ALCANCES QUE PUEDE TENER UNA INVESTIGACIÓN FORENSE DENTRO DE UN PROCESO LEGAL EN COLOMBIA

ESTEFANI GUEVARA DÁVILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

ALCANCES QUE PUEDE TENER UNA INVESTIGACIÓN FORENSE DENTRO DE UN PROCESO LEGAL EN COLOMBIA

ESTEFANI GUEVARA DÁVILA

Trabajo
Presentado como requisito para optar al Título de
Especialista en Seguridad Informática

Ing. YOLIMA ESTHER MERCADO PALENCIA
Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

PAGINA DE ACEPTACIÓN

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Presidente del Jurado

_____

Firma del Presidente del Jurado

DEDICATORIA

Dedicado de manera especial a:

Mi mayor motivación para el día a día ha sido primordialmente Dios y la Virgen de Guadalupe que a pesar de las dificultades, los problemas que se presentan no nos abandonan y siempre nos brindan un poco de su ayuda así no la sintamos. Gracias por ser mi guía en mis momentos alegres, tristes, en mis triunfos, debilidades, en mis fracasos y en mis aciertos. Gracias Dios porque este grado es un escalón más que avanzo y que me ayudará a sobresalir en la vida, a estar más cerca de cumplir mis metas y sueños.

A mi esposo por sus palabras y confianza, por su amor, por brindarme el tiempo necesario para realizarme profesionalmente, a mis amigos, compañeros y a todas aquellas personas que de una u otra manera han contribuido para el logro de mis objetivos.

AGRADECIMIENTOS

Agradezco de manera especial a:

Mi agradecimiento se dirige a quien ha forjado mi camino y me ha dirigido por el sendero correcto, a Dios, él que en todo momento está conmigo ayudándome a aprender de mis errores y a no cometerlos otra vez. Eres quien guía el destino de mi vida.

Te lo agradezco, padre Celestial.

TABLA DE CONTENIDO

PÁG.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

1. INTRODUCCIÓN

Los sistemas de computación comenzaron a ser considerablemente utilizados alrededor de los años 90´s dentro de diferentes entornos para los que fueron creados inicialmente, es decir, el uso de este tipo de sistemas no solo se observaban en el campo militar o en los centros de estudios, sino que también en las oficinas de diferentes compañías que ofrecían variedad de productos o servicios. El rápido crecimiento de éstos fue gracias a los sistemas ayudaban a mejorar la calidad y la productividad de sus servicios o productos, pronto pasaron de ser una herramienta de apoyo a un artículo de primera necesidad.

Con el pasar de los años el crecimiento tan abrumador del internet y la misma necesidad de comunicarnos a lo largo y ancho del planeta hizo convertir a los sistemas en un elemento indispensable para el desarrollo de toda empresa. Sin importar de qué tipo de empresa u organización fuese, existiendo un elemento altamente implicado en el desarrollo de estas organizaciones que resulta de vital importancia al igual que los sistemas que contribuyen a este crecimiento: el activo de la información.

El activo de la información es la representación digital de cualquier elemento de información que tenga un valor para una empresa u organización, esta información puede ser tan “irrelevante” como el inventario de bienes muebles o tan “sensibles” como la nómina de la misma. Quien posea la información, posee el poder.

Hay una pequeña relación entre estos dos elementos, los sistemas de cómputo maniobran los activos de información, ya sea generándolos, almacenándolos o transportándolos. La mayoría de las interacciones posibles con los activos de información es a través de dichos sistemas. Infortunadamente los sistemas utilizados no son perfectos, simplemente son perfectibles, es por esto que pérdida o el escape de la información es un riesgo latente dentro de una empresa.

Pueden existir muchas maneras de perder la información, ya sea inconscientemente a través de daños físicos en los equipos, desastres naturales, accidentes, entre otros, o intencionales como el robo, sabotaje, violaciones a la integridad de la información, por mencionar algunos. La pérdida de información se traduce en una pérdida de dinero, hecho intolerable para cualquier tipo de organización.

La implementación de las buenas prácticas con intensión de evitar la pérdida de información por alguna de estas causas puede resultar costosa y compleja según la cantidad de formas o riesgos que se pretendan evitar o disminuir.

Actualmente existen muchas acciones que atentan contra los activos de información de cualquier organización, estas acciones mal intencionadas son realizadas por diferentes personas alrededor del mundo que pueden tener, o no, un objetivo bien definido que los motiva a cometer estos delitos informáticos.

La mayoría de estas acciones son llevadas a cabo por personas mal intencionadas con el fin de obtener un beneficio como puede ser dinero. Éstas pueden conseguir activos de la información de determinada empresa y venderlos al mejor postor, puede obtener datos personales y manipularlos con la idea de ejecutar fraudes, puede inhabilitar parcial o totalmente a las empresas como forma de censura y a su vez usar la infraestructura de una de la misma para realizar estas actividades ilícitas.

Estas actividades o prácticas pueden ser consideras como delitos, según la legislación correspondiente. En Colombia existen leyes que contemplan dichas acciones y establecen sanciones para los infractores, sin embargo aún hace falta trabajo para contemplar toda la gama de actividades malintencionadas que atentan contra los activos informáticos de las empresas. Estas prácticas pueden ser rastreadas para sancionar a los infractores. Para lograrlo es necesario ejecutar las investigaciones oportunas para determinar qué fue lo que aconteció y quién fue el autor.

Para lograr esta tarea, existe una disciplina en los sistemas informáticos que se apodera del estudio de los sistemas para establecer, con base en la información hallada, qué fue lo que sucedió, cómo, cuándo y quién es el posible autor de las acciones que afectaron los activos de información de los sistemas, ésta es llamada informática forense.

Esta es una disciplina compleja que demanda de expertos altamente calificados para ejecutar las investigaciones que sean de interés para una empresa que se haya visto afectada en sus activos de información por algún tipo de actividades malintencionadas o cualquier persona del común que se vea afectada ya sea por robo de datos, suplantación de identidad y demás delitos de los que se pueda ser víctima. Por otra parte es importante recalcar que las evidencias halladas pueden ser primordiales para la resolución de un proceso judicial.

2. TÍTULO DEL PROYECTO

Alcances que puede tener una investigación forense dentro de un proceso legal en Colombia.

2.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad los medios digitales se han constituido como la manera de almacenar la información, lejos quedaron los días donde los documentos oficiales estaban firmados con tinta y papel, en estos días, las firmas electrónicas no sólo son válidas sino obligatorias en muchas transacciones.

De la misma forma las telecomunicaciones o la transmisión de datos de un lado a otro toma cuestión de segundos cuando en otros tiempos podría tardar días, esto ha dado paso a un nuevo campo o rama de la investigación criminal, que consiste en recuperar la información de manera confiable para sustentar un caso legal.

Pero nolo compete a los investigadores legales la recuperación de evidencias, sino también a los encargados de la seguridad en cualquier organización, debe ser de interés saber qué fue lo que paso y cómo pasó un incidente determinado.

La investigación forense en los medios digitales crece día a día, al existir cada vez nuevos dispositivos capaces de transportar información de un lugar a otro, desde teléfonos celulares, memorias portátiles, equipos de sonido o cámaras fotográficas que pueden almacenar no solo fotografías sino datos importantes.

También crece la problemática del investigador al desarrollarse mecanismos de encriptación cada vez más complejos, estos mecanismos son usados por los atacantes o por los criminales como ya se ha presentado en muchos casos en los estados unidos.

Sin embargo quizás el mayor problema que enfrenta un investigador de este tipo es el abismo legal que existe en muchos países, en los cuales no es posible llevar a cabo una persecución criminal de tipo informático, como es el caso de Colombia donde aún quedan muchos asuntos que resolver.

También se debe de mencionar que en la actualidad la investigación forense realiza ingeniería inversa y desempaquetado de archivos ejecutables

encontrados en los equipos vulnerados, estos pueden ser *rootkits*[1] o virus polimórficos, también se han presentado casos en los que se crean túneles de datos ya sea *VPN's*[2] o túneles *Ipv6*[3], que constituyen mayor complejidad debido a que existen pocos analizadores capaces de descifrar de manera correcta este tipo de tráfico.

Es así que surte la necesidad de un especialista informático con conocimientos en tareas de informática forense y criminalística, que logre colaborar con los organismos de justicia, desde la parte informática, como en el área investigativa y finalmente del área forense.

El presente documento pretende ser un iniciador en aquellos que tengan el interés de dedicarse a la investigación criminal informática o que busquen un apoyo completo acerca de cómo realizar su trabajo dentro de una organización.

[1] Conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático.

[2] Tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet

[3] Versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red.

2.2 FORMULACIÓN DEL PROBLEMA

¿Qué alcances puede tener una investigación forense dentro de un proceso legal en Colombia?

Es pertinente realizar el cuestionamiento de cuáles serían los alcances que puede tener una investigación forense dentro de un proceso legal en Colombia, con este interrogante se ha llegado a realizar la presente indagación con el fin de preparar a quienes deseen desempeñarse como peritos forenses para que amplíen el conocimiento con relación a esta área de estudio, a su vez sirva como herramienta de apoyo y de esta manera ayudar de forma correcta con el manejo de las pruebas o evidencias, su estudio, análisis y presentación, de tal forma que se constituya como una base de información y de culturización para tratar asuntos con relación a situaciones delictivas, procesos legales en cuanto a los delitos informáticos se refiere.

3. OBJETIVO DEL PROYECTO

3.1 OBJETIVO GENERAL:

Determinar los alcances que puede tener una investigación forense dentro de un proceso legal en Colombia, mediante la revisión de la normatividad vigente y las herramientas diseñadas para el área de la informática forense, para finalmente, obtener un documento que sirva como base para la adecuada presentación de las pruebas digitales ante las cortes colombianas.

3.2 OBJETIVOS ESPECÍFICOS:

- Indagar como la investigación forense está cambiando la manera de resolver los procesos legales en Colombia.

- Examinar cuales son las herramientas adecuadas para el manejo de un ambiente correcto en un laboratorio forense para realización de imágenes forenses y su respectivo análisis con el fin de asegurar la integridad de la evidencia.

- Presentar un análisis de cómo se lleva a cabo los resultados de una investigación forense de manera clara para que sean válidos y a su vez ser comprendidos tanto como por abogados, jueces y los entes de control.

- Analizar la Ley de delitos informáticos 1273 sancionada en el año 2009 en Colombia con el fin de aplicar estos conceptos dentro de la presente monografía.

4. JUSTIFICACIÓN

En Colombia la justicia busca por medio de la implementación y uso de diferentes instancias y normas jurídicas, disipar los conflictos causados por intereses en pugna con el fin de alcanzar y conservar un orden social en la comunidad de modo que esta rama no podía dejar de lado una nueva área del conocimiento como lo es el avance de la tecnología la cual ha permitido a los seres humanos mediante el uso de diferentes sistemas de comunicación en donde se ven involucrados todo tipo de dispositivos: móviles, de mesa, portátiles de uso alámbricos, inalámbricos, online, offline, etc. Es por ello, que se hace necesario el desarrollo de leyes y demás normas jurídicas, con el fin de regular la comunicación a través de medios tecnológicos, de manera que sea segura, confiable y no sea posible el desarrollo den ningún tipo de abuso o acto delictivo que atente contra en bienestar integral de los ciudadanos.

Debido a la amplia gama de disposiciones legales se desconoce, en la mayoría de los casos, la forma en como el peritaje informático y la evidencia digital, resultado del mismo, tiene lugar dentro de la justicia colombiana; por esta razón, con el fin de definir el estado actual de los alcances que puede tener una investigación forense dentro de un proceso legal en Colombia, se hace necesario la revisión del marco legal para los casos de delitos informáticos en nuestro país. (Policia Nacional Colombia, 2015).

Dado lo anterior se considera que la misma tecnología debe ser el medio o herramienta para crear el ataque o la vía para promover la resolución de los hechos de tipo delictivos. En éste sentido se considera que el estudio de esta ciencia ha logrado que la seguridad informática sea la herramienta que proporciona el contra taque de aquellos malhechores que ejecutan sus movimientos por medio de la informática teniendo en cuenta que aunque los delincuentes siempre dejaran una huella de sus movimientos y es allí cuando el perito informático entra a desempeñar su labor con el fin de dar con las evidencias que pueden resolver un caso.

Una vez terminadas las actividades de investigación se logra presentar un trabajo que muestra en profundidad y de manera exacta la situación actual de los delitos informáticos y su lugar dentro de la justicia en el país, proporcionando una herramienta para todos los interesados en llevar a cabo un proceso de peritaje informático, especialmente, personas particulares o entidades del sector privado, los cuales, debido al temor a generar una mala imagen o desconfianza ante sus clientes, no denuncian los casos de cibercrimen en los que se ven involucrados, con el propósito de que no se haga evidente las falencias que tienen tanto en su infraestructura física como tecnológica o las pérdidas sufridas después del ataque; por tal razón se lleva a cabo esta investigación 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.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

La finalidad del presente documento es el estudio de algunas investigaciones forenses digitales, esto con el fin de realizar el análisis que un investigador forense digital necesita llevar a cabo dentro de un proceso de análisis, la búsqueda detallada y minuciosa para reconstruir el log de acontecimientos que tuvo lugar hasta el momento en que se detectó algún estado comprometedor y de esta manera poder contribuir a dar solución a un proceso legal.

Por lo anterior se realizó el estudio y respectivo análisis a partir de diversas investigaciones previas desde el año 1978 hasta la actualidad 2018, realizadas en diferentes países como España, México, Argentina, Perú, Ecuador y Colombia para llegar a las conclusiones que traen el estudio de un caso forense completo con los más altos estándares de calidad para ejecución de un proceso legal en Colombia teniendo en cuenta la legislación vigente.

Esta monografía se delimita a la parte tecnológica ya que cuando hablamos de los conceptos legales en un proceso judicial como peritos informáticos no tenemos el alcance para dar un juicio o la resolución del mismo ya que para estos están a cargo los jueces de la República de Colombia.

6. METODOLOGÍA

6.1. METODOLOGÍA DOCUMENTAL

La presente monografía está desarrollada bajo una metodología tipo documental la cual es empleada en el momento de iniciar la búsqueda de antecedentes y hace referencia a los alcances que puede tener una investigación forense dentro de un proceso legal en Colombia como objeto de exploración de la información relacionada, básicamente, en documentos fundamentados del eje tratado, así como trabajos de investigación realizados en diferentes países como algunos ensayos, artículos, documentos publicados en revistas especializadas que cumplen con las características demarcadas para adentrarse en el tema investigado.

Gracias a esta metodología, se encontraron muchos aportes para llevar a cabo con los objetivos propuestos para el estudio de delitos informáticos y los procesos legales en el país en el momento de recopilar la información encontrada durante la investigación para llegar al resultado plasmado en este documento.

7. MARCO REFERENCIAL

7.1. MARCO TEÓRICO

La informática forense es una ciencia del área de la computación que ha surgido recientemente debido a la necesidad de entender los acontecimientos ocurridos durante un evento o incidente relacionado con la seguridad informática en el cual ésta ha sido vulnerada por un atacante con el fin de afectar a dicho sistema ya sea modificando , destruyendo, o robando la información, por mencionar algunas acciones que pueden afectar la integridad, confidencialidad o disponibilidad de un sistema, o el conjunto de ellos.

Gracias a esta ciencia de la informática forense es permitido determinar las acciones que fueron realizadas para violentar la seguridad del sistema de información y llegara descubrir la identidad del culpable del ataque, ya sea directa o indirectamente. Esta información es la conclusión de un análisis profundo dentro de los sistemas vulnerados, en donde gracias a la ejecución de las técnicas de investigación forense digital se puede comprobar el comportamiento dentro del sistema afectado, el o los usuarios que ejecutaron el ataque con la finalidad de obtener información confiable y contundente para proceder legalmente en contra del atacante para que reconozca ante la ley por las agresiones realizadas al sistema de información.

De tal modo que la informática forense es a la vez una herramienta altamente especializada dentro de la seguridad, ya que es necesario de conocimientos avanzados sobre sistemas de cómputo y a su vez puede ser aplicada como una herramienta legal que ayuda a la persecución de los delitos cibernéticos. Esta disciplina técnica legal tiene como principal objetivo hallar la mayor evidencia digital que pueda ser usada dentro de un proceso legal como evidencia sólida y contundente para determinar el curso de dicho proceso.

Dicha evidencia digital es consecuencia de un análisis forense, debe ser concisa y verídica, además de que los métodos utilizados para su obtención deben ser repetibles por cualquier persona, con la finalidad de que su veracidad no sea puesta en duda. Por lo tanto, una de las bases fundamentales de esta disciplina técnico-legal es el método científico. (Gaviria Pablo, 2015)

Este método suministra una plataforma bien conocida en todo el mundo que permite lograr el mismo resultado a cualquier persona que siga paso a paso cada una de las instrucciones que conforman a un experimento. Gracias a la estructura de este

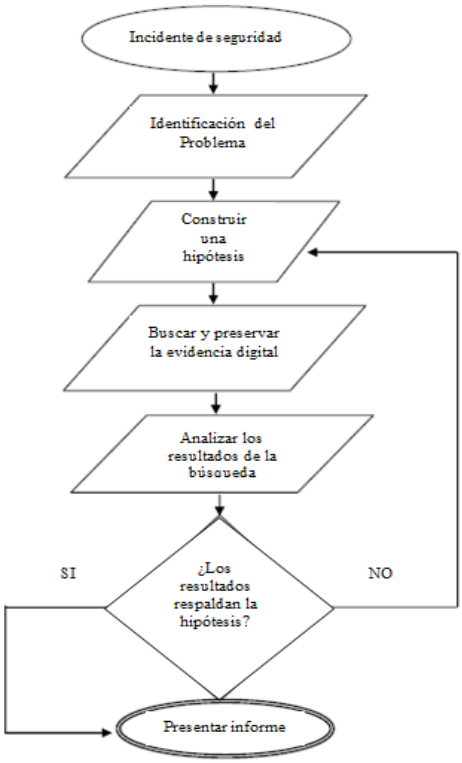
método es posible obtener un experimento repetible por cualquier persona que producirá siempre el mismo resultado teniendo en cuenta los mismos pasos y datos de entrada y se sigan las instrucciones al pie de la letra.

El método científico consiste en seis etapas:

1. Observación
2. Inducción.
3. Hipótesis.
4. Probar la hipótesis por experimentación.
5. Demostración de la hipótesis.
6. Tesis.

El siguiente diagrama de flujo, que aparece en la figura 1, se muestra a grandes rasgos la implementación del método científico en una investigación de informática forense:

Figura 3. Método científico en la investigación forense.



Fuente: PIZARRO., Natalia. Etapas esenciales del método científico para el trabajo digital [imagen]. Aplicación del método científico en estrategias digitales. Chile: 2015 Ideas Digitales Aplicadas SpA. [Consultado: 12 de noviembre de 2018]. Disponible en Internet: https://www.ida.cl/blog/estrategia-digital/metodo-cientifico-trabajo-digital/

En la actualidad no existe una estandarización que dicte los pasos a seguir para llevar a cabo una investigación utilizando la informática forense. A pesar de la falta de estandarización existen varias metodologías de trabajo para realizar una investigación de este tipo:

- La Metodología Forense del Departamento de Justicia de Estados Unidos
- La Metodología Forense del Instituto Nacional de Estándares de Tecnología (NIST)
- La Metodología de Análisis Forense de la Red Europea de institutos Forenses (ENFSI)
- La Metodología de Análisis Forense del Consejo Europeo.

En todas estas metodologías de trabajo es posible identificar similitudes en las acciones que marcan puntualmente para llevar a cabo la investigación. Estas similitudes pueden ser agrupadas en cuatro grandes fases que son: identificación, preservación, análisis, y presentación. Por lo cual se podría determinar que un proceso completo de análisis forense digital conlleva las siguientes fases:

- **Asegurar la escena digital e identificar el bien informático**: Se protege el bien informático para evitar la modificación o destrucción de evidencias digitales, y se identifica su uso dentro de la red, al igual que el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), y la revisión del entorno legal que protege el bien.
- **Capturar y preservar evidencias:** Se realiza una imagen forense (copia exacta) de la evidencia identificada utilizando tecnología de punta para mantener la integridad de la evidencia original y garantizar la cadena de custodia. Asimismo, se documenta detalladamente todos los procedimientos realizados sobre las evidencias y sobre la imagen forense.
- **Analizar evidencias:** Se aplica técnicas científicas y analíticas a la imagen forense para buscar pruebas de delitos. Se puede realizar búsquedas de cadenas de caracteres, acciones específicas de algún usuario (como el uso de dispositivos de USB), archivos específicos, correos electrónicos, últimos sitios visitados, el caché del navegador de Internet, etc.

