ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA

DIEGO ALEJANDRO JARAMILLO ARCINIEGAS
MARTHA LILIANA TORRES MONCADA

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y SEGURIDAD
ADMINISTRACION DE LA SEGURIDAD Y LA SALUD OCUPACIONAL
BOGOTA, D.C. COLOMBIA
2016

TRABAJO DE GRADO

ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA

DIEGO ALEJANDRO JARAMILLO ARCINIEGAS
MARTHA LILIANA TORRES MONCADA

SANDRA LILIANA URIBE
INGENIERA ELECTRÓNICA – MAGISTER EN TELEINFORMÁTICA
DOCENTE UMNG

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y

SEGURIDAD

ADMINISTRACION DE LA SEGURIDAD Y LA SALUD OCUPACIONAL

BOGOTA, D.C
2016

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3
TABLA DE FIGURAS 5
Siglas 6
Glosario 8
Introducción 11
Resumen 12
Abstract 13
Descripción del proyecto 14
- **Planteamiento del problema.** 14
- **Pregunta de investigación** 15
- **Objetivo general** 15
- **Objetivos específicos** 15

Justificación 16
Capítulo I - Marco conceptual 17
- **Seguridad informática** 17
- **Análisis Forense Digital** 17
- **Evidencia digital** 18

Capítulo II - Marco teórico 20
- **Historia de la Informática Forense** 20
- **Presencia del AFD en diferentes sectores** 21
- **Principios del Análisis Forense Digital** 23
- **Ventajas del Análisis Forense Digital** 23
- **Desventajas de la Informática Forense** 23
- **Estructura de un computador para Análisis Forense Digital** 24
  - **Hardware** 24
  - **Software** 24
- **Metodología de Análisis Forense Digital según ISO/IEC 27037** 25
- **Metodología del Análisis Forense Digital según artículo Framework** 25
- **Evidencia digital** 26

Clasificación de la evidencia digital 26
Características de la evidencia digital 27
Determinación de la veracidad de la evidencia digital 27
Problemas para la aceptación de evidencias digitales 28
Incidente de Seguridad Informática 29
Capítulo III – Origen y estado del Análisis Forense Digital en Colombia 31
Origen 31
Cuando llegó el AFD a Colombia 31
Porque llega a Colombia 32
Primer caso de AFD en Colombia 33
Estado 34
Histórico de algunos casos de AFD presentados 34
Liderazgo de Colombia en Ciberseguridad 36
Vulnerabilidad en Colombia 37
Empresas y entidades dedicadas al análisis de evidencias digitales en Colombia 41
Capítulo IV - Marco jurídico de la Informática Forense 43
Ley 527 de 1999 44
Sentencia C-662/2000 44
Ley estatutaria 1266 del 31 de diciembre de 2008 45
Ley 1273 de 2009 46
Ley 1453 de 2011 47
Resolución reglamentaria 202 de 2012 47
Ley 1564 de 2012 – Código general del proceso 48
Ley estatutaria 1581 de 2012 48
Decreto 1377 de 2013 49
Capítulo V – Análisis de la información obtenida 50
OCDE (Organización para la Cooperación y el Desarrollo Económico) 58
Análisis Forense Digital en equipos móviles 60
Documento CONPES 3701 de 2011 61
Documento CONPES 3854 del año 2016 61
Manual de cadena de custodia de la Fiscalía General de la Nación 62

Capítulo VI – Conclusiones **63**
Referencias **65**

TABLA DE FIGURAS

Ilustración 1 Histórico de delitos informáticos **33**
Ilustración 2 Ciberseguridad en Latinoamérica **37**
Ilustración 3 Sectores afectados en Colombia por incidentes digitales, 2015 ..... **38**
Ilustración 4 Incidentes digitales gestionados por el CCOC y el colCERT en el entorno digital en Colombia, 2015 ..... **39**
Ilustración 5 Incidentes gestionados por la CCP y CSIRT PONAL en el entorno digital en Colombia, 2015 ..... **39**
Ilustración 6 Capturas y denuncias de incidentes digitales en Colombia, 2015 ..... **40**
Ilustración 7 Principales organizaciones de Análisis Forense Digital en Colombia, Autores: Torres, L y Jaramillo, D (2016) **41**
Ilustración 8 Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia, 2015 ..... **43**
Ilustración 9 Histórico del Producto Interno Bruto en Colombia **58**

Siglas

AFD = Análisis Forense Digital

AMERIPOL = Comunidad de Policías de América

ARP = Protocolo de resolución de direcciones

ATA = Asistencia Antiterrorismo

CART = Equipo de Análisis y Respuesta informático

CCOC = Comando Conjunto Cibernético

CCP = Centro Cibernético Policial

CD = Disco Compacto

CFCE = certificado forense para examinador de ordenadores

COLCERT = Grupo de Respuesta a Emergencias Cibernéticas de Colombia

CONPES = Consejo Nacional de Política Económica y Social

CSIRT = Centro de Coordinación Seguridad Informática Colombia

CTI = Cuerpo Técnico de Investigación

DEA = Administración para el control de Drogas

DFRWS = Taller de Investigación Forense Digital

DIJIN = Dirección Central de Policía Judicial e inteligencia

DNP = Departamento de Planeación Nacional

DVD = Disco Versátil Digital

EC3 = Centro Europeo de Ciberdelincuencia

FARC = Fuerzas Armadas Revolucionarias de Colombia

FBI= Oficina Federal de Investigación

FIRST14 = Foro de Equipos de Seguridad y Respuesta de Incidentes

FTK = Juego de herramientas forenses

GB = Gigabyte

GLDTA= Grupo de Trabajo Americano de delitos Tecnológicos

GPS = Sistema de Posicionamiento Global

HTCIA = Asociación de Investigación de Delitos de Alta Tecnología.

IACIS = Asociación Internacional de Sistemas Informáticos

INTERPOL = Organización Policial Internacional

IOCE = Organización Internacional para la Cooperación en Evaluación

IP = Internet Protocol

IRS = Servicio de Impuestos Internos

KOICA = Agencia de Cooperación Internacional de Corea

L.I.F. = Laboratorio de Informática Forense

NCA = Agencia Nacional de delincuencia

OCDE = Organización para la cooperación y el desarrollo económico

RAM = Memoria de Acceso aleatorio

SCERS = Programa de formación incautados prueba informática Especialista en Recuperación

T.I = Tecnología de la información

TCP = Protocolo de Control de Transmisión

Glosario

Ataque DDoS: Este tipo de ataque consiste en un grupo de sistemas comprometidos (también conocidos como “ordenadores zombie”) que atacan a un solo objetivo para causar una denegación de servicios a los usuarios que sí son legítimos**.** (González, 2014)

Carta nigeriana: Es definida por el Centro cibernético policial como “Estafa que consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna”.

Crackers: en realidad son hackers maliciosos, cuyas intenciones tienen fines ilícitos, que van más allá de experimentar y conocer. Mediante ingeniería inversa crean seriales, generadores de claves/llaves (keygens) y cracks, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican. (Salcedo, Fernández y Castellanos, 2012)

Defacement: El defacing o defacement es la práctica de modificar o alterar una o varias páginas web de un sitio, sin autorización de su autor o dueño y con diversos motivos. (Borguello, 2009)

Dirección IP: Es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP. (Algesa, 2016)

Grooming: El "grooming" es "un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual". (Flores)

Hacker: Los verdaderos hackers tecnológicos son individuos con un alto nivel de conocimiento teleinformático, que en algunos casos se dedican a revisar y proponer soluciones a las vulnerabilidades en redes de computadores y sitios web. (Salcedo, Fernández y Castellanos, 2012)

Hacking: Arte que está enfocado en el diseño de sistemas de seguridad, para resolver y solucionar problemas hallados en los sistemas informáticos. Dichos problemas también son llamados vulnerabilidades (del inglés *bugs*). (Vergara, 2008)

Infraestructura crítica: El Plan Nacional de Protección de Infraestructuras Críticas las define como: "Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas"

Ingeniería social: La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo. (Sandoval, 2011)

Likejacking: Es una variación de clickjacking en el que la codificación maliciosa se asocia con Facebook en un botón. Los efectos más comunes de likejacking incluyen el robo de identidad y la difusión de virus, spam social y engaños. En una variación, al hacer clic en el mensaje en sí nos lleva a una página de bienvenida que se codifica de forma que si el usuario hace clic en cualquier lugar de la página, se registra como un "me gusta" y comparte el post original para el muro de Facebook del usuario. (Rousse, 2012)

Malware: Cualquier programa creado con intenciones de molestar, dañar o sacar provecho en las computadoras infectadas.
En general, es fácil determinar si un programa es (o contiene) un malware: sus actividades son ocultas y no son anunciadas al usuario. Pero existen casos en que la distinción no es clara, provocando hasta demandas por parte de los desarrolladores de estos programas a los antivirus y anti espías que los detectan como malignos. (Algesa, 2010)

Phishing: El phishing consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante. (Steffens, 2009)

Skimming: El skimming es uno de los sistemas más ingeniosos para captar tanto los datos de la banda magnética de las tarjetas bancarias como el número secreto o PIN que se utiliza para operar con dichas tarjetas (Pérez, 2009)

Smishing: El Smishing es una variante del phishing pero con el uso de los mensajes cortos o SMS. También es llamado SMS phishing.
La técnica Smishing consiste del envío de mensajes de texto (SMS) cuya actividad criminal es la de obtener, mediante engaños a los usuarios de telefonía móvil, información privada o suscripciones falsas online y ofertas de trabajo en sitios web, para luego introducir spyware o programas con intenciones maliciosas sin el consentimiento del usuario. (Algesa, 2016)

Técnica Anti forense: Una técnica anti forense es cualquier cambio intencional o accidental obscureciendo, cifrando, u ocultando datos de las herramientas forenses. (caballero 2015)

Valores hash: Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). (Gutiérrez, 2013)

Vishing: El Vishing es una variante del Phishing pero con el teléfono. Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computarizada de aspecto profesional requiere de las victimas la conformación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN, etc. (Algesa, 2010)

Introducción

La rápida evolución de la tecnología demuestra que de la misma manera los conocimientos y habilidades de los seres humanos avanzan progresivamente, generando grandes transformaciones en el diario vivir y debido a que la tecnología se convirtió en algo indispensable para la vida de las personas, ha logrado ocasionar dependencia debido a que todo gira en torno a los diferentes dispositivos y aparatos electrónicos existentes.

Por lo anterior, hoy en día encontramos que gran parte de las organizaciones dependen de los medios digitales, debido a que estos realizan varias funciones, como lo es archivar información confidencial y sustancial, que al ser vulnerada podría afectarlos de manera negativa.

Es por esto que al convertirse en un tema tan importante para la humanidad en general surge la necesidad de protección, análisis e investigación de la información manejada por estos medios, debido a que así como nacen grandes e innovadoras ideas para facilitar ciertos procesos nacen nuevas amenazas que pueden generar daños considerables y cuantiosos.

A causa del aumento de la Ciberdelincuencia o delitos informáticos, observamos que al día de hoy el tema de Análisis Forense Digital (AFD) es valioso para las entidades encargadas de la seguridad y custodia de un país (Ministerio de Defensa, Policía Nacional, Fuerzas Militares, entre otros), por tal motivo el enfoque de la investigación va encaminado a indagar cómo esta Colombia respecto a AFD el cual es definido por Miguel López Delgado, (2007) como "un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial" (p.10)

Por ser lo anterior tan importante decidimos realizar una investigación con la metodología de tipo exploratorio, donde se recolectará toda la información correspondiente al tema, luego se analizará, posteriormente se identificar las virtudes y falencias, para que finalmente se puedan exponer las conclusiones sobre el tema AFD en Colombia.

Resumen

Este proyecto va dirigido a la investigación del Análisis Forense Digital en Colombia, el cual consiste en realizar una exploración por los diferentes archivos, documentos e información consultada y recolectada con el fin de tener una visión completa de los avances realizados en el país, para el tema en cuestión; dentro del contenido se podrá encontrar en orden progresivo la información sobre antecedentes del AFD, casos de éxito, principios, evidencia digital, de igual manera profundización en el tema de Informática Forense y legislación existente para todo lo relacionado con delitos informáticos.

Después de recolectada la información se llevará a cabo el análisis de la misma, de este modo se pondrá en evidencia la importancia del tema para las organizaciones, personas y cualquier estado en general, permitiendo la aclaración y resolución efectiva de los delitos de este tipo y que puedan afectar a cualquier sector en los diferentes entornos internos y externos que manejan.

Finalmente se expondrán las debidas conclusiones del tema, mostrando las falencias y dificultades encontradas, pretendiendo con esto dejar expuestos los vacíos existentes en el tema y que no permiten que el Análisis Forense Digital en el país sea efectivo y se le dé la trascendencia necesaria para contribuir con la justicia tanto en la determinación de las actividades criminales cibernéticas como con la reducción de la presencia de las mismas en un medio tan utilizado y determinante hoy en día en la humanidad como lo es el Internet.

Palabras clave: Análisis Forense Digital, Informática Forense, Delitos Informáticos

Abstract

This project is directed to the investigation of the Digital Forensics in Colombia, which is to perform an exploration of the different files, documents and information consulted and harvested in order to have a complete overview of the progress made in the country, for the subject in question; within the content can be found in progressive order the information on the AFD, cases of success, principles, digital evidence, similarly deepening in the theme of Computer Forensics and existing legislation for everything related to computer crime.

After the information is collected to carry out the analysis of the same, this will put in evidence the importance of the issue for the organizations, persons and any state in general, allowing the clarification and effective resolution of crimes of this kind and that may affect any sector in the different internal and external environments that handle.

Finally you will discuss the appropriate conclusions of the item, showing the shortcomings and difficulties encountered, pretending with this leave exposed the gaps existing in the topic and does not allow the Digital Forensics in the country to be effective and that it will be given the necessary importance to contribute with the justice both in the determination of the cyber-criminal activities as with the reduction of the presence of the same in a medium as used and determinant today in humanity as it is the Internet.

Keywords: Digital Forensics, Computer Forensics, Computer Crime

Descripción del proyecto

Planteamiento del problema.

