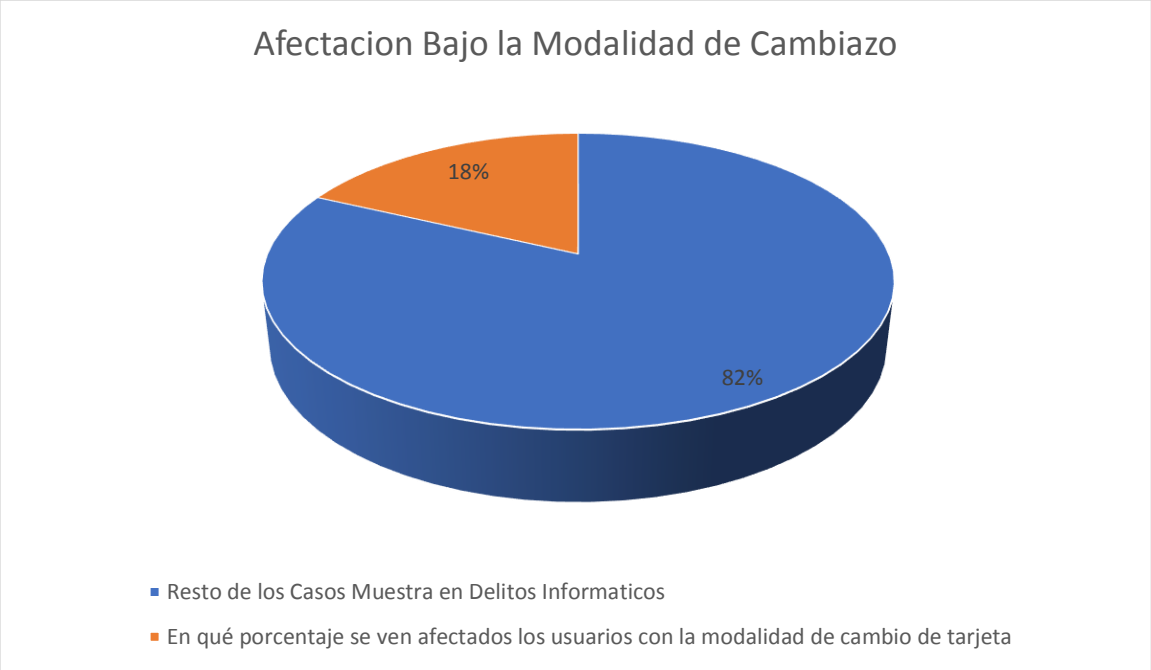

Con esta grafica se representa el porcentaje de entidades que están directamente relacionadas con los medios financieros, como por ejemplo los bancos o a fines, donde de la población de muestra tomada, representa el 32% de la misma que se ve afectada, esto con acciones delictivas como la creación d cuentas virtuales, compras de tiquetes, traslado de fondos, compras no consentidas con tarjetas de crédito, entre otras.

7. Qué población porcentual son afectados directamente en sus equipos de cómputo 5 de 50



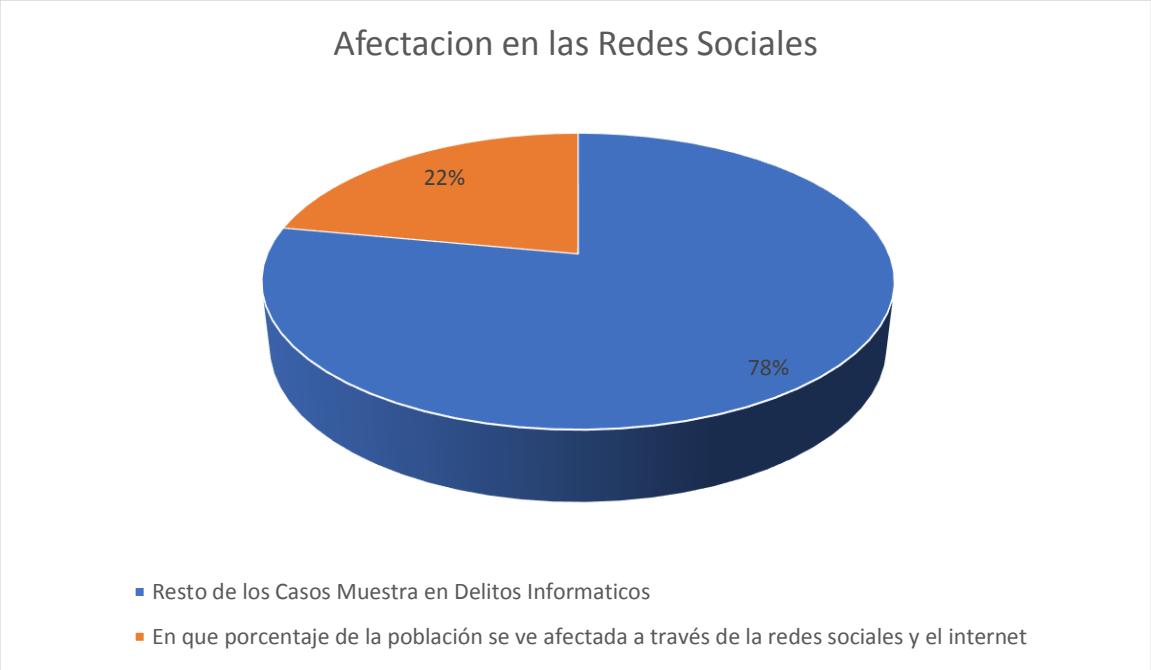

Cuando nos referimos a una afectación en su equipo de cómputo, es básicamente a aquellos delitos en los cuales no es el medio, sino más bien, el objeto de ataque, gracias a la información contenida en el mismo, ya sea con el fin de utilizar la información sustraída o con el fin de solicitar algún tipo de recompensa por devolver la misma, esto es realizado mediante distintos sistemas o herramientas, afortunadamente es solo el 10% de la muestra, pero esto viene en aumento.

8. En qué porcentaje se ven afectados los usuarios con la modalidad de cambio de tarjeta 9 de 50



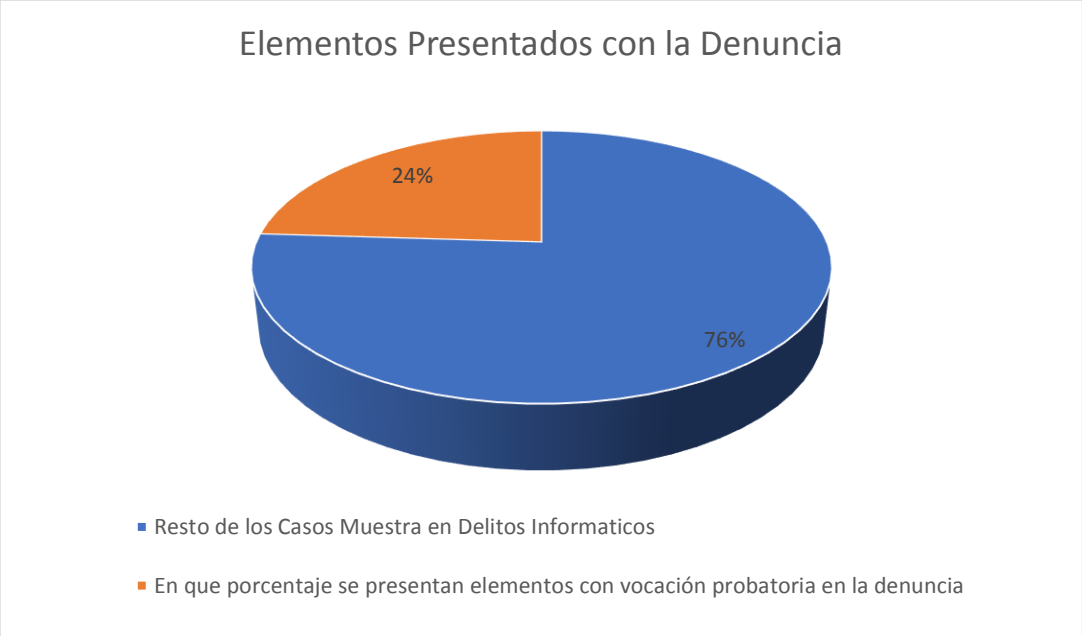

Esta es una modalidad delictiva que viene en aumento, por ahora solo hablamos de un 18% de la muestra, donde se mescla la habilidad del sujeto activo y la facilidad de hacer a la información en los medios tecnológicos, como a las claves de acceso de la misma al igual que es igualmente fácil adquirir documentos falsos para hacer la suplantación, algo que quiero resaltar en este tipo de acciones delictivas es que la gran mayoría de sujetos pasivos, son personas de la tercera edad.

9. En qué porcentaje de la población se ve afectada a través de las redes sociales y el internet 11 de 50



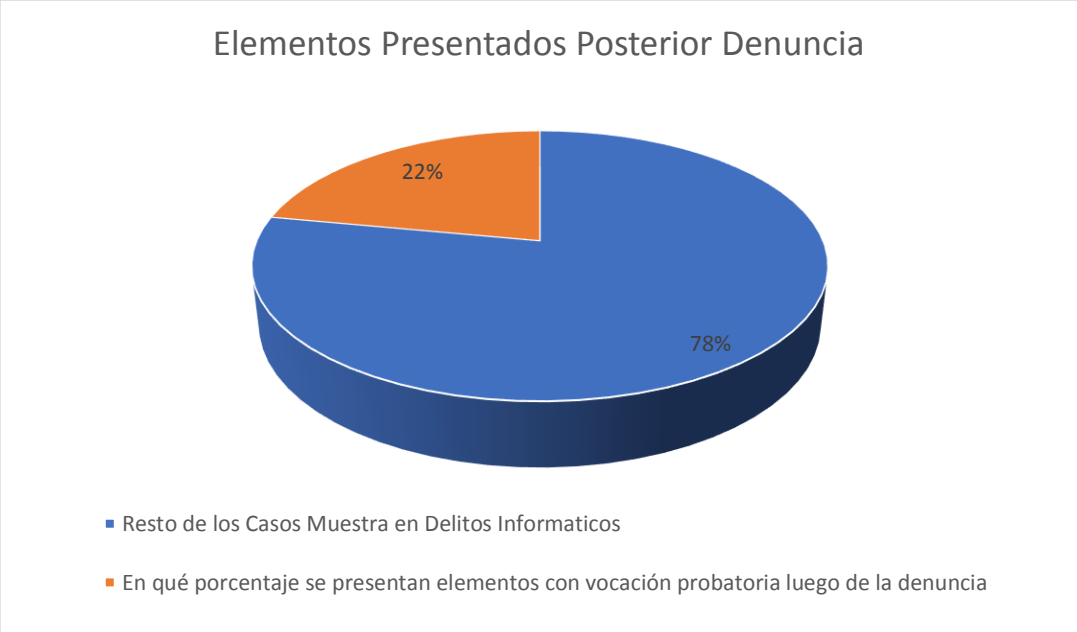

En relación a este flagelo, se ve una porcentaje, que aparentemente no es muy alto pero si bien es cierto un 22% de la población muestra de este trabajo, si podemos decir que es significativo, ya que tiene muchas variables delincuenciales, donde muchas de ellas se unen por su relación funcional, en grupos como afectaciones a través de las redes sociales como el facebook, instagran, twirer, etc, donde aprovechan y extraen información muy personal o intima para luego extorsionar o afectar el buen nombre de las personas.

