Cómo citar este artículo: J. J. K. Bustamante-Riaño, "Avances de la informática forense en Colombia en los últimos cuatro años" Revista Ingeniería, Investigación y Desarrollo, vol. 20 (1), pp. 69-78, enero. 2020.

DOI: https://doi.org/10.19053/1900771X.v20.n1.2020.13384

AVANCES DE LA INFORMÁTICA FORENSE EN COLOMBIA EN LOS ÚLTIMOS CUATRO AÑOS

Advances in computer forensics in Colombia in the last four years

José Jhon Kennedy Bustamante Riaño[1]
[1]Facultad de Ingeniería de Sistemas Virtual, Fundación Universitaria del Área Andina Semillero Informática Forense (Bogotá D.C.)
Email: [1]jbustamante14@estudiantes.areandina.edu.co

(Recibido 03 de agosto de 2021 y aceptado 18 de agosto de 2021)

Resumen

Este trabajo de investigación expone, inicialmente, cómo con el crecimiento de los avances tecnológicos que surgen a favor de la sociedad para procesar, guardar y asegurar grandes volúmenes de datos informáticos; paralelamente, se convierten en herramientas estratégicas en su contra, ya sea para eliminarlos o alterarlos; de acuerdo con los propósitos inescrupulosos de quienes cometen los delitos informáticos, problemática creciente que vulnera la confidencia e intelecto de la información. En consecuencia, se desarrolla un trabajo cualitativo, en el cual también se reconoce los conocimientos adquiridos en este proceso de investigación frente a las competencias básicas para el dominio de esta temática. Por está razón, el presente estudio revela un panorama general acerca de cómo ha sido la evolución de la informática forense en una pesquisa hecha entre los años 2017 al 2020, especificando algunos fundamentos, procederes y normativas, útiles en el proceso de recuperación de información y recolección de evidencia digital en el momento de un incidente; en este mismo sentido, se exponen cifras acerca de la vulneración que han tenido algunas industrias y, a partir de esto, se evidencia cómo actúan los delincuentes informáticos.

Palabras claves: *análisis forense, informática forense, cadena de custodia, pruebas digitales, delitos informáticos.*

Abstract

This research work shows, initially, how with the growth of technological advances that arise in favor of society to process, store and secure large volumes of computer data; in parallel, they become strategic tools against them, either to eliminate or alter them; according to the unscrupulous purposes of those who commit computer crimes, a growing problem that violates the confidentiality and intellect of information. Consequently, a qualitative work is carried out, in which the knowledge acquired in this research process is also recognized against the basic competences for domaining this subject. For this reason, the present study reveals an overview of how the evolution of forensic informatics has been in a research carried out among 2017 to 2020, specifying some bases, procedures and regulations, useful in the process of information retrieval and collection of digital evidence at the time of an incident; in this same sense, data are presented about the violation that some industries have had and, from this, it is evident how computer criminals act.

Key words: *forensic analysis, computer forensics, chain of custody, digital evidence, cybercrime.*

1. INTRODUCCIÓN

El desarrollo de la tecnología de la información y las comunicaciones permite que el procesamiento de datos se presente de una manera ágil y oportuna; sin embargo, estos quedan expuestos ante diversas vulnerabilidades de ataques informáticos o actos que atentan contra las leyes que rigen el derecho a la privacidad y la seguridad informática. La seguridad informática orientada a proteger los distintos recursos tecnológicos se ve amenazada porque nacen grandes e innovadores ataques informáticos que pueden generar daños considerables a los usuarios de las TICS, así como a las organizaciones gubernamentales y entidades privadas. Desde esta perspectiva, se aborda en el presente trabajo de investigación la informática forense como una estrategia de análisis que permite identificar, proteger, mitigar, salvaguardar la información y, así mismo, estudiar el dispositivo electrónico en el que ocurrió el delito informático o la escena del delito en la red que permita analizar las pruebas digitales. Por otra parte, Corrales y Osorio (2015) nombrado en [1] afirma que, si bien el mundo tecnológico es complejo, también adolece de diversas debilidades por fallas provocadas por el hombre, del programa o técnicas en la infraestructura de procesamiento de datos, señal de la tendencia de los intrusos informáticos amenazantes que desestabilizan la economía y el equilibrio social de una nación, generando conflictos, guerras, etc. (p.15)

