PROCESOS DE INFORMÁTICA FORENSE Y MARCO LEGAL COLOMBIANO

Gamboa Peña, Diego Alejandro
diego.a.gamboa.p@gmail.com
Universidad Piloto de Colombia
Bogotá, Colombia

Resumen—Los riesgos en seguridad de la información, cada año aumentan de manera exponencial, las empresas cada vez son mas conscientes de éste fenómeno y la gran mayoría se concentran en mitigar, transferir o aceptar el riesgo, algunas de ellas se encuentran en un mayor nivel de madurez en seguridad e implementan modelos de respuesta a incidentes que incluyen planes de continuidad de negocio y DRP (Disaster Recovery Plan), pero muy pocas, dentro de sus grupos de respuesta a incidentes, están capacitadas para llevar un proceso válido de recolección de evidencia digital. Para realizar un procedimiento de este tipo, es necesario tener en cuenta los principios de la ciencia forense, recolección de evidencia digital y cadena de custodia, además de un profundo conocimiento del marco legal del país en donde opera la compañía. En el presente documento, se presentan los diferentes conceptos que se deben tener en cuenta para el levantamiento de un proceso de recolección de evidencia digital y el marco legal de la República de Colombia, país en donde se desarrolló la investigación.

Abstract—The risks in information security increase exponentially every year, companies are increasingly aware of this phenomenon and the vast majority of them are focused on mitigating, transferring or accepting risk, some of them are at a higher level of maturity in security and implementation of incident response models that include business continuity plans and DRP (Disaster Recovery Plan), but very few within their incident response groups are trained to carry out a valid evidence collection process digital, to carry out a procedure of this type it is necessary to take into account the principles of forensic science, digital evidence collection and chain of custody, knowledge of the legal framework of the country where the company operates. In this document we present the different concepts that must be taken into account for the lifting of a digital evidence collection process and the legal framework of the Republic of Colombia, the country where the research is conducted.

Índice de términos—Informática forense, evidencia digital, cadena de custodia, marco Legal.

I. INTRODUCCIÓN

El análisis forense responde a una serie de técnicas específicas y muy bien definidas según procedimientos internacionales, con la finalidad de utilizar sus resultados, no solo en un proceso legal, sino como fuente de una mejora continua en los procesos de seguridad de la información. En el campo forense existen cuatro etapas, perfectamente definidas en las cuales se profundizará más adelante y consiste en identificar, adquirir, analizar y presentar los resultados de la investigación.

Teniendo en cuenta lo anterior, la seguridad de la información es una de las áreas de mayor crecimiento en el mundo tecnológico. Las amenazas son cada vez mayores y se hace necesario aprender de los ataques sufridos. Una de las cifras más alarmantes fue presentada por Kaspersky durante el 2017 (Ver Figura 1), en la cual mencionan que el 68 % [9] de las compañías Latinoaméricanas fueron víctimas de algún tipo de ataque informático. Lo preocupante de ésta situación, es que la mayoría de compañías realizan un proceso de gestión de incidentes mediante el cual restauran sus sistemas, pero no investigan la fuente real de la amenaza y probablemente continúan vulnerables a un nuevo ataque.

Es por esto que los procesos de gestión de incidentes en las compañías son necesarios, tanto para garantizar su productividad, como para el continuo mejoramiento de la seguridad de las diferentes plataformas.

En el caso de las empresas, los procesos de

informática forense ameritan estar mejor documentados. Es de primordial importancia que una compañía esté preparada tecnológicamente y su personal esté cualificado para realizar estos procesos en caso de ser necesario.

