CAPÍTULO 10

PROCEDIMIENTO FORENSE PARA IOT DIRIGIDO A LABORATORIOS FORENSES DE LA POLICÍA NACIONAL DE COLOMBIA

Data de submissão: 13/02/2025 *Data de aceite: 05/03/2025*

Diego Mauricio Negro Lozano
Escuela de Tecnologías de la Información y las Comunicaciones Tc. Jorge Luis Mauledoux
ORCID: 0009-0008-7738-6649

Sandra Milena Guzmán Bejarano
Escuela de Tecnologías de la Información y las Comunicaciones Tc. Jorge Luis Mauledoux
ORCID: 0009-004-3262-5141

Jorge Hernando Ruíz Otálora
Investigador en Ciencia Tecnología e Innovación
ORCID: 0000-0003-2214-3558

RESUMEN: La investigación en procedimientos forenses en IoT contribuye al desarrollo de prácticas de ciberseguridad a nivel global. El presente estudio descriptivo-propositivo, enfocado en la sobre creación un procedimiento forense para IoT dirigido a investigadores periciales de la Policía Nacional de Colombia, se conformó en 2 fases de investigación, Fase I relacionada con el análisis de la evidencia científica encontrada en bases de datos mediante el método PRISMA y la Fase II referente a la Propuesta estandarizada. Los resultados indican que la creación de un procedimiento dentro de la Policía Nacional de Colombia es un procedimiento complejo que prevé de la consideración cuidadosa de una variedad de parámetros institucionales, dentro de los cuales se encuentran: la alineación con la misión y visión que presenta la institución, la conformidad con las normativas legales, la compatibilidad con las políticas institucionales, la factibilidad operativa, la participación interinstitucional, y la mejora continua. Los cuales proveen la garantía de que el procedimiento no solo sea efectivo en la práctica, sino que también esté en plena consonancia con los objetivos y valores de la Policía Nacional de Colombia. Es importante indicar que la correcta adquisición de datos persistentes, volátiles, paquetes de red y datos de smartcards es fundamental en la investigación de eventos adversos sobre la seguridad asociados con dIoT en Colombia, siguiendo los procedimientos detallados anteriormente, se puede asegurar que la evidencia de tipo digital se recopile y se conserve de forma que sea admisible y útil en procesos judiciales, al tiempo que se respetan las consideraciones legales y éticas pertinentes.

PALABRAS-CLAVE: Laboratorio forense, Internet de las cosas, ciberseguridad, evidencia digital.

FORENSIC PROCEDURE FOR IOT AIMED AT FORENSIC LABORATORIES OF THE NATIONAL POLICE OF COLOMBIA

ABSTRACT: Research on IoT forensic procedures contributes to the development of cybersecurity practices at a global level. The present descriptive-propositional study, focused on the creation of a forensic procedure for IoT aimed at forensic investigators of the Colombian National Police, was made up of 2 research phases, Phase I related to the analysis of scientific evidence found in databases using the PRISMA method and Phase II referring to the standardized proposal. The results indicate that the creation of a procedure within the Colombian National Police is a complex procedure that requires careful consideration of a variety of institutional parameters, including: alignment with the mission and vision presented by the institution, compliance with legal regulations, compatibility with institutional policies, operational feasibility, inter-institutional participation, and continuous improvement. These provide the guarantee that the procedure is not only effective in practice, but is also fully in line with the objectives and values of the Colombian National Police. It is important to note that the correct acquisition of persistent, volatile, network packet and smartcard data is essential in the investigation of adverse security events associated with IoT devices in Colombia. By following the procedures detailed above, it can be ensured that digital evidence is collected and preserved in a way that is admissible and useful in judicial proceedings, while respecting relevant legal and ethical considerations.

KEYWORDS: Forensic laboratory, Internet of things, cybersecurity, digital evidence.

PROCEDIMENTO FORENSE PARA IOT DIRECIONADO AOS LABORATÓRIOS FORENSES DA POLÍCIA NACIONAL DA COLÔMBIA

RESUMO: A investigação em procedimentos forenses em IoT contribui para o desenvolvimento de práticas de segurança cibernética a nível global. O presente estudo descritivo-propositivo, focado na criação excessiva de um procedimento forense para IoT dirigido a investigadores peritos da Polícia Nacional da Colômbia, foi composto por 2 fases de pesquisa, Fase I relacionada à análise das evidências científicas encontradas em bancos de dados utilizando o método PRISMA e Fase II referente à Proposta padronizada. Os resultados indicam que a criação de um procedimento dentro da Polícia Nacional Colombiana é um procedimento complexo que requer consideração cuidadosa de uma variedade de parâmetros institucionais, entre os quais estão: alinhamento com a missão e visão apresentada pela instituição, cumprimento dos regulamentos legais, compatibilidade com políticas institucionais, viabilidade operacional, participação interinstitucional e melhoria contínua. O que garante que o procedimento não só é eficaz na prática, mas também está totalmente alinhado com os objetivos e valores da Polícia Nacional Colombiana. É importante indicar que a correta aquisição de dados persistentes e voláteis, pacotes de rede e dados de cartões inteligentes é fundamental na investigação de eventos adversos de segurança associados à dIoT na Colômbia, seguindo os procedimentos detalhados acima, pode-se garantir que as provas digitais sejam coletadas e preservadas de forma admissível e útil em processos judiciais, respeitando ao mesmo tempo as considerações legais e éticas relevantes.

PALAVRAS-CHAVE: Laboratório forense, Internet das coisas, segurança cibernética, provas digitais.

INTRODUCCIÓN

El *"internet de las cosas (IoT)",* se fundamenta sobre la interconexión que llevan a cabo dispositivos físicos mediante el internet, permitiéndoles recopilar y gestionar datos, estos dispositivos pueden abarcar una "*amplia gama de objetos cotidianos",* desde electrodomésticos, vehículos hasta dispositivos de salud y equipos industriales. La idea central es establecer una conexión entre estos objetos inteligentes que permita la comunicación y con sistemas centrales para recopilar, procesar y actuar en función de los datos generados (Madakam et al., 2015; Tran-Dang et al., 2020).

Dentro de las características fundamentales del IoT, se encuentra la Conectividad, ya que los "*dispositivos IoT (dIoT)",* se conforman de actuadores, sensores y sistemas tecnológicos de conectividad (como *Wi-Fi, Bluetooth, Zigbee,* etc.) para facilitar la comunicación (Mouha, 2021; Lombardi et al., 2021). Los sensores son los encargados de compilar información del entorno, como: humedad, temperatura, ubicación, etc. Mientras que los actuadores se encargan de que los dispositivos realicen acciones físicas en respuesta a la información recopilada (Qureshi et al., 2022). Frente a la *"Comunicación Máquina a Máquina (M2M)",* los dIoT se relacionan directamente entre sí, sin intervención humana, lo que permite la automatización de procesos. En cuanto a la Nube, los datos que se compilan por los dispositivos se transmiten a menudo a la nube para el almacenamiento, procesamiento y análisis centralizado (Verma et al., 2016; Kumar y Kumar, 2022; Ponis y Efthymiou, 2020)

Ahora bien, el análisis de información en tiempo real o posterior permite obtener información valiosa para la toma de decisiones. Los dispositivos pueden realizar acciones automáticamente basándose en la información recibida, mejorando la eficiencia y la respuesta a cambios en el entorno (Matarrese, 2020; Sarker, 2021). Dentro de los ejemplos de aplicaciones del IoT se encuentran; sistemas de salud conectados, termostatos inteligentes, sistemas de monitorización industrial, vehículos autónomos, ciudades inteligentes y mucho más. A medida que el IoT continúa evolucionando, se esperan desarrollos adicionales para la mejora de la eficiencia, la conectividad y la seguridad de los dispositivos interconectados (Sharma et al., 2019; Sahu et al., 2020). El IoT se utiliza en diferentes sectores como: la salud, la agricultura, la industria, el hogar inteligente, los vehículos conectados, la logística, entre otros, la seguridad en IoT es crucial para proteger la integridad, así como la confidencialidad de la información, para prevenir ataques a la privacidad de los usuarios (Gubbi et al., 2013; Chanal y Kakkasageri, 2020).

