UNIVERSIDAD TECNOLÓGICA DE PEREIRA

PROYECTO DE GRADO

MONOGRAFÍA

INFORMÁTICA FORENSE

AUTORES: JOHANNES CAÑON Y CATALINA GONZALEZ

DIRECTOR: SAULO DE JESÚS TORRES

PEREIRA, 2017

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

Dedicatorias

Dedicado de manera especial a:
Mi mayor alegría y guía desde que me levanto hasta que me acuesto es principalmente Dios, él ha sido mi guardián desde que empecé este sueño de ser una ingeniera de sistemas desde que estaba en el colegio. Siempre ha sido mi fuerza mi valentía para afrontar situaciones amargas como también momentos alegres e inolvidables. A veces nos olvidamos de él pero siempre está ahí escuchándonos en nuestras peticiones u oraciones y no bendice con su apoyo divina para salir adelante y seguir luchando cada día para cumplir metas, ilusiones y anhelos y no dejándonos desfallecer jamás. Y por último enseñarnos a valorar cada minuto de nuestras vidas.

A mi mama Lilian Henao Rojas, Por ser la mujer más maravillosa de este mundo que siempre me acompaña y me guía en todo momento de mi existencia, gracias por inculcarme estos valores tan bellos porque yo soy quien soy por ti. Por demostrarme que tan grande sea el problema siempre estás ahí guiándome y dándome una palabra de aliento para pararme y luchar por mis sueños y no dejarme caer. Por su amor incondicional, por ser mi mayor motivación para ser una profesional y persona de bien, y por llevarme siempre en sus oraciones. Gracias madre.

A mi padre Julio Cesar González, Por ser el padre más maravilloso de este mundo, porque siempre ha luchado para que ni me hermana ni a mi nos falte nada, por su amor incondicional, y por su apoyo económico. Gracias padre por todo esos lindos consejos que me das a diario, aunque a veces me regañas yo sé que es por mi bien. También quería agradecerte por todos esos valores que me inculcaste en mi vida y en mi progreso académico.

A mi hermana Natalia González, Por ser una gran amiga y una gran hermana, eres mi motivación a seguir luchando por mi sueños, gracias por todo esos momento hermosos e inolvidables que hemos pasado juntas, por ser una guía en mi vida por tus consejos y apoyo que me han ayudado a continuar con la realización de mis sueños, por su apoyo económico para terminar satisfactoriamente mis estudios.

Catalina González Henao

Dedicado de manera especial a:

Mi mayor motivación para el día a día ha sido primordialmente Dios que a pesar de las dificultades, los problemas que se presentan y las desmotivaciones no nos abandona y siempre nos brinda un poco de su ayuda así no la sintamos o a veces nos olvidemos de él. 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 subimos que nos ayuda a sobresalir en la vida, a estar más cerca de cumplir nuestras metas y sueños.

A cada uno de los miembros de mi familia porque cada uno de ellos directa o indirectamente ha puesto su grano de arena en mi proceso de formación académica.

A mi madre Alba Lucia Franco 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, por su ayuda económica y sobre todos porque siempre me lleva en sus oraciones.

A mi padre Carlos Cañón Calderón por ser mi mejor amigo, por esa 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 mi hermano Jeremy Cañón Franco por ser una compañía a lo largo de mi vida, por ser un hermano maravilloso que siempre ha estado conmigo en todo momento, que hemos tenidos nuestras peleas pero siempre salimos adelante, gracias hermano por su paciencia y compresión. Y sobre todo por estar ahí en este momento tan importante y valioso de mi vida.

A mi abuela María Florentina García Correa por ser como una segunda madre, por estar pendiente cada de mí, tener las puertas de su casa siempre abiertas para mí, por su sabios consejos por su amor y su preocupación por mí y por toda la familia.

Johannes Cañón Franco

Agradecimientos

Queremos agradecer primeramente a Dios, porque él es nuestra motivación día a día, por acompañarnos siempre en este camino llenos de obstáculos y de alegrías, por ser nuestro guardián y orientador en esta etapa académica, por darnos tanta fuerza y valentía para afrontar nuestras dificultades y debilidades a lo largo de esta etapa. Por habernos permitido llegar a este punto y darnos la salud para lograr nuestros logros y objetivos.

A nuestras familia que es el motor de nuestras vidas, que nunca nos dejaron caer, siempre estuvieron ahí apoyándonos y dándonos la fuerza necesaria para seguir con nuestras metas a pesar de las dificultades y sacrificios que tuvieron que hacer para vernos triunfar y cumplir nuestras ilusiones que teníamos desde pequeños ser unos ingenieros de sistemas, nosotros les agradecemos de todos corazón tanta paciencia que nos tuvieron y darles las gracias porque sin ustedes no hubiéramos tenido una buena educación a lo largo de nuestras vidas.

A nuestro director el Doctor Saulo de Jesús Torres Rengifo por ser un gran ejemplo a seguir, por motivarnos para cumplir nuestros sueños, por su pasión, dedicación y amor por la enseñanza, por ser una persona extraordinaria y excepcional, porque sin usted no hubiéramos acabado nuestro proyecto con éxito. Que Dios lo bendiga profesor.

A nuestros maestros que en el transcurro de nuestra formación académica nos ayudaron con su gran labor, dedicación y compromiso, aportando sus experiencias y orientaciones a nivel profesional que nos brindaron día a día para culminan con éxito esta etapa nueva de nuestras vidas.

Resumen

En el presente trabajo se hace referencia la importancia de saber acerca de la informática forense que se ocupa en reconocer o registrar pruebas encontradas en los delitos informáticos o impedir si todavía no ha pasado aun, para esto es necesario conocer a fondo todo acerca de la informática forense, la cadena de custodia, los delitos informáticos, las herramientas a utilizar para este tipo de delitos y las normas e leyes que existen en Colombia. Hoy en día está revolucionando las tecnologías y se espera que en el 2020 exista más de 20 mil millones de dispositivos conectados a internet donde será más fácil para los cibercriminales robar, alterar o eliminar información según sea su objetivo del ataque informático. En fin nosotros queremos que con este trabajo mostrarles el significado de este tema, para que en un futuro no sea víctimas de algunos ataques existentes en la actualidad tales como; falsificación de identidad, estafas, extorsiones, robos, pornografía, malawares, entre otros.

Palabras claves:

Informática forense, Delito informático, cadena de custodia, peritaje informático, perito informático, hackers, virus, evidencia digital.

Abstract

This paper refers to the importance of knowing about computer forensics that deals with recognizing or recording evidence found in computer crimes or preventing if it has not yet happened, for this it is necessary to know everything about computer science Forensic, chain of custody, computer crimes, tools to use for this type of crime and the rules and laws that exist in Colombia. Today it is revolutionizing technologies and it is expected that in 2020 there will be more than 20 billion devices connected to the Internet where it will be easier for cybercriminals to steal, alter or delete information depending on their purpose of the computer attack. In short we want this work to show you the meaning of this topic, so that in the future do not be victims of some existing attacks such as; Identity fraud, fraud, extortion, robbery, pornography, malawares, among others.

Keywords:

Computer forensics, Computer crime, chain of custody, computer expertise, computer expert, hackers, viruses, digital evidence.

PARTE I
Introducción a la investigación

CAPÍTULO 1

INTRODUCCIÓN

Actualmente, la era contemporánea está inmersa en un gran apogeo de gran evolución de las diferentes tecnologías, las cuales se desarrollaron rápidamente a raíz de la gran evolución industrial ocurrida en Inglaterra y que cada vez avanza a pasos agigantados con los grandes beneficios del Internet o de los medios informáticos, los datos pueden ser protegidos en cualquier parte del mundo y en diferentes recursos electrónicos con el fin de utilizarla de acuerdo al usuario interesado, volviendo simplemente eficaz, su obtención así como su manipulación de ser necesaria. Hoy en día, gran parte de la población desarrollan las faenas de la vida cotidiana a través del uso de los diferentes medios informáticos, igualmente con la ayuda de diversos recursos electrónicos. Estas actividades varían desde las consultas de diferentes tipos de información, también él envió y obtención de correos electrónicos, conocidos como los famosos e-mail, transferencias electrónicas, demanda de artículos, videoconferencias que pueden ejecutarse desde cualquier lugar del mundo, desde los sitios más alejados, sin importar las distancias, haciendo que se disminuya el tiempo de acción, por lo cual es mucho más efectivo y veloz, también se puede tener acceso para descargar películas, videos, documentales, entre otros, en la mayoría de casos de manera gratuita y en algunos otros, solo basta con hacer un registro para tener acceso a dichas descargas. De esta manera, podemos ver como el avance agigantado de las diferentes tecnologías y el uso masivo del internet o de los diversos medios informáticos han incidido positivamente en las personas, al generar más facilidad y rapidez en sus labores diarias tanto de tipo doméstico como de tipo laboral y de entretenimiento, pero a la vez ha generado consecuencias negativas en una parte de la población porque se pueden generar sucesos delincuenciales según las normas o ley, que no se deberían realizar, pues así como los diversos medios informáticos favorece en el desarrollo de las tareas o las actividades de la vida cotidiana, igualmente por este mismo medio o por los recursos electrónicos, podría accederse de manera inadecuada o ilegal perjudicando directamente a personas naturales o jurídicas, públicas o privadas. **[1]**

Así mismo, nuestro país, también ha sido constantemente víctima de estos delitos informáticos, debido a que frecuentemente se presentan suplantaciones de identidades (phishing), no solo en las entidades bancarias, sino también en la apropiación indebida en las entidades financieras o páginas de negocios en línea, extorsiones que frecuentemente están relacionadas directamente con los envíos de correos con código malicioso, lo cual perjudica notablemente, porque genera mayor facilidad para los conocidos como los delincuentes informáticos, el cual se beneficia de la información cada vez que se abre el correo electrónico, etc., generando allí, perjuicio para los usuarios o propietarios de dichos correos, al tener facilidad de acceso a éstos, por tal razón es aquí donde se debe aplicar la informática forense, la cual es una herramienta muy útil y de moda en la era actual y es una ciencia que se dedica a realizar diferentes estudios e investigaciones para aclarar un caso de estudio a través de pasos como: el de reconocer, recoger y examinar los recursos probatorios para aclarar la situación delictiva, protegiéndose de situaciones posteriores o a largo plazo. **[1]**

Desde éste punto de vista, la presente monografía pretende profundizar más con respecto a la informática forense, como herramienta y ciencia fundamental en los delitos informáticos, así como describir ¿Para qué sirve?, ¿Cuál es su importancia?, ¿En qué se basa?, ¿Cuáles son sus objetivos? ¿Cuáles son los métodos empleados? ¿Cuáles son los actores en la informática forense?, ¿En qué consiste evidencia digital? ¿En qué consisten los delitos informáticos? ¿Cuáles son los tipos de atacantes?, para esto existen mecanismos que reconocen, analizan, sacan y sustentan elementos probatorios y salvaguardados y posteriormente ser utilizados y así llegar a la judicialización de los delitos si es el caso.

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 consiste cadena de custodia?, ¿En qué consisten los delitos informáticos?, ¿Cuáles son los tipos de atacantes?, sus fines u objetivos, fase de la investigación forense, las herramientas, las aplicaciones y las metodologías apropiadas en la aplicación de dicha informática. En el capítulo segundo se manejarán los delitos informáticos en Colombia 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.

1.1. Generalidades

1.1.1. Formulación del problema

Frente a los agigantados desarrollos industriales generados con el transcurso de los años y el tiempo, principalmente en el campo de las telecomunicaciones, se alcanza a observar la gran disposición y la capacidad de algunos seres humanos, lo cual los ha conducido a generar diversidades de herramientas y misiones que hacen una vida mucho más cómoda para todos y más eficiente en el campo laboral, pero a la vez que se presentan los beneficios y aspectos positivos, también aparecen los negativos en todas estas tecnologías, entonces surgen, los llamados delitos informáticos que penetran en la sociedad, siendo cada vez más permanente su multiplicación, por lo tanto, se genera entonces, 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.
De acuerdo al anterior planteamiento, es pertinente realizar la presente investigación facilitando que los seres humanos posean mayor conocimiento con relación a la informática forense, para que sirva como herramienta fundamental y así de esta manera colaborar de forma correcta con el manejo de las pruebas o evidencias, su estudio, análisis y presentación, de esta manera se constituye como una base de información y de culturización para tratar asuntos con relación a situaciones delictivas, es considerada actualmente de gran utilidad en cuanto a los delitos informáticos se refiere.

1.1.2. Justificación

En la mayoría de países a nivel mundial se ha generalizado la informatización o uso de los recursos informáticos, ya que el avance tecnológico a través del tiempo así lo ha requerido e inclusive en el entretenimiento y ocio, el manejo de los recursos informáticos se ha convertido casi en una herramienta necesaria y hasta conveniente, pero junto a las innumerables y cuestionadas beneficios que aportan, también empiezan a generarse algunos matices negativos o poco adecuados , como es el caso de los hechos que se han catalogado como 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, hasta llegarse a convertir en hechos que nunca antes el hombre había pensado, pero que por su deseo de control y delincuencia desmesurada ha traspasado fronteras que anteriormente eran inexistentes aún en el mismo pensamiento del hombre, pero que su codicia y ambición lo han conllevado a la alteración y manipulación delictiva y fraudulenta de los ordenadores con el propósito de adquirir su propia ventaja de manera lucrativa, no importando para esto que tenga que recurrir a falsificación y la manipulación ilegal de la información destruyendo, dañando o

alterando el marco del ámbito privado, siendo algunos de los mecanismos enfocados con el manejo informático, a través de ésta es factible adquirir enormes ventajas económicos o producir notables daños no sólo materiales y económicos sino también de tipo moral, sin embargo no sólo el monto económico de los daños generados es frecuentemente muy alta con respecto a la conocida como la tradicional, sino que además tienen probabilidades muy altas de que no lleguen a descubrirse o por lo menos a aclararse, por tal razón se estaría hablando de una delincuencia de tipo de especialistas, audaces y capaces generalmente de no dejar ninguna huella o señal de los hechos que puedan culparlos. Por tales razones, se considera que la informática puede ser el medio o herramienta para crear el ataque o la vía para emprender otros hechos también de tipo delictivos. En éste sentido consideramos que la informática es una alta herramienta que presenta unas condiciones que la ubican como un mecanismo apropiado para generar de muy distintas formas actividades de tipo patrimonial (estafas, apropiaciones indebidas, chantajes, fraudes, entre otras.). La idoneidad se genera, generalmente, del gran número de información obtenida, por medio del práctico ingreso a ésta y la posible adulteración o falsificación de los datos que cada vez facilita aún más la delincuencia informática. **[2]**

La sociedad no es ajena a los delitos informáticos, debido a la constante presencia de sujetos y bandas con ambiciones para adquirir el control que los medios informáticos les ofrecen 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. 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. **(Miguel Garavilla Estrada, 2008, p, 1). [2]**

Por tales razones 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.

Según la Revista Cara y sello, durante el 2007 en Colombia perdieron más de 6.6 billones de pesos a raíz de delitos información. (Isabella Gandini, Andrés Isaza y Alejandro Delgado).

Cada vez y con mayor frecuencia las distintas entidades financieras y comerciales prefieren hacer sus diferentes transacciones o movimientos de dinero a través del uso del internet, aumentando así su posibilidad de ser víctimas de los tan nombrados hoy por hoy los delitos informáticos, más aún, sin cerciorarse de recursos de protección correctos; tener una herramienta informática forense en redes e internet para la obtención de la prueba digital que guíe a los operadores de justicia en el país de Colombia, puede colaborar con el esclarecimiento de estos delitos e identificar a los sujetos autores y obtener una

indemnización de los daños causados. También se puede hacer uso de un mecanismo para ejecutar una acción de tipo investigativa para mejorar el rendimiento ya que se previenen las desviaciones y retenciones en la adquisición de los resultados lo que redunda en disminuir el tiempo y los gastos operativos ejecutados en éste proceso. **(Verónica Mamani Saravia, p, 11). [4]**

Lo que representó un gran avance para hacer un control con respecto a estos delitos informativos, por tal razón llevaremos a cabo este proyecto con el propósito de ofrecer un mayor conocimiento para aquellas personas que han optado por dedicarse al campo de protección de los sistemas informáticos o seguridad de la información para que más adelante pueda desempeñarse lo mejor posible en cualquier delito que se le presente y de ésta forma evitar ser víctima de algún delito informático y reduce el peligro del mismo que puede ser de nivel personal o de índole laboral.