2. PROBLEMA DE INVESTIGACIÓN

Hoy en día los avances tecnológicos, se encuentran en constante evolución, permitiendo que millones de personas interactúen con facilidad. Gracias a estos recursos, se puede comunicar rápidamente desde cualquier parte del planeta, mediante dispositivos como: computadores, celulares inteligentes, redes sociales y muchos otros medios electrónicos. Cabe resaltar la gran cantidad de información y datos que se maneja diariamente, la cual es susceptible de ser vulnerada, captada, hurtada, generando posibles ataques a los medios informáticos. Esta agresión cibernética, la puede sufrir cualquier persona que usa o no la tecnología como medio de comunicación, y con ello ser víctima de fraudes financieros, infección de virus, denegación de servicios, *phishing* e innumerables ataques que día a día aparecen con su evolución. [2] Actualmente, el uso de la tecnología de información y comunicación se ha visto encaminada a la mejora continua de la sociedad, tanto en las entidades públicas, privadas, económicas que almacenan grandes cantidades de datos (Información).

Así también, el avance tecnológico en la gran mayoría de trabajos que se desempeñan en el mundo requiere la utilización de infraestructura, herramientas y personal con conocimientos en el manejo de ésta; así mismo, los grandes cambios en la tecnología han hecho que muchas empresas de tipo privado, gubernamentales y personales, tengan que mejorar los insumos tecnológicos, ayudando así a enriquecer o duplicar su productividad y eficiencia. La utilización continua de estas herramientas tecnológicas ha convertido a los seres humanos en personas dependientes y, el manejo excesivo los absorbe, llegando a enfrentarlos a situaciones en donde su práctica, en muchos casos, se ha convertido en un campo de batalla, ya que con el uso continuo se presta para que los delincuentes, encuentren una forma de vulnerar la seguridad.

De acuerdo con [3] afirma que los beneficios que se le dan a estos medios tecnológicos son grandes, pero también hay muchos aspectos negativos encontrados en su empleo, toda vez que su uso continuo y desmesurado ha permitido que se genere vulnerabilidades. Por esta razón, la aparición de herramientas tecnológicas de software y hardware, han ayudado a verificar los sistemas tecnológicos, previniendo así los ataques a la Información. Es aquí donde la Informática Forense juega uno de los papeles importantes, ya que ella estudia los procesos que se deben tener en cuenta para una buena recolección de evidencias; esta busca preservar que los datos informáticos, se encuentren a salvo, y evitar que caigan en manos equivocadas, así también, esclarecer el cómo, cuándo y dónde ocurrieron los hechos. Algunas leyes que protegen la información en Colombia, “Ley 1273”, tiene como objetivo primordial salvaguardar la Información y protección de los sistemas de tecnología de la información

y las Telecomunicaciones, la cual contempla capítulos específicos: "Ataques a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, así como ataques informáticos y otras violaciones", estas leyes nos sirven de guía para proteger jurídicamente los datos de las Empresas, Gobiernos y personas del común. En este sentido, [4] en su trabajo de investigación recopila algunos datos sobre el crimen informático en Colombia como muestra la Fig.1.

Figura 1. Delitos Informáticos en Colombia [4](p.4)

Actualmente, en Colombia, la cibercriminalidad exhibe incremento del número de incidentes cibernéticos; como consecuencia, empresas y ciudadanos han denunciado al menos 30.410 casos en el 2019, los cuales infringen la ley 1273 del 2009, cifra que corresponde al 57% de los casos denunciados. En este orden de ideas, [2] deja entrever que los índices de ciberdelincuencia han flagelado a nuestro país en los últimos años; de la misma manera, es notable observar cómo los delincuentes informáticos usan diferentes métodos y herramientas para cometer los delitos, al crear nuevas estrategias para la vulneración de los equipos como muestra la Fig.2.

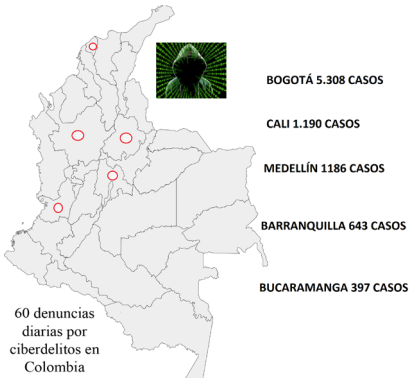

Figura 2. Ciudades más afectadas por los delitos Informáticos [4] p.5

La mayoría de las vulneraciones permiten identificar la manera cómo actúan los ciberdelincuentes, así como, las técnicas utilizadas y las herramientas implementadas; en este lugar, se debe tener y tomar conciencia acerca de la importancia de conocer que existen delitos referentes a temas tecnológicos y que los delincuentes están al acecho; por esta razón, no se debe bajar la guardia frente a este tipo de crimen. En este sentido es vital tener conocimientos y capacitación de las personas, logrando establecer una barrera. Es entonces la pedagogía, la mejor herramienta, frente a un delito informático para que los criminales no logren su objetivo. No obstante, esto no quiere decir que se puedan eliminar del todo, ya que los delincuentes cada día fraguan nuevas estrategias para vulnerar los sistemas informáticos y comentar sus actos delictivos.