Los procesos forenses en el *"Internet de las cosas (IoT)"* se refiere a la aplicación de técnicas y procedimientos forenses digitales para investigar incidentes relacionados con dIoT; dado que los dIoT están conectados a la red de internet y recopilan una gran cantidad de datos, es crucial llevar a cabo procedimientos forenses adecuados para recopilar, preservar y analizar evidencia de manera que sea aceptable en un estrado judicial (Stoyanova et al., 2020; Rani y Gill, 2020). En concordancia, la investigación se presenta como una necesidad crítica en el contexto actual, donde los dIoT conectados a la red ha generado una nueva dimensión de desafíos referentes a la seguridad y privacidad. El IoT, al integrar dispositivos físicos con capacidades de comunicación, ha ampliado significativamente la superficie de ataque, creando un escenario propicio para incidentes

cibernéticos y actividades maliciosas (Djenna et al., 2021; Pasdar et al., 2024). De igual manera, el número de dIoT en hogares, empresas e infraestructuras críticas, que han evidenciado un exponencial crecimiento, esta proliferación intensifica la complejidad de la ciberseguridad, haciendo esencial desarrollar procedimientos forenses específicos para abordar los desafíos únicos presentes en este entorno (Ahmad y Zhang, 2021). De otro lado, las amenazas dirigidas específicamente a dIoT, como: "*ataques de denegación de servicio"*, manipulación de datos y toma de control remoto, requieren enfoques forenses especializados. Investigar y comprender estas amenazas permitirá desarrollar estrategias de respuesta y prevención más efectivas (Salim et al., 2020; Parra de Gallo, 2022)

Es así como, la información recopilada por los dIoT a menudo incluye datos sensibles y privados. Los incidentes de seguridad pueden exponer la privacidad de los consumidores y erosionar la confianza en la adopción generalizada de estas tecnologías (Rashid et al., 2024; Babun et al., 2021). La investigación forense puede contribuir a mitigar estos riesgos y fortalecer la confianza en la adopción de IoT. De igual manera, la diversidad de dIoT, sus arquitecturas y procedimientos de comunicación plantean desafíos significativos en la recopilación y preservación de evidencia forense, investigar métodos y procedimientos específicos para manejar esta complejidad asegurará la integridad y admisibilidad de la evidencia en un entorno legal (Abiodun et al., 2022; Vaghela et al., 2024). A medida que el uso de IoT se convierte en una parte integral de la sociedad, la falta de normativas y estándares forenses específicos para este ámbito crea un vacío que debe abordarse (Parra-Sánchez et al., 2021)

De acuerdo con ello, actualmente no se cuenta con un procedimiento Forense en IOT que aporte a los procesos investigativos coadyuvando a la administración de justicia en Colombia, es por tanto que se plantea como interrogante: ¿Qué parámetros se deben tener en cuenta en un procedimiento forense para IoT dirigido a investigadores de la *Policía Nacional de Colombia, (PNC)*?

La investigación en procedimientos forenses en IoT contribuirá al desarrollo de prácticas de ciberseguridad a nivel global, pues la colaboración y el intercambio de los conocimientos en esta área son esenciales para la construcción de una infraestructura segura y resistente en el panorama del IoT. El presente estudio descriptivo- propositivo, se conforma en 2 fases de investigación, Fase I relacionada con el análisis de la evidencia científica encontrada en bases de datos mediante el método PRISMA y la Fase II referente a la Propuesta estandarizada, las cuales cumplieron con el enfoque principal de la investigación sobre **c**rear un procedimiento forense para IoT dirigido a investigadores de la PNC, para el fortalecimiento del análisis pericial. Así mismo se analizaron las particularidades de los dIoT más comunes utilizados en Colombia, considerando su diversidad y la frecuencia de su adopción, para que se identifique aquellos objetos sobre los cuales se extrae información relevante en procesos forenses, la identificación de los parámetros institucionales para la creación de un procedimiento en la *Policía Nacional (PN),* para que el procedimiento se alinee a las políticas institucionales y la definición de los componentes de un procedimiento que aborde los desafíos específicos relacionados con la recopilación, preservación y análisis de evidencia en casos de incidentes de seguridad en dIoT en el contexto colombiano, para que se garantice un proceso adecuado de análisis.

MATERIALES Y MÉTODOS

Tipo de estudio

La presente investigación se fundamentó en las teorías y estudios presentados por Parra, (2022) y Balanta et al., (2021). El enfoque cualitativo, descriptivo y propositivo es adecuado para esta investigación, ya que permite explorar y comprender en profundidad los procedimientos forenses en IoT desde la perspectiva de los investigadores de la PNC, este enfoque se centra en la recolección de datos no numéricos y en el análisis de fenómenos complejos, proporcionando una visión detallada sobre el enfoque analizado (Balanta et al., 2021; Parra de Gallo, 2022)

METODOLOGÍA

Fase I: análisis de la evidencia científica

Mediante el método *"Preferred Reporting Items for Systematic Reviews and Meta-Analyses, PRISMA",* se recopilan datos detallados sobre los procedimientos forenses en IoT, que requirió del establecimiento de una ecuación de búsqueda:

- (Internet de las cosas) AND (laboratorio forense) AND (policía) AND (forense)

Así como el establecimiento de preceptos de inclusión y exclusión para la elección del material idóneo. Se presenta el análisis de datos según distribución de la información a través del tiempo y distribución geográfica, mediante de las bases de datos de Scopus, Science Direct y el buscador de *Google académico*. Los datos relevantes fueron analizados, identificados en patrones, categorías y conceptos clave que emergen de la información recopilada.

Dentro de los preceptos de inclusión aplicados se enuncian:

- Se incluyen a la presente investigación documentos de tipo empíricos y retrospectivos.
- Se incluyen documentos de tipo descriptivos pero basados en la propuesta de un procedimiento forense para IoT dirigido a investigadores de la PNC, para el fortalecimiento del análisis pericial o temas relacionados que sirvan de base para la investigación.
- Se incluyen los documentos publicados en los últimos 7 años de investigación científica.
- Se incluyen documentos de acceso libre.
- Dentro de los preceptos de exclusión se enuncian:
- Se excluyen documento tipo o teóricos.
- Documentos enfocados en el uso de IoT en otras áreas de investigación.
- Documentos de acceso pago
- Documentos con más de 7 años de investigación científica.

Fase II: Desarrollo y validación de una propuesta estandarizada

Procesamiento de la información

Los documentos seleccionados para el análisis documental se llevaron a cabo mediate la lectura y análisis preliminar para obtener una comprensión general del contenido e identificar temas y patrones recurrentes. Seguido de la aplicación de una codificación abierta de la información identificando categorías y subcategorías emergentes. Este proceso implica descomponer los datos en unidades significativas y etiquetarlas con códigos descriptivos. El tercer paso del procesamiento se refirió a la codificación axial, donde se relacionaron las categorías y subcategorías identificadas en la *codificación abierta,* estableciendo conexiones entre ellas para formar un esquema coherente de los procedimientos forenses en IoT. El cuarto paso se consideró la aplicación de una codificación selectiva, que integra y redefine las categorías y subcategorías, seleccionando aquellas que son más relevantes y representativas para el estudio. Se construyen modelos y teorías emergentes que describen los procedimientos forenses en IoT. Por último, la interpretación de resultados y presentación de estos, se organizaron en formato comprensible y accesible, mediante diagramas que explican los procedimientos forenses en IoT y se destacan los alcances prácticos y teóricos de los hallazgos.

Validación de la información documental y de la herramienta mediante el jueceo de expertos

La herramienta jueceo de expertos (Abellán, 2021), fue llevada a valoración por los siguientes expertos:

1. PhD. Msc. Sistemas de Información. Jonh Roberth Correa.
2. Msc. Seguridad de la Información. Jhon Félix Rivera Gutiérrez
3. Msc. Tecnología e informática. Fabian Giovanni González Robayo.
4. Msc. Seguridad de las TIC´s. Jhon Alberto Talero Patarroyo.

Sobre la utilidad y análisis de áreas de conocimiento aplicadas en la herramienta, la cual posee 4 aspectos específicos de relevancia y análisis:

- *Adquisición de Datos Persistentes (ADP)*
- *Adquisición de Datos Volátiles (ADV)*
- *Adquisición de Paquetes de Red (APR)*
- *Adquisición de Datos de Smartcards (ADS)*

RESULTADOS

Fase I: Análisis de la línea de investigación

El metaanálisis reporta un incremento sobre la línea de investigación desde el año 2021 hasta el año 2024, siendo el 2023, el año que reporta gran mayoría de registros científicos en la base de datos de Scopus (figura 1).

