USO DE LA INFORMÁTICA FORENSE APLICADA A DELITOS INFORMÁTICOS EN LA INDUSTRIA COLOMBIANA

PERÚ CARMELO AYAZO VILLADIEGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MOMIL – CÓRDOBA
2019

USO DE LA INFORMÁTICA FORENSE APLICADA A DELITOS INFORMÁTICOS EN LA INDUSTRIA COLOMBIANA.

PERÚ CARMELO AYAZO VILLADIEGO

Proyecto de grado Para optar al título de
Especialista en Seguridad Informática

Director de Tesis
Ing. Hernando José Peña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MOMIL – CÓRDOBA
2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Momil, 20 de Mayo de 2019

Tabla de contenido

Pag.

LISTA DE TABLAS

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pag.

DEDICATORIA

De manera muy especial a Dios:
Por ser la mejor motivación en mi día a día primordialmente, a pesar de las dificultades, los problemas que se presentan y las desmotivaciones no me abandona y siempre me brinda un poco de su ayuda así no la sienta o a veces no lo tenga presente en el momento. Gracias por ser mi guía en mis momentos alegres, tristes, en mis triunfos, debilidades, en mis enfermedades y en mis fracasos. Gracias Dios porque este grado es un escalón más, que me ayuda a sobresalir en la vida, a estar más cerca de cumplir mis metas y sueños.

A cada uno de los miembros de mi familia porque cada uno de ellos directa o indirectamente han ayudado en mi proceso académico con sus consejos y entusiasmo.

A mi madre María del Rosario Villadiego Guevara, que gracias por sus consejos, orientaciones y valores inculcados desde un inicio para ser una persona de bien, y no tomar caminos que me puedan llevar al fracaso, por su amor y compresión en cada momento de mi vida, por sus palabras de motivación a diario.

A mi padre Gustavo Adolfo Ayazo Patiño, por ser una persona correcta en todo el sentido de la palabra, por la confianza que me brinda todos los días, por estar atento a cada situación que llega a mi vida y darme la mano en cada uno de ellas, por su amor incondicional que me das todos los días y ayudarme en mi proceso de formación con su apoyo económico.

A mis hijos, por ser esas personitas que llevo presente todos los días de mi vida, que con una sonrisa me alegran siempre, por ser esa motivación extra en cada una de las metas que me coloco y por su amor incondicional.

_____
Perú Ayazo Villadiego

RESUMEN

La presente monografía se centra en hacer referencia al uso de la informática forense aplicada a delitos informáticos en la industria colombiana, teniendo en cuenta la revolución sobre la seguridad informática surgida desde mediados del siglo XX hasta la actualidad, esto ha traído consigo un sinnúmero de beneficios, especialmente para el intercambio de información y la forma de comunicación a nivel mundial; sin embargo, aunque su evolución tiene importantes ventajas para nuestro diario vivir, también esta tiene sus desventajas, y con ella han surgido los delincuentes informáticos, donde estos han perfeccionado su modus operandi en todo lo que se referencia a la Ciberdelincuencia; siendo de los más frecuentes el hurto de información de las empresas mediante medios informáticos.

Las empresas colombianas se han visto seriamente afectadas por estos delincuentes informáticos, donde son blancos de robo de información, robo de cuentas bancarias, a través de sus computadoras, tablets, equipos celulares, todos aquellos dispositivos que puedan almacenar o copiar información.

Antes de la expedición de la Ley 1273 de 2009 que regula lo concerniente a los delitos informáticos, el delito en estudio, era solo catalogado como un delito de hurto de acuerdo al Código Penal (Ley 599 de 2000, Artículo 239), sin embargo, con la entrada en vigencia de esta nueva ley, el tratamiento penal es el de hurto calificado, consagrado en el artículo 240 de la Ley 599 de 2000, y tiene actualmente una pena de prisión de seis (6) a catorce (14) años, de acuerdo a las circunstancias de tiempo, modo y lugar.

Por lo anterior, se desarrollará la presente monografía, la cual busca analizar qué tan afectada se encuentra la industria colombiana en este sentido, tomando como referencia el articulo 269 I.

ABSTRACT

This monograph focuses on making reference to the use of computer forensics applied to cybercrime in Colombian industry, taking into account the revolution in computer security that emerged from the mid-20th century to the present, this has brought with it a number of benefits , especially for the exchange of information and the way of communication worldwide; However, although its evolution has important advantages for our daily life, it also has its disadvantages, and with it cyber criminals have emerged, where they have perfected their modus operandi in everything that is referred to Cybercrime; being the most frequent the theft of information of companies through computerized means.

Colombian companies have been seriously affected by these computer criminals, where they are targets of information theft, theft of bank accounts, through their computers, tablets, cell phones, all those devices that can store or copy information.

Before the issuance of Law 1273 of 2009 that regulates what concerns computer crimes, the crime under study was only classified as a crime of theft according to the Criminal Code (Law 599 of 2000, Article 239), however, With the entry into force of this new law, the criminal treatment is that of qualified theft, enshrined in Article 240 of Law 599 of 2000, and currently has a prison sentence of six (6) to fourteen (14) years, according to the circumstances of time, manner and place.

For the above, the present monograph will be developed, which seeks to analyze how affected the Colombian industry is in this regard, taking as reference the article 269 I.

1. TITULO

USO DE LA INFORMÁTICA FORENSE APLICADA A DELITOS INFORMÁTICOS EN LA INDUSTRIA COLOMBIANA.

INTRODUCCIÓN

En pleno siglo XXI, la era contemporánea está en un desespero constante de evolución a las diferentes tecnologías, las cuales se desarrollaron rápidamente a raíz de la gran evolución industrial ocurrida en Inglaterra y esta avanza a pasos agigantados con los grandes beneficios del internet y/o de los medios informáticos.

La seguridad informática tiene una directriz clara y es la de proteger los diversos recursos tecnológicos inherentes a la operación de la empresa o entidad, que en este caso serían de hardware y software.

La informática forense surge por la necesidad de investigar incidentes o delitos informáticos, en otras palabras, se aplican una serie de métodos con el fin de obtener Información, datos o evidencias que están en un equipo de cómputo o sistema de información, que se haya visto involucrado en algún acto delictivo.

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 desastrosa.

Es por esto que, al convertirse en un tema importante para el ser, 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, de igual forma nacen nuevas amenazas que pueden generar daños considerables y cuantiosos a las empresas

Debido al aumento de la Ciberdelincuencia o delitos informáticos, vemos que el tema de Análisis Forense Digital (AFD) es muy importante para las entidades encargadas de la seguridad y custodia de un país (Ministerio de Defensa, Policía Nacional, Fuerzas Militares, entre otros).

Teniendo en cuenta todo lo anteriormente descrito se realizará la siguiente monografía, donde se recolectará toda la información correspondiente al tema, luego se identificarán las virtudes y falencias, para que finalmente se puedan exponer las conclusiones sobre el tema AFD en Colombia.

La presente investigación está estructurada en tres partes, así:

En el capítulo uno, se muestra un marco global de la informática forense, sus elementos o antecedentes, ¿Qué es la informática forense?, ¿En qué consisten los elementos probatorios?, ¿En qué consisten los delitos informáticos?, ¿Cuáles son los tipos de atacantes?, sus fines u objetivos, fase de la investigación forense en las organizaciones, las herramientas, las metodologías apropiadas en la aplicación de dicha informática. En el segundo capítulo se manejarán los delitos informáticos en las industrias Colombianas y sus respectivas leyes y normas y finalmente en el capítulo tercero se mostrarán algunos ejemplos y recomendaciones donde se aplica la debida informática forense.

2. DEFINICIÓN DEL PROBLEMA

En la actualidad, el funcionamiento de las sociedades humanas se basa en los sistemas informáticos, no solo en las instancias públicas o privadas sino también en el sector comercial, como también en lo que actualmente grandes conjuntos de datos que se componen con datos cotidianos de la población, lo que compramos o decimos, y que luego según resultados de análisis, se establecen perfiles para ofrecer los productos o servicios, de una forma personalizada.

Tras los agigantados avances en el desarrollo industrial, generados con el transcurrir de los años y el tiempo; y principalmente en el campo tecnológico, de mismo modo se observa la gran disposición y capacidad de algunos seres humanos, lo que les ha permitido desarrollar herramientas y misiones que hacen que vivamos más apegados a las herramientas tecnológicas en el campo laboral, pero teniendo en cuenta que a pesar de que hay beneficios y aspectos positivos, también encontramos que hay muchos negativos en el campo tecnológico; es por ello que surgen los llamados delitos informáticos que se internan en la sociedad, siendo más permanente su multiplicación, por lo tanto se genera la necesidad de retroalimentar las herramientas y elementos adecuados en las actividades investigativas haciendo uso del marco legítimo vigente, tendiente a la protección de los datos informáticos.

Para la presente monografía se tiene como orientación la siguiente pregunta:

¿Se hace buen uso a la informática forense en los delitos detectados en las organizaciones colombianas?

3. JUSTIFICACIÓN

Dado que en los últimos años se han incrementado a nivel mundial el uso de los recursos informáticos, esto ha generado un gran impacto, ya que el avance tecnológico a través del tiempo ha requerido e inclusive es indispensable a la hora de entretenimiento y ocio, el manejo de los recursos informáticos se ha convertido casi en la herramienta necesaria de nuestro diario vivir y es hasta conveniente, pero a sus innumerables y cuestionados beneficios que aporta, también se generan matices negativas e inadecuados, como los catalogados delitos informáticos, o que se estudian más bien como criminalidad informática, asunto que se ha vuelto muy común en la era reciente debido al uso desmesurado de todas estas herramientas tecnológicas que ayudan a facilitar la vida del ser humano, tanto en sus actividades cotidianas como las laborales, así el increíble avance de la tecnología informática ha creado cada vez más apertura hacia nuevas líneas de delincuencia que se van acrecentando mucho más con el mismo uso de la tecnología, teniendo en cuenta el deseo de control y delincuencia ha traspasado fronteras que anteriormente ni se imaginaba del gran alcance que tendría.

Es importante profundizar en este tema, toda vez que constituye un problema en la actualidad en la industria colombiana, por eso es pertinente realizar un estudio forense que permitirá dimensionar los alcances que tienen los ciberdelincuentes a la hora de abordar una empresa y vulnerar su seguridad; dando a conocer sus alcances, los métodos utilizados.

Por estos motivos la sociedad no es ajena a los delitos informáticos, pues siempre ven el accionar de bandas y personas con conocimientos en el tema para adquirir el control que les ofrecen os medios electrónicos y así buscar sus objetivos personales sin importar los intereses de los demás y en perjuicio de los demás.

De igual manera, la problemática a largo plazo estará enfocada con los progresos de los múltiples avances y desarrollos informáticos donde estos afectan las organizaciones a nivel mundial. El cuidado de éstos sería teniendo en cuenta la óptica penal y desde la legalidad. Los diferentes mecanismos de protección están unidos y no deben ser discriminatorias entre éstos, deben ser claramente entrelazadas. En este sentido y teniendo en cuenta las características de esta problemática, sólo mediante el cuidado general, teniendo en cuenta diferentes estamentos del orden legal, se pretende el cuidado y la protección para minimizar o evitar las amenazas a los medios informáticos, que cada vez son más frecuentes en la sociedad actual.

Según **Estrada** en su articulo dice que **"**En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, por ejemplo, lo que ya se conoce como criminalidad informática."[1]

Por esos motivos en Colombia se crea la ley 1273 de 2009 enfocada a controlar y disminuir o evitar los delitos informáticos con esta ley se cambia el Código Penal y se hace una reforma llamada "de la protección de la información y de los datos" y se respalda totalmente mediante programas que empleen los recursos de la información y la comunicación, a través de dispositivos, que cada vez son más numerosos y sofisticados.

[1] Estrada, M. (2008). https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf. Recuperado el 7 de Abril de 2019

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar un estudio monográfico relacionado con el uso de técnicas de informática forense en la industria colombiana, en los casos presentados por fraude válidos dentro de un proceso legal.

4.2 OBJETIVOS ESPECÍFICOS

- Estudiar los métodos para tratar delitos informáticos en las industrias colombianas.
- Detallar cuales son los pasos adecuados para analizar un caso de delito informáticos.
- Analizar la cadena de custodia en el proceso de un delito informático, que garantice la contundencia de una prueba forense en las industrias colombianas.
- Proponer buenas prácticas para el análisis de los delitos informáticos a partir del análisis forense en las industrias colombianas.

5. ALCANCES Y LIMITES

5.1 ALCANCES

La monografía que se está describiendo pretende ser un trabajo de investigación, el cual está enfocado hacía la manipulación de pruebas o evidencia digital en el contexto de la informática forense en las industrias colombianas. Esta investigación comprende aquellas personas quienes han decidido dedicarse al área de protección de los sistemas informáticos o seguridad de la información requiriendo la adecuada recolección y presentación de pruebas o evidencias para la toma de decisiones y mecanismos de respuesta.

5.2 LIMITES

El mecanismo optado no tiene carácter preventivo de los delitos informáticos presentes en las industrias colombianas, sólo se limita a ofrecer una orientación o vía para obtener la admisión de la prueba o evidencia digital para aquellas empresas que requieran de este tema para así cuidar y proteger sus datos y disminuir el impacto de los delitos informáticos.

5.3 METODOLOGÍA

Desarrollada a través de la investigación, que consiste en descripción y el análisis de los mecanismos usados para abordar a cualquier delito informático en las empresas Colombianas. De igual manera para la realización del actual trabajo de investigación, se ha considerado como una orientación de conocimiento con respecto a la informática forense que se abordará en tres capítulos para el manejo de cualquier incidente de seguridad en computadores, y presenta las siguientes etapas: de identificación, preservación, análisis y presentación.

6. MARCO REFERENCIAL

6.1 MARCO TEÓRICO

En pleno siglo XXI, la tecnología ha tenido un desmesurado progreso, puesto que su avance es gigantesco, cada vez, encontramos herramientas (Software) más sofisticadas e innovadoras que se retan entre sí para ver las vulnerabilidades de estos avances y el desarrollo de la misma tecnología, si miramos retrospectivamente hacia el pasado nos damos cuenta que todo era transcrito y guardado en papel, como dice **Michelle (2016, p.1)**, “pero que el avance tecnológico conlleva a almacenar de manera digital estos registros, mediante ordenadores, también muchos de los procesos judiciales se hacen vía internet, sin tener en cuenta los innumerables beneficios que nos da la tecnología de información y comunicación, pero de igual forma debemos tener en cuenta que así como nos trae beneficios o aspectos positivos también tiene sus aspectos negativos o desventajas como la vulnerabilidad de los datos para ser borrados o duplicados del sistema; por esa razón surgen nuevas herramientas de control para los sistemas de información como lo es la Informática forense que se crea para proteger las políticas de control de la información y las tecnologías que faciliten la gestión de la información, protegiendo a la sociedad en general”.[2]

[2] http://primeranofcjpuc.blogspot.com/2016/06/analisis-de-informatica-forense-en-los.html

6.2 MARCO CONCEPTUAL

En el siguiente marco conceptual se desmesurarán los elementos que integran el análisis informático forense, sus características y su clasificación.

Informática forense

Se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia para borrar, adulterar u ocultar información. Es por lo tanto esperable que el mismo hecho de esta adulteración pase desapercibido.

El concepto forense se refiere a la utilización de métodos científicos en los procesos legales, no obstante, hay investigadores especializados en asuntos criminalísticas, que focalizan evidencias que representan dato determinante cuando se exponen a pruebas en los laboratorios destinados para tal fin. La informática forense se puede considerar como:

- Ciencia forense para la aplicación de prácticas científicas dentro del proceso legal; es decir, un conjunto de ciencias que la ley usa para atrapar a un criminal, ya sea físicamente, química, matemáticamente u otras más.

- En su artículo (Miranda, 2008) señala: “La informática forense es el proceso de investigar dispositivos electrónicos o computadoras con el fin de

descubrir y de analizar información disponible, suprimida, U ocultada que puede servir como evidencia en un asunto legal".[3]

Según (Zuccardi & Gutiérrez, 2015, pág. 9) el FBI (Oficina Federal de Investigación de los Estados Unidos): "La informática forense fue creada para atender las necesidades específicas y articuladas de aplicación de la ley para hacer la mayor parte de esta nueva forma de pruebas electrónicas"[4] y según (EUROLATINOAMERICA, 2017), la IFC (Informática Forense Colombiana), la informática forense se define "Como la disciplina que combina elementos de derecho y ciencias de la computación para recopilar y analizar datos de los sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que es admisible como pruebas en un tribunal de justicia"[5]

Si unificamos estos dos conceptos, tendríamos que la Informática Forense, es una disciplina auxiliar de la justicia, que ayuda a neutralizar o prevenir los ataques de delincuentes informáticos, con la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica, las cuales permiten identificar, preservar y analizar datos que han sido procesados electrónicamente, con el fin de obtener evidencias o pruebas de un delito informático (competencia desleal, robo) o conductas irregulares dentro de algún proceso, y así presentar la evidencia ante un tribunal o como defensa en alguna situación en el que esté involucrada la persona o entidad.