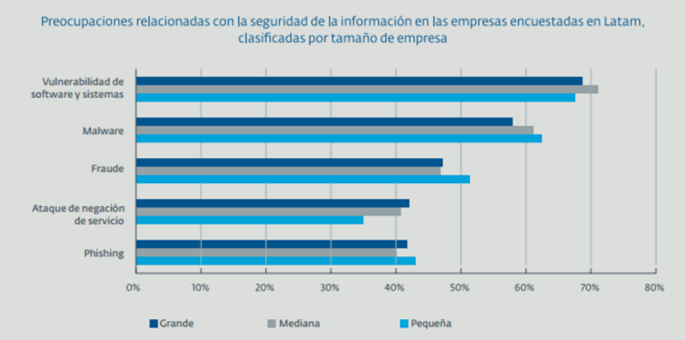

Figura 1. Preocupación de las empresas en seguridad de la información, ESET Security Report Latinoamerica 2017. [9]

Un proceso forense debe incluir todas las fases indispensables para culminar exitosamente la investigación de la ocurrencia de un evento. Existen diversas entidades a nivel mundial, tanto publicas como privadas, que han publicado múltiples estándares para la construcción de éste proceso. La correcta construcción de estos procesos llevan a las empresas, no solo a establecer responsables de las situaciones que se presenten; también a mejorar continuamente la infraestructura informática.

En el siguiente documento se hace un recorrido sobre la historia de las ciencias forenses y los axiomas existentes alrededor de ellas. La informática forense y su definición realizada por el Bureau federal de investigaciones FBI, los conceptos de cadena de custodia y evidencia digital, el marco legal colombiano y los diferentes documentos generados por la Fiscalía General de la Nación y el Ministerio de Tecnologías de Información y Comunicaciones de Colombia.

II. CIENCIA FORENSE

La ciencia forense nace en la antigua Roma, época en la cual se tenían que reunir tanto acusado como acusador y argumentar las pruebas en contra o a favor del encausado. De allí la palabra forense, que viene del latin Forum.

La ciencia forense se utiliza en procedimientos como:

- Recolección y análisis de rastros humanos.
- Recuperación de la información.

La principal labor de un investigador forense es perseguir la verdad, esto solo es posible mediante el método científico, claramente descrito en normas y procedimientos aceptados internacionalmente para, de esta manera, construir una hipótesis de lo ocurrido, apoyado por la evidencia encontrada. A pesar de que el presente documento trata de ciencias forenses en la informática, aplican los mismos principios de las ciencias forenses dentro de las cuales estan: Crimonologia, Entomologia, Antropologia, Toxicologia, Psicologia, Psiquiatria, Generica Biologica, Medicina Legal, Odontologia, Balistica.

A. *Principio de intercambio de Loccard*

El científico Edmond Loccard (Figura 2) estudió las ciencias forenses durante su vida y creía que toda persona que interactuaba con un objeto u otra persona, dejaba evidencia de esta acción e igualmente se llevaba consigo evidencia de que estuvieron en contacto con este objeto o persona [10].

“Toute action de l’homme, et a fortiori, l’action violente qu’est un crime, ne peut pas se dérouler sans laisser quelque marque”.

“Cualquier acción de un individuo, y obviamente la acción violenta que constituye un crimen, no puede ocurrir sin dejar rastros”.

III. INFORMÁTICA FORENSE

La ciencia forense informática nace como la necesidad de aplicación de la ley soportada en evidencia electrónica, esta disciplina junto al ADN son los dos medios científicos sobre los cuales más se han soportado procedimientos judiciales en los últimos años.

Figura 2. Edmond Loccard, (1877-1966), Crime Museum. [14]

Desde 1995, se observa una tendencia a construir laboratorios forenses en las diferentes entidades de control, una encuesta que realizó el servicio secreto de los Estados Unidos, indicó que el 48 % [11] de las agencias contaba con laboratorios forenses y el 68 % [11] de los organismos públicos envían materiales probatorios a laboratorios certificados.

Como resultado de este fenómeno el FBI convocó a la conferencia internacional de ciencias forenses, que se realizó en 1995, en Maryland, en 1996, en Australia y, en 1997, en Holanda. Lo anterior conllevo, a la creación de la organización internacional de evidencia informática y el grupo científico sobre evidencia digital SWGDE.