- **Presentar resultados:** Se recopila toda la información obtenida, se realiza un reporte y se presenta de forma clara y con el formato adecuado a los abogados encargados de la investigación. De ser necesario, se ratifican los informes periciales. (Mattica, 2012)

La prueba pericial hace énfasis en que los hechos constituyen el referente del proceso penal, ya que es precisamente frente a ellos que debe adoptarse una determinada decisión. Es de anotar que ni el fiscal ni el juez tienen conocimiento directo de los hechos, por lo que el primero debe lograrlo mediante evidencias físicas e información legalmente obtenida y el segundo mediante las pruebas practicadas en la audiencia de juicio en desarrollo de los principios de inmediación, contradicción. En los casos en que el asunto penalmente relevante incluye aspectos que superan el conocimiento corriente, puede ser necesaria la intervención de un experto para lograr que el conocimiento de los hechos sea el adecuado. En el ordenamiento jurídico colombiano y en el derecho comparado, se anota lo siguiente sobre el concepto e importancia de la prueba pericial:

> "La prueba pericial es procedente cuando sea necesario efectuar valoraciones que requieran conocimientos científicos, técnicos, artísticos o especializados".

> "La prueba pericial ha sido definida como aquella que se realiza para aportar al proceso las máximas de la experiencia que el juez no posee o no puede poseer y para facilitar la percepción y la apreciación de los hechos concretos objeto del debate".

> "una prueba de auxilio judicial para suplir la ausencia de conocimientos científicos o culturales de los jueces, porque en definitiva, y como medio probatorio, ayuda a constatar la realidad no captable directamente por los sentidos, en manifiesto contraste con la prueba testifical o la de inspección ocular (o reconocimiento judicial)".

> "Cuando conocimiento científico, técnico o especializado sea de ayuda para el juzgador entender la evidencia o determinar un hecho en controversia, un testigo capacitado como perito en relación con la materia sobre la cual va a declarar podrá testificar en forma de opiniones o de otra manera". (Sierra Bedoya, 2008)

7.2. MARCO HISTÓRICO

Historia de la Informática Forense: Para la comprensión adecuada de todo tema es indispensable aclarar y entender los antecedentes históricos relevantes del mismo, por tal razón en los siguientes párrafos se procede a explicar de forma detallada y clara el origen de esta ciencia. Toda la información fue consultada y tomada de dos fuentes de información. En 1978 Florida es el primero en reconocer los delitos en sistemas informáticos en el "*Computer Crimes Act* [4]", los delitos que se reconocieron fueron los siguientes: los casos de sabotaje, *copyright*[5], modificación de datos.

Posteriormente a la viabilidad de uso de los computadores personales para los usuarios, en año de 1980 es cuando con exactitud se dio origen a la Informática Forense y en 1984, el FBI crea un programa llamado en su momento como el Programa de Medios Magnéticos, que ahora es conocido como CART (*Computer Analysis and Response Team*)[6], en español; análisis de la informática y equipo de respuesta. Algún tiempo después aparece el señor Michael Anderson, quien era un agente especial de la División de Investigación Criminal del *IRS* (Departamento de tesorería de los Estados Unidos de América), y es a quien se le conoce como el padre de la Informática Forense y que trabajó hasta mediados del año 1990 con el gobierno, para que después fundara el *New Technologies*. En 1982 el Señor Peter Norton pública UnErase: Norton Utilities 1.0, la primera versión de un conjunto de herramientas dentro de las cuales hay una aplicación que permite la recuperación de archivos que se han borrado, ya sea o no accidentalmente, esta aplicación es conocida como *UnErase*[7]. En 1987 se crea una asociación en Santa Clara para ofrecer cursos e información relacionada al tema y está compuesta por profesionales de empresas privadas y gubernamentales, dicha sociedad se conoce como la High *Tech Crime Investigation Association (HTCIA),* en español Asociación de Investigación de Delitos de Alta Tecnología. En 1987 nace la compañía *AccessData*, principal compañía que ha desarrollado productos que contribuyen a la recuperación de contraseñas y el análisis forense, como lo es la actual *Forensic*

[4] Ley de delitos informáticos

[5] Derechos de autor

[6] Centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

[7] Posibilita rescatar archivos y datos que se borraron del disco duro por equivocación, un virus o un programa incorrecto.

Toolkit[8] *(FTK),* en español Juego de Herramientas Forenses. En 1988 se crea la *International Association of Computer Investigative Specialists (IACIS)*, quien desde entonces certifica a profesionales de agencias gubernamentales en el *Certified Forensic Computer Examiner (CFCE)*, certificado forense para examinador de ordenadores, y esta certificación es una de las más prestigiosas y con más nombre en el ámbito forense. Por otro lado en este mismo año se desarrolla el programa *Seized Computer Evidence Recovery Specialists (SCERS),* quien tiene a su cargo y como el objetivo principal la formación de profesionales en Informática Forense. (Jaramillo Arciniegas & Torres Moncada, 2016, pág. 20)

En 1995 se funda el *International Organization on Computer Evidence (IOCE),* quien tiene como objetivo ser la organización punto de encuentro de los especialistas en la evidencia electrónica. Posteriormente en 1996 la *INTERPOL*[9] organiza los *International Forensic Science Symposium*[10], permitiendo así crear espacios para foros con el fin de debatir los avances forenses y en año de 1998 la *INTERPOL* celebró un simposio sobre Informática Forense al año siguiente, y en 1999, el programa *CART* del FBI abordó 2000 casos sobre delitos informáticos. En el año 2001, crean la *Digital Forensic Research Workshop (DFRWS)*, el cual es un grupo encargado de debate y discusión internacional para compartir información relacionada con la Informática Forense. Presencia del *AFD*[11] en diferentes sectores teniendo en cuenta la importancia que tiene el contenido de la investigación, a continuación se citan algunos de los sectores dentro de los cuales tendría incidencia el AFD Prosecución Criminal: La evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil (*Grooming*). (Jaramillo Arciniegas & Torres Moncada, 2016, pág. 21)

Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la Informática Forense. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial. Mantenimiento de la ley: La Informática Forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva. (Jaramillo Arciniegas & Torres Moncada, 2016, pág. 22)

[8] Herramienta reconocida alrededor del mundo como el estándar en software forense de computadoras.

[9] Organización Internacional de Policía Criminal

[10] Simposio Internacional de Ciencias Forenses

[11] Análisis Forense Digital

A continuación se ilustran otros usos del Análisis Forense Digital, dicha información es tomada de un artículo de la revista Enter.co, según lo referido por Piñeros, G. (2008) Militar y Defensa Nacional: Se usa en actividades de contrainteligencia e inteligencia, protegiendo así la confidencialidad de la información y a su vez identificando los ataques a los cuales están expuestos. Investigación científica: Diferentes organismos académicos lo usan en temas de estudios de seguridad, identificación de amenazas y ataques informáticos. (Jaramillo Arciniegas & Torres Moncada, 2016, pág. 22)

Usuario final: Los usuarios usan diferentes software para encriptar documentos, recuperar archivos, entre otras funciones. Es necesario poner en contexto el tema planteado, por tal razón se deben explicar los principios por los cuales se rige el mundo en la práctica del Análisis Forense Digital. Para ello se tomará como material de referencia la *ISO/IEC 27037*[12]; este estándar internacional es la guía para la identificación, recolección, adquisición y preservación de la evidencia digital; la cual como alcance en materia de análisis incluye: dispositivos de almacenamiento masivo, Smartphone, GPS, sistemas de circuito cerrado de televisión, computadoras, dispositivos con conexión de red basados en protocolo TCP/IP, sin embargo puede ser aplicable a dispositivos con características y funcionalidades similares. (Jaramillo Arciniegas & Torres Moncada, 2016, pág. 22)

La ciencia forense tiene aproximadamente 800 años de experiencia científica, evolucionando en conjunto con la tecnología. Ésta se encarga del tratamiento de evidencias en un delito; desplegándose en diversas ramas de investigación siendo una de ellas la Informática Forense.

En 1978 Florida reconoce los crímenes de sistemas informáticos en el "*Computer Crimes Act*", en casos de sabotaje, copyright, modificación de datos y ataques similares. (Ramos, http://www.securitybydefault.com, 2011).

En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas "*Norton Utilities*"[13], entre las que destacan *UnErase*, una aplicación que permite recuperar archivos borrados accidentalmente. Otras

[12] "Tecnología de la información - Técnicas de seguridad - Pautas para la identificación, recopilación, adquisición y preservación de pruebas digitales" viene a renovar a las ya antiguas directrices RFC 3227 estando las recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales y están más de acorde con el estado de la técnica actual.

[13] Repara los problemas comunes que pueden provocar lentitud en el equipo o, peor, que falle; y lo ayuda a mantenerlo funcionando sin problemas.

aplicaciones también serán útiles desde la perspectiva forense, como *FileFix*[14] o *TimeMark*[15]. Con el éxito de la suite de aplicaciones Peter publica varios libros técnicos, como *Inside the I. B. M. Personal Computer: Access to Advanced Features and Programming*[16], del que su octava edición se publicó en 1999, 11 años después de la primera edición. La compañía será vendida a *Symantec*[17] en 1990. (Ramos, http://www.securitybydefault.com, 2011)

En 1984: El gobierno de EEUU y el FBI ante la reciente problemática criminal en dominios computacionales, iniciaron el "Programa de Medios Magnéticos", que se encargó de examinar evidencia computacional. (Valencia Sambony, 2011)

En 1986 Clifford Stoll colabora en la detección del *hacker*[18] Markus Hess. En 1988 publica el documento Stalking the Wily *Hacker* contando lo ocurrido. Este documento es transformado 1989 en el libro El huevo del cuco, anticipando una metodología forense. (Ramos, http://www.securitybydefault.com, 2011)

En 1988: Un agente del IRS (*Internal Revenue Service*), Michael Anderson, tuvo la iniciativa de armar un grupo de especialistas, lo que posteriormente se convertiría en *Symantec*. Hoy en día es el proveedor líder global de software, dispositivos y servicios para ayudar a personas, así como a pequeñas, medianas y grandes empresas a garantizar la seguridad, la disponibilidad y la integridad de su bien más preciado: la información. (Mamé, 2014)

En 1991: Empezó a operar CART (*Computer Analysis and Response Team*) en los laboratorios del FBI. CART proporciona exámenes de las computadoras y sus discos como un apoyo a las investigaciones y en juicios. (Acevedo González, 2016)

[14] Tipo de archivo EXE asociado a Norton Utilities desarrollado por Symantec para el Sistema Operativo de Windows.
[15] tipo de archivo EXE asociado a Autodesk Mechanical Desktop desarrollado por Autodesk para el Sistema Operativo de Windows.
[16] Examina detalladamente las capacidades de IBM Personal Computer, examina el microprocesador, sistema operativo, programas ROM y software, y también analiza disquetes, gráficos y lenguaje ensamblador.
[17] Corporación multinacional estadounidense que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática.
[18] Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

El libro "*A forensic methodology for countering computer crime*", de P. A. Collier y B. J. Spaul acuña en 1992 el término "*computer forensics*[19]". Otros libros posteriores continuarán desarrollando el termino y la metodología, como: "*High-Technology Crime: Investigating Cases Involving Computers*[20]" de Kenneth S. Rosenblatt. (Ramos, http://www.securitybydefault.com/, 2011)

En 1993-1995: Se formó el IOCE (Organización Internacional en Evidencia Computacional), que brinda un foro para intercambio de ideas sobre seguridad computacional. (Lavin, 2010)

Para marzo de 1998, *the High Tech Crime*[21], un subgrupo del G8, pide al *IOCE*[22] crear una serie de principio, procedimiento y métodos aplicables a las pruebas digitales a nivel mundial siendo fiables en cualquier lugar, esto tomó al *IOCE* dos años. (Castro Guerra, 2014)

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

Así mismo, Pérez y Merino (2008), ratifican la tesis que dan los anteriores autores definiendo la Seguridad Informática como “disciplina que se encarga de proteger los aspectos de confidencialidad, integridad y disponibilidad de la información, la cual esta almacenada en un sistema informático”. Y exponiendo igualmente que “no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema” lo que hace que el *AFD* resulte una técnica indispensable para judicialización de los delincuentes que utilizan el medio informático para realizar sus fechorías y por consiguiente generar soluciones efectivas de protección ante la presencia de la ciberdelincuencia. (Ramos, Martínez, Guasch, & Yago , 2011)

Como referencia, de acuerdo con el *Computer Crimen and Security Survey*[23] 2010/2011 del *Computer Security Institute*[24] (CSI) y el FBI, más del 40% de las empresas sufren incidentes de seguridad informática cada año, y uno de los principales tipos de ataques que sufren es el acceso no autorizado o ingreso sin

[19] Computo Forense
[20] Crimen de alta tecnología: casos de investigación que involucran computadores.
[21] Crimen de alta tecnología
[22] Organización internacional en evidencia de computadores
[23] Encuesta sobre seguridad y delitos informáticos.
[24] Instituto de seguridad informática

privilegios de empleados internos (13%), mientras que la penetración de externos en sistemas corporativos alcanza el 11%. Cabe señalar que la encuesta también indica que 20% de las pérdidas de las empresas podía ser atribuida a empleados internos maliciosos (87.1%) o sin intenciones maliciosas (66.1%). (Velázquez, 2012)

7.3. MARCO CONCEPTUAL

Para la investigación de la informática forense se deben tener en cuenta los siguientes conceptos básicos claros:

> En el mundo de los investigadores forenses digitales, no son los cabellos las pruebas que arrojarán luz sobre la escena del crimen: son los datos de modificación de un documento, los metadatos, los registros de acceso, las direcciones IP o los correos electrónicos lo que ayudará a encontrar y procesar a los delincuentes.
>
> Al igual que su contraparte en el mundo físico, el forense digital buscará identificar, recolectar, preservar, analizar y presentar evidencia que sea válida dentro de un proceso legal, sólo que en su caso será rescatada de un ámbito computacional. Para mantener la integridad de la evidencia forense digital, el investigador deberá utilizar sistemas con tecnología de punta y tener conocimientos avanzados en informática que le permitan analizar cuidadosamente su “escena del crimen” digital. Los conocimientos no sólo deben ser en informática, sino y de manera determinante en el manejo del Sistema de Cadena de Custodia.
>
> Si bien aún no es generalizado el uso de evidencias digitales en procesos judiciales, sí ha aumentado en los últimos años, a medida que la legislación y los propios tribunales y jueces han ido aceptando este tipo de pruebas en procedimientos laborales, civiles y penales. Sin embargo, la “novedad” de las pruebas digitales requiere un cuidado aún mayor en las técnicas de investigación forense digital.
>
> Las evidencias digitales son todos aquellos datos e información almacenados o transmitidos en formato electrónico que pueden tener valor probatorio en un procedimiento legal. Correos electrónicos, documentos, fotografías digitales,

archivos de video o audio, *logs*[25] de eventos o históricos son algunos ejemplos de lo que podría ser evidencias digitales.

La evidencia forense digital puede ser recuperada desde cualquier dispositivo que tenga una memoria informática. Es decir: discos duros de computadores y servidores, cintas de respaldo, dispositivos móviles (celulares, tabletas, agendas electrónicas), tarjetas de memoria, GPS, impresoras, memorias USB e incluso credenciales de autentificación, logs de seguridad y trazo de paquetes de red. Cabe señalar que en algunos casos un investigador forense digital puede llegar a recuperar información que haya sido borrada desde el sistema operativo. (Velázquez, 2012)

7.4. MARCO LEGAL

La Informática forense permite la solución de problemas íntimamente ligados con seguridad informática y la protección de datos. Basados en ella, las diferentes empresas obtienen una respuesta oportuna para sobreponerse a los delitos informáticos consagrados en la ley tanto nacional como internacional; algunos de ellos son: de privacidad, robo de identidad, acceso no autorizado a cuentas de email o redes sociales, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información, algunas de ellas al alcance de todos aquellos inescrupulosos y aún peor, muchas veces sin necesidad de ostentar muchos conocimientos, (herramientas shareware y/o *freeware*[26] no cuantificadas en la red de redes, las cuales permiten desde enseñanzas de cómo ejecutar un ataque por medio de la ingeniería social hasta ataques mucho más elaborados).

Mediante procedimientos que identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente en diferentes medios de almacenamiento de información como por ejemplo: discos duros los cuales presentan una dificultad inherente a las nuevas tecnologías desarrolladas como es la gran cantidad de información que podemos hoy en día guardar en estos dispositivos, USB, etc.; para que puedan ser aceptadas en un proceso legal como la Ley 1273 de 2009 la cual creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes, el 5 de enero de 2009, el Congreso de la República de Colombia promulgó

[25] Registros
[26] software que está disponible de forma gratuita

la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo y en nuestro país en gran parte del territorio nacional.

Anualmente se pierden en Colombia más de 6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado “De la Protección de la información y de los datos” que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.). (MinTic, 2009).

7.5. MARCO DE ANTECEDENTES

Para el desarrollo de la presente investigación monográfica se referenciará un caso en el cual se puede observar la importancia de la evidencia digital y como una investigación forense puede ser la estrategia para dar la resolución de un proceso legal, teniendo en cuenta la legislación española en cuanto a delitos informáticos que es una de las más avanzadas a nivel internacional.

> “*Dos años y medio de cárcel para un joven que instaló un sistema espía en el móvil de su pareja.*
>
> *El Juzgado de lo Penal número 4 de Jaén ha condenado a dos años y medio de prisión a un joven de 23 años, J.F.J., además del pago de una multa de 1.620 euros, por instalar un sistema espía en el móvil de su pareja sin que esta tuviera conocimiento de ello.*

Según recoge como hechos probados la sentencia a la que ha accedido Europa Press, el acusado mediante este sistema obtenía "acceso a las conversaciones telefónicas de la misma, que grababa el contenido de sus mensajes de correo electrónico y WhatsApp, fotografías, ubicación, contraseñas, claves bancarias, pudiendo efectuar fotografías desde el teléfono de ella y verla a través de las cámaras del aparato".

La condena es por un delito de revelación de secreto con la agravante de parentesco ya que la jueza considera que la prueba practicada en el juicio celebrado el pasado 4 de septiembre es "suficientemente clara, sólida y consistente" para considerar "incuestionable el ánimo subjetivo del acusado de descubrir los secretos" de su entonces pareja.

A la hora de establecer la agravante de parentesco, la jueza la argumenta que no ha quedado acreditado que la intención del acusado fuera la de proteger a su pareja de una amenaza externa.

De hecho, durante el juicio, J.F.J. aseguró en su declaración que lo hizo por "sobreprotegerla" ya que "tenía miedo de que le pasara algo" puesto que, según su versión, la joven estaba recibiendo "amenazas de violación y muerte" y "ella no quería denunciar por miedo".

La sentencia establece que el acusado instaló el sistema espía sin advertirle de ello a su pareja "para conseguir su propósito de saber siempre dónde estaba, conocer sus actividades y sus conversaciones". Una vez instalado le entregó el móvil para su uso. Según declaró la joven en el juicio fue un regalo.

Control absoluto

Tal fue la situación de control que la chica llegó a sospechar de que en todo momento el acusado conociera cada uno de sus pasos y finalmente, en julio de 2015, se dio cuenta de que tenía instalado un sistema espía en el móvil y optó por acabar con sus nueve meses de relación sentimental e interponer la correspondiente denuncia en la Policía Nacional.

La sentencia, que absuelve a J.F.J., de tres delitos de coacciones y una falta de vejaciones injustas por los que también acusaba inicialmente el Ministerio Público, establece también en su condena tres años de alejamiento y de prohibición de comunicación con la víctima por cualquier medio. Además, el joven deberá hacer frente a una quinta parte de las costas procesales.

La joven víctima declaró en el juicio que se enteró por una pareja de amigos que tenía el móvil 'pinchado' ya que el acusado se le comentó a uno de ellos.