3. OBJETIVOS

General: Describir cómo ha sido la evolución de la Informática Forense en Colombia en los últimos cuatro años (2017-2020).

Específicos:

- Explicar origen y reconocimiento de la Informática Forense en Colombia.
- Identificar cuáles han sido las prácticas o experiencias aplicadas.
- Enunciar cuáles son las entidades que regulan la Informática Forense en Colombia

4. JUSTIFICACIÓN DEL PROBLEMA

En la actualidad, la tecnología está avanzando a pasos agigantados y, con ella, el estilo en que los seres humanos actúan. Ahora bien, toda la información es almacenada en dispositivos electrónicos según el uso para el que aplique, esto genera ventajas tales como: alta disponibilidad en cualquier momento, facilidad en el manejo de la información, etc. En este sentido, también existe riesgos frente al manejo de la información, por lo cual se establecen estrategias para resguardar los datos informáticos, evitando con esto su

posible vulneración. En concordancia con lo anterior, [4] manifiesta que, en Colombia en los últimos años, el tema de ciberdelincuencia ha tomado índices elevados, en ocasiones por desinformación o ingenuidad de los usuarios. Es en este momento, los delincuentes se aprovechan del usuario y su desinformación, para apoderarse de la confianza de los consumidores y cometer sus fechorías. Por consiguiente, con el presente proyecto de investigación se tiene como propósito identificar cómo ha sido la evolución de la informática forense en Colombia en los últimos 4 años (2017 – 2020) y cómo la Informática Forense permite fortalecer procesos de aprendizaje y construcción de conocimiento básico para la implementación en la seguridad informática. No obstante, se debe tener en cuenta que la informática forense es un tema complejo y se deben tomar medidas de seguridad extremas para el personal que se especializa en el manejo de dicha evidencia, de tal manera que, se pueda evitar cualquier error que conduzca al fracaso del proceso legal. Algunas técnicas que deben se deben seguir al realizar procedimientos forenses informáticos se enuncian a continuación:

- Reconocer un incidente.
- Compilar evidencias.
- Resguardar evidencias
- Examinar evidencias
- Justificar y mostrar de los resultados

Según Piedrahita, 2014 anunciado en [5] la etapa del análisis forense es el procedimiento que sigue un investigador profesional para corregir los procesos forenses. Por consiguiente, las técnicas aplicadas al análisis forense informático sirven para garantizar la efectividad al momento de proceder y la diplomacia de la seguridad que se implementa al interior de una compañía u organización, cuyo fin es proteger los datos informáticos y la infraestructura que detecta las vulnerabilidades dentro de las empresas ayudando a mitigar los riesgos con el uso de los procedimientos legales, técnicas de recolección y equipos tecnológicos y aplicaciones para una correcta implementación para el análisis forense digital.

Desde el abordaje teórico, la informática forense se define como la disciplina que articula elementos del derecho y la informática, gracias a estas bondades, recopila y analiza datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que se pueda utilizar como prueba ante los tribunales. Esto significa que, es una disciplina que previene ataques informáticos, ayudada del análisis y las técnicas científicas a instalaciones técnicas; de esa manera, posibilita asemejar, salvar y examinar medios informáticos, así como, conseguir argumentos y evidenciar una infracción informática, con el fin de presentar estas mismas, ante un tribunal.

A. Informática Forense es un método complicado en su manejo, se debe exagerar en referencia a la seguridad, al recurso humano técnico en la administración de evidencias, así se evitará que se ejecute errores que involucre fracasos en el procesamiento jurídico legal.

B. Cadena de custodia tiene como finalidad ofrecer apoyo efectivo a argumentos digitales ante un ente judicial, se conoce como el correcto proceder. Por consiguiente, se deben instituir procesos adecuados garantizando la eficacia de los métodos empleados al extraer evidencia informática. El meticuloso proceso garantiza bases sólidas para el juzgamiento y la validez delante del fuero judicial, por esta razón, es necesario que se eviten suplantaciones, transformaciones, variaciones y falsificaciones en cada una de estas etapas.