Todo esto mediante el uso de técnicas, principios y herramientas forenses. También se usa para probar que se han cometido actos deshonestos. Algunos de

---

[3] Miranda. (2008). Importancia de la informática forense. septiembre 10, 2019, de Primer Congreso Estudiantil de Investigación del Sistema Incorporado 2013 Sitio web: https://www.academia.edu/23975452/Informatica_forense

[4] G. Zuccardi, and J. D. Gutiérrez, Informática Forense. [Online]. Available: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20 v0. 6.pdf

[5] Ciencia, Tecnología y Justicia. (2017). Informática Forense. 05//10/2019, de IFORENSE Sitio web: https://www.informaticaforense.com.co/informatica-forense/

los ámbitos en los que se pueden presentar los delitos informáticos o conductas irregulares, que ameritan una investigación forense son: mercantil, laboral, judicial, educativo, financiero, entre otros.

- **Informática forense**

Nace de la división de la seguridad informática con la intensión de tener, analizar y validar todo tipo de evidencia, capaz de recopilar, almacenar y mostrar datos o información.

- **Seguridad informática y de la información**

Estos términos son parecidos, pero realmente son totalmente diferentes, sabiendo que ambas conllevan a un mismo fin.

La seguridad informática busca proteger los diversos recursos tecnológicos inherentes a la operación de la empresa o entidad, estamos hablando de hardware y software, y a su vez se busca que estos sean utilizados de manera adecuada, es por ello que se identifican las siguientes fases:

- **Fase de Identificación**

La fase de identificación se refiere a la recopilación de información necesaria para trabajar sobre la fuente de datos presentada por el administrador de los servidores (solicitud forense).
La identificación debe prever los desafíos que se pasaran durante los procesos de las fases de preservación y extracción. Esta fase culmina con un plan a seguir.

Etapa 1: Levantamiento de información inicial para el Análisis Forense

La solicitud forense es un documento donde el administrador del equipo afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio

al proceso de análisis “Comprende obtener información sobre el o los equipos informáticos afectados como sistema operativo, datos técnicos, fecha, tipo de incidente, características de configuración como dirección IP, etc”[6] (Quintero, 2014)

- **Fase de Validación y preservación.**

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las “huellas del crimen”, se deben asegurar estas evidencias a toda costa “con el elemento identificado se procede a realizar una imagen exacta del contenido de la evidencia asignando un código único correspondiente a una combinación única de bytes que constituye la totalidad del medio en observación”[7] (eyasno, 2014).

- **Fase de Análisis de la evidencia.**

En su artículo, eyasno señala: “El punto de partida del análisis comienza cuando se detecta una tipo de ataque informático o se sospecha de manipulación no autorizada de información. Una actividad ilícita reportada puede ser el borrado la información que puede comprometer a una persona o información que pudo haber sido ocultada o almacenada en medios no convencionales como disquetes, cd rom, dvd rom, flash drive” (2014, pág. 2), Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

---

[6] Jairo Quintero. (2014). Blog Informática Forense. 09/10/2019, de Periódico Digital Galanista Sitio web: http://www.colegiogalanvilla.edu.co/blogs/archives/749

[7] eyasno. (2014). ESTUDIO DE CASO FORENSE. 09/10/2019, de elforense Sitio web: https://elforense.wordpress.com/2014/06/03/estudio-de-caso-forense-1/

Delito Informático

Son conductas en que el o los delincuentes se acuden a programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, pornografía infantil, etc (Galán, 2019).

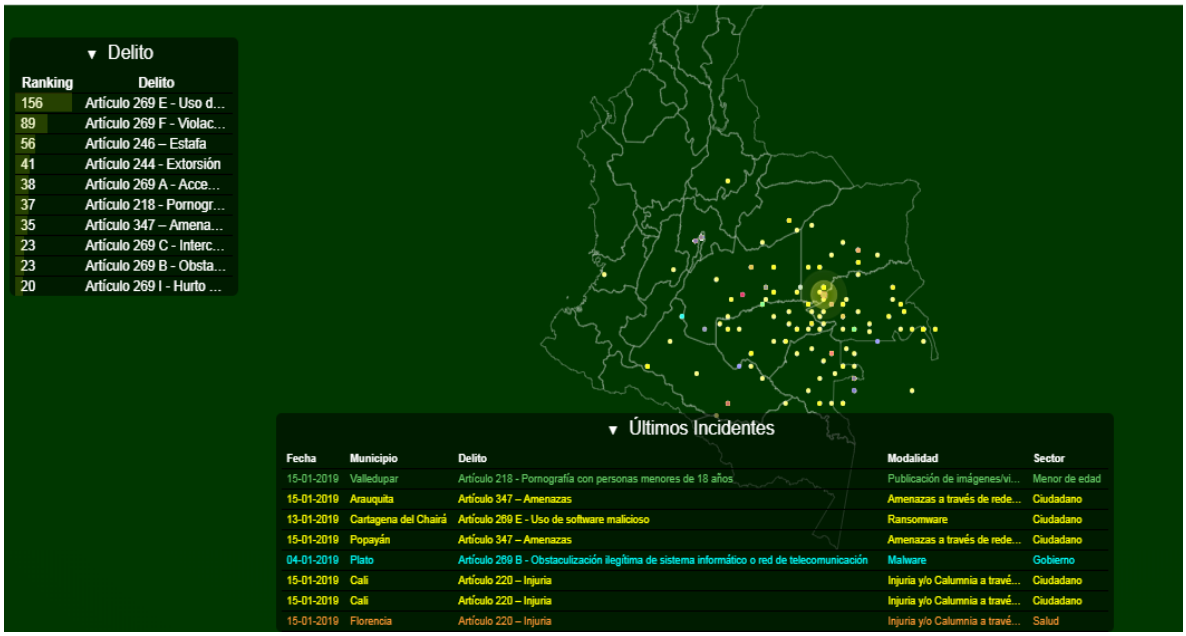
> El avance tecnológico constante que se presenta en la actualidad, que además se da a pasos agigantados, como la masificación del uso de la tecnología en el mundo, es una realidad que permea todas las actividades que se realizan en la sociedad de hoy día, cosas como la redes sociales, las aplicaciones que gestionan información de los usuarios, el internet de las cosas, entre otras, implican que quienes las utilizan se expongan a diversos riesgos de sufrir ataques contra su información, contra sus sistemas e incluso contra su propia integridad (Molina, 2018, s/p.).

Los también conocidos como Cibedelitos como lo señala (Telléz, 2014, pág. 7) que “Son actuaciones contrarias a los intereses de las personas donde utilizan a las computadoras como un instrumento o conductas atípicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)”[8].

En la siguiente imagen observamos un monitoreo en tiempo de real de la página de la policía nacional de Colombia, donde observamos el ranking y el delito con el artículo que da origen a la infracción que se ha causado; también se observan los últimos incidentes causados y mediante que modalidad se efectuaron (Phishing, Malware, Vishing, Amenaza a través de redes sociales; Ransomware, Grooming, Suplantación de identidad, Spoofing, Sextorsión).

[8] Julio Téllez. (2014). Derecho Informático. 11/10/2019, de clauditha2017 Sitio web: https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Figura 1. Ciberincidentes en Colombia.

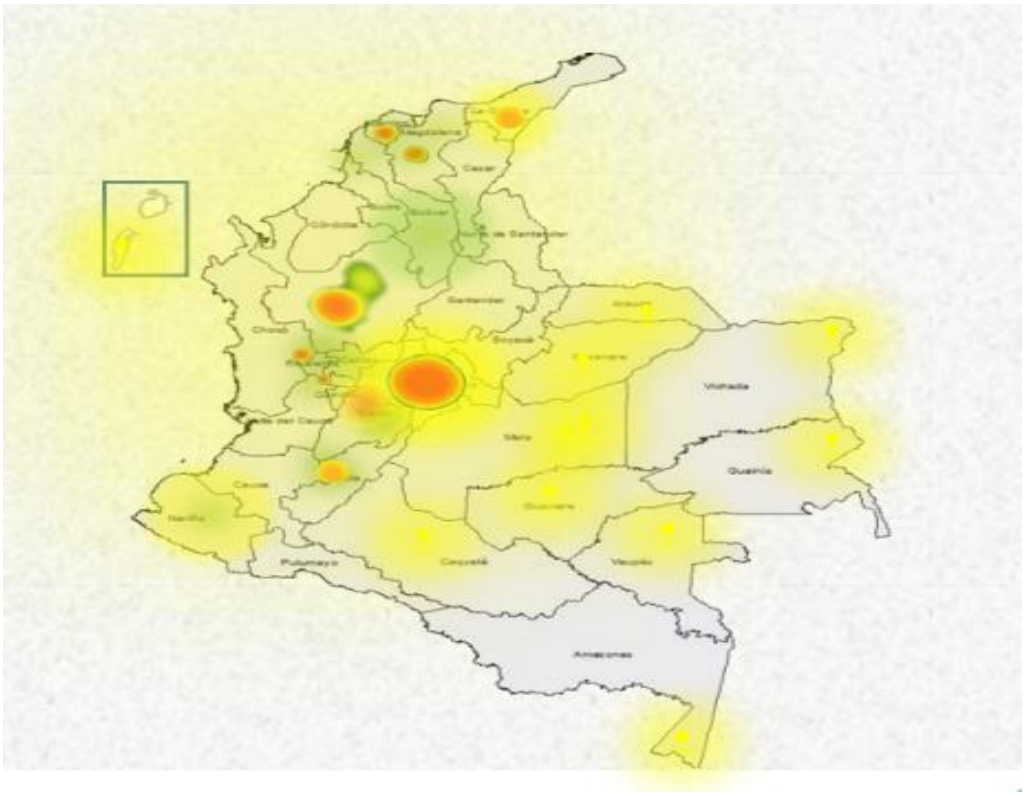


Fuente: Policía Nacional de Colombia. Ciberincidentes (Visualización Mapa Tiempo Real). [Figura]. https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

En la página de la policía nacional en la parte de ciber incidentes las cifras de los crímenes crecen todos los días en nuestro país, por ejemplo; estafas por compras, ingeniería social, malware, phishing, vishing, ransomware, o suplantación de identidades, entre otras. Es por esto que es muy importante alarmar o prevenir a todas las personas y organizaciones del país sobre estos tipos de delitos y buscar soluciones para generar un entorno sano y tranquilo.

En el país colombiano el panorama sobre el tema de los delitos informáticos se ve evidenciada por el siguiente mapa:

Figura 2. Mapa Ciberdelitos en los departamentos.



Fuente: Policía Nacional de Colombia. Cibercrimen (Visualización Mapa Tiempo Real). [Figura]. https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

Observamos en la figura anterior que la principal ciudad con más índices de delitos informáticos es Bogotá seguida por las ciudades de Cali, Medellín, barranquilla y Bucaramanga.

En Colombia, la panorámica del delito informático se ve reflejada en el siguiente mapa de calor, donde en las principales ciudades se encuentra más del 75% de suscriptores de internet fijo y el mayor índice de habitantes por ciudad.

Hace ya algún tiempo se viene operando en el ambiente tecnológico el concepto de Delito informático, muchos organismos han emitido sus conceptos desde diferentes puntos de vista.

Tipos de delitos informáticos

Principalmente hay varias falencias en la seguridad de la información, comprobados por la ONU, cada uno presenta las siguientes categorías:

A. Fraudes cometidos mediante manipulación de computadoras.

a) **Manipulación de los datos de entrada:** Este tipo de fraude informático, llamado también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

   No requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b) **La manipulación de programas:** es complicado descubrir y pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática.

   Este delito consiste en modificar los programas existentes en el sistema de las computadoras o en instalar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) **Manipulación de los datos de salida:** Frecuentemente los delitos se hacen por cajeros automáticos mediante los engaños o fraudes de identidad u obtenciones de información.

d) **Fraude efectuado por manipulación informática:** Este delito utiliza u obtiene las reproducciones automáticas de los procedimientos en las computadoras, en otras palabras es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

B. Falsificaciones informáticas.

a) **Como Objeto:** Se evidencia al momento en que se intercambian o alteran las informaciones (Documentos) acumuladas en los ordenadores electrónicos.

b) **Como herramienta:** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

C. Perjuicio informático

Está relacionada con el hecho de eliminar, anular, deshacer o cambiar sin consentimiento, funciones o informaciones de computadoras con el propósito de obstruir las actividades normales de los sistemas. Los métodos para realizar los sabotajes son:

- **Virus**: Es un suceso de cifras programáticas que logra o consigue

asociarse a los programas legales o auténticos y expandirse a diferentes programas informáticos. este suceso o virus es capaz de incorporarse en los sistemas por medio de piezas originales de apoyo lógicos que han sido contagiado la más común es una memoria USB.

- **Gusanos:** Estos se elaboran parecidos al virus infiltrando en programas originales o únicos en los procesamientos de registros o para modificar los registros, pero es opuesto al virus porque no se pueden volver a restablecer.
- **Bomba lógica o cronológica:** Requiere entendimientos especializados puesto que requiere de la programación de la destrucción o cambios en los datos en un instante dado del futuro. Es un procedimiento totalmente al revés de los virus o los gusanos, las bombas lógicas son dificultosas e complicados de localizar o descubrir antes de que se revienten; de tal modo, los aparatos informáticos criminales, las bombas lógicas son las que dominan el mayor latente nocivo. Su significado puede planificar o proyectar para que provoque el mayor perjuicio y para que colisione mucho tiempo después de que se haya ido el criminal. La bomba lógica se puede utilizar igualmente como mecanismos de extorsiones y se permite exigir una liberación o recuperación a cambio de dar a conocer el sitio en el cual se encuentra el detonante.

D. Acceso no autorizado a servicios y sistemas informáticos

Esta se genera por diversas razones: desde el sencillo espionaje, como en los acontecimientos de los hackers hasta el sabotaje o espionaje informático, que son delitos de alto compromiso.

- **Piratas informáticos o hackers:** este ataque se hace generalmente en sitios exteriores, ubicados en las redes de telecomunicaciones, aproximándose a diferentes formas de acceso. El criminal consigue usar o

emplear las faltas en las medidas de seguridad o en los sistemas de las empresas. Frecuentemente los hackers se hacen pasar por personas legales en los sistemas; suele pasar con mucha continuidad en los sistemas en que las personas deben utilizar claves.

- **Reproducción no autorizada de programas informáticos de protección legal:** Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales (Hall, 2018)[9].

Un punto de referencia que puede dar un concepto universal de Delito Informático en un ambiente internacional es el “Convenio de Ciberdelincuencia del Consejo de Europa”**,** del cual se puede decir:

Delitos Informáticos: Nidia Callegar lo define como “aquel que se da con la ayuda de la informática o de técnicas anexas”, los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos[10].

En definitiva, el Delito Informático es todo acto que haga uso de medios informáticos, que sea contrario a una legislación establecida en un país lo cual acarrea una sanción judicial.

---

[9] Andrés Hall. (2018). Tipos de delitos informáticos. 13/10/2019, de Cámara Argentina de Comercio Electrónico Sitio web: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

[10] Callegari, Nidia. (2015). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. 2019/10/12, de Revista de Investigación Jurídica Sitio web: http://www.pensamientopenal.com.ar/system/files/2016/08/doctrina44051.pdf

Convenio de Ciberdelincuencia De 2001.

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". Al día de hoy se han adherido al convenio más de 56 países de todo el mundo, incluyendo Chile, Costa Rica, República Dominicana, Panamá y recientemente Argentina, en lo que refiere a Latinoamérica. Mientras que Paraguay, México, Colombia y Perú han sido invitados a firmar el acuerdo y están próximos a concretar la adhesión.

El convenio tiene cuatro capítulos, en los que se establecen **tres ejes esenciales** para hacer frente a los delitos informáticos:

Tenemos que en el **primer eje**, se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática.

En este convenio se propone una clasificación de los delitos informáticos en cuatro (4) grupos:

- Delitos que tienen a la **tecnología como fin**: Son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información.
  Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.

- Delitos que tienen a la **tecnología como medio**: estos se refieren a delitos ya conocidos, los cuales son cometidos a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales.
  Por ejemplo, el fraude informático o la falsificación de datos digitales.

- Delitos relacionados con el **contenido**: se establecen como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

- Delitos relacionados con **infracciones a la propiedad intelectual**: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización.
  Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

En el **segundo eje** encontramos las **normas procesales**: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia.

La magnitud de alcance de esta sección va más allá de los delitos definidos en el punto anterior, debido a que aplica a cualquier delito cometido por un medio informático o cualquier evidencia en formato electrónico.