La pena impuesta conlleva el ingreso en prisión de este joven que carece de antecedentes penales. La sentencia no es firme y cabe recurso de apelación ante la Audiencia de Jaén." (m.20minutos, 2017)

8. HERRAMIENTAS ADECUADAS PARA REALIZACIÓN DE IMÁGENES FORENSES

Dentro de los objetivos establecidos en esta monografía tenemos el estudio de las herramientas más utilizadas y las más comunes dentro de los análisis forenses informático. Durante las etapas de una investigación forense, es fundamental contar con dichas herramientas para la extracción de la información necesaria en cada caso.

En algunas ocasiones las herramientas provistas por los sistemas operativos pueden llegar a ser muy útiles. También es indispensable el tener un ToolKit propio ya que es fundamental que las herramientas utilizadas no modifiquen la evidencia digital, por lo cual se mencionará lista de utilidades que seguramente deberán incluirse en un *ToolKit*[27] para realizar las siguientes tareas:

- Interpretar comandos en modo consola (*cmd, bash*)
- Enumerar puertos *TCP*[28] y *UDP*[29] abiertos y sus aplicaciones asociadas (*fport, lsoft*)
- Listar usuarios conectados local y remotamente al sistema
- Obtener fecha y hora del sistema (date, time)
- Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (*ps, pslist*)[30]
- Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas
- MAC con dichas IP (*ipconfig, arp, netstat, net*)[31]
- Buscar ficheros ocultos o borrados (*hfind, unrm, lazarus*)[32]

[27] Conjunto de herramientas diseñadas para ser utilizadas juntas o para un propósito particular. Software diseñado para realizar una función específica, especialmente para resolver un problema, kit de herramientas.
[28] Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP
[29] Protocolo del nivel de transporte basado en el intercambio de datagramas
[30] Comando que muestra información detallada acerca de procesos en ejecución
[31] Comando de red en sistema operativo Windows
[32] Comando de búsqueda

- Visualizar registros y logs del sistema (*reg, dumpel*)[33]
- Visualizar la configuración de seguridad del sistema (*auditpo*l)[34]
- Generar funciones hash de ficheros (*sah1sum, md5sum*)[35]
- Leer, copiar y escribir a través de la red (*netcat, crypcat*)[36]
- Realizar copias bit-a-bit de discos duros y particiones (*dd, safeback*)[37]
- Analizar el tráfico de red (*tcpdump, windump*)[38]

Según el sistema operativo que se esté examinando es posible indagar diversos subsistemas del mismo y extraer información relevante para el caso. En Windows puede ser útil el uso de herramientas administrativas como el Visor de Suceso, el de Servicios o el de Directivas de Seguridad Local. El registro de Windows accesible mediante la herramienta regedit.exe puede ser de gran utilidad.

En cuanto a Linux, existen una gran cantidad de archivos de log con información extremadamente útil que se puede encontrar en las siguientes rutas: /var/log/messages, /var/log/secure, /var/log/wmtp, /var/run/utmp, /var/log/btmp.

Este tipo de herramientas es muy útiles a la hora de analizar manualmente los sistemas para el hallazgo de evidencias, las herramientas que son utilizadas por los atacantes son cada vez más eficaces. Por lo cual es necesario contar con un conjunto concreto de herramientas para el análisis forense.

Comercialmente existen herramientas como es *EnCase de Guidance* Software el cual es considerado un estándar en el análisis forense de sistemas. Por otra parte también se pueden encontrar herramientas de código abierto creadas con este propósito. Algunas de ellas son:

[33] Comando de visualización
[34] Comando auditoria del sistema
[35] Tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija.
[36] Netcat es una herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST
[37] Comando de copiado bit a bit
[38] Comando para el análisis del tráfico de red

8.1.1 ***Forensic Toolkit***: Es una recopilación de herramientas forenses para plataformas Windows. Algunas de las funcionalidades proporcionadas son: búsqueda de archivos por tiempo de acceso, búsqueda de archivos ocultos en el sistema operativo, búsqueda de archivos ocultos en el disco duro, metadata de archivos, información de usuarios, recursos compartidos y servicios.

8.1.2 ***Sleuth Kit & Autopsy***: Es una recopilación muy poderosa de varias herramientas forenses para entornos UNIX/Linux creada por Brian Carrier, que incluye algunas partes del *ToolKit TCT* (*The Coroner's ToolKit*) de Dan Farmer. Algunas de las funcionalidades proporcionadas son: análisis de archivos, búsqueda por palabra clave, búsqueda por tipo de archivo, detalles de la imagen recolectada, visualización de metadatos, análisis de contenidos reales de archivos.

8.1.3 ***F.I.R.E. Linux*****:** Se trata de otro live CD de arranque que ofrece un entorno de respuesta ante incidentes y análisis forense basada en una distribución Linux con una serie de utilidades de seguridad adicionales. Algunas de las funcionalidades equipadas por esta distribución son: recuperación de datos de particiones dañadas, recolección de datos y análisis forense, tests de penetración y vulnerabilidades, chequeo de virus o malware.

8.1.4 ***Helix CD***: esta herramienta trata de un Live CD que da respuesta ante incidentes, basada en noppix (Debian). Posee un gran número de las herramientas necesarias para realizar un análisis forense tanto en imágenes de discos como en equipos. Proporciona dos modos de funcionamiento (MS Windows y Linux). El modo Linux provee un sistema operativo completo, posee un núcleo con excelente soporte de hardware y realiza montajes de discos del equipo anfitrión en modo solo lectura. Posee además de los comandos propios de Linux, una lista de *ToolKits* incluyendo *Sleuth Kit & Autopsy*.[39]

8.1.5 ***Volatility Framework***: Este *framework*[40], provee una colección de herramientas implementadas en Python que permiten extraer evidencia digital volátil a partir de imágenes de memoria RAM. El *framework* está

[39] Software forense

[40] Estructura real o conceptual destinada a servir de soporte o guía para la construcción de algo que expande la estructura en algo útil.

orientado a introducir a entusiastas en las técnicas de extracción de evidencia digital de imágenes pre-capturadas de memoria volátil y establece una plataforma de estudio en relación a esta área. El *framework r*equiere Python para ser ejecutado y necesita como insumo una imagen pre-capturada. Los autores proveen algunas capturas en un compendio de aproximadamente 500MB.

8.1.6 ***BackTrack*:** Esta es otra distribución GNU/Linux en formato Live-CD, la distribución está diseñada y pensada para la auditoría de seguridad y relacionada con la seguridad informática en general. Incorpora una gran variedad de herramientas y es muy conocido dentro del ámbito forense. De hecho, la última liberación de *BackTrack*, provee un modo "forense"' en el cual se asegura que las actividades realizadas sobre el equipo comprometido no generan cambios en los discos subyacentes

8.1.7 ***Live Response USB Key***: Este producto, creado por la compañía e-fense, la misma de Helix CD, se distribuye comercialmente como una unidad flash USB la cual contiene una aplicación orientada a la recolección de información volátil en plataformas Windows. Para utilizar la aplicación, ésta debe ser instalada en el sistema del equipo víctima; es decir, no se ejecuta directamente desde la unidad USB. Luego que ha sido instalada, la herramienta permite seleccionar que recursos volátiles se desean recolectar a partir de un conjunto de recursos predefinidos y permite generar reportes en base a los resultados obtenidos.

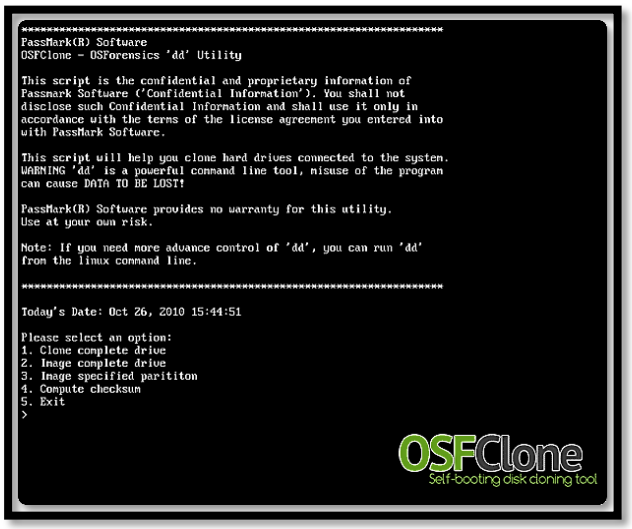
8.1.8 ***Live Response***: Provee un conjunto de utilidades que permiten recolectar y analizar información volátil asociada al estado de un sistema Windows luego de que ha ocurrido un incidente. La aplicación se distribuye como un archivo ejecutable y se encuentra en su versión 0.0.1, liberada en julio de 2007.

8.1.9 ***OSFClone***: En la figura 2 se observa la herramienta que 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*)[41], este formato es abierto y desplegable para conservar o asegurar imágenes de discos asociados que sirve para que los

[41] Formato forense anticipado

investigadores analicen eficientemente los datos para llevarlos a cabo un estudio forense.

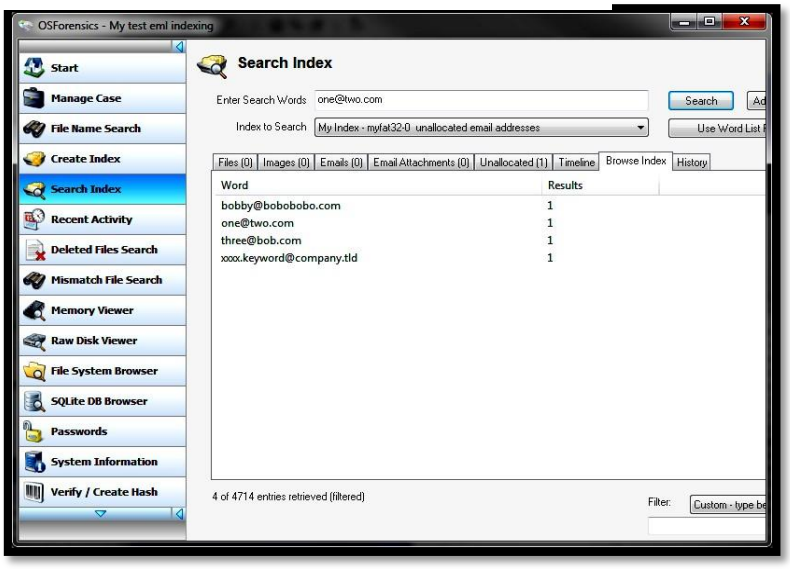
Figura 4. OSF Clone.



Fuente: PassMark® Software Pty Ltd**.** OSForensics, Digital Investigation for a new era [Consultado: 12 de noviembre de 2017]. Disponible en internet: https://www.osforensics.com/tools/create-disk-images.html

8.1.10 OSFClone: En la imagen 3, se puede observar cómo se realiza un escaneo del problema, 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 5. Escaneo del problema OSFClone.



Fuente: Ray PassMark., "Browse Index" shows a list of all the e-mail addresses that I expected. They're all intact and searchable. [Imagen]. [Consultado: 10 de noviembre de 2017]. Disponible en Internet: 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.

8.1.11 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. Ver imagen 4. (Ros Pedrera, 2005)

Figura 6. Programa drive clone.

Fuente: Drive Clone 2009 free download, Brothersoft Windows. (2009). Drive Clone 2009. [Imagen]. [Consultado: 20 de noviembre de 2017]. Disponible en Internet: http://www.brothersoft.com/drive- clone-207813.html

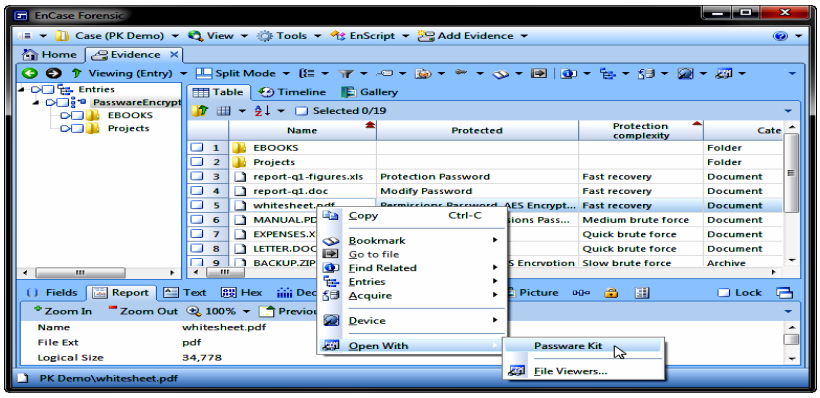
8.1.12 *Acronis True* Image: En la imagen 5 se puede observar la aplicación de pago, que sirve para ejecutar copias de seguridad de imágenes completas y rescatar algunas partes de un sistemas tales como: música, fotografías, videos, documentos o configuraciones personales. Es una herramienta que puede 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. (Ros Pedrera, 2005).

Figura 7. Programa Acronis True.

Fuente: Randy. (2017). Review of Acronis True Image. [Imagen]. [Consultado: 21 de noviembre de 2017]. Disponible en Internet: http://whatsabyte.com/P1/ATI_2015_Review.html

8.1.13 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, ver figura 6. 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. (Plainsight, 2008).

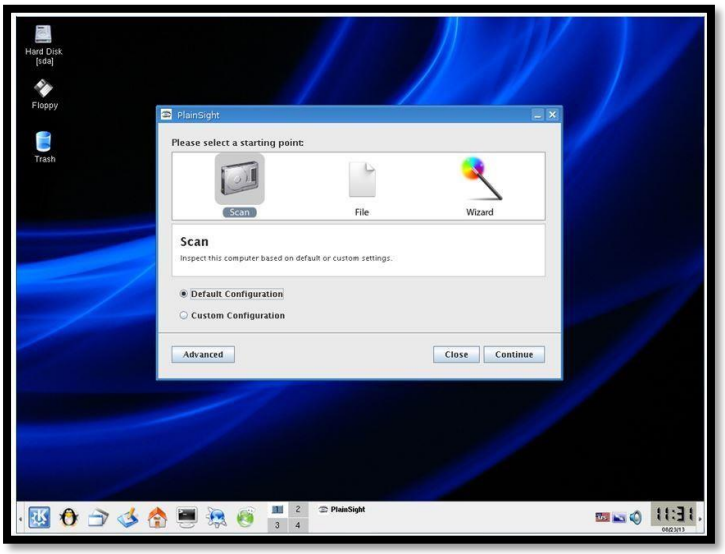
Figura 8. Programa EnCase.



Fuente: Passware. (2016). Kit forensic with Encase. [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet: http://www.lostpassword.com/encase.htm

8.1.14 Plainsight: En la figura 7 se observa la 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. (Plainsight, 2008).

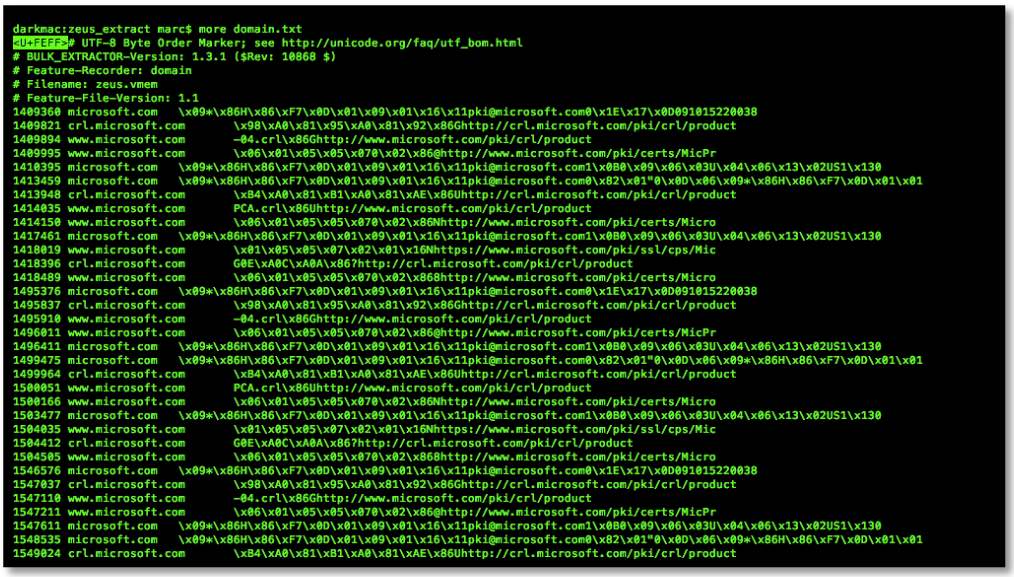
Figura 9. Programa Plainsight.



Fuente: Andrew Tabona. (2013). PlainSight. . [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet: https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

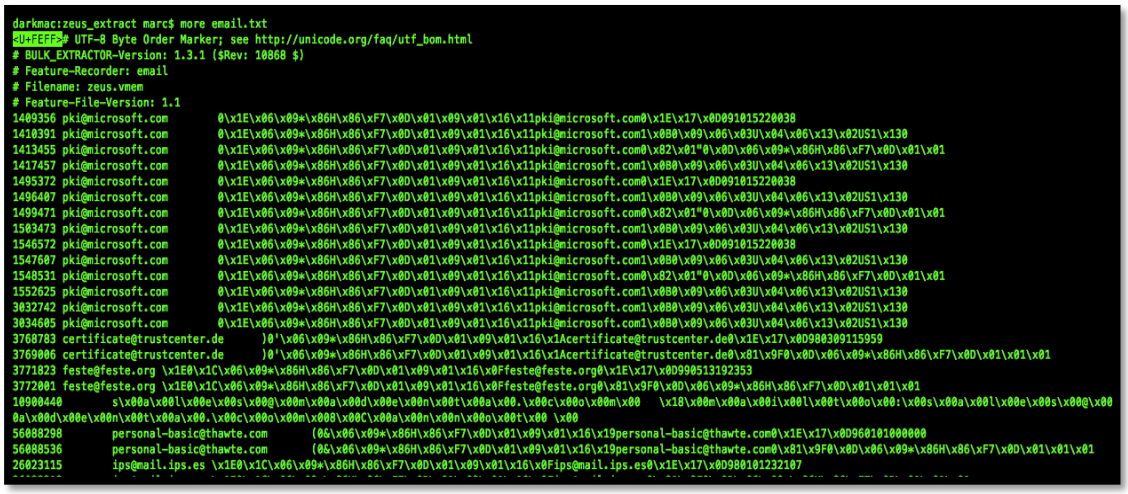
8.1.15 Bulk Extractor: Este es un software idóneo para examinar las imágenes en los discos, los archivos o directorios de archivos y extraer los datos útiles sin analizar las estructuras de los sistemas de archivos, ver imagen 8. El resultado de los análisis es sencillamente comprobados, estudiados o verificables con las herramientas mecanizadas. Este software establece histogramas de los resultados que fueron analizados en los discos. En la imagen 9 se puede observar que 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. (Extractor, 2015).

Figura 8. Examinador de imágenes.



Fuente: DragonjAR soluciones y seguridad informática S.A.S. (2014). Extrayendo dominios. . [Imagen]. [Consultado: 16 de noviembre de 2017]. Disponible en Internet:http://www.dragonjar.org/bulk-extractor.xhtml

Figura 10. Extrayendo e-mails.



Fuente: DragonjAR soluciones y seguridad informática S.A.S. (2014). Extrayendo dominios. . [Imagen]. [Consultado: 16 de noviembre de 2017]. Disponible en Internet:http://www.dragonjar.org/bulk-extractor.xhtml

Tabla 1. 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 BlacBag 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)
Recuperación de Datos	Herramientas de código abierto	BringBack
		RAID Reconstructor
		Salvation Data

Proceso	Sistema Operativo	Herramienta
Extracción De Metadatos	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
Recuperar Particiones	Herramientas de código abierto	Parted
		Active Partition Recovery
		Testdisk
		Partition Table Doctor

Fuente: Autor

8.2.1. Evidencia Digital

Una vez se ha establecido las herramientas para trabajar en el laboratorio forense informático se debe tener en cuenta los diferentes tipos de evidencia ya que el perito forense se encontrará con una gran variedad de información que seguramente contenga la evidencia potencial acerca del incidente de seguridad que ha desencadenado la investigación.

