PROPUESTA DE UN MODELO DE PROCEDIMIENTO PARA EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, ACORDE A LA NORMATIVIDAD COLOMBIANA SOBRE DELITOS INFORMÁTICOS.

PABLO ANDRÉS GAVIRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2015

PROPUESTA DE UN MODELO DE PROCEDIMIENTO PARA EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, ACORDE A LA NORMATIVIDAD COLOMBIANA SOBRE DELITOS INFORMÁTICOS.

PABLO ANDRÉS GAVIRIA

Trabajo de grado en la modalidad de monografía, como requisito para optar por el título:
Especialista en Seguridad Informática

Asesor:
Ing. Jhon Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2015

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., 10 de Noviembre de 2015

A nuestro Creador y arquitecto perfecto, por la oportunidad que me da para materializar sus Dones en cada uno de las metas que he alcanzado.

A mi madre, quien con su prudencia y oraciones al creador, ha sido fiel seguidora y cómplice de mis planes y proyectos.

Con Cariño y Aprecio: Luz María Gaviria.

AGRADECIMIENTOS

A la Fiscalía General de la Nación, por darme la oportunidad de ser parte activa en el cumplimiento de su Misión Constitucional, para desarrollar y aplicar el conocimiento adquirido durante estos años.

A mi Cuerpo Técnico de Investigación CTI Subdirección Seccional de Policía Judicial Nariño, sus directivos y compañeros, quienes día a día con el trasegar en el campo de la investigación, me aportaron desde su experiencia elementos claves para la consolidación y feliz término de este documento.

A la Universidad Nacional Abierta y a Distancia UNAD, como fuente indiscutible del saber y respaldo absoluto de las bases académicas, que permitieron enriquecer mi formación en el campo profesional.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

RESUMEN

La presente monografía en su pretensión, revisa la Normatividad vigente en Colombia frente al tema de los Delitos Informáticos, analiza las Norma Técnicas de Calidad NTC-ISO/IEC 17025 e ISO/IEC 27037:2012, y las Directrices emitidas por la ASCLD/LAB (American Society of Crime Laboratory Directors /Laboratory Accreditation Board), las cuales en su estructura, permitieron aportar desde su aplicación, el desarrollo de un Procedimiento y una Guía, como documentos que reúnen los parámetros frente al manejo de la evidencia digital.

Palabras clave: primer respondiente, perito informático, laboratorio de Informática forense, Normas Internacionales, delitos informáticos.

INTRODUCCIÓN

Desde la implementación de las Tecnologías de la Información y la Comunicación TIC como herramientas alternas para el cumplimiento efectivo en el desarrollo de nuestras actividades, el auge de los dispositivos electrónicos, las aplicaciones y su innegable vínculo con la Internet, han creado un mundo virtual y paralelo en el que converge mucha información. El acceso a entidades e instituciones de carácter público, privado y gubernamental han abierto una gran puerta de entrada a todo tipo de datos, como una nueva fuente utilizada por personas o personajes, quienes han encontrado en ella nuevos medios para alcanzar un objetivo o beneficio personal, que no siempre es el mejor.

Muchos de esos procesos o tareas desarrollados en el ejercicio diario, ya sea por desconocimiento, curiosidad o con un propósito claro y definido, pueden afectar la buena convivencia social, y aún más cuando el enfoque generalizado por alcanzar las tendencias mundiales y ser parte activa de los paradigmas de la tecnología, trajeron consigo una "actualización" fruto de la articulación de esfuerzos y recursos para extender el conocimiento frente al manejo y operación de todo tipo de dispositivos enmarcados en el tema de la informática, dejando de lado la conjunción del tema de los valores como base de estos nuevos escenarios.

Es ahí donde esta "transformación social" basada en el crecimiento tecnológico, trajeron consigo conductas negativas que van en contra de la normatividad, y el desconocimiento de muchos sectores frente a su tratamiento, podría verse reflejado en el incremento significativo de sucesos, con un panorama de impunidad, aun cuando existan herramientas y normas jurídicas que sancionan estas conductas.

Hablar de delitos desde el campo Informático, no solo en Colombia, involucra el conjugar un conocimiento del campo jurídico y tecnológico, enfocado a la obtención de evidencias, disciplinas que deben ser abordadas de manera conjunta y detallada; concepción que será la base y punto de partida para el desarrollo de la presente investigación, el cual en su pretensión podría ser utilizado como herramienta informativa dentro de un proceso de socialización, formación y/o educación frente a esta temática.

Actualmente, Colombia cuenta con el sistema penal acusatorio, el cual introdujo el término de evidencia, como:

> "Todo aquello que tiene vocación probatoria y que es aducido por las partes en el juicio para probar o excluir los elementos del delito, el grado

> de responsabilidad del acusado, circunstancias de atenuación o agravación punitivas, las consecuencias del daño causado y cualquier otro aspecto sustancial del debate"[1]

Así como también un marco juicio basado en una normatividad la cual reglamenta el tema de los delitos informáticos materializada en la ley 1273 de 2009 denominada "De la protección de la información y de los datos", la cual desde su promulgación el estado ha venido reforzando el tema en su tratamiento y prevención.

Y finalmente el régimen probatorio Colombiano, consagrado en el Código de Procedimiento Civil, sección tercera, Título XIII, y en la Ley 527 de 1999 denominada Ley de comercio electrónico, la cual soporta desde el tema jurídico la admisibilidad y fuerza probatoria de la prueba de los mensajes electrónicos, desde los parámetros de autenticidad, confiabilidad y autenticidad. Sin embargo, en mención de algunos apartes presentados en la publicación de Pietro Bogotá y Moreno Peña sobre la evidencia digital en Colombia, afirman que:

> Surge la necesidad de preguntarse si dicha regulación es suficiente para abarcar un tema de tanta trascendencia como es la evidencia digital, teniendo en cuenta que diariamente aumentan los eventos en que es transmitida y manejada la información a través de medios electrónicos[2].

Estos argumentos han permitido desarrollar y formular desde la presente investigación, una serie de sugerencias frente a los Procedimientos, actividades técnicas forenses, enfocadas a contribuir en gran medida con el adecuado tratamiento de la evidencia digital, como soporte legal en la consecución de pruebas, base de la investigación judicial de los delitos informáticos.

---

[1] REPÚBLICA DE COLOMBIA, Fiscalía General de la Nación. Manual de procedimientos de la Fiscalía en el sistema penal acusatorio. Bogotá D.C., 2006, p.158.

[2] PIETRO BOGOTÁ, Diana y MORENO PEÑA Claudia. Evidencia Digital en Colombia: Una reflexión en la práctica. En: Publicaciones Corporación Excelencia en la Justicia. Bogotá. D.C., 2007. P.1.

1. PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del Problema

La aparición de delitos desde el campo Informático en la sociedad, su constante "tecnificación" o especialización, crean la necesidad de reforzar las herramientas y elementos que permitan establecer su comisión, y soporten de manera adecuada y legal la actividad investigativa.

Desde el entorno legal, debilidades en la aplicación de los procedimientos forenses frente al tratamiento de la evidencia digital desde su hallazgo, podrían interferir en una investigación penal, perdiendo todo valor probatorio y su admisibilidad como soporte en la hipótesis de un caso.

Partiendo de esta concepción, es necesario desarrollar la presente investigación que permita formular recomendaciones en los Procedimientos inmersos de la criminalística Forense, enmarcada en el análisis de la normatividad vigente de los delitos informáticos en Colombia, las normas internacionales y la experiencia en el trabajo de campo y de laboratorio adquirida por el autor como Policía Judicial, que sirva como estrategia para contribuir con el adecuado manejo de la evidencia digital, su estudio, análisis y presentación. Así como también, en una guía de conocimiento o herramienta de socialización en procesos de formación entorno a esta temática.

1.2 Formulación del problema

¿Cómo mejorar el tratamiento de la evidencia digital y la aplicación de los procedimientos que permitan soportar desde el entorno legal, la consecución de Elementos materiales Probatorios o Evidencia Física (en adelante EMP y/o EF), frente a la normatividad de Delitos Informáticos existente en Colombia?

1.3 Objetivos

1.3.1 Objetivo general

Formular un Procedimiento y una Guía con el fin de mejorar el tratamiento de la evidencia digital como medio técnico de soporte judicial, mediante la aplicación de mecanismos forenses, dirigido apersonas que desarrollan funciones y tareas de Investigación judicial desde el campo Técnico – Científico.

1.3.2 Objetivos específicos

- ✓ Analizar en contexto, el panorama actual de los delitos informáticos en Colombia.

- ✓ Revisar las estructuras de las Norma Técnicas de Calidad aplicables en Colombia, así como también las Normas internacionales frente al tratamiento de la evidencia digital.

- ✓ Identificar formas, que desde un Procedimiento y una guía, mejoren el tratamiento de la evidencia digital desde su hallazgo hasta su presentación.

- ✓ Proponer algunos temas de prevención frente a los delitos informáticos en Colombia.

1.4 Justificación

Uno de los pilares dentro de la investigación judicial sin duda alguna es la estructuración de una hipótesis, fundamentada en la consecución de evidencia que la soporten y permitan establecer la veracidad en la ocurrencia de los hechos.

La veracidad de la evidencia, concebida tras un tratamiento adecuado de los EMP y/o EF y soportada debidamente tras los procedimientos aplicados, pueden ser la base de toda una investigación en el campo de la informática forense, los cuales sumados a diferentes actividades complementarias, son determinantes a la hora de establecer la culpabilidad de un sujeto frente a la comisión del delito.

Actualmente desde el ámbito jurídico es claro la existencia de la Ley 1273 de 2009 “de la protección de la información y de los datos”, la cual regula y reglamenta una serie de conductas que en su aplicación involucra procesos en el campo técnico y tecnológico, y esa articulación ha creado una serie de tratados y posiciones frente al tema, y su inadecuada interpretación puede verse reflejado en impunidad.

Estos vacíos frente al tratamiento de la Evidencia Digital se denotan en la falta de Procedimientos debidamente estructurados y el desconocimiento por las partes, razón por la cual creemos imperativo contribuir con el desarrollo de una propuesta que permita estandarizar los procesos entorno a la investigación forense frente a su manejo desde un punto de vista del campo técnico, aportando los conocimientos adquiridos y formulados por la Universidad Nacional Abierta y a Distancia UNAD, dentro del proceso de formación en el área de la Especialización en Seguridad Informática.

2. MARCO DE REFERENCIA

2.1 Antecedentes

- El Proyecto para el mejoramiento del laboratorio del grupo investigativo de delitos informáticos del Cuerpo Técnico de Investigación (CTI) Pasto. Tesis presentada por Estefanía Muñoz Cerón, Universidad de Nariño, Facultad de Ingeniería Electrónica. San Juan de Pasto. 2014, el cual en su estructura refiere la formulación de un proyecto para la adecuación del laboratorio de informática forense, haciendo referencia especialmente a la norma NTC-ISO/IEC 17025, que oriente a la Fiscalía General de la Nación en las actividades frente a la acreditación del laboratorio Forense del Grupo de Delitos Informáticos, el cual como punto de partida permite visualizar la necesidad de estandarizar los Procedimientos frente al tratamiento de la evidencia digital como elementos necesarios y obligatorios en una Norma Técnica de Calidad.

- El Diseño e implementación de un centro de informática forense en la Universidad Autónoma de Occidente. Tesis de grado elaborada por Guillermo Umaña Ramírez e Isabel Cristina Mosquera Navarrete. Universidad Autónoma de Occidente, Facultad De Ingeniería. Santiago de Cali 2014.

  > El proyecto reúne una serie de recomendaciones frente al montaje de un laboratorio de informática forense (LIF) en la Universidad Autónoma de Occidente (UAO), la cual consta en crear el modelo de implementación, es decir, definir todo lo necesario para su funcionamiento a nivel de software, hardware, manejo de riesgos, recurso humano y recurso económico para su funcionamiento, la segunda etapa consiste en la implantación de este LIF, es decir, su puesta en marcha, lo cual implica su promoción, construcción y operación[3]

- El documento denominado Metodología para el análisis forense en Linux, artículo presentado por Msc. Luz Marina Santos Jaimes y por el Ing. Anderson Smith Flórez Fuentes. Universidad de Pamplona, grupo de investigación Ciencias Computacionales, Revista Colombiana de

[3] UMAÑA RAMÍREZ, Guillermo y MOSQUERA NAVARRETE, Isabel Cristina. Diseño e implementación de un centro de informática forense en la Universidad Autónoma de Occidente. Santiago de Cali. Universidad Autónoma de Occidente. (2014).

Tecnología avanzada. ISSN: 16-7257 Volumen2 – Número 20- 2012, el cual presenta los resultados de un estudio realizado sobre las metodologías de análisis forense aplicado al sistema operativo Linux, y permite aproximarse a estructurar un proceso general desarrollado por medio de fases o etapas.

- El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos electrónicos. Publicación realizada por el Dr. Alexander Díaz García. Universidad Santiago de Cali. 2011. Facultad de Derecho. Dirección de Postgrados. Documento que permite profundizar en conceptos fundamentales sobre delitos informáticos, sus principios, naturaleza y los elementos estructurales del delito.

- ESET Security Report Latinoamérica 2014, informe que presenta una recopilación acerca del panorama actual de la seguridad informática para esta zona del continente.

- El fraude Informático: Valoraciones técnico jurídicas. Tesis de grado presentada por Pamela Nataly Garzón Tapia y Marco Fernando Vizuete Gallardo, Universidad Técnica del Cotopaxi, unidad académica de ciencias administrativas y humanísticas. La Tacunga Ecuador 2009. Desde su trabajo, presenta la inadecuada regulación del fraude informático dentro del ordenamiento jurídico Ecuatoriano, que ocasiona daños patrimoniales a las personas naturales y jurídicas; un documento que aporta desde un punto de vista analítico la evolución de la regulación de los delitos informáticos, los esfuerzos alcanzados para articular una definición general sobre el mismo frente a un elemento común y la utilización de técnicas informáticas en la obtención de un resultado, los cuales siguen suscitando debates.

- La Auditoria Forense: Metodología, herramientas y técnicas aplicadas en un siniestro informático de una empresa del sector comercial. Tesis de grado elaborada por Viviana Marcela Villacís Ruiz. Escuela Superior Politécnica del Litoral. Instituto de Ciencias Matemáticas Auditoría y Control de Gestión, Guayaquil – Ecuador 2006. Trabajo que tiene como objeto principal, presentar acciones premeditadas para reunir pruebas, analizarlas y emitir un juicio, orientando a las generaciones futuras sobre la importancia de la auditoria forense informática.

- Conceptos y retos en la atención de incidentes de seguridad y la evidencia digital. Jeimy J. Cano. Universidad de los Andes. Facultad de Ingeniería,

obra que analiza los Procedimientos del análisis de la evidencia digital frente a los incidentes de seguridad informática, así como también algunas guías para enfrentarse al reto del tratamiento de la evidencia digital.

2.2 Marco teórico conceptual

2.2.1 Delitos informáticos. Todos en su formación tenemos una idea aproximada de lo que es delito, y más allá de su definición, sabemos que su materialización trae consigo una responsabilidad social y su sanción o castigo.

Desde la antigüedad la conducta humana es uno de los centros de estudio y análisis, debido a que el hombre vive inmerso y hace parte activa de una comunidad, la cual le brinda los elementos que necesita para suplir sus necesidades básicas, y las necesidades básicas de todo el grupo o colectivo, implantando o desarrollando la aplicación de un sistema normativo articulado en el respeto, y las sanciones a su incumplimiento.

Esta normatividad en su evolución, trajo consigo una serie de elementos que protegían los valores humanos, culturales y sociales propios de cada comunidad basados en sus creencias, y lo que era considerado como falta por un grupo, tal vez, en otra parte del mundo o en otra sociedad quizá no, o no se percibía como tal. Estas posiciones, trajeron consigo todo tipo de definiciones frente al concepto de delito, el cual ha ido cambiando según el tiempo y la cultura.

Una definición usual del delito lo refiere como: Una acción típica, antijurídica y culpable y para algunos autores punible. Aunque el objetivo de este documento no es el estudio pragmático del delito, me atrevería desde un punto de vista muy personal definir al delito como: Un comportamiento, el cual por voluntad propia, por imprudencia o por desconocimiento, va en contra a lo establecido por la Ley y afecta un derecho fundamental, o un bien jurídico protegido.

Esta situación conceptual no es ajena frente al tema de los Delitos Informáticos, sin embargo, debemos buscar una aproximación que permita articular la normatividad jurídica existente con los conceptos técnicos y tecnológicos, además de sus elementos.

Sobre el particular el español Romeo Casabona señala que:

> En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho delictivo o merecedor de serlo presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información[4]

Este concepto, nos permite inferir que al no existir una base jurídica que soporte el tema normativo frente a la protección de un bien tutelado, los delitos informáticos no pueden considerarse como tal, y se reemplazarían por la expresión de criminalidad informática.

El Dr. alemán Klaus Tiedemann considera que con la expresión:

> "Criminalidad mediante computadoras: se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos, [y señala además] que existe una amenaza sobre la esfera privada del ciudadano y los daños patrimoniales producido por el abuso de estos datos procesados"[5]

Para Nidia Callegari el delito informático: "es aquel que se da con la ayuda de la informática o de técnicas anexas"[6].

---

[4] ROMEO CASABONA, Carlos María. Poder Informático y Seguridad Jurídica. Madrid – España. Fundesco. (1987).

[5] TIEDEMANN, Klaus. Poder informático y delito, citado por: ACUARIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. Quito – Ecuador. Pontificia Universidad Católica del Ecuador.p.10.

[6] CALLEGARI, Nidia. Delitos informáticos y legislación. En: Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín - Colombia. No. 70 (julio-agosto-septiembre, 1985).

Según el Mexicano Julio Téllez-Valdés, define al delito informático desde dos formas: Típica y Atípica, refiriendo a la primera: “las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”, y a la segunda: “actitudes ilícitas en que se tienen a las computadores como instrumento o fin”[7].

Sostiene en este sentido Alberto Suárez Sánchez:

> Las formas posibles de vinculación de un computador a la realización de un delito son casi ilimitadas, dado que puede ser aprovechado para preparar un delito (Por ej., la elaboración de un plan criminal) o ejecutar una conducta delictiva (Pr ej., lograr la trasferencia de un activo no consentida) o impedir el descubrimiento de un delito y/o copartícipes (por la posibilidad de borrar cualquier rastro de la conducta criminal), y el mismo autor concluye que: el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales[8]

No obstante, frente a estas discusiones doctrinales de algunos tratadistas podemos inferir que sus conceptos se basan en que el delito informático se ha enmarcado en dos elementos básicos: Las acciones derivadas del funcionamiento de la máquina y sus resultados, y las acciones que, reuniendo las características de delito, se lleven a acabo utilizando al medio informático como instrumento para tal fin. Sin embargo, es claro que el delito informático contextualiza las conductas que afecten y estén en contra de un bien jurídico tutelado, ya que de lo contrario se pensaría que toda conducta castigada por la norma la cual utilice un computador o medio tecnológico, sería un delito informático.

En conclusión desde una percepción muy particular, planteamos un concepto que debería aproximarse al delito informático: Toda acción generada por una conducta ilícita, ya sea consiente, por omisión o desconocimiento, que sea realizada por una

---

[7] TELLEZ VALDÉS, Julio. Derecho informático: Los delitos informáticos Situación en México. Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Citado por: ACUARIO DEL PINO, Op cit., p. 11.

[8] SUÁREZ SÁNCHEZ, Alberto. La estafa informática. [En línea]. [citado en octubre 9 de 2014]. Disponible en Internet: dialnet.unirioja.es/descarga/articulo/3308847.pdf>

persona mediante el uso de cualquier elemento telemático, y que como consecuencia afecte un bien informático jurídico y/o material que se encuentra legalmente amparado y protegido por la Ley (bien jurídico Tutelado).

2.2.1.1 Estructura de los delitos informáticos. Tomando como base el planteamiento presentado por la Dra. Esc. María José Viega Rodríguez, podemos establecer la existencia de los siguientes elementos que enmarcan el delito informático:

> **Sujeto activo:** Define a la persona responsable de la comisión del delito, quien como sujeto, presenta una alta capacidad técnica en el manejo de equipos en el campo telemático, por lo general, son personas que tienen cargos sensibles, con accesos preferenciales a sistemas encargados de la administración de la información y los datos, con motivaciones enfocadas a infinidad de objetivos que van desde la simple curiosidad, el desafío personal, o por violar un sistema de información.
>
> **Sujeto pasivo:** Son las personas o entidades sobre las cuales recae la afectación de las conductas materializadas por el sujeto activo. Como característica visible cabe resaltar, que gran parte de los afectados no denuncian la ocurrencia de los hechos, por desconocimiento frente al tema jurídico, o en el caso de algunas entidades en especial las financieras, por las consecuencias frente al desprestigio de su imagen que esto podría causar.
>
> **Bien jurídico tutelado:** Hace referencia al bien material e inmaterial que ha sido lesionado o puesto en peligro por la conducta del sujeto activo, y para nuestro caso, que están debidamente protegidos por el Derecho Penal[9]

Según el Dr. Alexander Díaz García:

[9] VIEGA RODRÍGUEZ, María. Un nuevo desafío jurídico: los delitos informáticos. [en línea]. [citado en 10 de octubre de 2014]. Disponible en Internet: <http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf>

> El Derecho Penal sólo es aplicable cuando para la protección de los bienes jurídicos se han puesto en práctica otras medidas no represivas, que pueden ser, por ejemplo, de carácter laboral, administrativo o mercantil, y ellas han resultado insuficientes; por tanto, sería desproporcionado e inadecuado comenzar con una protección a través del Derecho Penal[10]

El bien jurídico tutelado es la base de las discusiones Dogmáticas frente al tema de los delitos informáticos, ya que para muchos como se expuso anteriormente, son conductas que se desarrollan con el uso de computadores y que NO existe un bien jurídico protegido, tomando simplemente el concepto como herramienta de ejecución. De esta forma, dichas conductas eran tratadas o enmarcadas como delitos tradicionales.

> **La pena:** Como elemento indispensable de una norma, es la sanción impuesta al responsable de la materialización de la conducta, una vez se haya comprobado la existencia de elementos como la Tipicidad, Antijuricidad y culpabilidad, la cual se refleja en el carácter económico y privativo de la libertad.

2.2.1.2 Características de los delitos informáticos. Como se pudo observar, son variadas las posiciones frente al concepto de un delito informático lo cual redunda también en sus características, sin embargo, podemos exponer una aproximación de las más comunes citando algunas presentadas por la Esc. María José Viega Rodríguez:

> Son conductas basadas muchas veces en la oportunidad.
>
> El tiempo y el espacio, son elementos que pueden obviarse a la hora de ejecutar las conductas.
>
> Su nivel de ocurrencia es alto, contrastado con el escaso nivel de denuncias presentadas.

---

[10] DÍAZ GARCÍA, Alexander. El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos electrónicos. [en línea]. [citado en 15 de octubre de 2014]. Disponible en Internet: http://www.redipd.org/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICOS_USC.pdf

Por su carácter técnico presentan un nivel alto en el campo investigativo, debido a la dificultad para obtener EMP y/o EF, que respalden la ocurrencia de los hechos.

Los sujetos activos en algunas ocasiones tienen la característica de tener ciertos conocimientos técnicos en el área informática y telemática, que facilitan la materialización de las conductas, eliminando cualquier rastro de su ocurrencia.

El nivel ocurrencia y materialización van de la mano con los avances tecnológicos.

Los EMP y/o EF son "volátiles", y susceptibles en muchas ocasiones de eliminación y modificaciones[11]

2.2.2 La seguridad informática. La información para una empresa o entidad se ha convertido en uno de sus activos más valiosos el cual requiere dentro de sus medidas prioritarias de administración, su protección y seguridad, aún más cuando es procesada electrónicamente ya que puede exponerse a todo tipo de amenazas y riesgos.

Para prevenir este tipo de situaciones, se ha desarrollado una disciplina llamada seguridad informática, que reúne al conjunto de elementos como normas, métodos, técnicas y procedimientos que se articulan entre sí, con el fin de garantizar seguridad de la información contenida en un medio tecnológico.

Una definición más precisa presentada por Mifsud Elvira. La define como: "La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio"[12].

Cualquier factor de vulnerabilidad que intervenga con alguno de estos principios, pone en riesgo la información generando así un incidente de seguridad informática, que en su tratamiento activa el proceso investigativo inmerso dentro

---

11 VIEGA RODRÍGUEZ. Op. cit., p. 4.

12 MIFSUD Elvira. MONOGRÁFICO: Introducción a la seguridad informática [en línea].2012. [citado en 20 de octubre de 2014]. Disponible en Internet: <http://datateca.unad.edu.co/contenidos/233001/Material/Unidad%20I/Proteccion_seguridad_infomatica.pdf>

de los parámetros y procedimientos enmarcados dentro del análisis forense, los cuales buscan establecer la necesidad de determinar el autor, los motivos que condujeron a realizar el ataque e identificar los métodos utilizados, mediante la obtención de evidencias que sirvan de soporte dentro de una investigación judicial y que a futuro puedan generar esquemas de mejoramiento para evitar la repetición de estos sucesos.

2.2.3 Elementos materiales probatorios o evidencia física. El artículo 275 del Código de Procedimiento Penal Colombiano, define como Elementos materiales probatorios y evidencia física:

> a) Huellas, rastros, manchas, residuos, vestigios y similares, dejados por la ejecución de la actividad delictiva;
>
> b) Armas, instrumentos, objetos y cualquier otro medio utilizado para la ejecución de la actividad delictiva;
>
> c) Dinero, bienes y otros efectos provenientes de la ejecución de la actividad delictiva;
>
> d) Los elementos materiales descubiertos, recogidos y asegurados en desarrollo de diligencia investigativa de registro y allanamiento, inspección corporal y registro personal;
>
> e) Los documentos de toda índole hallados en diligencia investigativa de inspección o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados allí;
>
> f) Los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público;
>
> g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen;
>
> h) Los demás elementos materiales similares a los anteriores y que son descubiertos, recogidos y custodiados por el Fiscal General o por el fiscal directamente o por conducto de servidores de policía judicial o

de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente[13]

Ahora bien, la Corte Suprema de Justicia sobre el particular refiere:

> Por elementos materiales probatorios y evidencia física el código entiende los relacionados en el artículo 275, y los similares a ellos que hayan sido descubiertos, recogidos y custodiados por la fiscalía directamente, o por conducto de sus servidores de policía judicial o de peritos del Instituto de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente; y los obtenidos por la defensa en ejercicio de las facultades consagradas en los artículos 267, 268, 271 y 272 ejusdem[14]

Podemos referir sobre los EMP y/o EF, son todo el conjunto de elementos que se encuentran inmersos en un proceso y soportan las hipótesis referidas como base de la investigación y que tienen un significado probatorio, y toman el valor de prueba legalmente válido, siempre y cuando hayan sido aceptados por el Juez, tras un proceso de debate, tal como lo precisa la Corte Suprema de Justicia:

> Para el ejercicio de la acción de revisión en el marco del sistema oral, se considera prueba, desde el punto de vista formal, no sólo la que ha sido sometida a debate ante un juez de conocimiento en un juicio oral, sino los llamados en el nuevo modelo de enjuiciamiento medios cognoscitivos, entre los que se encuentra los elementos materiales probatorios y evidencia física, los informes, el interrogatorio a indiciado, la aceptación del imputado y la prueba anticipada[15].

---

13 REPUBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31 de agosto de 2004). Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004). Diario Oficial. Bogotá D.C. 2004. no. 45658.

14 REPUBLICA DE COLOMBIA. CORTE SUPREMA DE JUSTICIA. Sala de Casación Penal. Auto del 15 de octubre de 2008. Diario Oficial. Bogotá D.C., 2008.no. 29.626. p. 10 y 11.

15 Ibíd., p 10.

En el sistema penal acusatorio colombiano, los medios de conocimiento descubiertos, o evidencias con un tratamiento adecuado, presentados en las audiencias de acusación y preparatoria y que son admitidos por el juez en la audiencia del juicio oral obtienen la calidad de prueba, y se clasifican en: testimonial, documental, pericial, científica o nobel, física y demostrativa.

Para nuestro caso particular, nos enfocaremos en la evidencia pericial, la cual según la publicación presentada por Cristancho Vargas, la define como:

> La evidencia pericial está constituida por el concepto de un experto, es decir, una persona con conocimientos científicos, técnicos o especializados, sobre un hecho relacionado con el caso; el perito debe materializar sus conclusiones en un informe técnico que debe presentarse y sustentarse ante el juez en audiencia pública[16].

2.2.4 La Evidencia Digital. Desde el campo de la informática forense, uno de los aspectos básicos en el análisis es la consecución de elementos válidos dentro de una investigación, de tal forma que su hallazgo, recolección, preservación, análisis y presentación, se encuentren debidamente soportados y documentados, bajo un entorno de legalidad.

Ese soporte y documentación se desarrolla mediante:

- ✓ La aplicación del Procedimiento de cadena de custodia y los parámetros establecidos por la Fiscalía General de la Nación, los cuales articulan un protocolo en donde se garantice frente a los elementos susceptibles de análisis, la integridad, continuidad, autenticidad, identidad y registro, de acuerdo a su clase y naturaleza[17], mediante el rotulado o etiquetado, embalaje y/o empaquetamiento, acompañado de un registro de continuidad, el cual cronológicamente especifique las personas que

---

16 Universidad Católica de Colombia. Caracterización del concepto de evidencia demostrativa y su uso en el juicio oral. Bogotá D.C. [en línea]. [citado el 30 de marzo de 2015]. Disponible en Internet:<http://portalweb.ucatolica.edu.co/easyWeb2/files/105_14819_caracterizacian-del-concepto-de-evidencia-demostrativa.pdf>

17 REPUBLICA DE COLOMBIA. FISCALIA GENERAL DE LA NACIÓN. Manual del sistema de cadena de custodia: 7.3. FGN-CC-REREMP: Recolección, embalaje y rotulado de los elementos materia de prueba o evidencias [en línea]. [citado el 22 de octubre de 2014]. Disponible en Internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634>

tuvieron contacto directo con los EMP y/o EF, en todo su recorrido hasta su presentación en juicio y/o disposición final.

- ✓ La individualización o identificación de la evidencia digital, realizada mediante la aplicación dela función de “Hasheo” o “hash”, que representa en resumen, la manera compacta de un archivo o conjunto de datos, como resultado a la aplicación de algoritmos matemáticos como elMD5 o SHA1, lo cual garantiza la autenticidad e integridad de la información. Muchos lo asemejan como una huella digital del archivo.

En sí mismo, los datos, la información o sus fragmentos, que hayan sido almacenados y/o procesados en medios electrónicos y que tengan relación directa con la ocurrencia de hechos enmarcados dentro de la normatividad de los delitos informáticos, son considerados evidencia digital, y su tratamiento requiere de un cuidado especial, el cual es abordado en detalle más adelante.

2.2.5 Dispositivos de almacenamiento digital. Corresponde a todo el conjunto de dispositivos electrónicos, los cuales se fundamentan en Leyes físicas de la electricidad y el magnetismo para almacenar los datos sobre diversos materiales.

Dependiendo del principio utilizado para almacenar la información, podemos clasificarlos en:

- Dispositivos Magnéticos: los cuales utilizan partículas cargadas eléctricamente, que son activadas por un cabezal de lectura/escritura por medio de un imán, encargado de orientarlas y determinar su posición al escribir y leer los bits de datos.

  En este grupo encontramos las antiguas cintas y diskettes, así como también los Discos Duros y sus tipos: SCSI, IDE, ATA, PATA, SATA, SAS, ZIF, USB, Firewire o Thunderbolt.

- Dispositivos Ópticos: Una definición presentada por el Ing. Miguel Rebollo Pedruelo, refiere a esto como:

> Elementos que emplean una luz láser en lugar de un imán para leer y escribir bits de datos en una capa reflectante. Esta capa está protegida por una superficie de plástico transparente que permite que la luz pase. La capacidad de los discos ópticos varía en función de su tipo y del número de capas de datos que

contengan. La velocidad de lectura y de escritura depende del dispositivo lector/grabador[18]

En este grupo encontramos: CD-ROM (solo lectura), CD-R y CD-RW (en su orden discos grabables y re grabables), DVD, DVD–R, DVD-RW, DVD +R DL (Dispositivos de escritura de doble capa) y BLU-RAY.

- Dispositivos de estado Sólido: Su tecnología está basada en materiales similares a los empleados en las memorias (mediante chips), pero con la salvedad de que son capaces de mantener la información de forma definitiva sin necesidad de corriente eléctrica. Este tipo de tecnología no ha desplazado a la memoria RAM en los ordenadores porque es más lenta y porque el número de ciclos de escritura está limitado, por lo que con el tiempo iríamos perdiendo capacidad de memoria (más rápidamente que en el caso de un disco).

  En este grupo encontramos: Las tarjetas de memoria CF (Compact flash), SD (secure digital), MS (Memory Stick), MSD (micro memory stick), MMC (multimedia card), las USB o pendrive, y los SSD (solid state drives).

2.2.6 Sistema de archivos. Para Lars Wirzenius, Joanna Oja y Stephen Stafford, un sistema de archivos son:

> "Los métodos y estructuras de datos que un sistema operativo utilizan para seguir la pista de los archivos de un disco o partición; es decir, es la manera en la que se organizan los archivos en el disco. El término también es utilizado para referirse a una partición o disco que se está utilizando para almacenamiento, o el tipo del sistema de archivos que utiliza. Así uno puede decir "tengo dos sistemas de archivo" refiriéndose a que tiene dos particiones en las que almacenar archivos, o que uno utiliza el sistema de "archivos extendido", refiriéndose al tipo del sistema de archivos"[19]

---

[18] UNIVERSIDAD POLITÉCNICA DE VALENCIA. Dispositivos de almacenamiento [en línea]. [citado en 14 de octubre de 2014]. Disponible en Internet: <http://riunet.upv.es/bitstream/handle/10251/13706/Dispositivos_de_almacenamiento.pdf?sequence=1>

[19] WIRZENIUS, Lars OJA, Joanna y STAFFORD, Stephen. Guía Para Administradores de Sistemas GNU/Linux: Capítulo 6. Utilizando Discos y Otros Medios de Almacenamiento. Enibiblio.org: [En línea]. [citado el 30 de marzo de

El concepto también articulado como File System, es el sistema por medio del cual se determinan los métodos de almacenamiento, control de espacio libre, organización jerárquica, manipulación, acceso, direccionamiento y la recuperación de datos, dentro de un dispositivo de almacenamiento.

