Preprints.org

Article

Not peer-reviewed version

A Conceptual and Methodological Framework for Evaluating and Designing Wireless Networks Wi-Fi

Lorena Galeazzi *, Cristian Barria , Julio Hurtado , Camilo Garrido

Posted Date: 9 May 2025

doi: 10.20944/preprints202505.0690.v1

Keywords: wireless network Wi-Fi; Security Information; variable audit

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

A Conceptual and Methodological Framework for Evaluating and Designing Wireless Networks Wi-Fi

Lorena Galeazzi - Avalos [1,2], Cristian Barría - Huidobro [1], Julio Hurtado - Alegría [2,*] and Camilo Garrido - Briones [1,*]

[1] Centro de Investigación en Ciberseguridad, Universidad Mayor de Chile, Manuel Montt 367, Providencia 7500628, Chile

[2] Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Popayán 190003, Colombia

* Correspondence: ahurtado@unicauca.edu.co; camilo.garrido@mayor.cl

Abstract: Wireless networks, integral to our daily routines, present an escalating challenge for both users and companies to maintain security amidst technological advancements and the handling of sensitive data. The evolving consumption model and heightened device-related activities further complicate this issue. Existing regulations lack specificity, leaving auditors and network engineers frustrated, grappling with outdated information and localized challenges, especially in complex environments. This research identifies these deficiencies, emphasizing variables typically overlooked in current standards. A conceptual and methodological framework is introduced, focusing on users' perspectives as potential hackers, security technicians, or incident analysts. Validating with both consumer-grade and enterprise-grade equipment, we demonstrate the tangible impact of device security features on vulnerability, revealing the heightened susceptibility of home devices. Our findings culminate in a theoretical framework encompassing managerial, technical, communication channel protection, and end-user aspects. Additionally, we provide a comprehensive guide for assessing Wi-Fi performance within information security management systems, addressing knowledge and technological limitations in Wi-Fi security.

Keywords: wireless network Wi-Fi; Security Information; variable audit

1. Introduction

Wireless technologies are undergoing rapid evolution driven by the increasing demand for high-speed data [1], which is fueling the creation of new security protocols and performance optimization [2]. This advancement is fundamental for emerging applications such as vehicular networks and the Internet of Things (IoT). However, this digital revolution poses significant security challenges due to a lack of coordination in standardization, which increases the vulnerability of network-connected devices to cyber threats and fraud. The need to anticipate and respond swiftly to these vulnerabilities has resulted in an exponential proliferation of standards designed to integrate controls that mitigate security gaps [3]. These standards are developed by various multinational and non-profit organizations, composed of international committees, with the primary goal of harmonizing regulations among governmental entities and focusing on critical aspects such as network security. The lack of consensus in standardization further exacerbates these vulnerabilities, especially in client-related channels [4].

The recognition of this security gap has driven the creation and dissemination of various standards, among which IEEE 802.11 stands out, referring to Wi-Fi wireless networks. This standard oversees technological development and aligns with other international standards [5]. Additionally, there are standards focused on information security, such as ISO/IEC 27001 [6], NIST 800-53 [7], and CIS Control [8]. The improvement of wireless networks has become an urgent necessity, especially with the incorporation of advanced functionalities that increase speed, bandwidth, and

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

communication efficiency [9,10]. Simultaneously, security measures have been introduced to strengthen connections and mitigate the inherent vulnerabilities of Wi-Fi [11]. These measures often require direct interaction with the signal in the electromagnetic spectrum, presenting additional challenges for protecting these networks due to the open and unguided nature of the transmission medium [12,13].

When designing, auditing, monitoring, and managing a network using a specific standard, only particular controls relevant to that technology are applied. Auditors face the challenge of handling diverse information to conduct their evaluations effectively, requiring them to stay updated on the latest standard versions, technologies, and emerging threats [14].

The core problem is that current standardized approaches to wireless network security, while universally applicable, struggle to adequately address the rapidly evolving technological landscape and the unique physical and environmental contexts of implementation, leading to challenges in information management, delayed updates, reliance on experiential knowledge, and a need for a more integrated framework that considers real-world factors affecting Wi-Fi security [15].

The main objective of this research is the creation of a conceptual and methodological framework, integrating various variables from the context of standards, the physical phenomena of the signal, and real-world scenarios that affect the security of connectivity in Wi-Fi networks. This paper proposes a framework that links established resources and provides additional guidance on existing practices and controls to achieve optimal results in the evaluation, design, and management of Wi-Fi security, addressing the limitations of current approaches and facilitating the implementation of more effective and contextually relevant solutions.

The research methodology of this paper is projective, based on the positivist epistemological model [16,17]. The study adopts a mixed methods approach for analysis: qualitative for interpreting information from bibliographic reviews and quantitative for measuring experimental variables. Finally, the deductive hypothesis allows the argumentation of truths derived from general rules and true or false antecedents.

The research collects the necessary information to create a Methodological Framework developed from three key scientific articles [15–19]. These documents constitute the initial foundation for reviewing relevant theoretical and literary concepts, enabling the completion of the first stage of experimentation. This phase laid the groundwork for evaluating the experiments and determining which essential variables should be incorporated to contribute to the framework.

The main contribution of this research lies in the unification of currently scattered information regarding the evaluation and design of Wi-Fi wireless networks into a comprehensive conceptual and methodological framework. This framework is based on an exhaustive literature review and empirical results that validate the influence of critical variables such as the characteristics of the target device, the proximity of the attacker, and environmental conditions, demonstrating a greater effectiveness of attacks in lower temperatures. Through the identification of five fundamental pillars derived from experiments in real-world and laboratory settings, this study seeks to overcome the limitations of existing standardized approaches, which often do not adequately consider the rapid technological evolution or the specific physical and environmental contexts. The consolidation of these findings into a single framework provides an updated and holistic guide for auditors and implementers of Wi-Fi networks, facilitating a more effective and context-aware evaluation and design. With a long-term vision of five years, this contribution aims to establish a solid and unified foundation for the continuous improvement of security in wireless networks.

2. Materials and Methods

The methodology used in this research is of a projective nature [16,17], which involves the formulation of proposals, plans, or procedures designed as solutions to practical problems or needs. These problems may arise in various contexts, whether institutional or in a specific field of knowledge. This approach is based on a precise diagnosis of current needs, explanatory processes, and future trends.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

This experiment was divided into three main phases: literature review, data collection, and experimentation.

In the literature review phase, the scientific article "A Review of the Security Information Controls in Wireless Networks Wi-Fi" [15] was published, which allowed for the determination that the controls associated with Wi-Fi wireless networks present different approaches regarding information security. From this perspective, the relationship between controls and security varies across standards.

In the second phase, a literature review and data collection were conducted, and the scientific article "Conceptual Model of Security Variables in Wi-Fi Wireless Networks: Review" [18] was published. This allowed for the grouping of identified variables and, at the same time, the definition of four security concepts that clearly outline the research direction of the analyzed documentation.

In the third phase, the scientific article "Validation of Security Variables for Audits in Wireless Wi-Fi Networks" [19] was published. This allowed for the integration of the variables identified in the literature and the identification of new ones through empirical validation with a controlled experiment.

This research updates the experiment presented in the third publication [19] by incorporating additional variables not previously considered and validating key aspects not addressed in the previous study. This update is part of the ongoing evaluation and monitoring conducted over the past five years, completing the necessary phases for the creation of a comprehensive Conceptual and Methodological Framework aimed at evaluating and designing Wi-Fi wireless networks.

2.1. Experiment

The experiment was conducted in three phases, which included determination of the guidelines for carrying out the laboratory through the conceptual model and literature review. For this purpose, key concepts and their variables were considered, as shown in Figure 1.

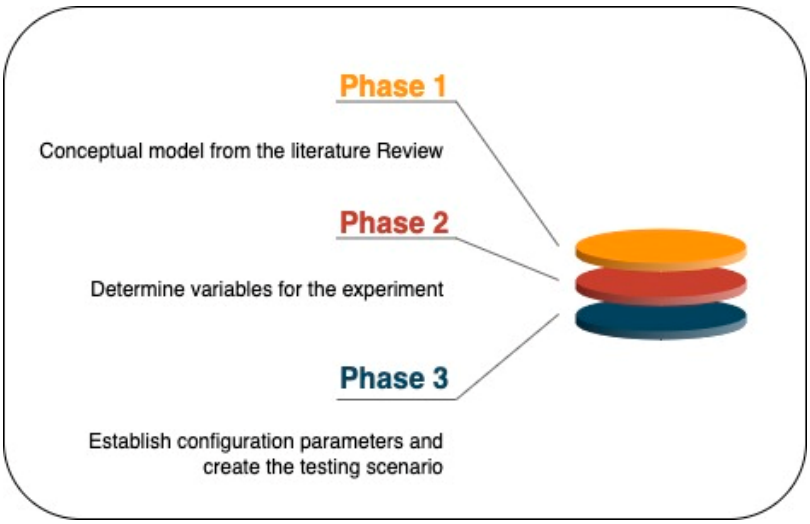


Figure 1. Phases to conduct the experiment [Source: Own elaboration].