1.2. Objetivos del proyecto

1.2.1. Objetivo general

- Hacer una investigación acerca de la informática forense como herramienta de soporte y apoyo para aquellos sujetos que han optado por trabajar el área del cuidado y protección de los sistemas informáticos usando la recolección y presentación de pruebas para tomar medidas y decisiones como medio de respuesta para proteger y cuidar sus equipos de persecuciones criminales o también llamados los delitos informáticos.

1.2.2. Objetivos específicos

- Mostrar los antecedentes relacionados con la informática forense.
- Explicar en qué consiste la informática forense
- Explicar los delitos informáticos.
- Determinar tipos de atacantes.
- Determinar tipos de ataques
- Indicar las diversas herramientas de prevención de incidentes.
- Sustentar en qué consiste la cadena de custodia.
- Presentar ejemplos relacionados con la informática forense
- Indicar las normas y leyes en Colombia para combatir los delitos informáticos.
- Presentar formatos ubicados en los anexos relacionados con la cadena de custodia.
- Algunas recomendaciones para evitar ser víctima de alguna ataque informático.

1.3. Alcances y límites

1.3.1. Alcances

- La monografía que estamos 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 de los diferentes dispositivos. Ésta 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 con el propósito de cuidar sus equipos de abusos y persecuciones criminales, lo cual es más viable mediante diferentes herramientas o aplicaciones usadas para éste fin.

1.3.2. Limites

- El mecanismo optado no tiene carácter preventivo de los delitos informáticos, sólo se limita a ofrecer una orientación o vía para obtener la admisión de la prueba o evidencia digital para aquellos sujetos que requieran del conocimiento con respecto de este tema para así cuidar y proteger nuestros datos personales y disminuir un poco el impacto de los delitos informáticos.

1.4. Metodología

- Desarrollada a través de la investigación, que consiste en descripción y el análisis de los mecanismos usados para abordar a cualquier delito informático o digital que se presente a nivel personal o laboral. 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.

1.4.1. Estructura de la metodología

Esta monografía está compuesta en 5 partes que incluye 5 capítulos formada de la siguiente manera:

1. **Parte I Introducción a la investigación que abarca:**
   a. **El capítulo 1. Introducción**. Donde se formula el problema, la justificación, los objetivos generales y específicos, los alcances e límites y la metodología.

2. **Parte II Estado del Arte que abarca:**
   a. **El capítulo 2. Introducción a la informática forense.** Se divide en dos partes: la primera es el marco teórico donde hace referencia de sus antecedentes e historia, definición de informática forense, los modelos, procedimientos e herramientas que se usan actualmente, y la descripción de la cadena de custodia y sus respectivas fases. Y la segunda y última parte es el marco conceptual donde hace referencia de la evidencia digital y los delitos informáticos con sus respectivos atacante y ataques.

3. **Parte III Desarrollo de la investigación:**
   a. **El capítulo 3. Delitos informáticos en Colombia.** Donde se hablará de las normas aplicadas en Colombia sobre informática forense, definición de peritaje informático e perito informático
   b. **El capítulo 4. Prevención para evitar delitos informáticos.** Donde se explicará algunos ejemplos e recomendaciones.

4. **Parte IV que abarca:**

a. **El capítulo 4. Conclusiones**. Donde se resumen la investigación y los alcances logrados.
b. Bibliografías en formato APA de todas las referencias utilizadas en esta investigación.

5. **Parte V**. Donde se presenta todos los anexos de mayor importancia en relación a esta investigación.

PARTE II
Estado del arte

CAPÍTULO 2

INTRODUCCIÓN A LA INFORMÁTICA FORENSE

2.1. Marco teórico

2.1.1. Antecedentes

- **En el año 1932:** Este año fue un motor de impulso debido a que El FBI 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 éste 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 las rastros digitales, con valor probatorio, pero sólo se utilizaron finalizando el siglo XIX **(Rodríguez & Doménech, n.d.).**
- **En el año 1993:** en éste año se conmemora la primera Conferencia Internacional sobre la Evidencia Digital.
- **En el año 1995:** en ésta 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. **[5]**

2.2. Reseña Histórica

En la época actual la tecnología ha tenido un desmesurado progreso, puesto que esta avanza a pasos gigantescos, cada vez, encontramos unas herramientas más sofisticadas e innovadoras capaces de desafiar constantemente los 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, pero hoy en día todos estos registros, los almacenamientos son digitales, requiriéndose sólo de un ordenador, 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. **[6]**

El interés por el estudio en el ámbito de la informática forense se originó en 1980, posteriormente después de que las computadoras personales empezaron a transformarsen como posibles opciones para los usuarios. En 1984, se hizo un programa del FBI, famoso por un periodo de tiempo como el Programa de Medios Magnéticos, que hoy se conoce como CART (CART, del inglés computer analysis and response team), o estudio de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", inició a laborar en este aspecto. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un grupo que lleva la firma forense. **(Heysel García, 2015). [7]**

De igual manera surge en los EUA, cuando la policía y los investigadores militares empezaron a observar que los delincuentes informáticos avanzaban en altos conocimientos más sofisticados, Agentes del Gobierno responsables de la protección de la información importante y confidencial con las investigaciones forenses desarrolladas en respuesta a las probables sendas de control y seguridad, con el propósito de examinar no sólo las suplantaciones a medida que aprenden a evitar casos semejantes a largo plazo. Finalmente, comenzar la unión entre ámbitos de la protección de la información, que se basan en el control de la información y la informática forense, que se focaliza en realizar a través de casos de información con respecto a la infracción, en cuanto a delitos informáticos se refiere.

Actualmente, este ámbito ha crecido así como la fuerza policial y militar, continúan trazando un control y seguridad a través de la informática forense. Las diversas Instituciones privadas han continuado el método de empleo directo a profesionales de informática forense. El ámbito de la informática forense sigue avanzando muy rápidamente y representan un nivel más amplio de conocimientos en este ámbito a medida que avanza el tiempo. Las compañías de software siguen innovando en programas forenses más amplios en cuanto a manejo de software, en éste sentido el nivel del campo legal y policial, se genera una inquietud constante

para determinar y capacitar y así incrementar su plantilla en respuesta a los delitos basados con la tecnología que demanda la época actual. **[5]**

2.3. ¿Qué es informática forense?

Iniciamos por diferenciar los conceptos de informática y de forense. La palabra Informática se puede definir como el grupo de saberes científicos y recursos que facilitan el análisis, el mejoramiento y la implementación de actualizaciones a la comunicación, el envío y la recepción de información a través de los ordenadores.
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. (Beatriz, 2007, p, 4). [8]

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. (Miranda, 2008, p, 4). [8]

En éste sentido se tiene que la ciencia forense es un mecanismo de investigación relacionada con los recursos electrónicos con el objetivo de hallar y de examinar la información disponible, eliminada u ocultada y que puede ser una prueba utilizada en determinado caso de estudio. Los diferentes recursos modernos y el software permiten que la Informática Forense sea un método viable para el personal especializado en ésta, para hallar y recuperar las evidencias más rápidamente y de manera precisa, identificando los delitos informáticos y para otro tipo de crímenes usando mecanismos y tecnologías avanzadas, así un funcionario emplea estos mecanismos para encontrar evidencias que pueden ser de diferentes clases de dispositivos electrónicos como discos duros, cintas de respaldo, computadores, almacenamientos extraíbles, archivos y los mismos correos electrónicos, entre otros. **(Raymond Orta, 2007). [9]**

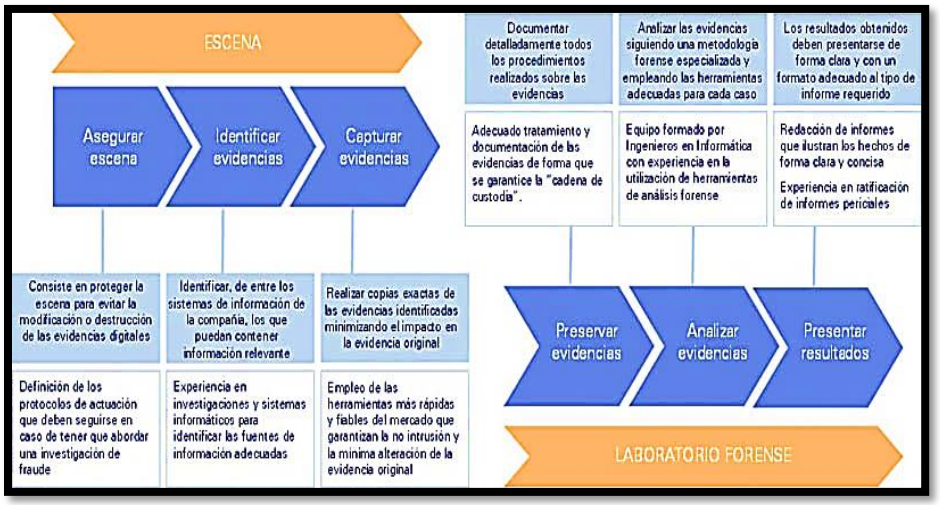


Figura 1. Manejo de evidencias.

Fuente. Vicente Sánchez Patón. (2014). Análisis forense en S.I. [Figura].
http://slideplayer.es/slide/1490888/

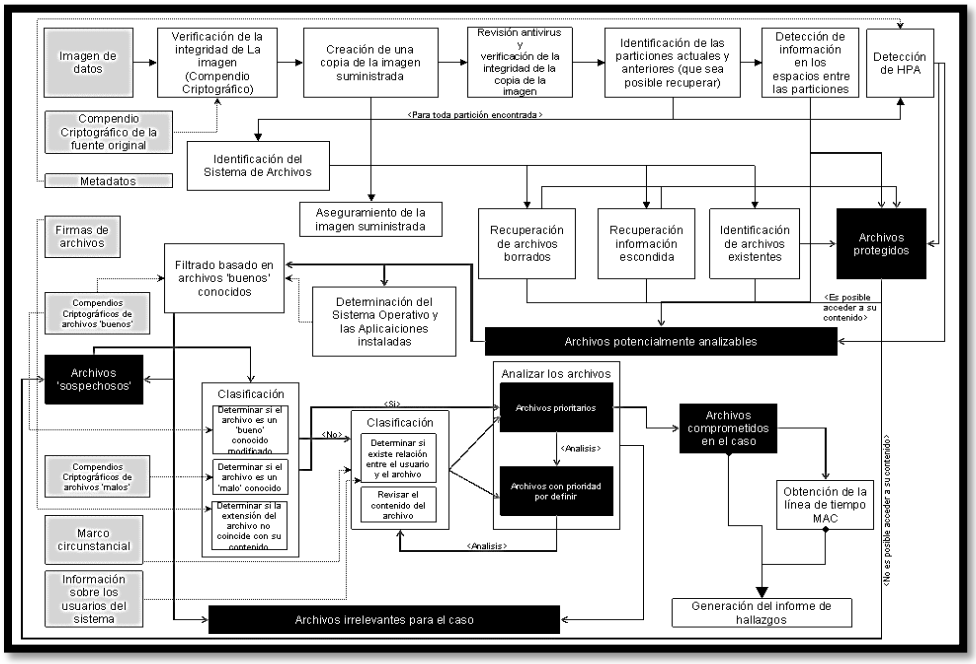


Figura 2. Metodología de análisis de datos.

Fuente. Siler amador donado (2017). Gráfico de la metodología de análisis de datos. [Figura].
http://webcache.googleusercontent.com/search?q=cache:http://190.90.112.209/informatica_forense.html

2.4. Modelos de procesos para informática forense

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:

2.4.1. 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:

1. La identificación
2. La conservación, la adquisición y la documentación
3. La clasificación, la comparación, y la individualización
4. La reconstrucción.

En los pasos 3 y 4 se hace el análisis de la prueba. Casey indica que es una etapa de almacenamiento de evidencia, puesto que al realizar la reparación pueden encontrarse elementos anexos que generen que la etapa se reinicie. El modelo se evalúa inicialmente en contextos de programas de cómputo independientemente de la red, y después realizado para las diferentes capas de red (desde física hasta la capa de aplicación, e incluyendo la infraestructura de la red) para detallar investigaciones en redes de computadoras. El modelo de Casey es general y se emplea muy bien en los dos, tanto en los computadores aislados como en los entornos de red. **[10]**

2.4.2. Modelo de Lee (2001)

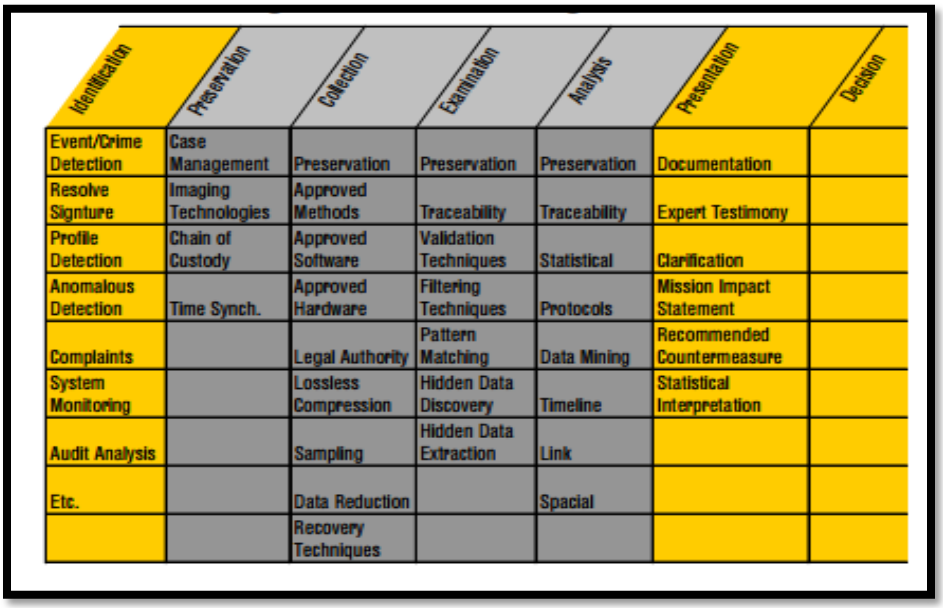
Este autor considera la investigación como un proceso. El modelo se dedica solo de la investigación de la escena de delito más no de la investigación total.
Consta de cuatro elementos inmersos en el proceso: Reconocimiento, Identificación, Individualización y Reconstrucción

- El reconocimiento, es la fase inicial, en ella se hallan bases fundamentales como evidencias potenciales.
- La identificación de los diferentes tipos de prueba es el paso a seguir, para ellos se requiere la selección de la prueba, una sub-actividad y la comparación.
- La individualización está relacionada a señalar si los ítems de prueba son auténticos, es decir originales para que puedan ser relacionados con un sujeto determinado.
- Y la reconstrucción tiene que ver con entrelazar el concepto de los anteriores elementos del proceso, y la otra información que corresponda a que los investigadores puedan obtener, para proporcionar una descripción de los sucesos y los hechos en la escena del crimen informático. **[8]**

2.4.3. Modelo de DFRWS (2001)

El primer Forensic Digital Research Workshop (Palmer, 2001) creó un modelo que abarca los siguientes pasos son: la identificación, la preservación, la colección, el examen, el análisis, la presentación y la decisión.

