Metodología para la investigación forense en entidades del Estado colombiano dando un adecuado tratamiento y gestión de la evidencia digital, como apoyo a procesos administrativos en el marco de la Ley 734 de 2002

Darling Stella Solano Oviedo

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2020

Metodología para la investigación forense en entidades del Estado colombiano dando un adecuado tratamiento y gestión de la evidencia digital, como apoyo a procesos administrativos en el marco de la Ley 734 de 2002

Darling Stella Solano Oviedo

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:
Magíster en Seguridad Informática

Director:
Magíster Andrés Alberto Gómez Acosta
Codirector:
Magíster Miguel Ángel Roldán Álvarez

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2020

“La ausencia de evidencia no es evidencia de ausencia”.

Eoghan Casey

Agradecimientos

Gracias a Dios por llenarme siempre de bendiciones y permitirme alcanzar esta meta. Una vez más afirmo y agradezco ser una de las “hijas favoritas de Dios”.

A mi familia y a mis padres, por confiar en mí y apoyarme en cada decisión y proyecto. Especialmente a mi madre, quien cambió su vida por acompañarme, cuando decidí seguir el camino que me trajo a donde estoy hoy.

A mis profesores y compañeros, familia del ITM, quienes compartieron sus conocimientos y experiencias durante los últimos dos años, despertando la creatividad, motivando el aprendizaje integral y estimulando siempre el trabajo en equipo.

A mis compañeros de la Procuraduría General de la Nación, por recibirme en su equipo y contar siempre con todo su apoyo para el desarrollo de este trabajo de grado.

¡Muchas gracias!

Resumen

En la actualidad las investigaciones forenses digitales son una herramienta indispensable en la lucha contra la ciberdelincuencia y su forma de acción: el cibercrimen, ya que pueden ofrecer una estrategia confiable y transparente para demostrar los delitos. Sin embargo, los investigadores forenses se enfrentan a innumerables retos cada día, debido a múltiples factores entre los que se encuentran la gran variedad de dispositivos que se utilizan para cometer los delitos, los diferentes tipos de ataques cada vez más sofisticados, la amplia cobertura de estos, el anonimato que ofrecen las herramientas del ciberespacio, entre muchos otros.

Uno de esos retos que hacen que las investigaciones de la informática forense sean poco confiables o valoradas al momento de exponerlas ante estrados judiciales o administrativos es la falta de protocolos o metodologías que permitan darle validez a sus hallazgos y que puedan determinar de manera inequívoca e indiscutible la forma cómo sucedieron los hechos y quién o quiénes fueron los responsables.

Es por esto por lo que surge la necesidad de este trabajo, en donde se diseñó una metodología que permite el desarrollo de una investigación forense mediante el uso de procesos y métodos aceptados por la comunidad científica y técnica para la adecuada gestión y tratamiento de la evidencia digital, de forma que sirve de apoyo para procesos disciplinarios y/o administrativos que adelante una entidad del Estado colombiano en el marco de la Ley 734 de 2002.

Para lograr el objetivo planteado se analizaron diversas metodologías propuestas por reconocidos autores del campo, por entidades técnicas y científicas y gobiernos de países con amplia experiencia en el área para evaluar y seleccionar las mejores prácticas que se ajustaran al contexto normativo y legal colombiano, para finalmente proponer una metodología acorde con las necesidades del entorno organizacional del país.

Palabras clave: digital, evidencia, forense, investigación, metodología.

Abstract

Nowadays digital forensic investigations are an indispensable tool in the fight against cybercrime since they can offer a reliable and transparent strategy to prove crimes. However, forensic investigators face countless challenges every day, due to multiple factors including the wide range of devices used to commit crimes, the different types of attacks becoming increasingly sophisticated, the wide coverage of these crimes, the anonymity offered by cyberspace, among many others.

One of those challenges that make digital forensic investigations unreliable or poor valued in judicial or administrative instances is the lack of protocols or methodologies that increase the evidentiary value of their findings and give them a unique way to determine how events occurred and who was responsible.

That is the primary reason for this research, where we designed a methodology that allows the development of a digital forensic investigation through the use of processes and methods accepted by the scientific and technical community for the proper handling and treatment of digital evidence, in order to be supportive for disciplinary and administrative issues carried out by a Colombian governmental institution under Law 734 of 2002.

To achieve the stated objective we analyzed different methodologies proposed by renowned authors in the field, by technical and scientific institutions and governments from countries with wide experience in the area, to assess and select the best practices that fit the Colombian legal context, in order to finally propose a methodology according to the needs of the country's organizational environment.

Keywords: digital, evidence, forensics, investigation, methodology.

Contenido

Lista de figuras

Lista de tablas

Introducción

El presente documento se encargará de plasmar los resultados del trabajo de investigación consistente en “Diseñar una metodología que permita el desarrollo de investigaciones forenses de tipo “post mortem” en entidades del Estado colombiano mediante el uso de buenas prácticas nacionales e internacionales, con el fin de dar un adecuado tratamiento y gestión de la evidencia digital, como apoyo a procesos administrativos y/o disciplinarios en el marco de la Ley 734 de 2002”.

Para lograr el objetivo anterior, se desarrollaron tres (3) objetivos específicos que, en conjunto, permitieron dar solución a la problemática planteada. En primer lugar, se buscó “identificar las metodologías o modelos existentes en el ámbito nacional y/o internacional para el desarrollo de investigaciones forenses, teniendo en cuenta sus alcances, ventajas, desventajas, similitudes y diferencias”.

Luego, se realizaron las actividades necesarias para “caracterizar las exigencias de ley en Colombia con relación a la seguridad informática y/o la informática forense, con el fin de determinar los aspectos fundamentales que deben hacer parte de una metodología para el desarrollo de investigaciones forenses digitales, de manera que se oriente el diseño ajustado a la normatividad nacional”.

Finalmente, la última fase de la investigación fue “validar la aplicación de la metodología propuesta en un caso de estudio donde se requiera el desarrollo de una investigación forense, aplicando un adecuado tratamiento y gestión de la evidencia digital”.

Desde la aparición de los computadores, en la década de los años cuarenta, los paradigmas de la vida de las personas han cambiado. El auge posterior del Internet, a partir de los años 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 fluye por la red y el alto valor 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 contexto de transnacionalización del delito, en donde los nuevos escenarios 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 [1].

En la actualidad 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 características particulares como el anonimato, la facilidad y rapidez de los actos, la inexperiencia de la mayoría 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" [1].

Un informe sobre las tendencias de la cibercriminalidad en Colombia [2] reveló que en el 2019 el número de incidentes reportados a las autoridades del ecosistema de ciberseguridad aumentó en un 54% con relación al 2018.

Los delitos informáticos más denunciados ante las autoridades en el país presentan al "Hurto por medios informáticos" en primer lugar, con un total de 31.058 casos; le sigue la "violación de datos personales", con 8.037 casos y en un tercer lugar se encuentra "acceso abusivo a sistema informático", con 7.994 casos [2]. En la Figura 1 se ilustran los cinco (5) delitos más denunciados.

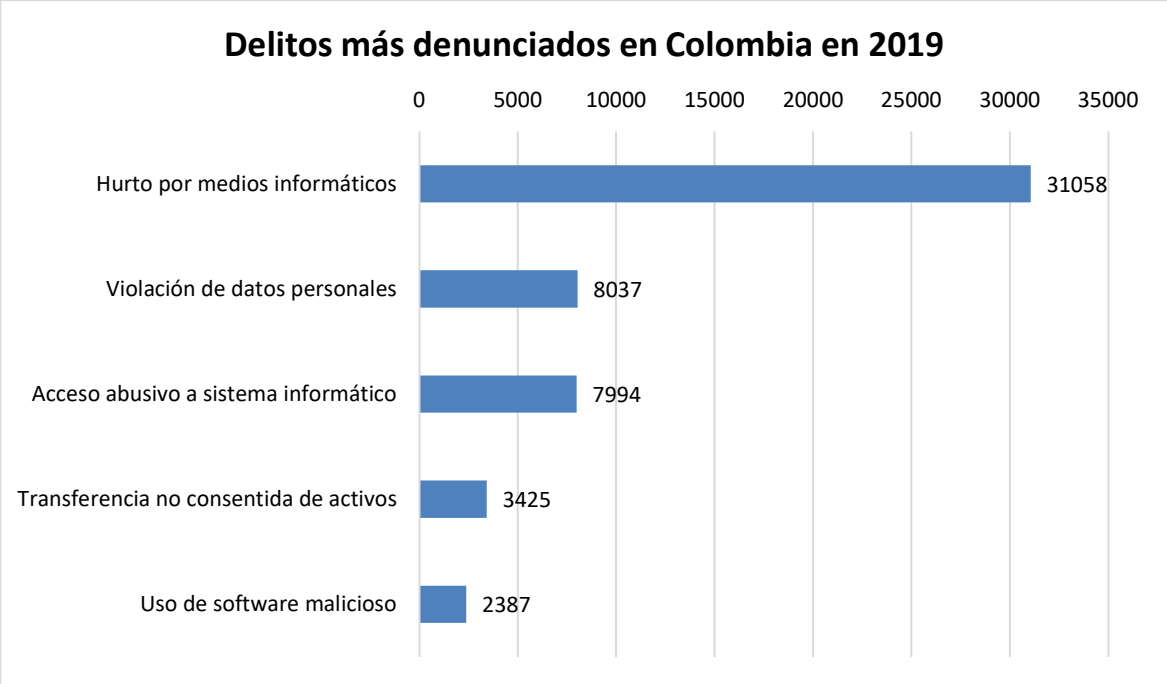


Figura 1: Delitos más denunciados en Colombia en el 2019.
Nota. Fuente: Elaboración propia a partir de [2]

De igual forma, el informe relaciona las ciudades de Colombia que presentan la mayor cantidad de incidentes, en donde se observa que "la concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados.

Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades" [2].

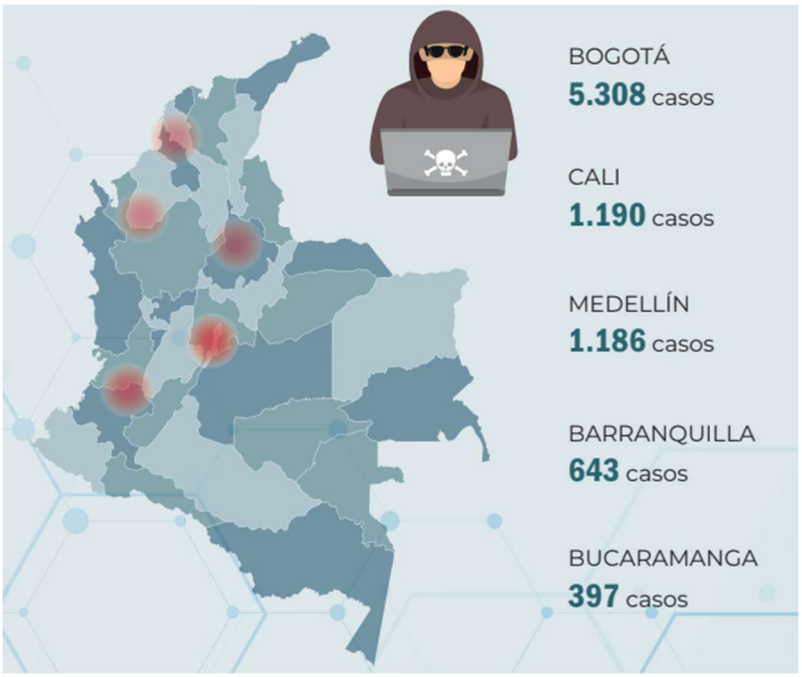


Figura 2: Ciudades con mayor afectación de cibercriminalidad
Nota. Fuente: [2]

Finalmente, el informe señala las tendencias que seguirán los cibercriminales durante el 2020, las cuales se han visto confirmadas y hasta excedidas, debido a la situación global que se generó con ocasión de la pandemia por COVID-19. El cibercrimen ha sofisticado su actuar delictivo y ha utilizado las circunstancias globales y las capacidades tecnológicas disponibles a su favor.

Figura 3: Tendencias del cibercrimen para el año 2020
Nota. Fuente: [2]

Ahora bien, es preciso tener en cuenta que los delitos informáticos no solo afectan a la ciudadanía y al sector empresarial, también se ven afectaciones en el gobierno el cual, según cifras de Almanza [3], en el año 2018 presentó incidentes de seguridad en un 54% de las entidades de gobierno o el sector público, cifra que resulta alarmante. Pero, igualmente alarmante resulta el hecho de que el 35% de las entidades del Estado, no cuenta con la información sobre los incidentes que pudo haber tenido. (Figura 4).

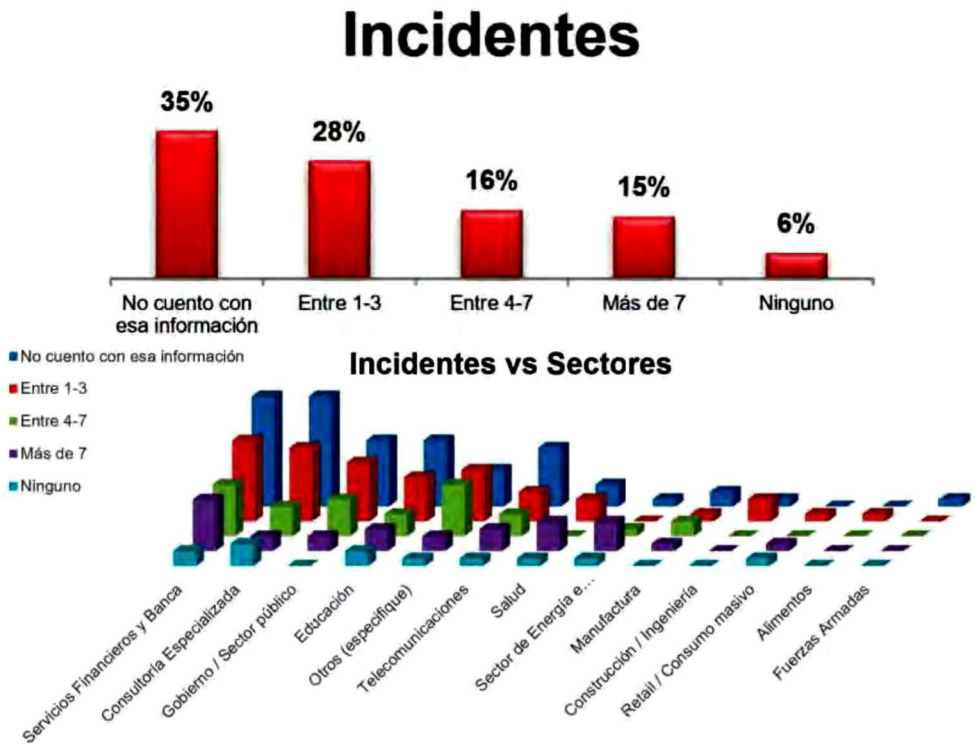


Figura 4: Incidentes de seguridad vs Sectores afectados
Nota. Fuente: [3]

Al respecto, 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 juega 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 Disciplinario Único o Ley 734 de 2002.

Según cifras de un informe emitido por el Monitor Ciudadano de la Corrupción [4], en el período comprendido entre enero de 2016 y julio de 2018, fueron reportados 327 hechos de corrupción en medios de comunicación del país y boletines oficiales de órganos de control, dentro de los cuales un alarmante 73% corresponde a corrupción administrativa (Figura 5).

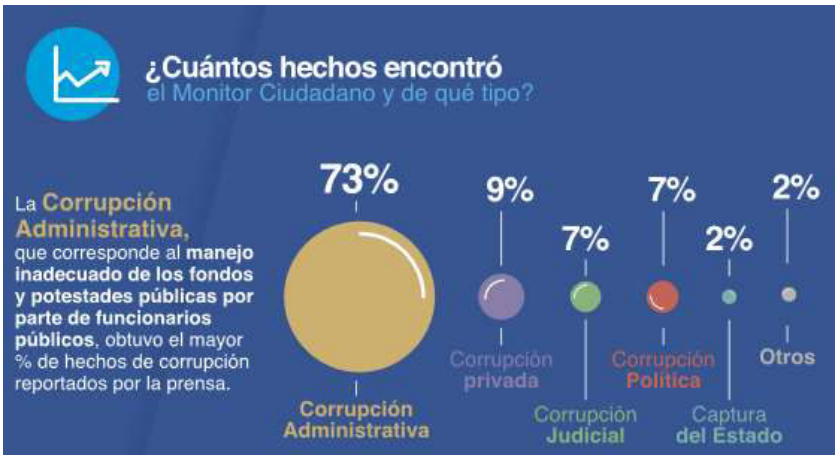


Figura 5: Tipos de hechos de corrupción reportados por Monitor Ciudadano
Nota. Fuente: [4]

Es de resaltar que los actores involucrados en la mayoría de los hechos reportados en el informe tienen como protagonistas a funcionarios públicos, en 39% de los casos, y a mandatarios elegidos por votación popular, en un 30%, como se observa en la Figura 6.

Figura 6: Actores de la corrupción
Nota. Fuente: [4]

Del mismo modo se destaca del informe, que de estos hechos se desprendieron 920 investigaciones, de las cuales un 71% fue de tipo penal, un 21% de tipo disciplinario y un 8% fueron de tipo fiscal, como se evidencia en la Figura 7.

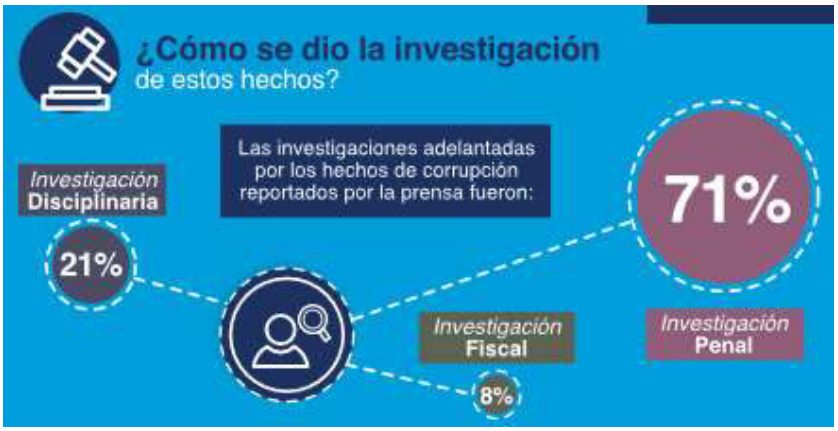


Figura 7: Tipos de investigaciones que se dieron
Nota. Fuente: [4]

En este contexto, cada día cobran mayor importancia las investigaciones disciplinarias, administrativas y/o penales con base 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, en casos de fraudes, ataques o incidentes de seguridad, debido especialmente a que este tipo de evidencia no puede ser descubierta utilizando mecanismos convencionales, sino con el uso de herramientas y mecanismos especializados [5].

Sin embargo, en la actualidad el desarrollo de las investigaciones forenses digitales se enfrenta a múltiples desafíos. 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 como el conocido como CaaS – Crimen como Servicio (por su sigla en inglés: Crime as a Service), la falta de legislación que cobije todo tipo de investigación cuando sobrepasa los límites de las jurisdicciones legales, son algunos de los retos más desafiantes de la informática forense [6].

Aunado a lo anterior, 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.

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 [7], [8], [9], [10], [11], [12].

En el contexto colombiano el caso no es diferente. En la actualidad solo existe un proceso parcialmente aplicable con relación a las investigaciones forenses digitales y es el procedimiento relacionado con la cadena de custodia expedido por la Fiscalía General de la Nación [13]. 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.

Lo anterior se puede observar al analizar el Manual del Sistema de Cadena de Custodia de la Fiscalía General de la Nación [13] en donde 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”.

Por otro lado, nuestro país está continuamente afectado por el flagelo de la corrupción, lo cual se puede ver reflejado en el descenso de Colombia en el Índice de Percepción de la Corrupción, calculado anualmente por Transparencia Internacional [14]. En el informe publicado en febrero de 2019, el país cae de 37 puntos a 36, de un total de 100, y desciende del puesto 96 al 99 entre los 180 países evaluados por la medición. Según la metodología de la medición, entre menos puntaje se le asigna a un país, más alto es su nivel de corrupción percibida. Lo anterior, aunado a las cifras de alta corrupción administrativa mostradas previamente, hace que cada día se incremente el número de investigaciones disciplinarias contra servidores públicos y personas naturales que ejercen funciones públicas, en las cuales también se ha incrementado el uso o participación de dispositivos electrónicos o el Internet. En este escenario cobra vital importancia lo establecido en la Ley 734 de 2002 o Código Disciplinario Único [15], 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 el país.

Finalmente, es necesario tener en cuenta que en el contexto actual de la normatividad 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, transparentes y válidos 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 734 de 2002, específicamente en el Título IV, artículos 128 al 142.

El documento presenta de manera secuencial el cumplimiento de los objetivos, iniciando por un marco teórico que fundamenta el trabajo realizado, para luego presentar la caracterización normativa que dio origen a la metodología propuesta, el diseño de esta y finalmente su validación en un caso de estudio. Por último, se entregan conclusiones, recomendaciones y trabajo futuro.

1. Marco Teórico y Estado del Arte

1.1 Cibercrimen o delito informático

Los computadores, las redes y en general, casi que cualquier dispositivo electrónico, se han vuelto ubicuos para la sociedad, de forma que se han convertido en parte de la vida diaria de todas las personas. En este contexto, las posibilidades de realizar actividades delictivas o criminales han venido tomando un nuevo camino, trasladándose al ámbito digital. En ese orden de ideas, resulta pertinente entrar a definir conceptos como cibercrimen o delito informático.

La empresa de seguridad Avast define en su sitio web[1] el cibercrimen como "cualquier actividad criminal que es llevada a cabo usando los computadores o el internet. El cibercrimen utiliza herramientas como el phising, los virus, spyware, ransomware y la ingeniería social para violar la ley" [16].

Por su parte, Panda Security lo define como "un crimen donde un computador es el objeto del crimen o es utilizado como una herramienta para cometer una ofensa. Un cibercriminal puede usar un dispositivo para acceder a la información personal de un usuario, información confidencial de empresas, información gubernamental o deshabilitar un dispositivo. También es un cibercrimen vender u obtener la anterior información en línea" [17].

Figura 1-1: Tipos de cibercrimen
Nota. Fuente: [18]

[1] Disponible en: https://www.avast.com/c-cybercrime

Existen 3 categorías principales para el cibercrimen o ciberdelito, dependiendo del tipo de "objetivo" al que le apuntan. Estas son: orientados a la propiedad, individuales y hacia el gobierno. Los tipos de métodos utilizados para cometer los delitos y los niveles de dificultad varían dependiendo de la categoría [17].

> *"Orientados a la propiedad: Es similar a su instancia en la vida real, en donde el criminal se apropia ilegalmente de la cuenta bancaria o los detalles de la tarjeta de crédito de un individuo. El criminal (hacker o similar) roba los datos bancarios personales para obtener acceso a los fondos, hacer compras en línea o realizar estafas de phising para que las personas entreguen su información. También pueden utilizar software malicioso para obtener acceso a páginas web que contengan información confidencial.*
>
> *Individuales: Esta categoría de cibercrimen involucra a un individuo distribuyendo en línea información maliciosa o ilegal. Puede incluir el ciber acoso, pornografía o pornografía infantil y el tráfico de drogas.*
>
> *Hacia el gobierno: Es el cibercrimen menos común, pero es el más serio y peligroso. Un crimen en contra del gobierno también es conocido como ciber terrorismo. El cibercrimen hacia el gobierno incluye el hackeo de sitios web gubernamentales, militares o distribuir panfletos y amenazas contra los estados. Estos criminales normalmente son terroristas o gobiernos enemigos de otras naciones"* [17].

Cada día más y más criminales están explotando la velocidad, conveniencia y anonimato que ofrece el internet para cometer una diversa variedad de actividades criminales que, hoy en día, no conocen fronteras, ya sea físicas o virtuales. La INTERPOL [18] reporta que en el pasado el cibercrimen era cometido principalmente por individuos o grupos pequeños, pero hoy se observan redes cibercriminales altamente complejas, que reúnen individuos a lo largo y ancho de la Tierra en tiempo real, para cometer crímenes a una escala sin precedentes.

Dada la naturaleza inherentemente transnacional del cibercrimen, es altamente probable que la evidencia de las actividades criminales esté presente a través de varias jurisdicciones, lo que dificulta la realización de las investigaciones de estos delitos. Por otro lado, actualmente muchas organizaciones o agencias de ley no tienen las capacidades para llevar a cabo los análisis de los datos que se requieren para estas investigaciones o no tienen acceso a la información de las amenazas en tiempo real, lo que puede tener un alto impacto en la seguridad de los ciudadanos y la infraestructura [18].

Como consecuencia de lo mencionado anteriormente, hoy en día cualquier investigación, disputa legal o administrativa, en ámbitos industriales, comerciales o estatales, probablemente involucrará algún tipo de evidencia digital. Dispositivos como computadores de escritorio, portátiles, dispositivos de almacenamiento, dispositivos de red, entre otros, pueden contener evidencia forense digital.

1.2 Informática forense y evidencia digital

En el contexto planteado, surge una rama de las ciencias forenses enfocada en la recolección, tratamiento y análisis de este nuevo tipo de evidencia: la informática forense.

La informática forense se define como el proceso de examinar metódicamente medios computacionales en busca de evidencia. Un análisis profundo de un examinador habilidoso puede llevar a la reconstrucción de las actividades de un usuario de un computador o dispositivo. En otras palabras, se trata de la recolección, preservación, análisis y presentación de evidencia digital, la cual puede ser útil en casos criminales, disputas civiles y procesos relacionados con recursos humanos u otros administrativos [19].

De manera similar, en [20], definen la informática forense como "la ciencia de ubicar, extraer y analizar tipos de datos de diferentes dispositivos, que los especialistas luego interpretan para servir como evidencia legal".

Una definición formal dada por el US-CERT [21] establece a la informática forense como "la disciplina que combina elementos legales y de la ciencia computacional para recolectar y analizar datos de sistemas de cómputo, redes, comunicaciones inalámbricas y dispositivos de almacenamiento, de forma que sean admisibles como evidencia en una corte".

De esta forma es notable que las definiciones de diversos autores coinciden en un aspecto en común: la evidencia digital, la cual es el punto clave fundamental de todo el proceso forense. Es importante tener en cuenta que, de acuerdo con lo planteado en [22], la evidencia digital ha pasado por un proceso de maduración a lo largo de los últimos 15 años, dado que esta disciplina no empezó en los laboratorios forenses, sino que los computadores que eran tomados como evidencia, eran analizados por oficiales de policía y detectives que tenían algún interés, habilidades o experiencia en informática. De esta manera, con el pasar de los años, este proceso se ha vuelto más rutinario y en la actualidad es sujeto al mismo rigor y expectativa de cualquier otro campo de la ciencia forense [22].

En consecuencia, aún permanecen 3 retos pendientes [22]:

- La comunidad de la evidencia digital no tiene un programa de certificación universalmente aceptado o una lista de habilidades y cualificaciones para los peritos forenses digitales.
- Algunas agencias aún tratan la examinación de la evidencia digital como una actividad investigativa, en vez de una actividad forense.
- Hay una amplia variabilidad e incertidumbre acerca de los estudios, experiencia y entrenamiento de aquellos que practican esta disciplina.

Al respecto, vale la pena mencionar algunas definiciones sobre evidencia digital que hacen ciertos autores; en [23]:

> *"Es una denominación usada de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional, que puede ser utilizado como prueba en un proceso legal y se refiere a la información contenida dentro de un elemento físico electrónico"* (p. 11).

En [24] se afirma que la evidencia digital "es un tipo de evidencia física, está constituida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" (p. 21).

Se destaca la definición establecida en [25] en los Lineamientos para la Administración de Evidencia IT (Guidelines for the Management of IT Evidence) en la cual precisan que la

evidencia digital es “cualquier información, que sujeta a intervención humana o semejante, ha sido extraída de un computador. La evidencia digital debe estar en una forma legible para los humanos o poder ser interpretada por personas que tengan habilidades en la representación de tal información con la ayuda de un programa informático” (p. 9).

Por su parte, el Departamento de Justicia de los Estados Unidos por intermedio del Instituto Nacional de Justicia [26], define la evidencia digital como:

> *“La evidencia digital es información y datos de valor para una investigación que es almacenada, recibida o transmitida por un dispositivo electrónico. Esta evidencia es adquirida cuando los datos o dispositivos electrónicos son incautados y asegurados para su análisis.*
>
> *La evidencia digital—*
> - *Está latente, como las huellas digitales o el ADN.*
> - *Cruza fronteras jurisdiccionales de forma rápida y sencilla.*
> - *Se altera, daña o destruye fácilmente.*
> - *Puede ser sensible al tiempo”* (p. ix).

A nivel nacional, es preciso hacer referencia a la Ley 527 de 1999 [27], la cual define y reglamenta el acceso y uso de los mensajes de datos, y a partir de la cual empieza a tener validez la evidencia digital como material probatorio en el ordenamiento jurídico colombiano. De esta forma, en su artículo 2, la mencionada ley define:

> *“ARTICULO* [sic] *2o. DEFINICIONES. Para los efectos de la presente ley se entenderá por:*
>
> *Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax; (…)”*

Por otro lado, el artículo 10 es el que reconoce la fuerza probatoria de la evidencia digital en términos de “mensaje de datos”:

> *“ARTICULO* [sic] *10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.*
>
> *En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo* [sic] *hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original”.*

Lo anterior se conoce como “principio de equivalencia funcional” el cual está definido por la Real Academia de la Lengua Española como “*la no discriminación jurídica de los mensajes de datos electrónicos respecto de los contenidos en papel u otro soporte*” [28].

A diferencia de la evidencia física, la evidencia digital tiene unas características específicas que la hacen muy valiosa para cualquier tipo de investigación, pero que a su vez representan retos y/o desafíos para su recolección, preservación y manipulación. Algunas de estas características son:

- Es fácilmente duplicable de manera exacta, conservando todas las propiedades de la original.
- Con las herramientas adecuadas es fácil determinar si la evidencia fue alterada, al compararla con la original.
- En la mayoría de los casos, es posible recuperar la información aún si esta fue borrada.
- Debido a las características propias de los sistemas, en la mayoría de las circunstancias, cuando se trata de destruir la evidencia, existen copias en otras ubicaciones del sistema.

Finalmente, en [29] se realiza un análisis de lo establecido por la norma ISO/IEC 27037:2012 “Guía para la identificación, recolección, adquisición y preservación de evidencias digitales”, resaltando los tres principios fundamentales a los que hace referencia esta norma sobre la evidencia digital: relevancia, confiabilidad y suficiencia. Estos principios definen la formalidad que debe guardar cualquier investigación que tenga como base la evidencia digital, con el fin de garantizar que esta sea admisible en cualquier proceso investigativo (p. 92).