Por lo cual es trascendental establecer el orden en el cual se recolectará dicha información. Para esto se recomienda seguir los conceptos del RFC 3227 ya que

éste establece el orden en base a la volatilidad de la data. A continuación se presenta una lista indicando el orden de recolección según la volatilidad de los datos en un sistema típico.

I. Registros y contenidos de la caché del procesador.

II. Tablas de ruteo, conexiones de red, caché arp, tabla de procesos, estadísticas del kernel, memoria.

III. Archivos temporales del sistema.

IV. Contenidos de otros archivos y discos duros.

V. Loging remoto y datos extraídos de herramientas de monitoreo relevantes para el sistema en cuestión.

VI. Configuración física, topología de red.

VII. Contenido de otros dispositivos de almacenamiento.

Se puede ver que en los puntos (I) y (II) están relacionados con información ubicada en los medios de almacenamiento más volátiles de una máquina, es decir, aquellos que pierden sus datos cuando se elimina el suministro de energía. Dentro de esa categoría, los datos de mayor interés son en general los siguientes:

- Fecha y hora
- Procesos activos
- Conexiones de red
- Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”
- Usuarios conectados remota y localmente.

En los puntos (III) y (IV) se relacionan con medios de almacenamiento secundario, típicamente discos duros, los cuales son capaces de retener la información durante largos períodos sin suministro de energía. No obstante, es importante destacar que, aunque el medio en el cual se almacene la información tenga la capacidad de retenerla cuando está apagado, los sistemas que manipulan el contenido

almacenado en ellos pueden modificar o eliminar evidencia potencial durante el inicio o el cierre del sistema.

Para dar un ejemplo de estos, puede nombrarse los archivos temporales, o también, en un sistema comprometido, el atacante puede haber dejado scripts configurados para eliminar el rastro de su intrusión al momento del cierre del sistema.
Los últimos tres puntos de la lista ubican la evidencia en un perímetro externo al computador en cuestión. La información recolectada aquí está ubicada en otros equipos distintos al equipo comprometido.

8.2.3. Técnicas para la recolección de evidencia

Antes de identificar pautas asociadas a la recolección de evidencia digital forense, es importante tener en mente alguno de los objetivos subyacentes de esta disciplina como lo son por ejemplo el descubrir la causa del incidente, como prevenir la reincidencia, como establecer un proceso en el cual los resultados sean aceptados en un ámbito judicial, entre otros.

Para esto, es necesario contar con herramientas que no modifiquen ni alteren la evidencia que está siendo recolectada así como métodos que aseguren resultados verificables, reproducibles e independientes del investigador y/o sus herramientas.

Algunas de las recomendaciones propuestas por el RFC 3227 son las siguientes:

- Capturar una imagen lo más precisa posible del sistema comprometido.
- Mantener notas detalladas, incluyendo fechas y timestamps, identificando si es hora local o UTC.
- Minimizar cambios sobre los datos y eliminar vías externas que puedan modificar los datos.
- Ante la duda entre recolectar y analizar, realizar la recolección primero y luego analizar.
- Los procedimientos deben ser viables, en lo posible, automáticos por un tema de velocidad y precisión. Ser metódico.

- Disponer de enfoques metódicos para los distintos tipos de dispositivos, paralelizables dentro del grupo de investigación forense.

- Recolectar evidencia desde el más volátil al menos volátil de los dispositivos.

- Realizar una copia bit a bit del sistema. No trabajar sobre la evidencia recolectada sino sobre una copia de la misma.

Los principios propuestos en el RFC 3227 son, en forma resumida, los siguientes:

- Orden de volatilidad. Proceder del más volátil al menos volátil.

- Cosas a evitar. Es muy fácil eliminar evidencia en forma inadvertida. Se sugiere: no apagar el equipo hasta completar la recolección de evidencia debido a scripts de inicio y/o cierre que pueden destruir evidencia; no confiar en los programas del sistema que pueden haber sido comprometidos; no ejecutar programas que modifiquen los tiempos de acceso de los archivos del sistema; tener en cuenta que acciones como simplemente desconectar un cable de red pueden lanzar acciones automáticas en el sistema que pueden eliminar evidencia.

- Consideraciones de Privacidad. Seguir la política de privacidad de la empresa y proteger la evidencia recolectada del acceso por personas que normalmente no podrían acceder a ella; no inmiscuirse en la privacidad de las personas sin una estricta indicación; contar con el respaldo de la empresa en los procedimientos utilizados.

8.2.4. Consideraciones Legales

La evidencia debe ser:

- Admisible. Debe seguir ciertas reglas legales antes de ser presentada ante una corte.

- Auténtica. Debe ser posible vincular la evidencia con el incidente.

- Completa. Debe describir todo el incidente y no solo parte de él.

- Confiable. No debe existir nada sobre el mecanismo de recolección de evidencia que genere dudas acerca de su autenticidad o veracidad.

- Creíble. Debe ser fácilmente creíble y entendible por una corte.

- Procedimiento de recolección. Debe ser tan detallado como sea posible.

- Transparencia. Los métodos utilizados para la recolección de evidencia deben ser transparentes y reproducibles por terceros de manera precisa.

- Pasos de la recolección. Algunas de las sugerencias son listar los sistemas involucrados, establecer qué tipo de información puede ser más relevante y admisible, eliminar vías de modificación externas, seguir el orden de volatilidad, documentar cada paso, considerar personas involucradas en el proceso, generar *checksums*[42] y firmas criptográficas de la evidencia recolectada de manera de preservar una cadena de evidencia robusta.

- Procedimiento de almacenamiento. Debe ser estrictamente seguro.

- Cadena de Custodia. Debe estar claramente documentada. Debe describir cómo, dónde y por quién la evidencia fue encontrada y recolectada; cómo, dónde y por quién fue gestionada o examinada; lugares, períodos y transferencias de custodia de la evidencia.
- ¿Dónde y cómo archivar la evidencia? Utilizar medios de almacenamiento estándares. Restringir el acceso. Debería ser posible detectar accesos no autorizados.

- Herramientas necesarias. Disponer de un conjunto de herramientas ejecutables desde un medio de solo lectura como un CD o DVD. El *toolkit* debería proporcionar herramientas para las realizar las siguientes actividades: examinar procesos, examinar el estado del sistema, realizar copias bit a bit, generación de checksums y firmas, generación de imágenes de procesos en ejecución, scripts de automatización de recolección de evidencia. Las herramientas deben estar linkeadas estáticamente y no deben depender de otras librerías que no sean aquellas que están en el medio de solo lectura.

Anteriormente se menciona que la evidencia digital se clasifica en dos grandes tipos; volátil y no volátil. La evidencia volátil contiene la información que desaparece una vez que el sistema pierde la alimentación eléctrica. En esta categoría se incluye el contenido de la memoria RAM, los procesos activos, usuarios conectados,

[42] Hace que sea fácil y rápido para cualquiera el poder calcular y verificar sumas de comprobación

información de red, aplicaciones a la escucha, entre otras. La segunda categoría de evidencia en general refiere a la información contenida en el disco duro la cual puede ser recolectada sin necesidad de tener el equipo comprometido prendido sino que es suficiente con tener acceso físico al disco.

Igualmente, el análisis forense puede dividirse también en dos categorías con base al estado del sistema sobre el cual se realiza dicho proceso; éstas son análisis sobre sistemas vivos y sistemas muertos.

Se denominan sistemas vivos a aquellos que han sido objeto de un ataque y que aún no han sido desconectados del suministro eléctrico o que no han sido reiniciados. Básicamente, la diferencia con los sistemas muertos es que aún poseen evidencia volátil que puede ser de utilidad para la investigación forense, en particular, en la memoria RAM.

Durante años, las investigaciones forenses se han enfocado en la información que queda disponible luego que ha ocurrido un ataque y el sistema ha sido restablecido a un modo seguro. La información analizada luego, típicamente ubicada en medios de almacenamiento como discos duros constituye el insumo para el proceso de análisis conocido como "*dead analysis*". Sin embargo, en los últimos años ha habido un creciente énfasis en el análisis de sistemas vivos. Una de las razones es que muchos de los ataques contra sistemas de computadores no dejan rastros en el disco duro; los atacantes solo explotan información en la memoria del equipo. Otra de las razones es el uso cada vez mayor de medios de almacenamiento encriptados dado que posiblemente, la única clave que permita desencriptar los datos esté en memoria, con lo que el apagado del equipo, provocará que ésta se pierda.

8.3. ORDEN DE RECOLECCIÓN DE EVIDENCIA

El primer tipo de evidencia a recoger es la que está en la memoria RAM, a pesar de que es habitual que, en muchos procesos forenses, ésta reciba poca o ninguna atención. Sin embargo, este tipo de memoria es una fuente muy importante de información, que será irremediablemente perdida en cuanto la máquina sea apagada o reiniciada. De hecho, existen clases de evidencia que en ocasiones sólo podrán ser encontradas en RAM, como los nuevos y sofisticados métodos de infección de ordenadores, utilizados por herramientas como el *rootkit* FU o el gusano SQL Slammer, los cuales residen únicamente en memoria y no escriben nunca nada en el disco duro.

8.3.1. Recolección de evidencia volátil: Dada su fragilidad, y que puede perderse con mucha facilidad, este tipo de evidencia es la primera que debe ser recogida. Por tanto, en la medida que sea posible, la máquina objeto del análisis no debería ser apagada o reiniciada hasta que se haya completado el proceso.

Las herramientas utilizadas en el proceso no deberían apoyarse en absoluto en el sistema operativo objeto del análisis, pues éste podría haber sido fácilmente manipulado para devolver resultados erróneos. Existen herramientas de hardware que se instalan en el equipo con anterioridad para este tipo de situaciones pero naturalmente, ese no es el escenario típico. En general, el investigador forense debe recolectar la información utilizando herramientas de software limitando el proceso a la mínima cantidad de pasos con el objetivo de minimizar el impacto sobre la máquina analizada. En general, se utiliza un dispositivo de solo lectura como un CD o DVD con las herramientas necesarias para el análisis. Existen varias distribuciones especializadas en análisis forense que se analizan en secciones posteriores.

8.3.2. Recolección de evidencia no volátil: Debido a que durante el proceso de análisis es posible que la información sea modificada de manera inadvertida, es común la utilización de una técnica llamada "*Disk Imaging*". Mediante esta técnica se busca obtener una copia exacta de la evidencia no volátil del equipo comprometido, generalmente, una copia de sus particiones o del disco duro completo. Típicamente se suele generar dos copias; una de ellas será utilizada como medio para el análisis y la otra como respaldo.

8.3.3. Almacenamiento de la Evidencia: Para almacenar las evidencias recogidas será necesario añadir al sistema analizado algún tipo de almacenamiento externo. Teniendo en cuenta que se está realizando la fase de análisis en vivo y que, por tanto, no es posible apagar el ordenador todavía, existen básicamente dos opciones. La primera consiste en utilizar una unidad externa, como un disco duro o una memoria USB de suficiente capacidad. Por otro lado, la segunda opción implica añadir a la red de la máquina analizada un nuevo sistema, habitualmente un ordenador portátil, en el que se puedan copiar los datos recogidos.

8.4. TÉCNICAS DE ANÁLISIS DE EVIDENCIA

Una vez que se ha recolectado la evidencia y ha sido almacenada de forma adecuada, el investigador forense debe realizar el proceso de análisis sobre la misma. El objetivo en esta etapa es reconstruir con la información disponible, la

línea temporal del ataque (timeline) determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento. El análisis se da por concluido cuando se descubre cómo se produjo el ataque, quién o quiénes lo llevaron a cabo, cuál era el objetivo, etc.

Al igual que en la etapa de recolección, es importante la utilización de herramientas adecuadas para realizar el análisis de la evidencia de manera que esta no sea alterada ni modificada. Existen diversos enfoques a la hora de analizar la evidencia no volátil obtenida en la etapa de recolección. Uno de ellos es montar una copia del disco del sistema comprometido en modo solo lectura sobre un equipo existente. El otro es utilizar una distribución de tipo live que permita estudiar el disco del equipo sin modificarlo.

8.4.1. *Timeline*

Para reconstruir la secuencia temporal del ataque es importante contar con cierta información acerca de los archivos contenidos en el disco del sistema comprometido: inodos asociados, marcas de tiempo MACD (fecha y hora de modificación, acceso, creación, borrado), ruta completa, tamaño en bytes y tipo de archivo, usuario y grupos a quien pertenece, permisos de acceso, si fue borrado o no.

Debida a la inmensa cantidad de archivos existentes en un sistema, el investigador forense debería hacer uso de scripts que automaticen el proceso de creación del timeline.
Algunos de los pasos a tomar son:

- Ordenar archivos por MAC. Esto es interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema mientras que los recientes tendrán inodos y fechas muy distintas.

- Buscar archivos recientemente creados, modificados, o borrados; instalaciones de programas en rutas poco comunes como directorios temporales.

- Detectar archivos de sistema modificados luego de la instalación.

- Analizar el espacio residual detrás de cada archivo (zonas que el sistema operativo no ve), debido a que el almacenamiento en general se realiza por bloques, por lo que podrían detectarse restos de logs eliminados por ejemplo.

- Detectar archivos eliminados que sean sospechosos y correlacionar los timestamps con la actividad sobre otros archivos. Analizar conjuntamente con los logs del sistema.

La secuencia temporal de eventos es un elemento importante para determinar cómo se realizó el ataque. En este punto, es importante retomar la evidencia volátil recolectada con anterioridad y verificar los procesos que estaban activos mientras que el sistema estaba vivo, los puertos TCP/UDP, conexiones activas, etc., de manera que sea posible detectar o intuir actividad sospechosa.

8.5. CADENA DE CUSTODIA

En la figura 10 se aprecian las etapas para resolver una cadena de custodia

Figura 11. Cadena de Custodia.

Fuente: ARIAS, Arles; RODRÍGUEZ, Arango Alejandro y SÁNCHEZ Adrián Sánchez. (2017). Cadena de custodia. [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet: 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.

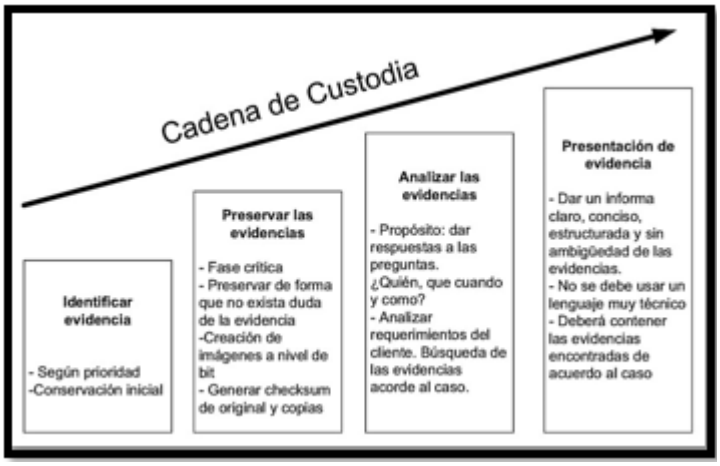
c) Mantener la firmeza de las pruebas.

d) Hacer registros de las duraciones de cada evidencia aprobados por los delegados.

e) Garantizar la solidez de las pruebas guardadas protegiendo su seguridad.

En la figura 11 se muestra los pasos a seguir durante la cadena de custodia.

Figura 12. Proceso de la cadena de custodia.



Fuente: Jaider. (2015). Cadena de custodia. [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet: http://eportafoliojaider.blogspot.com.co/2015/05/informatica-forense.html

8.5.1. 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 2. Evidencia electrónica.

Sistema Informático	
Hardware	**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, fraude u otra 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 usó para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción.

Fuente: DEL PINO, Santiago Acurio. Elementos físicos. [Consultado: 15 de noviembre de 2017]. Disponible en Internet: https://www.oas.org/juridico/spanish/cyber/cyb44_informatica.pdf

Tabla 3. 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: DEL PINO, Santiago Acurio. Elementos físicos. [Consultado: 15 de noviembre de 2017]. Disponible en Internet:
https://www.oas.org/juridico/spanish/cyber/cyb44_informatica.pdf

8.5.1. 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.

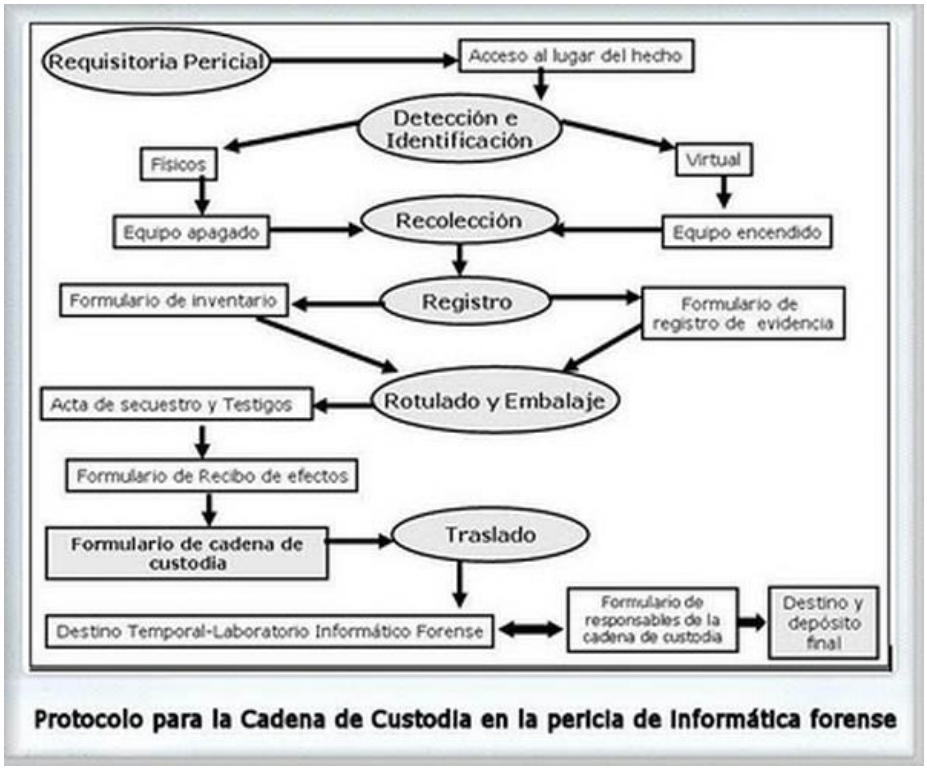
8.5.2. Fase de análisis

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.

8.5.3. Fase de presentación

En ésta fase final se obtiene los resultados encontrados por el investigador. Tan rápido como el hecho haya sido registrada e identificada 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, por lo cual se observa en la figura 12 los protocolos que se llevan a cabo en la cadena de custodia. (Informática, 2015)

Figura 13. Protocolos de la cadena de custodia para la información forense.



Fuente: MESEGUER González, Juan de Dios. (2013). Protocolo para la cadena de custodia en la pericia de informática forense. . [Imagen]. [Consultado: 18 de noviembre de 2017]. Disponible en Internet: http://www.elderecho.com/www-elderecho-com/contaminacion-custodia- invalida-periciales-informaticas_11_556555001.html

9 PRESENTACIÓN Y DESCRIPCIÓN DE UN CASO FORENSE

9.1 Descripción de la Escena

Eduardo Velásquez Gerente General de la comercializadora de textiles “Modatelas” dedicada al suministro de telas, descubrió el día 30 de enero de 2018 que su archivo base de datos con la información confidencial de sus clientes y proveedores ya no se encontraba guardado en el computador PC microtorre HP 280 G1 2.8GHz que se tiene como host de almacenamiento central de la comercializadora ya no existe.

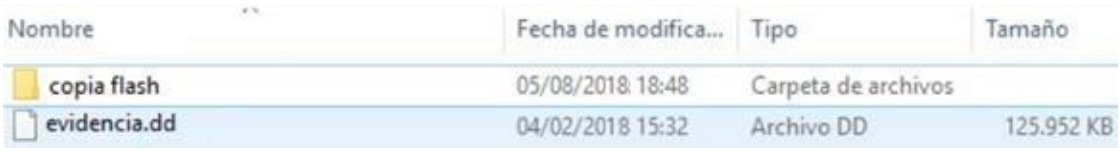
El Gerente informa que el día 15 de ese mes realizó la terminación del contrato de una de sus colaboradoras, la señora Ana Roa quien laboró hasta la fecha acordada que fue el día 29 de enero del 2018.

