v. 5, n. 4, 2025

Scientific Journal of Applied Social and Clinical Science

IOT FORENSIC PROCEDURE FOR FORENSIC LABORATORIES OF THE COLOMBIAN NATIONAL POLICE

Diego Mauricio Negro Lozano
School of Information and Communication Technologies Tc. Jorge Luis Mauledoux
ORCID: 0009-0008-7738-6649

Sandra Milena Guzmán Bejarano
School of Information and Communication Technologies Tc. Jorge Luis Mauledoux
ORCID: 0009-004-3262-5141

Jorge Hernando Ruíz Otálora
Researcher in Science, Technology and Innovation
ORCID: 0000-0003-2214-3558

Acceptance date: 26/02/2025

Abstract: Research on IoT forensic procedures contributes to the development of cybersecurity practices globally. This descriptive--propositional study, focused on the creation of a forensic procedure for IoT aimed at forensic investigators of the National Police of Colombia, was divided into 2 research phases, Phase I related to the analysis of scientific evidence found in databases using the PRISMA method and Phase II concerning 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, among which are: alignment with the mission and vision of 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 also fully in line with the objectives and values of the Colombian National Police. It is important to note that the proper acquisition of persistent, volatile, network packet and smartcard data is critical in the investigation of adverse security events associated with dIoT in Colombia, following the procedures detailed above can ensure that digital evidence is collected and preserved in a manner that is admissible and useful in legal proceedings, while respecting relevant legal and ethical considerations.
Keywords: Forensic laboratory, Internet of things, cybersecurity, digital evidence.

INTRODUCTION

The *"internet of things (IoT)"* is based on the interconnection of physical devices through the internet, allowing them to collect and manage data, these devices can cover a "*wide range of everyday objects*", from household appliances, vehicles to health devices and industrial equipment. The central idea is to establish a connection between these smart objects enabling communication and with central systems to collect, process and act on the data generated (Madakam et al., 2015; Tran-Dang et al., 2020) .

Among the fundamental characteristics of the IoT is Connectivity, since "*IoT (dIoT) devices"* are made up of actuators, sensors and technological connectivity systems (such as *Wi-Fi, Bluetooth, Zigbee,* etc.) to facilitate communication (Mouha, 2021; Lombardi et al., 2021) . Sensors are in charge of compiling information from the environment, such as: humidity, temperature, location, etc. While actuators are responsible for devices to perform physical actions in response to the collected information (Qureshi et al., 2022) . As opposed to *"Machine-to-Machine Communication (M2M)"*, dIoTs relate directly to each other, without human intervention, allowing process automation. As for the Cloud, data that are compiled by devices are often transmitted to the cloud for centralized storage, processing and analysis (Verma et al., 2016; Kumar and Kumar, 2022; Ponis and Efthymiou, 2020)

However, the analysis of information in real time or later allows obtaining valuable information for decision making. Devices can perform actions automatically based on the information received, improving efficiency and response to changes in the environment (Matarrese, 2020; Sarker, 2021) . Examples of IoT applications include; connected health systems, smart thermostats, industrial monitoring systems, autonomous vehicles, smart cities and more. As the IoT continues

to evolve, additional developments are expected for improved efficiency, connectivity and security of interconnected devices (Sharma et al., 2019; Sahu et al., 2020). IoT is used in different sectors such as: healthcare, agriculture, industry, smart home, connected vehicles, logistics, among others, security in IoT is crucial to protect the integrity as well as confidentiality of information, to prevent attacks on users' privacy (Gubbi et al., 2013; Chanal and Kakkasageri, 2020) .

Forensic processes in the *"Internet of Things (IoT)"* refers to the application of digital forensic techniques and procedures to investigate dIoT-related incidents; given that dIoTs are connected to the internet network and collect a large amount of data, it is crucial to carry out proper forensic procedures to collect, preserve and analyze evidence in a way that is acceptable in a court of law (Stoyanova et al., 2020; Rani and Gill, 2020) . Accordingly, research presents itself as a critical need in the current context, where networked dIoT has generated a new dimension of challenges concerning security and privacy. IoT, by integrating physical devices with communication capabilities, has significantly expanded the attack surface, creating an enabling scenario for cyber incidents and malicious activities (Djenna et al., 2021; Pasdar et al.,2024) . Similarly, the number of dIoT in homes, businesses and critical infrastructures, which have evidenced exponential growth, this proliferation intensifies the complexity of cybersecurity, making it essential to develop specific forensic procedures to address the unique challenges present in this environment (Ahmad and Zhang, 2021) . On the other hand, threats specifically targeting dIoT, such as: "*denial of service attacks*", data manipulation and remote takeover, require specialized forensic approaches. Investigating and understanding these threats will enable the development of more effective response and prevention strategies (Salim et al., 2020; Parra de Gallo, 2022).

Thus, the information collected by dIoTs often includes sensitive and private data. Security incidents can expose consumer privacy and erode confidence in the widespread adoption of these technologies (Rashid et al., 2024; Babun et al., 2021) . Forensics can help mitigate these risks and strengthen confidence in IoT adoption. Similarly, the diversity of dIoT, its architectures and communication procedures pose significant challenges in the collection and preservation of forensic evidence, investigating specific methods and procedures to handle this complexity will ensure the integrity and admissibility of evidence in a legal environment (Abiodun et al., 2022; Vaghela et al., 2024) . As the use of IoT becomes an integral part of society, the lack of specific forensic regulations and standards for this area creates a gap that must be addressed (Parra-Sánchez et al., 2021)

Accordingly, there is currently no forensic procedure in IoT that contributes to the investigative processes contributing to the administration of justice in Colombia, is therefore posed as a question: What parameters should be taken into account in a forensic procedure for IoT aimed at investigators *of the National Police of Colombia (PNC)*?