Tabla 1. Proceso investigativo para la ciencia forense digital



Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Fuente. Collective work of all DFRWS attendees. (2001). Investigative Process for Digital Forensic Science. [Tabla]. http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Este modelo no pretende ser el único, sino que funciona como un soporte para el trabajo posterior que determinará un modelo general y además como una estructura para la investigación a largo plazo. El modelo DFRWS se evalúa como lineal, pero la probabilidad de recuperación de un paso para los siguientes es nombrada. El informe DFRWS no discute los pasos del modelo con descripción detallada, más bien por cada paso se mencionan un número de casos por terminar. **[11]**

2.4.4. Modelo de Reith, Carry Gunsch (2002)

Reith, Carry Gunsch (2002) representan un modelo que hasta cierta parte se desprende del modelo DFRWS. Los elementos en su modelo son: identificación, preparación, estrategia de acercamiento, preservación, colección, examen, análisis y presentación y de la evidencia. Éste es importante porque representa una estrategia abstracta para diversos tipos de tecnología o ámbito de ciber-delito en cuanto a investigaciones se refiere, por lo que se cree que el modelo sea usado como base para otros métodos más explícitos para cada tipo determinado de análisis y estudios en los ciber - delitos. **[12]**

2.4.5. Modelo mejorado propuesto por Venansius Baryamureeba y Florence Tushabe (2004)

El presente modelo toma como referencia el anterior y procura superar algunos elementos, pero particularmente son semejantes. Abarca cinco fases principales:

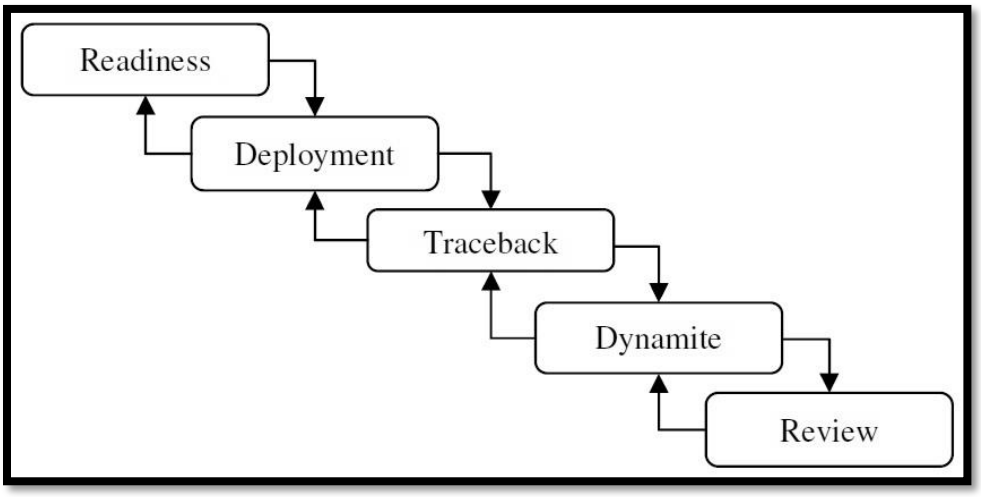


Figura 3: fases del modelo EIDIP

Fuente. Im Saidi. (2015). Enhanced Digital Investigation Process Model (EDIP) (2004). [Figura]. http://lmsaidi.blogspot.com.co/2015/08/masalah-dan-solusi-dari-rangkuman-paper.html

1. **Fases de preparación**: son iguales a las que se aplican al anterior modelo.

2. **Fases de despliegue**: Generan una estrategia para identificar y registrar un delito. Se hacen en el mismo sitio del delito y se presentan en cinco fases:
   - **Fase de detección y notificación:** se identifica el hecho y se informa a los sujetos indicados.
   - **Fase de investigación física de la escena del delito:** En ésta se verifica la escena física del delito y se detectan pruebas digitales potenciales y demostrables.
   - **Fase de investigación digital de la escena del delito:** se hace una revisión y se adquieren pruebas con la consecuente proyección del prejuicio provocado al manipular el sistema en búsqueda de pruebas del caso.
   - **Fase de confirmación:** cuando el hecho es asegurado y se adquiere respaldo legal para hacer un análisis o estudio profundo del caso.
   - **Fase de informe:** Es donde se cree se presentan las evidencias físicas y digitales a personas jurídicas o entidades legales para resolver el caso.

3. **Fases de Hipótesis**: Durante ésta se supone retomar los sucesos ocurridos en la escena física del delito para determinar los recursos que se utilizaron para realizar el hecho delictivo. Está dividida así:
   - **Investigación digital** de los hechos del crimen: se hace una hipótesis inicial con los datos obtenidos en fases anteriores. Por ejemplo, si tenemos una dirección IP de dudosa procedencia en nuestro sistema, podemos tratar de ubicar su origen a través de Internet.
   - **Fase de autorización:** se adquiere permiso de las entidades locales para realizar las investigaciones detalladas y así poder obtener más información en busca de los responsables de los delitos informáticos.

4. **Fases Dinamita**: Estas fases indagan acerca de las hipótesis creadas en el paso anterior. El propósito está orientado a la recopilación y análisis de las pruebas halladas en la etapa anterior, para adquirir pruebas o evidencias y así identificar lo sucedido y hallar los autores del delito, para lo cual se tiene en cuenta las siguientes subfases:
    - **Fase de Investigación Física de la escena del delito:** se revisa nuevamente la escena teniendo en cuenta como referencia la hipótesis preliminar hallando pruebas o evidencias digitales adicionales para aclarar los hechos.
    - **Fase de Investigación Digital de la escena del delito:** se revisa la prueba en consecución de otras nuevas que soporten el caso y así facilitar la aproximación al suceso que pretende aclararse.
    - **Fase de Reconstrucción:** reorganizar las piezas del puzle digital y determinar las hipótesis posibles.
    - **Fase de Comunicación:** se basa en realizar la presentación de las interpretaciones y conclusiones acerca de las pruebas que han sido analizadas por un experto o profesional determinado.

5. **Fase de Revisión:** La investigación es completa y requiere ser constantemente analizada y retroalimentada para buscar el mejoramiento. **[10]**

Tabla 2: Comparación de los modelos

Activity in new model	*MODEL* Lee et al.	Casey	DFRWS	Reith et al.
Awareness				✓
Authorisation				
Planning				✓
Notification				
Search/Identification	✓	✓	✓	✓
Collection	✓	✓	✓	✓
Transport				
Storage				
Examination	✓	✓	✓	✓
Hypothesis	✓		✓	✓
Presentation	✓		✓	✓
Proof/Defence			✓	
Dissemination				

Fuente. Séamus Ó Ciardhuáin. (2004). Comparison of activities in the models discussed. [Tabla]. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

Tabla 3: Comparación de terminología en modelos

Term in new model	MODEL			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				Identification
Authorisation				
Planning				Preparation
Notification				
Search/Identification	Recognition, Identification	Recognition	Identification	
Collection	Collection and Preservation	Preservation, Collection, Documentation	Preservation, Collection	Preservation, Collection
Transport				
Storage				
Examination	Individualization	Classification, Comparison, Individualization	Examination	Examination
Hypothesis	Reconstruction	Reconstruction	Analysis	Analysis
Presentation	Reporting and Presentation		Presentation	Presentation
Proof/Defence			Decision	
Dissemination				

Fuente. Séamus Ó Ciardhuáin. (2004). Comparison of terminology in models. [Tabla]. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

2.5. Procedimientos y tácticas basadas en informática forense

Las metodologías utilizadas son múltiples y autónomas, deben facilitar el trabajo de los expertos en informática forense, pero debe seguir algunas etapas con la información de la prueba, éstas son: las copias de la información recolectadas, conservar la totalidad del recurso original hallados y calificar, verificar y transferir correctamente las copias de la información, y los resultados del análisis de estudio. Así, entonces, la prueba no será discutida y tampoco descarta como recurso probatorio. **[13]**

Para hacer un estudio forense se requiere una estrategia científica comprobada y de la utilización de recursos apropiados para hallar, recopilar, tratar y analizar la información, igualmente de garantía en la protección de las pruebas. Los elementos fundamentales en una metodología para desarrollar un análisis forense es:

- **Marco Científico:** Se refiere a las búsquedas y practicas soportadas en el procedimiento científico como también en la elocuencia argumentativa propia de cada profesional para contribuir de forma lógica una sustentación precisa.
- **Marco Criminalística:** Interactuar con otros expertos del campo, laborar en forma integrada y con fundamentos propios, llegar a conclusiones razonables. Adquirir los saberes básicos para identificar, preparar, conservar y de ser indispensable apoderarse de los elementos demostrativo personales de otros expertos presentes en el sitio del suceso.
- **Marco Informático general:** Los procedimiento acerca de los estudios hallados en el sistema, se utilizan como táctica para poder ajustar esa acción a un perito informático.
- **Marco Informático específico:** con base a los mecanismos en los estudios forenses, la información encontrada debe ser recolectada lo más preciso conforme al avance en nuestro país, ya sean con software libre o software propietario

- **Marco Legal:** la personas encargada del peritaje informático gestiona de forma legal lo sucedido en el lugar de los hechos, cumpliendo acorde con las normas vigentes en nuestro país los plazo de las pruebas halladas y la posición del testigo competente. **[14]**

2.6. Elementos fundamentales del proceso forense

A. Esterilidad de los medios de informáticos de trabajo.

Los recursos informáticos usados por los expertos en este campo, deben estar calificados a tal punto, que éstos no hayan sido exhibidos a alteraciones magnéticas, ópticas (láser) o similares, a no ser que los datos de la evidencia que se localicen en ellos puedan estar adulterado. La esterilidad de los medios es un requisito indispensable para el comienzo de algún recurso utilizado en el análisis informático, puesto que al igual que en la medicina forense, un instrumento contaminado puede ser motivo de una conclusión equivocada originando así consecuencias funestas en el objeto de estudio, llámese prueba o paciente.

B. Verificación de las copias en medios informáticos.

Las informaciones ejecutadas esterilizadamente deben ser iguales a los datos originales de los cuales fueron extraídas. La comprobación de estas pruebas deben ser por mecanismos, técnicas y recursos matemáticos que implante la totalidad de los datos trasladada a la copia, para lo cual, se recomienda usar algoritmos y procedimientos de control basadas en firma digitales que puedan verificar que la información este tomada corresponde a la que se ubica en el recurso de copia.

C. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.

El profesional debe ser el vigilante de su propio desarrollo, por tanto cada uno de las etapas elaboradas, las estrategias empleadas, y los resultados adquiridos del análisis de los datos, deben estar plenamente documentados, de tal forma, que cualquier persona puedan examinarlos, lo que representa un nivel se seguridad para el experto, al ser prevenidos en el manejo científico para evitar o minimizar la reproducción de sus resultados empleando la misma prueba.

D. Mantenimiento de la cadena de custodia de las evidencias digitales.

Este proceso es el complemento del anterior. Es el cuidado de todos las piezas de los acontecimientos bajo el poder del investigador, deben asegurar una buena diligencia y tramites esenciales para certificar cada uno de los sucesos identificados y argumentar a ciertos interrogantes tales como: ¿quién la entregó?, ¿cuándo se entregó?, ¿en qué estado se entregó?, ¿cómo se ha trasladado?, ¿quién ha tenido acceso a ella?, ¿cómo se ha realizado su custodia?, entre otras, éstas deben estar resueltas para poder evaluar apropiadamente las pruebas bajo la responsabilidad del investigador.

E. Informe y presentación de resultados de los análisis de los medios informáticos.

Es fundamental como los anteriores, puesto que una presentación errada de los resultados que puede conducir a una incorrecta salida de los hechos que pongan en riesgo la capacidad del profesional. Por tanto, la precisión, la utilización de un idioma sociable y sin malos entendidos, una transcripción intachable, una preparación correcta de los sucesos y los desenlace del informe, son piezas claves a la hora de defender la documentación de las investigaciones. **[15]**

2.7. Cadena de custodia

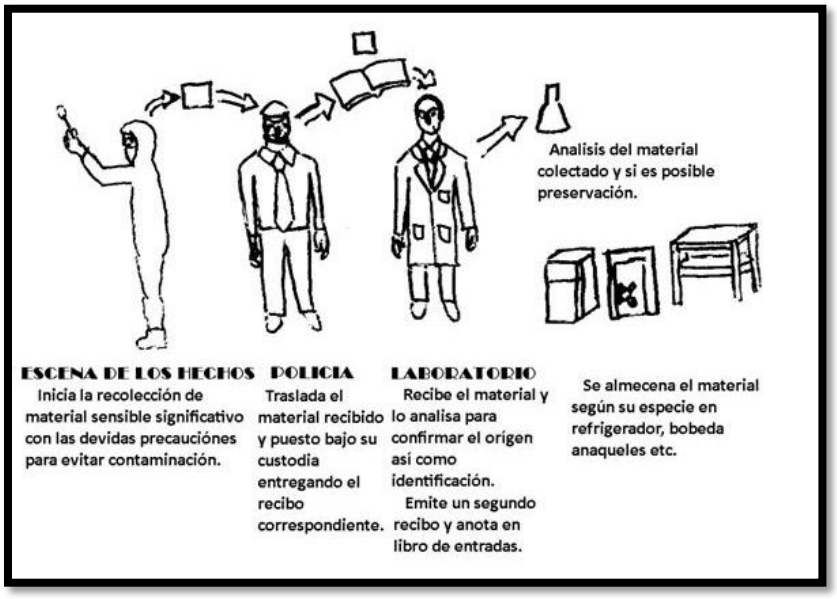


Figura 4. Etapas para resolver una cadena de custodia

Fuente. Arles Arias, Alejandro Rodríguez Arango y Adrián Sánchez. (2017). Cadena de custodia. [Figura]. http://hechosdetransito.com/cadena-de-custodia/

Esta se puede definir como la agrupación de etapas llevadas a cabo para custodiar la prueba convirtiéndola o utilizándola como evidencia digital en un procedimiento legal. La cadena de custodia proporciona los siguientes pasos:

A. Disminuir la cantidad de participantes en el empleo de las evidencias.
B. Sostener las identificaciones de los individuos involucrados desde los beneficios hasta las exhibiciones de las evidencias.
C. Mantener la firmeza de las pruebas.
D. Hacer registros de las duraciones de cada evidencia aprobados por los delegados.
E. Garantizar la solidez de las pruebas guardadas protegiendo su seguridad.

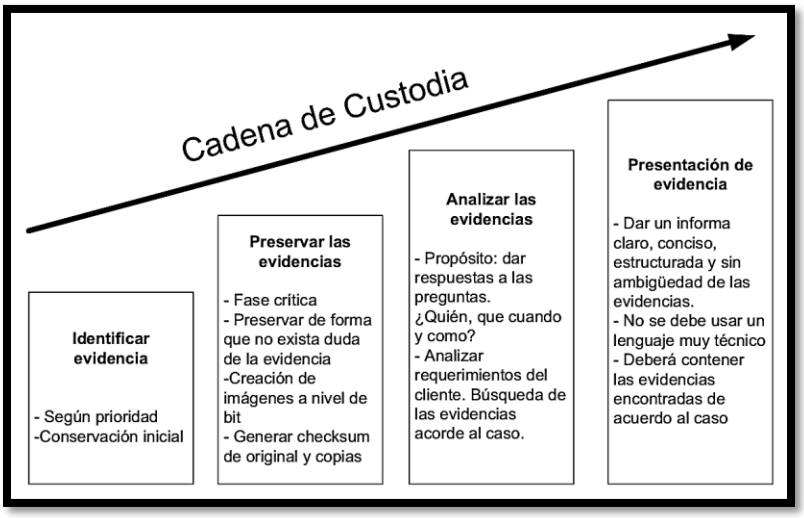


Figura 5. Proceso de la cadena de custodia

Fuente. Jaider. (2015). Cadena de custodia. [Figura].
http://eportafoliojaider.blogspot.com.co/2015/05/informatica-forense.html

2.7.1.1. Fase de Identificación

En esta fase, en el sitio de los hechos donde se ejecutó el ataque informático, se debe titular con sus pertinentes particularidades las piezas que va ser elemento fundamental en el análisis forense, para conservar los componentes tales como un disco duro de un computador hasta varias computadoras de una entidad. Puede decirse que en esta etapa se hace la recopilación de las pruebas digitales.