C. Evidencia Digital el autor expresa [7] (p.9) que toda información manipulable del ser humano, sacada de medios de datos informáticos, que lleguen a servir como evidencia para presentar en procesos legales y jurídicos los cuales se puede fraccionar en:

1. Investigaciones informáticas acumuladas en equipos, ya sea por medio de correos electrónicos, medios digitales, imágenes, etc.

2. Anotaciones generadas por equipos de tecnología, auditorías, evidencia de transacciones, registros de

eventos, etc.

3. Evidencias creadas y guardadas en aparatos tecnológicos tales como consultas a bases de datos, hojas de cálculo con información financiera, etc.

Según [8] quien considera que una infracción informática es "comportamientos antijurídicos, no éticos o no considerados, referentes a los procesos que involucran datos y/o transmisión de datos"(p.8) En este sentido, el delito informático es la forma en la que se quebranta la información y los datos personales; y en este caso, la informática forense es la encargada de observar conductas delictivas, antijurídicas frente a técnicas informáticas o su infraestructura.

5. ANÁLISIS Y PLANTEAMIENTO DE ANTECEDENTES

En primer lugar, este trabajo investigativo realiza una explicación breve de dónde surge la informática forense rastreando su historia, a través de los conceptos expuestos por otros investigadores que ya han hecho estudio de casos relacionados con la misma. El autor [9] en su trabajo de indagación *"Análisis de la evidencia digital en Colombia como soporte Judicial de delitos informáticos mediante cadena de custodia"*. La seguridad informática y lo relacionado con delitos informáticos en Colombia, es un tema relativamente nuevo. La informática forense se introduce como una serie estructurada de pasos que permiten la recolección, análisis y tratamiento de evidencia digital con el fin de dar solución a algún evento de seguridad informática.

Los conocimientos ganados sobre la seguridad informática son realizados por métodos, técnicas y procedimientos, implementados en otros países o naciones, tomando como ejemplo los casos de estudio y el análisis hechos en otros contextos. Particularmente, en Colombia, se acogen todas estas técnicas y se modifican según las normas y leyes que rigen a nuestro país. Las investigaciones en el mundo de la Informática forense son exhaustivas, muchas de ellas están encaminadas a diferentes campos de la computación forense.

En [10] en su trabajo investigativo *"Informática Forense en Colombia"* manifiesta que los instrumentos usados en la informática forense, permiten examinar conductos regulares provenientes de los actos indecorosos que se presentan en la informática, en muchos ambientes como: Laboral, Judicial, Educativo, Financiero, Gubernamental y muchos otros, que también se ven afectados con el uso de la Tecnología de la Información. Entonces, se hace uso de la IF, siendo esta la ciencia encargada de efectuar los estudios en la escena del crimen, de las redes o los equipos electrónicos que contengan la información; para lo cual, busca identificar, recolectar y analizar pruebas digitales que esclarezcan y prevengan casos similares.

6. DISCUSIÓN

Son diversas las exploraciones que se han llevado a cabo en el contexto del cómputo forense, como las cosmovisiones y espectros desde donde los distintos autores han estudiado sus herramientas y procedimientos técnicos. De esta forma desde una perspectiva nacional y cosmopolita se exponen algunos planteamientos como los siguientes:

Según [10] en su trabajo de investigación "*Informática Forense en Colombia",* plantea un análisis desde los grandes avances tecnológicos que permiten almacenar grandes volúmenes de información en diferentes medios electrónicos, haciendo más fácil su manipulación y procesamiento, en últimas, facilitando la vida a los usuarios; sin embargo, también estos avances han abierto las puertas tanto a los delitos informáticos como a innumerables situaciones de vulneración a los datos.