Research in IoT forensic procedures will contribute to the development of cybersecurity practices globally, as collaboration and exchange of knowledge in this area are essential for building a secure and resilient infrastructure in the IoT landscape. The present descriptive-propositional study is made up of 2 research phases, Phase I related to the analysis of the scientific evidence found in databases through the PRISMA method and Phase II regarding the standardized proposal, which fulfilled the main focus of the research on creating a forensic procedure for IoT aimed at PNC investigators, to strengthen the expert analysis. Likewise, the particularities of the most common dIoT used in Colombia were

analyzed, considering their diversity and the frequency of their adoption, in order to identify those objects on which relevant information is extracted in forensic processes, the identification of the institutional parameters for the creation of a procedure in the *National Police (PN),* The definition of the components of a procedure that addresses the specific challenges related to the collection, preservation and analysis of evidence in cases of dIoT security incidents in the Colombian context, in order to ensure an adequate analysis process.

MATERIALS AND METHODS

TYPE OF STUDY

The present research was based on the theories and studies presented by Parra, (2022) and Balanta et al., (2021). The qualitative, descriptive and propositional approach is suitable for this research, as it allows to explore and understand in depth the forensic procedures in IoT from the perspective of PNC investigators, this approach focuses on non-numerical data collection and analysis of complex phenomena, providing a detailed view on the approach analyzed (Balanta et al., 2021; Parra de Gallo, 2022).

METHODOLOGY

PHASE I: ANALYSIS OF SCIENTIFIC EVIDENCE

Using the *"Preferred Reporting Items for Systematic Reviews and Meta-Analyses, PRISMA"* method, detailed data on IoT forensic procedures are collected, which required the establishment of a search equation:

- (Internet of things) AND (forensic laboratory) AND (police) AND (forensic)

Data analysis is presented according to the distribution of information over time and geographic distribution, using Scopus, Science Direct and *Google academic* search engine databases. Relevant data were analyzed, identified in patterns, categories and key concepts that emerge from the information collected.

The inclusion precepts applied include the following:

- Empirical and retrospective documents are included in this research.
- Descriptive documents are included but based on the proposal of a forensic procedure for IoT aimed at PNC investigators, to strengthen the expert analysis or related topics that serve as a basis for the investigation.
- Papers published in the last 7 years of scientific research are included.
- Free access documents are included.
- The exclusion precepts include:
- Standard or theoretical documents are excluded.
- Papers focused on the use of IoT in other research areas.
- Paid access documents
- Documents with more than 7 years of scientific research.

PHASE II: DEVELOPMENT AND VALIDATION OF A STANDARDIZED PROPOSAL

Information processing

The documents selected for documentary analysis were carried out through preliminary reading and analysis to obtain a general understanding of the content and identify recurring themes and patterns. This was followed by the application of open coding of the information to identify emerging categories and subcategories. This process involved breaking down the data into meaningful units and labeling them with descriptive codes. The third processing step involved axial coding, where

the categories and subcategories identified in the *open coding* were related, establishing connections between them to form a coherent scheme of IoT forensic procedures. The fourth step considered the application of selective coding, which integrates and redefines the categories and subcategories, selecting those that are most relevant and representative for the study. Emerging models and theories describing IoT forensic procedures are constructed. Finally, the interpretation of results and their presentation were organized in an understandable and accessible format, using diagrams that explain IoT forensic procedures and highlight the practical and theoretical scope of the findings.

Validation of the documentary information and of the tool through expert judgement

The expert judgment tool (Abellán, 2021) was evaluated by the following experts:

1. PhD. Msc. Information Systems. Jonh Roberth Correa.
2. Msc. Information Security. Jhon Felix Rivera Gutierrez
3. Msc. Technology and Informatics. Fabian Giovanni Gonzalez Robayo.
4. Msc. ICT Security. Jhon Alberto Talero Patarroyo.

On the usefulness and analysis of areas of knowledge applied in the tool, which has 4 specific aspects of relevance and analysis:

- *Persistent Data Acquisition (PDA)*
- *Volatile Data Acquisition (VDA)*
- *Acquisition of Network Packages (APR)*
- *Smartcard Data Acquisition (ADS)*

RESULTS

PHASE I: ANALYSIS OF THE LINE OF RESEARCH

The meta-analysis reports an increase in the line of research from 2021 to 2024, with 2023 being the year that reports the majority of scientific records in the Scopus database (Figure 1).

Figure 2 shows that the countries with the greatest interest in the scientific production of IoT application are China, India and the United States, with records of 1957, 1316 and 1000, respectively.

Summary of the PRISMA Method

The present phase of information gathering used for the creation of a forensic procedure for IoT aimed at PNC investigators, for the strengthening of expert analysis, compiled a total of 170 documents of which 62 scientific documents that were available in duplicate or by critical reading were eliminated, of which 108 were subjected to a screening phase, for the selection of 42 documents that were assessed by choice criteria. A total of 15 papers were included in the present research, of which 2 papers were outside the range of scientific production (2018-2024), but were included by criteria of research approach as it provides relevant information for the study.

Analysis of the particularities of the most common dIoTs in Colombia

The Internet of Things (IoT) has gained a prominent place in everyday life and in the industrial area of Colombia, the growing use of dIoT in sectors such as health, agriculture, urban management and security has generated a growing need for specialized forensic procedures to extract relevant information from these devices in the context of criminal investigations (Ahmed et al., 2024; Montasari et al., 2020) . This section proposes to analyze

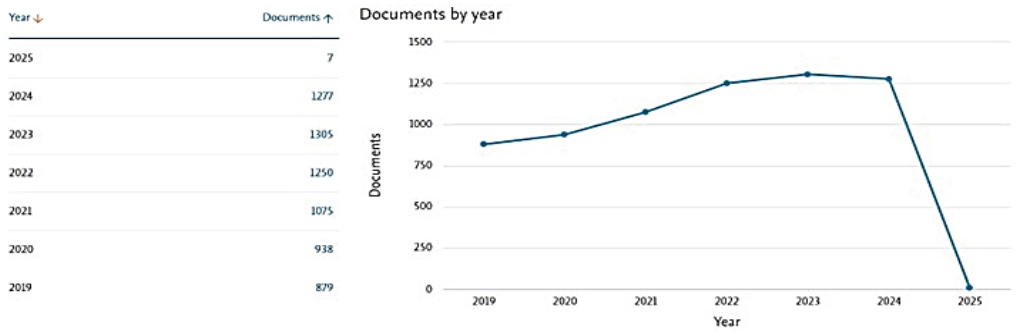

Figure .1 Distribution by years of scientific research of the IoT line.
Source: Meta-analysis taken from Scopus.