Las diferentes modalidades delictivas son de gran preocupación tanto a nivel nacional como internacional. No obstante para garantizar la seguridad en el país se deben tomar medidas que contrarresten esta problemática, y en temas de Seguridad Informática el país es participe con metodologías de Análisis Forense Digital (AFD), lo cual permite realizar un análisis y diagnóstico claro en circunstancias de manifestación, materialización e investigación de eventos que vulneran los sistemas de seguridad de las personas u organizaciones. Según la Interpol, en Colombia muchos han sido afectados, algunos casos que se pueden mencionar son los del famoso hacker Andrés Sepúlveda, el joven del caso de Lifemiles y en el caso del decomiso de equipos y ordenadores informáticos de las Fuerzas Armadas Revolucionarias de Colombia (FARC), a los cuales se les realizó el respectivo Análisis Forense.

Según el estudio realizado por la firma especializada en Seguridad informática Digiware, Colombia se encuentra entre uno de los países con más casos de ataques a la seguridad informática; dichos ataques se enfocan generalmente al sector financiero, gobierno, comunicaciones e industria. Lo anterior invita y promueve a realizar el proyecto investigativo del estado de Colombia en el tema AFD, pues es necesario observar, estudiar y justificar si los garantes de seguridad del país (Policía Nacional, Gobierno, Ministerio de defensa Nacional, entre otros) y de las organizaciones que la conforman (empresas públicas y privadas), cuentan con personal idóneo para protegerse ante la manifestación del riesgo, permitiendo así la continuidad y desarrollo normal de las operaciones de las personas y organizaciones.

Pregunta de investigación

¿Cuál es el estado actual del Análisis Forense Digital en Colombia?

Objetivo general

Definir el estado actual del Análisis Forense Digital en Colombia.

Objetivos específicos

- Recolectar información y documentación sobre el desarrollo de la metodología de Análisis Forense Digital en Colombia.
- Analizar la documentación e información obtenida de los casos presentados y del desarrollo del tema Análisis Forense Digital en Colombia.
- Proporcionar las conclusiones generadas del manejo del Análisis Forense Digital en Colombia.

Tipo de investigación: Investigación de tipo exploratorio

Diseño empleado: Para el tema propuesto se aplicará un Diseño longitudinal de tendencia o trend; debido a que se abordará desde los orígenes del AFD en Colombia, además se resaltarán los cambios en el tiempo y el estado actual del tema dentro de la población objeto de estudio.

Fuente: Para efectos del tema planteado, como fuente se basará en una Investigación Bibliográfica, debido a que se recolectará toda la información de artículos y páginas web en su mayoría de autoría Colombiana.

Población participante: La investigación se basará específicamente en el País de Colombia.

Sistema de muestreo: Para el tema planteado no se aplica un sistema de muestreo, debido a que la población objeto de estudio es Colombia como país o estado, y no como la población o personas que lo habitan.

Justificación

Este Proyecto de investigación es realizado debido a que por medio de la recolección de información sobre AFD y su respectivo análisis, se identificarán las virtudes y falencias, para que así finalmente se puedan exponer las conclusiones sobre el estado actual del Análisis Forense Digital en Colombia, el cual es de indispensable apoyo en la temática de Seguridad Informática empresarial, lo anterior debido a que la Seguridad Informática es la garante de la integridad, confiabilidad y disponibilidad de los procesos de información de las personas u organizaciones, quienes son afectadas por las diferentes modalidades delictivas y que para posteriores acciones reactivas y correctivas el AFD, los apoya a la hora de diagnosticar y tomar acciones judiciales en estos delitos.

Para esta investigación se tomará como base las diferentes teorías relacionadas y experiencias en el tema, además el resultado de la misma podrá permitir que el lector adquiera el conocimiento propio del tema y así contribuya con acciones correctivas sobre las personas u organizaciones privadas del país, para que de esta manera no sean vulnerables ante las diferentes amenazas y así prevenir futuras materializaciones de eventos que puedan afectarlos.

Otro aspecto importante a resaltar es que las personas en formación académica de Administración de la Seguridad y Salud ocupacional podrán ampliar su criterio sobre el campo de acción de la Seguridad.

Capítulo I - Marco conceptual

Seguridad informática

Para el contenido de Análisis Forense Digital es conveniente tener claridad del significado de la seguridad informática, así se lograra entender el porqué de la importancia de AFD para todo el tema de delitos informáticos, de esta manera, la seguridad informática es definida por Algesa (2010) como "una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios".

Teniendo en cuenta esta definición es posible observar que al momento de presentarse la vulnerabilidad de los diferentes sistemas se hace necesario realizar investigaciones digitales y dependiendo el caso o delito que se haya generado realizar un AFD.

De igual forma Galdámez (2003) expresa que "la seguridad informática trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada"

Asa mismo, Pérez y Merino (2008), ratifican la tesis que dan los anteriores autores definiendo la Seguridad Informática como "disciplina que se encarga de proteger los aspectos de confidencialidad, integridad y disponibilidad de la información, la cual esta almacenada en un sistema informático". Y exponiendo igualmente que "no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema" lo que hace que el AFD resulte una técnica indispensable para judicialización de los delincuentes que utilizan el medio informático para realizar sus fechorías y por consiguiente generar soluciones efectivas de protección ante la presencia de la ciberdelincuencia.

Análisis Forense Digital

Para el desarrollo de la investigación es preciso comprender que es el AFD, por lo cual Miguel López indica que es "un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial" (p.10), dentro de los

cuales se pueden encontrar delitos como: (homicidios, fraude financiero, terrorismo, pornografía infantil (grooming), piratería de software, hacking, spam, entre otros).

Igualmente, López explica que las técnicas utilizadas en el AFD incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Otra definición encontrada es la generada por Porolli (2013) en la cual explica que "el Análisis Forense Digital se corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, descubrir información que se encontraba oculta", lo anterior aplicado en casos donde se determine que se está alterando la triada de la seguridad de la información.

En la definición emitida por Paus (2015) "El análisis forense digital se define como un conjunto de técnicas de recopilación y exhaustivo peritaje de datos, la cual sin modificación alguna podría ser utilizada para responder en algún tipo de incidente en un marco legal", se observa que tiene relación con las emitidas por Porolli y López mostrando en resumen que son diversas técnicas las utilizadas por el AFD para investigar las vulnerabilidades presentadas por sistemas informáticas y la utilización de las evidencias en la resolución de casos.

Evidencia digital

La evidencia digital la comienza definiendo Ramos (2011) como "prueba electrónica, en su acepción general dentro del ámbito probatorio, puede ser considerada como cualquier información almacenada o transmitida en forma digital, la que una de las partes podrá utilizar en el juicio", si al finalizar el respectivo AFD que se haga se le da un manejo debido a este tipo de evidencias como lo manifiesta Ramos podría tenerse en cuenta como defensa ante un Juicio.

De igual manera Ghosh (2004) la define como cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático, tesis que realmente resulta insuficiente teniendo en cuenta que es una parte fundamental para la resolución de casos delictivos.

Caldana, Correa y Ponce (2014) exponen en su definición “Información creada, transmitida, procesada, registrada y/o mantenida electrónicamente, que respalda el contenido de un informe de auditoría y que puede tomar diferentes formas, tales como texto, imagen, audio, video, entre otros”, las formas como se pueden presentar este tipo de evidencias, información valiosa que no muestran los autores Ghosh y Ramos en sus definiciones.

Por lo anterior es trascendental darle un buen manejo a las evidencias digitales sin importar en la forma en la que se presenten ante un juez, con el único fin de contribuir a la resolución inequívoca de casos que se presenten a nivel de seguridad informática.

Capítulo II - Marco teórico

Historia de la Informática Forense

Para la comprensión adecuada de todo tema es indispensable aclarar y entender los antecedentes históricos relevantes del mismo, por tal razón se dedicara en los siguientes párrafos a explicar de forma detallada y clara el origen del AFD a nivel mundial. Toda la información fue consultada y tomada de dos fuentes de información.

En 1978 Florida es el primero en reconocer los delitos en sistemas informáticos en el "Computer Crimes Act", los delitos que reconocieron son: los casos de sabotaje, copyright, modificación de datos. Posteriormente a la viabilidad de uso de los computadores personales para los usuarios, en año de 1980 es cuando con exactitud se dio origen a la Informática Forense y en 1984, el FBI crea un programa llamado en su momento como el Programa de Medios Magnéticos, que ahora es conocido como CART (Computer Analysis and Response Team), en español; análisis de informática y equipo de respuesta. Algún tiempo después aparece el Señor Michael Anderson, quien era un agente especial de la División de investigación criminal del IRS (Departamento de tesorería de los Estados Unidos de América), y es a quien se le conoce como el padre de la Informática Forense y que trabajó hasta mediados del año 1990 con el gobierno, para que después fundara el New Technologies.

En 1982 el Señor Peter Norton pública UnErase: Norton Utilities 1.0, la primera versión de un conjunto de herramientas dentro de las cuales hay una aplicación que permite la recuperación de archivos que se han borrado, ya sea o no accidentalmente, esta aplicación es conocida como UnErase.

En 1987 se crea una asociación en Santa Clara para ofrecer cursos e información relacionada al tema y está compuesta por profesionales de empresas privadas y gubernamentales, dicha sociedad se conoce como la High Tech Crime Investigation Association (HTCIA), en español Asociación de Investigación de Delitos de Alta Tecnología.

En 1987 nace la compañía AccessData, principal compañía que ha desarrollado productos que contribuyen a la recuperación de contraseñas y el análisis forense, como lo es la actual Forensic Toolkit (FTK), en español Juego de Herramientas Forenses.

En 1988 se crea la International Association of Computer Investigative Specialists (IACIS), quien desde entonces certifica a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE), certificado forense para examinador de ordenadores, y esta certificación es una de las más prestigiosas y con más nombre en el ámbito forense. Por otro lado en este mismo año se desarrolla el programa Seized Computer Evidence Recovery Specialists (SCERS), quien tiene a su cargo y como el objetivo principal la formación de profesionales en Informática Forense.

En 1995 se funda el International Organization on Computer Evidence (IOCE), quien tiene como objetivo ser la organización punto de encuentro de los especialistas en la evidencia electrónica. Posteriormente en 1996 la INTERPOL organiza los International Forensic Science Symposium, permitiendo así crear espacios para foros con el fin de debatir los avances forenses y en año de 1998 la INTERPOL celebró un simposio sobre Informática Forense al año siguiente, y en 1999, el programa CART del FBI abordó 2000 casos sobre delitos informáticos.

En el año 2001, crean la Digital Forensic Research Workshop (DFRWS), el cual es un grupo encargado de debate y discusión internacional para compartir información relacionada con la Informática Forense.

Presencia del AFD en diferentes sectores

Teniendo en cuenta la importancia que tiene el contenido de la investigación, a continuación se citan algunos de los sectores dentro de los cuales tendría incidencia el AFD

Prosecución Criminal: La evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil (Grooming).

Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la Informática Forense.

Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

Mantenimiento de la ley: La Informática Forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

A continuación se ilustran otros usos del Análisis Forense Digital, dicha información es tomada de un artículo de la revista Enter.co, según lo referido por Piñeros, G. (2008)

Militar y Defensa Nacional: Se usa en actividades de contrainteligencia e inteligencia, protegiendo así la confidencialidad de la información y a su vez identificando los ataques a los cuales están expuestos.

Investigación científica: Diferentes organismos académicos lo usan en temas de estudios de seguridad, identificación de amenazas y ataques informáticos.

Usuario final: Los usuarios usan diferentes software para encriptar documentos, recuperar archivos, entre otras funciones.

Es necesario poner en contexto el tema planteado, por tal razón se deben explicar los principios por los cuales se rige el mundo en la práctica del Análisis Forense Digital. Para ello se tomará como material de referencia la ISO/IEC 27037; este estándar internacional es la guía para la identificación, recolección, adquisición y preservación de la evidencia digital; la cual como alcance en materia de análisis incluye: dispositivos de almacenamiento masivo, Smartphone, GPS, sistemas de circuito cerrado de televisión, computadoras, dispositivos con conexión de red basados en protocolo TCP/IP, sin embargo puede ser aplicable a dispositivos con características y funcionalidades similares.

Principios del Análisis Forense Digital

Relevancia: La evidencia digital debe estar relacionada con el hecho a investigar.
Confiabilidad: La evidencia debe ser repetible y auditable por un tercero.
Suficiencia: La evidencia debe ser efectiva, buscando una adecuada sustentación de los hallazgos que obtiene el analista.

La información expuesta anteriormente, es tomada como referencia según lo descrito por Presman, G. (2014).

Ventajas del Análisis Forense Digital

- Tiene papel de sistema preventivo
- Sirve para auditor, mediante la práctica de diversas técnicas para probar que los sistemas de seguridad instalados cumplen con ciertas condiciones básicas de seguridad
- Mediante el descubrimiento de falencias se podrán elaborar nuevas políticas de seguridad
- Permite realizar rastreo de intrusión y descubrimiento del daño generado
- Permite recopilar evidencias electrónicas
- Permite detectar el origen del ataque o las alteraciones realizadas al sistema

Desventajas de la Informática Forense

- 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

Estructura de un computador para Análisis Forense Digital

Las siguientes especificaciones son con las cuales cuentan los computadores que se usan para investigación forense digital y que usan las autoridades nacionales en las actividades de investigación, dicha información es fuente de un artículo publicado por la revistas Enter.co. y es importante resaltar que debido a la dificultad de obtener información referente al tema, se basará lo siguiente en información publicada en el año 2008 según lo descrito por Piñeros, G. (2008).