Una de las autoridades más importantes en las ciencias de informática forense, como se mencionó anteriormente, es el Bureau Federal de Investigaciones FBI que define la informática forense como: "La ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional". [11]

Mas, sin embargo, ésta no es la única definición. Civie and Civien en 1998 la enuncia como:

"La búsqueda de conocimiento mediante el descubrimiento de pruebas elementales extraídas de una computadora de una manera adecuada para los procedimientos judiciales. El término 'elemental' implica operaciones en un nivel fundamental; como los elementos microscópicos del medio o los bits y bytes de un sector individual. El término 'descubrir' se refiere a la presentación de algún aspecto de la evidencia no disponible a través de la observación simple". [15]

Farmer y Venema (1999) precisó:

"Recopilación y análisis de datos de una manera tan libre de distorsiones o sesgos como sea posible para reconstruir datos o lo que sucedió en el pasado en un sistema". [15]

Desde 1984, el FBI viene perfeccionando las técnicas de recolección y análisis de evidencia forense, encontrando definiciones para varios tipo de evidencia, así:

- Computación Forense: procura descubrir la verdad de los hechos, apoyándose en medios científicos y análisis en equipos o tecnologías relacionadas con la computación.
- Forensia en redes: Implica un análisis de alta complejidad y conocimiento profundo en el funcionamiento de protocolos de red, de esta forma seguir un rastro de actuación en las redes de computadores, manteniendo todos los protocolos de recaudación y análisis de evidencia.
- Forensia Digital: son métodos, conceptos, estrategias y procedimientos usados en criminalística tradicional con la finalidad de apoyar los mecanismos de justicia y luchar contra delincuentes que utilizan los medios informáticos para realizar sus crímenes.

La informática forense tiene tres objetivos fundamentales:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.

- La creación y aplicación de medidas para prevenir casos similares.

IV. EVIDENCIA DIGITAL

"Cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor". [12]

No	Framework	Ph
1	Computer Forensic Process (M.Pollitt, 1995)	4
2	Generic Investigative Process (Palmer, 2001)	7
3	Abstract Model of the Digital Forensic Procedure (Reith, Carr, Gunsch, 2002)	9
4	An Integrated Digital Investigation Process (Carrier Spafford, 2003)	17
5	End-to-End Digital Investigation (Stephenson, 2003)	9
6	Enhance Integrated Digital Investigation Process (Baryamureeba Tushabe, 2004)	21
7	Extended Model of Cybercrime Investigations (Ciardhuain, 2004)	13
8	Hierarchical, Objective-based Framework (Beebe, Clark, 2004)	6
9	Event-based Digital Forensic Investigation Framework (Carrier, Spafford, 2004)	16
10	Forensic Process (Kent K. , Chevalier, Grance, Dang, 2006)	4
11	Investigation Framework (Kohn, Eloff, Oliver, 2006)	3
12	Computer Forensics Field Triage Process Model (K.Rogers, Goldman, Mislan, Wedge, Debrota, 2006)	4
13	Investigative Process Model (Freiling, Schwittay, 2007)	4

Tabla 1. Número de fases por framework propuesto. Columna 1: Numeración de marco de trabajo. Columna 2: Nombre del marco de trabajo. Columna 3: Número de fases propuestas por el marco de trabajo. [16]

La evidencia digital representa desafíos para los investigadores, que distan de la evidencia física. La evidencia digital es susceptible de modificación, alteración o eliminación; adicionalmente, es particularmente susceptible de copiado. De aquí el interés por parte de los investigadores forenses en demostrar la integridad de la información con los respectivos originales. Técnicas como la generación de hashes o checksum, han sido las metodologías más usadas para este fin, así mismo, se han diseñado gran variedad de marcos de trabajo y procedimientos de tratamiento digital que podemos ver en la Tabla 1.

En éste documento se hará énfasis en cinco fases que se consideran las mas importantes del proceso forense, las cuales son: preparación, recolección, conservación, análisis y presentación. Según conclusiones de Siti, Robiah, Shahrin [16] el estudio de los diferentes frameworks arroja una serie de pasos redundantes expresados en diferentes terminologías. En su framework proponen un estándar llamado DFIF que hace especial énfasis en los pasos propuestos y que presentamos a continuación.

Valga aclarar que el Ministerio de las Tecnologías de Información y Comunicaciones, recomienda cinco fases que son las expuestas en la Figura 3.