Ya en el **último eje** contiene **las normas de cooperación internacional**, no son más que reglas de cooperación para investigar cualquier delito que involucre evidencia digital. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición.

Descripción de las Legislaciones sobre Delitos Informáticos.

Realizando un estudio a las diferentes legislaciones que pueden ser utilizadas para castigar el delito informático, a nivel internacional se ha tomado como referencia las leyes descritas a continuación:

- ✓ **Legislación Delitos Informáticos en Colombia**

El 5 de enero de 2009, el Congreso de la República promulgó la “Ley 1273”, la cual modificó el código penal adicionando nuevas sanciones en casos relacionados con los delitos informáticos, buscando proteger la información y preservar los sistemas de tecnologías de información y comunicaciones.

Esta ley contempla dos capítulos: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”, y “De los atentados informáticos y otras infracciones”. (Daccach, 2018)

Según (Daccach, 2017) sostiene que “dicha ley tipificó como delitos las conductas en el manejo de datos personales, por eso es que es de muchísima importancia que las empresas se protejan jurídicamente para evitar incurrir en alguno de estos tipos penales. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos”.[11]

- ✓ **Legislación Delitos Informáticos en Costa Rica**

La presidenta Laura Chinchilla firmó la Ley 9048 “Reforma de varios artículos y modificación de la sección VIII denominada delitos informáticos y conexos, del título VII del Código Penal”[12]. (Zdenko, 2012)

Esta ley sanciona el delito de corrupción, también contempla la violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa informática, daño informático, espionaje, sabotaje informático, suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación de delito informático y difusión de información falsa.

---

[11] Daccach, José. (2017). Ley de Delitos Informáticos en Colombia. 13/9/2019, de Delta Aesores Sitio web: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

[12] Zdenko, Seligo. (2012). LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS COSTA RICA. 16/9/2019, de DelitosInformaticos Sitio web: https://delitosinformaticos.com/legislacion/costarica.shtml

- ✓ **Legislación Delitos Informáticos en Perú**

> Podría pensarse que Perú llega tarde con su adhesión a una Convención aprobada en el año 2001. En realidad, al tratarse de un acuerdo del Consejo de Europa, fue inicialmente negociado y firmado exclusivamente por estados europeos y algunos invitados como Estados Unidos y Canadá. Casi dos décadas después, menos del 15% de naciones que no pertenecen al Consejo de Europa han decidido adherirse a él. De hecho, en nuestra región, solo algunas lo han hecho y muy recientemente: Argentina (2018), Chile (2017), y Paraguay (2018). México y Colombia, aunque invitados ya, están todavía tramitando su adhesión. Por tanto, realmente Perú no llega tarde a la firma de este acuerdo cuya suscripción fuera de Europa parece más bien la excepción y no la regla. (Morachimo, 2019, s/p).

Teniendo en cuenta el artículo del periódico (Peruano, 2013) nos dice que "la presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la Ciberdelincuencia"[13].

Integridad

Dentro de la seguridad informática, se puede ver como un servicio que permite que la información sea creada, modificada o eliminada sólo por las personas autorizadas para tal fin. Según **IS027002** "salvaguarda la precisión y completitud de la información y sus métodos de proceso", El sistema no debe permitir dañar o modificar la información contenida dentro del mismo ni permitir que personas que no estén autorizadas lo hagan; se debe tener en cuenta que la integridad incluye no solo modificaciones planeadas sino también las accidentales.

Tenemos que la importancia de la integridad de los datos la podemos ilustrar en el siguiente ejemplo:

---

[13] El peruano. (2013). Ley de Delitos Informáticos. 10/8/2019, de Normas Legales Sitio web: https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Podríamos imaginar una situación propia de una obra de ficción que antecediera al ataque del virus Stuxnet en 2010 y preguntarnos qué ocurriría si alguien interfiriera los sistemas de control de una central nuclear para que simularan condiciones de funcionamiento normal cuando, en realidad, se ha provocado una reacción en cadena[14].

Confidencialidad

Es la capacidad que tiene un sistema para evitar que la información contenida en él sea accesible por personas, entidades o procesos no autorizados para esto. La confidencialidad es de gran importancia debido a que las consecuencias en caso de que personal no autorizado acceda a la información, pueden ser muy graves para la organización.

> Consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, etc. (INFOSEGUR, 2013, s/p)

Disponibilidad

Tiene que ver con la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento, “supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados[15].” (pmg-ssi, 2018, s/p).

---

[14] Dobbs, Michael; The Edge of Madness, Simon & Shuster UK Ltd., RU, 2008

[15] pmg-ssi. (2018). Sistemas de Gestión de Seguridad de la Información. 5/9/2019, de SGSI Sitio web: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Análisis forense

Conjunto de técnicas científicas y analíticas especializadas en infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal, “cuyo fin es adquirir información importante de diferentes medios de almacenamiento sin llegar a modificar el estado de los mismos, esto con el fin de encontrar información oculta, patrones o comportamientos y que pueden ser usados o no en una investigación”[16] (Porolli, 2013)

.

[16] Porolli, Matías. (2013). welivesecurity. 14/4/2019, de eset Sitio web: https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

6.3 MARCO HISTÓRICO

Antecedentes

- **En el año 1932:** en ese año fue un motor de impulso para el FBI debido a que desarrolló un sistema para suministrar servicios forenses a todos los agentes de campo y otras autoridades **(De León-Huerta, 2009).**

- **En el año 1970:** En este año aparecieron los transistores. Entre los años 1971 y 1981 con el surgimiento de los circuitos integrados, comenzó la innovación de las computadoras **(Calderón-Toledo, 2008).**

- **En el año 1980:** Se dan a conocer las pruebas genéticas, por estos años la prueba genética, fue usada en Nueva Zelanda, sin embargo, no figura como prueba válida hasta años después, en los tribunales de los Estados Unidos de América **(Rodríguez & Doménech, n.d)**

- **En el año 1984:** Durante este año fue creado el Programa de recursos Magnéticos del FBI, pero luego se cambió por Jefe del Equipo de Análisis Digital (CART). También aparecieron la arquitectura Risc, que diseñan funciones inteligentes capaces de adaptarse a aplicaciones que así lo requieran **(Berzal, n.d).**

- **En el año 1990:** Fue importante porque aparecieron los rastros digitales, con valor probatorio, pero sólo se utilizaron finalizando el siglo XIX **(Rodríguez & Doménech, n.d.).**

- **En el año 1993:** en este año se conmemora la primera Conferencia Internacional sobre la Evidencia Digital.

- **En el año 1995:** en esta fecha se hizo la Organización Internacional de Evidencia Digital **(IOCE).**

- **En el año 1997:** en diciembre, los países del G8 en Moscú declararon que “los funcionarios responsables de dar cumplimiento a la ley, deben estar formados y dotados para hacer frente a los delitos de alta tecnología.”.

- **En 1998:** En Marzo, el G8 nombrado el IICE para hacer los principios internacionales, los procedimientos regessem basados con la prueba digital.

  En 1998: INTERPOL Forensic Science Symposium.

- **En 1999:** Se analiza el desempeño total de la FBI en informática forense superior a 2000 casos a través del análisis de 17 terabytes de datos.

- **En el 2000:** se crea el primer laboratorio regional de Informática Forense del FBI.

- **En el 2001:** se realiza un chequeo general: pretende investigar y monitorizar la funcionalidad en los Sistemas de Información e Internet: Informática Forense **(Fernández Bleda, 2004).**

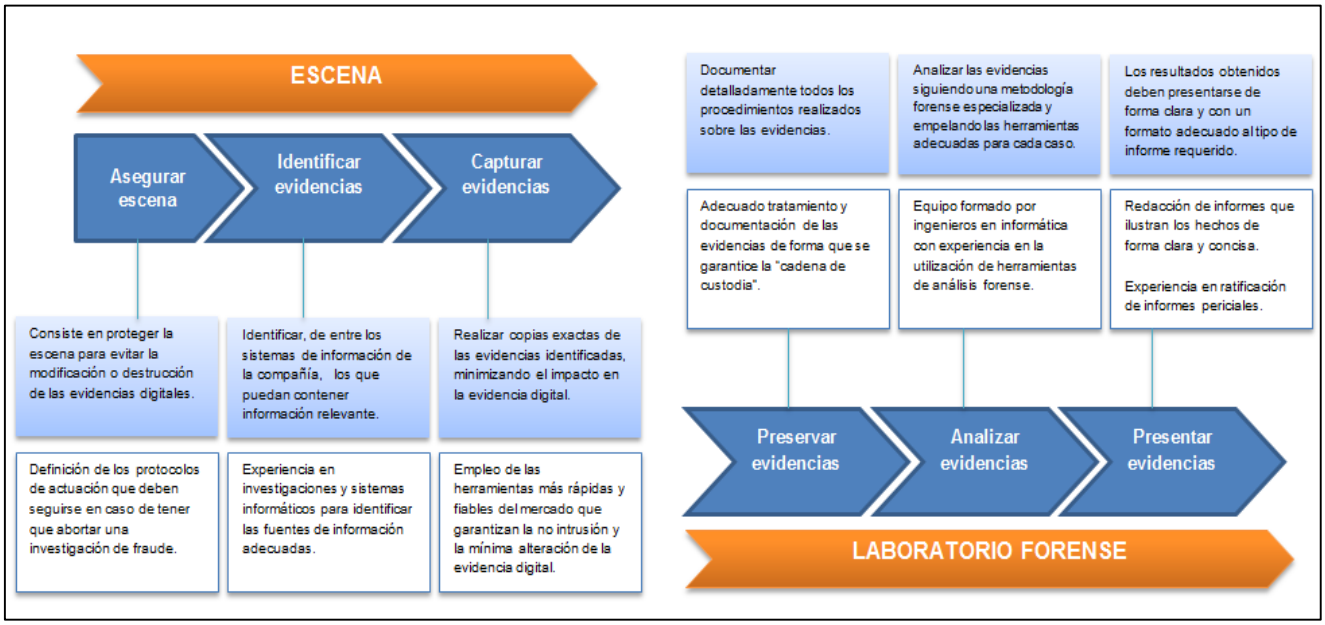
- **En el 2003:** El análisis general del FBI en casos de delitos informáticos supera los 6500, por medio del análisis de 782 terabytes de datos.

La gran mayoría de ataques a la seguridad de una empresa es en gran culpa por las malas prácticas de sus empleados, los cuales por falta de capacitación realizan jugadas infantiles las cuales les puede costar millonadas a las compañías, aunque también por agentes externos, lo que lleva a las compañías a sensibilizarse y tomar pautas y medidas para prevenir un ataque, los mecanismos más generales independientemente de la tecnología utilizada para prevenir ataques a la seguridad son por mencionar algunos los siguientes: autenticación, autorización, administración, auditoria y registración, mantenimiento y la integridad de los mismos datos.

Esos mecanismos son llevados a cabo por unas técnicas las cuales permiten que estos requisitos sean evaluados y revisados constantemente por parte de las compañías.

Por lo tanto las fases necesarias para finalizar con éxito un análisis forense en una investigación son:

Figura 3. Manejo de evidencias.



Fuente. http://slideplayer.es/slide/1490888/

Modelos de procesos para la informática forense aplicada

Hay diferentes aproximaciones a un modelo que se acerque a las fases por las que atraviesa un examen de pruebas digitales, por tanto, esbozamos una recolección de los diferentes modelos en orden cronológico:

A. Modelo de Casey (2000)

Eoghan Casey, en el año 2000 presenta un modelo para procesar y analizar pruebas digitales, pero este modelo ha mejorado con los siguientes elementos:

- ✓ **La identificación:** hay que identificar todo el hardware y el software que posteriormente vamos a analizar.

- ✓ **La conservación, la adquisición y la documentación:** aunque todo esté incluido en la misma etapa, la parte de documentación debemos tener en cuenta que se debe realizar a lo largo de todas las fases, especialmente en caso de estar trabajando para un juicio. Durante la adquisición, extraeremos el hardware que vayamos a analizar (por ejemplo, el disco duro del ordenador) y durante la fase de conservación se haría el clonado de los discos duros que hayamos extraído, ya que no se puede manipular el dispositivo original que se obtiene.

- ✓ **La clasificación, la comparación, y la individualización.**

- ✓ **La reconstrucción:** una vez analizados todos los datos en la fase anterior, debemos ser capaces de realizar una reconstrucción de los hechos y responder a las siguientes preguntas: ¿Qué? ¿Quién? ¿Dónde? ¿Cuándo? Y ¿Por qué?

En los pasos 3 y 4 se hace el análisis de la prueba. Según (Séamus Ó Ciardhuáin, 2004) “el modelo se evalúa inicialmente en contextos de programas de cómputo independientes de la red, y después realizado para las diferentes capas de red (desde física hasta la capa de aplicación) para detallar investigaciones en redes de computadoras”[17].

B. Modelo de Lee

Fue uno de los primeros modelos que se crearon para el análisis forense en 2001.

“En este modelo se distinguen, al igual que en el modelo del U.S. Dep. of Justice que veremos más adelante, cuatro fases, a diferencia del estadounidense el

[17] Séamus Ó Ciardhuáin. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3, 1.

modelo de Lee, describe el proceso de análisis de la escena del delito y no de todo el proceso”[18] (Lee, Palmbach, & Miller, 2001).

Además, tiene un enfoque metodológico clásico en cuanto a investigación forense, trasladándolo a la informática forense desde la perspectiva de las pruebas digitales.

Las diferentes fases que se describen son:

- **Reconocimiento:** durante esta fase el investigador debe saber qué buscar, por lo que se puede dividir en dos subfases: la de documentación y la adquisición/preservación de pruebas.

- **Identificación:** se clasifican las pruebas recogidas en la fase anterior según los estándares.

- **Individualización:** cada ítem o archivo es evaluado e interpretado de forma individual, comprobando si de alguna forma se pueden conectar con los hechos investigados.

- **Reconstrucción:** con todos los datos obtenidos en la fase anterior, se intenta reconstruir el hecho investigado, del que posteriormente se realizará una presentación.

C. Modelo extendido de Séamus Ó Ciardhuáin

“Gran parte de los modelos existentes están basados en el procesamiento de pruebas digitales, por tal razón en el año 2004”, (Ciardhuáin, 2004), se formula

[18] Colmenares Mendoza Alberto Yesid y Cruz Guzmán Diego. (2013). Importancia de la Informática Forense. 22/8/2019, de Primer Congreso Estudiantil de Investigación del Sistema Incorporado Sitio web: https://www.academia.edu/23975452/Informatica_forense

este modelo, que intenta cubrir todas las fases y aspectos de una investigación de ciberdelito[19].

Se trata de una metodología que consta de 13 fases y donde la cadena de custodia está formada por la lista de aquellos que han manipulado cada prueba digital, debiendo agregar los nombres a la lista cada vez que se pasa una fase. Debido al alto número de fases, es la que mejor establece los flujos de información y los puntos de control durante todo el proceso de la investigación. Además, la principal ventaja de este modelo es que describe todo el proceso desde el momento en el que se hace necesario realizar una investigación hasta que ha sido finalizada y presentada.

El mayor fallo en los modelos existentes es que explícitamente no identifican la información que fluye en las investigaciones. Por ejemplo, Reith Et Al. (2002) no menciona la cadena de custodia en su modelo. Este es un fallo primordial cuando se consideran las diferentes leyes, las prácticas, los lenguajes, entre otros que deben ser correctamente distribuidos en investigaciones reales en las empresas a nivel nacional y mundial.

A continuación, se detallan y comentan brevemente las 13 fases que describen el funcionamiento de este modelo:

Conciencia: Para Séamus Ó Ciardhuáin, el primer paso en una investigación es crear una conciencia de que esta investigación es necesaria.
Autorización: E paso previo para comenzar la investigación, es obtener una autorización para poder realizarla.

Planificación: En esta fase se planifica cómo será la investigación, que estará influenciada desde por las leyes que rigen el país hasta por las políticas internas

[19] Séamus Ó Ciardhuáin. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3, 1.

del cuerpo que esté investigando. Puede ocurrir que esta fase suponga una vuelta al punto dos, requiriendo de otro tipo de autorizaciones para poder continuar.

Notificación: Esta fase depende de cada investigación, en este punto puede ser necesario notificar al objetivo de la investigación que se está llevando a cabo.

Búsqueda e Identificación de Evidencias: Localizar e identificar a partir de distintos métodos es la ocupación de este punto y es esencial para tener las evidencian preparadas para la siguiente fase.

Adquisición: En esta fase se recogen las pruebas físicas. Por ejemplo, después de buscar e identificar el PC anterior de un sospechoso, se hace un clonado de su disco duro para su posterior análisis.

Transporte: Después de obtenidas las pruebas, estas deben ser transportadas al lugar de su posterior análisis.