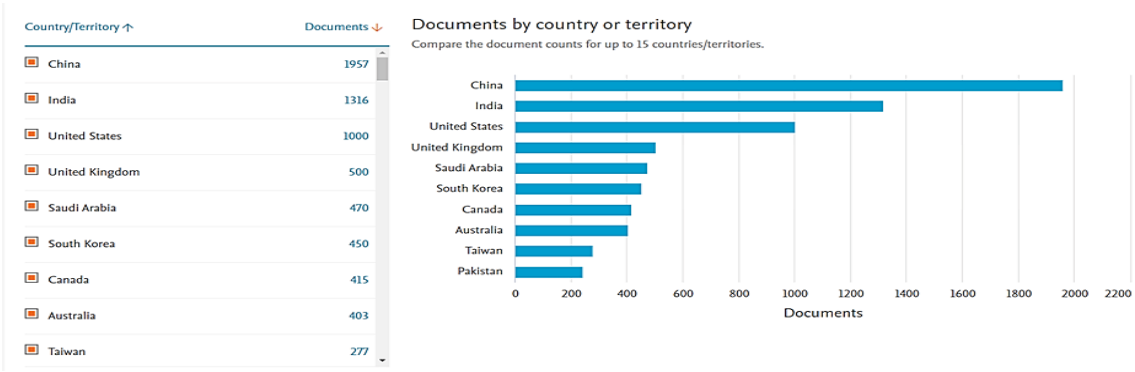

Figure .2 Geographical distribution of the scientific production of the IoT research line.
Source: Meta-analysis taken from Scopus.

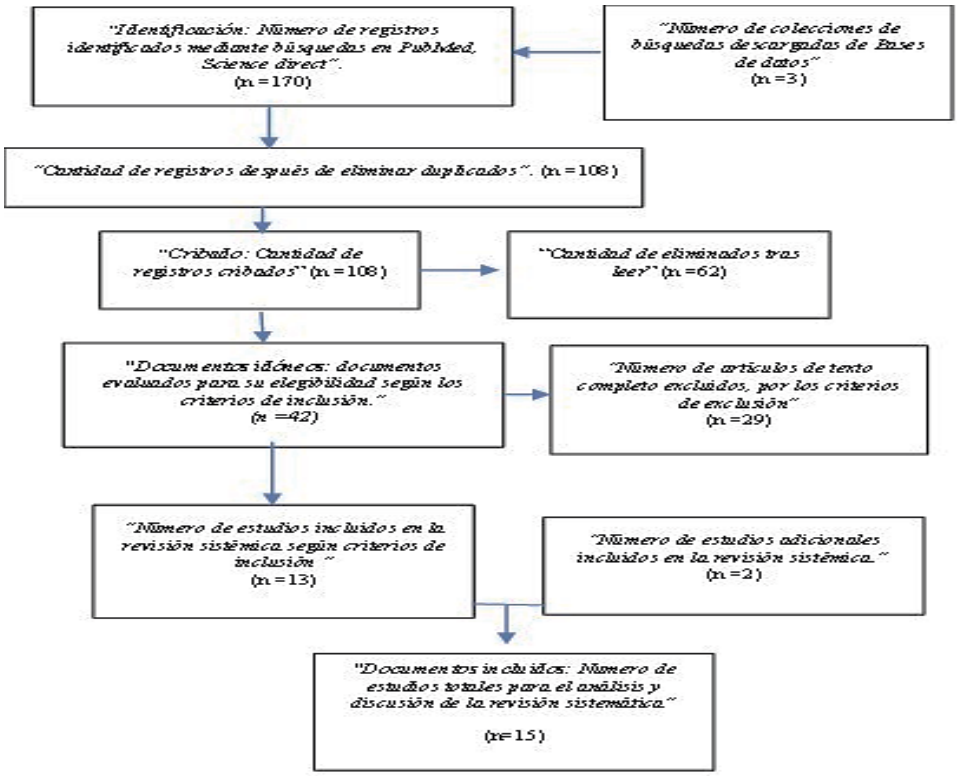

Figure .3 Diagram of inclusion using the PRISMA Declaration model.
Source: model taken from (Page et al., 2021; Ciapponi, 2021).

the particularities of the most common dIoTs used in Colombia, considering their diversity and frequency of adoption, to identify those objects on which relevant information is extracted in forensic processes (Balanta et al., 2021; Farfan Chiun, 2024) .

DIVERSITY AND FREQUENCY OF DIOT ADOPTION IN COLOMBIA

CATEGORIES OF DIOT

In Colombia, dIoT can be classified into several categories according to their application and use, these categories include, among others, smart home devices, health devices, environmental monitoring devices, smart agriculture devices, and urban infrastructure management devices. Smart home devices are increasingly common in Colombian homes, these devices include smart thermostats, security systems, surveillance cameras, smart lights, voice assistants such as Amazon Echo and Google Home, and connected home appliances, the adoption of these devices has grown due to their ability to improve comfort, energy efficiency and home security (Gómez Mendoza, 2024) .

In healthcare, dIoTs play a crucial role in patient monitoring and medical data management, among the most common devices are glucose monitors, physical activity wristbands, vital signs sensors, and connected medical equipment such as defibrillators and pacemakers, these devices allow continuous and real-time monitoring of patients' health, which improve the quality of medical care (Rodriguez et al., 2023) . Environmental monitoring devices are essential for *"natural resource management and environmental protection in Colombia";* air quality sensors, smart weather stations, and water monitoring devices are some examples, these devices collect crucial environmental data that help make decisions on resource management and environmental risk mitigation (Saucedo & Regalado, 2024) .

Agriculture in Colombia has adopted dIoT to improve productivity and sustainability, soil moisture sensors, automated irrigation systems, agricultural drones, and crop monitoring sensors are common tools that allow farmers to better manage resource use and improve crop yields (Aceros, 2020) . In Colombian cities, dIoTs are used to manage urban infrastructures and services efficiently, this includes "*traffic management systems*", smart public lighting, garbage sensors, and connected public transportation systems, these devices help improve the state of citizens' quality of life and optimize the management of urban resources (Perez, 2022) .