Figura 3. Diagrama de proceso de evidencia digital, Ministerio de Tecnologías de Información de Colombia. [13]

A. Preparación

La preparación de un proceso forense, comprende los procesos que se deben realizar previamente a la ejecución de la recolección de evidencia, dentro de la fase de preparación se debe incluir:

- Garantizar obtener todas las autorizaciones pertinentes y el soporte administrativo. Esto incluye procesos legales, de recursos humanos o de la misma persona a investigar. Así mismo se debe contar con la autorización expresa para realizar la investigación.
- Asegurar que se cuenta con todos los recursos, tanto de conocimiento como tecnológicos, que garanticen el soporte de la investigación, por ejemplo, en caso de la extracción de una imagen forense, se debe garantizar, como mínimo, tener un bloqueador de escritura y el software adecuado para realizar la imagen forense.
- Disponer de un método o mecanismo para garantizar que el incidente ha sido confirmado.
- Garantizar que la alta gerencia y la empresa tiene conciencia de la necesidad de realizar una investigación. La investigación forense conlleva costos implícitos, tanto en recursos humanos como tecnológicos y, se debe garantizar que las empresas son conscientes de ello.
- Tener un plan claro que la información es necesario dentro de la organización y fuera de ella.
- Identificar la estrategia de investigación, las políticas de la compañía y si hay investigaciones previas, tenerlas disponibles para consultas.
- Informar a todas las partes involucradas en la investigación que la misma se está ejecutando.

B. Recolección de evidencia digital

Los principios de recolección de evidencia, para que sea aceptada en un proceso legal, son tres principalmente: que auténtica, confiable y suficiente.

- Autenticidad: garantizar que la evidencia sea fiel reflejo del original.
- Confiabilidad: los registros proceden de fuentes que son creíbles y sobre todo verificables.
- Suficiencia: debe contar con mecanismos que proporcionen integridad, sincronización y centralización.

El proceso de recolección de información consta de tres fases según el Ministerio de Tecnologías de Información y Comunicaciones. Figura 3. [13]

C. Planificación de adquisición de datos.

Durante el proceso de planificación se debe tener en cuenta: orden de extracción, herramientas necesarias, conocimiento del profesional y volatilidad. En esta fase es posible tomar decisiones, como por ejemplo, la necesidad de una consultoría externa para realizar el proceso por falta de conocimiento del dispositivo a analizar.

- Adquisición de los datos: El proceso de adquisición de datos puede realizarse tanto en sitio como de manera remota, utilizando herramientas forenses que garanticen la integridad de la información.
- Verificación de integridad de los datos recolectados: Este procedimiento se realiza para garantizar la integridad de los datos, se utiliza mediante cálculos matemáticos que garanticen que la información no ha sido modificada. Ejemplos de estos procedimientos son el cálculo de MD5, SHA1, SHA256.

D. Conservación

La conservación de la evidencia digital es primordial, como lo hemos enunciado anteriormente. Todos los procedimientos deben ser repetibles y para esto se deben mantener las evidencias de manera idónea. Las personas que participan de todo o parte del proceso forense,

deben estar en capacidad de demostrar que la evidencia no fue modificada en ninguna fase del procedimiento.

E. Análisis

En este paso se analiza la información adquirida, existe software especializado para realizar búsquedas en cadenas de caracteres, minería de datos, búsqueda de archivos, claves, correos electrónicos, etc. Es muy importante tener en cuenta que una de las mejores formas de agilizar este proceso, es saber qué se está buscando o tener una idea clara del objetivo, es por eso que el estudio del entorno, la motivación del delito y los objetivos del presunto delincuente, son fundamentales para adelantarlo exitosamente.

F. Presentación

La presentación de evidencia regularmente se hace con formatos establecidos de acuerdo al entorno, debe ser detallada, descriptiva, de manera pericial y con una correcta interpretación de la fase de análisis, minimizando los tecnicismos.