En tal caso de estudio, solo se cuenta con una evidencia, la cual es el equipo de cómputo que la ex funcionaria tenía asignado en su puesto de trabajo.

9.2 Investigación Forense

El primer paso ejecutado en la investigación, es realizar una imagen del equipo de cómputo evidencia del caso de acuerdo a los estándares de seguridad, proceder a observar la figura número 13.

Figura 13. Imagen del equipo a investigar.

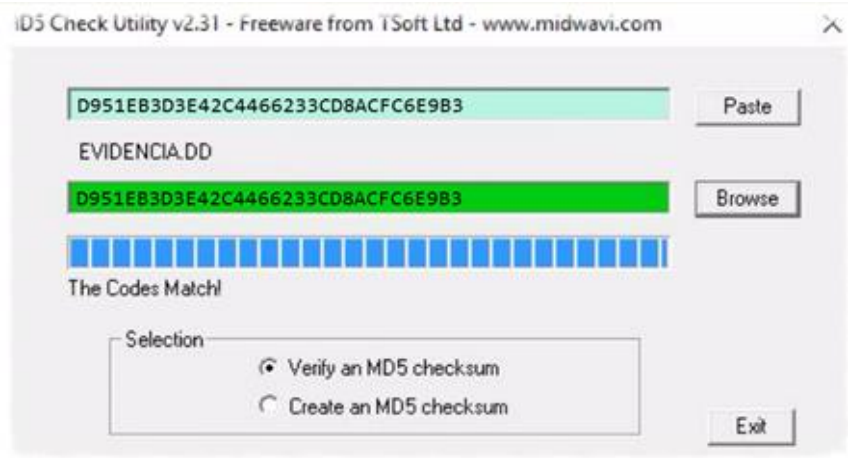


Fuente: Autor

El segundo paso consiste en la verificación del MD5, ya que aquí conocemos su valor por medio del software, tal como se observa en la figura 14 en donde se demuestra que el archivo no ha sido modificado por medio de software especializado MD5 & SHA Checksum Utility.

MD5: d951eb3d3e42c4466233cd8acfc6e9b3

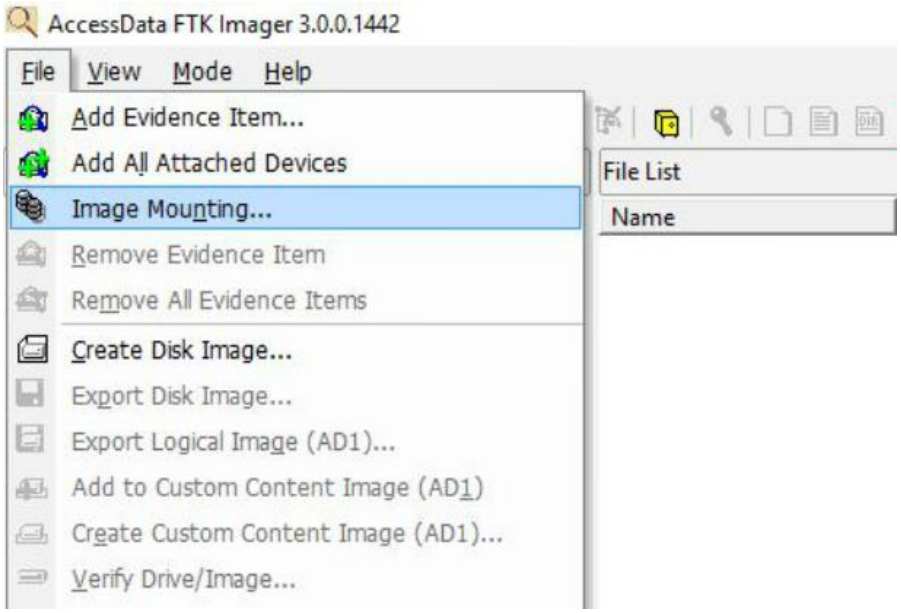
Figura 14. Verificación del HD5.



Fuente: Autor

Seguidamente se realiza el montaje de la imagen a replicar del equipo a investigar en este caso, a través del software AccessData FTK, el cual se observa en la figura 15.

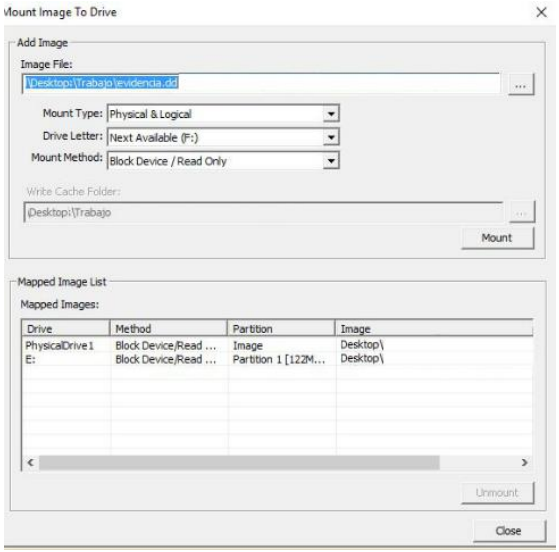
Figura 15. Montaje de la imagen a replicar del equipo a investigar en este caso.



Fuente: Autor

En la figura 16, se encuentra la continuación del proceso de montaje de la imagen la cual es la base de esta investigación.

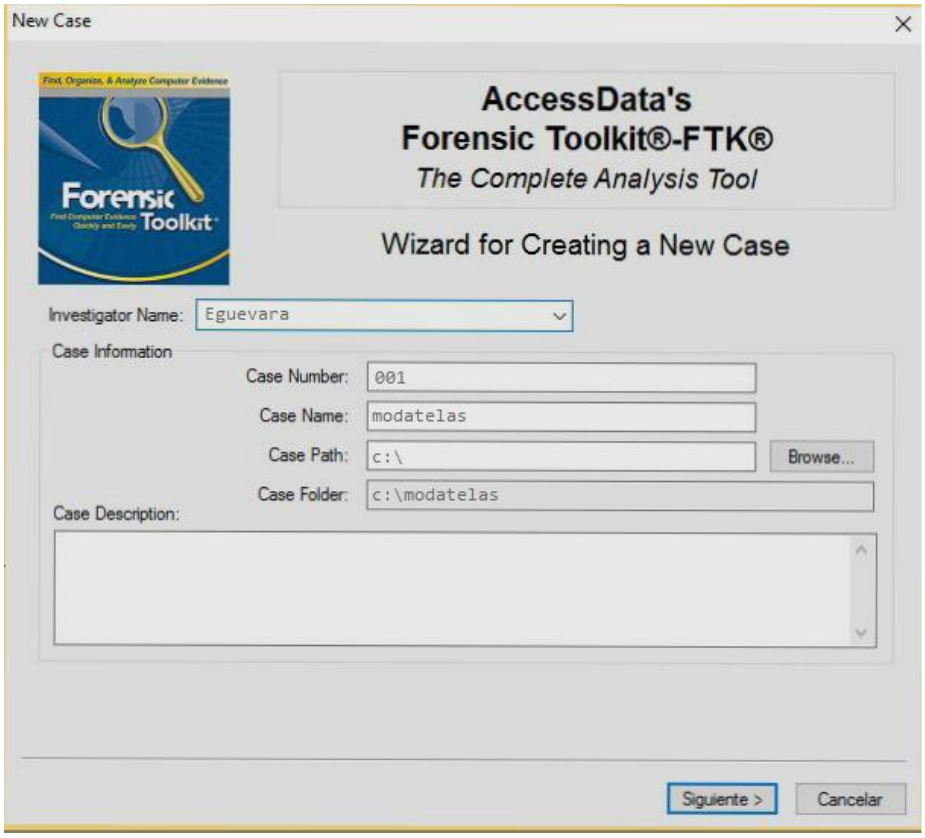
Figura 16. Continuación del montaje de la imagen a replicar del equipo a investigar.



Fuente: Autor

Una vez se tiene la imagen para hacer la investigación del caso se realiza instalación de la misma en el software FTK, el primer paso es hacer la creación del caso como se observa en la figura 17.

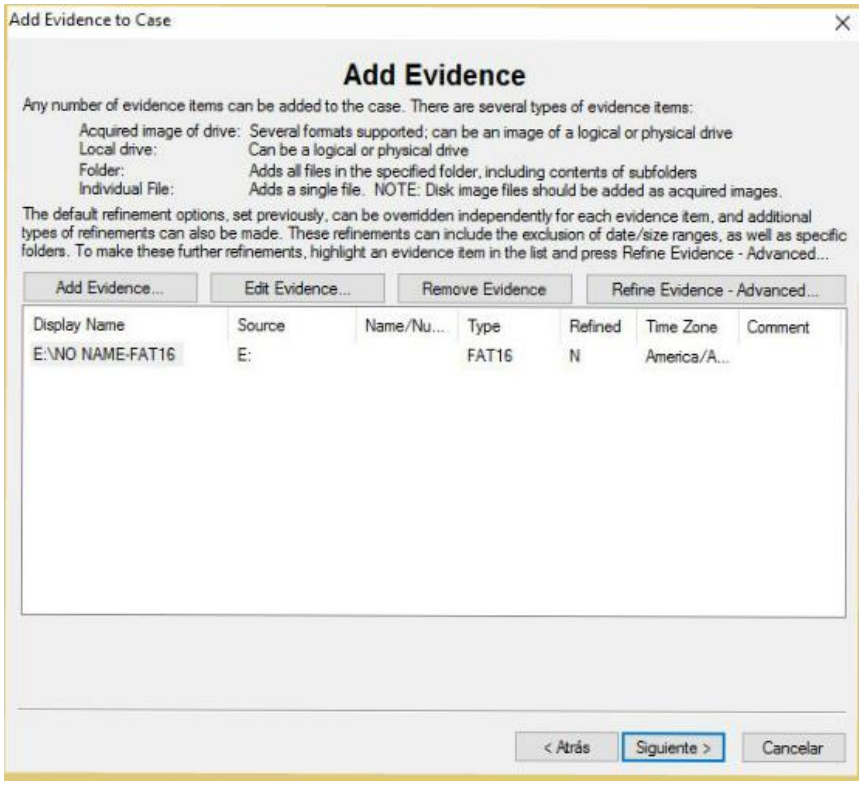
Figura 17. Creación del caso.



Fuente: Autor

En la figura 18, se encuentra la continuación del proceso de creación del caso en el software FTK.

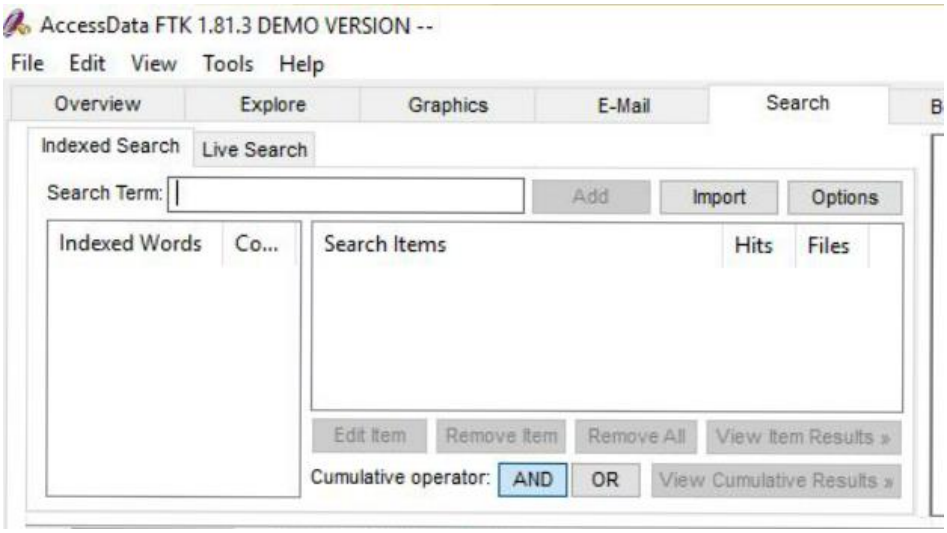
Figura 18. Continuación de la creación del caso en el software especializado FTK.



Fuente: Autor

Una vez creado el caso se realiza una búsqueda de términos específicos para intentar encontrar el archivo extraído de la empresa como se observa en la figura 19.

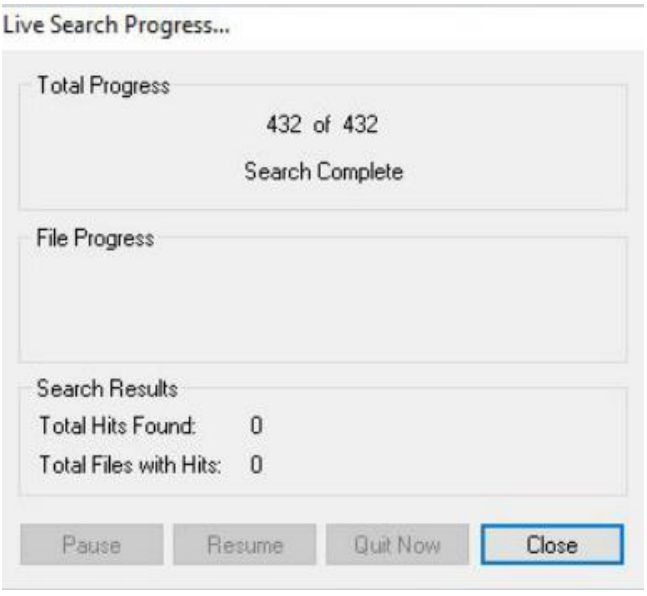
Figura 19. Búsqueda de términos específicos.



Fuente: Autor

En la figura 20 se evidencia el resultado de la búsqueda de los términos específicos el cual fue la palabra clave "CONFIDENCIAL", con un resultado de (0) cero aciertos.

Figura 20. Resultado 0 de 434 archivos.



Fuente: Autor

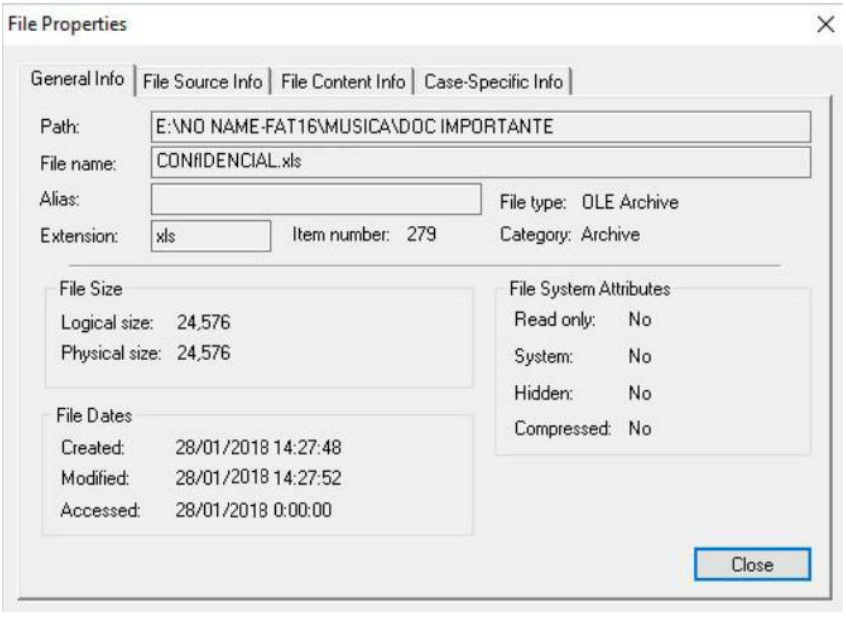
Para la siguiente búsqueda se ingresa la extensión del archivo objeto de esta investigación, el cual es un ".xls”. Ver el resultado en la imagen 21.

Figura 21. Resultado exitoso.

Estefani Guevara Dávila.

En la figura 22, se procede a observar las propiedades del archivo y corroborar parte de los metadatos del archivo hallado en la investigación.

Figura 22. Propiedades del archivo encontrado.

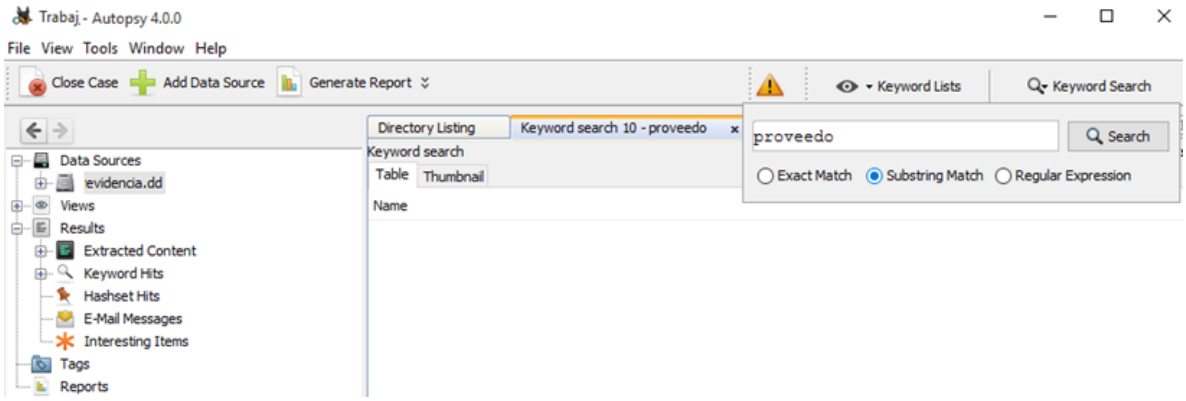


Fuente: Autor

Como segunda medida se examina la imagen nuevamente pero esta vez con el software Auopsy para verificar la información hallada anteriormente.

Se realiza una busqueda por palabra clave, en este caso el tema es la información de los clientes y proveedores por lo que se usa la palabra “proveedo”, como se aprecia en la figura 23.

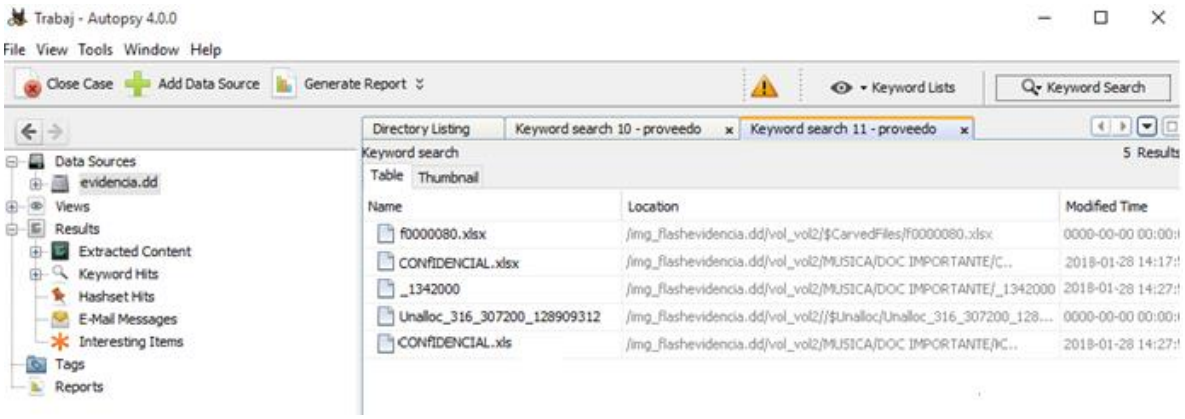
Figura 23. Búsqueda por palabra clave.



Fuente: Autor

En la figura 24, la busqueda tiene éxito y arroja cinco archivos que tienen esa palabra clave.