The frequency of dIoT adoption in Colombia varies by category and region, a study conducted by the *"Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)"* in 2016 revealed that smart home devices and health devices are the most adopted in urban areas, while smart agriculture devices are more common in rural areas. Environmental monitoring and urban infrastructure management devices are widely used in cities such as: Medellin, Bogota and Cali (Ministerio de Tecnologia e Informacion, 2016).

PARTICULARITIES OF THE DIOTS

Smart home devices present several particularities that make them relevant in the forensic context, these devices are designed to interact with each other and with the user through a home network and a central platform, such as a voice assistant or a mobile application, relevant information that can be extracted from these devices include activity logs, voice commands, video recordings and energy usage data. Extracting information from smart home devices presents unique challenges due to the diversity of manufacturers and *"lack of standardization in communication protocols"* and data storage, and security and privacy are important concerns as these devices store sensitive data about users' daily lives.

IoT health devices collect and transmit sensitive and critical medical data, these devices are often equipped with advanced sensors that measure a variety of health parameters, relevant information in the forensic context may include vital sign records, medical records and physical activity data. The main particularity of health devices is the requirement to provide assurance on aspects such as: the integrity and confidentiality of medical information, forensic investigators must comply with strict data protection regulations, such as *"Law 1581 of 2012 in Colombia",* which regulates the handling of personal data, interoperability and information security are critical aspects that must be addressed during forensic analysis.

IoT environmental monitoring devices collect data on environmental conditions such as air quality, temperature, humidity and pollution levels, these devices are crucial for environmental risk management and urban planning. The particularity of these devices lies in the large amount of data they generate and the need to contextualize this data in terms of location and time, forensic investigators must be able to correlate environmental data with specific events to provide conclusive evidence.

Smart farming devices are designed to optimize resource use and improve agricultural productivity; relevant information in the forensic context may include data on water use, fertilization, and crop conditions. The main particularity of these devices is the variability of the environments in which they operate and the need to adapt forensic procedures to different types of crops and farming practices, and connectivity in rural areas can be limited, posing additional challenges for data collection.

IoT urban infrastructure management devices are used to optimize the management of urban services such as traffic, street lighting and garbage collection, relevant information may include traffic data, energy usage patterns and maintenance records. The particularity of these devices is the need to manage large volumes of information in real time and to ensure the accuracy and reliability of the data collected, forensic investigators must be able to analyze and correlate this data to identify animals or patterns that are relevant to an investigation.

FORENSIC PROCEDURES FOR DIOT

Collecting dIoT information requires the use of specialized tools and techniques to access and extract data without having to compromise data integrity, which may include capturing network traffic, extracting data from memory, and accessing internal device databases.

Forensic dIoT data analysis involves pattern detection, event correlation and activity reconstruction, investigators must be able to interpret the data in the context of the device and its specific application.

The presentation of results in an IoT forensic investigation must be clear and understandable, providing a coherent narrative that explains how the information is compiled and analyzed and what conclusions are derived from this analysis.

Institutional parameters for the creation of a procedure in the National Police, so that the procedure is aligned with institutional policies.

The creation of specific procedures within institutions such as the PNC requires a careful approach that considers both existing institutional policies and operational and legal needs, this process not only ensures that the new procedures are aligned with institutional objectives and strategies, but also guarantees that the regulations and ethical standards governing police activities are respected.

REGULATORY AND POLITICAL FRAMEWORK OF THE P NC

INSTITUTIONAL MISSION AND VISION

The mission and vision of the PNC are fundamental for the definition of any procedure within the institution, the mission of the PN is to guarantee *"the necessary conditions for the exercise of public rights and liberties, as well as for the peaceful coexistence of all inhabitants of the national territory"*. For its part, the vision projects the Police as a modern, efficient and highly professional organization, recognized for its contribution to the improvement of security and justice in the country.

These strategic guidelines provide a general framework for the creation of procedures, ensuring that they contribute to the fulfillment of the institutional mission and are oriented towards the long-term vision of the PN. Any new procedures must therefore be evaluated in terms of their ability to improve the security of the population, *protect human rights* and enhance the efficiency and professionalism of the institution.

STANDARDS AND OPERATING GUIDELINES

The PNC operates under a set of regulations and guidelines that guide its daily activities, these regulations include laws, decrees, resolutions, manuals and other normative documents that establish how police activities should be carried out: therefore, for the creation of a new procedure, it is essential to review and understand these normative documents to ensure that the new procedure does not conflict with existing regulations.

Law 62 of 1993

Law 62 of 1993" is one of the most important regulations governing the organization and functioning of the PN, this law establishes the legal basis for the structure, functions and competencies of the Police; any new procedures must be in line with this law, ensuring that they respect the hierarchy, responsibilities and processes established therein.

National Code of Police and Coexistence

The "*National Code of Police and Coexistence (Law 1801 of 2016)"* is another crucial regulatory framework, this code establishes the rules governing the actions of the Police in matters of coexistence and citizen security; a new procedure must be aligned with the provisions of this code, especially with regard to the defense of citizens' rights and the promotion of peaceful coexistence.

Ethics and Transparency Policy

The ethics and transparency policy is one of the most important within the National Police. This policy emphasizes the importance of acting with integrity, responsibility and transparency in all police actions.

Innovation and Technology Policy

The innovation and technology policy emphasizes the need to modernize and adapt police procedures to technological advances and international best practices; any new procedures must consider the use of advanced technology and innovative tools to improve the efficiency and effectiveness of police activities.

IDENTIFICATION OF KEY INSTITUTIONAL PARAMETERS

Alignment with Mission and Vision

One of the most important institutional parameters is the alignment of the new procedure with the mission and vision of the PN, this means that the procedure must be designed to contribute to security and peaceful coexistence in Colombia, and to strengthen the professionalism and effectiveness of the institution, it is crucial that the procedure be evaluated in terms of its ability to support these strategic objectives.

Procedure Creation Process

- **Preliminary analysis**

The first step in creating the procedure is to conduct a preliminary analysis that identifies operational needs and gaps in existing procedures. This analysis should involve a review of current regulations, institutional policies and international best practices, and should include consultations with police personnel and other relevant stakeholders to identify key areas that the procedure should address.

