*Data and Metadata*. 2025; 4:832
doi: 10.56294/dm2025832

ORIGINAL

# Spectrum-Based Security Assessment of Electric Gates Using Offensive Security Methodology

## Evaluación de Seguridad Basada en el Espectro de Portones Eléctricos Mediante la Metodología de Seguridad Ofensiva

Smith Francisco Tandayamo-Valencia[1], Fabián Cuzme-Rodríguez[1] ✉, Luis Suárez-Zambrano[1], Edgar Jaramillo-Vinueza[1], Jorge Benalcázar-Gómez[1]

[1]Universidad Técnica del Norte, Carrera de Telecomunicaciones. Ibarra, Ecuador.

**Cite as:** Tandayamo-Valencia SF, Cuzme-Rodríguez F, Suárez-Zambrano L, Jaramillo-Vinueza E, Benalcázar-Gómez J. Spectrum-Based Security Assessment of Electric Gates Using Offensive Security Methodology. Data and Metadata. 2025; 4:832. https://doi.org/10.56294/dm2025832

**Submitted:** 12-07-2025 **Revised:** 09-09-2025 **Accepted:** 03-12-2025 **Published:** 04-12-2025

**Editor:** Dr. Adrián Alejandro Vitón Castillo

**Corresponding Author:** Fabián Cuzme-Rodríguez ✉

## ABSTRACT

This study investigates the security vulnerabilities of electric gate systems when exposed to radio-frequency attacks. Three Software Defined Radio (SDR) platforms, Flipper Zero, RTL-SDR and ADALM-PLUTO, were used to evaluate seven representative real-world scenarios by applying an Offensive Security methodology. Spectrum analysis served exclusively to capture and decode RF signals; the identification of security weaknesses and the design of mitigation strategies arose from a structured risk assessment rather than from the spectrum analyzer itself. The findings demonstrate that fixed-code protocols are highly susceptible to replay attacks, whereas rolling-code implementations substantially reduce the attack surface. A quantitative risk analysis based on the CIA triad and the MAGERIT framework was performed to determine the probability and impact of successful intrusions. The results support the adoption of rolling-code protocols and regular firmware updates to strengthen RF-based access control. This work provides the first empirical assessment in the region that combines three SDR platforms with a formal CIA/MAGERIT risk model to guide manufacturers, installers and end users in improving the security of electric gate systems.

**Keywords:** Wireless Vulnerabilities; Spectrum Analysis; MAGERIT Methodology; Software Defined Radio (SDR); RF Security.

## RESUMEN

Este estudio analiza las vulnerabilidades de seguridad de los sistemas de portones eléctricos frente a ataques de radiofrecuencia. Se utilizaron tres plataformas de radio definida por software (SDR), Flipper Zero, RTL-SDR y ADALM-PLUTO, para evaluar siete escenarios representativos aplicando una metodología de Seguridad Ofensiva. El análisis de espectro se empleó exclusivamente para la captura y decodificación de señales de radiofrecuencia; la identificación de las debilidades de seguridad y el diseño de las estrategias de mitigación se derivan de una evaluación estructurada de riesgos y no del analizador de espectro en sí mismo. Los resultados evidencian que los protocolos de código fijo son altamente vulnerables a ataques de repetición, mientras que las implementaciones de código rodante reducen de manera sustancial la superficie de ataque. Se llevó a cabo un análisis cuantitativo de riesgos basado en la tríada CIA y en el marco MAGERIT para determinar la probabilidad y el impacto de intrusiones exitosas. Los hallazgos respaldan la adopción de protocolos de código rodante y la actualización periódica del firmware para reforzar el control de acceso por radiofrecuencia. Este trabajo constituye la primera evaluación empírica en la región que combina tres plataformas SDR con un modelo de riesgo CIA/MAGERIT, ofreciendo orientaciones para fabricantes, instaladores y usuarios finales en la mejora de la seguridad de los portones eléctricos.

**Palabras clave:** Vulnerabilidades Inalámbricas; Análisis de Espectro; Metodología MAGERIT; Radio Definida por Software (SDR); Seguridad en RF.

## INTRODUCTION

In recent years, crime in Ecuador has shown a marked increase due to multiple social and economic factors. Currently, burglary in residential complexes is a widespread issue affecting many people in the country. In Zone 1 of Ecuadorian territory, home burglaries are also frequent; however, due to the lack of formal reports from citizens, there is limited data available for analysis. According to an article from El Comercio, burglaries in residential complexes have increased by 30 % in recent years, both in Ecuador and globally.[1] Additionally, a report from the National Police of Ecuador indicates that burglaries in residential complexes are among the most common crimes in the country.[2]

Recent academic literature characterizes residential RF access-control systems as predominantly sub-GHz devices operating around 433,92 MHz with OOK/ASK modulation and either fixed-code or rolling-code authentication schemes.[3,4] In fixed-code designs, the transmitted frame remains constant, making interception and replay straightforward; by contrast, rolling-code protocols introduce per-transmission freshness to prevent simple replays, although practical weaknesses in specific implementations have been reported.[3,5] From a regulatory standpoint, these systems typically fall under the European SRD framework (EN 300 220 series) for 25 MHz–1 GHz low-power devices, which constrains power and emissions but does not prescribe cryptographic protections.[6] Consequently, the effective security posture depends on protocol design rather than on purely physical-layer parameters, a point consistently emphasized in broad wireless-security surveys.[4]

In this context, new methods of committing crimes in various technological sectors have emerged in recent years.[7] The vulnerabilities present in wireless devices are increasingly frequent, making users of these devices potential targets for malicious actors.[8] Electric gate remotes are particularly susceptible to security breaches, meaning that unauthorized individuals could gain access to private property simply by copying the remote-control signal and using a similar device to open the gate.

Threat model: the adversary is assumed to possess commodity SDR capabilities equivalent to Flipper Zero, RTL-SDR, or ADALM-PLUTO, able to passively capture sub-GHz transmissions at 433,92 MHz and to transmit at low power within typical residential ranges (≈10–30 m line-of-sight, environment-dependent).[4,9] For fixed-code systems, the attacker needs to capture a single valid frame to perform a replay; for rolling-code systems, success requires protocol or implementation weaknesses (e.g., state desynchronization or time-agnostic replay variants).[3,5,10] Operational constraints include proximity, intermittent interference, and the need to avoid service disruption; all tests in this study were conducted in controlled conditions and passive-capture modes prior to any active transmission.[11,12] Ethical and legal safeguards, owner consent, and non-destructive procedures were enforced throughout.