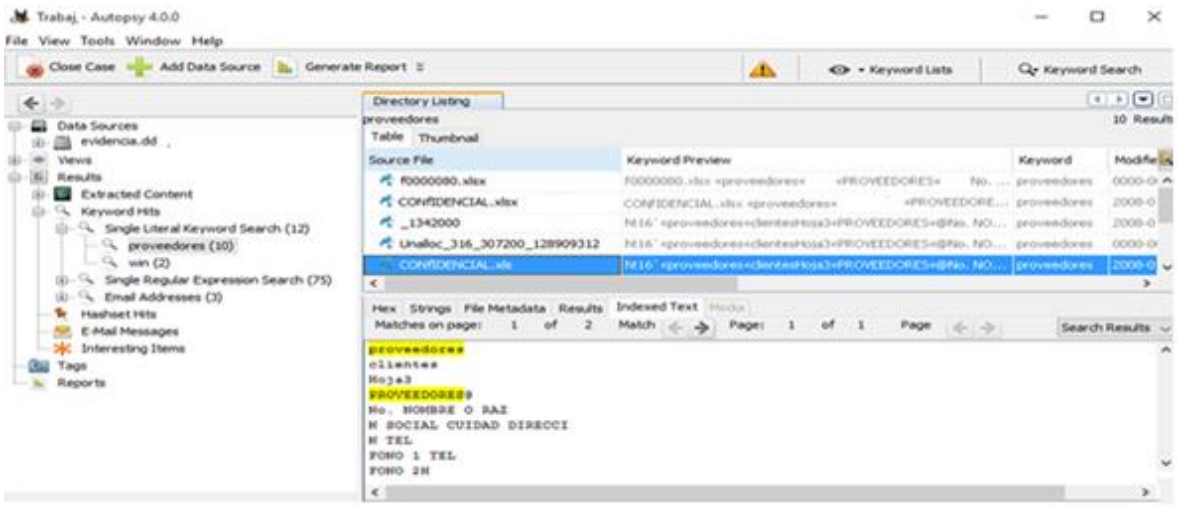
Figura 24. Resultado de la búsqueda por palabra clave.



Fuente: Autor

A continuacion se procede a examinar cada uno de los archivos hallados, en los cuales se confirma que efectivamente contienen datos importantes para esta investigación, tal como es la lista de los proveedores de la textilera. Ver imagen 25.

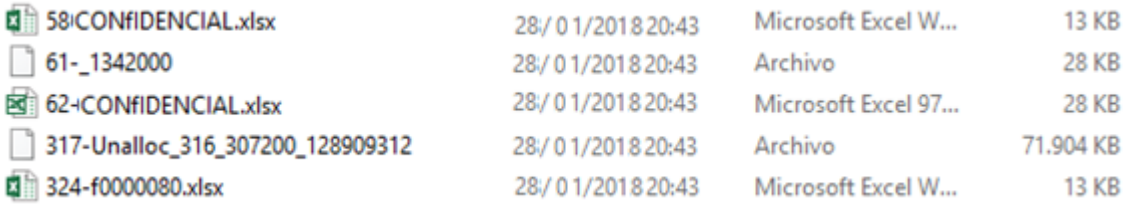
Figura 25. Datos encontrados en la búsqueda.



Fuente: Autor

Al confirmar que los archivos tienen información valiosa para esta investigación, se procede a extraerlos para su respectivo análisis. Como se puede ver en la figura 26.

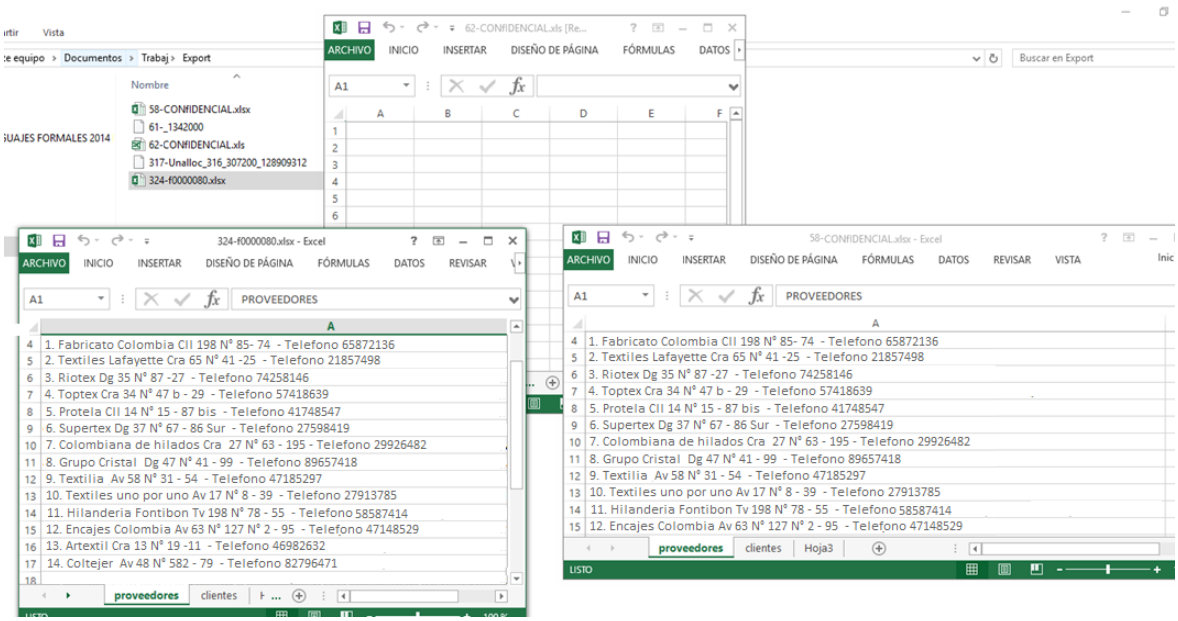
Figura 26. Archivos encontrados para proseguir con la investigación del caso.



Fuente: Autor

Cuando se procede a abrir los archivos encontrados, dos de estos contienen la información sustraída del equipo host, de esta manera se evidencia que la sospechosa accedió a la información confidencial de la base de datos de clientes y proveedores de la textilera ¨Modatelas¨. Ver figura 27.

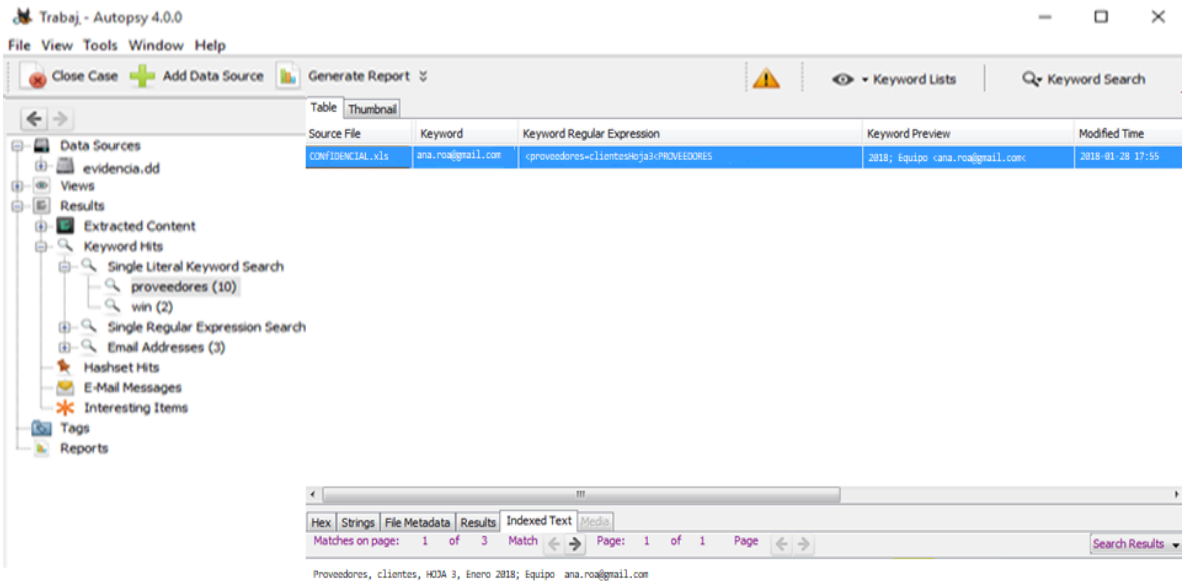
Figura 27. Archivos extraídos de los hallazgos en la búsqueda por palabra clave.



Fuente: Autor

Al continuar con la búsqueda se ingresa para revisar los mensajes enviados por correo electrónico para comprobar si alguno de los archivos hallados fue extraído por este medio y efectivamente se encuentra un correo electrónico enviado a ana.roa@gmail.com que corresponde a la persona despedida de la textilera. Ver figura 28.

Figura 28. Búsqueda de los correos electrónicos enviados.



Fuente: Autor

De esta manera se puede comprobar que la señora Ana Roa fue la persona responsable de eliminar y sustraer el archivo base de datos de los clientes y proveedores de la Textilera “Modatela”.

Ante la evidencia hallada en el caso se puede establecer que dentro de la empresa “Modatela” fue víctima de un hecho delictivo que se pude asociar con los artículos de la ley 1273 de 2009 de delitos informáticos en Colombia de la siguiente manera:

Articulo 269f: Violación de datos Personales - El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Articulo 269J: Transferencia no consentida de Activos- El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en

pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

9.3. RECOMENDACIONES FINALES

Según el Instituto Nacional de Ciberseguridad de España Incibe, para reducir la probabilidad de que este tipo de incidentes ocurran, se deberán establecer diferentes tipos de medidas vinculadas a la protección de la información de las empresas teniendo en cuenta tres tipos de medidas:

Técnicas. El mercado de soluciones de seguridad, ofrece servicios y herramientas para todo tipo y tamaño de empresas, que permiten detectar y prevenir la fuga de información. Las medidas básicas que podemos aplicar, independientemente del tamaño de la empresa, son:

- Cifrado de la información confidencial corporativa.
- Instalación, configuración y actualización de cortafuegos.
- Mantener actualizadas todas las aplicaciones del sistema.

Para empresas con mayores recursos económicos o que necesitan un nivel mayor de exigencia a la hora de gestionar y proteger la información, se podrá aplicar otras medidas más avanzadas utilizando:

- Soluciones de prevención de pérdida de datos o DLP (del inglés Data Loss Prevention) que suelen estar orientadas a la monitorización y control las destinadas a la gestión del ciclo de vida de la información o ILM (del inglés Information Lifecycle Management) desde que esta es generada o elaborada hasta su archivado o destrucción final.

- Herramientas de control de dispositivos externos de almacenamiento, que están destinadas a controlar el acceso físico a puertos y dispositivos extraíbles como USB para evitar fugas de información.

Organizativas. Este tipo de medidas están estrechamente relacionadas con la forma en que se maneja o se trata la información. Por un lado se tendrá que prevenir malas prácticas como compartir contraseñas o información confidencial en

directorios de trabajo a las que tiene acceso toda la empresa. Estas situaciones suelen darse por falta de conocimiento del usuario. Por este motivo, es importante fijar políticas de seguridad, junto con acciones de concienciación a todos los empleados.

Jurídicas. Es importante que los empleados o proveedores que gestionan la información corporativa, cumplan las políticas de seguridad; para ello podemos firmar acuerdos de nivel de servicio (SLA) con los proveedores y hacer que los usuarios firmen unos acuerdos de confidencialidad, en los que se regulen los aspectos relativos a la seguridad y la confidencialidad de la información en la prestación de un servicio, incluyendo las sanciones en caso de incumplimiento.

Un punto importante y de obligado cumplimiento, es el relacionado con el tratamiento de ficheros que contienen datos de carácter personal. Aplicando estas medidas, no solo se cumplen con las leyes, sino que también se demuestra el compromiso con el cliente en cuanto al manejo de la confidencialidad de su información y en caso de que se produzca una fuga de información intencionada por parte de alguien de la compañía, tener el respaldo legal para llevar a cabo las medidas pertinentes.

Finalmente para ampliar la información acerca de cómo gestionar una fuga de información dentro de una empresa ingresar a la guía de aproximación al empresario según lo indica el INCIBE ([43]).

[43] INCIBE Instituto Nacional de Ciberseguridad de España https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

10 ARTÍCULOS DE LA LEY 1273 DE 2009

Dentro del desarrollo de este documento se considera en sus objetivos el realizar un análisis sobre la ley 1273 de la protección de la información y de los datos, con el fin de abarcar todos los campos de la comisión de delitos informáticos, de esta forma tener claridad de la parte legal dentro del área de la seguridad informática para conocer qué tipo de castigo acarrean estos actos delictivos en Colombia.

Por consiguiente, a continuación se dan a conocer los artículos pertenecientes a la ya referida ley en estudio con sus respectivas modificaciones en el transcurso del tiempo de la siguiente manera:

10.1. ARTÍCULO 269A*:* Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, utilice equipos, dispositivos o programas para acceder en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

10.1.1. Modificación*:* Se requiere definir dentro de este artículo el uso de dispositivos o programas para ejecutar el acceso abusivo a un sistema informático, para lo que se añade —El que, sin autorización o por fuera de lo acordado, utilice equipos, dispositivos o programas…‖ en donde se deja claro que quien utilice estos medios y no solo ejecute el hecho de acceder de forma abusiva a un sistema también reciba castigo al emplear o poseer dispositivos o herramientas que así lo permitan.

10.2. ARTÍCULO 269C*:* Interceptación de datos informáticos. El que posea, adquiera o utilice con previo conocimiento o de formas empírica dispositivos o herramientas de tipo informático o telemático y sin orden judicial previa intercepte datos informáticos o documentos físicos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

10.2.1. Modificación: En este artículo se añade —El que posea, adquiera o utilice con previo conocimiento o de formas empírica dispositivos o herramientas de tipo informático o telemático y sin orden judicial previa intercepte datos informáticos o

documentos físicos…‖, esto con el fin de ser más específica la tipificación del delito de la interceptación de información y vincular el uso de dispositivos que puedan ser utilizados para cometer esta clase de delito, además de incluir los documentos o información de carácter físico que también hace parte del principio de salvaguarda de la seguridad informática.

10.3. ARTÍCULO 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos o realice la instalación sin autorización de software o programas informáticos de no contengan licencia, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Modificación: Se adiciona a este artículo —…realice la instalación sin autorización de software o programas informáticos de no contengan licencia…‖ lo que permite tener en cuenta el software que no se encuentra licenciado y que sin autorización puede llegar a descargarse e instalarse en los equipos de cómputo y que contengan sectores defectuosos (bugs) o virus que afecten la parte lógica y física de los sistemas de información.

10.4. ARTÍCULO 269E*:* Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso entendiéndose para ello como virus, malware, troyanos, spyware o spam u otros programas de computación de efectos dañinos como aquellos que no contengan licencia para su instalación y puedan contener defectos (bugs) que causen daño a los dispositivos informáticos o telemáticos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes

10.4.1.Modificación: Dentro de este artículo se incluye una definición más amplia de lo que significa software malicioso y programas de efecto dañino —…software malicioso entendiéndose para ello como virus, malware, troyanos, spyware o spam u otros programas de computación de efectos dañinos como aquellos que no contengan licencia para su instalación y puedan contener defectos (bugs) que causen daño a los dispositivos informáticos o telemáticos…‖, con la finalidad de clasificar mejor los mismos y poderles dar el tratamiento adecuado según sea el caso.

10.5. ARTÍCULO 269G*:* Suplantación para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, suplante perfiles o cree perfiles falsos tanto en sitios web como en el manejo de las redes sociales, o realice suplantación de identidad mediante el uso de medios de comunicación telefónica y telemática y

que a su vez diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

10.5.1. Modificación*:* Se modifica el título del artículo a —Suplantación para capturar datos personales‖ y se añade la siguiente especificación —El que con objeto ilícito y sin estar facultado para ello, suplante perfiles o cree perfiles falsos tanto en sitios web como en el manejo de las redes sociales, o realice suplantación de identidad mediante el uso de medios de comunicación telefónica y telemática y que a su vez…‖, con el fin de vincular y regularizar la suplantación no solamente como él envió de enlaces propiamente sino también abarcando todo el ámbito en el cual se pueda generar una suplantación ya sea vía telefónica, mensajes de texto, whatsapp, el uso de perfiles falsos en redes sociales o sitios web de igual manera.

10.6. ARTÍCULO 269I*:* Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

10.6.1. Modificación*:* Este artículo debería considerarse un parágrafo agravante dentro del artículo 239 del vigente Código penal colombiano, puesto que la figura que se maneja en este como hurto calificado y agravado se adapta a las necesidades provistas y no hay necesidad de crear un nuevo bien o apartado.

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

10.7.1. Modificación*:* Este artículo debería considerarse de igual manera que el articulo 269I como un parágrafo agravante dentro del artículo 239 y tomando parte

del artículo 246 del vigente Código penal colombiano, puesto que la figura que se maneja en el primero es hurto calificado y agravado y en el segundo artículo como estafa, lo que se adapta a las necesidades provistas y no hay necesidad de crear un nuevo bien o apartado.

10.8. ARTÍCULO 269K*:* Pornografía infantil por medios informáticos. El que, con premeditación y valiéndose de engaños o cualquier medio de intimidación mediante el uso de dispositivos o sistemas informáticos o telemáticos adquiera, venda, distribuya, trafique, transmita, exhiba material de tipo pornográfico o cualquier tipo de manifestación de tipo sexual abusiva con menores de edad y que sean pertenecientes a circunstancias de vulnerabilidad o discapacidad, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

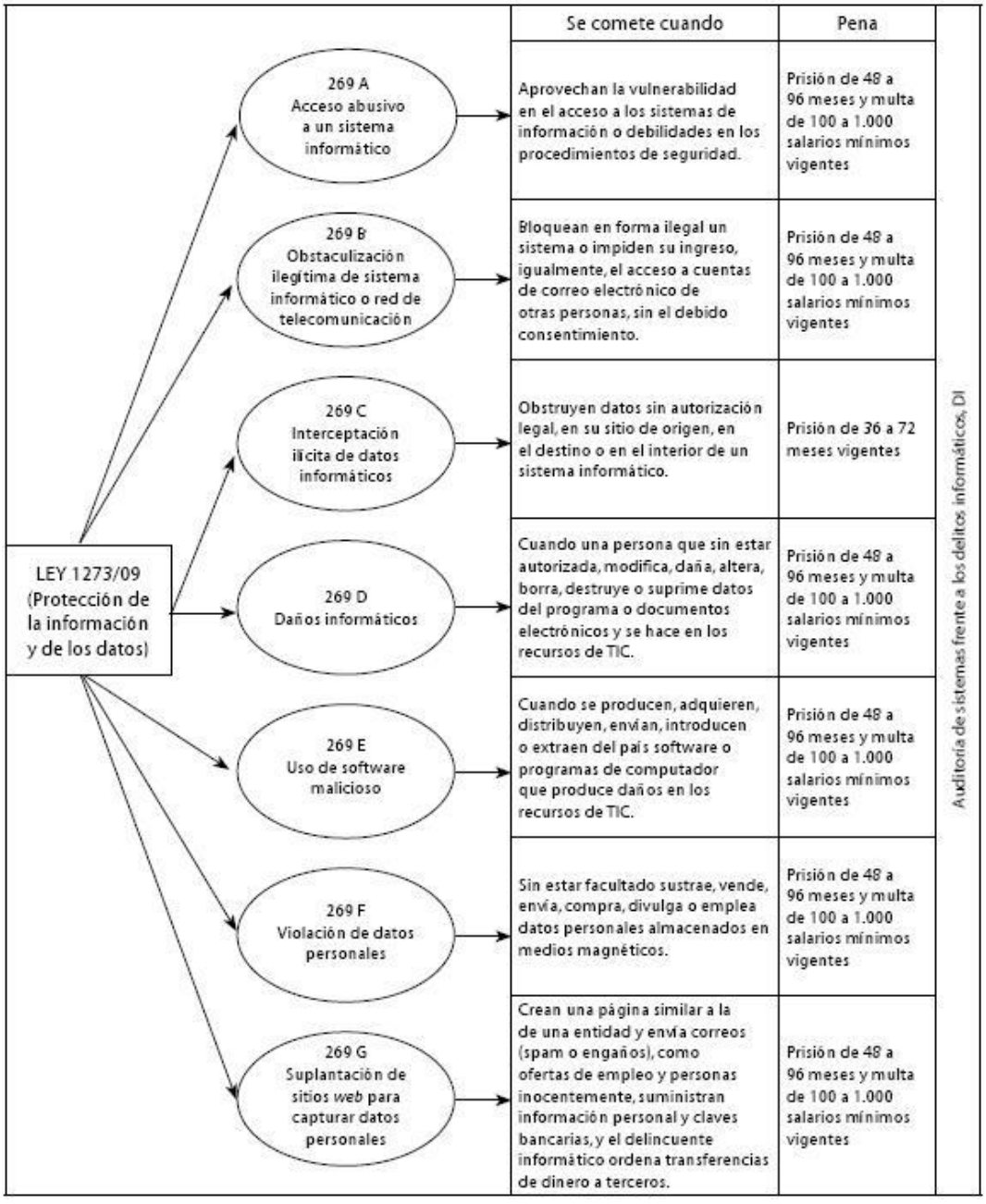
10.8.1. Adición*:* Se añade un nuevo artículo a la ley 1273 que contemple la pornografía infantil por medio del uso de sistemas informáticos y que sea sancionada no con penas administrativas como la ley 1336 de 2009 y 679 de 2001, sino que se considere penas agravantes de tipo penal para el que cometa este delito contra los menores de edad.