- **Design of the procedure**

Once the preliminary analysis has been carried out, the procedure is designed. This design must be detailed and specific, including all the necessary steps for its implementation; it is important that the design of the procedure be clear and understandable, with specific guidelines on how to carry out each of the tasks involved.

PHASE II: STANDARDIZED PROPOSAL ON THE COMPONENTS OF A PROCEDURE THAT ADDRESSES THE SPECIFIC CHALLENGES RELATED TO THE COLLECTION, PRESERVATION AND ANALYSIS OF EVIDENCE IN CASES OF DIOT SECURITY INCIDENTS IN THE COLOMBIAN CONTEXT

The exponential growth of IoT has transformed different sectors in Colombia, from the smart home to industry and critical infrastructure. However, this technological advancement has also generated new security and cybercrime challenges. The correct collection, storage and analysis of digital evidence is essential to investigate and resolve IoT-related security incidents,

This procedure provides detailed guidance for the acquisition of different types of data in the context of dIoT security incidents in Colombia. The data types covered include: ADP, ADV, APR, ADS. Each section describes the steps necessary to ensure the integrity and validity of the digital evidence, following international best practices and legal regulations applicable in Colombia.

Objectives of the standardized proposal

- Standardize the digital evidence collection process in dIoT-related security incidents.
- Ensure the integrity and authenticity of evidence using appropriate methods and tools.
- Comply with legal regulations and international standards, ensuring that evidence is admissible in legal proceedings in Colombia.
- Facilitate effective analysis of evidence to identify the root cause of the incident and support mitigation and prevention of future similar events.

GENERAL CONSIDERATIONS OF THE STANDARDIZED PROPOSAL

Before starting any data acquisition process, the following considerations should be taken into account:

- **Legal Authorization**: Ensure that you have the necessary legal authorizations, such as court orders or consents, as appropriate and in accordance with current Colombian legislation, including *"Law 1273 of 2009 on computer crimes and the protection of personal data under Law 1581 of 2012"*.
- **Preservation of Evidence**: Ensure that digital evidence is collected and stored in a way that preserves its integrity, avoiding any alteration or contamination of the data.
- **Detailed Documentation**: Compile step-by-step documentation of the procurement process, including: "*date, time, location, personnel involved, tools used"* and any relevant observations. This is essential to maintain a strong chain of custody.
- **Selection of Appropriate Tools**: Use recognized and validated forensic tools that are appropriate for the type of data and devices involved.
- **Personnel Security**: Ensure that procurement personnel are trained and take the necessary precautions to protect themselves and prevent damage to devices or loss of data.
- **Minimize System Disruption**: Conduct procurement in a manner that minimizes any impact on the normal operation of the devices and systems involved.

DISCUSSIONS

The inclusion of IoT in Colombia has been a growing phenomenon in recent years, which has influenced the need to update various sectors, where devices are commonly used for the management, monitoring and control of procedures. The analysis carried out discusses the relationship of IoT devices in forensic procedures, which have been taken into account for the creation of the standardized proposal, validated from the expert judgment tool.

Research indicates that these devices allow remote activation of alarm systems, enabling the transmission of important data associated with security events, such as intrusion attempts or suspicious activities in real time (Zona-Ortiz et al., 2020; Sharma et al., 2019). The data provided by IoT devices include information regarding location, time and security-related events, which are key for the collection of digital evidence during forensic investigations. It is relevant to indicate that the safeguarding of data, as well as the chain of custody, are *"key* aspects *that must be considered in the process to ensure the validity of the information*" (Aldana and Buitrago, 2023; Alonso, 2022; Ramirez, 2019).

Amador et al., (2018) suggests that the application of dIoT, presents challenges associated with the privacy of the information, as well as the protection of the compiled information, which evidences the requirement that regulations or regulatory frameworks that indicate clear objectives of its use and application during forensic investigations be established (Amador Arévalo et al., 2018) . In particular, the monitoring of the data generated and the sensor devices support the authorities in the process of investigating tax evasion, crimes and financial fraud, because they allow the verification of unusual behavior patterns (Parra-Sánchez et al., 2021).