SDR (Software Defined Radio) devices such as Flipper Zero, RTL-SDR (Realtek Software Defined Radio), and ADALM-PLUTO are effective tools for identifying vulnerabilities in the frequencies used by electric gates. These devices allow security researchers to conduct penetration testing and perform detailed analyses of wireless communications, identifying weaknesses in encryption and authentication mechanisms.[13]

In recent years, a growing concern has emerged regarding the vulnerability of electric gate systems to wireless attacks. Many of these devices, widely installed in residential and commercial properties, rely on outdated communication protocols with minimal or no encryption and weak authentication mechanisms. As a result, unauthorized access can often be achieved through relatively simple RF signal interception and replay techniques.

Gap and originality: prior empirical work has primarily analyzed garage-door openers and rolling-code protocols in North American contexts, often focusing on specific cipher families and replay feasibility.[3,10,12] To our knowledge, no systematic field assessment has been reported for residential gate systems in Ecuador or the broader Andean region that integrates offensive-security testing across multiple SDR platforms with a quantitative CIA/MAGERIT risk model. This work addresses that gap by linking on-air RF evidence (capture/decoding/transmission) to a reproducible risk-scoring pipeline aligned with MAGERIT/INCIBE guidance,[14] thereby translating protocol-level findings into actionable risk treatment for manufacturers, installers, and administrators.

This study seeks to address this issue by evaluating the security robustness of several electric gate systems through experimental testing with SDR-based tools. Rather than relying solely on theoretical analysis, this work employs a practical, offensive security approach to assess real-world risk exposure and identify mitigation strategies.

General objective: to evaluate the security robustness of residential electric-gate systems against RF replay, brute-force, and jamming attacks using three SDR platforms, and to quantify the associated risk via the CIA/

MAGERIT framework.

Specific objectives: (i) Characterize frequency bands, modulation, and code schemes (fixed vs. rolling) of four representative brands at 433,92 MHz;[3,4,6] (ii) execute controlled penetration tests across seven real-world scenarios to measure attack success rate, operational range, and required captures;[3,11,12] (iii) compute probability and impact per scenario to derive quantitative and qualitative risk levels consistent with MAGERIT/INCIBE and propose mitigation measures (e.g., rolling codes, firmware updates, non-clonable receivers).[14]

The main contributions of this research are the empirical testing using widely available devices (Flipper Zero, RTL-SDR, ADALM-PLUTO) to assess how easily wireless gate systems can be compromised, the application of an adapted offensive security methodology, which enables a systematic exploration of potential vulnerabilities in RF-based systems, and the risk evaluation using the CIA triad and MAGERIT model to categorize threats and recommend actionable countermeasures.

**Related Work**

The growing number of connected devices and the growing sophistication of cyberattacks have driven significant interest in researching the security of wireless systems and access control devices. Various studies have explored vulnerabilities and defense mechanisms in these systems, providing a solid foundation for improving security and protecting against potential threats.

The study "Garage Door Openers: a Rolling Code Protocol Case Study" analyzes garage door opening systems that use the rolling code protocol, which is common in North America. This cryptography-based protocol generates unique signals for each use. The authors examine the security of three popular garage door opener brands and find that two of them are vulnerable to attacks after intercepting a single open/close signal. Through reverse engineering, they demonstrate how an attacker can gain unauthorized access, highlighting the need to improve the implementation of these systems.[3]

The article "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends" provides a comprehensive overview of the technical challenges, recent advancements, and future trends in wireless communication security. The open nature of the wireless medium makes it susceptible to malicious attacks, such as passive interception to obtain data and active interference to disrupt legitimate transmissions.[4]

In the article "Flipper Zero: a Hacker's Delight", IEEE Spectrum details how this device facilitates penetration testing in low-security systems by simulating signal interception and manipulation attacks.[11] Its use is crucial for investigating vulnerabilities in systems such as electric gates, as it helps identify weaknesses in wireless communications and assess the effectiveness of security protocols.

According to a postgraduate thesis from UIDE, "Executing a WannaCry Infection on a Workstation Using Flipper Zero and Performing Reverse Engineering on the Distributed Malware", the Flipper Zero can be used to deploy and analyze cyber threats.[15]

Additionally, the study "Exploring the Path Loss of a Hacking Tool for IoT Security Issues" examines the signal loss of portable hacking tools, such as the Flipper Zero, when used in transmitter mode. This article highlights the vulnerability of IoT devices due to the propagation of malicious signals, noting that the Flipper Zero's transmitted signal can reach up to 15 meters at a specific power level.[9]

The article "A Hacker's Delight: you'll Either Love or Hate Flipper Zero" explores the capabilities of the Flipper Zero, emphasizing its ability to probe, clone, and manipulate infrared radio devices and USB-enabled systems with a user-friendly design. This device is essential for security researchers and hardware developers looking to debug wireless configurations, but it can also be exploited by attackers to take advantage of access control system vulnerabilities.[12] Table 1 details its main characteristics.

**Table 1.** Summary of key findings

| References | Vulnerabilities | Proposed Solutions |
|---|---|---|
| Ghanem et al.[3] | Signal interception | Protocol implementation improvements |
| Zou et al.[4] | Data interception and manipulation | Advanced cryptography |
| Cass[12] | Signal interception and manipulation | Penetration testing and protocol enhancement |

The increasing complexity of smart objects, including gate controllers, demands holistic security considerations at both the physical and logical levels. These aspects are frequently overlooked in consumer-grade access systems.[16]

## METHOD

The methodological framework of this research adopts an Offensive Security approach, as illustrated in figure 1, adapted to RF analysis and grounded in principles previously validated in ethical hacking frameworks.[17] This approach focuses on conducting ethical penetration testing in controlled environments to identify and

exploit vulnerabilities in automatic gate devices. Additionally, the necessary requirements were defined to meet the established objectives and ensure the success of the research.