10. En qué porcentaje se presentan elementos con vocación probatoria en la denuncia 12 de 50



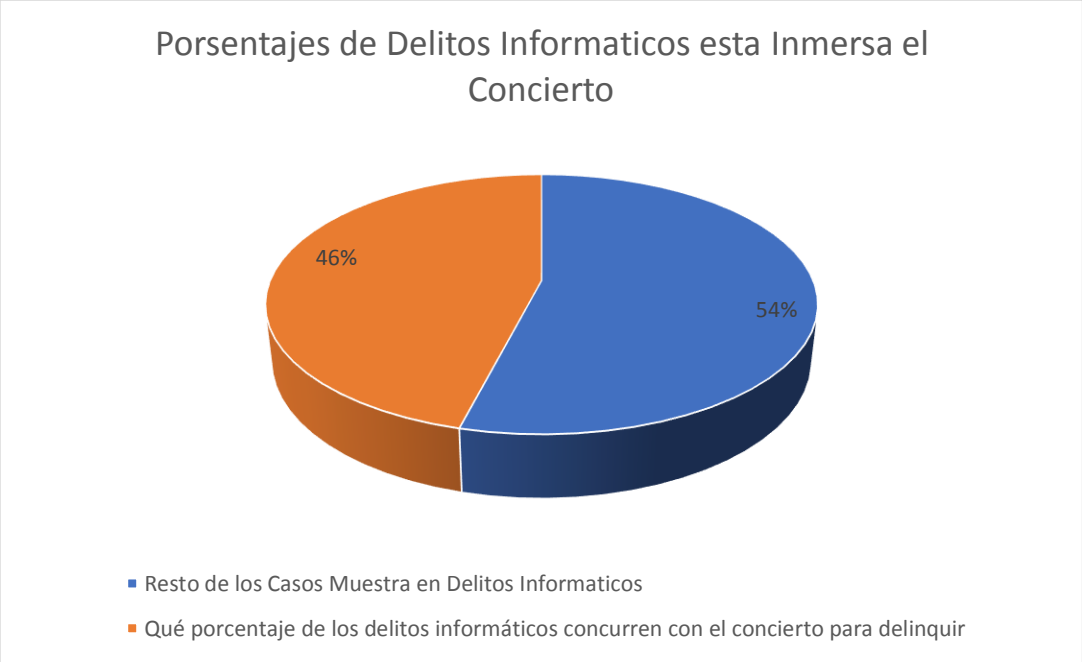

Dentro del proceso penal, más concretamente en la fase de indagación, la cual inicia con la denuncia, podemos detectar que solo en 24% de la muestra hace referencia a los elementos materiales probatorios aportados al momento de la recepción de la denuncia, que en su gran mayoría de personas no aportan ningún tipo de prueba de lo que refieren, solo se cuenta con la relación fáctica de los hechos, e incluso en los casos de delitos a través de mensajes de texto, la supuesta publicación indebida de imágenes privadas, en redes sociales o páginas web.

11. En qué porcentaje se presentan elementos con vocación probatoria luego de la denuncia 11 de 50



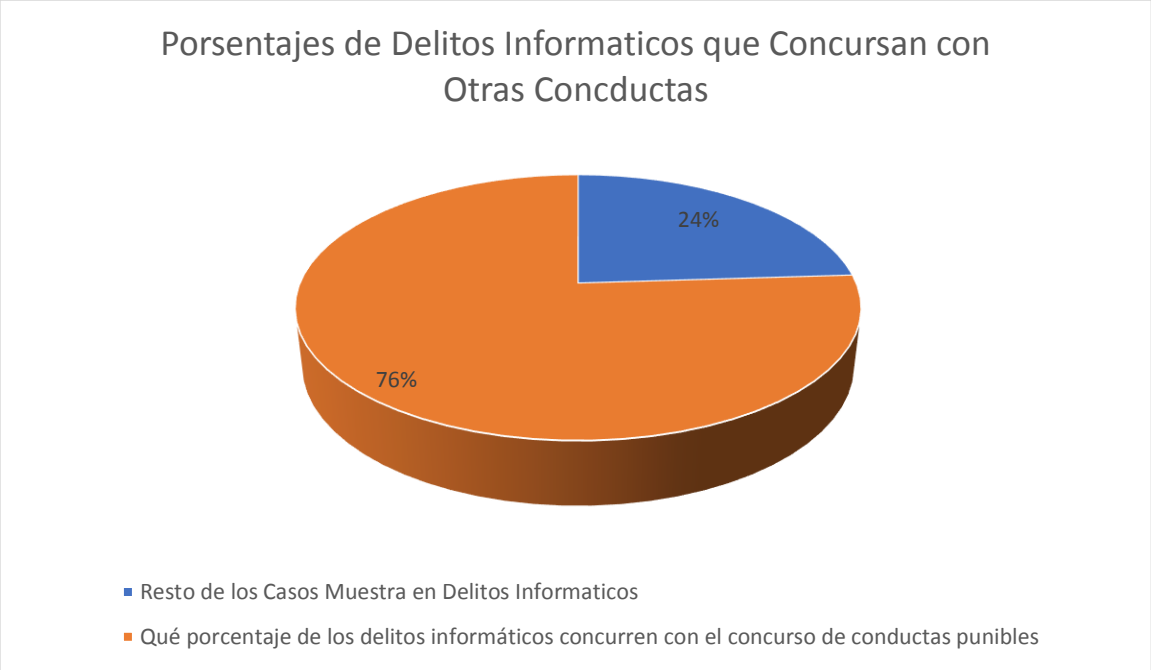

Con esta grafica quiero demostrar la gran dificultad probatoria y colaboración por parte de los denunciantes, ya que la administración de justicia espera al igual que las personas poder trabajar de forma conjunta, con la colaboración de la misma víctima, pero la gran mayoría de denunciantes como lo refleja la gráfica el 22% de la muestra, regresan a los despachos judiciales para entregar información o elementos materiales con vocación probatoria, ya que la gran mayoría pierden el interés o dejan todo en manos del aparato judicial.

12. Qué porcentaje de los delitos informáticos concurren con el concierto para delinquir 23 de 50



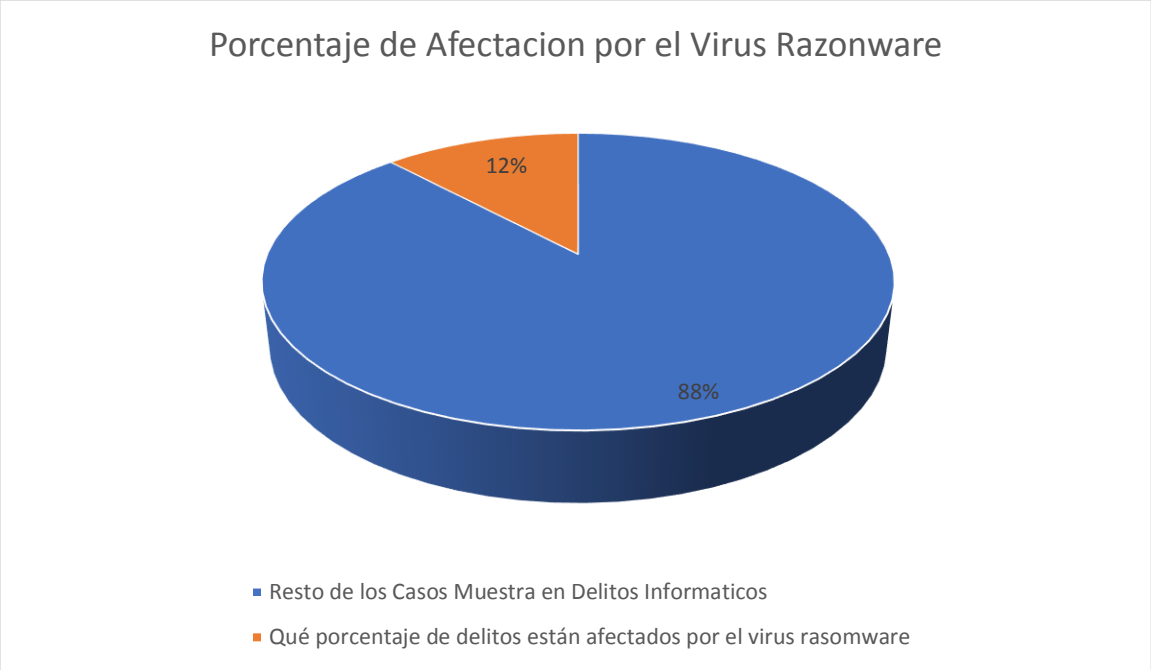

Lo que se pretende demostrar la existencia de un error de apreciación ya que muchas personas piensan que en esta clase de delitos solo hay un sujeto activo detrás de los medios tecnológicos, pero lo que aquí vemos es que el 46% de la muestra tomada, hacen parte de una empresa criminal. Como es el caso de los delitos comunes, en este tipo de delitos también se ve esta figura y aquí se logra demostrar.

13. Qué porcentaje de los delitos informáticos concurren con el concurso de conductas punibles 38 de 50



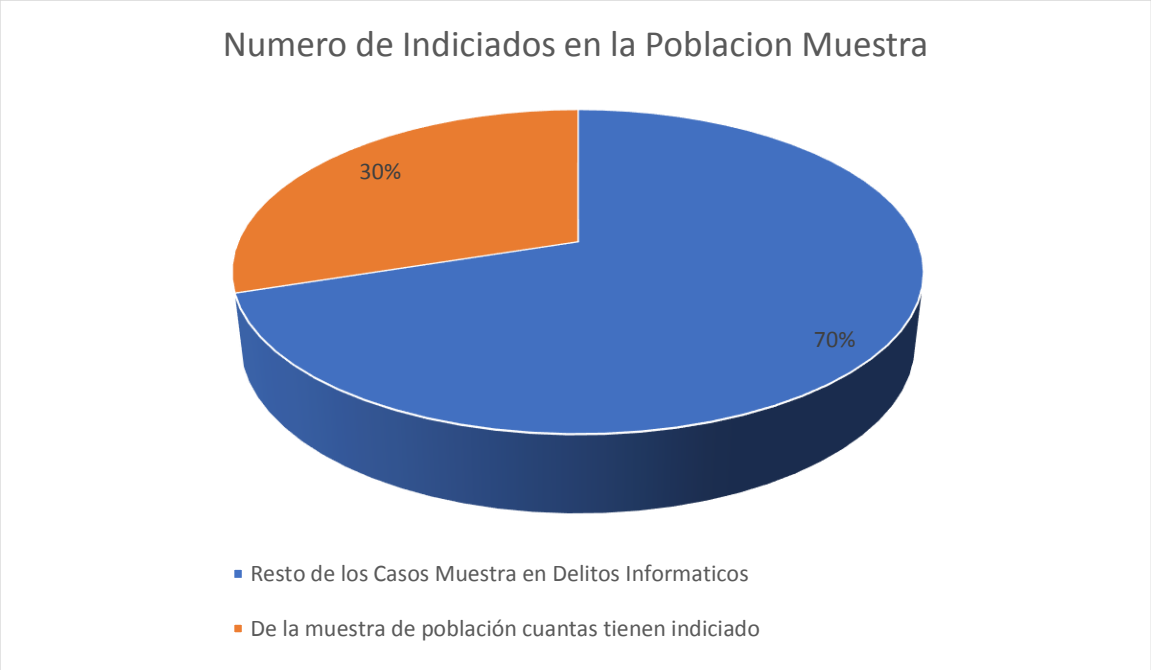

Con la presente grafica vemos como se presenta un porcentaje bastante alto en relación a la muestra tomada ya que nos indica que el 76% de la población, en la cual los delitos informáticos concursan con otras conductas punibles, como le son: extorción, constreñimiento ilegal, falsedad personal y material, calumnia, entro muchas otra más, esto debe ser un llamado de atención para los legisladores ya que parte de la normativa existente, está orientada es a los delitos contra el patrimonio económico y no han dimensionado, la evolución de la tecnología y la migración de los delitos a otras conductas punibles.