Tabla 4. Evidencia electrónica

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
• El hardware es mercancía ilegal o fruto del delito.	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• El hardware es un instrumento	• Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• El hardware es evidencia	• En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

Fuente. Dr. Santiago Acurio del Pino. Elementos fisicos. [Tabla].
https://www.oas.org/juridico/spanish/cyber/cyb44_informatica.pdf

Tabla 5. Evidencia digital

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
• La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
• La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

Fuente. Dr. Santiago Acurio del Pino. Información. [Tabla].
https://www.oas.org/juridico/spanish/cyber/cyb44_informatica.pdf

2.7.1.2. Fase de preservación

En ésta fase se desarrolla una representación puntual de las pruebas otorgándole un código único correspondiente a una combinación única de bytes que se ajusta a un conjunto de análisis; Dicho código validado debe ser idóneo para impedir vulneraciones en los datos recuperados y facilitar que sólo el personal autorizado y eficiente pueda manipularla para custodiar las pruebas analizadas; esto con el fin de implementar una cadena de cuidado permanente, desde ese instante se podrá duplicar copias textualmente idénticas de la imagen para que cada personal pueda asegurar copias de seguridad de las evidencias otorgadas.

2.7.1.3. Fase de análisis.

En ésta fase es donde se realiza una recopilación de las evidencias encontradas en el laboratorio. Debe procederse con analizar y buscar informaciones exhaustivas. El análisis empieza con la detección del tipo de ataque informático. Una función ilícita provocaría la eliminación de información que puede involucrar a una persona, también puede ser información ocultada o almacenada en medios no convencionales.
En el análisis se pueden examinar: registros eliminados, registros creados, accedidos o modificados dentro de un rango de fechas, tipos de registros con formato idénticos que fueron alterados. Por ejemplo; comunicaciones entre correos electrónicos, movimientos en internet, el nombre de una persona, ciudad o empresa o fotografías.

2.7.1.4. Fase de presentación

En ésta fase final se obtiene los resultados encontrados por el investigador. Tan rápido como el hecho haya sido registrado e identificado cada persona encargada de estos sucesos debe tomar apuntes de cada actividad que se llevan a cabo para estos tipos de investigaciones, debe estar documentado con fecha desde que descubren los acontecimientos hasta terminar

la presentación. Cada documentación debe ser entendible y contundente para que sean aceptadas legalmente por entidades judiciales. **[16].**

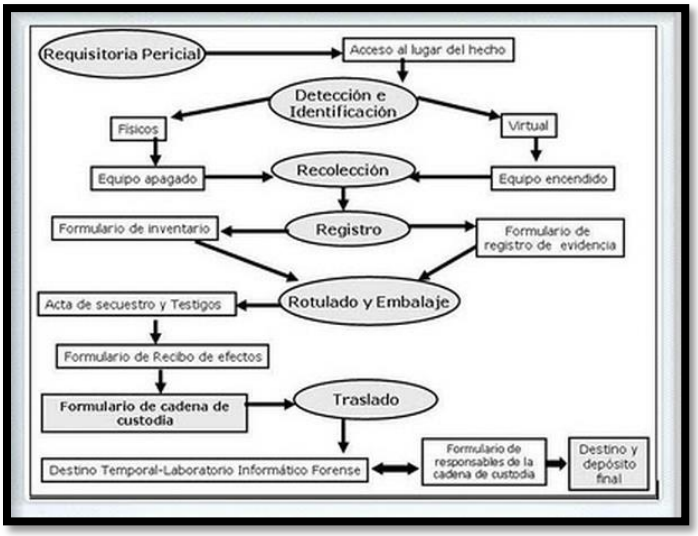


Figura 6. Protocolos de la cadena custodia para la información forense

Fuente. Juan de Dios Meseguer González. (2013). Protocolo para la cadena de custodia en la pericia de informática forense. [Figura]. http://www.elderecho.com/www-elderecho-com/contaminacion-custodia-invalida-periciales-informaticas_11_556555001.html

2.8. Herramientas y aplicaciones utilizadas en la informática forense

En informática forense existen variedades de herramientas en donde los investigadores buscan y analizan las evidencias recolectadas en los lugares de los hechos. Las siguientes herramientas son:

2.8.1.1. OSFClone

Esta herramienta es considerada como una aplicación libre o arrancable, que habilita la extracción pura de las imágenes encontradas rápidamente en los disco duro, es independiente de los sistemas operativos. OSFClone es compatible con AFF, (Advance Forensics Format), este formato es abierto y desplegable para conservar o asegurar imágenes de discos asociados que sirve para que los investigadores analicen eficientemente los datos para llevarlos a cabo a un estudio forense.

Figura 7. Programa OSFClone

Fuente. PassMark® Software Pty Ltd. (2010). OSFClone. [Figura]. https://www.osforensics.com/tools/create-disk-images.html

OSFClone genera imágenes forenses en los discos duros, conservando los sitios no utilizados, capacidad de holgura, división de archivos y búsqueda de los archivos no borrados del disco duro original. Esta herramienta se puede desplegar desde CD/DVD, o desde unidades flash USB, y puede crear imágenes en formato dc3dd.

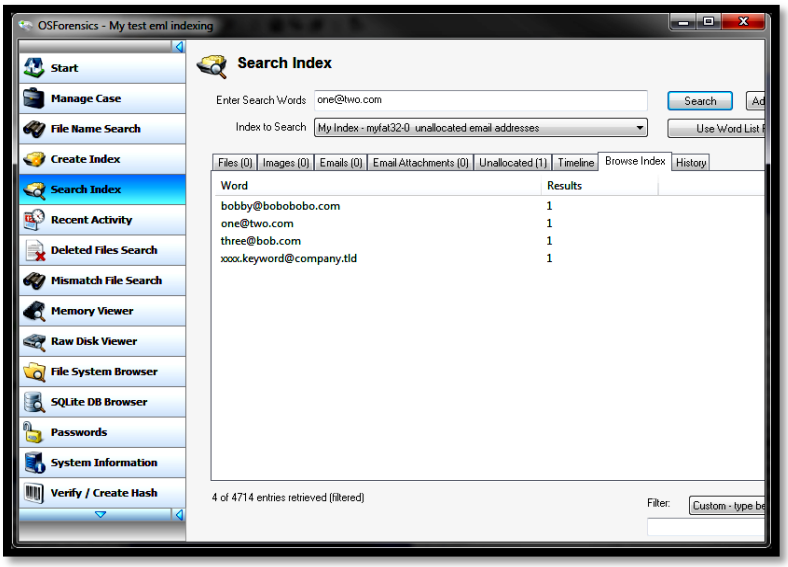


Figura 8. Escaneo del problema OSFClone

Fuente. Ingeniero de PassMark. (2012). [Figura]. https://www.passmark.com/forum/osforensics-osfmount-osfclone/3939-corrupt-case-item?3904-Corrupt-Case-Item=

Se puede aplicar OSFClone para ayudar a los metadatos forenses por ejemplo, las cifras de los casos, pruebas o el nombre del examinador con sus respectivas descripciones y la totalidad de las imágenes clonados o creadas. En fin es una herramienta muy útil para producir imágenes de disco para el análisis forense. **[17]**

2.8.1.2. Drive Clone:

Esta herramienta es muy útil para permitir clonar instantemente todo el equipo, como las aplicaciones, los registros del sistema, los correos electrónicos, las redes sociales, entre otros, esta se distingue de todas las demás porque desfragmenta rápidamente todos los registros encontrados en el sistema, también desecha la basura, renueva el tamaño de las particiones, y solos hace clonaciones de los registros que han sido cambiados desde la última vez que fueron clonados. Es una herramienta fácil de usar porque permite la clonación de los dispositivos o discos duros. **[17]**

Figura 9. Programa drive clone

Fuente. Brothersoft Windows. (2009). Drive Clone 2009. [Figura]. http://www.brothersoft.com/drive-clone-207813.html

2.8.1.3. Acronis True Image

Esta es una aplicación de pago, que sirve para ejecutar copias de seguridad de imágenes completas y rescatar algunas partes de un sistemas tales como: música, fotografías, videos, documentos o configuraciones personales. Es una herramienta que puede almacenar las imágenes en un dispositivo local o en la nube, guardar sistemas o archivos completos e individuales y rescatarlos en cualquier instante, ya que contiene un historial de versiones ejecutadas. Esta herramienta se puede emplear en Windows e MAcs. **[17].**

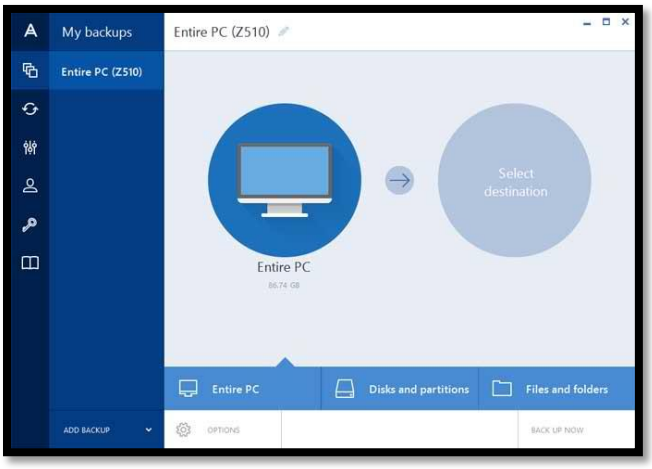


Figura 10. Programa Acronis True.

Fuente. Randy. (2017). Review of Acronis True Image. [Figura]. http://whatsabyte.com/P1/ATI_2015_Review.html

2.8.1.4. Encase

Es una herramienta desarrollada por Guidance Software Inc, es un software que permite colaborarles a los investigadores forenses en busca de pruebas en un hecho criminal. Es utilizada mucho en el campo del análisis forense, y es muy influyente en el mercado nacional o como internacional. Este software ofrece a los investigadores diferentes capacidad de almacenamiento, estudio rápidamente de los documentos que facilita la restauración de los archivos internos del sistemas, concede a los investigadores forenses clasificar las evidencias acorde de los diferentes campos tales como; nombres y firma de los archivos, cuando se creó y su ultimo acceso. Y por último Encase puede reconstruir los sistemas de archivos forenses en los sistemas operativos Windows, Linux y DOS. **[18]**

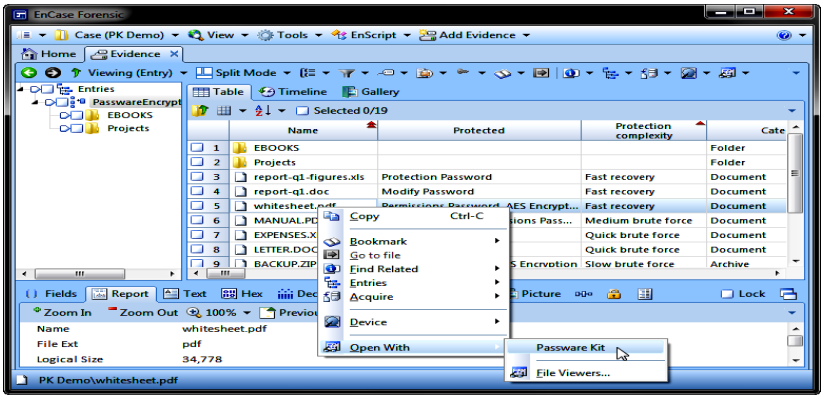


Figura 11. Programa EnCase

Fuente. Passware. (2016). Kit forensic with Encase. [Figura]. http://www.lostpassword.com/encase.htm

Tabla 6. Herramientas usadas en informática forense

PROCESO	SISTEMA OPERATIVO	HERRAMIENTA
ANÁLISIS DE DISCO	**Herramientas basadas en Linux**	LINRes, de NII Consulting Pvt.Ltd.
		SMART, by ASR Data
	Herramientas basadas en Macintosh	Macintosh Forensic Software, de BlackBag Technologies, Inc.
		MacForensicLab, de Subrosasoft
	Herramientas basadas en Windows	BringBack de Tech Assist, Inc.
		EnCase, by Guidance Software
		FBI, by Nuixy Pty Ltd.
		Forensic Toolkit (FTK), de AccessData
		ILook Investigator
		Safeback de NTI & Armor Forensics
		X-ways Forensics
		Prodiscover, de Techpathways
	Herramientas de código abierto	AFFLIB
		Zeitline
		Autopsy
		FOREMOST
		FTimes
		Gfzip
		Gpart
		Magic Rescue
		PyFlag
		Scalpel
		Scrounge-Ntfs
		The sleuth kit
		The coroner's Toolkit (TCT)
EXTRACCIÓN DE META-DATOS	**Herramientas de código abierto**	Antiword
		Catdoc y XLS2CSV
		Jhead
		VINETTO
		Word2x
		W v Ware
		XPDF
		Metadata Assistant
ANÁLISIS DE FICHEROS	**Herramientas de código abierto**	File
		Ldd
		Ltrace

		Strace
		Strings
		Galleta
		Pasco
		Riffiuti
		NetIntercept
		Rkhunter
		Snort
		Tcpextract
		TrueWitness
		Etherpeek
RECUPERACIÓN DE DATOS	**Herramientas de código abierto**	BringBack
		RAID Reconstructor
		Salvation Data
RECUPERACIÓN DE PARTICIONES	**Herramientas de código abierto**	Partition Table Doctor
		Parted
		Active Partition Recovery
		Testdisk

Fuente. Elaboración propia

2.8.1.5. Plainsight

Es una herramienta que permite a los investigadores forenses principiantes desarrollar tareas frecuentemente con aplicaciones de código abierto. Este software puede ejecutar algunas acciones tales como; conseguir los datos en los discos duros, extraer datos de los usuario, observar el historial de los dispositivos de los usuarios, investigar las configuraciones en los cortafuegos del sistema operativos Windows, revela los datos recientemente y los datos guardados en las unidades extraíbles. **[18].**

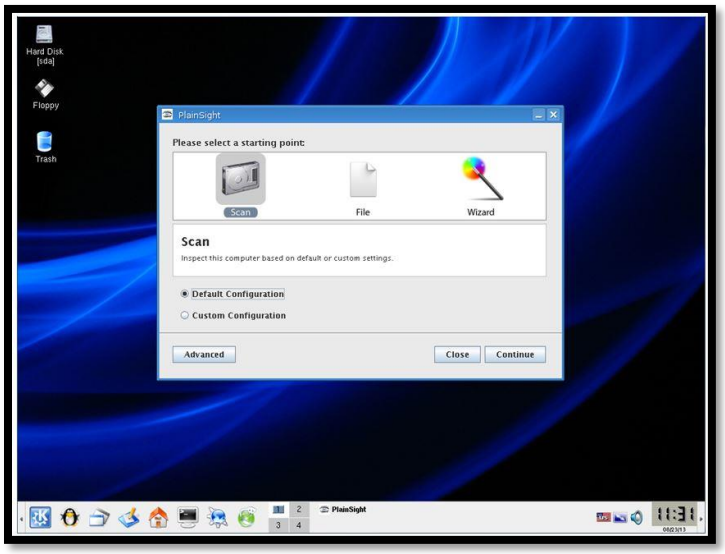


Figura 12. Programa plainsight

Fuente. Andrew Tabona. (2013). PlainSight. [Figura]. https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

2.8.1.6.Bulk Extractor

Este es un software idóneo para examinar las imágenes en los discos, los archivos o directorios de archivos y extraer los datos útiles sin analizar las estructuras de los sistemas de archivos. El resultado de los análisis es sencillamente comprobados, estudiados o verificables con las herramientas mecanizadas. Este software establece histogramas de los resultados que fueron analizados en los discos. El sistema puede usarse en campos de defensa, inteligencia o ciberinvestigaciones. También instaura directorios de salidas tales como: ccn.txt, domain.txt, email.txt, ether.tx, ip.txt, url.txt, zip.txt, entre otros. **[19].**