Almacenamiento: Ya sabiendo que el análisis de las evidencias adquiridas y transportadas no pueden ser analizadas de forma totalmente inmediata, lo siguiente será guardarlas en un lugar seguro.

Examen: Esta es la parte más importante de todo el proceso de investigación, donde se produce el análisis de las evidencias y se obtendrán los datos que posteriormente se utilizarán para el informe.

Hipótesis: Ya teniendo los datos obtenidos en el examen, el investigador deberá formular una hipótesis de lo ocurrido.

Presentación: La hipótesis se presenta al jurado, la empresa o quien corresponda según el caso.

Prueba/defensa: Dado que el investigador está detallando una hipótesis, este tendrá que defenderla delante de la persona que corresponda, ya que la hipótesis puede ser tumbada.

Difusión: Dependiendo de la investigación (esto es más complicado si estamos en el ámbito de las investigaciones privadas), la información y el resultado pueden ser difundidos.

D. Modelo del U.S. Dep. of Justice de EEUU.

Este es uno de los primeros modelos y más sencillos. Creado en 2001, aunque su última revisión es de 2007**. "**En él se detallan procedimientos para examinar todo tipo de dispositivos, desde los electrónicos hasta las armas de destrucción masiva"[20] (Justice, U.S. Department of., 2007).
En este libro se detallan todos los procedimientos y cómo se debe tratar la escena del crimen.

Se pueden distinguir cuatro fases durante el proceso de análisis de un ordenador:

- Identificación.
- Conservación.
- Análisis.
- Presentación.

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

[20] Justice, U.S. Department of. (2007). Handbook of Forensic Services. 14/5/2019, de FBI Sitio web: https://www.fbi.gov/file-repository/handbook-of-forensic-services-pdf.pdf/view

el cual dicho documento se conforma pensando estrictamente en el posicionamiento nacional del tema Ciberseguridad y Ciberdefensa.

6.4 MARCO LEGAL

Estatutos Nacionales

- **Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO**. Una persona que acceda sin permiso a los sistemas informáticos que se encuentran protegidos o con medidas de seguridad, pagara un castigo de cuarenta y ocho (48) a noventa y seis (96) meses, con un recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv).

- **Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN**. Una persona que no esté legalizado o aprobado para tener acceso a los sistemas informáticos, y evite las actividades o entradas normales a los sistemas informáticos, a las informaciones encontradas en los dispositivos, o en las redes de telecomunicaciones, pagara un castigo de cuarenta y ocho (48) a noventa y seis (96) meses y un recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv), siempre y cuando el comportamiento no erija delitos sancionados con una pena superior a la ya estipulada.

- **Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS**. Una persona, sin permiso judiciales que obstaculice o intercepte documentos informáticos encontrados en el interior de dispositivos electrónicos, haciendo mal uso de esas informaciones tales como chantajes, extorsiones, ataques cibernéticos, pornografía infantil entre otros datos informáticos pagara una condena de treinta y seis (36) a setenta y dos (72) meses según lo convenido.

- **Artículo 269D: DAÑO INFORMÁTICO**. Una persona que no tenga autorización en destruir, dañar, borrar o averiguar documentos informáticos, o elementos lógicos de un ordenador tales como; sistemas operativos, software de sistemas o editores de textos, pagara una condena de cuarenta y ocho (48)

a noventa y seis (96) meses y un recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv) según lo convenido.

- **Artículo 269E: USO DE SOFTWARE MALICIOSO**. Una persona que no tenga permisos o autorizaciones judiciales para comercializar, vender, distribuir software ilegales o maliciosos, o algún elemento dañino para los ordenadores, pagara una condena de cuarenta y ocho (48) a noventa y seis (96) meses y en recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv) según las normas vigentes.

- **Artículo 269F: VIOLACIÓN DE DATOS PERSONALES**. Una persona que no tenga autorizaciones previas para cambiar, vender, enviar, comprar, divulgar, sustraer, recopilar, obtener, ofrecer, interceptar, modificar, o emplear datos o códigos personales conseguidos por medio de bases de datos o algún fichero de un sistema para beneficio propio o de alguna persona allegada, pagara una de cuarenta y ocho (48) a noventa y seis (96) meses y un recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv) según lo estipulado.

- **Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES**. Una persona con propósitos ilícitos que no tenga autorizaciones judiciales para diseñar, desarrollar, ejecutar, traficar, vender, programar, codificar, o enviar páginas, enlaces o ventanas emergentes, pagara una condena de cuarenta y ocho (48) a noventa y seis (96) meses y un recargo de 100 a 1000 salarios mínimos legales mensuales vigentes (smlv).

- **Artículo 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

- **Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES:** El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 **manipulando un sistema informático**, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

- **Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS:** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

  Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad[21] (Secretaría Jurídica Distrital, 2009)

Peritaje informático

Este se encarga en recoger evidencias o pruebas en asuntos judiciales o extrajudiciales, “para determinar la responsabilidad o la inculpabilidad de las personas implicadas en estas investigaciones. Los peritajes extrajudiciales son otorgados para solicitar aclaraciones de un pleito o una demanda con otras personas, o averiguar acerca de materiales antes ser llevadas a una petición”[22] (Evidencias Informáticas, 2008, s/p)

[21] Secretaría Jurídica Distrital. (2009). Ley 1273 de 2009 Nivel Nacional. 26/5/2019, de Alcaldía Mayor de Bogotá D.C. Sitio web: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[22] Evidencias Informáticas. (2008). Peritaje Informático. 15/4/2019, de Evidencias Informáticas Sitio web: https://www.evidenciasinformaticas.com/index.asp?IdContenido=3

Perito informático

Este se refiere a peritos judiciales y tiene como función principal la de orientar a los jueces con relación a las violaciones o sobornos informáticos. El propósito de éste tema radica en el estudio de las piezas o componentes informáticos, en averiguaciones de documentos para lograr u obtener algunas evidencias o pruebas que serán útiles para el pleito jurídico al que ha sido otorgado. Los peritos informáticos deben tener perfiles únicamente técnicos y es fundamental que conozcan perfectamente las técnicas de análisis y restauración de documentos, además deben poseer grandes saberes judiciales que le faciliten realizar su labor sin ser desacreditadas o rechazadas mientas estén en juicio. “Es un auxiliar de la justicia, obligado a decir siempre la verdad, el cual hará un análisis forense de una evidencia informática, para dar un dictamen profesional sobre una o varias cuestiones planteadas por el cliente”[23] (Rubio, 2018, pág. 1)

Su función es exactamente la misma del perito judicial, su misión es recolectar informaciones que esté a su alcance para analizarla en busca de datos que los jueces le han solicitado realizar y así poder emitir informes esbozando los resultados de las investigaciones obtenidas en su totalidad.

Para las organizaciones uno de sus bienes más valiosos refiere a la información digital que estas manejan; por esa razón, se han creado e implementado sistemas y herramientas idóneos para el almacenamiento de datos que se generan diariamente. El Big Data es uno de ellos, que integra además distintos métodos para mitigar riesgos informáticos y optimizar cualquier proceso.

Para (Pérez, 2014) los riesgos en almacenamiento de información que las organizaciones deben evitar, con el uso de estas nuevas tecnologías permite a las distintas empresas y organizaciones gubernamentales hacer uso adecuado de los

[23] Rubio, Javier. (2018). Perito informático. 14/9/2019, de Perito informático Sitio web: https://peritoinformaticocolegiado.es/

datos, obteniendo seguridad frente a los riesgos que existen en el almacenamiento de la información.

Donde estos riesgos pueden ser:

- **Riesgos financieros.**
- **Riesgos dinámicos.**
- **Riesgo estático.**
- **Riesgo puro.**
- **Riesgo fundamental.**

Hay que tener en cuenta que para evitarlos, es ncesario contar con unos buenos recursos tecnológicos posibles. “Al transcurrir los años los delitos informáticos han tomado fuerza, los cibercriminales a través de códigos maliciosos exponen a sus víctimas a pérdidas económicas”[24] (siete24, 2016)

Por ejemplo, en Colombia, el año 2015 representó el 15 por ciento de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares. Según una encuesta hecha a directivos y gerentes de 118 empresas entre medianas y grandes en Colombia por PricewaterhouseCoopers, un 55% de los defraudadores es trabajador de la propia compañía.

En el sentido de las responsabilidades frente al control interno de la información, se debe exigir a las empresas que los revisores fiscales sean quienes dictaminen sobre la tecnología de la información orientada a protegerla (manejo de estos temas, en términos de conocimiento y buenas prácticas).

[24] siete24. (2016). 7 métodos altamente eficaces para evitar ser víctima de delitos informáticos. 18/7/2019, de siete24 Seguridad & Tecnología Sitio web: https://blog.siete24.com/big-data-prevencion-y-mitigacion-de-riesgos-informaticos

7. TIPOS DE DELITOS INFORMATICOS ELECTRONICOS

Para identificar los delitos electrónicos que son tendencia no sólo en la región, y que afecta el manejo de la información valiosa de las empresas, encontrar los siguientes tipos de delitos informáticos empresariales:

7.1 Ransomware

Esta es una de las actividades más rentables del mundo del cibercrimen, se consolidó hace un tiempo en plataformas móviles con nuevas técnicas para bloqueo de los equipos, “es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos”[25] (Malwarebytes, 2018)

Últimamente se están utilizan en aplicaciones populares en plataformas móviles como WhatsApp o Facebook para aumentar el alcance de campañas de malware, haciendo uso de viejas técnicas de Ingeniería Social.

7.2 Estafas multiplataforma

Según el concepto de (siete24, 2016) “La Ingeniería Social, es uno de los puntos fuertes en este tipo de fraudes. Los servidores maliciosos utilizan técnicas de geolocalización para potenciar la propagación, convirtiendo a un usuario no solo en víctima, sino también en vector de difusión”[26].

7.3 Phishing

Es la capacidad de duplicar la página Web de su empresa para hacer creer a cualquier visitante que está en la página original de su organización, “es un

[25] malwarebytes. (2018). Ransomware. 12/9/2019, de malwarebytes Sitio web: https://es.malwarebytes.com/ransomware/

[26] siete24. (2016). 4 tendencias en delitos electrónicos que afectan el manejo de la información de su compañía. 1/10/2019, de siete24 Seguridad y Tecnología Sitio web: https://blog.siete24.com/tendencias-delitos-electronicos-manejo-de-la-informacion

método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y números de cuentas bancarias. Lo hacen mediante E-mail fraudulentos o dirigiéndole a un sitio web falso”[27] (avast, 2015)

7.4 Spyware

En su página web (Moes, 2018) lo define como un programa espía que de manera silenciosa se instala en su ordenador para recoger cualquier información personal u organización, sin previo conocimiento y luego dañarlo[28].

En definitiva, cada vez hay más dispositivos, más tecnologías y un mayor número de desafíos en cuanto a cómo mantener la seguridad de la información, sea cual sea el ámbito de su implementación.

El spyware tiene la particularidad de poner ventanas de manera automática que intentan vender determinados productos y servicios, basados en la información que fue recopilada por esos programas. Existen miles de programas de tipo spyware y se estima que más del 80% de las computadoras personales puedan estar infectadas.

La probabilidad de que la computadora este infectada con algún código malicioso de este tipo es grande, pero no sirve de nada entrar en pánico o desconectarse de Internet para siempre, porque existe la manera de poder detectar y eliminar un spyware existente en nuestra computadora.

---

[27] avast.. (2015). Phishing. 16/8/2019, de avast Sitio web: https://www.avast.com/es-es/c-phishing

[28] Moes, Tibor. (2018). Qué es spyware. 10/9/2019, de softwarelab Sitio web: https://softwarelab.org/es/que-es-spyware/

En Colombia el manejo de información se encuentra en un punto avanzado, comparándolo con algunos países de la región; en el país existe una política pública de Big Data (Departamento Nacional de Planeación (DNP)) que busca crear una revolución de datos y así fortalecer la generación de soluciones en el análisis de los mismos para 2017.

Algunos aspectos que se debe saber sobre el Big data:

Hace referencia a “Datos masivos”, esto consiste en recolectar grandes cantidades de información, y de esta forma almacenar, analizar, clasificar y categorizar la información para beneficio de las organizaciones con el fin de conocer el historial de cada clic, según el portal (puromarketing, 2015) “ los clientes y empleados son una fuente de información que la gran mayoría de las organizaciones no analizan con la profundidad y sistemática suficientes, sin pensar que de sus opiniones se pueden extraer una gran cantidad de conocimiento para alcanzar sus objetivos”[29]

El Big Data, es muy importante para las organizaciones ya que gracias a esto se le puede realizar un análisis de la información que contiene la organización, la cual de manera rápida y precisa se obtiene en tiempo real que está ocurriendo; también diagnostica y realiza mapas de riesgos, recopilando información para ayudar a mitigar los posibles riesgos y realizar monitorización, con el fin de permitirle reaccionar de forma inmediata.

[29] puromarketing.. (2015). big-data. 15/10/2019, de puromarketing Sitio web: https://www.puromarketing.com/12/25575/cuales-son-aspectos-clave-big-data-debe-tener-cuenta-sector-retail.html

Las "tres V" del Big Data

Volumen

La cantidad de datos importa. Con big data, tendrá que procesar grandes volúmenes de datos no estructurados de baja densidad. Puede tratarse de datos de valor desconocido, como feeds de datos de Twitter, flujos de clics de una página web o aplicación para móviles, o equipo con sensores. Para algunas organizaciones, esto puede suponer decenas de terabytes de datos. Para otras, incluso cientos de petabytes.

Velocidad

La velocidad es el ritmo al que se reciben los datos y (posiblemente) al que se utilizan. Por lo general, la mayor velocidad de los datos se transmite directamente a la memoria, en vez de escribirse en un disco. Algunos productos inteligentes habilitados para Internet funcionan en tiempo real o prácticamente en tiempo real y requieren una evaluación y actuación en tiempo real.

Variedad

La variedad hace referencia a los diversos tipos de datos disponibles. Los tipos de datos convencionales eran estructurados y podían organizarse claramente en una base de datos relacional. Con el auge del big data, los datos se presentan en nuevos tipos de datos no estructurados. Los tipos de datos no estructurados y semiestructurados, como el texto, audio o video, requieren un preprocesamiento adicional para poder obtener significado y habilitar los metadatos.[30]

[30] oracle. (2018). Las tres V de big data. 15/8/2019, de oracle Sitio web: https://www.oracle.com/co/big-data/guide/what-is-big-data.html

Otro de los aspectos que nos ofrece es el de analizar un análisis predictivo, donde se trazan estrategias de seguimiento que identifiquen patrones repetitivos, para permitir la activación de acciones preventivas y finalmente optimiza procesos, esto ocurre después del estudio del problema, se facilita la toma de decisiones útiles para el negocio, se actualizan conocimientos y se obtiene un mayor control en el desarrollo de las actividades.

Las empresas que buscan ser líderes en el sector deben buscar las mejores prácticas, talento humano capacitado y estar en constante renovación de los elementos tecnológicos que les permita ser un referente del mercado.

Las ventajas que ofrece el Big Data son:

- Disminución de fallas en software para el almacenamiento de información.
- Análisis de información en tiempo real.
- fasesón y detección de fraude.
- Menor vulnerabilidad a fenómenos naturales.
- Personalización de servicio al cliente.
- Reducción de costos.
- Toma de decisiones pertinentes sin necesidad de expertos con perfiles distintos.

Es importante que todos los empleados de una organización tengan conocimiento de las buenas prácticas para combatir los riesgos electrónicos, es importante tener presente los siguientes aspectos para prevenir este tipo de situaciones:

- Es importante tener un control sobre los dispositivos personales como USB fase ideno discos eternos.

- Se puede implementar software que permite saber si hay alguien interno, ya sea un empleado, que esté intentando filtrar información a través de plataformas como correo electrónico, o Skype.
- Renovar infraestructuras viejas y obsoletas que puedan perjudicar los procesos de producción de la organización.
- Informar a los empleados para que estén alerta ante cualquier situación extraña que se pueda presentar, tales como encendido y apagado constante del router, o la reiniciación de los aparatos de cómputo sin que se les haya dado esa orden.

El desafío está en innovar y encontrar lo mejor que ofrece el mercado para la seguridad informática y la mitigación de riesgos. Este tipo de procesos es tan importante que Colombia cuenta con la ley 1273 de 2009 "de la protección de la información y de los datos" por eso es indispensable estar al día con los nuevos mecanismos de protección que permitan optimizar la productividad y ser un referente en el mercado.

Como hemos visto anteriormente, un delito informático ó crimen cibernético, se refiere a toda actividad ilegal por medio de ordenadores o del internet cuyo objetivo es la destrucción y el daño de ordenadores, medios electrónicos y redes de computadoras.

Algunos de estos delitos son aún mayores y complejos, estos pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación, en los cuales los ordenadores redes han sido utilizado.