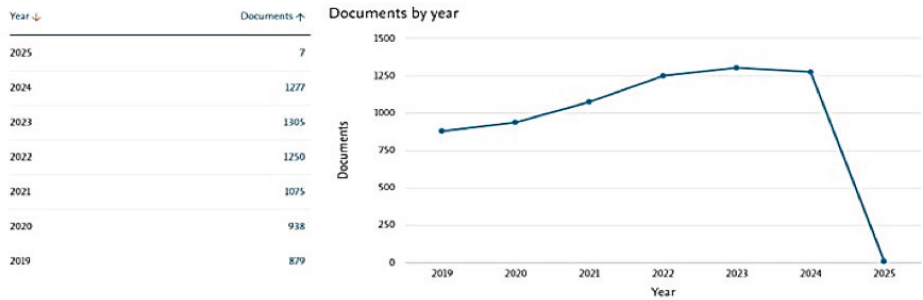

Figura 1. Distribución por años de investigación científica de la línea de IoT.
Fuente: Metaanálisis tomado de Scopus.

La figura 2, refleja que los países con mayor interés en la producción científica de la aplicación del IoT son China, India y Estados Unidos, con registros de 1957, 1316, 1000, respectivamente.

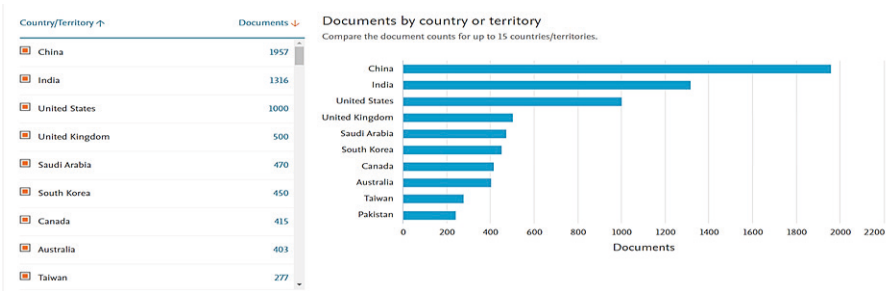

Figura 2. Distribución geográfica de la producción científica de la línea de investigación IoT.
Fuente: Metaanálisis tomado de Scopus.

Resumen del Método PRISMA

La presente fase de recopilación de información utilizada para la creación de un procedimiento forense para IoT dirigido a investigadores de la PNC, para el fortalecimiento del análisis pericial, compilo un total de 170 documentos de los cuales se eliminaron 62 documentos científicos que se disponían por duplicado o por lectura critica, de los que 108 fueron sometidos a fase de cribado, para la elección de 42 documentos que fueron valorados por criterios de elección. A la presente investigación se incluyeron un total de 15 documentos, de los cuales 2 documentos se encontraban fuera de del rango de producción científica (2018-2024), pero fueron incluidos por criterios de enfoque de investigación ya que aporta información relevante para el estudio.

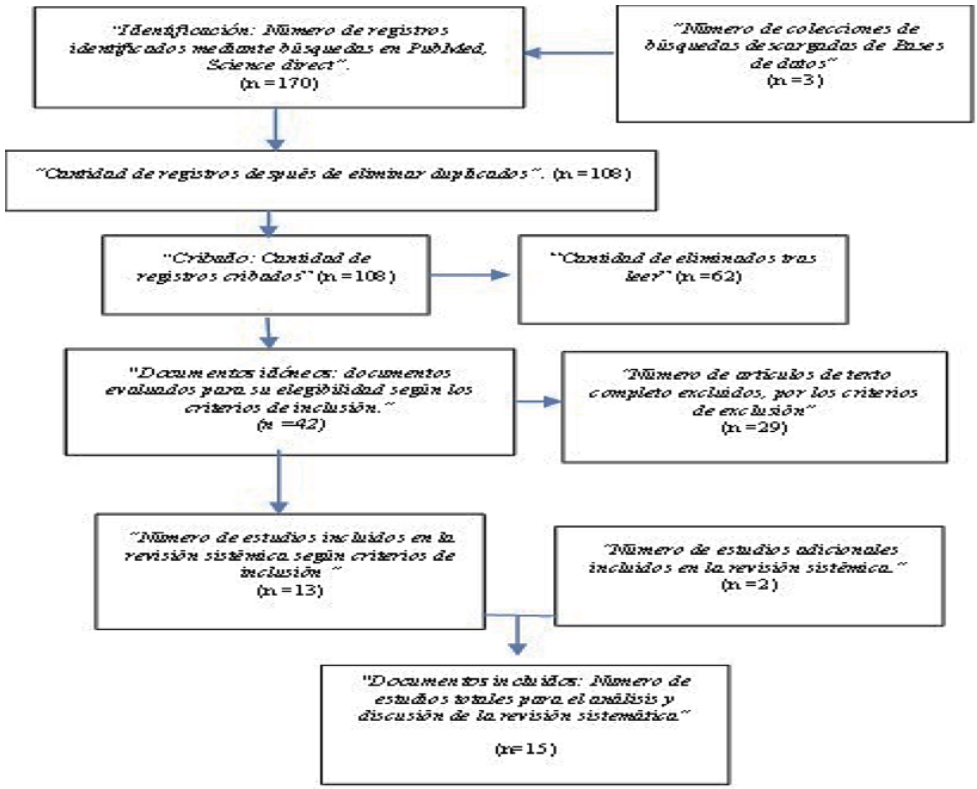

Figura 3. Diagrama de inclusión mediante el modelo de la Declaración PRISMA.

Fuente: modelo tomado de (Page et al., 2021; Ciapponi, 2021)

Análisis de las particularidades de los dIoT más comunes en Colombia

El Internet de las Cosas (IoT) ha ganado un lugar destacado en la vida cotidiana y en el area industrial de Colombia, el creciente uso de dIoT en sectores como la salud, la agricultura, la gestión urbana y la seguridad ha generado una necesidad creciente de procedimientos forenses especializados que permitan extraer información relevante de estos dispositivos en el contexto de investigaciones criminales (Ahmed et al., 2024; Montasari et al., 2020). Este apartado propone analizar las particularidades de los dIoT más comunes utilizados en Colombia, considerando su diversidad y frecuencia de adopción, para identificar aquellos objetos sobre los cuales se extrae información relevante en procesos forenses (Balanta et al., 2021; Farfan Chiun, 2024).

DIVERSIDAD Y FRECUENCIA DE ADOPCIÓN DE DIOT EN COLOMBIA

Categorías de dIoT

En Colombia, los dIoT pueden clasificarse en varias categorías según su aplicación y uso, estas categorías incluyen, entre otras, dispositivos de hogares inteligentes, dispositivos de salud, dispositivos de monitoreo ambiental, dispositivos de agricultura inteligente y dispositivos de gestión de infraestructuras urbanas. Los dispositivos de hogares inteligentes son cada vez más comunes en los hogares colombianos, estos dispositivos incluyen termostatos inteligentes, sistemas de seguridad, cámaras de vigilancia, luces inteligentes, asistentes de voz como Amazon Echo y Google Home, y electrodomésticas conectados, la adopción de estos dispositivos ha crecido debido a su capacidad para mejorar la comodidad, la eficiencia energética y la seguridad del hogar (Gómez Mendoza, 2024).

En el área de la salud, los dIoT juegan un papel crucial en el monitoreo de pacientes y la gestión de datos médicos, entre los dispositivos más comunes se encuentran los monitores de glucosa, pulseras de actividad física, sensores de signos vitales, y equipos médicos conectados como desfibriladores y marcapasos, estos dispositivos permiten un seguimiento continuo y en tiempo real de la salud de los pacientes, que mejoran el estado de la calidad de la atención médica (Rodríguez et al., 2023). Los dispositivos de monitoreo ambiental son esenciales para *"la gestión de recursos naturales y la protección del medio ambiente en Colombia";* sensores de calidad del aire, estaciones meteorológicas inteligentes, y dispositivos de monitoreo de agua son algunos ejemplos, estos dispositivos recopilan datos ambientales cruciales que ayudan a tomar decisiones sobre la gestión de recursos y la mitigación de riesgos ambientales (Saucedo & Regalado, 2024).

La agricultura en Colombia ha adoptado dIoT para mejorar la productividad y la sostenibilidad, los sensores de humedad del suelo, sistemas de riego automatizados, drones agrícolas, y sensores de monitoreo de cultivos son herramientas comunes que permiten a los agricultores gestionar mejor el uso de recursos y mejorar los rendimientos de los cultivos (Aceros, 2020). En las ciudades colombianas, los dIoT se utilizan para gestionar infraestructuras y servicios urbanos de manera eficiente, esto incluye "*sistemas de gestión de tráfico",* iluminación pública inteligente, sensores de basura y sistemas de transporte público conectados, estos dispositivos ayudan a mejorar el estado de la calidad de vida de los ciudadanos y a optimizar la gestión de los recursos urbanos (Pérez, 2022).