La relevancia es una condición jurídica que tiene que ver con los elementos pertinentes al hecho que se investiga, con el objetivo de probar o no alguna hipótesis planteada al respecto. Todo lo que no cumpla dicho requisito se considerará irrelevante y, en consecuencia, excluido del material probatorio (p. 92).

Ahora bien, la confiabilidad busca la validación de la capacidad de repetición y auditoría de cualquier proceso que sea aplicado para obtener una evidencia digital. En otras palabras, con esta característica se busca garantizar que, si se repite el mismo proceso, se deben obtener los mismos resultados, siendo estos verificables y comprobables (p. 92).

El tercer principio es la suficiencia, el cual hace referencia al grado de completitud de las pruebas informáticas. Tiene relación con el hecho de que las evidencias recolectadas y analizadas contienen los elementos suficientes que permitan sustentar las hipótesis de la investigación. Se destaca que este principio está estrechamente vinculado con la experiencia y formalidad del profesional encargado (p. 92).

1.2.1 Tipos de análisis forense digital

Ahora bien, es preciso entrar a definir las formas en las que puede realizarse el análisis de las evidencias digitales:

- Análisis post-mortem: Este tipo de análisis se conoce también como análisis en frío [30]. Se realiza principalmente con equipos dedicados especialmente para la informática forense. En un contexto de incidentes de seguridad se traduce a que este ya ha terminado y el equipo o red afectadas se encuentran apagados. Generalmente se lleva a cabo en laboratorios especializados con las características de hardware y las herramientas de software necesarias para el análisis [31].

- Análisis en caliente: Llamado también análisis online [30] es aquel que recoge pruebas y se lleva a cabo con el sistema afectado aún encendido, con el ataque en marcha. “El análisis se realiza en el equipo que se presume fue violentado o que ha sufrido algún incidente de seguridad. Para este caso se recomienda utilizar un medio de almacenamiento que contenga diferentes herramientas de análisis forense compiladas de tal forma que no modifiquen en ninguna manera el sistema comprometido. Luego de terminar el análisis en caliente, debe realizarse el análisis post-mortem” [31].

1.3 Metodologías en el ámbito de la informática forense

Uno de los aspectos que les da mayor validez a las investigaciones forenses es el uso de métodos y procedimientos rigurosamente científicos que le den soporte a los hallazgos. Por lo tanto, el uso de una metodología estructurada es fundamental para los procedimientos forenses. En [32] se establece que el término “metodología” está “compuesto de los vocablos griegos methodos, procedimientos, y logos, tratado, se transforma en una disciplina que estudia, analiza, promueve y depura el método, mismo que se va multiplicando y particularizando de conformidad con las ramas de las disciplinas científicas existentes” (p. 90).

En otras palabras, la metodología se encarga del análisis de la lógica que sustenta los métodos o procedimientos, con el fin de verificar su efectividad y eficacia, validar la fortaleza de los planteamientos que sustenta y la coherencia que posee para producir conocimiento relevante. Una metodología estudia los elementos de cada método o procedimiento, teniendo en cuenta su origen, fundamentación, razonabilidad y, en definitiva, el modo que se estructuran cada una de las fases que comprende para la generación de resultados. En palabras del autor:

> *“Si los métodos tienen pasos, reglas y procedimientos para llevar a cabo la manipulación inteligente de la realidad categorizada como problema, la metodología se encamina a su análisis y comprensión, con el fin de verificar sus fortalezas y debilidades. La aportación de la metodología se orienta por el lado de incursionar la eficiencia de los métodos cuando se aplican en el trabajo de investigación”* [32].

Realizando una abstracción de los planteamientos de [32] para el ámbito de aplicación de este trabajo, es posible afirmar que una metodología para el análisis forense consiste en una serie de procedimientos estructurados, los cuales han sido fundamentados y validados tomando como base el método científico, como forma de obtener resultados científicamente eficaces en una investigación.

1.4 Nociones sobre derecho disciplinario en Colombia

Teniendo en cuenta que el ámbito de aplicación de la metodología que se desarrolló en este trabajo es el proceso disciplinario en entidades del Estado en Colombia, resulta pertinente mencionar algunos conceptos que fundamentan el derecho disciplinario en el país.

Según la jurisprudencia colombiana “el Derecho Disciplinario comprende el conjunto de normas sustanciales y procesales en virtud de las cuales el Estado asegura la obediencia, la disciplina y el comportamiento ético, la moralidad y la eficiencia de los servidores públicos, con miras a asegurar el buen funcionamiento de los diferentes servicios a su cargo” [33].

De otra manera, es posible afirmar que se trata de una rama esencial del derecho que permite vigilar el funcionamiento del Estado, a través de la regulación del comportamiento de los servidores públicos y particulares que desempeñan funciones públicas, fijando los deberes y obligaciones que tienen según sus responsabilidades, así como también las faltas y sanciones correspondientes. En palabras de Martha Isabel Castañeda Curvelo, Viceprocuradora General de la Nación (2009 – 2016), “la función disciplinaria garantiza que la conducta de los servidores públicos y de los particulares que ejercen funciones públicas se adecúe a los fines y funciones del Estado, con acciones encaminadas a prevenir y corregir comportamientos que los transgredan” [34].

De esta forma, la acción disciplinaria en Colombia se encuentra en cabeza de la Procuraduría General de la Nación, representada por el Procurador General, quien constitucionalmente es el supremo director del Ministerio Público [35]. Al respecto, en [36] se resalta que “la acción disciplinaria se produce dentro de la relación de subordinación que existe entre el funcionario y la Administración en el ámbito de la función pública y se origina en el incumplimiento de un deber o de una prohibición, la omisión o extralimitación en el ejercicio de las funciones, la violación del régimen de inhabilidades, incompatibilidades, etc., y su finalidad es la de garantizar el buen funcionamiento, moralidad y prestigio del organismo público respectivo (esto es) la potestad disciplinaria ha de ejercerse con atención a los principios de la función administrativa y del servicio público, como a los fines esenciales del Estado” [36].

Es así como, ante el comportamiento fuera de lo reglado por parte de cualquier funcionario público, se da inicio a procesos disciplinarios que siguen el mismo rigor de cualquier investigación, ya sea en el ámbito penal o administrativo. Estos procesos se rigen por lo establecido en la Ley 734 de 2002, Código Disciplinario Único, la cual contiene los derechos, deberes, prohibiciones, impedimentos, inhabilidades, incompatibilidades y conflictos de intereses de los servidores públicos; de igual forma definen las faltas disciplinarias, las sanciones y el procedimiento que debe seguirse para su aplicación [34].

1.5 Estado del arte

En la literatura se ha documentado a nivel internacional la falta de protocolos o metodologías estandarizadas para llevar a cabo las investigaciones en informática forense. Tal necesidad se ha visto abordada por diversos autores entre los que se destaca el trabajo realizado en [11] en donde se desarrolló un estudio sobre la preparación forense digital (Digital Forensic Readiness - DFR). En este trabajo los autores realizan un análisis del contexto de las organizaciones y su grado de preparación para lo que llaman DFR (por sus siglas en inglés). Definen la DFR como el plan “pre-incidente” que se encarga de manejar la habilidad de una organización para maximizar el uso de la evidencia digital ante un posible incidente, y su capacidad de anticiparse a una situación que podría terminar en la corte. El análisis de diversas iniciativas organizacionales los llevó a concluir que la

inadecuada investigación técnica y las limitaciones de la legislación, conllevan a una necesidad creciente de contar con mecanismos de preservación de evidencia y estándares que permitan la realización de investigaciones forenses en cualquier momento requerido.

De manera similar, en [12] los autores exponen la falta de guías comprensivas y coherentes para que las organizaciones puedan alcanzar grados aceptables de preparación forense. Manifiestan la falta de madurez en el discurso del análisis forense digital, pese a llevar varios años siendo considerada como una de las ciencias forenses, aunado con las definiciones informales de términos y conceptos clave. Mediante el desarrollo de un estudio con grupos focalizados determinaron que los factores que impactan en el grado de preparación forense de una organización se agrupan en 4 áreas definidas como: factores organizacionales, estrategia forense, infraestructura forense y objetivos de preparación forense. Concluyen que, fortaleciendo las anteriores áreas, es posible que una organización obtenga un framework forense con un grado de madurez apropiado para el desarrollo de investigaciones forenses digitales.

En [10] se observa un análisis de los diferentes problemas y retos que rodean la implementación de un ambiente preparado para la investigación digital en cualquier organización. El estudio se enfoca las diferentes medidas que las entidades pueden implementar para incrementar su habilidad para responder a incidentes de seguridad y crear ambientes institucionales preparados para la investigación forense. Dentro de los problemas y retos identificados por los autores, se describe la falta de políticas y procedimientos establecidos que les indiquen a los actores involucrados cuál debe ser la forma de proceder frente a la materialización de un incidente de seguridad. Esta falta de un modelo o metodología con procedimientos y guías de implementación apropiadas para ayudar a las organizaciones a obtener la admisibilidad de la evidencia digital en cualquier corte civil o penal resulta un reto a superar, con el fin de que sea posible crear un proceso de investigación forense digital más eficiente y efectivo.

Por otro lado, en [7] los autores proponen un modelo de madurez basado en el componente de Gobierno de TI de COBIT 5 el cual puede ayudar a las organizaciones a determinar su estado actual en relación con su capacidad de llevar a cabo investigaciones forenses digitales y, a su vez, obtener asistencia para alcanzar el nivel deseado de tales capacidades. El modelo propuesto cuenta con cinco (5) niveles de madurez (inicial, administrado, definido, administrado cuantitativamente y optimizado) y los autores concluyen que su implementación, alineada con el Gobierno de TI es posible y efectiva.

También se encuentra el trabajo desarrollado en [37], en donde los autores proponen un framework para la investigación forense digital (DFFR por sus siglas en inglés) para el sector bancario de Nigeria, con el fin de proteger información sensible que pueda resultar comprometida en un incidente de seguridad digital. Los autores manifiestan que el uso del DFFR ayuda a maximizar el uso de la evidencia digital y, de igual forma, reduce el costo de la investigación. Los resultados de su investigación muestran los componentes más probables de ser usados en la mayoría del sector financiero de Nigeria, mientras que cubre los principales componentes necesarios para las investigaciones forenses digitales.

En [9] se realiza una aproximación interesante con relación a una metodología para la investigación forense digital, que incluye la retroalimentación partiendo de un historial de casos anteriores. Para su propuesta los autores analizaron 25 metodologías o frameworks diferentes, de los cuales identificaron cada una de las fases metodológicas, para luego tomar los puntos comunes y aplicar un algoritmo de reducción utilizando sinónimos. Como

resultado, obtienen una metodología de 40 fases, que incluye como aporte propio un módulo de registro de caso y un módulo de casos históricos, lo cual le permitiría al investigador obtener una hoja de ruta preliminar al tener un caso similar a cualquier histórico que haya trabajado en el pasado.

Uno de los trabajos más interesantes encontrados en la literatura, es el desarrollado en [8], en donde se planteó un framework para la investigación forense digital en Bangladesh (BDFF, por sus siglas en inglés). Los autores proponen una metodología generalizada que involucra diferentes procesos que deben completarse para llevar a cabo una investigación forense digital. Su propuesta inicia con un proceso de identificación del tipo de investigación forense a realizar: Investigación forense de computadores, de red, de dispositivos móviles, de la nube o de dispositivos IoT. Una vez finalizada esta etapa, el módulo de preparación permite el desarrollo del plan de la investigación, teniendo en cuenta los factores técnicos, organizacionales y legales. Luego, inicia la fase de investigación forense proactiva, en donde se dan los procesos de aseguramiento de la escena, preservación de la escena física y detección del incidente. Posteriormente se inicia el módulo de investigación forense reactiva, en la cual se realiza la identificación, adquisición, preservación, examinación y análisis de la evidencia digital. Luego, la fase de presentación incluye el reporte de hallazgos, reconstrucción del procedimiento, la diseminación de resultados y la devolución de la evidencia. Como aporte novedoso de estos autores se tiene el desarrollo de un Sistema Experto de Asistencia (Assistive Expert System – AES), el cual tiene como objetivo preservar un historial de casos y presentar sugerencias estructuradas y sistemáticas a los investigadores, mediante el proceso de priorización realizado por su motor de inferencia.

Otro trabajo interesante encontrado en la literatura es el trabajo doctoral titulado: “The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice” [38]. En dicho trabajo el autor propone un modelo integral para el proceso de investigación forense digital aplicable en las áreas penal, comercio y respuesta a incidentes en el Reino Unido. La aproximación es interesante debido a que se trata de un modelo “integral, formal y genérico” que abarca todo el proceso de la investigación forense digital y es lo suficientemente generalizado que permite su aplicación en tres áreas diferentes [38].

Finalmente, desde el punto de vista internacional, no se pueden desconocer las metodologías y mejores prácticas que entidades de gran reconocimiento en la comunidad científica y técnica han realizado, estableciendo sus propios protocolos para el desarrollo de investigaciones forenses digitales. Es así que tenemos entidades como el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés National Institute of Standards and Technology), el cual desarrolló la Guía para integrar las técnicas forenses en la respuesta a incidentes (SP 800-86), que es un documento técnico en donde se recogen las recomendaciones de esta entidad para la adecuada inclusión de la informática forense en el ámbito de la respuesta a incidentes [39].

De manera similar tenemos el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE, por sus siglas en inglés Scientific Working Group on Digital Evidence), el cual fue creado en 1998 por los directores del Laboratorio de Crimen Federal (Federal Crime Laboratory Directors) como un grupo inicial de analistas de evidencia digital como una disciplina forense [24]. Dicho grupo tiene una serie de documentos que reúnen las mejores

prácticas recomendadas para la adquisición, examen y evaluación de evidencia digital para la computación forense [40].

En este mismo sentido, desde el ámbito colombiano se destaca una aproximación realizada en [41] en el cual realizan una descripción general del proceso que debería seguir un investigador al llevar a cabo una investigación forense digital, partiendo de algunas guías y buenas prácticas establecidas por entidades como el IETF (Internet Engineering Task Force). En este trabajo los autores describen un "paso a paso" para el desarrollo de investigaciones forenses digitales el cual está compuesto de 12 pasos empezando por la incautación hasta el registro de seguridad de todo el proceso [41]. Sin embargo, se observa que lo planteado por los autores no es una metodología formal; no contiene los elementos técnicos y científicos que le den validez en cualquier entorno organizacional y carece de procedimientos establecidos.

De igual manera, se encuentra el trabajo ilustrado en [42], en el cual se realiza una caracterización de la legislación colombiana con el fin de determinar cuál es la normatividad específica y necesaria para el diseño de lo que los autores llaman "la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia" [42]. Los autores dentro de su estudio coinciden en afirmar que en el contexto colombiano no existe un procedimiento o metodología vigente para las investigaciones forenses digitales, haciendo especial énfasis en el procedimiento de cadena de custodia. Analizan lo establecido por la Fiscalía General de la Nación en la actualización del año 2008 del Manual de Procedimientos para Cadena de Custodia [43], pero reconocen que esto no tiene una aplicación totalmente compatible con la evidencia digital, dado que su contexto es el plano de la evidencia física.

En este sentido, se debe mencionar el Manual Único de Policía Judicial [44] como una aproximación de la Fiscalía General de la Nación hacia los procedimientos que deben implementarse para el desarrollo de una investigación forense. A través de este documento la Fiscalía brinda algunos lineamientos generales para la recolección, embalaje y transporte de evidencia digital hallada en diligencias de policía judicial; sin embargo, no es una metodología o protocolo formalmente establecido para investigaciones forenses.

Por otro lado, es importante mencionar la Guía N° 13 – Evidencia digital [45] que hace parte de la documentación soporte de la Estrategia Gobierno Digital del Ministerio de las Tecnologías de la Información y las Comunicaciones, en la cual se brindan unas indicaciones y lineamientos para el desarrollo de análisis forenses en las entidades y/o instituciones del Estado que hayan sufrido un incidente de seguridad de la información y que opten por la implementación voluntaria de dicho documento.

Es así como se hace necesario tener en cuenta los procedimientos establecidos al interior de la Procuraduría General de la Nación, como máxima entidad rectora del proceso disciplinario en el país, para el desarrollo de investigaciones técnico-científicas en el área de la informática forense. Dicha entidad ha definido 6 procedimientos para el desarrollo de pruebas técnicas de informática forense, específicamente planteados para 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 [46]. Dichos procedimientos se encuentran integrados al Sistema de Gestión de la Calidad de la entidad y hacen parte del trabajo realizado por la Dirección Nacional de Investigaciones

Especiales, como dependencia que brinda apoyos técnicos en diversas áreas a las investigaciones disciplinarias que adelanta cualquier entidad del Ministerio Público.

Sin embargo, es preciso mencionar que los procedimientos definidos por esta entidad, si bien es cierto que dictan unos lineamientos generales para el desarrollo de las actividades técnicas, carecen de estructura y soporte metodológico y científico que permita considerarlos como un estándar con el rigor técnico suficiente para dar validez universal a sus hallazgos. Por otro lado, categorizan en un mismo procedimiento dispositivos y/o servicios que implican procesos diferentes. En otras palabras, se trata de un primer acercamiento a un proceso metodológico, el cual pretendió ser mejorado a través del presente trabajo. Para lograr una metodología para investigaciones forenses que sea estructurada y científicamente rigurosa, se partió de lo ya establecido por la entidad complementándolo con las mejores prácticas internacionales y nacionales, que se identificaron en las etapas de análisis de este trabajo. En otras palabras, se logró brindar un marco metodológico que sustenta los procedimientos existentes.

Finalmente, se debe hacer claridad sobre el contexto específico regulatorio del país. Las particularidades normativas de nuestro país identifican a Colombia como un estado en el cual, si bien se han logrado avances en materia de legislación informática (Ley 527 de 1999: Ley de Comercio Electrónico, Ley 1273 de 2009: Ley de Delitos Informáticos, Ley Estatutaria 1581 de 2012: Ley de Protección de Datos Personales, Ley 1928 de 2018: Ratificación del Convenio sobre la Ciberdelincuencia de Budapest, entre otras), en lo referente a investigaciones forenses digitales la normatividad es nula; sin embargo, las mismas características de los procesos penales, administrativos y/o disciplinarios en el país, trae como consecuencia una limitada aplicación de estándares y metodologías internacionales, en muchas ocasiones incompatibles con nuestra legislación.

En este contexto, es preciso traer a colación las palabras del doctor David Alonso Roa Salguero [47] con relación a la falta de métodos y/o metodologías que regulen la práctica de pruebas informáticas en el ámbito jurídico, especialmente para el derecho disciplinario:

> *"Los avances tecnológicos obligan a que las normas que regulan las actuaciones judiciales y administrativas desarrollen también todo lo relacionado con la incorporación y recaudo de la prueba informática o electrónica.*
>
> *La ausencia de mecanismos legales, dogmáticos y jurisprudenciales con los que la autoridad disciplinaria enfrenta la valoración de este tipo de pruebas, genera incertidumbre jurídica.*
>
> *(…)*
>
> *Al establecerse normativamente estándares legales de la prueba informática conocidos con anticipación, se fortalecería el juicio disciplinario y los sujetos procesales tendrían mayor seguridad jurídica en las decisiones"* [47, p. 6].

Lo anterior evidencia la necesidad de unificar criterios y establecer, en lo posible, estándares y metodologías que fortalezcan el proceso disciplinario y se garanticen los derechos de los investigados.

2. Metodología

El desarrollo de este proyecto se estructuró en un proceso de 3 fases, ilustradas en el siguiente esquema metodológico:

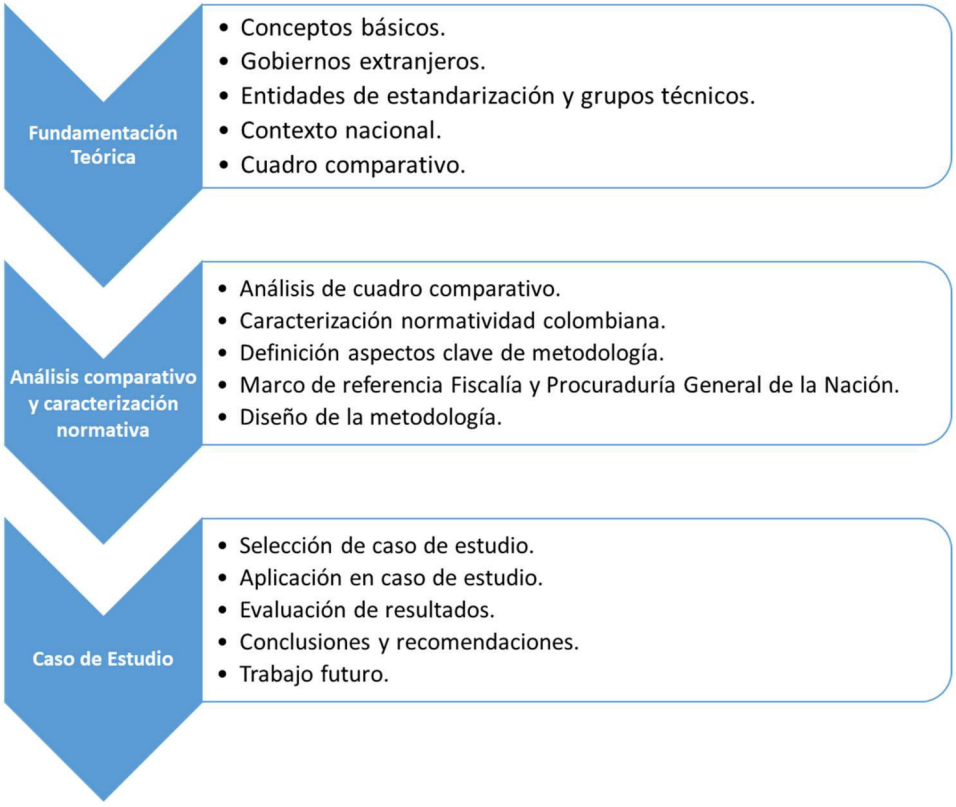


Figura 2-1: Esquema metodológico empleado
Nota. Fuente: Elaboración propia

Tabla 2-1: Actividades y productos de la metodología

Fase metodológica	Descripción actividad	Producto
Fundamentación teórica	Consulta bibliográfica conceptos básicos.	Marco teórico de conceptos básicos
	Consulta bibliográfica metodologías para investigaciones forenses digitales a nivel internacional.	Cuadro comparativo entre metodologías de análisis forense digital.

	Consulta bibliográfica metodologías para investigaciones forenses digitales a nivel nacional.	
	Elaboración de cuadro comparativo.	
Análisis comparativo y caracterización normativa	Análisis comparativo entre las metodologías y buenas prácticas identificadas.	Documento de análisis comparativo.
	Caracterización de la normatividad colombiana relacionada con seguridad informática y/o informática forense.	Metodología para investigaciones forenses digitales, enmarcada en la normatividad colombiana, para entidades del Estado.
	Análisis del proceso de recolección y manejo de evidencia de la Fiscalía General de la Nación.	
	Análisis de los procedimientos de informática forense de la Procuraduría General de la Nación.	
	Diseño de metodología para el desarrollo de investigaciones forenses digitales, para entidades del Estado colombiano.	
Caso de estudio	Selección y diseño de caso de estudio.	Documento de caso de estudio aplicado.
	Aplicación de la metodología propuesta en el caso de estudio seleccionado.	
	Evaluación de las observaciones realizadas durante el caso de estudio.	
	Conclusiones, recomendaciones y trabajo futuro.	
Diseminación del conocimiento	Elaboración y ajustes de documento final de trabajo de grado.	Documento de tesis de grado.

Nota. Fuente: Elaboración propia

2.1 Fundamentación teórica

En la primera etapa de esta investigación se llevó a cabo el 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 fin de identificar aquellas formalmente establecidas a nivel de diferentes países y entidades para su análisis.

Se realizó una definición de los aspectos básicos principales sobre la investigación forense, con el fin de lograr una comprensión y análisis del tema de forma 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.

Se tomaron dos normas internacionales para el análisis a saber: la ISO/IEC 27037:2012 [48], de la Organización Internacional de Estandarización (ISO, por sus siglas en inglés) y la NIST SP 800-86 [39] del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en ingles), teniendo en cuenta su amplio reconocimiento y aceptación entre la comunidad científica [9], [23], [24], [29], [30], [38], [41], [45], [49], [50], [51], [52], [53], [54].

Por otro lado, se tuvieron en cuenta las metodologías existentes en el plano de gobierno, identificando los países que han establecido sus propios procedimientos a nivel interno para el desarrollo de investigaciones forenses digitales. Se tomaron como referencia para el análisis los procedimientos establecidos por Argentina [55], [56], México [57], Australia [25], Reino Unido [58] y Estados Unidos [59].

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 [13] y el Manual Único de Policía Judicial [44] de la Fiscalía General de la Nación, la Guía N° 13 – Evidencia Digital del Ministerio de Tecnologías de Información y las Comunicaciones – MINTIC [45] y los procedimientos de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación [46].

El análisis que se realizó en esta fase es de tipo documental, mediante consultas bibliográficas en Internet y otras fuentes secundarias.

A partir del análisis de las normas y metodologías identificadas a nivel internacional y nacional, se realizó una correlación con el objetivo de identificar alcances, similitudes, diferencias, ventajas y desventajas.

Para la selección de los criterios que se utilizaron como base para la comparación se realizó un análisis de la normatividad colombiana que regula la realización de pruebas periciales en el ámbito de la Ley 734 de 2002, Código Único Disciplinario. Dicha ley en su artículo 130 establece que la práctica probatoria se realizará de acuerdo con 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 IV Pruebas, Capítulo III de la Ley 600 de 2000. Como resultado de este análisis se definieron los siguientes criterios:

1. Aspectos técnicos: La metodología analizada abarca aspectos técnicos de la investigación forense digital; involucra el desarrollo de análisis técnicos sobre la evidencia.
2. Cadena de custodia: La metodología analizada da lineamientos para iniciar y mantener una apropiada cadena de custodia sobre los elementos de evidencia.
3. 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. Herramientas técnicas: La metodología analizada ofrece lineamientos que contemplan el uso de herramientas técnicas.
5. 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. 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. Principios: La metodología analizada asegura la conservación de los principios de la evidencia digital [60], [29].

La evaluación de cada metodología se realizó teniendo en cuenta los anteriores criterios como características deseadas para el alcance del presente trabajo, toda vez que estos responden a las exigencias de la Ley 734 de 2002 para las pruebas periciales de informática forense.

La valoración se realizó utilizando una escala numérica comprendida por los siguientes valores:

- Cero (0): Se asignó un valor de cero (0) cuando la metodología analizada no cumple con el criterio en estudio.
- Uno (1): Se asignó un valor de uno (1) cuando la metodología analizada cumple parcialmente con el criterio en estudio.
- Dos (2): Se asignó un valor de dos (2) cuando la metodología analizada cumple completamente con el criterio en estudio.

En consecuencia, las metodologías 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). En el evento en que ninguna metodología obtuviera dicha calificación, se seleccionó aquella que cumpliera el(los) criterio(s) faltante(s) y/o cumplido(s) parcialmente, con el fin de diseñar una metodología integral que tenga en cuenta todos los criterios de análisis.

Con la información recopilada se elaboró la siguiente tabla comparativa con el fin de visualizar de manera unificada la valoración de cada norma, estándar, o país analizado, frente a cada uno de los criterios de interés:

Tabla 2-2: Tabla comparativa de metodologías analizadas

Norma/País / **Criterio**	**Norma/País 1**	**Norma/País 2**	**Norma/País 3**	**Norma/País 4**
Aspectos técnicos				
Cadena de custodia				
Preservación calidad				
Herramientas técnicas				
Informe final y documentación				
Proceso integral				
Principios de la evidencia digital				
TOTAL	∑	∑	∑	∑

Nota. Fuente: Elaboración propia

2.2 Análisis comparativo y caracterización normativa

Para el desarrollo de la metodología objeto de este trabajo el siguiente paso es el análisis de la normatividad 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 nuestro país.

Para lograr lo anterior se realizó un proceso de clasificación y caracterización de la normatividad 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 y/o informática forense. Como resultado de dicha clasificación inicial se obtuvo una tabla clasificatoria como la ilustrada a continuación:

Tabla 2-3: Tabla de clasificación de normatividad colombiana

Normatividad	Resumen	Artículos relacionados con SI y/o IF	
		Sí	No
Ley/Decreto/Resolución 1			
Ley/Decreto/Resolución 2			
Ley/Decreto/Resolución 3			
Ley/Decreto/Resolución 4			
Ley/Decreto/Resolución 5			

Nota. Fuente: Elaboración propia

Una vez identificadas las normas que tengan algún tipo de relación con la seguridad informática y/o informática forense, se evaluaron los siete (7) criterios establecidos en la fase anterior, con el fin de analizar la existencia o ausencia de estos elementos en las normas clasificadas.

Tabla 2-4: Tabla de cumplimiento de criterios de análisis

Criterios / Normatividad relacionada	C1		C2		C3		C4		C5		C6		C7	
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No
Ley / Decreto / Resolución 1														
Ley / Decreto / Resolución 2														
Ley / Decreto / Resolución 3														
Ley / Decreto / Resolución 4														
Ley / Decreto / Resolución 5														

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. Fuente: Elaboración propia

En caso de que ninguna norma tenga relación o haga referencia a los criterios definidos, se definirá como resultado “No aplica”, toda vez que, en este caso, se comprobaría la inexistencia de norma alguna que reglamente el desarrollo del análisis forense en el país.

2.3 Caso de estudio

Luego de haber diseñado la metodología objeto de este trabajo, se valoró su aplicación en un caso de estudio que permitió validar los resultados obtenidos por un analista con la metodología propuesta.

Desde el punto de vista de la metodología de la investigación, un caso de estudio permite analizar un fenómeno en su contexto “real” y realizar observaciones sobre su

comportamiento. En [61] se establece que "*el método del caso de estudio permite a los investigadores mantener las características holísticas y significativas de eventos de la vida real, tales como ciclos de vida individuales, comportamiento de pequeños grupos, procesos organizacionales y gerenciales, cambios en vecindarios, desempeño de las escuelas, relaciones internacionales y la maduración de las industrias*" (pág. 4).

En consecuencia, es la aproximación metodológica que más se ajusta a este trabajo, en donde se busca describir la aplicación de la metodología propuesta para el desarrollo de un análisis forense. De esta manera se desarrolló un caso de estudio simple y descriptivo utilizando un caso real llevado a cabo en el Laboratorio de Informática Forense de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación.

2.3.1 Protocolo del caso de estudio

Introducción

A continuación, se presenta la estructura del caso de estudio que se desarrolló con el fin de aplicar la metodología propuesta como mecanismo para llevar a cabo un análisis forense. Es de resaltar que este caso de estudio es particular para entidades del Estado que tengan la necesidad de realizar investigaciones forenses en el marco de procesos disciplinarios y/o administrativos enmarcados en la Ley 734 de 2002.