10.9. ARTÍCULO 269L*:* Falsificación de documentación digital. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, por medio del uso de un dispositivo o programa informático o telemático; o adultere, incluya un documento no existente a un sistema de información o lo que haga sus veces, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

10.9.1. Adición*:* Se hace necesario adicionar un artículo que contemple la falsificación mediante el uso de dispositivos o programas de carácter informático, puesto que con ello se pone en riesgo la información contenida en un sistema de información de una organización. De esta manera se crea un artículo que refuerce las sanciones impuestas vigentes y que vincule el uso de las nuevas tecnologías y no solo se clasifique como falsificación de documento las firmas y certificados digitales, además se tiene presente las nuevas formas de contener información como las Tablet, celulares, entre otros.

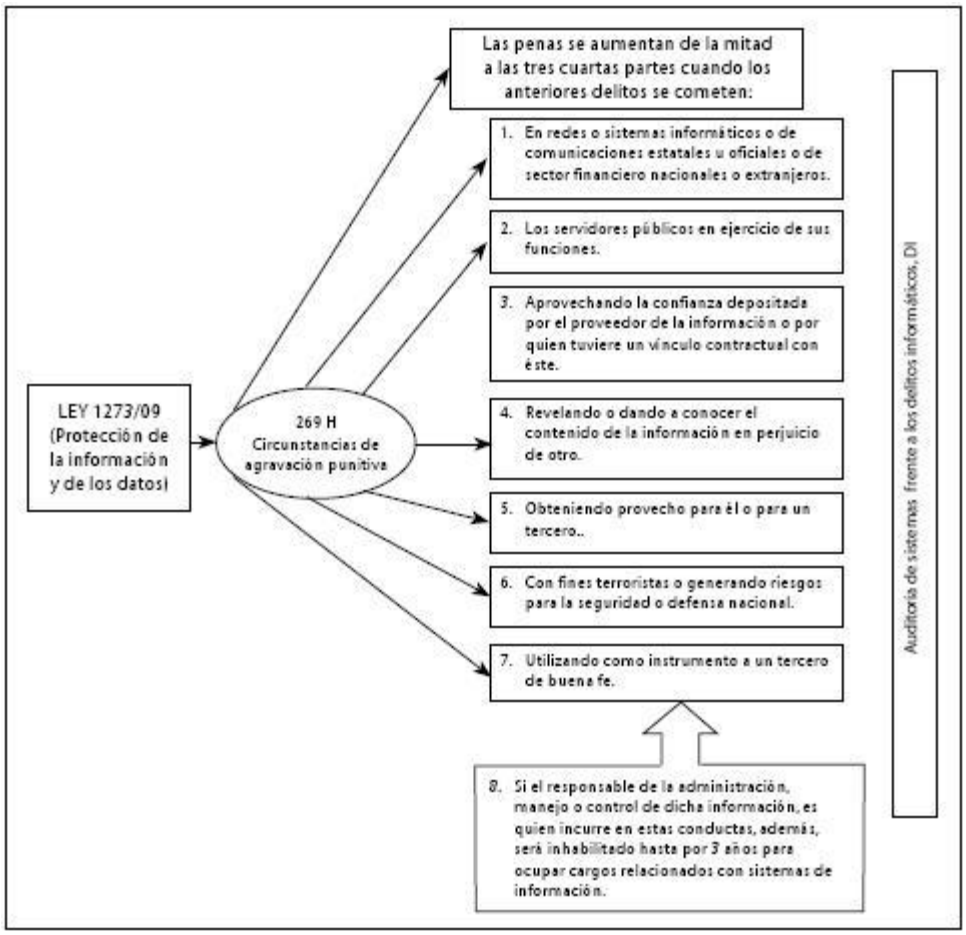
En la figura 29, se encuentra la legislación penal en Colombia frente a los delitos informáticos (Art. 1 de la Ley 1273 de 2009).

Figura 14. Legislación penal colombiana frente a los delitos informáticos.



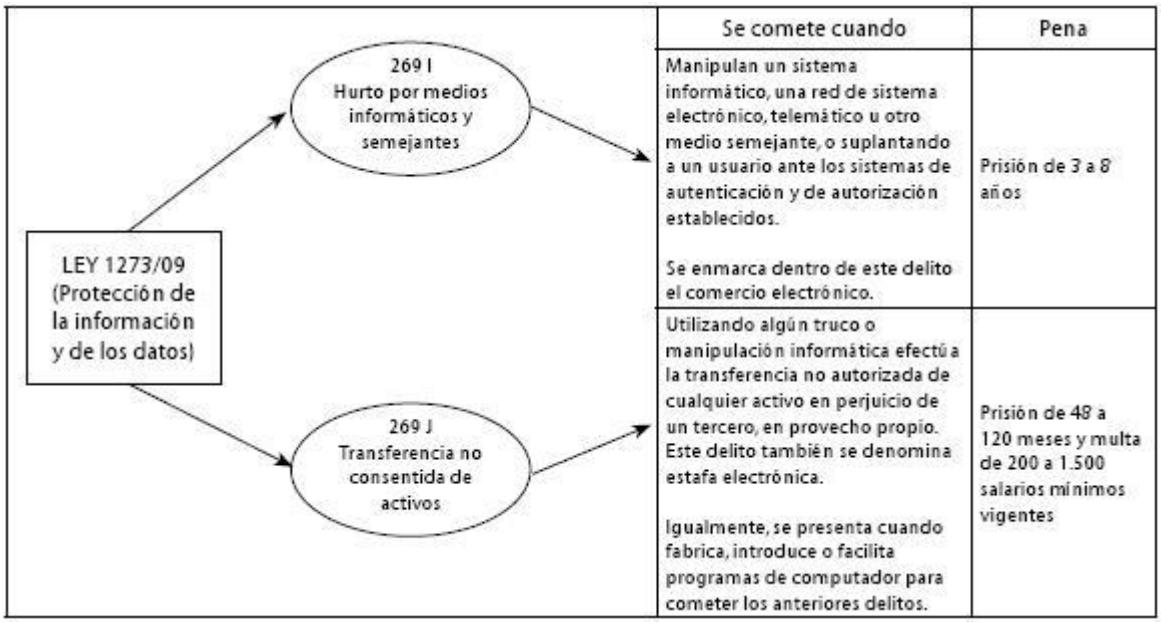
Fuente: OJEDA Pérez, Jorge Eliécer; RINCÓN Rodríguez, Fernando; ARIAS, Flórez, Miguel Eugenio; DAZA Martínez, Libardo Alberto. Con base a la Ley 1273 de 2009. Congreso de la Republica [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet
http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Figura 15. Legislación penal Colombiana frente a los delitos informáticos (Art. 1 de la Ley 1273 de 2009) Parte 2.



Fuente: OJEDA Pérez, Jorge Eliécer; RINCÓN Rodríguez, Fernando; ARIAS, Flórez, Miguel Eugenio; DAZA Martínez, Libardo Alberto. Con base a la Ley 1273 de 2009. Congreso de la Republica [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Figura 31. Legislación penal colombiana frente a los delitos informáticos (Art. 1 de la Ley 1273 de 2009) Parte 3.



Fuente: OJEDA Pérez, Jorge Eliécer; RINCÓN Rodríguez, Fernando; ARIAS, Flórez, Miguel Eugenio; DAZA Martínez, Libardo Alberto. Con base a la Ley 1273 de 2009. Congreso de la Republica [Imagen]. [Consultado: 15 de noviembre de 2017]. Disponible en Internet http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

En síntesis una vez recolectada la información en el proceso de indagación de este documento y los distintos temas que se derivaron del mismo, se efectuó el respectivo análisis en donde se logra identificar aspectos tanto positivos como negativos dando como resultado las siguientes conclusiones.

La investigación forense es una actividad la cual ha tomado fuerza a nivel internacional debido a la importancia que tiene dentro de los procesos judiciales donde la principal herramienta es la evidencia digital, teniendo en cuenta el aumento de los delitos informáticos en la actualidad, pues permite aclarar los hechos ocurridos en un proceso legal en específico, brindando los equipos para solucionar y lograr la impartir un dictamen de manera adecuada.

Colombia cuenta con un marco legal que incluye diferentes aspectos con relación a la ciberdelincuencia, la ciberdefensa y la ciberseguridad, en el cual se tratan aspectos referentes principalmente a la admisibilidad de la evidencia digital en las cortes, sin embargo, no se encuentra definido de forma clara muchas características

de la presentación y aceptación de la evidencia digital en el Código del Procedimiento Penal, sino que su definición está implícita.

En cuanto a los demás aspectos de la investigación forense referentes a los procesos legales en Colombia se encontró que hay sancionada la Ley 1273 de 2009 de delitos informáticos el cual contempla una amplia gama de delitos para poder sancionar a los ciberdelincuentes estando dentro de los países que contempla estos tipos de infracciones que se presentan a nivel mundial teniendo en cuenta los grandes avances tecnológicos y las grandes vulnerabilidades a los que nos encontramos expuestos.

Por otra parte el órgano judicial en Colombia cuenta con un marco jurídico amplio en relación a los aspectos referentes a la ciberdelincuencia, pero debido al desconocimiento por parte de los jueces, la impartición de la justicia flaquea y en ocasiones se pierde, dañando la confianza que la sociedad deposita en la justicia como medio para proteger sus derechos y castigar con rigor toda conducta ilícita.

También al analizar el marco de antecedentes se evidenció que en comparación con la legislación Española que es la más sólida a nivel mundial en cuento a los delitos informáticos se refiere, Colombia todavía está en proceso de evolución de la legislación informática ya que hay bastantes vacíos teniendo en cuenta la gran exposición a la que los ciudadanos o particulares se encuentran expuestos y hasta ahora todavía no estamos protegidos por parte del estado. Es así que queda evidenciado que todavía hay un gran camino por recorrer en cuanto a legislación se refiere para contar con los más altos estándares internacionales.

Con relación al caso forense presentado anteriormente se podría asociar a los siguientes artículos de ley de delitos informáticos:

- Artículo 269G
- Artículo 269I
- Artículo 269L

Por lo tanto las consecuencias que se presentan en el caso de estudio y con base a los resultados hallados, de acuerdo a la legislación vigente en Colombia la presunta sospechosa culpable del delito incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes y pagar una multa a la textilera “Modatelas”.

11 RECURSOS NECESARIOS PARA EL DESARROLLO

Este proyecto se realizó bajo la metodología de la investigación documental, por lo cual su mayor recurso será el tiempo que se debe utilizar para llegar a las conclusiones esperadas en esta monografía.

11.1 RECURSO HUMANO

El recurso humano utilizado para esta investigación será un ingeniero de sistemas idóneo que será el mismo investigador, el cual tiene los conocimientos, habilidades y destrezas necesarias para desempeñar su labor en el área designada, además de poseer conocimientos amplios en el área de seguridad informática lo que hará posible el desarrollo y obtención de resultados esperados de la problemática planteada en este proyecto.

El investigador cumplirá con funciones de recolección de información y análisis de la misma, observará la realidad de su entorno y resolverá mediante la indagación y estudio de la hipótesis formulada con la ayuda de la organización sistémica de las diferentes actividades prestablecidas para cumplir con el alcance y objetivo del mismo.

11.2 RECURSOS TECNOLÓGICOS

Tabla 4. Recursos Tecnológicos.

Nombre	Cantidad	V. Unitario	Total
Computador portátil	1	$2.200.000	2.200.000
Horas de electricidad computador	550	$ 3.800	$ 2’090.000
Horas de internet	400	$ 1.200	$ 480.000
TOTAL	950	$ 2.205.000	$ 4’770.000

Fuente: Autor

12 CONCLUSIONES

En Colombia la investigación forense proporciona a la administración de justicia evidencia científica imparcial sobre las circunstancias de tiempo, modo y lugar en el que ocurrieron los hechos motivo de investigación, de este modo la investigación forense digital está cambiando la manera de resolver los procesos legales en el país, pues este tipo de investigación brinda una amplia asesoría sobre los temas que le atañen, a las unidades de fiscalías, tribunales y demás autoridades competentes, además de servir en la verificación y control de las pruebas periciales y exámenes forenses practicados por los cuerpos de Policía Judicial del Estado y los demás organismos a solicitud de la autoridad competente.

En los laboratorios forenses no solo son necesarios excelentes equipos tecnológicos, si no también se requiere de un personal entrenado y con experiencia en la aplicación y ejecución de los procesos y procedimientos que permitan desarrollar de forma oportuna, eficiente y eficaz los requerimientos que la justicia exija. Por otra parte, cabe mencionar que un laboratorio forense para la realización de imágenes y su respectivo análisis con el fin de asegurar la integridad de la evidencia más que herramientas debe aplicar técnicas, actualmente las más usadas para tal fin no solo en Colombia si no a nivel mundial son: Los metadatos, la matriz de cuantización y el PRNU (Análisis de ruido de foto respuesta no uniforme).

Dentro de la ley 1273 de 2009 se encuentran descritos los diferentes delitos cibernético e informáticos, esta ley se encuentran dividida principalmente en dos partes, la primera dicta medidas penales de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; la segunda se centra en los ciudadanos que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero. Bajo esta ley colombiana se pretende ser equivalente con la de otros países en cuanto a la normatividad del cibercrimen, el cual he venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales, situaciones y conceptos ya descritos dentro de la presente monografía.

Al realizar el análisis de cómo se lleva a cabo la presentación y descripción de un caso forense, se evidencia la manera de como una investigación a través de la evidencia digital obtenida del equipo afectado se utiliza para la resolución de un proceso legal por medio de la cadena de custodia y la entrega de la evidencia hallada, entregada en los formatos anexos (responsable cadena de custodia, registro cadena de custodia), al emplear las herramientas tecnológicas diseñadas

para este tipo de investigaciones como lo es el software especializado y los equipos tecnológicos que se encuentran disponibles en un laboratorio forense digital con el fin de que ésta sea comprendida y aceptada por los diferentes entes de control.

Por último se determinan los alcances que puede tener una investigación forense dentro de un proceso legal en Colombia teniendo en cuenta la ley 1273 de 2009, en la cual se aplican nuevas tecnologías, permitiendo así a los especialistas del área forense la elaboración de informes periciales los cuales facilitan a los diferentes entes de control, el correcto procedimiento para la resolución de los casos en cuanto a delitos informáticos se refiere.

13 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, malware, injurias y/o calumnia, ransomware, pishing, ingeniera social, entre otras. A continuación veremos algunas recomendaciones que nos ayudara a prevenir estos ataques:

13.1. Ataques Sexting

Figura 32. Evitar ataques sexting.

Fuente: Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). (2016). Sexting. [Imagen]. [Consultado: 10 de noviembre de 2017]. Disponible en Internet https://caivirtual.policia.gov.co/sites/default/files/bacin_-_001_0_0.pdf

Tabla 5. Recomendaciones Sexting.

Ítem	Acciones
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)

Fuente: Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). [Consultado: 10 de noviembre de 2017]. Disponible en Internet https://caivirtual.policia.gov.co/sites/default/files/bacin_-_001_0_0.pdf

13.2. Evitar Ataques Ransomware

Tabla 6. Recomendaciones Ransomware.

Ítem	Acciones
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)

Fuente: Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). [Consultado: 10 de noviembre de 2017]. Disponible en Internet https: //caivirtual.policia.gov.co/sites/default/files/ransomware_wannacry_0.pdf, p, 2, 2017

13.3. Evitar ataques grooming

Figura 33. Ataque Grooming.

Fuente: Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). Como evitar un grooming. [Imagen]. [Consultado: 10 de noviembre de 2017]. Disponible en Internet https://caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf

Tabla 7. Recomendaciones Grooming.

Ítem	Acciones
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)

Fuente: Policía Nacional de Colombia (Dirección de investigación Criminal e Interpol). Consultado: 10 de noviembre de 2017. Disponible en Internet https: //caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf, p,2, 2016).

14 DIVULGACIÓN

La divulgación de este documento de investigación se realizará inicialmente a través de correo electrónico a todo los interesados en los temas de informática forense, como lo son los compañeros de la Especialización en Seguridad Informática de la UNAD.

Por otra parte esta investigación será publicada en el siguiente blog:

- https://aspectoseticosylegalesblog.blogspot.com/2017/12/que-alcances-puede-tener-una.html

15. BIBLIOGRAFÍA

Acevedo González, Diego Fernando, D. F. (enero de 2016). *http://cv.uoc.edu.* Obtenido de http://cv.uoc.edu/webapps/dspace_rei/bitstream/10609/56284/7/dgonzalez85TFM0916mem%C3%B2ria.pdf

Castro Guerra, Christian David, C. D. (2014). Análisis y aplicación de software para la recuperación forense de evidencia digital en dispositivos móviles android. Quito, Ecuador: Pontificia Universidad Católica del Ecuador.

Estrada Garavilla, Miguel. (2008). *https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf.* Obtenido de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Extractor Bulk. (2015). *Aplicación para análisis informático*. Obtenido de http://www.forensicswiki.org/wiki/Bulk_extractor: http://www.forensicswiki.org/wiki/Bulk_extractor

Jaramillo Arciniegas, Diego Alejandro., & Torres Moncada, Martha Liliana. (2016). *http://repository.unimilitar.edu.co*. Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/14401/1/TorresMoncadaMarthaLiliana2016.pdf

Gaviria Pablo, Andrés. (10 de 01 de 2015). *http://repository.unad.edu.co/.* Obtenido de http://repository.unad.edu.co/handle/10596/4008

Lavin, Murena. (16 de junio de 2010). *http://www.magazcitum.com.mx*. Obtenido de http://www.magazcitum.com.mx/?p=24#.WSZe4PmGPIU

m.20minutos. (19 de septiembre de 2017). Dos años y medio de cárcel para un joven que instaló un sistema espía en el móvil de su pareja. *Diario 20minutos*, pág. 14.

Mamé, Kass. (7 de octubre de 2014). *https://es.slideshare.net*. Obtenido de https://es.slideshare.net/ksamlop/ley-de-delitos-informticos-en-el-per-39978262

Mattica. (02 de marzo de 2012). *https://mattica.com* . Obtenido de https://mattica.com/como-asegurar-la-evidencia-forense-digital/

Gaviria Estrada, Mguel. (2008). *https://www.unifr.ch.* Obtenido de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

MinTic. (4 de enero de 2009). *http://www.mintic.gov.co.* Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Noblett, Michael G. (2000). *Recovering and Examining Computer Forensic Evidence.* Scientific Working Group on Digital Evidence (SWGDE).

Plainsight. (2008). *Aplicación para análisis informático*. Obtenido de http://www.plainsight.info/index.html

Ramos, Alejandro. (marzo de 2011). *http://www.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

-------- (marzo de 2011). *http://www.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

-------- (marzo de 2011). *http://www.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

-------- (25 de marzo de 2011). *http://www.securitybydefault.com/*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

-------- (25 de marzo de 2011). *http://www.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

-------- (25 de marzo de 2011). *http://www.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

Ros Pedrera, Alberto José. (2005). Proyecto de grado de Alberto José PedrClasificación y estudio de herramientas para periciales informático. *Proyecto de grado de Alberto José PedClasificación y estudio de herramientas para periciales informático.* España: Proyecto de grado de Alberto José Pedrera Ros (2015) Clasificación y estudio de herramientas para perihttps://riunet.upv.es/bitstream/handle/10251/55775/Memoria.pdf?sequence=1.

Saravia, Verónica Mamani (2015). Método forense en redes de telecomunicación para la admisión de evidencia digital en la justicia Bolivariana. La Paz, Bolivia: Universidad Mayor de San Andrés.