La frecuencia de adopción de dIoT en Colombia varía según la categoría y la región, un estudio realizado por el *"Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)"* en 2016 reveló que los dispositivos de hogares inteligentes y los dispositivos de salud son los más adoptados en las zonas urbanas, mientras que los dispositivos de agricultura inteligente son más comunes en las zonas rurales. Los dispositivos de monitoreo ambiental y de gestión de infraestructuras urbanas se utilizan ampliamente en ciudades como: Medellín, Bogotá y Cali (Ministerio de Tecnologia e Informacion, 2016).

Particularidades de los dIoT

Los dispositivos de hogares inteligentes presentan varias particularidades que los hacen relevantes en el contexto forense, estos dispositivos están diseñados para interactuar entre sí y con el usuario a través de una red doméstica y una plataforma central, como un asistente de voz o una aplicación móvil, la información relevante que se puede extraer de estos dispositivos incluye registros de actividad, comandos de voz, grabaciones de video y datos de uso de energía. La extracción de información de dispositivos de hogares inteligentes presenta desafíos únicos debido a la diversidad de fabricantes y *"la falta de estandarización en los protocolos de comunicación"* y almacenamiento de datos, además, la seguridad y la privacidad son factores preocupantes e importantes, ya que estos dispositivos almacenan datos sensibles sobre la vida cotidiana de los usuarios.

Los dispositivos de salud IoT recopilan y transmiten datos médicos sensibles y críticos, estos dispositivos suelen estar equipados con sensores avanzados que miden una variedad de parámetros de salud, la información relevante en el contexto forense puede incluir registros de signos vitales, historiales médicos y datos de actividad física. La principal particularidad de los dispositivos de salud es el requerimiento de brindar garantía sobre aspectos como: la integridad y la confidencialidad de la información médica, los investigadores forenses deben cumplir con estrictas normativas de protección de datos, como la *"Ley 1581 de 2012 en Colombia",* que regula el manejo de datos personales, la interoperabilidad y la seguridad de la información son aspectos críticos que deben abordarse durante el análisis forense.

Los dispositivos de monitoreo ambiental IoT recopilan datos sobre las condiciones ambientales, como la calidad del aire, la temperatura, la humedad y los niveles de contaminación, estos dispositivos son cruciales para la gestión de riesgos ambientales y la planificación urbana. La particularidad de estos dispositivos radica en la gran cantidad de datos que generan y la necesidad de contextualizar estos datos en términos de ubicación y tiempo, los investigadores forenses deben ser capaces de correlacionar los datos ambientales con eventos específicos para proporcionar evidencia concluyente.

Los dispositivos de agricultura inteligente están diseñados para optimizar el uso de recursos y mejorar la productividad agrícola, la información relevante en el contexto forense puede incluir datos sobre el uso de agua, la fertilización, y las condiciones de los cultivos. La principal particularidad de estos dispositivos es la variabilidad de los entornos en los que operan y la necesidad de adaptar los procedimientos forenses a diferentes tipos de cultivos y prácticas agrícolas, además, la conectividad en áreas rurales puede ser limitada, lo que plantea desafíos adicionales para la recolección de datos.

Los dispositivos de gestión de infraestructuras urbanas IoT se utilizan para optimizar la gestión de servicios urbanos, como el tráfico, la iluminación pública y la recolección de basura, la información relevante puede incluir datos de tráfico, patrones de uso de energía y registros de mantenimiento. La particularidad de estos dispositivos es la necesidad de gestionar volúmenes grandes de información en tiempo real y de garantizar la precisión y la fiabilidad de los datos recopilados, los investigadores forenses deben ser capaces de analizar y correlacionar estos datos para identificar animalias o patrones que sean relevantes en una investigación.

Procedimientos forenses para dIoT

La recolección de información de dIoT requiere el uso de herramientas y técnicas especializadas que permitan acceder y extraer datos sin tener que comprometer la integridad de estos, lo que puede incluir la captura de tráfico de red, la extracción de datos de memoria y el acceso a bases de datos internas de los dispositivos.

El análisis de datos forenses de dIoT implica la detección de patrones, la correlación de eventos y la reconstrucción de actividades, los investigadores deben ser capaces de interpretar los datos en el contexto del dispositivo y su aplicación específica.

La presentación de resultados en una investigación forense de IoT debe ser clara y comprensible, proporcionando una narrativa coherente que explique cómo se compila y analiza la información y cuáles son las conclusiones derivadas de este análisis.

Parámetros institucionales para la creación de un procedimiento en la Policía Nacional, para que el procedimiento se alinee a las políticas institucionales.

La creación de procedimientos específicos dentro de instituciones como la PNC requiere un enfoque cuidadoso que considere tanto las políticas institucionales existentes como las necesidades operativas y legales, este proceso no solo asegura que los nuevos procedimientos se alineen con los objetivos y las estrategias institucionales, sino que también garantiza que se respeten las normativas y los estándares éticos que rigen las actividades policiales.

MARCO NORMATIVO Y POLÍTICO DE LA PNC

Misión y Visión Institucional

La misión y visión de la PNC son fundamentales para la definición de cualquier procedimiento dentro de la institución, la misión de la PN es garantizar *"las condiciones necesarias para el ejercicio de los derechos y libertades públicas, así como para la convivencia pacífica de todos los habitantes del territorio nacional".* Por su parte, la visión proyecta a la Policía como una organización moderna, eficaz y altamente profesional, reconocida por su contribución la mejora sobre; la seguridad y la justicia en el país.

Estas directrices estratégicas proporcionan un marco general para la creación de procedimientos, asegurando que estos contribuyan al cumplimiento de la misión institucional y estén orientados hacia la visión a largo plazo de la PN. Cualquier procedimiento nuevo debe, por lo tanto, ser evaluado en términos de su capacidad para mejorar la seguridad de la población, *proteger los derechos humanos* y mejorar la eficiencia y profesionalidad de la institución.

Normativas y Directrices Operativas

La PNC opera bajo un conjunto de normativas y directrices que guían sus actividades diarias, estas normativas incluyen leyes, decretos, resoluciones, manuales y otros documentos normativos que establecen cómo deben realizarse las actividades policiales: por tanto, para la creación de un nuevo procedimiento, es esencial revisar y comprender estos documentos normativos para garantizar que el nuevo procedimiento no entre en conflicto con las regulaciones existentes.

Ley 62 de 1993

La *"Ley 62 de 1993"* es una de las normativas más importantes que regulan la organización y el funcionamiento de la PN, esta ley establece las bases legales para la estructura, las funciones y las competencias de la Policía; cualquier procedimiento nuevo debe estar en consonancia con esta ley, asegurando que respete la jerarquía, las responsabilidades y los procesos establecidos en ella.

Código Nacional de Policía y Convivencia

El "*Código Nacional de Policía y Convivencia (Ley 1801 de 2016)"* es otro marco normativo crucial, este código establece las normas que rigen las acciones de la Policía en materia de convivencia y seguridad ciudadana; un nuevo procedimiento debe alinearse con las disposiciones de este código, especialmente en lo que refiere a la defensa de los derechos de los ciudadanos y la promoción de la convivencia pacífica.

Política de Ética y Transparencia

La política de ética y transparencia es una de las más importantes dentro de la Policía Nacional, esta política enfatiza la importancia de actuar con integridad, responsabilidad y transparencia en todas las acciones policiales.

Política de Innovación y Tecnología

La política de innovación y tecnología destaca la necesidad de modernizar y adaptar los procedimientos policiales a los avances tecnológicos y las mejores prácticas internacionales, cualquier nuevo procedimiento debe considerar el uso de tecnología avanzada y herramientas innovadoras para la mejora de la eficiencia y la eficacia de las actividades policiales.

Identificación de Parámetros Institucionales Clave

Alineación con la Misión y Visión

Uno de los parámetros institucionales más importantes es la alineación del nuevo procedimiento con la misión y visión de la PN, esto significa que el procedimiento debe estar diseñado para contribuir a la seguridad y convivencia pacífica en Colombia, y para fortalecer la profesionalidad y eficacia de la institución, es crucial que el procedimiento sea evaluado en términos de su capacidad para apoyar estos objetivos estratégicos.

Proceso de Creación del Procedimiento

- **Análisis preliminar**

El primer paso en la creación del procedimiento es realizar un análisis preliminar que identifique las necesidades operativas y las brechas en los procedimientos existentes, este análisis debe involucrar la revisión de la normativa vigente, las políticas institucionales y las mejores prácticas internacionales, además, debe incluir consultas con el personal policial y otros actores relevantes para identificar las áreas clave que el procedimiento debe abordar.