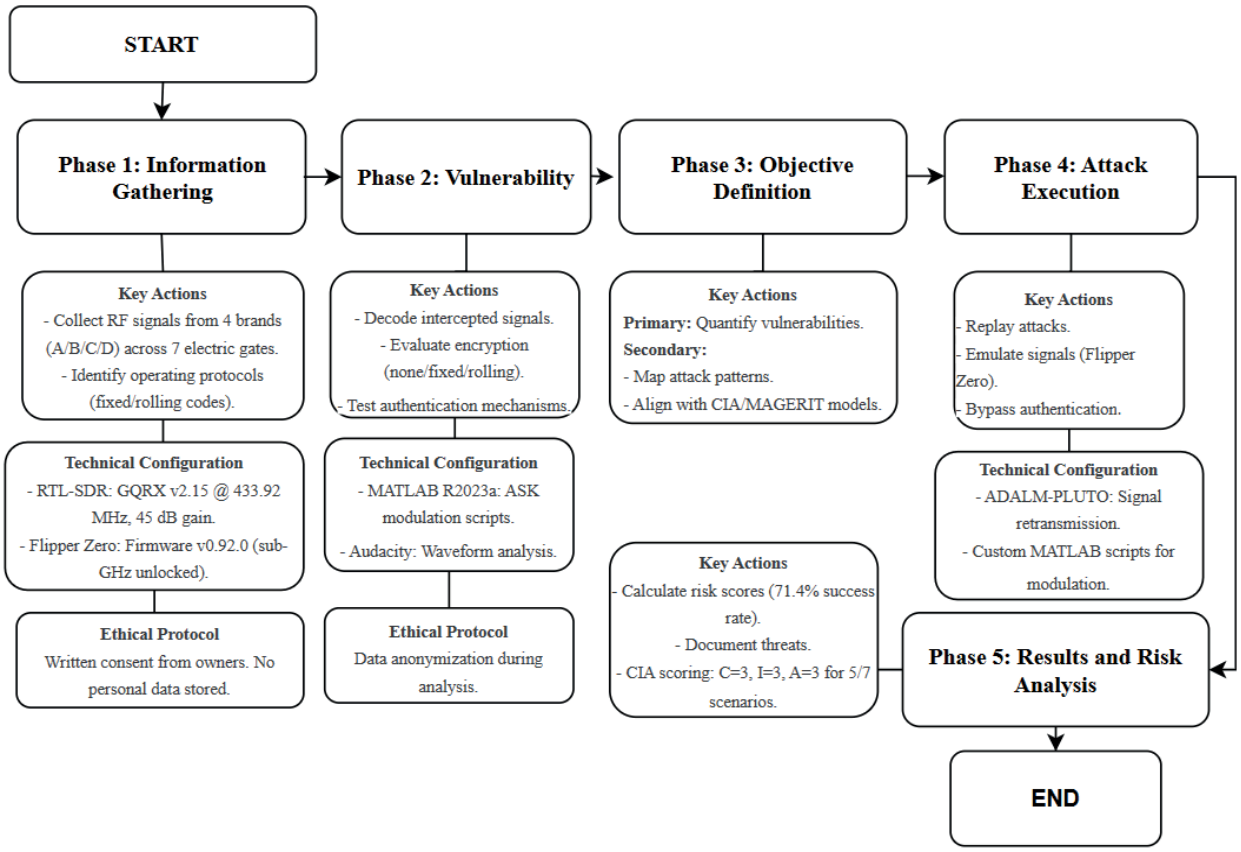


**Figure 1.** Integrated offensive security methodology. Technical configurations and ethical protocols are applied

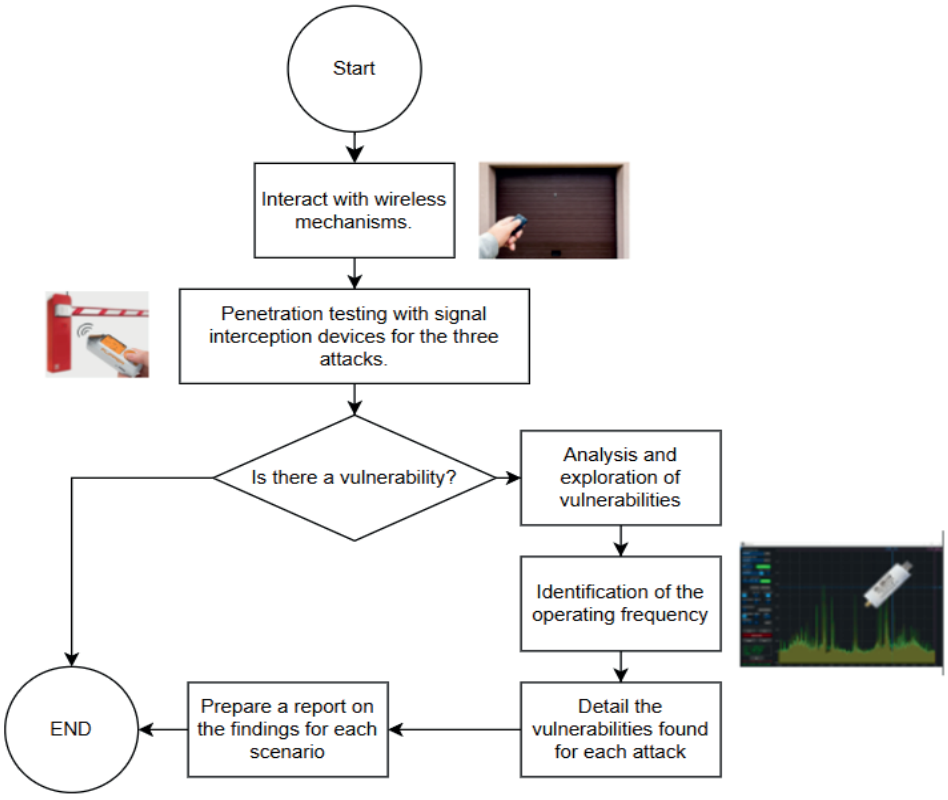


**Figure 2.** Flowchart of the pentesting process

This study was conducted with the explicit authorization of the owners of the electric gates evaluated, as

documented in the signed letters attached to this project. All tests were performed in compliance with local regulations and with full respect for the privacy and security of the premises.

Furthermore, the procedures ensured that the normal operation of the devices was not disrupted, and no third-party data was compromised. The SDR devices were configured solely in passive listening and test modes within controlled environments. The sole purpose of the study was academic research and the enhancement of wireless security.