14. Qué porcentaje de delitos están afectados por el virus razonware 6 de 50



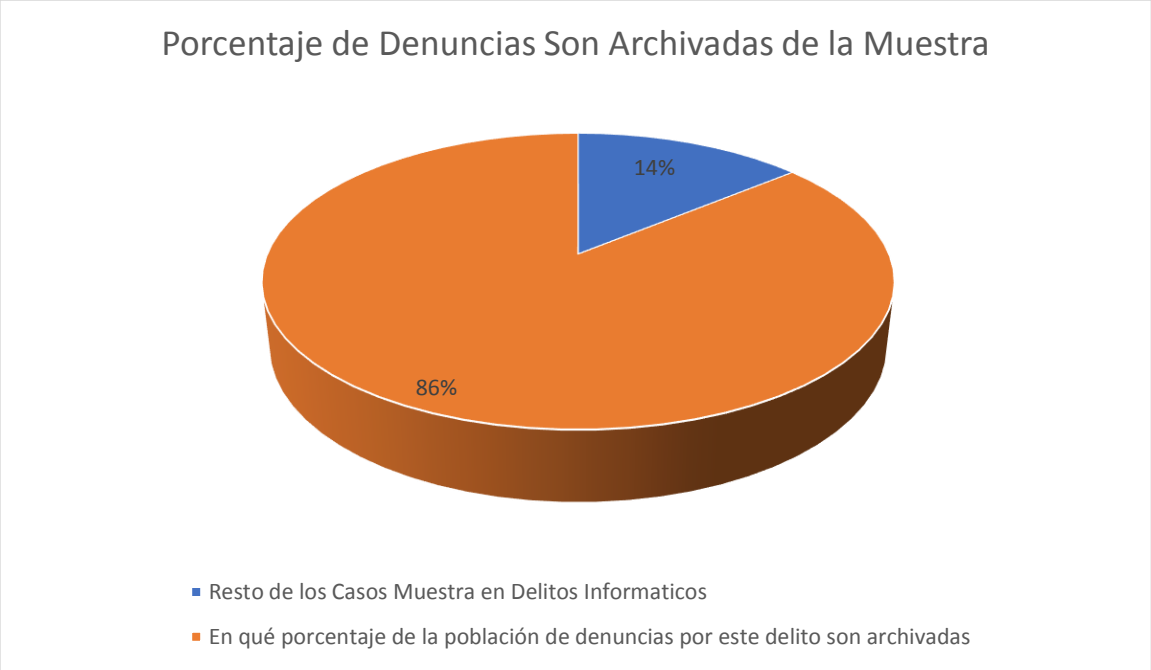

Que es el Razonware, es una especie de virus, esto por su comportamiento, pero realmente no lo es, pues su función principal no es destruir, eliminar o deteriorar el sistema, sino que con este sistema el delincuente lo que hace es encriptar toda la información que se tiene al interior del equipo tecnológico o de computo, para luego pedir a cambio una fuerte suma de dinero, casi siempre solicitan no dinero efectivo de la moneda corriente, sino dinero virtual (criptomoneda), por su facilidad de ser intercambiada por el mismo medio y más difícil aun su rastreo. por lo general esta situación se presenta, afectando grandes empresas o pequeñas empresas, con una gran posibilidad de crecimiento, es cierto que el porcentaje es aparente mente bajo, pero es el 12% de la muestra, pero también se debe tener en cuenta que esto afecta básicamente a personas jurídicas, a las cuales ya nos referimos anteriormente.

15. De la muestra de población cuantas tienen indiciado 15 de 50



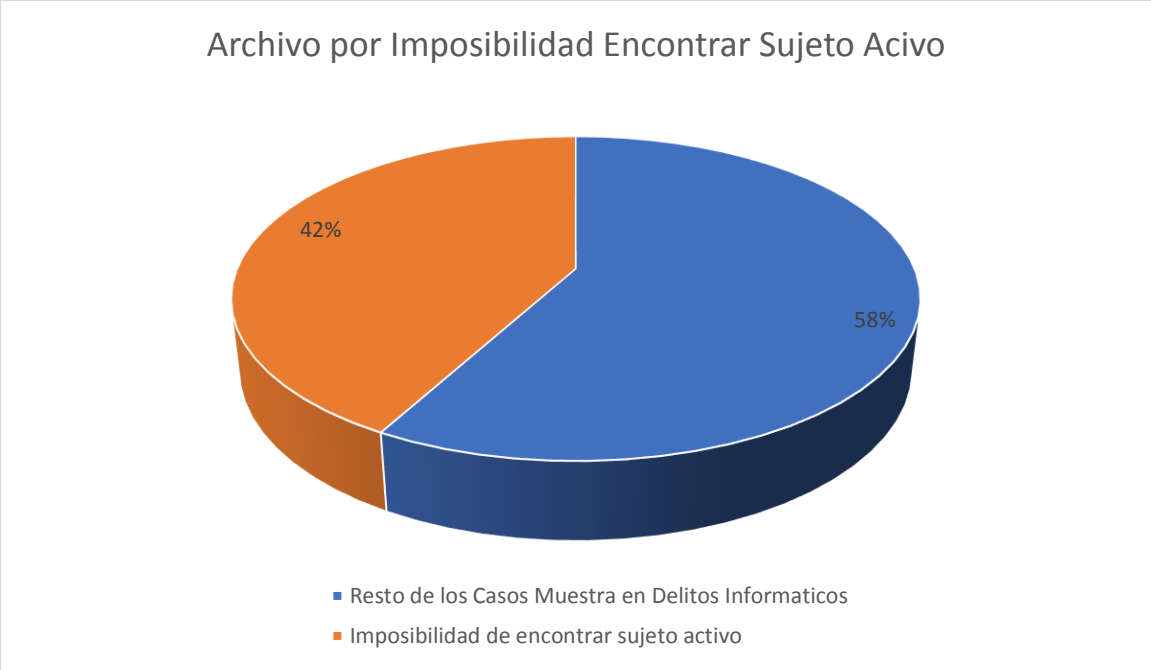

Lo que se pretende demostrar con esta gráfica, es la poca identificación del sujeto activo en este tipo de procesos, ya que como vemos en esta estadística es solo el 30% de la población mostraría, lo que considero muy copo; pero esto se debe a muchos factores los cuales en su gran mayoría se han analizado a lo largo de este trabajo, pero por ahora y como lo vimos en una gráfica anterior también obedece a el escaso aporte probatorio y colaboración por parte de las víctimas y d aquellas personas encargadas del tratamiento de la información, pues en muchos casos cuando se solicitada la misma, ya no existe gracias a lo volátil de la información y al

16. En qué porcentaje de la población de denuncias por este delito son archivadas 43 de 50



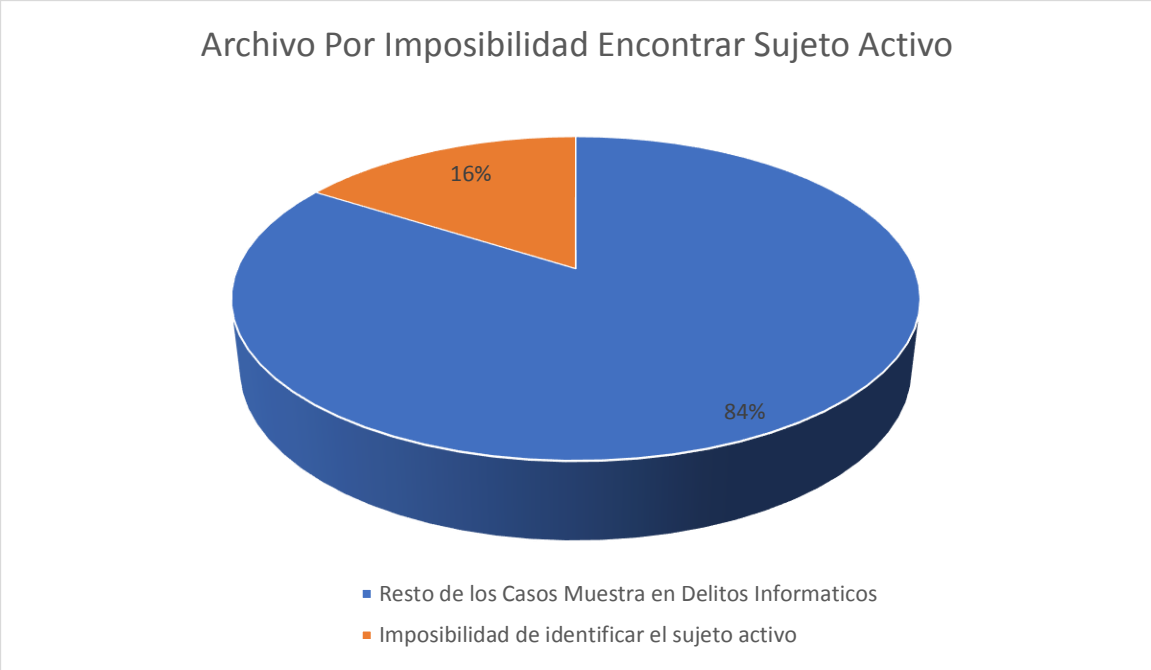

Cabe decir que desafortunadamente y como se hizo mención en la gráfica anterior por muchas razones, pero sin duda alguna la más importante y representativa es la falta de conocimiento, abonado a esto, está la falta de interés en situaciones que debemos prevenir a futuro, pero nosotros estamos acostumbrados a actuar de forma mediata y vivir el día a día, esta es la principal razón que nos lleva a ver como el 86% de la población, en la muestra refleja la cantidad de procesos archivados por falta de elementos con vocación probatoria, son procesos que “nacen muertos”.

a. Imposibilidad de encontrar sujeto activo 21 de 50



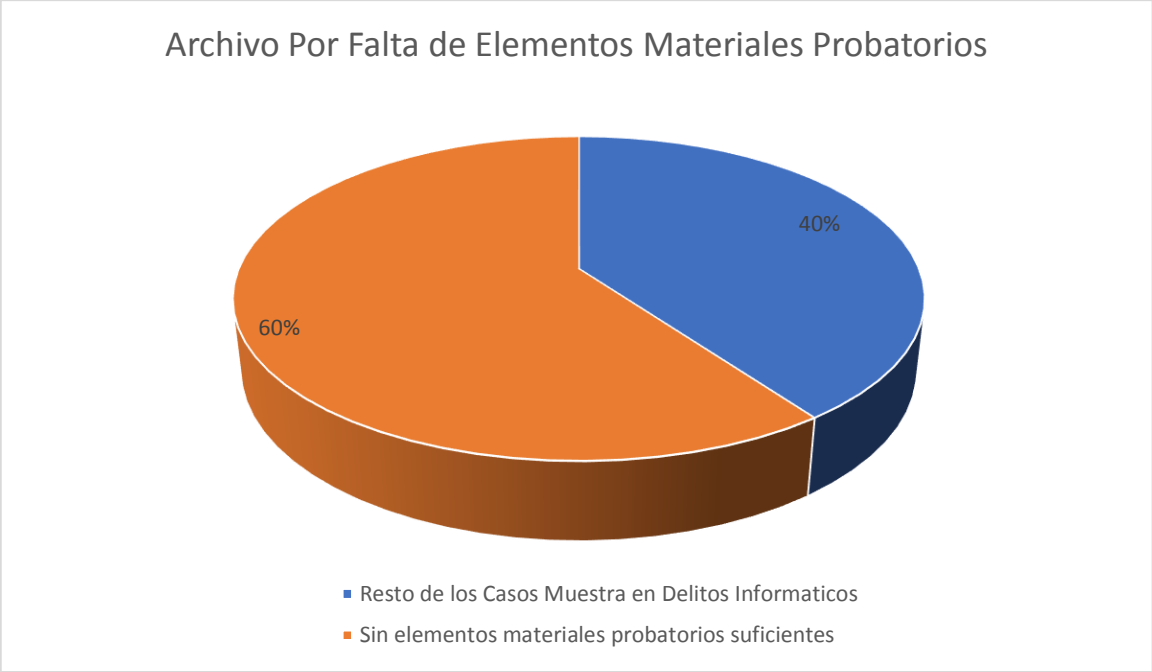

Esta grafica como las otras dos siguientes son unas variables de la anterior, la pretensión con la misma es demostrar uno de los factores que más incide en el archivo de las diligencias, que para este caso es del 42% de la población muestracional, el cual, en mi concepto es bastante alto, los factores que en esto inciden son, la misma naturaleza del delito el cual se presta a que no haya presencia física, sino que todo sea a través de los medios tecnológicos y la falta de precaución y conocimiento al no conservar los elementos con vocación probatoria, ya sea en lugares y de la forma adecuada o por una mayor extensión de tiempo.