Desafortunadamente existe una gama de actividades delictivas realizadas por medios informáticos como:

- El ingreso ilegal a sistemas.
- La intercepción ilegal de redes.
- Interferencias de datos.
- Daños a la información (borrado, deterioro, alteración).
- Mal uso de artefactos.
- Chantajes, fraudes electrónicos.
- Ataques a sistemas.
- Violación de información confidencial.

El cambio en la selección de las víctimas, pasando del ciudadano común a las grandes empresas del sector público-privado, las cuales generan una mayor rentabilidad a la actividad criminal.

7.5 Caracterización del cibercrimen

Durante los últimos 3 años a través de las plataformas dispuestas por Centro Cibernético Policial se recibieron 15.565[31] incidentes informáticos. A partir del análisis de información, se identificaron aspectos comunes que permiten caracterizar el delito informático en Colombia, así:

En el **2014**, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el **2015** el 63% y en el **2016** el 57%, presentando una disminución del 35%. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos[32].

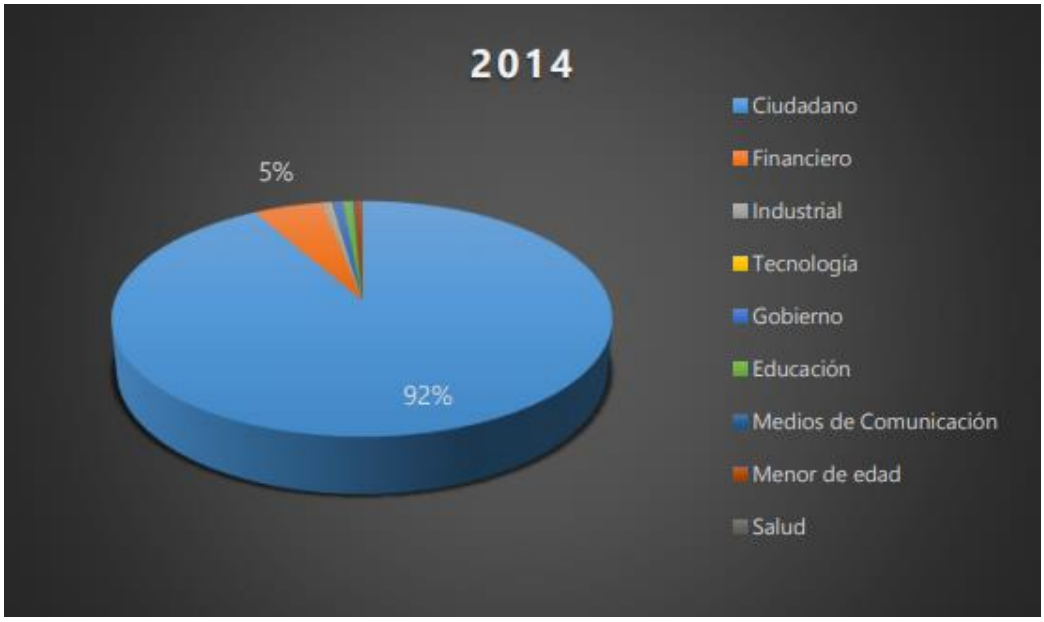
---

[31] Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017

[32] Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017

Estas cifras ratifican lo planteado en el documento IOCTA 201610[33] (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency de EUROPOL[34], referente a la Tricotomía del delito, en donde se estipula que, a mayor volumen de ataque, con mayor número de víctimas, donde su nivel de seguridad y protección es bajo, el beneficio por ataque es menor. Pero si, por el contrario, el ataque se realiza a un sector reducido o especializado, por ejemplo, el sector financiero, con un ataque más sofisticado, que requiera de mayor habilidad y destreza, con niveles de innovación alto, el beneficio por ataque será mucho mayor.

Figura 4. Tendencia de delitos informáticos 2014.



[33] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[34] EUROPOL, 28 Estados miembros de la Unión Europea en su lucha contra la gran delincuencia internacional y el terrorismo. De igual forma con numerosos estados asociados no pertenecientes a la UE y organizaciones internacionales

Figura 5. Tendencia de delitos informático 2015.

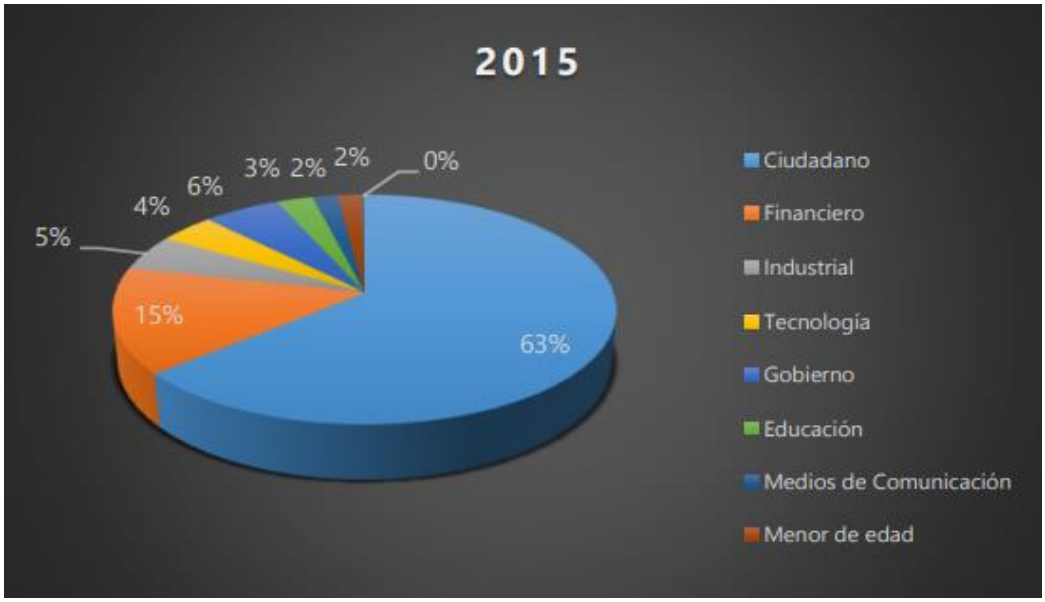


Figura 6. Tendencia de delitos informático 2016.

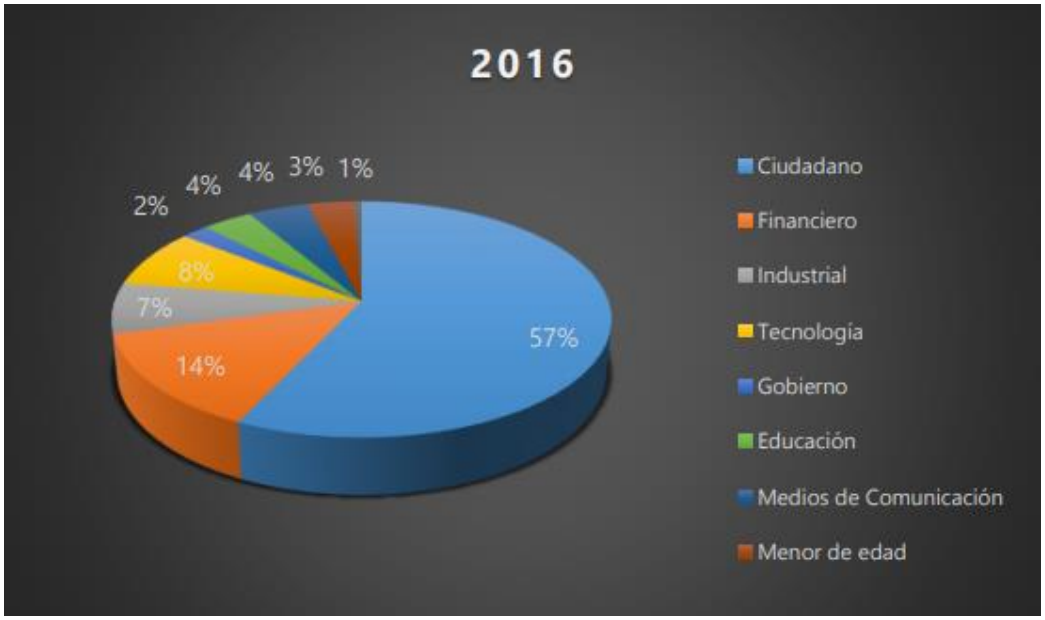
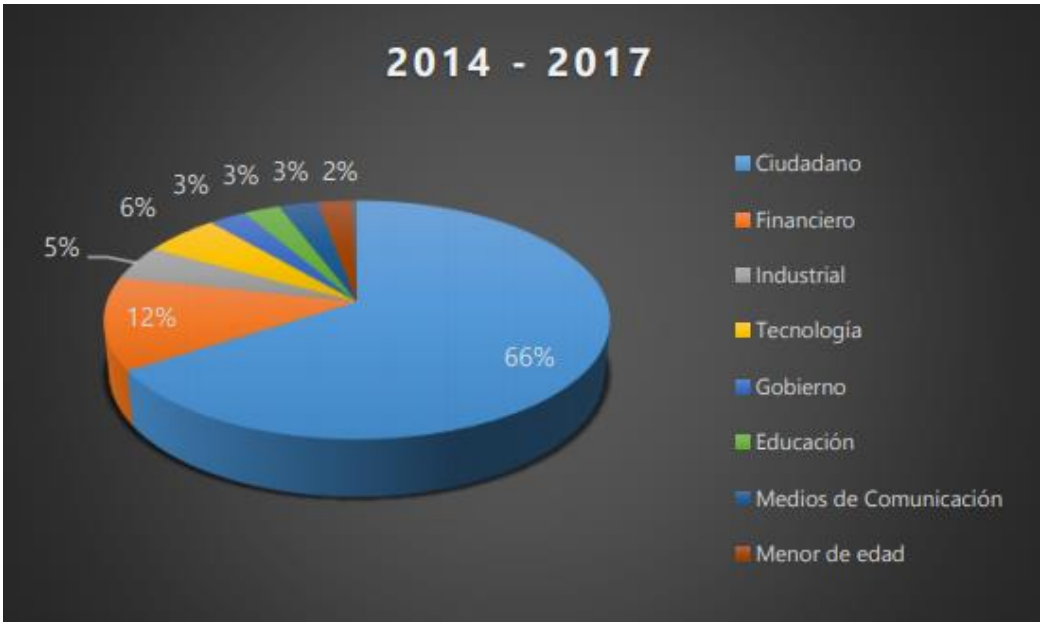


Figura 7. Tendencia de delitos informático 2017.



A la hora de detallar el delito informático, hay que adjudicarse 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.

Es por ello que este tipo de técnicas va en aumento en los últimos años, y normalmente se encuentra relacionada a casos de estudio en donde ocurrió un delito financiero, evasión de impuestos, investigación sobre seguros, acoso o pedofilia, robo de propiedad intelectual, fuga de información y ciberterrorismo o ciberdefensa, entre muchos otros campos.

Estas técnicas están usualmente divididas en 5 fases que nos ayudan a mantener un estudio estructurado, facilitando la verificabilidad, la reproducibilidad del análisis.

8. Etapas

8.1 Adquisición

En esta fase se obtienen copias de la información que se sospecha y que además puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados.

Rotulando con fecha y hora acompañado del uso horario, las muestras deberán ser aisladas en recipientes que no permitan el deterioro ni el contacto con el medio. En muchos casos, esta etapa es complementada con el uso de fotografías con el objetivo de plasmar el estado de los equipos y sus componentes electrónicos.

Es muy recomendable usar guantes, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas como son los celulares.

La recolección de muestras debe respetar una regla fundamental que está ligada a la volatilidad de las muestras, por lo que se deberán recolectar en el orden de la más volátil en primera instancia a la menor, sobre el final.

8.2 Preservación

Al llegar a esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir, no debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia.

De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra.

8.3 Análisis

Una vez obtenida la información y preservada, esta es llevada a la parte más compleja. Sin duda, es la fase más técnica, donde se utilizan tanto ***hardware*** como ***software*** específicamente diseñados para el análisis forense. Si bien existen métricas y metodologías que ayudan a estructurar el trabajo de campo, se podrán obtener grandes diferencias dependiendo de las herramientas que se utilicen, las capacidades y experiencia del analista.

Además, es muy importante tener en claro qué es lo que estamos buscando, debido a que esto dará un enfoque más preciso a la hora de ir a buscar pruebas. Sin embargo, el estudio de la línea de tiempo (timeline), logs de accesos y una descarga de la memora RAM será muy útil para la mayoría de las pericias.

8.4 Documentación

Esta es una de las etapas finales, donde se recomienda ir documentando todas las acciones, en lo posible, a medida que vayan ocurriendo. Aquí ya deberíamos tener claro por nuestro análisis qué fue lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa. Debemos citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación.

8.5 Presentación

Normalmente se suelen usar varios modelos para la presentación de esta documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos

más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos. Este informe debe ser muy claro, certero y conciso, dejando afuera cualquier cuestión que genere algún tipo de duda.

Un segundo informe llamado “Informe Técnico” es una exposición que nos detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales[35]. (Arnedo, 2014)

En Colombia podemos referirnos a Henry William Torres Torres, ya que amplía el concepto a lo internacional definiendo al delito informático como: “toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software al que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como infracción informática[36]. (Ojeda, Rincón, Arias, & Daza, 2010)

La cadena de custodia es un procedimiento que debe tenerse en cuenta un principio, ya que esto conlleva a realizar el proceso de evidencia forense, debido a que este procedimiento, basado en el principio de la “mismidad”, tiene como fin garantizar la autenticidad e integridad de las evidencias encontradas en alguna situación determinada, es decir, que lo mismo que se encontró en la escena, es lo mismo que se está presentando al tribunal penal o comité disciplinario según sea el caso.

---

[35] Arnedo, Pedro. (2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. 18/8/2019, de Universidad Internacional de la Rioja Sitio web: https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

[36] Ojeda Pérez, J., Rincón Rodríguez, F., Arias Flórez, M., & Daza Martínez, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia, 11 (28). Obtenido de https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

La información mínima que se maneja en una cadena de custodia, para cualquier caso, es la siguiente:

- ✓ Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega.
- ✓ Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta.
- ✓ Rótulos o etiquetas que van pegados a los empaques de las evidencias, por ejemplo, a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.
- ✓ Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.

Esta trazabilidad, brindará la confianza suficiente a quienes reciban las evidencias para certificar que toda la información ha conservado su integridad, que no ha sido alterada o modificada.

9. FASES

9.1 FASE I. Aislamiento de la escena

Una vez el evento reportado se cataloga como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia que pueda recolectarse para la posterior investigación.

"En el mejor de los casos, lo mejor sería que alguna autoridad competente (como el CCP o el COLCERT) realizara el aislamiento de la escena, pero dado que estos procedimientos deben ejecutarse a la mayor brevedad posible"[37] (mintic, 2016)

9.2 FASE II. Identificación de fuentes de información, pasos iniciales de adquisición de información

Lo primero que hay que realizar para accionar la recolección de datos, es identificar fuentes potenciales de información de donde se puedan extraer datos para soportar el proceso de evidencia digital.

9.2.1 Identificación de posibles fuentes de datos

Las fuentes más comunes para encontrar información son las siguientes:

- Computadoras de escritorio y portátiles
- Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP o cualquier servicio de filesharing).
- Almacenamiento en red.
- Medios tanto internos como externos que contemplan: Dispositivos USB, Firewire, CD/DVD, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD etc.

[37] mintic. (2016). Seguridad y privacidad de la información. 17/8/2019, de mintic Sitio web: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

- Dispositivos celulares, PDAs, Camaras Digitales, Gradaboras de video y audio.

9.2.2 Adquisición de datos

La adquisición de los datos debe realizarse teniendo en cuenta 3 pasos principales:

Planificación de la adquisición de datos: Se debe planificar bien a que fuentes de información se les extraerá la información y el orden en el que se debe hacer, teniendo en cuenta aspectos como, volatilidad de la información, complejidad para obtener los datos o por experiencia propia del analista.

Adquisición de los datos: El proceso general de recolección generalmente requiere del uso de herramientas forenses para copiar los datos volátiles y poderlos almacenar, así como también para adquirir la información de fuentes no volátiles. El proceso de recolección puede variar si es posible acceder localmente al sistema o si se puede hacer a través de la red.

Verificación de la integridad de los datos recolectados: Una vez se recolectan los datos, se debe asegurar que la información mantiene su integridad y no ha sido modifica. Esto se puede realizar empleando herramientas de cálculo de resumen de mensajes que generan un valor determinado. Dicho valor debe ser igual tanto en la fuente original como en la copia. Esta verificación de integridad se utiliza principalmente para efectos legales, para que la información se certifique como auténtica.