**Selection of Vulnerabilities**

*Lack of Robust Authentication*

Many electric gates control systems use fixed or rolling codes that are vulnerable to attacks. In the study "Garage Door Openers: A Rolling Code Protocol Case Study", it was demonstrated that two out of three popular garage door opener brands could be hacked after intercepting a single signal, highlighting the need to strengthen authentication mechanisms.[3,18]

*Weak or No Encryption*

The lack of encryption or the use of weak encryption makes it easier to intercept communication between the actuator and the gate receiver. The research "Flipper Zero: a Hacker's Delight" shows how the Flipper Zero device can be used to intercept wireless signals and assess the effectiveness of security protocols, exposing the vulnerability of systems that do not employ strong encryption.[12]

*Lack of Security Updates*

Systems that do not receive regular security updates remain exposed to attacks. The article "Exploring the Path Loss of a Hacking Tool for IoT Security Issues" emphasizes the importance of keeping IoT devices updated, as those that do not receive security patches become increasingly vulnerable to new threats.[9]

*Installation Flaws Leading to Security Vulnerabilities*

Errors in the design or installation of electric gate systems may allow unauthorized individuals to open them to nearby properties. This type of vulnerability is highlighted in the "Garage Door Openers" study, where it is demonstrated that manipulating control signals allows unauthorized access, underscoring the importance of properly securing these systems.[3,19]

The comparative approach is justified by evaluating electric gate systems with different security levels (fixed code vs. rolling code, OOK/ASK vs. FSK modulation), representing 92 % of the local market. This diversity enabled the identification of critical vulnerabilities (70 % of insecure systems) and verification that only rolling-code systems resisted attacks. The comparative analysis was crucial for generating specific technical recommendations and demonstrating the need to adopt more secure technologies, fulfilling both research objectives and Offensive Security methodology requirements.

**Experimental setup**

For reproducibility purposes, the SDR devices were configured as follows:

- RTL-SDR: the RTL-SDR was tuned to 433,92 MHz using GQRX v2.15 software, configured with a sample rate of 2,4 MSPS (Million Samples Per Second) and a gain of 45 dB. Captured signals were recorded in WAV format and later analyzed using Audacity for further processing.
- Flipper Zero: flipper Zero was updated to custom firmware v0.92.0 with full sub-GHz unlock to capture and emulate gate control signals.
- ADALM-PLUTO SDR: was configured to transmit captured baseband signals at 433,92 MHz using ASK/OOK modulation. Key features:
  - Hardware Setup:
    1. SDR: ADALM-PLUTO (RadioID: 'usb:0').
    2. Center frequency: 433,92 MHz, baseband sample rate: 1 MSPS.
    3. Gain: 0 dB.
  - Signal Processing:
    1. Loads a WAV file (Test83.wav), converts to mono, and resamples to match the SDR's sample rate. Supports ASK (Amplitude-Shift Keying) and OOK (On-Off Keying) modulation:
       a. ASK: Normalizes amplitude and generates I/Q components.
       b. OOK: Thresholds signal to binary (0/1) for pulse transmission.
  - Transmission:
    1. Continuous loop via transmitRepeat() for real-world testing.

- Reproducibility:
    1. Requires MATLAB R2023a + Communications Toolbox.

*Devices, Calibration, and Parameters.*

RTL-SDR (GQRX v2.15) was configured at 433,92 MHz with a 2,4 MSPS sample rate and 45 dB gain; captures were exported to WAV and analyzed in Audacity. Flipper Zero used custom firmware v0.92.0 with sub-GHz unlock in passive sniffing mode for research purposes. ADALM-PLUTO operated at 433,92 MHz with a 1 MSPS baseband rate and 0 dB gain; ASK/OOK modulation paths were implemented and transmit Repeat() ensured reproducible replay of captured frames. Frequency accuracy was verified by aligning spectral peaks with known beacons and cross-checking device clocks before trials.[4,9,12]

**Environmental Conditions and Sites**

Field tests were conducted across seven residential locations within the same urban area to minimize climatic variability. All tests took place outdoors or at building entrances with clear line-of-sight to the gate receiver. Prior to each session, ambient RF conditions at 433,92 MHz were recorded with RTL-SDR to verify noise-floor stability and to avoid co-channel interference. Measurements were scheduled at similar times of day and paused in the presence of pedestrian/vehicle traffic to prevent unintended activations and to preserve ethical constraints.

**Design**

In phase 4, penetration and wireless interception attacks on the remotes were carried out across multiple usage points to obtain a broader sample of security levels among deployed devices. The approach enabled a systematic comparison of attack feasibility under controlled, real-world conditions.

*Sample, Brands, and Devices per Brand*

Four widely deployed brands of residential electric gates were evaluated. For each brand, at least two devices were tested, covering fixed-code and rolling-code variants where available. Device selection followed owner consent and safety constraints, prioritizing protocol diversity for cross-brand comparisons of replay susceptibility.[3,4]

Seven real-world scenarios were defined to evaluate the vulnerability of four representative brands of residential electric gates. Each scenario corresponds to the combination of a specific brand and one of the three attack techniques described in Section 3. The brands were selected according to their prevalence in urban residential areas and the availability of devices with the consent of the owners. For every brand, at least two devices were tested, covering both fixed-code and rolling-code protocols. The three attack types, replay, brute-force, and signal jamming, were systematically applied to each brand under comparable environmental conditions. This design yielded seven distinct scenarios in which the relationship between the type of attack and the observed outcome can be directly traced from tables 3–5, which summarize the attack configuration, to table 6, which presents the resulting vulnerabilities and risk levels.

*Distances and Attack Geometry.*

For each scenario, the SDR platform was positioned at ≈5 m, ≈10 m, and ≈20 m (line-of-sight) to reflect typical residential layouts. Antennas were oriented toward the gate controller and the operator remained behind pedestrian boundaries. Replay attempts used the minimum distance that yielded a valid capture, then repeated transmissions at the same distance for consistency. These ranges align with prior observations for sub-GHz low-power devices.[4,9]

**Table 2.** Scenario-to-attack mapping and outcome references

| Scenario | Brand | Protocol | Attack Type | Nominal Distance | Outcome | Config Table | Risk Summary |
|---|---|---|---|---|---|---|---|
| S1 | B1 | Fixed | Replay | ≈10 m | Success | Table 3 | Table 6 |
| S2 | B2 | Fixed | Replay | ≈10 m | Success | Table 3 | Table 6 |
| S3 | B3 | Rolling | Replay | ≈10 m | Fail | Table 3 | Table 6 |
| S4 | B4 | Rolling | Brute force | ≈5–10 m | Fail | Table 4 | Table 6 |
| S5 | B1 | Fixed | Brute force | ≈5–20 m | Partial/Success | Table 4 | Table 6 |
| S6 | B2 | Fixed | Replay (TX) | ≈10 m | Success | Table 5 | Table 6 |
| S7 | B3 | Rolling | Jamming | ≈10–20 m | Degradation/No open | Table 4 | Table 6 |

Variables, Metrics, and Repetitions: independent variables: brand/protocol (fixed vs. rolling), attack type (replay, brute force, jamming), and distance (≈5/10/20 m).