b. Imposibilidad de identificar el sujeto activo 8 de 50



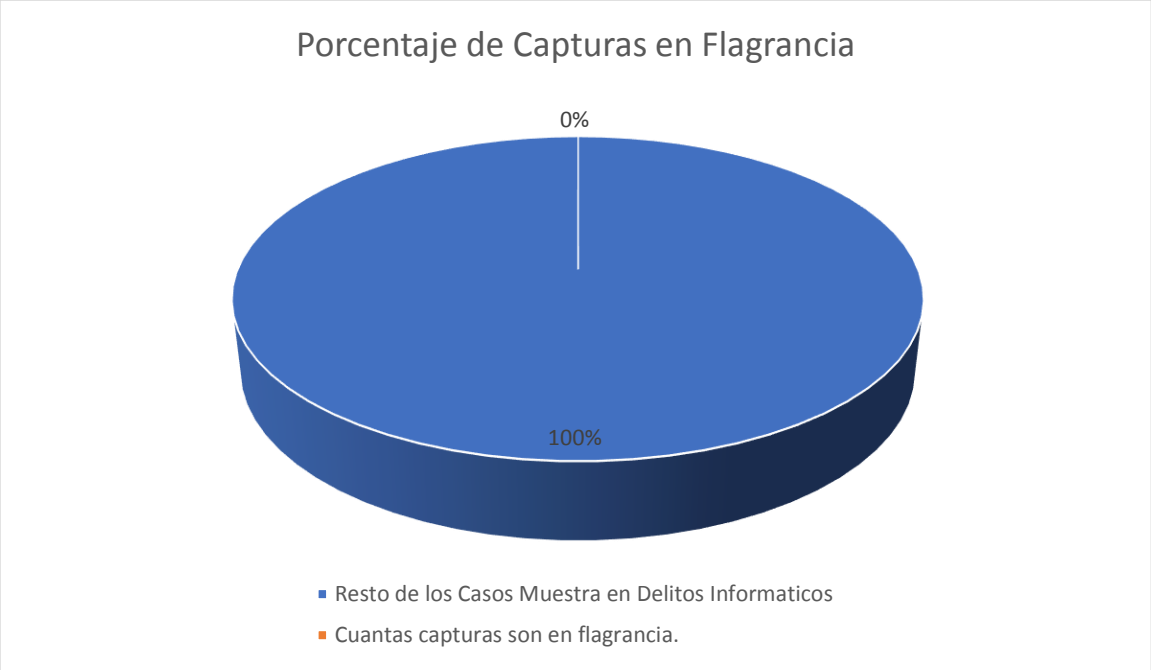

Continuando con esta línea, en algunos eventos se logra obtener elementos von vocación probatoria, tales como videos o imágenes fotográficas, tomadas en los cajeros electrónicos, por ejemplo, pero no es posible la identificación del sujeto activo, pues aún no se cuenta como en algunos otros países, con sistemas de reconocimiento facial, razón por la cual estas indagaciones no se pueden continuar y es por esta razón que dicha estadística nos refleja un 16% de la muestra, con relación al archivo de dichos procesos.

c. Sin elementos materiales probatorios suficientes 30 de 50



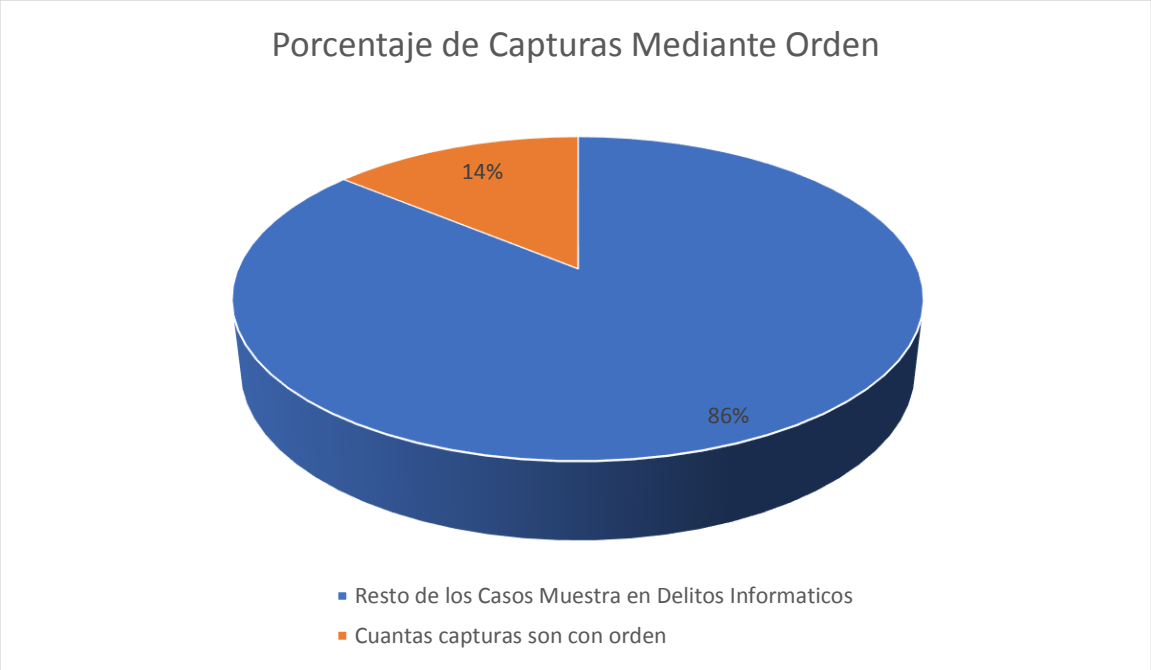

Esta grafica es otra variable, la cual de una forma indirecta se une a la del archivo por la imposibilidad de encontrar el sujeto activo, la cual cuenta con un porcentaje de 60%, el cual es bastante elevado, esto gracias a que en la gran mayoría de los casos no se cuenta con elementos con vocación probatoria y es por qué no se cuenta con el personal idóneo y capacitado en la recolección y tratamiento de la información, sumado a esto, está la falta de celeridad en que se actúa, la falta de convenios o colaboración, entre muchas otras cosas más que no permiten acceder a dichas evidencias de manera oportuna o eficaz.

17. Cuantas capturas son en flagrancia. 0 de 50



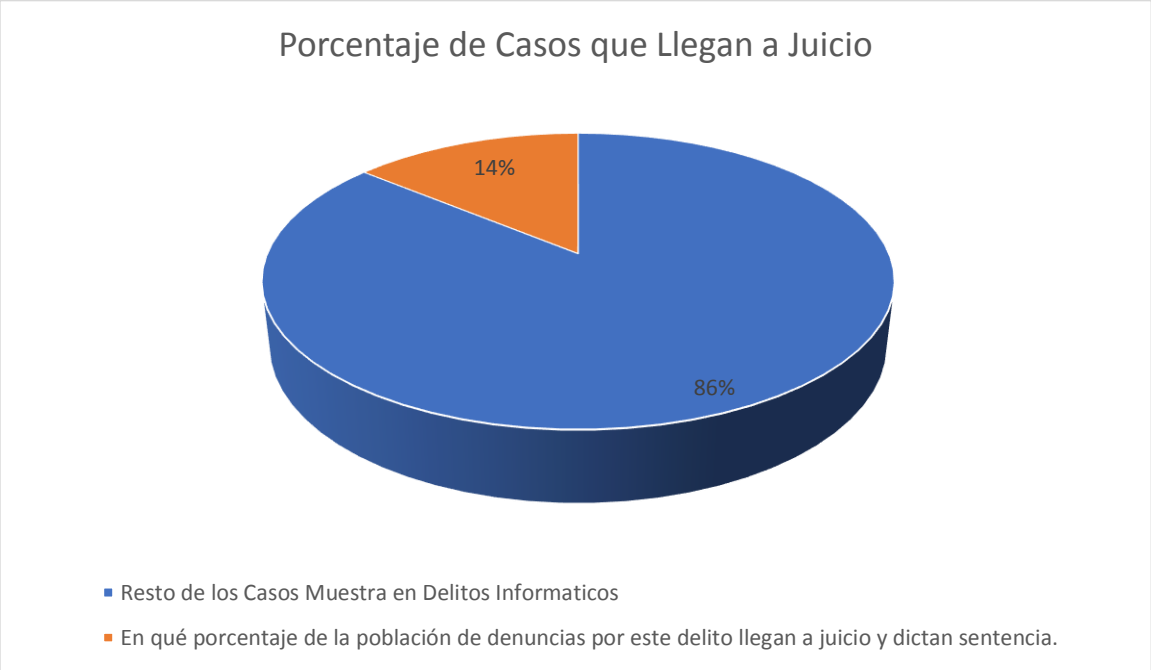

La importancia de esta grafica está en su mismo resultado, el cual no quiere decir que nunca se dé la flagrancia para este tipo de procesos, no, a pesar que la muestra poblacional escogida nos refleja el 0% de capturas en flagrancia la experiencia nos indica que si ha habido algunos eventos en que se ha presentado, pero esto se ve menguado a que la gran mayoría de las veces estos sujetos son dejados en libertad por el desconocimiento de todos los operadores judiciales e incluso de la policía judicial, que frente al desconocimiento de ciertas herramientas, elementos y hasta del manejo del tipo penal, para estos la mejor opción es dejarlos en libertad. Por ejemplo, es el caso de las clonaciones.