Sierra Bedoya, Luis Fernando. (2008). *La Prueba en el Proceso Penal Colombiano.* Bogotá: ISBN 978-958-8374-10-9.

Valencia Sambony, Williams. (marzo de 2011). *http://problemasconlatecnologia.blogspot.mx*. Obtenido de http://problemasconlatecnologia.blogspot.mx/2011/03/informatica-forenseif-marco-conceptual.html

Vázquez, Andrés. (15 de febrero de 2012). *https://mattica.com*. Obtenido de https://mattica.com/evidencia-forense-digital-pruebas-validas-para-procesos-legales/

-------- (2 de marzo de 2012). *http://tic-seguridad.blogspot.mx*. Obtenido de http://tic-seguridad.blogspot.mx/2012/03/los-delitos-informaticos-y-la-evidencia.html

16. ANEXOS

16.1. ANEXO A Formato primer responsable de cadena de custodia

	USO EXCLUSIVO POLICIA JUDICIAL No. CASO
No. Expediente CAD	Dto / Mpio / Ent / U. Receptora / Año / Consecutivo

ACTUACION DEL PRIMER RESPONDIENTE -FPJ-4-

Departamento | Municipio | Fecha | Hora

1. LUGAR DE LOS HECHOS

DIRECCION: _____

UBICACIÓN EXACTA

BARRIO _____ ZONA _____

LOCALIDAD _____ VEREDA _____

CARACTERISTICAS _____

HORA PROBABLE DE OCURRENCIA DE LOS HECHOS _____

2. PROTECCION AL LUGAR E LOS HECHOS

ACORDONAMIENTO SI ☐ NO ☐

3. OBSERVACIONES DEL LUGAR E LOS HECHOS

¿HUBO ALTERACION DEL LUGAR DE LOS HECHOS? SI ☐ NO ☐

¿POR QUE ?

_____

_____

INTERVINIENTES _____

OBSERVACIONES _____

4. INFORMACION OBTENIDA SOBRE LOS HECHOS (Breve descripción)

_____

_____

_____

5. VICTIMAS

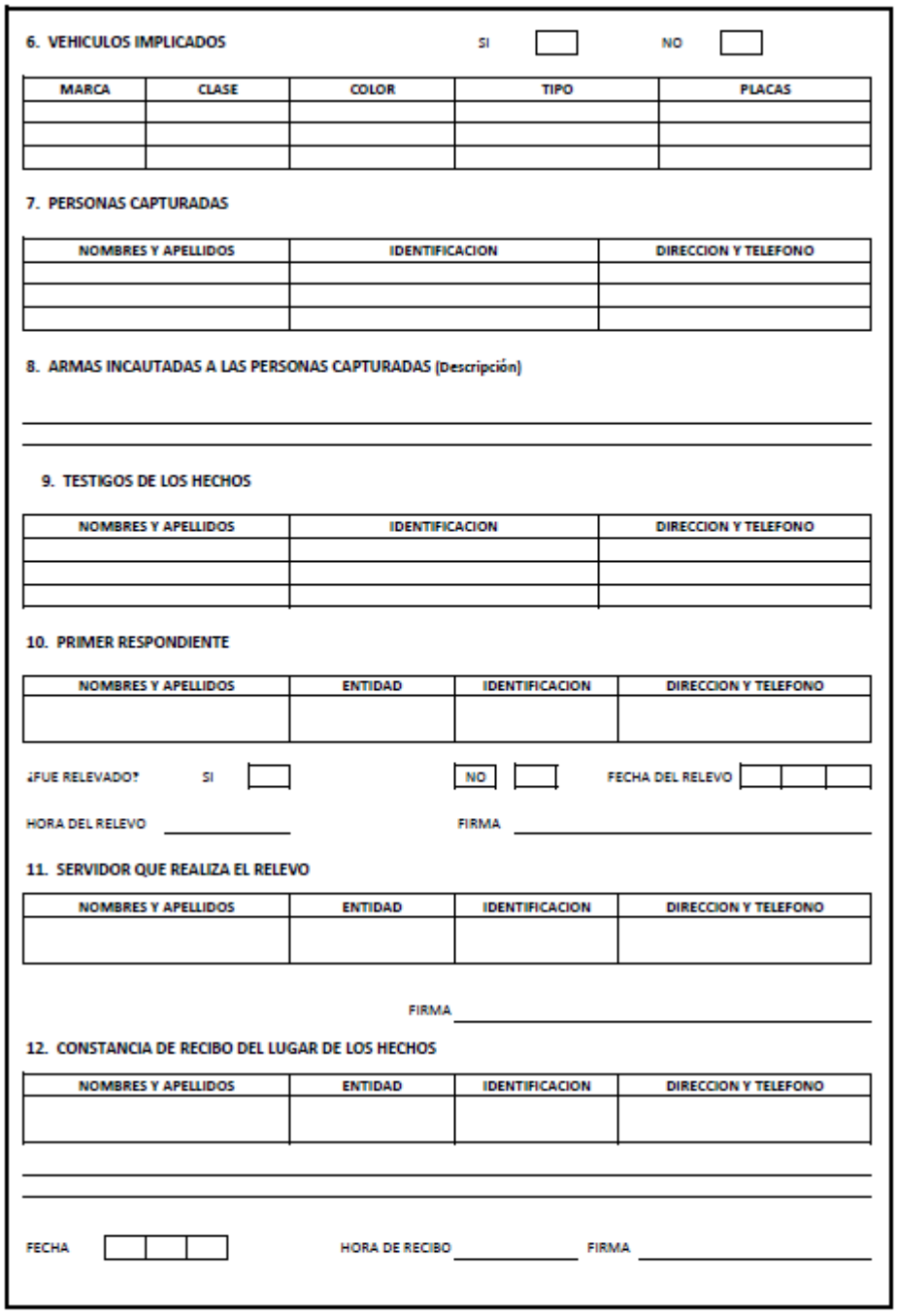
HERIDAS ☐ CUANTAS? ☐

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

MUERTAS ☐ CUANTAS? ☐

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

ANEXO A Formato primer responsable de cadena de custodia (Continuación)



6. VEHICULOS IMPLICADOS SI ☐ NO ☐

MARCA	CLASE	COLOR	TIPO	PLACAS

7. 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 DEL RELEVO ☐☐☐

HORA DEL RELEVO _____ FIRMA _____

11. SERVIDOR QUE REALIZA EL RELEVO

NOMBRES Y APELLIDOS	ENTIDAD	IDENTIFICACION	DIRECCION Y TELEFONO

FIRMA _____

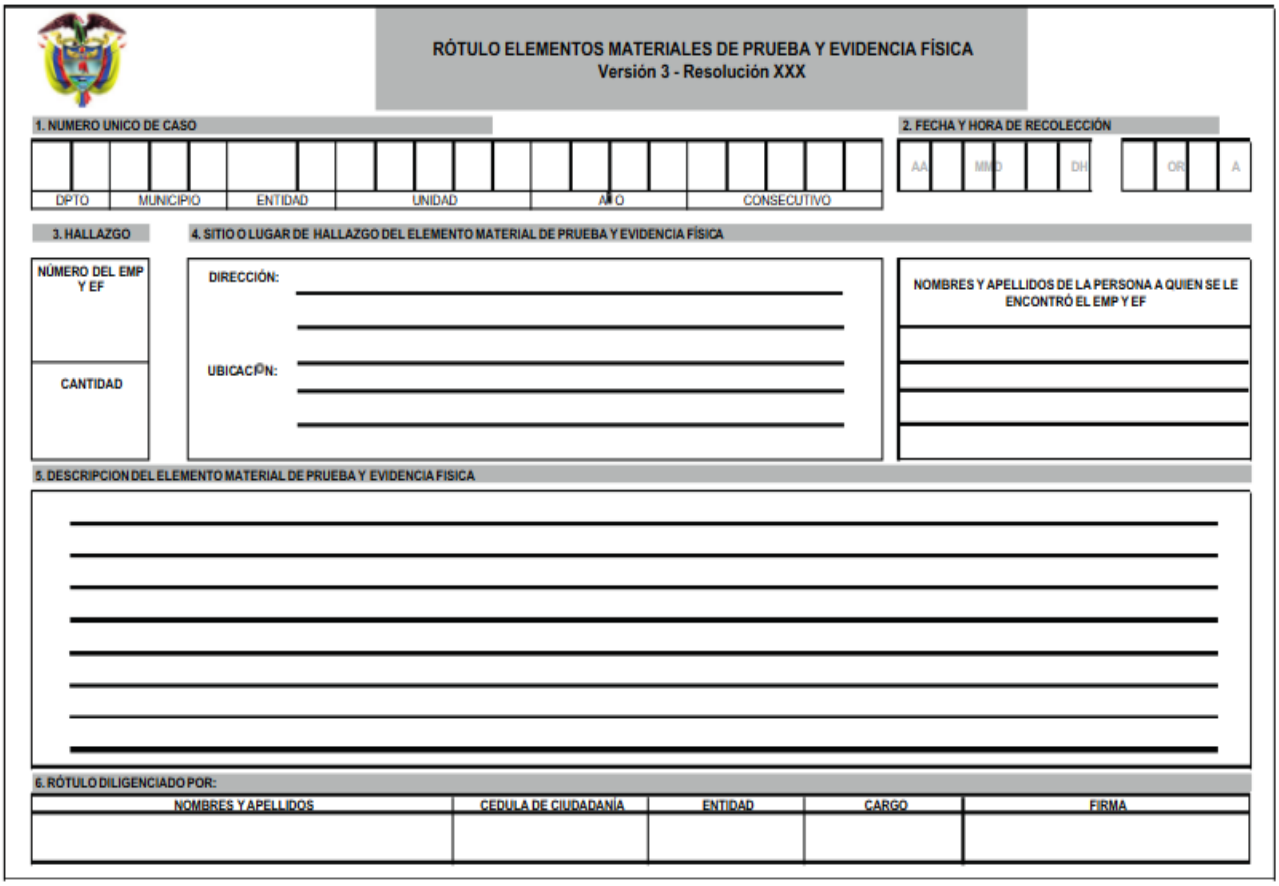
12. CONSTANCIA DE RECIBO DEL LUGAR DE LOS HECHOS

NOMBRES Y APELLIDOS	ENTIDAD	IDENTIFICACION	DIRECCION Y TELEFONO

FECHA ☐☐☐ HORA DE RECIBO _____ FIRMA _____

ANEXO A Formato primer responsable de cadena de custodia

16.2. 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 RECOLECCIÓN

AA MM DD OR A

3. HALLAZGO

NÚMERO DEL EMP Y EF

CANTIDAD

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

DIRECCIÓN:

UBICACIÓN:

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

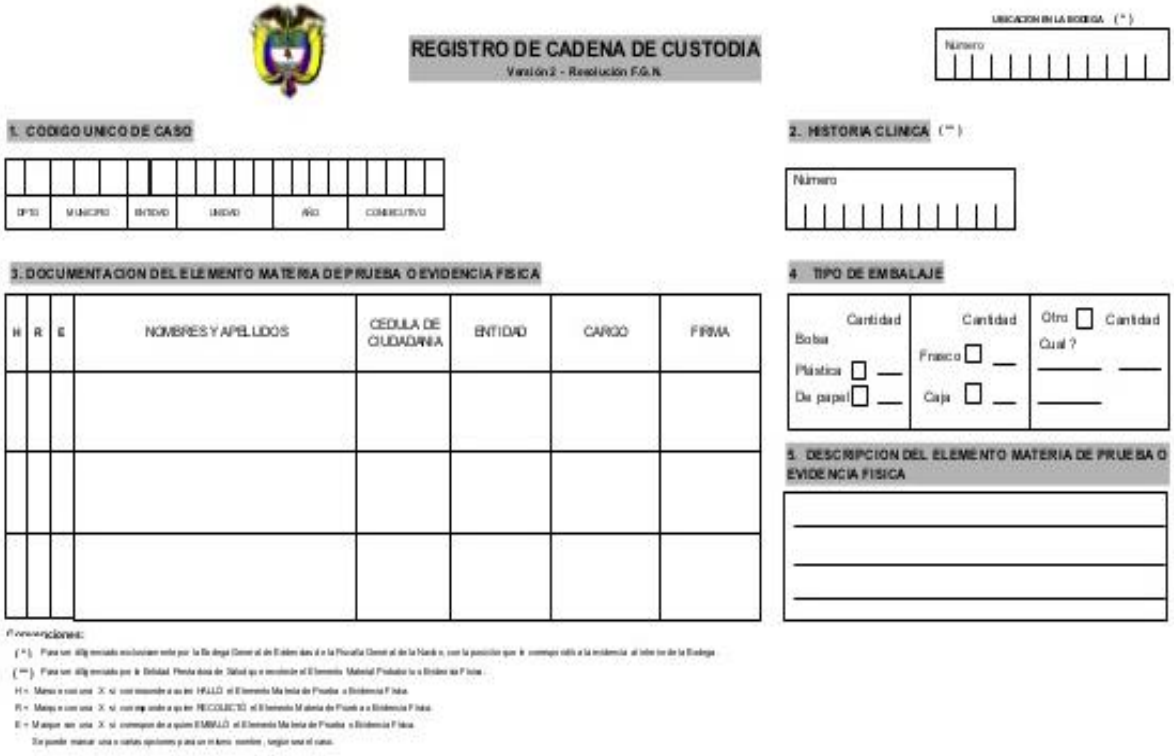
5. DESCRIPCION DEL ELEMENTO MATERIAL DE PRUEBA Y EVIDENCIA FISICA

6. RÓTULO DILIGENCIADO POR:

NOMBRES Y APELLIDOS	CEDULA DE CIUDADANÍA	ENTIDAD	CARGO	FIRMA

ANEXO B Rotulo EMP y EF

16.3. ANEXO C Formato de registro de cadena de custodia



REGISTRO DE CADENA DE CUSTODIA

Versión 2 - Resolución F.G.N.

UBICACION EN LA BODEGA (*)

Número

1. CODIGO UNICO DE CASO

DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO

2. HISTORIA CLINICA (**)

Número

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 exclusivamente por la Bodega Central de Evidencias de la Fiscalía General de la Nación, con la posición que le corresponda ubicar la evidencia al interior de la Bodega.

(**): Para ser diligenciado por la Entidad Prestadora de Salud que atendió el Elemento Material Probatorio o Evidencia Física.

H = Marque con una X si corresponde a quien HALLÓ el Elemento Material Probatorio o Evidencia Física.

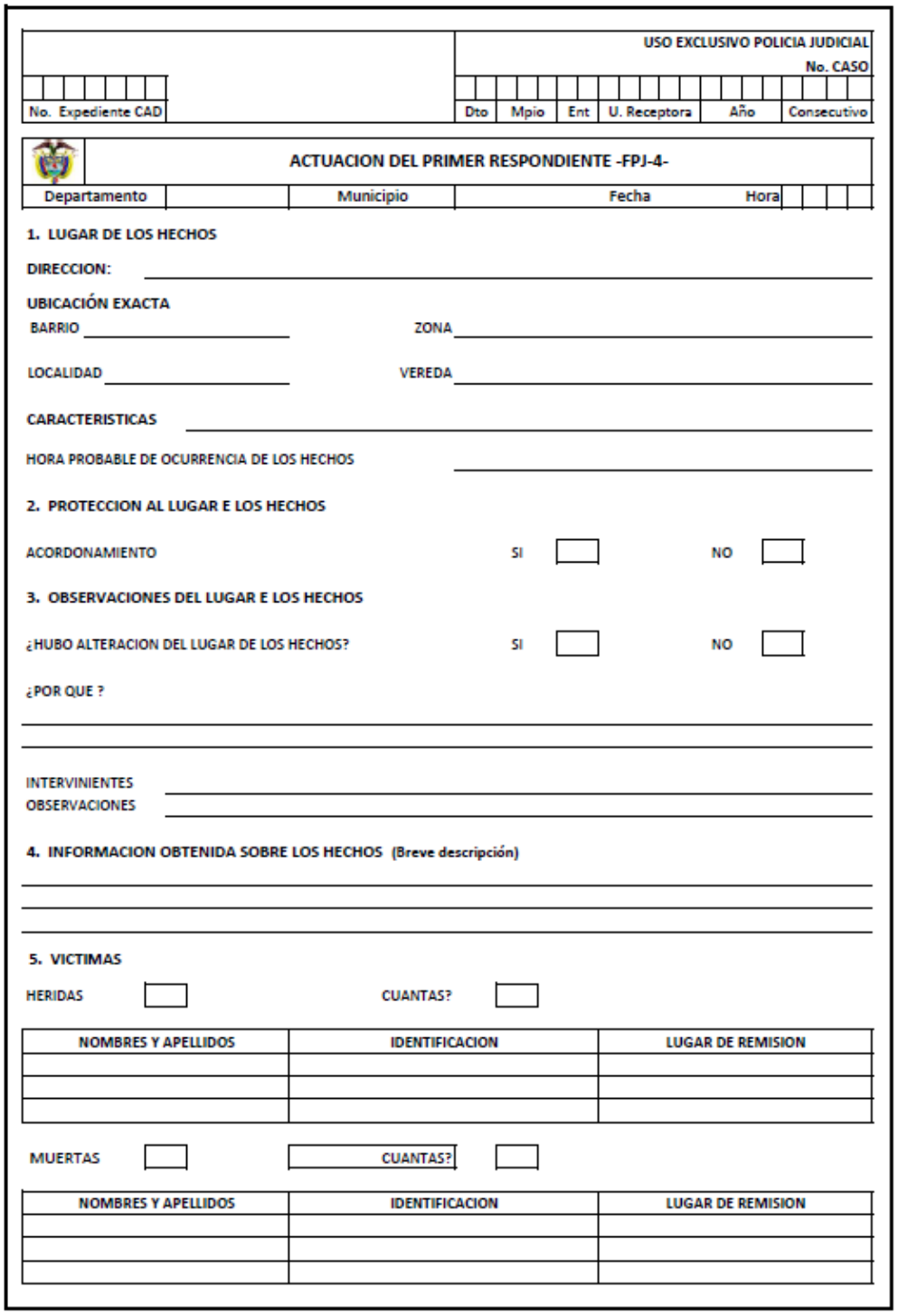
R = Marque con una X si corresponde a quien RECOLECTÓ el Elemento Material Probatorio o Evidencia Física.

E = Marque con una X si corresponde a quien EMBALÓ el Elemento Material Probatorio o Evidencia Física.

Se puede marcar una o varias opciones y para un mismo nombre, según sea el caso.

ANEXO C Formato de registro de cadena de custodia

16.4. ANEXO D Actuación Del Primer Respondiente



USO EXCLUSIVO POLICIA JUDICIAL

No. CASO

No. Expediente CAD	Dto	Mpio	Ent	U. Receptora	Año	Consecutivo

ACTUACION DEL PRIMER RESPONDIENTE -FPJ-4-

Departamento		Municipio	Fecha	Hora

1. LUGAR DE LOS HECHOS

DIRECCION: _____

UBICACIÓN EXACTA

BARRIO _____ ZONA _____

LOCALIDAD _____ VEREDA _____

CARACTERISTICAS _____

HORA PROBABLE DE OCURRENCIA DE LOS HECHOS _____

2. PROTECCION AL LUGAR E LOS HECHOS

ACORDONAMIENTO SI ☐ NO ☐

3. OBSERVACIONES DEL LUGAR E LOS HECHOS

¿HUBO ALTERACION DEL LUGAR DE LOS HECHOS? SI ☐ NO ☐

¿POR QUE ?

_____

_____

INTERVINIENTES _____

OBSERVACIONES _____

4. INFORMACION OBTENIDA SOBRE LOS HECHOS (Breve descripción)

_____

_____

_____

5. VICTIMAS

HERIDAS ☐ CUANTAS? ☐

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

MUERTAS ☐ CUANTAS? ☐

NOMBRES Y APELLIDOS	IDENTIFICACION	LUGAR DE REMISION

ANEXO D Actuación del primer responsable

ANEXO D Actuación Del Primer Respondiente (Continuación)

6. VEHICULOS IMPLICADOS SI ☐ NO ☐

MARCA	CLASE	COLOR	TIPO	PLACAS

7. 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 DEL RELEVO ☐☐☐

HORA DEL 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 RECIBO _____ FIRMA _____