Cada Sistema Operativo determina su propio sistema de archivos y facilita su administración gracias a un gestor o herramienta que el permite el acceso a la información.

Por ejemplo: la Familia de los sistemas operativos Windows, refieren sistemas de archivos FAT 16, FAT 32, NTFS, EXFAT. La familia de sistemas operativos Linux, manejan sistemas EXT2, EXT3, EXT4, JFS, ReinserFS y XFS, mientras que Android refiere sistemas de archivos F2FS y EXT4.

De ahí la importancia de conocer y establecer los diferentes sistemas de archivos, ya que su estructura determinara la forma como se almacena la información en un dispositivo de almacenamiento, la clasificación y ubicación de los archivos propios del sistema y los que hayan sido generados por los usuarios.

2.2.7 La criminalística y la informática forense. En la actualidad el auge de las herramientas informáticas tanto a nivel físico como lógico (hardware y software), convirtieron a este tipo de tecnología no solo en herramientas de apoyo al trabajo si no en un "modo de vida" por la necesidad de estar conectado permanentemente en un mundo cada vez más globalizado. En consecuencia la ocurrencia de los delitos informáticos tanto en las organizaciones como en las personas naturales, no debería ser motivo para que estos se beneficien de todas las bondades que brinda la tecnología, situación que brinda nuevos retos profesionales frente a controles que permitan establecer un nivel de seguridad en la información.

Como se analizó anteriormente, la naturaleza de los delitos informáticos puede volver confusa su tipificación, ya que en cada uno de los hechos pueden incurrir un sinnúmero de escenarios y circunstancias, y sumado a la NO aplicación correcta de las herramientas, podría interferir en el alcance de los resultados esperados. Es importante resaltar que la comisión de muchos de estos delitos, ocurren tras la falta de una cultura informática por parte de las víctimas, la cual en muchas ocasiones redunda en la falta de conocimiento sobre el manejo de los equipos tecnológicos y por ende de la información.

Es entonces cuando se presenta como herramienta fundamental en el Proceso de Investigación, a la criminalística como una disciplina auxiliar del Derecho Penal,

---

2015]. Disponible en Internet: <http://www.ibiblio.org/pub/linux/docs/LDP/system-admin-guide/translations/es/html/index.html>.

que se ocupan del descubrimiento y verificación científica del delito, su autor y la evidencia que la soporte.

Una definición más profunda presentada por R. Moreno sobre la criminalística:

> Nos acercaría a precisar que es una disciplina que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación, de las ciencias naturales en el examen del material sensible significativo relacionado con un presunto hecho delictuoso con el fin de determinar en auxilio de los órganos encargados de administrar justicia, su existencia o bien reconstruirlo o bien señalar y precisar la intervención de uno o varios sujetos en el mismo[20]

Y es claro que busca sobre el tratamiento de los EMP y/o EF, validar su existencia y establecer la veracidad en la ocurrencia de un delito, cuyos resultados estarán encaminados en auxiliar la administración de justicia.

Para ello, la criminalística se fundamenta en una serie de objetivos generales:

> Investigar técnicamente y demostrar científicamente, la existencia de un hecho en particular probablemente delictuoso.
>
> Determinar los fenómenos y reconstruir el mecanismo del hecho, señalando los instrumentos u objetos de ejecución, sus manifestaciones y las maniobras que se pusieron en juego para realizarlo.
>
> Aportar evidencias o coordinar técnicas o sistemas para la identificación de la víctima, si existiese
>
> Aportar evidencias para la identificación del o los presuntos imputados autores[21].

---

[20] Moreno. R. Manual de Introducción a las Ciencias Penales. págs. 344-345. Citado por: ARBUROLA VALVERDE, Allan. Criminalística: Parte general. p. 5.

[21] Ibíd., p 5.

Es así como dentro de la clasificación o subdivisión de la criminalística basada en la naturaleza de la investigación, surgió una nueva disciplina enmarcada en un conjunto de herramientas, procedimientos, estrategias y acciones desarrolladas en el campo de los medios telemáticos, y que permite descubrir en ellos, elementos de prueba y evidencia que respalde la acusación frente a los delitos informáticos, llamada Informática Forense.

Una definición presentada por Michael G. Noblett, la refiere como: "la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional"[22].

El resultado de las actividades desarrolladas por la informática forense, se resumen en el tratamiento de la evidencia digital, la cual según Eoghan Casey la define como: "cualquier dato que puede establecer que un crimen se ha ejecutado (commint) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor"[23].

A diferencia del tipo común de evidencia en lo penal, en el campo digital observamos que existen unos factores que la podrían clasificar y diferenciar, entre ellos:

- Volatilidad.
- Duplicidad.
- Alterabilidad.
- Posibilidad de modificación y eliminación.

Estas características proponen retos adicionales frente a la aplicación de las ciencias y procesos de investigación, los cuales podrían complicar la respuesta a los interrogantes de: quién, cómo, dónde, cuándo, para qué, con qué y por qué de la ocurrencia de un hecho.

---

[22] NOBLETT, Michael. Recovering and Examining Computer Forensic Evidence. Citado por: ZUCCADI, Giovanni. y GUTIÉRREZ, Juan. Informática forense. Bogotá. D.C.: Universidad Javeriana. p. 3.

[23] CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Gran Bretaña: Academic Press, 2001. Citado por: ZUCCADI, Giovanni. y GUTIÉRREZ, Op Cit., p.8.

Es fundamental en la aplicación de la criminalística, contar con elementos, recursos y medios que garanticen su razón de ser, por lo tanto una de las piezas claves es la adecuación de los laboratorios forenses donde se desarrollen cada una de las actividades frente al tratamiento de la evidencia digital de manera controlada, garantizando así la transparencia en las investigaciones. Para ello debe contar como mínimo con una estructura basada en una metodología, que soporte todos sus procesos.

Es ahí donde esta investigación toma como base de aplicación, la norma Técnica ISO/IEC 17025:2005 adaptada por el ICONTEC, la cual desarrolla los parámetros para la acreditación de los laboratorios de ensayo y de calibración, aplicable a los laboratorios de informática forense, así como también, los parámetros definidos por la ASCLD/LAB (American Society of Crime Laboratory Directors /Laboratory Accreditation Board), y la norma Técnica ISO/IEC 27037:2012, la cual sin duda alguna define un modelo totalmente estructurado y soportado para el tratamiento de la evidencia digital.

2.3 MARCO TEÓRICO CONTEXTUAL

Definir un contexto particular para desarrollar la investigación de los Delitos Informáticos se torna algo complejo, toda vez que su aplicación toma en ocasiones una estructura trasnacional, sin embargo, la aplicación de la presente investigación está dirigida a fortalecer los procedimientos existentes sobre la manipulación de la evidencia digital en Colombia, frente a la normatividad Penal existente.

Para Colombia, el actual sistema penal oral acusatorio introdujo cambios estructurales fundamentales respecto a la actividad probatoria en cada una de las partes que la componen, entre ellas: la Fiscalía, el imputado, el acusado, el defensor y el juez, cambios que son importantes mencionar:

> Tanto la Fiscalía como el imputado, están facultados para el recaudo de material probatorio, relativo a evidencia física e información que permita esclarecer los elementos del delito, material que será decisivo para el posterior desarrollo del proceso penal, especialmente para el momento de la acusación y el descubrimiento de las pruebas de cargo por parte de la Fiscalía, como para que el imputado y su defensa hagan valer durante el juicio oral el material probatorio por ellos aportado; Es fundamental distinguir los actos de investigación y los actos de

> prueba. Los primeros tienen como finalidad recaudar y obtener las evidencias o los elementos materiales probatorios que serán utilizados en el juicio oral para verificar las proposiciones de las partes y el Ministerio Público y, para justificar, con grado de probabilidad, las decisiones que corresponden al juez de control de garantía en las etapas preliminares del procedimiento. Los segundos, los actos de prueba, son aquellas actuaciones que realizan las partes ante el juez de conocimiento con el objeto de incorporar los actos de investigación al proceso y convertirlas en pruebas dirigidas a obtener la verdad de lo sucedido y verificar sus proposiciones de hecho[24]

De esta forma, dentro del sistema Penal Acusatorio la responsabilidad sobre el tratamiento de la evidencia digital actualmente se encuentra en cabeza de la Fiscalía General de la Nación como ente acusatorio, y de las instituciones judiciales que prestan el apoyo y colaboración en la investigación de los delitos amparados por la Constitución y la Ley bajo el concepto de Policía Judicial, así como también de las entidades particulares que ofrecen los servicios técnicos de soporte legal y jurídico a la defensa. Para la Corte Constitucional de Colombia: "La concepción moderna de la Policía judicial es la de un cuerpo que requiere la aplicación de principios de unidad orgánica y, sobre todo, de especialización científica y que actúa bajo la dirección funcional de los fiscales o los jueces"[25].

Dentro de los organismos con funciones de Policía judicial encontramos: Al Cuerpo Técnico de Investigación (CTI), adscrito a la Fiscalía General de la Nación:

> Cuya función principal es asesorar al Fiscal general en la determinación de políticas y estrategias relacionadas con las funciones de policía judicial, en los temas como la investigación del delito, los servicios forenses, servicios de genética y en la

---

[24] CORTE CONSTITUCIONAL DE COLOMBIA. Sentencia C-536/08 Cosa juzgada constitucional-configuración Cosa juzgada absoluta y cosa juzgada relativa-distinción [en línea]. [citado en 25 de octubre de 2014]. Disponible en Internet: <http://www.corteconstitucional.gov.co/relatoria/2008/C-536-08.htm>

[25] CORTE CONSTITUCIONAL DE COLOMBIA, Sentencia C-024/94, Policía judicial-concepto/policía judicial-funciones [en línea]. [citado en 26 de octubre de 2014]. Disponible en Internet: <http://www.corteconstitucional.gov.co/relatoria/1994/c-024-94.htm>

> gestión de la información técnica y judicial útil para la investigación penal[26].

A la Dirección de Investigación Criminal(DIJIN y SIJIN) adscrito a la Policía Nacional - Ministerio de Defensa, quienes dentro de sus funciones crearon en su estructura orgánica, los grupos encargados del tratamiento y análisis de evidencia digital, y :

> Contribuye a la prevención y control de la criminalidad, ejerciendo las funciones de Policía Judicial que le otorga la Ley en forma permanente y que junto a otros organismos del Estado apoya la investigación criminal en las áreas técnicas, científicas y operativas, por iniciativa propia o según orden impartida por la Fiscalía General, para recaudar Elementos Materiales de Prueba o Evidencias Físicas que permitan determinar una conducta punible y la responsabilidad de sus autores o participes[27]

2.4. MARCO LEGAL

Partiendo de la base de que todos los componentes que hacen parte de una sociedad están basados en unos derechos y unas obligaciones, los planteamientos aquí presentados se encuentran regulados o enmarcados por las normas establecidas en Colombia:

- La Constitución Política de Colombia de 1991 y sus diferentes artículos.

- El Decreto 1360 de 1989 frente al tema relacionado con los derechos de autor y la inscripción del soporte lógico (software), que más tarde se reglamentaría mediante los Artículos 51 y 52 del capítulo IV de la Ley 44 de

---

[26] REPUBLICA DE COLOMBIA. DIRECCION NACIONAL DEL CUERPO TECNICO DE INVESTIGACIÓN. Resolución 010. 2008. p. 2.

[27] REPUBLICA DE COLOMBIA. POLICIA NACIONAL, Resolución No. 02057 DEL 15 JUN. 2007 [en línea]. [citado en 26 de octubre de 2014]. Disponible en Internet: <http://www.policia.gov.co/portal/page/portal/INSTITUCION/normatividad/resoluciones>

1993, en el cual se determinan una serie de conductas que modificarían el Código Penal mediante la Ley 599 de 2000, en su Capítulo séptimo del libro segundo, del Título II, donde refiere la violación a la intimidad, reserva e interceptación de comunicaciones.

- Ley 600 de 2000 por la cual se expide el Código de Procedimiento Penal Colombiano.

- La Ley 679 de 2001, la cual estableció parámetros para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad y la utilización de medios tecnológicos para tal fin.

- La Resolución No. 0-1890, de noviembre 5 de 2002, de la Fiscalía General de la Nación, por medio de la cual se reglamenta el artículo 288 de la Ley 600 de 2000. Respecto a la responsabilidad de esta entidad de "dirigir, coordinar las funciones de policía Judicial y los demás organismos que señala la Ley, y garantizar en el proceso penal la autenticidad e identidad de los elementos físicos materia de prueba"[28].

- La Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación, por medio de la cual: "refiere la necesidad de establecer el manual que permita desarrollar los procedimientos de cadena de custodia, adoptado mediante resolución 0-1890 de noviembre 5 de 2012, permitiendo estandarizar y unificar el método de trabajo con el cual se debe aplicar dicho sistema"[29].

---

[28] REPUBLICA DE COLOMBIA. FISCALIA GENERAL DE LA NACION. Policía Judicial. En: Informativo Interno Huellas. Bogotá D.C. No. 46. Diciembre 2003, p. 19.

[29] REPUBLICA DE COLOMBIA. FISCALIA GENERAL DE LA NACION. Resolución No. 0-2869. 2003 [en línea]. [citado el 31 de octubre de 2014]. Disponible en Internet: <http://www.medellin.gov.co/transito/archivos/normatividad/resoluciones_nacionales/2003/2003-resolucion2869.pdf>

- La Ley 906 de 2004 Por la cual se expide el Código de Procedimiento Penal, frente a la reforma del sistema penal acusatorio en Colombia, (Corregida de conformidad con el Decreto 2770 de 2004).

- La Ley Estatutaria 1266 de 2008, de hábeas data y otras disposiciones, e involucra al tema del dato personal, refiriendo textualmente: "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que pueden asociarse con una persona natural o jurídica"[30], y que más adelante sería modificada y regulada por la Ley 1581 de 2012 denominada de "Hábeas Data" la cual protege el derecho que tenemos todas las personas a conocer, actualizar y rectificar la información que reposen en bancos de datos de entidades públicas y privadas.

- La Ley 1273, promulgada en el año 2009 por el Congreso de la Republica, por medio de la cual se modificó el código penal y se creó 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.

  Esta Ley agregó un nuevo título al Código Penal Colombiano denominado "De la Protección de la información y de los datos", enmarcado en dos capítulos: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos" y "De los atentados informáticos y otras infracciones". En contexto estos capítulos tipifican una serie de Delitos, entre los cuales tenemos:

  > El acceso abusivo a un sistema informático, la obstaculización ilegítima del sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, hurto por medios informáticos y semejantes, violación de datos personales, suplantación de sitios WEB para

[30] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266 (31 de Diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario oficial. Bogotá D.C., 2008. p. 1- 17.

capturar datos personales y transferencia no consentida de activos[31].

Una característica relevante y discutida es que aumenta considerablemente las penas 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.

- Ley 527 DE 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, como referencia y normatividad frente a la admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil[32].

- La norma Técnica ISO/IEC 17025 Internacional, la cual contiene todos los requisitos que tienen que cumplir los laboratorios de ensayo y calibración, de cara a la aplicación de un sistema de gestión en el proceso de certificación, demostrando que son técnicamente competentes con capacidad para general resultados válidos, y que es utilizada como marco normativo para la acreditación de los laboratorios de informática forense en el mundo.

- La norma Técnica Colombiana NTC-ISO/IEC 17025, la cual establece 122 cláusulas susceptibles de aplicación para la acreditación de laboratorios de

---

[31] REPUBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009 (5 de enero de 2009). Por medio de la cual se modifica el código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C. 2009. no. 47223.

[32] REPUBLICA DE COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones: Art. 10. Diario oficial. Bogotá D.C. 1999. No. 43.673

ensayo y calibración, como una aproximación sobre la base o soporte normativo de los laboratorios de informática forense en Colombia.

- La norma Técnica ISO/IEC 27037:2012, la cual ofrece los parámetros suficientes frente al tratamiento de la evidencia digital y las actividades de identificación, recolección, consolidación y/o análisis y preservación inmersas en su procedimiento.

Adicionalmente encontramos una serie de tratados y demás disposiciones, entre ellos:

- El documento COMPES 3701: Lineamientos de Política para seguridad y ciberdefensa. "orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país y adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema"[33].

- La creación del ColCert (Equipo de respuesta a emergencias informáticas de Colombia), y algunas recomendaciones formuladas en el tema de las organizaciones tales como: La UIT (Unión Europea de Telecomunicaciones), la IOCE (International Organization on Computer Evidence), la IEEE (Institute of Electrical and Electronics Engineers), la ASCLD (American Society of crime Laboratory Directors), elementos que son utilizados frente a la lucha contra los delincuencia informática y que dieron paso para establecer algunos parámetros muy generales frente al tratamiento de la evidencia digital y el análisis forense.

- La ASCLD/LAB (American Society of Crime Laboratory Directors /Laboratory Accreditation Board).La ASCLD/LAB [Sociedad Americana de directores de laboratorios contra el crimen / Junta de acreditación de laboratorios], es una organización Norte Americana sin ánimo de lucro, especializada en la acreditación de laboratorios públicos y privados en Estados Unidos y otros países frente al tema del análisis forense, y desde

[33] COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Documento Compes2011 [en línea]. [citado el 4 de noviembre de 2014]. Disponible en Internet:<http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>

1982 se encuentran comprometidos en el apoyo, educación, supervisión y acompañamiento en esta área.

Presentan un programa mejorado de ISO para la acreditación de laboratorios criminales en diferentes disciplinas para pruebas forenses y calibración, basados en la norma técnica ISO/IEC 17025, con el que garantizan a sus asociados contar con los estándares en calidad y propender por las aplicaciones justas y objetivas de la justicia.

3 DISEÑO METODOLÓGICO

3.1 Tipo de investigación

Desde el punto de vista metodológico, el trabajo desarrollado está basado en acciones descriptivas y explicativas convergentes en una investigación bibliográfica o documental, para lo cual se identifican, recolectan y analizan elementos suficientes que permitan proporcionar una visión general sobre la evidencia digital frente a la normatividad de los delitos informáticos en Colombia.

La investigación bibliográfica, según el aporte o definición presentada por Manuel Luis Rodríguez en su publicación sobre el tema, la refiere como: "un proceso sistemático y secuencial de recolección, selección, clasificación, evaluación y análisis de contenido del material empírico impreso y gráfico, físico y/o virtual que servirá de fuente teórica, conceptual y/o metodológica para una investigación científica determinada…[34]"

La aplicación de este método de investigación, ha permitido utilizar todo un conjunto de técnicas y herramientas para localizar, identificar, analizar y obtener información relevante y pertinente dentro de la presente investigación.

3.2 Diseño de la investigación

Tomado como punto de partida los postulados y propuestas existentes en la actualidad frente a los Procedimientos para el manejo de la evidencia digital, esta investigación en su pretensión busca una solución al planteamiento del problema, con un acercamiento real basado en la normatividad internacional existente y a las experiencias en el trabajo de campo y de laboratorio en la investigación penal de los delitos informáticos, que evidencian la necesidad de estandarizar criterios y documentar Procedimientos, el cual podría ser utilizado en un futuro, como un elemento imperativo de cara a un proceso de certificación de calidad de los laboratorios forenses.

Para ello, se desarrollan una serie de etapas basadas en "los criterios de selección de la pertinencia, exhaustividad y actualidad"[35], presentados por Manuel Rodríguez, los cuales permiten inicialmente:

---

[34] RODRIGUEZ, L. Acerca de la investigación bibliográfica y documental. Guía de Tesis. Agosto 2013.

[35] Ibíd.

- La definición de los tipos de fuentes bibliográficas y documentales, acordes con los objetivos de la presente investigación.

- La clasificación de las fuentes bibliográficas consultadas en función de la investigación y que en su contenido, aporten datos significativos para la construcción del documento.

- La verificación de las fuentes de consulta frente a su actualización, con el fin de garantizar que su aporte este acorde con la normatividad legal en Colombia y de las normas internacionales sobre el tratamiento de la evidencia digital y los procedimientos vigentes.

De esta forma, se presentan como elementos primarios los relacionados con las experiencias obtenidas en los apoyos a las investigaciones judiciales en el campo Penal, y la aplicación de la Criminalística desde la función operativa y técnico-científica desarrollada en los laboratorios de informática forense del Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación, y como elementos secundarios, los parámetros y normas que conducen el comportamiento de nuestra sociedad.

4 RESULTADOS

4.1 LOS DELITOS INFORMÁTICOS EN COLOMBIA

4.1.1 Contexto general. La invención de nuevas herramientas desde un contexto histórico, han sido el producto de la necesidad de suplir muchas actividades frente al tema de la supervivencia, y han contribuido en gran medida al ahorro de recursos adicionales permitiendo cumplir las tareas de manera fácil, rápida y efectiva; argumentos que han creado una dependencia absoluta sobre su uso. Sin embargo, desde nuestros antepasados hemos encontrado que muchas de esas herramientas han sido utilizadas como objetos y elementos para cumplir otro tipo de objetivos, que pueden perturbar el bienestar de los demás, o simplemente por competir frente a la base de esa supervivencia.

Esta situación no ha sido ajena a los sistemas informáticos. La evolución social marcada en las últimas décadas por la sistematización y automatización de las labores, han requerido de nuevas herramientas y formas frente al manejo de la información que nos permiten su administración y divulgación, con la premisa de estar actualizados e influenciados cada vez más por las nuevas tecnologías. Hemos caído en una dependencia, que si bien abrió nuevas posibilidades, olvidamos por un momento los riesgos inmersos que acompañarían este desarrollo hasta que no desestabilizaron nuestro bienestar y afectaron nuestros derechos.

Desde el campo de la informática, observamos que en un principio sus elementos se concentraban en entornos específicos, y los riesgos frente al tema de la seguridad y vulnerabilidad de la información tenían un contexto diferente en su manejo. Los ataques por así decirlo, se centraban mediante sistemas de infección distribuidos en medios de almacenamiento portables, los cuales utilizaban las víctimas como medios de difusión. Sin embargo la masificación de las redes de datos y su fusión, trajo consigo nuevos riesgos frente a su uso inadecuado que abrieron espacios a nuevas formas o conductas sociales.

Nace entonces el término de “ciberdelincuente”, el cual enmarca las actuaciones de quienes de manera fraudulenta evadiendo toda clase de permisos, desarrollan y generan todo tipo de herramientas para cumplir actividades que ponen en riesgo la información y los datos, situación que pese a la dificultad existente para descubrirlos y procesarlos, se sumaba un pobre y débil sistema judicial que permitiera castigar y sancionar dichas conductas, de la cual Colombia, no fue ajeno a esta situación.

Existen muchos factores para que el tema de seguridad informática no haya sido discutido y que su reacción haya sido lenta y tardía, entre los cuales podemos destacar:

- Debilidades en el tema de educación y desconocimiento en la aplicación de medidas de seguridad informáticas.
- Deficiencia en la planeación por parte de las entidades públicas y privadas sobre el tema de la seguridad informática.
- Falta de controles en el uso y abuso de los sistemas informáticos.
- Y finalmente, los altos y elevados costos en la inversión de medios que garanticen el tema de la seguridad de la información.

Estos factores pueden desencadenar ataques, los cuales en su gran mayoría pueden utilizar medios como: virus informáticos, abusos por parte de usuarios, y penetración por partes externas, tal como lo precisa ESET en su informe de Tendencias 2014: "el desafío de la privacidad en Internet", la utilización de dispositivos portátiles con conexión a Internet aumenta en cantidad y de formas curiosas, los ataques entre los que se presentan: infección por malware, phishing, falta de disponibilidad, exploración de vulnerabilidades, accesos indebidos, entre otros"[36].

Antes de la promulgación de la Ley 1273 de 2009, NO existía en Colombia un tipo penal que sancionara y enmarcara los delitos informáticos, el único artículo que establecía y sancionaba este tipo de conductas estaba enmarcado en el código penal por el Art. 195 como Acceso abusivo a un sistema informático, y textualmente refería: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa", es decir, no se había definido un tipo penal y su castigo conllevaba simplemente al pago de una multa, y por esta razón estas conductas, trataban de enmarcarse dentro de los delitos tradicionales generalmente en las que protegen los bienes patrimoniales.

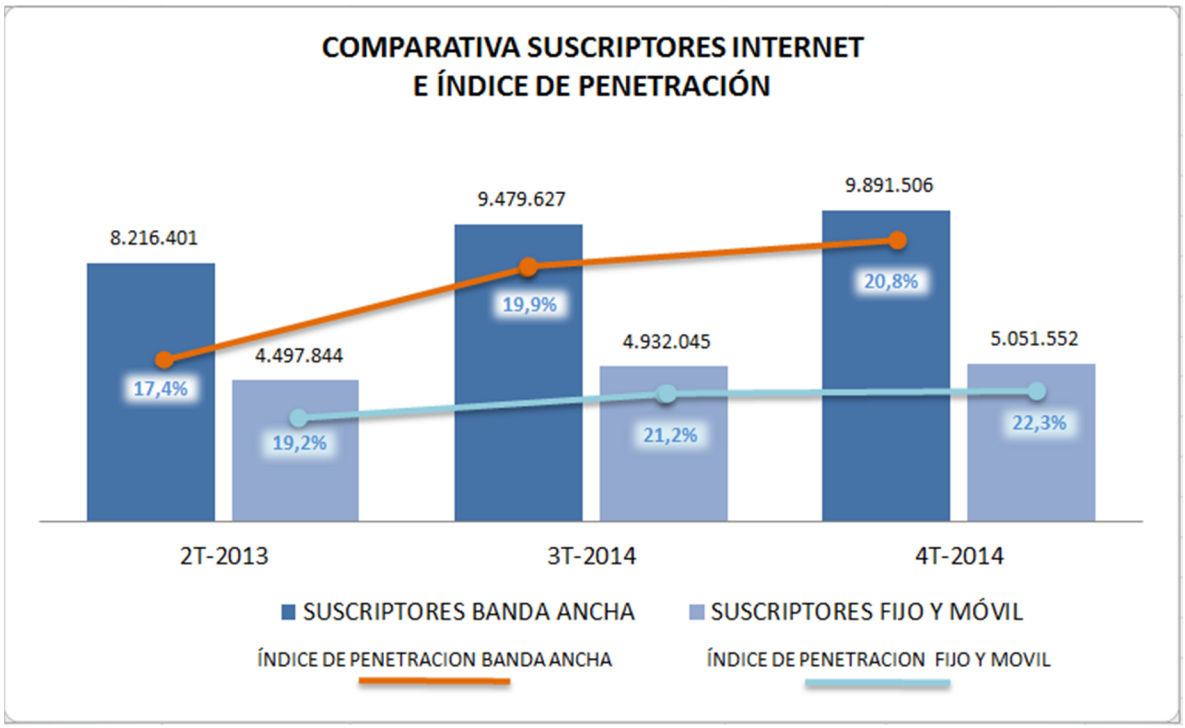
[36] ESET. Tendencias 2014: El desafío de la privacidad en Internet [en línea]. [citado en 10 de noviembre de 2014]. Disponible en Internet: <http://www.welivesecurity.com/wp-content/uploads/2014/02/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf>

En los últimos años, Colombia ha experimentado un incremento significativo en el uso de tecnologías de la información, de las telecomunicaciones y del internet. Según el ministerio de las Telecomunicaciones, en su boletín de las TIC afirma que:

> Continúa la tendencia presentada durante los últimos cuatro años. Es así como como al término del año 2014 el total de conexiones Banda Ancha alcanzó los 9.891.506 accesos en el país, mientras que las demás conexiones a Internet (conexiones con velocidad efectiva de bajada – Downstream <1.024 Kbps + Móvil 2G) suman menos de un millón de accesos, 725.709 conexiones a Internet.
>
> El índice de penetración del servicio de Internet de Banda Ancha en Colombia al finalizar el cuarto trimestre del año 2014 aumentó 0,9 puntos porcentuales con relación al trimestre inmediatamente anterior, y con referencia al cuarto trimestre del año 2013 aumentó 3,4 puntos porcentuales.
>
> Respecto a los accesos de internet fijo dedicado y móvil, al cierre del año 2014, el número total de conexiones en el país alcanzó los 10.617.215 suscriptores, cifra compuesta por accesos a Internet fijos y móviles, lo que representa un incremento absoluto de 521.250 suscriptores con relación a la cifra alcanzada en el trimestre inmediatamente anterior.
>
> El servicio de acceso a Internet fijo dedicado y móvil en Colombia, al finalizar el cuarto trimestre de 2014, presentó un índice de penetración del 22,3%, lo que representa un aumento de 1,1 puntos porcentuales con relación al índice de penetración del tercer trimestre de 2014[37]

[37] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Boletín trimestral de las TIC: Cifras cuarto trimestre de 2014 [en línea]. [citado en 10 de abril de 2015]. Disponible en Internet: <http://colombiatic.mintic.gov.co/602/articles-8598_archivo_pdf.pdf>

Figura 1. Comparativa suscriptores a Internet



Fuente: Proyección de población DANE 2013 -2014 y datos reportados por los proveedores de redes y servicios al SIUST – Colombia TIC

Este incremento se ve reflejado paralelamente con el aumento significativo en las amenazas informáticas, las cuales tienen una connotación sustancial creando la necesidad de establecer y adoptar las medidas y controles que permitan combatirlas, dado que su impacto se refleja en la seguridad de la información en el ámbito público y privado.

La firma especializada en seguridad informática “Digiware” en un análisis desarrollado sobre las tendencias y las respuestas a las amenazas para el año 2015 señaló a la revista Portafolio, que:

> Colombia es el país de Latinoamérica que más genera ataques informáticos, con más del 20 por ciento, seguida por Argentina, Perú, México y Chile. Y un buen porcentaje de estos afectan a las empresas, aclarando que no necesariamente las víctimas son colombianos sino que habría una articulación con redes internacionales que gozan de información y experiencia para sacarles provecho a la vulneración de los sistemas corporativos.

> Así mismo refiere que la tabla de vulnerabilidad ante los ataques la encabezan el sector Gobierno (49,5 %), financiero (14,3), comunicaciones (12,8), industria (10,7) y energía (6,5 %), y advierte que las modalidades más usuales en el campo corporativo son los llamados “malware de día cero”, seguidos por el “cross-site scripting” como un agujero de seguridad usual en aplicaciones web, seguido de la “suplantación de usuario”, el “defacement” o modificación es de páginas web gubernamentales[38]

Por otra parte las cifras y datos presentados en el primer foro de seguridad y defensa cibernética : Una estrategia de País, organizado por la Universidad de los Andes y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), en el mes de mayo de 2014, refiere:

> En lo que respecta al número total de ataques, según un estudio realizado por la compañía McAfee y la Organización de Estados Americanos (OEA), Colombia se posicionó como el sexto país en generar una mayor actividad maliciosa en línea para el año 2013. Por otro lado, en lo que respecta al costo, esta misma compañía estimó que el ciber-delito causó un daño económico al consumidor cercano a los 500 millones de dólares durante lo corrido de 2013, acercándose así cada vez más a los país que reciben mayores ataques cibernéticos en el mundo. Si bien estos ataques han estados dirigidos a todas las esferas de la economía, los delincuentes digitales se han concentrado principalmente contra los ciudadanos, el sector bancario, la fuerza pública y el Gobierno Nacional según el balance del Centro Cibernético Policial (CCP). Finalmente, según la información disponible por la Policía Nacional se registraron 422 arrestos por delitos cibernéticos y otros actos ilegales semejantes en el año 2013, frente a 323 en 2012 y 252 en 2011[39]

---

[38] PORTAFOLIO.COM. Colombia, principal fuente de ciberataques en Latinoamérica. [en línea]. (Octubre 17 de 2014). [citado el 5 de abril de 2015]. Disponible en Internet:<http://www.portafolio.co/negocios/ataques-ciberneticos-colombia>

[39] CAMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Reporte Ciberseguridad CCIT y Fedesarrollo: Coyuntura TIC Avances y retos de la defensa digital en Colombia. [en línea]. (noviembre 2014). [citado el 1 de abril de 2015]. Disponible en Internet:

Según el Comando Cibernético Policial (CCP) de la Policía Nacional, bajo la dirección de Investigación Criminal e INTERPOL (DIJIN), organización designada para investigar todos los casos en los que se ha visto comprometida la ciber-seguridad de las entidades del Gobierno y del sector privado del país, el número de sitios WEB bloqueados con contenido de pornografía infantil en los años 2013 fue de 2.119 y 2014 de 822, resultados obtenidos tras la puesta en marcha del sistema o aplicativo "Protectio" como primer control parental desarrollado por una institución gubernamental en Latinoamérica, para mejorar las buenas prácticas de Ciberseguridad en los hogares colombianos.[40], así mismo Los datos recopilados por la Policía Nacional revelan estadísticas interesantes en relación al crecimiento del uso de las TIC y el aumento consiguiente de incidentes y delitos cibernéticos.