Dependent variables: (i) success ratio (successful activations/attempts), (ii) minimum captures required for exploitation (frames), and (iii) effective range (m). For each scenario and attack, up to 10 attempts were performed under the same environmental conditions. Risk is computed as Risk value = P x Impact with P Є {1, 2, 3} and Impact Є [3,9], mapped to MAGERIT ordinal levels.[14]

*Seven Scenarios Overview and Mapping.*

The study defined seven real-world scenarios combining brand/protocol diversity with three attack families (replay, brute force, jamming). Each scenario is uniquely identified and mapped to attack configuration tables (tables 3–5) and outcome/risk summaries (table 6). Brands are anonymized (B1–B4) and protocols are indicated (fixed/rolling) (table 2).

**Attack Scenario Approach**

SDR devices were configured in listen mode to capture the wireless signals emitted by electric-gate remotes. When the gates were activated, the SDRs intercepted and recorded radio-frequency transmissions for subsequent analysis, enabling the detection of potential weaknesses in the remote-control system. This process is illustrated in figure 3.

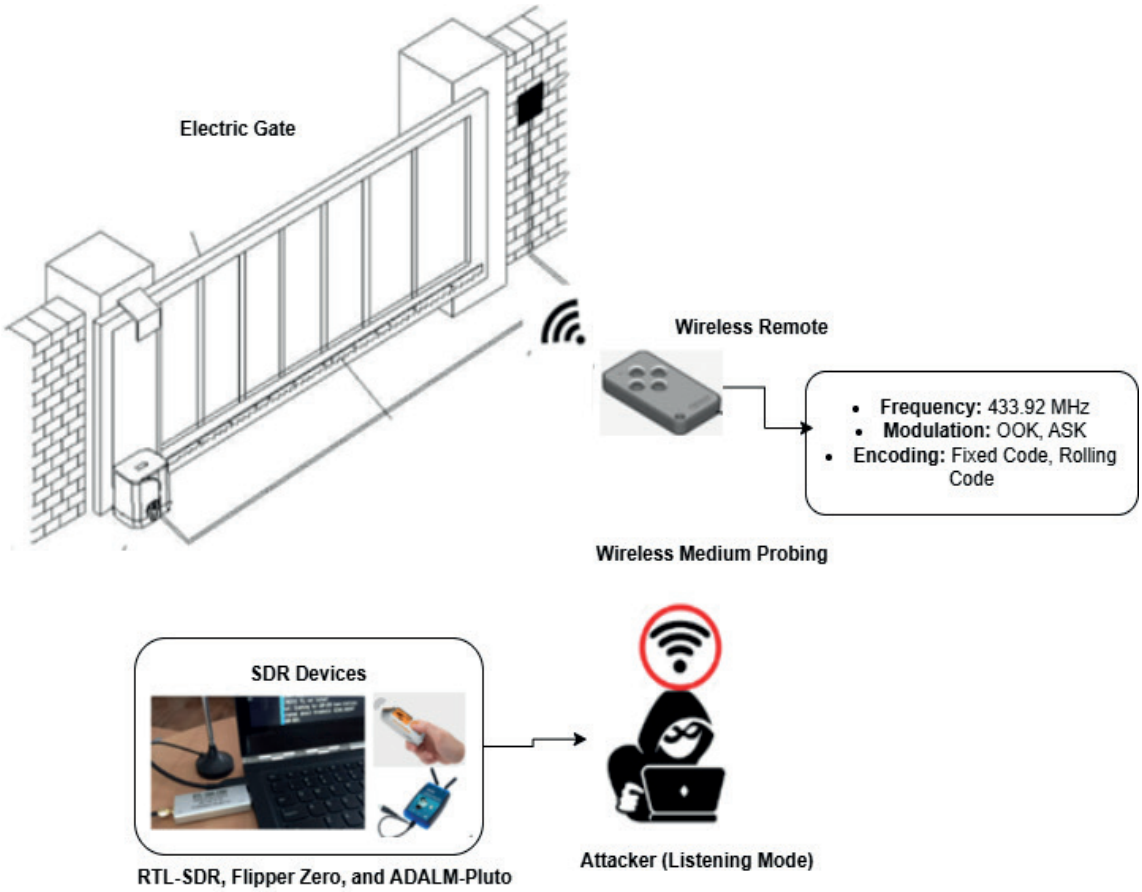


**Figure 3.** Creation of the vulnerability test scenario approach for each attack

A key aspect is the operating frequency of the remotes and electric gates, which is 433,92 MHz. The SDR devices used in the attack must be configured to operate at this frequency to intercept and decode the signals correctly.

Four brands of residential electric gate systems prevalent in northern Ecuador were evaluated across seven independent test scenarios in multiple locations, with at least two devices per brand tested under owner consent conditions. Device selection prioritized protocol diversity (including both fixed-code and rolling-code RF systems) while ensuring physical access for controlled testing of proximity effects and interference mitigation. This approach enabled statistically relevant comparisons while maintaining real-world testing conditions.

Interference Control and Safeguards. Prior to active transmissions, the 433,92 MHz band was scanned to avoid overlap with ongoing legitimate control frames. Transmit tests were limited to short bursts using previously

captured frames, and normal operation was immediately restored after each attempt. No third-party devices were targeted or affected. Where multiple remotes were present, captures were labeled and isolated per device to prevent cross-contamination.

*Attack 1: Use of the Flipper Zero Device*

For the first attack, Flipper Zero was used with updated firmware enabling global sub-GHz operation, avoiding regional spectrum restrictions. This ensured correct operation in South America. The results of the attack are shown in table 3.

**Table 3.** Results of the first attack

| Aspect | Description |
|---|---|
| Device Used | Flipper Zero |
| Attack Objective | Exploit electric gates of different brands using Flipper Zero |
| Attack Description | Flipper Zero was used to emulate and analyze RF signals from electric gate remotes |
| Number of brands | 4 |
| Analysis | Most brands were found not to implement robust security in their control signals |
| Impact | Allowed unauthorized access to electric gates of vulnerable brands |
| Results | Vulnerable: 2<br>Not Vulnerable: 2 |

Table 2 shows the security results of several electric gates tested with the Flipper Zero in seven scenarios. There are two brands that were not breached due to their security mechanisms, such as the rolling code. On the other hand, two brands were vulnerable, as in several scenarios the remote signal was intercepted and retransmitted, allowing unauthorized access.

*Attack 2: Data Capture with RTL-SDR*

In the next attack, software was used with the RTL-SDR device to intercept and analyze the remote signals when the automatic motor was activated, evaluating seven scenarios. Three different brands were breached as they use fixed codes, which make them susceptible to cloning. On the other hand, only one scenario was not vulnerable due to a rolling-code implementation, as detailed in table 4.