Es importante tener en cuenta que, si la información va a utilizarse para fines legales, desde el inicio debe tenerse total cuidado con la manipulación, llevando a cabo la cadena de custodia adecuadamente, registrando cada acción, desde que

se recolecta, se almacena, se guarda, quien lo hace y la hora exacta, que herramientas se han utilizado para la recolección etc[38].

9.3 FASE III. Recolección y examinación de información

Una vez se han identificado las posibles fuentes de información, se debe proceder a realizar la recolección y examinación de los datos disponibles.
La secuencia para llevar a cabo la recolección y examinación de medios/información es la siguiente:

9.3.1 Creación del archivo / bitácora de hallazgos (cadena de custodia).

Esta consiste en la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado.

9.3.2 Imagen de datos

Consiste en la generación de las imágenes de datos que conciernen al caso en investigación. Se recomienda utilizar herramientas de extracción de imágenes como Linux dd o Encase Forensic Software.

9.3.3 Verificación de integridad de la imagen

Para cada imagen suministrada se debe calcular su compendio criptográfico (SHA1/MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.

---

[38] mintic. (2016). Seguridad y privacidad de la información. 17/8/2019, de mintic Sitio web: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

9.3.4 Creación de una copia de la imagen suministrada

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada. Debe realizarse una copia master y a partir de esta, se reproducen las imágenes que se requieran.

9.3.5 Aseguramiento de la imagen original suministrada

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

9.3.6 Revisión de antivirus y verificación de la integridad copia de la imagen

Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido.
Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original. De hecho, esta actividad es de tipo transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

9.3.7 Identificación de las particiones actuales y anteriores

La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

9.3.8 Detección de información en los espacios entre las particiones

Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables.

9.3.9 Detección de un hpa (host protected area)

Este paso debe realizarse solo si en los Meta-datos se indica la existencia del HPA ya que de otro modo es imposible de identificar. En el caso en que exista, se debe seguir el mismo procedimiento del paso anterior.

9.3.10 Identificación del sistema de archivos

Para cada una de las particiones identificadas, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar las actividades posteriores del análisis de datos.

9.3.11 Recuperación de los archivos borrados

Durante esta actividad se deben tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente dado el frecuente borrado de archivos para destruir evidencia.

Dependiendo de las características técnicas y del estado del sistema de archivos puede no ser posible la recuperación de la totalidad de los archivos eliminados, por ejemplo, si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

9.3.12 Recuperación de información escondida

En esta etapa se debe examinar exhaustivamente el slack space, los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Los archivos protegidos también se tendrán en cuenta durante la fase de análisis de este tipo de archivos.[39]

9.3.13 Identificación de archivos existentes

Seguidamente, se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte la fase de análisis de archivos protegidos.

9.3.14 Identificación de archivos protegidos

Esta es la fase de consolidación de archivos protegidos identificados en las fases anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formarán parte del conjunto de archivos sospechosos.

---

[39] ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements

9.3.15 Consolidación de archivos potencialmente analizables

Durante esta fase se reúnen todos los archivos encontrados durante las fases de recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.

9.3.16 Determinación del sistema operativo y las aplicaciones instaladas

Al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de los estos archivos de encontrarse en la imagen sometida a análisis.[40]

9.3.17 Identificación de información de tráfico de red

A parte de los sistemas de información, es convencional realizar una verificación minuciosa de la información registrada por los dispositivos de red, ya que puede ayudar a reconstruir y analizar ataques basados en red o a rastrear algún tipo de acceso o movimientos específicos que puedan estar relacionados con el incidente reportado (Ataques DoS, DDoS, mal uso de los recursos de la organización, comportamientos anómalos).

La principal fuente de información a consultar (de estar disponible), es un sistema tipo SIEM, que tiene la capacidad de almacenar logs de distintos dispositivos de red y relacionarlos por el tiempo en que son generados. Esto permite ver la trazabilidad de un paquete desde que ingresa, hasta que abandona la red.

Cuando se identifica algún evento de interés (en una hora exacta), el análisis puede llegar a consistir en solo acceder a verificar logs en los tiempos

[40] NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response.

aproximados o puede llegar a ser más profundo y verificar varias fuentes de información adicionales, llegando a incluir a los proveedores de servicio de internet. Estos análisis se pueden llevar a cabo empleando software tipo NFAT (Network Forensic Analysis Tool) que puede ayudar a correlacionar dirección IP, direcciones MAC y realizar sus búsquedas en las fuentes de información disponibles.

Otras fuentes de información relevantes son servidores DHCP, Aplicaciones Cliente Servidor (Por ejemplo, Correo Electrónico), Logs Del Proveedor De Servicios, Plataformas De Acceso Remoto (VPN).
Es importante que todas estas plataformas tecnológicas se encuentren previamente sincronizadas a través de NTP.

9.3.18 Depuración de archivos buenos conocidos

El objetivo de este paso es descartar información que no será relevante para analizar. Con la lista de compendios criptográficos obtenida, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, estos archivos se consideran “buenos” y por lo tanto son descartados del proceso de análisis en la fase posterior.

9.3.19 Consolidación de archivos sospechosos

Como resultado del filtrado de “buenos conocidos”, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.[41]

[41] mintic. (2016). Seguridad y privacidad de la información. 17/8/2019, de mintic Sitio web: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

9.4 Clasificación de los archivos

9.4.1 Primera clasificación de archivos

Divide los archivos sospechosos en:

9.4.1.1 Archivos "Buenos" Modificados: Son identificados en la fase de filtrado como archivos buenos cuya versión original ha sido modificada.

9.4.1.2 Archivos "Malos": Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos "malos" relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: sniffers, troyanos, backdoors, virus, keyloggers entre otros.

9.4.1.3 Archivos Con Extensión Modificada: Aquellos cuya extensión no es consistente con su contenido (para ello siempre es necesario verificar los encabezados de los archivos y no su extensión).[42]

9.4.2 Segunda clasificación de archivos

Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial.

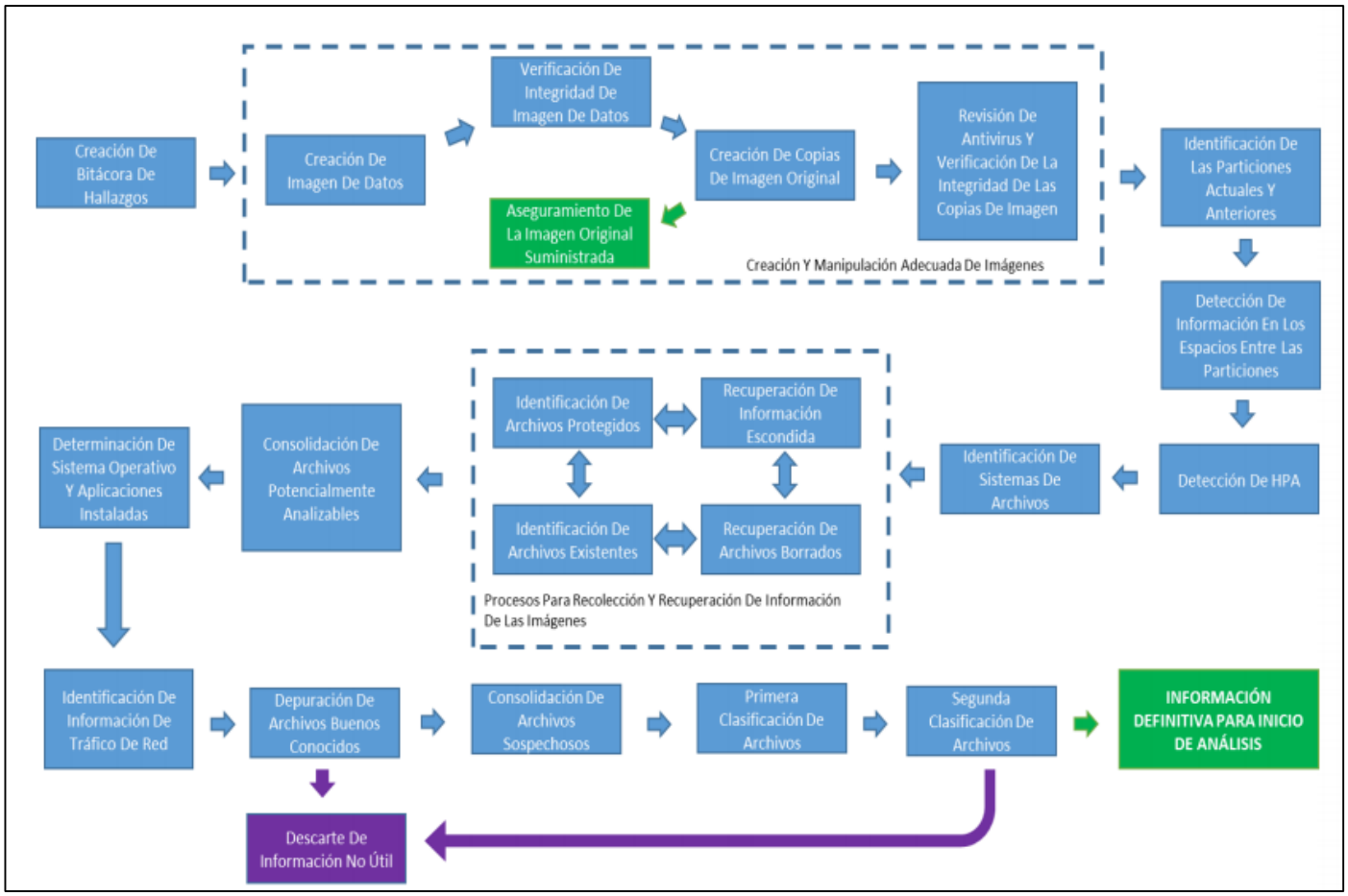
De esta manera, se busca obtener información complementaria útil para la fase de análisis.

---

[42] mintic. (2016). Seguridad y privacidad de la información. 17/8/2019, de mintic Sitio web: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

A continuación, se muestra un diagrama que ilustra un posible orden lógico para la ejecución del procedimiento de examinación y recolección de información:

Figura 8. Diagrama de examinación y recolección de información.



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

9.5 Recomendaciones para examinación y recolección de información

- ✓ El analista forense deberá trabajar junto con el equipo de incidentes, para decidir la manera adecuada de contener el incidente permitiendo a su vez recolectar la mayor cantidad de información posible (siempre y cuando sea posible).
- ✓ En ocasiones el sistema afectado debe aislarse del entorno para disminuir el impacto del incidente o para preservar la evidencia (de hecho, es el método más común).
- ✓ Debe evaluarse el impacto o la consecuencia de sacar un sistema de línea por mucho tiempo para poder generar las imágenes y/o copias de disco para la investigación, se debe evitar la mayor pérdida posible.
- ✓ Para realizar las manipulaciones de los sistemas, es pertinente que se tengan a la mano herramientas de tipo forense (software y hardware como una estación forense), que asegurará la integridad de la información a la hora de ser recolectada y verificada por primera vez.
- ✓ Siempre se deberán realizar los análisis en copias de la información, nunca deberá hacerse en la información original (la cuál debe ser almacenada de manera segura para evitar que sea alterada).
- ✓ Es importante para los analistas forenses poder recibir u obtener toda la información recolectada con las estampas de tiempo precisas, es decir, que todas las plataformas de información se encuentren sincronizadas con un mismo reloj o servicio NTP. Esto garantizará mayor precisión en los estudios posteriores.
- ✓ Es importante decidir hasta qué punto la organización se encontrará en capacidad de realizar la recolección y/o análisis de la evidencia que se presentará en las siguientes fases, es por ello que dependiendo el caso deberá contactarse al COLCERT o CCP para recibir instrucciones o colaboración en la realización de estos procedimientos.

10. FASE IV. Análisis de la información

En esta fase se realizará un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada (después de realizar la depuración en las fases anteriores).
Dicho análisis puede involucrar y relacionar los eventos, archivos, logs, testimonios, fotografías, videos de vigilancia etc… para así llegar a alguna conclusión determinada.[43]

Dentro del análisis de la información se involucran las siguientes etapas:

10.1 Análisis de la información prioritaria

Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador[44].
Es importante resaltar que los procesos de la segunda clasificación y análisis, pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente.

En cada iteración cada archivo de alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.
Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o porque se agotan los datos por analizar.

10.2 Generación de listado de archivos comprometidos con el caso

Es el conjunto de archivos que forman parte de la evidencia del caso, este criterio es definido por el investigador, quien indicará lo que finalmente se empleará como

---

[43] NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response
[44] ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management

evidencia a presentar en el informe final o en el proceso judicial según sea requerido.

10.3 Obtención de la línea de tiempo de la evidencia

Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia. Se debe tener en cuenta que muchos los sistemas pueden manejan varias estampas de tiempo para sus archivos.[45]

Las estampas de tiempo más comunes son:

- **Fecha De Modificación:** Indica la última vez que el archive fue modificado de cualquier manera, así sea a través de otro programa.
- **Fecha De Acceso:** Es la última vez que el archivo fue accedido (abierto, impreso o visto).
- **Fecha De Creación:** Es la fecha en la que el archivo fue creado por primera vez en un sistema, sin embargo, cuando un archivo es copiado hacia otro sistema, la fecha de creación se renovará para dicho sistema, sin embargo, la fecha de modificación si permanecerá intacta.

Estas estampas de tiempo pueden llegar a ser fundamentales para el proceso de análisis del incidente de seguridad de la información que se encuentra activo o recientemente contenido, por ello, se recalca de la importancia de la sincronización de todos los sistemas de información (incluyendo PC, Laptops) a través de NTP.

En algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que, como todos los hallazgos, debe ser consignada en el informe final.

---

[45] Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, Organización De Estados Americanos

10.4 Generación de informe final

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación metodológica.[46]

11. FASE V. Reporte

La fase final del procedimiento de evidencia digital es el reporte, el cuál presenta toda la información y la evidencia obtenida en la fase de análisis. Este reporte debería contemplar los siguientes aspectos:

- Resultado de los análisis.
- Cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información, eso sustentará el trabajo realizado.
- Se debe tener en cuenta la audiencia a la cual se presentará el informe, dado que, si debe presentarse a nivel gerencial, el contenido técnico no debe tener la misma densidad que para un grupo de ingeniería, ya que en este punto es probable que se deba indicar exactamente ¿Qué ocurrió?, ¿En qué plataforma?, ¿Qué tipo de ataque fue realizado?, sus consecuencias y las posibles contramedidas para evitar que ocurra nuevamente.
- Acciones a tomar (si es para remediar algún incidente o crimen), como por ejemplo mejorar determinados controles de seguridad, reducir alguna vulnerabilidad encontrada, refuerzo en el entrenamiento del personal (sea usuario final o equipo de respuesta a incidentes), todo esto depende de contexto del incidente.

---

[46] ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements

- Determinar si es necesario realizar más estudios para llegar a una conclusión definitiva o si únicamente es posible llegar a explicaciones alternativas o hipótesis, estas deben ir plasmadas en el documento con su justificación respectiva.
- Recomendaciones relacionadas a mejoramiento en las políticas, procedimientos, herramientas de detección y otras observaciones para mejorar el proceso forense.

11.1 Recomendaciones generales

- La Cadena De Custodia, es esencial para el desarrollo de un buen procedimiento de evidencia digital, ya que brinda la confiabilidad de que la información ha sido manipulada apropiadamente asegurando su integridad.
- Recurrir a las entidades públicas COLCERT y CCP para la gestión de incidentes de seguridad de la información, según el tipo de incidente que se presente (En la Guía # 25 “Gestión De Incidentes De Seguridad De La Información”), se dan indicaciones sobre este tema.
- Las entidades deberán evaluar hasta que fase del procedimiento de evidencia digital pueden o desean llegar, pero siempre pueden recurrir a las instituciones mencionadas previamente.
- Los sistemas operativos pueden configurarse para auditar y almacenar ciertos tipos de eventos, como intentos de autenticación, cambios en las políticas de seguridad entre otra información útil.
- Los sistemas tipo SIEM con NTP configurado correctamente, son unas de las herramientas más poderosas de trazabilidad y de detección de incidentes o comportamiento anómalos. Es importante disponer de un sistema con estas características, de lo contrario, una gestión de logs de los dispositivos, puede ser de gran utilidad, debe invertirse en sistemas que permitan retener cantidades considerables de dichos logs.

- Siempre debe trabajarse con copias de la información original y a cada una de las copias deberá verificarse su integridad para certificar que sean copias válidas de la información base.
- Disponer de un kit forense (software, herramientas, estación forense) para realizar la obtención de la información necesaria en los sistemas, con el fin de asegurar la preservación de la integridad de la información a analizar y que pueda ser presentada como evidencia.
- Debe existir un grado de entrenamiento suficiente en las áreas de gestión de incidentes para poder realizar los procedimientos de evidencia forense, así como también deben poseer conocimientos sobre protocolos de red, aplicaciones, amenazas basadas en red y métodos de ataque.
- Siempre debe primar el restablecimiento del servicio y la contención del impacto del incidente que el encontrar el responsable de los mismos (es decir realizar la toma de evidencia forense).[47]

12. Delitos Informáticos a nivel global

En la siguiente tabla se mostrarán y nombraran algunos de los delitos informáticos que están causando problemas a nivel global y en algunos el tiempo que tendrían que pagar los involucrados por ese delito:

[47] ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management

Tabla 1. Delitos informáticos a nivel global.