> Se informaron las siguientes cifras para 2013: 448.983 seguidores en Twitter; 256,987 visitantes al sitio web www.ccp.gov.com; 2652 nuevas alertas de amenazas cibernéticas; 422 personas detenidas por delitos cibernéticos y un total de 4,290 reclamos recibidos por la Policía Nacional en relación con incidentes asociados a las TIC (lo cual representa un aumento de 1,194 quejas respecto del año anterior).
>
> En 2013, el CCP respondió a 1,647 ataques o incidentes cibernéticos, de los cuales 62% involucró a ciudadanos particulares y 21%, a entidades del sector bancario. El resto de los incidentes involucró a una combinación casi igual de entidades pertenecientes a los sectores de gobierno, fuerzas de seguridad, comunicaciones, energía, salud y educación. Lo que trajo como resultado un marcado aumento de la cantidad de personas arrestadas por haber cometido delitos cibernéticos y otros actos ilegales semejantes en 2013, que ascendió a los 422 arrestos frente a 323 en 2012, y 252 en 2011[41]

<http://www.ccit.org.co/images/Reporte%20Ciberseguridad%20CCIT%20y%20Fedesarrollo.pdf>

40 COLOMBIA. DIRECCION DE INVESTIGACION CRIMINAL E INTERPOL. Boletín informativo de cibercrimen. [en línea]. (mayo de 2014). [citado el 2 de abril de 2015]. Disponible en Internet:<http://www.ccp.gov.co/sites/default/files/boletin_cibercrimen_002.pdf>

41 SYMANTEC. Tendencias de seguridad cibernética en américa latina y el caribe. [en línea]. (junio de 2014). [citado en 5 de abril de 2014]. Disponible en Internet:

La firma Symantec con los resultados plasmados en su “Reporte Norton 2013”, afirma que:

> Más de seis millones de Colombianos fueron víctimas de algún tipo de ciberataque, reflejando que en los últimos 12 meses el costo total del crimen cibernético en el país fue de 873 mil 466 millones de pesos, que el 64% de los usuarios adultos ha experimentado algún crimen cibernético, así como también refiere que el 64% de los colombianos usa sus dispositivos móviles para trabajar, y para el último año el 42% de los usuarios de Smartphone ha experimentado algún delito cibernético, y 6 millones de personas han sido víctimas de cibercrimen”[42]

Desde una opinión personal, la incidencia de estos resultados está enmarcada por la creciente tendencia en la masificación del uso del internet, el uso de dispositivos móviles, el débil conocimiento frente al tema de seguridad por parte de los usuarios y la facilidad de obtener en el mercado software especializado en ataques informáticos totalmente documentado, el cual está diseñado para ser utilizado por cualquier persona, sin importar su nivel de conocimiento frente al tema.

Sin embargo como se precisó con anterioridad los esfuerzos en materia de prevención adelantados por el gobierno de Colombia se encuentran regidos y articulados principalmente por el documento COMPES 3701, el cual sirvió como base para la creación del Centro Cibernético Policial (CPP), como unidad principal para la investigación de delitos cibernéticos en todo el país, la cooperación del Departamento de Estado de los Estados Unidos (DS/ATA) y el FBI en materia de capacitación y análisis forense, bajo el eje principal del marco legislativo nacional de la Ley 1213 de 2009 “de la protección de la información y de los datos”

<http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf>

[42] SYMANTEC. Reporte Norton 2013. [en línea]. [citado en 20 de noviembre de 2014]. Disponible en Internet: <http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf>

4.1.2 El Proceso Penal Colombiano. A modo general y muy básico se presenta en contexto el modelo adoptado por Colombia, frente al tratamiento de las conductas referidas como delitos.

La Constitución Política de Colombia de 1991, estableció el sistema de enjuiciamiento penal Colombiano y en su Artículo 1:

> Define a Colombia como un Estado Social de Derecho, basado en la aplicación de la justicia y el respeto por la dignidad humana, mediante la aplicación de un sistema debidamente estructurado en las autoridades públicas, los principios, derechos y deberes sociales de orden constitucional y el reconocimiento y garantía de los derechos humanos[43]

Para el caso del Derecho Penal, su objetivo es el de garantizar los bienes e intereses de las personas en un conglomerado social, promoviendo sus derechos fundamentales, y restringiendo otros a título de sanción degradándolos como delitos, siempre y cuando generen un reproche social y vayan en contra de las normas, estableciendo el interés general sobre el particular. Sobre este tema Pedro Avella Franco refiere:

> Los sistemas jurídico políticos, entre otras actividades y objetivos, controlan las conductas de los ciudadanos evitando o solucionándolos conflictos de intereses que ordinariamente ocurren, a través de diferentes instrumentos de reacción que limitan las libertades y otros derechos fundamentales. Es el caso del derecho penal. Todo derecho penal permeado por una Constitución Política como la de Colombia, se dirige a garantizarlos bienes e intereses de las personas restringiendo los derechos de unas a título de sanción, pero, en ese horizonte, es también promotor de los derechos fundamentales de los asociados. Separa los actos que generan reproche social y los

[43] REPUBLICA DE COLOMBIA. CORTE CONTITUCIONAL. CONSTITUCION POLITICA DE COLOMBIA 1991. Bogotá, Imprenta Nacional de Colombia, 2010.

> degrada como delitos, de los que las personas realizan para vivir y desarrollarse en términos normales[44]

Frente a este panorama Colombia adoptó mediante la Ley 906 de 2004, un sistema penal basado en los modelos acusatorios americano y continental europeo, sin ser asociado a uno en particular, pero presenta importantes particularidades en su estructura en su interpretación, así mismo, establece una serie de instituciones jurídicas responsables de su aplicación y administración, diferenciando entre las que investigan, acusan y juzgan mediante el principio acusatorio y define como columna vertebral la audiencia de juicio oral como un escenario donde se realizará la práctica, presentación y admisión de la prueba física, testimonial, documental y pericial. Sobre el particular Avella señala:

> El máximo Tribunal Constitucional, luego de la comparación delos esquemas continental europeo y anglosajón respecto del sistema acusatorio adoptado por el Acto Legislativo 03 de 2002, mediante la Ley 906 de 2004, concluyó: "la realización de un parangón entre los modelos acusatorios americano y continental europeo evidencia, una vez más, que el nuevo modelo procesal penal colombiano no se adscribe a ninguno de los anteriores sino que por el contrario presenta numerosas e importantes particularidades, que es preciso tener en cuenta al momento de interpretar la Ley 906 de 2004"[45]

El proceso penal acusatorio en su estructura, según Avella:

> Está compuesta por dos etapas claramente definidas: una es la investigación, de la que además forma parte la fase de indagación; la otra es la de juicio. Corresponde anticipar que la fase de indagación comienza con la noticia criminal y termina con la formulación de la imputación, con la que se da lugar a la

---

44 AVELLA FRANCO, Pedro. Naturaleza constitucional del procedimiento penal colombiano. Estructura del proceso penal acusatorio. Bogotá D.C.: Fiscalía General de la Nación, Diciembre de 2007. p. 19.

45 Ibíd., p 37.

> investigación propiamente tal, la que concluye a su vez con la presentación del escrito de acusación, que da inicio a la etapa de juicio, misma que termina con la ejecutoria de la sentencia qué pone fin al proceso[46]

Su aplicación se desarrolla mediante dos etapas: una fase de indagación inmersa en una etapa de investigación, a cargo de la Fiscalía General de la Nación como institución responsable de adelantar las investigaciones cuando las acciones revistan características de delito, apoyándose para ello en las autoridades de policía judicial y enmarcando sus actuaciones mediante la aplicación de herramientas como el Código de Procedimiento Penal, siempre y cuando existan motivos, circunstancias y elementos legales que indiquen su posible comisión.

La fase de investigación y sus características, partiendo del señalamiento presentado por la Corte Constitucional en la Sentencia C-1194 de 2005, refiere:

> La Fiscalía, en una primera fase de indagaciones, determina la ocurrencia de los hechos y delimita los aspectos generales del presunto ilícito. Dado que los acontecimientos fácticos no siempre son fácilmente verificables y que las circunstancias que los determinan pueden hacer confusa la identificación de su ilicitud, el fin de la indagación a cargo de la Fiscalía, y de las autoridades de policía judicial, es definir los contornos jurídicos del suceso que va a ser objeto de investigación y juicio. La fase de indagación es reservada y se caracteriza por una alta incertidumbre probatoria, despejada apenas por los datos que arroja la noticia criminis[47]

Dentro de los procesos o fases de indagación e investigación, tomando como referencia a Avella, quien presenta las siguientes figuras como intervinientes:

> La Fiscalía General de la Nación como responsable de coordinar todas las actuaciones que se desarrollaran, para la consecución de EMP yo EF o información legalmente obtenida, con el fin de presentar una formulación de imputación y formalizar así una

---

46 Ibíd., p 61.

47 REPUBLICA DE COLOMBIA. Corte Constitucional. Contextualización de la institución del Descubrimiento de la Prueba en el esquema del proceso penal acusatorio En: Sentencia C-1194 de 2005. Bogotá D.C., 2005; p. 14.

etapa subsiguiente de investigación, o la prescripción de la conducta que conllevará a su archivo.

Los funcionarios de Policía Judicial actúan como receptores de noticia criminal y tienen a su cargo la búsqueda, fijación, recolección y embalaje de los elementos materiales probatorios y evidencia física que por cualquier medio encuentren o reciban.

El Juez de Control de Garantías tiene como función esencial controlar que los actos de investigación desarrollados por la policía judicial, en cumplimiento de las órdenes emitidas por el fiscal director de la misma, que impliquen limitaciones a los derechos fundamentales se ajusten a la Constitución y a la ley.

La defensa estará a cargo del abogado principal que libremente designe el imputado, o en su defecto, el que le ha sido asignado por el Sistema Nacional de Defensoría Pública.

Las víctimas. Al tenor del artículo 132 de la Ley 906 de 2004 son víctimas las personas naturales o jurídicas y demás sujetos de derechos que individual o colectivamente hayan sufrido algún daño (directo) como consecuencia del injusto.

El Ministerio Público, [encargados de] señalar que los Fiscales y la policía deben enterarlo de las diligencias y actuaciones de su competencia, para que ejerza la defensa del orden jurídico y, especialmente, para que actúe como garante de los derechos humanos y de los derechos fundamentales.

Juez de Conocimiento. Le corresponde resolver sobre la procedibilidad de la preclusión de la investigación, cuando se verifique alguna de las causales previstas en el artículo 332 de la Ley906 de 2004.

El imputado, quien tiene derecho al ejercicio de todas las garantías establecidas en la Constitución y en los tratados internacionales que hacen parte del bloque de constitucionalidad. Por lo mismo, no serán disponibles sus derechos superiores como el de la dignidad humana, igualdad, intimidad y a que su libertad

> no se restrinja sino en presencia de motivos fundados, y atendiendo a los criterios de excepcionalidad, razonabilidad, ponderación y proporcionalidad[48]

Y finalmente una etapa de Juicio como fase final del proceso penal. En ella básicamente se practican las pruebas bajo los principios de oralidad, ejercicio de la defensa, contradicción, concentración, inmediación y controversia. Adicionalmente AVELLA refiere:

> La etapa de Juicio es la fase final del proceso penal previsto en la ley 906 de 2004. Está integrado por las audiencias de formulación de acusación, preparatoria, juicio oral, y fijación de sentencia. Eventualmente se tramita incidente de reparación integral, que tiene lugar luego de emitido fallo de culpabilidad, y cuya decisión debe incorporarse a la sentencia[49]

El sistema penal acusatorio ofrece como uno de sus principios fundamentales el de igualdad de armas, lo que permite que en el marco del proceso, tanto la parte que acusa (Fiscalía) como la defensa, cuenten en igualdad de condiciones con los mismos derechos y garantías en el uso de los elementos, que convenzan y soporten legalmente la acusación, mediante la presentación de evidencias que prueben las teorías presentadas.

Y como mencionamos anteriormente, el soporte del proceso se encuentra determinado por el correcto tratamiento de los EMP y/o EF, los cuales se convertirán en prueba, siempre y cuando se sigan los lineamientos técnicos y científicos desde cada una de las ciencias que apoyan las investigaciones.

---

48 AVELLA, Op. Cit. p. 66 – 75.

49 AVELLA, Op. Cit. p. 87.

4.1.3 La evidencia digital como prueba en Colombia. Sin caer en redundancias, hemos presentado la necesidad de la prueba como pieza fundamental en el proceso penal colombiano ya que determina la imputación de una conducta. Desde el campo informático, hemos encontrado la inexistencia de manera taxativa, de una norma que indique los lineamientos específicos y los requisitos que debe cumplir la prueba frente al proceso penal.

Sin embargo, se ha dado la necesidad de incorporar a la información contenida en medios electrónicos y otros medios tecnológicos, los requisitos estipulados por la Ley frente al manejo del respaldo probatorio de los documentos consignados en papel; requisitos basados en la fiabilidad, inalterabilidad y rastreabilidad, gracias al principio de equivalencia funcional, el cual según el profesor Jeimy Cano: "El principio en mención establece que un mensaje de datos que cumpla con la función de declaración o representación tendrá los mismos efectos jurídicos propios de los medios de prueba tradicionales"[50] .

Ahora bien, la Ley 527 de 1999 (ley de mensaje de datos), es utilizada en la actualidad como norma interpretativa, por cuanto su contenido permite un acercamiento acorde a la realidad tecnológica, y el régimen probatorio en el Derecho Colombiano, se encuentra consagrado en el Código de Procedimiento Civil, sección tercera, título XIII, el cual en su artículo 165 permite como medio de prueba "cualesquiera otros medios que sean útiles para la formación del convencimiento del juez". El profesor Cano considera que: "los archivos digitales o mensajes de datos podrían verse involucrados dado que harían parte de "otros medios" presentados para aportar al caso en estudio, pero la forma como sean identificados, generados y recogidos puede influir en la manera como sean valorados por la Corte"[51].

De esta forma, un Juez no podrá desestimar la fuerza de la prueba proveniente de datos y deberá "estudiar y valorar la confiabilidad en la forma que se haya

---

50 CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá: Ediciones Uniandes, 2010. 348p.

51 Ibíd.

generado, archivado o comunicado el mensaje y en la forma en que se identifique a su iniciador y cualquier otro factor pertinente"[52].

Esto nos permite concluir que en Colombia existe una alternativa jurídica basada en la valoración de la prueba electrónica, que surge tras el proceso de portazgo decretado por un Juez, que desde un punto de vista penal debe ser tratada por personal especializado, quien sustenta a través de sus dictámenes los hallazgos encontrados.

Concluimos entonces, la existencia de una normatividad vigente frente a la admisibilidad de las pruebas tecnológicas en los procesos judiciales, sin embargo, la presentación de la evidencia digital y la exposición de los procesos utilizados en su tratamiento implican algunas dificultades, ya que conjuga términos propios de la informática que deben ser abordados por personal calificado que soporte desde su conocimiento, el soporte en un juicio de la intangibilidad y virtualidad de los elementos aportados. Sobre el particular según el profesor Cano[53]: Es menester que el sistema de justicia penal este orientado hacia una aplicación de la Ley, que se encuentre basada en estudios previos, principalmente en áreas de conocimiento, como lo son: informática básica, evidencia digital y delitos informáticos.

4.2 Normas Técnicas aplicables al tratamiento de la evidencia digital en Colombia

Como parte activa en la estructuración de un procedimiento documentado, está el indagar la existencia de normas técnicas aplicables en el medio, y que desde la comunidad internacional soporten cada una de las actividades desarrolladas, las metodologías generales y específicas sobre los procesos, equipos, elementos de medida y control, entre otros, y que enmarquen los pasos consecutivos para iniciar, desarrollar y concluir una actividad, los elementos técnicos, condiciones de trabajo, alcances y limitaciones, así como también, las características del personal que los ponen en práctica. Procedimientos que garantizarán la calidad en los

[52] Ley 527 de 2009, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Art 11.

[53] CANO MARTINEZ, Op. Cit.

resultados generados por los laboratorios, y permiten su reproductibilidad, uniformidad y consistencia en los proceso, detallando claramente cada una de las actividad, funciones y responsabilidades.

En la actualidad, desde el campo de la informática forense encontramos las siguientes normas que regulan las actividades, frente al tratamiento de la evidencia digital:

4.2.1 La ASCLD/LAB (American Society of Crime Laboratory Directors /Laboratory Accreditation Board). La American Society of Crime Laboratory Directors /Laboratory Accreditation Board (ASCLD/LAB)[54] [Sociedad Americana de directores de laboratorios contra el crimen / Junta de acreditación de laboratorios], es una organización Norte Americana sin ánimo de lucro, [especializada en la acreditación de laboratorios públicos y privados en Estados Unidos y otros países frente al tema del análisis forense, y desde 1982 se encuentran comprometidos en el apoyo, educación, supervisión y acompañamiento en esta área…].

Presentan un programa mejorado de ISO para la acreditación de laboratorios criminales en diferentes disciplinas para pruebas forenses y calibración, basados en la norma técnica ISO/IEC 17025, con el que garantizan a sus asociados contar con los estándares en calidad y propender por las aplicaciones justas y objetivas de la justicia.

Dentro de sus programas, se encuentra referido el programa de pruebas ASCLD/LAB-International para la acreditación exclusiva de laboratorios de ciencias forenses en las disciplinas de química, toxicología, evidencia del rastro, biología, armas de fuego y herramientas, documento logia, huellas latentes, escena del crimen, evidencia digital y multimedia, para ello, los laboratorios forenses que desean obtener su acreditación deben cumplir con algunos requisitos, entre ellos: la certificación otorgada en norma técnica de calidad ISO/IEC 17025 y los requisitos suplementarios de ASCLD/LAB para los laboratorios de análisis (Supplemental Requirements for Testing Laboratories), obtenidos tras obtener un contrato con dicha organización.

Se resalta que la adquisición de toda la documentación actualizada, requieren de una licencia especial otorgada por la ASCLD/LAB para lo cual se deben cumplir unos requisitos especiales, y un costo adicional.

[54] American Society of Crime Laboratory Directors /Laboratory Accreditation Board (ASCLD/LAB). 2015. Disponible en Internet: < http://www.ascld-lab.org/>

Para ello, cualquier laboratorio de criminalística forense puede solicitar la acreditación en cualquiera de las disciplinas, una vez dentro de su gestión, operaciones, personal, procedimientos, equipos, planta física, seguridad cumplan con los requerimientos establecidos por la ASCLD/LAB, sin embargo, esta acreditación no incluye la certificación del personal a cargo de adelantar los peritajes forenses, ya que ellos necesitan adicionalmente unas pruebas individuales y requisitos en el área de educación, capacitación, pruebas de aptitud, entre otros.

Los requerimientos y Directrices frente al cumplimiento se encuentran en el manual de acreditación de ASCLD/LAB, el cual contiene los principios, las normas básicas y alrededor de 145 criterios para su evaluación, si el laboratorio quisiera acreditar tan solo una de las cuatro disciplinas del tratamiento de evidencia digital (análisis de audio, computer forensic, análisis de imágenes digitales, análisis de video) tendrá que documentar y demostrar el cumplimiento de 102 criterios, entre ellos: 38 esenciales, 44 aplicables y 20 importantes (según su clasificación).

Varios de esos criterios son inspeccionados por la ASCLD/LAB periódicamente, para lo cual el laboratorio debe cumplir con:

- Marca o rotulado, sellado o embalaje y protección de la evidencia física, respecto al tratamiento de la evidencia digital, aplica los criterios 1.4.1.2 el cual requiere que cada elemento debe marcarse con un identificador único, para no confundir las evidencias, el criterio 1.4.1.3 refiere que se deben sellar adecuadamente los contenedores que refieren los elementos, el criterio 1.4.1.4 exige que se utilicen empaques especiales de acuerdo a la naturaleza de los elementos a analizar, con el fin de prevenir daños especiales.

- Validación y verificación de los Procedimientos, el cual refiere un proceso por medio del cual se realizan una serie de experimentos que demuestran confiabilidad y eficacia en los procedimientos o técnicas utilizadas, antes de ser aplicadas, los cuales se encuentran referidos en el criterio 1.4.2.6.

  En la disciplina de la evidencia digital, requiere que cada herramienta forense debe ser validada y verificada antes de su aplicación, para ello se debe adelantar diferentes pruebas sobre la misma, y demostrar que cumple adecuadamente su función sin alterar el contenido de la evidencia.

- Uso de normas y controles, referido por el criterio 1.4.2.8, requiere que para asegurar la validez de los resultados y las conclusiones, los procedimientos deben incluir un estándar y control, debidamente documentado, esto se puede lograr tras asegurar que las herramientas e instrumentos funcionan adecuadamente.

- Estado y actualización de equipos forenses, para lo cual es necesario llevar un control adecuado de las herramientas, frente a sus mantenimientos preventivos y correctivos, así como sus actualizaciones, el cual debe estar debidamente documentado y soportado.

- Calibración de instrumentos, enmarcado por el criterio 1.4.2.12 el cual requiere que todas las herramientas deben mantenerse en perfecto estado de funcionamiento, y el criterio 1.4.2.13 que afirma que los instrumentos deben ser calibrados correctamente. Esto se logra tras la aplicación de un control en la bitácora de cada instrumento, la cual refiere la fecha en la cual fue puesto en operación, sus parámetros, registros de daños, correcciones y actualizaciones de software y hardware, documentación frente al software utilizado, entre otros.

4.2.2 La Norma Técnica Colombiana NTC-ISO/IEC 17025. La ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) son dos organismos que integran el sistema mundial que regulan la normatividad internacional sobre campos particulares de la actividad técnica, y su resultado involucra también la participación de otras organizaciones públicas y privadas frente a un proceso de evaluación de la conformidad denominado CASCO, quien es el responsable de la documentación de Normas y Guías Internacionales.

Esta norma internacional establece los requisitos generales para la competencia en la realización de ensayos y/o calibraciones, incluido el muestreo. Cubre los ensayos y las calibraciones que se realizan utilizando métodos normalizados, métodos no normalizados y métodos desarrollados por el propio laboratorio[55].

- **Requisitos Generales**

[55] ICONTEC. Norma técnica Colombiana NTC-ISO/IEC 17025. Requisitos generales para la competencia de los laboratorios de ensayo y calibración. I.C.S:03.120.20. Primera actualización. 2005. p 1.

Esta norma dentro de su estructura, establece los requisitos generales que un laboratorio debe cumplir con el fin de adelantar calibraciones y/o ensayos, así como también el muestreo.

- **Alcance**

Como mencionamos es aplicable a todas las organizaciones que cuenten con áreas de laboratorio que desarrollen calibraciones o ensayos. Se utiliza como herramienta que normaliza los sistemas de calidad, administrativos y técnicos que rigen sus operaciones y actividades, así como también para los clientes y las autoridades reguladoras y encargadas de la acreditación y reconocimiento de los laboratorios.

- **Control de documentación**

✓ Generalidades

Los laboratorios deberán establecer, aplicar, mantener y validar procedimientos que articulen el control de documentos que forman parte de su sistema de calidad, entre ellos, normas, métodos de calibración y ensayo, software, equipos, guías, instructivos o manuales.

✓ Aprobación y edición de documentos

Los documentos deben ser revisados por personal autorizado antes de su edición, estableciendo un control de documentos que normalice la forma como se generan, se mantienen y se clasifiquen.

De igual forma, deberán contar con una identificación única, la cual refiera la fecha de edición o de revisión, numeración de páginas, número total de páginas, marca que indique el final del documento y quien lo elaboró.

✓ Cambios en los documentos

Deben ser revisados y aprobados por el personal quien generó o publicó el documento original, o por alguna otra persona designada para desarrollar dicha labor, para lo cual deberá soportar mediante los respectivos anexos los fundamentos de dichos cambios. Todas estas directrices, deberán estar referidas en procedimientos especiales frente al control de documentos.

- **Acciones correctivas**

  El laboratorio tendrá que establecer una política y un procedimiento, designando la autoridad encargada de implementar las acciones correctivas, cuando se identifica un trabajo no conforme, como resultado a las actividades aplicadas entre ellas: el control de trabajo no conforme, auditorías internas o externas, revisiones por la alta dirección, comunicación con el cliente, acciones de mejora.

- **Requisitos técnicos**

  El laboratorio deberá contar con todos los elementos que permitan establecer un seguimiento de auditoria, entre ellos, las observaciones, resultados de los procesos aplicados, informes de ensayo y calibración, que para el caso específico referirían las hojas de vida de cada uno de los equipos forenses. Para ello debe definirse un procedimiento, con su persona responsable en la ejecución, y chequeo de los resultados.

- **Auditorías Internas.**

  Con el fin de verificar el cumplimiento de los requisitos establecidos en la norma técnica, se deben adelantar periódicamente auditorías internas de cada una de las tareas desarrolladas. En su orden deberá incluir para su revisión todos los elementos que componen el sistema de calidad, y sus resultados deberán estar consignados en el informe respectivo para su revisión por la alta dirección.

- **Revisiones de la Dirección**

  Es un proceso por medio del cual, los responsables de la implementación del sistema de calidad, revisan periódicamente cada una de las políticas y procedimientos, los resultados de auditorías internas, el cumplimiento de las normas y de los procedimientos operativos estandarizados, las acciones correctivas y preventivas, evaluaciones de entidades externas, satisfacción de los clientes, control de calidad del producto y el adecuado estado de los equipos y herramientas.

La implementación de un sistema de gestión de calidad y las normas técnicas de calidad, facilitan la labor frente a la aceptación internacional de los resultados

obtenidos, y la cooperación entre los laboratorios forenses de otros países, así como también la estandarización de los protocolos y procedimientos.

4.2.3 La Norma Técnica ISO/IEC 27037:2012. Denominada "Information tecnology –security techniques- guidelines for identification, collection, acquisition, and preservation of digital evidence", refuerza y renueva las antiguas directrices enmarcadas en el RFC 3227, actualizando las técnicas frente a los dispositivos actuales.

Su escenario de aplicación está orientado al procedimiento pericial y la actuación del personal involucrado con la identificación, recolección, embalaje, custodia de la evidencia digital y transporte de la evidencia digital en trabajo de campo, sin embargo, no incluye la etapa de análisis o de laboratorio.

- **Principios básicos**

  De acuerdo a los parámetros contenidos por la ISO/IEC 27037:2012, en su ítem 5.4.1, la evidencia digital deberá estar articulada por los siguientes principios: Reducir al máximo su manipulación, documentar los cambios o acciones adelantadas, cumplir con todas las normas, no tomar acciones más allá de su competencia, y frente a la evidencia digital:

  - ✓ La relevancia, la cual establece y soporta de una manera jurídica, los elementos vinculados a la investigación como soporte de una hipótesis planteada alrededor de los hechos.

  - ✓ La confiabilidad, que garantice que los resultados obtenidos frente a la aplicación de procedimientos no presenten algún tipo de variación a ser repetidos y garanticen su validez y respaldo.

  - ✓ La suficiencia, que garanticen que las evidencias y sus procesos aplicados son suficientes para demostrar y verificar las hipótesis planteadas.

  Adicionalmente podemos mencionar o complementar mencionando que la aplicación de la norma busca:

  - ✓ Proceso Auditable[56], en razón a que los procedimientos y documentación aplicable, hayan sido debidamente validados y

[56] ISO 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence. Item 5.3.2.

aprobados atendiendo las directrices enmarcadas en el sistema de gestión de calidad frente a las buenas prácticas de laboratorio y que permitan hacer un seguimiento efectivo a los resultados obtenidos.

- ✓ Proceso Repetible y reproducible[57], se refiere a que la repetitividad en los resultados de la prueba se haga en las mismas condiciones, usando los mismos procedimientos de medición o método, se pueda desarrollar en cualquier momento y bajo las mismas condiciones.

- ✓ Proceso Justificable[58]**,** por medio del cual se garantiza que la recolección de la evidencia digital adelantada por el primer respondiente, sea lo menos intrusiva, y preserve su originalidad sobre la fuente de información y que justifique las acciones adelantadas.

La norma establece los roles para las personas que desarrollarán las actividades requeridas en la informática forense, entre ellos:

- ✓ DEFRF (Digital Evidence Firts Responder), [primer respondiente de la evidencia digital], quien es una persona idónea, avalada por el marco jurídico de cada país y autorizada para atender una escena del crimen y quien tiene el primer contacto con la evidencia inmersa en dicho escenario, encargada de asegurar el área, custodiar los elementos, evitando que otras personas tengan contacto con los mismos, documentando las condiciones del área de trabajo.

- ✓ DES (Digital Evidence Specialist), [especialista en evidencia digital], que es la persona idónea capaz de desarrollar las tareas del primer respondiente, quien cuenta con la preparación, entrenamiento y destrezas en el tratamiento especializado de la evidencia digital, o un perito en informática.

Su idoneidad debe ser avalada, ya sea por su experiencia en el campo de trabajo o por su título profesional como experto en la disciplina.

---

[57] Ibídem. Item 5.3.3, 5.3.4.

[58] Ibídem. Item 5.3.5.

- **Fases o etapas de la norma según su estructura**

  Se fundamenta en el tratamiento de la evidencia digital frente a los siguientes procesos:

  - ✓ La identificación[59], por medio del cual se identifican los elementos materiales susceptibles de análisis y que pudieran contener información relevante a la evidencia digital, estableciendo la categoría de lógica o física, para ello deben tenerse en cuenta los siguientes principios: Prioridad a la recopilación de pruebas volátiles, reducción al mínimo en el daño de los elementos o información original, identificar evidencia oculta.

  - ✓ La recolección y/o adquisición[60], que define el proceso por medio del cual se recolectan los dispositivos y el proceso de documentación de los mismos, tanto de manera lógica tras la extracción de una imagen forense, así como también la recolección física de los elementos contenedores de la información.

  - ✓ La conservación y/o preservación[61], la cual garantiza su preservación frente a la utilidad, de tal forma que se respete su originalidad e integridad, garantizando a futuro que al evidencia sea admisible en un proceso, respaldada por un proceso de cadena de custodia. La ISO/IEC 27037 define la preservación como “the process to maintain and safeguard the integrity and/or original condition of the potential” ,[El proceso de mantener y salvaguardar la integridad y/o el estado original]

  Respecto a la aplicación de la cadena de custodia, los roles, las responsabilidades, competencias y demás directrices, la norma ofrece en su Capítulo 6 (Key Components of Identification, Collection, Acquisitionand Preservation of Digital Evidence – ISO 27037), toda la información no técnica sobre su manejo, mediante la siguiente estructura documental:

  - ✓ 6.1 Cadena de custodia

  - ✓ 6.2 Precauciones en el sitio del incidente

  - ✓ 6.3 Roles y responsabilidades

---

59 Ibídem. Item 5.4.2.

60 Ibídem. Item 5.4.3 y 5.4.4

61 Ibídem. Ítem 5.4.5.

- ✓ 6.4 Competencias
- ✓ 6.5 Cuidado razonable
- ✓ 6.6 Documentación
- ✓ 6.7 Sesiones de retroalimentación
- ✓ 6.8 Priorización en la recolección y adquisición de la evidencia
- ✓ 6.9 Preservación de la evidencia digital

Desarrolla un capítulo 7 Instances of Identification, Collection, Acquisition and Preservation [Instancias de identificación, recolección, adquisición, y preservación] - ISO 27037, para lo cual subdivide una serie de recomendaciones a tener en cuenta:

- ✓ 7.1 Ordenadores, periféricos y medios de almacenamiento digital
    - o 7.1.1 Identificación, desarrolla los procesos o actividades de: Búsqueda física en la escena del incidente, recopilación de evidencia NO digital, toma de decisiones para determinar la recolección o adquisición de evidencia
    - o 7.1.2 Recolección y 7.1.3 Adquisición: define los parámetros sobre la adquisición de la evidencia, frente a: dispositivos que se encuentren encendidos, donde el primer respondiente debe garantizar la adquisición de la información, la cual debe ser exacta en su fuente, la importancia de la evidencia volátil, recomienda la utilización de programas o herramientas verificadas y avaladas para su uso, así como también de los dispositivos de almacenamiento los cuales deben ser desinfectados.

      Adicionalmente refiere otras actividades adicionales frente al tratamiento de la detección de datos encriptados, y el manejo de equipos apagados, su adquisición o recolección la cual debe fijarse en parámetros como capacidad y tamaño de los dispositivos de almacenamiento originales, complejidad en los sistemas de información, precauciones con el tema de las garantías sobre los equipos.

- 7.1.4 Preservación, la cual refiere que debe adelantarse un proceso de verificación sobre los contenedores donde se almacena la evidencia digital, los cuales garanticen su integridad.

✓ Dispositivos de Red

Parte desde un proceso de observación, el cual busca identificar las dificultades frente a su manejo ligado al sistema que se esté inspeccionando, recomienda adelantar un proceso de Identificación mediante la observación física, refiriendo características tales como el diseño del dispositivo, elementos, conector de alimentación o dispositivo, etiquetas, entro otros.

Un proceso de documentación del incidente de manera visual, fotografiando, filmando o dibujando la escena, tareas que deben desarrollarse valorando las circunstancias, costos, tiempo disponible, recursos y prioridades.

Antes de desconectar un equipo, debe evaluarse si se trata de dispositivos críticos, centralizan información o prestan dependencia a otros, lo cual permitirá tomar decisiones frente a su desconexión o apagado, de ahí que requiere algunos conocimientos por parte del primer respondiente en la aplicación de herramientas que permitan adelantar tareas específicas de recolección lógica sobre la red.

4.3 PROCEDIMIENTO PROPUESTO PARA EL MANEJO DE LA EVIDENCIA DIGITAL

Se plantean dos etapas o campos de acción: La que se desarrolla por los primeros respondientes en su trabajo de campo, y la desarrollada por los peritos especialistas en el trabajo de laboratorio frente al tratamiento de la evidencia digital.

4.3.1 Trabajo de Campo. Esta etapa está dirigida a las personas que cumplen su rol y/o desarrolla actividades como primer respondiente. Presenta las pautas generales de investigación y de trabajo en los escenarios donde se desarrollaron los hechos, y tiene por objeto el hallazgo, la recolección y preservación de EMP y/o EF que sustenten y soporten las hipótesis establecidas dentro de la investigación.