Procedimientos de recolección de información

Para la recolección de información se realizaron observaciones directas de los procesos de análisis forense llevados a cabo en el Laboratorio de Informática Forense de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación.

Se diseñó un formato de registro de observaciones en donde se realizaron las validaciones de cada etapa de la metodología propuesta. De igual forma se utilizaron los formatos aplicables establecidos por la Procuraduría General de la Nación dentro del procedimiento de "Investigación Técnico-Científica" [62] del Sistema de Gestión de Calidad de la entidad.

Preguntas del caso de estudio

El desarrollo del caso de estudio estuvo orientado por las siguientes preguntas generales:

1. ¿Las etapas propuestas en la metodología presentan dificultad en su aplicación?

2. ¿Qué dificultades se observaron en la aplicación de la metodología?

3. ¿Los hallazgos y resultados obtenidos al finalizar el análisis forense usando la metodología propuesta son de valor probatorio suficiente para la investigación?

FORMATO DE REGISTRO DE OBSERVACIONES

ETAPA 1: EVALUACIÓN

Evaluación del caso

Evaluación de la evidencia digital potencial

Evaluación del sitio de procesamiento

ETAPA 2: ADQUISICIÓN

Planear la adquisición

Adquirir los datos

Verificación de integridad

Cadena de custodia y documentación

ETAPA 3: EXAMINACIÓN

Extracción de los datos

1. **Extracción física**
2. **Extracción lógica**

Cadena de custodia y documentación

ETAPA 4: ANÁLISIS

Análisis de tiempo

Análisis de datos ocultos

Análisis de aplicaciones y de archivos

Propiedad y posesión

Generar conclusiones

Cadena de custodia y documentación

ETAPA 5: REPORTE

Explicaciones alternativas

Tenga en cuenta la audiencia objetivo

Información procesable

Informe del investigador

Cadena de custodia y documentación

3. Resultados

A continuación, se presentarán los resultados obtenidos de las actividades realizadas para el cumplimiento de los objetivos del trabajo.

3.1 Identificación y análisis de metodologías a nivel internacional y nacional

3.1.1 Análisis de buenas prácticas internacionales

NORMA NIST SP 800-86

Esta norma describe el proceso forense compuesto por cuatro (4) fases básicas: recolección, examinación, análisis y reporte [39]. Está diseñada para el uso de las agencias federales de los Estados Unidos, pero puede ser utilizada por organizaciones no gubernamentales de forma voluntaria. La norma presenta el proceso forense desde el punto de vista de IT, no desde el punto de vista legal, por lo cual debe ser complementada con la respectiva normatividad legal de la jurisdicción aplicable.

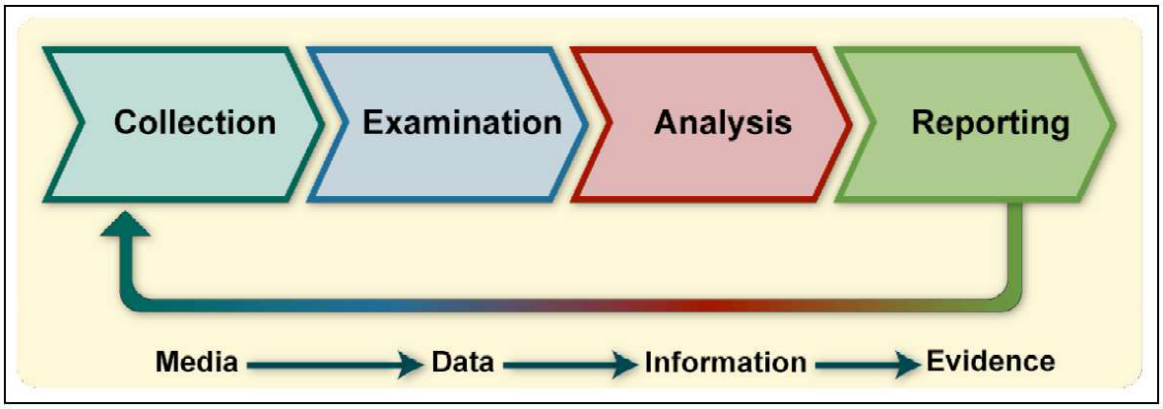


Figura 3-1: Fases del proceso forense según NIST SP 800-86
Nota. Fuente: [39]

Como se observa en la figura anterior, el proceso forense transforma los medios en evidencia. La primera transformación ocurre cuando los medios son examinados para extraer los datos relevantes a la investigación. Luego estos datos se transforman en información, durante la fase de análisis; para finalmente convertirse en evidencia lo cual, según la norma, es el proceso análogo de llevar el conocimiento a la acción, utilizando la información obtenida en el análisis para resaltar los aspectos relativos al caso durante el reporte [39].

1. Recolección: El primer paso en el proceso forense es identificar fuentes potenciales de datos y adquirir los datos de ellas [39].

   Teniendo en cuenta el sinnúmero de dispositivos que pueden contener datos importantes para el caso, los investigadores deben ser capaces de identificar claramente en la escena, todas las fuentes potenciales de datos.

   De igual forma esta fase de recolección incluye la adquisición de estos datos para lo cual se debe realizar un proceso de 3 etapas:
   a. Desarrollar un plan para adquirir los datos: Evaluar todas las fuentes potenciales y determinar su prioridad de adquisición, dependiendo de factores como el valor probatorio, la volatilidad y la cantidad de esfuerzo requerido.
   b. Adquirir los datos: Si los datos no han sido adquiridos por herramientas de seguridad, de análisis o por otros medios, el proceso general para la adquisición de los datos involucra usar herramientas forenses para recolectar los datos volátiles, duplicar las fuentes de datos no volátiles y asegurar las fuentes originales de datos no volátiles.
   c. Verificar la integridad de los datos: Siempre es necesario verificar la integridad de los datos para garantizar que estos no han sido alterados o modificados. Generalmente este proceso involucra el cálculo de funciones hash de verificación.

   Antes de realizar la adquisición de los datos, se debe tener en cuenta la necesidad de la cadena de custodia exhaustiva si se requiere asegurar la evidencia para futuros procesos legales. Los investigadores deben tomar la decisión adecuada a partir de la normatividad legal y de las políticas de empresa aplicables.

2. Examinación: Luego de recolectados los datos sigue la examinación de estos, lo cual involucra evaluar y extraer las piezas relevantes de información. Para esto deben utilizarse técnicas y herramientas que permitan realizar la búsqueda de patrones de texto, identificación de contenido de archivos, análisis de archivos comprimidos, entre otras; que faciliten la tarea de identificación y extracción de contenidos pertinentes al caso en estudio [39].

3. Análisis: Una vez que se ha extraído la información relevante, el analista debe estudiar y analizar los datos para llegar a conclusiones a partir de estos. A menudo, esta actividad puede involucrar la correlación de múltiples fuentes. Herramientas como logs centralizados y software de administración de eventos de seguridad pueden facilitar este proceso, reuniendo y correlacionando los datos automáticamente [39].

   Si la evidencia puede ser necesaria para acciones legales o disciplinarias, los analistas deben documentar cuidadosamente los hallazgos y todos los pasos que se siguieron en el proceso.

4. Reporte: La etapa final es el reporte, la cual es el proceso de preparar y presentar la información de la fase de análisis [39]. Deben tenerse en cuenta los siguientes aspectos:
   a. Explicaciones alternativas: Cuando la información relacionada con un evento está incompleta, es posible que no se pueda llegar a una explicación definitiva. Si existen diversas explicaciones para un evento en particular, se le debe dar a cada una de ellas la suficiente consideración en el proceso de reporte. En este contexto, los analistas deben usar una aproximación metodológica que intente probar o desmentir cada explicación posible.
   b. Audiencia objetivo: Es importante conocer la audiencia a la cual se le presentará la información. En algunos casos se requieren grandes volúmenes de detalles técnicos, mientras que en otros es posible que solo sea suficiente con un resumen administrativo de los hallazgos.
   c. Información procesable: Los informes también incluyen la identificación de información procesable obtenida de los datos que pueden permitir que un analista recopile nuevas fuentes de información.

ESTÁNDAR ISO/IEC 27037:2012

El estándar internacional ISO/IEC 27037:2012 principalmente trata con el proceso inicial de recolección y almacenamiento de evidencia digital potencial y no se involucra con el trabajo subsiguiente con dicha evidencia, como su análisis, presentación y disposición final [63].

El estándar ISO/IEC 27037:2012 establece un proceso cíclico de cuatro (4) fases [64] que se ilustra en la siguiente figura:

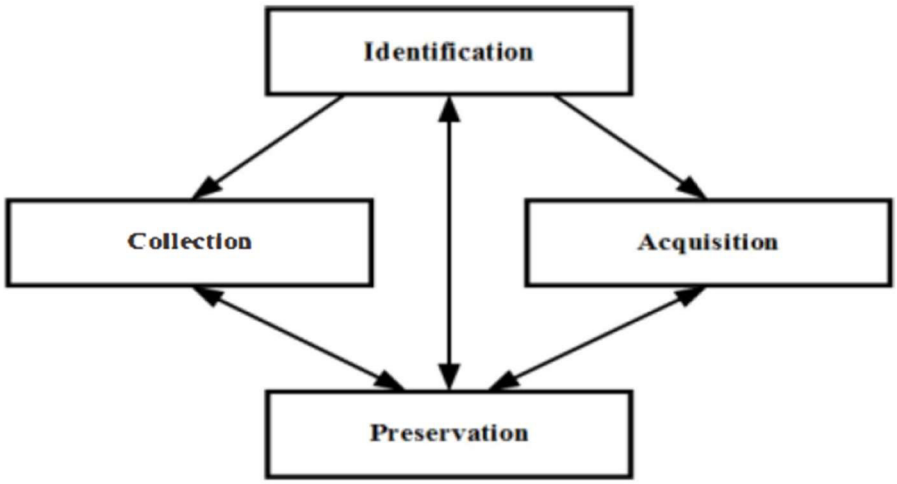


Figura 3-2: Modelo del proceso de gestión digital según ISO/IEC 27037
Nota. Fuente: [64]

1. Identificación: Es la primera fase en el proceso de investigación forense de dispositivos digitales. Involucra la búsqueda, reconocimiento y documentación de la evidencia digital potencial. Deben identificarse todos los dispositivos que puedan contener evidencia digital [63]. Incluye la priorización de la recolección de la evidencia con base

en la volatilidad, lo cual es un proceso crucial para asegurar el orden correcto de recolección y adquisición, de forma tal que se obtenga la mejor evidencia y no haya pérdidas de información importante [64].

2. Recolección: En esta fase se debe decidir si se recolectan los potenciales medios o fuentes de evidencia o se adquiere la información en sitio. En general, la recolección es un proceso donde los dispositivos que puedan contener evidencia digital son removidos de su ubicación original a un laboratorio u otro ambiente controlado para su posterior adquisición y análisis. Este proceso es documentado en todo momento, incluyendo el embalaje y transporte al laboratorio [63]. Es importante que se asegure también cualquier otro material físico que pueda estar relacionado con los dispositivos recolectados como, por ejemplo, notas de papel que puedan contener contraseñas, conectores y cables de poder, etc. [64].

3. Adquisición: Este proceso involucra la creación de una copia de la evidencia digital recolectada, que pueden ser discos duros completos, particiones, archivos, entre otros, y la documentación de todas las acciones y métodos que se utilizaron para este procedimiento, en especial cuando ocurren alteraciones inevitables de la información. Es importante también garantizar la integridad de los datos adquiridos para garantizar que estos no han sido alterados desde el momento de su adquisición [64].

4. Preservación: La última fase es el proceso de asegurar el mantenimiento de la cadena de custodia sin alterar o cambiar el contenido de los datos que residen en los dispositivos y medios extraíbles. El proceso de preservación es crítico para que la evidencia digital potencial sea útil en la investigación [64]. La cadena de custodia debe iniciarse y mantenerse a lo largo de todos los procesos de manejo de evidencia digital, con el fin de mantener su integridad para su admisibilidad en un tribunal de justicia.

COMPARATIVO BUENAS PRÁCTICAS INTERNACIONALES

A partir del análisis de la norma ISO/IEC 27037:2012 y la NIST SP 800-86, se realizó una correlación con el objetivo de identificar alcances, similitudes, diferencias, ventajas y desventajas.

Tabla 3-1: Tabla de análisis de ventajas y desventajas buenas prácticas internacionales

Norma	Ventajas	Desventajas
ISO/IEC 27037	• Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Garantiza la validez de los hallazgos manteniendo la preservación de la información durante todo el proceso. • Le da importancia a la documentación de todo el proceso forense. • Durante las fases indicadas se da prioridad a los principios de relevancia, confiabilidad y	• Es una norma de carácter general, y como tal, no abarca los procesos técnicos del análisis forense. • No incluye lineamientos relacionados con el uso de herramientas técnicas. • No incluye la fase de análisis y/o tratamiento de la información recolectada ni la presentación de resultados.

Norma	Ventajas	Desventajas
	suficiencia, como elementos clave para la evidencia digital.	
NIST SP 800-86	• Es de carácter específico y presenta lineamientos que abarcan los procesos técnicos del análisis forense de diversos tipos de dispositivos. • Preserva la cadena de custodia como parte fundamental de todo el proceso forense. • Promueve la preservación de la calidad de la información durante todo el proceso forense. • Incluye lineamientos para el uso de herramientas forenses por cada tipo de fuente de información identificada. • Brinda recomendaciones sobre la correcta documentación y reporte final de los resultados. • Dado su alcance específico, incluye lineamientos y recomendaciones detalladas sobre el proceso forense en todas sus fases, desde la adquisición hasta el reporte final de hallazgos. • Promueve la conservación de los principios de la evidencia digital.	

Nota. Fuente: Elaboración propia

El análisis de ventajas y desventajas permite concluir que, teniendo en cuenta los criterios de análisis definidos (descritos en la sección 2.1), la norma NIST SP 800-86 resulta más ventajosa que la ISO/IEC 27037 para los objetivos de este proyecto, toda vez que no se observan desventajas frente a los aspectos analizados en cada criterio.

Tabla 3-2: Tabla de análisis de comparación de características – diferencias, similitudes, alcances buenas prácticas internacionales

Aspecto	ISO/IEC 27037	NIST SP 800-86
Número de fases	4	4
Público objetivo	Está dirigida a un público internacional, organizaciones privadas o públicas.	Está dirigida a un público mayoritariamente nacional: agencias federales de los Estados Unidos y a cualquier otra organización de forma voluntaria.
Alcance	Tiene un alcance general. Abarca los aspectos generales de la recolección y preservación de la evidencia digital. No abarca el análisis de esta. Incluye lineamientos generales para diversos tipos de dispositivos.	Tiene un alcance específico. Abarca además el análisis y reporte de la información. Incluye lineamientos específicos para diversas fuentes de datos.
Fases	Identificación Recolección	Recolección Examinación

Aspecto	ISO/IEC 27037	NIST SP 800-86
	Adquisición Preservación	Análisis Reporte
Aspectos técnicos	Se enfatiza en procesos no técnicos de la investigación forense.	Se enfatiza en procesos técnicos y no técnicos de la investigación forense.
Cadena de custodia	Preserva la cadena de custodia como parte fundamental de todo el proceso forense.	Preserva la cadena de custodia como parte fundamental de todo el proceso forense.
Preservación de la calidad	Promueve la preservación de la calidad de la información durante todo el proceso forense.	Promueve la preservación de la calidad de la información durante todo el proceso forense.
Herramientas técnicas	No tiene dentro de su alcance la fase de análisis, por lo que no menciona el uso de herramientas forenses.	Contiene indicaciones específicas sobre el uso de herramientas forenses para el análisis.
Informe final y documentación	No brinda indicaciones para la elaboración de un informe final de presentación de resultados. Promueve la documentación de todo el proceso forense.	Incluye la fase de reporte de los hallazgos, en donde se brindan recomendaciones y lineamientos del informe final de resultados. Asimismo, promueve la documentación de todo el proceso forense.
Proceso integral	Abarca las fases de identificación, adquisición y preservación de la evidencia digital. No incluye las fases de análisis y reporte de resultados.	Abarca todas las fases del proceso forense, desde la adquisición de la evidencia hasta el reporte de resultados finales.
Principios de la evidencia digital	Durante las fases indicadas se da prioridad a los principios de relevancia, confiabilidad y suficiencia.	Durante las fases indicadas se da prioridad a los principios de relevancia, confiabilidad y suficiencia.
Actualización	Actualizada en 2012.	Publicada en 2006.

Nota. Fuente: Elaboración propia

Tabla 3-3: Tabla de valoración comparativa buenas prácticas internacionales

Norma / Criterio	ISO/IEC 27037	NIST SP 800-86
Aspectos técnicos	0	2
Cadena de custodia	2	2
Preservación calidad	2	2
Herramientas técnicas	0	2
Informe final y documentación	1	2
Proceso integral	1	2
Principios de la evidencia digital	2	2
TOTAL	**8**	**14**

Nota. Fuente: Elaboración propia

Finalmente, la valoración comparativa de cumplimiento total, parcial o nulo de los criterios de análisis definidos en la metodología (descritos en la sección 2.1) permite concluir que el estándar ISO/IEC 27037 no cumple con dos (2) de los criterios de interés para este proyecto, como son la inclusión de aspectos técnicos de la investigación forense y el uso de herramientas técnicas de análisis; mientras que cumple parcialmente los criterios relacionados con los lineamientos para el informe final y documentación de resultados, y el proceso integral de la investigación forense. De igual forma es posible determinar que

dicho resultado corresponde al carácter general de la norma y a que esta no incluye el análisis de la evidencia digital, sino solamente aspectos relacionados con la adquisición y extracción de esta.

Por otro lado, se observa que la norma NIST SP 800-86 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.

3.1.2 Análisis de metodologías a nivel gobierno en países

ARGENTINA

Si bien Argentina no cuenta en la actualidad con una metodología, protocolo o procedimiento formalmente establecido para una investigación forense digital en su totalidad [65], se destaca que cuenta con algunos acercamientos que formalizan las directrices generales para la recolección y manipulación de evidencia digital. Es así como figuran algunas provincias con procedimientos y protocolos oficiales para sus fuerzas de ley, como la Provincia de Neuquén, que cuenta con el "Protocolo de actuación para pericias informáticas" [66].

Por otro lado, a nivel país existen dos actos administrativos que establecen el procedimiento a seguir al momento de realizar un proceso que involucre la recolección, almacenamiento, procesamiento y/o análisis de evidencia digital: la Resolución N° 234/2016 del Ministerio de Seguridad de la Nación [55] y la Resolución N° 756/2016 de la Procuración General de la Nación [56].

- Resolución N° 234/2016: Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos [55]

El procedimiento descrito en este acto administrativo es de uso obligatorio para las fuerzas de ley a nivel nacional, en la persecución de delitos informáticos en especial el grooming.

Describe el proceso que debe seguirse desde el momento de la denuncia, pasando por el allanamiento, secuestro de dispositivos, embalaje, transporte y almacenamiento. Dicho procedimiento puede resumirse en los siguientes pasos:

1. Denuncia: Cuando se recibe una denuncia que involucre un presunto ciberdelito, esta debe cumplir los lineamientos generales que se encuentran establecidos en la normatividad pertinente (entiéndase el Código Procesal Penal argentino, códigos procesales de cada provincia y el de la Ciudad Autónoma de Buenos Aires), en cuanto a su recepción, forma, contenido [55].

   Una vez recepcionada, se deben tomar las medidas necesarias para la conservación de la evidencia aportada por el denunciante (en caso de haberla) o solicitar la realización de las pruebas pertinentes, dando especial énfasis al material digital que pueda verse involucrado.

2. Allanamiento: Previo a la práctica de esta actividad, es necesario que las fuerzas policiales y de seguridad realicen las investigaciones preliminares pertinentes para la identificación de todos los dispositivos y/o equipos electrónicos y digitales que se encuentren involucrados en el delito denunciado, y principalmente, identificar al supuesto autor del mismo, con el fin de que la diligencia de allanamiento cumpla con los requisitos establecidos en la normatividad pertinente [55].

   El procedimiento se resume en:
   a. Visualización de la escena y fijación fotográfica o en video de esta.
   b. Identificación de todos los dispositivos que se encuentran en la escena.
   c. Documentación de la escena, especificando el lugar exacto y el estado en que se encontraron los dispositivos, así como el tipo de dispositivo. Dentro de los tipos de dispositivo que se pueden hallar están: computadores, dispositivos periféricos, de almacenamiento de datos, de mano, cualquier dispositivo que tenga el potencial de contener evidencia digital.
   d. Determinar, de ser posible, el usuario o usuarios de los dispositivos.
   e. Utilizar las medidas de seguridad y de aislamiento necesarias para la protección de los dispositivos hallados (guantes de látex, cajas de aislamiento de señal, bolsas de papel, cajas de cartón, etc.).
   f. Registrar marca, modelo, números de serie, en general, cualquier dato que identifique cada uno de los dispositivos encontrados en la escena.

3. Secuestro de dispositivos: Durante la diligencia de allanamiento, siempre debe darse prioridad al secuestro o captura de los dispositivos hallados e identificados, para la posterior extracción de la evidencia digital en el laboratorio mediante el uso de procedimientos forenses. En estos casos, la captura de los dispositivos debe tener en cuenta los siguientes pasos [55]:
   a. Fotografiar el estado en que se encuentra el dispositivo (en especial la pantalla en caso de encontrarse encendido).
   b. Nunca encender un dispositivo apagado o si está encendido no apagarlo inmediatamente.
   c. Si se trata de un dispositivo de red, no apagarlo (ya que esto puede acarrear daños al dispositivo o interrupciones del servicio), consultar direcciones IP y solicitar asesoría con el experto en redes.
   d. Documentar, fotografiar y hacer un esquema de todos los cables y dispositivos conectados.
   e. Desconectar y etiquetar el cable de suministro y los demás cables, alambres o dispositivos USB conectados.
   f. Documentar la existencia de cámaras web y el estado de estas (activas o inactivas).
   g. Cuando se tengan dudas sobre el estado de un dispositivo electrónico prestar especial atención a cualquier luz o sonido que indique que se encuentra encendido, por ejemplo, el sonido de los ventiladores, o las luces led de la parte frontal del equipo.
   h. Verificar cualquier estado o indicio que indique si se está accediendo al dispositivo de manera remota, si la información está siendo borrada o destruida o si existen señales de comunicación con otro dispositivo o usuario, mediante ventanas emergentes, chats o mensajería instantánea.

4. Embalaje, transporte y almacenamiento: Es necesario tener presente que la prueba digital es frágil y sensible a altas temperaturas, humedad, electricidad estática y campos magnéticos. En consecuencia, se deben tomar las medidas necesarias de protección para estos casos [55].
    a. Embalar toda la evidencia digital en bolsas antiestáticas.
    b. Todo lo que pertenezca a un mismo dispositivo, debe ser etiquetado, embalado y transportado en su conjunto, para evitar que se mezcle con otros y poder facilitar la reconfiguración del sistema.
    c. Sellar cada entrada, puerto o tornillo del dispositivo con cinta de seguridad, de forma que no se puedan remover o reemplazar las piezas internas de este.
    d. Asegurar el estado de cualquier bandeja (CD o DVD) del dispositivo.
    e. Desconectar el cable de suministro.
    f. Guardar las baterías de forma separada al equipo, debidamente etiquetadas.
    g. Se debe realizar el registro de la cadena de custodia, identificando quién tiene contacto en todo momento con la evidencia, así como las operaciones realizadas.
    h. Inventariar apropiadamente toda la evidencia recibida en el sitio de almacenamiento.

5. Extracción de la prueba: Se identifican dos tipos de prueba: la extraída directamente de los dispositivos secuestrados, mediante procedimientos forenses, y la obtenida de los diferentes proveedores de servicio (Internet, servicios en la nube, etc.) [55].
    a. No trabajar con la evidencia original, se requiere realizar las pruebas y análisis sobre una copia de esta.
    b. Realizar copia forense de todos los dispositivos que lo permitan.
    c. Se deben utilizar dispositivos bloqueadores de escritura, para garantizar la integridad de la prueba y la no alteración de esta.
    d. Verificación de las funciones hash de las copias realizadas.
    e. Como recomendación se tiene realizar dos copias de la evidencia, asegurando su exactitud con la original, así como la inalterabilidad de esta.

- Resolución N° 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital [56]

Este documento pretende brindar recomendaciones que se implementan a nivel mundial para incautar, analizar y preservar evidencia digital, lo cual debe ser considerado e implementado por los operadores judiciales argentinos.

De igual forma, el documento hace referencia a estándares y protocolos internacionales que recopilan las buenas prácticas forenses a nivel internacional y que dan cuenta de la importancia del fenómeno de la cibercriminalidad.

Abarca temas relativos con la definición y características, los principios básicos de tratamiento y la recolección y preservación de la evidencia digital. El proceso general de recolección y preservación se resume en:

1. Asegurar el lugar del hecho, mediante la fijación fotográfica y documentación del estado de la escena.
2. Documentación de cualquier tipo de actividad que se esté dando en los dispositivos informáticos.
3. Determinación del estado de los dispositivos (encendido o apagado); fijación fotográfica de cada dispositivo (cables y conexiones, pantallas, etc.).

4. Embalaje, traslado y resguardo de la evidencia digital, teniendo en cuenta que todo lo recolectado se encuentre documentado, etiquetado, marcado, fotografiado, filmado o esquematizado apropiadamente. Tener en cuenta las recomendaciones para la protección y aislamiento de los dispositivos electrónicos recolectados.
5. Manipulación adecuada del hardware, asegurando que todos los procedimientos se realicen en zonas seguras antiestáticas, los medios de almacenamiento sanitizados y utilizar guantes de látex o similares y pulseras o brazaletes antiestáticos.
6. Realizar imagen o copias forenses, asegurándose de utilizar las herramientas software y hardware adecuadas, como los dispositivos bloqueadores de escritura y, por otro lado, calcular las funciones hash para garantizar la integridad de la información.

MÉXICO

Desde junio de 2016 México se encuentra en un período de transición de un sistema penal inquisitivo a uno acusatorio, en el cual se le da mayor importancia a la evidencia, como mecanismo de acusación o defensa, en lugar de las confesiones, como se hacía en el sistema anterior. Es así como dentro de las transformaciones que están ocurriendo al interior del país se encuentra el paso de la Procuraduría General de la República a una Fiscalía General, con el propósito de que sea la parte acusadora del poder ejecutivo y que tenga la suficiente autonomía. En este contexto, el rol de los peritos informáticos toma mayor importancia, toda vez que sus dictámenes son pieza clave de los procesos investigativos [65].

En materia de informática forense (cómputo forense, como es llamado en México) se cuenta con algunos referentes normativos y académicos que orientan el accionar de las labores periciales. De esta manera, las autoridades periciales toman como referencia académica el libro “Cibercriminalidad, Fundamentos de Investigación en México” de Óscar Manuel Lira Arteaga y como estándar normativo la norma NMX-I-289-2016: “Tecnología de la Información – Metodología de Análisis Forense de Datos y Guías de Ejecución” [57].

El proceso forense en general se compone de las siguientes fases [57]:

1. Identificar la evidencia: Se deben identificar los indicios que puedan conducir a evidencias sobre el caso. Determinar los dispositivos que pueden contener dicha evidencia, puede implicar muchos retos para los investigadores. En este paso es fundamental la documentación de la escena, lo que incluye la fijación fotográfica de los equipos y dispositivos que serán analizados.

2. Preservación de la evidencia: Luego de identificada la evidencia se debe preservar la misma, lo cual es un paso crucial y necesario para no desacreditar lo realizado durante el proceso legal. Los investigadores deben implementar los mecanismos necesarios para garantizar que la evidencia no se modifique. La utilización de las funciones hash como verificador de la integridad es un procedimiento común en esta fase, debido a que hace las veces de cadena de custodia digital. Del mismo modo, la cadena de custodia y el adecuado embalaje de los equipos y dispositivos debe iniciarse como mecanismo de preservación de la evidencia digital.

Las acciones a seguir pueden variar dependiendo del tipo de sistema encontrado en la escena; de esta forma se deben tomar decisiones que varían si se trata de sistemas activos (o "en vivo" – dispositivos encendidos) o cuando son sistemas apagados.

3. Analizar la evidencia: Se refiere a la revisión de los dispositivos para hallar los elementos materiales probatorios que sustenten o desvirtúen la hipótesis del caso. Esta es la fase que demanda mayor tiempo, ya que comprende el procesamiento y análisis del gran cúmulo de información que reside en los dispositivos asegurados.

   "El análisis de la evidencia debe de llevar un orden estructurado y ordenado, cuidando las minucias, los detalles técnicos. Desde el momento de llevar a cabo primero la creación de los duplicados forenses con el fin de no realizar ninguna operación sobre los discos originales de los equipos sujetos a investigación hasta el momento de haber emitido el reporte o peritaje del análisis realizado" [57].

4. Presentar la evidencia: Esta fase implica la unión de las actividades de "análisis tecnológico, las acciones legales y el lenguaje coloquial que puedan entender las partes involucradas" [57]. Se requiere que los investigadores sean capaces de explicar sus hallazgos de una forma tal que sea comprensible por todos los actores que intervienen en la investigación. De igual forma, este debe enmarcar sus resultados en la normatividad existente, con el fin de coadyuvar a la tipificación de los delitos.

AUSTRALIA

Australia, como miembro de la Commonwealth of Nations (Mancomunidad de Naciones), desarrolló y estableció el estándar HB171: Lineamientos para la Gestión de la Evidencia Digital (HB171: Guidelines for the Management of IT Evidence). Este estándar es parte de la Agenda de e-Seguridad Nacional del gobierno australiano y es el punto de partida de Australia para satisfacer las recomendaciones de la Commonwealth [25].