Hardware

- Procesador de cuatro núcleos
- Memoria RAM de 4-8 GB
- Disco duro con capacidad de almacenamiento de 1TB
- Sistemas operativos que trabajan a 32 y 64 bits
- Unidades ópticas que cuenten con lectura de discos, quemador de CD y DVD

El costo aproximado es de 10.000 Dólares

Software

- Encase Forensic Edition: Es un programa que está en capacidad de desencriptar archivos de correo, recuperar información borrada y puede crear imágenes espejo de los discos duros.
- Stego suite: Se usa en actividades de esteganografía (información escondida en imágenes y archivos de audio).
- Access data suite: Es un programa que incluye usos como recuperación de contraseñas, análisis de información borrada y creación de imágenes espejo de discos duros.
- Ilook: Este programa permite el acceso y análisis de datos digitales.
- El costo aproximado es de: 50.000 Dólares

Metodología de Análisis Forense Digital según ISO/IEC 27037

Para la comprensión adecuada de la metodología de AFD, es importante explicar el proceso por el cual está compuesto el análisis bajo el estándar de la norma ISO/IEC 27037 del año 2012 y como según refiere Presman, G. (2014), esta norma estable:

Identificación: Es el reconocimiento inicial de donde se halla la evidencia digital, y esta puede ser física o lógica.

Recolección: Es cuando el perito tomará la decisión de recolectar la evidencia y trasladarla al laboratorio, para lo cual debe tener en cuenta los recursos informáticos y el tiempo disponibles en el lugar de los hechos. Este proceso debe estar documentado y sustentado adecuadamente en caso que deba defenderla en una corte.

Adquisición: Este proceso incluye por parte del perito, realizar la copia exacta del contenido físico o lógico de los objetos involucrados en la investigación.

Preservación: Se refiere a que la evidencia digital debe conservar su integridad durante todo el proceso.

Metodología del Análisis Forense Digital según artículo Framework

Es importante describir la información tomada de otro artículo, la cual es similar a la anteriormente ilustrada, sin embargo esta incluye otros aspectos, los cuales se mencionan en un orden secuencial y que se muestra a continuación, dicha información es tomada como referencia en lo expuesto por Álvarez et al. (2015, p 65).

Recolección: En esta actividad se incluye desde la identificación de las posibles fuentes de datos, la recolección de las evidencias encontradas y finalmente la verificación de la integridad de la información.

Examinar: En esta actividad bajo técnicas y herramientas el investigador determinará cuáles datos son los importantes y que puedan aportar a la investigación, además puede obtener datos

como el tipo de sistema operativo usado para el hecho delictivo, el tipo de conexión, datos digitales como gráficos, documentos y textos, los cuales dan mayor fuerza a la evidencia.
Análisis: En esta actividad se revisará la información examinada, a fin de determinar lugares, relación entre las evidencias halladas y finalmente llegar a la conclusión para determinar quién, cómo, cuándo y dónde dieron a lugar los hechos.
Entrega de informe: En este actividad se presentará toda la información encontrada en el análisis, este informe debe ser claro, sin tecnicismos, escrito cronológicamente, sin sugerir culpables y en caso de ser necesario hacer referencia a la norma objeto de violación por parte del presunto delincuente.

Evidencia digital

Muchos son los conceptos que se pueden encontrar sobre la evidencia digital, sin embargo en su mayoría comprenden el mismo vocabulario, por ello bajo el concepto del profesor Cano el cual tomó como referencia Bogota & Moreno (2012), se puede definir la evidencia digital como un "tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" todos ellos están contenidos en dispositivos electrónicos que son usados diariamente en la actualidad, algunos de estos son: celulares, Tablet, computadoras de escritorio y portátiles, además de videos, sonidos, máquinas de fax, entre otros dispositivos que permitan el almacenamiento, envío y recepción de información.

Clasificación de la evidencia digital

Esta clasificación está basada en el estándar norteamericano, el cual clasifica la evidencia digital en tres categorías, como refiere Bogotá & Moreno (2012)

- Registros no generados en computadores pero almacenados en estos
- Registros generados por computador
- Registros híbridos, donde se incluyen los generados por computador y almacenados en los mismos

Características de la evidencia digital

Los autores mencionados en el párrafo anterior explican las siguientes características:

Autenticidad: Se caracteriza porque la evidencia ha sido generada y registrada en los lugares relacionados con el caso, específicamente en la escena del posible ilícito, esta característica es la que resalta la inalterabilidad de los medios originales.

Confiabilidad: Establece si efectivamente los medios probatorios que se están aportando provienen de fuentes creíbles y verificables.

Suficiencia: Es la presencia de toda la evidencia necesaria para adelantar el caso.

Estas características las deben contener todas las posibles evidencias que se quieran presentar, para que de esta manera sean contundentes y los organismos judiciales las puedan tomar en cuenta en los diferentes casos que involucran actos delictivos por medios informáticos.

Determinación de la veracidad de la evidencia digital

La aceptación de la evidencia digital en las cortes Colombianas es un tema determinante a la hora de presentarlas ante un juez, para lo cual el investigador en Informática Forense debe garantizar ante el juez que la evidencia es veraz y no ha sido objeto de manipulación inadecuada, por tal razón como explica Juan Pablo Caro, uno de los investigadores de Mattica; uno de los primeros laboratorios de investigación en delitos informáticos para Latinoamérica creado en México hace siete años, en una entrevista realizada por el periódico El Universal, “Nosotros, al igual que los forenses, utilizamos técnicas para manipular la información de forma que no sea contaminada o en el caso de la informática modificada y/o manipulada.” (Mora, V. 9 de septiembre de 2013), por lo cual el hecho de modificar o manipular inadecuadamente la información podría entenderse como “la contaminación de la escena del crimen”. Por otro lado Caro explica que el método que existe y que se utiliza para demostrar la veracidad de las evidencias, es por medio de valores “hash” el cual consiste en una función matemática que genera un resultado numérico (claves o llaves a un documento o conjunto de datos). Finalmente Caro explica una de las características de un hash y refiere que “Ese valor debe ser inmutable siempre y cuando el

contenido de información no haya cambiado. Si dicho contenido (que puede ser material evidenciario) varía en un solo bit o carácter, el resultado numérico va a ser diferente.” Por ello es que desde el levantamiento de la evidencia, durante la investigación y el reporte final de la misma los valores hash son revisados con el fin de mantener un material probatorio íntegro y confiable, asegurando así la veracidad e integridad de las evidencias.

Problemas para la aceptación de evidencias digitales

Algunos de los problemas que se observan actualmente para la aceptación de estas evidencias, es la deficiencia y carencia de normativa legal que contemple dentro de ella aspectos importantes como la cadena de custodia de la evidencia digital, y a su vez esta deficiencia afecta de manera negativa al juez encargado de un caso, debido a que como mencionan Álvarez, A, Et al (2015) en algunos casos por desconocimiento e incertidumbre técnica el juez prefiere apartarse del material probatorio digital, (p 66.), por ello como lo indican los autores es indispensable que en aspectos de dudas por parte del juez; éste pueda solicitar un peritaje a las evidencias para garantizar su confiabilidad. Otro aspecto problemático que indican los autores para la presentación de evidencia digitales es que en ocasiones los delitos informáticos pueden abarcar múltiples ámbitos y jurisdicciones geográficas, donde muchos países pueden ser víctimas, sin embargo al involucrar varias legislaciones de diferentes países, se produce un efecto desfavorable para la parte demandante, debido a que se debe acoger a las normas locales en las cuales tiene autoridad

Un aspecto importante es que en ocasiones el tecnicismo de los peritos informáticos juega un papel en contra de la aceptación de la evidencia digital, por ello es importante que el lenguaje tecnológico y científico se deje a un lado y se describa de la manera más clara y concisa para que el juez comprenda totalmente los resultados de la Investigación Forense Digital y pueda tomar en cuenta estos medios informáticos.

A continuación, se explicarán detalladamente algunos de los incidentes que se presentan en medios informáticos y que para posteriores acciones el AFD se encarga de realizar su respectivo análisis mediante las metodologías anteriormente sustentadas.

Incidente de Seguridad Informática

Es importante tener claros los diferentes incidentes que se presentan en el área de la informática para así tener conocimiento de las modalidades utilizadas y el tipo de Análisis Forense a aplicar durante el proceso que se realice, es así que el incidente informático se define como:

"cualquier evento anómalo que pudiese afectar la Seguridad de la Información, que comprende la pérdida de la disponibilidad, integridad o confidencialidad de la misma. También se puede definir como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos" (Miguel López, p.10),

Para comprender detalladamente este tema, es importante mencionar algunos de los incidentes informáticos más comunes en ambientes informáticos, algunos de estos los explica Miguel López, (p.11)

Incidentes de denegación de servicios (DoS): Se caracteriza por obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones.

Incidentes de código malicioso: Cualquier tipo de código como virus, gusanos, troyanos y que estos puedan ser ejecutados en un sistema e infectarlo.

Incidentes de acceso no autorizado: Se caracteriza porque un usuario o aplicación accede por medio de hardware o software, sin solicitar los permisos bien sea un sistema, una red, datos o aplicación.

Incidentes por uso inapropiado: Es cuando los usuarios no respetan la política de uso apropiado de sistemas y en ocasiones ejecutan aplicaciones restringidas en la organización, como lo es el caso de aplicaciones para descarga de música.

Incidente múltiple: Se caracteriza porque comprende varios de los incidentes anteriormente mencionados.

Otros ataques:

El mundo de la informática ha sido tan cambiante y objeto de desarrollo a medida que pasan los años, y cuando aparecen nuevas herramientas tecnológicas también lo hacen los delincuentes que buscan vulnerar la seguridad con el fin de causar daños, por ello una de las técnicas o delitos que comúnmente dan a lugar en el estado Colombiano es la clonación de tarjetas débito o crédito, así lo explica Fabio Herrera, ingeniero del Grupo de Delitos Informáticos, dependencia adscrita al CTI de la Fiscalía General de la Nación, en una entrevista realizada por el periódico El Universal, "la forma más fácil es a través de lectores de banda magnética, que hoy en día se consiguen fácilmente a través de Internet. Estados Unidos es el país que más las vende. Esas máquinas se conocen en el mercado como skinner o skimming y lo que hacen es copias de toda la información de la cuenta bancaria" Rodríguez, J. (4 de marzo de 2014) y esta consiste básicamente en colocar o sobreponer dicha banda magnética en la del cajero y una cámara que capte el teclado del mismo con el fin de obtener la información necesaria para luego sustraer el dinero de las cuentas de las víctimas.

Capítulo III – Origen y estado del Análisis Forense Digital en Colombia

Es importante resaltar que la normatividad jurídica Colombiana en relación al Análisis Forense Digital, se ampliarán en el capítulo IV.

Origen

Cuando llegó el AFD a Colombia

El año 2004 fue decisivo e importante en aspectos de Seguridad Informática para el país, debido a que a partir de esta fecha en la Policía Nacional de Colombia surge la Informática Forense como una ciencia para apoyar las investigaciones judiciales. El Gabinete de Informática Forense surge por el efecto nocivo y negativo que produjo el mal uso de medios informáticos y que desde su momento llevó al incremento de delitos por este medio y que como se evidencia en el artículo del periódico El Tiempo, donde resaltan la creación de 7360 virus para el año (2004) lo que representaba un aumento de 332% comparando el año anterior (2003), además del incremento en un 93% de problemas de Seguridad Informática en las empresas, así como las pérdidas generadas a entidades financieras en el año 2003 equivalentes a 666 millones de dólares. (s.d., 5 de mayo de 2005); es por ello que surgió la necesidad de crear una entidad que cumpliera con el rol de la Investigación Forense dedicada específicamente a medios informáticos y desde entonces surge La Dirección de Investigación Criminal, quienes apoyan desde su momento a la Policía Nacional en sus labores investigativas, sin embargo para que dicho organismo funcionara adecuadamente necesitaba del apoyo de un organismo de control, por ello fue importante la presencia de una entidad con más jerarquía para dar una mejor estructura a tan importante tema, como menciona Restrepo (2008) “la Contraloría delegada para investigaciones, juicios fiscales y jurisdicción coactiva de la Contraloría General de la república crea un laboratorio de Informática Forense con el fin de determinar actos ilícitos o fraudes donde el patrimonio del estado está en riesgo”(Restrepo, A. (2008), de esta manera en el año 2004 se empieza hablar de temas de investigación criminal forense en Colombia y que para efectos en años posteriores, el estado Colombiano desarrollaría normatividad en lo que concierne a la seguridad de la información, entre otras normas que más adelante se ampliarán.

Porque llega a Colombia

El desarrollo tecnológico que se genera día a día no solo trae consigo aspectos positivos, sino que por el contrario en ocasiones estas nuevas formas de tecnología son usadas de manera incorrecta. Este es el caso del auge de las computadoras y de las tecnologías de la información (de ahora en adelante TI), cuyas herramientas han sido usadas por delincuentes informáticos muy bien preparados y con suficientes conocimientos en las TI, y que cada vez encuentran nuevas formas para continuar con su accionar, estos delincuentes son conocidos popularmente como **Hackers**, sin embargo el concepto de este término debe ampliarse para no generar ambigüedad en la comprensión del mismo, pues esta palabra en realidad hace referencia a "personas aficionadas a la tecnología y que se sienten bien resolviendo problemas tecnológicos", (S.d., S.f), así como "persona apasionada, curiosa, dedicada, libre, comprometida con el aprendizaje y con enormes deseos de mejorar sus habilidades y conocimientos." (s.d., s.f), por lo anterior el término adecuado para atribuir delitos de tipo informático es a los llamados **Crackers** o hackers de sombrero negro y a continuación se definirá desde la información tomada en el artículo del concepto anteriormente mencionado en este mismo párrafo. Los crackers están definidos como "personas que consiguen ganar acceso a sistemas por medio de mecanismos agresivos, como por ejemplo ataques de fuerza bruta para la obtención de una cuenta de usuario o incluso técnicas mucho más sofisticadas"; algunas de estas técnicas que incluyen desde el robo de información específicamente de los datos personales de clientes de Bancos como; contraseñas, números de cuentas, etc., y que técnicamente en la actualidad son conocidas con los nombres de: sabotaje informático, grooming, ingeniería social, skimming y entre otras acciones que interrumpen el desarrollo normal de las operaciones de una empresa, persona, sistema, comunidad, etc…

Como ejemplo claro de la problemática que vivió el país, es importante resaltar y mencionar las acciones llevadas a cabo por la Dijín en pro de contrarrestar el accionar delictivo. Estos hechos dieron a lugar en el territorio nacional e ilustra que "En 2006 el grupo de delitos informáticos de la Dijín realizó 433 investigaciones de ciberdelincuencia en el país, y a septiembre de 2007, se han conocido 85 amenazas virtuales, 25 casos de pornografía, 381 de fraude electrónico, ocho de extorsión y 16 de phishing." (Restrepo, A. (2008). Por otra parte este mismo autor menciona que en el año 2007, en Colombia las empresas perdieron 6.6 billones de pesos a raíz de delitos informáticos, de las cuentas de personas naturales se llegaron a sustraer 311 mil millones de pesos, situación que originó el aumento en un 71% de la ciberdelincuencia respecto al año

anterior. En la Figura (1) se logra evidenciar el aumento presentado año tras año por delitos informáticos en Colombia debido al incremento de usos de la tecnología.