V. DESCRIPCIÓN TÉCNICA DE RECOLECCIÓN DE IMAGEN FORENSE Y DATOS VOLÁTILES

Para los procesos técnicos de recolección de evidencia digital existen variadas técnicas e infinidad de procedimientos. En este documento se explican dos procesos que se consideran fundamentales en la recolección de evidencia digital.

A. Imagen forense

Durante el proceso forense y posterior al aislamiento de la escena y la identificación de fuentes de información, se debe proceder a la recolección de la información. El proceso de recolección de la información debe garantizar la preservación de la evidencia digital, para esto utilizaremos técnicas de extracción de imágenes forenses que garanticen la integridad de la información.

Uno de los principales métodos para recolección de evidencia de un disco duro, es la extracción de una imagen forense, garantizando no escribir ningún dato sobre la evidencia. Para esta finalidad existen dispositivos llamados bloqueadores de escritura, el TABLEAU (Figura 4) es conocido como un Bridge Forense que permite realizar análisis directamente contra el dispositivo, más, sin embargo es recomendable realizar una copia forense previamente con este Bridge, combinado con FTK (Forensic Tool Kit) que es una herramienta de análisis, se puede hacer la imagen del disco bit a bit y realizar un análisis posterior sobre la imagen, garantizando la integridad de la evidencia.

Figura 4. Dispositivo bloqueador de escritura para análisis de información o creación de imagen forense, [19].

El tableau evita cualquier tipo de escritura sobre la evidencia original, de esta forma se garantiza que se mantengan los principios de integridad en cumplimiento del artículo 11 de la ley 527 de 1999, que a la letra reza:

"Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o

comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente."

Las imágenes forenses son útiles en cualquier tipo de caso de investigación criminal, a manera de ejemplo, si en una investigación criminal se realiza un hallazgo de un computador portátil, es de crucial importancia no contaminar la información que almacena el disco duro de ese computador.

Para estos casos se realizan copias forenses que se evidencia como un solo archivo de formato"raw" o "dd" o algunos investigadores, con mayores recursos, prefieren realizar una copia idéntica en un disco con la misma capacidad del original.

Uno de los problemas de las imágenes de tipo "raw" es que no permiten guardar metadatos de la misma imagen, ya que es una copia exacta sector por sector del disco original. Esta metadata es muy importante ya que en ella se pueden almacenar datos como el nombre del investigador, el motivo de la adquisición o la fecha de realización de la imagen. Cuando ésta información no es almacenada con la imagen, es posible perderla ya que tendría que ser almacenada por separado.

Para solucionar este tipo de inconvenientes se han diseñado formatos, como por ejemplo AFF (Advanced Forensic Format) que permite tanto comprimir la información, como almacenar metadata de la adquisición. Otro formato muy utilizado en procedimientos forenses es el EnCase Forensic Format (Figura 5) cuyos archivos de evidencia son almacenados como .E01, este tipo de archivos contiene metadata almacenada en el encabezado de los mismos, con el prefijo "Case Info" entrelazados con bloques de 64 sectores, y finalizado con un footer que contiene un md5 que verifica el bitstream completo.

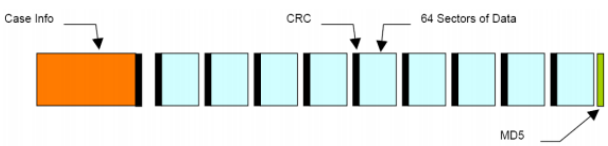

Figura 5. Formato de almacenamiento utilizado por EnCase. Disk Imaging with the Advanced Forensic Format [17].

B. Recolección de datos volátiles

Los datos volátiles son aquellos datos que se pierden cuando un equipo se reinicia, se apaga o simplemente pierde el flujo eléctrico. Existen diferentes técnicas anti-forenses mediante las cuales un delincuente puede hacer más difícil el trabajo de un analista forense, como cifrado u ofuscación de los datos en disco, pero aun para los delincuentes una de las fuentes de información que es más difícil de ocultar o manipular son los datos volátiles.

La Random Access Memory conocida como memoria RAM, es el dispositivo en el cual los computadores almacenan todos los datos a los que accede el usuario en tiempo de ejecución, en la memoria RAM podemos encontrar ejecutables, archivos y hasta lo que escriben los usuarios, es una memoria de acceso rápido utilizada para agilizar los procesos de computo.