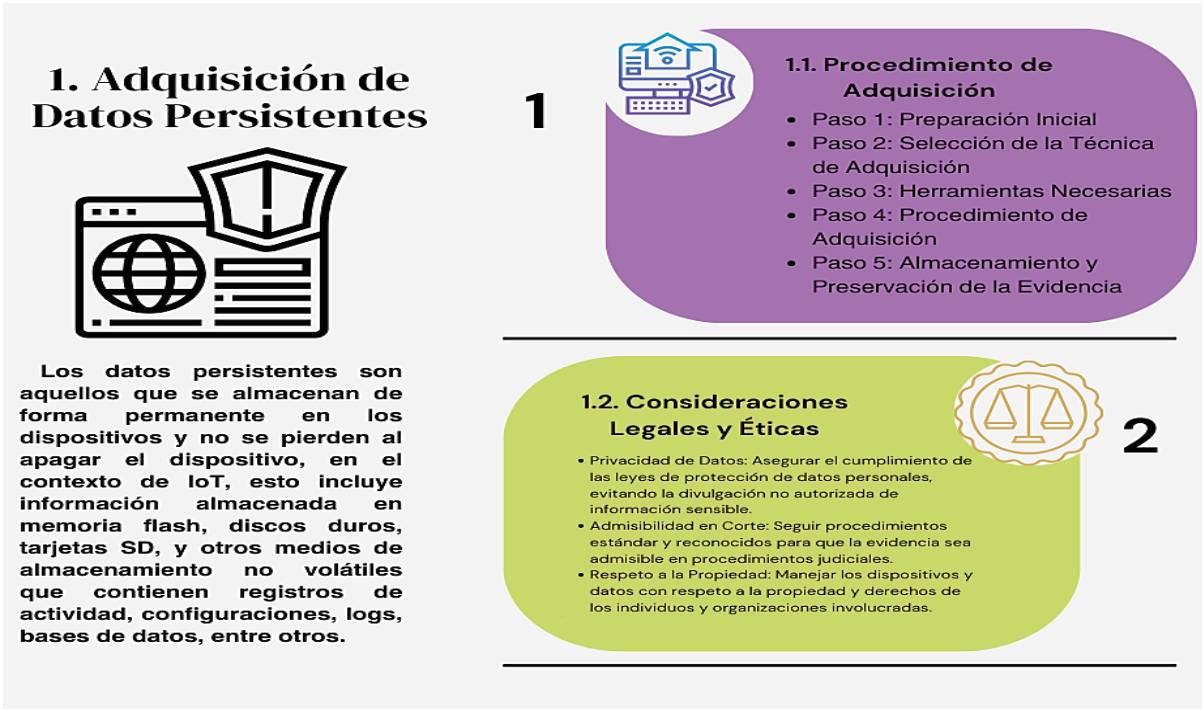

Figure4 . Persistent Data Acquisition

Source: Own

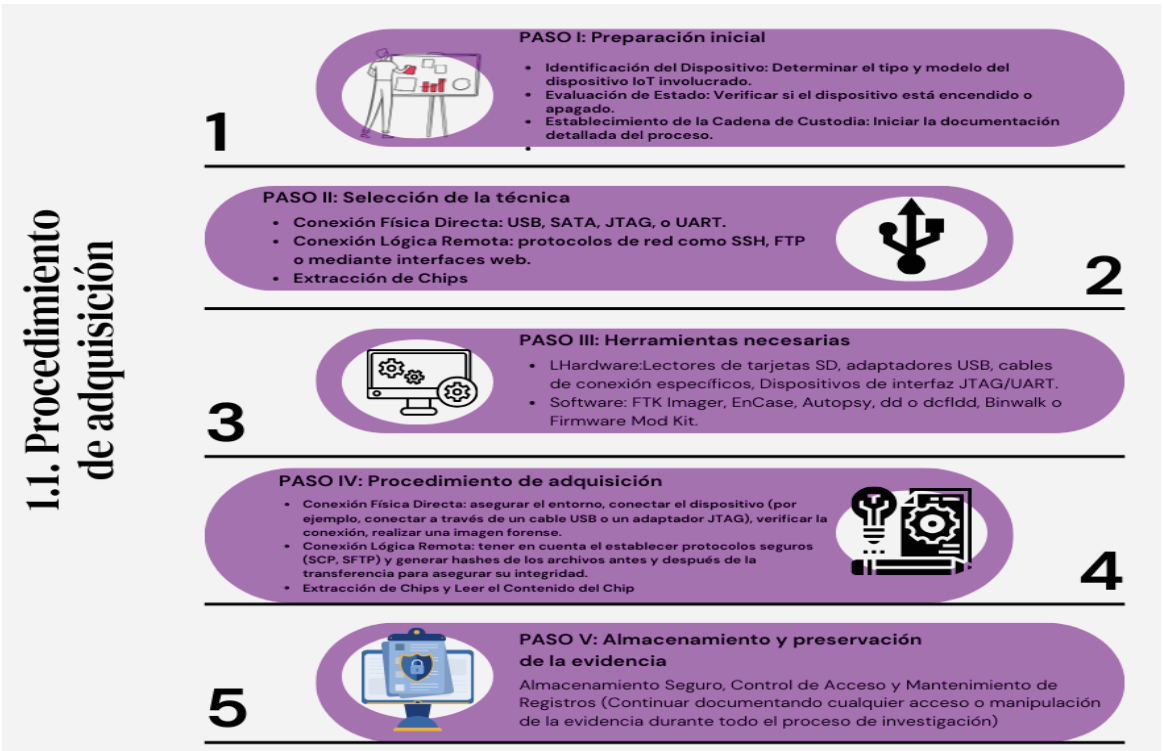

Figure 5. Steps of the Procurement Procedure

Source: Own

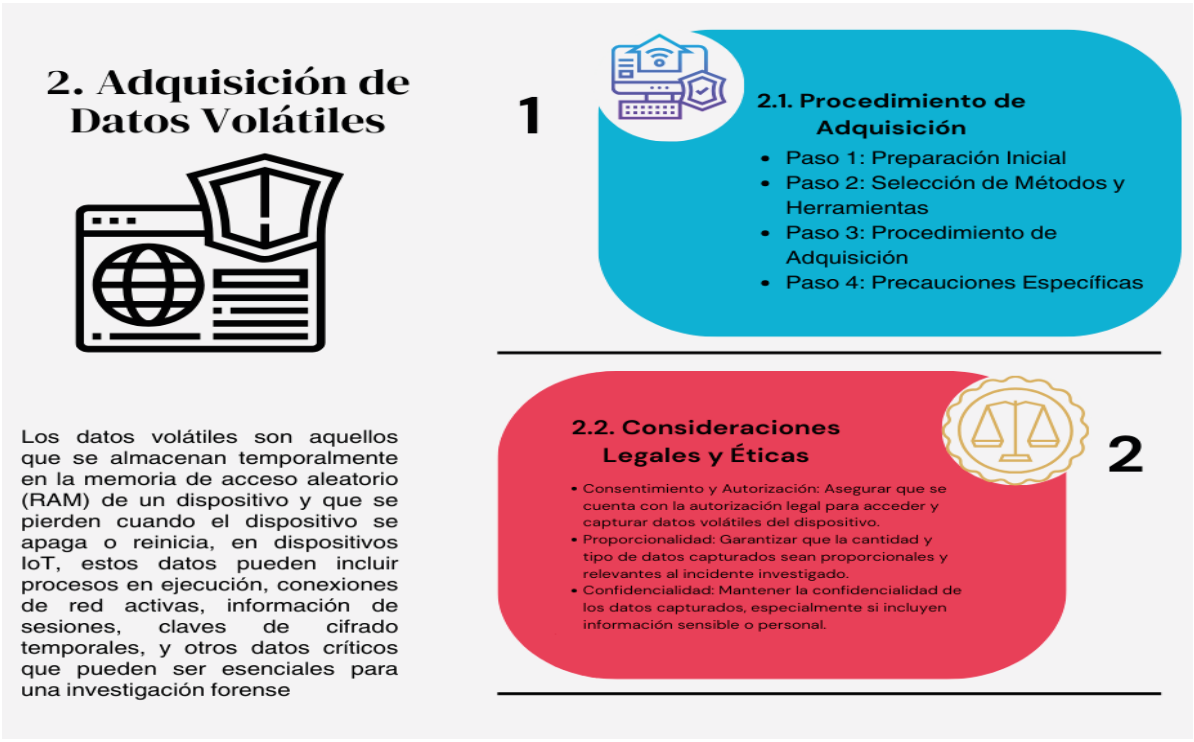

Figure 6. Volatile Data Acquisition

Source: Own

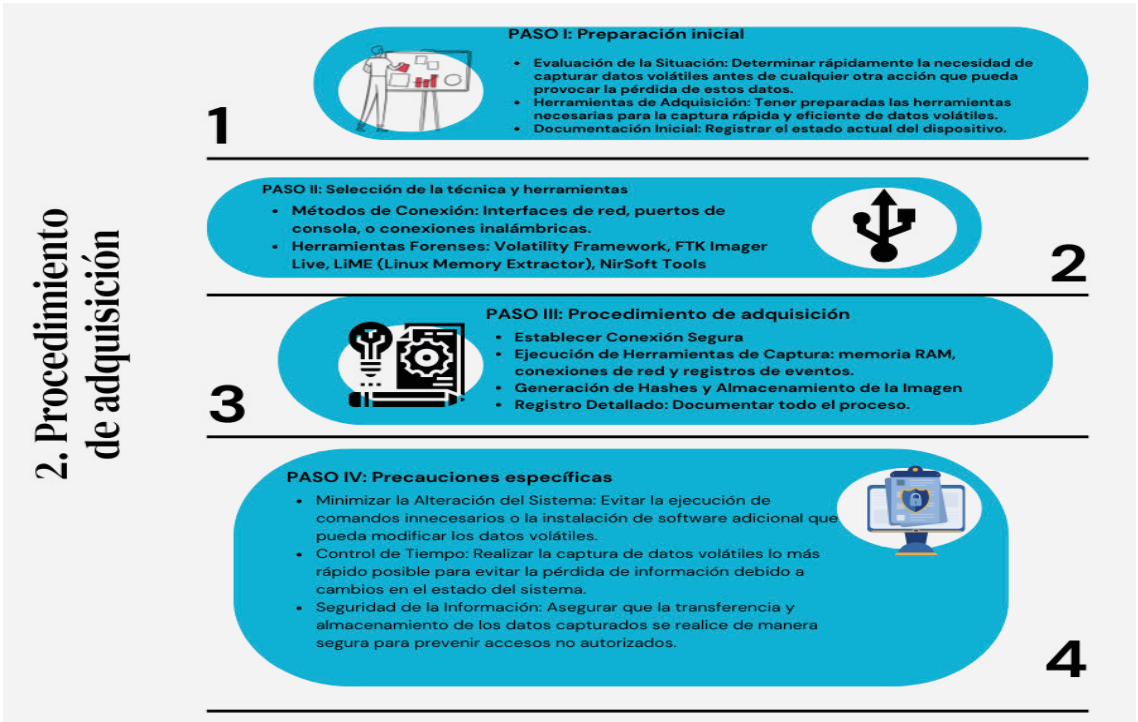

Figure 7. Steps of the Procurement Procedure

Source: Own

Figure 8. Network Packet Acquisition

Source: Own

Figure 9. Steps of the Procurement Procedure

Source: Own

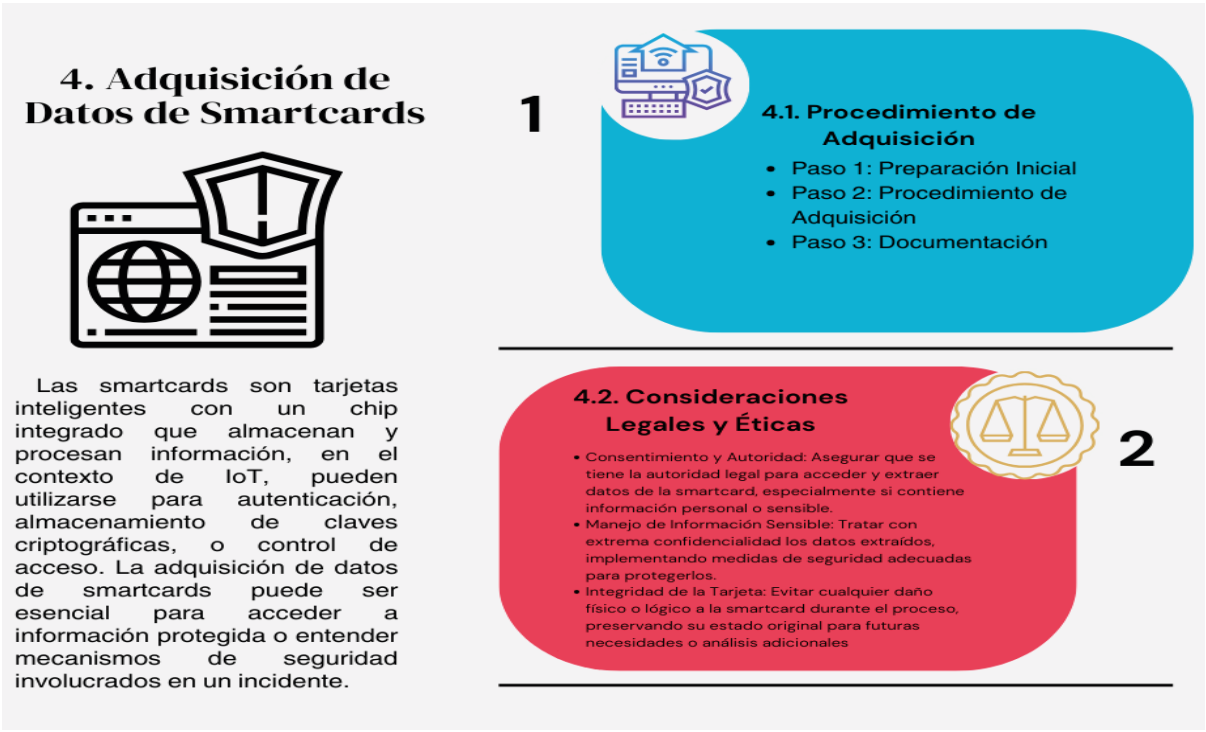

Figure 10. Smartcard Data Acquisition

Source: Own

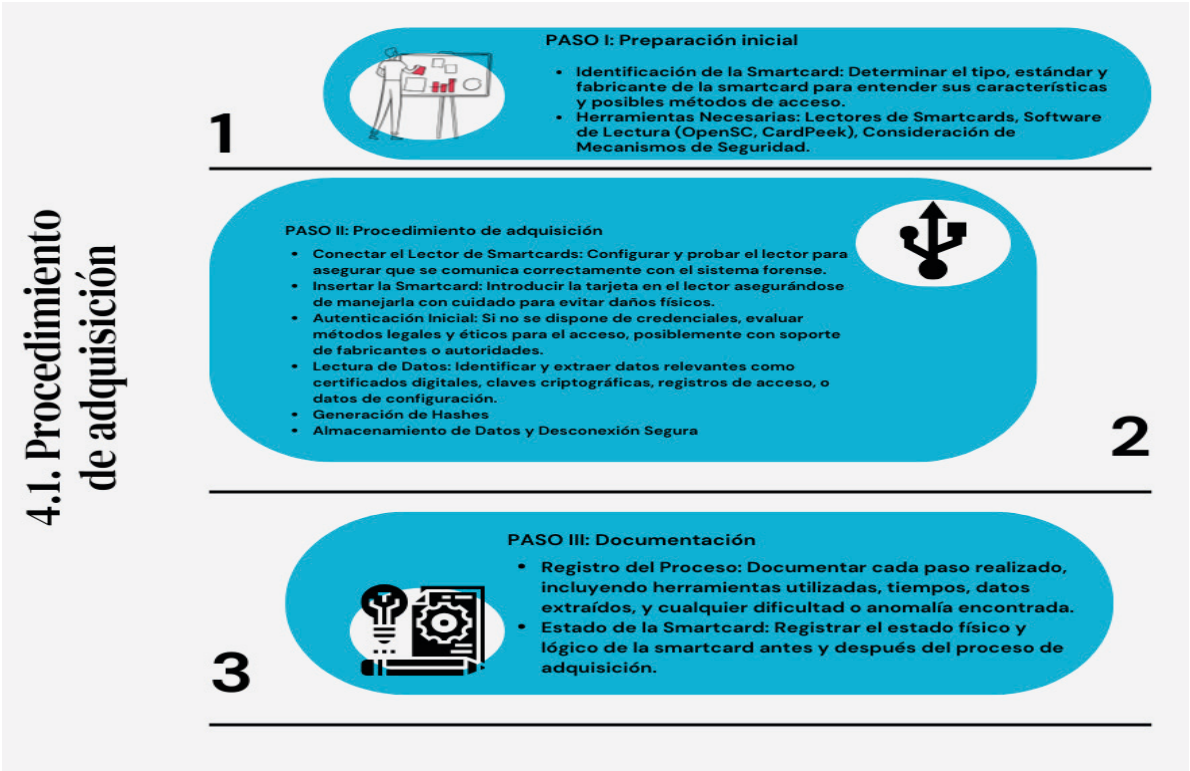

Figure 11. Steps of the Procurement Procedure

Source: Own

Empirical research indicates that one of the main challenges associated with the implementation of IoT is due to the lack of interoperability between devices. Where the standardization of a forensic process is essential for the management of compatible data between different systems and the safeguarding of the information obtained. Therefore, there is a need to create proposals or standardized protocols with regulations that promote the compilation and analysis of IoT data to improve the effectiveness of forensic investigations (Yacchirema, 2019; Estupiñan & Mora, 2019; Villegas, 2019) . Likewise, the security presented by dIoT is one of the challenges to be taken into account, where research proposes the use of *"technologies such as blockchain, for the assurance of information integrity"* in the environment generated by dIoT Chen et al., 2014; Christidis & Devetsikiotis, 2016) . The