Figura (1)

Ilustración 1 Histórico de delitos informáticos

(Villamizar, et al. Histórico de delitos Informáticos. [Figura]Recuperado de: file:///C:/Users/DIEGO/Downloads/1122-1142-1-PB%20(1).pdf

Por lo anteriormente sustentado fue necesario que se realizarán acciones en pro del refuerzo y favorecimiento de la seguridad, para ello llegó a Colombia la Informática Forense, que desde entonces apoya en el país las labores de investigación criminal en medios informáticos.

Primer caso de AFD en Colombia

Como se mencionó anteriormente, en el año 2004 se crearon las entidades de apoyo en temas de Seguridad Informática, quienes desde entonces han realizado varias investigaciones desde su momento, algunas de ellas se desarrollaron durante el transcurso del año 2006, sin embargo es importante resaltar uno de los más importantes casos de labores de Investigación Forense en el país. Una de ellas fue en el año 2008, cuando las Fuerzas Militares de Colombia llevaron a cabo la operación Fénix, donde incautaron los computadores del integrante de las Fuerzas Armadas Revolucionarias de Colombia (FARC) Raúl Reyes, “Según el Ministro de Defensa de Colombia, Juan Manuel Santos, los investigadores hallaron más de 16.000 archivos en los tres computadores portátiles encontrados en el campamento donde murió Reyes, informó el diario The New York Times.” (Piñeros, G. (2008), y que posteriormente especialistas de informática de la Fiscalía sometieron estos elementos a exhaustivos análisis a fin de extraer toda la información posible.

En este mismo artículo se menciona que en 2006 se presentó el caso del jefe paramilitar Jorge 40, donde durante un mes los especialistas en informática de la Fiscalía y con el apoyo de expertos de Estados Unidos de Norteamérica (EE UU), lograron extraer del computador del jefe paramilitar algunos datos, los cuales posteriormente iniciaron el escándalo conocido como la parapolítica, que tiene a un gran número de congresistas Colombianos detenidos.

Por último ejemplo y bajo la misma fuente de información, se encuentran datos sobre el computador portátil de Iván Ríos, miembro del Secretariado de las FARC, quien fue asesinado por uno de sus subalternos y al realizar los Análisis de Investigación Forense de su computador, las autoridades hallaron datos que informaron que; entre el 2005 y el 2007, Ríos ordenó más de 200 asesinatos, entre sus víctimas habían personas que él consideró en su momento como infiltradas del Ejército y de las Autodefensas.

Estado

Histórico de algunos casos de AFD presentados

Reconociendo la importancia de las evidencias digitales para aclarar y resolver casos judiciales, a continuación se describirán algunos procesos en los cuales fue clave la presencia, análisis y custodia de las pruebas digitales para resolver satisfactoriamente delitos informáticos.

El 8 de octubre de 2015 se dio captura en Caldas (Antioquia) a alias “gemido ruidoso”, un joven de 27 años de edad sindicado por el delito de Grooming, gracias a la investigación y seguimiento realizado por el Centro Cibernético Policial de la DIJÌN el cual logró su rastreo en internet, además de evidencias digitales encontradas en discos duros de computadores, CD´s y otros equipos digitales; logrando hallar 84.850 imágenes y videos los cuales fueron pieza clave para su captura y posterior judicialización, durante la investigación se estableció que alias gemido ruidoso distribuía material pornográfico en el país y en el Reino Unido por medio de correos electrónicos a organizaciones dedicadas al tráfico de pornografía infantil. (S.d., 7 de junio de 2015).

Otro caso importante y resuelto por el Centro Cibernético policial, fue el relacionado con la captura de la organización delincuencial dedicada a realizar defraudaciones millonarias a través de medios informáticos en diferentes entidades financieras, el hurto fue de aproximadamente

diez mil millones de pesos afectando 326 cuentas financieras, la modalidad delictiva empleada por esta organización criminal, consistía en el desarrollo de programas informáticos especializados llamados (MALWARE), que aprovechan las vulnerabilidades que ofrece la banca online y el uso desprevenido de dichos servicios por parte de los usuarios para el apoderamiento de información personal y privilegiada; como lo son números de cuentas, contraseñas, cédulas, entre otros datos de productos financieros que son utilizados posteriormente para realizar la sustracción de los dineros. (S.d., s.f).

Adalid Corp. (Organización dedicada al Análisis Forense Digital), analiza las pruebas en el caso de un joven que denunció ante las autoridades a un funcionario de una entidad de salud por fotografiarlo desnudo en medio de un examen oftalmológico. Su abogado defensor el Dr. Andrés Guzmán Caballero, fue entrevistado por Caracol Noticias y asegura que el equipo de Adalid Corp. Colombia, en su laboratorio forense realizó el análisis de la memoria Micro SD del sindicado, descubriendo más de 40 fotografías de otras personas también desnudas. (S.d., s.f).

Situando en funcionamiento los laboratorios creados para uso del CTI, se logró la captura de los autores de una compleja modalidad de hurto informático en el comercio en línea, quienes por medio de una tarjeta de crédito de la víctima (un reconocido empresario), consiguieron llevar a cabo un hurto por valor de 14 millones de pesos de una de sus cuentas bancarias. El hurto fue cometido con la tarjeta de crédito de la víctima, que sólo se percató del robo al ver su extracto personal, con ella los delincuentes adquirieron en tan sólo dos días, seis procesadores portátiles, en una empresa que brinda el servicio de pago en línea (funciona como un datafono virtual). Con esa información, los agentes se desplazaron a esa empresa, en el centro de Bogotá, y con la autorización de un juez de control de garantías, analizaron con herramientas de hardware y software de última generación, los computadores utilizados para la venta de productos en el internet.

Lo que buscaban los agentes del CTI era Ubicar la dirección IP del computador utilizado por los delincuentes para hacer la compra. La novedad del caso es que la técnica utilizada por los agentes del CTI facilitó rastrear la dirección IP o rastreo de direccionamiento; el cual es un número de identificación que tienen todos los procesadores del mundo y queda registrada cada vez que ingresa a la autopista virtual del internet, lo que le permitió a investigadores del CTI de

Bogotá descubrir y capturar a los autores de una compleja modalidad de hurto informático en el comercio en línea. (Lombo, M. (17 de julio de 2007, p.18-19.)

Liderazgo de Colombia en Ciberseguridad

En el país se inicia a hablar fuertemente del tema desde la creación del documento CONPES 3701 de 2011 en el cual pretenden contrarrestar los casos de amenazas informáticas que en su momento estaban en incremento, motivo por el cual dicho documento se conforma pensando estrictamente en el posicionamiento nacional del tema Ciberseguridad y Ciberdefensa.

Por lo tanto, tras la divulgación del CONPES 3701 se logra observar los avances obtenidos en Colombia en el tema logrando así posicionarse dentro de los 5 primeros países con mejores prácticas en seguridad como lo revela la corporación Colombia digital en su artículo Colombia en el top 5 de Ciberseguridad en Latinoamérica, donde exponen que la Unión Internacional de Telecomunicaciones (UIT), público los resultados del Índice Mundial de Ciberseguridad (IMC), investigación que mediante 5 ámbitos de trabajo clasifica a cada uno de los países, estos ítems evaluados son:

- Medidas legales
- Medidas técnicas
- Medidas organizacionales
- Capacitación
- Cooperación

Es así que Colombia logra posicionarse en el quinto lugar superando a México, Argentina y otros grandes países de América así como quedando por debajo de Brasil, Estados Unidos, Uruguay y Canadá como se observa en la siguiente gráfica.

Figura (2)

Americas	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
United States of America*	1.0000	0.8333	0.8750	1.0000	0.5000	0.8235	1
Canada*	0.7500	1.0000	0.8750	0.8750	0.5000	0.7941	2
Brazil	0.7500	0.6667	0.8750	0.7500	0.5000	0.7059	3
Uruguay	1.0000	0.6667	0.6250	0.5000	0.5000	0.6176	4
Colombia	0.7500	0.5000	0.7500	0.7500	0.2500	0.5882	5
Argentina*	1.0000	0.3333	0.3750	0.5000	0.1250	0.4118	6
Chile*	0.7500	0.5000	0.2500	0.3750	0.2500	0.3824	7
Costa Rica*	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	8
Ecuador	0.2500	0.6667	0.1250	0.5000	0.2500	0.3529	8
Mexico*	0.2500	0.5000	0.1250	0.3750	0.3750	0.3235	9

Ilustración 2 Ciberseguridad en Latinoamérica

Tomado de Colombia Digital, Colombia en el top 5 de ciberseguridad en Latinoamérica.

Consultado el 10 de Junio de 2016

Además a nivel mundial Colombia logra posicionarse en el noveno puesto, dejando ver los extraordinarios resultados que ha generado el plan de gobierno establecido en el país para el tema de Ciberseguridad. Por otro lado frente al liderazgo de Colombia se puede deducir que aunque el año 2004 fue cuando llegó el AFD al país y que por medio del CONPES 3701 se da mayor fuerza a temas normativos, aún el desarrollo del tema es regular, por tal razón es importante resaltar que teniendo en cuenta la historia de la Informática Forense que inicia desde 1980; se logra determinar que este tema tiene como antecedentes 36 años en el mundo como origen Estados Unidos y Colombia; quien cuenta con un desarrollo en el país de escasos 12 años que equivalen a menos de la mitad de la experiencia y experticia con la que cuenta el primer país nombrado.

Vulnerabilidad en Colombia

El CONPES 3854 menciona que un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo hacktivista autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en línea y de los Ministerios del Interior, de Justicia, de Cultura y de Defensa, dejando fuera de servicio sus páginas web por varias horas.

A continuación se ilustrara en varios gráficos información tomada del diagnóstico realizado en el CONPES 3854, la cual detalla claramente la vulnerabilidad y la gestión realizada en Colombia.

En la figura (3), se observa claramente los sectores económicos que son afectados por los delincuentes.

Figura (3)

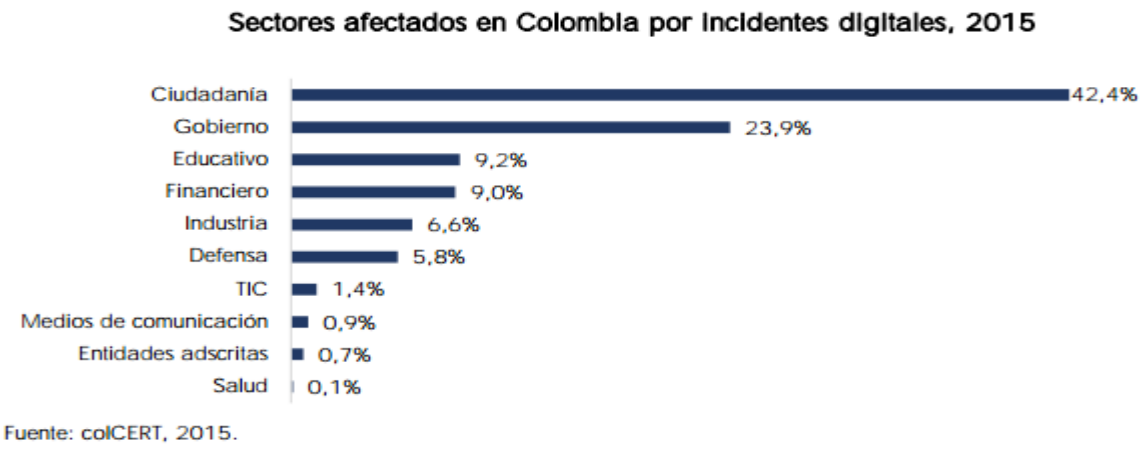


Ilustración 3 Sectores afectados en Colombia por incidentes digitales, 2015

CONPES 3854(2016) Política Nacional de Seguridad Digital

En el anterior gráfico se logra evidenciar que el sector de las TIC y el financiero es regularmente víctima de afectaciones, sin embargo el ciudadano es el principal objetivo de los delincuentes, situación que es obvia debido a que la ciudadanía no cuenta en su mayoría con sistemas de protección eficientes que garanticen la no vulnerabilidad de sus bienes.

El figura (4) detalla los incidentes de tipo informático que fueron gestionados por el Comando Conjunto Cibernético del comando General de las Fuerzas Militares de Colombia y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia durante el año 2015.

Figura (4)

Ilustración 4 Incidentes digitales gestionados por el CCOC y el colCERT en el entorno digital en Colombia, 2015

CONPES 3854(2016) Política Nacional de Seguridad Digital

El figura (5) detalla los incidentes de tipo informático que fueron gestionados por el Centro Cibernético Policial de la Policía Nacional de Colombia y el Equipo de Respuestas ante Incidentes de Seguridad de la Policía Nacional de Colombia durante el año 2015.

Figura (5)

Ilustración 5 Incidentes gestionados por la CCP y CSIRT PONAL en el entorno digital en Colombia, 2015

CONPES 3854(2016) Política Nacional de Seguridad Digital

La figura (6) detalla las capturas y denuncias sobre delitos informáticos que se presentaron durante los años 2014 – 2015.