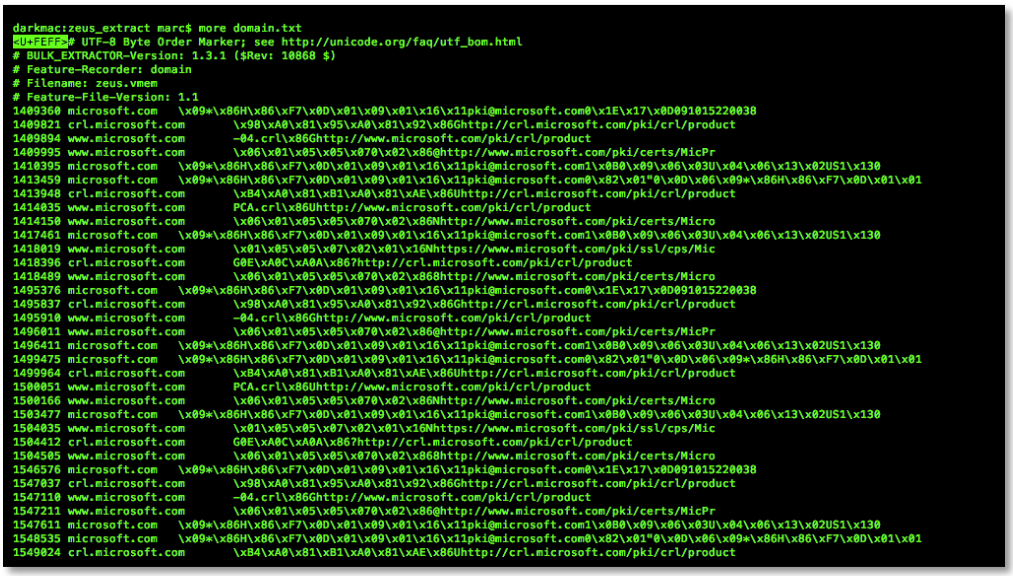


Figura 13. Extrayendo dominios

Fuente. DragonjAR soluciones y seguridad informática S.A.S. (2014). Extrayendo dominios. [Figura]. http://www.dragonjar.org/bulk-extractor.xhtml

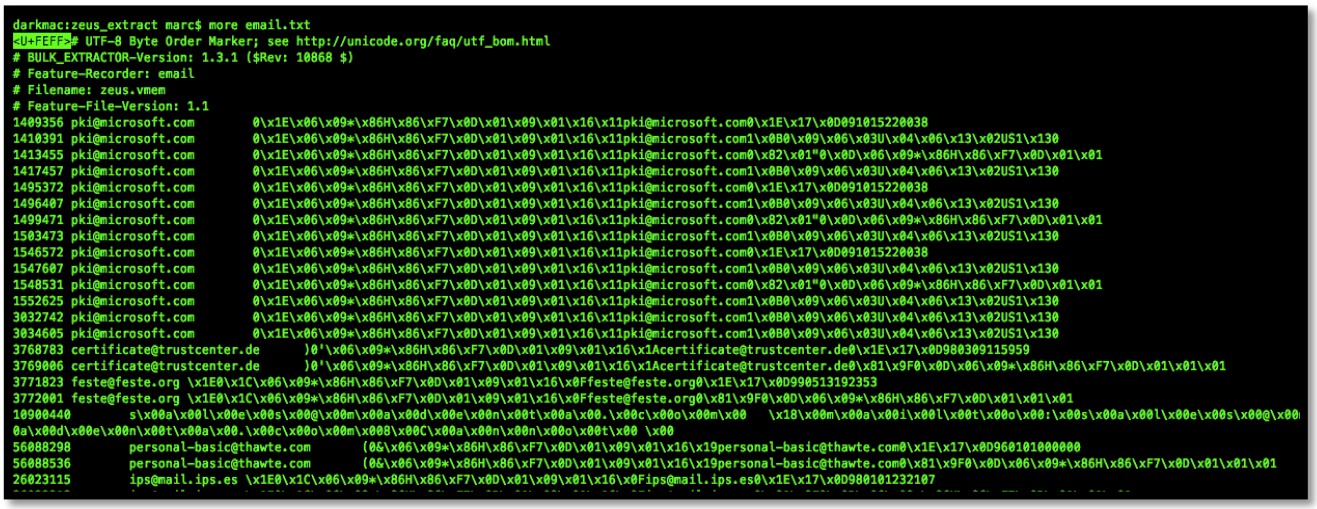


Figura 14. Extrayendo emails

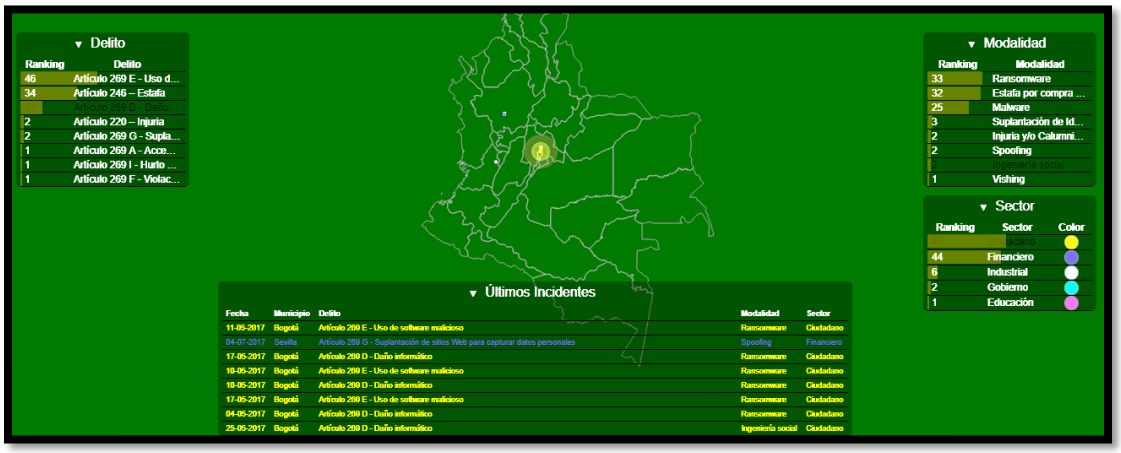
Fuente. DragonjAR soluciones y seguridad informática S.A.S. (2014). Extrayendo emails. [Figura]. http://www.dragonjar.org/bulk-extractor.xhtml

2.9. Marco Conceptual

En el siguiente marco conceptual se definirán cada uno de los elementos que componen el análisis informático forense, sus características, clasificación y papel dentro del proceso desarrollado.

2.9.1. Delitos informáticos

Sin lugar a dudas la importancia que tiene la Internet ha tomado movimientos enormes en los contextos de la sociedad actual por tanto diariamente son innumerables los intercambios comerciales que se ejecutan en las redes, los cambios de datos entre las distintas compañías y miles de comunicaciones en generales, es por esto que la mayoría de las personas ve las redes sociales, las plataformas que se encuentran en internet como un mecanismo fácil de acceso para ejecutar o desarrollar algunos cambios a nivel personal o laboral positivamente, pero asimismo hay personas en cualquier parte del mundo que ve este medio para hacer daños, atentando contra otras personas inocente haciéndoles el mal; generado algunos delitos muy comunes como tales; las estafas, el desfalco en las empresas, las extorsiones, las difamaciones, la pornografía, la explotación sexual tanto en adolescentes como en niños, la infamia, fraudes, falsificaciones de documentos o suplantación de identidades, entre otras.



Figuras 15. Ciberincidentes en Colombia.

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

En la página de la policía nacional en la parte de ciberincidentes las cifras de los crímenes crecen todos los días en nuestro país como 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 sobre estos tipos de delitos y buscar soluciones para generar un entorno sano y tranquilo en nuestro país.

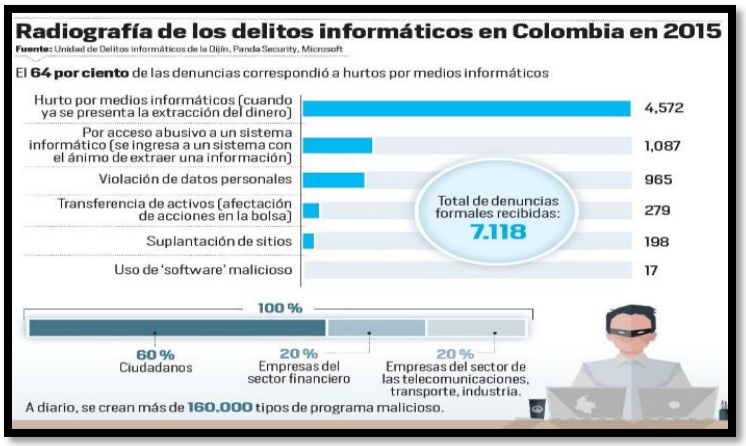


Figura 16. Delitos informáticos aumentaron en Colombia en el año 2015

Fuente. Édgar Medina. (2016). Infografía ETCE. [Figura].
http://www.eltiempo.com/archivo/documento/CMS-16493604

El crimen informático es un acto que produce daños a personas naturales o jurídicas sin que inevitablemente implique una utilidad material para su autor, o que por el contrario genera un rendimiento ilegal para sus autores aun cuando no lastime de forma aledaño a la víctima, según algunos autores el significado de un delito informático es:

Francesco Carnelutti, un delito es el acto típico, antijurídico, culpable, sancionado por una pena, o en su reemplazo, con una medida de seguridad y conforme a las condiciones objetivas de punibilidad. (Libro seguridad de la información por la revista de la segunda cohorte del doctorado en seguridad estratégica, Guatemala, 2014, p, 125).

El mexicano Julio Téllez señala que no es un labor fácil dar un concepto sobre delitos informáticos, es razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión: delitos informáticos este consignada en los códigos penales. (Libro seguridad de la información por la revista de la segunda cohorte del doctorado en seguridad estratégica, Guatemala, 2014, p, 126).

Para Carlos Sarzana, en su obra criminalística y tecnología, los crimines por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena. (Libro seguridad de la información por la revista de la segunda cohorte del doctorado en seguridad estratégica, Guatemala, 2014, p, 126).

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

Figura 17. Mapa ciberdelitos

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. **(Consultada en el informe de amenazas de cibercrimen. (2016-2017), p, 12, en la página de la policía nacional con el siguiente link** https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf**).**

2.9.1.1. Tipos de delitos informáticos

Principalmente hay varias faltas informáticas, 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 modelo es distinguido por el hurto de información, que es muy sencillo y elemental incurrir por las personas encargadas de cometer estos fraudes y es muy complicado de exhibir. Estos fraudes no requiere mucha ciencia ni entendimientos informáticos y cualquier persona puede realizarlos obteniendo registros o archivos de cualquier sistemas.
b) **La manipulación de programas:** Está técnica es bastante complicada de hallar y frecuentemente pasa desapercibida ya que el criminal debe poseer estudios tecnológicos informáticos. Esta falta radica en cambiar los programas verdaderos que se aloja en los sistemas de una computadora o en incluir actuales programas. Este procedimiento o táctica es muy usado por individuos que posee estudios tecnológicos informáticos denominado Trojan Horse, basado en introducir instrucciones en las computadoras de manera oculto o incognito en programas informáticos para que sea capaz de realizar funciones no autorizadas al mismo tiempo que su funcionamiento usual.
c) **Manipulación de los datos de salida:** Usualmente los delitos se hacen frecuentemente por cajeros automáticos mediante los engaños o fraudes de identidad u obtenciones de información. Habitualmente estos delitos se realizaban con tarjetas bancarias hurtadas, sin embargo hoy en día se utilizan equipos y programas de computadoras preparadas o aplicadas para decodificar informaciones electrónicas en las bandas magnéticas de las tarjetas bancarias o de créditos que son usadas mediante transacciones en red o vía internet.
d) **Fraude efectuado por manipulación informática**: Este delito utiliza u obtiene las reproducciones automáticas de los procedimientos en las computadoras. Es un método especializado que se llama sistema del salchichón en la que "rodajas muy finas" ligeramente ostensible, de transacciones financieras, extrayendo incesantemente de una cuenta y se traspasa a otra cuenta sin que la persona lo perciba en seguida.

B. Falsificaciones informáticas.

a) **Como elemento:** Se presenta en el momento en que se intercambian las informaciones acumuladas en los ordenadores electrónicos o digitales.
b) **b) Como herramienta:** En los ordenadores electrónicos o digitales son capaces de utilizar o elaborar alteraciones de datos de tipo comerciales. En el momento en que llego a nuestro país las fotocopiadoras computarizadas en colores realizadas por un rayo láser, surgió ideas para los criminales de delitos informáticos desarrollar o elaborar documentos tales como; billetes, cedulas, pasaportes, tarjetas de identidad, registro civil, licencias de conducciones, entre otros documentos, falsificándolos obteniendo así resultados de buena calidad dificultándoles a los expertos descubrirlos.

C. Daños o modificaciones de programas o datos computarizados.

a) **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.

b) **Acceso no autorizado a servicios y sistemas informáticos:** Esta se genera por diversas razones: desde el sencillo espionaje, como en los acontecimiento 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 diferente 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.

Existen diferentes clases de delitos que son unidos inmediatamente a los hechos o actividades verificadas contra los sistemas, éstos son:

a) **Acceso no autorizado:** Está relacionada con la utilización ilegal de las claves y las entradas a los sistemas informáticos sin el permiso o aprobación del dueño o los propietarios de cualquier entidad pública o privada.
b) **Destrucción de datos:** Se refiere a los perjuicios ocasionados en las redes causados por los virus, bombas lógicas, entre otros.
c) **Infracción al copyright de bases de datos**: Está relacionada con la función no autorizada en una base de datos para obtener informaciones guardadas.

d) **Interceptación de correo electrónico:** Este tipo de delito está relacionado con las lecturas de los correos electrónicos de otras personas, es decir sin la autorización del usuario o propietario.
e) **Estafas electrónicas:** Relacionada por medio de adquisiciones ejecutadas por las redes.
f) **Transferencias de fondos:** Está relacionada con las falsedades o mentiras en las ejecuciones de tareas bancarias electrónicas sin autorización del cliente o usuario.

Las redes nos permiten caer en delitos informáticos tales como:

a) **Espionaje:** Se refiere a la entrada de los accesos no autorizados a un sistema informático de empresas pequeñas, medianas o grandes interceptando los correos electrónicos sin la debida autorización, considerada de tipo ilegal.
b) **Terrorismo:** Generalmente está enmarcada en mensajes anónimos que comúnmente son estudiados por agrupaciones criminales para enviar frases o acciones a nivel internacionales.
c) **Narcotráfico:** Son personas encargadas en la elaboración de estupefacientes, para obtener fácilmente plata o patrimonio. **(Delitos informáticos identificados por la organización de las naciones unidas (ONU), p, 8, por Miguel Garavilla Estrada, 2008)[2].**

2.10. Evidencia digital

Casey, concibe la evidencia de digital como "cualquier dato que puede establecer que un delito se ha realizado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor". "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". (p, 8).

La evidencia digital son pruebas probatorias por los investigadores para llevarlas a un juicio. Hay que tener en cuenta que las informaciones digitales obtenidas no deben ser alteradas de los datos originales encontrados en los discos, lo cual sería invalida la prueba, por eso cada investigador deberá examinar o investigar con mayor repetición las copias para que sean iguales a las del disco del criminal o malicioso, para todo este proceso se maneja varias tecnologías, tales como hash MD5 o checksums. En el momento que ha ocurrido el suceso, frecuentemente, los individuos involucrados en los hechos pretenden adulterar las pruebas, procurando eliminar cualquier huella que pueda dar evidencia del perjuicio causado. De tal modo, este asunto se puede disminuir con varias soluciones que contenga la prueba y que deben tenerse siempre presentes:

- La prueba puede ser copiada de manera puntual y se puede reproducir copias para ser revisada como si fuera la auténtica, lo cual se hace generalmente para proteger los originales e impedir el peligro de destruirlos.