2.2. Phase 1. Conceptual Model from the Literature Review

In the initial literature review on information security controls from three sources, ISO/IEC 27001, CIS controls, and NIST 800-53, it was observed that controls related to Wi-Fi wireless networks present diverse approaches. Firstly, it was confirmed that there is a discrepancy among the specific standards examined, as they differ in their parameters, meaning each one focuses on controls and audits with different objectives. Additionally, it was identified that the ISO/IEC 27001 standard encompasses much broader and more comprehensive controls compared to the others, addressing aspects of operation, control, security, and monitoring [15].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

In the second narrative literature review, data were extracted from specific literature to identify sources that have addressed the topic in question. A selective approach was adopted to apply data interpretation techniques, identifying patterns and trends. This review focused on security variables in wireless networks, considered primary due to their commonalities and interrelation [18].

The analysis of collected data confirmed the presence of diverse variables with a variety of characteristics and functions. This meticulous evaluation allowed for detailed search and identification, leading to a more precise understanding of each. To establish a conceptual relationship, a Venn diagram was used, facilitating the determination of interrelation among the variables identified during the review. Initially, four variables associated with Wi-Fi network security were identified: Firewall/IDS, Cryptography, Wireless Network Monitoring, and Users. These variables are related to a range of vulnerabilities, threats, and risks addressed in the literature from different perspectives, whether from an attacker, an information security officer, or an incident response analyst. Furthermore, the review reveals that there is no direct focus on users, hence it was important to incorporate them as a variable in the conceptual model. Users have a direct relationship with the storage, processing, and transfer of the information they handle. Figure 2 illustrates the result of the conceptual model of the identified variables [18].

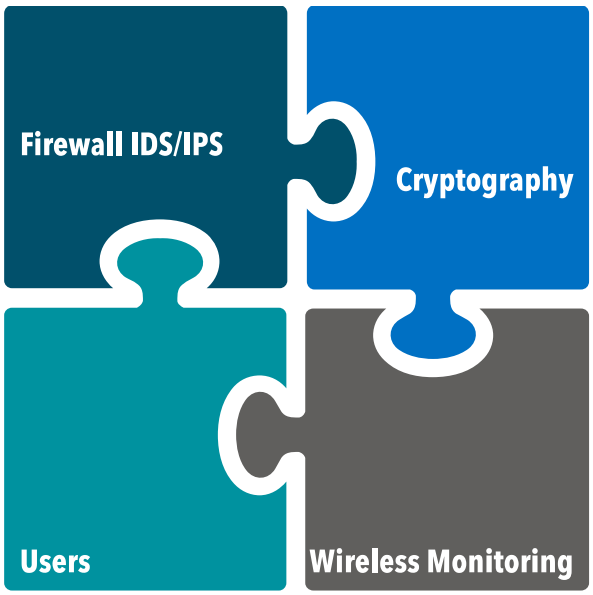


Figure 2. The conceptual model obtained from the literature review [18].

An investigation was conducted with the aim of selecting the type of attack, seeking to identify one that was pervasive, meaning it could provide generalized or extrapolatable measurements to other contexts.

Phase 2. Determining variables for the experiment.

For the study, a scenario was established where this set of variables could be evaluated and integrated to obtain valuable results for a Wi-Fi wireless network audit. Considering the experiment, attack phases, such as the reconnaissance phase and the actual attack, were established to guide the procedure and information gathering.

The experiment aims to identify new variables that may influence the evaluation results. Therefore, the attack itself is not the primary focus of the process; instead, the study examines the physical and environmental effects that may impact this unguided medium during its direct interaction with the signal in the electromagnetic spectrum.

Initially, different parameters can be identified during the reconnaissance of a target. It is important to note that this data can be obtained using applications such as Wifianalyzer [20] and Wiggle [21], which enable Wi-Fi wireless network mapping using a mobile device. These applications

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

are known as "stumblers" and are used exclusively as network scanners, not for conducting WLAN network attacks or hacks. Their primary function is to verify signal strength levels, among other utilities [22].

Network mapping provides an overview of the network architecture, including the relationships between devices and how they are connected. These maps help administrators visualize the network structure, facilitating network management and security evaluation [23], as shown in Table 1.

Table 1. Parameters obtained from a Wi-Fi analysis application.

Phase	Category	Parameters
Recognition	Data link connection	Encryption Frequency SSID Channel BSSID Location (Latitude – Longitude) Status Speed Signal strength Security IP address Mac address (Vendor) Signal meter WPS Connected AP clients

The scouting phase also involves variables related to social engineering, allowing for their visualization at the target location. Furthermore, through geolocating the capture, it is possible to identify aspects of the environment using tools like Google Earth. Various applications enable the saving of files in KML format, as this format allows for the storage of geographic information and its visualization in map applications [24], facilitating not only the analysis of specific parameters but also an analysis of the surrounding environment, as detailed in Table 2.

Table 2. Parameters obtained in the target environment.

Phase	Category	Parameters
Recognition	Environmental variables	Distance Height Types of building materials Signal obstacles

2.3. Phase 3. Establishing Configuration Parameters and Creating the Testing Scenario

In this phase, it was determined to establish configuration parameters that could be measurable for both domestic and enterprise devices, as well as to define the test scenario that would serve as a basis for testing with various wireless devices. In accordance with the above, the following points are detailed:

Equipment for the experiment:

The following equipment was selected for each of the tests, with the aim of detecting changes in the results, both in domestic and enterprise devices. Table 3 describes the devices used for the tests of each of the conducted trials.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Table 3. Details of devices used to perform laboratory tests.

Device	Brand	Model	Category
Router	Cisco 2940	-.-	-.-
Wireless Router	Linksys	WRT610N	Home
Wireless Router	TP-Link	TL-WR802N	Home
Wireless Router	Ruckus	R550	Enterprise
Wireless Router	Aruba	IAP-330	Enterprise
Notebook	MacBook Pro 2018 15"	-.-	-.-
Notebook	ASUS GV301q	-.-	-.-
Computer	Raspberry PI3	-.-	-.-
Notebook	MacBook Pro 2017 13"	-.-	-.-
Notebook	Surface Pro 6	-.-	-.-

Design of the indoor experiment.

The design of the indoor experiment was established with the aim of achieving consistent results by utilizing different devices within the same setting, thereby enabling precise measurements to be conducted, as depicted in Figure 3.

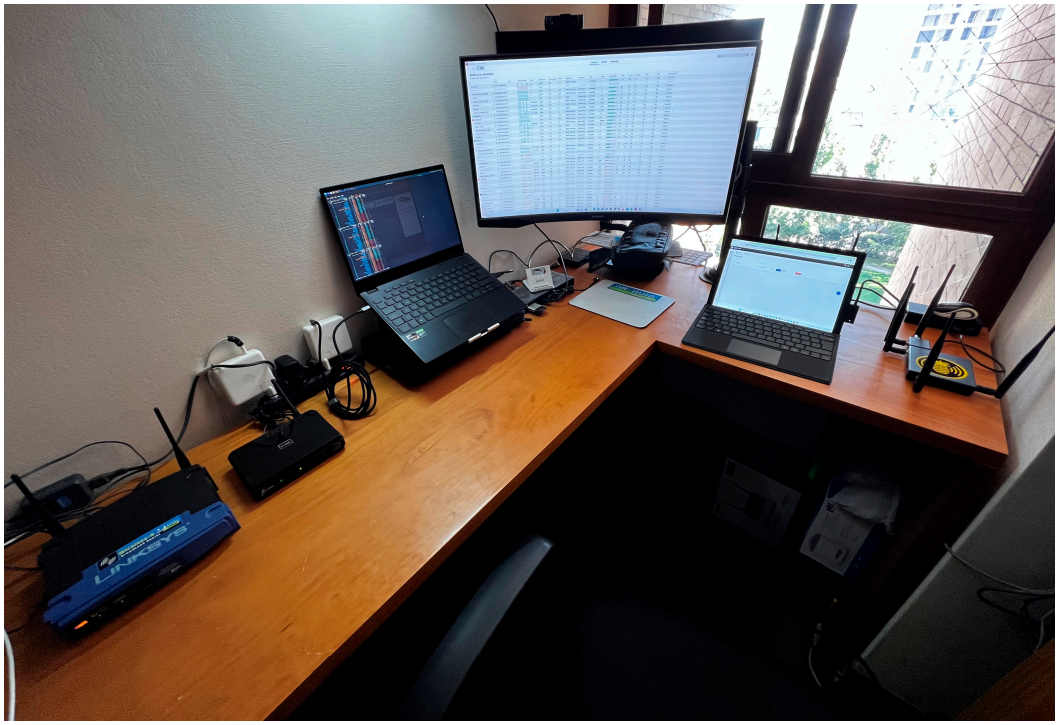


Figure 3. Laboratory experiment, same testing scenario [Source: Own elaboration].

Indoor testing topology

The proposed indoor testing topology involves setting up a local network that includes a Wi-Fi wireless router, either for home or enterprise use, with at least one client connected to the access point (AP). In this case, a Surface Pro 6 was used as the client to carry out deauthentication tests and capture the handshake as a standard attack. These tests were conducted using two types of attack devices: a Pineapple and a laptop running the "Wifite" software, a tool from the Kali Linux operating system. All of this was done while considering two types of obstacles to the Wi-Fi signal: a wooden wall and a glass wall, as shown in Figures 4, 5, 6, and 7.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

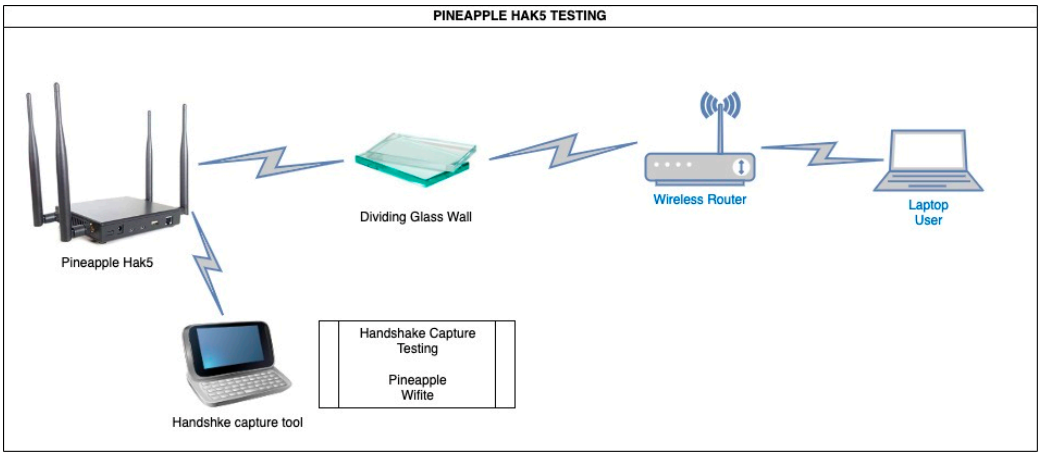


Figure 4. Topology of tests performed with the Pineapple device, with dividing glass wall [Source: Own elaboration].

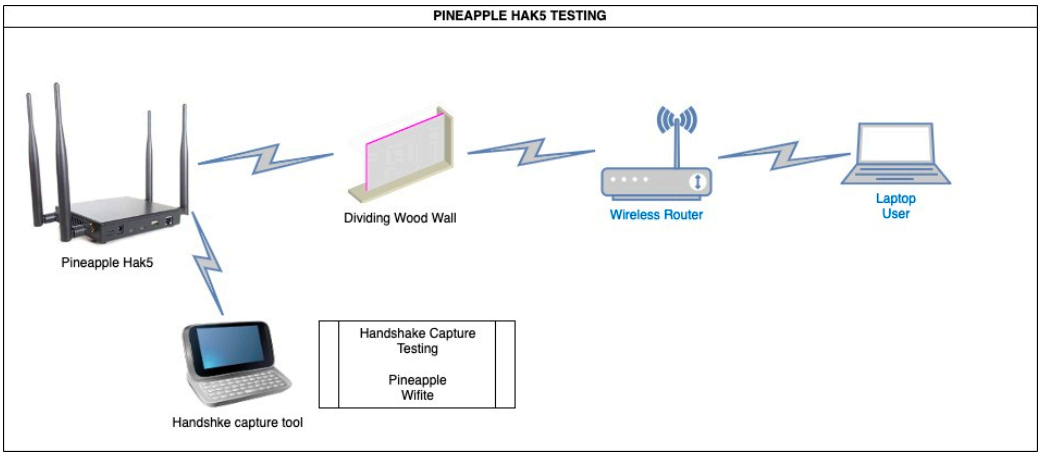


Figure 5. Topology of tests performed with the Pineapple device, with dividing wood wall [Source: Own elaboration].

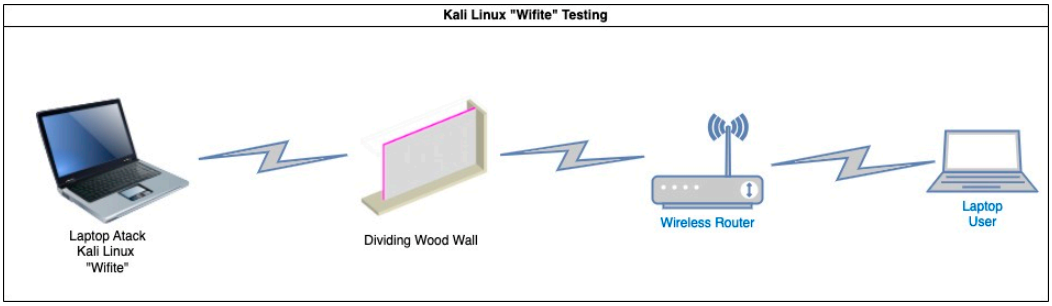


Figure 6. Topology of tests performed with the Kali Linux, with dividing wood wall [Source: Own elaboration].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

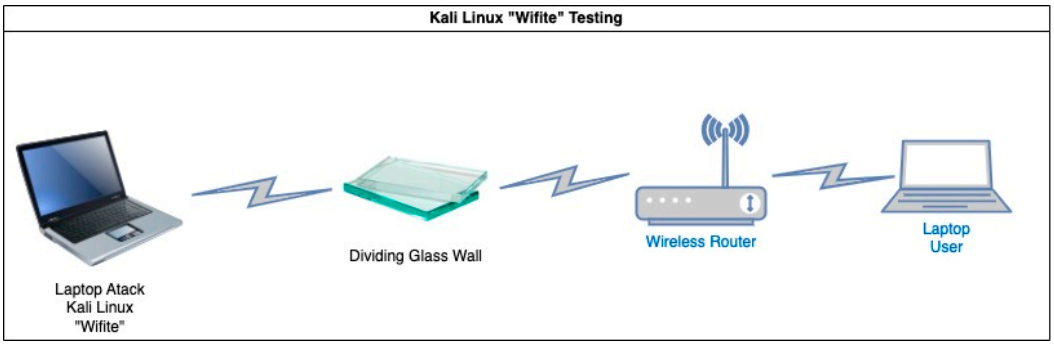


Figure 7. Topology of tests performed with the Kali Linux, with dividing glass wall [Source: Own elaboration].

Regarding the obstacles selected for the experiment, it was determined to use walls made of wood and glass, as they exhibit different characteristics depending on the material type, allowing for the observation of differences in their physical properties, such as their resistance to an electromagnetic signal.

Wood has low electrical conductivity, which allows this type of signal to pass through it with low attenuation, as well as minimal absorption and dispersion. At the same time, it was considered to conduct the same test using a glass wall to ascertain if there are significant changes. This is because glass allows the passage of radio waves but may affect the signal, such as through reflection and refraction.

Outdoor Experiment Design.

The same test was conducted at a distance of 30 meters. The proposed design for the outdoor environment focuses on conducting tests that allow determining differences in results compared to the laboratory scenario used in previous tests. These considerations include distance, height, and obstacles present in the environment of the selected test area. A representative and suitable location has been identified to conduct black box testing, especially in situations where accessing the devices is not straightforward, as depicted in Figure 8.

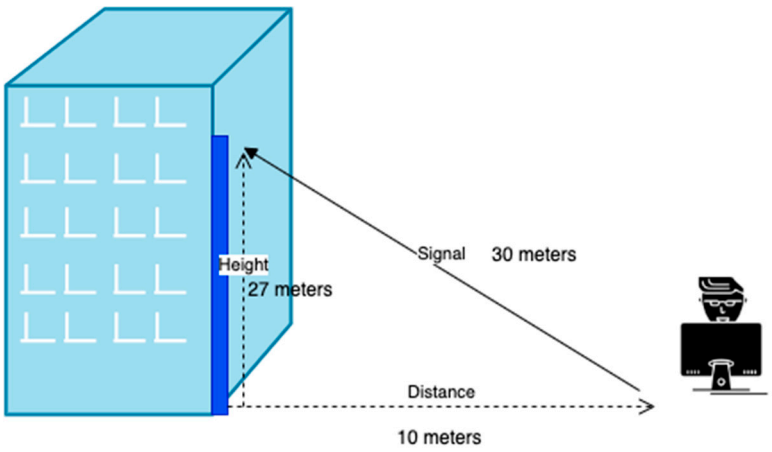


Figure 8. Outdoor experiment parameters in a real-world environment [Source: Own elaboration].

2.3.1. Determining the Type of Attack

To select the type of attack, an investigation was conducted with the aim of identifying a cross-cutting attack capable of providing generalized or extrapolatable measurements to other contexts. The best option was to use "handshake capture," which constitutes an initial phase for most attacks recorded on Wi-Fi wireless networks [25].

With the selection of the attack, two different formats could be opted for, using the same software but with different tools. The first format involves using the Wifite software from a computer

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

with an omnidirectional wireless antenna, while the second format entails the use of a Wi-Fi network attack device called Pineapple.

2.3.2. Test Framework

For this experiment, a test framework has been defined to obtain results from different devices facing the same type of attack. To achieve this, the use of two types of wireless equipment was considered: one for domestic use and another for enterprise use.

Based on the established variables, each device possesses various capabilities that may vary due to its physical characteristics, software, and configurations inherent to its manufacturing. In this regard, the following tables describe the parameters used for the measurements in the experiment.

2.3.3. Test Parameters with Pinneapple Hacking Device

The following parameters were considered for the test conducted in January 2022:

- Type Atack: HandShake
- WPA Personal Encryption Method
- TKIP Encryption Algorithm
- CTS/RTS Communication Protection **off**
- Distance: 10, 20 and 30 meters
- Height: 1 meter
- Obstacle: Dividing wood wall and glass wall
- Weather [26]: **30 cº, 26 January 2022**

Table 4. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	1	3600	30	No	No	Yes	Yes
20	1	7200	30	No	No	Yes	Yes
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No
10	1	3600	30	No	No	Yes	Yes
20	1	7200	30	No	No	Yes	Yes
30	1	14400	30	No	No	Yes	Yes
15	1	5400	30	No	No	Yes	Yes
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No

For this test, the following parameters were considered:

- Type Atack: HandShake
- WPA2 Personal Encryption Method
- AES Encryption Algorithm
- CTS/RTS Communication Protection **on**
- Distance: 10, 20 and 30 meters
- Height: 1 meter
- Obstacle: Dividing wood wall and glass wall

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

- Weather [26]: **30 cº, 26 January 2022**

Table 5. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	1	3600	30	No	No	No	No
20	1	7200	30	No	No	No	No
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No
10	1	3600	30	No	No	No	No
20	1	7200	30	No	No	No	No
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No

For this test, the following parameters were considered for the experiment conducted in May 2024:

- Type Atack: HandShake
- WPA Personal Encryption Method
- TKIP Encryption Algorithm
- CTS/RTS Communication Protection **off**
- Distance: 10, 20 and 30 meters
- Height: 30 meters
- Obstacle: Dividing wood wall and glass wall
- Weather [27]: **14 cº, 5 May 2024**

Table 6. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	30	3600	14	No	No	Yes	Yes
20	30	7200	14	No	No	Yes	Yes
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No
10	30	3600	14	No	No	Yes	Yes
20	30	7200	14	No	No	Yes	Yes
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

The following parameters were taken into account for this test:

- Type Atack: HandShake
- WPA2 Personal Encryption Method
- AES Encryption Algorithm
- CTS/RTS Communication Protection **on**
- Distance: 10, 20 and 30 meters
- Height: 30 meters
- Obstacle: Dividing wood wall and glass wall
- Weather [27]: **14 cº, 5 May 2024**

Table 7. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	30	3600	14	No	No	No	No
20	30	7200	14	No	No	No	No
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No
10	30	3600	14	No	No	No	No
20	30	7200	14	No	No	No	No
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No

2.3.4. Test Results with Kali Linux Software, "Wifite"

The following parameters were considered for the test conducted in January 2022:

- Type Atack: HandShake
- WPA Personal Encryption Method
- TKIP Encryption Algorithm
- CTS/RTS Communication Protection **off**
- Distance: 10, 20 and 30 meters
- Height: 1 meter
- Obstacle: Dividing wood wall and glass wall
- Weather [26]: **30 cº, 26 January 2022**

Table 8. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	1	3600	30	No	No	Yes	Yes
20	1	7200	30	No	No	Yes	Yes
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

35	1	21600	30	No	No	No	No
10	1	3600	30	No	No	Yes	Yes
20	1	7200	30	No	No	Yes	Yes
30	1	14400	30	No	No	No	Yes
15	1	5400	30	No	No	No	Yes
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No

For this test, the following parameters were considered:

- Type Atack: HandShake
- WPA2 Personal Encryption Method
- AES Encryption Algorithm
- CTS/RTS Communication Protection on
- Distance: 10, 20 and 30 meters
- Height: 1 meter
- Obstacle: Dividing wood wall and glass wall
- Weather [26]: **30 cº, 26 January 2022**

Table 9. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	1	3600	30	No	No	No	No
20	1	7200	30	No	No	No	No
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No
10	1	3600	30	No	No	No	No
20	1	7200	30	No	No	No	No
30	1	14400	30	No	No	No	No
15	1	5400	30	No	No	No	No
25	1	10800	30	No	No	No	No
35	1	21600	30	No	No	No	No

For this test, the following parameters were taken into account for the experiment conducted in May 2024:

- Type Atack: HandShake
- WPA Personal Encryption Method
- TKIP Encryption Algorithm
- CTS/RTS Communication Protection **off**
- Distance: 10, 20 and 30 meters
- Height: 30 meters
- Obstacle: Dividing wood wall and glass wall
- Weather [27]: **14 cº, 5 May 2024**

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Table 10. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	30	3600	14	Yes	Yes	Yes	Yes
20	30	7200	14	Yes	Yes	Yes	Yes
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No
10	30	3600	14	Yes	Yes	Yes	Yes
20	30	7200	14	Yes	Yes	Yes	Yes
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No

For this test, the following parameters were considered:

- Type Atack: HandShake
- WPA2 Personal Encryption Method
- AES Encryption Algorithm
- CTS/RTS Communication Protection **on**
- Distance: 10, 20 and 30 meters
- Height: 30 meters
- Obstacle: Dividing wood wall and glass wall
- Weather [27]: **14 cº, 5 May 2024**

Table 11. Details of the results obtained in the test.

Distance (mts)	Height (mts)	Time (seg)	Weather (cº)	Successful Aruba	Successful Ruckus	Successful TP-Link	Successful Linksys
10	30	3600	14	No	No	No	No
20	30	7200	14	No	No	No	No
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No
10	30	3600	14	No	No	No	No
20	30	7200	14	No	No	No	No
30	30	14400	14	No	No	No	No
15	30	5400	14	No	No	No	No
25	30	10800	14	No	No	No	No
35	30	21600	14	No	No	No	No

3. Results

In relation to the results obtained from the literature review and the empirical experiment, it was observed that the variables selected for integration were suitable for validating the fundamental

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

pillars of the theoretical framework. The experiment was conducted on two occasions: first in January 2022 and then in May 2024, with the purpose of determining additional variables such as altitude and temperature.

During the experiment tests conducted with the Pineapple device, compared to the "Wifite" software tool of the Kali Linux operating system, significant differences in the results were identified. These discrepancies allow us to assert that, depending on the characteristics of the target device, especially regarding its security measures, it is possible to detect a security gap in domestic devices. The successful results of these tests highlight the inherent vulnerability in many of these devices, emphasizing the need to improve security measures in domestic environments to protect them against potential attacks.

Regarding distance variables, it was determined that the attacker's device should not be more than 20 meters away to achieve successful handshakes. Additionally, a direct relationship with waiting time was observed, which in this case was approximately 2 hours. Therefore, the greater the distance, the longer the waiting time needed to successfully capture the handshake. This correlation underscores the importance of proximity in the effectiveness of attacks.

With respect to tests conducted in different environments associated with temperature and the height difference of the target device, a higher number of successful cases were determined in low temperatures among the four observed devices. This trend suggests that environmental conditions, such as temperature, can significantly influence the effectiveness of attacks, emphasizing the importance of considering these factors when evaluating device security.

From the results obtained from the literature review and experiments conducted, it was possible to construct a Conceptual and Methodological Framework for the Evaluation and Design of Wi-Fi Wireless Networks, from which five fundamental pillars are derived that encompass the aspects influencing the auditing of a Wi-Fi wireless network.

Determining these pillars relied heavily on conducting empirical experiments in real-world and laboratory environments, as this allowed for the validation of aspects specific to the integrated variables.

Fundamental Pillars:

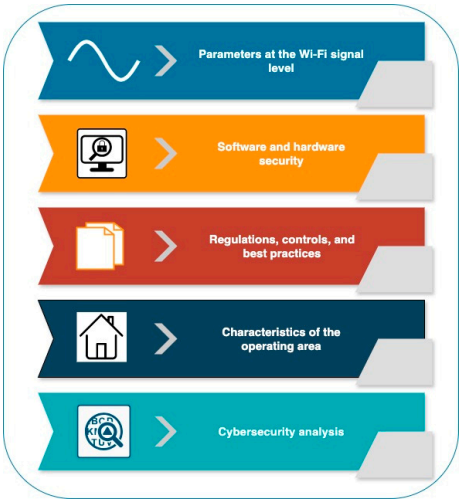


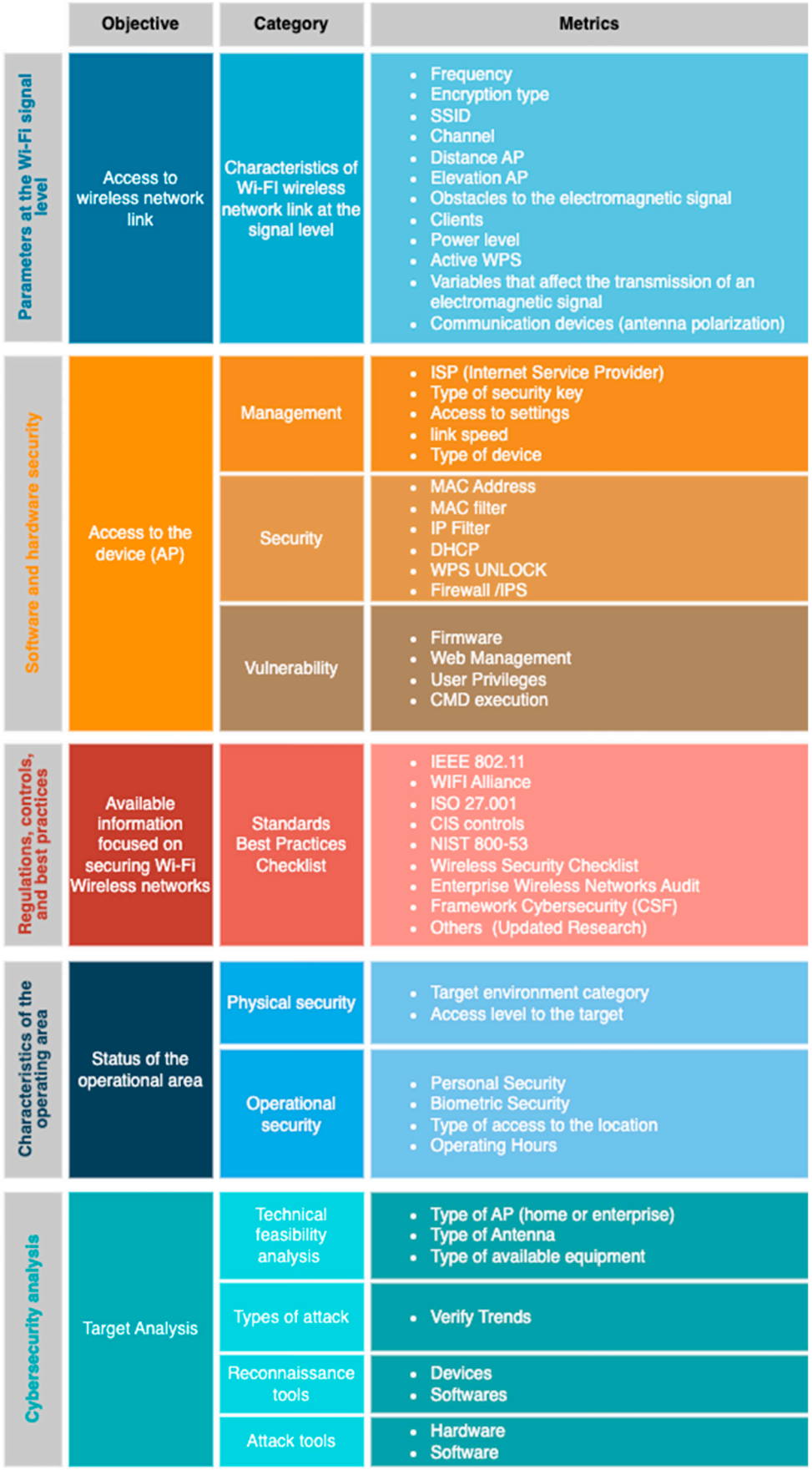
Figure 9. Fundamental pillars [Source: Own elaboration].

4. Conceptual and Methodological Framework: Evaluating and Designing Wireless Networks Wi-Fi Guide

This guide introduces using this framework, aimed at planning and integrating its application processes, with a focus on auditor use. From this perspective, each of the fundamental pillars of the

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

conceptual and methodological framework is detailed. Figure 10 illustrates the comprehensive approach to the framework's pillars.



Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Figure 10. Conceptual and Methodological Framework for Evaluating and Designing Wireless Networks Wi-Fi [Source: Own elaboration].

The diagram outlines the pillars of a Wi-Fi wireless network audit across its various categories, including the metrics required to conduct a comprehensive evaluation. See Figure 10.

The framework consists of five fundamental pillars, each with specific objectives, categories, and evaluation metrics to ensure comprehensive Wi-Fi network security management. These pillars are Wi-Fi network signal parameters, which focus on optimizing and protecting wireless communication; software and hardware security, addressing the protection of devices and systems against vulnerabilities; regulations, controls, and best practices, ensuring regulatory compliance and the adoption of recognized standards; operational area characteristics, which consider the physical and operational environment of the network; and cybersecurity analysis, which includes tools and strategies for identifying and mitigating risks. Each pillar contributes integrally to the robustness of the security system.

As the study results show, these metrics play a fundamental role in security aspects. It is important to note that their significance varies depending on the context of the device, as their application and relevance depend on specific circumstances and the environment in which they are implemented. Therefore, the auditor or implementer will determine the use of each metric according to the situation being addressed. Ideally, it is recommended to initially apply all metrics.

The following sections provide a detailed description of each pillar of the framework, along with their respective evaluation metrics:

4.1. Wi-Fi Signal Level Parameters

This section determines the configurations and technical aspects related to the Wi-Fi connection signal. In this regard, it encompasses all information gathered during the reconnaissance phase of an attack, as well as the physical properties of the electromagnetic signal.

4.1.1. Access to Wireless Network Link

Access to a Wi-Fi wireless network link is the process by which devices connect without the need for physical cables, and it constitutes the main objective of the first pillar of the model.

The strength of the signal and its proper configuration are essential for minimizing risks. This category defines the characteristics of the Wi-Fi wireless network link at the signal level, describing the metrics detailed below.

- **Frequency:**

The choice of frequency is essential for the security and implementation of wireless networks. Currently, bandwidth advances have optimized transmission range and signal coverage aspects. Proper frequency selection not only improves signal performance but also significantly contributes to strengthening the security aspects of the network.

According to the Wi-Fi Alliance, the frequencies used in Wi-Fi networks are primarily the 2.4 GHz, 5 GHz, and, more recently, 6 GHz bands (introduced with Wi-Fi 6E).

- 2.4 GHz: This frequency offers greater range due to its ability to penetrate obstacles, but it has lower speeds and may be more congested due to sharing with other devices such as Bluetooth and microwaves.
- 5 GHz: Provides higher speeds and less interference thanks to its multiple channels, although its range is more limited due to its microwave characteristics.
- 6 GHz: Introduced with the arrival of Wi-Fi 6E, this band offers even greater capacity, higher speeds, and less interference, making it ideal for environments with multiple connected devices.

The choice of band depends on factors such as range, required speed, and the implementation environment. These frequencies are designed to enhance the performance and security of wireless networks.

- **Encryption type:**

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

The type of encryption used in a Wi-Fi network refers to the methods employed to protect data transmission between the router and connected devices.

The main types of Wi-Fi encryption are:

- WEP (Wired Equivalent Privacy) is the oldest and least secure standard. Although it was widely used in the past, it is now considered obsolete due to vulnerabilities that allow an attacker to crack it quickly. WEP is not recommended.
- WPA (Wi-Fi Protected Access) is an improvement over WEP, offering a higher level of security. WPA uses the TKIP (Temporal Key Integrity Protocol) to encrypt data. While more secure than WEP, it is still vulnerable to specific attacks.
- WPA2 (Wi-Fi Protected Access 2): The enhanced version of WPA, and for many years, the de facto standard for Wi-Fi security. It uses the AES (Advanced Encryption Standard) encryption protocol, which is much stronger than the TKIP used in WPA. WPA2 remains the recommended standard to this day.
- WPA3 (Wi-Fi Protected Access 3): WPA's latest and most secure version. It introduces improvements in authentication and protection against brute-force attacks. It also provides better security for public networks (such as open networks) and more effectively protects data during transmission.

WPA3 is the recommended encryption for a Wi-Fi network, but if it is not available, WPA2 is a secure option. WEP and WPA should be avoided, as they are vulnerable to attacks.

- **SSID:**

The SSID (Service Set Identifier), which is the name that identifies a Wi-Fi network, should be configured strategically to avoid compromising security. It is advised against using default, personal, or identifiable names. While hiding the SSID can make detection more complex, it does not provide full protection, as advanced tools can still trace it. It is recommended that separate SSIDs be set up for guest networks to prevent access to the main network. Additionally, it is essential to complement this configuration with robust security protocols like WPA3 or WPA2. These actions and simple and secure names help improve security without relying solely on the SSID [Wifi alliance].

- **Channel:**

Properly configuring the channel of a Wi-Fi network reduces interference and improves security by minimizing vulnerabilities such as jamming attacks or unstable connections.

Using saturated channels, especially in urban environments, can cause interference that slows the network and makes data more susceptible to disruptions or potential eavesdropping.

Channels 1, 6, and 11 are recommended because they do not overlap in the 2.4 GHz frequency range. More channels are available in the 5 GHz range, which reduces congestion, but it will depend on the required coverage range. The 6 GHz band (Wi-Fi 6E) is an emerging option with wider channels and less interference.

Enabling automatic channel selection can improve performance, reduce interference, and mitigate intentional jamming attacks.

- **Distance AP:**

The distance between devices and the Access Point (AP) in a Wi-Fi network is important for both performance and security. The coverage, signal strength, and range of a wireless network directly affect the possibility of unauthorized access and the quality of communication. As distances increase, the signal weakens, making the network more susceptible to disruptions and attacks such as sniffing (data interception) or attempts to crack passwords through brute force. Keeping the distance between devices and the AP within the optimal range improves encryption quality and reduces the likelihood of incomplete or manipulated data captures.

In terms of security, obtaining a successful handshake from up to 10 meters away is possible.

- **Elevation AP:**

The importance of the AP's height is a consideration for its implementation and the network's security.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

From an implementation perspective, it is essential to note that an elevated position helps maximize signal propagation and reduces weak coverage areas. It also minimizes physical tampering of devices by unauthorized individuals, decreases interference from physical obstacles, and limits the horizontal spread of the signal to undesired areas.

It has been established that the recommended height is between 2.5 to 3 meters from the ground, depending on the environment, to balance coverage and security.

- **Obstacles to the electromagnetic signal:**

Electromagnetic signals face various obstacles that affect their performance in wireless networks, such as attenuation caused by physical obstructions (walls, furniture, metal structures), the distance between the transmitter and receiver, and electromagnetic interference from other devices. Atmospheric factors such as rain, fog, and humidity can weaken the signal, especially in long-range links. Additionally, higher-frequency signals are more susceptible to signal loss due to obstacles and adverse conditions. Electromagnetic shielding and the presence of human bodies also affect signal propagation.

Obstacles to the propagation of electromagnetic signals are more complex due to the high urban density and the presence of various structures. Skyscrapers, metal buildings, and areas with a high concentration of users can block, reflect, or scatter signals, creating dead zones or interference. Many connected devices can cause network congestion, especially in the 2.4 GHz bands, while urban equipment such as traffic lights and security cameras cause additional interference. Weather conditions and vehicular traffic also affect the signal, as does interference from competing Wi-Fi networks. The importance of your role in network design is underscored by the need for efficient coverage and minimal interference. These factors must be considered to achieve these goals.

- **Clients:**

The number of users connected to a Wi-Fi network has a significant impact from an attacker's perspective. A higher number of connected devices can lead to network congestion, which affects performance and facilitates Denial of Service (DoS) attacks, where the infrastructure is overloaded, and the service is interrupted for legitimate users. The difficulty in detecting intruders increases in networks with many users, as legitimate connections can mask suspicious behavior, allowing attackers to hide their activities through spoofing or sniffing. Furthermore, the diversity of connected devices, including smartphones, laptops, and IoT devices, exposes the network to vulnerabilities, as many of these devices may not be adequately secured, making them entry points for attacks such as AP spoofing or deauthentication attacks, which allow attackers to intercept legitimate communications or deny access.

In networks with a high number of users, distributed attacks like Distributed Denial of Service (DDoS) become more effective, exploiting traffic saturation and the difficulty of managing multiple devices. Additionally, the lack of proper network segmentation and robust security policies increases the likelihood of an attacker being able to move laterally within the network once a device has been compromised.

- **Power level:**

Signal power levels in a Wi-Fi network are important for security, as they directly influence coverage, performance, and the exposure of the signal to potential attacks. High signal power can increase the network's range, but it also expands the area vulnerable to interception by attackers, which increases the risk of unauthorized access. To mitigate this risk, adjusting the transmission power so that it is limited to the desired area is recommended, reducing the likelihood of the signal being detected outside the protected zone and making it more difficult for interception or remote access attempts.

- **Active WPS:**

When WPS is enabled on a Wi-Fi network, it can be detected from the outside using scanning tools such as Reaver, Bully, Kismet, or mobile applications like WPS Connect. These tools detect the presence of WPS on routers and provide information about its status. However, it is important to

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

note that these tools can also perform brute force attacks on the WPS PIN, which introduces risks to the Wi-Fi network.

- **Variables the affect the transmission of an electromagnetic signal:**

Electromagnetic signals are fundamental for wireless Wi-Fi communications, and their behavior directly impacts the security and performance of these networks.

Signal attenuation, or the loss of intensity as the signal propagates through obstacles such as walls, furniture, glass, and others, affects the quality of communication and can decrease the effectiveness of the network. Interference from other signals, whether from nearby electronic devices or other Wi-Fi networks, is also important, as it can degrade the signal quality. Signal modulation, which refers to how information is encoded in the electromagnetic wave, directly impacts transmission efficiency and security. Modulation techniques such as OFDM (Orthogonal Frequency Division Multiplexing), used in Wi-Fi, can improve the network's capacity and make it more resistant to interference.

Signal propagation, which describes how waves travel through different media, also influences the network's security. Electromagnetic waves can reflect, refract, or scatter, and poor handling of these factors can cause the signal to propagate beyond controlled areas, exposing the network to unwanted access.

Signal polarization, which refers to the orientation of the waves, is another important factor in signal reception, and improper configuration can facilitate attackers' capture of the signal.

- **Communication devices (antenna polarization)**

Antenna polarization is crucial for the security of Wi-Fi networks, as it influences signal quality, coverage, and protection against interference and attacks. Proper polarization selection, whether linear (horizontal or vertical) or circular, can reduce external interference and make passive listening or sniffing attacks more difficult, as attackers would need antennas compatible with the same polarization to intercept the signals. Additionally, using a different polarization between the access point and the attacker can minimize the impact of interference or jamming attacks, making the attacker’s signals less effective. It also improves network coverage and reliability, increasing its resistance to Denial of Service (DoS) attacks. In summary, proper polarization optimizes network performance and strengthens security by making interception, spoofing, and other attacks more challenging.

4.2. Software and Hardware Security

Within this pillar, emphasis is placed on security aspects covering both software and hardware levels. From this perspective, it is crucial to always employ the highest available security capacity in the devices comprising the Wi-Fi wireless network.

Access to the device (AP):

Management:

- ISP (Internet Service Provider):

Understanding the security measures that the Internet Service Provider (ISP) can apply to the access point (AP) installed in the home is crucial for ensuring the protection of the home network. ISPs typically offer default configurations for APs, but these settings may not be secure enough, leaving the network vulnerable to external attacks. Users can ensure their network is adequately protected by understanding the security levels the provider can implement, such as authentication, data encryption, automatic firmware updates, and protection against unauthorized access. Additionally, some ISPs allow users to customize security settings, such as changing default passwords, disabling WPS (Wi-Fi Protected Setup), and setting up an appropriate firewall. The security of the home AP is essential not only to protect personal information and connected devices but also to prevent cyberattacks that could compromise the network and data stored on connected devices. Knowing and applying the security measures recommended by the ISP helps strengthen the integrity and confidentiality of the home network.

- **Type of security key:**

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Security keys on access points (APs) protect wireless networks against unauthorized access and cyberattacks. The length and complexity of the keys are essential, as long and complex keys make decryption attempts more difficult. Using dynamic keys instead of static ones is important, as the former are generated automatically in each session, providing greater security.

- **Access to settings:**

Wi-Fi network access points (APs) have various levels of access that allow management of who can connect and what resources they can use within the network. The most common levels include:

- Guest access, which provides limited Internet-only access without compromising the internal network.
- Regular user access, which grants standard permissions for browsing and using services within the network.
- Administrator access, reserved for configuring and managing the AP, including modifying security settings, networks, and shared resources.
- Network control access, used in business environments to manage traffic, quality of service (QoS), and resource distribution; and
- Monitoring access, which allows for network performance monitoring without altering its configuration.

Each level has different security permissions, and proper management is crucial for maintaining the network's security and efficiency. Proper control of these levels ensures a more secure, stable, and organized network.

- **Link speed:**

The link speed in a Wi-Fi wireless network indirectly influences its security, primarily through the amount of data transmitted and the risk of attack exposure. Higher speeds facilitate data transfer, making detecting potential vulnerabilities more difficult if appropriate security measures are not implemented. Additionally, high-speed networks may be susceptible to denial-of-service or deauthentication attacks, as higher traffic volumes can complicate monitoring abnormal behavior. However, high-speed networks, such as those based on the latest standards (Wi-Fi 6 and Wi-Fi 6E), offer advanced security features but require compatible devices to take advantage of these improvements.

Although link speed does not directly affect wireless security, higher speeds can increase the risk if protection mechanisms are not properly managed. The key is to balance network speed with effective security protocols.

- **Type of device:**

Access points (APs) are key devices in wireless networks, with different types that adapt to various coverage and management needs. Standalone APs are autonomous and suitable for small to medium networks, providing security through protocols like WPA3 and WPA2 and authentication with 802.1X. Controller-based APs, on the other hand, are centrally managed, making them ideal for large networks. They allow security policies to be applied uniformly across all connected devices. These APs support mechanisms such as WPA3 and RADIUS for more robust authentication.

Mesh APs provide extended and flexible coverage by interconnecting multiple devices, improving coverage in large spaces and offering advanced security features like traffic encryption between nodes. Dual-Band and Tri-Band APs operate on multiple frequencies (2.4 GHz and 5 GHz, or even 6 GHz in the case of Tri-Band), allowing for higher performance and better traffic management, reducing congestion and improving security. APs with Wi-Fi 6 support significantly improve efficiency and speed, optimizing security by handling multiple devices more effectively and supporting the WPA3 protocol. Finally, Wi-Fi 6E APs expand the spectrum by including the 6 GHz band, which enhances speed and capacity, reduces interference, and increases security in high-demand environments.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

Regarding wireless Wi-Fi security, APs implement various security standards to protect networks. WPA3 is the latest and most secure protocol, providing stronger protection through enhanced authentication and robust data encryption.

The differences in device capabilities are relevant to security, as access points (APs) vary significantly between domestic and business environments, especially regarding security. APs tend to be simpler in homes, with basic features such as WPA2/WPA3, MAC address filtering, and guest networks, suitable for a limited number of devices. In contrast, enterprise APs are more complex, centrally managed, and use advanced technologies such as WPA3 Enterprise, 802.1X authentication with RADIUS servers, network segmentation through VLANs, and security monitoring. These enterprise devices are designed to handle higher traffic, provide controlled access, and protect confidential information through robust security measures.

Security:

- **MAC Address:**

The MAC address is crucial in Wi-Fi devices because it allows control of network access through address filtering, helping to block or allow specific devices. It also facilitates monitoring of connected devices, efficient traffic management, and connection tracking. Although it is not an infallible security mechanism (since MAC addresses can be spoofed), it is used alongside other security methods like WPA2/WPA3 to strengthen network protection. Additionally, it is employed to separate guest networks, allowing limited access without compromising the leading network.

- MAC Filter:

MAC filtering is a security technique that controls access to a Wi-Fi network by authorizing or blocking devices based on their unique MAC address. It can be implemented through whitelist (only allowing authorized devices) or blocklist (blocking specific devices) methods. While it provides additional control over who can access the network, it has limitations, such as the possibility of MAC address spoofing, which can undermine its effectiveness. It is more suitable for small or home networks and should be combined with other security measures, such as WPA3 or 802.1X authentication, to enhance protection.

- IP Filter

IP filtering is a security technique that controls access to a network by authorizing or blocking specific IP addresses, allowing management of incoming and outgoing traffic. It provides detailed control over which devices can communicate with the network, helping to prevent attacks such as DDoS and port scanning. However, it has limitations, such as the possibility of IP address spoofing and the complexity of large networks, where managing many addresses can be complicated. Despite this, it is helpful in firewalls and routers but should be combined with other security measures to be effective.

- DHCP

The DHCP protocol, by assigning dynamic IP addresses to devices on a network, can impact the security of a wireless network if not implemented correctly. It can be vulnerable to attacks such as DHCP Spoofing, where an attacker sets up a fake DHCP server to redirect or intercept traffic, and DHCP starvation, which disrupts network access by exhausting available IP addresses. Additionally, the need for control over assigned IP addresses complicates the implementation of security filters. To mitigate these risks, it is recommended to use WPA3 authentication, protect the DHCP server, and enable features such as DHCP Snooping in enterprise environments.

- WPS UNLOCK

WPS Unlock refers to exploiting a vulnerability in the Wi-Fi Protected Setup (WPS) protocol, which allows an attacker to gain access to a Wi-Fi network through a brute force attack on the 8-digit PIN used to connect devices. This attack can compromise the network's security, allowing the attacker to intercept traffic and access sensitive information. To mitigate these risks, it is recommended to disable the WPS feature on the router. It is essential to ensure that WPS is not

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

enabled by default and to note that, on some devices, disabling it is done via a physical button, while on others, it must be done through the device's settings.

- Firewall /IPS

The use of firewalls and Intrusion Prevention Systems (IPS) in Wi-Fi networks is essential to ensure security against unauthorized access, cyberattacks, and internal threats. The firewall is a barrier that controls incoming and outgoing traffic, protecting the network from intrusions and attacks such as DDoS. On the other hand, the IPS provides additional protection by identifying and blocking attacks in real-time, preventing damage before it occurs. The combined implementation of both systems creates a defense-in-depth approach that significantly enhances the wireless network's security. However, it is vital to configure them correctly to avoid performance impacts, as improper configuration can lead to latency or block legitimate access.

Vulnerability:

- Firmware

Firmware in Wi-Fi devices is crucial for network security, as it controls their operation and protection. If not updated, it may contain exploitable vulnerabilities, weak configurations such as generic passwords or outdated encryption, and a lack of support for new standards. Additionally, it could become a target for persistent malware or contain backdoors. It is essential to keep the firmware updated, configure security settings properly, and periodically audit the device to mitigate risks.

- Web Management

Web management of access points (APs) in Wi-Fi networks can pose serious security risks, such as default credentials, the use of HTTP instead of HTTPS, exposure of the interface on public networks, unnecessary enabling of remote access, and firmware vulnerabilities that allow attacks such as XSS or CSRF. Additionally, insecure sessions and the lack of robust authentication increase the likelihood of intrusion. To mitigate these risks, it is essential to use strong passwords, enable HTTPS, disable unnecessary remote management, restrict access by IP, regularly update firmware, implement multifactor authentication, and audit access logs.

- User Privileges

User privileges in Wi-Fi networks directly affect security by determining access to critical configurations and resources. If not properly managed, they can allow malicious or compromised users to access sensitive information, modify security settings, carry out internal attacks, propagate malware, or access internal networks. The lack of control over privileges makes detecting malicious activities and protecting the network difficult.

- CMD execution

Enabling command execution privileges (CMD execution) on Wi-Fi devices can severely compromise network security, allowing attackers to execute malicious code, modify security settings, access internal devices, and disable protective measures. This can lead to credential theft, theft of sensitive data, installation of backdoors, and complete control over the network. To mitigate these risks, it is essential to disable unnecessary command execution.

4.3. Regulation, Controls, and Best Practices

It is important to consider regulatory aspects, including standards, along with the proper implementation of controls associated with information security. Additionally, it is fundamental to consider publicly known best practices to support Wi-Fi network security. Technological updates should also be regarded as a guiding principle.

Available information focused on securing Wi-Fi Wireless networks

- Standards
- Best Practices
- Checklist

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

The following metrics cover a wide range of information sources that should be considered for supporting the implementation of security measures in Wi-Fi wireless networks.