Este estándar establece el ciclo de vida para la gestión de la evidencia digital que está compuesto por seis (6) fases, las cuales pretenden articular el proceso de informática forense de forma tal que no sea una actividad post-mortem [25]. Dicho ciclo de vida se ilustra en la siguiente gráfica:

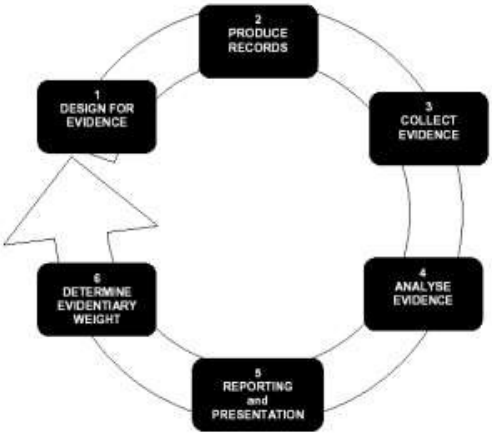


Figura 3-3: Ciclo de vida de la gestión de la evidencia digital según la norma HB171
Nota. Fuente: [25]

1. Diseño de la evidencia: Hay cinco (5) objetivos que deben tenerse en cuenta cuando se diseña un sistema de cómputo para maximizar el valor probatorio de los registros digitales [25]:

    a. Asegurar la identificación, disponibilidad y usabilidad de los registros electrónicos significativos como evidencia digital, teniendo en cuenta su período de retención acorde a los lineamientos de la ley.
    b. Identificar el autor de los registros electrónicos. Esto puede significar un reto cuando se trata de registros o documentos almacenados o generados por computador, toda vez que, el hecho de que una cuenta o dirección haya sido usada para crear o alterar determinado registro, no establece de una forma concluyente la identidad o ubicación de la persona en particular que la usó. Como resultado, tal evidencia basada principalmente en historial de cuentas o registros IP deben demostrar una conexión suficiente entre los logs y la persona o ubicación.
    c. Establecer la fecha y hora de creación o alteración, utilizando sistemas de tiempo de referencia, como la hora del sistema, estampas de tiempo, entre otros.
    d. Establecer la autenticidad de los registros electrónicos, es decir, ofrecer la evidencia suficiente para determinar que los hallazgos mostrados por los registros son lo que dicen ser y que no han sido fabricados o manipulados. La autenticidad de la evidencia digital puede ponerse en duda de tres formas: cuestionando si los registros digitales fueron alterados, manipulados o dañados después de creados; en segundo lugar, cuestionando la confiabilidad del programa de cómputo que generó los registros y, en tercer lugar, cuestionando la identidad del autor. Dentro de los mecanismos utilizados para asegurar la autenticidad se encuentran: mantener el documento original en una forma no electrónica (impresión, microficha, etc.), usar técnicas criptográficas como los códigos hash, almacenar el documento digital original o una copia validada en un medio de una sola escritura, por ejemplo, en CD-ROM.
    e. Establecer la confiabilidad de los programas computacionales. En algunas ocasiones comprobar la autenticidad de los registros digitales implica demostrar la confiabilidad de los sistemas computacionales que crearon esos registros. El objetivo de establecer la confiabilidad de un programa de cómputo que produce registros almacenados en computador es demostrar que el texto (o los gráficos, voz, etc.) es una reproducción exacta de la declaración del autor humano. Para el caso de los registros generados por computador, el objetivo es demostrar que el programa estaba funcionando apropiadamente. En ambos casos se debe demostrar que: i) el programa fue diseñado apropiadamente y que sus resultados o salidas son consistentes con el diseño, predecibles y repetibles, y ii) el programa estaba funcionando apropiadamente cuando el registro electrónico fue creado, copiado o alterado.

2. Producir registros: La siguiente fase del ciclo de vida de la gestión de la evidencia digital es la producción de los registros. Íntimamente ligada con la anterior, es necesario que se tenga conocimiento de la obligatoriedad de los casos en los que se deben producir, mantener, entregar y retener los registros digitales de los sistemas informáticos [25].

3. Recolección de la evidencia: El objetivo de esta fase es localizar toda la información relevante y preservar los registros electrónicos originales de forma que no se altere nada de la evidencia original. En este contexto cobran vital importancia los estándares con los cuales se recolecta la evidencia, ya que de esto depende el grado de admisibilidad de esta. De igual forma, la documentación de toda acción, decisión o proceso ejecutado sobre la evidencia original, en especial la fecha y hora, debe tenerse presente [25].

   Por otro lado, es necesario que se recolecte solo la información relevante para la investigación, por lo cual el personal involucrado en la recolección debe estar lo suficientemente familiarizado con el caso para poder determinar la relevancia de pequeñas piezas de evidencia.

   Otro factor importante en esta fase del ciclo de vida es la cadena de custodia. Las organizaciones deben ser capaces de identificar quién tiene acceso a un registro electrónico en particular, en cualquier momento dado desde la recolección, pasando por la copia de la evidencia hasta su presentación como prueba. Este es un factor clave para darle valor probatorio a la evidencia.

   Es posible encontrar registros muy útiles como evidencia en documentos electrónicos no legibles, los cuales son registros que no poseen caracteres que puedan leerse o imprimirse; tales registros solo pueden ser leídos por programas especiales. Los registros electrónicos no legibles pueden ser críticos durante la fase de “análisis de la evidencia”. Cuando se recolectan registros electrónicos, se debe tener cuidado para descubrir y no alterar los registros electrónicos no legibles.

   Finalmente se deben tener en cuenta las limitaciones estipuladas por la ley para la recolección de la evidencia. La violación de estas reglas reducirá el valor probatorio de los registros electrónicos y puede resultar en la inadmisibilidad de estos.

4. Análisis de la evidencia: El objetivo de esta fase es [25]:
   a. Identificar hechos materiales a partir de los registros de evidencia digital.
   b. Deducir opiniones relacionadas con esos hechos.
   c. Determinar qué otra evidencia digital falta para ayudar a la investigación.

   En este contexto se deben tener en cuenta que el análisis se debe hacer sobre una copia de la evidencia, a excepción de los casos en los que se solicite determinar si las copias son duplicados de la evidencia original o si la original ha sido alterada.

   Por otro lado, se requiere que el personal involucrado en el análisis de evidencia digital tenga las cualificaciones necesarias según el nivel de experticia requerido para el caso particular.

   Finalmente, teniendo en cuenta que la evidencia digital es circunstancial, es necesario identificar claramente la necesidad de otros elementos que apoyen los hallazgos identificados. Se deben presentar explicaciones para (a) Las circunstancias en que se crearon los registros electrónicos; y (b) Los sistemas informáticos que crean los registros electrónicos. Sin una comprensión profunda de los antecedentes, los registros electrónicos materiales pueden no ser incluidos o disminuir su valor probatorio.

5. Reporte y presentación: En esta fase se pretende persuadir a los tomadores de decisiones (ya sean administrativos, abogados, jueces, etc.) sobre la validez de los hechos y opiniones que se dedujeron de la evidencia.

6. Determinar el valor probatorio de la evidencia: La valoración probatoria de los registros digitales se realiza durante todas las fases del ciclo de vida, pero la valoración final es realizada por una tercera parte, que puede ser un magistrado, un juez, un miembro de un tribunal o árbitro o un superior administrativo.

   De esta manera, la parte que presenta los registros electrónicos o evidencia digital debe convencer a la corte y/o tribunal de su admisibilidad y la parte contraria puede cuestionarla.

REINO UNIDO

En el Reino Unido existe la “Guía de buenas prácticas para la evidencia digital” [58] (ACPO Good Practice Guide for Digital Evidence, version 5) la cual es un documento expedido por la Asociación de Oficiales Jefes de Policía de Inglaterra, Gales e Irlanda del Norte (Association of Chief Police Officers of England, Wales & Northern Ireland) como lineamientos para el personal de las fuerzas de ley del Reino Unido que pueden manejar o gestionar la evidencia digital.

Establece que el proceso forense debe garantizar la preservación de los siguientes principios [58]:

- Inalterabilidad: Ninguna acción de las agencias de ley o cualquiera de sus agentes, debe alterar los datos que podrían ser posteriormente presentados en los tribunales.
- Justificación: En los casos en los que una persona considere necesario acceder a los datos originales, esa persona debe ser competente para hacerlo y ser capaz de presentar pruebas que expliquen la relevancia y las implicaciones de sus acciones.
- Repetición y auditabilidad: Se debe crear y preservar un registro de auditoría u otro registro de todos los procesos aplicados a la evidencia digital. Un tercero independiente debería poder examinar esos procesos y lograr el mismo resultado.
- Responsabilidad: La persona a cargo de la investigación tiene la responsabilidad general de garantizar que se cumplan la ley y estos principios.

El proceso de gestión de la evidencia digital establecido por la ACPO está compuesto por las siguientes fases o etapas [58]:

1. Plan: Debido a que en la actualidad existen innumerables dispositivos que pueden almacenar información, es necesario que los investigadores desarrollen las estrategias adecuadas para identificar la existencia de la evidencia digital y asegurar e interpretar esa evidencia a lo largo de su investigación.

2. Captura: En esta fase se realiza la captura de los dispositivos que pueden contener la potencial evidencia digital, los cuales deben ser apropiadamente manejados y confiscados, y deben tratarse con tanto cuidado como cualquier otro artículo que deba ser objeto de un examen forense.

Es necesario tener la mayor cantidad de información posible sobre la investigación antes de realizar la captura de los dispositivos, para garantizar que se tomen aquellos con la mejor evidencia. Del mismo modo, se debe documentar la escena ampliamente y a detalle, como soporte de las acciones realizadas.

3. Análisis: Una vez son capturados los dispositivos que contienen la potencial evidencia digital es necesario analizarlos. Debido al volumen y complejidad de los datos almacenados en los dispositivos digitales, no es posible o deseable extraer todos los datos contenidos en estos para ser analizados por los investigadores. Por lo tanto, se necesita formular una estrategia forense que permita que el análisis se enfoque la información relevante.

   Por otro lado, al igual que con cualquier otra evidencia forense, a menudo se requiere la interpretación para asegurar que el valor probatorio de la evidencia digital recuperada es claro. Los investigadores que realizan la interpretación de los datos digitales deben ser competentes y tener el entrenamiento suficiente para llevar a cabo la tarea asignada a ellos.

   Establecer la procedencia de la evidencia digital es otra tarea clave del profesional forense, quien debe usar sus conocimientos y habilidades para identificar no solo que la evidencia existe, sino también cómo llegó a estar allí. Es responsabilidad del forense que lleva a cabo el análisis identificar la procedencia cuando sea necesario, para mitigar el riesgo de que sus hallazgos sean malinterpretados.

   También debe tenerse en cuenta que el desarrollo de la tecnología digital es dinámico y que los profesionales pueden enfrentar desafíos significativos para su conocimiento. No es posible ser un experto en todos los aspectos del examen forense digital, pero un profesional debe ser consciente de los límites de su conocimiento y dónde se requiere más investigación o conocimiento especializado adicional.

4. Presentación: La siguiente fase del proceso es la presentación de los resultados o hallazgos. Un profesional forense digital debe ser consciente de su deber de imparcialidad y debe comunicar tanto el alcance como las limitaciones de la evidencia forense digital. Esto es especialmente importante ya que, debido a la naturaleza de la evidencia digital, no siempre es fácil su comprensión inmediata para las personas comunes.

   Los resultados pueden ser presentados de diversas maneras: verbalmente al investigador u oficial del caso, por medio de una declaración o informe con las conclusiones del caso o en la corte si es llamado como testigo.

ESTADOS UNIDOS – NATIONAL INSTITUTE OF JUSTICE NIJ

El Instituto Nacional de Justicia (NIJ por sus siglas en inglés) del Departamento de Justicia de los Estados Unidos expidió la guía titulada: “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” [59], la cual tiene como público objetivo a los oficiales de las fuerzas de ley y otros miembros de la comunidad de la justicia que son responsables del examen de evidencia digital.

Establece que el proceso de gestión de la evidencia digital debe garantizar la aplicación de los siguientes principios [59]:

- Inalterabilidad: Las acciones llevadas a cabo para asegurar o adquirir la evidencia digital no deben afectar la integridad de esa evidencia.
- Idoneidad: Las personas que conducen una investigación forense digital deben estar entrenadas para ese propósito.
- Documentación: Las actividades de captura, análisis, almacenamiento o transferencia de evidencia digital deben ser documentadas, preservadas y disponibles para revisión.

El procedimiento descrito por el NIJ en esta guía establece las siguientes etapas [59]:

1. Evaluación: Los investigadores forenses deben evaluar la evidencia digital profundamente con relación al alcance del caso para determinar el curso de acción a seguir.

   Para realizar una buena evaluación de la potencial evidencia digital, el investigador forense debe tener buena información sobre el caso para tomar las decisiones adecuadas sobre el orden de prioridad de la evidencia a adquirir, los dispositivos periféricos que podrían contener información adicional, entre otros aspectos que podrían ser importantes y relevantes para el caso.

2. Adquisición: La evidencia digital, por su propia naturaleza, es frágil y puede ser alterada, dañada o destruida por un manejo o examen inapropiado. Por lo que se necesitan precauciones especiales, dado que, en caso de no hacerlo, podría conducir a la inadmisibilidad de la evidencia o a conclusiones erróneas. El examen se realiza mejor en una copia de la evidencia original. La evidencia original debe adquirirse de manera que proteja y conserve la integridad. La cadena de custodia debe mantenerse y asegurarse durante todo el proceso.

3. Examen: El propósito de la fase de examen es extraer y analizar la evidencia digital. La extracción se refiere a la recuperación de los datos de los dispositivos o medios. El análisis se refiere a la interpretación de los datos recuperados y a ponerlos en un formato lógico y útil.

   Se deben seguir los siguientes pasos:

   a. *Preparación:* Alistar un directorio/directorios de trabajo en medios separados en los cuales serán almacenados los archivos y datos de evidencia recuperados o extraídos.

   b. *Extracción:* Existen dos tipos de extracciones: lógica y física. La fase de extracción física identifica y recupera datos a través de todo el dispositivo físico, sin tener en cuenta el sistema de archivos. Puede incluir los métodos de búsqueda de palabras clave, excavación de archivos y extracción de la tabla de particiones y espacio no utilizado del dispositivo físico.

      La fase de extracción lógica identifica y recupera archivos y datos con base en el(los) sistema(s) operativo(s) instalado(s), sistema(s) de archivos y/o aplicaciones. Esto puede incluir datos de archivos activos, borrados, archivos ocultos y espacio de archivos sin asignar.

c. *Análisis de los datos extraídos:* Es el proceso de interpretar los datos extraídos para determinar su relevancia para el caso. Algunos ejemplos de análisis que pueden ser llevados a cabo incluyen estampa de tiempo, datos ocultos, aplicaciones y archivos, propiedad y posesión. Esto podría requerir la revisión de las facultades legales que se tienen para el registro de la evidencia digital.

d. *Conclusión:* Por sí mismos, los resultados obtenidos de cualquiera de estos pasos pueden no ser suficientes para llegar a una conclusión. Sin embargo, cuando se ve como un todo, las asociaciones entre resultados individuales pueden proporcionar una imagen más completa. Como paso final en el proceso de examen, es necesario considerar los resultados de la extracción y el análisis en su totalidad.

4. Documentación y reporte: Las acciones y observaciones deben ser documentadas ampliamente durante todo el procesamiento forense de la evidencia. El investigador es responsable de informar de manera completa y precisa sus hallazgos y los resultados del análisis de la evidencia digital. Esto concluirá con la preparación de un informe escrito de los hallazgos, el cual debe estar dirigido hacia la audiencia prevista.

COMPARATIVO METODOLOGÍAS A NIVEL GOBIERNO

A partir del análisis de las metodologías a nivel gobierno identificadas en Argentina, México, Australia, Reino Unido y Estados Unidos, se realizó una correlación con el objetivo de identificar alcances, similitudes, diferencias, ventajas y desventajas.

Tabla 3-4: Tabla de análisis de ventajas y desventajas metodologías a nivel gobierno

País	Ventajas	Desventajas
ARGENTINA	• El procedimiento descrito abarca lineamientos técnicos para el aseguramiento de la evidencia. • Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Promueve la preservación de la calidad de la información durante todo el proceso forense, para darle validez a los hallazgos. • Relaciona la importancia de la documentación durante el proceso de la investigación.	• No incluye lineamientos relacionados con el uso de herramientas técnicas. • No incluye la fase de análisis y/o tratamiento de la información recolectada ni la presentación de resultados. • No presenta indicaciones ni lineamientos relacionados con la presentación de los resultados en un informe final. • No se hace alusión a la conservación de los principios de la evidencia digital.
MÉXICO	• Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Promueve la preservación de la calidad de la información durante todo el proceso forense, para darle validez a los hallazgos. • Abarca el proceso forense en todas sus fases, aunque sea de carácter general.	• Es de carácter general, por lo que no incluye procesos técnicos de la investigación. • No incluye lineamientos relacionados con el uso de herramientas técnicas. • No se hace alusión a la conservación de los principios de la evidencia digital.

País	Ventajas	Desventajas
	• Resalta la importancia de la documentación del proceso y la presentación de resultados en el informe final.	
AUSTRALIA	• El procedimiento descrito abarca lineamientos técnicos para el aseguramiento y procesamiento de la evidencia. • Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Promueve la preservación de la calidad de la información durante todo el proceso forense, para darle validez a los hallazgos. • Relaciona la importancia de la documentación durante el proceso de la investigación. • Abarca el proceso de investigación forense en todas sus fases. • Promueve la conservación de los principios de la evidencia digital.	• No incluye lineamientos relacionados con el uso de herramientas técnicas. • No presenta indicaciones ni lineamientos relacionados con la presentación de los resultados en un informe final.
ESTADOS UNIDOS	• Es de carácter específico y presenta lineamientos que abarcan los procesos técnicos del análisis forense. • Preserva la cadena de custodia como parte fundamental de todo el proceso forense. • Promueve la preservación de la calidad de la información durante todo el proceso forense. • Incluye lineamientos para el uso de herramientas forenses. • Brinda recomendaciones y lineamientos sobre la correcta documentación y reporte final de los resultados. • Abarca todo el proceso forense en todas sus fases, desde la adquisición hasta el reporte final de hallazgos. • Promueve la conservación de los principios de la evidencia digital: inalterabilidad, idoneidad y documentación.	
REINO UNIDO	• Presenta lineamientos que abarcan los procesos técnicos del análisis forense. • Preserva la cadena de custodia como parte fundamental de todo el proceso forense.	• Aunque presenta algunas recomendaciones sobre el uso de herramientas forenses, su alcance es general. • Presenta algunas recomendaciones generales sobre el reporte de los resultados.

País	Ventajas	Desventajas
	• Promueve la preservación de la calidad de la información durante todo el proceso forense. • Promueve la importancia de la correcta documentación de todo el proceso investigativo. • Abarca todo el proceso forense en todas sus fases, desde la adquisición hasta el reporte final de hallazgos. • Promueve la conservación de los principios de la evidencia digital: inalterabilidad, justificación, repetición y auditabilidad, responsabilidad.	

Nota. Fuente: Elaboración propia

El análisis de ventajas y desventajas de la normatividad de los países seleccionados permite concluir que, teniendo en cuenta los criterios de análisis definidos (descritos en la sección 2.1), la metodología establecida por Estados Unidos, 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 analizados para los objetivos de este proyecto, toda vez que no se observan desventajas frente a los aspectos analizados en cada criterio.

En general, se identificó que los países latinoamericanos (Argentina y México) tienen una normatividad 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.

Por otro lado, 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 3-5: Comparación de características – diferencias, similitudes, alcances metodologías a nivel gobierno

País / Aspecto	ARGENTINA	MÉXICO	AUSTRALIA	US NIJ - DEPARTMENT OF JUSTICE	REINO UNIDO
Número de fases	5	4	6	4	4
Público objetivo	Está dirigida a las fuerzas de ley a nivel nacional en Argentina.	Está dirigida a un público mayoritariamente nacional: autoridades periciales mexicanas.	Está dirigida a un público nacional: autoridades del sistema de justicia australiano, como respuesta a las exigencias de la Commonwealth of Nations (Mancomunidad de Naciones).	Está dirigida a los oficiales de las fuerzas de ley y otros miembros de la comunidad de la justicia que son responsables del examen de evidencia digital en los Estados Unidos.	Está dirigida al personal de las fuerzas de ley del Reino Unido que pueden manejar o gestionar la evidencia digital.
Alcance	Tiene un alcance general. Abarca los aspectos generales de la recolección y preservación de la evidencia digital. No abarca el análisis de esta.	Tiene un alcance específico. Abarca además el análisis y reporte de la información.	Tiene un alcance específico. Abarca el proceso desde la recolección hasta la presentación de la evidencia. Es un estándar de aplicación nacional en Australia.	Tiene un alcance específico. Abarca el proceso desde la recolección hasta la presentación de la evidencia.	Tiene un alcance específico. Abarca el proceso desde la recolección hasta la presentación de la evidencia.
Fases	Denuncia Allanamiento Secuestro de dispositivos Embalaje, transporte y almacenamiento Extracción de la prueba	Identificar la evidencia. Preservación de la evidencia. Analizar la evidencia. Presentar la evidencia.	Diseño de la evidencia. Producir registros. Recolección de evidencias. Análisis de la evidencia. Reporte y presentación. Determinar el valor probatorio de la evidencia.	Evaluación Adquisición Examen Documentación y reporte	Planeación Captura Análisis Presentación

País / Aspecto	ARGENTINA	MÉXICO	AUSTRALIA	US NIJ - DEPARTMENT OF JUSTICE	REINO UNIDO
Aspectos técnicos	Brinda lineamientos generales sobre aspectos técnicos de la investigación forense.	Es de carácter general, por lo que no incluye procesos técnicos de la investigación.	Abarca lineamientos técnicos para el aseguramiento y procesamiento de la evidencia.	Abarca lineamientos técnicos para el aseguramiento y procesamiento de la evidencia.	Abarca lineamientos técnicos para el aseguramiento y procesamiento de la evidencia.
Cadena de custodia	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.
Preservación de la calidad	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.
Herramientas técnicas	No tiene dentro de su alcance la fase de análisis, por lo que no menciona el uso de herramientas técnicas forenses.	No incluye lineamientos sobre el uso de herramientas técnicas forenses.	No incluye lineamientos sobre el uso de herramientas técnicas forenses.	Incluye lineamientos para el uso de herramientas técnicas forenses.	Incluye algunas recomendaciones generales sobre el uso de herramientas técnicas forenses.
Informe final y documentación	Resalta la importancia de la documentación de todo el proceso. Dado su alcance limitado del proceso forense, no presenta indicaciones ni lineamientos relacionados con la presentación de los	Resalta la importancia de la documentación del proceso y la presentación de resultados en el informe final.	Resalta la importancia de la documentación de todo el proceso. Sin embargo, no presenta indicaciones ni lineamientos relacionados con la presentación de los resultados en un informe final.	Resalta la importancia de la documentación del proceso y la presentación de resultados en el informe final.	Resalta la importancia de la documentación de todo el proceso. Presenta recomendaciones generales relacionadas con la presentación de los resultados.

Aspecto \ País	ARGENTINA	MÉXICO	AUSTRALIA	US NIJ - DEPARTMENT OF JUSTICE	REINO UNIDO
	resultados en un informe final.				
Proceso integral	No incluye la fase de análisis y/o tratamiento de la información recolectada ni la presentación de resultados.	Abarca el proceso forense en todas sus fases, aunque algunos aspectos son de carácter general.	Abarca el proceso forense en todas sus fases, aunque algunos aspectos son de carácter general.	Abarca el proceso forense en todas sus fases.	Abarca el proceso forense en todas sus fases.
Principios de la evidencia digital	No se hace alusión a la conservación de los principios de la evidencia digital.	No se hace alusión a la conservación de los principios de la evidencia digital.	Promueve la conservación de los principios de la evidencia digital.	Promueve la conservación de los siguientes principios: inalterabilidad, idoneidad y documentación.	Promueve la conservación de los siguientes principios: inalterabilidad, justificación, repetición y auditabilidad, responsabilidad.
Actualización	Expedida en 2016.	Expedida en 2016.	Publicado en 2003.	Publicado en 2004.	Publicado en 2012.

Nota. Fuente: Elaboración propia

Tabla 3-6: Tabla de valoración comparativa metodologías a nivel gobierno

País / Criterio	ARGENTINA	MÉXICO	AUSTRALIA	ESTADOS UNIDOS	REINO UNIDO
Aspectos técnicos	2	0	2	2	2
Cadena de custodia	2	2	2	2	2
Preservación calidad	2	2	2	2	2
Herramientas técnicas	0	0	0	2	1
Informe final y documentación	1	2	1	2	1
Proceso integral	1	2	2	2	2
Principios de la evidencia digital	0	0	2	2	2
TOTAL	**8**	**8**	**11**	**14**	**12**

Nota. Fuente: Elaboración propia

La valoración comparativa de cumplimiento total, parcial o nulo de los criterios de análisis definidos en la metodología (descritos en la sección 2.1) permite concluir que la metodología establecida por el Instituto Nacional de Justicia de los Estados Unidos 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.

De manera similar que, en el análisis de ventajas y desventajas, se puede observar que los países latinoamericanos (Argentina y México) tienen un cumplimiento parcial de los criterios del estudio (obtuvieron 8 de 14 puntos posibles, respectivamente). Vale la pena destacar que el grado de cumplimiento es similar en ambos países, lo que se ve determinado por la orientación hacia los primeros respondientes de los estándares y leyes identificadas. Por otro lado, Australia y Reino mostraron un cumplimiento mayor de los criterios, con 11 y 12 puntos, respectivamente.

3.1.3 Análisis de metodologías a nivel nacional

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 [13], [44] y disciplinario, por parte de la Procuraduría General de la Nación [46], sin embargo, “todavía no existen procedimientos realmente unificados en el país, 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” [65].

Por otro lado, es importante resaltar que en Colombia “desde la publicación de la política de seguridad digital en el país, es posible identificar el compromiso del gobierno en su marco institucional por seguir fortaleciendo las capacidades, instancias y entidades de ciberseguridad, como es evidenciado en el CONPES 3854, Política Nacional de Seguridad Digital” [67]. Es así, como dentro de la Estrategia de Gobierno Digital del Ministerio de las Tecnologías de Información y las Comunicaciones se expidió la “Guía N° 13 – Evidencia digital” [45], la cual es un documento guía no obligatorio ni vinculante para las entidades del Estado, que ofrece lineamientos para las investigaciones forenses digitales.

En este sentido, se realizará un análisis de cada uno de estos documentos teniendo en cuenta los aspectos que cada uno de ellos abarca. Debido a que no se trata de metodologías y/o procedimientos formalmente establecidos (en especial los de la Fiscalía General de la Nación) el análisis se ajustará al alcance de estos con relación al desarrollo de una investigación forense digital.

FISCALÍA GENERAL DE LA NACIÓN

En el año 2018, la Fiscalía General de la Nación en un trabajo conjunto con la Policía Nacional realizó la actualización del Manual del Sistema de Cadena de Custodia [13] y del Manual Único de Policía Judicial [44], documentos que rigen las actuaciones de los miembros de la fuerza pública en el desarrollo de investigaciones criminales y administrativas. Pese a que su contexto está orientado al desarrollo de investigaciones que no corresponden exclusivamente al ámbito de la informática forense, en dichos documentos se incluyeron orientaciones generales para el tratamiento de elementos materiales probatorios que contengan evidencia digital potencial.

Manual del Sistema de Cadena Custodia

Se resaltan las indicaciones sobre el correcto embalaje, transporte y manipulación de los elementos digitales como son dispositivos de almacenamiento (computadores, USB, discos duros, entre otros) y teléfonos celulares. En la sección 9 del manual de cadena de custodia [13]: “Formas de recolección, embalajes y recomendaciones prácticas para el manejo de EMP y EF” se encuentra la única referencia a la posible evidencia digital potencial, al incluir los dispositivos de almacenamiento y los teléfonos celulares en la subsección B, “Esquema de formas de recolección, embalajes y recomendaciones prácticas para el manejo de EMP y EF”.

No se trata de una metodología o procedimiento como tal para el proceso forense, por lo que su alcance solo está dado hacia los aspectos técnicos que tienen que ver con la recuperación de los elementos en las escenas y/o diligencias en campo.

Establece algunas recomendaciones técnicas sobre la correcta manipulación de los dispositivos, como por ejemplo evitar campos magnéticos, no encender si se encuentra apagado, apagar directamente desde la toma de corriente o retirar la batería si se trata de un computador encendido, no colocar rótulos o adhesivos directamente sobre la superficie del elemento, entre otras.

Manual Único de Policía Judicial

La única aproximación que se encuentra en este documento con relación a la evidencia digital es el apartado en el cual se brindan algunas recomendaciones generales para la recuperación de información producto de transmisión de datos a través de la red de comunicaciones, en la sección 3.10 específicamente.

Se brindan orientaciones técnicas generales sobre los procedimientos a seguir para el embalaje, transporte y manipulación de los dispositivos que puedan contener evidencia digital. De igual forma se dan algunas recomendaciones sobre las acciones que deben o no realizarse con los dispositivos, como por ejemplo evitar campos magnéticos, no encender si se encuentra apagado, apagar directamente desde la toma de corriente o

retirar la batería si se trata de un computador encendido, no colocar rótulos o adhesivos directamente sobre la superficie del elemento, entre otras.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC

Dentro del marco de la Estrategia de Gobierno Digital del MINTIC en el año 2016 se publicó la “Guía N° 13 – Evidencia digital” [45] en la cual se dan los lineamientos para realizar un proceso de informática forense adecuado dentro de un proceso de gestión de incidentes de seguridad de la información. En la actualidad es la aproximación más estructurada hacia una metodología nacional para el análisis forense en Colombia, pese a no ser un estándar o norma de obligatorio cumplimiento y tratarse solo de una guía de aplicación voluntaria y no vinculante para las entidades públicas.

El proceso presentado en la guía está compuesto por 5 fases [45]:

Figura 3-4: Diagrama del proceso de evidencia digital
Nota. Fuente: [45]

1. Fase I. Aislamiento de la escena: El primer paso dentro de la investigación es restringir el acceso a la zona donde se produjo el incidente de seguridad. Se debe documentar toda la escena, mediante la fijación fotográfica y/o en video; tomar en cuenta el estado de los dispositivos: apagado, encendido, realizando procesos de borrado, etc.; de igual

forma los investigadores deben asegurarse de contar con los elementos (hardware y software) necesarios para desarrollar todas las tareas.

Uno de los aspectos clave de todo el proceso es la cadena de custodia de los elementos y/o dispositivos que contienen la potencial evidencia digital. A este respecto se refiere el proceso de cadena de custodia de la Fiscalía General de la Nación [13].

2. Fase II. Identificación de fuentes de información, pasos iniciales de adquisición de información: En esta fase se debe, en primer lugar, identificar las potenciales fuentes de información, dentro de las que se encuentran computadores portátiles, de escritorio, medios de almacenamiento, entre otros.

   Finalmente, en esta fase se realizan los pasos iniciales para la adquisición de datos, los cuales comprenden la planificación de la prioridad de adquisición, teniendo en cuenta volatilidad de la información, complejidad para la obtención de los datos y la experiencia propia del investigador.