Para ello se desarrollaran las actividades, basadas en los siguientes parámetros:

4.3.1.1 Aseguramiento de la escena, cuyo objetivo es garantizar la seguridad física del entorno frente al escenario donde se desarrollaron los hechos, evitando cualquier tipo de riesgo que ponga en peligro la integridad del investigador y de los EMP y/o EF que ahí se encuentren, evacuando el personal que se pueda encontrar en las zonas afectadas y definiendo un sistema de acordonamiento o delimitación de las área de trabajo.

4.3.1.2 Observación y planificación con el fin de determinar una hipótesis frente a los hechos, y las diferentes labores que se van a desarrollar, como: áreas de aislamiento y acordonamiento, zonas de trabajo, rutas de acceso y evacuación, personal y cada una de sus funciones, métodos de búsqueda y recolección de elementos, herramientas y recursos a utilizar.

4.3.1.3 Utilización de los elementos de bioseguridad, los cuales garantizan la integridad física de los investigadores y de los elementos encontrados por transferencia, los cuales incluyen: protectores oculares, protectores naso bucales, guantes de látex, “tyvek” o trajes que previenen el intercambio o contaminación de la escena.

4.3.1.4 Documentación y registros: video gráfico, fotográfico y documental por medio de la narrativa y bosquejos topográficos, la cual acompañe el ingreso al escenario con el fin de identificar y fijar los EMP, tarea que enmarque los métodos búsqueda (Espiral o concéntrico, punto a punto, franjas, áreas o zonas) establecidos de acuerdo el espacio físico o geográfico del escenario.

4.3.1.5 Recolección de EMP y/o EF, actividad que debería desarrollarse por personal calificado, o con conocimientos en el campo de la telemática, esto como soporte objetivo, frente a la conservación y recuperación de datos e información, teniendo en cuenta las siguientes recomendaciones:

- Utilizar elementos de protección para elementos electrónicos, como manillas o trajes de aislamiento antiestático.

- Clasificación de la Evidencia (triage forense) según su prioridad, atendiendo a los parámetros comprendidos entre los “Datos volátiles” y “Datos NO volátiles”.

- Determinar si los equipos involucrados corresponden o desarrollan funciones de centralización de información, tal es el caso de datacenter o servidores, los cuales por su naturaleza su mala manipulación podrían afectar considerablemente las funciones y procesos misionales de una entidad.

- Documentar de las condiciones en las cuales se encontraron los elementos, determinando características físicas, fecha y hora del sistema, procesos en pantalla, su individualización por medio de seriales, códigos, entre otros, adicionalmente, valorar con criterios objetivos para NO desconectar o retirar ningún dispositivo como USB, discos de almacenamiento, entre otros, hasta que no se tenga claro el procedimiento de recolección (físico – lógico).

- Si los equipos de cómputo o sistemas telemáticos se encuentran operando, deberán establecerse métodos de recuperación de información sobre el sistema “vivo” o “en caliente”, que permitan recolectar datos e información “volátil” almacenada generalmente en memorias o en dispositivos de almacenamiento bajo criterios de archivos temporales.

  Su manipulación debe contar con herramientas especiales incluidas en su ToolKit, las cuales garanticen en su tratamiento:

  ✓ Como se mencionó, recuperar información o datos que se encuentren activos o en ejecución, los cuales generalmente almacenan en la estructura de datos de la memoria RAM, o memoria Cache y/o archivos pagefile.sys en el caso de la familia de sistemas operativos Windows.

  ✓ Extraer una imagen o espejo forense de las unidades principales de almacenamiento donde se está ejecutando el sistema.

  ✓ La manipulación del equipo deberá ser lo menor posible, documentando cronológicamente cada uno de los procesos que se desarrollaron.

- Si la máquina se encuentra apagada, se desarrollan las siguientes tareas:

- ✓ Documentar de las condiciones en las cuales se encontraron los elementos, determinando características físicas, y su individualización por medio de seriales, códigos, entre otros.

- ✓ Desconectar los diferentes periféricos asociados a la torre de cómputo.

- ✓ Recolección de cada uno de los EMP y/o EF, susceptibles de análisis (Dispositivos de almacenamiento de información), o que sean valiosos para la investigación (periféricos de entrada o de salida como impresoras, escáner, cámaras de video, entro otros).

- Definir los tipos de contenedores que se utilizaran en el procedimiento de embalaje de cada uno de los EMP encontrados, los cuales por lo general están provistos de protectores o aislantes Faraday.

- Aplicación del respectivo Procedimiento de Cadena de custodia, establecido por la Fiscalía General de la Nación, que garantice la integridad, continuidad, autenticidad, identidad y registro, de acuerdo a su clase y naturaleza[62], mediante su rotulado o etiquetado, acompañado de un registro de continuidad, el cual cronológicamente especifique las personas que tuvieron contacto directo con los EMP y/o EF, y su traslado al sitio de custodia y almacenamiento, o en su defecto, a los laboratorios forenses para su respectivo análisis.

Los parámetros presentados anteriormente se desarrollarían en escenarios totalmente controlados, donde el investigador tenga a favor el factor tiempo vs seguridad. En caso contrario:

- Todo el procedimiento debe estar enmarcado por la fijación de los EMP y/o EF, mediante la documentación Video gráfica y/o fotográfica que permita registrar las condiciones en las cuales se encontraron los equipos.

---

62 COLOMBIA. Fiscalía General de la Nación. Manual del sistema de cadena de custodia. Op. Cit.

- Determinar que EMP y/o EF son valiosos para la investigación (Triage forense).

- Aunque es indudable e indiscutible la perdida de algún tipo de dato que se encuentre almacenado en la memoria temporal de las máquinas o equipos, deben ser desconectados de sus fuentes de alimentación, sin manipular o adelantar sobre ellos procesos de apagado o salida desde su sistema operativo, en el caso de las laptops o equipos portátiles que cuenten con sus propios sistemas de alimentación se deben recolectar sin algún tipo de manipulación, dejando el respectivo registro de su fecha y hora del sistema.

- Finalmente la recolección y custodia de los EMP y/o EF, para su posterior embalaje, rotulado y traslado para su almacenamiento o análisis.

4.3.2 Trabajo en laboratorio. Tiene como finalidad: la adquisición, preservación, hallazgo, documentación y presentación de resultados frente al contenido de los EMP y/o EF aportados en la investigación, los cuales según la terminología empleada en esta campo toma el nombre de Evidencia Digital, y reúne todo el conjunto de datos binarios, fragmentos y/o archivos o ficheros, cuyo contendido soporte la comisión de un delito.

Los Protocolos y/o Procedimientos de la Informática Forense, generalizan etapas que en su pretensión organizan y presentan un modelo que regulan la investigación, y su tratamiento debería manejarse como un incidente de seguridad informática, sin embargo, es claro que factores como: el contexto en que se desarrollaron los hechos, el funcionamiento y estructura de cada uno de los sistemas de cómputo involucrados, marcarán sin duda alguna la diferencia en cada una de las investigaciones.

Para el desarrollo de esta etapa podemos establecer las siguientes Fases:

4.3.2.1 Identificación y Análisis de los hechos. Esta Fase toma gran importancia debido a que determinará la bitácora y objetivos del procedimiento, partiendo de un análisis exhaustivo sobre los hechos ocurridos y los EMP y/o EF aportados dentro de la investigación.

Partiendo del Procedimiento de cadena de custodia, revisaremos detalladamente el embalaje físico de cada uno de los EMP y/o EF, dejando constancia de los hallazgos encontrados, es recomendado dejar registro fotográfico y documental del mismo.

4.3.2.2 Recopilación o adquisición. Hablando de un proceso de recolección lógico, implica la extracción de una copia exacta de las unidades de almacenamiento para su posterior análisis. Si la recolección es producto de un procedimiento metódico habrá mayores posibilidades de establecer respuesta a cada uno de los interrogantes planteados frente a la investigación, y contar así con suficientes EMP y/o EF que la soporten. Se recomienda:

- ✓ Contar con un equipo de cómputo de alto rendimiento (high performance computer), el cual cuente con los suficientes recursos a nivel de procesador, memoria, puertos de conexión y almacenamiento, debido a que los aplicativos forenses consumen muchos de esos recursos. Aunque en el mercado existen máquinas diseñadas como estaciones forenses, su costo puede ser algo elevado.

- ✓ Es indispensable el uso de Bloqueadores, herramientas que permitan proteger contra la modificación de datos y la escritura, las unidades de almacenamiento y/o los dispositivos para análisis. Actualmente en el mercado se ofrecen a nivel de software, aplicativos que bloquean contra escritura los puertos (generalmente USB) de las máquinas donde se conectan los puentes y las unidades de almacenamiento, entre ellos: USB Write Blocker de DSicovery[63], sin embargo este tipo de aplicaciones está diseñado para un tipo de plataforma de Sistema Operativo específica, limitando su uso.

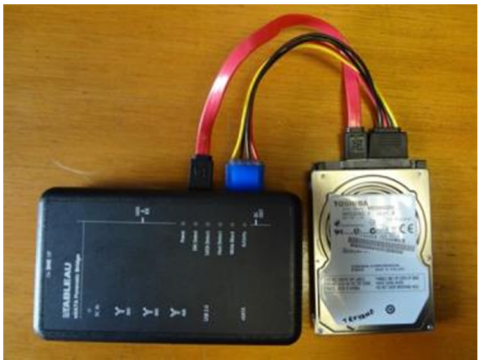
  Otro tipo de soluciones a nivel de hardware, que por cierto son las más recomendadas, pueden ser utilizados con varias plataformas de sistema operativos, y además ofrecen todo tipo de conectores y adaptadores que garantizan compatibilidad con un sinnúmero de dispositivos de almacenamientos de información digital. Su costo puede ser un factor a tener en cuenta. Algunos ejemplos, son los dispositivos marca Tableau:

63 DSicovery. USB Write Blocker [en línea]. [citado en 12 de noviembre de 2014]. Disponible en: <http://dsicovery.com/dsicovery-software/usb-write-blocker/>

Figura 2. Tableau T8-R2 Forensic USB Bridge

Fuente: El autor.

Figura 3. Tableau Forensic Bridge Model T35u



Fuente: El autor.

Figura 4. Tableau Forensic ultrabay 3

Fuente: El autor.

- ✓ Para el almacenamiento de las imágenes forenses, se debe contar con medios estériles con una capacidad considerable, partiendo del hecho que como resultado del proceso, se obtendrá una copia bit a bit de los dispositivos

originales, lo cual incluirá toda la información que este contenga, entre: sistemas de archivos, archivos o ficheros eliminados y el espacio libre.

Actualmente, existen en el mercado diferentes soluciones forenses o toolkits a nivel de hardware o software según las necesidades, las cuales permiten extraer y generar imágenes de los dispositivos originales, con la opción de comprimirlas y encriptarlas, entre ellas: Herramientas específicas en ambiente comercial como: Logicube y sus equipos de clonado y extracción de imágenes forenses, EnCase Forensic de Guidance Software, FTK de AccesData, y las herramientas de código abierto (Open Source) como: e-fense y sus paquetes de aplicaciones, Autopsy, Clonezilla, entre otros.

4.3.2.3 Preservación. El aseguramiento de los EMP y/o EF tanto físicos, como lógicos, son uno de los elementos claves dentro del proceso del análisis forense, ya que como mencionamos anteriormente, son los pilares que soportan una investigación, y en cualquier momento puede necesitarse análisis posteriores (principio repetible y reproducible), por lo tanto es recomendado generar estrategias que garanticen la integridad de dichos elementos, entre ellas: contar por lo menos una copia de las imágenes forenses originales para trabajar sobre ella, la cual deberá estar respaldada, tras la aplicación estricta del procedimiento de cadena de custodia

Esta fase tal vez es una de las más delicadas frente al procedimiento general, debido a que requiere la articulación de muchos recursos para garantizar así la integridad de los EMP y/o EF, entre los que podemos mencionar:

- ✓ Un adecuado sistema de almacenamiento que garantice la capacidad y soporte necesario donde permanecerán las imágenes forenses.

- ✓ Diseñar controles específicos frente al tiempo en el cual se mantendrán las imágenes forenses.

- ✓ Los dispositivos telemáticos y de almacenamiento, están compuestos de piezas electrónicas y materiales que con el paso del tiempo pueden deteriorarse. Para el Ministerio de minas y energía de Colombia, para prevenir factores ambientales que pudieran afectar la integridad de la evidencia digital, debe garantizarse:

  Un espacio físico con ambiente controlado donde permanecerán los contenedores de evidencia digital, y demás EMP y/o EF, que

garantice un nivel de temperatura y humedad adecuados, libre de campos y radiaciones electromagnéticas, y que se encuentre protegido bajo un reglamento técnico de instalaciones eléctricas "RETIE"[64]

- ✓ Los espacios físicos, deben garantizar las medidas de seguridad necesarias, para evitar intrusiones y restricciones de personal que pudiera poner en riesgo la confidencialidad de los elementos almacenados.

4.3.2.4 Análisis de Información. Una vez se han definido cuáles serán los objetivos del análisis, se disponga de EMP y/o EF recopilados y almacenados de forma segura y debidamente documentados, entramos a la fase más laboriosa y básica de todo el análisis forense, en la cual convergen factores como: la pericia, suspicacia, conocimiento y destreza del perito o examinador forense, frente al manejo de cada una de las herramientas con que cuenta y sobre todo, de la naturaleza de la evidencia digital.

Esta fase tendrá por objeto determinar toda una cadena de acontecimientos desde que se produjeron los hechos hasta su descubrimiento, los cuales deberán estar debidamente soportados, la cual finalizará, una vez se hayan dado respuesta a los interrogantes planteados en la primera Fase.

Para ello, se plantea como requisitos mínimos que garanticen y soporten con transparencia los resultados:

- ✓ Entorno de trabajo, a nivel físico un espacio que garantice la seguridad de los EMP y/o EF recolectados y su tratamiento, y las condiciones ambientales para desarrollar las actividades.

  Generalmente estos espacios son totalmente aislados y restringidos al público, cuentan con sub divisiones donde se almacenan temporalmente los EMP y/o EF, y donde se efectúan los procesos de análisis físico y lógico.

[64] REPUBLICA DE COLOMBIA. MINISTERIO DE MINAS Y ENERGÍA. Resolución 9 0708 (25 OCTUBRE DE 2013).Mediante la cual se expide el nuevo Reglamento Técnico de Instalaciones Eléctricas RETIE. Bogotá D.C.: El ministerio, 2013. 5 p.

- ✓ Recursos o herramientas suficientes para desarrollar el estudio de la evidencia digital, que estén debidamente actualizadas y soportados por la comunidad internacional.

  Es muy frecuente encontrar, que una herramienta forense de elección no es capaz de analizar un tipo de evidencia en especial, y es deber del examinador o perito, utilizar una segunda herramienta.

- ✓ Aplicación metódica que permita reproducir los procesos cuantas veces sea necesario obteniendo siempre los mismos resultados, a través de Procedimientos avalados.

Entrando en materia, el desarrollo del análisis deberá centrase en:

- ✓ Identificar el tipo de contenedor, o Dispositivo de almacenamiento digital de información.

- ✓ Identificar los sistemas de archivos, que conlleva a determinar el sistema operativo instalado en la máquina.

- ✓ Considere recuperar y explorar el sistema de archivos en búsqueda de particiones o ficheros y carpetas modificados y/o eliminados, reconstruyendo una estructura, la cual deberá ser descubierta y analizada en su totalidad.

- ✓ Examine los log´s del sistema, fechas y horas del sistema, su respectiva zona horaria, los recursos y hardware instalado.

- ✓ La aplicación de funciones contenidas en las herramientas forenses, permiten que de manera metódica, en el menor tiempo posible y de forma sencilla, se obtengan elementos que infieran algún tipo de rastro frente al objeto de la investigación. Desarrollar tareas de exploración manual, pueden consumir grandes esfuerzos, que conllevarían a “buscar una aguja en un pajar”.

  Recordemos que la información se almacena en: fragmentos de archivos y espacios no asignados en disco, archivos producto de una compresión, de un proceso de encriptación, o como resultado de un proceso de estenografía, entre otros.

- ✓ Identificar los eventos que lo pudieran ubicar de manera tempo espacial en los hechos sucedidos, pueden orientar la búsqueda en los log's del sistema y su correlación con toda clase de archivos.
- ✓ Documentar todos los procesos desarrollados y los resultados obtenidos, determinado que tareas o actividades conllevaron a la consecución de los resultados, es un buen momento para repasar todo el proceso de análisis y reforzar las hipótesis, recuerde que los procedimientos pueden ser reproducibles y sus resultados verificables.

- ✓ Finalmente, analice todos los resultados y su correlación entre los diferentes EMP y/o EF recolectados en la escena evaluando su impacto.

4.3.2.5 Documentación y presentación de resultados. Podemos observar que el desarrollo de cada una de las Fases aquí presentadas, atienden a un proceso metódico con base en la documentación, y sus resultados, deberán ser debidamente integrados, consolidados y expuestos en dos tipos de formatos:

4.3.2.5.1 Informe técnico de laboratorio. El cual refiera: Los EMP y/o EF analizados, los equipos y herramientas forenses empleados, las técnicas y/o Procedimientos, resultados y descripción de hallazgos, y las conclusiones del análisis.

En su estructura, de manera general deberá contener:

- Un encabezado, el cual refiera como título el tipo de documento que se está elaborando: INFORME DE LABORATORIO**,** el número de noticia o expediente, la ubicación tempo espacial donde se desarrollan las actuaciones, así como también el número de Orden de trabajo asignada y el número de validación o de producción para el informe.

- El destino del informe, donde se relacione el cliente o autoridad solicitante.

- Objetivo de la diligencia, la cual refiera textualmente la solicitud presentada por el cliente.

- Descripción precisa de los EMP y/o EF que serán examinados, para ello, se debe transcribir la información contenida en sus rótulos (descripción, número de hallazgo, cantidad), así como también, el estado del embalaje y los contenedores.

- Descripción de los Procedimientos Técnicos empleados, entre ellos, la documentación fotográfica o videográfica, el proceso de extracción de la imagen forense y las actividades adelantadas, el destino de esa imagen, y cada uno de los procesos subsiguientes.

- Soporte o validación Técnico científica de los Procedimientos adelantados. Para ello, deberán referirse la normatividad jurídica que ampara las actuaciones, y las bases o lineamientos que soportan nuestros Procedimientos, entre ellos: La Normas Técnicas de Calidad, las certificaciones del sistema de Gestión de calidad en el caso de tenerlas.

- Instrumentos empleados y su estado al momento de realizar el examen, los cuales expongan los recursos físicos y lógicos con que cuenta el laboratorio.

- Descripción detallada de cada uno de los procesos adelantados, en el análisis forense.

- Presentación de resultados y su interpretación, las cuales señalan la información o datos obtenidos frente a la solicitud, las recomendaciones, conclusiones y el destino de los EMP y/o EF.

- Glosario de Términos, organizados de manera alfabética, relacionar las palabras técnicas, tecnicismos, abreviaturas o términos incluidos en el informe.

- Anexos, refieren algún tipo de documentos anexos en cuanto a Procedimientos auxiliares aplicados.

- Servidor o perito quien desarrolló el examen, relacionando la entidad, código interno, grupo o laboratorio, nombres completos, número de identificación y su firma.

4.3.2.5.2 Informe ejecutivo. El cual reúna desde el empleo de lenguaje común, la traducción técnica por así decirlo, de los procedimientos y resultados obtenidos, el cual sea de fácil comprensión exponiendo los hechos más destacables.

En su estructura, de manera general deberá contener:

- Un encabezado, el cual refiera como título el tipo de documento que se está elaborando: INFORME EJECUTIVO, el número de noticia o expediente, la ubicación tempo espacial donde se desarrollan las actuaciones, así como también el número de Orden de trabajo asignada y el número de validación o de producción para el informe.

- El destino del informe, donde se relacione el cliente o autoridad solicitante.

- La Información respecto al delito, lugar de los hechos.

- Objetivo de la diligencia, la cual refiera textualmente la solicitud presentada por el cliente.

- Actuaciones realizadas, en donde se refieran cada una de las actividades y los Procedimientos que las avalan.

- Resultados de la actividad Técnico – científica desarrollada, la cual de manera cronológica referirá cada una de las actividades desarrolladas en todo el proceso y sus resultados, en donde debe primar la utilización de un vocabulario NO técnico y de fácil comprensión.

- Anexos, en donde se refiera la orden de solicitud, el informe de laboratorio, y cualquier otro documento que haya sido generado dentro del proceso, entre ellos, la comunicación con el cliente.

- Servidor o perito quien desarrolló el examen, relacionando la entidad, código interno, grupo o laboratorio, nombres completos, número de identificación y su firma.

4.4 GUIA PRACTICA DE ANALISIS FORENSE DE EVIDENCIA DIGITAL CON FTK IMAGER DE ACCESSDATA Y ENCASE VERSIÓN 7.9. DE GUIDANCE SOFTWARE

4.4.1 Extracción de la Imagen Forense

4.4.1.1 Descripción del Proceso

- ✓ Creación de una bitácora o documento que puede ser físico o electrónico en el cual se consignen de manera cronológica todas las actividades que se llevaran a cabo durante el procedimiento y de sus hallazgos, de modo que servirá como historial y soporte para la construcción del informe de laboratorio.

- ✓ Empleo o utilización de herramientas que garanticen el bloqueo contra escritura y/o modificación del contenido de los elementos o dispositivos de almacenamiento digital que vayan ser analizados.

- ✓ Creación del archivo de imagen forense.

- ✓ Aseguramiento y/o verificación de la integridad del archivo de imagen forense.

- ✓ Almacenamiento de la imagen forense.

4.4.1.2 Herramientas y Recursos. En la aplicación y desarrollo de esta metodología es indispensable la utilización de herramientas, las cuales tanto a nivel de hardware como de software, garantizarán el cumplimiento del objetivo propuesto en cada una de los pasos descritos en el numeral anterior.

A nivel de hardware se empleó:

- ✓ Computador de escritorio compuesto por un procesador AMD Phentom (tm) II x4 Procesor 3.20 GHZ, con una memoria RAM de 8 GB, Disco Duro de 1 Tb, unidad DVD con compatibilidad DL, 2 puertos USB, y con un Sistema Operativo Windows 7 a 64 bits.

- ✓ Bloqueadores contra escritura marca Tableu puente TS35es, el cual es un dispositivo diseñado por la firma TABLEU* con el fin de restringir y/o deshabilitar la opción de escritura por medio de hardware, en los dispositivos de almacenamiento digital tipo discos duros, y el TABLEU puente forense T8 USB, dispositivo capaz de restringir y/o deshabilitar la opción de escritura en dispositivos de almacenamiento digital USB.

- ✓ Un disco duro externo con interfaz USB, con una capacidad de almacenamiento de 1TB, debidamente esterilizado bajo un procedimiento de "weep" o borrado seguro.

- ✓ Unidades de almacenamiento óptico de información tipo DVD+L DL con capacidad de 8.4 GB.

A nivel de Software se utilizó:

- ✓ Como el desarrollo práctico se adelantó sobre la plataforma WINDOWS, se propuso la utilización del software FTK IMAGER, solución proporcionada por la firma AccessData, en su versión 3.2.0, la cual puede ser descargada desde su página WEB oficial http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.2.0, y en su pretensión permite extraer (copia bita a bit), montar y analizar de manera básica mediante una pre visualización de información, una imagen forense de cualquier dispositivo de almacenamiento digital de información.

---

* TABLEU: Productos Tableau están diseñados y construidos para satisfacer las necesidades críticas de la comunidad forense digital de todo el mundo. Ofrecen soluciones frente a duplicadores y bloqueadores con sus respectivos accesorios para el análisis forense.

- ✓ Aplicativo para el borrado seguro en dispositivos de almacenamiento digital de información como el caso de Eraser, disponible en http://eraser.heidi.ie/, con el cual esterilizaremos el dispositivo de almacenamiento externo, donde se guardó la imagen forense obtenida.
- ✓ Aplicativo md5summer, solución gratuita creada por Luke Pascoe, la cual se empleó para comprobar la integridad de los archivos a través de la suma de verificación de los HASH MD5 o SAH1. Disponible en: http://www.md5summer.org/download.html.

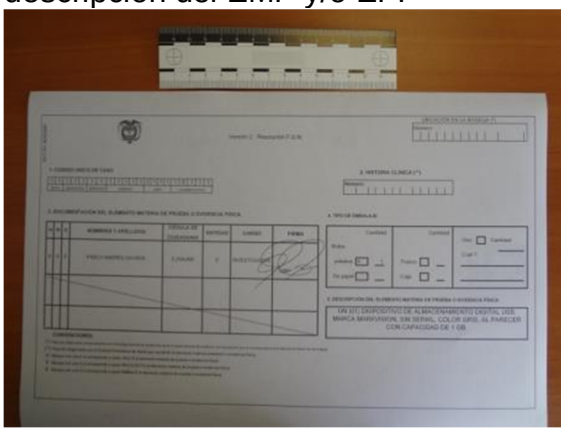
4.4.2 Desarrollo Práctico con FTK Imager. La práctica se desarrolló sobre un dispositivo de almacenamiento tipo UBS con una capacidad de 1 GB como elemento susceptible de análisis.

- ✓ Fijación fotográfica del EMP y/o EF allegado para estudio.

Figura 5. Rótulo y estado del embalaje del EMP y/o EF allegado para estudio

Fuente: El Autor.

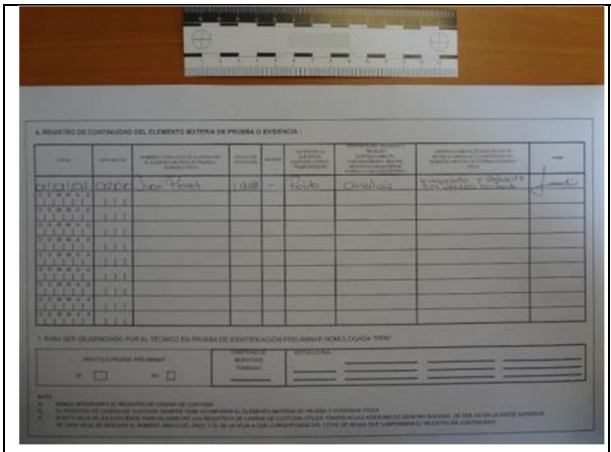
Figura 6. Documentación como soporte de la cadena de custodia, en el cual coincidan: el número de proceso,y la descripción del EMP y/o EF.



Fuente: El Autor.

Figura 7. Documentación referente al registro de continuidad, 2da parte de la cadena de custodia.

Figura 8. Documentación contenido el embalaje del EMP y/o EF allegada para estudio, La cual refiera: marcas, seriales, o características que individualicen el elemento.



Fuente: El Autor.

Fuente: El Autor.

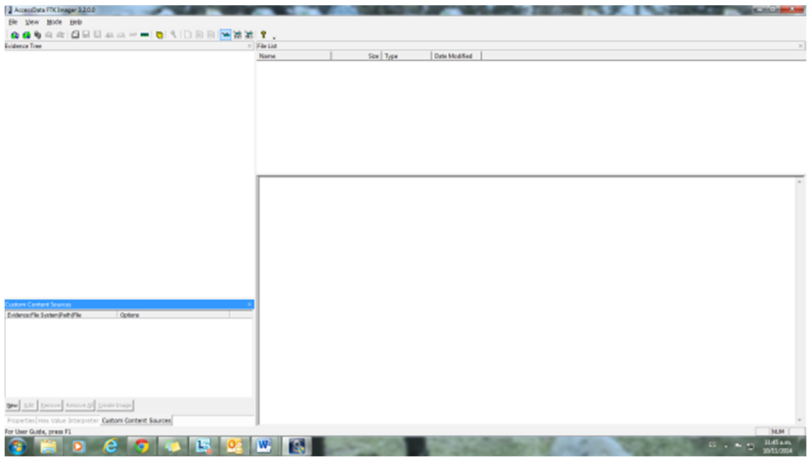
- ✓ Bloqueo y conexión del Dispositivo para análisis por medio de las interfaces provistas por la herramienta TABLEU T8.

Figura 9. Tableau T8-R2 Forensic USB Bridge

Fuente: El Autor.

- ✓ Una vez se descargó e instaló la aplicación AccessData FTK Imager3-2-0, su ejecución se adelantó sobre la plataforma Windows 7.

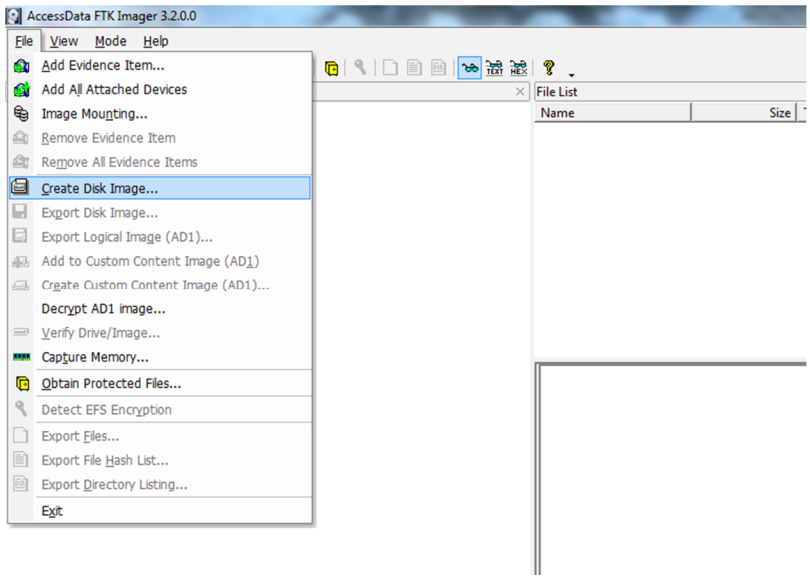
Figura 10. Pantalla principal AccessData FTK Imager3-2-0



Fuente: El Autor.

Opción “File -> Create Disk Image” o Archivo -> [Crear Imagen de Disco].

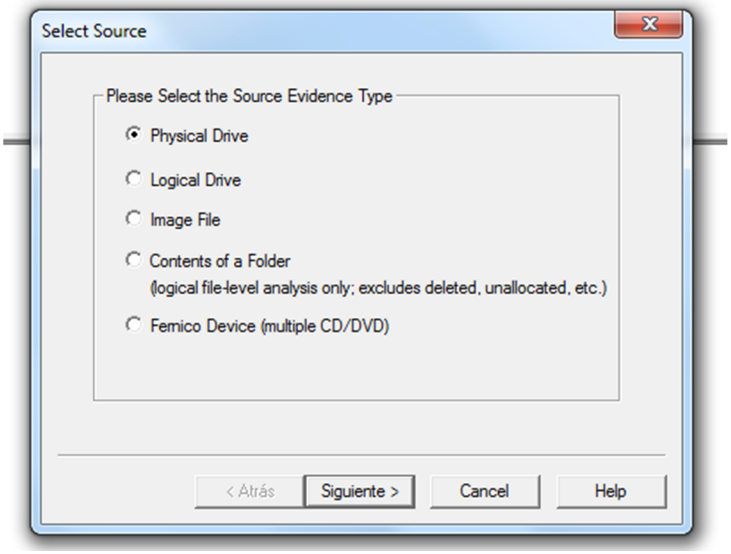
Figura 11. Menú principal AccessData FTK Imager3-2-0



Fuente: El Autor.

Ofrece una ventana donde se definió la Fuente de donde se extrajo la imagen forense. Para este propósito opción “Physical Drive” [Unidad Física].

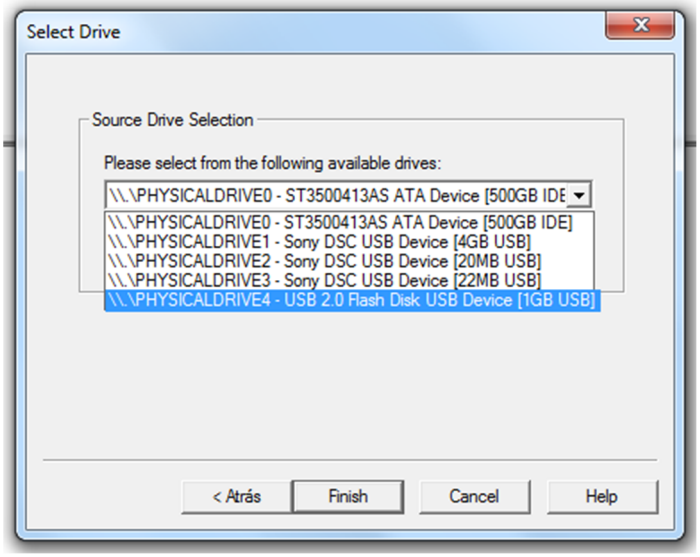
Figura 12. Selección fuente AccessData FTK Imager3-2-0 (Parte 1)



Fuente: El Autor.

En una nueva ventana un menú desplegable, en el cual se seleccionó la Unidad Fuente correspondiente, seguido de un clic en el botón “Finish” [Finalizar].

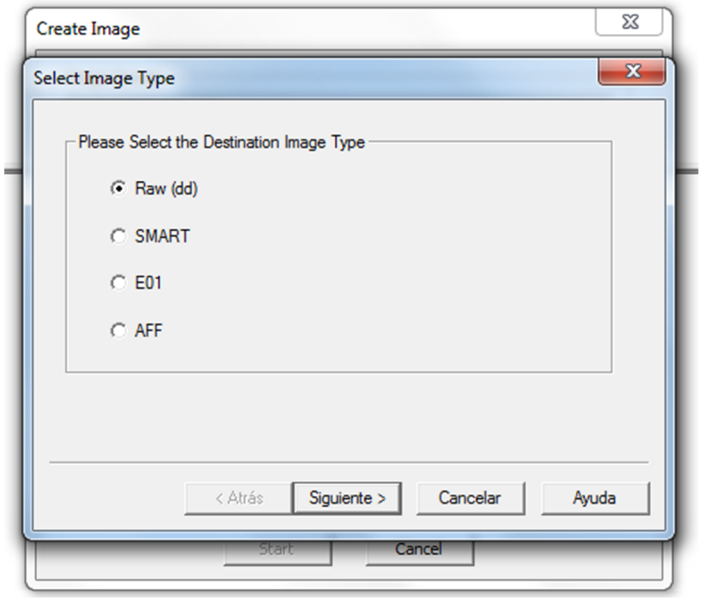
Figura 13. Selección fuente AccessData FTK Imager3-2-0 (Parte 2)



Fuente: El Autor.