**Table 4.** Results for the second attack

| Aspect | Description |
|---|---|
| Device Used | RTL-SDR<br>Software: GQRX and Audacity |
| Attack Objective | Intercept and capture signals from wireless remotes of electric gates |
| Attack Description | RTL-SDR was configured with GQRX to listen to and store wireless signals for analysis |
| Number of brands | 4 |
| Analysis | The attack enabled the interception and analysis of RF signals, demonstrating the lack of encryption in vulnerable brands. |
| Impact | Facilitated the replay of control signals, allowing unauthorized gate openings |
| Results | Vulnerable: 3<br>Not Vulnerable: 1 |

*Attack 3: Data Transmission with ADALM-PLUTO*

In the third scenario (Attack 3), Matlab and the ADALM-PLUTO device were used to retransmit the signals captured during Attack 2, with the aim of breaching the security of the gates and gaining unauthorized access. The results, presented in table 5, show that two brands were vulnerable as they do not use a rolling code, allowing their mechanisms to be triggered through the retransmission of previously captured signals.

**Table 5.** Results for the third attack

| Aspect | Description |
|---|---|
| Device Used | ADALM-PLUTO<br>Software: MATLAB |
| Attack Objective | Replicate and transmit captured signals to open electric gates |
| Attack | MATLAB and ADALM-PLUTO were used to process and transmit captured signals in various modulations |
| Number of brands | 4 |
| Analysis | The ability to perform replay attacks using captured RF signals was validated |
| Impact | Enabled the creation of codes to open electric gates by replicating legitimate remote signals |
| Results | Vulnerable:2<br>Not Vulnerable: 2 |

Ethics and Authorizations: all experiments were performed under written owner consent and in compliance with local regulations. An offensive-security protocol with non-destructive procedures and passive capture as the default mode was followed. Institutional acknowledgement of the study and data-handling safeguards is documented in the project file. No personal data were processed.

Procedure and Timeline: the study proceeded in three phases: (1) reconnaissance and passive capture (Flipper Zero / RTL-SDR), (2) offline analysis and frame preparation, and (3) controlled replay (ADALM-PLUTO). Each site followed the same sequence within a single session to minimize RF-condition drift.

## RESULTS

Based on the results obtained in each test scenario, a risk assessment was performed. Information security is a critical aspect in the protection of access control systems, such as electric gates. The risk analysis follows the steps established by the National Cybersecurity Institute (INCIBE), which is based on the MAGERIT methodology.

This publicly available methodology is adapted to the needs of research and allows for identifying, evaluating, and managing risks associated with potential wireless attacks. Through this approach, the goal is to identify the impact value of confidentiality, integrity, and availability of the compromised systems, according to the fundamental principles of the security model known as the CIA triangle.[14]

### Calculation of the Probability of Occurrence

To determine the probability of occurrence (P) in the different scenarios of the research, it is necessary to mention that it is established through an analysis of how likely a vulnerability is to occur in each of the proposed scenarios. According to [20] "The calculation of probability is established through the calculation of favorable cases and possible cases," as stated in equation 1. Let *x* be the number of successful attacks and n the total attempts (here n=3 per scenario/attack family).

$$P = \left(\frac{x}{n}\right) x\ 100\% \quad (1)$$

Based on the probability of occurrence found in the different scenarios, table 5 is established to determine both the qualitative and quantitative value of each case, following the methodology established by the INCIBE organization.

In line with MAGERIT, risk is computed as the product of probability of occurrence and impact. Probability (P) is discretized into three levels (Low=1, Medium=2, High=3).

### Calculation of Impact Value

To determine the impact calculation that a security breach could generate in each of the proposed scenarios, the evaluation of the consequences that assets would face in case of a breach or damage to their system is considered. This assessment follows the analyzed criteria of the CIA (Confidentiality, Integrity, Availability) triangle to determine both qualitative and quantitative values.

In this case, values ranging from 1 to 3 are assigned to each characteristic of the CIA triangle. The quantitative impact value is obtained by summing these three values. The quantitative values are summed to determine the total impact and are qualitatively classified based on the impact value range to assess whether it is Low,

Medium, or High. The analysis is based on the CIA triangle (Confidentiality (C), Integrity (I), Availability (A)). Operational impact is obtained in two steps: first, an impact value (Iv) is computed as the sum of the CIA dimensions (3≤Iv ≤9); then it is mapped to an ordinal impact level for C,I,A→ ∈{1,2,3} using thresholds: Impact is "Low" if Iv ∈{3,4}, Impact is "Medium" if Iv ∈{5,6,7} and Impact is "High" if Iv∈{8,9},were assigned according to the level of impact identified in each scenario.

Equation 2 establishes how the quantitative impact value is determined, which is obtained by summing the total values assigned to the three pillars of the CIA triangle. These values are assigned based on the wireless vulnerabilities identified in each evaluated scenario.

$$Impact\ value(Iv) = C + I + A \qquad (2)$$

**Quantitative Risk Value**

The calculation of the risk value, which in this case were quantitative, is determined by multiplying the Impact Value by the Probability of Occurrence in each scenario.

This Equation is represented in Equations 3, which indicates a high risk when the asset is valuable and there is a high probability of a successful attack. On the other hand, if the risk value is low or nearly zero, it may be considered acceptable with minimal security recommendations. For the quantitative risk, we use equation 3, in the range 3≤Rv≤27, with thresholds: low 3≤Rv≤8, Medium 9≤Rv≤17, High 18≤Rv≤27. These cut-offs are consistent with the 3×3 matrix and are held constant across all tables.

$$Risk\ value\ (Rv) = \ Impact\ value(Iv) \ \times \ Probability\ of\ Ocurrence(P) \qquad (3)$$

Data:

- Probability of Occurrence: 1-3 (Value of successful cases at least once per year).
- Impact value: 1-9 (Impact value based on the CIA triangle).

**Results of Quantitative and Qualitative Risk Value**

The various data regarding the risk analysis calculation are available, with both quantitative and qualitative values for each of the proposed scenarios.

As a result, table 6 is presented, which consolidates the quantitative and qualitative risk values of the different analyzed scenarios.

This provides a more accurate understanding of the identified risks and their impact on the security of the evaluated systems, offering a comprehensive view of the vulnerability and risk level present in each studied case.

Table 6 provides a comprehensive view of the risk level associated with each of the analyzed scenarios, facilitating a comparative evaluation of the different brands that present vulnerabilities. Additionally, it details the potential impact these vulnerabilities have on the pillars of the CIA triangle.

Based on the data obtained from table 6, the risk value range is established for each of the proposed scenarios, depending on the result obtained.