3. Fase III. Recolección y examinación de la información: Una vez realizada la adquisición de los dispositivos continúa la fase de recolección y examen de la información, para lo cual establece la siguiente secuencia de actividades:
   a. Creación del archivo / bitácora de hallazgos (cadena de custodia).
   b. Imagen de datos.
   c. Verificación de integridad de la imagen.
   d. Creación de una copia de la imagen suministrada.
   e. Aseguramiento de la imagen original suministrada.
   f. Revisión antivirus y verificación de la integridad de la copia de la imagen.
   g. Identificación de las particiones actuales y anteriores.
   h. Detección de información en los espacios entre las particiones.
   i. Detección de un HPA *(Host Protected Area).*
   j. Identificación del sistema de archivos.
   k. Recuperación de los archivos borrados.
   l. Recuperación de información escondida.
   m. Identificación de archivos existentes.
   n. Identificación de archivos protegidos.
   o. Consolidación de archivos potencialmente analizables.
   p. Determinación del sistema operativo y las aplicaciones instaladas.
   q. Identificación de información de tráfico de red.
   r. Depuración de archivos buenos conocidos.
   s. Consolidación de archivos sospechosos.
   t. Primera clasificación de archivos.
   u. Segunda clasificación de archivos.

4. Fase IV. Análisis de la información: En esta etapa se realiza un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada (después de realizar la depuración en las fases anteriores) [45].

   Se definen las siguientes etapas como parte integrante de esta fase:
   a. Análisis de la información prioritaria: De acuerdo con la depuración de archivos realizada en la fase anterior.

   b. Generación de listado de archivos comprometidos con el caso.
   c. Obtención de la línea de tiempo de la evidencia.
   d. Generación de informe final.

5. Fase V. Reporte: La etapa final del proceso es el reporte o presentación de toda la información y la evidencia que se obtuvo en el análisis. Se deben incluir todos los resultados, las herramientas utilizadas, los procedimientos realizados para la recolección y análisis de la información, etc. Es importante tener en cuenta la audiencia hacia la cual está dirigido el informe, con el fin de utilizar el lenguaje apropiado para ella.

PROCURADURÍA GENERAL DE LA NACIÓN

La Procuraduría General de la Nación como ente rector de la potestad disciplinaria en el país ha definido seis (6) procedimientos para el desarrollo de pruebas técnicas de informática forense, específicamente planteados para 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.

El objetivo de cada uno de estos procedimientos está definido como [46]:

1. Realizar imágenes forenses: Crear una copia (bit a bit) de dispositivos de almacenamiento digital y/o electrónico, vinculados en un proceso investigativo para recaudar el material probatorio que permitan determinar aspectos relevantes de la actuación disciplinaria.
2. Recolectar datos volátiles: Generar una imagen forense de la memoria RAM (datos volátiles) sin apagar el dispositivo que permita posteriormente en la fase de análisis “extraer” información valiosa del sistema operativo.
3. Tratamiento, procesamiento y análisis de evidencia digital: Garantizar la conservación, documentación, análisis y presentación de evidencias y que llegado el caso puedan ser aceptadas legalmente en un proceso disciplinario.
4. Tratamiento, procesamiento y análisis de dispositivos móviles: Garantizar la conservación, documentación, análisis de material probatorio y que llegado el caso puedan ser aceptadas legalmente en un proceso disciplinario.
5. Recuperación de información de medios de comunicación y fuentes abiertas: Recuperar la información dejada al navegar por Internet u otros medios tecnológicos como redes sociales, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen y esta evidencia material probatorio llegado el caso pueda ser aceptada legalmente en un proceso disciplinario.
6. Verificación y revisión de software, bases de datos y documentos electrónicos: Verificar que la información generada por los sistemas de información, aplicación, software, documentos electrónicos, bases de datos, cumplan con temas de autenticación, integridad, seguridad, confiabilidad y que estén salvaguardadas o resguardadas de accesos incorrectos que faciliten su adulteración.

Es importante tener en cuenta que estos procedimientos no hacen parte de ninguna metodología o protocolo formalmente establecido, sino que fueron definidos como parte del Sistema de Gestión de la Calidad de la entidad y, en consecuencia, carecen de una

estructura formal dentro de una investigación forense. Sin embargo, se resalta que son un intento de estandarización y estructuración con el fin de establecer al interior de la entidad una metodología para el desarrollo de los apoyos técnico científicos requeridos ante la Dirección Nacional de Investigaciones Especiales.

COMPARATIVO METODOLOGÍAS A NIVEL NACIONAL

A partir del análisis de las aproximaciones identificadas a nivel nacional por parte de la Fiscalía General de la Nación, el Ministerio de las Tecnologías de Información y las Comunicaciones y la Procuraduría General de la Nación, se realizó una correlación con el objetivo de identificar alcances, similitudes, diferencias, ventajas y desventajas.

Tabla 3-7: Análisis de ventajas y desventajas de metodologías a nivel nacional

Entidad	Ventajas	Desventajas
FISCALÍA GENERAL DE LA NACIÓN	• El procedimiento descrito abarca algunos lineamientos técnicos generales para el aseguramiento de la evidencia. • Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Promueve la preservación de la calidad de la información durante todo el proceso, para darle validez a los hallazgos. • Relaciona la importancia de la documentación durante el proceso de la investigación.	• No se trata de metodologías formales para la investigación forense digital. • No incluye lineamientos relacionados con el uso de herramientas técnicas. • Tienen un alcance limitado, por lo cual solo abarca el aseguramiento de la prueba. No incluye la fase de análisis y/o tratamiento de la información recolectada ni la presentación de resultados. • No presenta indicaciones ni lineamientos relacionados con la presentación de los resultados en un informe final. • No se hace alusión a la conservación de los principios de la evidencia digital.
MINTIC	• Tiene un alcance específico, por lo que incluye aspectos técnicos de la investigación. • Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • Promueve la preservación de la calidad de la información durante todo el proceso forense, para darle validez a los hallazgos. • Incluye lineamientos generales sobre el uso de herramientas técnicas. • Resalta la importancia general de la documentación del proceso y la presentación de resultados en el informe final. • Abarca el proceso forense en todas sus fases, aunque sea de carácter general.	• No incluye lineamientos específicos sobre la correcta presentación de los resultados y/o elaboración del informe final. • No se hace alusión a la conservación de los principios de la evidencia digital.

Entidad	Ventajas	Desventajas
PGN	• El procedimiento descrito abarca algunos lineamientos técnicos generales para el manejo de la evidencia. • Hace especial énfasis en la conservación de la cadena de custodia sobre la evidencia digital. • En términos generales promueve la preservación de la calidad de la información durante todo el proceso forense. • Incluye lineamientos generales sobre el uso de herramientas técnicas. • Relaciona la importancia de la documentación durante el proceso de la investigación.	• No se trata de metodologías formales para la investigación forense digital. • No presenta indicaciones ni lineamientos relacionados con la presentación de los resultados en un informe final. • Tienen un alcance limitado, por lo cual solo abarca algunos aspectos del proceso forense. No ofrece lineamientos sobre el análisis y/o tratamiento de la información recolectada ni la presentación de resultados. • No se hace alusión a la conservación de los principios de la evidencia digital.

Nota. Fuente: Elaboración propia

El análisis de ventajas y desventajas permite concluir que, teniendo en cuenta los criterios de análisis definidos (descritos en la sección 2.1), el procedimiento de “Evidencia Digital” definido por el Ministerio de las Tecnologías de Información y las Comunicaciones – MINTIC [45] es el que presenta menos desventajas frente a los criterios de interés para los objetivos de este proyecto. Se identificó un procedimiento estructurado que resulta una buena primera aproximación del gobierno colombiano hacia una metodología de análisis forense. Sin embargo, presenta falencias frente a aspectos muy importantes como son la presentación de resultados e informe final y el aseguramiento de los principios de la evidencia digital.

Tabla 3-8: Comparación de características – diferencias, similitudes, alcances metodologías a nivel nacional

Entidad / Aspecto	FISCALÍA GENERAL DE LA NACIÓN	MINTIC	PROCURADURÍA GENERAL DE LA NACIÓN
Número de fases	N/A	5	N/A
Público objetivo	Funcionarios públicos con funciones de policía judicial que realicen diligencias de campo donde se encuentren dispositivos digitales.	Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital.	Funcionarios de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación encargados del desarrollo de las pruebas técnicas en informática forense.
Alcance	No se trata de metodologías formales para la investigación forense digital. Tienen un alcance muy limitado que se reduce al	Tiene un alcance específico. Abarca el proceso desde la recolección hasta la presentación de la evidencia.	No es una metodología formal para la investigación forense. Son procedimientos generales de actuación

Entidad / Aspecto	FISCALÍA GENERAL DE LA NACIÓN	MINTIC	PROCURADURÍA GENERAL DE LA NACIÓN
	embalaje, transporte y manipulación de dispositivos digitales.		para el desarrollo de pruebas técnicas.
Fases	N/A	Aislamiento de la escena Identificación de fuentes de información Examinación y recolección de información Análisis de datos Reporte	N/A
Aspectos técnicos	Presentan algunas recomendaciones técnicas generales para la manipulación de potencial evidencia digital.	Abarca lineamientos técnicos para el aseguramiento y procesamiento de la evidencia.	Presentan algunas recomendaciones técnicas generales para la adquisición y manipulación de la evidencia digital.
Cadena de custodia	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.	Resalta la importancia del mantenimiento de la cadena de custodia durante todo el proceso.
Preservación de la calidad	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	Promueve la preservación de la calidad de la información como mecanismo para garantizar la validez de los resultados.	La preservación de la calidad de la información se trata en términos generales.
Herramientas técnicas	Menciona algunas recomendaciones sobre el uso de herramientas técnicas para el desarrollo de algunos procedimientos.	Incluye algunas recomendaciones generales sobre el uso de herramientas técnicas forenses.	Menciona algunas recomendaciones sobre el uso de herramientas técnicas para el desarrollo de algunos procedimientos.
Informe final y documentación	Resalta la importancia de la documentación de todo el proceso. Presenta recomendaciones generales limitadas relacionadas con la presentación de los resultados en el informe de investigador de campo.	Resalta la importancia de la documentación de todo el proceso. Presenta recomendaciones generales relacionadas con la presentación de los resultados.	Resalta la importancia de la documentación de todo el proceso. Presenta recomendaciones generales relacionadas con la presentación de los resultados.
Proceso integral	No abarca el proceso forense. Brinda solo algunas recomendaciones durante la fase de recolección.	Abarca el proceso forense en todas sus fases.	No abarca el proceso forense. Brinda solo algunas recomendaciones durante la fase de recolección.

Entidad / Aspecto	FISCALÍA GENERAL DE LA NACIÓN	MINTIC	PROCURADURÍA GENERAL DE LA NACIÓN
Principios de la evidencia digital	No se hace alusión a la conservación de los principios de la evidencia digital.	No se hace alusión a la conservación de los principios de la evidencia digital.	En algunos procedimientos se hace alusión a la conservación de los principios de la evidencia digital.
Actualización	Actualizado en 2018.	Publicado en 2016.	Publicados en 2018.

Nota. Fuente: Elaboración propia

Tabla 3-9: Tabla de valoración comparativa metodologías a nivel nacional

Entidad / Criterio	FISCALÍA GENERAL DE LA NACIÓN	MINTIC	PROCURADURÍA GENERAL DE LA NACIÓN
Aspectos técnicos	1	2	1
Cadena de custodia	2	2	2
Preservación calidad	2	2	1
Herramientas técnicas	1	2	1
Informe final y documentación	1	1	2
Proceso integral	1	2	1
Principios de la evidencia digital	0	0	1
TOTAL	**8**	**11**	**9**

Nota. Fuente: Elaboración propia

La valoración comparativa de cumplimiento total, parcial o nulo de los criterios de análisis definidos en la metodología (descritos en la sección 2.1) permite concluir que no existe una metodología de análisis forense digital en el país que cumpla a cabalidad todos los criterios de interés definidos para este proyecto; lo cual, a su vez, permite agregar valor a este trabajo ya que se brindaría una alternativa de solución a la necesidad identificada.

Así las cosas, luego del análisis realizado de las metodologías identificadas a nivel nacional e internacional, aquellas que obtuvieron una calificación total de catorce (14) puntos fueron la norma NIST 800-86 y la metodología del NIJ de Estados Unidos, las cuales cumplen a cabalidad cada uno de los siete (7) criterios de evaluación. En consecuencia, estas serán las normas que se utilizarán para el diseño de la metodología objeto del presente trabajo.

Tabla 3-10: Tabla de valoración comparativa final

Metodología / Criterio	ISO/IEC 27037	NIST SP 800-86	Argentina	México	Australia	US NIJ	Reino Unido	FGN	MINTIC	PGN
Aspectos técnicos	0	2	2	0	2	2	2	1	2	1
Cadena de custodia	2	2	2	2	2	2	2	2	2	2
Preservación calidad	2	2	2	2	2	2	2	2	2	1
Herramientas técnicas	0	2	0	0	0	2	1	1	2	1

Metodología / Criterio	ISO/IEC 27037	NIST SP 800-86	Argentina	México	Australia	US NIJ	Reino Unido	FGN	MINTIC	PGN
Informe final y documentación	1	2	1	2	1	2	1	1	1	2
Proceso integral	1	2	1	2	2	2	2	1	2	1
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. Fuente: Elaboración propia

3.2 Clasificación de normatividad colombiana

Para el análisis se tomó como punto de partida la normativa nacional relacionada en el Anexo C del documento CONPES 3854 – Política de seguridad digital [68], actualizada al año 2019, concerniente con asuntos de seguridad digital.

En cada norma se realizó la identificación de artículos específicos que tuvieran alguna relación con la seguridad informática (SI) y/o informática forense (IF), obteniendo los siguientes resultados:

Tabla 3-11: Clasificación de normatividad colombiana (1999 – 2019)

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Constitución Política	Artículos 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.		X
Ley 527 de 1999 (Comercio electrónico y mensajes de datos)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 12º, 13º y 28º), la integridad y fuerza probatoria de un mensaje de datos (artículos 9°, 10° y 11°), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).		X
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.		X
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano. TÍTULO VII BIS. DE LA PROTECCIÓN DE LA INFORMACIÓN Y LOS DATOS (adicionado por el artículo 1 de la Ley 1273 de 2009), establece los delitos informáticos penados por la ley colombiana.		X
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal. TÍTULO VI. PRUEBAS. CAPÍTULO III. PRUEBA PERICIAL. Artículo 251. Requisitos. Establece los requisitos generales que deben tener las pruebas periciales. Es posible establecer que estos requisitos deben ser cumplidos también por los dictámenes de informática forense. Artículo 257. Criterios para la apreciación del dictamen. Artículo 288. Cadena de custodia. Sin embargo, no involucra artículos específicos relacionados con la seguridad informática y/o informática forense.		X
Ley 679 de 2001 (Pornografía y	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de		X

[2] SI: Seguridad Informática
[3] IF: Informática Forense

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
explotación sexual con menores)	Tecnologías de la Información y las Comunicaciones-, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.		
Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004). Artículo 236. Recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones. LIBRO II. TÍTULO I. CAPÍTULO V. CADENA DE CUSTODIA (Artículos 254-266).	X	
Ley 962 de 2005 (racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.		X
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).		X
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).		X
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.	X	
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales con relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.		X
Ley 1273 de 2009 (Delitos Cibernéticos)	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 TIC”.		X

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)	A través de esta ley se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC, en primer lugar establece en el artículo 4 (autorregulación de café internet códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.		X
Ley 1341 de 2009 (Sector TIC)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones		X
Decreto 1727 de 2009 (Habeas Data)	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.		X
Decreto 2952 de 2010 (Habeas Data)	Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial.		X
Ley 1437 de 2011 (Uso de medios electrónicos Procedimiento Administrativo Electrónico)	Código de Procedimiento Administrativo y de lo Contencioso Administrativo. PARTE PRIMERA. TÍTULO III. CAPÍTULO IV. Consagra la utilización de medios electrónicos en el procedimiento administrativo permitiendo adelantar los trámites y procedimientos administrativos por medios electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen por medios electrónicos con validez jurídica y probatoria.		X
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. Se modifica el artículo 236 de la Ley 906 de 2004: Recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones.	X	

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Ley 1474 de 2011 (Uso de medios tecnológicos)	Esta norma permite la utilización de medios tecnológicos en los trámites y procedimientos judiciales, en las diligencias, práctica de pruebas y notificaciones de las decisiones.		X
Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad)	Se incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico. El artículo 26 de esta Ley, consagra que la SIC determinará las condiciones mínimas bajo las cuales operar la información pública de precios de los productos que se ofrezcan a través de cualquier medio electrónico. CAPÍTULO VI. PROTECCIÓN AL CONSUMIDOR DE COMERCIO ELECTRÓNICO.		X
Ley 1564 de 2011 (Uso de las TIC)	Permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.		X
Resolución CRC 3066 de 2011	Se establece el régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones. En particular, se establece que los proveedores de servicios de comunicaciones deberán implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor.		X
Resolución CRC 3067 de 2011	Se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones. Está Resolución establece en el artículo 2.3, que los proveedores que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia de este.	X	
Resolución CRC 3502 de 2011 (Neutralidad de Internet)	A través de la Resolución CRC 3502 de 2011, se establecen condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011 (PND 2010 2014). Se contempla en el artículo 3 los principios de libre elección, no discriminación, transparencia e información, que deben aplicar los proveedores que prestan el servicio de acceso a internet. El artículo 6 recalca las medidas de seguridad en la red.	X	
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios. El artículo 4 establece los principios rectores para el tratamiento de datos personales, dentro de los cuales se encuentra el literal g. “Principio de seguridad”.	X	

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Ley 1712 de 2012 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.		X
Decreto 1704 de 2012 (Interceptación legal de comunicaciones)	Este Decreto determina que la interceptación legal de comunicaciones es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional, deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.		X
Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente le encarga a la Dirección de seguridad pública y de infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.		X
Decreto Ley 019 de 2012 (Entidades de Certificación Digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999, entre otras.		X
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.		X

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Decreto 2364 de 2012 (Firma electrónica)	Establece la reglamentación del artículo 7º de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Se definen algunas características que benefician el uso de los medios electrónicos, tales como la definición de los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación, la fijación de la relación de género y especie entre firmas electrónicas y firmas digitales, señalando las diferencias en su tratamiento probatorio, pues en el último mecanismo existe una inversión probatoria, y el uso de la firma electrónica mediante acuerdo de las múltiples partes de una relación jurídica, entre otras.		X
Resolución 3933 de 2013 (Ministerio de Defensa Nacional)	Creó el Grupo colCERT y asignó funciones a la dependencia de la Dirección de seguridad pública y de infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.	X	
Decreto 1377 de 2013 (Habeas Data)	Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.		X
Ley 1621 de 2013 – Ley de inteligencia y contrainteligencia en Colombia	Esta ley expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.		X
Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el Documento CONPES 3701, creó a través de este decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.		X
Decreto 333 de 2014 (Habeas Data)	Se reglamenta el artículo 160 del Decreto 019 de 2012, definiendo el régimen de acreditación de las entidades de certificación abierta, se deroga el Decreto 1747 de 2000, que reglamenta de manera parcial la Ley 527 de 1999, referente a las entidades de certificación digital, certificados y firmas digitales, de manera que las entidades que deseen seguir prestando los servicios de certificación digital, deberán iniciar la		X

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
	correspondiente acreditación, ya no ante la Superintendencia de Industria y Comercio, sino ante el Organismo de Acreditación en Colombia (ONAC).		
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos. Se reglamenta la información mínima que debe contener dicho registro, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.		X
Decreto 2573 de 2014 (Gobierno en Línea)	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. TÍTULO II. COMPONENTES, INSTRUMENTOS Y RESPONSABLES. Artículo 5. Componentes, literal 4. Seguridad y privacidad de la información.		X
Decreto 1070 de 2015 (Decreto Único Reglamentario del Sector Defensa)	Por medio del cual se expide el Decreto único reglamentario del sector defensa, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Se establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos.		X
Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo)	Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012, 333 de 2014, entre otros.		X
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. TÍTULO 9 POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPÍTULO 1 POLÍTICA DE GOBIERNO DIGITAL; Artículo 2.2.9.1.1.3. Principios (Seguridad de la información)	X	
Circular Externa SIC 02 del 3 de noviembre de 2015	Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015.		X
Directiva 6 de 11 de octubre de 2016	Establece el cumplimiento de la obligaciones de la Procuraduría General de la Nación como sujeto obligado de la Ley 1712 de 2014 y demás normas reglamentarias.		X

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
(Procuraduría General de la Nación)			
Decreto 1759 de 2016	Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.		X
Resolución 5050 de 2016 (Comisión de Regulación de Comunicaciones)	Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones.	X	
Resolución 5076 de 2016 (Comisión de Regulación de Comunicaciones)	Por la cual se modifica el Título Reportes de Información de la Resolución CRC 5050 de 20 de noviembre de 2016, relacionado con el Reporte de Información Periódica por parte de los Proveedores de Redes y Servicios de Telecomunicaciones, los Operadores de Televisión y los Operadores de Servicios Postales, a la Comisión de Regulación de Comunicaciones, y se dictan otras disposiciones.		X
Resolución 5079 de 2017 (Comisión de Regulación de Comunicaciones)	Por la cual se modifica la Sección 2 del Capítulo 2 del Título Reportes de Información de la Resolución CRC 5050 de 10 de noviembre de 2016.		X
Circular Nº 1 de 2017 de la Superintendencia de Industria y Comercio	Modifica el Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio, relacionados con el procedimiento de inscripción en el Registro Nacional de Bases de Datos — RNBD y la información contenida en este, teniendo en cuenta la modificación del plazo para inscribir las bases de datos, efectuada mediante el Decreto 1759 de 2016, incorporado al Decreto Único 1074 de 2015- Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.		X
Resolución 5111 de 2017 (Comisión de Regulación de Comunicaciones)	Por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones y se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 10 de noviembre de 2016 y se dictan otras disposiciones. Deroga la resolución 3066 de 2011, salvo el artículo 88 de la misma y las definiciones contenidas en los numerales 1.6, 1.7, 1.43, 1.49, 1.50, 1.67, 1.68, 1.69, 1.79, 1.119, 1.163, 1.170, 1.175, 1.189, 1.191, 1.194, 1.214, 1.217, 1.227, 1.229, 1.233, 1.247, 1.252, 1.259, 1.266.		X
Circular Externa 5 de 2017 (Superintendencia de Industria y Comercio)	Adiciona un Capítulo Tercero (Transferencia de datos personales a terceros países) al Título V de la Circular Única.		X

Normatividad	Resumen	Artículos relacionados con SI[2] y/o IF[3]	
		Sí	No
Resolución 5199 de 2017 (Comisión de Regulación de Comunicaciones)	Por la cual se modifica el artículo 12 de la Resolución CRC 5111 de 24 de febrero de 2017, modificando el plazo de cumplimiento para los operadores de servicios de comunicaciones del nuevo régimen de protección de los usuarios de servicios de comunicaciones.		X
Circular 8 de 2017 (Superintendencia de Industria y Comercio)	Modifica el numeral 3.2 del Capítulo Tercero, del Título V de la Circular Única, con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio.		X
Decreto 90 del de 2018 (Ministerio de Comercio, Industria y Turismo)	Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 – Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, con el fin de modificar los plazos de inscripción de las bases de datos de los sujetos obligados en el Registro Nacional de Bases de Datos.		X
Circular Única, de 28 de marzo de 2018 (Superintendencia de Industria y Comercio)	Circular Única, TÍTULO V.- PROTECCIÓN DE DATOS PERSONALES, se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en este Título.		X
Ley 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de Derecho de Autor y Derechos Conexos.		X
Ley 1928 de 2018	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.		X
Circular Externa 3 de 2018 (Superintendencia de Industria y Comercio)	Modifica los numerales 2.1 al 2.4 y elimina los numerales 2.5 al 2.7 del Capítulo Segundo, del Título V de la Circular Única de la Superintendencia de Industria y Comercio, en relación con el Registro Nacional de Bases de Datos – RNBD.		X
Circular externa Nº 1 de 2019 (Superintendencia de Industria y Comercio)	Recuerda a los sujetos obligados de la Ley 1581 de 2012 sobre la obligación de registro de bases de datos en el Registro Nacional de Bases de Datos – RNBD.		X

Nota. Fuente: Elaboración propia a partir del compendio de normas de [68]

El análisis de la legislación colombiana permitió identificar la existencia de nueve (9) 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. Lo anterior permite concluir, de manera preliminar, que en el país 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 utilicen e implementen, 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.

Ahora bien, una vez identificadas las normas con artículo(s) relacionado(s) con la seguridad informática y/o informática forense, se procedió con la siguiente etapa de clasificación, que corresponde a la correlación con los siete (7) criterios de análisis definidos en la etapa anterior; este análisis arrojó los resultados ilustrados en la Tabla 3-12.

Tabla 3-12: Tabla de cumplimiento de criterios de análisis – Normas entre 1999 – 2019

Criterios / Normatividad relacionada	C1		C2		C3		C4		C5		C6		C7	
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	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 C3: Preservación calidad C5: Informe final y documentación C7: Principios de la evidencia digital
C2: Cadena de custodia C4: Herramientas técnicas C6: Proceso integral

Nota. Fuente: Elaboración propia

Como resultado del análisis anterior se pudo determinar que no existe una normatividad que de alguna forma regule o reglamente la práctica de la informática forense o la realización de un análisis forense en el país. 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 permite concluir que su aplicación está orientada principalmente a la evidencia física, más no a la evidencia digital.

Sin embargo, en aplicación del principio de equivalencia funcional introducido con la Ley 527 de 1999, para el desarrollo de la metodología objeto del presente trabajo se realizará la integración del régimen de cadena de custodia de acuerdo con lo dictaminado por la Fiscalía General de la Nación.

3.3 Metodología propuesta

Partiendo del análisis e integración de las dos metodologías escogidas como resultado de la primera fase de este trabajo, para el desarrollo de una investigación forense se propone un proceso compuesto por las siguientes cinco (5) etapas:

Figura 3-5: Metodología de investigación forense propuesta
Nota. Fuente: Elaboración propia

A través de las etapas propuestas se transforman los medios en datos, luego de estos se extrae la información de interés para finalmente convertirse en la evidencia probatoria del caso en estudio.

1. **Evaluación:** El primer paso es evaluar las posibles fuentes de evidencia digital potencial con relación al alcance del caso. La evaluación del alcance del caso permitirá identificar las fuentes de datos relevantes y de esta forma orientar el sentido de la investigación.

2. **Adquisición:** El siguiente paso es la adquisición de la evidencia de su fuente original. 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:** Durante la examinación se aplican procedimientos y técnicas forenses para extraer y/o recuperar la información de las evidencias adquiridas. Mediante la utilización de métodos automáticos y/o manuales se realiza la extracción, preservando

siempre la integridad de los datos. Debe seguirse respetando el procedimiento de cadena de custodia.

4. **Análisis:** En esta fase se interpretan los datos recuperados y se traducen a un formato legible. Consiste en analizar los resultados de la examinación mediante la implementación de métodos y técnicas científicas y legalmente aceptadas para obtener información útil que dé respuesta a los planteamientos que dieron origen a la investigación.

5. **Reporte:** La fase de reporte de resultados consiste en la preparación del informe escrito con los hallazgos. La documentación es un proceso que debe ejecutarse en paralelo durante toda la investigación forense, haciendo un apropiado registro de todas las observaciones que se generen. De esta forma, el reporte de los resultados puede incluir la descripción de las acciones realizadas, explicación de las herramientas y procedimientos seleccionados, recomendaciones de otras acciones requeridas, entre otros.

Paralelo a estas cinco (5) etapas, debe llevarse un proceso riguroso de cadena de custodia y una documentación detallada.

3.3.1 Principios forenses generales aplicables

El procesamiento apropiado de la evidencia es fundamental para resolver incidentes de seguridad o disputas en entornos corporativos, así como también en asuntos criminales, administrativos y disciplinarios. Por lo tanto, se definen unos principios generales aplicables a todas las ciencias forenses [60] y que deben tenerse en cuenta en cada etapa de la investigación.

1. Intercambio de evidencia

La tarea de todo analista forense es descubrir vínculos convincentes entre el delincuente, la víctima y la escena del crimen. De acuerdo con el principio de intercambio de Locard, el contacto entre dos elementos resultará en un intercambio. Este principio aplica en todos los ámbitos o contextos; en cualquier contacto en una escena del crimen, incluyendo al delincuente con la víctima, entre una persona y un arma, y entre las personas y la escena del crimen. En resumen, siempre habrá evidencia de la interacción, aunque en algunas ocasiones esta no sea fácilmente detectable.

Esta transferencia ocurre en ambas esferas, física y digital, y puede proporcionar vínculos entre ellas, como los ilustrados en la siguiente figura:

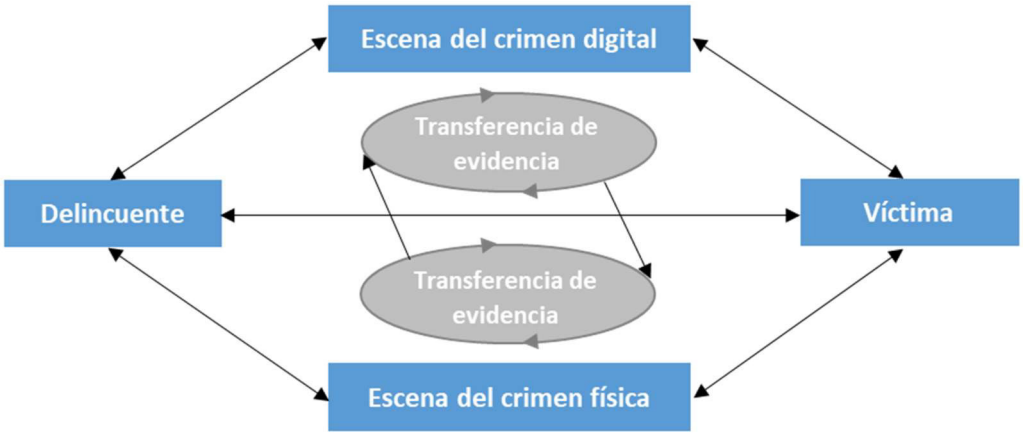


Figura 3-6: Ciclo de transferencia de evidencia
Nota. Fuente: Elaboración propia a partir de [60]

Por lo tanto, la tarea del investigador forense es identificar los rastros de ese intercambio, la transferencia de la evidencia.

2. Características de la evidencia

Los intercambios que ocurren entre los individuos y la escena del crimen producen evidencias que pertenecen a una de dos categorías generales: (1) evidencia con atributos que encajan en el grupo llamado *características de clase* y (2) evidencia con atributos que encajan en el grupo llamado *características individuales*. Las características de clase son rasgos comunes en elementos similares, mientras que las características individuales son más únicas y pueden ser vinculadas a una persona o actividad con mayor certeza.

Consideremos el ejemplo del mundo físico de una huella de zapato dejada debajo de una ventana en la escena del crimen. El análisis forense de esas impresiones solo puede revelar la marca y el modelo del zapato, colocándolo en la clase de todos los zapatos de la misma marca y modelo. Por lo tanto, si se descubre que un sospechoso posee un par de la misma marca y modelo, se puede establecer un vínculo circunstancial tenue entre el sospechoso y el delito. Si el análisis forense revela patrones de desgaste detallados en las huellas de los zapatos y se encuentra un desgaste idéntico de las suelas del sospechoso, es posible establecer un vínculo mucho más fuerte. El margen de error se reduce significativamente por el descubrimiento de una característica individual, lo que hace que el vínculo sea mucho menos circunstancial y más difícil de refutar.