Delitos Informáticos a Nivel Mundial			
N°	Delito	Descripción	Pena
1	**Sabotaje Informático**	Dañar o destruir o modificar información de carácter electrónico (virus, gusanos, bombas lógicas, bombas cronológicas). Según los datos de la fiscalía, estos delitos alcanzaron la cifra de 143 casos registrados. No obstante, otras fuentes apuntan que podrían haberse dado muchos más casos.	
2	**Suplantación de Identidad**	También llamado delito de usurpación de estado civil o de identidad consiste en la acción apropiarse una persona de la identidad de otra, haciéndose pasar por ella para acceder a recursos y beneficios, actuando en el tráfico jurídico simulando ser la persona suplantada. Con este delito se trata de proteger la fe pública de la comunidad o la confianza en la identificación de las personas. Por ello la jurisprudencia entiende que no es suficiente suplantar una identidad ficticia. Para poder cometer este delito el autor tiene que usurpar la identidad de una persona real, resultando impune la acción en el caso de que el culpable decidiera inventarse un personaje ficticio y hacerse pasar por él –suplantación de identidad-. Pensemos por ejemplo en quien faltando a la verdad se inventa un perfil ficticio crea un personaje y se hace pasar por él: la acción no tendría ninguna relevancia penal y resultaría impune.	6 meses a 3 años de prisión
3	**Piratería**	Creación y distribución de copias de productos originales, sean libros, películas, canciones y entre otras.	

Tabla 2. Continuación de Delitos informáticos a nivel global.

4	**Pornografía Infantil**	Actos con menores de edad, creación de videos haciendo actos sexuales. La Interpol, el FBI y autoridades en países latinoamericanos, especialmente en Argentina, Colombia, Brasil, Chile y Venezuela, realizan más esfuerzos para controlar el problema. Más de 280.000 casos al año de utilización de niños para pornografía en Internet, prostitución infantil, abuso sexual, venta de niños, práctica difundida y continuada del turismo sexual, se reportan solamente en Estados Unidos, pero el número de casos no reportados es aún mayor si se tiene en cuenta el número de niñas y niños latinoamericanos utilizados para este aberrante delito.	
5	**Interceptación ilícita de datos informáticos**	Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses de vigencia
6	**Violación de datos personales**	Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.
7	**Daños Informáticos**	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.
8	**Falsificación o Phising**	Phishing es un ciberdelito por el que los ciberdelincuentes intentan conocer los datos confidenciales de cualquier usuario de internet, principalmente datos de acceso a diferentes servicios, así como números de tarjetas de crédito o cuentas bancarias con el objetivo principal de robar dinero o conseguir datos bancarios con los que efectuar un fraude, es decir, compras a nuestro nombre. Su modus operandi es mediante el envío de un correo electrónico que nos reconduce a sitios web falsos construidos a imagen y semejanza de los auténticos. Por ello resulta tan importante no pulsar enlaces de correo que no conocemos, ni de ofertas increíbles.	

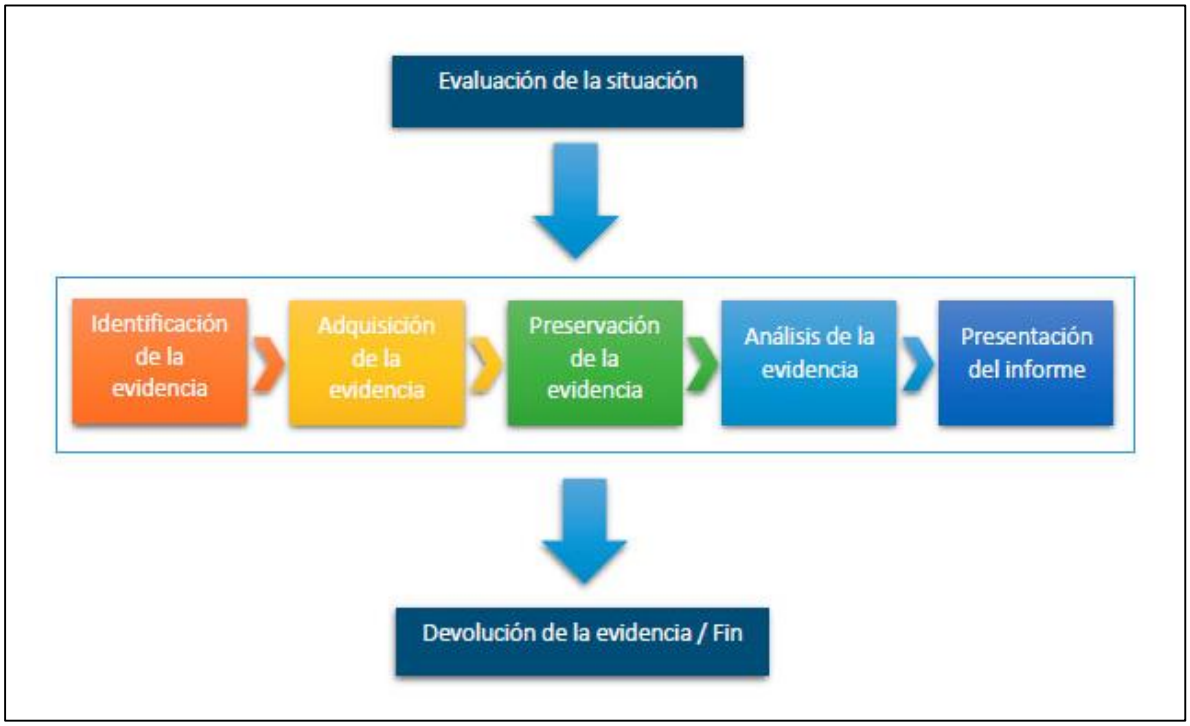
Tabla 3. Continuación de Delitos informáticos a nivel global.

9	**Spam**	El spam o correo basura se envía también junto con un enlace web o propuesta de negocio. Al hacer clic en este enlace o en respuesta a la propuesta de negocios, podemos ser objeto de phishing o instalar un malware en nuestro ordenador que proporcione nuestros datos personales, bancarios, etcétera a los ciberdelincuentes. Una variedad de spam es el bombardeo de correo electrónico consistente en enviar grandes cantidades de correos electrónicos a la dirección de destino lo que provoca la caída de la dirección de correo electrónico o del servidor de correo.	
10	**Acceso Abusivo a un sistema informático**	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.

13. Metodología del análisis forense

Aunque no existe una metodología que sea única y universal en el análisis forense, a tenor de la documentación consultada y tomando en consideración la normativa legal y los estándares vigentes a nivel internacional, sí que se puede decir que existen una serie de fases o puntos importantes que se tienen que tomar en consideración para que el análisis forense sea adecuado y sirva como elemento probatorio ante un incidente.[48]

Figura 9. Metodología de Análisis Forense

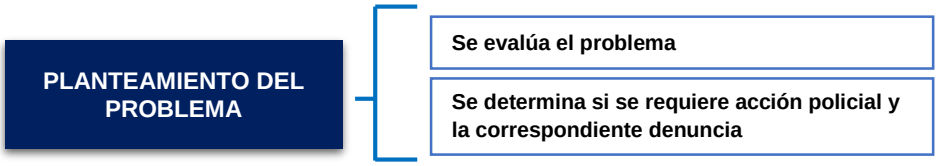


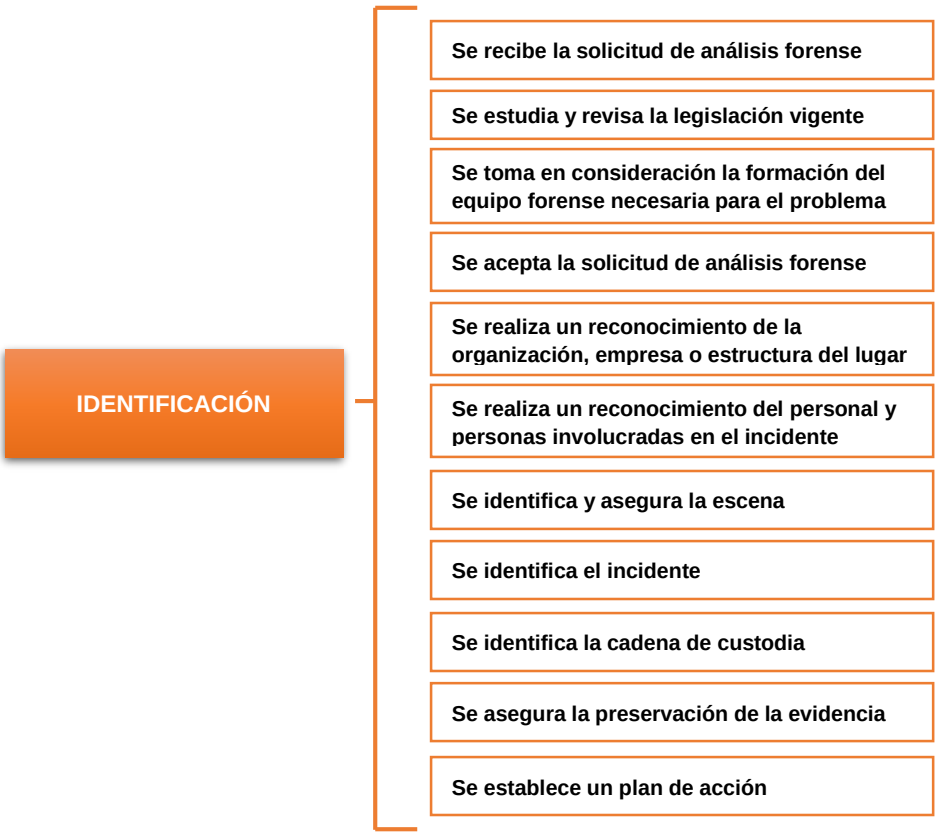
Fuente: https://ninjasdelaweb.com/metodologia-de-analisis-forense/

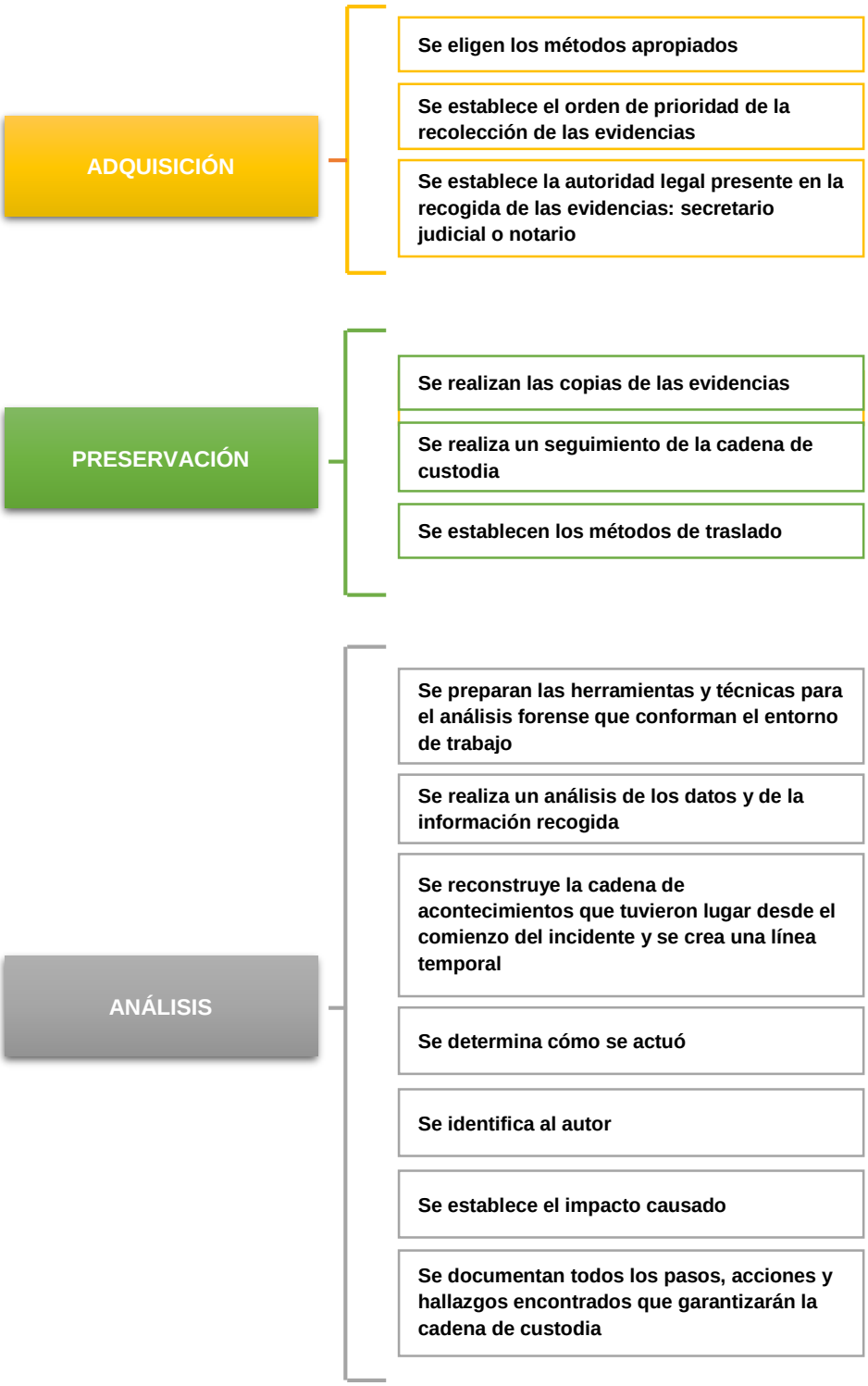
[48] García, M. A. (2014). Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informática. Obtenido de edu.ec: http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf

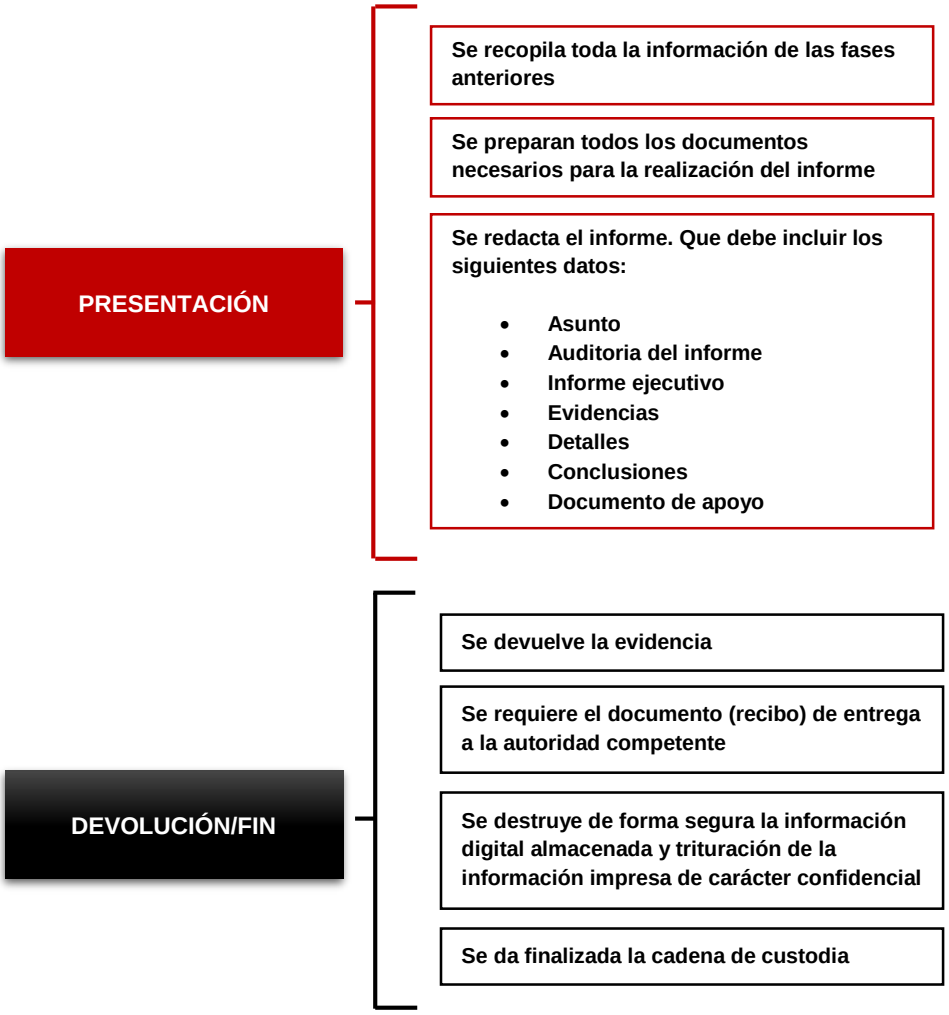
En sí, el objetivo de todas las fases es analizar, recopilar las pruebas y determinar quiénes han sido los autores que han originado el incidente, las personas o elementos involucrados, al igual que el impacto que ha podido suponer la realización del mismo. Pero siempre intentando salvaguardar de la mayor manera posible tanto la objetividad y la profesionalidad de los forenses implicados como de la integridad y la cadena de custodia de las pruebas o elementos analizados.