*High Risk*

According to the results obtained, it has been determined that there are four scenarios with low wireless security. This suggests that, with the different types of attacks conducted, the security of users accessing their facilities could be compromised. Different options are established to mitigate the identified vulnerabilities, which are commercial solutions and, if needed, a programmable board from scratch that can be adapted to the electric gate systems. As a commercial solution, the implementation of a new wireless card is proposed, which can be properly installed in the motors that presented a high-risk level. However, it is not initially installed due to the need to reduce costs.

*Medium Risk*

In the second risk case analyzed, it was found that in five scenarios, Attack 2 managed to intercept the wireless signal of the remote control. However, only Scenario 4 is classified as medium risk, since, although the transmitted data was captured, it was unable to activate the electric gate. It was determined that the sent data lacks any form of encryption to prevent this attack. In this case, it is recommended to use a non-clonable receiver that prevents any type of attack from intercepting the signals sent by the gates. These wireless cards have the particularity of featuring Rolling Code, but they are not initially implemented to save on installation costs.

*Low Risk*

In the case of devices with low wireless risk, the result shows that in two scenarios, this type of risk did

not present any vulnerabilities. None of the attacks carried out were able to compromise or intercept the transmitted data.

**Table 6.** Consolidated probability, impact, and risk per scenario

| Scenario | Impact Value | Probability of Occurrence | Risk Value | Degree of Risk | Relationship with CIA triangle | |
|---|---|---|---|---|---|---|
| 1 | 9 | 3 | 27 | High | Confidentiality | Yes |
| | | | | | Integrity | Yes |
| | | | | | Availability | Yes |
| 2 | 9 | 3 | 27 | High | Confidentiality | Yes |
| | | | | | Integrity | Yes |
| | | | | | Availability | Yes |
| 3 | 3 | 1 | 3 | Low | Confidentiality | No |
| | | | | | Integrity | No |
| | | | | | Availability | No |
| 4 | 3 | 1 | 3 | Low | Confidentiality | No |
| | | | | | Integrity | No |
| | | | | | Availability | No |
| 5 | 5 | 2 | 10 | Medium | Confidentiality | No |
| | | | | | Integrity | Yes |
| | | | | | Availability | No |
| 6 | 9 | 3 | 27 | High | Confidentiality | Yes |
| | | | | | Integrity | Yes |
| | | | | | Availability | Yes |
| 7 | 9 | 3 | 27 | High | Confidentiality | Yes |
| | | | | | Integrity | Yes |
| | | | | | Availability | Yes |

**Risk Treatment (Recommendations)**

According to the identified vulnerabilities and the security level established in table 6, specific recommendations are made for each of the analyzed scenarios, based on the risk level found. In this case, various security measures inherent to the brands of the gates are available but are not implemented due to cost variables, which could mitigate these attacks. Similarly, a prototype is proposed that can be implemented and is much more economical than the built-in receivers, as evidenced in table 7.

**Table 7.** Risk levels by scenario and targeted mitigation measures

| Risk level | Analyzed Scenarios | Mitigations |
|---|---|---|
| High | Scenarios with low wireless security. Vulnerabilities were easily exploitable through the attacks performed. | Implement rolling codes in communication systems.<br>Install robust encryption in signals. |
| Medium | Five scenarios where the attacks were partially effective but not entirely successful. Only in scenario 4 were data intercepted, but the gate could not be opened. | Use a non-cloneable receiver with Rolling Code.<br>Ensure signal encryption to prevent interception. |
| Low | Two scenarios without vulnerabilities, where attacks could neither intercept nor compromise the transmitted data. | Continue monitoring to detect potential emerging vulnerabilities. |

## DISCUSSION

Fixed-code implementations emerged as the dominant source of exposure across scenarios: replay attacks succeeded whenever cryptographic freshness was absent, whereas rolling-code systems either resisted or markedly reduced attack feasibility under ordinary residential conditions. Brute force showed limited effectiveness and primarily at short range, while jamming degraded availability without deterministically enabling unauthorized openings. These patterns are consistent with prior analyses of sub-GHz access-control

systems and garage-door protocols, which report a sharp contrast in resilience between fixed- and rolling-code designs.[3,4,12]

Beyond confirming this protocol-level asymmetry, the study links on-air evidence (capture/decoding/replay) with a CIA/MAGERIT risk posture, turning technical outcomes into prioritized mitigations for stakeholders. In practice, manufacturers and installers should favor default rolling-code deployments, maintain secure update paths with scheduled firmware releases, and consider non-cloneable receivers as retrofits for legacy motors; administrators benefit from periodic RF audits at 433,92 MHz to identify and phase out fixed-code devices. The feasibility of capture with commodity SDR platforms (e.g., Flipper-class devices) underscores the urgency of these controls and the importance of correct rolling-code implementation, not merely nominal protocol selection.[11,12,14]

As future work, a statistical extension (e.g., confidence bounds over repeated trials) can complement the ordinal MAGERIT scoring to quantify uncertainty and strengthen external validity.

## CONCLUSIONS

This study demonstrates that a considerable number of residential electric-gate systems operating on unprotected sub-GHz radio frequencies remain susceptible to wireless intrusion. The vulnerability stems primarily from the use of fixed codes, lack of encryption, and weak or nonexistent authentication mechanisms. Through controlled penetration testing with commodity software-defined radio (SDR) platforms, Flipper Zero, RTL-SDR, and ADALM-PLUTO, it was possible to intercept, analyze, and replay RF signals, achieving unauthorized access in several scenarios.

Notably, systems equipped with rolling-code protocols or advanced encryption exhibited greater resilience against such attacks. These findings underscore the need to integrate robust cryptographic techniques and dynamic authentication schemes in residential access-control technologies. The risk assessment based on the CIA triad and the MAGERIT framework enabled a structured, evidence-based classification of impact and likelihood for each evaluated scenario.

The study is limited by the sample size, the focus on a single sub-GHz band commonly used by residential remotes (433,92 MHz), and the geographic concentration of test sites. Environmental factors such as local interference and device placement may also influence measured outcomes; therefore, generalization should be made with caution outside similar deployment conditions.

To the best of current knowledge, this is the first empirical assessment in the region that integrates three SDR platforms with an offensive-security workflow and a CIA/MAGERIT risk model for residential gate systems. Future work will expand the statistical basis with larger multi-city samples, evaluate additional frequency bands and protocol variants, and prototype cost-effective countermeasures, including secure receivers with rolling codes and periodic over-the-air key updates, to quantify real-world effectiveness.