- **Diseño del procedimiento**

Una vez que se ha realizado el análisis preliminar, se procede al diseño del procedimiento, este diseño debe ser detallado y específico, incluyendo todos los pasos necesarios para su implementación, es importante que el diseño del procedimiento sea claro y comprensible, con directrices específicas sobre cómo llevar a cabo cada una de las tareas involucradas.

Fase II: Propuesta estandarizada sobre los componentes de un procedimiento que aborde los desafíos específicos relacionados con la recopilación, preservación y análisis de evidencia en casos de incidentes de seguridad en dIoT en el contexto colombiano

El crecimiento exponencial del IoT ha transformado diferentes sectores en Colombia, desde el hogar inteligente hasta la industria y la infraestructura crítica. Sin embargo, este avance tecnológico también ha generado desafíos nuevos en materia de seguridad y cibercrimen. La correcta compilación, almacenamiento y análisis de evidencia digital es esencial para investigar y resolver incidentes de seguridad relacionados con dIoT,

Este procedimiento proporciona una guía detallada para la adquisición de diferentes tipos de datos en el contexto de incidentes de seguridad en dIoT en Colombia. Los tipos de datos cubiertos incluyen: ADP, ADV, APR, ADS. Cada sección describe los pasos necesarios para garantizar la integridad y validez de la evidencia digital, siguiendo las mejores prácticas internacionales y las normativas legales aplicables en Colombia.

Objetivos de la propuesta estandarizada

- Estandarizar el proceso de recolección de evidencia digital en incidentes de seguridad relacionados con dIoT.
- Garantizar la integridad y autenticidad de la evidencia mediante métodos y herramientas apropiados.
- Cumplir con las normativas legales y estándares internacionales, asegurando que la evidencia sea admisible en procedimientos judiciales en Colombia.
- Facilitar el análisis efectivo de la evidencia para identificar la causa raíz del incidente y apoyar en la mitigación y prevención de futuros eventos similares.

Consideraciones Generales de la propuesta estandarizada

Antes de iniciar cualquier proceso de adquisición de datos, se deben tener en cuenta las siguientes consideraciones:

- **Autorización Legal**: Asegurarse de contar con las autorizaciones legales necesarias, como órdenes judiciales o consentimientos, según corresponda y conforme a la legislación colombiana vigente, incluyendo la *"Ley 1273 de 2009 sobre delitos informáticos y la protección de datos personales bajo la Ley 1581 de 2012".*
- **Preservación de la Evidencia**: Garantizar que la evidencia digital se recopile y almacene de manera que se conserve su integridad, evitando cualquier alteración o contaminación de los datos.
- **Documentación Detallada**: Compilar el paso a paso del proceso de adquisición, incluida: "*la fecha, la hora, la ubicación, el personal involucrado, herramientas utilizadas"* y cualquier observación relevante. Esto es esencial para mantener una cadena de custodia sólida.
- **Selección de Herramientas Adecuadas**: Utilizar herramientas forenses reconocidas y validadas que sean adecuadas para el tipo de datos y dispositivos involucrados.
- **Seguridad del Personal**: Asegurar que el personal que realiza la adquisición esté capacitado y tome las precauciones necesarias para protegerse y evitar daños a los dispositivos o pérdida de datos.
- **Minimizar la Alteración de los Sistemas**: Realizar las adquisiciones de manera que se reduzca al mínimo cualquier impacto en el funcionamiento normal de los dispositivos y sistemas involucrados.