A continuación, se expondrá un pequeño resumen de la metodología forense actual.






ADQUISICIÓN
Se eligen los métodos apropiados
Se establece el orden de prioridad de la recolección de las evidencias
Se establece la autoridad legal presente en la recogida de las evidencias: secretario judicial o notario
PRESERVACIÓN
Se realizan las copias de las evidencias
Se realiza un seguimiento de la cadena de custodia
Se establecen los métodos de traslado
ANÁLISIS
Se preparan las herramientas y técnicas para el análisis forense que conforman el entorno de trabajo
Se realiza un análisis de los datos y de la información recogida
Se reconstruye la cadena de acontecimientos que tuvieron lugar desde el comienzo del incidente y se crea una línea temporal
Se determina cómo se actuó
Se identifica al autor
Se establece el impacto causado
Se documentan todos los pasos, acciones y hallazgos encontrados que garantizarán la cadena de custodia



Fuente: https://ninjasdelaweb.com/metodologia-de-analisis-forense/

13.1 Tipo De Investigación

“La metodología para el desarrollo del este trabajo de grado, se basara en los planteamientos definidos en materia de la seguridad de la información y hacer uso

de la informática forense aplicada a delitos informáticos en la industria colombiana”[49].

Principalmente se busca para tales fines el sistema de seguridad apropiado para las empresas en el sector empresarial debido a las malas prácticas que a veces por falta de conocimiento o capacitaciones del personal, estos son los más vulnerados en el mundo informático.

13.2 Técnicas e Instrumentos de recolección de información

Para la realización de este trabajo, se utilizara todas las fuentes bibliográficas posibles (En todos los idiomas posibles, para tener una mejor investigación), relacionadas con los conceptos de seguridad de la información y de la informática forense, esto con el fin de establecer antecedentes y/o tener unas buenas bases en la investigación y así dar un buen desarrollo al trabajo propuesto.

Las técnicas que se utilizaran en la recolección de información elegida para el desarrollo son los antecedentes que se tienen referentes a la informática forense en las empresas.

[49] Pinto, D. (2014). Metodología de análisis forense orientada a incidentes en dispositivos. Obtenido de dspace.ucuenca.edu.ec: http://dspace.ucuenca.edu.ec/bitstream/123456789/21381/1/TIC.EC_04_Pinto.pdf

14. CONCLUSIONES

- Colombia, en pleno desarrollo pero con un avance tecnológico importante en la última década se enfrenta a cambiar y a acostumbrarse a situaciones las cuales antes no ha manejado como lo son la judicialización en términos tecnológicos y es algo que le ha causado al país algo de traumatismo pero está en el proceso , cosa que no muchos países vecinos no han hecho, pero cabe resaltar que hay un desconocimiento masivo tanto por las personas naturales , como para las compañías y esto es aún más grave porque las compañías no se preparan y no están bien informadas de cómo opera la ley como se pueden proteger , y como mitigar el riesgo que una situación la cual amanece la seguridad de la información sea controlado y mejor aún prevenida.

- A través de la informática forense, que es considerada como una ciencia, se pueden ejecutar diferentes investigaciones relacionadas con cualquier crimen o delito informático dentro de una empresa y adquirir las pruebas o evidencias indispensables y válidas ante un juzgado, puesto que éstas facilitaran el juzgamiento de los sujetos autores del delito o implicados en éste.

- 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 en las organizaciones, además de prestar asesoría y apoyo al momento de realizar investigaciones para generar soluciones prontas y eficientes según sea la circunstancia.

- La Constitución Política de Colombia en su artículo 15 permite fundamentar el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia, donde se establece el derecho a la intimidad, por lo que se deben respetar la libertad y promover las demás garantías consagradas en la Constitución, apoyado en la Ley 527 de Agosto 18

de 1999 que trata de los instrumentos magnéticos e informáticos, así como la ley 527 de 1999 sobre el comercio electrónico para Colombia, la Ley 1273 de 2009 para la protección de la información y de los datos y la Ley 1273 del 2009 que tipifica los delitos informáticos con el fin de penalizar a los infractores.

15. RESULTADOS

Los resultados logrados mediante el desarrollo del presente trabajo de grado, cumple básicamente en documentar y concientizar a las personas, a las empresas sin importar su régimen económico y a los administradores de tecnología acerca de la importancia que tiene la implementación de cualquier metodología de seguridad en las organizaciones, siempre cumpliendo con unas normas establecidas por la constitución colombiana.

16. BIBLIOGRAFIAS

Arnedo, P. (11 de 3 de 2014). *Universidad Internacional de la Rioja.* Recuperado el 19 de 9 de 2019, de https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

avast. (2015). *phishing.* Recuperado el 16 de 8 de 2019, de https://www.avast.com/es-es/c-phishing

Callegari, N. (2015). *pensamientopenal*. Recuperado el 12 de 10 de 2019, de http://www.pensamientopenal.com.ar/system/files/2016/08/doctrina44051.pdf

Ciardhuáin, S. Ó. (2004). *An Extended Model of Cybercrime Investigations.* (I. J. 2004, Ed.) Recuperado el 10 de 9 de 2019, de https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-

Daccach, J. (2017). *Delta Aesores*. Recuperado el 15 de 9 de 2019, de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Estrada, M. (2008). *https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf.* Recuperado el 7 de Abril de 2019

EUROLATINOAMERICA. (2017). *Informática Forense Colombia*. Recuperado el 05 de 10 de 2019, de https://www.informaticaforense.com.co/informatica-forense/

eyasno. (03 de 06 de 2014). *elforense*. Obtenido de https://elforense.wordpress.com/2014/06/03/estudio-de-caso-forense-1/

Ferri. (s.f.). *Monografias*. Obtenido de Definiciones de delito: http://www.todoiure.com.ar/monografias/mono/penal/Definiciones_de_delito.htm.

Forencis, D. (2019). *delitosinformaticos*. Obtenido de https://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

Galán, A. (2019). *Los delitos informáticos en nuestro Código Penal*. Obtenido de https://iurisnow.com/es/delitos-informaticos/

Gallegos, A. (2013). *Importancia de la informática forense.* Obtenido de https://www.academia.edu/23975452/Informatica_forense

Hall, A. (2018). *forodeseguridad*. Recuperado el 13 de 10 de 2019, de http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Informáticas, E. (2008). *Peritaje Informático.* Recuperado el 15 de 4 de 2019, de https://www.evidenciasinformaticas.com/index.asp?IdContenido=3

INFOSEGUR. (10 de 11 de 2013). *Seguridad Informática*. Recuperado el 5 de 10 de 2019, de https://infosegur.wordpress.com/tag/integridad/

Justice, U. D. (2007). *Handbook of Forensic Services.* Recuperado el 14 de 5 de 2019, de https://www.fbi.gov/file-repository/handbook-of-forensic-services-pdf.pdf/view

Lee, H. C., Palmbach, T. M., & Miller, M. T. (6 de 6 de 2001). *Henry Lee's Crime Scene Handbook. AcademicPress*, 1a Edición. Recuperado el 7 de 8 de 2019, de https://www.academia.edu/23975452/Informatica_forense

Malwarebytes. (2018). *malwarebytes.* Recuperado el 12 de 9 de 2019, de https://es.malwarebytes.com/ransomware/

Martín, S. (2010). *http://gpd.sip.ucm.es*. Obtenido de http://gpd.sip.ucm.es/sonia/docencia/master1011/delito.pdf

Michelle. (01 de 06 de 2016). *Informatica U.C Guia de estudio*. Obtenido de http://primeranofcjpuc.blogspot.com/2016/06/analisis-de-informatica-forense-en-los.html

Michelle. (01 de 06 de 2016). *Informática U.C Guía de Estudio.* Obtenido de http://primeranofcjpuc.blogspot.com/2016/06/analisis-de-informatica-forense-en-los.html

mintic. (28 de 3 de 2016). *Evidencia Digital*, 1.0. Recuperado el 17 de 8 de 2019, de https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Miranda. (2008). *Importancia de la informática forense*. Obtenido de https://www.academia.edu/23975452/Informatica_forense

Moes, T. (2018). *softwarelab*. Recuperado el 10 de 9 de 2019, de https://softwarelab.org/es/que-es-spyware/

Molina, A. (2018). *cloudseguro*. Obtenido de https://www.cloudseguro.co/que-es-delito-informatico/

Morachimo, M. (12 de 2 de 2019). *Hiperderecho*. Obtenido de https://hiperderecho.org/2019/02/sentido-comun-frente-a-la-convencion-de-budapest/#more-5979

Ó Ciardhuáin, S. (s.f.). *An ExtendedModel of Cybercrime Investigations.*, Volume 3, número 1. Obtenido de International Journal of Digital Evidence.

Ojeda Pérez, J., Rincón Rodríguez, F., Arias Flórez, M., & Daza Martínez, L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia*, 11 (28). Obtenido de https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

Ojeda, J., Rincón, F., Arias, M., & Daza, L. (2010). *revistas.javeriana*. Recuperado el 13 de 9 de 2019, de https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

Orta, R. (08 de 01 de 2008). *grafotecnica*. Obtenido de Informatica Forense en Venezuela (Audio): http://www.grafotecnica.com/grafotecnia/index.php?option=com_content&view=article&id=169:informatica-forense-en-venezuela-audio&catid=8&Itemid=118

Paus, L. (2015). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/

Pérez, L. (11 de 6 de 2014). *searchdatacenter.* Recuperado el 19 de 9 de 2019, de https://searchdatacenter.techtarget.com/es/cronica/Los-7-principales-riesgos-de-TI-para-las-organizaciones-de-acuerdo-con-Zurich

Peruano, E. (22 de 10 de 2013). *http://busquedas.elperuano.pe*. Obtenido de http://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

pmg-ssi. (1 de 2 de 2018). *Sistemas de Gestiónde Seguridad de la Información*. Recuperado el 7 de 9 de 2019, de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Porolli, M. (12 de 08 de 2013). Recuperado el 14 de 4 de 2019, de https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

puromarketing. (15 de 10 de 2015). *puromarketing*. Recuperado el 6 de 5 de 2019, de https://www.puromarketing.com/12/25575/cuales-son-aspectos-clave-big-data-debe-tener-cuenta-sector-retail.html

Quintero, J. (04 de 06 de 2014). *colegiogalanvilla*. Obtenido de http://www.colegiogalanvilla.edu.co/blogs/archives/749

Rubio, J. (2018). *Perito informatico*. Recuperado el 14 de 9 de 2019, de https://peritoinformaticocolegiado.es/

Secretaría. (5 de 1 de 2009). *alcaldiabogota.* Recuperado el 26 de 6 de 2019, de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

siete24. (1 de 11 de 2016). *Seguridad & Tecnología.* Recuperado el 18 de 7 de 2019, de https://blog.siete24.com/big-data-prevencion-y-mitigacion-de-riesgos-informaticos

siete24. (2016). *siete24 Seguridad & Tecnologia.* Recuperado el 1 de 10 de 2019, de https://blog.siete24.com/tendencias-delitos-electronicos-manejo-de-la-informacion

Telléz, J. (2014). *Derecho Informático*. (McGRAW-HILL, Editor) Obtenido de Julio Téllez. (2014). Derecho Informático. 11/10/2019, de clauditha2017 Sitio web: https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Terreros, F. (2016). *derecho.edu.pe*. Obtenido de http://www.derecho.usmp.edu.pe/cedp/revista/edicion_1/articulos/Felipe_Villavicencio_Terreros-Delitos_Informaticos_Ley30096_su_modificacion.pdf

Zdenko, S. (2012). *delitosinformaticos*. Recuperado el 16/9/2019, de https://delitosinformaticos.com/legislacion/costarica.shtml

Zuccardi, G., & Gutiérrez, J. D. (2015). Informática Forense en Colombia. *Ciencia, Innovación y Tecnología (RCIYT), II*, 9. Obtenido de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

ANEXOS

Anexo A Formato RAE

Fecha de Realización: 13/09/2019
Título: Uso de la informática forense aplicada a delitos informáticos en la industria Colombiana
Autor: AYAZO, Perú
Palabras Claves: Seguridad, Forense, Ciberataques, Phishing, Manejo de evidencia, Ransomware, Empresas.
Descripción: Trabajo de grado para optar por el título de Especialista en Seguridad Informática
Fuentes: El presente documento se basó en una investigación realizada en 26 fuentes bibliográficas tomadas de internet en las cuales se abordan los temas contenidos en este documento, adicionalmente gran parte de los textos y párrafos fueron complementados con la experiencia y conocimiento del autor de este documento monográfico.
Contenido del documento: En este Proyecto Aplicado que se presenta como trabajo de grado para optar por el título de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia sede Valledupar. Este proyecto persigue como objetivo principal que es realizar un análisis de seguridad de la infraestructura tecnológica del centro de datos de la Cámara de Comercio de Valledupar y para lo cual se estipula una ejecución de 4 meses aproximadamente. “La Cámara de Comercio de Valledupar, es una entidad privada, representativa del sector empresarial, la cual desarrolla seis (6) funciones básicas: llevar en forma eficiente el Registro Mercantil, Registro Único de Proponentes, Centros de Conciliación y Arbitraje, Registrar las Entidades Privadas sin Ánimo de Lucro, Promover el desarrollo empresarial en la ciudad de Valledupar y en el Departamento del Cesar, y el desarrollo social y cívico de la comunidad Con el objetivo de buscar mayor satisfacción de los usuarios de la Cámara de Comercio de Valledupar que son su razón de ser, fortalecer todos los procesos de la entidad y dar cumplimiento a la Misión, es necesario realizar un análisis de las condiciones en que se encuentra el centro de datos de la entidad, para

tener una orientación sustentada basada en estudios, que señalen las mejoras que se deben de implementar en cuanto hardware y software.

Los resultados esperados de este proyecto se centran en proporcionar en cumplimiento de las mejores prácticas y estándares de calidad, un centro de datos moderno que comprenda una adecuación física y de software acorde a las exigencias que el mismo negocio requiere, como son equipos de última tecnología, sistema eléctrico adecuado, mecanismos de seguridad avanzados, cableado estructurado, software actualizado que sean aptos para soportar la interacción eficiente con los sistemas de información con que trabaja actualmente la entidad y las nuevas tecnologías que se implementen a futuro.

Conceptos nuevos: conceptos nuevos.

Conclusiones:

- Colombia, en pleno desarrollo pero con un avance tecnológico importante en la última década se enfrenta a cambiar y a acostumbrarse a situaciones las cuales antes no ha manejado como lo son la judicialización en términos tecnológicos y es algo que le ha causado al país algo de traumatismo pero está en el proceso , cosa que no muchos países vecinos no han hecho, pero cabe resaltar que hay un desconocimiento masivo tanto por las personas naturales , como para las compañías y esto es aún más grave porque las compañías no se preparan y no están bien informadas de cómo opera la ley como se pueden proteger , y como mitigar el riesgo que una situación la cual amanece la seguridad de la información sea controlado y mejor aún prevenida.

- A través de la informática forense, que es considerada como una ciencia, se pueden ejecutar diferentes investigaciones relacionadas con cualquier crimen o delito informático dentro de una empresa y adquirir las pruebas o evidencias indispensables y válidas ante un juzgado, puesto que éstas facilitaran el juzgamiento de los sujetos autores del delito o implicados en éste.

- 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 en las organizaciones, además de prestar asesoría y apoyo al momento de realizar investigaciones para generar soluciones prontas y eficientes según sea la circunstancia.

- La Constitución Política de Colombia en su artículo 15 permite fundamentar el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia, donde se establece el derecho a la intimidad, por lo que se deben respetar la libertad y promover las demás garantías consagradas en la Constitución, apoyado en la Ley 527 de Agosto 18 de 1999 que trata de los instrumentos magnéticos e informáticos, así como la ley 527 de 1999 sobre el comercio electrónico para Colombia, la Ley 1273 de 2009 para la protección de la información y de los datos y la Ley 1273 del 2009 que tipifica los delitos informáticos con el fin de penalizar a los infractores.

AUTOR: Perú Carmelo Ayazo Villadiego