18. Cuantas capturas son con orden 7 de 50



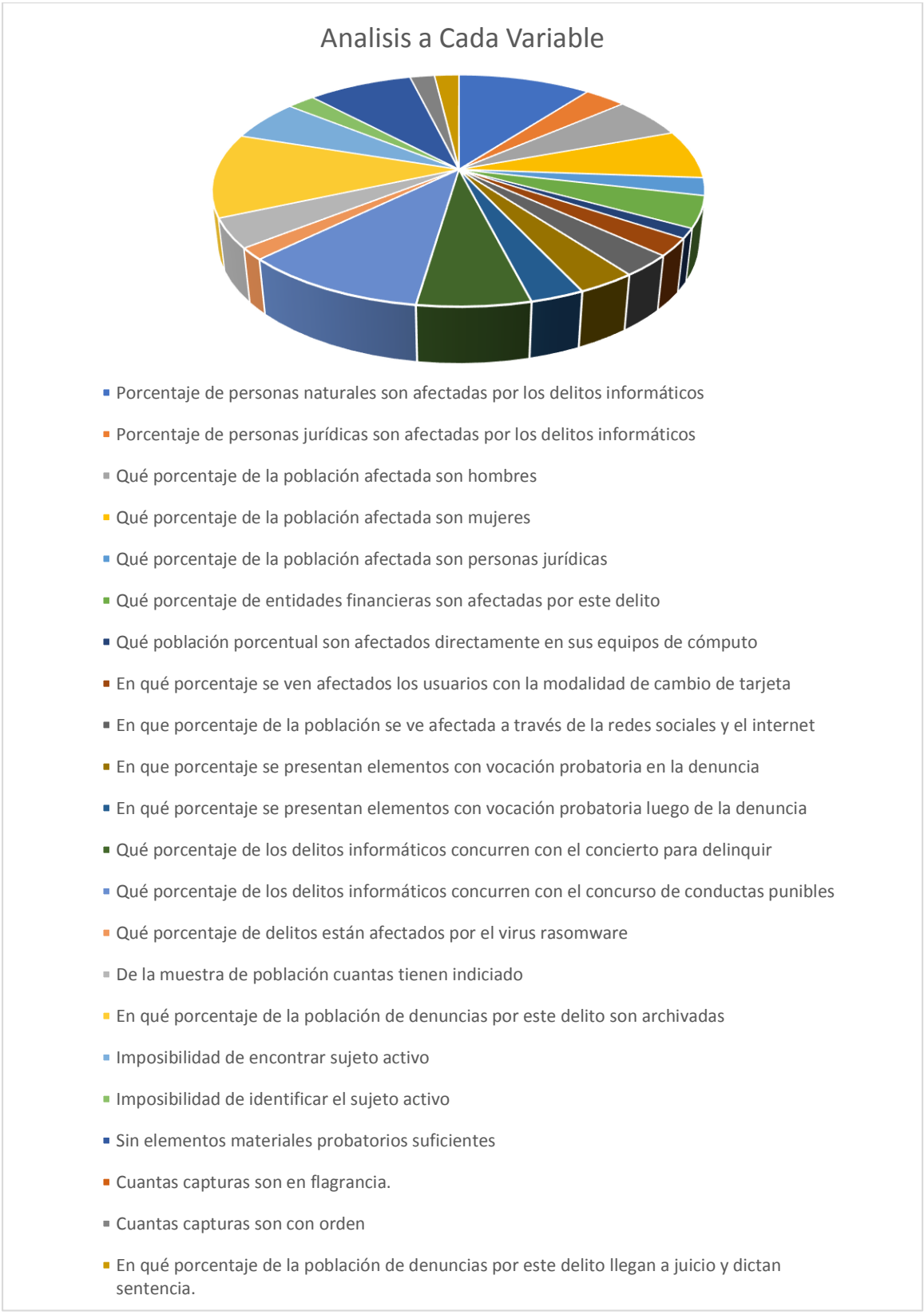

Con esta grafica podemos ver que no todos los procesos que hasta la fecha se viene adelantando por parte de los operadores judiciales quedan impunes, si bien las grafica nos muestra un 14% de la muestra han contado con elementos suficientes al menos para solicitar la orden de captura de unos posibles responsables de conductas reprochables bajo el entendido de los delitos informáticos, ya sea por afectaciones a entidades financieras o a personas naturales.

19. En qué porcentaje de la población de denuncias por este delito llegan a juicio y dictan sentencia. 7 de 50




Si bien es cierto esta grafica tiene estrecha relación con la anterior, pues ambas tienen un porcentaje igual del 14% de la muestra, pero esto no siempre es igual, en este caso fue coincidencia, ya que en algunos casos se logra identificar al sujeto activo de la conducta típica y antijurídica, pero por la falta de elementos con vocación probatoria e incluso falta de denuncia, no se logra llegar a este fin, en el caso en cuestión son hechos que se logran adelantar y que gracias a la colaboración de algunas entidades, se ha podido adelantar con éxito la investigación hasta llegar a juicio y demostrar su responsabilidad, en otros casos con la terminación anticipada, como el preacuerdo o la aceptación de cargos, lo que no implica el llegar a la etapa probatoria.

## Análisis general



Ahora bien, a manera de reflexión frente al análisis presentado, puedo manifestar que muchos de los procesos no tienen buen fin o al menos el fin esperado por las victimas que acuden ante los representantes del estado para que avoquen y en cierta forma les protejan sus intereses, como es el deber ser. Ya que inicialmente no se cuenta con los recursos necesarios que este tipo de delitos exige, además y lo más importante el desconocimiento frente al manejo concreto del tipo penal y más aún del acervo probatorio, ya que muchos de estos delitos como se manifestó en uno de los esquemas no hay flagrancia efectiva, ya que así sean retenidos en el momento del aparente hecho, las autoridades desisten de su legalización, ya sea por el desconocimiento del tipo penal en que se puede enmarcar o porque se desconoce el tratamiento para el mismo, razón por la cual en muchos casos a lo máximo a que llegan es a incautar los elementos y dejarlo en libertad. Así de esta forma se ve en muchos otros casos como el de los virus, la encriptación de la información, que se deben solicitar el apoyo a otras entidades nos solo gubernamentales (oficina de asuntos internacionales) para poder hacer un puente de comunicación y donde muchos de los delitos son operados desde plataformas internaciones. Todo este trámite dilata los procesos y abonado a esto no dejan de ingresar más y más denuncias, cada día.

Considero que estas son unas de las circunstancias que hacen que por ahora muchos de estos delitos sean archivados como mínimo y queden impunes.

# Capítulo 3

## 1. Análisis de resultados.

Confrontando todo a lo que me he referido anteriormente, con los análisis, comentarios y referencias de otros autores que han presentado su postura respecto al tema, puedo decir que; en el desarrollo de esta investigación se ha hecho necesario indagar a cerca de un sin número de definiciones, las cuales son necesarias para abordar con mayor exactitud y precisión el tema en cuestión razón por la cual lo dividiremos en dos subtemas, para así poder hacer un análisis más completo del tema; primero hablaremos de una **aproximación conceptual**, debiendo iniciar por definir la diferencia entre información y datos, según Suarez Sanchez (2106), pues si bien es cierto hablar de datos es hablar de una representación simbólica, ya sea en forma numérica, alfabética, algorítmica, etc. Pero para nuestro caso nos referimos a signos, dibujos o cualquier símbolo que represente una descripción e incluso un señalamiento, un hecho o situación, que se percibe a través de los sentidos; Pero cuando hacemos referencia a la información, decimos que en la mayoría de casos debemos de asociar los datos para así convertirlos en una información, es lo que sucede cuando los ponemos de forma agrupada y estructurados, para así poder obtener una estructura conceptual ordenada del pensamiento. Es aquí donde hacemos hincapié para el otro subtema a abordar y es el de la **contextualización teórica**; pues según los conceptos recopilados de diferentes autores los cuales nos hacen ver la necesidad de tener muy claro los conceptos y así hablar un mismo idioma, pues ahora bien, la agrupación de datos la cual se nos va a ver reflejado en una idea de un hecho ocurrido o un fenómeno, de acuerdo con el orden que genera nuestro procesador mental: conjunto de datos, procesamiento de los mismos, de forma adecuada y en el contexto determinado, representación o imagen, causando un efecto tal y como refiere Suarez Sanchez (2106). Pero si bien es cierto la sumatoria de estos datos, luego de generar cierta información no implica que esta, sea un concepto único y que no dé pie para generar otro tipo de hipótesis fáctica de un hecho ocurrido.

Luego de identificar la diferencia entre dato e información, podemos referirnos a la definición de evidencia digital (Cano martinez, 2010) “aquella información o rastro hallado en un medio informático de la tecnología y la comunicación, el cual puede ser utilizado dentro de un proceso legal como medio probatorio, siendo esta la materia prima, para demostrar la existencia o inexistencia de un hecho”.

Es así, como de esta forma da pie para poder hacer referencia a lo que he considerado como base del problema planteado. la información que se ha logrado recopilar a través de una serie de datos, obtenidos a través de los medios tecnológicos o de la comunicación, convertirlos en información relevante al proceso y llevados como una evidencia digital, ahora bien, la separación de conceptos. de forma cronológica lograra resolver la problemática inicial, de igual forma es necesario saber que pretendemos proteger como bien jurídicamente tutelado y vulnerable, para esto he traído a colación la obra de (Grisales Pérez, 2013) “la legislación penal recoge ese grupo de faltas a través de las cuales se puede vulnerar un determinado bien jurídico, ya sea la vida e integridad personal, el patrimonio económico, la dignidad humana, etc.” De esta forma se confirma el interés de nuestros legisladores, por tratar de  regular la problemática se presenta y afecta los distintos bines jurídicos que deben evolucionar en la misma forma que la sociedad y la globalización lo exige, al igual que la falencia existente frente al manejo de la evidencia, pues es claro que el operador judicial ha tratado de pasear la legislación por los diferentes tipos penales, vinculándolos como delitos perpetuados a través de un medio que es la tecnología y la comunicación, lo ha hecho directamente frente a los delitos contra el patrimonio económico como bien jurídicamente tutelado y dejando de lado otros bienes como el de la vida, la libertad e integridad personal, la dignidad humana, peculado, extorsión, etc.

Debemos tener en cuenta que estamos en el desarrollo de un tema relacionado con la evidencia digital y que gracias a esto se debe tener en cuenta lo delicado de la información y el manejo de la misma, es necesaria saber que es un análisis forense,

tal y como nos refiere, (Rifà Pous, Sierra Ruiz, & Rivas López, 2009, pág. 9) “El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad”.

Incidente de seguridad, son todas aquellas acciones beligerantes que afectan a una sujeto determinado, en algunos de sus bienes jurídicamente protegidos e incluso personas jurídicas, las cuales pueden ver más afectado o comprometido su estabilidad económica e industrial, con la fuga de información confidencial, pero para esto existen una serie de programas y métodos que pueden ayudar a la prevención, o en el caso que nos interesa a detectar una serie de datos muy importantes tales como: la clase de ataque, desde donde se realiza el ataque, como es el ataque, quien lo perpetua y cuáles son las evidencias o rastros dejados; para detectar todo esto, también se debe tener en cuenta los tipos de sujetos que realizan este tipo de acciones, ya que no siempre es a través de personas altamente calificadas, sino que incluso desde la llamada ingeniería social, por las redes sociales, cuentas de correo personal, clonación de medios electrónicos o de comunicación, etc., no requieren equipos altamente sofisticados, sino que gracias a la evolución de la tecnología, con simples programas de software, acceden a la información necesaria o gracias a la información que nosotros dejamos, aun existiendo algunas normas que supuestamente protegen la información, autorizamos su tratamiento. Una vez detectado el incidente que se debe hacer y son recomendaciones que nos hacen (Rifà Pous, Sierra Ruiz, & Rivas López, 2009), algunas de ellas y dependiendo del caso, apagado del equipo, fijación de las partes del equipo recolección o extracción de las memorias, realizar las copias del caso a dichas memorias, etc.

De esta forma llegamos a un tema muy delicado y es cualquier persona está en capacidad de realizar dichos actos, no solo en cuanto a la recolección de la evidencia digita, sino también del análisis forense y la elaboración del informe de

dicha evidencia. Como refiere (Rifà Pous, Sierra Ruiz, & Rivas López, 2009, pág. 28) “La redacción del informe es una tarea ardua a la par que compleja, porque no sólo hay que recoger todas las evidencias, indicios y pruebas recabados, sino que, además, hay que explicarlos de una manera clara y sencilla. Hay que tener en cuenta que muchas veces dichos informes van a ser leídos por personas sin conocimientos técnicos y obviamente tiene que ser igual de riguroso y debe ser entendido, con lo que habrá que explicar minuciosamente cada punto.”