Figura (6)

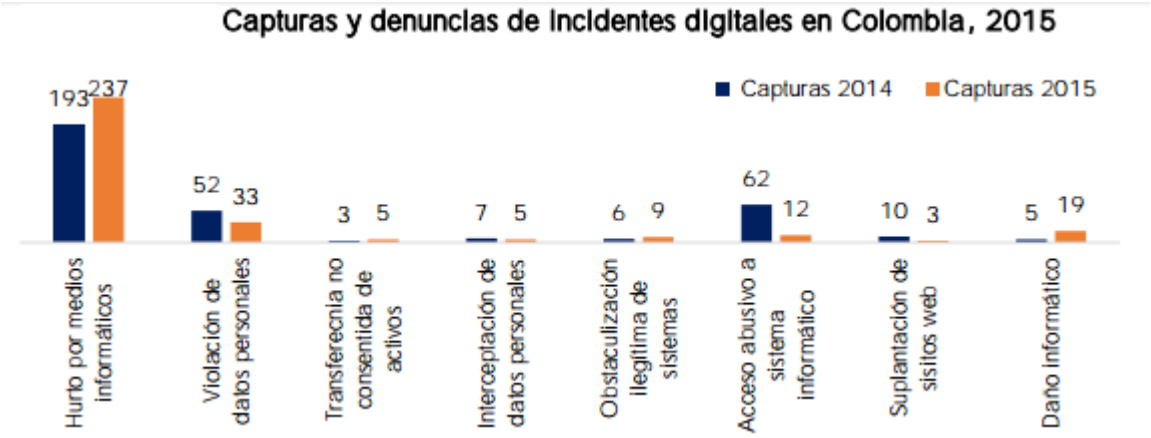
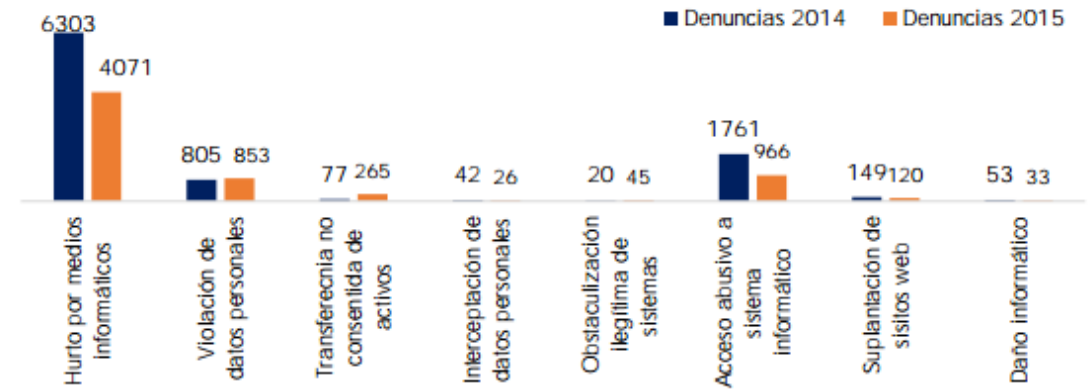


Figura (6)



Fuente: CCP, 2015.

Ilustración 6 Capturas y denuncias de incidentes digitales en Colombia, 2015

CONPES 3854(2016) Política Nacional de Seguridad Digital

En esta figura se evidencia que el total de denuncias realizadas entre los años 2014 – 2015 por delitos de tipo informático son aproximadamente 15589, y las capturas realizadas durante este mismo periodo son de aproximadamente 661, cifra que equivale a un 4.24% de gestión efectiva sobre estos delitos que terminaron exitosos. Otro dato a resaltar es que la mayor cantidad de

casos gestionados corresponden a hurto por medios informáticos, violación de datos personales y acceso abusivo a sistema informático, los cuales están contemplados en la Ley 1273 de 2009.

Empresas y entidades dedicadas al análisis de evidencias digitales en Colombia

En Colombia a raíz de la problemática en el tema, han surgido empresas las cuales brindan sus servicios a grandes organizaciones o población en general, como es el ejemplo de la empresa Digital center, Adalid Corp., Asoto Group y el Centro Cibernético Policial, entre otras, las cuales desde sus diferentes ámbitos de aplicación o especialización prestan apoyo con el fin de erradicar o contrarrestar los delitos informáticos que se presentan. Consultar Gráfico (7)

Figura (7)

	**DIGITAL ENTER**	**ADALID CORP**	**CENTRO CIBERNETICO POLICIAL**	**ASOTO GROUP**
AÑOS DE SERVICIO	21 Años	10 Años	14 Años	20 Años
ESPECIALIZACIÓN	Líder en recuperación profesional de datos	Especialistas en nuevas tecnologías	Investigación y prevención de delitos cibernéticos	Recuperación de datos
SERVICIOS	• Recuperación de datos • Back up en sitio o remoto • Análisis Forense Digital • Borrado total y permanente de archivos • Peritaje informático • Reciclaje de medios	• Servicio de laboratorio • Asesoría Técnica y legal ISO 27001 • Investigación de Fraude empresarial • Protección de marcas y personas por Internet • Ethical Hacking	• Caí Virtual • Laboratorio de informática Forense • Investigación de casos de Cibercrimen y Ciberseguridad	• Laboratorio Forense Digital • Seguridad Informática • Recuperación de datos Cadena de custodia para casos Forenses

Ilustración 7 Principales organizaciones de Análisis Forense Digital en Colombia, Autores: Torres, L y Jaramillo, D (2016)

Así mismo, encontramos que en el país fueron instaurados cinco (5) laboratorios informáticos forenses ubicados en Medellín, Bucaramanga, Bogotá, Pereira y Cali los cuales se encuentran dotados con computadoras portátiles, torres y herramientas para su funcionamiento tanto en Hardware como Software, dichos equipos permiten recoger evidencias digitales, recuperar archivos, imágenes y correos, todo con el fin principal de mejorar el tratamiento de la evidencia digital en los procesos penales. (Lombo, M. (17 de julio de 2007).

Capítulo IV - Marco jurídico de la Informática Forense

Debido al aumento de casos de ciberdelincuencia y las innumerables pérdidas que se presentaron, se ha establecido legislación en temas de Seguridad Informática, sin embargo es importante resaltar que en este tema se mencionan normas que en determinado momento pueden favorecer o entorpecer a la metodología de Análisis Forense Digital, y además no se evidencian muchas normas que guarden relación con el tema AFD a excepción de La Resolución Reglamentaria 202 de 2012, algunas de estas se ampliarán a continuación.

Es importante lo que se evidencia en el diagnóstico incluido en el CONPES 3854, el cual se logra detallar que el nivel de la normatividad Colombiana frente al tema sobre delitos informáticos aún no está ni en el nivel estratégico; lo cual indica que en el país existe normatividad legal relacionada al tema a tratar, pero aún no se encuentra en un nivel dinámico que garantice la efectividad de la misma. En la figura (2) detalla el nivel de madurez que hay en Colombia frente a la normativa legal, la fuente de información es el diagnóstico realizado en el CONPES 3854.

Figura (8)

Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia, 2015

	Nivel de madurez[a]				
	Inicial	Formativo	Establecido	Estratégico	Dinámico
Marcos jurídicos de seguridad cibernética					
Para la seguridad de las TIC	■	■			
Privacidad, protección de datos y otros derechos humanos	■	■	■		
Derecho sustantivo de delincuencia cibernética	■	■	■		
Derecho procesal de delincuencia cibernética	■	■	■		
Investigación jurídica					
Cumplimiento de la ley	■	■	■		
Fiscalía	■	■			
Tribunales	■	■			
Divulgación responsable de la información					
Divulgación responsable de la información	■				

Fuente: BID & OEA (2016).

Ilustración 8 Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia, 2015

CONPES 3854(2016) Política Nacional de Seguridad Digital

Ley 527 de 1999

Donde se encuentra información relacionada al Derecho Probatorio y medios electrónicos. Esta ley es más conocida como ley de comercio electrónico, sin embargo en el tema de AFD se puede mencionar que el artículo diez (10) de dicha norma indica “Admisibilidad y fuerza probatoria de los mensajes de datos”. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil”, para este caso de lo anteriormente mencionado se cita el ARTÍCULO 251.“Distintas clases de documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares” Decreto 1400 DE 1970 (Agosto 06)Por el cual se expide el Código de Procedimiento Civil".

Por otro lado el artículo once (11) menciona “Criterio para valorar probatoriamente un mensaje de datos”. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente..”(Ley 527 de 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, Colombia, 18 de Agosto de 1999.)

Sentencia C-662/2000

En la cual es importante resaltar una parte del texto donde menciona que los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y en la mayoría de los casos, un mayor grado de confiabilidad y rapidez , además en esta sentencia el

Magistrado Fabio Morón Díaz hizo las siguientes consideraciones respecto a la constitucionalidad de ley 527 de 1999, dentro de las cuales resalta que “el mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento”, por lo tanto aporta un carácter de igualdad a todo aquel elemento material probatorio de carácter digital frente a los documentos físicos, escritos, fotos, entre otros que no cumplen con las mismas características de datos informáticos. (Constitucional, C. sentencia C-662 de 2000. *Magistrado Ponente Dr. Fabio Morón Díaz*.)

Ley estatutaria 1266 del 31 de diciembre de 2008

El objeto de esta norma se refiere al desarrollo de dos derechos constitucionales, uno de ellos consagrado en el artículo quince (15) de la Constitución Política de Colombia, el cual indica que “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. “de igual modo se tiene derecho a conocer, actualizar y rectificar las informaciones que estén inmersas en los bancos de datos y archivos de entidades públicas y privadas, así como los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de dichos datos. Esta norma define principios para la administración de datos personales, derechos de los ciudadanos titulares de la información, deberes de los operadores, las fuentes y usuarios de la información, para que de esta manera la información de los ciudadanos reciba un tratamiento y manejo adecuado por parte de quienes la custodian.

(Datas, L. H., & Estatutaria, L. 1266 de 2008, Congreso de la República. Diario Oficial No. 47.219 de 31 de diciembre de 2008.)

Ley 1273 de 2009

Esta norma define los atentados generados por la delincuencia a los sistemas de información, específicamente a los principios de confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos, dentro de los cuales se encuentra el acceso abusivo a un sistema informático, interceptación o violación de datos, daño informático, suplantación de sitios web, entre otros y además define las circunstancias que pueden agravar la pena. Por consiguiente define dos atentados informáticos y son: el hurto por medios informáticos y semejantes, y la transferencia no consentida de activos, lo anterior son acciones de las cuales han sido víctimas ciudadanos, organizaciones y gobiernos. (Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, Colombia, 5 de Enero de 2009)

En el artículo sobre delitos informáticos publicado por el periódico El universal, el señor Fabio Herrera, ingeniero del Grupo de Delitos Informáticos, dependencia adscrita al CTI de la Fiscalía General de la Nación; explica además que la ley 1273 de 2009, se ha fortalecido logrando así judicializar a delincuentes con penas entre cuatro (4) y ocho (8) años de cárcel y que “A esto se le suma el agravante de utilizar medios electrónicos para dicho fin, lo que le puede dar hasta 12 años de prisión. Según Herrera, estas conductas vienen unidas a delitos como el concierto para delinquir, hurto agravado y calificado.”, de esta manera evidenciando que cada vez son más los casos que son investigados y que terminan a favor de las víctimas. ” (Rodríguez Johana. (2014).

Ley 1453 de 2011

En esta norma para efectos legales sobre delitos informáticos, se evidencia que en su artículo 236 señala en lo referente a recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones.

> "Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en Informática Forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado." (Ley 1453. por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad, Colombia, Junio 24 de 2011)

Resolución reglamentaria 202 de 2012

Por la cual se da la disposición de crear el Grupo de Laboratorio de Informática Forense (LIF) como apoyo a los diferentes procesos que adelanta la Contraloría General, en la evidencia y documentos que se obtengan de las diferentes actuaciones de vigilancia y control fiscal.

Dicho apoyo será realizado mediante la identificación, preservación, análisis y presentación de evidencia digital con el fin de que el elemento material probatorio sea aceptado, permitiendo lograr los resultados esperados por la Contraloría. (Resolución reglamentaria 202 de 2012. Por la cual se deroga la Resolución Reglamentaria 126 de 2011 y se crea el grupo de Laboratorio de Informática Forense (LIF), adscrito al Despacho del Vice contralor, Colombia, 7 de Diciembre de 2012).

Ley 1564 de 2012 – Código general del proceso

En lo que respecta a este código, solo se mencionara la información relacionada con AFD, y para ello se iniciará con el artículo 165, donde se mencionan los medios de prueba e indica que "Son medios de prueba la declaración de parte, la confesión, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios, los informes y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez. El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio, preservando los principios y garantías constitucionales.", sin embargo el juez debe evaluar su autenticidad y seguridad, para lo cual estas evidencias deben cumplir con las características de admisibilidad de evidencia digital anteriormente mencionadas y así de esta manera se pueda convencer al juez que tiene a cargo el proceso. En lo que concierne a pruebas documentales el artículo 243, establece distintas clases de documentos, los cuales define como "Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares". Por otro lado sobre la prueba pericial, el artículo 226, el cual menciona sobre la **Procedencia**. La prueba pericial es procedente para verificar hechos que interesen al proceso y requieran especiales conocimientos científicos, técnicos o artísticos. Sobre un mismo hecho o materia cada sujeto procesal sólo podrá presentar un dictamen pericial. Todo dictamen se rendirá por un perito.", de acuerdo a lo anterior los jueces están facultados para solicitar el concepto de peritajes informáticos y de esta manera aportar información y elementos importantes que pueden ser definitivos en estos casos. (Del Proceso, C. G. Ley 1564 de 2012. In *Congreso De La Republica de Colombia*, *Art* (Vol. 422).