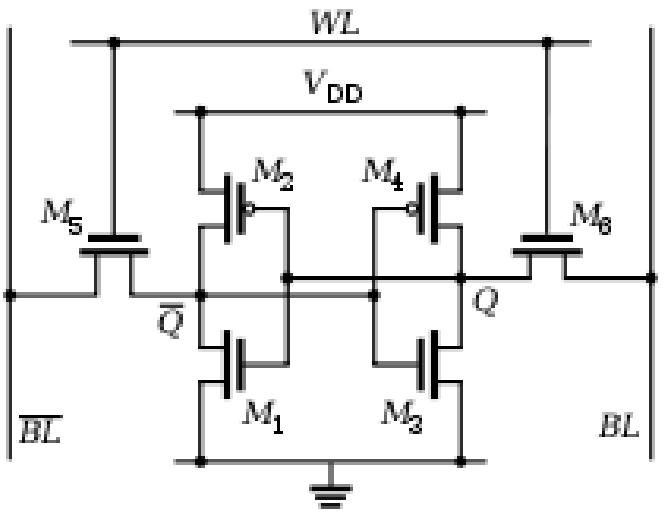

Figura 6. Célula SRAM de seis transistores, Random-access memory. [18]

La información en la memoria RAM a diferencia de los discos duros que escriben sobre una superficie, mantiene la información en transistores, en la RAM estática conocida como SRAM; el circuito es de tipo flip-flop normalmente implementado con transistores de tipo FET (figura 6). En la RAM Dinámica conocida como DRAM (Figura 7) se utiliza un capacitor que actúa como cargado o descargado, que en términos digitales se interpreta como un 1 o un 0 (ver figura 7). Es por este motivo que cuando los equipos son apagados, todos los circuitos alimentados pierden la información almacenada.

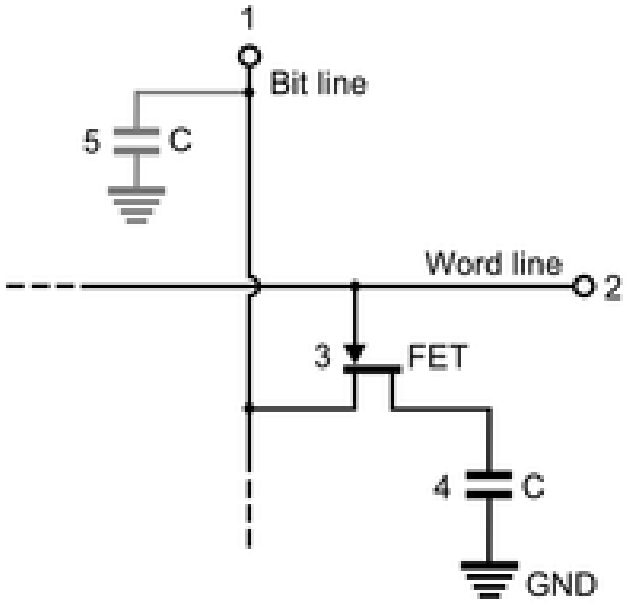

Figura 7. Célula DRAM con un capacitor, Random-Access Memory [18].

Una de las herramientas mas utilizadas para realizar volcado de memoria RAM en sistemas windows es conocida como dumpit. Creada por Comae Technologies hace bastante sencillo el volcado de la RAM que consiste únicamente en ejecutar la herramienta y almacenar la información en una memoria no volátil (puede ser USB). Esta información puede ser analizada posteriormente con software como Volatility, Rekall o Redline, obteniendo funcionalidades, por ejemplo:

- Conseguir lista de procesos en ejecución.
- Escanear procesos en búsqueda de malware.
- Verificar DLL utilizados en procesos en ejecución.
- Listar conexiones activas al momento del volcado.

Pero no solo la memoria RAM almacena datos volátiles, están los registros en cache, tablas de enrutamiento, cache ARP y procesos en ejecución en el sistema.