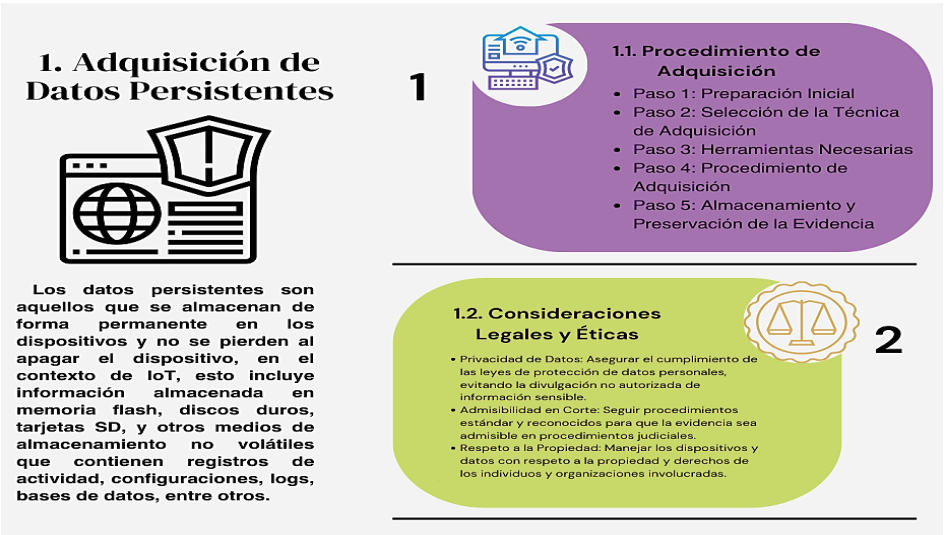

Figura 4. Adquisición de Datos Persistentes

Fuente: Propia

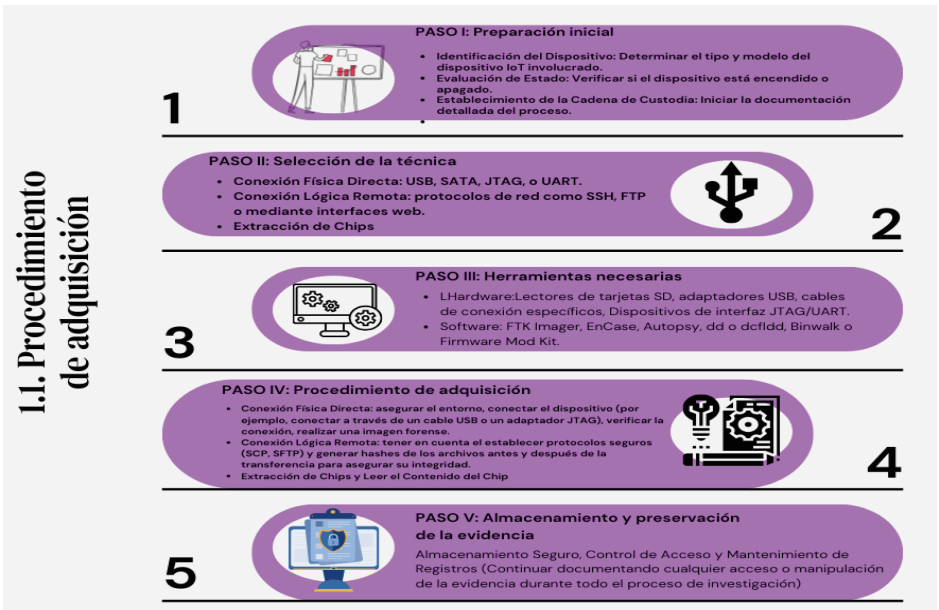

Figura 5. Pasos del Procedimiento de Adquisición

Fuente: Propia

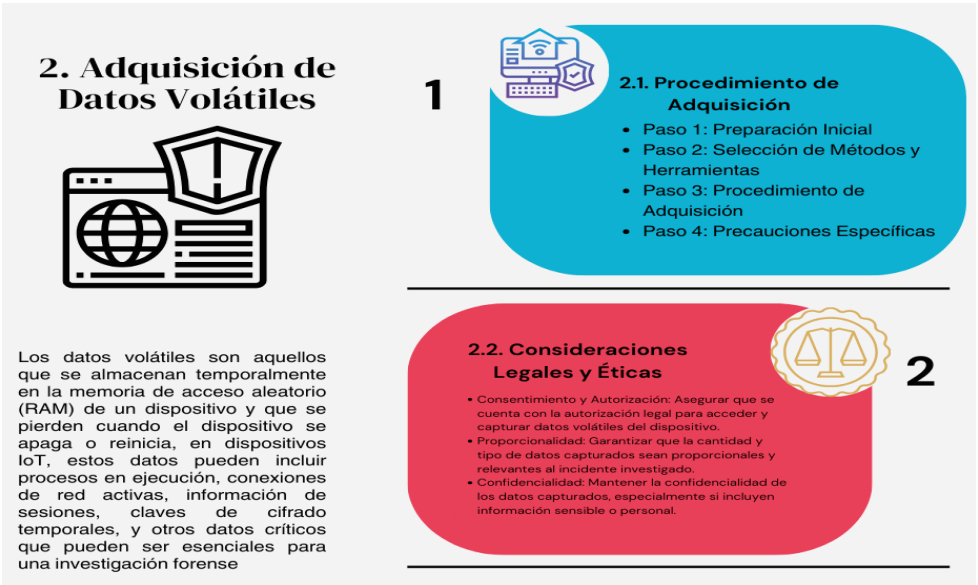

Figura 6. Adquisición de Datos Volátiles

Fuente: Propia

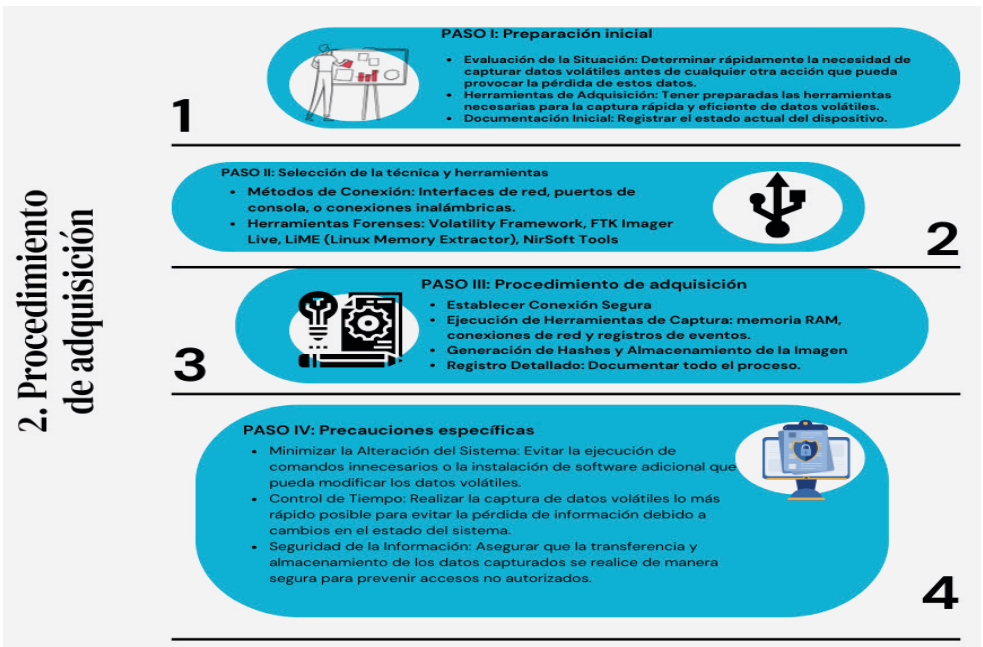

Figura 7. Pasos del Procedimiento de Adquisición

Fuente: Propia

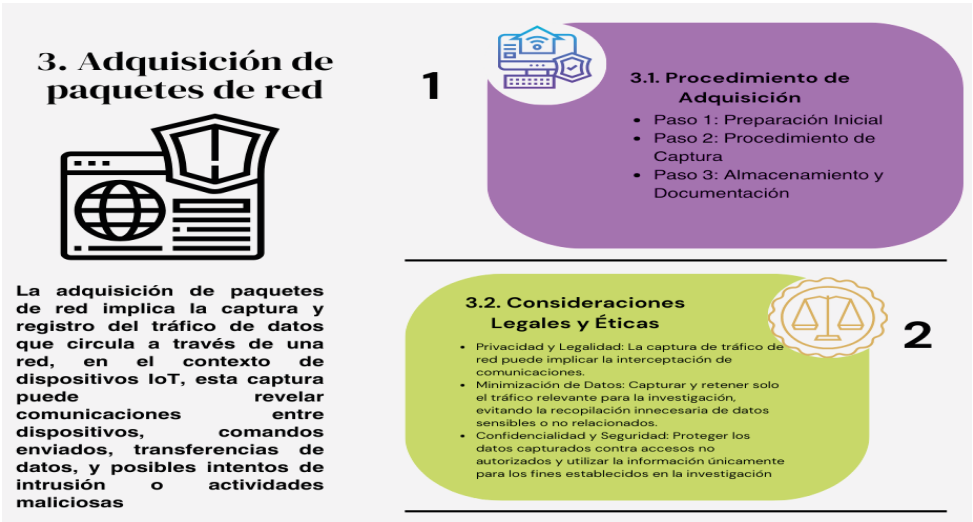

Figura 8. Adquisición de Paquetes de Red

Fuente: Propia

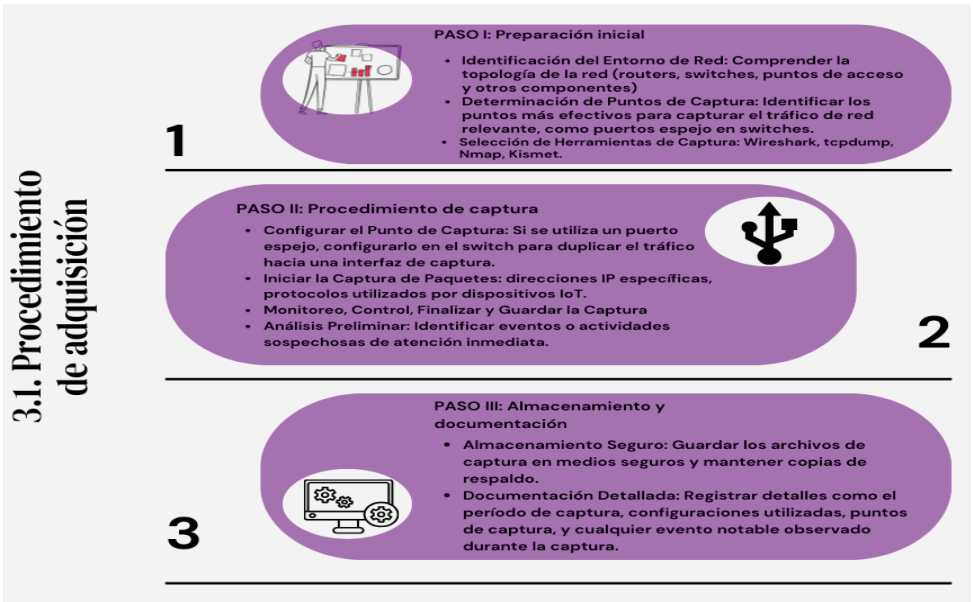

Figura 9. Pasos del Procedimiento de Adquisición

Fuente: Propia

Figura 10. Adquisición de Datos de Smartcards

Fuente: Propia

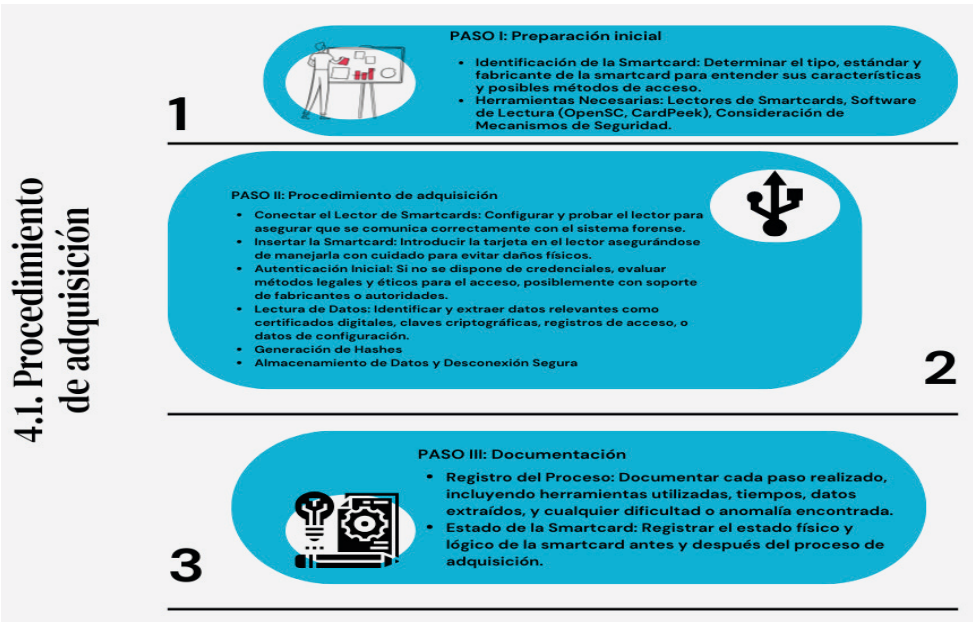

Figura 11. Pasos del Procedimiento de Adquisición

Fuente: Propia

DISCUSIONES

La inclusión del IoT en Colombia, ha sido un fenómeno creciente de los últimos años, el cual ha influido sobre la necesidad de actualizar diversos sectores, donde los dispositivos son comúnmente utilizados para la gestión, monitoreo y control de procedimientos. El análisis llevado a cabo discute la relación de los dispositivos de IoT en los procedimientos forenses, los cuales se han tenido en cuenta para la creación de la propuesta estandarizada, validada a partir de la herramienta de jueceo de expertos.