Se estableció el dispositivo de almacenamiento (unidad Destino) donde se almacenará la imagen. Para lo cual fue necesario hacer clic en el botón “Add...”

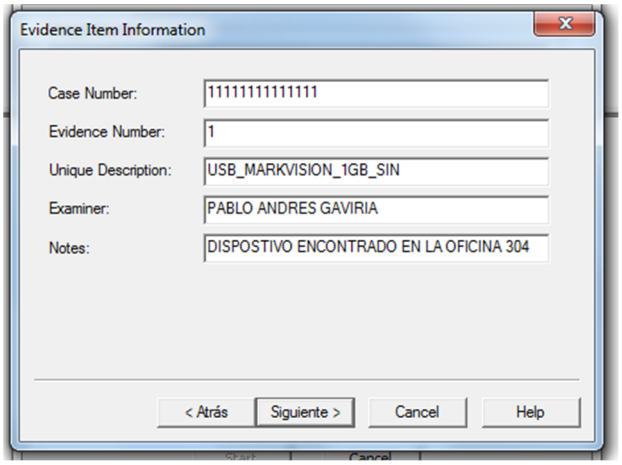
Figura 14. Selección fuente AccessData FTK Imager3-2-0 (Parte 3)



Fuente: El Autor.

Para este momento fue necesario definir el tipo de archivo de imagen que se iba a crear, dependiendo del tamaño, software de análisis y su compatibilidad; para nuestro particular la opción seleccionada fue en formato E01.

Figura 15. Selección fuente AccessData FTK Imager3-2-0 (Parte 4)

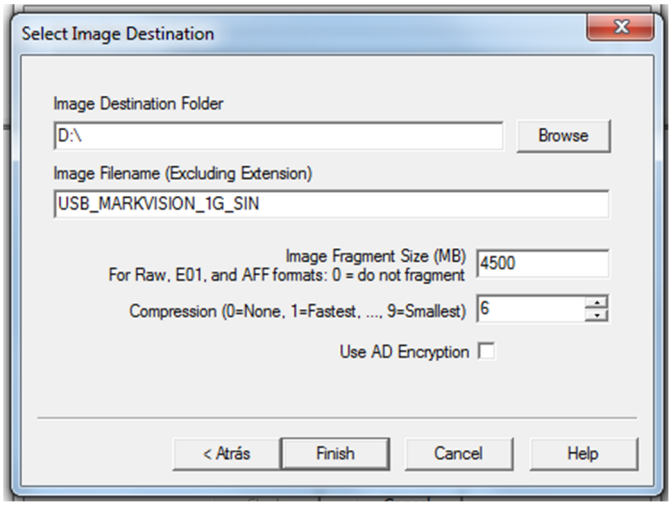


Fuente: El Autor.

Se ingresó, a manera de ejemplo: la información correspondiente al número de caso, el número de evidencia (la cual depende de la secuencia numérica definida en el proceso de hallazgo y recolección), la descripción del dispositivo, el nombre del examinador, y notas adicionales.

Frente al ítem “Unique description” [descripción única], se recomienda definir a manera de abreviatura una estructura conformada por: El tipo de dispositivo (USB, DD para disco duro, MSD para micro SD, seguido del nombre o marca, capacidad de almacenamiento y finalmente su número de serial o identificación, el cual puede ser reemplazado por la silaba SIN, en el caso de no contar con esta información.

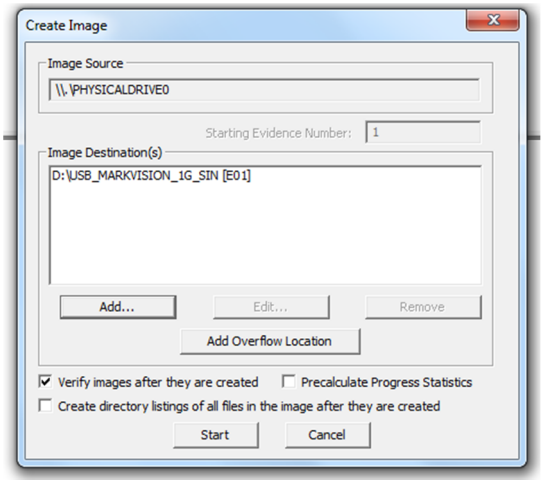
Figura 16. Selección fuente AccessData FTK Imager3-2-0 (Parte 5)



Fuente: El Autor.

Se estableció la unidad destino de almacenamiento para la imagen y su nombre o identificador, siguiendo la recomendación presentada frente a la descripción única (paso anterior), estableciendo el tamaño para la fragmentación del archivo de imagen, el cual atiende a los parámetros definidos por la capacidad del o los dispositivo (s) de almacenamiento contenedores utilizados para guardar la imagen.

Figura 17. Selección fuente AccessData FTK Imager3-2-0 (Parte 6)



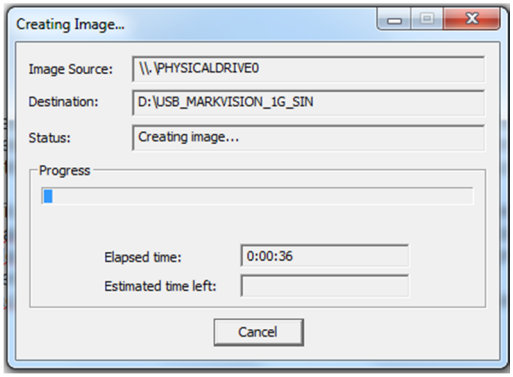
Fuente: El Autor.

Se comprobaron los parámetros definidos para el almacenamiento, y finalmente se inició la ejecución del proceso de extracción tras cliquear sobre el botón “Start”.

Así como también de algunas opciones complementarias, como:

- ✓ Verificación de las imágenes, una vez hayan sido creadas. (Recomendado)
- ✓ Precalcular estadísticamente el progreso o tiempo de ejecución frente a la recolección de la imagen. (opcional por el incremento significativo del proceso).
- ✓ Creación de un listado de archivos resultado del proceso. (Opcional)

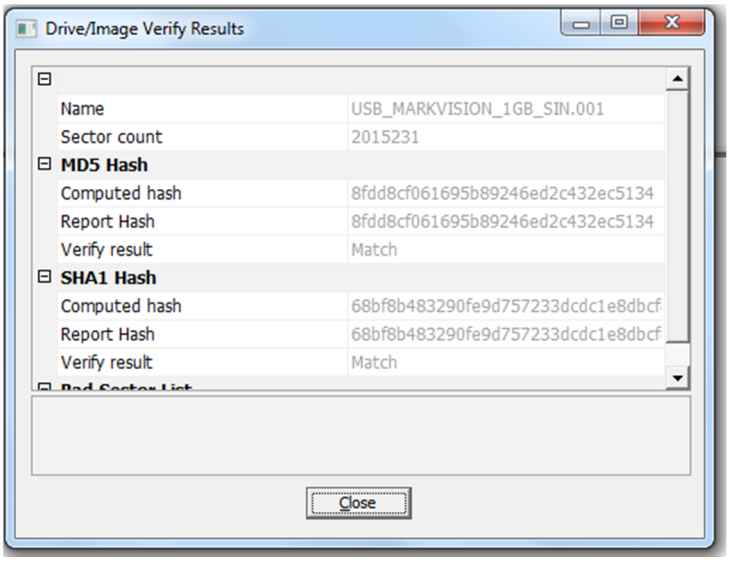
Figura 18. Selección fuente AccessData FTK Imager3-2-0 (Parte 7)



Fuente: El Autor.

Finalizada la creación de la imagen forense, inició la verificación de la imagen creada.

Figura 19. Selección fuente AccessData FTK Imager3-2-0 (Parte 8)

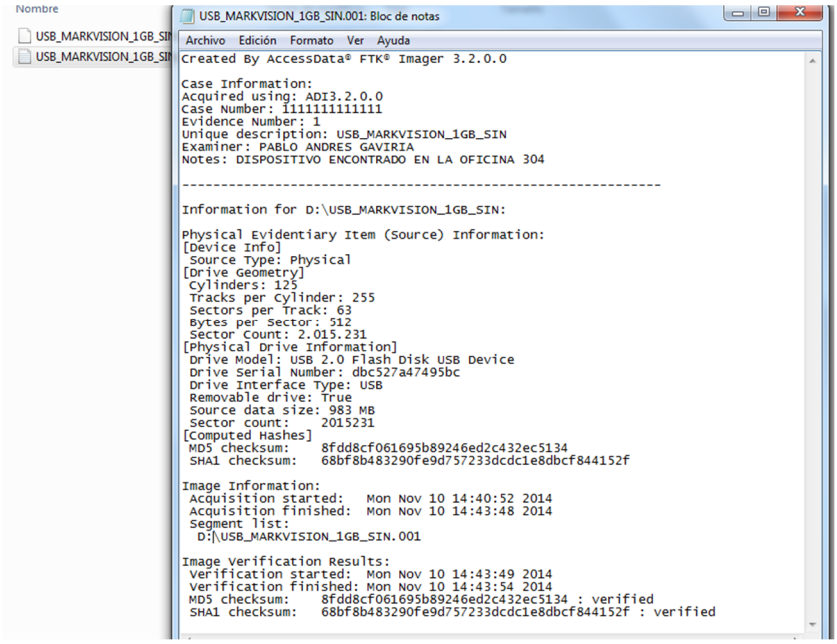


Fuente: El Autor.

Al finalizar todo este procedimiento se presentaron algunos resultados, los cuales permitieron identificar el número de sectores copiados, los sectores defectuosos y la generación de un Hash MD5 y un Hash SHA-1.

En el mismo directorio o carpeta donde se creó la imagen forense, se encontrará un archivo de texto con el mismo nombre seleccionado para la imagen forense en formato .TXT, en el cual registra toda la información detallada del proceso realizado.

Figura 20. Archivo resumen AccessData FTK Imager3-2-0



Fuente: El Autor.

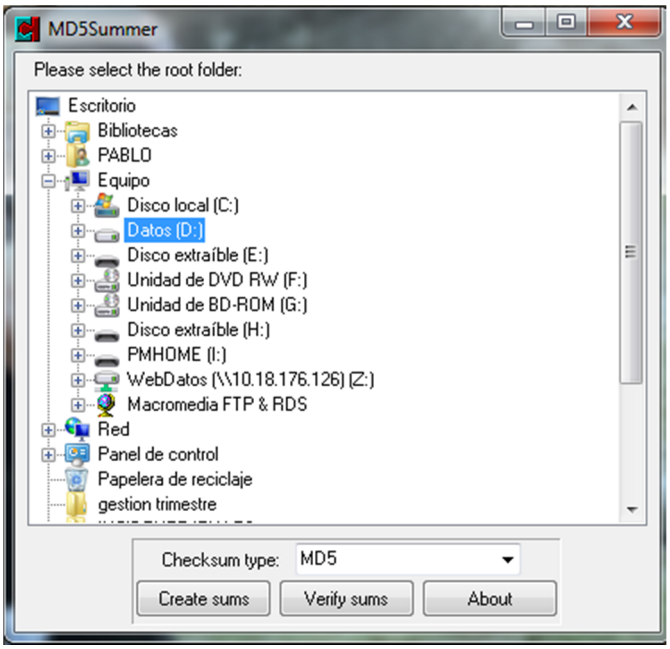
El archivo de imagen forense obtenido puede ser verificado, analizando dentro del archivo .TXT, las líneas contenidas en el aparte “Image verification Results” [verificación de resultados de imagen], donde se presenta un procedimiento el cual permite recalcular el HASH MD5 y SHA1.

4.4.3 Comprobación de las imágenes. Uno de los objetivos de este cálculo es básicamente garantizar la integridad de los datos, para ello, aplica un procedimiento el cual representa de manera compacta a un archivo o a un conjunto de datos. Los procedimientos de comprobación utilizan como base, el cálculo de los resultados obtenidos a través de la aplicación de algoritmos matemáticos MD5 o SHA1, tras un proceso denominado HASH.

En el desarrollo de la práctica presentada, se utilizó la herramienta md5summer.

Una vez se instaló y ejecutó instalada la aplicación, encontramos:

Figura 21. MD5 Summer

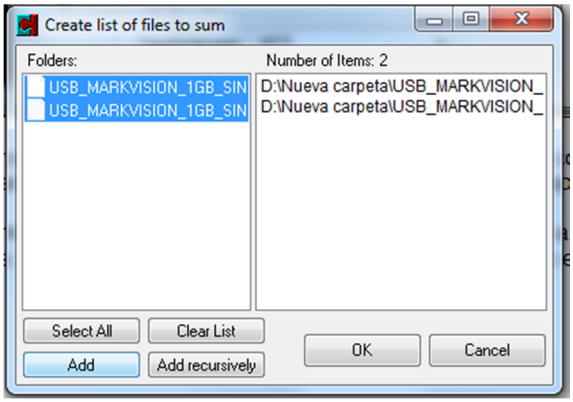


Fuente: El Autor.

Una ventana la cual permite explorar y observar la estructura y el contenido del sistema de archivos de la maquina en la cual se está ejecutando la aplicación.

Seleccionar el sitio donde se encuentran almacenados los archivos producto de la aplicación de FTK imager, definiendo en la opción “Checksum type”, el tipo de algoritmo que se va a aplicar, como ejemplo MD5. Cliqueando la opción “Create Sums”:

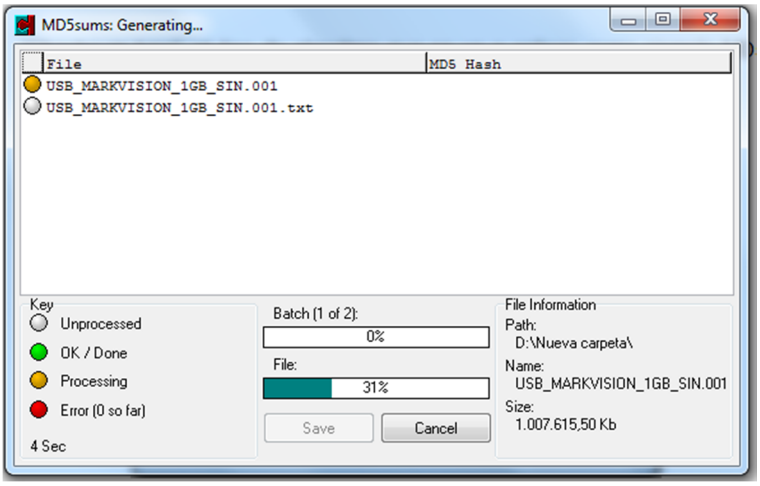
Figura 22. MD5 Summer (parte 1)



Fuente: El Autor.

Una vez seleccionados los archivos susceptibles de aplicación del procedimiento de verificación, se confirmó el proceso cliqueando sobre el botón “OK”.

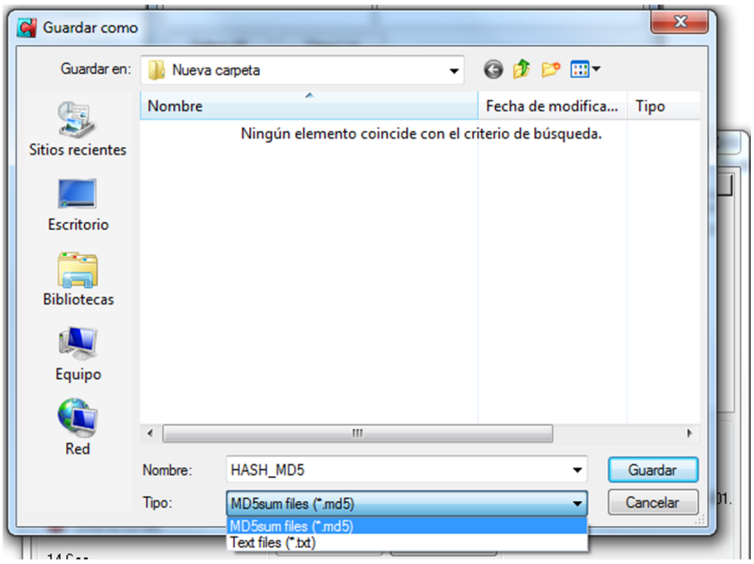
Figura 23. MD5 Summer (parte 2)



Fuente: El Autor.

Una vez finalizado el proceso, se estableció la ruta donde almacenamos el producto (Archivo) de verificación, el cual puede ser creado en formato MD5sumfile .md5 o en TXT.

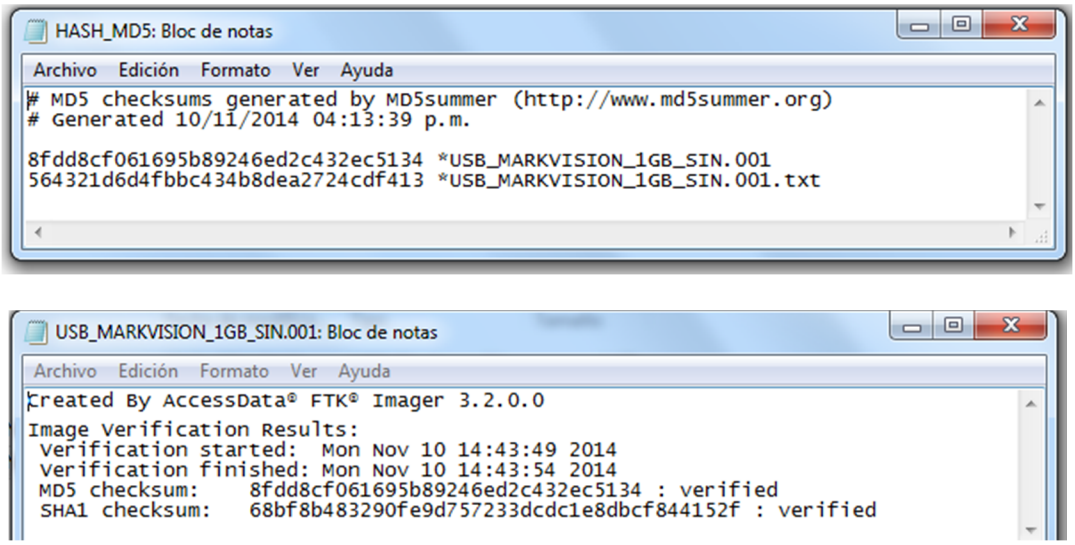
Figura 24. MD5 Summer (parte 3)



Fuente: El Autor.

El resultado de esta operación, permitió observar la aplicación del algoritmo HASH MD5, el cual debe coincidir con la información obtenida en el archivo resumen .TXT de FTK Imager.

Figura 25. MD5 Summer archivo resumen



Fuente: El Autor.

Finalmente, con el fin de garantizar y preservar el archivo de imagen creado, es recomendable exportar tanto el archivo forense, como el archivo resumen .TXT generado por FTK Imager, así como también el archivo de texto creado como resultado de la aplicación de MD5 SUMMER, y almacenarlos en un dispositivo de almacenamiento externo, el cual por lo general es de tipo óptico, al que deberá aplicarse el respectivo procedimiento de cadena de custodia, y garantizar así su validez jurídica. Adicionalmente, por recomendación deberá obtenerse una segunda copia, dejando las respectivas constancias, la cual será utilizada en el proceso de análisis.

4.4.4 Análisis de la Imagen Forense. Este procedimiento permitirá obtener concretamente los resultados frente a la hipótesis planteada dentro de la investigación, por lo tanto el objeto general del análisis diferirá para cada caso.

Sin embargo, el tratamiento de estos elementos como evidencia digital se materializa en estructuras de directorios, archivos o ficheros, y fragmentos de datos, que pudieran brindar algún tipo de información sobre el particular.

Todo Sistema Operativo determina la forma como administra los datos que vayan almacenando, lo que técnicamente se conoce como “sistema de archivos”, para ello utiliza, tablas de asignaciones, particiones, directorios del sistema, entre otros elementos, que conjugados configuran una plataforma de trabajo. Es importante resaltar la pericia y el conocimiento del investigador sobre un sistema de archivos en particular, su funcionamiento, los recursos que este utiliza, y un sin número de características particulares que garantizarán efectividad y eficacia en la búsqueda de información.

Con esta guía se pretende generalizar elementos claves dentro del análisis forense, que ayudan a comprender la aplicación y el funcionamiento de las herramientas diseñadas para este fin, y su práctica, se desarrolló bajo la plataforma Windows 7, utilizando como software de análisis EnCase.

4.4.4.1 Herramientas y recursos. A nivel de hardware se utilizó:

- ✓ Computador de escritorio compuesto por un procesador AMD Phentom (tm) II x4 Procesor 3.20 GHZ, con una memoria RAM de 8 GB, Disco Duro de 1 Tb, unidad DVD con compatibilidad DL, 2 puertos USB, y con un Sistema Operativo Windows 7 a 64 bits.

  Si bien es cierto, esta configuración es una de las más básicas, nos será útil para desarrollar el ejercicio planteado, aunque el factor tiempo redundará en el procesamiento de tareas específicas.

A nivel de Software utilizaremos:

- ✓ Sistema operativo Windows 7 a 64 bits.

- ✓ Software Forense EnCase en su Versión 7.9.

  Este aplicativo es una solución creada por la firma Guidance Software, y lleva algunas décadas liderando el campo forense como software comercial, brindando una serie de características que lo hacen flexible y funcional a la hora de analizar una gran variedad de dispositivos de almacenamiento, incluidos algunos smartphones y BlackBerry.

En las últimas versiones, ha implementado la automatización de procesos, lo que lo hace más amigable como herramienta forense, con una funcionalidad marcada en la creación de informes y reportes.

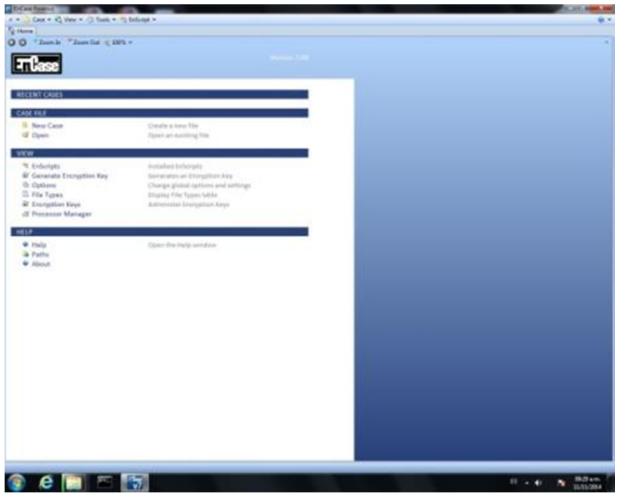
Sin embargo, su costo es algo elevado y requiere de máquinas robustas que permitan su ejecución, ya que su demanda de recursos en procesador y memoria es aceptable.

4.4.4.2 Desarrollo práctico con EnCase. Como base de análisis, utilizamos el archivo de imagen forense obtenida en el apartado anterior, desarrollando los siguientes pasos:

- ✓ Creación del caso

Una vez se ingresó al aplicativo EnCase.

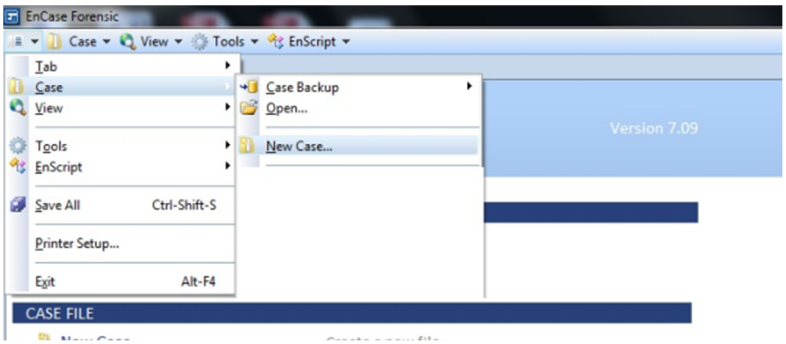
Figura 26. EnCase pantalla principal



Fuente: El Autor.

Desde la barra de menú, se localizó el icono de inicio o general, seleccionando la opción: Case/New Case.

Figura 27. EnCase menú principal

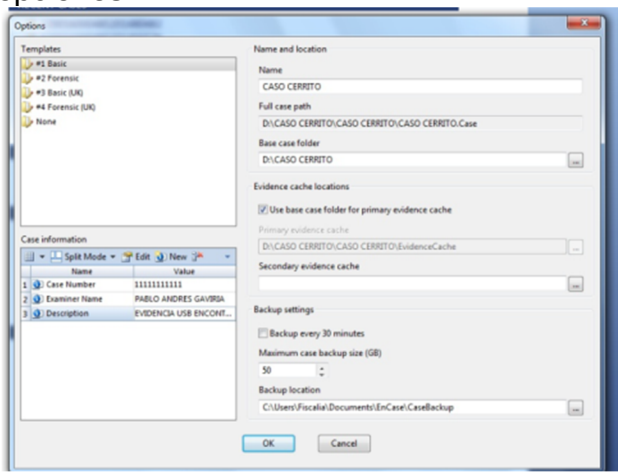


Fuente: El Autor.

Dentro de las opciones de identificación de la sesión o proyecto, EnCase permite establecer un nombre de caso, el cual dependiendo de los parámetros definidos por el laboratorio, podría referirse al número de caso, o un nombre específico, la ruta de directorio donde se almacenará toda la estructura de directorios que automáticamente lo genera el aplicativo para el desarrollo de sus procedimientos, el número de caso asignado por la autoridad judicial, el nombre del investigador que desarrolla el análisis, y un espacio para la descripción del caso.

Adicionalmente presenta opciones que permiten controlar la generación de un backup del proyecto, la ruta de almacenamiento y el tiempo en que se ejecutará dicha copia, procedimiento que puede ser opcional.

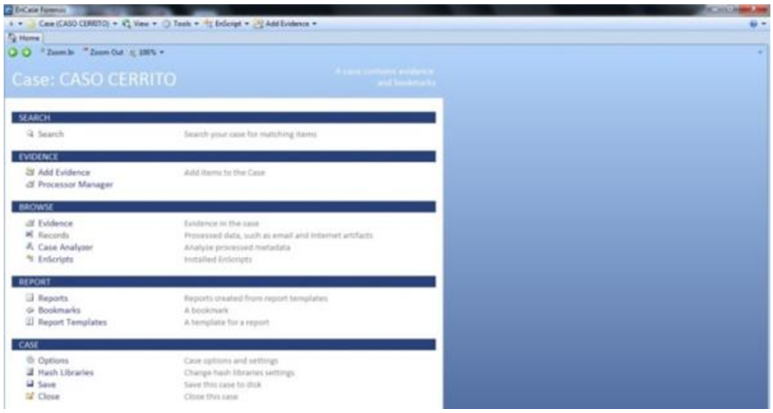
Figura 28. EnCase opciones



Fuente: El Autor.

Una vez definidos los parámetros sobre la sesión, el aplicativo activa las opciones de trabajo, por medio de una pantalla que ofrece accesos rápidos a las diferentes funciones.

Figura 29. EnCase pantalla principal de caso

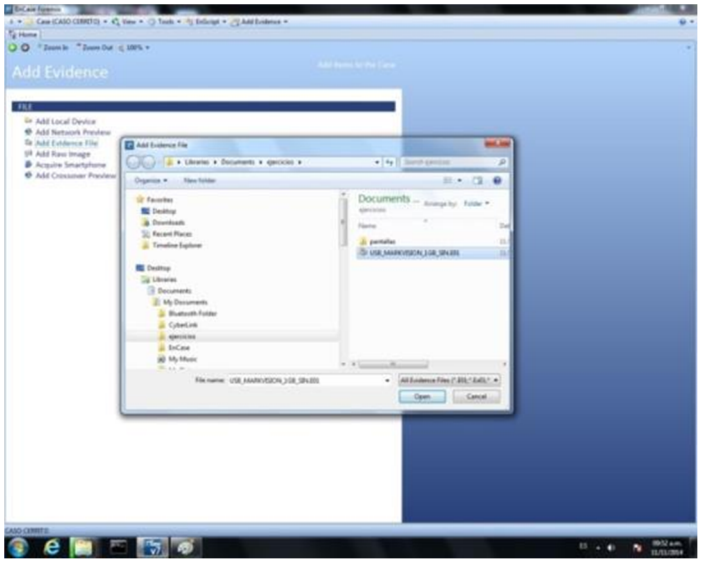


Fuente: El Autor.

- ✓ Agregar las Imágenes Forenses.

Para este momento se agregaron las imágenes forenses a procesar, utilizando para ello la opción “Add evidence”.

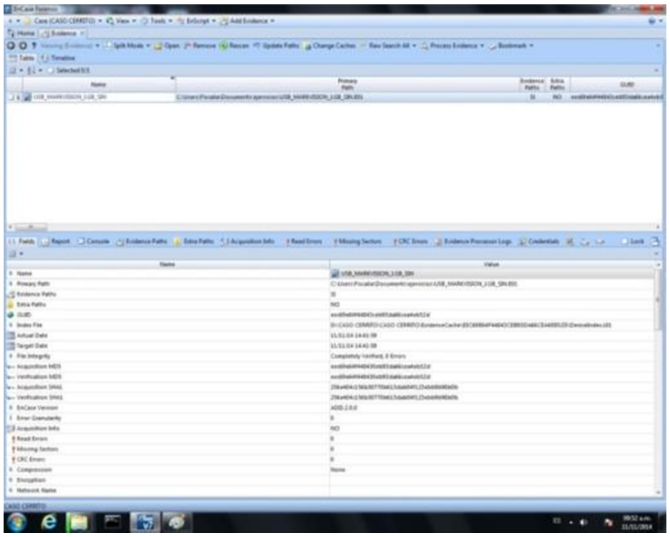
Figura 30. EnCase “Add Evidence” (parte 1)



Fuente: El Autor.

Se visualizaron por medio de un listado, los archivos de imágenes forenses agregadas al proyecto.

Figura 31. EnCase “Add Evidence” (parte 2)

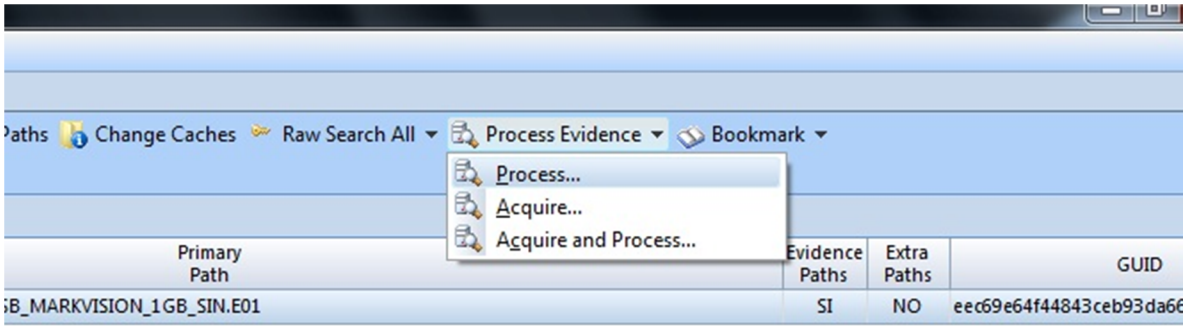


Fuente: El Autor.

- ✓ Procesar los archivos de imagen

Esta tarea tiene por objeto, realizar diferentes procesos de procesamiento sobre la imagen forense, los cuales en versiones anteriores debían desarrollarse de manera individual.

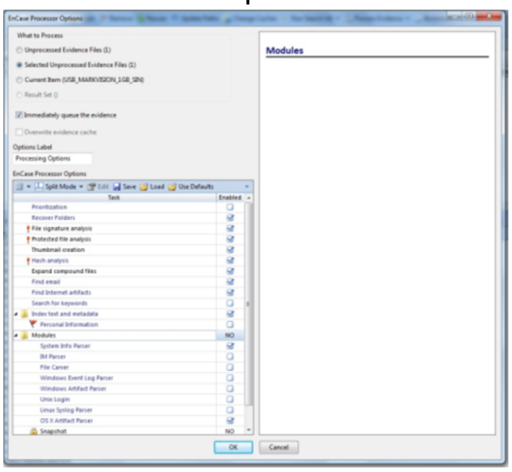
Figura 32. EnCase “Process Evidence”



Fuente: El Autor.

Los procesos o tareas, refieren la búsqueda de particiones, recuperación de archivos, análisis de firmas de archivos, descompresión o clasificación de archivos comprimidos,

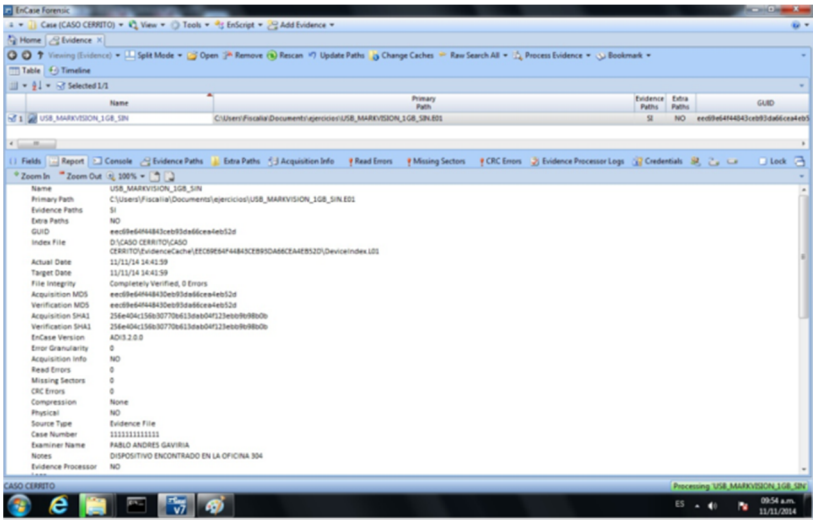
Figura 33. EnCase “Process Evidence/ options”



Fuente: El Autor.