VI. MARCO LEGAL COLOMBIANO

En Colombia existe un marco legal definido, que protege, ante todo, los derechos de los ciudadanos, por eso es fundamental el conocimiento, como mínimo de las siguientes normas:

A. Ley 527 de 1999

Define y reglamenta el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, también establece las entidades de certificación. En su articulo 8, se define la originalidad de la información, en la cual se establecen dos requisitos:

- Integridad: existe una garantía de que el mensaje de datos se ha conservando en forma original, sin presentar ningún tipo de cambios.
- De requerirse la información recolectada en el proceso forense, puede ser presentada en el momento de su solicitud.

En el articulo 11 se define el criterio para valorar probatoriamente un mensaje de datos. En el cual se establecen las reglas de la sana critica, la confiabilidad de la generación de la información, método de comunicación y confiabilidad en el método utilizado para conservar la integridad de la información. Los conceptos fundamentales para la conservación de la información se incluyen en el articulo 12 y son tres:

- La información se puede consultar.
- Ser conservada en el formato original.
- Que sea posible determinar origen, destino, fecha y hora del mensaje o documento producido.

B. Ley 599 de 2000

El profesional forense esta continuamente en contacto y manipulación de material probatorio, por tanto, requiere el conocimiento del articulo 293, que textualmente reza: *"El que destruya, suprima u oculte, total o parcialmente un documento privado que pueda servir de prueba, incurrirá en prisión de uno (1) a seis (6) años"*.

C. Ley 1581 de 2012

Esta ley define las disposiciones generales para la protección de datos personales. En la recolección de evidencia digital pueden presentarse escenarios que incluyan información personal de los implicados en el análisis; la ley 1581 de 2012 define:
"la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos."
Es de vital importancia, en casos corporativos de levantamiento de evidencia digital, garantizar el cumplimiento de todas las disposiciones legales sobre la materia y que los empleados tengan pleno conocimiento y hallan autorizado, previamente, la recolección de evidencia de los dispositivos directamente relacionados con sus actuaciones en actividades incluidas en su contrato laboral.

VII. CADENA DE CUSTODIA

La cadena de custodia está definida como:

"El procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones". [7]

En el procedimiento de identificación, análisis y conservación de evidencia digital se deben mantener los mismos estándares de cadena de custodia, tenidos en cuenta respecto de otro tipo de material probatorio.

Los objetivos principales del procedimiento de cadena de custodia son:

- Orientar a los servidores y particulares involucrados en la investigación penal, para ejecutar sus actividades en forma secuencial, ordenada y segura.
- Describir los lineamientos básicos para el desarrollo del sistema de cadena de custodia, mejorando el desempeño y confiabilidad de quienes tengan contacto con los elementos materia de prueba o evidencias físicas, con miras a la excelencia en la administración de justicia.
- Normalizar y estandarizar la ejecución del trabajo en el manejo del sistema de cadena de custodia.

Con este fin la Fiscalía General de la Nación ha generado una lista de procesos y procedimientos que se enuncian a continuación: [7]

- Manejo del lugar de los hechos.
- Aseguramiento del lugar de los hechos.
- Observación análisis y valoración del lugar de los hechos.
- Fijación del lugar de los hechos.
- Recolección embalaje y rotulado de los elementos materia de prueba o evidencias.
- Envío de los elementos materia de prueba o evidencias al laboratorio.
- Recepción o análisis de los elementos materia de prueba o evidencias en el laboratorio autorizado.
- Recepción y custodia de los elementos materia de prueba o evidencias en el almacén de evidencias.
- Requerimiento judicial de los elementos materia de prueba.
- Disposición final de los elementos materia de prueba o evidencia.
- Documentación final del sistema de cadena de custodia.

VIII. CONCLUSIONES

La informática forense es una ciencia, que paso a paso ha venido abriendo espacios en todos los procesos tecnológicos pero a medida

que avanza el proceso de digitalización también aumentan los delitos informáticos, no solo ataques de tipo económico, los delincuentes utilizan la tecnología para ejecutar sus crímenes, los grupos armados al margen de la ley emplean medios de comunicación y sistemas de cifrado, al igual que las Fuerzas Militares. La necesidad de informáticos forenses en capacidad de recolectar y analizar este tipo de evidencia está en aumento; los procesos forenses han ido avanzando con el tiempo y a la par con la evolución de los delitos.