7. RESULTADOS

Se antepone una breve reseña histórica de dónde nace la informática forense, dedicando un pequeño acápite de los orígenes. Según [11] en su trabajo investigativo acerca del análisis de la ciencia forense digital en Colombia, Florida. Identificó por primera vez delitos en sistemas informáticos en 1978. La informática comenzó en 1980,

y en 1984, el FBI creó el programa *"Magnetic Media Program, Computer Analysis and Response Team"*, tiempo después, apareció el Sr. Michael Anderson era un agente del Departamento de Investigación Criminal del Servicio de Impuestos Internos de los Estados Unidos quien fue conocido como el padre de la informática forense hasta mediados de la década de 1990 cuando cooperó con el gobierno y luego creó nuevas tecnologías" (p.20)

En 2004, gracias a la Policía Nacional de Colombia, la informática forense se convirtió en una ciencia de apoyo a las investigaciones judiciales, es decir, los efectos nocivos y negativos provocados por el abuso de los medios informáticos y el aumento de las tasas de criminalidad desde entonces. El diario El Tiempo destacó este punto, que comprobó que se crearon 7.360 virus este año (2004), un aumento del 32% con respecto al año anterior (2003), y los problemas de seguridad informática aumentaron en un 93%. La pérdida equivale a 666 millones dólares a entidades bancarias. Por esta razón, es necesario crear una entidad que realice el rol de las investigaciones forenses dirigidas específicamente a los medios informáticos. Desde entonces, ha surgido la Dirección de Investigación Criminal, que ha apoyado la labor de la Policía Nacional desde un principio; no obstante, necesitan el apoyo de las instituciones de control. En ese sentido, es vital que existan entidades con estructuras mejor jerarquizadas para brindar soluciones óptimas a estos temas.

La Auditoría General, que tiene a su cargo las investigaciones, los juicios tributarios y la jurisdicción obligatoria de la Contraloría General de la Nación, ha creado un laboratorio de informática forense para determinar hechos ilícitos o fraudulentos en los que se encuentran en riesgo bienes nacionales. La investigación criminal forense en Colombia comenzó a estar en boga en el 2004, y para los próximos años, el Estado colombiano ha venido creando normas sobre seguridad de la información, como se observa en la Fig. 3.

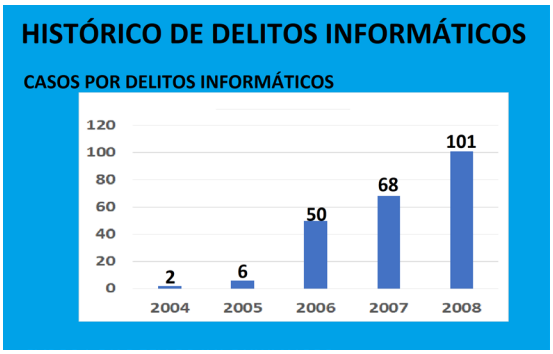

Figura 3. Histórico de delitos informáticos [10]

En 2004, se creó una entidad de apoyo para problemas de seguridad informática, y desde entonces, esta ha realizado múltiples investigaciones. Algunas de ellas fueron desarrolladas en 2006, sin embargo, es importante destacar uno de los casos de investigación forense más importantes del país. En 2008, el Ejército Colombiano confiscó las computadoras de Raúl Reyes miembro de las Fuerzas Armadas Revolucionarias de Colombia (FARC) durante la Operación Fénix. "Según el Ministro de Defensa de Colombia, Juan Manuel Santos, los investigadores encontraron más de 16.000 archivos en tres computadoras portátiles, halladas en el campo de exterminio de Reyes", informó el New York Times. En seguida, la Fiscalía Pericial, realizó un análisis detallado de estos elementos para extraer la mayor cantidad de información posible.

El ciberdelito mundial está creciendo a un ritmo bastante rápido y continúan surgiendo nuevas tendencias. Los ciberdelincuentes se están volviendo cada vez más especializados, capaces de utilizar nuevas tecnologías con fines de lucro, adoptar nuevos métodos para ajustar y establecer redes cooperativas para que puedan llevar a cabo ataques cibernéticos en pocos minutos.

2017

La delincuencia online aumentó un 28% en 2017, provocando pérdidas de más de 50 mil millones de pesos. Según [12], el ciberdelito representa una amenaza creciente para la seguridad de Colombia. Según datos

de DIJÍN, durante 2017, las autoridades buscaban la forma de abordar este panorama, primero a través de la coordinación de investigaciones y operativos entre la Policía y la Fiscalía. Este año, una de las ofensivas más peligrosas de Internet es el *Blue Whale Challenge*. Un juego diseñado en Rusia y difundido por todo el mundo, en el que niños y jóvenes afrontan el reto de hacerse daño física y psicológicamente y acabar por suicidarse. En Colombia, las autoridades emitieron 508 advertencias para el juego, que abarcan a más de 6 millones de personas. Durante el año, la policía bloqueó 3.891 páginas web que contenían pornografía infantil.