Esto sin tener en cuenta que no hablamos de un informe técnico o pericial, porque si bien es cierto anteriormente hacíamos referencia a una ingeniaría social, pero esta fase probablemente nos lleva a pensar, más allá de nuestra cuenta de Facebook, e Instagram, entre otras. Pero este flagelo se ve en situaciones más graves o de mayor envergadura y es cuando vemos a grandes empresas criminales utilizando este tipo de medio para alcanzar sus objetivos y más aún cuando son naciones las que perpetúan ataques utilizando los medios de comunicación o la tecnología, con fines bélicos, entonces es aquí cuando nuestra legislación y nuestra forma de ver las cosas tiene que ser con una mentalidad más amplia que de lo que estamos acostumbrados a ver como pequeños actos beligerantes, sino como cibercrimen o ciberdelincuencia, temas que ya están siendo tratados a nivel mundial y nosotros no podemos ser ajenos a esto como nos lo hace saber (Rincón Ríos & Naranjo Duque, 2011, pág. 249) **“a) Delito cibernético en sentido estricto (“delitos informáticos”):** Todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y de los datos procesados por ellos;
**b) Delito cibernético en sentido lato (“delito relacionado con computadoras”):** Todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos información por medio de un sistema o una red informáticos.”.

Gracias a las grandes dificultades que se presentan para poder detectarlos, nos lleva a pensar que es altamente necesario el conocimiento y la capacitación

constante para los investigadores, que cuenten con las herramientas y los protocolos necesarios para enfrentar este tipo de actos, no solo es crear normas, sino generar recursos, es así como nos lo hace saber con una serie de alternativas (Cano Martínez, 2009, pág. 218).

Los delincuentes informáticos son una nueva generación de criminales qué, Utilizando sus técnicas naturales en el mundo físico renuevan y afianzan las mismas para producir acciones punibles de mayor Impacto, con alta efectividad en el logro de sus objetivos y limitadas trazas para ser rastreados o detectados. Si bien los crímenes perfectos son difíciles de lograr en el mundo virtual esta teoría se hace menos evidente porque los rastros propios de las acciones de los delincuentes pueden ser y serán alterados, Manipulados, escondidos o eliminados según la habilidad de estos últimos.

En este escenario, Dónde tenemos un enemigo que se mimetiza en los tejidos de las redes de los bits y los bytes, es necesario desarrollar una nueva raza de investigadores, de que se delincuente en medio tecnológicos. este nuevo investigador debe saber que siempre estará a Un paso atrás del atacante, que sus técnicas se podrán a prueba en cada caso y su razonamiento lógico podrá ser controvertido por la constante evolución del atacante para tratar de evadir las investigaciones. Este investigador debe reconocer en el criminal informático un blanco móvil, Generalmente invisible y altamente técnico que hará que sus técnicas y procedimientos se actualizan constantemente y se ajusten, según la realidad de la inseguridad en la tecnología de la información y Comunicaciones.

Gracias a una serie de conceptos teóricos analizados hasta el momento podemos decir que se hace necesario afianzar y hacer general los conceptos teóricos y prácticos para así poder hablar un solo lenguaje en el momento de referirnos a una prueba bajo el concepto de evidencia digital, además que como una enorme y principal dificultad que hasta el momento encontramos y de acuerdo con Cano Martínez (2009), al referisce en la necesidad de capacitar no solo a los

investigadores sino a todos los intervinientes en un proceso de indole de evidencia digital, pues una de las grandes dificultades que hasta el momento se ha logrado vivenciar el la divergencia teorica y que podria mejorarse a modo de propuesta es tratando de unir conceptos y estandarizando unos protocolos adecuados para dicha problemática.

Pues si bien viene sindo cierto, no se pude desconocer la el *principio de transferncia.* El cual no es otro asi como el trabajo criminal en un dlito comun requiere la presencia fisica del mismo y asi de esta forma deja rastros o huellas fisicas, en los delitos informaticos, no existe la presencia fisica del sujeto activo, sino la trasmision de datos, emisiones electromagnatica, es decir la manipulacion de un medio tecnologico o telematico, como lo hemos venido avisorando.

Si bien es cierto en nustro pais existe la libertada probatoria, la cual se encuentra debidamente regulado en nuestro codigo e procedimento penal ley 906 de 2004, pero esta librtad probatoria es de manera parcial ya la evidencia digital no es aceptada o no puede ser introducida como prueba si y solo si esta acompañada d un “experto” perito, es en tonces que no podemos decir que es una evidencia autonoma y es asi como en vez de ser tomada como una evidencia digital mas bien es aceptada desde su tratamiento como una evidencia fisica tal como refiere (Maria, 2013), de igual forma vemos la necesidad de que los operadores juricos conoscan mas del tema, como lo emos venidoinsitiendo a lo largo de mis comentarios, pues la doctora maria elneser (2013), da cuenta de ellos en su libro de investigacion “la aproximacion a la informatica forense y el derecho informatico, Ambito colombiano”, cuando hace una serie de tabulaciones demostrando el grado de aceptacion y de conocimento que existe en nustro pais con relacion al tema. Es asi como nos da pie para fortalecer nuestra teoria, pues esto es solo desde la infromatica forence, ahora bien en la parte probatoria si que hay mas falencias.

Tema muy preocupante no solo para nosostros sino para muchos paices, donde hasta la misma corte biene hacendo fuertes pronuinciamintos respecto al temas

como es el caso de la “sentencia de la sala segunda del alto tribunal en españa STS 300/2015 19 de mayo” (Alfonso, 2015), el cual confirma que todo medio de prueba es una comunicación bidireccional y que por ende puede ser manipulado o alterado, razon porla cual traslada la carga probatoria a la parte que la presenta, demostrando su autenticidad como todo medio de prueba, esto gracias a las politicas mundiales, en proteccion del medio ambiente y la ecologia, razon por la cual se aprovecha la tecnologia y se sta eliminaddo de forma gradual la utilizacion del papel, lo que nos llevaria a la implementacion o utilizacion de nuevas herramientas, y para esto nos debemos ir preparando, pues esta es una realidad factica y a corto plazo.

Es de esta forma que debemos estar atentos a la implementacion de la evidencia eleectronica, pues si ants enviamos cartas, memoriales, ahora los estamos cambiando por mensajes de texto o correos electronicos.

Es asi como entramos en un concepto no desconocido por nosotros y que desde inicio de este nuevo siglo se biene referenciando por todas parts y es la *la era de la globalizacion,* la cual nos exige una cambio, una trasformacion no solo en nuestra forma de actuar sino en la forma como opera nuestro sistema penal, el cual ya no debe ser articulado para nuestro entorno social y cultural, sino que debe transender fropnteras y ajustarse a una cultura internacional o trasnacional, de sto damos cuenta en las transacciones comerciales, pero que lo hace posible todas y cada una d las herramientas que aparecen en el mercado respecto a la tecnologia, las cuales permiten y hacen mas facil el contacto con otras personas sin importar la distancia, la fecha o zona horaria.

Pero bueno como refiere (Alejandra, 2010), cuando referencia que “esto no es nuevo para nuestro siglo ya que desde el siglo anterios ya desde 1982 en colombia se ha tratado de regular frente al tema, es asi tambien que vemos la ley 527 de 1999”, donde tratan de regular las formas de comercio lectronico, pero no se le ha prestado la suficiente atencion y solo hasta ahora nos estamos dando cuenta d la necesidad de ser mas operativos en el tema, pues inicial mente era solo una forma

de comunicación informal pero ahora vemos que no es solo eso sino mas bien una herraminta fundamental y que tiene la misma importancia o valides que el papel en su defecto, es por esto que nuestra legislacion no solo debe hacer adaptaciones en relacion al derecho comercial, civil, sino en el caso del derecho penal y mas en su parte procesal, pues asi como todo cambia y se transforma la capacitacion de los delincuentes e incluso com haciamos referencia anterior mente, sin ninguna mala intencion, desconociendo la parte volitiva del sujeto activo este solo por curiosidad ingresa a lugares descnocidos que puden llegar a afectar grandes e inportantes plataformas tecnologicas, pero sinedo muy insisivos en el tema esto como lo podemos contrarestar, no solo con prestarle atencion, crear mas y nuevas leyes, sino tambien con brindar buenas capacitaciones y con la coperacion internacional.
Es importante tener en cuenta que para el tema en cuestion, su parte principal esta en el analisis forense, dentro del cual esta recopilada la informacion mas importante, pero para este se hace ncesario saber el almacenamiento, el trataminto que debe recibir, la forma de extrer la informacion y de que forma se debe hacer, esto con el fin de sostener la autenticidad, asi como conocer unos terminos esenciales en este tipo de temas. Estos son temas y lenguajes que se deben hablar a nivel mundial e incluso no solo entre los operadores judiciales, sino en el publico en general.

De una forma muy placentera, descubri, cuando me introduje en la investigacion de este tema y fue haber encontrado como con el tema de la globalizacion se ha tratado este tema en otros paices como ecuador por personajes muy importantes y no menos influllentes en ese pais como es el caso del señor fiscal acurio del pino santiago (2009) quien, se ha manifestado frente al tema crando un discreto manual para el tema en cuastion lo que deenota la gran preocupacion que se tiene en todas partes del mundo, asi como ya lo habiamos mencionado dese la corte española, la fiscalia de cuador y hara nosotros estamos legislando y tratando de brindarle la importancia que se merece y que ademas nos exige para enfrentarnos a la dinamica delictiva que hoy nos preocupa a todos los paices, y mas que eso es la dinamica probatoria como manifista (Pino A. d., 2009), "*La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis*

*o afirmación precedente, se llega a la posesión de la verdad material*.", que hace una muy buena referencia entre la evidencia electrónica y la evidencia digital, ya que la una refiere a los componentes o partes del equipo electrónico (hardware) y la otra hace más referencia a el componente no físico, sino operativo del mismo. En la parte de programación (software), es por esto entonces que decimos que evidencia digital es cualquier mensaje de dato, almacenado y tramitado por medio de un sistema de información que, a través de campos magnéticos e impulsos electrónicos trasmiten una información. Y en el caso de la evidencia electrónica, podemos darnos cuenta que la ilicitud puede ser desde la compra y venta de insumos o partes no licenciadas o reproducidas ilegalmente, hasta la compra y venta de elementos no permitida su comercialización.

Por otra parte, podemos decir que la evidencia digital es lo más delicado, ya que por no ser algo tangible se hace más difícil su recolección y almacenamiento, para lo cual se debe contar con una experiencia muy amplia y un alto grado de conocimiento, además de que se reitera una enorme capacitación en el tema ya que como se mencionaba antes este puede ser muy volátil, lo que indica que se puede perder muy fácilmente y de esta forma el proceso se puede decir que "nació muerto", pero esta expresión no solo se aplica en ecuador esta expresión es a nivel mundial, en todos y cada uno de los países que de una u otra forma se ven involucrados con el tema de los delitos electrónicos, es claro que debemos manejar un lenguaje común, claro y sencillo, pues así de esta forma se nos facilita la colaboración internacional ya sea por solicitud o por respuesta.

Quiero resaltar la importancia de dicho manual el cual podría ser replicado todos los países, así como en el nuestro a nivel de tema de capacitación para los operadores judiciales, pues el manejo de la terminología es muy fácil, adecuado y sencillo.