- En la época actual, con los mecanismos presentas, es demasiado útil verificar las evidencias digitales con su original y definir si las evidencias digitales ha sido cambiada o tergiversada.
- Las pruebas son demasiadas complicadas de suprimir, más aún cuando los registros ha sido borrados del disco duro del computador, y este haya sido formateado, es probable rescatarlos para efectuar el respectivo análisis de la información. **[22].**

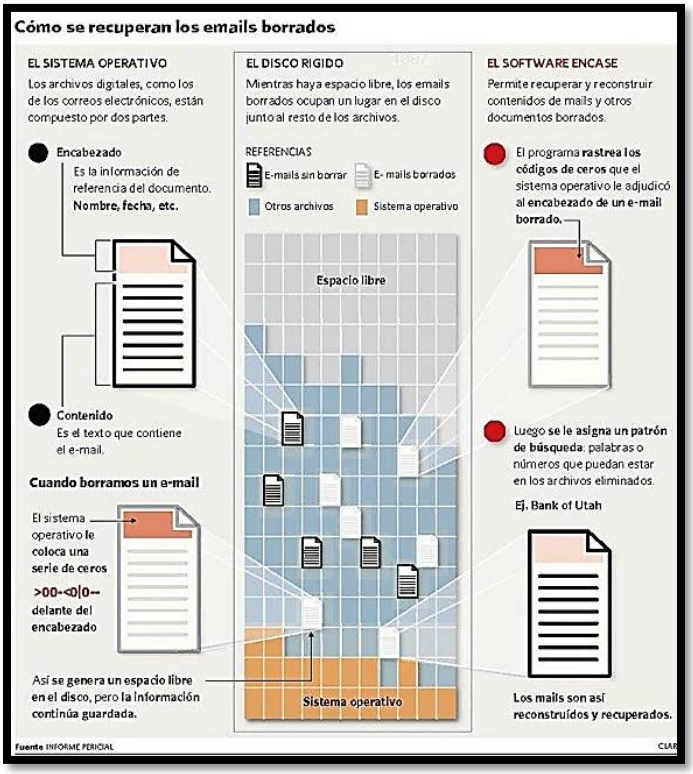


Figura 18. Caso de una evidencia digital

Fuente. Marcelo Romero. (2015). Ejemplo de una evidencia digital. [Figura]. http://romeromarcelo.blogspot.com.co/2015/10/evidencia-digital.html

2.10.1. Tipos de atacantes

Con la introducción de la informática de tipo doméstico, es decir en las viviendas y los procesos tecnológicos, se ha creado una generación de criminales que actúan en las redes o en los sistemas computacionales, cada uno son llamados "piratas informáticos" o "piratas de la Red" la actual invasión de las tecnologías aportando sabiduría, inteligencia, educación, preparación y entre otros, asimismo generando destrucciones en delitos informáticos. Hay que tener en cuenta quien es cada quien y clasificarlos dependiendo de sus acciones de indisciplina en totalidad de los casos. Hasta el momento esta generación, ha sido repartida en cantidades espacios esenciales en las que reposan con fuerza, la teoría de cada uno de

ellos. Todos estos grupos brindan, en gran tamaño algo eficiente en un mundo sometido por las tecnologías, pero esto, no ocurre así. Algunos grupos al margen de la ley, optan por estas decisiones como salida a sus actos ilícitos. **(Proyecto de Harold Miller Buitrago, 2014, p, 64). [23]**

2.10.1.1. Hackers

Los hackers son los primeros grupos de una comunidad "delictiva" conforme los consideran los expertos. Estos individuos son muy agiles en sistemas desarrollados. En la actualidad se concentran en los campos informáticos y de comunicaciones. Manejando a la perfección las programaciones y la electrónica para conseguir y entender sistemas tan difíciles como las comunicaciones móviles. Su fin es conocer los movimientos de los sistemas. Su propósito es acceder a sistemas informáticos, con la intención de dejar un mensaje para que las personas se dé cuenta que ellos estuvieron allí, sin obtener nada de los computadores que atacaron. Esta persona pretende, conocer ante todo los sistemas tanto el hardware como el software. Otro objetivo que persigue es conseguir cambiar los datos para utilizaciones personales o particulares y de averiguar los movimientos frecuente de los sistemas.

2.10.1.2. Crackers

Los crackers son personas atraídos por su talento para destruir sistemas y software dedicándose solamente a craquear sistemas. Técnicamente estas personas son indispensable para legitimar un software sin límites de tiempo y sin tener que pagarle a las empresas desarrolladoras de software su correspondiente licencia. Para las reconocidas empresas dedicadas a la fabricación de sistemas estas personas son perjudiciales para el entorno del software porque siempre destruyen la seguridad. Ellos son expertos en crear y elaborar programas para romper software y comunicaciones tales como los teléfonos, los correos electrónico o el domino de otras computadoras remotas.

2.10.1.3. Copyhackers

Estos son famosos solamente en los terrenos del craqueó de hardware, considerablemente en las tarjetas inteligentes utilizadas en los sistemas de telefonía celular. La gran aspiración de estas personas, es el factor económico, es decir el dinero.

2.10.1.4. Bucaneros

Estos son aún más malos o inferiores que otros atacantes, puesto que no conocen ni identifican las tecnologías, estos personajes solamente buscan los comercios negros de los artículos otorgados por los Copyhackers. Ellos sólo poseen espacio en la parte externa de las redes, llamados "piratas informáticos" porque solo son encargados de los artículos craqueados, normalmente los bucaneros son negociante, no posee autoestima, honorabilidad, ni melindroso al momento de comercializar un artículo craqueado a una altura máxima como generalmente se hace en la época actual.

2.10.1.5. Phreaker

Estos personajes son muy reconocidos en las redes por su entendimiento en las telefonías. Se utiliza para impedir mecanismos de registro en las empresas telefónicas. Facilitando llamadas a cualquier parte del mundo de manera gratis. A veces obstaculiza la posibilidad de

que se pueda averiguar o investigar el recorrido de las llamadas telefónicas desde su comienzo, disminuyendo muchas veces la probabilidad de ser capturados. En fin este personaje para los organismos dedicados a las informáticas, piensa que es un proceso o medio muy eficiente y de utilidad.

2.10.2. Tipos de ataques

Hay diversos métodos o recursos al hacer un ataque, tales como:

2.10.2.1. Ingeniería social

Se refiere a la utilización y uso de los individuos para persuadirlos de que realicen actividades o hechos que habitualmente no desarrollan para que descubra o delate todo lo indispensable para vencer los obstáculo de seguridad. Si el sujeto delictivo posee un estudio capacitado o idóneo, son capaces de estafar o enredar sencillamente a los usuarios que desconoce los conocimientos necesarios de seguridad. Esta estrategia es muy común y practica a la hora de encontrar nombres de usuario con sus respectivas contraseñas. Un ejemplo frecuentemente es cuando llaman o envían un correo electrónico a un usuario en el cual se hacen pasar por administradores de sistemas y con mucha formalidad le piden la contraseña con cualquier pretexto contundente.

2.10.2.2. Trashing (Cartoneo)

Normalmente, las personas apuntan o escriben su usuario y contraseña en una hoja de papel y después, cuando lo memoriza, lo botan al basurero. Este mecanismo por más sencillo que sea es el más usado por los atacantes para conseguir esos datos y lograr entrar a los sistemas. Este mecanismo puede ser físico o lógico.

2.10.2.3. Ataques de monitorización

Este modelo de ataques se lleva a cabo para examinar o estudiar a la personas que van hacer las víctimas y sus respectivos sistemas, con el propósito de fijar sus debilidades.

2.10.2.4. Ataques de autenticación

Generalmente este prototipo de ataques posee el propósito de enredar los sistemas de las víctimas para acceder inmediatamente. Frecuentemente esta trampa se hace apropiándose de las entradas al sistema establecidas por la víctima u obteniendo su nombre de usuario y contraseña que era el objetivo fundamental. **(Por Cristian Borghello 2000-2009). [24]**

PARTE III
Desarrollo de la investigación

CAPÍTULO 3

Delitos informáticos en Colombia

3.1. Marco legal

3.1.1. 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). **(Publicadas en el diario oficial 47.223 de enero 5 de 2009, sancionada por el expresidente Álvaro Uribe Vélez) [25].**

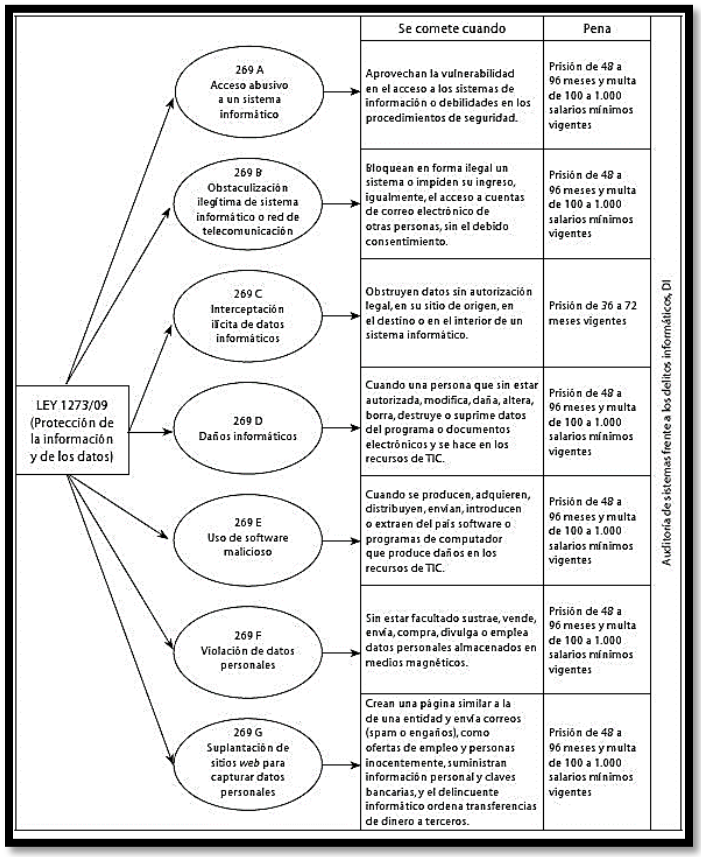


Figura 19. Decretos para proteger los datos parte 1

Fuente. Jorge Eliécer Ojeda, Fernando Rincón, Miguel Eugenio Arias y Libardo Alberto Daza. (2010). Legislación penal colombiana frente a los delitos informáticos (Artículo 1 de la ley 1273 de 2009). [Figura]. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

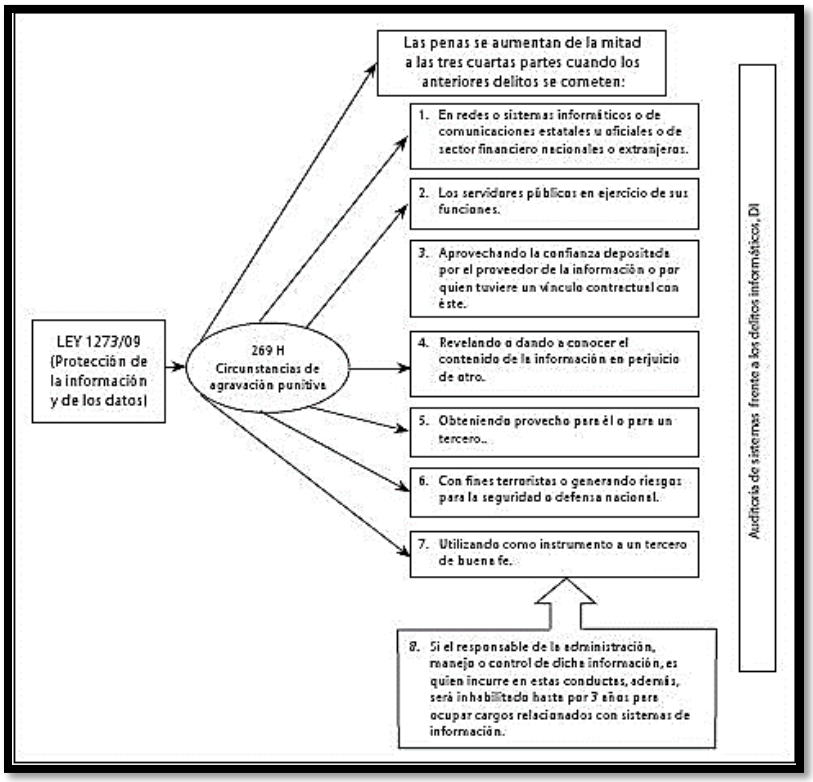


Figura 20. Decretos para proteger los datos parte 2

Fuente. Jorge Eliécer Ojeda, Fernando Rincón, Miguel Eugenio Arias y Libardo Alberto Daza. (2010). Legislación penal colombiana frente a los delitos informáticos (Artículo 1 de la ley 1273 de 2009). [Figura]. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

3.2. Peritaje Informático

Son estudios o búsquedas dirigidas a la adquisición de 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. Los peritajes judiciales son encargados de las investigaciones orientadas a conseguir o lograr evidencias para ser llevadas antes un juicio. En fin los peritajes informáticos son evidencias relacionadas con temas tales como; irregularidades en los correos electrónicos, violaciones en la seguridad, piraterías, ilegalidades en los sistemas informáticos o manejo inapropiados de los dispositivos electrónicos. **[26]**

Figura 21. Etapas de un peritaje informático.

Fuente. Ing. William Gutiérrez Salvador. (2010). Fases de un peritaje informática. [Figura]. https://www.youtube.com/watch?v=XZrkrONlZTY

3.2.1. 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. Su función es exactamente la misma del perito judicial anterior, su misión es recolectar informaciones que este 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. **[27]**

CAPÍTULO 4

Prevención para evitar delitos informáticos

4.1. Ejemplos

4.1.1. Ciberataque mundial impacta a instituciones estatales y privadas en "una dimensión nunca antes vista"

El hackeo generalizado con sistemas de ransomware, con el cual los perpetradores exigen dinero a cambio de liberar el acceso a los datos, cerró las redes informáticas en organizaciones de Europa, América Latina y Asia, es decir en una gran parte de países del mundo.

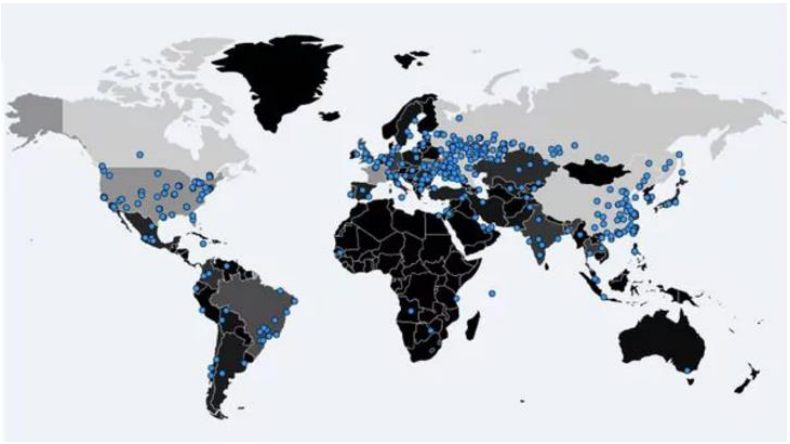


Figura 22. Países afectados por el ciberataque

Fuente. Infobae. (2017). Al menos 74 países resultaron afectados por el ciberataque de este viernes. [Figura]. http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/

Una gran expansión de ciberataques ha afectado actualmente los sistemas e infraestructuras informáticos de por lo menos 74 países, en algunos de los cuales, como el Reino Unido, ha sobrepasado a más de una docena de hospitales y centros médicos. El ataque con software de tipo ransomware, que desarrolla un secuestro de datos y a cambio exige un rescate para salvar el sistema, bloqueó las redes informáticas en instituciones generalizadas a nivel mundial.

Por tanto la infección y la propagación del virus se forman creando una vulnerabilidad del sistema operativo Windows, para el caso de las entidades afectadas, el ransomware que ha infectado el primer equipo ha sido soportado a través de un archivo adjunto descargado para propagar dicho virus.

El virus mencionado es una variante de versiones anteriores de WannaCry**,** que ataca principalmente a sistemas con Windows y que, tras dañar y cifrar los archivos, pide un importe para desbloquear el equipo. El programa Wanna Decryptor es conocido entre los expertos informáticos como un ransomware, una clase de virus informático que puede ocultarse tras enlaces de correo electrónico de apariencia benigna e inofensiva. Ese software codifica los ficheros del ordenador y amenaza con borrarlos si no se paga en pocos días una cantidad en bitcoins, una moneda electrónica, la famosa popularidad en la época actual.

Figura 23. Sistema Ransomware

Fuente. Infobae. (2017). Virus afecta la computadora. [Figura].
http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/

Teniendo en cuenta el personaje Jakub Kroustek, que ha sido considerado como uno de los grandes fuertes en cuanto al manejo de antivirus de la compañía Avast, se han ubicado más de 57.000 hackeos. "Este es una gran amenaza y ataque cibernético relevante, que repercute en las organizaciones de toda Europa en un alcance nunca antes visto", afirmó el experto en seguridad Kevin Beaumont a la cadena **BBC**. Este ciberataque fue "indiscriminado", perjudicó a otros países y es "principalmente virulento", pues mezcla un malware con un sistema de propagación que emplea una vulnerabilidad detectada en Microsoft, afirmó a **EFE** Agustín Muñoz-Grandes, director ejecutivo de S21sec, una empresa española especializada en ciberseguridad.