Como resultado, 56 personas fueron arrestadas, con lo anterior, es evidente que Colombia no es inmune a los grandes ciberataques a escala mundial. Para este año, el programa malicioso *Wannacry,* que secuestró los datos del dispositivo atacado, afectó a más de 150 países y se convirtió en uno de los ataques más famosos de la historia de Internet, con posibles amenazas internacionales.

2018

Colombia reportó 22.366 casos de delitos informáticos. Según [13] durante 2018, el número de casos relacionados con delitos informáticos aumentó en un 40%; es decir, de 15.962 en 2017 pasó a 22.366 casos registrados por las autoridades. Lo que significa, que el ciberdelito, por ejemplo, a nivel de incidentes informáticos, fue de 8.090 en 2017 frente a 11.529 en 2018, un aumento similar de 46%. Actualmente [14] según el coronel Fredy Bautista, el ciberdelito es el segundo elemento delictivo tipificado como actividades ilegales, que trae el mayor beneficio para los delincuentes, se estima hasta 8 mil millones de dólares en delitos cibernéticos para 2022. En Colombia, las cifras no son muy alentadoras, el número de denuncias de víctimas sigue aumentando año tras año; un ejemplo de ello, son las 12,014 denuncias relacionadas con el robo de computadoras.

Esto significa que el 55% de los delitos, están relacionados con el fraude y el robo de cuentas bancarias. En 2018, los informes de ciberataques aumentaron en un 42%, de ellos, se denunciaron 11.524 casos a la Policía Nacional. Este ente de control revela un aumento significativo de las amenazas y los desafíos cada vez más severos que enfrentan los bancos y las empresas para proteger su ciberseguridad, lo que significa que hay una media de 131 millones de intentos de ciberataques al día.

2019

Los métodos de ataque más comunes siguen siendo el ***phishing*** y la ***social engineering***. Este tipo de fraudes, se valen de la negligencia o ignorancia momentánea de los usuarios para convertirlos en copias fraudulentas de sitios web. A fines de 2019, las autoridades informaron que los incidentes cibernéticos en el país habían aumentado en un 54% en comparación con 2018. En este caso en particular, el ataque cibernético aprovechó una vulnerabilidad en Windows que fue corregida por Microsoft; no obstante, al final requerían que los usuarios actualizarán sus sistemas para evitar el daño.

2020

[15] El delito de más rápido crecimiento en 2020 es el engaño de sitios web, en el que se registraron 1.224 casos en 2019 y 5.051 respectivamente, reportados en el centro de control policial durante el año. Lo que significa un aumento del 313%. Como se muestra en las Figuras (4-5).

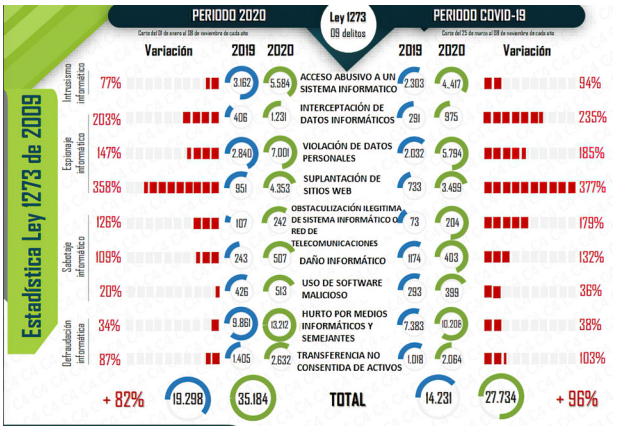

Figura 4. Estadística ley 1273 de 2009 [15]

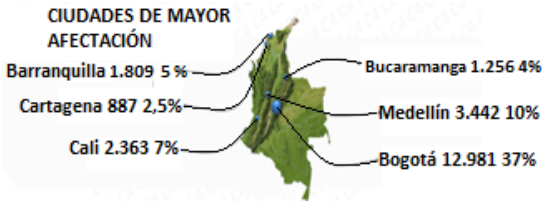

Figura 5. Ciudades con mayor afectación criminal [15]

Así también, para este año, el centro de control policial manejó 11,950 incidentes y 7,862 correos electrónicos a través de CAI virtual. Como se ilustra en la Figura 6.

- 845 intercambios de comunicaciones internacionales.
- Análisis 640 muestras de malware.

180 charlas de prevención para niños y jóvenes, padres y profesores.