Para realizar un proceso de recolección y análisis de evidencia digital, se deben tener en cuenta como mínimo, los títulos expuestos en el presente documento, la recolección de evidencia, el marco legal y la cadena de custodia. Teniendo esta base, es posible para cualquier empresa enmarcada en las leyes colombianas, construir un proceso forense y lograr los principales objetivos de esta ciencia.

IX. Glosario

INFORMÁTICA FORENSE: es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

CADENA DE CUSTODIA: se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones.

CIBERSEGURIDAD: Es la capacidad del estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética.

CONFIDENCIALIDAD: es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

MALWARE: es la abreviatura de “Malicious software”, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

CONPES: El Consejo Nacional de Política Económica y Social (Conpes) es un organismo asesor del Gobierno en materia de desarrollo económico y social, y es el encargado de estudiar y recomendar políticas generales en esas áreas.

DISPONIBILIDAD: es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

INCIDENTE: Cosa que se produce en el transcurso de un asunto, un relato, etc, y que repercute en él alterándolo o interrumpiéndolo.

INTEGRIDAD: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Groso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Referencias

[1] Rezakhani, Afshin, Hajebi, AbdolMajid Mohammadi, Nasibe(2011) “Standarization of all Information Security Management Systems”, International Journal of Computer Applications, Vol.18, No. 8.

[2] Lopez Óscar, Amaya Haver, Leon Ricardo. Informatica Forense: Generalidades, Aspectos técnicos y herramientas, Universidad de Los Andes.

[3] Gaston Semprini, Alfredo Bozzetti (2013). Informática Forense al Servicio de una Justicia Moderna, Simposio Argentino de Informática y Derecho.

[4] Ocampo S Carlos Alberto; Trejos Buriticá Omar Iván; Solarte Martínez Guillermo Roberto. LAS TÉCNICAS FORENSES Y LA AUDITORÍA, Scientia et Technica Año XVI, No 45, agosto de 2010. Universidad Tecnológica de Pereira. ISSN 0122-1701.

[5] Francisca Rodríguez Más, Alfredo Doménech Rosado. LA INFORMÁTICA FORENSE: EL RASTRO DIGITAL DEL CRIMEN.

[6] Di Lorio Ana Haydée, Sansevero Rita Evelina, Martin Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo Julián Waimann. La recuperación de la información y la informática forense: Una propuesta de proceso unificado.

[7] Fiscalia General de la Nacion, Iguaran Arana Mario German, Manual de procedimientos para cadena de custodia. ISBN 958-97542-8-7

[8] Zuccardi Giovanny, Gutierrez Juan Davis (Noviembre de 20016), Informatica Forense

[9] ESET Security Report Latinoamerica 2017, (2017), Enjoy Safer Technology

[10] Forensic Handbook: "Locard's Exchange Principle" [Online] http://www.forensichandbook.com/locards-exchange-principle/

[11] Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley Forensic Science Communications (Octubre de 2000), [Online] https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

[12] Casey, E. (2001) Handbook of Computer Crime Investigation. Academic Press.

[13] Ministerio de tecnologias de informacion y telecomunicaciones De Colombia, Evidencia Digital (2016), [Online] https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

[14] Crime Museum, [Online] https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard/

[15] Hannan Matew, To Revisit: What is Forensic Computing?.

[16] Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib. Mapping Process of Digital Forensic Investigation Framework

[17] Simson L. Garfinkel, David J. Malan, Karl-Alexander Dubec,Christopher C. Stevens, Cecile Pham, Disk Imaging with the Advanced Forensic Format, Library and Tools

[18] Random-access memory, [Online] https://en.wikipedia.org/wiki/Random-access_memory

[19] Tableau Forensic USB 3.0 Bridge T8u [Online] https://www.guidancesoftware.com/tableau/hardware//t8u