Para nuestro pais de be ser igual de importante y realmente mevos aque si lo viene haciendo al prestarle importancia atraves d la normas creada, pero consideroq uqe se a quedado algo corto pues no le ha prestado la suficiente importancia en realcion

al tema del analisis forense, pues su gran invesion la ha realizado solo en tres crandes ciudades, aunque diriamos principales, como son bogotá, cali y medellin, donde existen grandes laboratorios forences para el analisis de este tipo de eventos, pero su gran falencia esta en la falta de personal y mas la capacitacion del mismo. Para esto es importante saber y distinguir que es el analisis forense digital, se refiere al estudio sistematico, extensivo y profundo, de un equipo, medio informatico o telematico,on el proposito de extraer la informacion que alli repose, sin dejar de lado la aplicación de los protocolos, con el fin de encontrar rastros o huellas dejadas en el sistema, asi como lo vemos en una escena del delito comun, con el fin de identificar el autor, autores o complices, ya que si bien es cierto hemos podido detectar que este tipo de delitos, no solo esta el sujeto activo detrás de un equipo tecnologico, sino que tambien se encuentra toda una organización criminal (son los delitos del futuro), este analisis forense digital tiene nos solo una ventajas, sino tambien unas grandes desventajas, como lo manifiesta (Torres Moncada Martha Liliana, 2016) “Para desarrollarla es necesario contar con programas que permitan la detección de la intrusión realizada al sistema, Es estrictamente necesario contar con un equipo de trabajo preparado y entrenado para desarrollar el trabajo de manera efectiva”; pero al igual que esto se hace necesario contar con equipos muy robustos en cuanto a la capacidad de procesamiento de datos, además que deben ser altamente protegidos y contar con personal muy calificado en el manejo del mismo, reiterando la insistencia. Así de esta forma nos da pie para hacer referencia al manejo de la evidencia electrónica, a la que hemos hecho referencia anterior mente y que también es muy importante pues es en esta donde se almacena, aloja conserva o se procesa la evidencia digital y que en muchas ocasiones no se hace necesario someter a cadena de custodia o al tratamiento de los protocolos para el análisis forense, sino única y exclusivamente el componente electrónico (hardware) donde está la información o los rastros buscados. Esta evidencia digital puede presentar una serie de problemas para su aceptación, la cual no es solo la carencia normativa en cuanto a su parte procesal, sino el manejo o estandarización de protocolos que sean mundialmente aceptados y conocidos por todos los operadores judiciales así como el público en general, al menos lo as elemental, iniciando desde

los mismos conocimiento de que es un incidente de seguridad informática, el cual lo expresa de una forma muy clara (Torres Moncada Martha Liliana, 2016) "*cualquier evento anómalo que pudiese afectar la Seguridad de la Información, que comprende la pérdida de la disponibilidad, integridad o confidencialidad de la misma."* Es importante resaltar que este tipo de eventos no solo se presentan en quipos de computo, sino en cualquier equipo tecnológico, tales como los celulares, las Tablet, los relojes Smart, todos aquellos quipos que tengan directa o indirecta relación con la trasmisión de datos.

Es de esta manera que nos referimos a los delitos informáticos como refiere (Cortes Botero , Ballen Rojas, & Duque Montes, 2015) "*toda conducta punible, es decir típica, antijurídica y culpable señalada por el legislador; haciendo uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computarizada, como método, medio o fin que menoscabe, mengüe o ponga en riesgo el bien jurídico de la información y de los datos; además que con ocasión de ellos en circunstancias específicas se pueda afectar otros bienes jurídicos como la vida, la libertad, la familia, el patrimonio, la seguridad pública y la seguridad del Estado…"* evidentemente vemos como a través de estos sistemas si se ven altamente afectado no solo el patrimonio, sino la intimidad, la vida, la seguridad publica entre otros, lo que de una u otra forma nos obligan a involucrar cada una de las disciplinas que atañen con el tema como es el caso de la criminología, dentro de un marco de delincuencia no convencional, por la calidad de conocimiento que este debe de tener con relación al tema, es así como vemos el incremento y proliferación ofensiva de esta nueva forma de criminalidad, como lo manifesté anteriormente por las misma facilidad de enmascararse y la no necesidad de entrar a afectar más de lo que él quiere sin generarse un mayor riesgo en su actuar, más aun en su persecución, procesamiento y juzgamiento no se hace bajo el deber ser, sino bajo el conocimiento del actuar común, esto significa la adecuación típica de estos delitos en delitos comunes y si estos no encajan son dejados en libertad o su pena es mínima, como trataremos de demostrarlo en el analisis técnico de este trabajo. Es así que bajo esta gran preocupación el estado

colombiano crea un documento COMPES 3701 DE 2011, al cual hace referencia (Torres Moncada Martha Liliana, 2016) "*Lineamientos de política para Ciberseguridad y Ciberdefensa" este documento se creó con el fin de plantear una política Nacional de Seguridad Digital, vinculando a todos los actores de interés como gobierno nacional, entidades Públicas y Privadas, la academia y la Seguridad Social, en vista del aumento del uso de la Internet y la digitalización de los procesos en las organizaciones"* al igual que el que fue creado en el año 2016, es así como pretendo demostrar que nuestra legislación se ha esforzado en atacar este tipo de delitos como es el caso de la ley 527 de 1999, de la cual ya había hecho una pequeña referencia de la misma pero voy a ahondar un poco en ella tocando apartes muy puntuales.

Esta ley hace especial énfasis más que en su parte procesal es la norma sustancial y más en materia comercial y civil tal como ella misma refiere (Republica, Congreso de la, 1999) "*Por medio de la cual se define y 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 y se dictan otras disposiciones"* , pero que a su vez puede ser aplicable a otras legislaciones como es el caso del derecho penal, pero que muy a pesar de que nuestro operadores judiciales y legisladores la conocen, existe un enorme temor en su aplicación, tal vez por el mismo desconocimiento de los términos y el manejo tan amplio que aparentemente se tiene frente a la tecnología, en muchos casos hemos oído la expresión "nos atropella la tecnología" pero no solo es la tecnología sino todo lo que de ella se deriva, pero es más por el temor mismo a enfrentarnos y a creer que las cosas sean posible como es el caso de la autenticación.

Algo muy importante que resalto de la misma es la definición de mansaje de datos, toda información procesada por medios electrónicos o telemáticos. Pero si bien es sierto considero que es una definición demasiado amplia, la cual puede o debe ser ajustada a cada caso en concreto y más si se pretende llevar como medio probatorio para sustentar una evidencia digital o evidencia electrónica.

Pero esta norma lo más importante es que tiene un carácter vinculante como me refería anteriormente, al igual que una gran fuerza probatoria, a partir del entendido que sea aceptado por los operadores judiciales con la demostración y aceptación científica de cada proceso realizado con los protocolos y personal capacitado.

Continuando con la línea de aciertos normativos por parte de nuestra legislación encontramos la ley estatutaria 1581 de 2012, la cual refiere (Republica C. d., 2012) "*Por La Cual Se Dictan Disposiciones Generales Para La Protección De Datos Personales*" la cual de igual forma supremamente importante y otro gran acierto de nuestro legisladores, aunque vuelvo a resaltar son normas creadas con mayor énfasis de la protección en materia civil y comercial que en penal, pero reitero son aplicables y tiene la misma fuerza probatoria, aun que toda ella es bastante importante lo que puedo resaltar de la misma, es la regulación al manejo de los datos personales y la regulación a quien la procesas y conservan, norma que ha sido bastante discutida y ha provocado muchos traspiés en materia penal más en cuanto a la solicitud de evidencias digitales o electrónicas, las cuales aún no se pueden ni pedir de esta forma sino elementos materiales probatorios y que así le refiere la corte en su sentencia 336 de 2007, la cual refiere a la búsqueda selectiva en bases de datos, que tengan relación con el hecho investigado, pues bien es cierto que hay información sensible a la cual hace tanto la presente ley como la sentencia "***Artículo 5°. Datos sensibles.*** *Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.*

***Artículo 6°. Tratamiento de datos sensibles.*** *Se prohíbe el Tratamiento de datos sensibles, excepto cuando (…)*" lo que se convierte en un obstáculo en razón a que

algunos operadores o encargados del tratamiento de los datos se escudan en esta norma bajo su interpretación para no permitir el acceso a la misma, teniendo así que acudir ante un juez de control de garantías y congestionando mas sistema judicial. Por lo cual considero que es más un problema de trámite y de ser un poco más claros para así evitar estos inconvenientes. Ya que de esta forma considero que se esta es revictimisando, ya que mientras se hace todo este proceso la evidencia digital se ha perdido y no va a ver prueba en contrario, lo que se ve reflejado en cada estadística mencionada.

En esta misma línea hago referencia a la resolución complementaria 277 de 2014 la cual refiere (Republica C. G., 2014) "*Por la cual se adopta el Sistema de Aseguramiento Electrónico de Expedientes (SAE) y se Regulan Aspectos Relacionados con su Utilización y Funcionamiento*" de la cual quiero resaltar su importancia por la implementación, de la herramienta institucional y de aplicación general ya que con la misma pretende evitar o abolir el uso del papel, y de esta forma darle a la importancia legal y jurídica a los tramites que d esta dependen, es así como implementan y regulan la firma digital al igual que la entrega de copias en medios magnéticos, que para ellos tiene total valides como el original, igual pasa con la firma digital, la cual es tan autentica como la que es plasmada en un papel, claro que es importante aclarar que no es cualquier firma ni plasmada de cualquier forma estos deben cumplir con unos protocolos y atributos para certificar su autenticidad.

De igual forma hacen toda una serie de parámetros entorno a la tecnología y su aplicación adelantándose a la evolución y los medios, pero también es cierto que esto genera grandes riesgos, los cuales aún no alcanzan a dimensionar. Manejando así un paralelo entre lo común y cotidiano con la tecnología.

A nivel personal considero que nuestro más agrande acierto para la legislación colombiana ya que considero que es un gran salto, que nos puede permitir avanzar en materia penal y procesal es la aprobación del convenio de Budapest, mediante

la ley 1924 de 2018 la cual reza (Republica, Congreso de la, 2018) "*por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest*" de gran importancia para nuestro país ya que de esta forma Colombia ingresa en un medio de cooperación internacional, de una forma legítima y donde tendrá el apoyo de país con una cultura muy avanzada y con una experiencia en el campo y la temática superior a la nuestra, dicho convenio tiene unos parámetros muy definidos y establecidos respecto a la delincuencia y como ellos bien la llaman la ciberdelincuencia, así pues Colombia tendrá que adaptarse al manejo de la evidencia digital como lo hacen otros países en el mundo, al igual que debemos recordar que por el hecho de ser un tratado tiene fuerza vinculante y de obligatorio cumplimiento, se espera de esta que así se pueda dar una gran avance en materia procesal y más n el manejo de la evidencia digital, la cual debe ser conocida y aplicada por todos los operadores judiciales, bajos unos mismos estándares y protocolos internacionales.

# Capítulo 4

## 1. CONCLUSIÓN

Quiero resaltar la importancia de tener claro los conceptos y términos que se utilizan para este tipo de temas, ya que son una mezcla entre la informática y el derecho, ya que como lo he mencionado a lo largo de este trabajo, se hace necesario mínimo saber la diferencia entre el dato y la información, algo que aparente mente es muy básico y sencillo, pero que realmente no lo es, pues esto ya se le dio la explicación necesaria y suficiente, pero que de una u otra forma me sirve para poder adentrarme en esta conclusión, con esa pequeña muestra, de esta forma poder demostrar que para todos los operadores judiciales e incluso para la sociedad en general, que no tienen contacto directo con esta problemática, pero que en un determinado momento se pudieron ver afectados, ya sea de una forma directa e indirecta y es por esto que considero que es importante se dé a conocer ampliamente esta tema con todas las dificultades que de una u otra forma he dado a conocer. Tal es el caso de cuando podemos decir que hay una evidencia digital y que está a su vez debe ser sometida a un análisis forense digital, para poder ser llevada a un juicio y que esta sea valorada como realmente es una prueba digital y no que se tenga que cambiar su naturaleza o esencia para poder ser analizada y valorada como un delito común, el cual ya no lo es, realmente es un delito informático o de “nueva generación”.