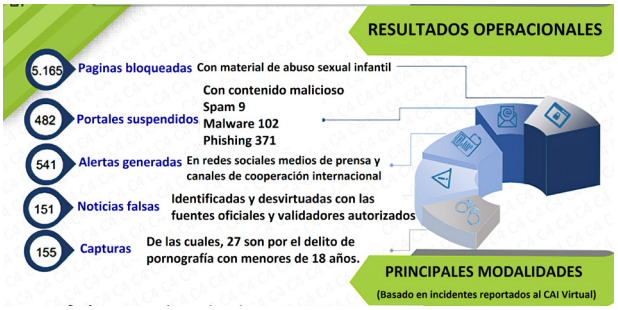

Figura 6. Resultados Operacionales y Principales modalidades [15]

8. CASOS

[16] En Barranquilla, el Centro de Policía Cibernética de la DIJIN capturó a una organización criminal dedicada al fraude informático contra diversas entidades financieras, por valor de más de 10 mil millones de pesos (US $ 10,000,000,000), de los cuales 326 cuentas financieras fueron afectadas, que fueron incidentes relacionados con el pago de salarios de la seguridad social a través de PSE. [16] advierte, además que investigadores del centro de la red policial capturaron a 8 miembros de una peligrosa pandilla en Barranquilla. La pandilla se infiltró en la empresa para liberar cuentas salariales y logró robar más de $77.128.5 mil millones de pesos; el patrón delictivo incluyó el desarrollo de programas informáticos para violación de los servicios de banca virtual, como el acceso remoto y el uso desprevenido de computadoras sin el nivel de seguridad requerido. Algunos de los organismos que cumplen vigilancia sobre los crímenes cibernéticos, se relacionan en seguida:

Policía Nacional: [1] En Colombia mediante el decreto 1000 de noviembre 5 de 1891, manifiesta la organización de un grupo llamado Policía Nacional, que más adelante se convierte en el inicio de este cuerpo policial conocido como la Policía Nacional de Colombia, a su vez, adopta "el propósito principal de la agencia, a saber, mantener la convivencia como condición necesaria para el ejercicio de los derechos y libertades públicas, y asegurar que los residentes colombianos convivan pacíficamente de acuerdo con las normas "como misión de la ética policial", mediante la innovación, uso de herramientas técnicas y optimización de recursos ".

Procuraduría General de la Nación [1]dentro de su misión establece: La Procuraduría General es una entidad que representa a los ciudadanos ante el estado. Es el máximo órgano del Ministerio de Asuntos Públicos y también está integrado por la Defensoría del Pueblo y las personas jurídicas. Tiene la responsabilidad de iniciar, adelantar y suspender las investigaciones de acuerdo con lo establecido en el "Código Disciplinario Único" o la Ley No. 734 de 2002 porque estas investigaciones se realizan contra servidores públicos y personas que desempeñan funciones públicas o manejan fondos estatales por violaciones a la ley anteriormente relacionada.

9. CONCLUSIONES

Con la presente revisión investigativa, se logró conocer y analizar cómo desde otras perspectivas o cosmovisiones de diferentes autores se ha abordado la Informática Forense, así como, las herramientas para su aplicación. En esta pesquisa, se encontró diversas miradas investigativas desde donde se han trabajado enfoques que hacen alusión a: la auditoria forense, los marcos normativos, los estudios de caso, el funcionamiento e instalación de un programa, el paso a paso del procedimiento forense,

entre otros; por consiguiente, en la medida que dichos marcos metodológicos se pongan en práctica, se requiere de conocimiento y dominio de los procedimientos técnicos y de sus herramientas.

La IF es una ciencia que permite realizar investigaciones sobre los delitos informáticos, de donde se obtienen evidencias necesarias para aclarar un delito informático, las cuales son validadas en un estrado judicial, determinando si una persona es culpable o no. Con lo anterior, es pertinente afirmar que, las personas deben conocer sobre la tipología delictiva, en especial, toda aquella que involucra el uso y la evolución tecnológico. Así también, se hace necesario crear mecanismos a través de los cuales los estudiantes de Ingeniería de Sistemas adquieran los conocimientos pertinentes en cuanto a la IF, su análisis, sus herramientas de software y hardware, profundizando en temas afines, aplicando lo aprendido en el área destinada para la adquisición de procedimientos Informáticos.