En el ámbito digital, nos encontramos en un espacio más virtual y menos tangible. El intercambio de evidencia digital a menudo implica una copia de los datos que se transfieren, dejando al original prácticamente inalterado. Además, la propia noción de identidad individual es un reto frente al anonimato que existe en algunas comunidades de Internet. A pesar de estos problemas, los intercambios de evidencia en el ámbito digital dejan rastros con características de clase e individuales que pueden usarse para ayudar a responder preguntas cruciales o incluso resolver un caso.

En consecuencia, el investigador forense 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 forense es la documentación. Un caso sólido se basa en la documentación soporte que establece dónde se originó la evidencia y cómo fue manejada. Desde un punto de vista forense, el proceso de adquisición debe cambiar la evidencia original lo menos posible y cualquier cambio debe documentarse y evaluarse en el contexto de los resultados finales. 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. Sin embargo, en algunos casos este proceso es más sutil, dado que, desde el punto de vista técnico, no siempre es posible realizar esta comparación; por ejemplo, en el caso de la memoria RAM de un computador. Esta está en constante cambio y los contenidos capturados en determinado momento son una instantánea de ese momento y no existe un “original” para comparar.

De hecho, la autenticación es un proceso de dos pasos, con un examen inicial de la evidencia para determinar que es lo que afirma su proponente y, más tarde, un análisis más detallado para determinar su valor probatorio.

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. Por tal motivo, se debe dar un estricto cumplimiento al procedimiento de cadena de custodia establecido por la Fiscalía General de la Nación.

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. En el análisis forense, el proceso de verificación de integridad de la evidencia generalmente implica una comparación de la huella digital (hash) de esa evidencia tomada en el momento de la adquisición con la huella digital (hash) de la evidencia 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.

En consecuencia, el investigador debe mantener la objetividad, dejando que la evidencia hable por sí misma tanto como sea posible. Cada conclusión debe presentarse junto con toda la evidencia objetiva de soporte. Otro enfoque efectivo para garantizar la objetividad es tener un proceso de revisión por pares que evalúe los hallazgos de un analista forense en busca de sesgos o cualquier otra debilidad.

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.

Para posibilitar tal verificación de los hallazgos forenses, es importante documentar los pasos que se siguieron para encontrar, adquirir y analizar la evidencia digital con suficiente detalle para que otros puedan verificar los resultados independientemente. Esta documentación puede incluir la ubicación y otras características de la evidencia digital, así como las herramientas utilizadas para analizar los datos.

3.3.2 Definición de cada etapa metodológica

ETAPA 1: EVALUACIÓN

Principio: Durante esta fase se busca que la evidencia digital sea ampliamente evaluada con relación al alcance del caso para determinar el curso de acción.

Procedimiento: Realice una evaluación exhaustiva revisando la orden de solicitud de apoyo investigativo o el auto de investigación que lo faculta, los detalles del caso, la naturaleza del hardware y el software, la evidencia potencial buscada y las circunstancias que rodean la adquisición de la evidencia que se examinará.

Evaluación del caso

- Revisar la solicitud de investigación del operador disciplinario y/o administrativo.
    - Identificar la autoridad legal que le confieren: si cuenta con funciones de policía judicial o no. Si es necesaria orden jurisdiccional o no.
    - Verificar la completa documentación de la cadena de custodia. Correcto diligenciamiento de los formatos vigentes establecidos por la Fiscalía General de la Nación y el estado del(los) contenedor(es) de la evidencia recibida, si aplica.
- Analizar el expediente del caso e identificar las acciones realizadas por el operador disciplinario y/o administrativo y el estado actual de la investigación.

Evaluación de la evidencia digital potencial

- Identificar las posibles fuentes de evidencia digital.

- Analizar el contexto del caso para identificar los dispositivos (computadores, servidores, dispositivos de red, dispositivos de almacenamiento, etc.) que pueden contener la evidencia digital de interés.
- Considerar la relevancia de tener en cuenta fuentes periféricas de información para la investigación, como por ejemplo escáneres, impresoras, documentos, etc.
- Determinar la evidencia digital potencial que se busca, es decir, intente identificar el tipo de elemento probatorio que prueba el caso (por ejemplo, fotografías, correos electrónicos, documentos de texto, hojas de cálculo, bases de datos, registros financieros, etc.).
- Identificar información adicional necesaria que esté relacionada con el caso como, por ejemplo, cuentas de correo, configuración de red y usuarios, registros del sistema, que deba solicitarse a la entidad.
- Identificar y evaluar la posible existencia de fuentes de evidencia digital potencial en otras ubicaciones.

Evaluación del sitio de procesamiento

- El conocimiento del caso permitirá determinar el sitio donde el procesamiento debería ocurrir. Siempre es preferible llevar a cabo el examen y procesamiento de la evidencia en un ambiente controlado, como un laboratorio o un área dedicada al análisis forense. Sin embargo, siempre que las circunstancias requieran un examen in situ, intente controlar el medio ambiente. Algunas consideraciones pueden incluir:

  - El tiempo que se requiere en el sitio para lograr la recuperación de la evidencia.
  - Posibles problemas logísticos y de personal asociados con el despliegue a largo plazo.
  - El impacto en el negocio debido a una larga búsqueda.
  - La idoneidad de los equipos, recursos, medios, capacitación y experiencia para un examen in situ.

ETAPA 2: ADQUISICIÓN

Principio: La evidencia digital, por su propia naturaleza, es frágil y puede ser alterada, dañada o destruida por un manejo o examen inapropiado. Por lo que se necesitan precauciones especiales, dado que, en caso de no hacerlo, podría conducir a la inadmisibilidad de la evidencia o a conclusiones erróneas, lo que limitaría el valor probatorio del informe técnico.

Procedimiento: Adquiera la evidencia digital original de forma que se proteja y conserve la integridad.

Para llevar a cabo el proceso de adquisición de los datos se deben tener en cuenta tres (3) pasos principales:

1. **Planear la adquisición:** Con el conocimiento del caso desarrollado en la etapa anterior, es posible planificar la forma en la que se extraerá la información de las posibles fuentes identificadas. Para esto se deben priorizar las fuentes y establecer el orden en que se adquirirán los datos. Algunos factores importantes para establecer la priorización son:

- *Valor probable:* Teniendo en cuenta su propia experiencia con casos similares anteriores y su entendimiento y comprensión del caso actual, el analista debería poder estimar el valor probable relativo de cada fuente de datos potencial.

- *Volatilidad de la información:* Analice el grado de volatilidad de los datos a adquirir. En muchos casos, adquirir los datos volátiles debe ser una prioridad, por encima de aquellos no volátiles. Sin embargo, tenga en cuenta que algunos datos volátiles también son dinámicos por naturaleza (por ejemplo, los archivos de log, que se sobrescriben cuando ocurren nuevos eventos).

- *Esfuerzo requerido:* Considere que la cantidad de esfuerzo requerido para obtener diferentes fuentes de datos puede variar. Esto involucra no solo el tiempo que gasta el analista y las demás personas de la entidad, sino también el costo de los equipos y/o servicios (por ejemplo, adquirir los datos de un router de red requeriría mucho menos esfuerzo que adquirirlos del ISP).

2. **Adquirir los datos:** Si los datos no han sido recopilados por herramientas de seguridad, de análisis o por otros medios, el proceso de recolección involucra el uso de herramientas forenses para adquirir los datos volátiles, y para duplicar y asegurar las fuentes originales de datos no volátiles. La adquisición se puede hacer localmente o a través de la red. Siempre priorice una adquisición local, pero cuando no sea posible (por ejemplo, cuando el sistema se encuentra en una habitación cerrada, o en otra ubicación) la decisión debe tomarse teniendo en cuenta los tres (3) criterios de la planeación.

   Nota: Tenga en cuenta que siempre debe utilizar dispositivos hardware o software bloqueadores de escritura, para proteger y preservar la evidencia original.

3. **Verificación de integridad:** Una vez se adquieren los datos, debe verificarse su integridad. Esto es particularmente importante para que un analista pueda demostrar que los datos no han sido modificados o alterados, lo cual se requiere para darle validez al elemento probatorio y certificar la información como auténtica. Esta verificación de integridad generalmente consiste en el cálculo de funciones hash, tanto en los datos originales como en la copia, los cuales deben ser iguales.

Cadena de custodia y documentación

En el momento de la adquisición de los datos debe iniciarse la cadena de custodia, utilizando los mecanismos apropiados para asegurar la calidad de la evidencia recolectada y evitar futuras acusaciones de malos manejos o manipulación de evidencia. Esto involucra mantener un registro de cada persona que tiene contacto con la evidencia, documentando las acciones que desarrollaron sobre esta y registrando la fecha y hora. Deben utilizarse los formatos vigentes establecidos por la Fiscalía General de la Nación. De igual forma se debe almacenar la evidencia en una ubicación segura cuando no esté en uso; realizar una copia de esta y desarrollar todas las operaciones de análisis y procesamiento en dicha copia, verificando la integridad de los datos originales y de la copia.

Es de aclarar que todo lo anterior debe ser documentado apropiadamente, incluyendo cada herramienta usada en el proceso. La documentación garantiza el principio de repetición. Adicionalmente, debe tomarse un registro fotográfico de la evidencia para proporcionar recordatorios visuales de la configuración del sistema y de los dispositivos periféricos. Además, antes de tocar un sistema y/o dispositivo, el analista debe tomar una nota o

fotografía de cualquier imagen, documento, programa en ejecución y otra información relevante que se muestre en el monitor o se encuentre a su alrededor.

Si es posible, una persona del equipo investigador debe encargarse de custodiar la evidencia, asumiendo la responsabilidad de fotografiar, documentar y etiquetar cada ítem que se recolecta, y registrar cada acción que se ejecuta, quién lo hizo y a qué hora. Ya que la evidencia puede permanecer durante mucho tiempo en el laboratorio sin ser requerida legalmente, la documentación apropiada permite que un analista recuerde exactamente qué se hizo para recolectar los datos, lo cual puede ser útil para refutar acusaciones de malos manejos o manipulación de evidencia.

ETAPA 3: EXAMINACIÓN

Principio: Diferentes tipos de casos y medios pueden requerir diferentes métodos de examinación. Las personas que lleven a cabo la examinación de la evidencia digital deben tener el entrenamiento adecuado.

Procedimiento: Realice la examinación de los datos que se adquirieron usando procedimientos forenses apropiados. Como regla general, la examinación no debe realizarse sobre la evidencia original.

Extracción de los datos

Típicamente la etapa de examinación de los datos involucra la extracción de información relevante de los dispositivos adquiridos. Se describen dos tipos de extracción que se realizan: física y lógica. Durante la extracción física se identifican y se recuperan los datos en todo el disco físico, sin tener en cuenta el sistema de archivos. Durante la extracción lógica se identifican y recuperan archivos y datos en función de los sistemas operativos, sistemas de archivos y/o aplicaciones instaladas.

1. **Extracción física:** Esta ocurre a nivel físico, independientemente del sistema de archivos presente en el dispositivo. Esto puede incluir los siguientes métodos: búsqueda de palabras clave, file carving y extracción de la tabla de particiones y espacio no utilizado de un dispositivo físico.

    - Realizar una búsqueda de palabras clave en todo el dispositivo físico puede ser útil ya que le permite al analista extraer datos que el sistema operativo y el sistema de archivos puede que no tengan en cuenta.

    - Las utilidades de file carving ejecutadas sobre el dispositivo físico pueden ayudar a recuperar y extraer archivos y datos utilizables que el sistema operativo y el sistema de archivos puede que no tengan en cuenta.

    - Examinar la estructura de las particiones puede identificar los sistemas de archivos presentes y determinar si se tiene en cuenta todo el tamaño físico del disco duro.

2. **Extracción lógica:** Durante esta fase, la extracción de los datos está basada en el(los) sistema(s) de archivos presente(s) en el dispositivo y puede incluir datos de áreas

tales como archivos activos, archivos borrados, espacio libre de archivos (file slack) y espacio no asignado. El proceso puede incluir:

- Extracción de la información del sistema de archivos para revelar características tales como la estructura de directorios, atributos de archivos, nombres, estampas de tiempo y fecha, tamaño y ubicación.

- Reducción de datos para identificar y eliminar archivos conocidos, mediante la comparación de valores hash calculados con valores hash autenticados.

- Extracción de archivos pertinentes con la investigación. Para lograr esto es posible realizar búsquedas basadas en nombre y extensión de archivos, encabezados, contenido y ubicación en el dispositivo.

- Recuperación de archivos borrados.

- Extracción de datos protegidos por contraseña, encriptados y comprimidos.

- Extracción del espacio libre de los archivos (file slack).

- Extracción del espacio no asignado del dispositivo.

Cadena de custodia y documentación
En esta etapa el mantenimiento de la cadena de custodia y la documentación detallada sigue siendo la prioridad. Debe dejarse un registro de los procesos llevados a cabo para la extracción, indicando las herramientas utilizadas y la fecha y hora de inicio y finalización de los procesos. Usualmente esta información es generada automáticamente por las herramientas forenses de extracción; sin embargo, en caso de que no se cuente con esta funcionalidad, es preciso que los investigadores se aseguren de realizarlo.

ETAPA 4: ANÁLISIS

Principio: Cuando se trata de evidencia digital también tienen aplicación los principios generales de las ciencias forenses.

Procedimiento: Realice el análisis de la información extraída de los medios adquiridos. Para este proceso debe tener en cuenta las reglas y principios generales de las ciencias forenses, cuyo fundamento se encuentra en usar una aproximación metodológica para llegar a conclusiones basadas en los datos disponibles o determinar que aún no se pueden sacar conclusiones. Asegúrese de realizar un registro apropiado de todas las acciones ejecutadas sobre la evidencia, así como de mantener la cadena de custodia.

Realice un análisis previo de la autoridad legal que tiene para llevar a cabo el análisis. Verifique las conclusiones a las que llegó en la etapa de evaluación, acerca de la necesidad de orden jurisdiccional.

Análisis de tiempo
El análisis de tiempo puede ser útil para determinar cuándo ocurrieron los eventos en un sistema o dispositivo, lo cual puede resultar crucial para vincular un usuario a un evento específico.

- Revise la fecha y hora de los metadatos del sistema de archivos (por ejemplo, última modificación, último acceso, fecha de creación, modificación, etc.) para vincular los archivos de interés con los períodos de tiempo relevantes para la investigación.

- Revise los registros del sistema y de las aplicaciones que se encuentren disponibles. Esto puede incluir logs de errores, de instalación, de conexión, de seguridad, etc. Lo anterior puede ayudar a determinar, por ejemplo, cuándo una combinación de usuario/contraseña se usó para iniciar sesión en un sistema.

Nota: Es importante que tenga en cuenta la configuración horaria del sistema analizado.

Análisis de datos ocultos
Los datos pueden encontrarse escondidos en un sistema o dispositivo. En consecuencia, el análisis de datos ocultos puede ser útil para detectar y recuperar tal información y puede indicar conocimiento, propiedad o intención. Los métodos que se pueden usar incluyen:

- Correlacionar los encabezados de los archivos con las correspondientes extensiones para identificar posibles disparidades.

- Obtener acceso a todos los archivos protegidos por contraseña, encriptados o comprimidos, lo que puede indicar un intento de esconder datos de usuarios no autorizados. Una contraseña por sí misma puede ser tan reveladora como el contenido del archivo.

- Obtener acceso al área protegida del host (HPA – Host Protected Area). La presencia de datos creados por el usuario en la HPA puede indicar un intento por esconder información.

Análisis de aplicaciones y de archivos
Muchos programas y archivos identificados pueden contener información relevante para la investigación y proporcionan una visión sobre la capacidad del sistema y el conocimiento del usuario. Los resultados de este análisis pueden indicar la necesidad de pasos adicionales en los procesos de extracción y procesamiento. Lo anterior puede incluir:

- Revisar los nombres de archivo en búsqueda de patrones de relevancia.

- Examinar el contenido de los archivos sospechosos.

- Identificar el número y tipo de sistema(s) operativo(s).

- Correlacionar los archivos con las aplicaciones instaladas.

- Considerar las relaciones entre los archivos. Por ejemplo, correlacionar el historial de internet con la memoria caché y los archivos de correo electrónico con los adjuntos.

- Identificar los tipos de archivos desconocidos para determinar su valor para la investigación.

- Examinar las ubicaciones de almacenamiento por defecto del usuario para las aplicaciones y la estructura de los archivos del dispositivo, para determinar si los archivos se almacenaron en la ubicación por defecto o en otras ubicaciones.

- Examinar las configuraciones propias del usuario.

- Analizar los metadatos de los archivos, para identificar información adicional sobre el usuario autor de estos, lo cual generalmente está disponible para la aplicación con que se crearon. Por ejemplo, los archivos creados con procesadores de texto pueden incluir autoría, última edición, número de veces editado, dónde se imprimieron o dónde se guardaron.

Propiedad y posesión
En algunas circunstancias puede ser importante identificar todos los elementos posibles que permitan determinar la autoría de un determinado archivo. Aunque esta tarea puede ser particularmente compleja.

El problema es de carácter práctico: en general, el hecho de que se haya utilizado una cuenta o dirección no establece de manera concluyente la identidad o la ubicación de la persona en particular que la utilizó. Como resultado, dicha evidencia basada en gran medida en los registros de cuentas o direcciones IP debe demostrar una conexión suficiente entre los registros y la persona o ubicación.

El autor humano de un registro digital puede identificarse electrónicamente y su valor probatorio dependerá, entre otras características, de la solidez del sistema de autenticación del usuario. En muchos casos, un autor humano también puede identificarse a partir de evidencia circunstancial que demuestra el uso de un sistema informático particular en el momento en que se creó y/o modificó el registro. Dicha evidencia puede compilarse a partir de testigos, video, sistema de acceso al edificio, registros telefónicos o evidencia forense latente (por ejemplo, huella digital). La evidencia circunstancial también puede usarse para refutar que alguien fue el supuesto autor de un registro electrónico.

El proceso puede incluir uno o más de los siguientes factores:
- Ubicar al sujeto en el computador o dispositivo en una fecha y hora particular puede ayudar a determinar la propiedad y posesión (análisis de tiempo).

- Los archivos de interés pueden estar localizados en ubicaciones personalizadas (por ejemplo, un directorio creado por el usuario llamado “pornografía infantil”) (análisis de aplicaciones y de archivos).

- El nombre del archivo en sí mismo puede ser de valor probatorio y también puede indicar los contenidos de este (análisis de aplicaciones y de archivos).

- Los datos ocultos pueden indicar un intento deliberado de evitar la detección (análisis de datos ocultos).

- Si se recuperan las contraseñas necesarias para obtener acceso a los archivos encriptados y protegidos por contraseña, estas, por sí mismas, pueden indicar posesión y propiedad (análisis de datos ocultos).

- Los contenidos de un archivo pueden indicar propiedad o posesión conteniendo información específica de un usuario (análisis de aplicaciones y archivos).

En resumen, siempre que sea posible identifique la mayor cantidad de elementos probatorios (evidencia del tipo *individual*) que le sean de utilidad al operador requirente para determinar la autoría de los hechos que se investigan.

Por otro lado, es importante tener en cuenta que la evidencia obtenida de herramientas de gestión de eventos de seguridad y software de registros centralizados son elementos probatorios muy importantes y estos pueden facilitar el proceso de análisis, ya que la mayoría de estas herramientas reúnen y correlacionan los datos automáticamente.

Generar conclusiones
Por sí solos, los resultados obtenidos de cualquiera de estos análisis puede que no sean suficientes para llegar a una conclusión. Sin embargo, cuando se ve como un todo, las asociaciones entre resultados individuales pueden proporcionar una imagen más completa. Como paso final de esta etapa, asegúrese de considerar los resultados de la extracción y el análisis en su totalidad.

Cadena de custodia y documentación
Es importante 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.

Por último, debe realizarse una verificación final de la integridad de la copia o imagen de los elementos probatorios analizados durante la investigación, con el fin de certificar que estas no han resultado modificadas o alteradas y que sean copias válidas de la información original base.

ETAPA 5: REPORTE

Principio: El investigador es responsable de reportar sus hallazgos y los resultados del análisis de la evidencia digital de manera completa, clara y precisa. La documentación es una etapa paralela que se lleva a cabo durante todo el proceso de análisis forense.

Procedimiento: Toda la documentación debe ser completa, precisa y de fácil comprensión. Esta etapa corresponde al proceso de preparar y presentar la información resultado del análisis. Escriba el informe de los hallazgos teniendo en cuenta la audiencia objetivo.

Las notas del investigador son elementos muy valiosos para la construcción del informe final de resultados. Para el desarrollo del informe final es necesario que tenga en cuenta los siguientes aspectos:

Explicaciones alternativas
Cuando la información relacionada con un evento en particular está incompleta, podría no ser posible llegar a una explicación o conclusión definitiva sobre qué pasó. Cuando un evento tiene dos o más explicaciones posibles, en el proceso de elaboración del informe es necesario darle la debida consideración a cada una de ellas. En este caso, los investigadores deben usar una aproximación metodológica para intentar probar o refutar cada explicación posible que se plantea.

Tenga en cuenta 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; se recomienda generar dos (2) informes: un reporte general dirigido al operador disciplinario o administrativo que solicitó el apoyo técnico, en el cual se detallen los hallazgos y conclusiones utilizando un lenguaje sin tecnicismos, que deje claro qué sucedió, cuándo, cómo y dónde.

El otro informe debe contener todo el detalle técnico de los procedimientos, análisis y herramientas utilizados; en algunos casos, puede ser necesario incluir copia de todos los elementos probatorios obtenidos. Generalmente los informes generados por las herramientas forenses tienen el grado y nivel de detalle requerido para esta clase de reporte.

Información procesable
Esta etapa también incluye identificar cualquier información que conlleve a posibles procesos disciplinarios y/o administrativos, relacionados o no con la actual investigación. Por ejemplo, una lista de contactos pudo ser un resultado del análisis y esta podría conducir a información adicional sobre un delito o falta disciplinaria.

De manera similar, también podría obtenerse información que pudiera prevenir incidentes, eventos o faltas futuras, como un delito que se está planeando, una vulnerabilidad que podría explotarse o un acto de corrupción que se está gestando.

Informe del investigador
Al preparar el informe final de reporte de hallazgos y conclusiones, el investigador debe seguir los lineamientos, políticas, procedimientos y/o formatos establecidos por la entidad. Sin embargo, algunas recomendaciones generales que pueden tenerse en cuenta para la elaboración del informe general o ejecutivo son:

- Identificar la entidad a la que pertenece el investigador que realiza el reporte.
- Identificación del caso, auto de solicitud de apoyo técnico.
- Investigador a cargo.
- Fecha de recepción de la solicitud.
- Fecha de elaboración del informe.

- Lista descriptiva de los elementos sometidos a análisis, incluyendo número de serie, marca y modelo.

- Breve descripción de los pasos llevados a cabo durante el análisis, tales como búsqueda de términos, búsqueda de imágenes y recuperación de archivos borrados.

- Resumen de hallazgos: Puede ser útil ofrecer una sección con un breve resumen de los resultados de los análisis llevados a cabo sobre los elementos adquiridos. De esta forma se ofrece una idea general del contenido del informe. Sin embargo, es importante recordar que todos los hallazgos listados en el resumen deben estar contenidos en la sección de detalles del informe.

- Detalles de los hallazgos: En esta parte del informe se deben describir en mayor detalle los resultados de los análisis y puede incluir:
  - Archivos específicos relacionados con la solicitud o las preguntas realizadas por el operador solicitante.
  - Otros archivos, incluyendo archivos borrados, que soportan o apoyan los hallazgos.
  - Búsqueda de cadenas de texto y búsqueda de palabras clave.
  - Evidencia relacionada con el comportamiento en internet, tales como análisis de tráfico web, registros de chat, archivos de cache, correos electrónicos, historial de navegación, etc.
  - Análisis de imágenes.
  - Indicadores de propiedad, que pueden incluir datos de registro de programas y aplicaciones.
  - Descripción de programas relevantes en los elementos analizados.
  - Técnicas utilizadas para ocultar o enmascarar datos, tales como la encriptación, esteganografía, atributos ocultos, particiones ocultas y anomalías en nombres de archivo.

- Conclusiones: Es importante que los hallazgos permitan responder las preguntas de la solicitud de apoyo; en consecuencia, se debe finalizar el informe con las conclusiones derivadas de la evidencia y los hallazgos de forma que se le dé respuesta a la solicitud que originó la investigación. Es importante que se indique, en caso de que aplique, la necesidad de realizar más estudios o análisis para llegar a conclusiones definitivas. De la misma forma, se debe dejar indicado si solo es posible obtener explicaciones alternativas o hipótesis, con su respectiva justificación.

- Anexos o materiales de soporte: Listado de elementos de soporte que se incluyen en el informe, tales como impresiones de ítems específicos, copias digitales de la evidencia, documentación de cadena de custodia, entre otros. En este apartado se deben incluir todos los informes técnicos detallados generados por las herramientas forenses.

- Glosario: Puede incluirse un glosario de términos para ayudar al lector a comprender cualquier tecnicismo utilizado. Se deben utilizar fuentes aceptadas para las definiciones proporcionadas e incluir las referencias apropiadas.

Cadena de custodia y documentación
Finalmente, en la etapa de reporte la documentación generada durante todo el proceso de la investigación cobra vital importancia y se convierte en los anexos del informe final. El(los) investigador(es) debe(n) revisar las anotaciones realizadas, los listados parciales de resultados y cualquier otra información que le permita elaborar el informe final de la mejor manera, teniendo siempre presente la audiencia a la cual va dirigido.

3.3.3 Lecciones aprendidas

Es importante tener en cuenta que el proceso descrito en esta metodología no es estático ni una camisa de fuerza para la entidad que requiera realizar investigaciones forenses. Este proceso está en constante evolución, a la par de los avances tecnológicos y de la aparición de nuevos dispositivos y nuevas formas de cometer delitos o faltas. 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, con el fin de valorar las experiencias particulares que pudieran haber tenido lugar en el caso específico.

Se deben revisar las actividades de cada etapa para identificar las dificultades que pudieran haberse presentado y en general, identificar los aspectos a mejorar del proceso forense de manera integral. Esta revisión incluye los registros de las herramientas software, el estado de hardware, condiciones de almacenamiento, entre otros. De igual forma se deben considerar posibles mejoramientos a los lineamientos y procedimientos definidos, los cuales deberán ser revisados y aprobados para su implementación formal dentro de la entidad.

Una vez que sean aprobados dichos cambios (en caso de que se realicen), se debe informar a todos los miembros del equipo acerca de estos, utilizando las estrategias de difusión apropiadas para que cada uno de ellos tenga acceso a la documentación relacionada y tenga un recordatorio frecuente de los cambios realizados y de los procedimientos a seguir.

Además de abordar los problemas identificados y los aspectos a mejorar, los analistas siempre deben tener presente el mantenimiento y desarrollo de sus habilidades. Con este fin, las actualizaciones rutinarias con las últimas herramientas y técnicas que aborden las últimas tecnologías relacionadas con medios de almacenamiento, tipos y formatos de datos, y otros temas relevantes. Ya sea necesario o no, la actualización periódica de habilidades a través de cursos, experiencia en el trabajo y fuentes académicas ayuda a garantizar que las personas que realizan acciones forenses se mantengan al día con las tecnologías y las responsabilidades laborales que cambian rápidamente.

3.4 Caso de estudio: Institución universitaria de carácter público de Colombia

3.4.1 Descripción del caso de estudio

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.

3.4.2 Desarrollo

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. Se tiene competencia por tratarse de un funcionario público de una entidad nacional bajo la vigilancia de la Procuraduría General de la Nación.

Evaluación del caso
El auto de asignación recibido, proferido por el Director Nacional de Investigaciones Especiales, faculta a los funcionarios de la DNIE con funciones de policía judicial para el aseguramiento de la evidencia, inicio de la cadena de custodia y levantar el acta correspondiente.

Se requiere hacer visita especial a la institución universitaria, con el fin de asegurar y extraer el disco duro del equipo de cómputo asignado al investigado, para lo cual se tienen las facultades requeridas. Sin embargo, para el procesamiento y análisis de la imagen forense se necesita orden jurisdiccional del Procurador General de la Nación, toda vez que el disco duro puede contener información personal y privada del implicado. En consecuencia, el procesamiento y análisis se realizará una vez se expida la orden jurisdiccional de rigor.

Evaluación de la evidencia digital potencial
El caso en cuestión se trata de presuntos usos no autorizados de la tarjeta de crédito y la cuenta corriente institucionales a cargo del investigado para sufragar gastos de índole privada y personal. En consecuencia, se indagarán archivos que puedan contener registros financieros de los gastos realizados, como hojas de cálculo, archivos de texto, pdf, correos

electrónicos, archivos de imagen, utilizando criterios de búsqueda relacionados con la investigación.

Se solicitará al operador disciplinario un listado de palabras clave específicamente vinculadas a la investigación con el fin de identificar los archivos relacionados.

Evaluación del sitio de procesamiento
El procesamiento del dispositivo adquirido se realizará en el Laboratorio de Informática Forense 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. En consecuencia, en la diligencia de visita especial se realizará solo el aseguramiento de la evidencia y el inicio de la cadena de custodia del elemento. Por lo cual se realiza la preparación de los formatos vigentes de cadena de custodia de la Fiscalía General de la Nación y los elementos necesarios para el embalaje del disco duro a adquirir: bolsas antiestáticas, cinta de evidencia, sobres de manila, entre otros.

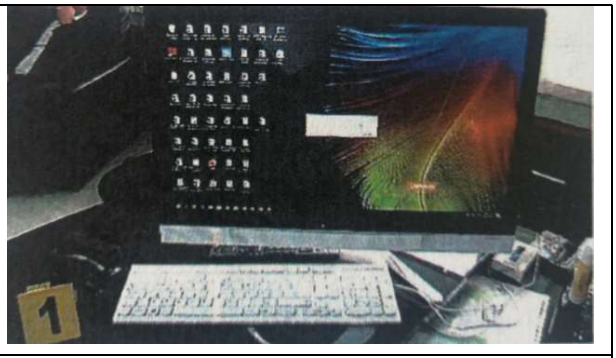
ETAPA 2: ADQUISICIÓN
En esta etapa se realiza la planeación y desarrollo de la visita especial requerida en el auto de solicitud de apoyo técnico, para el aseguramiento del disco duro.

Planear la adquisición
La visita especial tiene como fin dos objetivos: (1) el aseguramiento de los discos duros del equipo de cómputo del servidor público investigado, a cargo de funcionarios adscritos al Laboratorio de Informática Forense de la DNIE y (2) asegurar documentación relevante al caso, como material probatorio, a cargo de técnicos investigadores adscritos al Grupo Financiero de la DNIE.