Debemos tener en cuenta que una de las mayores dificultades en este tipo de delitos, entre muchas, es que no hay una presencia física, no hay un atacante directo o presencial, ya que los hechos son acaecidos aprovechando la red, los sistemas de información o tecnológicos, con lo cual no se hace necesaria la proximidad, e incluso son acciones cometidas desde distintos continentes, afectando así la información de tu empresa, o la información personal, vulnerando la intimidad de las personas, sin ni siquiera tocarlas, este es un flagelo que cada día crece más y como ya había hecho mención no necesariamente son cometidas por

personas expertas en el tema, los mal llamados hackers, no, pueden ser simple curiosos, o jóvenes inexpertos con ganas de divertirse y aprender un poco más, son aquellos mal llamados “gomosos”, los cuales encuentran puertas abiertas en los sistemas, o en las redes y van avanzando. Como también hay otros que si tienen el conocimiento, la experiencia y el ánimo de hacer daño o de obtener provecho del descuido, desconocimiento, de la confianza o de la misma ingenuidad de algunas personas, como es el caso de las publicaciones en las redes sociales, que muchas personas la utilizan como una forma de compartir y conocer personas de una forma “sana”, pero algunos sujetos aprovechas esto para insertar virus e ingresar a sus bases de datos, obtener información no solo personal sino familiar, apoderarse de la información no solo la publicada, sino que incluso de la que poseen en sus discos duros.

Ha pero esto no solo seda a través de la ingeniería social, esta situación la vemos ya a grandes escalas, la cual es denominada cibercriminalidad o ciberdelincuencia, como es el caso del espionaje industrial, e incluso a nivel de estados, de grandes potencias mundiales que se ven envueltas cada día más en este tipo de situaciones, donde ya el medio, no son las personas, sino las maquinas que en muchas partes vemos la expresión, pero el medio que realmente se está utilizando es la tecnología, los medios de comunicación y las redes, los ataques son virtuales es una nueva era, a la cual debemos estar atentos y adaptarnos a ella, esa es mi mayor insistencia, ya que no debemos esperar a que los delitos evolucionen más, pues si bien es cierto los delincuentes se perfeccionan o se especializan en unos delitos específicos, mientras que nosotros los operadores judiciales no lo hacemos estamos inmerso un sin número de delitos y acciones, que no alcanzamos a dimensionar la verdadera situación y que por eso en muchos casos como lo explique en un capitulo anterior, preferimos adaptar un delito informático a un delito común o en el peor de los casos, hacer de cuenta que no pasó nada y ni siquiera la retención, por el mismo desconocimiento, pues en muchos casos cunado estos sujetos son retenidos se eles encuentran en su poder ciertos aparatos (equipos), que son de completo desconocimiento, pero de alta tecnología, tal es el caso de los squimer, datafonos

payasos, escáner, equipos clonadores, etc. Ellos invierten grandes cantidades de dinero en tecnología, pues bien saben que rápidamente la recuperan. pues si ya conocemos de su existencia y de su evolución, por ende, entendemos nuestras dificultades para poder contrarrestarla, lo único que nos queda es aplicarla de una forma adecuada, lo que nos exige, que estemos debidamente capacitados y estar adaptándonos a los cambios no solo desde nuestra norma sustancial, sino a la par con la procedimental.

## 2. **RECOMENDACIÓNES**.

Estas recomendaciones, en gran parte, he sido muy reiterativo y enfático, pues si lo hago de una forma programada y ordenada, debo iniciar, por pensar en organizarnos todos los operadores judiciales y fomentar la creación de grupos de tares con enfoques específicos, como es el caso de una verdadera unidad de delitos informáticos, con diferentes modalidades (especialidad), la cual pueda contar con el suficiente personal, pues si bien es cierto debemos recordar que los delitos están migrando y casi la gran mayoría de los que hoy llamamos comunes se están convirtiendo en delitos, cometidos a través de un medio informático y que para esto se requiere un tratamiento especial, desde la recolección de la evidencia, su procesamiento, custodia, el análisis forense, su presentación o forma de ser llevada a juicio, para que esta sea reconocida como prueba y pueda tener el valor probatorio que se merece. Lo me conduce, más que a una recomendación es una solicitud, para aquellos jefes y directores de entidades, para que tengan en cuenta las necesidades de esta problemática, la cual no solo es el personal adecuado, sino también la capacitación del mismo, y este sería el tema más importante, pues si los delincuentes se capacitan, se especializan en una área determinada nosotros debemos salirle al paso y estar por encima de ellos, ya que somos la representación de un estado, de una sociedad, donde diríamos que somos más. Es por esto que quiero enfatizar en la capacitación de todos y cada uno de los operadores judiciales,

ya que de esta forma podemos contrarrestar estos delitos o todos aquellos que migren al medio tecnológico.

Para esto podemos formar escuelas y con el apoyo de entidades internacionales capacitarnos más, para estar a la vanguardia, pero a esto le debemos sumar, el invertir en buenos equipos los bastante robustos capaz de procesar la información hallada, en el menor tiempo posible pero adecuada, ajustándose a los protocolos internacionales con su análisis necesario y respectivo, para poder ser aportada en un juicio.

En síntesis, que sea requiere para afrontar este tipo de delitos y darles el tratamiento adecuado y necesario: personal adecuado, capacitación constante, con el aprovechamiento de los convenios internacionales y equipos altamente adecuados. Pienso que invertir en capacitación e infraestructura es disminuir los costos operativos y el desgaste humano, que generarían grandes resultados y poder intervenir adecuadamente y en el momento preciso.

# LISTA DE REFERENCIAS


Alejandra, M. R. (2010). *La informatica forense como herramienta para la aplicacion de la prueba electronica.* Bogota: Estudios juridicos de la Universidad CES. https://dialnet.unirioja.es/descarga/articulo/4863623.pdf.

Alfonso, D. d. (2015). La Actividad Probatoria Reforzada en la Evidencia Digital. *Nuevas Tecnologias*, 3.

Bogota Prieto, D., & Moreno Peña, C. (s.f.). *Evidencia Digital en Colombia: una reflexion en la práctica*. Obtenido de www.cej.orj.co/.../377-evidencia-digital-en-colombia-una-reflexxion-en-la-practica

Cabrera, C. (2005). El Arte de la Computación Forense. *Revista Internacional del Derecho Penal Contemporaneo*.

Cano Martinez, J. J. (2009). *Computacion forense. descubrimiento de los rastros informaticos* . Mexico DF: Alfaomega grupo editor, S.A de C.V.

Cano martinez, J. J. (2010). El Espionaje Informatico y La Evidecia Digital en Colombia. Bogotá: kimpres Ltda.

CARVAJAL, L. (17 de enero de 2013). *LA INDUCCIÓN COMO MÉTODO DE INVETIGACION CINTIFICA* . Obtenido de http://www.lizardo-carvajal.com/la-induccion-como-metodo-de-investigacion-cientifica/

Cortes Botero , R., Ballen Rojas, J. A., & Duque Montes, J. J. (2015). La persecucion judicial contra los delitos informaticos en el distrito judicial de Villavicencio. *Revista de derecho, comunicaciones y nuevas tecnologias*, 24.

Doctrina. (s.f.). *Guia Actualizada Futuros Peritos Informaticos Ultimas Herramientas Analisis Forense*. Obtenido de http://www.pensamientopenal.com.ar/doctrina/43429

Florez, A. ,. (2016). *Evidencia digital, distribución musical y derecho de consumo: discusiones desde el derecho privado.* . Obtenido de http//eboocentral.proquet.com

G., P. (2014). Hurto por medios informáticos y transferencia no consentida de activos en Colombia. *Revista Internacional de Derecho Penal Contemporaneo*.

Grisales Pérez, G. S. (2013). Análisis Dogmático de las Conductas de Hurto por Medios Informáticos y Semejantes (Art. 269i) y Tranferencia No Consentida de Activos (Art. 269j) ley 1273 de 2009. Medellin: Universidad EAFIT Escuela de Derecho, Maestria en Derecho Penal.

Howlet., T. (s.f.). *Software Libre. Herramientas de Seguridad.* . Ed. Anaya Multimedia. .

*La actividad Provatoria Rforzada en la Evidencias Digitasles*. (29 de Junio de 2015). Obtenido de http://www.abogacia.es/2015/06/29/la-actividad-probatoria-reforzada-en-las-evidencias-digitales/

Maria, M. E. (2013). *Aproximacion a la informatica forense y el derecho informatico .* Medellin: Fulam .

Maya, R. (2013). EL DELITO DE ACCESO ABUSIVO A SISTEMA INFORMÁTICO: A PROPÓSITO DEL ARTÍCULO 269A DEL CÓDIGO PENAL DEL 2000. *Revista Internacional Derecho Penal Contemporaneo*.

Pascale, M. (2007). MANUAL DE PERITAJE INFORMATICO. Uruguay: Fundacion de Cultura Universitaria .

Pino, A. d. (2009). *Informatica forense en el Ecuador.* Ecuador: Fiscalia General del Estado de Ecuador.

Prieto, B. (13 de Diciembre de 2014). *Diario la Republica*. Obtenido de El Valor Provatorio De Un Mensaje De Datos: http://www.larepublica.co/el-valor-provatorio-de-un-mensaje-de-datos

Republica, C. d. (2012). *Ley estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la proteccion de datos personales.* Colombia: Diario Oficial.

Republica, C. G. (2014). *Resolucion reglamentaria 277 del 2014, por la cual se adopta el sistema de aceguramiento electronico de expedientes y se regulan aspectos relacionados con su utilizacion y funcionamiento.* Colombia: Diario Oficial.

Republica, Congreso de la. (1999). *ley 527 de 1999, por medio de la cual se define y reglamenta, el acceso y uso de los mensajes de datos, del cmercio electronico y de las firmas digitales y se establecen las entidades de certificacion y se dictan otras disposiciones.*

Republica, Congreso de la. (2018). *Ley 1924 de 2018, Por medio de la cual se aprueba el convenio sore la ciberdelincuencia.* Colombia: Diario Oficial.

Rifà Pous, H., Sierra Ruiz, J., & Rivas López, J. L. (2009). Ananlis Forense de Sistemas Informaticos. Barcelona: Universidad Oberta de Catalunya.

Rincon Rios Jarvey, N. d. (2011). *Delito informatico de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia.* Cali: Universidad Santiago de Cali .

Rincón Ríos, J., & Naranjo Duque, V. (2011). Delitos Informaticos, de las Telecomunicaciones y de los Derechos de Autor y Normas Complementarias en Colombia. Cali - Colombia: Universidad Santiago de Cali.

Sanchez, A. S. (2016). *Manual de delito informatico en Colombia, analisis docmatico ley 1273 de 2009.* Bogota: Universidad Esternado de Colombia.

Stalin, G. P. (2013). *Analisis dogmatico de las condctas de hurto por medios informaticos y semejantes y tranferencia no concentida de activos.* Medellin: Universidad EAFIT escuela de derecho .

Torres Moncada Martha Liliana, J. A. (2016). *Estado del analiss forense digital en Colombia .* Bogota : Universidad Militar Nueva Granada, Facultad de relaciones Internacionales estrngeria y seguridad.

torres, L. A.-A. (s.f.). DERECHO INFORMATICO Y TELEINFORMÁTICA JURÍDICA" N° 51. *Revista Peruana del Derecho de la Empresa* .

# 3. ANEXOS

**13.1 Tabla No. 1**

**Acta del grupo de investigaciones tecnológicas de la Sijín Meval**

**13.2 Tabla No. 2**

**Relación de fichas análisis de casos de delitos informáticos**