- IEEE 802.11
- WIFI Alliance
- ISO 27.001
- CIS controls
- NIST 800-53
- Wireless Security Checklist
- Enterprise Wireless Networks Audit
- Framework Cybersecurity (CSF)
- Others (Updated Research)

4.4. Operating Area Characteristics

This section addresses potential scenarios in a real environment from an attacker's perspective, as well as the physical parameters of the location concerning the security of the operating area. From this standpoint, all variables that could influence the outcomes of a successful attack on a Wi-Fi wireless network are included, such as Black Box pentesting audits.

Status of the operational area

The status of the operational area in terms of physical security refers to the evaluation of the conditions and characteristics of the environment in which a Wi-Fi network operates to identify factors that could impact its security. This analysis considers the following key aspects:

Physical security

- Target environment category

Classification of the operational area based on its nature, such as residential, commercial, industrial, or public. Each category has specific risks and security requirements that influence the protection needed for the network.

- Access level to the target

Evaluates the facilities or restrictions that an attacker must overcome to physically access the environment, such as areas open to the public, restricted or controlled zones, and physical barriers (doors, cameras, guards, etc.). A high level of access can facilitate direct attacks on devices, such as routers or access points, while a restricted level adds additional barriers that make exploitation more difficult.

Operational security

- Personal Security
- Biometric Security
- Type of access to the location
- Operating Hours

4.5. Cybersecurity Analysis.

The purpose of this pillar is to conduct research and analysis on cybersecurity, as there exists a gap between the update of 802.11 technology and emerging threats stemming from new needs associated with technological advancements.

Target Analysis

- Technical feasibility analysis
- Type of AP (home or enterprise)
- Type of Antenna
- Type of available equipment

Types of attack

- Verify Trends

Reconnaissance tools

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

- Devices
- Software

Attack tools

- Hardware
- Software

5. Conclusions

In conclusion, this work has confirmed the crucial need to transcend conventional technical standards in the evaluation and design of Wi-Fi networks. The integration of environmental factors and the consideration of a broader range of information sources are revealed as essential elements for a comprehensive understanding. While the literature review exposed a heterogeneous theoretical and methodological basis, it offers significant potential for the unification of criteria in the field.

In response to this landscape, a conceptual and methodological framework was proposed, aimed at facilitating thorough evaluations and a more robust design of Wi-Fi networks. The experimental results support the feasibility of incorporating aspects that are not currently systematically considered.

The validation of the selected variables, based on the empirical experiments conducted in January 2022 and May 2024, confirms their suitability for substantiating the principles of the proposed theoretical framework. The significant differences observed in the effectiveness of auditing tools, specifically between the Pineapple device and the "Wifite" software in Kali Linux, underscore the dependence on the security characteristics of the target device and expose potential vulnerabilities in domestic environments, highlighting an urgent need to strengthen security measures in these contexts.

The experiments revealed a distance limitation of 20 meters for successful handshake capture and a positive correlation between lower temperatures and the success rate of attacks, which underscores the importance of physical proximity and environmental conditions in Wi-Fi network security. This demonstrates that environmental security is a key factor significantly contributing to the Wi-Fi network security evaluation process. This section addresses potential scenarios in a real environment from an attacker's perspective, as well as the physical parameters of the location concerning the security of the operating area. From this viewpoint, all variables that could influence the outcomes of a successful attack on a Wi-Fi wireless network are included, such as Black Box pentesting audits. The "status of the operational area" is defined as the evaluation of the environmental conditions to identify factors that impact Wi-Fi network security.

Finally, the synthesis of the knowledge derived from the literature review and empirical investigations, both in real-world and laboratory settings, culminated in the construction of a robust conceptual and methodological framework for the evaluation and design of wireless Wi-Fi networks. This framework, based on five key pillars, encompasses the essential aspects that influence the auditing process of a wireless Wi-Fi network. The identification and validation of these pillars were significantly enriched by empirical experimentation, allowing for the evaluation of specific aspects related to the integrated variables.

References

1. Yang, H.-C.; Alouini , M.-S. A. Advanced Wireless Transmission Technologies: Analysis and Design. 1ª edición ed. Cambridge CB2 8BS United Kingdom: University Printing House, 2020
2. WiFi Alliance, Available online: https://www.wi-fi.org/who-we-are (accessed on 10 Nov 2024).
3. Van Puyvelde, D.; Brantly, A. Cybersecurity. 1ª edición ed. Medford, USA: Polity Press, 2019.
4. Goralski, W. The Illustrated Network. 2ª edición ed. United States: Morgan Kaufmann, 2017.
5. IEEE, Available online: https://standards.ieee.org/ (accessed on 10 Nov 2024)
6. ISO, Available online: https://www.iso.org/about-us.html (accessed on 10 Nov 2024)
7. NIST, Available online: https://www.nist.gov/ (accessed on 10 Nov 2024)

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 May 2025 doi:10.20944/preprints202505.0690.v1

8. CIS, Available online: https://www.cisecurity.org/about-us/ (accessed on 10 Nov 2024)
9. De Haes, S.; Van Grembergen, W. Enterprise Governance of Information Technology. 2ª edición ed. Belgium: Springer, 2015.
10. Barria, C., Cordero, D., Galeazzi, L.; Acuña, A., Proposal of a Multi-standard Model for Measuring Maturity Business Levels with Reference to Information Security Standards and Controls. Intelligent Methods in Computing, Communications and Control, 1243(978-3-030-53650-3), 2020, pp. 121-132.
11. Karnel, E. Hacking: 4 Books in 1- Hacking for Beginners, Hacker Basic Security, Networking Hacking, Kali Linux for Hackers. 1ª edición ed. United States: Independently Published, 2019.
12. Valchanov, H., Edikyan, J. & Aleksieva, V. An Empirical Study of Wireless Security in City Environment. In Proceedings of ACM Balkan conference in Informatics (BCI'19), 9(11), 2019, pp. 1-4.
13. Osterhage, W. Wireless Network Security. 2ª edición ed. Frankfurt, Germany: CRC Press, 2018.
14. Alan, C. & Steve, W. IT Governance An international guide to data security and ISO27001/ ISO27002. 6ª edición ed. London: KoganPage, 2015.
15. Ávalos, L.G., Huidobro, C.B., Hurtado, J.A. A Review of the Security Information Controls in Wireless Networks Wi-Fi. In: Mata-Rivera, M.F., Zagal-Flores, R., Barria-Huidobro, C. (eds) Telematics and Computing. WITCOM 2020. Communications in Computer and Information Science, vol 1280. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62554-2_30
16. Hurtado, J. Metodología de la Investigación: Guía para una comprensión holística de la ciencia. 4ª edición ed. Caracas: Quirón Ediciones, 2010.
17. Hurtado, J. Cómo formular objetivos de investigación. 3ª edición ed. Caracas: Sypal, 2012.
18. Galeazzi, L., Barría, C., Hurtado, J. (2021). Conceptual Model of Security Variables in Wi-Fi Wireless Networks: Review. In: Latifi, S. (eds) ITNG18th International Conference on Information Technology-New Generations. Advances in Intelligent Systems and Computing, vol 1346. Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-70416-2_8
19. Galeazzi, L., Garrido, C., & Barría, C. (2022, October). Validation of Security Variables for Audits in Wireless Wi-Fi Networks. In International Congress of Telematics and Computing (pp. 422-433). Springer vol 1659, Cham. https://doi.org/10.1007/978-3-031-18082-8_28
20. PlayGoogle, Available online: https://play.google.com/store/apps/details?id=abdelrahman.wifianalyzerpro&hl=es_CL (accessed on 10 Nov 2024).
21. Wigle, Available online: https://wigle.net/ (accessed on 10 Nov 2024).
22. Astudillo, K. Wireless Hacking 101. Babelcube Inc., 2017.
23. El Fiky, A. *Wireless Penetration Testing: Up and Running*. BPB Online, 2023.
24. Google, Available online: https://support.google.com/earth/answer/7365595?hl=en&co=GENIE.Platform%3DAndroid (accessed on 10 Nov 2024).
25. Botwrite, R. Wireless Exploits And Countermeasures: Kali Linux Nethunter, Aircrack-NG, Kismet, And Wireshark, Pastor Publishing Ltd, 2024.
26. Meteored, Available online: https://www.meteored.cl/tiempo-en_Santiago+de+Chile-America+Sur-Chile-Region+Metropolitana+de+Santiago-SCEL-sactual-18578.html (accessed on 10 Nov 2024).
27. Meteored, Available online: https://www.meteored.cl/tiempo-en_Santiago+de+Chile-America+Sur-Chile-Region+Metropolitana+de+Santiago-SCEL-sactual-18578.html (accessed on 10 Nov 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.