4.1.2. Virus informático denominado Peyta puso en jaque a varios países europeos.

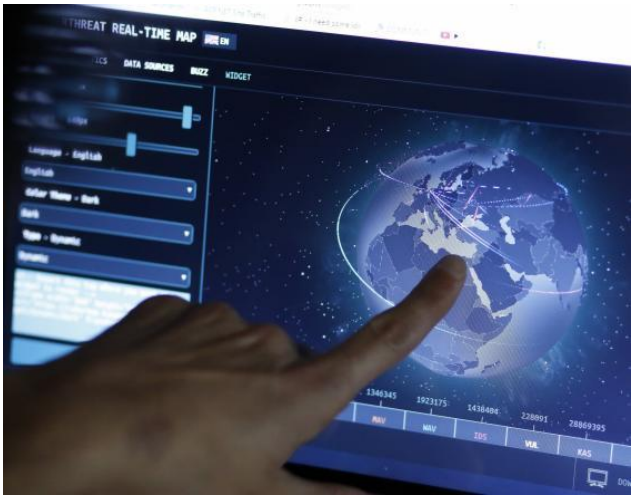


Figura 24. Virus Peyta

Fuente. EFE/ El país. (2017). Este virus informático afecto a centenares de instituciones en varios países del mundo. [Figura]. http://www.elpais.com.co/tecnologia/petya-el-virus-informatico-que-puso-en-jaque-a-varios-paises-europeos.html

El mes pasado ocurrió otro delito información, esta infección informática puso en alerta roja a muchas compañías e organismos europeos, especialmente en los países de Rusia y Ucrania, el ataque fue semejante al del 12 de mayo de este año haciendo inmediatamente daños a millones de personas en el mundo.

Este ataque Peyta es idéntico al ataque Wannacry, en donde cierra o inmoviliza los dispositivos electrónicos, exigiendo pagos de 300 dólares en bitcoines. Este virus se define como un troyano que se propaga o se difunde de manera rápida, similar al ataque anterior.
Muchas empresas de Europa como el banco central de rusa, la compañía petrolera Rosneft, la compañía de danesa maersk, el grupo francés Saint-Gobain, entre otras organizaciones que fueron contagiadas con este virus inmovilizando toda su función a nivel global obtenidas en sus equipos de cómputos.

4.2. Recomendaciones

Actualmente tenemos mucha protección y apoyo por parte de la policía nacional de Colombia que nos comunican por medio de boletines, guías, cartillas o nos ofrece un mapa de rastreo con todas las modalidades de ataques que han surgido en el recorrido de este año mostrando los riegos que hoy en día existen sobre los delitos informáticos y cómo podemos prevenirlos; tales como suplantación de identidades, sexting, estafas por compras en líneas, malaware, injurias y/o calumnia, ransomware, vishing, ingeniera social, entre otras. A continuación veremos algunas recomendaciones que nos ayudara a prevenir estos ataques:

4.2.1. Evitar ataques sexting

Figura 25. Ataque sexting

Fuente. Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). (2016). Sexting. [Figura]. https://caivirtual.policia.gov.co/sites/default/files/bacin_-_001_0_0.pdf

Tabla 7. Recomendación sexitng

1. Prevenir enviar o mostrar fotografías o elementos íntimos a personas extrañas.
2. No conservar las fotografías o elementos íntimos guardándolos en los equipos de cómputo o unidades extraíbles como una USB o discos duros externos, porque debemos ser conscientes de que podemos ser víctimas de jaqueos o hurtos por terceras personas. **(Publicado por la policía nacional, con el siguiente link (**https://caivirtual.policia.gov.co/sites/default/files/bacin_-_001_0_0.pdf**, p, 2, 2016)**

4.2.2. Evitar ataques ransomware

Tabla 8. Recomendación Ransomware

1. Ignorar los correos electrónicos que entran como spam o como asuntos extraños ubicados en las bandeja de entrada.
2. No contestar ningún correo que requiere dar datos personales o financieras.
3. Eliminar rápidamente estos correos ubicados en la bandeja de entrada.
4. Realizar copias de seguridad frecuentemente.
5. Actualizar los antivirus rápidamente cuando el sistema nos de aviso.
6. Mantenernos alejados de páginas extrañas ubicadas en internet. (Publicado por la policía nacional, con el siguiente link **(**https://caivirtual.policia.gov.co/sites/default/files/ransomware_wannacry_0.pdf, **p, 2, 2017)**

4.2.3. Evitar ataques grooming

Figura 26. Ataque grooming

Fuente. Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). (2016). Como evitar un grooming. [Figura]. https://caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf

Tabla 9. Recomendación Grooming

1. Prevenir mandar elementos eróticos o sexuales.
2. No añadir gente extraña a las redes sociales que actualmente utilizan.
3. Si son atacadas por este delito, solicitar auxilio a las autoridades y especialmente a un miembro de la familia que tengan más afinidad.
4. No seguirles el juego o la extorsión. (Publicado por la policía nacional, con el siguiente link **(**https://caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf, **p, 2, 2016)**

PARTE VI
Conclusiones y Bibliografías

CAPÍTULO 5

Conclusiones

- A través de la informática forense, que es considerada como una ciencia, se pueden ejecutar diferentes investigaciones relacionadas con cualquier crimen o delito informático 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 fundamental que los seres humanos conozcan que los peritos de la informática forense son los únicos autorizados para llevar a cabo diferentes investigaciones de los delitos informáticos, puesto que para adquirir las pruebas o evidencias se hace indispensable aplicar los procesos definidos, y usar las estrategias adecuadas para llevar a cabo la investigación, y de igual manera la manipulación de las pruebas o evidencias correctamente para que esta sea válida. En éste sentido fuera de ser una ciencia de investigación de delitos informáticos, la informática forense también colabora con las grandes empresas a determinar si están sujetas a alguna amenaza cibernética, llevándolas a emplear nuevas estrategias y procesos de seguridad, con el objetivo de reducir las amenazas de índole cibernéticos porque pueden representar grandes peligros informáticos.
- Los seres humanos como principales víctimas de estos crímenes o delitos, deben ser conscientes de la necesidad de utilizar métodos de control y de seguridad Informática en sus sistemas domésticos o empresariales para salvaguardar y evitar al máximo padecer las consecuencias de estas acciones consideradas de tipo ilegal.
- En éste sentido la cadena de custodia es una herramienta que nos facilita tener la veracidad de que las pruebas halladas en el lugar de los hechos y las conclusiones a las cuales arriban los peritos, el fiscal, el Juez y las partes; son realizadas dentro de medidas de calidad; siendo muy confiables y fidedignas las conclusiones a las cuales se pueden llegar.
- Las recomendaciones mencionadas en esta investigación es para ayudar a las personas a evitar o prevenir estos delitos y establecer medidas de seguridad para combatir estos crimines ya sea en el campo laboral o en el hogar.
- Es muy necesario dar a conocer acerca de este tema a personas que desconocen o son vulnerables a la hora de navegar por internet descargando videos, música, imágenes o documentes sin saber que puede contener esos contenidos. Es por esto que en esta investigación se pretende dar una descripción acerca de que es informática forense, delitos informáticos, cadena de custodia, tipos de atacantes, tipos de ataques y evidencia digital, para que en la actualidad o en un futuro pueden combatir acerca de estos delitos como: robo, extorsiones, calumnias, sexting, grooming o ataques tipo malaware entre otros delitos.
- Nosotros recomendamos cambiar las contraseñas de las redes sociales o correos electrónicos continuamente, no mandar fotos a nadie así sea familiares, no dar los números telefónicos a nadie, solo a personas que conozca o sea necesario darlo y por ultimo colocar antivirus o cortafuegos que detecte paginas no deseadas para evitar jaqueos o abrir documentos sospechosos.

Bibliografías

[1] Investigación por Luisa Fernanda Castillo y John Bohada [En línea]. Informática forense en Colombia <http://www.revistasjdc.com/main/index.php/rciyt/article/view/413/405> [Consultado el 07 de marzo del 2017]

[2] Documento por Miguel Garavilla [En línea] <https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf> [Consultado el 07 de marzo]

[3] Articulo por Isabella Gandini, Andrés Isaza y Alejando Delgado [En línea] Normas colombianas acerca de violaciones informáticas. <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia> [Consultado el 08 de marzo]

[4] Tesis de grado por Verónica Mamani Saravia (La paz-Bolivia 2015) [En línea] Método forense en redes de telecomunicación para la admisión de evidencia digital en la justicia boliviana. <https://es.slideshare.net/veronicadestelloazul/metodo-informatico-forense > [Consultado el 08 de marzo]

[5] IFUNAD (Jueves, 27 de marzo de 2014) [En línea] Informática forense UNAD. <http://ifunad.blogspot.com.co/2014/03/historia-informatica-forence.html> [Consultado el 08 de marzo]

[6] Informática U.C Guía de estudio (1 de junio de 2016) [En línea] Análisis de informática forense en los estados unidos. <http://primeranofcjpuc.blogspot.com.co/2016/06/analisis-de-informatica-forense-en-los.html> [Consultado el 12 de marzo]

[7] Sus inicios por Heysel García (2015) [En línea] Informática forense.<http://informaforen.blogspot.com.co/2015/09/sus-inicios.html> [Consultado el 12 de marzo]

[8] Trabajo por Colmenares Mendoza Alberto Yesid y Cruz Guzmán Diego. [En línea] Importancia de la informática forense. <http://www.academia.edu/23975452/Informatica_forense> [Consultado el 14 de marzo]

[9] Entrevista a Raymond Orta por Alta densidad Radio [En línea] Informática 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> [Consultado el 14 de marzo]

[10] An Extended Model of Cybercrime Investigations, de Séamus Ó Ciardhuáin, [En línea] International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1.

<https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf> [Consultado el 22 de marzo]

[11] Collective work of all DFRWS attendees (Agosto de 2001, Utica, New Cork) [En línea] Report from the First Digital Forensic Research Workshop (DFRWS). <http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf> [Consultado el 23 de marzo]

[12] An Examination of Digital Forensic Models, de Mark Reith, Clint Carr, Gregg Gunsch [En línea] International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3 <https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf> [Consultado el 24 de marzo]

[13] Tácticas basadas en informática forense (18 de noviembre de 2014) [En línea] Análisis de las evidencias. <https://joselodev.wordpress.com/2014/11/18/analisis-informatica-forense/> [Consultado el 25 de marzo]

[14] Trabajo por María Elena Darahuge y Luis Enrique Arellano González [En línea] Metodología de la inspección ocular en informática forense <http://psicologiajuridica.org/psj181.html> [Consultado el 01 de abril]

[15] Semillero de investigación en Seguridad de la información [En línea] Introducción a la informática forense. <https://siensi.wikispaces.com/INTRODUCCION+A+LA+INFORMATICA+FORENSE> [Consultado el 08 de abril]

[16] Cadena de custodia (17 de mayo de 2015) [En línea] Blog E-portafolio Informática forense. < http://eportafoliojaider.blogspot.com.co/2015/05/informatica-forense.html> [Consultado el 12 de abril]

[17] Proyecto de grado de Alberto José Pedrera Ros (2015) [En línea] Clasificación y estudio de herramientas para periciales informático. < https://riunet.upv.es/bitstream/handle/10251/55775/Memoria.pdf?sequence=1> [Consultado el 12de abril]

[18] Plainsight (2008) [En línea] Aplicación para análisis informático. <http://www.plainsight.info/index.html> [Consultado el 12 de abril]

[19] Bulk extractor (2015) [En línea] Aplicación para análisis informático. < http://www.forensicswiki.org/wiki/Bulk_extractor> [Consultado el 15 de abril]

[20] Área de tecnología e Informática (Instituto educativa Ramón Giraldo Ceballos (Medellín Antioquia, Colombia) [En línea] Delitos informáticos. < http://tecnologiasweb2456.blogspot.com.co/p/delitos-informaticos.html> [Consultado el 22 de abril]

[21] Revista de la segunda cohorte del doctorado en seguridad estratégica, Guatemala, 2014 [En línea] Seguridad de la información. < https://books.google.com.co/books?id=xKkYBgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false> [Consultado el 24 de abril]

[22] Documento por Giovanni Zuccardi y Juan David Gutiérrez (Noviembre de 201) [En línea] Informática forense. < http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf> [Consultado el 24 de abril]

[23] Proyecto de grado de Harold Miller Buitrago López (2014, Pereira) [En línea] Viabilidad de implementación de un laboratorio de informática forense en la ciudad de Pereira. (Página 64) <http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/3653/1/CDMIST92.pdf> [Consultado el 24 de abril].

[24] Seguridad de la información (Copyright @ Cristian Borghello 2000-2009) [En línea] Amenazas lógicas-Tipos de ataques. < http://www.segu-info.com.ar/ataques/tipos.htm > [Consultado el 25 de abril]

[25] Ley 1273 de 2009) [En línea] Decretos de delitos informáticos. < http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [Consultado el 25 de abril]

[26] Evidencias informáticas (2008) [En línea] Peritaje informático <http://www.evidenciasinformaticas.com/index.asp?IdContenido=3> [Consultado el 28 de Abril]

[27] Blog delitos informáticos [En línea] Pericia informática y Deberes del perito informático < http://crimenescyberneticos.blogspot.com.co/p/pericia-informatica.html > [Consultado el 1 de mayo]

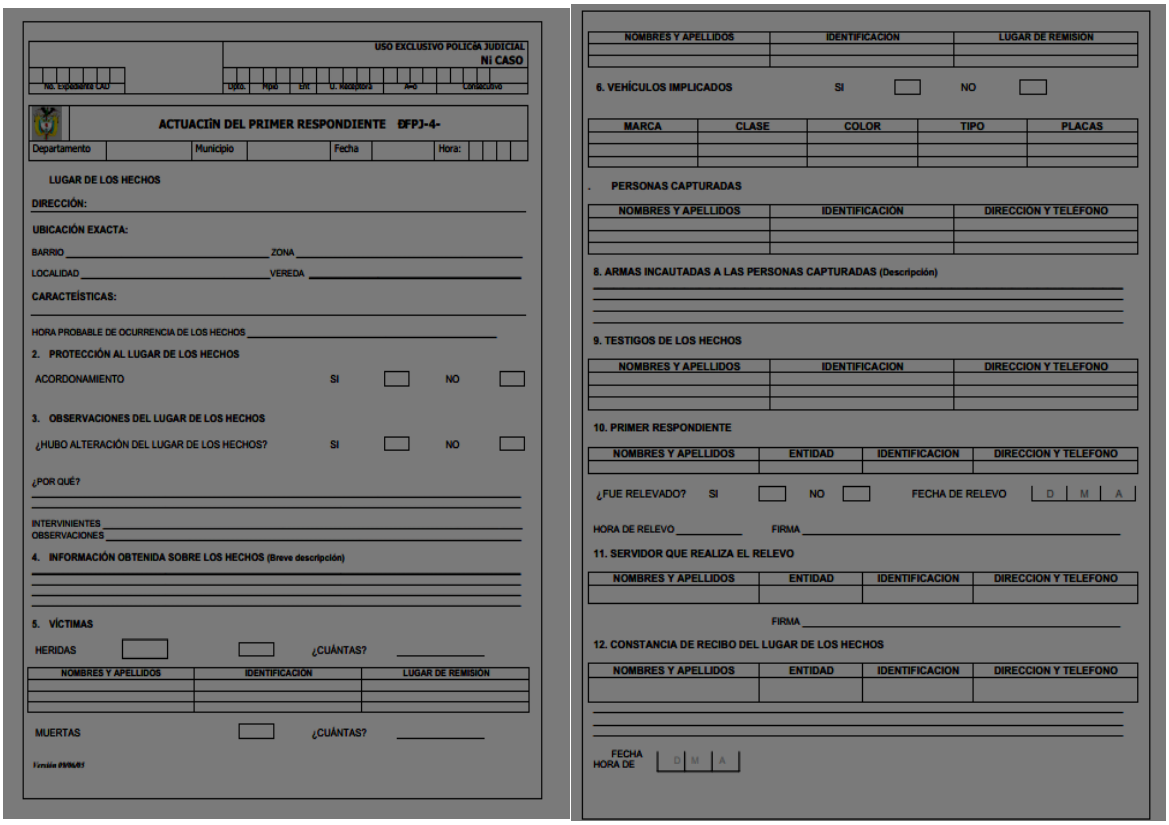
[28] Noticiero infobae (12 de mayo de 2017) [En línea] Ciberataque mundial impacta a instituciones estatales y privadas en “una dimensión nunca antes vista”<http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/ > [Consultado el 12 de mayo]

[29] Periódico virtual el país (27 de junio de 2017) [En línea] Virus petya jaqueo a varios países europeos < http://www.elpais.com.co/tecnologia/petya-el-virus-informatico-que-puso-en-jaque-a-varios-paises-europeos.html > [Consultado el 05 de julio]

PARTE V
Anexos

Anexo A

Formato primer responsable de cadena de custodia 2016



USO EXCLUSIVO POLICÍA JUDICIAL

NI CASO

No. Expediente CAO | Unid. | Rpid | Ent. | U. Receptora | A-S | Consecutivo

ACTUACIÍN DEL PRIMER RESPONDIENTE DFPJ-4-

Departamento | Municipio | Fecha | Hora:

LUGAR DE LOS HECHOS

DIRECCIÓN:

UBICACIÓN EXACTA:

BARRIO ZONA

LOCALIDAD VEREDA

CARACTEÍSTICAS:

HORA PROBABLE DE OCURRENCIA DE LOS HECHOS

2. PROTECCIÓN AL LUGAR DE LOS HECHOS

ACORDONAMIENTO SI NO

3. OBSERVACIONES DEL LUGAR DE LOS HECHOS

¿HUBO ALTERACIÓN DEL LUGAR DE LOS HECHOS? SI NO

¿POR QUÉ?