Ley estatutaria 1581 de 2012

Dicha norma es también garante de los derechos contemplados en los artículos 15 y 20 de la Constitución Política de Colombia, pero además habla sobre un régimen general de protección de

datos personales aplicable a todas las bases de datos personales de empresas públicas y privadas que almacenen y utilicen datos personales, sin importar su actividad económica. No obstante resalta ciertas excepciones a la norma, como lo es la información de Seguridad Nacional, inteligencia y contrainteligencia, las de contenido periodístico y de censos, y como carácter adicional define dos categorías especiales de datos; los sensibles, que afectan la intimidad de las personas, lo cual puede generar discriminación; y los datos personales de niños, niñas y adolescentes, los cuales deberán ser administrados de forma estricta. (Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Colombia, 18 de Octubre de 2012)

Decreto 1377 de 2013

Este decreto se crea básicamente para facilitar la implementación y cumplimiento de la ley 1581 de 2012, la cual brinda políticas con las que deben contar los responsables y encargados que manejan datos personales para dar un adecuado tratamiento a estos, previa autorización del titular de la información. (Decreto 1377 de 2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Colombia, 27 de Junio de 2013)

Capítulo V – Análisis de la información obtenida

Luego de documentar toda la información correspondiente al tema de Análisis Forense Digital, es indispensable realizar un análisis de todo lo documentado y por ello se dará paso para describir los hallazgos, iniciando desde el capítulo de marco teórico, donde se debe resaltar que la Informática Forense actualmente abarca varios campos de acción donde es importante resaltar que el tema de Análisis Forense Digital tiene otro campo de aplicación, en el cual se hace fundamental su conocimiento y por ello es que se hace necesaria una técnica especializada para la telefonía móvil, pues actualmente abundan las modalidades y los delitos cometidos por este medio y además ya se cuenta con una serie de herramientas de recuperación forense en telefonía móvil según y cómo se describen en las 165 páginas del documento Cell Phone Forensic Tools: An overview and Analysis Update, donde se mencionan aproximadamente 15 tipos de Herramientas. (Guerrero, A. (2009, p 105-107), las cuales apoyan el AFD logrando así minimizar las acciones delincuenciales en medios informáticos. Por otro lado y como se evidenció, son grandes las ventajas que proporciona en Análisis Forense Digital, pero está a su vez para que se desarrolle bien debe ser llevada a cabo por personal idóneo, competente y que sobre todo cuente los recursos físicos y tecnológicos.

En cuanto a la evidencia computacional, se puede decir que esta es única, cuando se la compara con otras formas de "evidencia documental", a diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original, además otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario. (Guerrero, A. (2009, p 105-107) No obstante, es importante mencionar que la evidencia digital es frágil, debido a que puede ser objeto de manipulación y modificación, además que en ocasiones se puede dificultar la recolección y análisis, debido a su facilidad de reproducción y cambio o que algunas de estas evidencias son anónimas; como las generadas en páginas web, que no tienen información detallada de su autor. Lo anterior puede convertirse en una desventaja para el sistema judicial y por ello estaría en contravía de lo que se

mencionó anteriormente en las características con las cuales debe cumplir una evidencia digital, para que esta sea tomada en cuenta o sea válida a la hora de un proceso penal.

En cuanto al proceso para la recolección de evidencia, los autores del artículo de Framework consideran que es indispensable tomar a consideración las buenas prácticas para el manejo de la evidencia y que debido a la inexistencia de procedimientos oficiales avalados para este fin, sugieren que se tome como referencia el RFC 3227, guidelines for Evidence Collection and Archiving, la cual se describe como una buena guía para la recolección de la evidencia digital, la cual según la guía inicia desde la información más volátil; que es la contenida en memoria RAM, memoria cache, tablas de procesos y de enrutamiento, entradas ARP y sistemas de archivos temporales, y finalmente recolectar la información menos volátil como la contenida en sistema de archivos y topologías de red. Por tal razón y como se evidencia en el proceso para la recolección de evidencias digitales en Colombia, aún no se tiene definido un estándar.

Como se ilustró en la definición de AFD, se evidencia que esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. No obstante y según lo descrito anteriormente en la estructura del computador para uso forense donde se indica el costo en dólares del software y hardware con el cual deben contar los equipos cuyos valores oscilan en los U$ 60.000 Dólares, y por consiguiente se logra evidenciar que la inversión para realizar estas actividades son demasiado altas, lo anterior es debido a que basándose en el precio del Dólar consultado para la fecha del día 20 de Junio de 2016 que equivale a $ 3.010,91 pesos Colombianos, la suma total sería de $ 180´654.600 para un equipo de Análisis Forense Digital, esto sin incluir costos de capacitación y formación de personal idóneo para el tema, los cuales como según refiere Carlos Álvarez un abogado en derecho informático y propiedad intelectual los costos aproximados para la formación de un perito forense son de $ 50´000.000 pesos Colombianos, sin embargo es enfático en resaltar que estas labores de investigación son realizadas por policías y no ingenieros de sistemas, por lo cual esta inversión en ocasiones se pierde debido a la rotación de personal que hay en la institución, lo anterior es tomado como fuente del artículo citado anteriormente: “Los detectives de la era digital”.

Para dar mayor apoyo de sustentación a lo descrito por el abogado Carlos Álvarez, se mencionara primero el documento CONPES 3701, donde como parte del problema central nos muestran una gran falencia con la que se cuenta en el país, como describe este documento "El entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la Comisión de los Delitos Informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de análisis forenses, de igual manera que existe una oferta limitada de programas de capacitación para entidades que realizan funciones de Policía Judicial en el tema", por lo tanto se basan en dichas falencias para proponer las contramedidas que protejan la infraestructura crítica nacional, diseñar y ejecutar planes para la Ciberseguridad y Ciberdefensa y fortalecer la normatividad existente y cumplimiento de la misma. En segundo lugar se resalta lo descrito en el CONPES 3854 que dentro de las falencias se identifica que los organismos, instancias y entidades encargadas del análisis, identificación, prevención, investigación y persecución al Cibercrimen y la Ciberdelincuencia en el país, no cuentan con los recursos humanos, técnicos y financieros suficientes para enfrentar nuevos tipos de crimen y delincuencia a nivel nacional y transnacional. Tampoco se basan en la gestión de riesgos de Seguridad Digital, lo que ocasiona mayor oportunidad para la materialización de amenazas cibernéticas, situación que resulta aún más preocupante si se tiene en cuenta que los esfuerzos de las entidades en el desarrollo de temas relacionados con investigación, desarrollo e innovación no son suficientes con relación a las necesidades y avances que se tienen de forma cotidiana en ataques cibernéticos, hecho que repercute en la capacidad que tiene el Gobierno Nacional para afrontar las amenazas cibernéticas a las que está constantemente expuesto.

En aspectos como la investigación jurídica, Colombia quedó clasificada en un nivel formativo para la fiscalía, por ejemplo. CONPES (2016) "De esta forma se identifica que el número de fiscales capacitados para lograr construir un caso validado sobre pruebas electrónicas es limitado. Lo anterior, porque a pesar que se han tenido algunos programas de formación especializada, aún hace falta institucionalizar estos esfuerzos y ampliar los mecanismos de colaboración entre la Fiscalía y la Policía, obteniendo de esta forma un apoyo en la resolución de casos de delitos cibernéticos". (p.42).

Además es importante resaltar lo descrito en el CONPES 3854, donde describen que Colombia cuenta con aliados internacionales para la colaboración en temas de Seguridad Informática y por tal razón señala que la Policía Nacional a través del CCP (Centro Cibernético Policial de la Policía Nacional de Colombia) sostiene relaciones de cooperación internacional con organismos tales como: Organización Internacional de Policía Criminal (INTERPOL), la Oficina Federal de Investigaciones de los Estados Unidos (FBI), la Administración para el Control de Drogas de los Estados Unidos (DEA), el Centro Europeo contra el Cibercrimen (EC3), la Comunidad de Policías de América (AMERIPOL), la Agencia Internacional de Cooperación Coreana (KOICA), la Agencia Nacional contra el crimen del Reino Unido (NCA), el Grupo de Trabajo Americano de delitos Tecnológicos del INTERPOL (GLDTA) y el Programa de Asistencia Anti-Terrorismo de Estados Unidos (ATA); todos estos organismos trabajando en conjunto a fin de combatir el Cibercrimen. Por otro lado este CONPES ilustra que Colombia cuenta con ocho CSIRT (Equipos de Respuestas ante Incidentes de Seguridad) con membresía en el Foro de equipos de seguridad y respuesta de incidentes, llamado FIRST14 (es la principal organización mundial y líder reconocido en respuesta a incidentes digitales), lo cual les permite responder de manera más eficaz a incidentes de seguridad, al tener acceso a información acerca de las mejores prácticas, además de ser invitados a eventos y a capacitaciones y cursos relacionados con la seguridad digital. (CONPES 3854, Política Nacional de Seguridad Digital, Bogotá, 11 de Abril de 2016, p 16).

Por otro lado en materia de cooperación nacional el CONPES 3854 resalta que, el CCOC (Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia) viene adelantando el proceso de elaboración del catálogo de infraestructuras críticas cibernéticas nacionales en el país el cual permitirá, a futuro, coordinar y gestionar los planes y programas de protección y defensa a infraestructuras críticas cibernéticas nacionales. (p16).

Finalmente es necesario ilustrar uno de los aspectos que contempla el CONPES 3854 dentro de sus objetivos específicos: (CONPES 3854, Política Nacional de Seguridad Digital, Bogotá, 11 de Abril de 2016, p 57)

"E3.1. Fortalecer las instancias y entidades responsables de ciberseguridad (DE1)"

Esta estrategia busca contribuir en la construcción de un marco institucional adecuado en materia de ciberseguridad para gestionar la seguridad digital bajo el liderazgo del Gobierno Nacional. Es por esto que su campo de acción está definido por la primera dimensión estratégica de esta política: gobernanza de la seguridad digital.

Para tener un marco institucional adecuado en materia de ciberseguridad, en primer lugar se deben fortalecer las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del CCP de la Policía Nacional y de los organismos de Inteligencia del Estado, incluyendo la UIAF. Para esto, el Ministerio de Defensa Nacional (en el caso del CCP) y la Dirección Nacional de Inteligencia (en el caso del sector Inteligencia) elaborarán durante los años 2016 y 2017 respectivamente, un plan de fortalecimiento en el que se definirán y ponderarán las actividades puntuales que se ejecutarán para robustecer las capacidades mencionadas; se estima que el horizonte de este proyecto será hasta la vigencia 2019.

En segundo lugar y teniendo en cuenta que la investigación e innovación son herramientas fundamentales para enfrentar los continuos avances que exhiben los ataques cibernéticos y desarrollar capacidades avanzadas, se evaluará la creación de nuevas instancias en las que se desarrolle formación, investigación e innovación, especialmente en relación con capacidades técnicas inherentes a la Seguridad Digital. Estas nuevas instancias apoyarían la institucionalidad existente, separando el trabajo operativo de aquel necesario para lograr nuevos desarrollos en esta materia. Las capacidades desarrolladas por estas nuevas instancias brindarían al país mayor autonomía. Para garantizar la pertinencia de la creación de las nuevas instancias, el Ministerio de Defensa Nacional efectuará los estudios de viabilidad que sean necesarios, y creará las que resulten viables. Deberá analizar, al menos, la viabilidad de la creación de las siguientes

instancias, (CONPES 3854, Política Nacional de Seguridad Digital, Bogotá, 11 de Abril de 2016, p 58):

- Centro criptológico nacional
- Centro de excelencia de Seguridad Digital
- Centro de fusión para investigación de crímenes económicos y financieros
- Centro de comunicaciones, cómputo, control y comando para la Seguridad Digital
- Observatorio de crímenes y delitos en el entorno digital.
- Laboratorio de Informática Forense.
- Centro de investigación en Seguridad Digital.

En atención al rol que cumplen los jueces y fiscales en el proceso judicial en torno a casos relacionados con el Cibercrimen, no son suficientes las competencias técnicas de estas instancias. Se debe encaminar a construir un marco jurídico maduro que apoye los procesos judiciales, juzguen conductas de manera efectiva, apoyen procesos de investigación estructural, y cuente con la capacidad de adaptarse dinámicamente en función de las circunstancias imperantes.

El proceso probatorio requiere conocimientos sobre el alcance del tema, así un juez o un fiscal que conozca los tipos de afectaciones a la Seguridad Digital o la comisión de Delitos Cibernéticos, podrá avanzar de manera más efectiva en la investigación de estas conductas. En ese orden de ideas, la capacitación es fundamental y contribuye a una mejora en la judicialización de estas conductas.

Otro aspecto que se debe describir en lo jurídico, es que si observamos el Análisis Forense Digital que se lleva a cabo desde el aspecto estrictamente jurídico, es decir al elemento material probatorio recolectado de sistemas informáticos, donde se pretende demostrar la relación de alguna persona u organización con delitos de tipo informático, se logra observar que en Colombia en varias ocasiones no se les da el manejo o la trascendencia adecuada para la conclusión de un caso, según lo expone la revista de investigación e innovación en ingenierías de la Universidad Simón Bolívar de Cúcuta en su artículo “Análisis Forense en un sistema de información en el marco normativo Colombiano”, basado en la investigación realizada en la ciudad de Cúcuta y su departamento, se afirma que “ en Colombia los procesos judiciales en

muchos de los casos no ha constituido la evidencia digital como prueba en la resolución de los mismos, ya que los entes encargados como la Policía judicial, no han sabido llevar dichas investigaciones judiciales, determinando así el cierre de los casos trascendentales por el desconocimiento de un procedimiento que no altere la evidencia digital y la cadena de custodia. (Villamizar et al. (2015, p 1-8.)