Las investigaciones indican que estos dispositivos permiten la activación de forma remota de sistemas de alarmas, posibilitando la transmisión de datos importantes asociados a los eventos de seguridad, tales como; intentos de intrusión o actividades sospechosas en tiempo real (Zona-Ortiz et al., 2020; Sharma et al., 2019). Los datos que brindan los dispositivos de IoT, incluyen información respecto a la ubicación, hora y eventos relacionados con la seguridad, los cuales son claves para la recopilación de evidencia digital durante investigaciones forenses. Es relevante indicar que el resguardo de los datos, así como la cadena de custodia, son aspectos *"claves que deben ser considerados en el proceso para garantizar la validez de la información"* (Aldana y Buitrago, 2023; Alonso, 2022; Ramírez, 2019)

Amador et al., (2018) sugiere que la aplicación de dIoT, presenta desafíos asociados con la privacidad de la información, así como la protección de la información compilada, lo que evidencia el requerimiento de que se instauren normativas o marcos regulatorios que indiquen objetivos claros de su uso y aplicación durante las investigaciones forenses (Amador Arévalo et al., 2018). En particular, el monitoreo de los datos generados y los dispositivos sensores son de apoyo a las autoridades en el proceso de investigación de evasión fiscal, delitos y fraudes financieros, debido a que dan paso a la verificación de patrones de comportamiento inusual (Parra-Sánchez et al., 2021)

Las investigaciones empíricas indican que uno de los principales desafíos asociados a la aplicación de IoT se debe a la falta de interoperabilidad entre los dispositivos. Donde la estandarización de un proceso forense es indispensable para la gestión de datos compatibles entre diversos sistemas y el salvaguardo de la información obtenida. Por lo que se dispone la necesidad de crear propuestas o protocolos estandarizados con normatividades que promuevan la compilación y análisis de datos IoT para el mejoramiento de la eficacia de las investigaciones forenses (Yacchirema, 2019; Estupiñan & Mora, 2019; Villegas, 2019). Así mismo, la seguridad que presenten los dIoT es uno de los desafíos que debe tenerse en cuenta, donde las investigaciones proponen el uso de *"tecnologías como blockchain, para el aseguramiento de la integridad de la información"* en el entorno generado por dIoT (Chen et al., 2014; Christidis y Devetsikiotis, 2016). La aplicación del blockchain puede ser indispensable para que los datos obtenidos no puedan ser manipulados o alterados antes de ser usados como evidencia en un proceso de investigación forense (Díaz et al., 2019). Las investigaciones infieren que es indispensable contar con una infraestructura tecnológica óptima para la integración de los datos compilados a partir de dIoT en un sistema centralizado, donde pueda ser analizado y procesado de forma efectiva (Sarabia, 2020; Medina-Barahona et al., 2022)

CONCLUSIONES

Para los investigadores de la PNC, es crucial desarrollar procedimientos forenses especializados que aborden las particularidades de cada tipo de dispositivo IoT, esto incluye la necesidad de herramientas y técnicas avanzadas para la compilación y análisis de información, así como una comprensión profunda de los contextos en los que operan estos dispositivos. La creciente adopción de IoT en Colombia ofrece muchas oportunidades para la mejora de la eficiencia y la efectividad de las investigaciones forenses, sin embargo, también plantea desafíos significativos en términos de seguridad, privacidad y manejo de grandes volúmenes de datos. A través de un enfoque metodológico riguroso y adaptado a las particularidades del IoT, los investigadores pueden maximizar el valor de la información extraída de estos dispositivos y contribuir de manera significativa a la resolución de casos y el mejoramiento en lo que respecta a la seguridad pública.

La creación de un procedimiento dentro de la PNC, es un proceso complejo que requiere la consideración cuidadosa de una variedad de parámetros institucionales. Estos incluyen la alineación con la misión y visión de la institución, la conformidad con las normativas legales, la compatibilidad con las políticas institucionales, la factibilidad operativa, la participación interinstitucional, y la mejora continua. Al seguir estos parámetros, se puede garantizar que el procedimiento no solo sea efectivo en la práctica, sino que también esté en plena consonancia con los objetivos y valores de la PNC.

Este enfoque estructurado no solo facilita la creación de procedimientos alineados con las políticas institucionales, sino que también contribuye a la profesionalización y modernización de la PN, asegurando que la institución esté preparada para enfrentar los desafíos actuales y futuros en materia de seguridad y convivencia.

La correcta adquisición de datos persistentes, volátiles, paquetes de red y datos de smartcards es fundamental en la investigación de sucesos de seguridad asociados con dIoT en Colombia, siguiendo los procedimientos detallados anteriormente, se puede asegurar que la evidencia digital se recopile y preserve de forma que sea admisible y útil en procesos judiciales, al tiempo que se respetan las consideraciones legales y éticas pertinentes.

Es esencial que el personal encargado de estas tareas esté debidamente capacitado y actualizado en las mejores prácticas y herramientas forenses, además de estar consciente de las normativas legales aplicables, la documentación y *mantenimiento de una cadena de custodia* sólida son pilares fundamentales para la seguridad y calidad de la evidencia.

La adaptación y cumplimiento de estos procedimientos contribuirán significativamente a la eficacia de las investigaciones forenses en el ámbito del IoT, apoyando la labor de las autoridades en la prevención, detección y resolución de delitos cibernéticos en el contexto colombiano.

REFERENCIAS

Abellán, M. G. (2021). Sistema Bibliotecario de la Suprema Corte de Justicia de la Nación Catalogación. *Ideas para un" control de fiabilidad" de las pruebas forenses. Un punto d e partida para seguir discutiendo, 51*.

Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *Journal of King Saud University-Computer and Information Sciences, 34*(10), 10217-10245. https://doi.org/10.1016/j.jksuci.2022.10.018

Aceros, D. F. (2020). Prototipo de una ruta tecnológica para el IOT, enfocada en las tecnologías de riego, para los agricultores de pequeña escala en Colombia. *Universidad Autonoma de Bucaramanga*.

Ahmad, T., & Zhang, D. (2021). Using the internet of things in smart energy systems and networks. *Sustainable Cities and Society, 68*. https://doi.org/10.1016/j.scs.2021.102783

Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT forensics: current perspectives and future directions. *Sensors, 24*(16), 5210. https://doi.org/10.3390/s24165210

Aldana, L. A., & Buitrago, J. G. (2023). mplementación de modelo de prototipo para el desarrollo de un sistema de alarma comunitaria IoT controlada desde dispositivos móviles: Prototype model implementation for the development of a IoT community alarm system controlled from mobile devices. *Tecnología Investigación y Academia, 11*(2), 156-169.

Alonso, Y. (2022). Desarrollo de un prototipo de telegestión IoT para los tomacorrientes en instalaciones eléctricas de Baja Tensión en Colombia. *Universidad Nacional Abierta y a Distancia*.

Amador Arévalo, D. A., Aya-Parra, P. A., Sarmiento Rojas, J., Quiroga-Torres, D. A., Muñoz Bernal, D. A., & Cruz, A. M. (2018). Diseño e implementación de un sistema para el seguimiento de los fallos en dispositivos médicos utilizando Internet de las cosas. *Universidad del Rosario*.

Arias, M. M., & Martínez, M. L. (2022). Herramientas de lectura crítica. Un ejemplo práctico. *Medicina paliativa*, 128-132.

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks, 192*. https://doi.org/10.1016/j.comnet.2021.108040

Balanta, G. A., Cabezas, J. L., Gómez, M. Á., & Aguja, F. A. (2021). Google Cardboard 3D-VR: Dispositivo de realidad virtual para el aprendizaje inmersivo en el entrenamiento policial. *Perspectivas*, 211-226. https://doi.org/10.26620/uniminuto.perspectivas.6.21.2021.211-226

Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. *Wireless Personal Communications, 115*(2), 1667-1693. https://doi.org/10.1007/s11277-020-07649-9

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile networks and applications, 19*, 171-209. https://doi.org/10.1007/s11036-013-0489-0

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE access, 4*, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Ciapponi, A. (2021). La declaración PRISMA 2020: una guía actualizada para reportar revisiones sistemáticas. *Evidencia, actualizacion en la práctica ambulatoria, 24*(3). https://doi.org/10.51987/evidencia.v24i4.6960

Díaz, D. O., Gómez, F., Rodriguez, A., & Mesa, P. (2019). BSIEM-IoT: A blockchain-based and distributed SIEM for the Internet of Things. *Universidad del Rosario*. https://doi.org/10.1007/978-3-030-29729-9_6

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580. https://doi.org/10.3390/app11104580

Estupiñan, T. V., & Mora, K. T. (2019). Gestión de evidencia digital en escenarios convencionales e IoT. *Escuela Colombiana Julio Garavito*.