Se ofició a la entidad y al implicado y su apoderado con el fin de notificar la visita especial de actividad probatoria, en donde se requirió la presencia de la Oficina de Sistemas, el área de Archivo y el área de Tesorería de la institución universitaria.

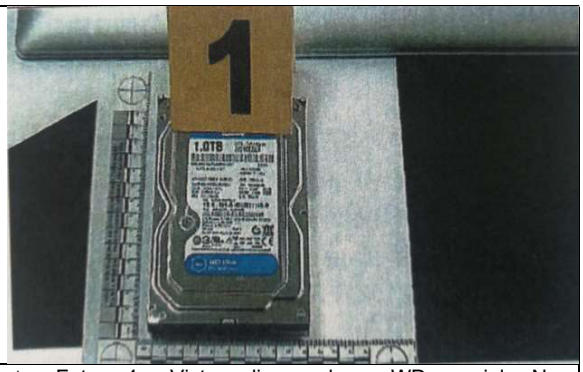
Adquirir los datos
En desarrollo de la visita especial practicada a la entidad, se identificó el computador marca LENOVO, color gris, referencia 210, serial No. PGO1MU0G, el cual se encontraba asignado al investigado; se procedió a extraer el disco duro de marca WESTERN DIGITAL, capacidad de 1 TB, interfaz Sata, serial No. WMCGYOK83WEF. Se efectuó la fijación fotográfica, embalaje, rotulado y registro del formato de cadena de custodia.

▲ Foto 1. Vista puesto de trabajo del investigado.

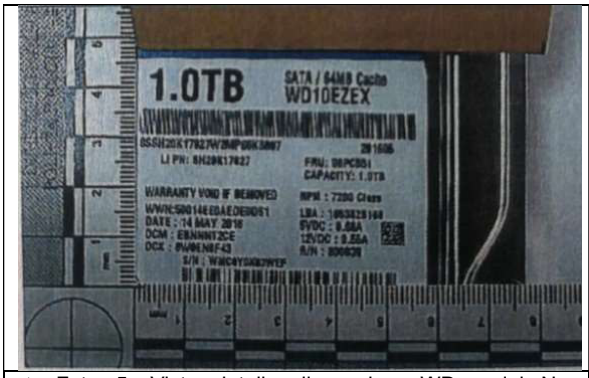


▲ Foto 2. Vista frontal computador Lenovo asignado al investigado.

▲ Foto 3. Vista posterior computador Lenovo asignado al investigado.



▲ Foto 4. Vista disco duro WD serial No. WMCGYOK83WEF.



▲ Foto 5. Vista detalle disco duro WD serial No. WMCGYOK83WEF.

▲ Foto 6. Vista rótulo del disco duro WD serial No. WMCGYOK83WEF

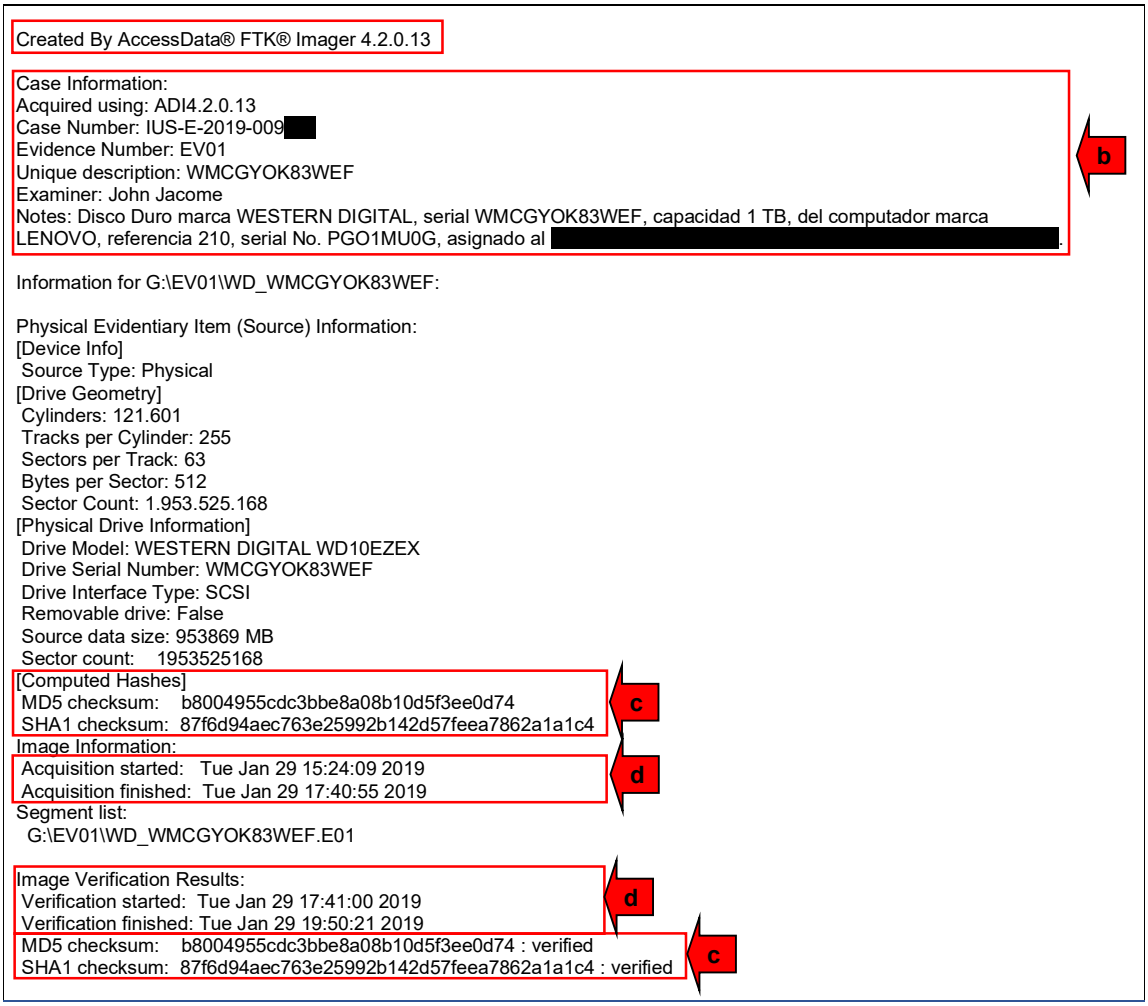
El disco duro fue llevado a las instalaciones del Laboratorio de Informática Forense de la DNIE en donde se procedió a efectuar la apertura del contenedor, previa verificación del estado e información del rótulo, con el fin de realizar la adquisición de la imagen forense del elemento recaudado. De igual forma se realizó el respectivo registro de continuidad de esta actividad en la cadena de custodia.

Como resultado de la adquisición, se obtuvo una (1) imagen forense de la información contenida en el elemento en mención, mediante la utilización de la herramienta de informática forense software AccessData FTK Imager versión 4.2.0.13, debidamente licenciada para la Procuraduría General de la Nación, surtiendo las siguientes actividades:

a. Preparar las herramientas de hardware y software forense a ser usadas.
b. Realizar la creación del caso en la herramienta forense, con los datos requeridos por esta para la correcta identificación de la evidencia.
c. Confirmar la integridad de la imagen forense, comparando los valores de los hash (MD5 y SHA1), reflejados en el reporte generado por la herramienta forense FTK.
d. Verificar la línea de tiempo de la adquisición.

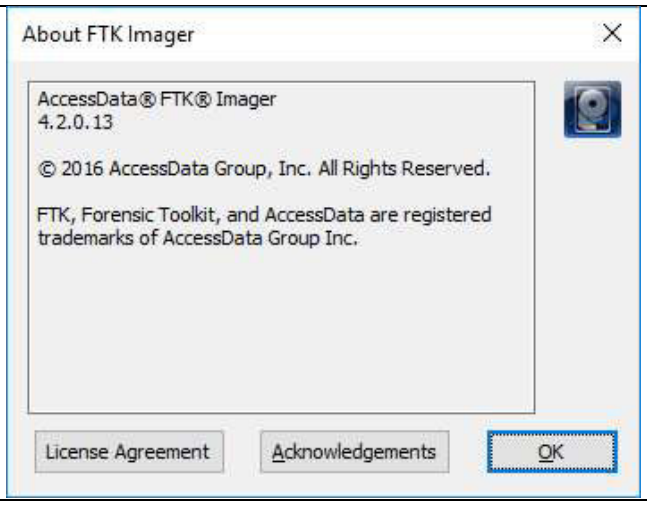
Una vez realizado el proceso de adquisición de la imagen forense del disco duro marca WESTERN DIGITAL, serial No. WMCGYOK83WEF, se hizo entrega de este, debidamente embalado y rotulado, a un contratista autorizado de la universidad pública.

Verificación de integridad
A continuación, se listan las características de la imagen obtenida:



Cadena de custodia y documentación
Las herramientas utilizadas para la extracción fueron:

- Software AccessData FTK Imager versión 4.2.0.13: Con este software es posible crear imágenes forenses de datos de computadores y otros dispositivos de almacenamiento sin realizar cambios en la evidencia original. Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realiza una imagen duplicado bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense.



▲ Foto 7. Ficha Técnica del Software AccessData FTK Imager versión 4.2.0.13

Una vez realizada la extracción de la imagen forense, se procedió a embalar nuevamente el disco duro marca WESTERN DIGITAL, serial No. WMCGYOK83WEF, para realizar la entrega al funcionario autorizado de la universidad pública.

ETAPA 3: EXAMINACIÓN
En esta etapa se realiza la extracción de los datos de la imagen forense adquirida.

Es de anotar, que dentro de la información extraída como resultado del procesamiento, era posible encontrar información de carácter institucional reservado, secreto y/o privado de interés personal, que pudiera hacer parte de la intimidad y del buen nombre del investigado, por tanto se atendió lo dispuesto en la "Orden Jurisdiccional para Práctica de Pruebas" proferida por el despacho del señor Procurador General de la Nación, para que se permitiera, de ser inevitable, afectar sus derechos bajo las restricciones legales y en uso exclusivo sobre la acción que se adelantaba con el fin de que, en el ejercicio de funciones de policía judicial, se realizaran las actividades de análisis de la información contenida en el disco duro adquirido, en atención a lo solicitado por la Procuraduría Delegada para la Función Pública.

Extracción de los datos
Se realizaron las siguientes actividades para la extracción y procesamiento de la información:

e. Se configuró la herramienta forense para obtener la información solicitada.
f. Se configuraron los criterios de búsqueda, mediante la parametrización de las palabras clave, de acuerdo con lo solicitado por el operador disciplinario y efectuar las búsquedas respectivas en la herramienta forense.

Es así como, en el desarrollo de las actividades mencionadas, se recibió un listado de palabras clave obtenido de la lectura de los diferentes documentos que hacen parte del proceso disciplinario, con los cuales se parametrizaron los criterios de búsqueda en la herramienta forense, para obtener los resultados requeridos por la autoridad disciplinaria.

El listado de palabras remitido fue:

Listado de palabras clave			
491330	ikea sunrise	Convenio	Satena
6774454	instituto	Cuenta corriente	tarjeta crédito
230082711	Ishop	Despegar	tiquetes baratos
230-08271-1	Itunes	Despegar Colombia	Tornamesa
491330-2-254819-160	Lacoste	Dick	Tullanta
491330-7-145280-975	Latam	Expedia local	Visa
Avianca	Massimo Dutti	hotel las colinas	i shop
Banco Occidente	Mcafee	hotel obelisco	Cheapair
Biferia	Orlando	Pago	

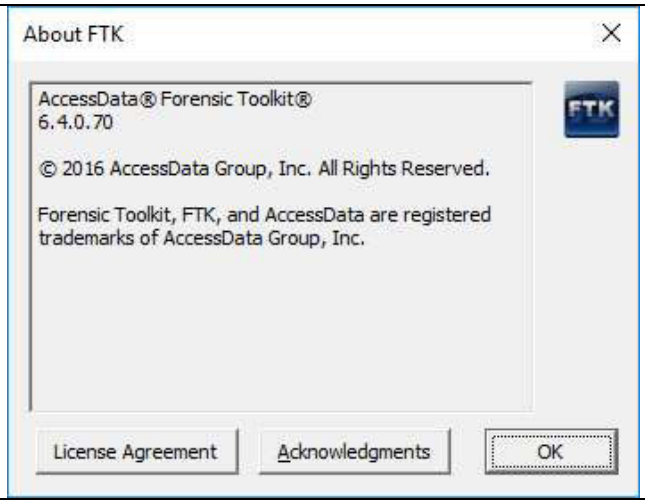
Como complemento al listado anterior, se realizaron búsquedas por tipos de archivos de manera específica así:

- Archivos de Imágenes: jpeg, tiff, raw, bmp, gif, png, psd, jpg, btw.
- Archivos de Correo: pst y msg.
- Archivos de Office: doc, docx, xls, xlsx, ppt, pptx.
- Archivos de Formato de documento portátil: pdf.

Cadena de custodia y documentación

La extracción, procesamiento y análisis de la imagen forense se realizó utilizando las siguientes herramientas forenses:

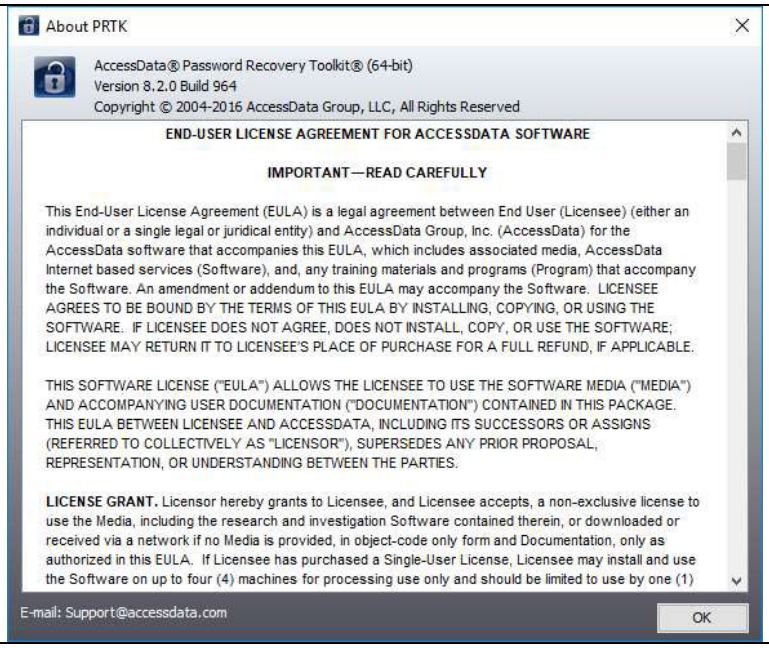
- AccessData Forensic Toolkit versión 6.4.0.70: Es una solución de investigación digital que recopila datos de cualquier dispositivo o sistema digital que produzca, transmita o almacene datos; y realiza el análisis forense de los mismos.



▲ Foto 8. Ficha Técnica del Software AccessData Forensic Toolkit versión 6.4.0.70

- AccessData PRTK (Password Recovery Toolkit) versión 8.2.0: Es un software que se utiliza para la recuperación de contraseñas en archivos cifrados o protegidos con clave de acceso, por medio de la cual se pueden:

- Crear posibles listas de contraseñas de muchas fuentes.
- Crear diccionarios personalizados basados en hechos del caso.
- Crear un perfil sospechoso usando la información biográfica del mismo caso, para generar contraseñas probables.



▲ Foto 9. Ficha Técnica del Software AccessData Password Recovery Toolkit versión 8.2.0

ETAPA 4: ANÁLISIS

En esta etapa se realiza el análisis y compilación de resultados del procesamiento de la imagen forense realizado en la etapa anterior.

Resultados obtenidos y análisis de la imagen forense

Para la obtención de resultados y posterior análisis de la información se llevaron a cabo las siguientes actividades:

g. Generar reporte con la información correspondiente a los metadatos, propiedades y listados de los archivos.

h. Crear reporte de hallazgos con la información detallada de los archivos seleccionados como resultado de la búsqueda de parámetros por palabras clave.

Así mismo, y una vez aplicados los criterios de búsqueda en el software AccessData Forensic Toolkit sobre la imagen forense, y efectuado el análisis sobre los mismos, fue encontrada la información de interés para la autoridad disciplinaria; se encontraron trescientos cuarenta y un (341) archivos de diferentes tipos, los cuales se describen a continuación:

Archivos Gráficos (jpg): Corresponde a archivos de fotos, que pudieron ser imágenes almacenadas en un espacio físico del disco duro o imágenes recuperadas en los procesos

de adquisición y extracción, que en algún momento fueron eliminadas del disco duro. Se encontraron dieciséis (16) archivos en formato jpg.

Archivos tipo Texto (doc, docx, txt): Corresponden a los documentos generados a través del software Microsoft Office – Word (en sus diferentes versiones). Se encontraron veinte (20) archivos en forma doc y docx.

Archivos de Hoja de Cálculo (xls, xlsx): Corresponden a los documentos generados a través del software Microsoft Office – Excel (en sus diferentes versiones). Se encontraron dos (2) archivos en formato xlsx.

Archivos de Presentación (ppt, pptx): Corresponden a los documentos generados a través del software Microsoft Office – Power point (en sus diferentes versiones). Se encontraron seis (6) archivos en formato pptx.

Archivos de formato de documento portátil (pdf): Una de las características principales de este tipo de archivos es que no pueden ser editables por un usuario común, de tal forma que los metadatos se encuentran inmersos en cada uno de los archivos seleccionados.

Se encontraron treinta y un (31) archivos "pdf", de los cuales catorce (14) de ellos estaban protegidos con clave de apertura, razón por la cual se utilizó el software AccessData PRTK, con el fin de obtener las claves y desbloquear los archivos para acceder a ellos. Se logró obtener la contraseña de trece (13) de los archivos pdf protegidos. Para un (1) archivo **NO** fue posible recuperar la clave por los medios forenses del laboratorio. Esta actividad se relaciona a continuación:

▲ Foto 10. Vista archivo "Reportepdfconclave.pdf", donde se identifica el rompimiento de la clave del archivo "20990125136[912597].pdf"

Archivos de Correo Electrónico (ost). El software AccessData Forensic Toolkit, ubicó y desempaquetó el archivo "ost" que contenía el correo electrónico del investigado**.** Se encontraron 262 archivos relacionados con correos electrónicos enviados desde la cuenta institucional del investigado con contenido relacionado con los términos de búsqueda relevantes para la investigación.

Archivos de diversas extensiones: Se encontraron (4) cuatro archivos relacionados con cookies, history file y text internet email:

No	Nombre del archivo	Extensión	Categoría
1	Cookies	<missing?>	Cookies File
2	History	<missing?>	History File
3	History	<missing?>	History File
4	Link de pago.eml.eml	eml	Text Internet Email

Generación de conclusiones

- Mediante el uso de diferentes herramientas de la suite forense AccessData FTK de la entidad, se obtuvo información a nivel de documentos, hojas de cálculo, presentaciones, documentos pdf, imágenes, entre otros, relacionados con los términos de búsqueda relevantes para el caso.

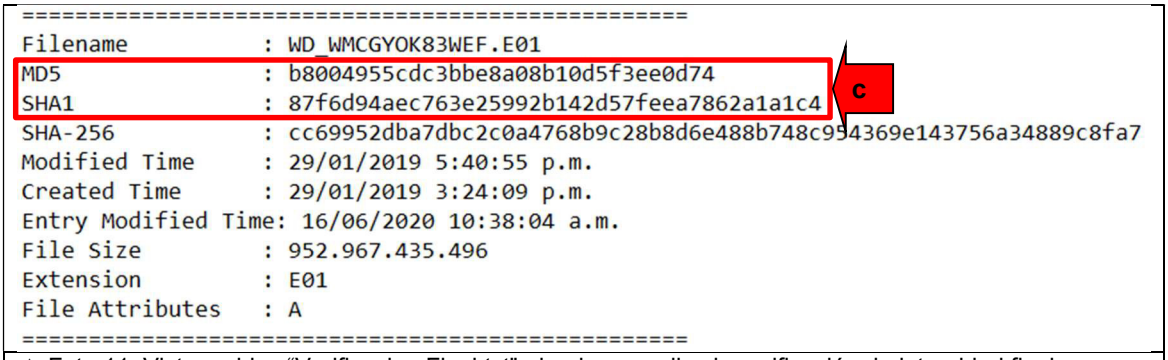
- El análisis de los archivos pdf protegidos indicó que, en su mayoría se trata de extractos bancarios correspondientes a la tarjeta de crédito institucional de la institución universitaria, a cargo del investigado.

- El análisis del correo electrónico indicó el intercambio de mensajes entre la cuenta correspondiente al investigado y comercios de artículos de lujo, concesionarios de alta gama, prestadores de servicios de comunicaciones, agencias de viajes, entre otros.

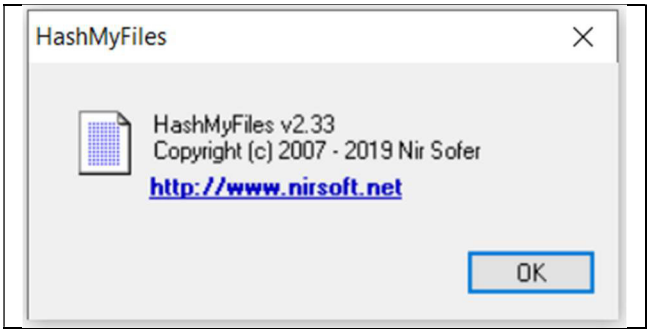
- El análisis de tiempo de archivos y mensajes de correo electrónico evidenció archivos de texto, hojas de cálculo, documentos pdf y mensajes correspondientes con los criterios de búsqueda definidos por la autoridad disciplinaria entre el 2017 y 2019.

Cadena de custodia y documentación

Al finalizar el análisis se realizó una nueva verificación de integridad de la imagen forense procesada, utilizando la herramienta HashMyFiles versión 2.33. con lo cual se comprobó que la imagen no fue alterada durante los procedimientos realizados.



▲ Foto 11. Vista archivo “Verificacion Final.txt”, donde se realiza la verificación de integridad final.



▲ Foto 12. Ficha software HashMyFiles versión 2.33.

ETAPA 5: REPORTE

La etapa final de la metodología consiste en el reporte de resultados y hallazgos en el informe final.

Informe del investigador

Para la presentación de los resultados del análisis al operador disciplinario se utilizó el formato de informe técnico – científico establecido por la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación, en el cual se incluyen todos los procedimientos realizados, la herramientas utilizadas y los hallazgos obtenidos.

El informe técnico final ajustado al formato mencionado tiene la siguiente estructura:

Información del documento: En esta sección se detallan los elementos identificatorios del caso, como número del expediente, investigado(s), cargo(s), entidad(es), autor(es) del informe (profesionales adscritos a la DNIE).

1. ***Objeto del informe:*** Detalles de la solicitud recibida y los actos administrativos que facultan a los funcionarios para el desarrollo de las actividades.

2. ***Alcance:*** Descripción detallada de los alcances del informe técnico.

3. ***Metodología:*** En esta sección se citan las actividades técnicas desarrolladas para obtener el resultado del apoyo técnico científico y/o asesoría especializada, de conformidad con los protocolos establecidos.

4. ***Documentos técnicos soporte del informe y gestiones realizadas:*** En esta sección se declara, si aplica, el estado en el que se reciben los elementos (embalados, rotulados y en cadena de custodia), realizando una descripción detallada de todos aquellos elementos y/o documentos que sean allegados para estudio.

5. ***Análisis y concepto técnico (desarrollo de la investigación):*** En esta sección se registran todas las actividades realizadas, en concordancia con el método descrito, el cual deberá ser consecuente en dar respuesta concreta a lo solicitado por el operador disciplinario. Para el caso específico en estudio, se incluyeron las siguientes subsecciones:
   - ***5.1.*** Recolección del disco duro
   - ***5.2.*** Apertura del contenedor
   - ***5.3.*** Adquisición de la imagen forense

5.4. Extracción y procesamiento de la imagen forense
5.5. Resultados obtenidos y análisis de la imagen forense

6. Conclusiones: En esta sección se describen los hallazgos que se consideren relevantes y aporten a la investigación realizada. Para el caso de estudio específico se concluyó:

- Mediante el uso de diferentes herramientas de la suite forense AccessData FTK de la entidad, se obtuvo información a nivel de documentos, hojas de cálculo, presentaciones, documentos pdf, imágenes, entre otros, relacionados con los términos de búsqueda relevantes para el caso.

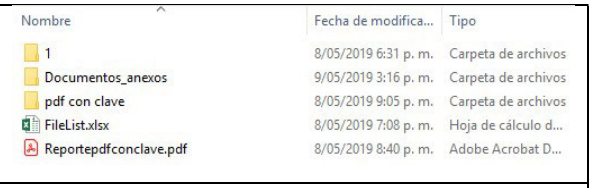
- El análisis de los archivos pdf protegidos indicó que, en su mayoría se trata de extractos bancarios correspondientes a la tarjeta de crédito institucional de la institución universitaria, a cargo del investigado.

- El análisis del correo electrónico indicó el intercambio de mensajes entre la cuenta correspondiente al investigado y comercios de artículos de lujo, concesionarios de alta gama, prestadores de servicios de comunicaciones, agencias de viajes, entre otros.

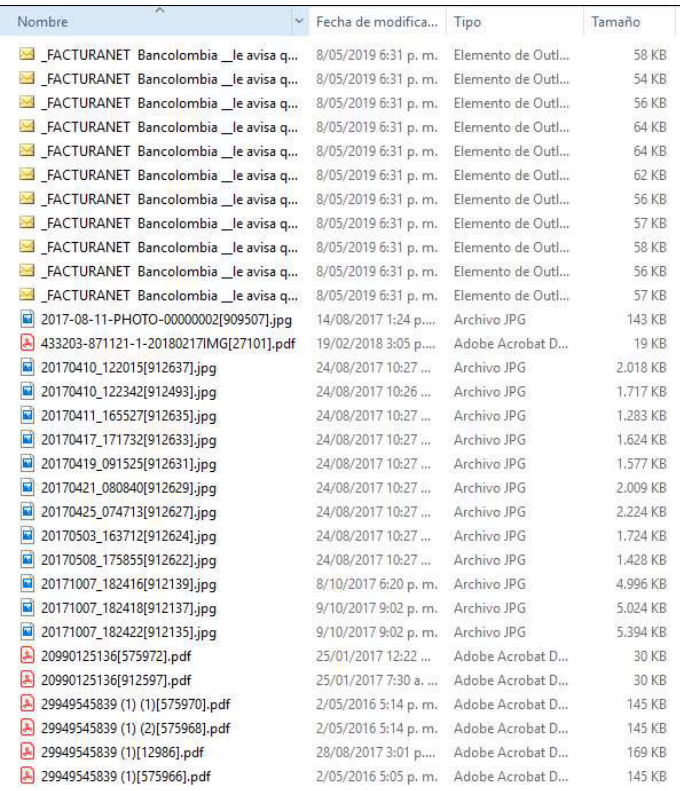
- El análisis de tiempo de archivos y mensajes de correo electrónico evidenció archivos de texto, hojas de cálculo, documentos pdf y mensajes correspondientes con los criterios de búsqueda definidos por la autoridad disciplinaria entre el 2017 y 2019.

7. Anexos: Relación de archivos recuperados y considerados relevantes, informes generados por las herramientas forenses utilizadas.

▲ Foto 13. Vista archivo comprimido denominado “Soporte_Informe_IUS_2019_009XXX.rar”.

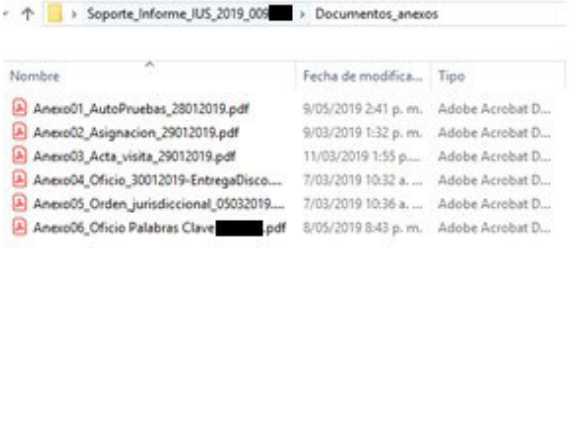


▲ Foto 14. Vista contenido de la carpeta denominada “Soporte_Informe_IUS_2019_009XXX”.



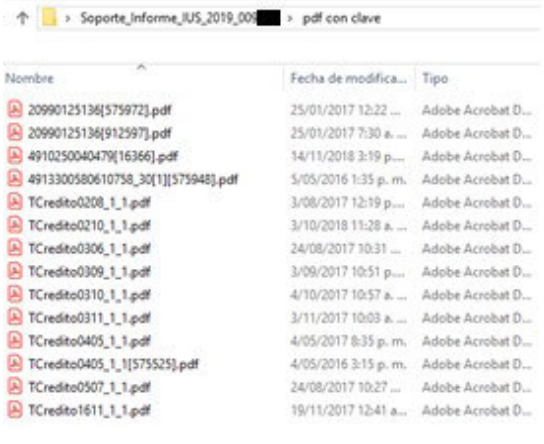
Nombre	Fecha de modifica...	Tipo	Tamaño
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	58 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	54 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	56 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	64 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	64 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	62 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	56 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	57 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	58 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	56 KB
_FACTURANET Bancolombia __le avisa q...	8/05/2019 6:31 p. m.	Elemento de Outl...	57 KB
2017-08-11-PHOTO-00000002[909507].jpg	14/08/2017 1:24 p....	Archivo JPG	143 KB
433203-871121-1-20180217IMG[27101].pdf	19/02/2018 3:05 p....	Adobe Acrobat D...	19 KB
20170410_122015[912637].jpg	24/08/2017 10:27 ...	Archivo JPG	2.018 KB
20170410_122342[912493].jpg	24/08/2017 10:26 ...	Archivo JPG	1.717 KB
20170411_165527[912635].jpg	24/08/2017 10:27 ...	Archivo JPG	1.283 KB
20170417_171732[912633].jpg	24/08/2017 10:27 ...	Archivo JPG	1.624 KB
20170419_091525[912631].jpg	24/08/2017 10:27 ...	Archivo JPG	1.577 KB
20170421_080840[912629].jpg	24/08/2017 10:27 ...	Archivo JPG	2.009 KB
20170425_074713[912627].jpg	24/08/2017 10:27 ...	Archivo JPG	2.224 KB
20170503_163712[912624].jpg	24/08/2017 10:27 ...	Archivo JPG	1.724 KB
20170508_175855[912622].jpg	24/08/2017 10:27 ...	Archivo JPG	1.428 KB
20171007_182416[912139].jpg	8/10/2017 6:20 p. m.	Archivo JPG	4.996 KB
20171007_182418[912137].jpg	9/10/2017 9:02 p. m.	Archivo JPG	5.024 KB
20171007_182422[912135].jpg	9/10/2017 9:02 p. m.	Archivo JPG	5.394 KB
20990125136[575972].pdf	25/01/2017 12:22 ...	Adobe Acrobat D...	30 KB
20990125136[912597].pdf	25/01/2017 7:30 a. ...	Adobe Acrobat D...	30 KB
29949545839 (1) (1)[575970].pdf	2/05/2016 5:14 p. m.	Adobe Acrobat D...	145 KB
29949545839 (1) (2)[575968].pdf	2/05/2016 5:14 p. m.	Adobe Acrobat D...	145 KB
29949545839 (1)[12986].pdf	28/08/2017 3:01 p....	Adobe Acrobat D...	169 KB
29949545839 (1)[575966].pdf	2/05/2016 5:05 p. m.	Adobe Acrobat D...	145 KB

▲ Foto 15. Vista contenido de la carpeta denominada “1”.