Análisis y aplicación de Hash MD5 y SHA1, clasificación de elementos referentes a navegación en internet, archivos de correo electrónico, módulos que analizan las llaves y logs del sistema operativo, los cuales contienen información particular del mismo, como hardware, software, entre otros.

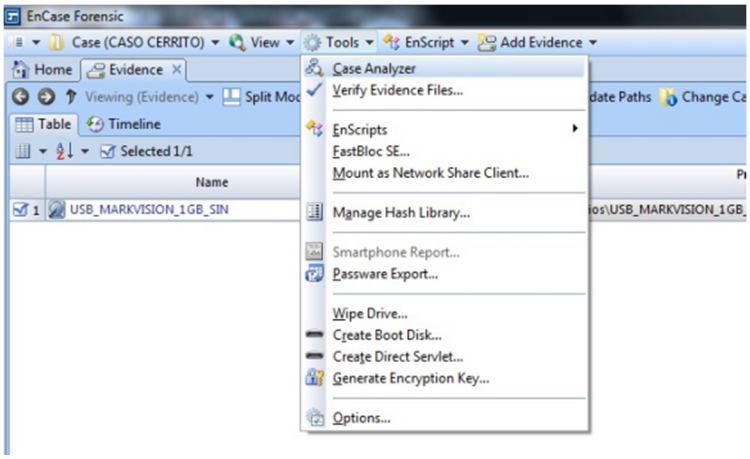
Figura 34. EnCase “Report”



Fuente: El Autor.

Los resultados a este procedimiento, pueden ser vistos con ayuda del “Case Analizer”

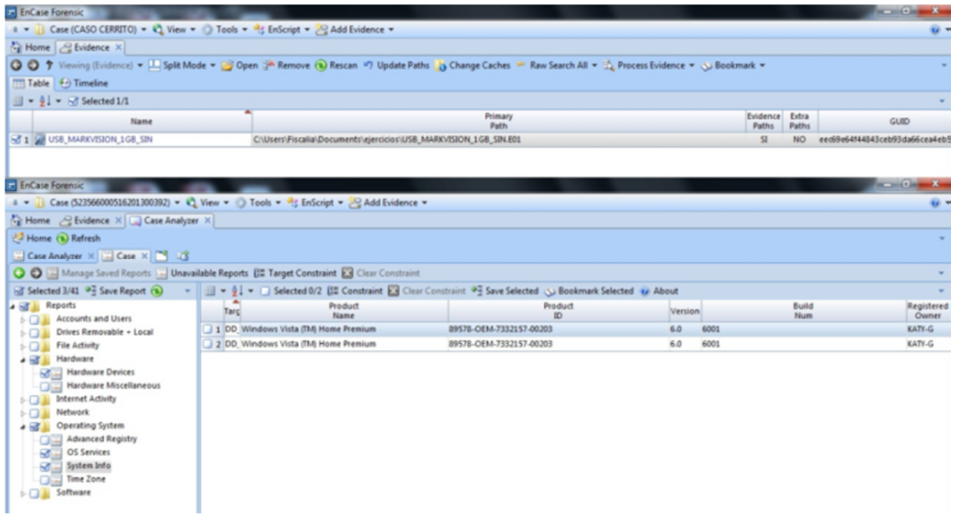
Figura 35. EnCase “Case Analizer”



Fuente: El Autor.

Dependiendo el tipo de dispositivo de almacenamiento que se esté analizando, la información resultado del procedimiento puede variar, tal como se puede observar en la siguiente imagen, la cual muestra los resultados del análisis del dispositivo USB, en comparación al análisis adelantado a un Disco Duro.

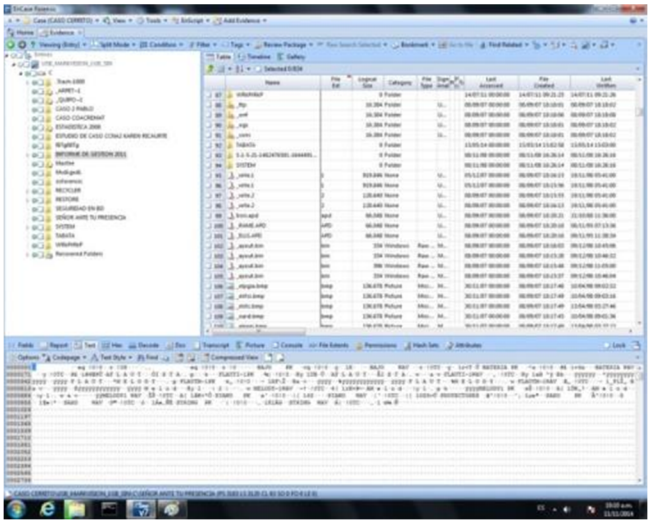
Figura 36. EnCase comparación dispositivos



Fuente: El Autor.

EnCase en su manejo, ofrece un ambiente de trabajo a partir de una ventana de navegación, por ejemplo, es fácil observar y explorar el contenido de la imagen forense, desde un árbol de directorios:

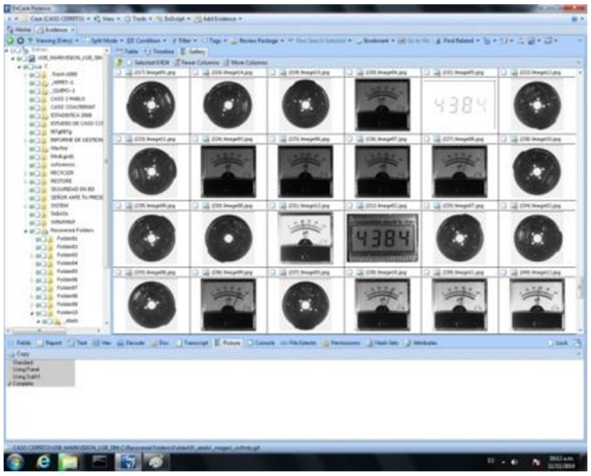
Figura 37. EnCase Estructura de directorios



Fuente: El Autor.

Ofrece un botón o comando que permite visualizar directamente las imágenes contenidas en el dispositivo, desde la opción “Gallery”:

Figura 38. EnCase “Gallery”



Fuente: El Autor.

Cada uno de los directorios y subdirectorios, cuentan con dos elementos:

Uno de ellos hace referencia a una bandera la cual una vez activada se marca de color verde, útil para seleccionar y visualizar todo el contenido de la imagen, unidad o partición, carpeta, subcarpeta, y un cuadro checklist útil para seleccionar algunos elementos, con el fin de exportarlos, o aplicar alguna operación directa sobre ellos.

Figura 39. EnCase selección de elementos

Fuente: El Autor.

Las opciones presentadas anteriormente permiten explorar el contenido completo de la imagen forense, sin embargo, la búsqueda de información sería algo complicada demandando tiempo ya que ese haría de forma manual.

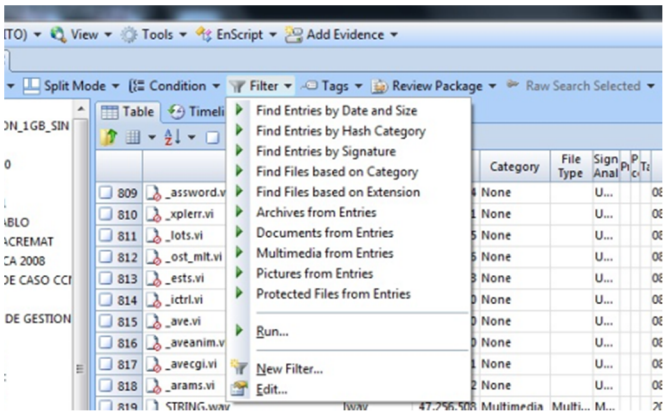
EnCase ofrece distintas posibilidades para localizar datos frente a una investigación, entre ellos.

Aplicación de Filtros.

Encontramos la posibilidad de clasificar la información por medio de filtros automáticos que facilitan ubicar un determinado archivo, esos criterios pueden ser: fecha y hora, tipo de archivo, extensión de archivo, tamaño, entre otros.

Una vez seleccionado los elementos, activamos el filtro desde la opción Filter:

Figura 40. EnCase “Filter”

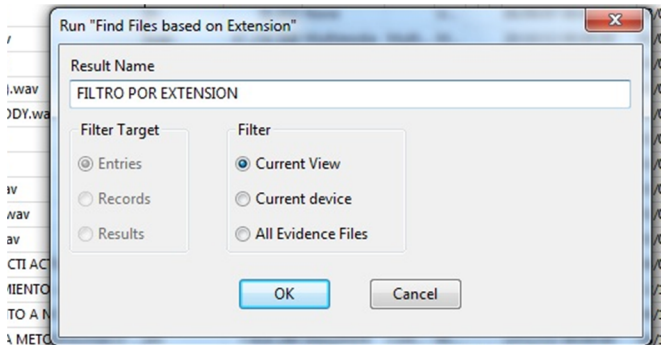


Fuente: El Autor.

Siguiendo con nuestro ejemplo, se buscaran todos los documentos de texto asociados a Microsoft Word y asociamos las extensiones DOC y DOCX.

Para ello, dentro de Filter, se ubicará la opción /Find Files base on Extension.

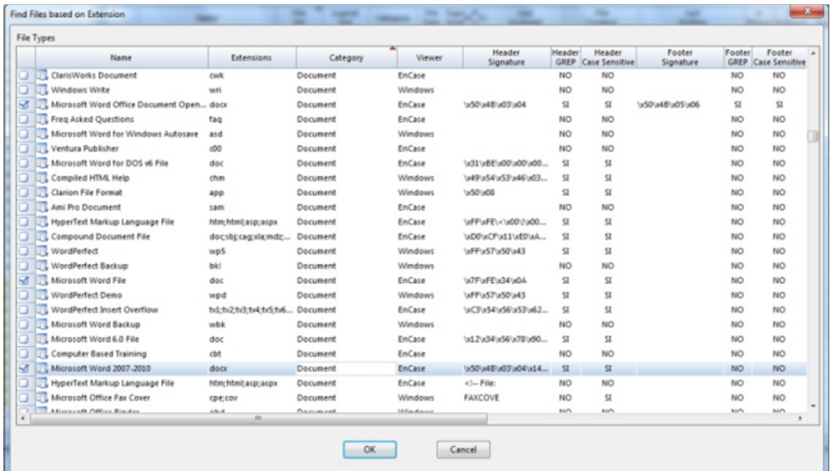
Figura 41. EnCase “Find Files” (parte1)



Fuente: El Autor.

Se establece un nombre para identificar el filtro, complementando la búsqueda a la vista actual, dispositivo actual o a todas las evidencias (imágenes forenses) agregadas a la sesión o al proyecto.

Figura 42. EnCase “Find Files” (parte2)

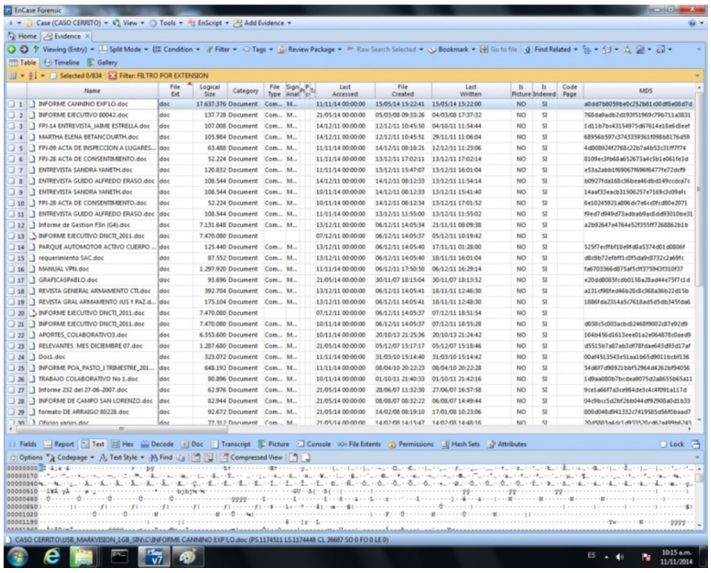


Fuente: El Autor.

Para este momento, se presenta una ventana en la cual se seleccionarán las extensiones o File Types como parámetro de clasificación.

La cual una vez ejecutada, se presentarán todos los resultados en una nueva ventana.

Figura 43. EnCase “Find Files” (parte3)

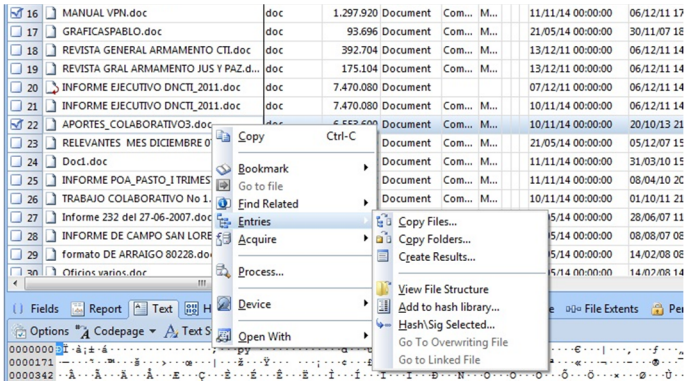


Fuente: El Autor.

La búsqueda para este momento, reduce el número de posibilidades visualizando los archivos, cuya extensión se relaciona con los parámetros establecidos en el filtro.

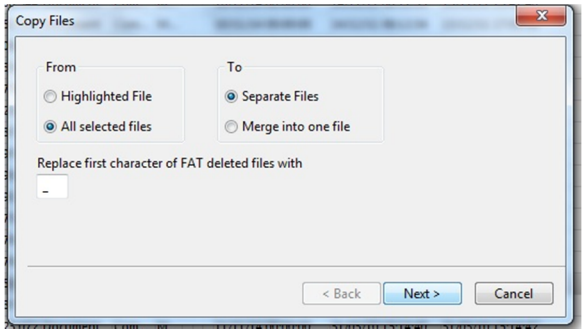
Una vez ubicados los archivos o elementos útiles para la investigación, se pueden exportar, activando los checklist, click botón derecho, opción entires/Copy files.

Figura 44. EnCase "Export Files" (parte1)



Fuente: El Autor.

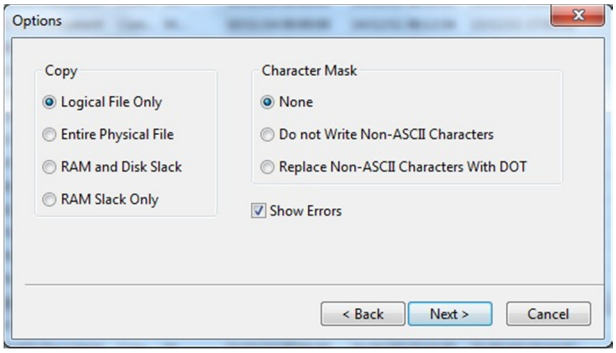
Figura 45. EnCase "Export Files" (parte 2)



Fuente: El Autor.

Se activa o selecciona la fuente sobre la cual se aplicará el filtro desde la opción From.

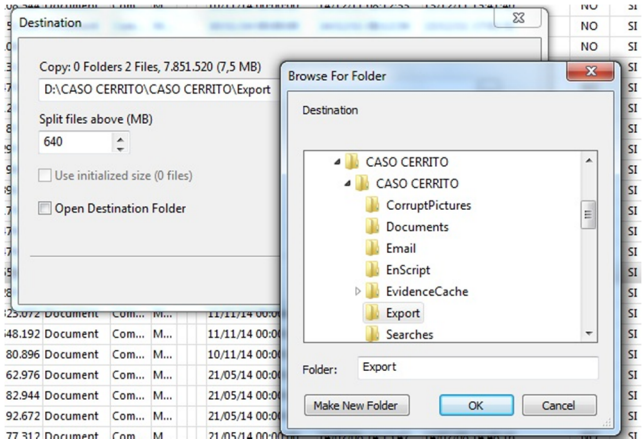
Figura 46. EnCase “Export Files” (parte3)



Fuente: El Autor.

Se selecciona la forma como se extraerá la información, ubicando la carpeta o directorio donde se copiaran los archivos.

Figura 47. EnCase “Export Files” (parte 4)



Fuente: El Autor.

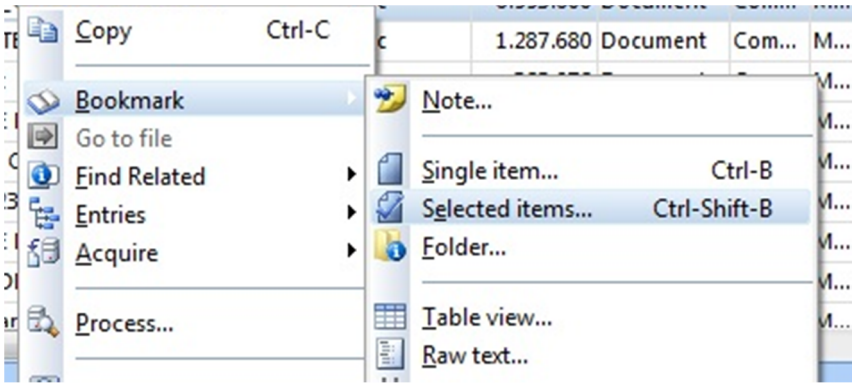
Bookmarks

Los Bookmarks o marcadores se utilizan con el fin de clasificar la información encontrada y que sea mucho más fácil la construcción del informe final.

Para ello, una vez se hayan seleccionado los elementos o archivos que contengan información relevante sobre el caso en investigación, se cliquea

con el botón derecho del mouse, seleccionando la opción bookmark/selected ítems.

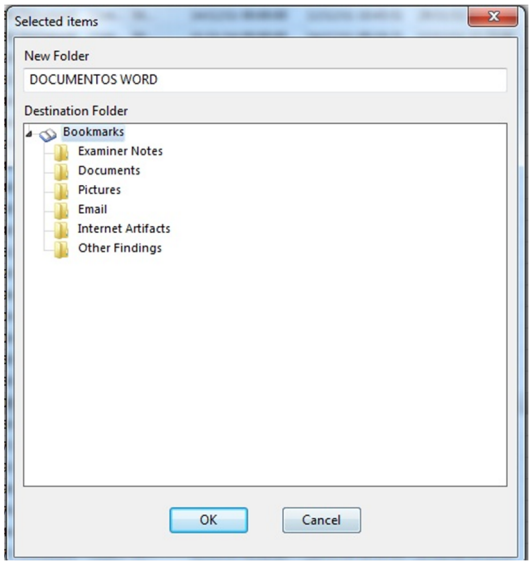
Figura 48. EnCase “Bookmarks” (parte 1)



Fuente: El Autor.

Se establece el nombre para el marcador y el lugar donde será almacenado:

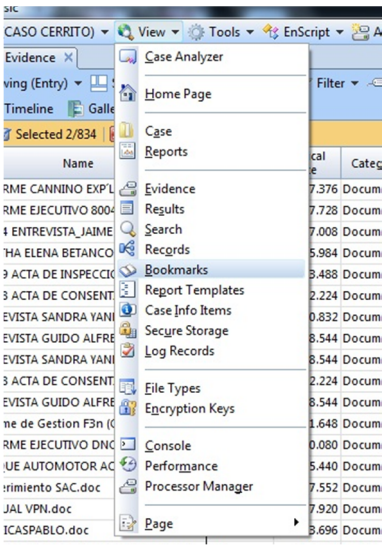
Figura 49. EnCase “Bookmarks” (parte 2)



Fuente: El Autor.

Una vez se han creado los bookmark se pueden encontrar desde la opción View/Bookmarks:

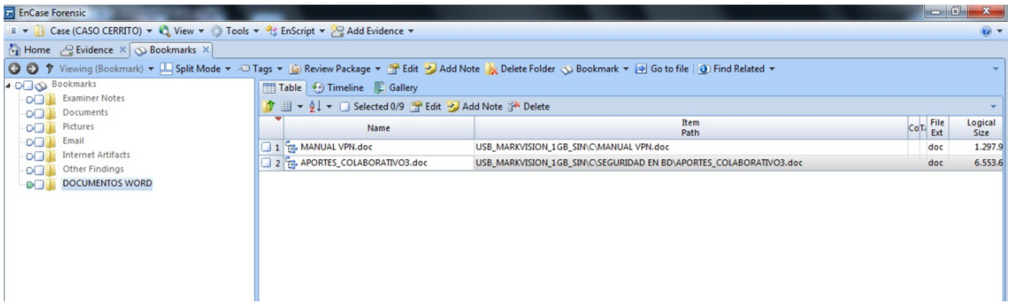
Figura 50. EnCase “Bookmarks” (parte 3)



Fuente: El Autor.

Se presenta una ventana en la cual se presentan los “bookmarks” creados

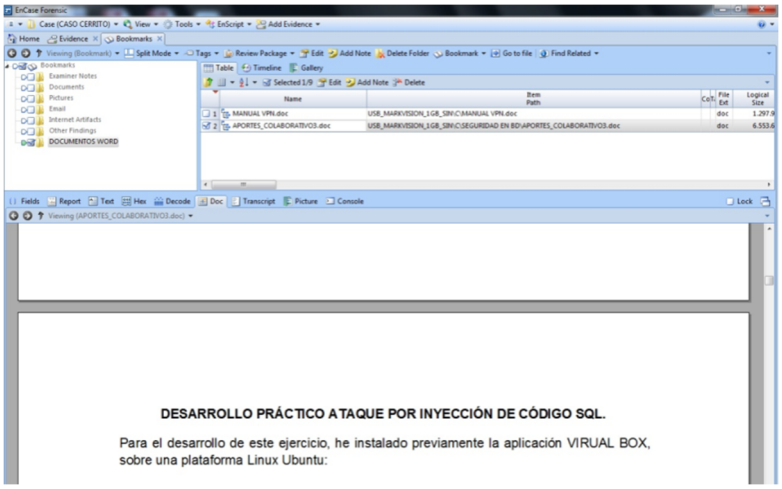
Figura 51. EnCase “Bookmarks” (parte 4)



Fuente: El Autor.

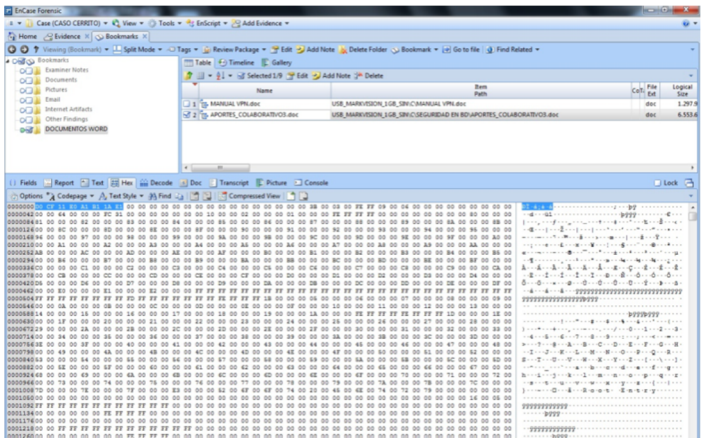
La visualización del contenido de los archivos encontrados, puede ser activada desde las opciones “Doc”, “text” “hex”, o report.

Figura 52. EnCase “Bookmarks” (parte 5)



Fuente: El Autor.

Figura 53. EnCase “Bookmarks” (parte 6)

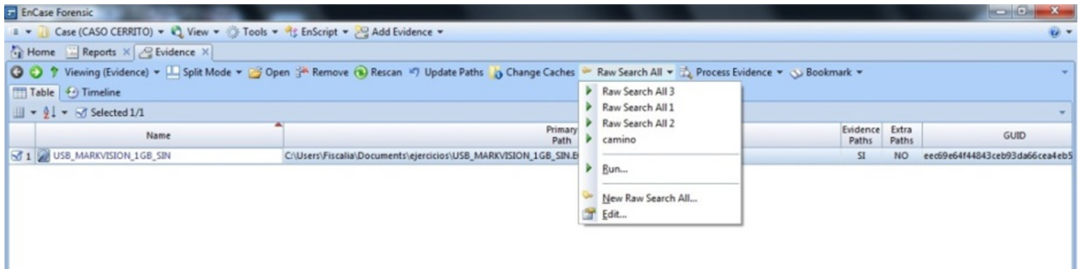


Fuente: El Autor.

Búsqueda por cadena de caracteres

EnCase permite adelantar procedimientos de búsqueda por palabras o frases, definiendo parámetros como cadenas de caracteres, que permiten ampliar las posibilidades de encontrar información relacionada al caso, y automatizan el procedimiento.

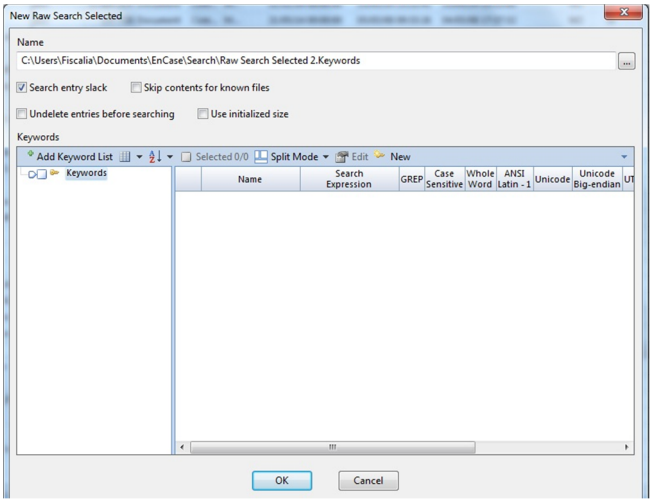
Figura 54. EnCase “Raw Search” (parte 1)



Fuente: El Autor.

Esta herramienta se encuentra ubicada en la opción “Raw Select All”/ New Raw Search All.

Figura 55. EnCase “Raw Search” (parte 2)

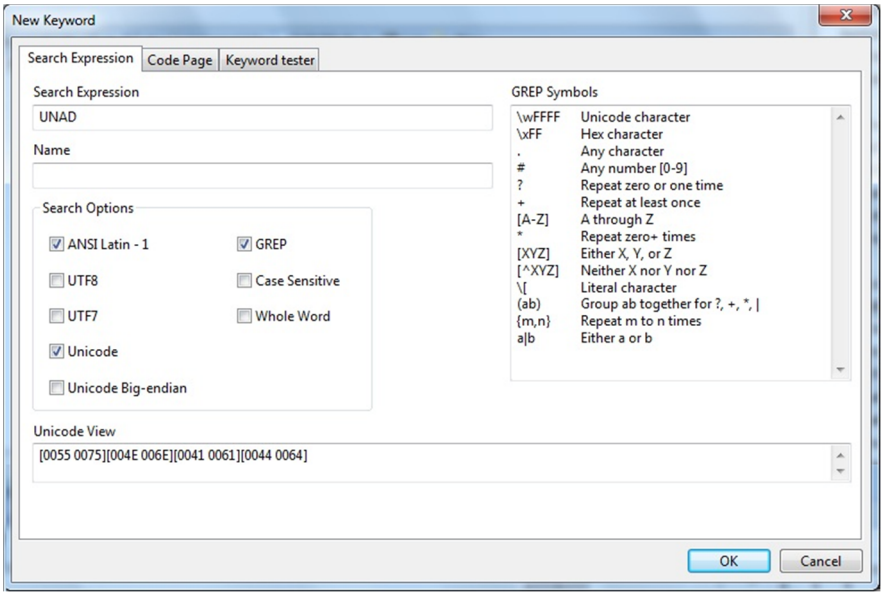


Fuente: El Autor.

Se define el sitio o lugar donde se almacenará el criterio de búsqueda, el cual se crea desde la opción “New”.

Nuestro ejemplo se desarrolló teniendo como base el criterio de búsqueda la cadena de caracteres “UNAD”, criterio que puede ser complementado, utilizando algunas combinaciones de comodines o GREP Symbols, así como también las opciones de búsqueda, entre los diferentes opciones de búsqueda y codificación de texto como lo es ANSI Latin -1, UTF7, Unicode.

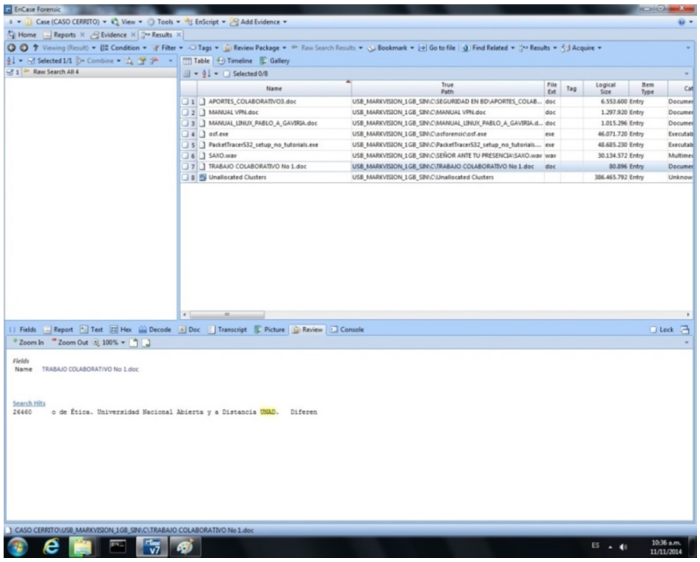
Figura 56. EnCase “Raw Search” (parte 3)



Fuente: El Autor.

Una vez se ejecuta el parámetro de búsqueda creado se puede observar en sus resultados, los archivos que cumplen con los parámetros, así como también las líneas de texto que coinciden con la cadena de texto

Figura 57. EnCase “Raw Search” (parte 4)



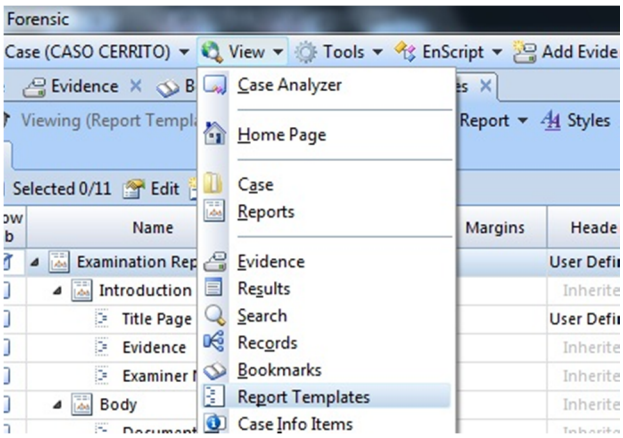
Fuente: El Autor.

Generación de reportes

Como se mencionó anteriormente EnCase ofrece flexibilidad en la creación de reportes, automatizando algunos parámetros o presentando la información agrupada por los “Bookmarks” creados por el usuario.

Esta opción se activa desde el menú View/Report Templates.

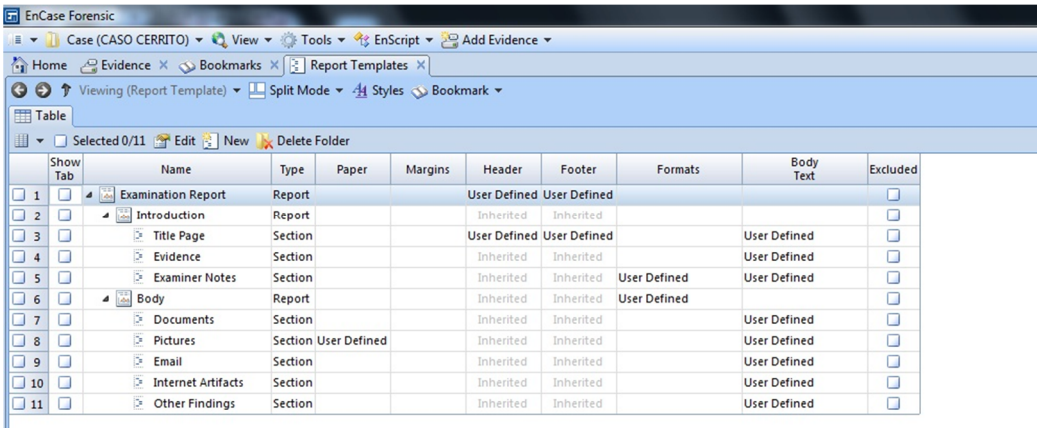
Figura 58. EnCase “Report Templates” (parte 1)



Fuente: El Autor.

Se presenta la estructura por defecto que EnCase ofrece frente a la creación de reportes, sin embargo, se puede crear otros criterios desde la opción “NEW”.

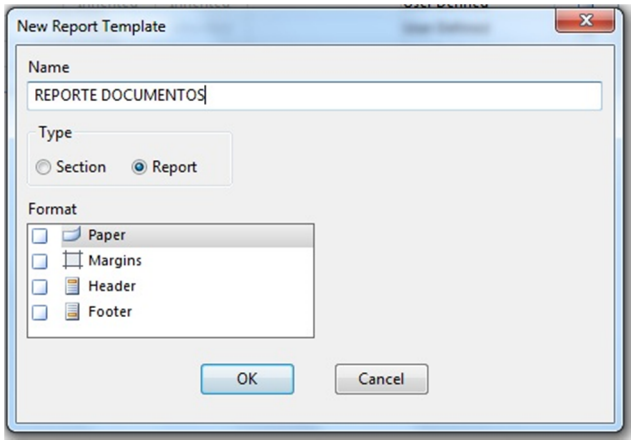
Figura 59. EnCase “Report Templates” (parte 2)



Fuente: El Autor.

Se establecen los parámetros para la nueva sección del informe, estableciendo un nombre, un tipo (sección dentro de la estructura por defecto, o un nuevo reporte), así como también su formato.