Farfan Chiun, J. E. (2024). ISO 27037: 2012 para mejorar el análisis informático forense en la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, Lima 2022. *Universidad Nacional Federico Villareal*, 1-104.

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introducción al IOT. *Revista Internacional de Investigación Avanzada en Ciencia, Ingeniería y Tecnología* , 41-44.

Gómez Mendoza, E. J. (2024). Ciberseguridad del internet de las cosas (IoT) en el sector doméstico y su estado actual en Colombia. *Universidad Nacional Abierta y a distancia*.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Kumar, M., & Kumar, S. (2022). Communication technologies for m2m and iot domain. *In Internet of Things*, 132-160. https://doi.org/10.1201/9781003122357-10

Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information, 12*(2), 87. https://doi.org/10.3390/info12020087

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, 3*(5), 164-173. https://doi.org/10.4236/jcc.2015.35021

Matarrese, J. E. (2020). Exploración de la confluencia entre agroinformática, IoT, grandes datos y extracción del conocimiento . *Universidad Nacional de La Plata*.

Medina-Barahona, C. J., Mora, G. A., Calvache-Pabón, C., Salazar-Castro, J. A., Mora-Paz, H. A., & Mayorca. (2022). Propuesta de arquitectura IOT orientada a la creación de prototipos para su aplicación en plataformas educativas y de investigación. *Revista Colombiana de Tecnologías de Avanzada (RCTA), 1*(39), 118-125. https://doi.org/10.24054/rcta.v1i39.1405

Ministerio de Tecnologia e Informacion. (2016). *Informe sobre la adopcion de IoT en Colombia. MinTIC*. https://www.mintic.gov.co/portal/715/articles-152219_doc_pdf.pdf

Montasari, R., Hill, R., Montaseri, F., Jahankhani, H., & Hosseinian-Far, A. (2020). Internet of things devices: digital forensic process and data reduction. *International Journal of Electronic Security and Digital Forensics, 12*(4), 424-436. https://doi.org/10.1504/IJESDF.2020.110676

Mouha, R. A. (2021). Internet of things (IoT). *Journal of Data Analysis and Information Processing, 9*(2), 77. https://doi.org/10.4236/jdaip.2021.92006

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & Alonso-Fernández, S. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista española de cardiología, 74*(9), 790-799. https://doi.org/10.1016/j.recesp.2021.06.016

Parra de Gallo, H. B. (2022). Propuesta de una guía de actuación forense para entornos de internet de las cosas (IoT). *Computación y Sistemas, 26*(1), 441-460. https://doi.org/10.13053/cys-26-1-3898

Parra-Sánchez, D. T., Talero-Sarmiento, L. H., & Guerrero, C. D. (2021). Assessment of ICT policies for digital transformation in Colombia: technology readiness for IoT adoption in SMEs in the trading sector. *Digital Policy, Regulation and Governance, 23*(4), 412-431. https://doi.org/10.1108/dprg-09-2020-0120

Pasdar, A., Koroniotis, N., Keshk, M., Moustafa, N., & Tari, Z. (2024). Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems. *IEEE Transactions on Sustainable Computing*, 1-20. https://doi.org/10.1109/TSUSC.2024.3443256

Pérez, L. C. (2022). Inteligencia artificial y Big data en ciudades inteligentes. *Universidad de Bogota Jorge Tadeo Lozano*.

Ponis, S. T., & Efthymiou, O. K. (2020). Cloud and IoT applications in material handling automation and intralogistics. *Logistics, 4*(3), 22. https://doi.org/10.3390/logistics4030022

Qureshi, J. N., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., & Zikria, Y. B. (2022). Blockchain applications for the Internet of Things: Systematic review and challenges. *Microprocessors and Microsystems, 94*, 94. https://doi.org/10.1016/j.micpro.2022.104632

Ramírez, M. A. (2019). Metodología integral de protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las historias clínicas en Colombia. *Institución Universitaria Reacreditada de Alta Calidad*.

Rani, D., & Gill, N. S. (2020). Internet of Things (IoT) Characteristics, Applications, and Digital Forensics Investigation Process: A Review. *International Journal, 8*(9). https://doi.org/10.30534/ijeter/2020/254892020

Rashid, M., Haque, M. M., & Wang, W. (2024). IoT Complexity: Security, Vulnerabilities and Risks. *European Journal of Electrical Engineering and Computer Science, 8*(1), 1-9. https://doi.org/10.24018/ejece.2024.8.1.597

Rodríguez, I. R., Rodríguez, J. V., & Valera, M. C. (2023). El internet de las cosas médicas (IoMT): una revolución tecnológica aplicable a la gestión de la diabetes mellitus tipo 1. El internet de las cosas médicas (IoMT): una revolución tecnológica aplicable a la gestión de la diabetes mellitus tipo 1. *Universidad de Malaga*.

Sahu, K. S., Oetomo, A., & Morita, P. P. (2020). Enabling remote patient monitoring through the use of smart thermostat data in canada: exploratory study. *JMIR mHealth and uHealth, 8*(11). https://doi.org/10.2196/21016

Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing, 76*, 5320-5363. https://doi.org/10.1007/s11227-019-02945-z

Sarabia, D. F. (2020). Arquitectura de análisis de datos generados por el internet de las cosas IoT en tiempo real. *Universitat Politècnica de València*.

Sarker, I. H. (2021). Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. *SN Computer Science, 2*(5), 377. https://doi.org/10.1007/s42979-021-00765-8

Saucedo, C. Y., & Regalado, G. R. (2024). Monitoreo ambiental de las microcuencas Colpamayo y San Mateo utilizando estaciones meteorológicas e hidrológicas automáticas con tecnología GSM/GPRS, chota. *Universidad Nacional Autonoma de Chota*.

Serrano, S. S., Navarro, I. P., & González, M. D. (2022). ¿ Cómo hacer una revisión sistemática siguiendo el protocolo PRISMA?: Usos y estrategias fundamentales para su aplicación en el ámbito educativo a través de un caso práctico. *Bordón: Revista de pedagogía*, 51-66.

Sharma, B., Obaidat, M. S., Singh, K., & Bajaj, K. (2019). A Comparative Study on Frameworks, MAC Layer Protocols and Open Research Issues in Internet of Things. *Adhoc & Sensor Wireless Networks, 45*, 275-291. https://doi.org/10.5120/12029-7995

Sharma, B., Obaidat, M. S., Singh, K., & Bajaj. (2019). A Comparative Study on Frameworks, MAC Layer Protocols and Open Research Issues in Internet of Things. *Adhoc & Sensor Wireless Networks, 45*.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191-1221. https://doi.org/10.1109/COMST.2019.2962586

Tran-Dang, H., Krommenacker, N., Charpentier, P., & Kim, D. S. (2020). Toward the internet of things for physical internet: Perspectives and challenges. *IEEE internet of things journal, 7*(6), 4711-4736. https://doi.org/10.1109/JIOT.2020.2971736

Vaghela, R., Gowda, V. D., Taj, M., Arudra, A., & Chopra, M. (2024). Digital Evidence Collection and Preservation in Computer Network Forensics. I. *n Handbook of Research on Innovative Approaches to Information Technology in Library and Information Science* , 42-62. https://doi.org/10.4018/979-8-3693-0807-3.ch003

Verma, P. K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., & Abogharaf, A. (2016). Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications, 66*, 83-105. https://doi.org/10.1016/j.jnca.2016.02.016

Villegas, J. E. (2019). Desarrollo de un sistema IoT para la mejora de la seguridad ciudadana en una Smart City en el Perú. *Consejo Nacional de Ciencia, tecnología e Innovación tecnológica*.

Yacchirema, D. C. (2019). Arquitectura de Interoperabilidad de dispositivos físicos para el Internet de las Cosas (IoT). *Universitat Politècnica de València*.

Zona-Ortiz, A. T., Fajardo-Toro, C. H., & Pirachicán, C. M. (2020). Propuesta de un marco general para el despliegue de ciudades inteligentes apoyado en el desarrollo de Iot en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*(E28), 894-907.