POLITÉCNICO GRANCOLOMBIANO INSTITUCIÓN UNIVERSITARIA

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

EVIDENCIA DIGITAL: PROCEDIMIENTOS Y PROTOCOLOS A LA LUZ DE LOS PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

PRESENTA:

JAURIGUY CHACÓN BARBOSA
Cód 1712010149

ASESOR TEMÁTICO:

WILMAR JAIMES FERNANDEZ

MAYO 07 DE 2018

ÍNDICE GENERAL

Pág.

ÍNDICE DE ANEXOS

ÍNDICE DE TABLAS

Resumen

El presente estudio de corte cualitativo se constituye en un análisis adelantado en la Fiscalía General de la Nación con investigadores del grupo de delitos informáticos, en torno al tema de la evidencia digital y su relación con los pilares de la seguridad de la información. Este planteamiento partió del trabajo previo de análisis de prospectiva y viabilidad, realizado durante el segundo semestre del año 2017 el cual arrojó la necesidad de abordar la problemática que se desarrolla a lo largo del documento.

Los resultados se convierten en la evidencia de las necesidades y falencias que se presentan cuando prospera el procedimiento de recolección y manipulación de la evidencia digital lo que da cuenta de la afectación de la información en cuanto a los pilares de la confidencialidad, integridad y disponibilidad. De la misma manera se encuentra que existe mucho por hacer y por reflexionar para que la realidad de la informática forense se asuma desde una perspectiva más normativa, de forma que se garanticen procesos judiciales óptimos y coherentes.

Palabras Clave: evidencia digital, informática forense, confidencialidad, integridad y disponibilidad.

Abstract

This qualitative study is an analysis developed with the informatics group investigation of the Fiscalía General de la Nación (FGN), about digital evidence and its relation with the security information pillars. All of this was taken from a previous work, prospective and feasibility analysis, developed during the second semester on 2017. It showed the need to study the problem presented along this document.

The gotten results are the evidence of the needs and flaws found when someone speaks about collection and management of digital evidence ´cause there are many affected information when we have to make reference to confidentiality, integrity and availability. It is important to say too that exist a long way to go and to reflect in order to assume the forensic informatics from a normative perspective to achieve optimal and coherent judicial processes.

***Key Words*:** digital evidence, forensic informatics, confidentiality, integrity and availability

1. Introducción

Con los avances tecnológicos en el ámbito de las comunicaciones y su paulatina inclusión en el proceso judicial, se han gestado una serie de cambios cuya principal pretensión ha sido lograr que la justicia actúe con rapidez y eficacia, pero en esta tarea se choca con un gran obstáculo y es que las personas quienes adelantan la recolección de información contenida en las evidencias digitales, carecen de los conocimientos técnicos necesarios, lo que hace, en algunos casos que se pierda el valor probatorio que se requiere para llevar los procesos judiciales que se adelantan en el país.

Es así como aparecen una serie de normas que buscan responder a esta problemática pero en el marco de la seguridad y privacidad de la información y / o estándares internacionales; estos no hacen un énfasis en lo relacionado con protocolos de la seguridad de la información para realizar la recolección de la evidencia digital.

En este contexto es relevante reconocer la definición del problema, la justificación y los objetivos trazados para identificar el marco en el que se da esta investigación.

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente personas inescrupulosas aprovechan, cada vez con más frecuencia, las herramientas de la informática y los medios tecnológicos dispuestos para el tratamiento de la información, con el propósito de cometer actos criminales y evadir la ley. Ante esta situación los gobiernos se ven abocados a reglamentar y establecer unas directrices para llevar a cabo la gestión de la recolección de la evidencias digitales que contengan información clave para ser usadas como pruebas ante la autoridad judicial, teniendo en cuenta que las evidencias en un proceso legal, es de especial importancia. Por lo anterior, la actividad de obtención de Información a través de medios digitales se constituye hoy en día en una de las facetas primordiales para el éxito de una investigación judicial. Por lo anterior es evidente que se requiere de los investigadores que intervienen en el manejo de recolección de evidencia digital, calificación y cualificación para intervenir en los procedimientos, y de esta manera realizar acciones que puedan invalidar las pruebas digitales, cuando se adelante un proceso judicial.

Los procesos judiciales en Colombia, específicamente, la recolección y manipulación de evidencia digital, son responsabilidad, en primera instancia de los investigadores y los peritos ya que son ellos quienes entran en contacto directo con aquella, por lo que deben dar cuenta de su autenticidad, integridad y confidencialidad. Existen entidades seguidoras de estos temas de justicia que velan por que los procesos de justicia se den en el marco de la trasparencia y siguiendo la normatividad existente en esta materia, en beneficio de una persona en particular o de un caso en general. Finalmente es imperativo que en las instituciones educativas que ofrecen programas de formación en temas relacionados con la justicia y funciones de policía judicial, aborden aspectos relacionados con protocolos y profesionalización en la recolección y manipulación de evidencia digital.

El problema con los datos de la evidencia digital es que estos son menos tangibles que otros tipos de pruebas físicas, se consideran pruebas frágiles puesto

que pueden ser fácilmente destruidos o modificados, de hecho el acto mismo de la recolección o el examen forense, pueden ser individual o conjuntamente alterados. Para que la evidencia sea admisible debe demostrarse que esta no ha sido alterada ni modificada desde el momento mismo que se inició su proceso de acopio.

1.2 Justificación

Para la fiscalía General de la Nación –FGN-, en cabeza de su grupo de investigación de delitos informáticos, es importante desempeñar sus funciones de la mejor manera posible, dando cumplimiento a las exigencias del sistema judicial colombiano. Es así que al adelantar procedimientos relacionados con recolección de evidencia digital, se nota que existen falencias que se han visibilizado a través de los informes y actas que dan cuenta de diligencias, también esto se manifiesta en las inquietudes y diferencias de criterio existentes al no contar con protocolos establecidos para tal fin. Capacitar al personal, permitiría solucionar en gran parte los inconvenientes en este aspecto, además que se agilizarían procesos y optimizarían recursos dispuestos para garantizar la veracidad y confiabilidad al manipular datos contenidos en la evidencia digital recolectada.

1.3 Objetivos

1.3.1 Objetivo general

Revisar los procedimientos que se adelantan en la recolección de evidencia digital, a la luz de los pilares de la seguridad de la información, para garantizar el óptimo desarrollo de procesos judiciales colombianos.

1.3.2 Objetivos específicos

- Reconocer el estado del arte de la informática forense en cuanto a la recolección de la evidencia digital.
- Determinar las falencias que se dan cuando se realizan procedimientos relacionados con la recolección de evidencia digital.
- Proponer metodologías especializadas y rigurosas que conlleven a preservar la evidencia digital, desde la perspectiva de los pilares de la información

2. Revisión de la literatura

2.1 Antecedentes

Luego de realizar un rastreo de las tesis de pregrado y posgrado, artículos y documentos relacionados con estudios en torno al tema de la recolección de evidencias digitales, se encontraron siete (7) tesis y artículos de carácter nacional y dos (2) adelantados en el exterior.

El artículo titulado "*propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos (CSIRT)* de Uyana (2014), tiene por objeto mostrar un estudio relacionado con ataques y estrategias de invasión "que van siendo perfeccionados día tras día por las personas con conocimientos avanzados en el área informática y de sistemas, atentando contra la integridad de la información, seguridad y privacidad de las personas, instituciones, gobiernos y sociedad"(p.1) Para ello adelantó una investigación exploratoria y descriptiva que desembocó en la propuesta para diseñar un área de informática forense que atendiera los incidentes de seguridad informáticos; la autora concluye que este equipo permitiría el establecimiento de controles de seguridad y su seguimiento, de manera que se puedan esclarecer los delitos informáticos, análisis de incidentes, reconstrucción de escenas, entre otros.

Se halló también un artículo colombiano de Ariza, Ruíz y Cano (2017) *iPhone3G: un nuevo reto para la informática forense* en donde los autores presentan un panorama general de la seguridad en el dispositivo iPhone 3G, desde allí se habla de unos modelos para realizar un análisis forense, aplicación y procedimientos para adelantar dicha labor, estableciendo la importancia de los mismos. Los autores encontraron que la aparición de nuevas tecnologías y que la heterogeneidad de las mismas, no permiten un estricto seguimiento a los procedimientos forenses que se adelantan y que se requiere desarrollar guías metodológicas que detallen el cómo obtener evidencia evitando incidentes de seguridad informática sobre los dispositivos.

Otro artículo que aparece en el rastreo es el del artículo de la Universidad Piloto de Colombia, *respuesta a incidente informático* de Acosta (2013) quien pretende plantear un plan de respuesta a incidentes informáticos que contribuya con elementos relevantes para identificar, controlar y registrar acertadamente los posibles incidentes de manera que se puedan prevenir posibles ataques que comprometan la seguridad de la información. Se plantea la importancia de que las empresas inicien un proceso de transformación para afrontar de manera eficiente y oportuna los momentos de crisis que se presentan con los avances tecnológicos. Hace énfasis en que para hablar de cadena de custodia se debe manejar un formato de rotulación de los elementos, previa verificación de la existencia de pruebas "que permitan sustentar un procedimiento de incautación de elementos probatorios" (p.3).

En el documento de investigación *informática forense: generalidades, aspectos técnicos y herramientas* de López, Amaya y León (2002), se muestra una panorámica de la informática forense haciendo énfasis en su descripción, definición de evidencia informática, almacenamiento en medios magnéticos y técnicas para asegurar evidencia. Los autores encuentran que existen unas limitaciones en cuanto a la imposibilidad de profundizar en algunos temas particulares relacionados con detalles técnicos como grabaciones, eliminación de datos entre otros, debido a que existe poca literatura en torno al tema.

Se halló el trabajo de grado de una especialización de Rendón (2012), titulado *La eficacia de la prueba digital en el proceso penal colombiano* cuyo objetivo central era evaluar las dificultades que presentaban las pruebas digitales dentro del proceso penal colombiano; para ello se adelantó una investigación de corte cualitativo y documental, pensando en que debido a los avances tecnológicos se hace cada vez más difícil abordar la investigación de los delitos en este ámbito por lo que se debe estar en constante actualización contando con apoyo institucional de organizaciones que se encargan de esta labor. La autora concluye que siempre

debe conservarse la integridad de la evidencia digital, por lo que es necesario que quienes adelanten esta labor deben estar calificadas:

> (…) se debe asegurar que las evidencias tomadas, no se modifiquen, pues deben conservar su estado original, y la persona que la recolecte debe estar debidamente entrenada y calificada para este propósito, en su obtención deben estar completamente documentadas, preservadas y disponibles para su revisión. (Rendón, 2012, p. 27)

En el artículo *conceptos y retos en la atención de incidentes de seguridad y la evidencia digital* de Cano (2002), se advierte la necesidad de prepararse para enfrentar posibles ataques a infraestructuras de computación y comunicación debido a los crecientes reportes de incidentes de seguridad, presencia de distintas vulnerabilidades y recientes formas de acceso a los recursos de las máquinas. A modo de conclusión habla del uso de guías para enfrentar el reto de la evidencia digital y el manejo de incidentes; hace énfasis en la importancia de preparar a las organizaciones para enfrentar estas situaciones de crisis, lo que puede redundar en la presencia de fallas y desaciertos que comprometen la seguridad y el adelanto de procesos que cuenten con elementos de juicio que validen las evidencias. En este sentido propone la autora que se promueva la conformación de equipos de trabajo capacitados y entrenados, con funciones y sistemas de notificación debidamente definidos para mejorar la capacidad de reacción y control de situaciones críticas, dando prioridad al tema de la evidencia digital. Concretamente dice la autora:

> (…) promover iniciativas gubernamentales que sensibilicen al aparato judicial y legislativo de la nación para desarrollar estrategias, estándares y legislaciones que promuevan el estudio y difusión del conocimiento de los delitos informáticos, para forjar un nuevo perfil de fiscales que se integren al reto de una sociedad digital. (…) (Cano, 2002, p. 71)

El artículo de Roatta, Casco y Fogliato (2015) *El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012* habla del cómo debe aprovecharse la evidencia digital bien procesada en distintos escenarios que esta sea probatoria,

sea precisa para proporcionar credibilidad a la investigación teniendo en cuenta la metodología, y la cualificación de las personas que intervienen en el proceso investigativo, particularmente quienes recolectan la evidencia. Como resultado de su trabajo se encuentran a la espera de financiación para la construcción de un bloqueador de escritura por hardware SATA para la adquisición de evidencia digital de discos rígidos sin contaminar la evidencia.

Ramírez y Castro (2018) en su *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia,* hablan de que la seguridad informática debe propender por proteger los diversos recursos tecnológicos inherentes a la operación de una empresa o entidad de manera que sean utilizados de manera óptima. El principal objetivo del estudio fue identificar las falencias en el tratamiento de pruebas digitales que ocasionen perdidas, daños o destrucción cuando se adelanta un proceso judicial para lo cual desarrollan un estudio del proceso de cadena de custodia en la investigación de delitos informáticos en Colombia. Concluyen los autores que una de las grandes falencias se encuentra en la falta de capacitación o conocimiento de las metodologías en torno al tema, también mencionan el uso de herramientas inadecuadas y debilidades en los procedimientos.

Finalmente el escrito *Modelo de seguridad y privacidad de la información* (MINTIC, 2016), presenta como objetivo general generar un documento respecto a los lineamientos de buenas prácticas de seguridad y privacidad para las entidades del Estado; En este compendio se describen los modelos de seguridad y privacidad de la información, los ciclos de operación y post correspondientes. Se mencionan los protocolos a adoptar y algunas guías a ejecutar.

2.2 Marco teórico

El presente trabajo enmarcado en el énfasis en desarrollo, desde la perspectiva de la informática forense, partió de tres categorías a saber: evidencia digital, protocolos de recolección y manipulación de evidencia digital y seguridad de la información.

Para contextualizar estas categorías se tomó como referente para abordar la evidencia digital y los protocolos de recolección / manipulación de información, las normas ISO 27037 de 2012 y la Guía de seguridad y Privacidad de la información del Ministerio de las Tics (2016). Finalmente para el tema de la seguridad de la información se tomó la ISO/IEC 27001 de 2005.

2.2.1 Evidencia digital

Según el documento del Ministerio de las Tics (MINTIC) y la norma ISO 27037 de 2012, la evidencia digital en cuanto a análisis forense, “es un procedimiento gobernado por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia” (ISO 27037, 2012, p. 3); el cumplimiento de estos principios es lo que da piso y soporte a la formalidad de las investigaciones que se adelantan en el ámbito judicial.

La evidencia digital es el paso más importante para iniciar alguna acción de tipo legal, para el caso específico de este estudio, los investigadores o personas que hacen parte de la Fiscalía General de la Nación son las encargadas de adelantar esta labor para dar curso a las investigaciones que le corresponde iniciar.

Hablar de este tipo de procedimiento lleva a pensar en una etapa previa que tiene que ver con el análisis del incidente reportado, es decir, el establecimiento de si se trata de una acción que ha atentado contra alguno de los pilares de la información: la confidencialidad, integridad o la disponibilidad de la información (MINTIC, 2016).

2.2.2. Protocolos de recolección y manipulación de evidencia digital

La norma ISO 27037 de 2012 presenta algunos aspectos claves para el manejo de la evidencia digital que tiene que ver con “la sistematización de la identificación, recolección, adquisición y preservación de aquella” (p. 3). Se habla de que dichos procesos deben adelantarse cabalmente si se quiere conservar la integridad de la evidencia y por ende llevar a buen término procesos judiciales.

De acuerdo con el MINTIC (2016, p.12) la metodología general del procedimiento de evidencia digital se centra en 5 pasos principales:

1. Aislamiento de la escena
2. Identificación de fuentes de información
3. Examinación y recolección de información
4. Análisis de datos
5. Reporte

2.2.3. Seguridad de la información

Según la norma ISO 27001,

> La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información (ISO-IEC 27001, 2005, p. 3)

Continuando con la norma, es preciso decir que esta es bastante clara con relación a la definición de cada uno de los pilares. El primero de la confidencialidad lo define como el hecho de que la información no sea revelada a personal no autorizado; de la integridad se puede decir que consiste en mantener la información completa y fiel así como conservar sus métodos de procesamiento; finalmente también se habla de la disponibilidad que no es más que contar con la información de manera que quien la requiera pueda acceder fácilmente a ella. (MINHAC, 2013).

3. Estrategia metodológica

3.1 Enfoque Metodológico: Cualitativo

El presente trabajo se cimienta en la teoría del enfoque cualitativo que se utiliza para descubrir y modificar preguntas de investigación, basándose en una recolección de datos a través de la descripción y la observación, sin medición numérica. (Hernández, Fernández y Baptista, 2003). De acuerdo con lo anterior se puede decir que se tiene la finalidad de describir, comprender e interpretar una realidad tomando como referencia las experiencias de los participantes; igualmente facilita la comprensión de una situación social real, como lo es, la recolección de evidencia en el campo de la informática forense.

El enfoque cualitativo plantea una realidad por descubrir, maneja un lenguaje natural, busca adentrarse en el contexto y en el punto de vista del actor social, además busca la dispersión o expansión de los datos o informaciones, es decir, va de lo particular a lo general. De acuerdo con Hernández, Fernández y Baptista (2003):

> Los estudios cualitativos involucran la recolección de datos utilizando técnicas que no pretenden medir ni asociar las mediciones con números, tales como observación no estructurada, entrevistas abiertas, lectura de documentos, discusión en grupo, evaluación del crecimiento personal, inspección de historias de vida, análisis semántico y de discursos cotidianos (…)(p.14).

3.2. Técnicas y muestra de investigación

Para obtener datos que permitieran alcanzar el objetivo general de investigación, se utilizó la técnica de la encuesta y el análisis documental.

La primera técnica se aplicó a diez investigadores (50%) de los veinte que conforman el grupo de delitos informáticos. A todos se les formuló la misma pregunta la cual buscaba identificar la percepción de los investigadores respecto al manejo de la evidencia digital; esta encuesta fue anónima y contaba con una pregunta abierta. (Ver Anexo 1).

La segunda técnica, el análisis documental consistió en revisar la normatividad que se tenía, en el ámbito nacional, respecto al tema que planteaban las categorías ya expuestas. Estos documentos permitieron contrastar la norma a la luz de la experiencia con la que cuentan los investigadores del grupo de la Fiscalía General de la Nación, partiendo del planteamiento de Herrero (1997) quien define esta técnica como una serie de operaciones destinadas a describir y analizar la información escrita que se ha producido sobre el objeto de estudio para hacerla más accesible.

Gracias al trabajo realizado a través del análisis de prospectiva de la situación problema, se pudieron identificar las variables que permitirían definir el rumbo del estudio que se presenta, estas son: evidencia digital, protocolos para recolección y manipulación de evidencia digital y seguridad de la información.

3.3. Análisis de la información

Para analizar los datos recolectados a través de los investigadores, en primera instancia se tomaron palabras clave organizadas en una matriz que a la par consolidaba aspectos relevantes de dichas palabras y además el pilar que fallaba en cada caso. Posteriormente se realizó un proceso de triangulación entre lo que los funcionarios decían, lo que los autores y documentos postulaban (artículos académicos, investigaciones periodísticas y otra información pública) y la visión del investigador a través de su experiencia en el campo de la informática forense.

4. Resultados

Después de hacer una revisión de las respuestas dadas por los investigadores, se procedió a buscar recurrencias entre sus escritos encontrando de manera contundente el manejo de dos grandes categorías: por un lado se tiene la falta de capacitación, preparación y entrenamiento a los investigadores que adelantan la recolección de la evidencia digital, y por otro se detecta como una problemática el hecho del tratamiento que se da a la información en cuanto a dos variables que son la falta de procedimientos –protocolos- claros y el manejo de la evidencia digital.

Con el propósito de abordar el objetivo se estableció una matriz que diera cuenta de las categorías descritas, de su definición desde la perspectiva planteada por los encuestados y de los pilares de la información que se veían afectados con la situación presentada.

Tabla 1. Matriz de hallazgos

SITUACIÓN PROBLEMA	DESCRIPCIÓN DE LA PROBLEMÁTICA	PILAR COMPROMETIDO
1. Preparación y capacitación	• Los investigadores hablan de la necesidad de hacer una divulgación de técnicas • Se plantea la falta de conocimiento técnico del personal • Se manifiesta que no hay interés por parte de las entidades para	• Confidencialidad • Integridad • Disponibilidad

	capacitar a funcionarios • Los investigadores hablan de falta de personal idóneo • Se dice que no hay una buena capacitación a funcionarios de policía judicial • Falta documentación, experiencia y entrenamiento del funcionario • Los conceptos no son claros y presentan muchas interpretaciones	
2. Tratamiento de la información	• Se plantea la ausencia de protocolos para lo que se deben tener en cuenta manuales, guías e instructivos • El procedimiento no se ajusta a los protocolos internacionales	• Confidencialidad • Integridad • Autenticidad • Disponibilidad • Trazabilidad

	• La evidencia digital es frágil • Falta de precaución en el manejo de dispositivos • Fallas en el embalaje que afecta la integridad del elemento material probatorio (EMP)	

Considerando el primer aspecto de la falta de capacitación, los investigadores hablan de la necesidad de hacer una divulgación de técnicas y de la falta de compromiso de las entidades por hacer que sus funcionarios se entrenen en el tema, así lo afirma uno de los investigadores entrevistados (E1), “falta de conocimiento técnico del personal que realiza la recolección (…) falta de interés de las entidades para capacitar a sus funcionarios (…), de acuerdo con lo mencionado, se evidencia que al no contar con el conocimiento en el tema, la información queda expuesta y por lo tanto pone en peligro el cumplimiento de la confidencialidad en cuanto a que no se garantiza un manejo prudente, aunque se le dé un uso estricto; al fallar los métodos de procedimiento, como consecuencia del desconocimiento, se falta a la integridad de la información, mientras que por el lado de la disponibilidad las cosas no son distintas ya que pueden existir casos en que la información no se encuentre lista cuando alguien lo requiera, como se ha mencionado, como consecuencia de la inexperiencia. Hablar de la adecuada conservación de la evidencia remite a la guía N° 13 de seguridad y privacidad de la información cuando plantean que “(…) es necesario verificar que el evento que está siendo reportado, es en realidad un incidente que atenta contra la confidencialidad, integridad o

disponibilidad de la información" (p.13), en este sentido la ISO/IEC 27037 complementa "la evidencia digital potencial debe ser preservada para asegurar su utilidad en la investigación. Es importante para proteger la integridad de las pruebas" (MINTIC, 2016, p.13).

Con relación a la falta de capacitación que se evidencia en la carencia de personal idóneo, sin experiencia y entrenamiento, lleva a pensar que mientras adquiere esa experiencia, es decir al ser empíricos, se cometerán varios errores los cuales con el pasar del tiempo serán enmendados, pero mientras se dan dichas falencias pondrán en peligro los procedimientos, por ende las evidencias y la información contenida en ellas. En este aspecto la normatividad emanada por MINTIC es clara al mencionar que "debe existir un grado de entrenamiento suficiente (…) para poder realizar los procedimientos de evidencia forense, así como también deben poseer conocimientos sobre protocolos de red (…)" (p.29). Por parte de la norma ISO-IEC 27001 se establece "la organización debe implementar programas de formación y de toma de conciencia" (p.7) y más adelante amplía "además debe asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI, sea competente para realizar las tareas exigidas" (p.11). Un claro ejemplo de esta situación se nota en las respuestas de servidores entrevistados, "las inconsistencias se dan por falta de capacitación y personal idóneo" (E6), por su parte otra persona manifestó "(…) por falta de entrenamiento y experiencia del funcionario judicial que lo ejecuta"(E5); la problemática se hace más evidente cuando se especifica que esto ocurre con la evidencia digital, la cual contiene información crucial para adelantar procesos judiciales "(…) adicionalmente los investigadores no son preparados para hacer recolección de evidencia digital". La norma ISO/IEC 27037 especifica que "en el cumplimiento de su función, el funcionario debe tener experiencia adecuada, habilidades y conocimientos en el manejo de la evidencia digital potencial" (p.16).

Si se habla de que los conceptos no son claros y presentan muchas interpretaciones, es claro que hay ambigüedad en la ejecución de los procedimientos, lo que en últimas se verá reflejado en la manera como se expone

la información, faltando a los pilares de la seguridad de la misma, de esto se da cuenta en la siguiente respuesta, “el proceso de recolección de evidencia digital es inconsistente porque los conceptos no son claros y presentan diversidad de interpretaciones” (E9). En este sentido la literatura consultada propone “Emprender revisiones regulares de la eficacia del SGSI (…) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas” (ISO-IEC 27001, p.8).

Con relación al segundo hallazgo que tiene que ver con el tratamiento de la información, se encuentran varios aspectos como la falta de protocolos en la organización, el desconocimiento de los protocolos internacionales y su respectiva aplicación al contexto colombiano y, fallas en el embalaje que afecta la integridad del elemento material probatorio (EMP), teniendo en cuenta que la evidencia es altamente frágil. Éste último aspecto es destacado por la norma ISO/IEC 27037 “la evidencia digital puede ser frágil en la naturaleza. Puede ser modificado, alterado o destruido debido a una manipulación inadecuada (…)” (p.11). La pertinencia de estos hallazgos radica en que son las causas detectadas para que la información esté expuesta y por tanto no cuente con la respectiva seguridad que garantice su confidencialidad, integridad y disponibilidad.

Hacer alusión a los protocolos obliga a mencionar dos problemáticas, por un lado es claro que existen unos protocolos internacionales los cuales son desconocidos por los servidores encargados de adelantar la recolección de la evidencia digital y, por otro no existen unos protocolos que garanticen que los procedimientos se hagan bien. Al respecto los encuestados afirman “(…) la actividad de recolección no se ajusta a los procedimientos internacionales, o no se cumplen a cabalidad por mala e insuficiente documentación (…) (E5), es importante destacar que el encuestado dice que no se ajusta, es decir que de hecho se sabe de la existencia de los protocolos internacionales pero el inconveniente radica en que no son lo suficientemente conocidos o integrados a un protocolo propio de la institución, lo cual se nota cuando se dice “el proceso de recolección de evidencia digital presenta inconsistencias porque no existe un protocolo adecuado” (E6). Estas dos

situaciones se abordan desde la norma ISO/IEC 27037 “esta norma internacional proporciona directrices para las actividades específicas en el manejo de la evidencia digital potencial (…) diseñado para mantener la integridad de la evidencia digital” (p.4).

A través de las encuestas se detectó también que la parte del proceso al que se alude, como el que está fallando, es el trabajo de embalaje. El embalaje se define como la forma como “se debe proteger todo dispositivo digital” (ISO/IEC 27037, p.20), y se realiza para “evitar la contaminación del dispositivo (s) digital antes de transportar a otro lugar (s)” (p.20); si se parte de esta definición es válido afirmar que allí radica el hecho de que la información quede expuesta, por lo que no se asegura su confidencialidad en tanto que cualquiera puede acceder a ella, alterarla vulnerando su integridad y dejándola a disposición de cualquier persona malintencionada faltando al pilar de la disponibilidad. A parte de esto cuando llega para ser utilizada en procedimientos judiciales, los jueces terminan desestimando las pruebas por carecer de los aspectos anteriormente mencionados. Una evidencia de lo planteado se halla en lo relatado “(…) para estos casos se debe recolectar lo necesario y embalarlo de forma adecuada para garantizar la integridad del EMP” (E2).

5. Discusión y conclusiones

5.1 Discusiones generales

- Es importante mencionar que cuando los autores plantean la importancia de adelantar un proceso adecuado, en lo relacionado con la recolección de evidencia digital, lo que en esencia se sugiere es la protección de la información para que pueda conservarse su integridad, tal es el caso de Rendón (2012) quien enumera los principios de la identidad, integridad, preservación, seguridad, almacenamiento, continuidad, autenticidad y originalidad, para garantizar la integridad de la evidencia digital.
- La literatura consultada, especialmente en la parte de antecedentes, es reiterativa cuando alude a la relevancia que tiene la capacitación y la formación de personal en el tema de la seguridad de la información para que los procesos judiciales que se adelanten tengan éxito en lo que a evidencia digital se refiere; es pertinente mencionar a Cano (2012) cuando hace énfasis en la necesidad de "promover iniciativas gubernamentales que sensibilicen al aparato judicial y legislativo de la nación para desarrollar estrategias, estándares y legislaciones que promuevan el estudio y difusión del conocimiento de los delitos informáticos"(p. 71). Por otra parte está el estudio de Roatta, Casco y Fogliato (2015) quienes hablan de cómo debe aprovecharse la evidencia digital bien procesada en distintos escenarios para proporcionar credibilidad a la investigación teniendo en entre otras cosas, la cualificación de quienes participan del hecho investigativo, es decir de quienes recolectan la evidencia.
- Acorde con las investigaciones realizadas por los autores mencionados en este estudio, es claro que para atender los incidentes de seguridad informáticos, hablando de esclarecer delitos informáticos, y, en este caso, cuando existen serias falencias en los procesos de recolección de evidencia digital, deben establecerse protocolos y procedimientos para adelantar la diligencia de manera que se garanticen los pilares de la información, así lo confirma Ariza, Ruiz y Cano (2017) "se requiere desarrollar guías

metodológicas que detallen el cómo obtener evidencia evitando incidentes de seguridad informática sobre los dispositivos".

- Cabe aclarar que a la luz de las normas ISO / IEC 27037 (2012) y teniendo en cuenta lo expuesto en la parte de hallazgos, aunque los entrevistados mencionan al embalaje como una de las falencias del proceso, las normas especifican que este embalaje de la evidencia digital es solo una de las actividades que se consideran para preservar la evidencia digital (p. 20).
- De acuerdo al cómo se ha abordado el tema de la evidencia digital, es pertinente mencionar, que en este contexto, hay que darle relevancia ya que se trata de emprender acciones legales, investigaciones disciplinarias internas o de aprendizaje MINTIC (2016).
- Teniendo en cuenta el objetivo general del presente trabajo, que consiste en revisar los procedimientos que se adelantan en la recolección de evidencia digital, a la luz de los pilares de la seguridad de la información, es de notar que existen serias dificultades que llevan a exponer la información de manera que con la confidencialidad no se garantiza el acceso a personal autorizado y además se da pie a la modificación de la información faltando a la integridad, como lo plantea Mccumber (1991).

5.2 Conclusiones

- Es relevante destacar que no existe literatura suficiente ni amplia que aborde el tema de la recolección de la evidencia digital partiendo de la base de los pilares de información, aspecto clave cuando se habla de informática forense y de dar validez a la cadena de custodia.
- Se puede concluir que, cuando se habla de recolección de evidencia digital, los servidores que realizan dicha labor presentan varias dudas con relación a cómo se adelantan los procedimientos pues actúan de acuerdo con su experiencia, reconociendo que las falencias se hacen evidentes cuando los casos se caen por incurrir en errores procedimentales.
- Los errores en los procedimientos pueden corregirse si se realiza un adecuado estudio de seguridad de la información y si se tienen como base

los pilares de la confidencialidad, integridad y disponibilidad, para garantizar que todos los servidores hagan el mismo seguimiento y como consecuencia se optimice el trabajo que se hace.

- Es importante que los investigadores del grupo de delitos informáticos, se beneficien de capacitaciones y sesiones de entrenamiento en relación a la recolección de evidencia digital, para que de manera conjunta y a la luz de los documentos y normatividad internacional en materia, se establezcan los protocolos que han de regir los procedimientos que garanticen la seguridad de la información.
- Las principales falencias que detectan los servidores que adelantan los procedimientos, se encuentran en la parte del embalaje, pues es allí en donde se expone principalmente la información y se corre el riesgo de contaminarla o incluso perderla, debido a su calidad de frágil.

5.3 Limitaciones

- Hacer un acercamiento más amplio con la población en donde se adelantó el estudio –FGN-, es complejo pues se trata de una entidad oficial, del orden judicial que no .puede hacer pública ninguna clase de información con respecto a los procedimientos confidenciales que sigue, por lo tanto el acceso a documentos es 100% restringido.
- Es escasa la literatura que da cuenta de los protocolos que deben seguirse cuando se va a recolectar evidencia y más si se habla de conservar la confidencialidad, integridad y disponibilidad. Es aún un tema sin explorar y/o sistematizar.

5.4 Recomendaciones

- Se recomienda fijar espacios de capacitación, análisis y retroalimentación, contando como punto de partida los errores cometidos y que quedan registrados en las sentencias o en los conceptos que dan los jueces que dictan sentencia de los casos.

- Para futuros estudios sería conveniente proponer un protocolo basado en la experiencia de los servidores y crear una cartilla que sirva como medio de capacitación para las personas nuevas que se incorporen al grupo de investigación.
- Es importante establecer la relación estrecha que existe entre el término cadena de custodia y pilares de la seguridad de la información, pues allí se podría encontrar la clave para el diseño de los protocolos que se requieren para realizar la recolección de la evidencia digital.
- A modo de sugerencia, las personas que realizan los procedimientos mencionados deberían sistematizar sus experiencias y adelantar un estudio de seguridad de la información que les permita detectar riesgos y vulnerabilidades que redunden en la creación de protocolos ajustados a las necesidades y realidad nacional.