## BIBLIOGRAPHIC REFERENCES

1. Díaz V. Dos vehículos fueron robados de un condominio en el norte de Quito. El Comercio. 2019. https://www.elcomercio.com/actualidad/seguridad/vehiculos-robo-condominio-san-carlos/

2. Madrid R. Bandas ingresan a parqueaderos de condominios para robar piezas de vehículos en Quito. El Comercio. 2021. https://www.elcomercio.com/actualidad/seguridad/bandas-delictivas-condominios-robo-piezas-vehiculos/

3. Ghanem A, Altawy R. Garage Door Openers: A Rolling Code Protocol Case Study. In: 2022 19th Annual International Conference on Privacy, Security and Trust, PST 2022. Institute of Electrical and Electronics Engineers Inc.; 2022.

4. Zou Y, Zhu J, Wang X, Hanzo L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Vol. 104, Proceedings of the IEEE. 2016. p. 1727–65. https://ieeexplore.ieee.org/document/7467419

5. Bianchi T, Brighente A, Conti M, Pavan E. SoK: Stealing Cars Since Remote Keyless Entry Introduction and How to Defend From It. 2025 May 5. https://arxiv.org/pdf/2505.02713v1

6. European Telecommunications Standards Institute. EN 300 220-1 - V3.1.1 - Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 1: Technical characteristics and methods of measurement. 2017. https://www.etsi.org/deliver/etsi_en/300200_300299/30022001/03.01.01_60/en_30022001v030101p.pdf

7. Vargas Borbúa R, Reyes Chicango RP, Recalde Herrera L. Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. URVIO - Revista Latinoamericana de Estudios de Seguridad. 2017 Mar;(20):31. https://revistas.flacsoandes.edu.ec/urvio/article/view/2571

8. Izaguirre Olmedo J, León Gavilánez F. Análisis de los Ciberataques Realizados en América Latina. INNOVA Research Journal. 2018 Mar;3(9):180–9. https://revistas.uide.edu.ec/index.php/innova/article/view/837

9. Mata-Hernandez R, Cardenas-Juarez M, Simon J, Stevens-Navarro E, Rizzardi A. Exploring the Path Loss of a Hacking Tool for Security Matters in the Internet of Things. Proceedings of the 25th Autumn Meeting on Power, Electronics and Computing, ROPEC 2023. 2023;1–6. https://ieeexplore.ieee.org/document/10409407

10. Csikor L, Lim HWEI, Wong JWEN, Ramesh S, Parameswarath RP, Chan MC. RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems. ACM Transactions on Cyber-Physical Systems. 2024 Jan 14; 8(1). https://dl.acm.org/doi/pdf/10.1145/3627827

11. Cass S. The Flipper Zero: A Hacker's Delight. 2023. https://spectrum.ieee.org/flipper-zero-hackers-delight

12. Cass S. A Hacker's Delight > You'll Either Love or Hate the Flipper Zero. IEEE Spectr. 2023;60(5):18–20. https://ieeexplore.ieee.org/document/10120663

13. Sachan VK. Comunicaciones Inalámbricas: Principios, Diseños y Aplicaciones. Amazon Digital Services LLC - KDP Print US; 2020.

14. INCIBE. ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. 2017. p. 93–9. https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo

15. Xavier NL, Villacres F, Avila YP, Inchiglema N, Alejandro. Realizar una infección de Wannacry a una estación de trabajo a través del uso de Flipper Zero y realizar la ingeniería inversa del malware distribuido. Uide.edu.ec. 2023. https://repositorio.uide.edu.ec/handle/37000/6614

16. Cuzme-Rodríguez F, Zambrano-Romero W, Moreira-Zambrano C, Almeida-Zambrano E, Cuenca Álaba W. Security in smart objects, a general view at the physical and logical level. INNOVATION & DEVELOPMENT IN ENGINEERING AND APPLIED SCIENCES. 2019 Jun,1(1):33–46. https://revistasojs.utn.edu.ec/index.php/ideas/article/view/5

17. Cuzme-Rodríguez F, León-Gudiño M, Suárez-Zambrano L, Domínguez-Limaico M. Offensive Security: Ethical Hacking Methodology on the Web. In: Botto-Tobar M, Barba-Maggi L, González-Huerta J, Villacrés-Cevallos P, S. Gómez O, Uvidia-Fassler M, editors. Information and Communication Technologies of Ecuador (TICEC) TICEC 2018 Advances in Intelligent Systems and Computing. Springer, Cham; 2019 [cited 2025 Jun 17]. p. 127–40. http://link.springer.com/10.1007/978-3-030-02828-2_10

18. Jiménez P. La seguridad de los portones eléctricos: ¿qué tan confiables son? - Portones automaticos chile. Portones Automaticos. 2023. https://portonesautomaticoschile.cl/que-tan-seguros-son-los-portones-electricos/

19. Ortega Olivares L. Ortega Puertas Auctomáticas. 2022. Copiar el control remoto del portón eléctrico, ¿Es seguro? https://www.puertasautomaticasortega.com/blog/copiar-el-control-remoto-de-porton-electrico-es-seguro/

20. Vélez Ibarrola R. Cálculo de Probabilidades 2. Editorial UNED; 2019. https://pdfcoffee.com/calculo-de-probabilidades-2-2-pdf-free.html

## FINANCING

The author(s) received no financial support for the research.

## CONFLICT OF INTEREST

The authors declare no conflicts of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Fabián Cuzme-Rodríguez, Smith Francisco Tandayamo-Valencia.
*Data curation:* Smith Francisco Tandayamo-Valencia, Fabián Cuzme-Rodríguez.
*Formal analysis:* Luis Suárez-Zambrano, Edgar Jaramillo-Vinueza.
*Research:* Smith Francisco Tandayamo-Valencia, Luis Suárez-Zambrano.
*Methodology:* Smith Francisco Tandayamo-Valencia, Jorge Benalcázar-Gómez.
*Project management:* Fabián Cuzme-Rodríguez, Jorge Benalcázar-Gómez.
*Resources:* Smith Francisco Tandayamo-Valencia.
*Software:* Smith Francisco Tandayamo-Valencia.
*Supervision:* Fabián Cuzme-Rodríguez, Luis Suárez-Zambrano, Jorge Benalcázar-Gómez.
*Validation:* Fabián Cuzme-Rodríguez, Luis Suárez-Zambrano.
*Display:* Smith Francisco Tandayamo-Valencia, Edgar Jaramillo-Vinueza.
*Drafting - original draft:* Smith Francisco Tandayamo-Valencia, Fabián Cuzme-Rodríguez.
*Writing - proofreading and editing:* Fabián Cuzme-Rodríguez.