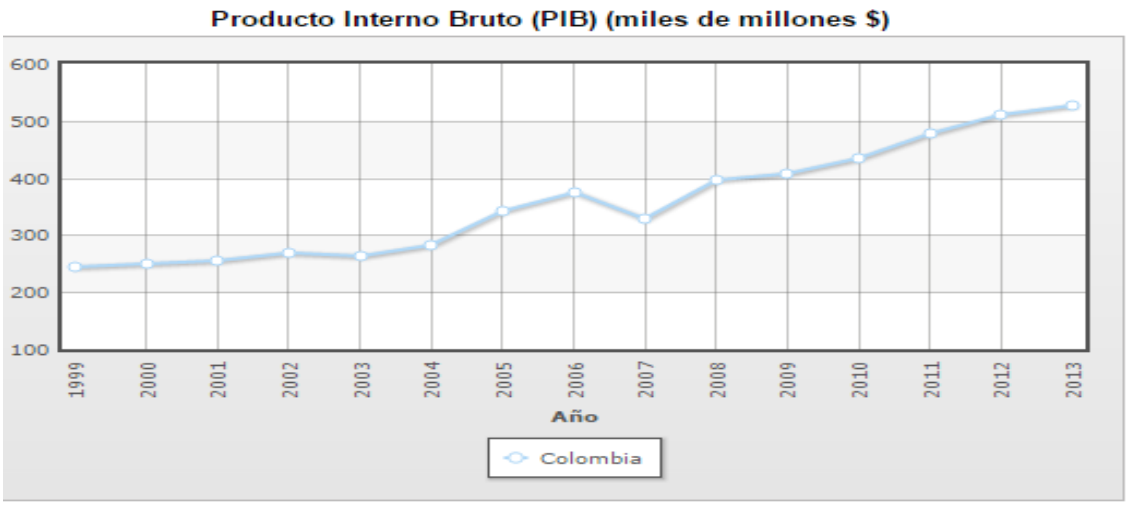
Otra de las falencias encontradas durante el proceso investigativo del tema y no menos importante, es la mencionada en el artículo Framework, donde explican que "uno de los grandes obstáculos para la aceptación de evidencia digital en Colombia, es la carencia de códigos procesales penales de normas especializadas destinadas a salvaguardar la cadena de custodia y admisibilidad de la evidencia digital. Este vacío afecta a todas las partes involucradas incluyendo al juez encargado de administrar justicia que en algunos casos por el desconocimiento e incertidumbre técnica prefiere apartarse del material probatorio digital". (Álvarez et al. (2015, p 65.) Las dificultades descritas anteriormente en cuanto a tratamiento y presentación de evidencias digitales se da además por el desconocimiento del juez tal y como se señala en el artículo Framework, donde describen que hay una técnica anti forense generalmente utilizada por la defensa para desvirtuar la solidez del material probatorio por la falta de custodia de las mismas; de igual manera otro obstáculo para la aceptación de la evidencia digital se presenta por la utilización de lenguaje técnico por parte del perito informático, lo que no permite la comprensión al juez del procedimiento y resultados arrojados durante la investigación forense digital. (Álvarez et al. (2015, p65.)

A pesar de las normas anteriormente mencionadas, se observa que en Colombia existe normatividad relacionada al tema Informático Forense, debido a que se tienen definidos e identificados ciertos delitos de este tipo, además se tiene regulación sobre la protección de datos personales en los diferentes medios de información y sobre quienes los almacenan, pero lo más importante es que Colombia quiere ser partícipe y pionero en cuanto a Ciberseguridad, sin embargo se evidencia que la delincuencia no disminuye y mucho menos se erradica, sino que por el contrario aumenta cada vez más generando grandes pérdidas como lo muestra el artículo publicado por el periódico El Tiempo, donde sustenta que "El cibercrimen representa el 15 por ciento de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el último año" esta pérdida se da durante el tiempo en el que las

empresas deben detener la continuidad de su negocio mientras son solucionados los percances generados por los ataques informáticos, poniendo en evidencia una de las problemáticas por las que se generan este tipo de delitos en las empresas, como lo es la escasa inversión y poco interés que se presta al tema de Seguridad Informática en las organizaciones, lo cual debería ser un tema esencial en cualquier entidad teniendo en cuenta que la información es uno de los activos más importantes con los que cuentan. (Tecnosfera. (2016). En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. 5 de Mayo de 2016, de EL TIEMPO)

Un aspecto importante para análisis, es lo sustentado en el capítulo del marco teórico, donde se expone en uno de los párrafos del subtitulo "Porque llega a Colombia", que en un periodo del año 2007, en Colombia las empresas perdieron 6.6 billones de pesos a raíz de delitos informáticos, de las cuentas de personas naturales se llegaron a sustraer 311 mil millones de pesos, cifra que es bastante elevada y por ello teniendo en cuenta los datos de la Figura (9), se evidencia que el PIB para el año 2007 fue de 327.700.000.000 millones de pesos y si se toma como base las pérdidas económicas para el 2007 que fueron de aproximadamente 6.6 billones de pesos, se logra estimar que dicha perdida corresponde al 4.96% del PIB para ese año. No obstante para la afirmación de pérdidas económicas por 600 millones de dólares en 2015 mencionada en el artículo del Tiempo del párrafo anterior, se aprecia que esta suma basándose en el precio del Dólar consultado para la fecha del día 20 de Junio de 2016 que equivale a $3.010,91 pesos Colombianos, daría como cifra $ 1.806.546.000.000 billones de pesos y si esta suma la comparamos con el precio del PIB del año 2013 que equivale a 526.500.000.000, (lo anterior debido a que no fue posible encontrar una cifra en miles de millones, exacta y de fuente confiable), daría como resultado 29.14% del PIB para este año. Por último análisis de este tema, es importante mostrar que esta cifra del 29.14% del PIB para el año 2013 que fueron perdidas demasiado elevadas para el país y estas comparándolas con el presupuesto que destinó para el año 2016 el entonces alcalde de Bogotá Gustavo Petro mediante decreto 517 de 2015, que estimo 16.700.000.000.000, se logra evidenciar que las pérdidas económicas corresponden al 3.15% del presupuesto destinado a Bogotá; lo cual es importante resaltar debido a que estos dineros podrían ser aprovechados para la capital Colombiana o en su defecto para diferentes zonas del país en las cuales se necesita inversión económica.

Figura (9)



2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
255	268	263,2	281,1	341,1	374,4	327,7	395,4	407,5	435,4	478	511,1	526,5

Ilustración 9 Histórico del Producto Interno Bruto en Colombia

Sd, (Sf. Recuperado de: http://www.indexmundi.com/

OCDE (Organización para la Cooperación y el Desarrollo Económico)

La OCDE (Organización para la cooperación y el desarrollo económico), se encarga de coordinar políticas económicas y sociales, contando con la ayuda de 34 países miembros quienes pretenden ayudar a países no miembros en su crecimiento económico y desarrollo de diferentes aspectos, los cuales benefician enormemente a un país como por ejemplo, en el caso de expandir sus mercados internacionalmente.

Es así que se crea esta organización con la finalidad de emitir guías y directrices que pueden ser adoptadas por los países miembros o colaboradores en busca de obtener resultados positivos, por lo tanto Colombia por encontrarse dentro de los países colaboradores de la OCDE, adopta algunas de las disposiciones emitidas por esta organización, dentro de ellas las enfocadas al tema de Seguridad Informática, donde en sus directrices dirigidas a este asunto la organización pretende brindar respuestas y soluciones al ambiente cambiante que hoy en día se viene generando en la parte de seguridad, para lo cual se tienen estipulados unos propósitos

enunciados en el documento “Directrices de la OCDE para la seguridad de sistemas y las redes de información”, dichos propósitos plasmados en las directrices establecidas procuraran llevarse a cabo para garantizar el cumplimiento de objetivos y metas.

De esta manera en Colombia dentro del Plan de Desarrollo Nacional del Presidente Juan Manuel Santos se adoptan directrices emitidas en la OCDE, dentro las cuales se adopta una de suma importancia como se nombró anteriormente y son las dirigidas a seguridad de sistemas y redes de información, estas fueron incluidas dentro del documento CONPES 3854 publicado el 11 de abril de 2016 y dirigido a la Política Nacional de Seguridad Digital, catalogando de esta manera a Colombia como “el primer país de América Latina que va a adoptar la política de seguridad digital con estándar OCDE y el séptimo en el mundo con una política tan avanzada” según lo refiere Luis Fernando Mejía, Subdirector Sectorial del DNP (Departamento de Planeación Nacional). Con el documento se pretende implementar en las empresas de carácter público y privado ambientes digitales seguros, donde puedan realizar transacciones en línea, participar de foros, interactuar virtualmente, entre otras actividades que se puedan realizar en el entorno del internet de manera segura y sin ningún tipo de temor. Es por esto que el CONPES se centra en cinco (5) frentes específicos para llevar a cabo su accionar, los cuales se basan en:

- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

La información anteriormente expuesta, es tomada como referencia de: Colombia cuenta con una política nacional de Seguridad. (13 abril de 2016).

Análisis Forense Digital en equipos móviles

Es común que en cada uno de los hogares existan dos (2), tres (3) o más dispositivos móviles, pues es el medio de comunicación más utilizado hoy en día por la humanidad, esto por la facilidad de adquisición, la comodidad de pago generada por los diferentes operadores y la variedad de servicios que estos prestan, ocasionando en la comunidad tal necesidad que se hace imprescindible obtener un equipo de este tipo.

Es tal la trascendencia que ha tenido el uso de estos dispositivos, que es muy común encontrar menores de cinco (5) o seis (6) años con equipos de alta gama de su propiedad los cuales manejan con tal desenvoltura que terminan por enseñar su manejo a los adultos. Debido a la gran acogida que ha tenido la sociedad con este tipo de tecnología, la delincuencia ha encontrado un excelente campo para desarrollar e implementar nuevas modalidades para llevar a cabo su actividad delincuencial.

Dentro de los tipos de delitos comúnmente cometidos a estos equipos encontramos:

- La clonación de Sim Card
- Smishing
- Intercambio de imágenes de pedofilia (Pornografía infantil)
- Extorsión

Motivo por el cual los diferentes organismos estatales de seguridad y protección nacional han tenido que diseñar e implementar nueva legislación para la penalización de estos delitos, además de crear técnicas de Análisis Forense para permitir la investigación y resolución favorable de los casos que día a día se registran.

Esta información se fundamenta al contemplar la información transmitida por los diferentes medios de comunicación donde relatan casos de ataques a móviles, un ejemplo de ellos es el crecimiento de trasmisión de malware en equipos móviles, lo cual es aprovechado por la ciberdelincuencia para tener acceso a cuentas bancarias, comunicación o a la vida íntima de cada persona. Verdú, D. (21 de septiembre de 2015).

Otro de los ataques generado a equipos móviles se da por medio de la vulnerabilidad generada por otros tipos de virus como por ejemplo el Stagefright 2.0 el cual se propaga y se activa en el

equipo con tan solo reproducir un video o descargar cualquier archivo. (S.d. (19 de octubre de 2015). De este tipo se encuentran múltiples noticias en los medios informativos, pues día a día continúan presentándose ataques cibernéticos que afectan a la mayoría de la humanidad debido al aumento en el uso de esta clase de dispositivos.

Documento CONPES 3701 de 2011

"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, el objetivo primordial de esta política planteada por el CONPES, va de la mano con los objetivos de defensa del país los cuales pretenden luchar contra el crimen y la delincuencia en el entorno digital. (CONPES 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa, Bogotá, 14 de Julio de 2011, pp 1-43)

Documento CONPES 3854 del año 2016

El fin primordial de este documento es generar en el país unas bases fundamentales y vigorosas con las cuales la seguridad nacional pueda contrarrestar los delitos que se vienen generando en el ámbito cibernético, dentro de los objetivos que tiene planteados se busca fomentar la cultura de seguridad en las organizaciones e individuos, previniendo, controlando y generando recomendaciones para evadir la presencia de este tipo de amenazas y buscando la manera de afrontarlos, esto teniendo completa claridad del modo de actuar ante la presencia de los mismos. De la misma forma se pretende fortalecer y generar los cambios que sean necesarios en la legislación Nacional existente, todo con el apoyo de organizaciones internacionales desde la adhesión de Colombia a los diferentes temas y procesos que se manejen. (CONPES 3854, Política Nacional de Seguridad Digital, Bogotá, 11 de Abril de 2016, pp 1-91)

Manual de cadena de custodia de la Fiscalía General de la Nación

En el marco normativo Colombiano, para el tema de procedimientos que garanticen la cadena de custodia del material probatorio, se tiene en cuenta el Manual de Procedimientos del Sistema de Cadena de Custodia, el cual fue publicado en el año 2004 por la Fiscalía General de la Nación, sin embargo es importante resaltar que dicho manual se enfoca únicamente en la evidencia física más no en la evidencia digital, por lo Álvarez et al.(2015) mencionan que se sugiere, a modo de ejemplo la acción de aseguramiento del lugar de los hechos que se refiere al aislamiento físico del material, con el propósito de que este no sea objeto de alteración; y para el caso de evidencia digital el aislamiento debe contemplar la desconexión total de la red y de los mecanismos de acceso remoto tratando de evitar el error de apagar el sistema o prenderlo(p 65).

En el mismo manual para evidencia física se encuentra la recolección, embalaje y rotulado del elemento de prueba o evidencia, donde no se tienen en cuenta los mecanismos o herramientas tecnológicas necesarias para proporcionar el embalaje adecuado a la evidencia digital y para el caso de AFD, los autores sugieren que se deben contemplar mecanismos de control para energía estática y electromagnetismo y para diferentes condiciones de ambiente como calor y humedad, los cuales pueden ocasionar la pérdida de la información (p 67).

Finalmente los autores sugieren que para la presentación del elemento en diligencia judicial, es necesaria la presencia de un perito informático, idóneo en el tema y con certificación o reconocimiento por parte de alguna organización reconocida, quien tendrá a su cargo la valoración científica de las pruebas a presentar (p 67

Capítulo VI – Conclusiones

Teniendo en cuenta la información recolectada durante el proceso de investigación sobre Análisis Forense Digital y los temas que se derivan del mismo, se realizó un análisis de los aspectos positivos y negativos lo que permitió obtener las siguientes conclusiones:

- A pesar de la normatividad existente y de la importancia que al día de hoy se le da a la Ciberseguridad y la Ciberdelincuencia en el mundo, es continuo el crecimiento de casos y modalidades en el tema, además, durante el proceso de investigación y estudio del contenido, se puede observar que en Colombia hay un déficit considerable de aspectos como normatividad, custodia y manejo de las evidencias digitales, así mismo en aspectos de formación y capacitación del personal requerido para realizar el debido proceso, lo cual no permite el desempeño eficiente del Análisis Forense Digital.

- Se hace necesario capacitar a los jueces sobre algunos aspectos técnicos que utilizan los peritos para el análisis de las pruebas, o en su defecto solicitar y recalcar en los peritos la importancia de evitar los tecnicismos y/o el lenguaje científico, usando en su lugar lenguaje claro y conciso, que permita al juez comprender los resultados que arroje el Anàlisis Forense Digital realizado a los medios informáticos y de esta manera pueda tener en cuenta este tipo de pruebas, evitando así que por inconvenientes como los ya nombrados se pierdan casos tan importantes como por ejemplo el de Raúl Reyes, en el cual fue necesario realizar análisis a equipos de cómputo .