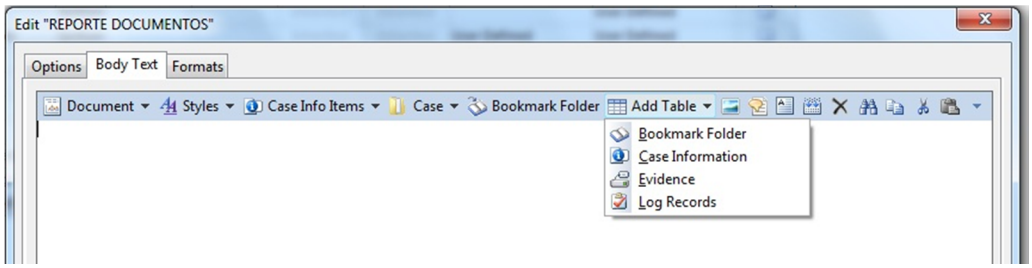
Figura 60. EnCase "Report Templates" (parte 3)



Fuente: El Autor.

Una vez creada la sección o reporte, se edita, teniendo como base los elementos que se listarán, la forma de presentación de su contenido, el formato, entre otros.

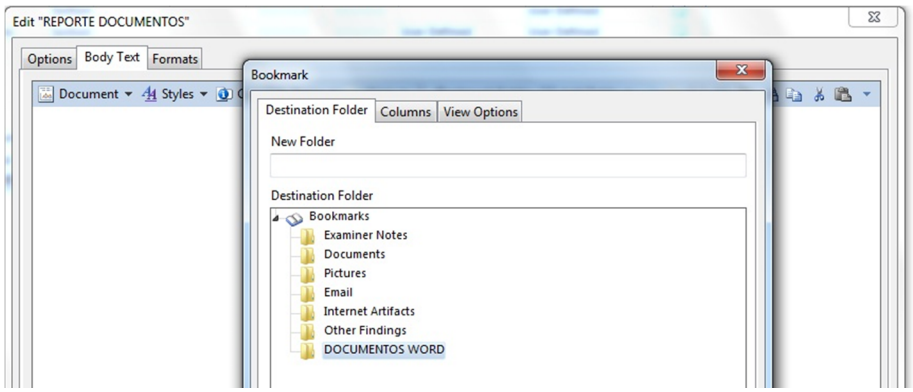
Figura 61. EnCase "Report Templates" (parte 4)



Fuente: El Autor.

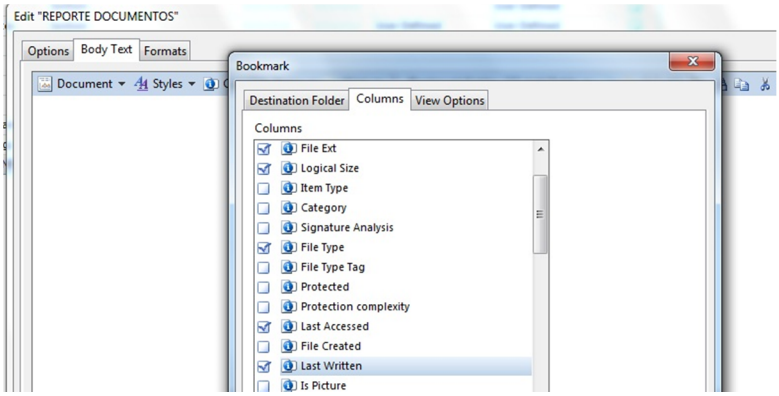
Se plantea la continuación del ejercicio, optando la opción de crear un reporte con los "bookmark" generados en el aparte anterior.

Figura 62. EnCase “Report Templates” (parte 5)



Fuente: El Autor.

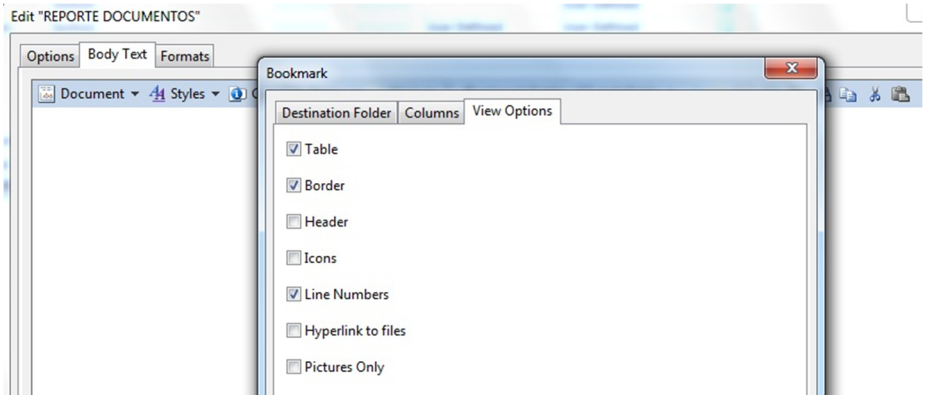
Figura 63. EnCase “Report Templates” (parte 6)



Fuente: El Autor.

Se establecen o definen los datos o información correspondiente a los metadatos aportados por cada uno de los archivos agregados a los “bookmark”.

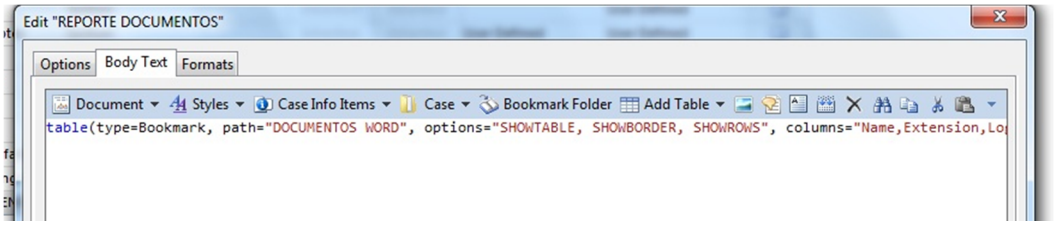
Figura 64. EnCase “Report Templates” (parte 7)



Fuente: El Autor.

De igual forma se definen las opciones de visualización del contenido, para tabla, bordes, encabezados, número de líneas, entre otros.

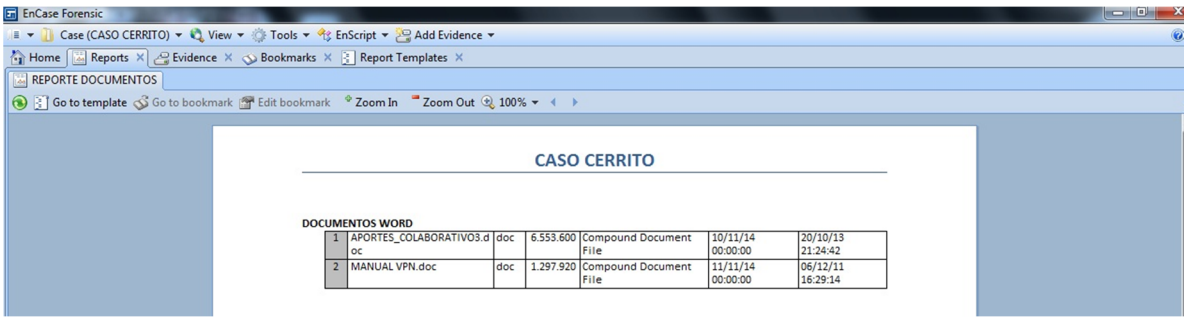
Figura 65. EnCase “Report Templates” (parte 8)



Fuente: El Autor.

Parámetros con los cuales EnCase crea o define una sintaxis o cadena de instrucciones.

Figura 66. EnCase “Report Templates” (parte 9)

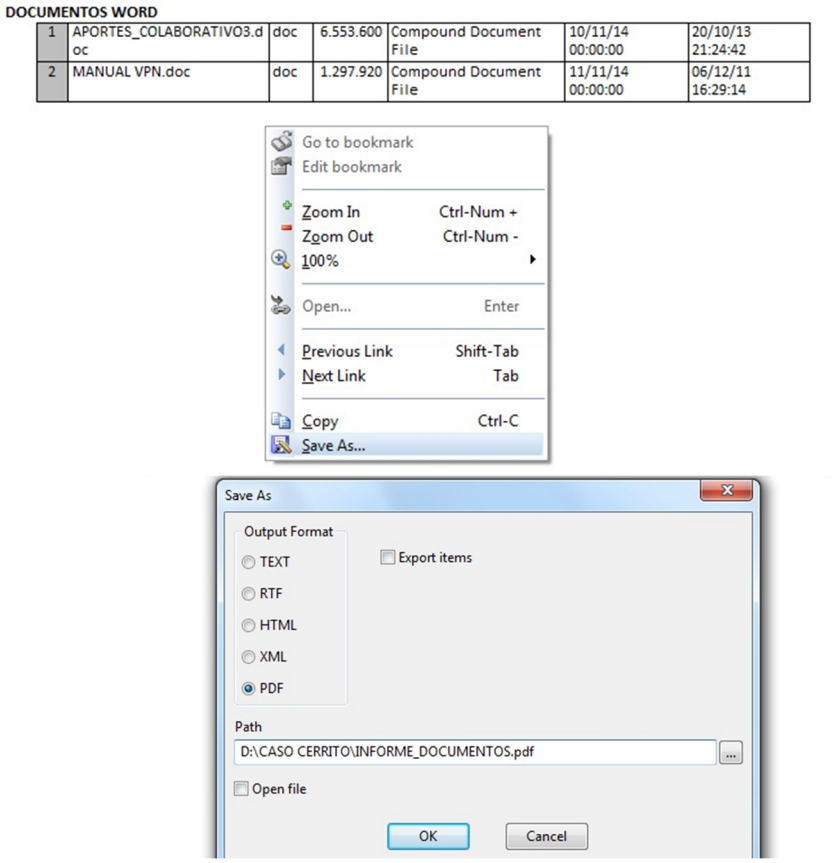


Fuente: El Autor.

Las cuales finalmente permiten generar el informe sobre el contenido seleccionado.

Este informe es posible exportarlo como archivo: Xls, Pdf, Doc, entre otros. Activando la opción Save As…, desde el click del botón derecho del mouse

Figura 67. EnCase "Report Templates" (parte 10)



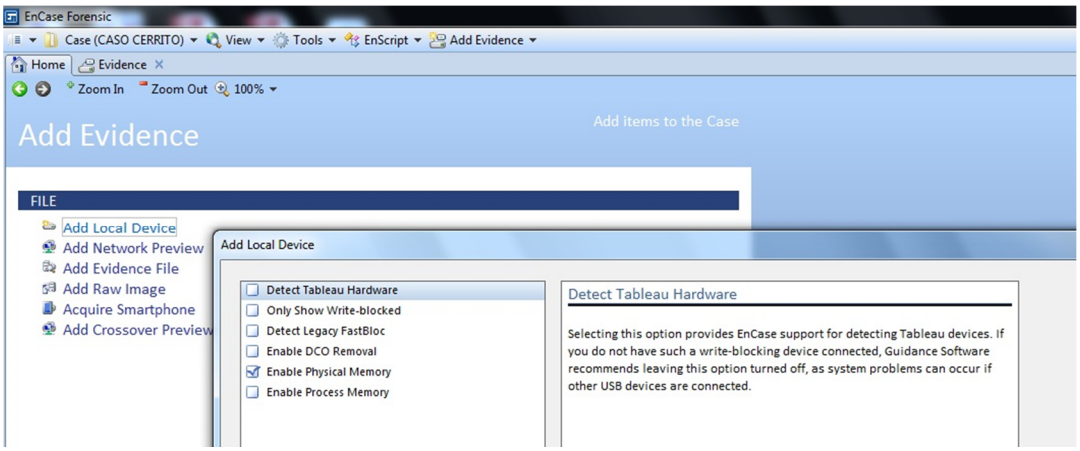
Fuente: El Autor.

Generación de imágenes forenses

Otra de las opciones formuladas por EnCase, es la obtención de un archivo de imagen forense, de dispositivos de almacenamiento entre ellos Smartphones

Para ello, al momento de agregar la evidencia (vista en el apartado anterior), se selecciona la opción “Add local devices”

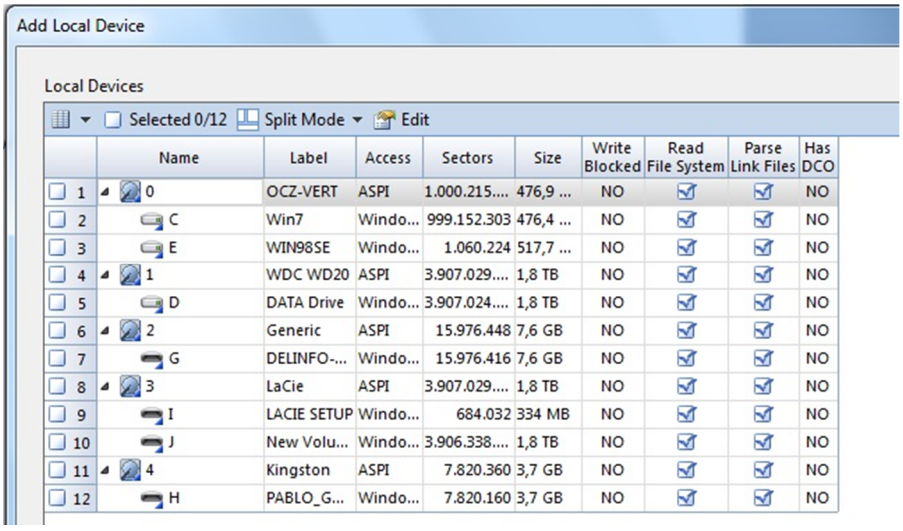
Figura 68. EnCase “Acquire evidence” (parte 1)



Fuente: El Autor.

EnCase permite seleccionar diferentes fuentes para la obtención de las imágenes forenses, particularmente de Hardware Tableu, dispositivos bloqueados contra escritura, memoria Física o datos en proceso (Extracción en caliente).

Figura 69. EnCase “Acquire evidence” (parte 2)

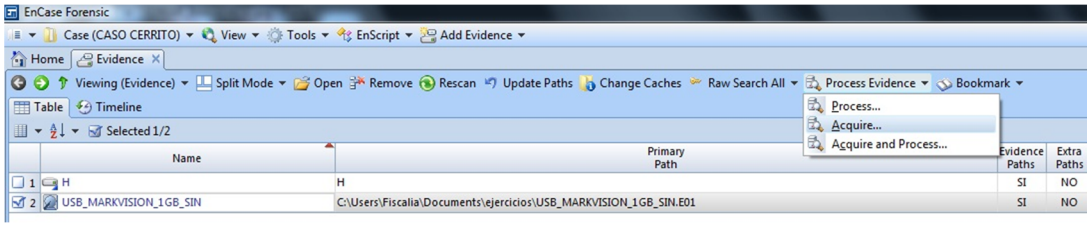


	Name	Label	Access	Sectors	Size	Write Blocked	Read File System	Parse Link Files	Has DCO
1	0	OCZ-VERT	ASPI	1.000.215....	476,9 ...	NO			NO
2	C	Win7	Windo...	999.152.303	476,4 ...	NO			NO
3	E	WIN98SE	Windo...	1.060.224	517,7 ...	NO			NO
4	1	WDC WD20	ASPI	3.907.029....	1,8 TB	NO			NO
5	D	DATA Drive	Windo...	3.907.024....	1,8 TB	NO			NO
6	2	Generic	ASPI	15.976.448	7,6 GB	NO			NO
7	G	DELINFO-...	Windo...	15.976.416	7,6 GB	NO			NO
8	3	LaCie	ASPI	3.907.029....	1,8 TB	NO			NO
9	I	LACIE SETUP	Windo...	684.032	334 MB	NO			NO
10	J	New Volu...	Windo...	3.906.338....	1,8 TB	NO			NO
11	4	Kingston	ASPI	7.820.360	3,7 GB	NO			NO
12	H	PABLO_G...	Windo...	7.820.160	3,7 GB	NO			NO

Fuente: El Autor.

De acuerdo a la selección formulada, se presentan las unidades físicas y lógicas de los dispositivos que se encuentran instalados en la máquina donde se ejecuta el aplicativo.

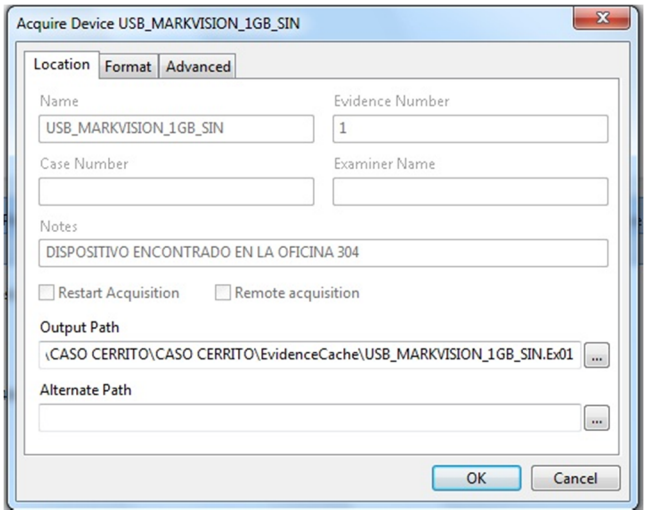
Figura 70. EnCase “Acquire evidence” (parte 3)

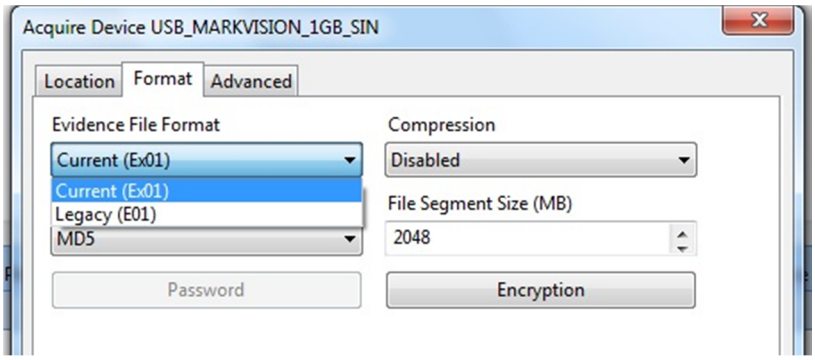


Fuente: El Autor.

Una vez montado o agregado el dispositivo, se activa la opción “Process evidence/ Adquire”, definiendo los parámetros para la imagen, como nombre, formato, hash y ubicación donde será almacenada.

Figura 71. EnCase “Acquire evidence” (parte 4)





Fuente: El Autor.

Los archivos o información, deberá ser exportada en un dispositivo de almacenamiento externo, no sin antes, aplicar el proceso de HASH con la herramienta md5summer tal como se refirió anteriormente. Finalmente, a este elemento debe aplicarse el respectivo Procedimiento de cadena de custodia, para garantizar su legalidad.

4.5 RECOMENDACIONES FRENTE AL TEMA DE LA PREVENSIÓN DE LOS DELITOS INFORMÁTICOS

Para las organizaciones y/o entidades públicas y privadas, la materialización de Políticas de Seguridad en Informática, indiscutiblemente se ve reflejada en su aplicación y en el uso adecuado de los recursos informáticos, garantizando así la protección frente a todo tipo de amenazas deliberadas o accidentales. Estas políticas, aparte de cumplir con los lineamientos establecidos en la Norma Técnica Colombiana NTC-ISO/IEC 27001, deben ser debidamente supervisadas tras un estricto seguimiento.

Al hablar de conductas negativas o delitos informáticos, debemos ser coherentes y consecuentes frente al tema, lo cual éticamente nos obliga a cumplir con las normas existentes en el uso adecuando de los recursos informáticos con los que contamos y con los cuales desarrollamos nuestras funciones. Es muy común observar el tema de piratería informática, no solo en la distribución de software ilegal, sino cuando adquirimos todo tipo de programas a través de diferentes fuentes, contribuyendo con esta conducta frente a la demanda que generamos.

Contar con las herramientas y recursos suficientes a nivel de los equipos informáticos, lo cual garantice la actualización regular del sistema y el software

instalado, así como también un antivirus que deberá ser actualizado con frecuencia, ejecutándolo cada vez que se utilice nuevos dispositivos de almacenamiento externo, un Firewall o cortafuegos que permita restringir los accesos No autorizados a internet y finalmente un Anti-spyware para evitar la instalación de espías que puedan recopilar información confidencial.

Materializar las normas de convivencia y seguridad frente al uso del internet, los correos electrónicos y demás recursos que esta ofrece, de nosotros depende el nivel de vulnerabilidad que vamos a establecer:

- ✓ Utilizando siempre contraseñas con una longitud mínima de 8 caracteres compuestos por letras, números y símbolos, las cuales serán modificadas frecuentemente y sobre todo de carácter personal e intransferible.

- ✓ El acceso a sitios críticos y/o restringidos de la red que pongan en riesgo algún tipo de bien, debe hacerse desde sitios NO públicos, o en su defecto que cuenten con las normas mínimas de seguridad.

- ✓ La navegación debe hacerse recomendablemente por sitios seguros de la red, y si es el caso, que ofrezcan certificados de seguridad y firma digital los cuales por lo general utilizan el protocolo https, de lo contrario se deben extremar medidas de atención frente a la información que va a suministrar, sobre todo en sitio de compras online.

- ✓ Utilizar con mucha precaución los programas y herramientas que permiten compartir software, música y videos, o también conocidos como “Pear to Pear”, ya que pueden abrir compuertas y accesos a nuestro sistema sin que nos demos cuenta, o utilizar técnicas de suplantación de archivos, camuflando algún tipo de mallware, el cual podemos instalar en una máquina.

- ✓ Frente al uso del correo electrónico, no abrir correos de personas desconocidas o hacer caso a sus instrucciones y/o pretensiones, desconfié de mensajes con contenido sospechoso y NO propague o reenvíe este tipo de correos a sus contactos, los cuales contienen información de difusión conocidos como “cadenas” o “hoaxes” que en su estructura ofrecen plegarias, mensajes de solidaridad, premios y concursos, noticias e imágenes impactantes, ya que su objetivo es reunir la mayor cantidad de

información respecto a cuentas y direcciones de correo con fines publicitarios o en su defecto, para difundir algún tipo de mallware o spam.

- ✓ Actualmente las redes sociales han contribuido con el incremento significativo de conductas materializadas en la comisión de delitos. Uno de los escenarios es cuando se utiliza la tecnología como herramienta generar panoramas utilizados como escudo, en donde se exponen, ridiculizan o denigran posiciones o personas creyendo que van en contra del pensamiento clásico, afectando el derecho a la integridad moral, al buen nombre, a la honra, y que materializan en los delitos de injuria o de calumnia, Art. 220 y 221 del C.P.P. Acciones que considerábamos "tan simples" en su ejecución, podrían conllevarnos a una responsabilidad penal.

Hoy en día es muy común encontrar que frente a discusiones de pareja, por desconfianza o celos, uno de ellos decide ingresar sin autorización a uno de los correos electrónicos del otro, sin percatar que estaría incurriendo en un acceso abusivo a un sistema informático, incurriendo en una sanción de 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, según lo consagra el Art. 269A del C.P.P.

Otro de los casos muy comunes es la creación de perfiles falsos en las redes sociales, suplantando a una determinada persona y publicando en él, todo tipo de información personal, como fotografías y videos, conducta que puede ser catalogada como una clara violación de datos personales, según lo establece el Art. 269F.

La regulación del uso y abuso de las redes sociales en Colombia es demasiado deficiente, y una política en materia de cooperación internacional podría ser el elemento fundamental que lograría frenar este tipo de acciones y sucesos, de los cuales su investigación se vuelve cada vez más complicada, debido a que los administradores de dichos portales se encuentran en el exterior, en países donde su aparato judicial difiere del nuestro.

- ✓ Anteriormente se mencionó el uso mesurado de los sitios públicos de acceso a internet, los llamados “café internet” actualmente tienen un deficiente control de acceso, y si bien es cierto la responsabilidad jurídica del mal uso de los recursos recaería sobre el propietario o administrador de dichos sitios, la verdad es otra. Colombia debería adoptar una normatividad frente al control y registro, en el uso de estas herramientas.

- ✓ El tema de los Smartphone está abriendo mucho más las posibilidades de acceder a los diferentes servicios de Internet, y por ende se ha convertido en un medio más para la comisión de delitos, por lo cual, deben fijarse políticas claras frente a la regulación de dichos elementos. Mientras tanto, seguir la regla de oro que de niños nos inculcaban nuestros padres: desconfiar y no recibir regalos de extraños.

No se debe dejar a un lado el tema de las transacciones financieras, las cuales se han concentrado en internet, tras la famosa “Banca Virtual”. Estas entidades se preocupan por brindar elementos de seguridad que blindan por así decirlo los servicios bancarios, sin embargo, el desconocimiento por parte de los usuarios frente al tema, ha causado que este escenario sea uno de los objetivos más buscados por los delincuentes. Las recomendaciones más claras al respecto, se encuentran inmersas en casi la mayoría de políticas de seguridad de las diferentes entidades financieras, entre ellas:

- ✓ Utilizar una clave de acceso a los portales virtuales de manera personal, y que se esté actualizando en determinado tiempo.

- ✓ Activar la segunda clave para el movimiento y transacción electrónica.

- ✓ No compartir estas claves con ninguna otra persona.

- ✓ Registrar las direcciones IP desde donde se van a realizar las transacciones, con el fin de autorizar su uso exclusivo.

- ✓ Activar la opción de aviso por medio de mensajería instantánea al equipo celular, cada vez que se realiza una operación o movimiento bancario.

- ✓ Utilizar sitios seguros frente al acceso del portal en internet, siempre digitar la URL o dirección de la página y no utilizar vínculos que las re direccionen.

- ✓ Nunca aportar datos sobre: número de cuentas, número de tarjetas de crédito, dígitos de verificación, números de documentos de identificación o mucho menos contraseñas a través de sitios Web.

Toda entidad bancaria tiene la tarea de Colaborar oportuna y diligentemente con el Defensor del Consumidor Financiero, las autoridades judiciales y administrativas y los organismos de autorregulación en la recopilación de la información y la obtención de pruebas, en los casos que se requieran, entre otros, los de fraude, hurto o cualquier otra conducta que pueda ser constitutiva de un hecho punible realizada mediante la utilización de tarjetas crédito o débito, la realización de transacciones electrónicas o telefónicas, así como cualquier otra modalidad[66].

La mayor cobertura y acceso a los recursos o fuentes de información, actualmente se encuentran amparados por la ley y el derecho a la privacidad de información, como lo es el caso de la Ley habeas data. Sin embargo, si bien es cierto la política actual frente a la solicitud de esa información debe estar respaldada y amparada por una orden emitida por un Juez de Control de Garantías, se debería analizar los canales de cooperación e incluir los tiempos de respuesta, que se verían reflejados en el acceso oportuno a la información.

En la actualidad no existe un marco legal o política clara frente a los tiempos de almacenamiento de información concerniente a log´s y/o registro por parte de entidades públicas o privadas, quienes garantizan su almacenamiento por un periodo máximo de seis (6) meses en alguno casos, lo cual sumado a la alta

[66]REPUBLICA DE COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1328 DE 2009, DEL REGIMEN DE PROTECCION AL CONSUMIDOR FINANCIERO: Art. 7, Parágrafo [en línea] <http://www.secretariasenado.gov.co/senado/basedoc/ley_1328_2009.html> [citado en 25 de noviembre de 2014]

congestión judicial, implican y materializan dificultades en la obtención y recolección de EMP y/o EF que sustenten una investigación.

Sería interesante generar la necesidad de analizar en profundidad los instrumentos y elementos con que cuenta Colombia en materia de colaboración internacional frente al tema jurídico y penal de delitos informáticos, en esencia permitiría observar las debilidades y alcances en materia investigativa.

Por otro lado, si las políticas del Estado colombiano van encaminadas al aumento de las penas frente a la comisión de los delitos, debería fomentar en el sistema actual de educación parámetros de convivencia en el sistema “virtual”, así como también los mecanismos y medios necesarios para combatir la ciberdelincuencia. Esto se logra, fortaleciendo los canales de cooperación interinstitucional, mejorando e invirtiendo en herramientas, equipos y medios para la investigación.

CONCLUSIONES

El respaldo probatorio de los resultados obtenidos frente al tratamiento de la evidencia digital, está basado no solo en la confirmación o no de una hipótesis delictiva, sino en el tratamiento en sí de la prueba. La implementación del Procedimiento y la Guía propuesta en el presente documento, garantizará el respaldo necesario, y documentará las fases de hallazgo, recolección, embalaje, almacenamiento, análisis y presentación de los resultados, con un soporte metodológico.

Hablando desde el campo de la informática forense, se evidencia que si bien se establece una metodología para el análisis de evidencia digital dentro de una investigación, esta está sujeta a otros factores, entre ellos: la discrecionalidad del investigador frente a su aplicación guiada por el tipo de información que esté buscando, la pericia del analista forense, y la destreza con que el Fiscal coordinador del caso exponga y respalde los resultados ante un tribunal.

Desde un punto de vista del autor, respetando las posiciones de muchos tratadistas frente al tema, infiere que si bien es cierto Colombia cuenta con las herramientas jurídicas que permiten sancionar los delitos informáticos, es claro que existe aún contraposiciones, discusiones e hipótesis dogmáticas, si la normatividad vigente es la adecuada en su aplicación frente a los diferentes escenarios y contextos donde se desarrollan las conductas, aun mas, cuando en la actualidad se está agudizando la utilización de los medios informáticos como herramientas o medios para cometer otro tipo de delitos que ya se encuentran inmersos en la Ley.

La materialización de la norma Técnica de calidad ISO/IEC 27037:2012 es elemento necesario y relevante en el ejercicio de las practicas forenses, no solo a nivel nacional, sino a nivel internacional, lo cual permite hablar el mismo idioma estandarizando las prácticas y los procesos que ofrezcan mayor confiabilidad a los resultados obtenidos, y sobre todo, que exige la mejora continua de las entidades que hacen parte de todo el proceso.

Creemos necesaria la acreditación de los laboratorios de informática forense bajo los estándares internacionales ISO 17025:2005, norma técnica Colombiana NTC-ISO/IEC 17025, la cual establece cerca de 122 cláusulas plausibles de aplicación para la acreditación de laboratorios de ensayo y calibración.

Colombia debería adoptar y generar nuevos espacios de educación frente al tema de los delitos informáticos desde el punto del peritaje, ya que en la actualidad a diferencia de otros países NO existen organismos que garanticen y certifiquen la idoneidad de los analistas forenses en el grado de peritos.

Desde el punto de visa del análisis y la interpretación de la evidencia digital, puede tornarse en un proceso complejo, toda vez que las circunstancias y la subjetividad por parte del equipo de trabajo, puede conllevar a la aplicación de diferentes métodos que redunden en un mayor tiempo de análisis y que a criterio de otros analistas, pueden generar algo de duda en su aplicación. Este factor tan decisivo puede jugar en contra en un proceso de contravención de evidencia a la hora del juicio, que obliga a que los métodos aplicados estén justificados técnicamente y que permitan demostrar de manera científica su elección.

La propuesta presentada sirve como punto de partida frente al análisis de la evidencia digital, ya que involucra en su Procedimiento, cual es el deber ser de su tratamiento, que puede ser adoptado por los diferentes actores que hacen parte del sistema judicial, desde el primer respondiente, la defensa, hasta los señores jueces encargados de tomar las decisiones judiciales.

Es importarte aclarar que la guía no pretende generalizar un único proceso de análisis, plantea una metodología general, ya que habrán escenarios en los cuales por el tipo de información almacenada, su estructura lógica, el tipo de dispositivo físico utilizado, la tecnología, entre otros aspectos, crean la necesidad de ampliar los estudios y desarrollar nuevas y diversas técnicas de tratamiento de la evidencia digital desde el plano de los laboratorios de informática forense.

Estamos totalmente convencidos con la premisa en cual la educación y la socialización de los procesos debe ser un punto de partida para alcanzar y

establecer un sistema de convivencia y respeto de los recursos con que cuenta una organización; sistema que genere un ambiente de trabajo que brinde los recursos necesarios para el desarrollo de las actividades misionales, que involucre directamente el talento humano, el cual finalmente, puede contribuir a que se adopte un sistema de seguridad. Sin embargo, es cierto que una buena parte de esta sociedad desde su formación ética y moral puede en algún momento asumir conductas y actividades que vayan en contra, afectando los procesos internos de la organización, es entonces cuando debe existir un conjunto de normas y/o reglas que regulen y sancionen dichas conductas.

Se hace necesario que el aparato judicial desarrolle una estrategia clara de formación y entrenamiento para comprender el actuar delictivo frente a los medios tecnológicos, que permitirán materializar elementos claros frente a posibles vulnerabilidades de los bienes jurídicos tutelados.

Sin importar que tan severas sean las Leyes existentes sobre los delitos informáticos, debemos analizar, que estas conductas traspasan las fronteras y no todos los países han legislado al respecto y mucho menos se han puesto de acuerdo para aplicar y consolidar una normatividad básica globalizada.

Estamos en la era del “Big-Data”, cada día la humanidad produce cantidades inimaginables de información que años atrás utilizaban periodos de tiempo más largos en generarse. Esta situación genera necesidades que pueden llegar a afectar el manejo de toda esa información, y aún más desde el campo forense, el cual dependerá en su gran mayoría de las capacidades de las instituciones al afrontar este tipo de situaciones.

BIBLIOGRAFÍA

AccessData. FTK Imager User Guide. Utha-USA Revisión [en línea]. 2012. [citado el 10 de octubre de 2014]. Disponible en Internet: <https: //ad-pdf.s3.amazonaws.com/Imager%203_1_4_UG.pdf.>

ACUARIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. Pontificia Universidad Católica del Ecuador. [En línea]. (Sin fecha) [Citado el 15 de octubre de 2014]. Disponible en Internet: <http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

ALAMILLO DOMINGO, Ignacio y otros. Robo de identidad y protección de datos. Primera edición. Cizur Menor Navarra: Aranzadi Thomson Reuters, 2010. 323 p. ISBN 9788499034003.

AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORIS /LABORATORY ACREDITATION BOARD. ASCLD/LAB-International. Program Overview. ADL-OD-VER 3.0 [En línea]. Estados Unidos: 2014. [Citado el 25 de octubre de 2014]. Disponible en Internet: <http: //www.ascld-lab.org/wp-content/uploads/2014/08/AL-PD-3041_Intl_2014_Program_Overview_v3.0.pdf.>

ARBUROLA VALVERDE, Allan. Criminalística: Parte general [en línea] (sin fecha) [citado el 25 de octubre de 2014]. Disponible en Internet: <https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCQQFjAB&url=http%3A%2F%2Fwww.alfonsozambrano.com%2Fdoctrina_penal%2F141009%2Fdp-criminalistica_general.doc&ei=MG0kVZblFcuYgwSJ_oHIBw&usg=AFQjCNEV48SXKeBcjvoXNeNU4FMhXinp2g&sig2=rdJPS2Bh8rdXtgABRjRf4w>

AVELLA FRANCO, Pedro. Estructura del proceso penal acusatorio. Primera edición. Bogotá D.C.: Fiscalía General de la Nación, Diciembre de 2007. 174 p. ISBN 978-958-8374-03-1.

BEDOYA SIERRA, Luis Fernando. La prueba en el proceso penal colombiano. Primera edición. Bogotá D.C.: Fiscalía general de la nación. Diciembre de 2008. 273 p. ISBN 978-958-8374-10-9.

BRENNER, Susan W. La convención sobre Cibercrimen del consejo de Europa. En: Revista Chilena de Derecho y Tecnología. Universidad de Chile. 2012. Vol. 1 No. 1. ISS ISSN 0719-2576.

CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier. Conflictos de Leyes y Conflictos de Jurisdicción en Internet. Primera edición. Madrid: Colex. 2001. 172 p. ISBN: 978-84-7879-636-6.

CALLEGARI, Nidia. Delitos informáticos y legislación. En: Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. No. 70 (julio-agosto-septiembre, 1985). Medellín - Colombia: Universidad Pontificia Bolivariana. 1985. 115 p.

CAMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Reporte Ciberseguridad CCIT y Fedesarrollo: Coyuntura TIC Avances y retos de la defensa digital en Colombia [en línea]. (Noviembre 2014). [Citado el 1 de abril de 2015]. Disponible en Internet: <http://www.ccit.org.co/images/Reporte%20Ciberseguridad%20CCIT%20y%20Fedesarrollo.pdf>

CANO MARTINEZ, Jeimy José. Computación forense. Descubriendo los rastros informáticos. México. Editorial Alfaomega. 2009. 329 p. ISBN: 9789586827676.

CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá D.C.: Ediciones Uniandes, 2010. 348p.

CANO MARTINEZ, JeimyJosé. Unidades de estado sólido. El reto de la computación forense en el mundo de los semiconductores [en línea]. (10 de junio

de 2013) [Citado el 25 de octubre de 2014]. Disponible en Internet: < http://insecurityit.blogspot.com/2013/06/unidades-de-estado-solido-el-reto-de-la.html>.

Caracterización del concepto de evidencia demostrativa y su uso en el juicio oral [en línea]. Bogotá: Universidad Católica de Colombia, ene.-jun. 2012, Vol. 6, no. 1. [Citado el 30 de marzo de 2015]. Disponible en Internet: <http://portalweb.ucatolica.edu.co/easyWeb2/files/105_14819_caracterizacian-del-concepto-de-evidencia-demostrativa.pdf>. ISSN: 1692-6013.

CORTE CONTITUCIONAL. CONSTITUCION POLITICA DE COLOMBIA 1991. Bogotá, Imprenta Nacional de Colombia, 2010. 216p.

CORTE CONSTITUCIONAL DE COLOMBIA, Sentencia C-024/94, Policía judicial-concepto/policía judicial-funciones [en línea]. Bogotá. D.C. 1994. [Citado en 26 de octubre de 2014]. Disponible en Internet: <http://www.corteconstitucional.gov.co/relatoria/1994/c-024-94.htm>

CORTE CONSTITUCIONAL DE COLOMBIA. Sentencia C-536/08 Cosa juzgada constitucional-configuración Cosa juzgada absoluta y cosa juzgada relativa-distinción [en línea]. Bogotá. D.C. 2008. [Citado en 25 de octubre de 2014]. Disponible en Internet: <http://www.corteconstitucional.gov.co/relatoria/2008/C-536-08.htm>.

DÍAZ GARCÍA, Alexander. El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos electrónicos [en línea]. Universidad Santiago de Cali. 2010. [Citado el 2 de mayo de 2014]. Disponible en Internet: <http://www.redipd.org/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICOS_USC.pdf>

ESTADOS UNIDOS DE AMERICA. NATIONAL INSTITUTE OF JUSTICE. Electronic Crime Scene Investigation: A Guide for First Responders [on line]. 2008.

Second Edition. [Cited 2014-08-30], p. 62. Available from Internet: <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf >

ESTADOS UNIDOS DE AMERICA. NATIONAL INSTITUTE OF JUSTICE. Forensic Examination of Digital Evidence: A Guide for Law Enforcement [on line]. 2008. [Cited 2014-08-30], p. 88. Available from Internet: <https: //www.ncjrs.gov/pdffiles1/nij/199408.pdf.>

Equipo de Investigación de ESET Latinoamérica. Tendencias 2014: El desafío de la privacidad en Internet [en línea]. 2014. [citado en 10 de noviembre de 2014]. Disponible en Internet: <http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf>

GUIDANCE SOFTWARE. EnCase USER´S GUIDE. VERSION 7.10 [on line]. 2014. [Cited 2015-09-12] Available from Internet: <http: //download.guidancesoftware.com/4WvA%2BMlPSYGLT7Tga1YWHXUQ4tZmkE8niU4eHr4bKzmzWOG86w4yvz0P6YUEPtdaGJvN72U7KR4%3D.>

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACIÓN. Requisitos generales para la competencia de los laboratorios de ensayo y calibración. Norma Técnica Colombiana NTC ISO/IEC 17025 [en línea]. Noviembre de 2005. [Citado el 20 de noviembre de 2014]. 35 p. Disponible en Internet: <http://www.itp.gob.pe/normatividad/demos/doc/Normas%20Internacionales/Union%20Europea/ISO/ISO17025LaboratorioEnsayo.pdf>

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACIÓN. Documentación. Presentación de Tesis, Trabajos de grado y otros trabajos de investigación. NTC/1486. Sexta actualización. Bogotá D.C.: El instituto, 2008. 37 p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACIÓN. Citas y notas de pie de página. NTC/1487. Segunda actualización. Bogotá D.C.: El instituto, 1995. 7 p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACIÓN. Referencias documentales para fuentes de información electrónicas. NTC/4490. Bogotá D.C.: El instituto, 1998. 23 p.

GARZÓN TAPIA, Pamela Nataly y VIZUETE GALLARDO, Marco Fernando. El fraude Informático: Valoraciones técnico jurídicas. Tesis de grado Abogado De Los Tribunales y Juzgados de La República. La Tacunga Ecuador. Universidad Técnica del Cotopaxi, Unidad Académica de Ciencias Administrativas y Humanísticas. 2009. 59 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO. ISO/IEC 27037:2012. ISO. ISO/IEC 27037:2012. 1 ed. Geneve, Suiza: ISO, 2012. 38 p.

INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE. Guidelines for Best Practice in the Forensic Examination of Digital Technology. ENFSI Forensic IT Working Group. Forensic Science Service. Version 6, United Kingdom. 2009. 30 p.

La oportunidad criminal en el ciberespacio. En: Revista Electrónica de Ciencia Penal y Criminología. [En línea] Barcelona – España, Julio de 2011 [citado el 15 de octubre de 2014]. Disponible en Internet: < http://criminet.ugr.es/recpc/13/recpc13-07.pdf>. ISSN 1695-0194.

LÓPEZ, Oscar, AMAYA. Haver, LEÓN Ricardo, ACOSTA Beatriz. Informática Forense: Generalidades, aspectos técnicos y herramientas. Universidad de los Andes [en línea]. Bogotá. 2002. [citado el 20 de octubre de 2014]. Disponible en Internet: <http://www.criptored.upm.es/guiateoria/gt_m180b.htm>

LOURIDO RICO, Ana María. La Asistencia Judicial Penal en la Unión Europea. Primera edición. Valencia – España: Tirant lo Blanch. 2004. ISBN: 84-8442-931-8

MIFSUD ELVIRA. Monográfico: Introducción a la seguridad informática [en línea]. 2012. [citado el 25 de marzo de 2015]. Disponible en Internet: <http://datateca.unad.edu.co/contenidos/233001/Material/Unidad%20I/Proteccion_seguridad_infomatica.pdf>

MORRIS, Jamie. Forensics on the Windows Platform. Symantec [on line]. United States. 27 Jan. 2003. [Citado el 25 de noviembre de 2015] Disponible en Internet: <http://www.symantec.com/connect/articles/forensics-windows-platform-part-one>

MUÑOZ CERÓN, Estefanía. Proyecto para el mejoramiento del laboratorio del grupo investigativo de delitos informáticos del Cuerpo Técnico de Investigación "CTI" Pasto. Tesis de grado Ingeniería Electrónica. San Juan de Pasto. Universidad de Nariño, Facultad de Ingeniería Electrónica. 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Forensics web services [on line]. Gaithersburg. 2010. [Cited on 2014-10-20]. Available from Internet: <http://csrc.nist.gov/publications/nistir/ir7559/nistir-7559_forensics-web-services.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guidelines on cell phone forensics [on line]. Gaithersburg. 2007. [Cited on 2014-10-20]. Available from Internet: <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Definition of Cloud Computing [on line]. Gaithersburg. 2011. [Cited on 2014-10-20]. Available from Internet: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

NOBLETT, Michael. Recovering and Examining Computer Forensic Evidence. Citado por: ZUCCADI, Giovanni. Y GUTIÉRREZ, Juan. Informática forense [en línea]. [Citado en octubre 25 de 2014] Disponible en Internet: <http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf >

PIETRO BOGOTÁ, Diana y MORENO PEÑA Claudia. Evidencia Digital en Colombia: Una reflexión en la práctica [en línea] .Bogotá. D.C. 2007. [Citado el 30 de marzo de 2015]. Disponible en Internet: <http://www.cej.org.co/index.php/component/search/?searchword=Evidencia%20Digital%20en&searchphrase=all&Itemid=453>

PORTAFOLIO.COM. Colombia, principal fuente de ciberataques en Latinoamérica [en línea]. (Octubre 17 de 2014). [Citado el 5 de abril de 2015]. Disponible en Internet: <http://www.portafolio.co/negocios/ataques-ciberneticos-colombia>

REBOLLEDO PEDRUELO, Miguel. Dispositivos de almacenamiento. Universidad Politécnica de Valencia [en línea]. Valencia – España. [Citado el 25 de abril de 2015]. Disponible en Internet: <http://riunet.upv.es/bitstream/handle/10251/13706/Dispositivos_de_almacenamiento.pdf?sequence=1>

REPUBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31 de agosto de 2004). Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004). Diario Oficial. Bogotá D.C. 2004. no. 45658.

REPUBLICA DE COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266 (31 de Diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario oficial. Bogotá D.C., 2008. p. 1- 17.

REPUBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009 (5 de enero de 2009). Por medio de la cual se modifica el código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C. 2009. no. 47223

REPUBLICA DE COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1328 DE 2009, DEL REGIMEN DE PROTECCION AL CONSUMIDOR FINANCIERO: Art. 7, Parágrafo [en línea]. Bogotá. D.C., Diario Oficial No. 47.411, Julio de 209. [Citado en 25 de noviembre de 2014]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1328_2009.html>

REPUBLICA DE COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 DE 1999por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [En línea] Bogotá D.C. Diario oficial No. 43.673., agosto de 1999. [Citado el 26 de noviembre de 2014]. Disponible en Internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276>

REPUBLICA DE COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-1194/05. SISTEMA PENAL ACUSATORIO-Etapas, INVESTIGACION PENAL-Concepto, procedimiento penal acusatorio-descripción, procedimiento penal acusatorio-fase de indagación, procedimiento penal acusatorio-formulación de la imputación, procedimiento penal acusatorio-condición de imputado, derecho de defensa en investigación penal-ejercicio desde antes de la imputación, procedimiento penal acusatorio-presentación de la acusación, material probatorio en investigación penal-Solo se convierte en prueba desde que juez de conocimiento lo decreta [En línea]. Bogotá D.C.: 2005. [Citado el 25 de Marzo de 2015]. Disponible en: <http://www.corteconstitucional.gov.co/relatoria/2005/C-1194-05.htm>

REPUBLICA DE COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Documento Conpes 2011 [en línea]. [Citado el 4 de noviembre de 2014]. Disponible en Internet: <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>

REPUBLICA DE COLOMBIA. CORTE SUPREMA DE JUSTICIA. Sala de Casación Penal. Auto del 15 de octubre de 2008. Diario Oficial. Bogotá D.C., 2008. No. 29.626. 95 p.

REPÚBLICA DE COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701 Lineamientos de Política para Ciberseguridad y

Ciberdefensa [en línea]. Bogotá. D.C. 14 de julio de 2011. [Citado el 20 de noviembre de 2014] Disponible en Internet: <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>

REPUBLICA DE COLOMBIA. DIRECCION NACIONAL DEL CUERPO TECNICO DE INVESTIGACIÓN (CTI). Resolución 010. 2008.

REPUBLICA DE COLOMBIA. DIRECCION DE INVESTIGACION CRIMINAL E INTERPOL. Boletín informativo de cibercrimen [En línea]. Bogotá. D.C. mayo 2015. [Citado el 2 de abril de 2015]. Disponible en Internet: <http://www.ccp.gov.co/sites/default/files/boletin_cibercrimen_002.pdf>

REPÚBLICA DE COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Manual de Procedimientos del Sistema de Cadena de Custodia [en línea]. Bogotá. D.C. (mayo de 2014). [Citado el 2 de abril de 2015]. Disponible en Internet:<http: //www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634.>

REPÚBLICA DE COLOMBIA, Fiscalía General de la Nación. Manual de procedimientos de la Fiscalía en el sistema penal acusatorio [en línea]. Bogotá. D.C, 2006). [Citado el 10 de octubre de 2014]. Disponible en Internet: < http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/03/spoa.pdf>. ISBN 958-97542-5-2

REPUBLICA DE COLOMBIA. FISCALIA GENERAL DE LA NACION. Policía Judicial. En: Informativo Interno Huellas. Diciembre 2003. No. 46. ISSN 1657 – 6829.

REPUBLICA DE COLOMBIA. FISCALIA GENERAL DE LA NACION. Resolución No. 0-2869. 2003 [en línea]. [Citado el 31 de octubre de 2014] Disponible en Internet:
<http://www.medellin.gov.co/transito/archivos/normatividad/resoluciones_nacionales/2003/2003-resolucion2869.pdf>

REPUBLICA DE COLOMBIA. MINISTERIO DE MINAS Y ENERGÍA. Resolución 9 0708 (25 OCTUBRE DE 2013). Mediante la cual se expide el nuevo Reglamento Técnico de Instalaciones Eléctricas RETIE. Bogotá D.C.: El ministerio, 2013. 5 p.

REPUBLICA DE COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Boletín trimestral de las TIC: Cifras cuarto trimestre de 2014 [en línea]. Bogotá. D.C. Marzo 2005. [Citado en 10 de abril de 2015]. Disponible en Internet: <http://colombiatic.mintic.gov.co/602/articles-8598_archivo_pdf.pdf>

REPUBLICA DE COLOMBIA. POLICIA NACIONAL, Resolución No. 02057 DEL 15 JUN. 2007 [en línea]. Bogotá D.C. [citado en 26 de octubre de 2014]. Disponible en Internet: <http://www.policia.gov.co/portal/page/portal/INSTITUCION/normatividad/resoluciones>

RODRÍGUEZ BERNAL, Antonio Pedro. Los cibercrímenes en el espacio de libertad, seguridad y justicia. En: Revista de Derecho Informático [en línea] Málaga España: Alfa Redi, 2006. [Citado el 20 de octubre de 2014]. Disponible en Internet: <http://www.alfa-redi.org/sites/default/files/articles/files/rodriguez.pdf>

RODRIGUEZ, L. Acerca de la investigación bibliográfica y documental [en línea]. (19 de agosto de 2013). [Citado en 30 de noviembre de 2014]. Disponible en Internet: <https://guiadetesis.wordpress.com/2013/08/19/acerca-de-la-investigacion-bibliografica-y-documental/>

ROMEO CASABONA, Carlos María: El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales. Primera edición. Albolote – España: Editorial Comares, 2006. 348 p. ISBN: 8498360943 ISBN-13: 9788498360943.

SANTOS JAIMES, Luz Marina y FLÓREZ FUENTES, Anderson Smith. Metodología para el análisis forense en Linux. En: Revista Colombiana de

Tecnología avanzada. Universidad de Pamplona. 2012. Volumen2 – Número 20. ISSN: 16-7257.

SUÁREZ SÁNCHEZ, Alberto. La estafa informática [en línea]. (Sin fecha). [Citado el 9 octubre de 2014]. Disponible en Internet: <dialnet.unirioja.es/descarga/articulo/3308847.pdf>

SYMANTEC. Tendencias de seguridad cibernética en américa latina y el caribe [en línea]. (Junio de 2014). [Citado en 5 de abril de 2014]. Disponible en Internet: <http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf>

SYMANTEC. Reporte Norton 2013. [En línea]. (Octubre 2013). [Citado en 20 de noviembre de 2014] Disponible en Internet: <http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf>

SHEETZ, Michael. Computer Forensics: An Essential Guide for Accountants. Miami - United States: Lawyers, and Managers, 2007. ISBN: 978-0-471-78932-1

TABLEU: Productos Tableau [en línea]. (Sin Fecha). [Citado el 25 de noviembre de 2014]. Disponible en Internet: <https://www.guidancesoftware.com/products/Pages/tableau/overview.aspx>

UNIVERSIDAD CATÓLICA DE COLOMBIA. Caracterización del concepto de evidencia demostrativa y su uso en el juicio oral [en línea]. Bogotá. D.C., Vol. 6, No.1, enero – junio 2012. [Citado el 30 de marzo de 2015] <http://portalweb.ucatolica.edu.co/easyWeb2/files/105_14819_caracterizacian-del-concepto-de-evidencia-demostrativa.pdf>. ISSN: 1692-6013

UNIVERSIDAD POLITÉCNICA DE VALENCIA. Dispositivos de almacenamiento [en línea]. Valencia – España. (Sin fecha). [Citado en 14 de octubre de 2014].

Disponible en Internet: <http://riunet.upv.es/bitstream/handle/10251/13706/Dispositivos_de_almacenamiento.pdf?sequence=1>

UMAÑA RAMÍREZ, Guillermo y MOSQUERA NAVARRETE, Isabel Cristina. Diseño e implementación de un centro de informática forense en la Universidad Autónoma de Occidente. Tesis de grado Ingeniero Informático. Santiago de Cali. Universidad Autónoma de Occidente, Facultad De Ingeniería. 2014. 132p.

VIEGA RODRÍGUEZ, María. Un nuevo desafío jurídico: los delitos informáticos., Fundación de Cultura Universitaria [en línea]. Montevideo: 2001. [Citado el 10 de octubre de 2014]. Disponible en Internet: <http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf>

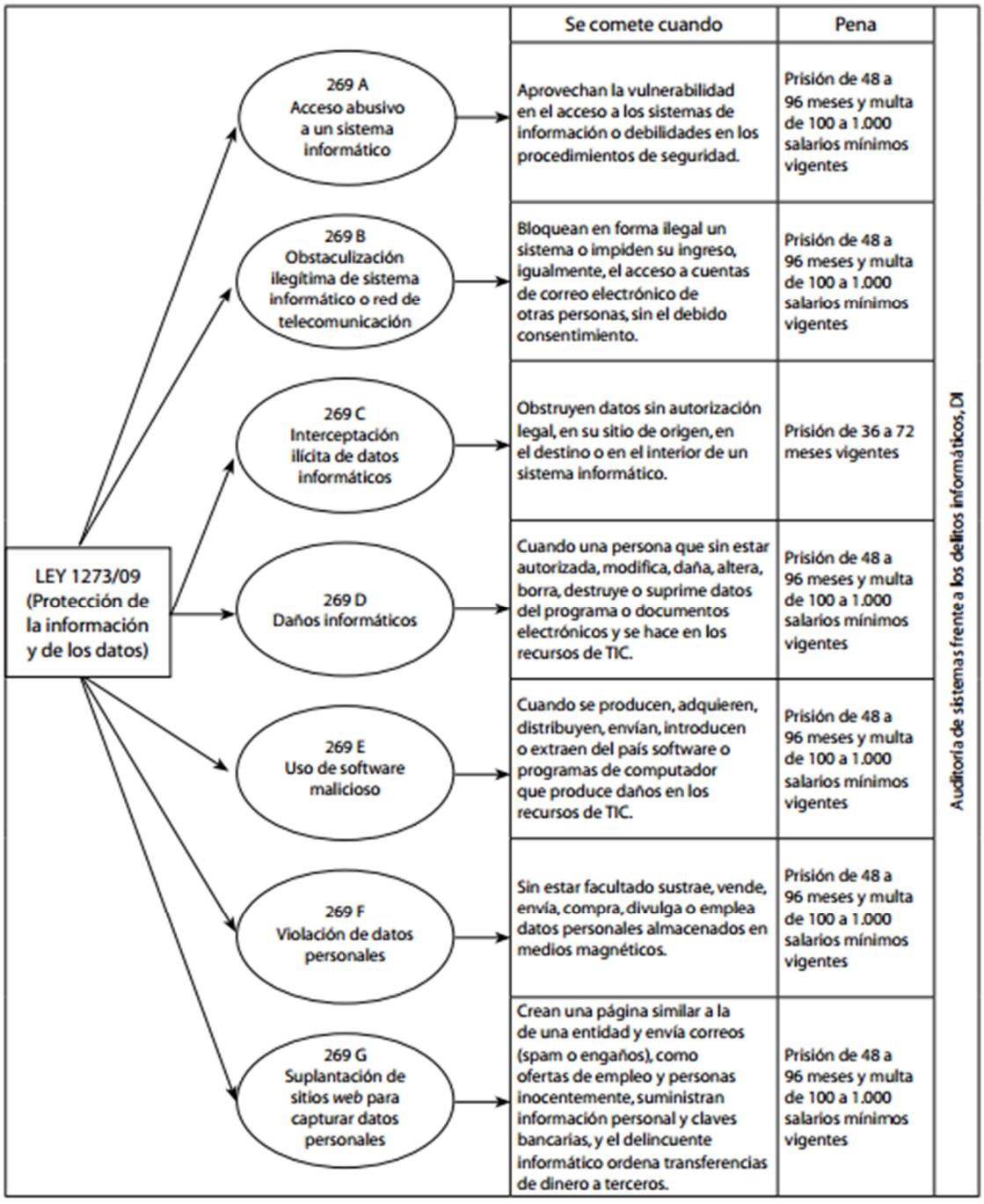
VILLACÍS RUIZ, Viviana Marcela. Auditoria Forense. Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial. Tesis de grado Auditor en Control de Gestión. Guayaquil – Ecuador: Escuela Superior Politécnica Del Litoral. 2006. 135 p.

WIRZENIUS, Lars, OJA, Joanna y STAFFORD, Stephen. Guía Para Administradores de Sistemas GNU/Linux: Utilizando Discos y Otros Medios de Almacenamiento. En ibiblio.org: [En línea]. (Sin fecha). [Citado el 30 de marzo de 2015]. Disponible en Internet: <http://www.ibiblio.org/pub/linux/docs/LDP/system-admin-guide/translations/es/html/index.html>.

ZUCCADI, Giovanni. Y GUTIÉRREZ, Juan. Informática forense [en línea]. (Sin fecha). [Citado en octubre 25 de 2014]. Disponible en Internet: <http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf>

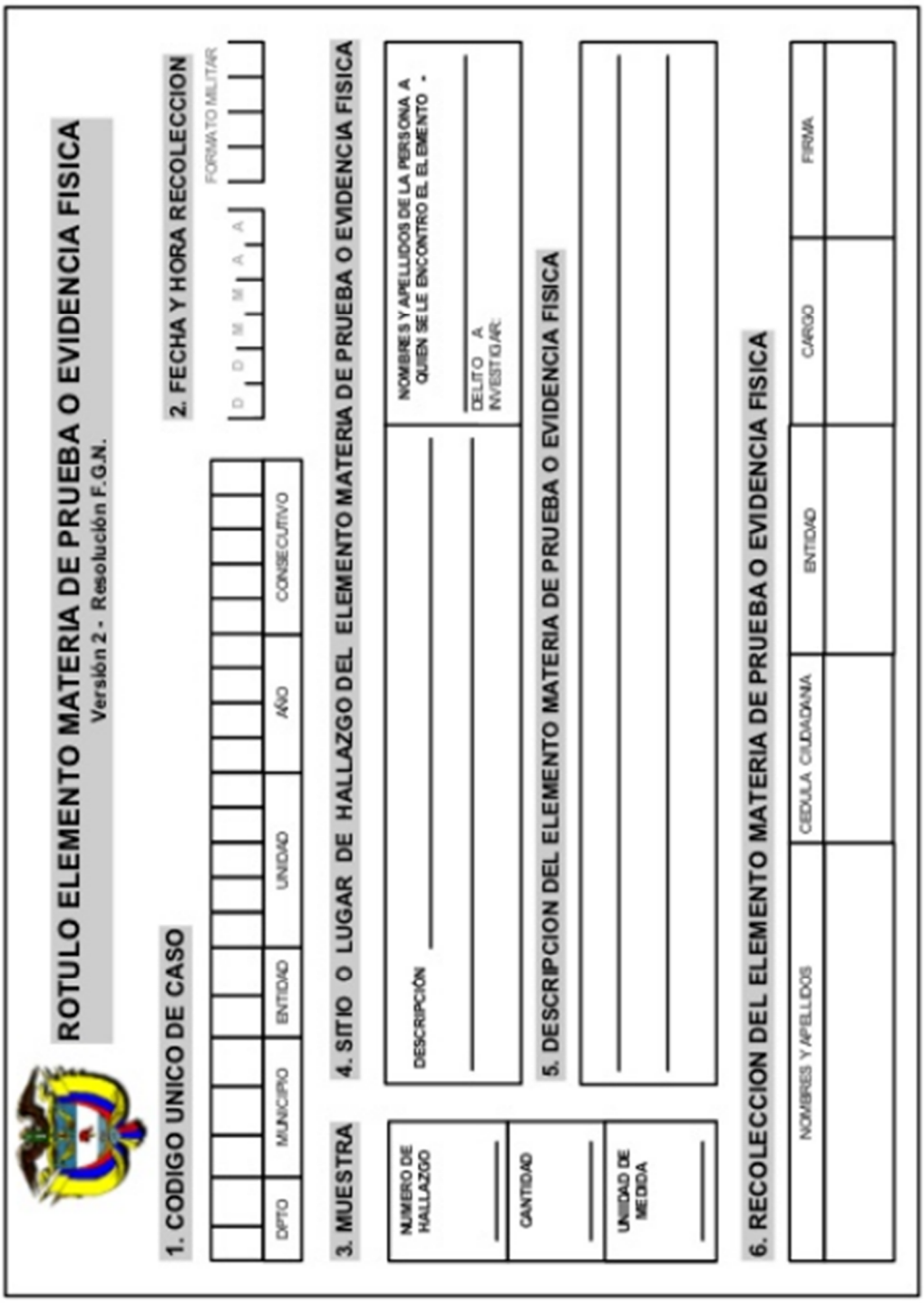
ANEXOS

Anexo A Ley 1273 “De la protección de la información y de los datos”



Fuente: Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.

Anexo B Formato Rotulo Cadena de Custodia



ROTULO ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

Versión 2 - Resolución F.G.N.

1. CODIGO UNICO DE CASO

DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO

2. FECHA Y HORA RECOLECCION

FORMATO MILITAR

D D M M A A

3. MUESTRA

NUMERO DE HALLAZGO

CANTIDAD

UNIDAD DE MEDIDA

4. SITIO O LUGAR DE HALLAZGO DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

DESCRIPCIÓN

NOMBRES Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRO EL ELEMENTO -

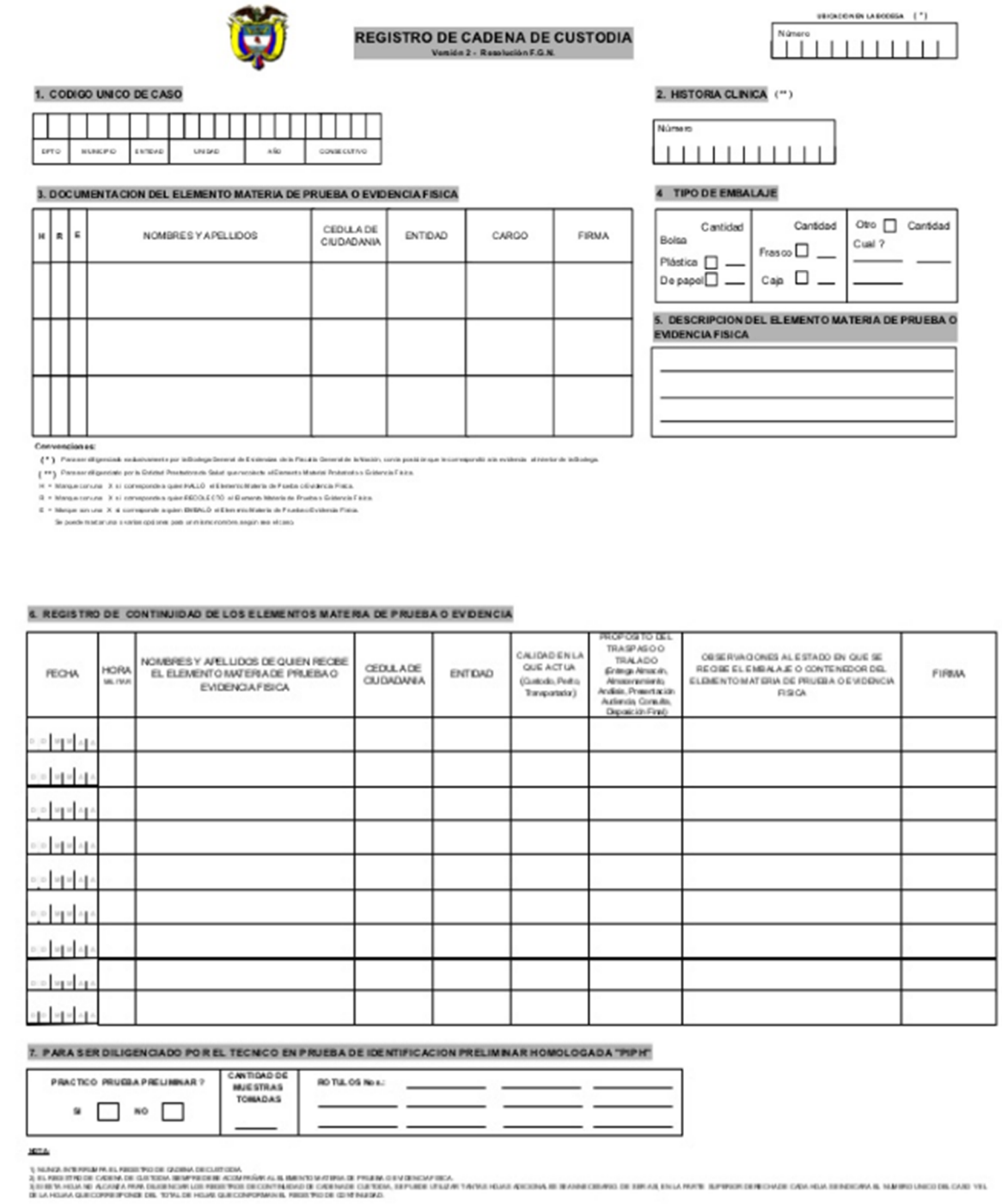
DELITO A INVESTIGAR:

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

6. RECOLECCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

NOMBRES Y APELLIDOS | CEDULA CIUDADANIA | ENTIDAD | CARGO | FIRMA

Anexo C Formato registro de Continuidad 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 Plástica ☐ ___ De papel ☐ ___	Frasco ☐ ___ Caja ☐ ___	Cual ? _____ _____ _____

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

Convenciones:

(*) Persona diligenciada exclusivamente por la Bodega General de Evidencias de la Fiscalía General de la Nación, cuando posteriormente sea entregada al interior de la bodega.

(**) Persona diligenciada por la Entidad Prestadora de Salud que recolecta el Elemento Material Probatorio o Evidencia Física.

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

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

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

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

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

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

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

PRACTICO PRUEBA PRELIMINAR ?	CANTIDAD DE MUESTRAS TOMADAS	ROTULOS No.s:
SI ☐ NO ☐	_____	_____ _____ _____ _____ _____ _____ _____ _____ _____

NOTA

1) NUNCA INTERRUMPA EL REGISTRO DE CADENA DE CUSTODIA.

2) EL REGISTRO DE CADENA DE CUSTODIA SIEMPRE DEBE ACOMPAÑAR AL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA.

3) SI EL NUMERO DE HOJAS NO ALCANZA PARA DILIGENCIAR LOS REGISTROS DE CONTINUIDAD DE CADENA DE CUSTODIA, SE PUEDE UTILIZAR TANTAS HOJAS ADICIONALES SE REQUIERAN PERO DE ESTAS EN LA PARTE SUPERIOR DERECHA DE CADA HOJA SE INDICARA EL NUMERO UNICO DEL CASO Y EL DE LA HOJA QUE CORRESPONDE DEL TOTAL DE HOJAS QUE COMPONEN EL REGISTRO DE CONTINUIDAD.