INTERVINIENTES

OBSERVACIONES

4. INFORMACIÓN OBTENIDA SOBRE LOS HECHOS (Breve descripción)

5. VÍCTIMAS

HERIDAS ¿CUÁNTAS?

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

MUERTAS ¿CUÁNTAS?

Versión 09/06/01

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

6. VEHÍCULOS IMPLICADOS SI NO

MARCA	CLASE	COLOR	TIPO	PLACAS

. PERSONAS CAPTURADAS

NOMBRES Y APELLIDOS	IDENTIFICACION	DIRECCION Y TELEFONO

8. ARMAS INCAUTADAS A LAS PERSONAS CAPTURADAS (Descripción)

9. TESTIGOS DE LOS HECHOS

NOMBRES Y APELLIDOS	IDENTIFICACION	DIRECCION Y TELEFONO

10. PRIMER RESPONDIENTE

NOMBRES Y APELLIDOS	ENTIDAD	IDENTIFICACION	DIRECCION Y TELEFONO

¿FUE RELEVADO? SI NO FECHA DE RELEVO D M A

HORA DE RELEVO FIRMA

11. SERVIDOR QUE REALIZA EL RELEVO

NOMBRES Y APELLIDOS	ENTIDAD	IDENTIFICACION	DIRECCION Y TELEFONO

FIRMA

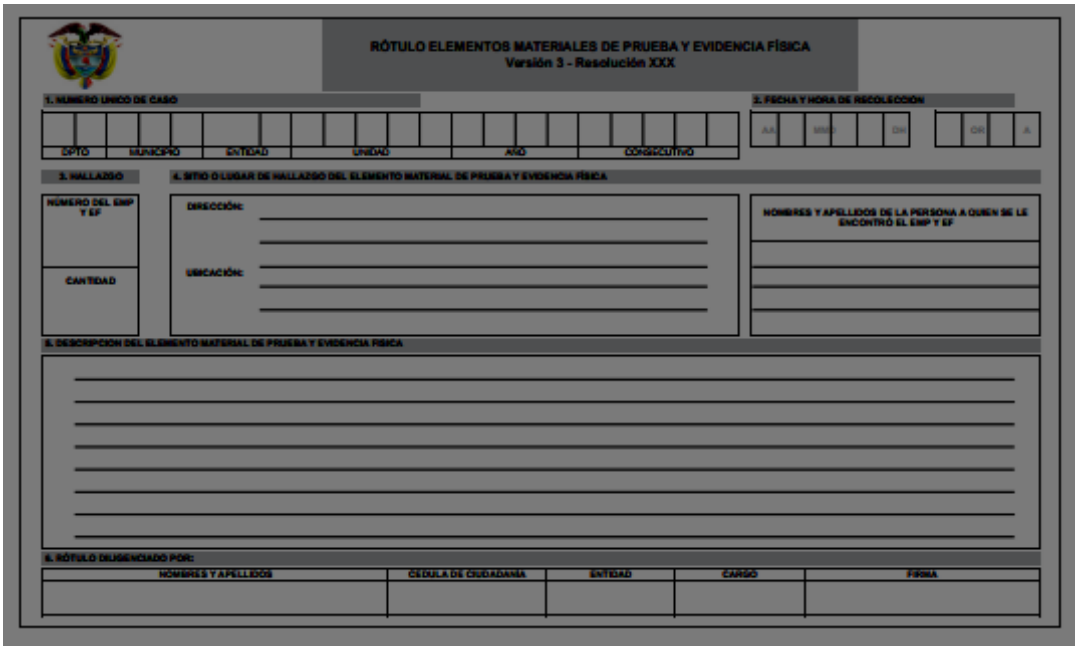
12. CONSTANCIA DE RECIBO DEL LUGAR DE LOS HECHOS

NOMBRES Y APELLIDOS	ENTIDAD	IDENTIFICACION	DIRECCION Y TELEFONO

FECHA HORA DE D M A

Anexo B

Rótulo EMP y EF



RÓTULO ELEMENTOS MATERIALES DE PRUEBA Y EVIDENCIA FÍSICA
Versión 3 - Resolución XXX

1. NUMERO UNICO DE CASO
DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO

2. FECHA Y HORA DE RECOLECCION
AA MM DD HH

3. HALLAZGO

4. SITIO O LUGAR DE HALLAZGO DEL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FÍSICA

NUMERO DEL EMP Y EF

CANTIDAD

DIRECCIÓN:

UBICACIÓN:

NOMBRES Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRÓ EL EMP Y EF

5. DESCRIPCION DEL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FISICA

6. RÓTULO DILIGENCIADO POR:

NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	CARGO	FIRMA

Anexo C

Formato de registro de cadena de custodia

REGISTRO DE CADENA DE CUSTODIA
Versión 2 - Resolución F.G.N.

UBICACION EN LA BODEGA (*)
Numero

1. CODIGO UNICO DE CASO
DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO

2. HISTORIA CLINICA (**)
Numero

3. DOCUMENTACION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

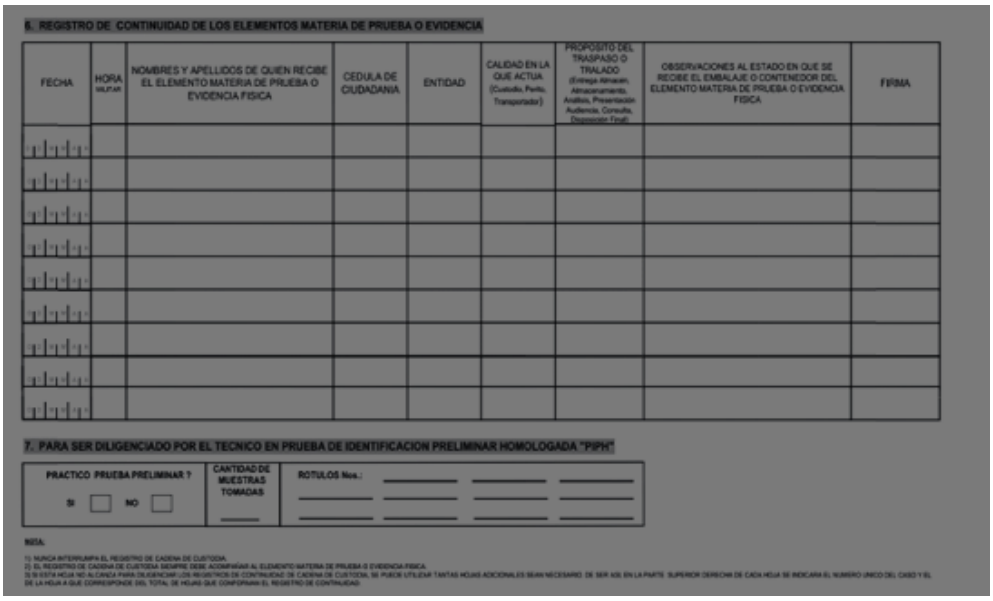
H	R	E	NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	CARGO	FIRMA

4. TIPO DE EMBALAJE

Cantidad	Cantidad	Otro ☐ Cantidad
Bolsa		Cual ?
Plástica ☐ ___	Frasco ☐ ___	_____ ____
De papel ☐ ___	Caja ☐ ___	_____

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

Convenciones:
(*) ...
(**) Para ser diligenciado por la Entidad Prestadora de Salud que recolecta el Elemento Material Probatorio o Evidencia Física
H = Marque con una X si corresponde a quien HALLÓ el Elemento Material de Prueba o Evidencia Física.
R = Marque con una X si corresponde a quien RECOLECTÓ el Elemento Material de Prueba o Evidencia Física.



6. REGISTRO DE CONTINUIDAD DE LOS ELEMENTOS MATERIA DE PRUEBA O EVIDENCIA

FECHA	HORA MILITAR	NOMBRES Y APELLIDOS DE QUIEN RECIBE EL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA	CEDULA DE CIUDADANIA	ENTIDAD	CALIDAD EN LA QUE ACTUA (Custodio, Perito, Transportador)	PROPOSITO DEL TRASPASO O TRALADO (Entrega Almacen, Almacenamiento, Analitico, Presentación Audiencia, Consulta, Disposición Final)	OBSERVACIONES AL ESTADO EN QUE SE RECIBE EL EMBALAJE O CONTENEDOR DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA	FIRMA

7. PARA SER DILIGENCIADO POR EL TECNICO EN PRUEBA DE IDENTIFICACION PRELIMINAR HOMOLOGADA "PIPH"

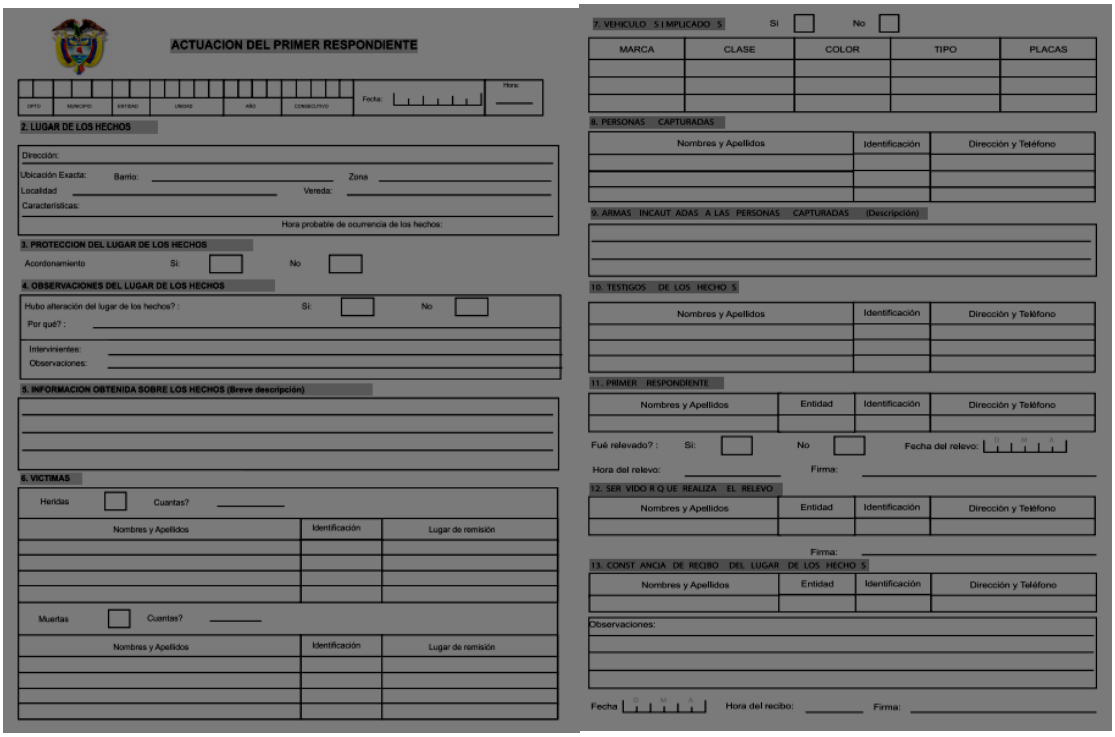
PRACTICO PRUEBA PRELIMINAR ? SI ☐ NO ☐	CANTIDAD DE MUESTRAS TOMADAS	ROTULOS Nos.:

NOTA:

1) NUNCA INTERRUMPA EL REGISTRO DE CADENA DE CUSTODIA.
2) EL REGISTRO DE CADENA DE CUSTODIA SIEMPRE DEBE ACOMPAÑAR AL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA.
3) SI ESTA HOJA NO ALCANZA PARA DILIGENCIAR LOS REGISTROS DE CONTINUIDAD DE CADENA DE CUSTODIA, SE PUEDE UTILIZAR TANTAS HOJAS ADICIONALES SEAN NECESARIO. DE SER ASI, EN LA PARTE SUPERIOR DERECHA DE CADA HOJA SE INDICARA EL NUMERO UNICO DEL CASO Y EL DE LA HOJA A QUE CORRESPONDE DEL TOTAL DE HOJAS QUE CONFORMAN EL REGISTRO DE CONTINUIDAD.

Anexo D

Formato para actuadores del primero respondiente



ACTUACION DEL PRIMER RESPONDIENTE

DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO | Fecha: D M A | Hora:

2. LUGAR DE LOS HECHOS

Dirección:
Ubicación Exacta: Barrio: Zona
Localidad Vereda:
Caracteristicas:
Hora probable de ocurrencia de los hechos:

3. PROTECCION DEL LUGAR DE LOS HECHOS

Acordonamiento Si: ☐ No: ☐

4. OBSERVACIONES DEL LUGAR DE LOS HECHOS

Hubo alteración del lugar de los hechos? : Si: ☐ No: ☐
Por qué? :
Intervinientes:
Observaciones:

5. INFORMACION OBTENIDA SOBRE LOS HECHOS (Breve descripción)

6. VICTIMAS

Heridas ☐ Cuantas?

Nombres y Apellidos	Identificación	Lugar de remisión

Muertas ☐ Cuantas?

Nombres y Apellidos	Identificación	Lugar de remisión

7. VEHICULO S I MPLICADO S Si ☐ No ☐

MARCA	CLASE	COLOR	TIPO	PLACAS

8. PERSONAS CAPTURADAS

Nombres y Apellidos	Identificación	Dirección y Teléfono

9. ARMAS INCAUT ADAS A LAS PERSONAS CAPTURADAS (Descripción)

10. TESTIGOS DE LOS HECHO S

Nombres y Apellidos	Identificación	Dirección y Teléfono

11. PRIMER RESPONDIENTE

Nombres y Apellidos	Entidad	Identificación	Dirección y Teléfono

Fué relevado? : Si: ☐ No ☐ Fecha del relevo: D M A
Hora del relevo: Firma:

12. SER VIDO R Q UE REALIZA EL RELEVO

Nombres y Apellidos	Entidad	Identificación	Dirección y Teléfono

Firma:

13. CONST ANCIA DE RECIBO DEL LUGAR DE LOS HECHO S

Nombres y Apellidos	Entidad	Identificación	Dirección y Teléfono

Observaciones:

Fecha D M A Hora del recibo: Firma: