Revista Logos Ciencia & Tecnología, 15(1): 122-140 | Enero-abril, 2023
https://revistalogos.policia.edu.co:8443/index.php/rlct

Artículo de revisión

Revista Logos Ciencia & Tecnología
ISSN-L 2145-549X
ISSN 2422-4200 (en línea)

Investigación forense digital en entidades del Estado colombiano: acercamiento a la Ley 1952 de 2019

Forensic computing methodology in Colombian government institutions: an approach from Law 1952 of 2019

Metodologia de computação forense em instituições governamentais colombianas: uma abordagem a partir da Lei 1952 de 2019

Darling Stella Solano Oviedo[a] | Miguel Ángel Roldán Álvarez[b] | Héctor Fernando Vargas Montoya[*c]

a https://orcid.org/0000-0002-5754-1962 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia
b https://orcid.org/0000-0002-6160-0021 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia
c https://orcid.org/0000-0002-0861-2883 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia

- Fecha de recepción: 2022-10-26
- Fecha concepto de evaluación: 2022-11-03
- Fecha de aprobación: 2022-11-09

https://doi.org/10.22335/rlct.v15i1.1698

Para citar este artículo / To reference this article / Para citar este artigo: Solano Oviedo, D. S., Roldán Álvarez, M. A., y Vargas Montoya, H. F. (2023). Investigación forense digital en entidades del Estado colombiano: acercamiento a la Ley 1952 de 2019. *Revista Logos Ciencia & Tecnología*, *15*(1), 122-140. https://doi.org/10.22335/rlct.v15i1.1698

RESUMEN

Cuando se está en frente de un posible delito informático o una falta disciplinaria en donde se ha usado un medio digital (como medio o como fin) y que es objeto de investigación, se requiere de diferentes procedimientos para lograr hallar el qué, cómo, quién y cuándo sucedió el posible hecho punible o falta disciplinaria. Este artículo tiene como objetivo proponer un diseño de una metodología para el desarrollo de una investigación forense digital, para ello, el método utilizado fue hacer uso de procesos y métodos aceptados por la comunidad internacional, así como la adecuada gestión y tratamiento de la evidencia digital (cadena de custodia), de forma que sirva como una herramienta técnica de apoyo para procesos administrativos y disciplinarios que adelante una entidad del Estado colombiano en el marco de la Ley 1952 de 2019. Como resultado, se cuenta con una propuesta que puede ser usada para la aplicación del Código General Disciplinario en cuanto a la obtención de pruebas digitales, con lo cual, se concluye que los diferentes investigadores tienen a disposición una metodología que puede llevar resultados óptimos y con ello dar cumplimiento a la ley.

Palabras clave: cibercrimen, disciplinario, evidencia digital, informática forense, metodología.

ABSTRACT

In the face of a possible computer crime or disciplinary offense in which digital elements have been used (as a means or as an end) and that is the subject of investigation, different procedures are required to know what, how, who and when the possible punishable act has occurred. The objective of this paper is the design of a methodology for the development of a forensic investigation. For this, the method used were the processes and methods accepted by the scientific and technical community for the adequate management and treatment of digital evidence (chain of custody), in order to be a technical support tool for administrative cases in Colombian government institutions within the context of Law 1952 of 2019. As a result, there

* Autor de correspondencia. Correo electrónico: hectorvargas@itm.edu.co

is a proposal that can be used for the application of the General Disciplinary Code in terms of obtaining digital evidence, with which, it is concluded that the different researchers have at their disposal a process that can lead to optimal results, thereby comply with the law.

Keywords: cybercrime, digital evidence, forensics, methodology, disciplinary code.

RESUMO

Perante um eventual crime informático ou infracção disciplinar em que tenha sido utilizado um suporte digital (como meio ou como fim) e que é objecto de investigação, são necessários diferentes procedimentos para apurar o que, como, quem e quando ocorreu o ato punível. Este artigo tem como objetivo propor o desenho de uma metodologia para o desenvolvimento de uma investigação forense digital, para isso, o método utilizado foi fazer uso de processos e métodos aceitos pela comunidade internacional, bem como o adequado gerenciamento e tratamento de provas digitais (cadeia de custódia), para que sirva como ferramenta de apoio técnico para processos administrativos e disciplinares realizados por uma entidade do estado colombiano no âmbito da Lei 1952 de 2019. Como resultado, surge uma proposta que pode ser utilizada para a aplicação do Código Disciplinar Geral em termos de obtenção de provas digitais, com a qual se conclui que os diferentes investigadores dispõem de um processo que pode conduzir a óptimos resultados, com isso a cumprir a lei.

Palavras-chave: cibercrime, código disciplinar, evidência digital, computação forense, metodologia.

Introducción

En la actualidad, la gran influencia y dependencia del Internet en todos los aspectos de la sociedad es innegable. Desde la aparición de los computadores, en la década de los cuarenta, los paradigmas de nuestra vida han cambiado. El desarrollo posterior del Internet, a partir de los noventa, creó un punto de quiebre en la forma en que las personas venían accediendo a la información, productos y servicios.

De manera paralela a este avance tecnológico, ante la gran cantidad y tipo de información que hoy transita por la red de redes, así como la gran importancia que esta tiene tanto para las personas como para las organizaciones, se ha visto un incremento en la actividad criminal trasladada al ámbito digital. Frente a este panorama, el mundo se encuentra en un escenario de transnacionalización del delito, en donde los nuevos entornos generados por los procesos de globalización plantean nuevos retos para la seguridad digital que implican la implementación de estrategias de protección, que coadyuven a la efectiva defensa de las identidades digitales (CCIT, 2020).

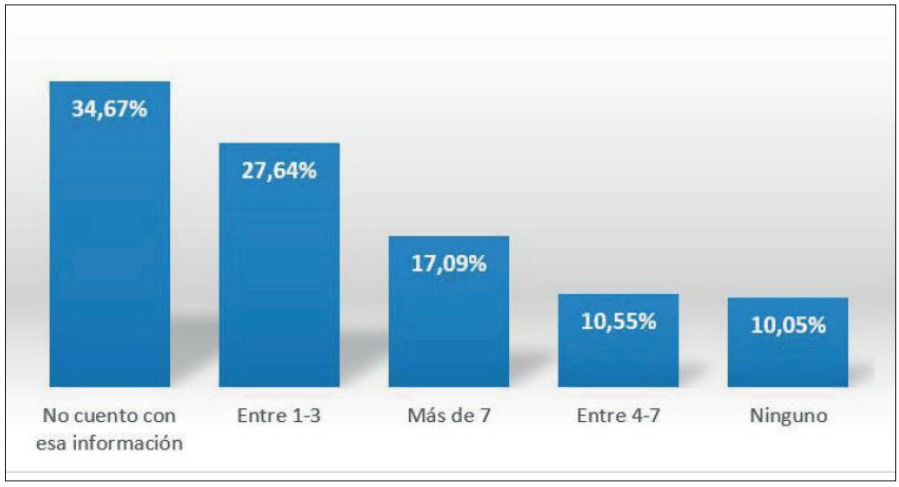
En los últimos tiempos, el crimen digital o cibercrimen ha tenido una evolución constante y exponencial, debido a que Internet y el ciberespacio son el escenario perfecto para su expansión. Este proporciona supuestas creencias de anonimato y de facilidad y rapidez de los actos; por otro lado, la inexperiencia de los usuarios finales, la dificultad del rastreo de actividades ilícitas, entre otras, que han propiciado que "delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación, con un alcance local, en la actualidad constituyan organizaciones trasnacionales complejas de cibercrimen" (CCP, 2017, p. 1).

Un informe sobre las tendencias de la cibercriminalidad en Colombia (CCIT, 2022), reveló que en el 2021 el número de incidentes reportados a las autoridades del ecosistema de ciberseguridad aumentó en un 21 % con relación al 2020. De esta manera, los delitos informáticos más denunciados ante las autoridades, presentan a la "violación de datos personales" en primer lugar, con un total de 13458 casos; le sigue el "acceso abusivo a sistemas informáticos", con 9926 casos; y en un tercer lugar, el "hurto por medios informáticos" (CCIT, 2022).

Ahora bien, es preciso tener en cuenta que los delitos informáticos reglamentados bajo la Ley 1273 de 2009 no solo afectan a la ciudadanía y al sector empresarial, también se ven afectaciones en el gobierno, el cual, según cifras (Almanza, 2022), es alarmante que el 35 % de las entidades encuestadas no cuenta con la información sobre los incidentes que pudo haber tenido (ver Figura 1).

Figura 1

Información sobre incidentes de seguridad



Nota. Cantidad de incidentes (Almanza, 2022).

En ese sentido, un delito informático tiene diferentes matices, ya que se considera que posibles delincuentes pueden hacer uso de diferentes estrategias para robar, dañar o exfiltrar información de algún medio informático, llegando a ejecutar ataques por canales encubiertos o por algún acceso directo, con lo cual, establecer una línea de actuación se convierte en vital para identificar y contrarrestar este tipo de actividades (Vargas *et al.*, 2022).

Por otro lado, la preocupación es más alta cuando la cantidad de empleados que están al frente de los temas de seguridad o ciberseguridad no son consistentes con las necesidades del medio o del mercado; en ese sentido, en el sector gobierno o sector público, el 5 % de las entidades con empleados entre 1001 y 5000 (Almanza, 2022), cuentan con personal de seguridad informática (de 1 a 5) y solo el 1.69 % tienen entre 11 y 15 empleados en esa área, siendo positivo que el 85 % de las entidades con 501-100 empleados, tienen de 6 a 10 funcionarios en temas de seguridad (ver Figura 2), las demás organizaciones tienen un déficit importante en personal especializado.

Figura 2

Tamaño de empresa vs. Número de empleados en seguridad

Tamaño de empresa:	**Tamaño del área / sector**				
Gobierno/sector público	**1 a 5**	**6 a 10**	**11a**	**más de 15**	**ninguno**
1001-5000 empleados	5,08%	0,00%	1,69%	0,00%	0,00%
501-100 empleados	3,39%	85,00%	0,00%	0,00%	0,00%
Mayor de 5001 empleados	0,00%	0,00%	0,85%	0,85%	0,00%
201-500 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
51-200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%

Nota. Relación área/sector. Tomado y ajustado de Almanza (2022).

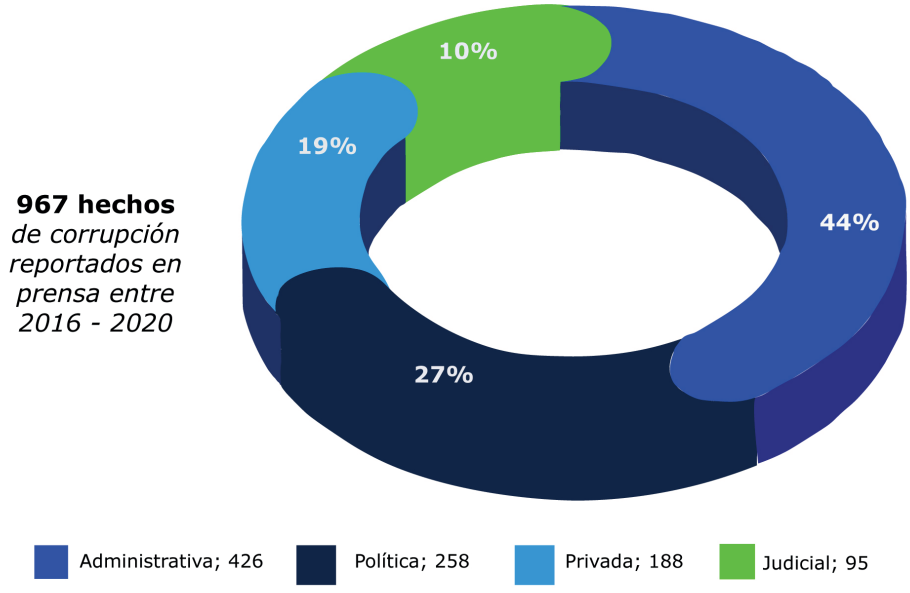
En consecuencia, de lo anterior es preciso tener en cuenta que, en el ámbito del Estado colombiano, las causas de dichos incidentes no solamente son de origen externo, sino también interno, en donde desempeña un papel importante la corrupción, lo que da origen a procesos que pueden tener implicación tanto desde la óptica penal como administrativa, específicamente desde el Código General Disciplinario o Ley 1952 de 2019 (el cual ha derogado la Ley 734 de 2002 y otras leyes asociadas). Dicha ley fija las pautas necesarias para llevar a cabo un proceso disciplinario a funcionario público, lo que crea una línea de seguridad en diferentes investigaciones.

En consideración de las diferentes violaciones que pueden ejecutar diferentes funcionarios, la Ley 1952 de 2019 en mención no establece claramente las pautas o procedimiento que deben ejecutarse para determinar si una falta disciplinaria o un delito informático pudo haber sido consolidado en algún recurso de una entidad del Estado, dejando abierta la posibilidad de que diferentes investigadores asuman un rol informático poco claro a la hora de recolectar evidencia digital para lograr demostrar el hecho, por lo cual se genera la pregunta: ¿Cómo diseñar y aplicar una investigación forense digital en entidades del Estado colombiano que dé cumplimiento a la Ley 1952 de 2019?

Según cifras de un informe emitido por el Monitor Ciudadano de la Corrupción (2021), entre el período comprendido entre enero de 2016 y julio de 2020, fueron reportados 967 hechos de corrupción en medios de comunicación y boletines oficiales de órganos de control, dentro de los cuales un alarmante 44 % corresponde a corrupción administrativa y 10 % judicial (ver Figura 3).

Figura 3

Tipos de hechos de corrupción

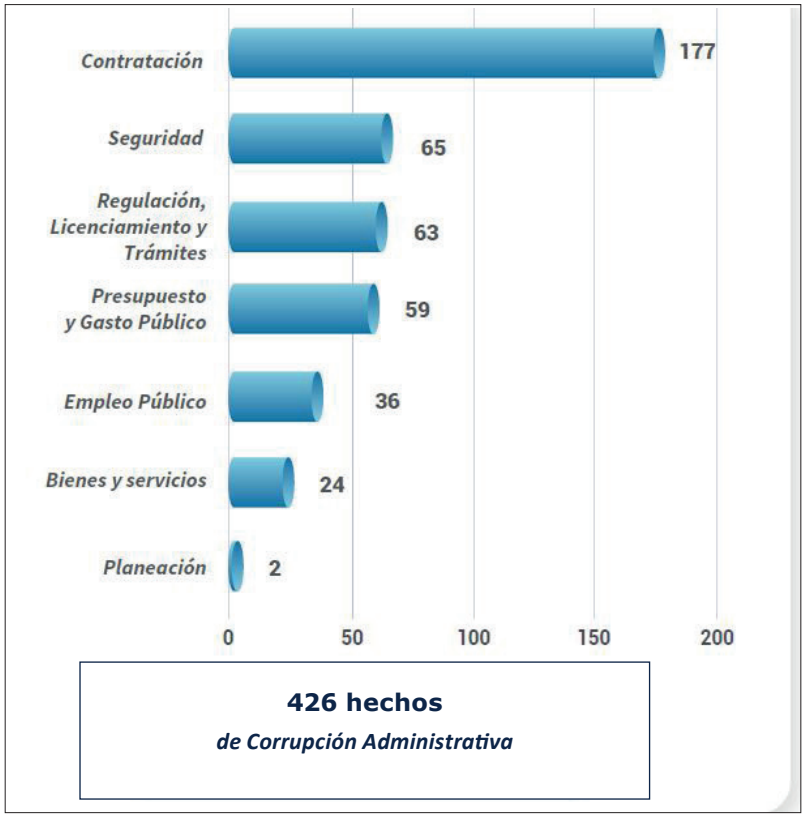


Nota. Reportes de prensa (Monitor Ciudadano de la Corrupción, 2021).

Es de resaltar que el ámbito de corrupción (ver Figura 4) tiene un alto índice en la contratación (41.5 %), seguido de los temas de seguridad (15.2 %) y regulación, licenciamiento y trámites con un 14.7 %.

Figura 4

Ámbito de corrupción administrativa



Nota. Hechos distribuidos. Tomado de Monitor Ciudadano de la Corrupción (2021).

En este contexto, cada día cobran mayor importancia las investigaciones disciplinarias, administrativas y/o penales apoyadas en la informática forense, ya que se convierten en una herramienta muy valiosa para la obtención, preservación y análisis de evidencia en ambientes digitales, los cuales son el escenario perfecto para la comisión de los delitos. Es así como la informática forense aprovecha su enfoque científico para ser un mecanismo de recolección, análisis, verificación y validación de todo tipo de información digital, en casos de fraudes, ataques o incidentes informáticos (Espinoza, 2019).

Sin embargo, se ha visto que el desarrollo de las investigaciones forenses digitales se enfrenta a múltiples desafíos, dado el rápido crecimiento de toda clase de dispositivos, el aumento en los volúmenes de información que deben recopilarse, almacenarse y analizarse, el surgimiento de nuevos paradigmas de crimen (cibercrimen), la falta de legislación que cobije todo tipo de investigación cuando sobrepasa los límites de las jurisdicciones legales, la débil capacidad del poder judicial para entender, interpretar y valorar la evidencia digital, son algunos de los retos más desafiantes de la informática forense (Haro, 2021).

En este mismo sentido, los investigadores forenses digitales se enfrentan a otro reto: implementar una metodología estandarizada que le dé validez y universalidad a sus hallazgos y que permita que los resultados de sus investigaciones sean de plena aceptación en procesos judiciales y/o administrativos (Haro, 2021).

En la literatura existen múltiples metodologías, *frameworks* o modelos para el desarrollo de investigaciones forenses digitales o investigaciones de informática forense. Muchos autores han planteado sus propias metodologías y han documentado la falta de un proceso estandarizado que permita conducir una investigación forense digital partiendo de postulados universalmente aceptados por la comunidad internacional (Haque y Hossain, 2017; Jain y Dhananjay, 2015).

En el contexto colombiano, el caso no es diferente; en la actualidad, solo existe un proceso parcialmente aplicable a las investigaciones forenses digitales y es el procedimiento relacionado con la cadena de custodia expedido por la Fiscalía General de la Nación, en donde se afirma que dicho procedimiento es parcialmente aplicable, debido a que está concebido para las investigaciones forenses en el plano físico y, aunque presenta algunas directrices para la gestión y manejo de evidencia digital, dicho procedimiento no comprende una investigación forense en su totalidad, sino que corresponde a solo una de sus fases: la recolección y tratamiento de la evidencia (Fiscalía General de la Nación, 2018).

Con base en lo anterior, se puede observar que, al analizar el Manual del Sistema de Cadena de Custodia de la Fiscalía General de la Nación, solo se encuentra referencia a la evidencia digital en el aparte "B. Esquema de formas de recolección, embalajes y recomendaciones prácticas para el manejo de EMP y EF" de la sección "9. Formas de recolección, embalajes y recomendaciones prácticas para el manejo de EMP y EF".

En consideración de los índices de corrupción ya indicados asociados al sector público, cobra vital importancia lo establecido en la Ley 1952 de 2019 o Código General Disciplinario (Congreso de la República de Colombia, 2019), el cual es la carta de navegación que deben emplear las entidades públicas para llevar a cabo un proceso administrativo o disciplinario y de la misma manera los procedimientos implementados por la Procuraduría General de la Nación, como ente rector del tema disciplinario en Colombia.

Finalmente, es necesario tener en cuenta que, en el contexto actual de la normativa colombiana, los procedimientos para el desarrollo de investigaciones forenses digitales no están reglados por ninguna ley o jurisprudencia nacional. Sin embargo, deben llevarse a cabo de la forma más estandarizada y científicamente posible, con el objetivo de que sus hallazgos sean lo suficientemente técnicos, coherentes, íntegros, transparentes y válidos, para que puedan ser presentados como material probatorio en estrados judiciales y en procesos administrativos y/o disciplinarios.

En el contexto disciplinario, las pruebas deben estar ajustadas a los requerimientos y características establecidos en la Ley 1952, en particular el título V, arts. 118 y 119, título VI – pruebas (diferentes articulados), así como el art. 185 sobre la cadena de custodia; sin embargo, la ley no hace alusión de cómo hacerlo o cuál debería ser el marco procedimental para la ejecución de la extracción de evidencia digital de cualquier componente tecnológico, lo que deja a los investigadores con un posible vacío a la hora de evidenciar una falta disciplinaria.

Los resultados presentados en este artículo ilustran el diseño de una metodología que puede ser usada por cualquier entidad del Estado colombiano, para llevar a cabo investigaciones forenses en las que se le dé un correcto tratamiento y gestión a la evidencia digital, con el objetivo de que estas sean un apoyo a los procesos administrativos y disciplinarios que se lleven en el marco de la Ley 1952 de 2019.

Método

El método usado para la obtención de los resultados se estructuró mediante un proceso de tres fases ilustradas en el siguiente esquema (ver Figura 5):

Figura 5

Método usado para la obtención de resultados

Nota. Las 3 fases ejecutadas dan como resultado un proceso adecuado para un análisis forense digital.

A continuación, se detallan de cada una de las etapas.

Fundamentación teórica

Con respecto a la fundamentación teórica, se hizo un levantamiento de la información documental relacionada con los conceptos básicos sobre la investigación forense digital y las metodologías existentes para el desarrollo de estas, con el propósito de identificar aquellas formalmente establecidas a nivel de diferentes países y entidades para su análisis (buenas prácticas). Para ello, se tuvo en cuenta procesos de países como Argentina (Ministerio de Seguridad de la Nación, 2016; Procuración General de la Nación, 2016), México (Banco de México, 2022), Australia (Ghosh, 2003), Reino Unido (Association of Chief Police Officers - ACPO, 2012) y EE. UU. (National Institute of Justice, 2004).

Con base en estas fuentes, se realizó una definición de los aspectos básicos principales sobre la investigación forense, con el fin de lograr una comprensión y análisis del tema que facilitara la identificación de los componentes que debe tener una buena metodología para el desarrollo de estas investigaciones, teniendo en cuenta el adecuado manejo de la evidencia digital. Igualmente, se tomaron dos normas internacionales para el análisis, a saber: la ISO/IEC 27037:2012 (International Organization for Standardization, 2012) y la NIST SP 800-86 (NIST, 2006) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés).

Del mismo modo, se realizó un sondeo a nivel nacional, para identificar la forma en que las entidades del orden penal, administrativo y disciplinario llevan a cabo las investigaciones forenses digitales. De esta forma, hizo parte del análisis, lo establecido por el Manual del Sistema de Cadena de Custodia (Fiscalía General de la Nación, 2018), el Manual Único de Policía Judicial (Fiscalía General de la Nación, 2018) de la Fiscalía General de la Nación, la Guía Nro. 13 – Evidencia Digital del Ministerio de Tecnologías de Información y las Comu-

nicaciones – MINTIC (MINTIC, 2016) y los procedimientos de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación (Procuraduría General de la Nación, 2019).

Dada la amplia información de ámbito nacional y regional, fue necesario establecer una serie de parámetros que permitieron conocer y seleccionar aquellas fuentes que puedan dar cumplimiento a la Ley 1952, para lo cual, dicha selección de los criterios fueron obtenidos desde la misma ley, considerando los arts. 111, 163, 182, 185 y 208, así como las reglas previstas en la Ley 600 de 2000; en consecuencia, los requisitos que deben cumplir las pruebas periciales en el ámbito disciplinario son los establecidos en el Título VI Pruebas, Capítulo III de la Ley 600 de 2000.

Como resultado de este análisis, se definieron los siguientes siete criterios a evaluar en las buenas prácticas ya relacionadas:

1. C1-Aspectos técnicos: la metodología analizada abarca aspectos técnicos de la investigación forense digital e involucra el desarrollo de análisis técnicos sobre la evidencia.

2. C2-Cadena de custodia: la metodología analizada da lineamientos para iniciar y mantener una apropiada cadena de custodia sobre los elementos de evidencia.

3. C3-Preservación de la calidad: la metodología analizada ofrece lineamientos y/o procedimientos que garanticen la preservación de la calidad de la información recolectada y de la evidencia hallada.

4. C4-Herramientas técnicas: la metodología analizada ofrece lineamientos que contemplan el uso de herramientas técnicas.

5. C5-Informe final y documentación: la metodología analizada presenta lineamientos específicos para la construcción y/o generación de un informe final que recopila los hallazgos; de igual forma, permiten la generación de documentación apropiada para cada fase del proceso forense.

6. C6-Proceso integral: la metodología analizada abarca el proceso forense desde la identificación de la evidencia hasta la presentación de resultados en el informe final.

7. C7-Principios:la metodología analizada asegura la conservación de los principios de la evidencia digital (Casey, 2011; Semprini, 2017).

Con el fin de seleccionar o dar prioridad a las buenas prácticas, a cada documento revisado se le dio la siguiente valoración numérica:

1. Cero (0): cuando la metodología analizada no cumple con el criterio en estudio.

2. Uno (1): cuando la metodología analizada cumple parcialmente con el criterio en estudio.

3. Dos (2): cuando la metodología analizada cumple completamente con el criterio en estudio.

Finalmente, se seleccionaron aquellas buenas prácticas con mejor puntaje que le pueda aportar a los resultados, para así, poder consolidar una metodología que tenga aplicabilidad en cumplimiento de la ley.

Sobre normativa colombiana

El siguiente paso y en línea con el paso anterior, fue el análisis de la normativa colombiana con el fin de identificar la existencia o ausencia de requerimientos formales relacionados con la seguridad informática y/o la informática forense en el compendio de leyes vigentes en Colombia y que puedan servir de apoyo a la Ley 1952.

Para lograr lo anterior, se realizó un proceso de clasificación y caracterización de la normativa vigente en el tema, teniendo en cuenta, como primer criterio de selección, la existencia o ausencia de artículos sobre temas relacionados con la seguridad informática (SI) y/o informática forense (IF); para ello, se construyó un resumen de la norma o normativa e indicó si estaba asociada a SI y/o IF.

En consecuencia, una vez seleccionadas las normas vigentes, se hizo un resumen de ellas y, acorde a su contexto, se indicó si estaban relacionadas con seguridad informática (SI) y/o informática forense (IF), con ello, lograr identificar qué legislación colombiana debe ser cumplida o apoya el proceso.

Finalmente, para el proceso de selección de normas, se estableció cuáles de ellas cumplían con los siete criterios de análisis definidos en la etapa anterior, así se logró comprender el apoyo general de la normativa colombiana en los temas de análisis forense digital.

Creación de la metodología propuesta

Con base en los resultados de las fases anteriores, se hace una propuesta de metodología para la investigación forense digital a ser aplicada a un caso de estudio, y con ello, validar qué tan funcional puede ser. La metodología propuesta establece diferentes parámetros que reúnen las buenas prácticas nacionales e internacionales, y que pueden ser aplicadas para dar cumplimiento a la ley.

Resultados

Acorde a lo indicado en el método, a continuación, se muestran los resultados obtenidos de cada una de las fases.

Fundamentación teórica

Al realizar la revisión de las diferentes normas o documentos gubernamentales, las que se seleccionaron como base para el desarrollo de este trabajo fueron aquellas que cumplieron completamente (calificación de 2) todos los criterios (calificación total de 14 puntos).

Tabla 1

Valoración comparativa final

Metodología / Criterio	ISO/IEC 27037	NIST SP 800-86	Argentina	México	Australia	US NIJ	Reino Unido	FGN	MINTIC	PGN
C1-Aspectos técnicos	0	2	2	0	2	2	2	1	2	1
C2-Cadena de custodia	2	2	2	2	2	2	2	2	2	2
C3-Preservación calidad	2	2	2	2	2	2	2	2	2	1
C4- Herramientas técnicas	0	2	0	0	0	2	1	1	2	1
C5- Informe final y documentación	1	2	1	2	1	2	1	1	1	2
C6- Proceso integral	1	2	1	2	2	2	2	1	2	1
C7- Principios de la evidencia digital	2	2	0	0	2	2	2	0	0	1
TOTAL	**8**	**14**	**8**	**8**	**11**	**14**	**12**	**8**	**11**	**9**

Nota. La comparación se hace entre varios países con gran relevancia para la valoración realizada.

En la Tabla 1 se detalla el comparativo de normas vs. criterios con la respectiva calificación, con lo cual, la norma NIST SP 800-86 resulta más ventajosa que la ISO/IEC 27037, toda vez que no se observan desventajas frente a los aspectos analizados en cada criterio. En consecuencia, cumple completamente todos los criterios de interés definidos para este proyecto, razón por la cual fue una de las normas seleccionadas para el diseño de la metodología propuesta.

Por otro lado, en el ámbito de gobiernos internacionales, la metodología establecida por EE. UU., a través del Instituto Nacional de Justicia del Departamento de Justicia (US-NIJ, por sus siglas en inglés), resulta más ventajosa que las definidas por los demás países. Asimismo, se identificó que los países latinoamericanos (Argentina y México) tienen una normativa básica para el desarrollo de las investigaciones forenses digitales, y se encuentran enfocadas principalmente en las acciones que deben realizar los primeros respondientes en las escenas donde se identifiquen elementos electrónicos que podrían contener evidencia digital.

Asimismo, países como Australia y Reino Unido presentan normas y estándares más robustos, los cuales, si bien abarcan todo el proceso forense, son de carácter general en algunos de los aspectos de interés de este proyecto.

Tabla 2

Cumplimiento de criterios de análisis – Normas entre 1999–2019

Criterios / Normatividad relacionada	C1		C2		C3		C4		C5		C6		C7	
	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No
Ley 906 de 2004 (Código de Procedimiento Penal)		X	X			X		X		X		X		X
Circular Externa SFC 052 de 2007		X		X		X		X		X		X		X
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)		X		X		X		X		X		X		X
Resolución CRC 3067 de 2011		X		X		X		X		X		X		X
Resolución CRC 3502 de 2011 (Neutralidad de Internet)		X		X		X		X		X		X		X
Ley 1581 de 2012 (Habeas Data)		X		X		X		X		X		X		X
Resolución 3933 de 2013 (Ministerio de Defensa Nacional)		X		X		X		X		X		X		X
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)		X		X		X		X		X		X		X
Resolución 5050 de 2016 (Comisión de Regulación de Comunicaciones)		X		X		X		X		X		X		X

C1 Aspectos técnicos
C2 Cadena de custodia
C3 Preservación calidad
C4 Herramientas técnicas
C5 Informe final y documentación
C6 Proceso integral
C7 Principios de la evidencia digital

Nota. Normativa relacionada. Basado en las Normas y leyes desde 1999 a 2019.

De manera similar, desde el punto de vista nacional, existen aproximaciones hacia las investigaciones forenses digitales en el ámbito penal, por parte de la Fiscalía General de la Nación (2018) y disciplinario (Procuraduría General de la Nación, 2019), estas aproximaciones no definen claramente el procedimiento a seguir frente a un proceso investigativo de esta índole. En ese sentido,

> todavía no existen procedimientos realmente unificados en Colombia, es más, en diversas unidades de análisis forenses no existen procedimientos documentados en absoluto, y si bien los investigadores suelen tener en claro las tareas que deben llevar a cabo, las mismas no están cristalizadas en algún documento estructurado (Asociación por los Derechos Civiles [ADC], 2018, p. 20)

Finalmente, no existe una metodología o buena práctica de análisis forense digital en Colombia que cumpla a cabalidad todos los criterios de interés.

Resultados de la normativa colombiana

Ahora bien, el análisis de la legislación colombiana permitió identificar la existencia de nueve elementos normativos (entre leyes, decretos, resoluciones y circulares) que contienen, al menos, un artículo relacionado directamente con la seguridad informática y/o la informática forense. Dado lo anterior, se infiere que en Colombia no existe la suficiente reglamentación de la práctica del análisis forense digital, lo que conlleva a que los actores involucrados en este tipo de investigaciones bajo la Ley 1952 deban implementar, a criterio propio, las metodologías y/o procedimientos que mejor se ajusten a sus necesidades, probablemente restándole valor a los posibles hallazgos a nivel probatorio ante cualquier investigación.

En la Tabla 2 se tiene el análisis comparativo de lo encontrado frente a los siete criterios de medición ya relacionada en la etapa 1. Si bien es cierto que se identificó que la Ley 906 de 2004 tiene artículos relacionados con uno de los criterios de análisis, específicamente la cadena de custodia, un análisis más detallado de la ley en cuestión permitió concluir que su aplicación está orientada principalmente a la evidencia física, mas no a la evidencia digital.

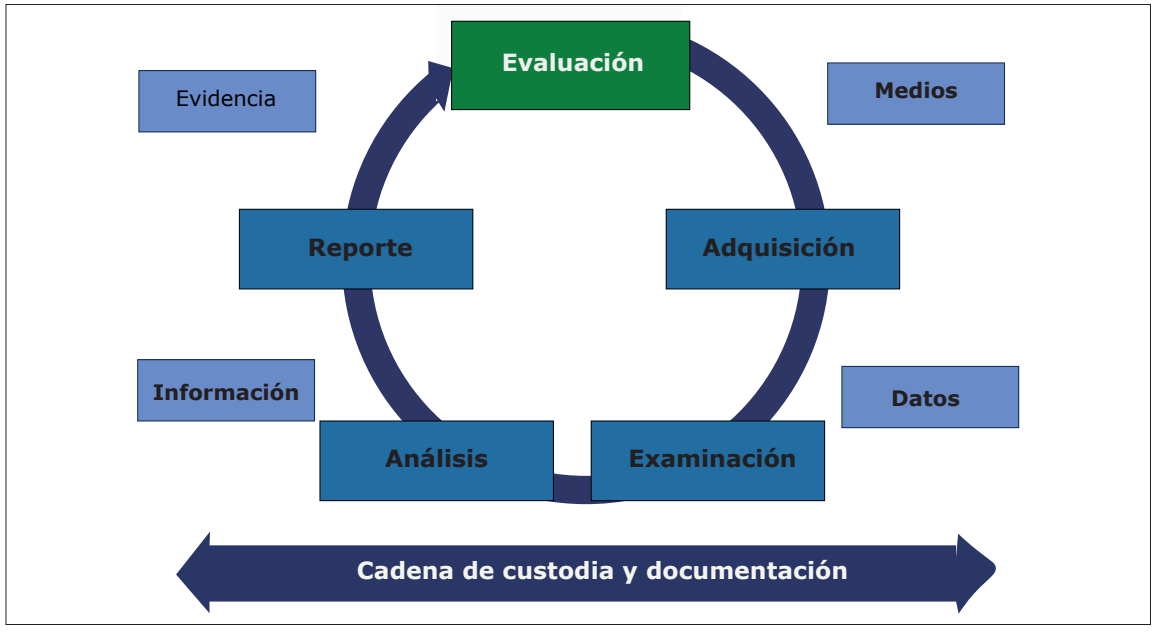
Propuesta de metodología

Para la creación de la metodología, se partió del análisis e integración de las buenas prácticas seleccionadas como resultado de la primera fase (dado que a nivel Colombia no existe una recomendación fuerte al respecto). Se propone un proceso para el análisis forense digital compuesto por cinco etapas: evaluación, adquisición, examinación, análisis y reporte (ver Figura 6).

Dicho proceso establece igualmente algunas recomendaciones entre etapas para tener en cuenta, con el propósito de obtener mejores resultados como lo son los medios usados para la adquisición, los datos recolectados, la información relevante que evidencia el hecho a investigar y la forma como se debe presentar la evidencia digital.

Figura 6

Metodología de investigación forense propuesta



Nota. El proceso de 5 etapas tiene el manejo de la cadena de custodia como transversal a todo.

Es importante precisar la necesidad de conservar los principios generales de la informática forense (Casey, 2011), que permiten generar un proceso investigativo fiable. Dichos principios son:

1. Intercambio de evidencia

La tarea de todo analista forense es descubrir vínculos convincentes entre el delincuente, la víctima y la escena del crimen, lo que permite considerar el principio de intercambio de Locard, que indica que, en cualquier contacto en una escena del crimen, siempre habrá evidencia de la interacción, aunque en algunas ocasiones esta no sea fácilmente detectable.

2. Características de la evidencia

Las posibles evidencias están entre dos categorías, (a) la llamada características de clase y (b) las características individuales. Las primeras son rasgos comunes en elementos similares, mientras que las segundas son más únicas y pueden ser vinculadas a una persona o actividad con mayor certeza.

El intercambio de evidencia digital a menudo implica una copia de los datos que se transfieren, dejando al original prácticamente inalterado. En consecuencia, el investigador forense digital debe concentrar sus esfuerzos en la identificación de evidencia con características tanto de clase como individual.

3. Solidez forense

Para que sea útil en una investigación, la evidencia digital debe preservarse y analizarse de manera apropiada desde el punto de vista forense. Uno de los puntos clave de la solidez es la documentación, siempre que el proceso de adquisición conserve una representación completa y precisa de los datos originales, y se puedan validar su autenticidad e integridad, generalmente se considera sólido desde el punto de vista forense.

4. Autenticación

La autenticación de la evidencia digital es un concepto que tiene muchos matices. En la mayoría de los casos, la autenticación se logra cuando se demuestra que la evidencia recuperada es la misma que los datos originalmente adquiridos, aunque puede variar si la evidencia es volátil y se tomó en un tiempo determinado (como el volcado de memoria RAM). Lo importante es lograr conservar adecuadamente la cadena de custodia.

5. Cadena de custodia

Uno de los aspectos más importantes de la autenticación es mantener y documentar la cadena de custodia de la evidencia. Sin una cadena de custodia sólida, podría argumentarse que la evidencia fue manejada de forma inapropiada y que podría haber sido alterada, reemplazada con evidencia incriminatoria o contaminada de alguna manera.

6. Integridad de la evidencia

El propósito de las verificaciones de integridad es demostrar que la evidencia no ha sido alterada desde el momento en que fue recolectada, apoyando así el proceso de autenticación, y esto se hace realizando una comparación de la huella digital (*hash*) tomada en el momento de la adquisición con la huella digital (*hash*) en su estado actual.

7. Objetividad

Una piedra angular del análisis forense es la objetividad. La interpretación y presentación de la evidencia debe estar libre de sesgos, para proporcionarle a los operadores disciplinarios y/o administrativos la visión más clara posible de los hechos.

8. Repetición

En el contexto de un análisis forense, es importante que el proceso se desarrolle de tal manera que permita su repetición tantas veces como sea requerido, ya que, en algunas ocasiones, puede ser necesario que un investigador forense deba repetir algunos o todos los análisis realizados por otro, especialmente, por parte de la defensa del implicado.

Partiendo de las cinco etapas ilustradas en la Figura 6, a continuación, se hace una breve explicación de cada una de estas.

1. Evaluación: el primer paso es evaluar las posibles fuentes de evidencia digital potencial con relación al alcance del caso.

2. Adquisición: debido a la naturaleza frágil y volátil de la evidencia digital, se deben implementar mecanismos que protejan y preserven la integridad de los datos. La implementación del procedimiento de cadena de custodia empieza en esta fase.

3. Examinación: acá se aplican procedimientos y técnicas forenses para extraer y/o recuperar la información de las evidencias adquiridas.

4. Análisis: en esta fase se interpretan los datos recuperados y se traducen a un formato legible. Se debe obtener información útil que dé respuesta a los planteamientos que dieron origen a la investigación.

5. Reporte: esta fase es la preparación del informe escrito con los hallazgos. La documentación es un proceso que debe ejecutarse en paralelo durante toda la investigación forense, dar explicación de las herramientas y procedimientos seleccionados, recomendaciones de otras acciones requeridas, entre otros. La documentación debe ser un reflejo coherente de la cadena de custodia, lo que supone tener un registro claro, detallado y preciso de todos los análisis realizados, las herramientas utilizadas y el personal involucrado en cada proceso. Los listados parciales de resultados arrojados por las herramientas forenses conforman parte de este grupo de registros documentales que deben custodiarse y anexarse al informe técnico final.

Asimismo, es necesario considerar la audiencia objetivo: un punto importante en la etapa de reporte es el conocimiento que se tenga sobre la audiencia a la cual se le presentarán los resultados o hallazgos del análisis. Los informes deben contener un lenguaje apropiado según los destinatarios finales de estos.

Finalmente, la metodología considera fundamental las lecciones aprendidas, dado que el proceso no es estático y puede ser flexible para la entidad que requiera realizar investigaciones forenses. Por lo tanto, luego de finalizado el análisis, resulta muy valioso que el equipo investigador realice una autoevaluación de todo el proceso llevado a cabo durante el desarrollo del apoyo técnico, considerando las fallas y aciertos.

Con respecto a la validación de la metodología creada, objeto de este trabajo, se valoró su aplicación en un caso de estudio que permitió validar los resultados obtenidos por un analista.

Para dicho caso de estudio, se tomó el de una universidad pública en Colombia, el cual es un caso que ya fue juzgado, por lo cual se hace un breve resumen: el Director Nacional de Investigaciones Especiales de la Procuraduría General de la Nación emite auto de pruebas dentro de un proceso disciplinario llevado en contra de un funcionario de una universidad pública de Colombia, para asegurar y extraer el disco duro del equipo asignado al investigado y, previa expedición de la orden jurisdiccional del señor Procurador General de la Nación, realizar el respectivo análisis forense para identificar la información relevante relacionada con el presunto uso de la tarjeta de crédito y cuenta corriente institucionales, en custodia del investigado, para costear gastos de orden privado y personal, no relacionados con los fines legítimos de esta, configurándose un presunto abuso de las funciones propias del cargo, peculado por apropiación, falsedad de documento, entre otras conductas disciplinables.

En consideración de la metodología, esta se ha desarrollado de la siguiente manera para resolver el caso:

1) Etapa 1: Evaluación

Una vez recibido el auto de asignación, se procedió a evaluar el caso con el fin de identificar las facultades legales otorgadas, las fuentes de evidencia digital potencial y determinar el mejor sitio para el procesamiento. En consecuencia, se consideró que se otorgó la facultad a los funcionarios de la Dirección Nacional de Investigaciones Especiales - DNIE con funciones de policía judicial para el aseguramiento de la evidencia.

El procesamiento del dispositivo adquirido se realizó en el Laboratorio de Informática Foren-

se de la Dirección Nacional de Investigaciones Especiales, en donde se cuenta con las herramientas (*hardware* y *software)* idóneas para las actividades de procesamiento y análisis.

2) Adquisición

Los objetivos de esta etapa son (1) el aseguramiento de los discos duros del equipo de cómputo, y (2) asegurar documentación relevante al caso, como material probatorio.

Se identificó el computador (ver Figura 7) marca LENOVO, color gris, referencia 210, serial Nro. PGO1MXXX, el cual se encontraba asignado al investigado.

Figura 7

Vista frontal computador Lenovo asignado al investigado

Nota. Es importante, dentro del proceso investigativo, documentar todos los elementos técnicos involucrados.

Se procedió a extraer el disco duro (ver Figura 8) de marca *WESTERN DIGITAL*, capacidad de 1 TB, interfaz Sata, serial Nro. WMCGYXXXXWEF.

Figura 8

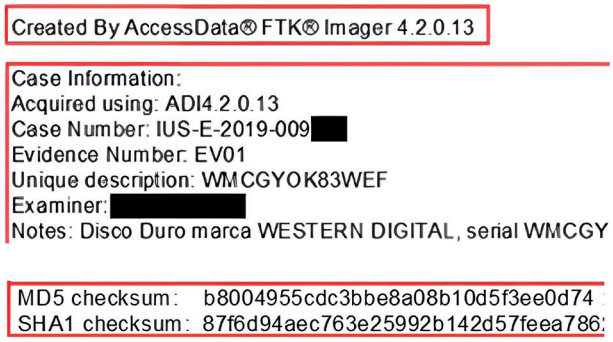
Vista disco duro WD serial No. WMCGYXXXXWEF

Nota. Captura de la evidencia física.

Como resultado de la adquisición (ver Figura 9), se obtuvo una (1) imagen forense de la información haciendo uso del software *AccessData FTK Imager* versión 4.2.0.13, y los respectivos códigos *hash* (MD5 y SHA-1).

Figura 9

Imagen del disco y validación de integridad



Nota. Los códigos *hash* o validación de la integridad son fundamentales para la evidencia.

3) Examinación

Dado que en esta etapa se hace la revisión de la información, fue necesario establecer algunas palabras claves, las cuales son buscadas en la imagen forense, palabras como "Avianca", "Banco Occidente", "Despegar", "Tornamesa", "Tullanta", entre otras; de igual manera, se realizó búsqueda en archivo de tipo imagen (jpeg, tiff, bpm, etc.), correo y Office.

4) Análisis

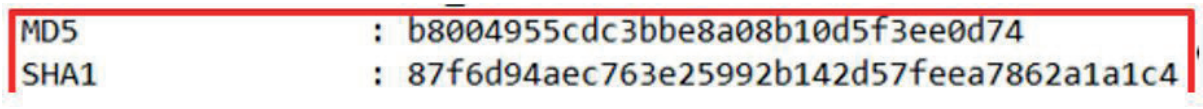
En esta etapa, se realizó el análisis y compilación de resultados del procesamiento de la imagen forense, con los siguientes hallazgos:

- Archivos gráficos: 16 archivos con extensión .jpg
- Documentos *Office*: 28 archivos y 14 archivos .PDF protegidos con contraseña.

A cada uno de los elementos le fue revisada su integridad (cadena de custodia) a través de los respectivos códigos *hash* (ver Figura 10).

Figura 10

Códigos hash de los archivos extraídos



Nota. Es necesario que estos códigos queden identificados en los informes, dado su importancia para la validación de integridad.

En los diferentes archivos PDF se encontraron extractos bancarios que dan cuenta de compras por fuera de lo reglamentario, así como correos electrónicos hacia/desde almacenes de lujo, concesionarios y otros servicios.

Es claro que, dentro de las etapas ya abordadas, haciendo uso de las búsquedas selectivas de datos e información, se logró obtener posible evidencia que demuestra una falta disciplinaria (considerando que las palabras claves fueron encontradas en la imagen forense generada).

5) Reporte

En consideración de la audiencia objetivo, el informe técnico se redactó de forma comprensible y sencilla para el público objetivo, correspondiente al operador disciplinario y la defensa del investigado (abogados y personal jurídico), considerando los siguientes ítems:

- Objeto del informe,
- Alcance,
- Metodología,
- Documentos técnicos soporte del informe,
- Análisis y concepto técnico, incluyendo todas las evidencias recolectadas, y
- Conclusiones del proceso investigativo.

Una vez entregado el reporte, fue necesario establecer, desde la Ley 1952 de 2019, cuál o cuáles son los hechos punibles disciplinarios que el funcionario debe afrontar, con lo cual, el uso de la informática forense es clave.

Ahora bien, con respecto a la conservación de los principios generales de la informática forense, la metodología propuesta da cumplimiento a estos, considerando el intercambio de evidencia y las características de esta, al obtener una copia de la evidencia original; asimismo, la solidez forense y la autenticación, considerando que los archivos extraídos y analizados dan cuenta de una posible falta disciplinaria. De igual forma y considerando uno de los procesos fundamentales, tanto la cadena de custodia y la integridad de la evidencia se conserva a través de la obtención de los códigos *hash* de verificación, concentrando todos los esfuerzos en la objetividad de lo solicitado.

Discusión

Contar con procedimientos técnicos, que le permitan al sector público establecer una línea de actuación frente a diferentes investigaciones disciplinarias o administrativas, es fundamental en consideración de que, si bien existen leyes como la Ley 527 de 1999: Ley de Comercio Electrónico, Ley 1273 de 2009: Ley de Delitos Informáticos, Ley Estatutaria 1581 de 2012, entre otras, Colombia no cuenta con una legislación fuerte que permita realizar un proceso de informática forense, lo que lo pone en desventaja con respecto a países de la región.

Al dar cumplimiento al Código General Disciplinario o Ley 1952 de 2019 en cuanto a las investigaciones disciplinarias, considerando que la legislación no aborda la investigación forense como mecanismos de apoyo, se hace difícil demostrar la ocurrencia de una falta cuando la tecnología sirve como medio o como fin.

La ejecución de la metodología en el caso de estudio permitió conocer cómo, a partir de un procedimiento estructurado, se puede obtener evidencia digital en el marco de ley, en consideración de que el caso ya fue juzgado, se aprove-

cha la oportunidad para mostrar la importancia de contar con una estrategia clara a la hora de enfrentarse a un proceso disciplinario que esté de por medio la tecnología y, en ese sentido, sentar las bases para la investigación forense digital en entidades del Estado.

Asimismo, la cadena de custodia es un proceso fundamental, que permite establecer la integridad de los datos a través de todo el proceso investigativo y hasta su culminación; con ello, desde la misma etapa de "adquisición", es necesario obtener los respectivos códigos *hash*, los cuales permiten en el tiempo, la validación de la respectiva integridad de datos y, en ese sentido, se da cumplimiento al art. 185 de la Ley 1952 sobre la cadena de custodia.

Las etapas de "adquisición" y "análisis" constituyen un hito importante, toda vez que acá se coteja la información buscada de forma digital (a través de las herramientas tecnológicas) con el objetivo de la investigación, descartando o aceptando la evidencia digital respectiva que logre demostrar el hecho punible, con lo cual se daría cumplimiento al título V, arts. 118 y 119, título VI de la ley sobre la recolección de pruebas y el cuidado que debe tenerse en su adquisición y resguardo.

Por otro lado, en la construcción del informe, es imprescindible que este se haga de una forma clara, consecuente y transparente para diferentes públicos lectores, dado que, de acuerdo al proceso investigativo, dicho informe puede estar en manos de personas no técnicas adscritas a la Procuraduría General de la Nación o algún juzgado (dependiendo de las fases investigativas); con lo cual, el personal destinatario del informe podrá constatar el procedimiento ejecutado y comprender las conclusiones o hallazgos finales del análisis forense digital.

En comparación con otros trabajos desarrollados, se ha propuesto un modelo que tiene aplicabilidad en lo penal dentro del Reino Unido, abarcando diferentes procesos de la investigación forense, pero muy generalizado en su diseño, lo que supone establecer una serie de procedimientos para llevarlos a una organización específica y, con ello, buscar su aplicabilidad y posibles resultados positivos (Montasari, 2017).

De manera similar, el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE, por sus siglas en inglés *Scientific Working Group on Digital Evidence*), ha venido estableciendo diferentes metodologías de cómo realizar un análisis de evidencia digital como una disciplina forense (SWGDE, 2015). El grupo SWGDE ha publicado una serie de apartados y documentos para la adquisición, examen y evaluación de evidencia digital para la computación forense, lo que supone una buena estrategia para extraer procedimientos a implementar, lo que sugiere un esfuerzo importante para ajustarse a la ley colombiana.

Finalmente, en revisión del Estado colombiano, se deben tener en cuenta los procesos establecidos por la Procuraduría General de la Nación (2019), como máxima entidad rectora del proceso disciplinario en Colombia, con respecto a la posible ejecución de investigaciones técnico-científicas haciendo uso de la informática forense. Dicha entidad ha definido seis procedimientos para dichas pruebas técnicas, planteando: 1) realizar imágenes forenses, 2) recolectar datos volátiles, 3) tratamiento, procesamiento y análisis de evidencia digital, 4) tratamiento, procesamiento y análisis de dispositivos móviles, 5) recuperación de información de medios de comunicación y fuentes abiertas, 6) verificación y revisión de software, bases de datos y documentos electrónicos. Sin embargo, si bien es cierto que dichos procedimientos tienen diferentes lineamientos a realizar, no se evidencia una estructura técnica o metodológica para llevar a cabo una correcta investigación forense, dejando en manos del investigador, la ejecución de pasos de la mejor manera.

Conclusiones

En este artículo, se presentó el desarrollo de las actividades conducentes al diseño de una metodología para la realización de investigaciones forenses digitales en entidades del Estado, como apoyo a procesos administrativos y/o disciplinarios en el marco de la Ley 1952 de 2019.

Teniendo en cuenta todos los aspectos mencionados anteriormente, fue posible diseñar la metodología para la realización de investigaciones forenses digitales, mediante un proceso

de cinco etapas, en las cuales se abarca una investigación forense digital, desde la recepción del caso, hasta el reporte de hallazgos y/o resultados, pasando por la identificación de los tipos y fuentes de evidencia digital potencial, la adquisición de los elementos y su posterior examinación y análisis.

En este sentido, y con el objetivo de validar la utilidad de la metodología propuesta, se realizó su aplicación en un caso de estudio práctico, lo que permitió evaluar el grado de dificultad en la aplicabilidad de cada una de las etapas de la metodología, a través de la observación directa de su ejecución. Asimismo, comprender que, si no se tiene un procedimiento de actuación, es difícil obtener resultados confiables ante una investigación.

Sin embargo, también se identificaron algunas dificultades con el desarrollo de ciertas actividades de análisis, asociadas al desconocimiento en el uso de algunas técnicas forenses, lo que resulta en una oportunidad de mejora para que el personal adscrito a la DNIE se someta a entrenamiento y capacitación de estas.

En comparación con las normas para la ejecución de análisis forense, la metodología acá propuesta se ha diseñado para el cumplimiento de la ley, conteniendo todos los pasos para que un investigador, cuando se enfrente a elementos tecnológicos, pueda generar valor con respecto a los posibles hallazgos ante faltas disciplinarias, con lo cual el personal de la Procuraduría General de la Nación tendría un proceso alineado con buenas prácticas internacionales para la adquisición de evidencia digital.

Finalmente, la metodología que acá se presenta contiene procedimientos formales para el desarrollo de investigaciones forenses digitales, en el cual se incluyen los principios generales del peritaje, se abarca el proceso desde la evaluación de la evidencia hasta el reporte final de hallazgos y resultados y se encuentra ajustado a la normatividad general colombiana para la práctica probatoria. De esta forma, se garantiza que las investigaciones forenses practicadas utilizando la metodología propuesta tienen solidez probatoria para efectos de un proceso disciplinario y/o administrativo en el marco de la Ley 1952 de 2019.

Como trabajo futuro, se propone establecer un plan de acción para llevar a cabo la implementación formal de la metodología; si bien se ejecutó bajo un caso de estudio real con unos resultados muy positivos, es necesario articular la estrategia para que sea tenida en cuenta de manera formal y reglada para otros casos que se presenten.

Referencias

Almanza, A. (2022). *XXII* Encuesta Nacional de Seguridad Informática: Aprendiendo del futuro de la ciberseguridad. *ACIS Sistemas*, (163), 20-82. https://sistemas.acis.org.co/index.php/sistemas/article/view/186

Asociación por los Derechos Civiles [ADC]. (2018). *La investigación forense informática en América Latina. Argentina: Asociación por los Derechos Civiles* - ADC. https://adc.org.ar/wp-content/uploads/2019/06/037-la-investigacion-forense-informatica-en-america-latina-vol-2-04-2018.pdf

Association of Chief Police Officers [ACPO]. (2012). *ACPO Good Practice Guide for Digital Evidence. United Kingdom: Association of Chief Police Officers - ACPO*. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Banco de México. (2022). *Decálogo Forense Digital.* https://www.banxico.org.mx/sistema-financiero/d/%7B631B6BC5-FAFA-A0EC-C464-7D1A7A-753D95%7D.pdf

Cámara Colombiana de Informática y Telecomunicaciones [CCIT]. (2020). *Tendencias del cibercrimen en Colombia 2019-2020.* https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Cámara Colombiana de Informática y Telecomunicaciones [CCIT]. (2022). *Tendencias del cibercrimen (2021-2022), nuevas amenazas al comercio electrónico.* https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

Casey, E. (2011). *Digital evidence and computer crime, forensic science, computer and the Internet*. Elsevier Inc. https://books.google.es/books?hl=es&lr=&id=lUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Digital+evidence+and+computer+crime,+forensic+science,+computer+and+the+Internet.+Elsevier+Inc.&ots=aLu8HjATWf&sig=AwHi8PifrUkbQzDaej-7c6J-dnI

Centro Cibernético Policial [CCP]. (2017). *Amenazas del Cibercrimen en Colombia 2016-2017*. https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Congreso de la República de Colombia. (1999, 18 de agosto). *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.* Diario Oficial Nro. 43673. http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso de la República de Colombia. (2000, 24 de julio). *Ley 600 de 2000. Por la cual se expide el Código de Procedimiento Penal*. Diario Oficial Nro. 44097*.* http://www.secretariasenado.gov.co/senado/basedoc/ley_0600_2000.html

Congreso de la República de Colombia. (2004, 31 de agosto). *Ley 906 de 2004. Por la cual se expide el Código de Procedimiento Penal*. Diario Oficial Nro. 45658*.* http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 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 Nro. 47223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial Nro. 48587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República de Colombia. (2019, 28 de enero). *Ley Nro. 1952 de 2019. Código General Disciplinario*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=90324

Espinoza, M. (2019). Informática forense: una revisión sistemática de la literatura. *ReHuSo: Revista de Ciencias Humanísticas y Sociales, 4*(2), 12-128. https://doi.org/10.33936/rehuso.v4i2.1641

Fiscalía General de la Nación. (2018). *Manual del Sistema de Cadena de Custodia. Fiscalía General de la Nación*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

Fiscalía General de la Nación. (2018). *Manual Único de Policía Judicial*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

Ghosh, A. (2003). *Guidelines for the Management of IT Evidence.* https://www.saiglobal.com/pdftemp/previews/osh/as/misc/handbook/hb171.pdf

Haque, M., y Hossain, S. (2017, 7-9 de diciembre). *National digital forensics framework for Bangladesh* [Conference]. Electrical Information and Communication Technology (EICT)], Khulna, Bangladesh. https://ieeexplore.ieee.org/document/8275133

Haro, F. (2021). Crimen, cibercrimen y análisis forense informático. *Scientia Omnibus Portus, 1*(1), 1-18. https://dialnet.unirioja.es/servlet/articulo?codigo=8180667

International Organization for Standardization [ISO]. (2012). *ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html

Jain, N., y Dhananjay, K. (2015, 15-17 de febrero). *Digital forensic framework using feedback and case history keeper* [conferencia]. International Conference on Communication, Information & Computing Technology (ICCICT). IEEE, Mumbai, India. https://ieeexplore.ieee.org/document/7045670

Montasari, R. (2017). Testing the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM). *Technology for Smart Futures. Springer Link*, 303-327. https://dx.doi.org/10.1007/978-3-319-60137-3_15

Ministerio de las Tecnologías de la Información y las Comunicaciones [MINTIC]. (2016). *Seguridad y privacidad de la información*. *Guía Nro. 13. Evidencia Digital*. https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Ministerio de Seguridad de la Nación Argentina. (2016). *Resolución 234/2016: Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm

Monitor Ciudadano de la Corrupción. (2021). *Así se mueve la corrupción. Radiografía de los hechos de corrupción en Colombia 2016-2020*. https://www.monitorciudadano.co/documentos/hc-informes/2021/Radiografia-2016-2021.pdf

National Institute of Justice, U.S. Department of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

NIST. (2006). *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response*. https://csrc.nist.gov/publications/detail/sp/800-86/final

Procuración General de la Nación Argentina. (2016). *Resolución 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital*. https://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2016/04/PGN-0756-2016-001.pdf

Procuraduría General de la Nación Colombia (2019). *Procedimientos de Investigación Técnico Científica*. https://www.procuraduria.gov.co/portal/Mapa-de-procesos-component.page#postfind

Scientific Working Group on Digital Evidence [SWGDE]. (2015). *SWGDE Best Practices for Computer Forensic Acquisitions*. https://athena-forensics.co.uk/wp-content/uploads/2019/01/SWGDE-Best-Practices-for-Computer-Forensic-Acquisitions-042518.pdf

Semprini, G. (2017). El Análisis integral de la evidencia digital [conferencia]. SID, Simposio Argentino de Informática y Derecho, Córdoba, Argentina. 1(1), 88-99. http://sedici.unlp.edu.ar/bitstream/handle/10915/65212/Documento_completo.pdf-PDFA.pdf?sequence=1

Vargas, H., Vallejo, C. y Ruiz, C. (2022). Fuga de información por ultrasonido: un delito sobre datos personales. *Revista Logos Ciencia & Tecnología*, *14*(3), 102-116. https://doi.org/10.22335/rlct.v14i3.1618