- Se evidencia que varias de las falencias encontradas para el tema de análisis de pruebas digitales se basa en la falta de equipos y tecnologías aptas para el estudio y peritaje de las pruebas documentales y medios informáticos, sin embargo al indagar el costo real para contar con la estructura adecuada de la máquina a utilizar en temas forenses, se observa que los costos resultan ser elevados lo que nos da una razón clara de la falta de los mismos.

- Las pérdidas que deja la Ciberdelincuencia especialmente en el sector empresarial son enormes, teniendo en cuenta las cifras ya nombradas durante el desarrollo de la investigación

el tema causa graves inconvenientes en la economía del País, lo cual resulta preocupante considerando que el porcentaje de pérdidas podría ser empleado para generar soluciones efectivas al tema.

- Si bien es cierto que cualquier tema debe trabajarse desde el ámbito preventivo en busca de evitar que se presenten dificultades, de la misma manera se hace importante la intervención que se haga posterior al inconveniente que haya acontecido y así generar soluciones, esto con el fin de descubrir el modus operandi de las organizaciones delictivas, es allí donde se visualiza la importancia del AFD en la investigación y resolución de casos, a lo cual no se le ha dado la relevancia necesaria teniendo en cuenta que en el documento conpes 3701 fueron evidenciadas algunas fallas en el proceso, las cuales al día de hoy continúan presentándose y no se les ha intervenido de forma eficiente. Igualmente se contempla a lo largo del documento que el tema de AFD no es tenido en cuenta en el plan de acción instaurado para el manejo de la ciberdelincuencia y ciberseguridad en el país.

- El documento CONPES 3854 publicado el 11 de abril del presente año, busca intervenir de lleno en la política nacional de Seguridad Digital, pero se observa que se enfatiza poco en el álgido tema del Análisis Forense Digital, demostrando que para las autoridades competentes no resulta significativo o no lo consideran como crítico en la actualidad.

- Se observa déficit en el marco jurídico, en lo que respecta al debido proceso de cadena de custodia que se debe realizar para salvaguardar la integridad y solidez del material probatorio digital con el que se cuente, para permitir la admisibilidad de dicha evidencia digital en los juicios.
- Es importante para los profesionales de la seguridad tener conocimientos en la temática de Análisis Forense Digital, con el fin de prepararse para afrontar situaciones de crisis que se puedan presentar en los diferentes ámbitos laborales en los que se desempeñe, además de prestar asesoría y apoyo al momento de realizar investigaciones para generar soluciones prontas y eficientes según sea la circunstancia.

Referencias

- (Algesa, L. (2010). Definición de malware. Junio 10, 2016, de diccionario de informática y tecnología. Sitio web: http://www.alegsa.com.ar/Dic/malware.php)
- (Algesa, L. (2010). Definición de seguridad informática. Agosto 19, 2016, de diccionario de informática y tecnología. Sitio web: http://www.alegsa.com.ar/Dic/seguridad%20informatica.php)
- (Alegsa, L. (2016). Definición de Dirección IP: Diccionario de Informática y tecnología. Julio 10, 2016, de Alegsa.com.ar Sitio web: http://www.alegsa.com.ar/Dic/direccion%20ip.php)
- (Alegsa, L. (2016). Definición de Smishing: Diccionario de Informática y tecnología. Junio 30, 2016, de Alegsa.com.ar Sitio web: http://www.alegsa.com.ar/Dic/smishing.php)
- (Alegsa, L. (2010). Definición de Vishing: Diccionario de Informática y tecnología. Junio 20, 2016, de Alegsa.com.ar Sitio web: http://www.alegsa.com.ar/Dic/vishing.php)
- Álvarez et al. (2015). Framework para la computación forense en Colombia. *Ingenierías USBmed*, *3*(2), pp 61-69.
- (Borguello, C, (2009) Modificación de sitios web (defacing) con objetivos económicos. Junio 20, 2016. Segu-Info. Sitio web: http://www.segu-info.com.ar/articulos/96-defacing-objetivos-economicos.htm)
- Bogota & Moreno. (2012). Evidencia Digital en Colombia: Una reflexión en la práctica. Marzo 4 de 2016, de Portal de e-governo, inclusão digital e sociedade do conhecimento Sitio web: http://www.egov.ufsc.br/portal/conteudo/evidencia-digital-en-colombia-una-reflexi%C3%B3n-en-la-pr%C3%A1ctica
- Caballero, A. (2015). Técnicas Anti forenses Básicas. Julio 14, 2016 de Reydes Sitio web: http://www.reydes.com/archivos/slides/webinars/AC_WG_TecnicasAntiforensesBasicas.pdf
- Centro Cibernético Policial, Carta Nigeriana Herencia, Bogotá, 20 de agosto de 2016, Sitio Web: http://www.ccp.gov.co/contenido/carta-nigeriana-herencia
- Colombia cuenta con una política nacional de Seguridad. (13 abril de 2016). Departamento Nacional de Planeación. Bogotá D.C. Grupo de comunicaciones y Relaciones Publicas. Recuperado de https://www.dnp.gov.co/Paginas/Colombia-cuenta-con-una-Política-Nacional-de-Seguridad-Digital.aspx

- CONPES 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa, Bogotá, 14 de Julio de 2011, pp 1-43
- CONPES 3854, Política Nacional de Seguridad Digital, Bogotá, 11 de Abril de 2016, pp 1-91
- Constitucional, C. sentencia C-662 de 2000. *Magistrado Ponente Dr. Fabio Morón Díaz*.
- Datas, L. H., & Estatutaria, L. 1266 de 2008, Congreso de la República. Diario Oficial No. 47.219 de 31 de diciembre de 2008.
- de Bogotá, A. (2012). Ley Estatutaria 1581 de 2012. *Recuperado de http://www. alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp*.
- de la Nación, F. G. *Manual de procedimientos para cadena de custodia, Fiscalía General de la Nación* (p. 23). ISBN 958-97542-8-7.
- Decreto 1377 de 2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Colombia, 27 de Junio de 2013
- Decreto 1400 DE 1970 (Agosto 06)Por el cual se expide el Código de Procedimiento Civil.
- Del Proceso, C. G. Ley 1564 de 2012. In *Congreso De La Republica de Colombia, Art* (Vol. 422).
- Flores, J. (S.f). ¿Qué es el "grooming"?. junio 10, 2016, de muyinteresante Sitio web: http://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-grooming
- (Galdámez, P. (2003). Seguridad Informática. Agoto 19, 2016, de Actualidad TIC. Sitio web: http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf)
- (González, G. (2014) ¿Que es un ataque DDos y cómo funciona?. Junio 20 de 2016, de Blogthinkbig.com. Sitio web: http://blogthinkbig.com/ataque-ddos/)
- Guerrero, A. (2009). Informática forense y sus beneficios. RITS, 3, pp. 105-107
- (Gutiérrez, P. (2013). Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales. Junio 14, 2016, de Genbeta: Dev Sitio web: http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales)
- informaticahoy. (S.f). ¿Qué es un cracker?. Junio 10, 2016, de informaticahoy Sitio web: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

- INTERPOL, Informe forense de INTERPOL sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia. OIPC-INTERPOL. FRANCIA 2008
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, Colombia, 5 de Enero de 2009
- Ley 1453. por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad, Colombia, Junio 24 de 2011
- Ley 527 de 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, Colombia, 18 de Agosto de 1999.
- Lombo, M. (17 de julio de 2007). Tras el rastro de la evidencia digital. Huellas, 55, pp 18-19.
- López, M. (2007). Análisis Forense Digital. 13 de Marzo 2016, de GNU Free Documenta-tion Licence Sitio web: http://www.gnu.org/copyleft/fdl.html
- Mora, V. (9 de septiembre de 2013). Así funciona la informática forense en Colombia. *El Uuniversal.*
- (Paus, L. (2015). 5 fases fundamentales del análisis forense digital, agosto 19, 2016, de welivesecurity. Sitio web: http://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/)
- (Pérez, A, (2009). Medios de pago y delincuencia internacional. Junio 10, 2016, de universidad nacional de educación a distancia. Sitio web: http://iugm.es/uploads/tx_iugm/Medios_de_pago_y_delincuencia_internacional.pdf)
- (Pérez, J y Merino, M. (2008) Definición de Seguridad Informática. Julio 14 de 2016, de Definición.De. Sitio web: http://definicion.de/seguridad-informatica/)
- Pérez, Y. (2015). Delitos cibernéticos y Análisis Forense Digital. Junio 29 de 2016, de Ventajas de la Seguridad de la Informática. Sitio web: http://ventajasdeseguridadinformatica.blogspot.com.co/2015_10_01_archive.html

- Piñeros, G. (2008). *LOS DETECTIVES DE LA ERA DIGITAL*. 10 de Marzo de 2016, de *Enter.co*
- (Porolli, M. (2013). ¿En qué consiste en el análisis forense de la información?, agosto 19, 2016, de welivesecurity. Sitio web: http://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/)
- portafolio, Colombia, principal fuente de ciberataques en Latinoamérica Bogotá: [Octubre 17 de 2014]
- Presman, G. (2014). ISO/IEC 27037: ¿Plantea una nueva forma de hacer Análisis Forense?. 20 de mayo de 2016, de ISSA Sitio web: http://www.issaarba.org/node/70
- Ramírez, A. (2008). Informática Forense. Junio 01, 2016, de La consigna Sitio web: https://laconsigna.wordpress.com/2008/05/26/informatica-forense/
- Ramos, A. (25 de Marzo de 2011). Historia de la informática forense. 20 de Mayo de 2016, de Securutybydefault Sitio web: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html
- (Ramos, C. (2011). La evidencia digital, agosto 19, 2016, de Hipotesis acusatoria. Sitio web: http://hipotesis-acusatoria.blogia.com/2011/052601-la-evidencia-digital.php)
- Resolución reglamentaria 202 de 2012. Por la cual se deroga la Resolución Reglamentaria 126 de 2011 y se crea el grupo de Laboratorio de Informática Forense (LIF), adscrito al Despacho del Vice contralor, Colombia, 7 de Diciembre de 2012
- Restrepo, A. (2008). *Computación forense, análisis de "cadáveres" virtuales*. 28 Marzo de 2016, de Dragonjar.org Sitio web: http://www.dragonjar.org/computacion-forense-analisis-de-cadaveres-virtuales.xhtm)
- Rodríguez, J. (4 de marzo de2014). El delito informático es muy joven en Colombia. *El Universal*.
- Rousse, M. (2012). likejacking. Junio 10, 2016, de TechTarget Sitio web: https://translate.google.com.co/translate?hl=es&sl=en&u=http://whatis.techtarget.com/definition/likejacking&prev=search
- (Sánchez, M. (2011). ¿Qué es una infraestructura crítica?. Julio 15, 2016, de Infraestructuras críticas y ciberseguridad. Sitio web: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/
- (Salcedo, J, Fernández, C, Castellanos, L. (2012) Hackers en la sociedad de la información: análisis de su dinámica desde una perspectiva social. Junio 10, 2016. Visión

electrónica. Sitio web: http://revistas.udistrital.edu.co/ojs/index.php/visele/article/view/3754/6003)

- (Sandoval, E. (2011). Ingeniería social: Corrompiendo la mente humana. Junio 10, 2016, de .seguridad. Sitio web: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana
- Sd, (29 de mayo de 2016). Informática Forense, pasado, presente y futuro. Recuperado de http://informaticaforenseuccaraucacolombia.blogspot.com.co/
- S.d. (19 de octubre de 2015). Vulnerabilidad afecta a 1000 millones de dispositivos Android. *El tiempo.*
- s.d. (5 de mayo de 2005). *SEGURIDAD INFORMÁTICA, EL RETO EMPRESARIAL DEL MOMENTO. El Tiempo.*
- S.d. (7 de junio de 2015). Cayo "gemido ruidoso", el zar de la pornografía infantil. Semana. Recuperado de: http://www.semana.com/nacion/articulo/antioquia-cayo-gemido-ruidoso-gran-distribuidor-de-pornografia-infantil/445297-3).
- S.d. (s.f). caso "profesional de la salud". mayo 03, 2016, de Adalid Corp. Sitio web: http://www.adalid.com/nosotros/casos-de-exito/
- Sd. (S.f). Infraestructuras críticas. Julio 15, 2016, de Grupo Control seguridad Sitio web: https://www.grupocontrol.com/infraestructuras-criticas
- S.d. (s.f). Millonario fraude. Mayo 03, 2016, de Centro cibernético policial Sitio web: http://www.ccp.gov.co/ciberseguridad/casos-operativos/op-pasarela-ii-0
- (Steffens, H. (2009). ¿Qué es el phishing?. Junio 10, 2016, de Amenazas informáticas seguridad informática. Sitio web: http://liacolombia.com/2009/12/%C2%BFque-es-el-phishing/)
- Tecnosfera. (2016). En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. 5 de Mayo de 2016, de EL TIEMPO Sitio web: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604
- Verdú, D. (21 de septiembre de 2015). Los móviles, objetivo de los virus. *El País*
- Vergara, k.. (2008). Hacking: definiciones básicas e inauguración categórica oficial. junio 15, 2016, de Blog informático Sitio web: http://www.bloginformatico.com/hacking-definiciones-basicas-e-inauguracion-categorica-oficial.php

- Villamizar et al. (2015). Análisis forense en un sistema de información en el marco normativo colombiano. *Revista de investigación e innovación en ingenierías*., 3(1), pp 1-8.
- Yailin Pérez, (2015). Ventajas de Seguridad informática. Recuperado de: http://ventajasdeseguridadinformatica.blogspot.com.co/2015_10_01_archive.html

Referencias figuras

- Villamizar, et al. (Sf.) análisis forense en un sistema de información en el marco normativo colombiano. Recuperado de: file:///C:/Users/DIEGO/Downloads/1122-1142-1-PB%20(1).pdf
- CONPES 3854(2016) Política Nacional de Seguridad Digital
- Corporación Colombia Digital. (2015). Colombia en el top 5 de ciberseguridad en Latinoamérica. Recuperado de: http://www.colombiadigital.net/actualidad/noticias/item/8111-colombia-en-el-top-5-de-ciberseguridad-en-latinoamerica.html
- Sd, (Sf. Recuperado de: http://www.indexmundi.com/