Este trabajo de revisión investigativa, enfatiza en el buen uso y manejo cuidadoso de los datos, la información, la infraestructura, que se constituyen como los activos más importantes en este mundo lleno de tecnología. Así también es menester resaltar que, que la Informática Forense brinda las herramientas y técnicas necesarias para mitigar los ataques informáticos, igualmente, permite reconocer que todo usuario está expuesto y no se encuentra excepto a sufrir de ataques cibernéticos y, por lo mismo, se debe tener los conocimientos necesarios para lograr reaccionar de forma frente a estas situaciones delictivas. En consecuencia, con esta revisión se lograrán reconocer futuros trabajos investigativos acerca de herramientas de software que permitan resolver problemas relacionados con ataques informáticos y, especialmente, herramientas de software libre.

REFERENCIAS

[1] O. Meneses Obando, «Judiciales Que Cuentan Con El Servicio Especializado De Peritaje Informático En Colombia,» Universidad Externado de Colombia, Bogotá, D.C., Colombia, 2019.

[2] W. Pedreros Martínez y J. Suárez Urrutia, «Herramientas Aplicadas En El Desarrollo Del Análisis Forense Informático En Colombia,» Universidad Militar Nueva Granada, Bogotá D.C., 2016.

[3] P. Ayazo Villadiego, «Uso De La Informática Forense Aplicada A Delitos Informáticos En La Industria Colombiana,» Universidad Nacional Abierta y a Distancia "Unad", Momil – Córdoba, 2019.

[4] A. Ceballos López, F. Bautista García , L. Mesa Guzmán y C. Argaez Quintero, «Tendencias Cibercrimen en Colombia 2019-2020,» Centro Cibernético Policial, Bogotá, 2019.

[5] Y. Atehortúa y F. Jaramillo, «Análisis de herramientas opensource para la informática forense con énfasis en la recolección de evidencia digital.,» Instituto Tácnico Metropolitano, Medellín, 2018.

[6] L. Enrique Arellano y M. Castañeda, «La cadena de custodia informático-forense,» Revista ACTIVA, pp. 67-81, 2012.

[7] F. Bautista , J. Mosquera, A. Meneses y D. Rios, «Evidencia Digital procedimientos técnicos,» Rama Judicial Concejo Superior de la Judicatura, Bogotá, 2020.

[8] J. de la Ossa y R. Baena, «Notas sobre Informatica Forense,» Universidad Cooperativa de Colombia, Montería, 2016. [En línea]. Available: doi: http://dx.doi.org/10.16925/greylit.1903

[9] A. Ramírez y F. Castro, «Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia,» Universidad Nacional Abierta y a Distancia "UNAD", Villavicencio, 2018.

[10] F. Castillo y J. Bohada, «Informática Forense en Colombia,» Revista Ciencia, Innovación y Tecnología (RCIYT) | Vol. II, p. 12, 2015.

[11] A. Jaramillo y L. Torres, «Estado del análisis forense digital en Colombia,» Universidad Militar Nueva Granada, Bogotá, D.C., 2016.

[12] P. S. S.A, «El cibercrimen en 2017: la amenaza crece sobre Colombia,» 8 junio 2021. [En línea]. Available: https://www.semana.com/nacion/

articulo/cibercrimen-en-colombia-balance-de-2017/551979/.

[13] R. 360 , «En 2018 se reportaron 22.366 casos de delitos informáticos en Colombia,» 17 mayo 2019. [En línea]. Available: https://360radio.com.co/en-2018-se-reportaron-22-366-casos-de-delitos-informaticos-en-colombia/#:~:text=En%202018%20se%20reportaron%2022.366%20casos%20de%20delitos%20informáticos%20en%20Colombia.

[14] D. Arias, «Colombia, el país con más ransomware en Latinoamerica, en 2018,» 15 Mayo 2019. [En línea]. Available: https://www.enter.co/empresas/colombia-ataques-ciberneticos-18/.

[15] E. Espectador, «En 2019 se registraron 48 billones de intentos de ciberataques en Colombia,» 11 Marzo 2020. [En línea]. Available: https://www.elespectador.com/tecnologia/en-2019-se-registraron-48-billones-de-intentos-de-ciberataques-en-colombia-article-908787/.

[16] C. C. Policial, «Operación DARKODE,» 5 abril 2021. [En línea]. Available: https://caivirtual.policia.gov.co/ciberseguridad/casos-operativos/operacion-darkode.

[17] L. Herrera, «Informática forense,» 2015. [En línea]. Available: https://digitk.areandina.edu.co/bitstream/handle/areandina/1955/RP_eje2.pdf?sequence=1&isAllowed=y.

[18] S. Rosero, «Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012",» Universidad Internacional SEK, Quito, 2019.