Nombre	Fecha de modifica...	Tipo
Anexo01_AutoPruebas_28012019.pdf	9/05/2019 2:41 p. m.	Adobe Acrobat D...
Anexo02_Asignacion_29012019.pdf	9/03/2019 1:32 p. m.	Adobe Acrobat D...
Anexo03_Acta_visita_29012019.pdf	11/03/2019 1:55 p....	Adobe Acrobat D...
Anexo04_Oficio_30012019-EntregaDisco....	7/03/2019 10:32 a. ...	Adobe Acrobat D...
Anexo05_Orden_jurisdiccional_05032019....	7/03/2019 10:36 a. ...	Adobe Acrobat D...
Anexo06_Oficio Palabras Clave[redacted].pdf	8/05/2019 8:43 p. m.	Adobe Acrobat D...

▲ Foto 16. Vista contenido de la carpeta denominada “Documentos Anexos”.



Nombre	Fecha de modifica...	Tipo
20990125136[575972].pdf	25/01/2017 12:22 ...	Adobe Acrobat D...
20990125136[912597].pdf	25/01/2017 7:30 a. ...	Adobe Acrobat D...
4910250040479[16366].pdf	14/11/2018 3:19 p....	Adobe Acrobat D...
49133005806107 58_30[1][575948].pdf	5/05/2016 1:35 p. m.	Adobe Acrobat D...
TCredito0208_1_1.pdf	3/08/2017 12:19 p....	Adobe Acrobat D...
TCredito0210_1_1.pdf	3/10/2018 11:28 a. ...	Adobe Acrobat D...
TCredito0306_1_1.pdf	24/08/2017 10:31 ...	Adobe Acrobat D...
TCredito0309_1_1.pdf	3/09/2017 10:51 p....	Adobe Acrobat D...
TCredito0310_1_1.pdf	4/10/2017 10:57 a. ...	Adobe Acrobat D...
TCredito0311_1_1.pdf	3/11/2017 10:03 a. ...	Adobe Acrobat D...
TCredito0405_1_1.pdf	4/05/2017 8:35 p. m.	Adobe Acrobat D...
TCredito0405_1_1[575525].pdf	4/05/2016 3:15 p. m.	Adobe Acrobat D...
TCredito0507_1_1.pdf	24/08/2017 10:27 ...	Adobe Acrobat D...
TCredito1611_1_1.pdf	19/11/2017 12:41 a...	Adobe Acrobat D...

▲ Foto 17. Vista contenido de la carpeta denominada “pdf con clave”.

3.4.3 Evaluación del caso de estudio

Utilizando el formato de registro de observaciones diseñado se realizó la evaluación de lo evidenciado durante el desarrollo del caso de estudio, obteniendo los siguientes resultados:

ETAPA 1: EVALUACIÓN
En general se observó esta etapa como de fácil implementación. Algunas dificultades que pueden presentarse en su ejecución se relacionan con el grado de completitud de la documentación que acompañe la solicitud de apoyo, o el grado de claridad del requerimiento.

Evaluación del caso
Siempre que la solicitud de apoyo sea clara, precisa, completa y venga acompañada del cuestionario de rigor que debe resolver el perito forense, la evaluación del caso se llevará a cabo de manera fluida y sin inconvenientes.

Una buena comunicación entre el operador disciplinario y/o administrativo solicitante del apoyo técnico científico es un aspecto que puede influir positivamente en el desarrollo de esta fase.

Evaluación de la evidencia digital potencial
La identificación de las fuentes de evidencia digital potencial es un proceso de fácil implementación en la medida en que el analista tenga mayor experiencia en el área de análisis forense.

Se debe asegurar que el equipo humano del laboratorio tenga entrenamientos y capacitaciones periódicas con el fin de que sus habilidades se mantengan vigentes y actualizadas con los avances tecnológicos.

Evaluación del sitio de procesamiento
El equipo analista da prioridad al procesamiento en el laboratorio.

ETAPA 2: ADQUISICIÓN
En esta etapa se llevaron a cabo los procesos de planeación y adquisición de forma adecuada; sin embargo, se evidenciaron algunas dificultades relacionadas con el manejo de la cadena de custodia y la documentación.

Planear la adquisición
Se observó un buen desarrollo de esta fase, mediante una adecuada planeación de la visita especial para el aseguramiento del elemento probatorio. Se surtieron las notificaciones de rigor para garantizar el debido proceso del investigado y el desarrollo de la visita se llevó a cabo sin dificultades. Se utilizó el formato de acta de visita especial vigente de la DNIE para el registro de la actividad.

Adquirir los datos
El proceso de adquisición de la imagen forense del elemento probatorio incautado se desarrolló de forma apropiada, utilizando las herramientas técnicas idóneas con las que cuenta el laboratorio (AccessData FTK Imager versión 4.2.0.13, con licencia para la Procuraduría General de la Nación).

En este proceso influye también el grado de entrenamiento del personal que realiza la adquisición; se observó el correcto uso de elementos de protección antiestática y

mecanismos bloqueadores de escritura durante la extracción del disco y posterior creación de la imagen forense.

Verificación de integridad
La verificación de integridad fue realizada automáticamente por la herramienta forense de adquisición.

Cadena de custodia y documentación
Es importante fortalecer el conocimiento sobre la cadena de custodia de todo el equipo de trabajo del laboratorio, con el fin de que se les dé un correcto uso a los formatos vigentes de la Fiscalía General de la Nación y haya un adecuado manejo del vocabulario relacionado, ya que se identificaron algunas falencias en el diligenciamiento del rótulo y registro de cadena de custodia.

Con relación a la documentación, se deben fortalecer los registros fotográficos realizados durante el aseguramiento del elemento y posterior adquisición de la imagen forense.

ETAPA 3: EXAMINACIÓN
El proceso de examinación se realizó adecuadamente, mediante la extracción física y lógica de los datos para su posterior análisis.

Extracción de los datos
De manera similar que, en la etapa de adquisición, el proceso de extracción de los datos se realiza de una mejor manera entre mayor sea la experticia y conocimiento del analista, toda vez que esto garantiza una buena configuración y un mejor aprovechamiento de las herramientas forenses con que cuenta el laboratorio.

1. Extracción física
Se configuró la herramienta forense AccessData Forensic Toolkit (FTK) con el listado de palabras clave remitido por el operador disciplinario para realizar las búsquedas de contenido.

Como dificultad se identificó que el conocimiento del caso por parte de los analistas debe ser amplio para poder recopilar un listado de palabras que sean de utilidad para la investigación. En consecuencia, se necesita que exista un buen canal de comunicación entre los operadores disciplinarios y los analistas para contar con los fundamentos fácticos del caso que permitan construir un listado de términos útiles y relevantes para cada caso específico.

Los resultados de la etapa de evaluación también son un fundamento para esta fase.

2. Extracción lógica
La herramienta forense se configuró de manera apropiada para la búsqueda de archivos recientes, ocultos, borrados y protegidos, por lo cual esta actividad se desarrolló sin dificultades.

Se detectaron archivos protegidos con contraseña para los cuales se utilizó la herramienta forense AccessData Password Recovery Toolkit (PRTK) de forma adecuada, logrando recuperar la contraseña de la mayoría de los archivos protegidos detectados.

Cadena de custodia y documentación
Se documentaron apropiadamente las herramientas forenses utilizadas, así como los procedimientos realizados.

ETAPA 4: ANÁLISIS
En esta etapa, en general, no se presentaron dificultades que impidieran su desarrollo. Se observaron algunas deficiencias en el análisis de tiempo y el análisis de propiedad y posesión.

Análisis de tiempo
El análisis de tiempo de la información recuperada permitió establecer un marco de ocurrencia de los presuntos hechos en investigación entre los años 2017 y 2019, sin embargo, se identificaron algunas dificultades para acotar este lapso a fechas más específicas; básicamente se evidenció desconocimiento de la herramienta forense para realizar este tipo de análisis.

En consecuencia, para esta etapa también resulta importante el entrenamiento y capacitación del equipo analista en el manejo de las herramientas forenses con que cuenta el laboratorio.

Análisis de datos ocultos
Para el caso de estudio en específico no se identificaron datos ocultos. Sin embargo, la herramienta fue correctamente configurada para realizar este análisis.

Análisis de aplicaciones y de archivos
Este análisis permitió identificar los diferentes tipos de archivos relacionados con los términos de búsqueda relevantes para la investigación. El proceso se desarrolló sin dificultades.

Propiedad y posesión
Para el caso de estudio específico el disco duro analizado pertenecía al equipo de cómputo asignado al investigado, en consecuencia, se identificó que los archivos recuperados pertenecían a la cuenta de usuario principal del equipo, correspondiente al investigado.

Se observaron algunas dificultades para la identificación de evidencia de tipo individual que permitiera una correlación más directa entre el usuario (tanto del equipo como de la cuenta de correo electrónico) y el investigado.

Generar conclusiones
Luego de los procesos de análisis se llegó a conclusiones generales sobre los archivos recuperados de forma que se dio respuesta a lo requerido por el operador disciplinario solicitante.

Se observó que este proceso final del análisis depende en gran medida del grado de completitud de la solicitud, específicamente del hecho de si se cuenta o no con un cuestionario para el perito.

El valor probatorio de la evidencia recuperada es valorado jurídicamente por el operador disciplinario y este determina su inclusión como prueba dentro del proceso.

Cadena de custodia y documentación
Durante esta etapa se realizó la verificación de integridad final de la imagen forense analizada, proceso que se llevó a cabo sin dificultades.

Esta verificación de integridad final, a juicio del operador disciplinario les otorga mayor valor probatorio a los resultados del análisis.

ETAPA 5: REPORTE
Esta etapa se desarrolló sin dificultades, utilizando el formato de informe técnico científico vigente y anexando a este los soportes documentales y probatorios resultado del análisis.

Explicaciones alternativas
Para el caso de estudio observado no se realizaron explicaciones alternativas, toda vez que la solicitud de análisis solo involucraba la recuperación de evidencia relacionada con términos de búsqueda específicos.

Tenga en cuenta 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).

Información procesable
No se identificó información procesable.

Informe del investigador
Se utilizó el formato de informe técnico científico vigente para la DNIE como informe general de resultados. De igual forma se anexaron los reportes generados por las herramientas forenses utilizadas en el análisis.

Cadena de custodia y documentación
Se incluyeron como anexos del informe la evidencia recuperada en el análisis y todos los documentos que complementan el expediente.

4. Conclusiones y recomendaciones

4.1 Conclusiones

A lo largo de este documento se ha presentado 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 734 de 2002.

Como primer objetivo de este proyecto se buscaba identificar las metodologías o modelos existentes en el ámbito nacional y/o internacional para el desarrollo de investigaciones forenses, lo cual fue alcanzado exitosamente, como se observa en la sección “3.1 Identificación y análisis de metodologías a nivel internacional y nacional”. A través de la revisión de la literatura se pudo comprobar la existencia de diferentes procedimientos y métodos establecidos en diversos contextos (académico, organizacional, legal) por diversas entidades, gobiernos e instituciones; en donde algunos brindan lineamientos generales para todo el proceso forense, otros están orientados hacia alguna fase en específico (adquisición, análisis), mientras que otros se enfocan en aspectos complementarios de la investigación forense, como la cadena de custodia.

Se identificó como aspecto común que cada país o institución reconoce la importancia de contar con elementos metodológicos definidos que permitan realizar investigaciones forenses digitales de una forma científicamente válida, para obtener mayor valor probatorio de los resultados y hallazgos de los análisis, razón por la cual se ha visto una tendencia generalizada en el interés de definir mecanismos y/o metodologías de alguna forma estandarizados.

Sin embargo, teniendo en cuenta el análisis realizado del contexto colombiano en lo referente a metodologías y/o procedimientos de análisis forense y a la caracterización normativa, no se encontró una metodología formalmente establecida a nivel gobierno con fuerza obligatoria y vinculante sobre las entidades del Estado que desarrollan procesos de análisis forense digital en el país.

La caracterización de la normatividad de nuestro país se planteó como segundo objetivo del proyecto para buscar un fundamento jurídico en la legislación que permitiera diseñar la metodología forense con arreglo a las leyes vigentes que rijan el tema. En la sección “3.2 Clasificación de normatividad colombiana” se vieron los resultados de ese proceso de caracterización, en donde se pudo confirmar que en nuestro país no existe un marco regulatorio unificado con relación a la seguridad informática y/o la informática forense. Si bien, se identificaron algunos acercamientos del legislador por incluir el tema en la normatividad, con la expedición de leyes como la Ley 527 de 1999: Ley de Comercio

Electrónico, Ley 1273 de 2009: Ley de Delitos Informáticos, Ley Estatutaria 1581 de 2012: Ley de Protección de Datos Personales, Ley 1928 de 2018: Ratificación del Convenio sobre la Ciberdelincuencia de Budapest, CONPES 3854: Política Nacional de Seguridad Digital, entre otros, Colombia todavía carece de una norma, ley o metodología de carácter vinculante definida institucionalmente que regule de alguna forma la realización de las investigaciones forenses digitales en el país.

Como resultado del análisis de la normatividad vigente en el país se identificó la necesidad de que se siga trabajando en el tema desde las esferas legislativas, con el fin de que se incluyan, no solamente lo relacionado con la práctica del análisis forense, sino temas transversales de la seguridad digital que permitan contar con un marco regulatorio que determine el accionar de los profesionales de la seguridad de la información y que a su vez brinde las garantías procesales suficientes en las investigaciones penales, disciplinarias y/o administrativas para los sujetos involucrados.

Teniendo en cuenta todos los aspectos mencionados anteriormente, fue posible diseñar la metodología para la realización de investigaciones forenses digitales objeto del presente proyecto, tal como se ilustró en la sección “3.3 Metodología propuesta”.

Con las cinco (5) fases propuestas se abarca todo el proceso de 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 cada una de las etapas propuestas se incluyeron los fundamentos normativos aplicables que permitieran darle un mayor sustento y valor probatorio a los hallazgos; de esta forma la inclusión de la cadena de custodia y la documentación como requisitos transversales a toda la investigación, hacen que se conserve la trazabilidad e integridad de la evidencia durante todo el proceso, permitiendo otorgar mayor confiabilidad a los resultados.

Finalmente, con el objetivo de validar la utilidad de la metodología propuesta, se realizó su aplicación en un caso de estudio práctico, como se ilustró en la sección “3.4 Caso de estudio: Institución universitaria de carácter público de Colombia”, el cual fue llevado a cabo en el Laboratorio de Informática Forense de la Dirección Nacional de Investigaciones Especiales de la Procuraduría General de la Nación.

Este caso de estudio permitió evaluar el grado de dificultad en la aplicación de cada una de las etapas de la metodología, a través de la observación directa de su ejecución. En este ejercicio de valoración se pudo concluir que, en general, las etapas de la metodología propuesta son de fácil aplicación para el equipo investigador del laboratorio; se identificó como un factor de éxito el hecho que los funcionarios ya se encontraban familiarizados con uno de los estándares que se tomaron como base para la metodología propuesta, específicamente la norma SP 800-86 de la NIST. De igual forma, los funcionarios manifestaron que la claridad de los procedimientos y actividades a desarrollar permitía un fácil seguimiento de lo propuesto.

Sin embargo, también se identificaron algunas dificultades con el desarrollo de ciertas actividades de análisis, lo cual se atribuyó al desconocimiento de algunas de las características y funcionalidades de las herramientas forenses con que cuenta el

laboratorio. En consecuencia, resulta necesario que el personal adscrito a la DNIE y perteneciente al laboratorio de informática forense se someta a entrenamientos y capacitaciones periódicas y constantes que refuercen sus habilidades y conocimientos forenses, en especial en lo relacionado con el adecuado manejo de las herramientas hardware y software que se requieren para desempeñar sus funciones.

De igual forma se identificó una deficiencia en la forma como se vienen realizando los análisis forenses digitales en el laboratorio, específicamente en lo relacionado con la verificación de integridad de la evidencia, dado que solo se realiza al inicio del proceso forense, como mecanismo para comprobar que la imagen adquirida es una copia idéntica del dispositivo original (verificación que realiza automáticamente la herramienta forense de adquisición). La metodología propuesta permite subsanar esta deficiencia ya que establece la verificación de integridad en diversos momentos del análisis: como mínimo, al principio y al final del proceso forense.

Durante el desarrollo del caso de estudio se realizó la comprobación de la integridad de la evidencia, realizando el cálculo del código hash (MD5 y SHA1) para la imagen forense utilizada en los análisis, verificando la igualdad con aquellos generados por el FTK Imager al momento de la extracción. Lo anterior brinda un grado de confianza superior en los hallazgos y resultados, otorgándole mayor valor probatorio en el proceso disciplinario.

Por último, como conclusión final es posible decir que se alcanzó el objetivo general del trabajo ya que se obtuvo una metodología que presenta un procedimiento formal, estructurado y con fundamento científico-técnico 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 734 de 2002.

4.2 Recomendaciones, lecciones aprendidas y trabajo futuro

El desarrollo del presente proyecto permitió ofrecer un marco metodológico para la realización de análisis forense digital en entidades del Estado, de forma que consoliden los hallazgos y resultados con mayor valor probatorio dentro de un proceso disciplinario y/o administrativo. Así las cosas, sería muy valioso que esta metodología se logre convertir en un estándar para las entidades gubernamentales que desarrollen investigaciones forenses digitales, de forma que se cuente a nivel país con un procedimiento científicamente válido y seguido por los actores nacionales que realizan este tipo de procesos.

Teniendo en cuenta que se encontraron dificultades para establecer un marco normativo integral para este tipo de pruebas periciales dentro de la legislación colombiana, se evidencia la necesidad de que, desde el nivel gobierno, se trabaje por la inclusión del tema del análisis forense digital en las normas colombianas, para que se puedan contar con procedimientos con respaldo jurídico, de la forma en que se encuentra ahora establecido el procedimiento de cadena de custodia, por ejemplo.

Referencias

[1] Centro Cibernético Policial, «Amenazas del Cibercrimen en Colombia 2016 - 2017,» Policía Nacional - Dirección de Investigación Criminal e INTERPOL, Bogotá, 2017.

[2] Policía Nacional de Colombia, «Informe de las tendencias del cibercrimen en Colombia (2019-2020),» Policía Nacional de Colombia, Bogotá, 2019.

[3] A. R. Almanza J., «XVIII Encuesta Nacional de Seguridad Informática: Evolución del perfil del profesional de Seguridad Digital,» *Sistemas,* nº 147, pp. 16-42, Abril - Junio 2018.

[4] Monitor Ciudadano de la Corrupción, «Así se mueve la corrupción. Radiografía de los hechos de corrupción en Colombia 2016 - 2018,» Corporación Transparencia por Colombia, Bogotá, 2019.

[5] R. Gallardo Rosales, A. G. Fuentes Covarrubia y R. Fuentes Covarrubia, «Un enfoque básico sobre Informática Forense,» México, 2016.

[6] L. Caviglione, S. Wendzel y W. Mazurczyk, «The Future of Digital Forensics: Challenges and the Road Ahead,» *IEEE Security & Privacy,* vol. 15, nº 6, pp. 12-17, Noviembre/Diciembre 2017.

[7] L. Englbrecht, S. Meier y G. Pernul, «Towards a capability maturity model for digital forensic readiness,» *Wireless Networks,* vol. 26, nº 7, p. 4895–4907, 2020.

[8] M. M. Haque y S. A. Hossain, «National digital forensics framework for Bangladesh,» de *2017 3rd International Conference on Electrical Information and Communication Technology (EICT)*, Khulna, Bangladesh, 2017.

[9] N. Jain y K. Dhananjay R, «Digital forensic framework using feedback and case history keeper,» de *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, Mumbai, India, 2015.

[10] N. m. 2. Karie y S. M. D. Karume, «Digital Forensic Readiness in Organizations: Issues and Challenges,» *Journal of Digital Forensics, Security and Law:,* vol. 12, nº 4, pp. 43-54, 2017.

[11] A. Mouhtaropoulos, C.-T. Li y M. Grobler, «Digital forensic readiness: Are we there yet?,» *Journal of International Commercial Law and Technology,* vol. 9, nº 3, pp. 173-179, 2014.

[12] M. Elyas, A. Ahmad, S. B. Maynard y A. Lonie, «Digital forensic readiness: Expert perspectives on a theoretical framework,» *Computers & Security,* vol. 52, pp. 70-89, 2015.

[13] Fiscalía General de la Nación, Manual del Sistema de Cadena de Custodia, Bogotá: Fiscalía General de la Nación, 2018, p. 72.

[14] Transparency International, «Corruption Perceptions Index 2018,» Transparency International, Berlín, 2019.

[15] Congreso de la República de Colombia, *Ley N° 734 de 2002,* Bogotá, 2002.

[16] Avast, «Cybercrime,» s.f.. [En línea]. Available: https://www.avast.com/c-cybercrime. [Último acceso: 23 mayo 2019].

[17] Panda Security, «Types of Cybercrime,» 20 agosto 2018. [En línea]. Available: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/. [Último acceso: 23 mayo 2019].

[18] INTERPOL, «Cybercrime,» 2018. [En línea]. Available: https://www.interpol.int/content/download/5267/file/Cybercrime.pdf. [Último acceso: 24 mayo 2019].

[19] J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation, Third ed., Boston: Charles River Media, 2008, p. 865.

[20] I. Resendez, P. Martínez y J. Abraham, «An Introduction to Digital Forensics,» *ResearchGate,* pp. 2-11, 2014.

[21] Cybersecurity and Infrastructure Security Agency (CISA), «Computer Forensics,» 2008. [En línea]. Available: https://www.us-cert.gov/sites/default/files/publications/forensics.pdf. [Último acceso: 20 mayo 2019].

[22] E. Casey, Ed., Handbook of Digital Forensics and Investigation, San Diego: Elsevier Inc., 2010, p. 594.

[23] C. R. García Dahinten, «Cadena de custodia digital de las evidencias para la realización de un peritaje,» Universidad de San Carlos de Guatemala, Guatemala, 2014.

[24] F. J. De León Huerta, «Estudio de metodologías de análisis forense digital,» Instituto Politécnico Nacional, Ciudad de México, 2009.

[25] A. Ghosh, «Guidelines for the Management of IT Evidence,» de *Incident Response & Forensics Workshop APEC-Tel 29*, Hong Kong, 2004.

[26] National Institute of Justice, «Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition,» U.S. Department of Justice, Washington, DC, 2008.

[27] Congreso de la República de Colombia, *Ley 527 de 1999,* Bogotá, 1999.

[28] Real Academia de la Lengua Española, «Diccionario del español jurídico,» 2020. [En línea]. Available: https://dej.rae.es/lema/principio-de-equivalencia-funcional. [Último acceso: 28 abril 2020].

[29] G. Semprini, «El Análisis integral de la evidencia digital,» de *SID, Simposio Argentino de Informática y Derecho*, Córdoba, 2017.

[30] L. D. Lobo Parra, «Desarrollo e implementación del análisis digital forense utilizando una metodología post-mortem,» Universidad Francisco de Paula Santander, Ocaña, 2014.

[31] C. E. López Grande y R. S. Guadron Gutiérrez, «Informática forense: Cuando el delito hace uso de la tecnología,» *Revista Tecnológica,* nº 10, pp. 20-26, 2017.

[32] R. M. Aguilera Hintelholher, «Identidad y diferenciación entre Método y Metodología,» *Estudios Políticos,* nº 28, pp. 81-103, 2013.

[33] M. F. Daza Pérez, «La naturaleza jurídica del derecho disciplinario ¿autónoma e independiente?,» *Actualidad Jurídica,* vol. 3 y 4, pp. 57-63, 2012.

[34] Procuraduría General de la Nación, «Código Disciplinario Único - Notas de vigencia 2011,» Imprenta Nacional de Colombia, Bogotá, 2011.

[35] Procuraduría General de la Nación, «Constitución Política de Colombia 1991 - Procuraduría Ciudadana,» Imprenta Nacional de Colombia, Bogotá, 2017.

[36] C. A. Gómez Pavajeau, «El derecho disciplinario en Colombia. "Estado del arte",» *Revista Derecho Penal y Criminología,* vol. XXXII, nº 92, pp. 115-154, 2011.

[37] A. A. Garba y A. M. Bade, «A recommended digital forensic readiness framework for Nigerian banks,» *International Journal of Development Research,* vol. 9, nº 8, pp. 28920-28928, 2019.

[38] R. Montasari, «The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice,» University of Derby, Reino Unido, 2016.

[39] K. Kent, S. Chevalier, T. Grance y H. Dang, «NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response,» National Institute of Standards and Technology - NIST, Gaithersburg, Maryland, 2006.

[40] Scientific Working Group on Digital Evidence - SWGDE, *SWGDE Best Practices for Computer Forensic Acquisitions,* 1.0 ed., 2018.

[41] A. F. Álvarez Serna, O. D. Marín Rivera y J. D. Victoria Morales, «Framework para la computación forense en Colombia,» *Ing. USBMed,* vol. 3, nº 2, pp. 61-69, 2012.

[42] C. Villamizar, A. Orjuela y M. Adarme, «Análisis forense en un sistema de información en el marco normativo colombiano,» *Investigación e Innovación en Ingenierías,* vol. 3, nº 1, pp. 36-43, Enero - junio 2015.

[43] Fiscalía General de la Nación, Manual de Procedimientos para cadena de custodia, Bogotá: Fiscalía General de la Nación, 2008, p. 147.

[44] Fiscalía General de la Nación, «Manual Único de Policía Judicial,» Fiscalía General de la Nación, Bogotá, 2018.

[45] Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, Guía N° 13. Evidencia Digital, Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, 2016, p. 30.

[46] Procuraduría General de la Nación, «Procedimientos de Investigación Técnico Científica,» 10 enero 2019. [En línea]. Available: https://www.procuraduria.gov.co/portal/Mapa-de-procesos-component.page#postfind. [Último acceso: 5 febrero 2019].

[47] D. A. Roa Salguero, «La justicia digital en el derecho disciplinario,» *Artículo inédito,* pp. 1-10, 2020.

[48] International Organization for Standardization - ISO, «ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence,» International Organization for Standardization - ISO, Geneva, Switzerland, 2012.

[49] C. Gervilla Rivas, «Metodología para un análisis forense,» Universitat Oberta de Cayalunya - INCIBE (Instituto Nacional de Ciberseguridad), España, 2014.

[50] M. Grobler, «Digital Forensic Standards: International Progress,» de *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, Port Elizabeth, South Africa, 2010.

[51] R. V. Huanca Quispe, «Metodología de análisis forense digital para la extracción de datos almacenados en dispositivos móviles basados en sistema operativo Android,» Universidad Mayor de San Andrés, La Paz, Bolivia, 2014.

[52] D.-Y. Kao, G.-J. Wu y Y.-H. Chiu, «A Novel Process Framework for Digital Forensics Tools: Based on ISO/IEC 27037:2012,» de *The Asian Conference on Business & Public Policy 2014*, Taiwan, 2015.

[53] A. M. Nessi, Manual de Evidencia Digital, Lima, Perú: American Bar Association, 2017, p. 64.

[54] J. S. Rueda Rueda, D. Rico Bautista y C. D. Guerrero, «Guía práctica abierta para el análisis forense digital en dispositivos Android,» *Revista Ibérica de Sistemas e Tecnologias de Informação,* nº E18, p. 442–457, Febrero 2019.

[55] Ministerio de Seguridad de la Nación, «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,» Ministerio de Seguridad de la Nación, Buenos Aires, 2016.

[56] Procuración General de la Nación, «Resolución 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital,» Procuración General de la Nación, Buenos Aires, 2016.

[57] A. Grego Kibrit, «Estado de la Investigación Forense Digital en México,» Asociación por los Derechos Civiles, México D.F., 2017.

[58] Association of Chief Police Officers - ACPO, «ACPO Good Practice Guide for Digital Evidence,» Association of Chief Police Officers - ACPO, United Kingdom, 2012.

[59] National Institute of Justice, «Forensic Examination of Digital Evidence: A Guide for Law Enforcement,» U.S. Department of Justice, Washington, DC, 2004.

[60] E. Casey, Digital evidence and computer crime, Third ed., San Diego, California: Elsevier Inc., 2011, p. 837.

[61] R. K. Yin, Case Study Research: Design and Methods, Fourth edition ed., USA: SAGE Publications, 2009.

[62] Procuraduría General de la Nación, «Caracterización Subproceso de Investigación Técnico Científica,» Procuraduría General de la Nación, Bogotá, 2018.

[63] J. Veber y Z. Smutny, «Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic,» de *14th European Conference on Cyber Warfare & Security*, Hatfield, UK, 2015.

[64] A. Ajijola, P. Zavarsky y R. Ruhl, «A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012,» de *World Congress on Internet Security, WorldCIS 2014*, London, UK, 2014.

[65] Asociación por los Derechos Civiles - ADC, «La investigación forense informática en América Latina,» Asociación por los Derechos Civiles - ADC, Argentina, 2018.

[66] Poder Judicial Provincia del Neuquén, «Protocolo de actuación para pericias informáticas,» Poder Judicial Provincia del Neuquén, Neuquén, Argentina, s.f..

[67] G. Cruz Forero, «Estado de la Investigación de Evidencias Digitales en Colombia,» Asociación por los Derechos Civiles, Bogotá, 2017.

[68] Departamento Nacional de Planeación, «Documento CONPES 3854. Política Nacional de Seguridad Digital,» Consejo Nacional de Política Económica y Social, Bogotá, 2016.

[69] European Network of Forensic Science Institutes (ENFSI), «Best Practice Manual for the Forensic Examination of Digital Technology,» European Network of Forensic Science Institutes (ENFSI), Wiesbaden, Alemania, 2015.

[70] European Network of Forensic Science Institutes (ENFSI), «Guidelines for Best Practice in the Forensic Examination of Digital Techonology,» European Network of Forensic Science Institutes (ENFSI), Wiesbaden, Alemania, 2009.