application of blockchain may be indispensable so that the data obtained cannot be manipulated or altered before being used as evidence in a forensic investigation process (Diaz et al., 2019) . Research infers that it is essential to have an optimal technological infrastructure for the integration of data compiled from dIoT in a centralized system, where it can be effectively analyzed and processed (Sarabia, 2020; Medina-Barahona et al., 2022).

CONCLUSIONS

For PNC investigators, it is crucial to develop specialized forensic procedures that address the particularities of each type of IoT device, including the need for advanced tools and techniques for information gathering and analysis, as well as a thorough understanding of the contexts in which these devices operate. The growing adoption of IoT in Colombia offers many opportunities for improving the efficiency and effectiveness of forensic investigations, however, it also poses significant challenges in terms of security, privacy and handling of large volumes of data. Through a rigorous methodological approach tailored to the particularities of IoT, investigators can maximize the value of information extracted from these devices and contribute significantly to solving cases and improving public safety.

The creation of a procedure within the PNC is a complex process that requires careful consideration of a variety of institutional parameters. These include alignment with the mission and vision of the institution, compliance with legal regulations, compatibility with institutional policies, operational feasibility, inter-agency participation, and continuous improvement. By following these parameters, it can be ensured that the procedure is not only effective in practice, but also fully aligned with the objectives and values of the PNC.

This structured approach not only facilitates the creation of procedures aligned with institutional policies, but also contributes to the professionalization and modernization of the PN, ensuring that the institution is prepared to face current and future security and coexistence challenges.

The proper acquisition of persistent, volatile, network packet and smartcard data is critical in the investigation of security events associated with dIoT in Colombia. Following the procedures detailed above can ensure that digital evidence is collected and preserved in a manner that is admissible and useful in legal proceedings, while respecting relevant legal and ethical considerations.

It is essential that the personnel in charge of these tasks are properly trained and updated on best practices and forensic tools, in addition to being aware of the applicable legal regulations, documentation and *maintenance of a* solid *chain of custody* are fundamental pillars for the security and quality of the evidence.

The adaptation and compliance with these procedures will contribute significantly to the effectiveness of forensic investigations in the IoT field, supporting the work of the authorities in the prevention, detection and resolution of cybercrime in the Colombian context.

REFERENCES

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.