Referencias

Acosta, W. (2013). *Respuesta a incidente informático.* Universidad Piloto de Colombia: Colombia. WA Valencia - polux.unipiloto.edu.co.

Ariza, A. Ruíz, J y Cano, J. (2017). *iPhone3G: un nuevo reto para la informática forense.* Pontificia Universidad Javeriana: Colombia.

Cano, J. (2002). Conceptos y retos en la atención de incidentes de seguridad y la evidencia digital. *Revista de ingeniería.* Número 15. Universidad de los Andes: Colombia.

Hernández, R., Fernández, C. y Baptista, P. (2003). Metodología de la Investigación. México, D.F.: Mc Graw Hill.

Herrero, C. (1997). La investigación en análisis documental. Revista Educación y Biblioteca, 83, 44-46.

ISO/IEC 27037: 2012. Tecnología de la información - Técnicas de seguridad - Pautas para la identificación, recopilación, adquisición y preservación de pruebas digitales.

ISO/IEC NORMA TÉCNICA COLOMBIANA NTC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la Información (SGSI). Requisitos. Editada 2006-04-03. Bogotá: Colombia.

López, O. Amaya, H y León, R. (2002). *Informática forense: generalidades, aspectos técnicos y herramientas.* Universidad de los Andes: Colombia.

Mccumber, J. (1991). *Information Systems Security: A comprehensive model.* Computer Security Conference N° 14.

MINTIC. *Modelo de seguridad y privacidad de la información.* Guía N°13. https://www.mintic.gov.co/.../articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Ramírez, D. y Castro, E. (2018) en su *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia.* Repositorio Institucional UNAD: Colombia. http://hdl.handle.net/10596/17370.

Rendón, A. (2012). *La eficacia de la prueba digital en el proceso penal colombiano.* Repositorio institucional Universidad de Medellín: Colombia.

Roatta, S. Casco, M y Fogliato, G. (2015). *El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012.* Repositorio Institucional de la UNLP: Argentina.

Uyana, M. (2014). *Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos (CSIRT).* Repositorio Universidad de las fuerzas armadas ESPE. Maestría en gerencia y seguridad de riesgo: Ecuador.

Anexo 1

E1 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

El proceso no tiene inconsistencias el problema es la persona que manipula la evidencia y para el tratamiento se debe tener un manual, guías, instructivos y claro.

E2 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

- puede presentarse problemas a la hora de recolectar evidencias por que estas pueden dañarse, o alterarse lo que podría causar demandas por parte de la defensa por daño y alteración del sistema. para estos casos es necesario recolectar lo necesario y embalarlo de manera adecuada para garantizar la integridad del EMP.

E3 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

LAS INCONSISTENCIAS PRINCIPALMENTE SERIA EN EL TRATAMIENTO DE LA EVIDENCIAS YA QUE NO SE TIENE LA SUFICIENTE PRECAUCION EN EL MANEJO DE ESTE TIPO DE DISPOSITIVO EN CUANTO A QUE ESTOS NO SUFRAN GOLPES O MANTENER LOS EN UN SITIO ADECUADO

E4 Considero que presentan problemas al momento de realizar la identificacion de que información debe ser recolectada. En muchas ocasiones se recolecta información que al momento de ser analizada no se obtiene ningun resultado y se ha gastado tiempo hombre y maquina tiempo sin obtener un buen resultado adicionalmente los investigadores no son preparados para hacer recoleccion de evidencia digital este es muy importante debido que la evidencia digital se encuentra en cualquier variable dispositivo

E5 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

E5

* Porque la actividad de recolección no se ajusta a los procedimientos internacionales y no se cumple a cabalidad por mala e insuficiente documentación por falta de entrenamiento y experiencia de funcionario judicial que lo ejecuta.
* por la fragilidad de la evidencia digital

E6 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

R/ta/: Por falta de capacitación y Personal idóneo.
Por la Premura al momento de la Recolección
NO Existe un protocolo adecuado

E7 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

FALTA DE CONOCIMIENTO TÉCNICO DEL PERSONAL QUE REALIZA LA RECOLECCIÓN Y FALTA DE INTERES LAS ENTIDADES EN CAPACITAR A SUS FUNCIONARIO TEMAS ESENCIALES QUE SE REQUIEREN EN LA ACTUALI

E8 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

Porque no Hay una Buena capacitación a los funcionarios de policía Judicial, donde se enseñe, el Que, el como, el porque (si ocurrió), se debe recolectar una evidencia Digital
Esto conlleva A Que se recolecten elementos que no so

E9 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

Porq los conceptos no son claros y Presen muchas interpretaciones.

E10 ¿Porque considera que el proceso de recolección y/o tratamiento de la evidencia Digital presenta inconsistencias en el proceso judicial?

El proceso como tal, no presenta inconsistencias. Desde mi punto de vista, necesita ser Social